

Leitfäden der angewandten Mathematik
und Mechanik LAMM

This book is intended for advanced undergraduate and beginning graduate students in theoretical computer science and mathematics. It presents a theory of formal languages with main emphasis on rational transductions and families of context-free languages

Context-free languages, Rational and recognizable sets, Rational transductions and transducers

Rational functions, Unambiguous representations, Sequential and subsequential transducers

Families of languages, Rational cones and full AFLs, Linear languages, One counter languages, Quasi-rational or nonexpansive languages

Operators on families of languages, Principal families, Generators, Infinite chains of cones

Iterative pairs, Systems of iterative pairs, Transfer theorems and applications



B.G. Teubner Stuttgart

ISBN 3-19-02340-7

519.7
Ber

UNIVERSITAT AUTÒNOMA DE BARCELONA
Servei de Biblioteques



1500002284

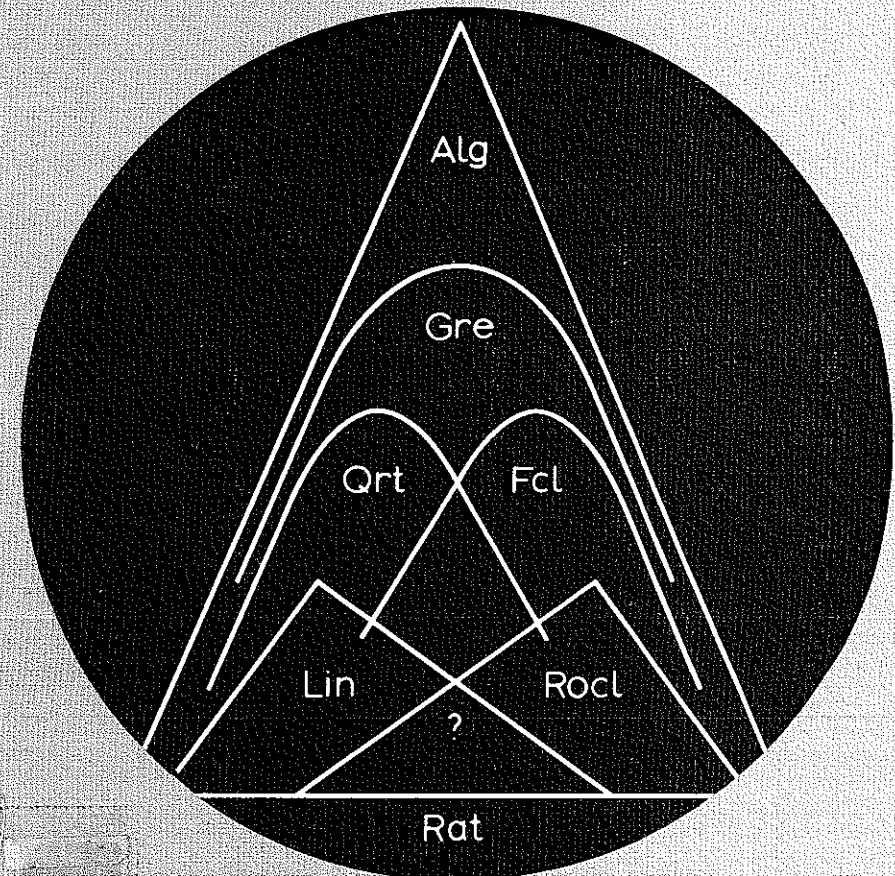
nbücher



Informatik

Transductions and Context-Free Languages

J. Berstel
**Transductions and
Context-Free Languages**



Leitfäden der angewandten Mathematik und Mechanik LAMM

Unter Mitwirkung von

Prof. Dr. E. Becker, Darmstadt

Prof. Dr. G. Hotz, Saarbrücken

Prof. Dr. P. Kall, Zürich

Prof. Dr. K. Magnus, München

Prof. Dr. E. Meister, Darmstadt

Prof. Dr. Dr. h. c. F. K. G. Odqvist, Stockholm

Prof. Dr. Dr. h. c. Dr. h. c. Dr. h. c. E. Stiefel †

herausgegeben von

Prof. Dr. Dr. h. c. H. Görtler, Freiburg

Band 38

Die Lehrbücher dieser Reihe sind einerseits allen mathematischen Theorien und Methoden von grundsätzlicher Bedeutung für die Anwendung der Mathematik gewidmet; andererseits werden auch die Anwendungsgebiete selbst behandelt. Die Bände der Reihe sollen dem Ingenieur und Naturwissenschaftler die Kenntnis der mathematischen Methoden, dem Mathematiker die Kenntnisse der Anwendungsgebiete seiner Wissenschaft zugänglich machen. Die Werke sind für die angehenden Industrie- und Wirtschaftsmathematiker, Ingenieure und Naturwissenschaftler bestimmt, darüber hinaus aber sollen sie den im praktischen Beruf Tätigen zur Fortbildung im Zuge der fortschreitenden Wissenschaft dienen.

Transductions and Context-Free Languages

By Dr. Jean Berstel

Professor at the Université P. et M. Curie, Paris

With 32 figures, 158 exercises
and numerous examples



B. G. Teubner Stuttgart 1979

R. 18.345

Prof. Jean Berstel

Born in 1941 at Nîmes (France). From 1961 to 1966 studies in mathematics at the University of Paris. 1967 Thèse de troisième cycle, 1972 Thèse d'Etat at the University of Paris. From 1970 to 1972 Chargé d'Enseignement at the University of Strasbourg. Since 1972, Maître de Conférence, then Professor at the Institut de Programmation, University of Paris VI. During the Summer Semester 1976 on leave at the University of Saarbrücken. Activity: Mathematics and Theoretical Computer Science.

CIP-Kurztitelaufnahme der Deutschen Bibliothek

Berstel, Jean:

Transductions and context-free languages / by Jean Berstel. – Stuttgart : Teubner, 1979. –

(Leitfäden der angewandten Mathematik und Mechanik ; Bd. 38) (Teubner Studienbücher : Informatik)

ISBN 3-519-02340-7

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically those of translation, reprinting, re-use of illustrations, broadcasting, reproductions by photocopying machine or similar means, and storage in data banks.

Under § 54 of the German Copyright Law where copies are made for other than private use, a fee is payable to the publisher, the amount of the fee to be determined by agreement with the publisher.

© B. G. Teubner, Stuttgart 1979

Printed in Germany

Setting: The Universities Press (Belfast) Ltd., Belfast

Printer: J. Beltz, Hemsbach/Bergstr.

Cover design: W. Koch, Sindelfingen

Preface

This book presents 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 [1971], 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. There, the structures of "rational cone" and "full AFL" are introduced, and some general results are established. The chapter ends with the treatment of several examples of cones of linear languages. Chapter VI contains a theory of operators on families of languages, setting up an algebraic framework for transformation and comparison of families of languages. Other general results on cones and full AFLs are easily derived from a series of inequalities involving only operators. Chapter VII is concerned with the study of principal cones and full AFLs, that is families generated by one language only. Main interest is in subcones of the context-free languages. First, several languages are proved to generate the entire cone of context-free languages. Then S. Greibach's "Syntactic Lemma" is proved and used to exhibit nonprincipal cones. A detailed study of two important families follows, namely the family of one counter and the family of quasi-rational (nonexpansive, derivation-bounded $\cdot \cdot \cdot$) languages. Chapter VIII presents a general method (due to Boasson and Beauquier) for proving strict containment or incompara-

bility of cones of context-free languages, using iterative pairs and systems of iterative pairs. This method yields easy proofs of the existence of several wellknown and of new hierarchies of cones of context-free languages, showing thus the intimate connection between iterative pairs and the structure of context-free languages.

Main interest is in languages rather than in grammars or in acceptors. Indeed, a language (even a context-free one) exists independently from the grammars generating it, and a great number of context-free languages can be described by a combinatorial or an algebraic property, without any reference to a grammar. Moreover, grammatical characterizations of classes of languages usually require just the existence of one grammar of some special type. Thus to prove that a given language is not in the family, one must show that all grammars generating it violate some property. This is usually a very delicate proof. Finally there are results which are proved by the method of iterative pairs and which cannot be proved—up to now—by considering only grammars.

Rational cones are treated in greater detail than full AFLs. They are indeed in a natural relationship with rational transductions; further full AFLs are a secondary structure in the sense that any full AFL is the rational closure of some cone. Since we are mainly concerned with context-free languages, a description of AFLs and “trios” (in opposition to full AFLs and rational cones) seemed unnecessary, all the more as some fundamental results such as the Syntactic Lemma are still lacking for these families.

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 and 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 also 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

I Preliminaries

I.1 Some Notations	9
I.2 Monoids, Free Monoids	9
I.3 Morphisms, Congruences	12
I.4 Finite Automata, Regular Languages	15

II Context-Free Languages

II.1 Grammars, Languages, Equations	22
II.2 Closure Properties, Iteration	31
II.3 Dyck Languages	35
II.4 Two Special Languages	47

III Rational Transductions

III.1 Recognizable Sets	51
III.2 Rational Sets	55
III.3 Rational Relations	61
III.4 Rational Transductions	65
III.5 Examples	72
III.6 Transducers	77
III.7 Matrix Representations	80
III.8 Decision Problems	87

IV Rational Functions

IV.1 Rational Functions	92
IV.2 Sequential Transductions	96
IV.3 The Cross-Section Theorem	111
IV.4 Unambiguous Transducers	114
IV.5 Bimachines	123
IV.6 A Decidable Property	128

V Families of Languages

V.1 Definition	134
V.2 Rational Equivalence, Rational Cones	135
V.3 Rationally Closed Families	138
V.4 Full AFLs	141

V.5 Substitution	145
V.6 Example: The Cone of Linear Languages	150
V.7 Examples of Incomparable Languages.	156
VI Operators	
VI.1 Operators	162
VI.2 Examples of Operators	164
VI.3 Closure Operators	166
VI.4 Subcommutative Relations	171
VI.5 Marked Substitution	177
VII Generators	
VII.1 Generators of the Context-Free Languages	185
VII.2 The Syntactic Lemma.	194
VII.3 Substitution Closure	197
VII.4 One Counter Languages	201
VII.5 Quasi-Rational Languages	208
VIII Iterative Pairs	
VIII.1 Types of Iterative Pairs.	219
VIII.2 Grammatical Pairs	223
VIII.3 Transfer of Iterative Pairs	227
VIII.4 Systems of Iterative Pairs	232
VIII.5 Grammatical Systems	237
VIII.6 Transfer of Systems	246
VIII.7 Applications.	251
IX Open Problems, Further Developments	265
Bibliography	268
List of Symbols	274
Index.	275

I Preliminaries

This chapter is a short review of some basic concepts used in the sequel. Its aim is to agree on notations 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.

I.1 Some Notations

$\mathbb{N} = \{0, 1, 2, \dots\}$ is the set of nonnegative integers. $\mathbb{Z} = \{\dots -2, -1, 0, 1, \dots\}$ is the set of integers. Let E be a set. Then $\text{Card}(E)$ is the number of its elements. The empty set is denoted by $\emptyset$. If A, B are subsets of E , then we write $A \subset B$ iff $x \in A \Rightarrow x \in B$, and $A \subsetneq B$ iff $A \subset B$ and $A \neq B$. Further

$$A \setminus B = \{x \in E \mid x \in A \text{ and } x \notin B\}.$$

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 , i.e. the powerset of E , is denoted by $\mathfrak{P}(E)$ or 2^E . With the preceding convention, $E \subset \mathfrak{P}(E)$.

The domain $\text{dom}(\alpha)$ of a partial function $\alpha: E \rightarrow F$ is the set of elements x in E for which $\alpha(x)$ is defined. α 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 $\text{dom}(\alpha) = \{x \in E \mid \alpha(x) \neq \emptyset\}$.

I.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 $m_1, m_2, m_3 \in M$, $m_1(m_2 m_3) = (m_1 m_2)m_3$. A neutral element or a unit is an element $1_M \in M$ (also noted 1 for short) such that $1_M m = m 1_M = m$ for all $m \in M$. A semi-group which has a neutral element is a monoid. The neutral element of a monoid is unique. Indeed, if $1'$ is another neutral element then $1' = 1'1 = 1$.

Given two subsets A, B of a monoid M , the product AB is defined by

$$AB = \{c \in M \mid \exists a \in A, \exists b \in B : c = ab\}. \quad (2.1)$$

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

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

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

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

$$u = (x_1, x_2, \dots, x_n) \quad (n \geq 0) \quad (2.2)$$

of elements of X . If $v = (y_1, \dots, y_m)$ is another element of X^* , the product uv is defined by concatenation, i.e.

$$uv = (x_1, x_2, \dots, x_n, y_1, \dots, y_m).$$

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

$$u = x_1 x_2 \cdots x_n.$$

Because of this, u is called a word, $x \in X$ is called a letter and X itself is called an alphabet. By the convention $x = (x)$, X can be considered as a subset of X^* . This justifies the notation X^* , since indeed X^* is the only submonoid of X^* containing X . Further $X^+ = X^* \setminus 1$. 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 X^* generated by an alphabet X . A (formal) language over X is any subset of X^* . The length $|u|$ of a word $u \in X^*$ is the number of letters composing it. The neutral element of X^* is called the empty word, and is noted 1 or ε . It is the only word of length 0. Clearly $|uv| = |u| + |v|$. If $Y \subset X$, then $|u|_Y$ is the number of occurrences of letters $y \in Y$ in u . Thus

$$|u| = \sum_{x \in X} |u|_x.$$

The reversal of a word $u = x_1 x_2 \cdots x_n$ ($n \geq 0, x_i \in X$) is denoted by $\tilde{u}$ or u^r and is defined by $\tilde{u} = x_n x_{n-1} \cdots x_2 x_1$. Clearly $\tilde{\tilde{u}} = u$, $\tilde{1} = 1$, $(uv)^r = \tilde{v} \tilde{u}$. For $A \subset X^*$, $\tilde{A} = \{\tilde{u} \mid u \in A\}$. If $B \subset X^*$, then $(AB)^r = \tilde{B} \tilde{A}$, and $(A^*)^r = (\tilde{A})^*$.

Let $u \in X^*$. Then a word v is a factor of u if $u = avb$ for some $a, b \in X^*$. If $a = 1$, then v is a left factor; if $b = 1$, then v is a right factor of u . v is a proper factor (left factor, right factor) 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 $u = avb$. If $u' = a'v'b'$ is another factorization, then the segment v' is contained in the segment v iff a is a left factor of a' and b is a right factor of b' . Finally v is a subword of u iff $u = w_0 x_1 w_1 \cdots x_n w_n$, ($n \geq 0, x_1, \dots, x_n \in X, w_0, \dots, w_n \in X^*$) and $v = x_1 \cdots x_n$.

Let M be a submonoid of X^* . Then $A = (M \setminus 1) \setminus (M \setminus 1)^2$ is a system of generators of M , i.e. $A^* = M$. Further A is minimal with this property, i.e. $B^* = M$ implies $B \supset A$. A submonoid M of X^* is free with base C if any word $u \in M$ has one and only one factorization $u = c_1 c_2 \cdots c_n$, with $n \geq 0$ and $c_1, \dots, c_n \in C$. The base of a free submonoid M is unique and is equal to $(M \setminus 1) \setminus (M \setminus 1)^2$. Thus X^* is free with base X . A base of a free submonoid is called a code. Examples of codes are supplied by prefix and suffix sets. A subset A of X^+ is prefix iff $AX^+ \cap A = \emptyset$, i.e. if A contains no proper left factor of some of its word, and A is suffix iff $X^+ A \cap A = \emptyset$. A is bifix if it is both prefix and suffix. Any prefix or suffix subset is a code.

Let M be any monoid, and let $A, B \subset M$. The left and right quotients $B^{-1}A$ and AB^{-1} are the sets

$$B^{-1}A = \{c \in M \mid \exists a \in A, \exists b \in B : a = bc\},$$

$$AB^{-1} = \{c \in M \mid \exists a \in A, \exists b \in B : a = cb\}.$$

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 iff v is a right factor of u ; thus uM^{-1} is the set of left factors 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 multiplication;
- (iii) the multiplication is distributive with respect to the addition:

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

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

If M is a monoid, then $\mathfrak{B}(M)$ 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 $(m_1, m_2)(m'_1, m'_2) = (m_1 m'_1, m_2 m'_2)$.

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

2.3 Let M be a monoid, and let $A, B, C \in M$. Prove the following formulas: $(AB)^{-1}C = B^{-1}(A^{-1}C)$; $(A^{-1}B)C^{-1} = A^{-1}(BC^{-1})$.

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

2.5 Let X be an alphabet, and let $a, b \in X^+$. Show that the three following conditions are equivalent:

- (i) $a = d^r$, $b = d^s$ for some word d and $r, s \geq 1$;
- (ii) $ab = ba$;
- (iii) $a^m = b^n$ for some $m, n \geq 1$.

2.6 Two words a and b are conjugate if $ac = cb$ for some word c . Show that this equation holds iff $a = uv$, $b = vu$, $c = (uv)^k u$ for some words u, v , and $k \geq 0$.

2.7 A word a is primitive iff it is not a nontrivial power of another word, i.e. if $a = d^n$ implies $n = 1$.

- a) Show that any word $a \neq 1$ is a power of a unique primitive word.
- b) Show that if a and b are conjugate, and a is primitive, then b is also primitive.
- c) Show that if $ac = cb$ and $a \neq 1$, then there are unique primitive words u, v , and integers $p \geq 1$, $k \geq 0$, such that $a = (uv)^p$, $b = (vu)^p$, $c = (uv)^k u$.

I.3 Morphisms, Congruences

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

$$\alpha(m_1 m_2) = \alpha(m_1) \alpha(m_2) \quad \text{for all } m_1, m_2 \in M \quad (3.1)$$

$$\alpha(1_M) = 1_{M'}.$$

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

$$\alpha(A \cup B) = \alpha(A) \cup \alpha(B); \quad \alpha^{-1}(A' \cup B') = \alpha^{-1}(A') \cup \alpha^{-1}(B'),$$

$$\alpha^{-1}(A' \cap B') = \alpha^{-1}(A') \cap \alpha^{-1}(B'); \quad \alpha(\alpha^{-1}(A') \cap B) = A' \cap \alpha(B).$$

Next if α is a semigroup morphism, then

$$\alpha(AB) = \alpha(A)\alpha(B), \quad \alpha(A^+) = (\alpha(A))^+.$$

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

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

Let X, Y be alphabets, and let $\alpha: X^* \rightarrow Y^*$ be a morphism. Then α is called:

alphabetic if $\alpha(X) \subset Y \cup 1$;

strictly alphabetic if $\alpha(X) \subset Y$;

continuous or ε -free if $\alpha(X) \subset Y^+$;

a projection if $Y \subset X$, and if $\alpha(y) = y$ for $y \in Y$, $\alpha(x) = 1$ for $x \in X \setminus Y$.

Thus projections are particular alphabetic morphisms.

If $\alpha: X^* \rightarrow Y^*$ is an alphabetic morphism, then

$$\alpha^{-1}(AB) = \alpha^{-1}(A)\alpha^{-1}(B), \quad \alpha^{-1}(A^+) = (\alpha^{-1}(A))^+ \quad \text{for } A, B \subset Y^*.$$

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

$$Z = \{x \in X \mid \alpha(x) = 1\} = \alpha^{-1}(1) \cap X; \quad Z_y = \{x \in X \mid \alpha(x) = y\} = \alpha^{-1}(y) \cap X$$

for $y \in Y$.

$$\text{Then } \alpha^{-1}(1) = Z^*, \quad \alpha^{-1}(y) = Z^* Z_y Z^* \quad (y \in Y).$$

If $g = y_1 \cdots y_n$ ($y_i \in Y$), then

$$\alpha^{-1}(g) = Z^* Z_{y_1} Z^* Z_{y_2} Z^* \cdots Z^* Z_{y_n} Z^*.$$

Thus $\alpha^{-1}(g_1 g_2) = \alpha^{-1}(g_1) \alpha^{-1}(g_2)$ for all $g_1, g_2 \in Y^*$. This completes the proof. Note that the formula $\alpha^{-1}(A^*) = (\alpha^{-1}(A))^*$ is only true if further α is continuous, or if $1 \in A$ i.e. $A^* = A^+$.

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

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

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

Thus if $\alpha: Y^* \rightarrow X^*$ is an alphabetic morphism, the function α^{-1} is a substitution iff $\alpha^{-1}(1) = 1$. A substitution σ is extended to $\mathfrak{P}(X^*)$ by the convention

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

For sake of simplicity, we write $\sigma: X^* \rightarrow Y^*$ for a substitution from X^* into Y^* . If $\tau: Y^* \rightarrow Z^*$ is another substitution, then the function $\tau \circ \sigma$ from X^* into Z^* is a substitution.

Finally we note that any finitely generated monoid is a homomorphic image of a free monoid. Consider indeed a monoid M , and let $S = \{m_1, \dots, m_k\}$ be a system of generators of M . Set $X = \{x_1, \dots, x_k\}$, and define a morphism $\alpha: X^* \rightarrow M$ by $\alpha(x_i) = m_i$ for $i = 1, \dots, k$. Then $\alpha(X^*) = (\alpha(X))^* = S^* = M$. 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 θ 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 $x \sim y$, $x \equiv y$ if no confusion can arise. If $E = F$, then θ is a relation over E . Relations are ordered by (set) inclusion.

Let M be a monoid. A congruence over M is an equivalence relation θ which is compatible with the monoid operation, i.e. which satisfies

$$m_1 \equiv m'_1 \pmod{\theta}, m_2 \equiv m'_2 \pmod{\theta} \Rightarrow m_1 m_2 \equiv m'_1 m'_2 \pmod{\theta}. \quad (3.2)$$

For each $m \in M$, the class of $m \pmod{\theta}$ is

$$[m]_{\theta} = \{m' \in M \mid m \equiv m' \pmod{\theta}\}.$$

Then (3.2) is equivalent to

$$[m_1]_{\theta} [m_2]_{\theta} \subset [m_1 m_2]_{\theta}.$$

If θ 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/θ . Conversely, if $\alpha: M \rightarrow M'$ is a morphism, then the relation θ defined by

$$m \sim m' \pmod{\theta} \text{ iff } \alpha(m) = \alpha(m')$$

is a congruence. The number of equivalence classes of an equivalence relation θ is the index of θ . The index is a positive integer or infinite.

Given a relation θ over a monoid M , the congruence $\hat{\theta}$ generated by θ is the least congruence containing θ . The congruence $\hat{\theta}$ can be constructed as follows: Define a relation θ_1 on M by

$$\begin{aligned} m \sim m' \pmod{\theta_1} \text{ iff } m &= uav, \quad m' = ubv, \\ &\text{and } (a \sim b \pmod{\theta} \text{ or } b \sim a \pmod{\theta}). \end{aligned}$$

Next define a relation θ_1^* by $m \equiv m' \pmod{\theta_1^*}$ iff there exist $k \geq 0$ and $m_0, \dots, m_k \in M$ such that $m = m_0$, $m' = m_k$ and $m_i \sim m_{i+1} \pmod{\theta_1}$ for $i = 0, \dots, k-1$. Then it is easily shown that $\theta_1^* = \hat{\theta}$.

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

$$xy \sim yx \quad \text{for } x, y \in X, \quad x \neq y.$$

Let $\hat{\theta}$ be the congruence generated by this relation. Then $u \equiv v \pmod{\hat{\theta}}$ iff $|u|_x = |v|_x$ for all $x \in X$. The quotient monoid $X^*/\hat{\theta}$ is denoted by $X^{\oplus}$ and is called the free commutative monoid generated by X .

Exercises

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

3.2 Give examples of morphisms $\alpha: X^* \rightarrow Y^*$, such that $\alpha^{-1}(AB) \not\subseteq \alpha^{-1}(A)\alpha^{-1}(B)$, and $\alpha^{-1}(A^*) \not\subseteq (\alpha^{-1}(A))^*$.

3.3 Let X, Y be alphabets and let $\alpha: X^* \rightarrow Y^*$ be a morphism. Show that there are an alphabet Z , an injective morphism $\beta: X^* \rightarrow Z^*$ and a projection $\gamma: Z^* \rightarrow Y^*$ such that $\alpha = \gamma \circ \beta$.

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

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

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

$$d(A, B) = \|A \setminus B \cup B \setminus A\|.$$

a) Show that $\|\cdot\|$ and d are a norm and a distance in the usual topological sense, and that d satisfies the ultrametric inequality: $d(A, B) \leq \max\{d(A, C), d(C, B)\}$.

b) Let $\alpha: X^* \rightarrow Y^*$ be a morphism. Show that the mapping from $\mathfrak{P}(X^*)$ into $\mathfrak{P}(Y^*)$ defined by α is continuous for this topology iff $\alpha(X) \subset Y^+$. (This is the reason why an ε -free morphism is called continuous.)

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

$$u \equiv v \pmod{\theta_L} \text{ iff for all } f, g \in X^*: f u g \in L \Leftrightarrow f v g \in L.$$

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

3.6 Let M, N be monoids, $\alpha: M \rightarrow N$ a morphism. Let $A \subset M$, $Q \subset N$, and set $B = \alpha(A)$, $P = \alpha^{-1}(Q)$. Show that $A^{-1}P = \alpha^{-1}(B^{-1} \cdot Q)$.

I.4 Finite Automata, Regular Languages

In this section, we review some basic facts concerning finite automata, mainly in order to fix notations 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 $\mathbf{A} = \langle X, Q, q_-, Q_+, \delta \rangle$ consists of an alphabet X , 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 $\delta: Q \times X \rightarrow Q$.

If no confusion can arise, we denote δ by a dot, and we write

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

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

$$q \cdot 1 = q \quad (4.1)$$

$$q \cdot ux = (q \cdot u) \cdot x \quad u \in X^*, x \in X. \quad (4.2)$$

Then the formula

$$q \cdot uv = (q \cdot u) \cdot v \quad u, v \in X^* \quad (4.3)$$

is easily verified. A word $u \in X^*$ is recognized or accepted by $\mathbf{A}$ iff $q_- \cdot u \in Q_+$. The language recognized by $\mathbf{A}$ is

$$|\mathbf{A}| = \{u \in X^* \mid q_- \cdot u \in Q_+\}. \quad (4.4)$$

A language $L \subset X^*$ is recognizable or regular iff $L = |\mathbf{A}|$ for some finite automaton $\mathbf{A}$.

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

Example 4.1 Let $\mathbf{A}$ be defined by $X = \{x, y\}$, $Q = \{1, 2, 3, 4\}$, $q_- = 1$, $Q_+ = \{4\}$, and the next state function given by

	x	y
1	2	1
2	1	3
3	4	1
4	2	3

Then $\mathbf{A}$ is represented in Fig. I.1. A word is recognized by $\mathbf{A}$ iff it has xyx as a right factor. Thus $|\mathbf{A}| = X^*xyx$.

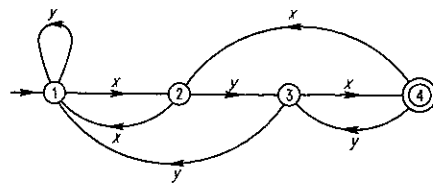


Fig. I.1

The following result is known as Kleene's Theorem.

Theorem 4.1 (Kleene [1956]) *The family of regular languages over X is equal to the least family of languages over X 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 III.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 $\sigma: X^* \rightarrow Y^*$ is called regular iff $\sigma(x)$ is a regular language for all $x \in X$.

There are several variations for the definition of finite automata. Thus in a nondeterministic finite automaton, the next state function is a function from $Q \times X$ into the subsets of Q . Thus $q \cdot x \subset Q$ for $q \in Q$, $x \in X$. This notation is extended by defining first

$$Q' \cdot x = \bigcup_{q \in Q'} q \cdot x \quad \text{for } Q' \subset Q. \quad (4.5)$$

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

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

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

Example 4.2 Fig. I.2 represents a nondeterministic finite automaton $\mathbf{A}$, with alphabet $X = \{x, y\}$. It is easily verified that $|\mathbf{A}| = X^*xyx$.

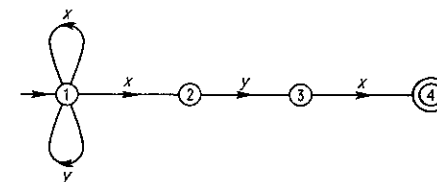


Fig. I.2

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

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

$$q \equiv q' \text{ iff for all } u \in X^*, \quad q \cdot u \in Q_+ \Leftrightarrow q' \cdot u \in Q_+.$$

This equivalence relation is easily seen to be right regular, i.e. to verify $q \equiv q', w \in X^* \Rightarrow q \cdot w \equiv q' \cdot w$. Hence a next state function can be defined on the quotient set $Q/\equiv$ by $[q] \cdot x = [q \cdot x]$ ($[q]$ is the class of q in the equivalence). Let $L = |A|$, and let

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

be the quotient automaton with the next state function defined above. Then it can be shown that $|A/\equiv| = |A|$, and that the accessible part of $A/\equiv$ 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 $S = \langle X, Q, q_- \rangle$ is defined as a finite automaton, but without specifying the set of final states. There is a language recognized by S for any subset $Q' \subset Q$, defined by $|S(Q')| = \{u \in X^* \mid q_- \cdot u \in Q'\}$. Semiautomata are used to recognize "simultaneously" several regular languages: Consider two (more generally any finite number) regular languages $A, B \subset X^*$, and let $A = \langle X, Q, q_-, Q_+ \rangle$, $B = \langle X, P, p_-, P_+ \rangle$ be finite automata with $|A| = A$, $|B| = B$. Define a semiautomaton $S = \langle X, Q \times P, (q_-, p_-) \rangle$ by

$$(q, p) \cdot x = (q \cdot x, p \cdot x) \quad x \in X, \quad (q, p) \in Q \times P.$$

Then $A = |S(Q_+ \times P)|$ and $B = |S(Q \times P_+)|$. Usually only the accessible part of S is conserved in this construction.

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

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

$$K = (UX^* \cap X^*V) \setminus X^*WX^*$$

$$\text{or } K = 1 \cup (UX^* \cap X^*V) \setminus X^*WX^*.$$

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 $X^2 \setminus W$ is called the set of authorized transitions.

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

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

$$Z = \{(q, x, q \cdot x) \mid q \in Q, x \in X\}$$

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

$$U = \{(q, x, q \cdot x) \mid q = q_-\}, \quad V = \{(q, x, q \cdot x) \mid q \cdot x \in Q_+\}$$

$$W = \{(q_1, x_1, q_1 \cdot x_1)(q_2, x_2, q_2 \cdot x_2) \mid q_1 \cdot x_1 \neq q_2\}$$

and set $K = (UZ^* \cap Z^*V) \setminus Z^*WZ^*$. Then for $n \geq 1$,

$$c = (q_1, x_1, q_1 \cdot x_1)(q_2, x_2, q_2 \cdot x_2) \cdots (q_n, x_n, q_n \cdot x_n) \in K \quad (4.6)$$

$$\text{iff } q_1 = q_-, \quad q_{i+1} = q_i \cdot x_i \quad i = 1, \dots, n-1, \quad q_n \cdot x_n \in Q_+. \quad (4.7)$$

Consequently $\alpha(c) = x_1 x_2 \cdots x_n \in L$. Conversely, if $u = x_1 x_2 \cdots x_n \in L$, ($n \geq 1, x_i \in X$), then there are states $q_1, \dots, q_n$ such that (4.7) holds, and in view of (4.6), $u \in \alpha(K)$. Thus $L = \alpha(K)$ if $1 \notin L$. If $1 \in L$, 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 $L \subset X^*$ is regular iff there exist a finite monoid M , a morphism $\alpha: X^* \rightarrow M$, 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 $A = \langle X, Q, q_-, Q_+ \rangle$ such that $L = |A|$. For each word w define a mapping $\bar{w}: Q \rightarrow Q$ 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

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

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

Let α be the function from X^* into the (finite!) monoid Q^Q of all functions from Q into Q defined by $\alpha(w) = \bar{w}$. Then α 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 $w \in L$ iff $q_- \cdot w \in Q_+$, thus iff $\alpha(w) \in R$. Consequently $L = \alpha^{-1}(R)$.

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

$$m \cdot x = m\alpha(x) \quad m \in M, \quad x \in X.$$

Since α is a morphism, $m \cdot w = m\alpha(w)$ for all $w \in X^*$. Consequently $w \in |A|$ iff $1_M\alpha(w) = \alpha(w) \in R$, thus iff $w \in \alpha^{-1}(R)$. ■

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 proved by Ogden (Lemma II.2.3). Let X be an alphabet, and consider a word

$$f = x_1 x_2 \cdots x_n \quad (x_i \in X).$$

Then a position in f is any integer $i \in \{1, \dots, n\}$. Given a subset I of $\{1, \dots, n\}$, a position i is called marked with respect to I iff $i \in I$.

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

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

Proof. Let $A = \langle X, Q, q_-, Q_+ \rangle$ be a finite automaton recognizing L , and set $N = \text{Card}(Q)$. Let $f = x_1 x_2 \cdots x_n$, ($x_i \in X$) be a word in L , and consider a choice $I \subset \{1, \dots, n\}$ of at least N marked positions in f . Since $\text{Card}(I) \geq N$, 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

$$f = g_0 g_1 \cdots g_N g_{N+1}$$

$$\text{by} \quad g_0 = x_1 \cdots x_{i_1-1}, \quad g_1 = x_{i_1}, \quad g_k = x_{i_{k-1}+1} \cdots x_{i_k} \quad (k=2, \dots, N), \\ g_{N+1} = x_{i_N+1} \cdots x_n.$$

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

$$q_0 = q_- \cdot g_0, \quad q_k = q_{k-1} \cdot g_k \quad (k=1, \dots, N), \quad q_+ = q_N \cdot g_{N+1}.$$

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

$$a = g_0 g_1 \cdots g_i, \quad u = g_{i+1} \cdots g_j, \quad b = g_{j+1} \cdots g_{N+1}.$$

Then $q_- \cdot a = q_- \cdot au = q_- \cdot au^m = q_j$ for all $m \geq 1$, whence $q_- \cdot au^m b = q_+$ for all $m \geq 0$, and $au^*b \subset L$. Next u contains exactly $j-i$ marked positions. Since $0 < j-i \leq N$, this proves the lemma. ■

If the marked positions in f are chosen to be consecutive, the same proof gives the following corollary.

Corollary 4.6 *Let $L \subset X^*$ be a regular language. Then there exists an integer $N \geq 1$ such that for any word $f \in L$, and for any factorization $f = hgh'$ with $|g| \geq N$, g admits a factorization $g = aub$ such that*

- (i) $0 < |u| \leq N$;
- (ii) $hau^*bh' \subset L$.

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

Corollary 4.7 *Let $L \subset X^*$ be a regular language, and let $Y \subset X$. Then there is an integer $N \geq 1$ such that for any $f \in L$, and for any factorization $f = hgh'$ with $|g|_Y \geq N$, g admits a factorization $g = aub$ such that*

- (i) $0 < |u|_Y \leq N$;
- (ii) $hau^*bh' \subset L'$.

Exercises

4.1 Let K be a local regular language, and let a, u, b be words. Show that if $aub, au^2b \in K$, then $au^+b \subset K$.

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

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

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 the 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.

II.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 languages and algebraic grammars.

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

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

$$\xi \rightarrow \alpha.$$

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

$$\xi \rightarrow \alpha_1 \mid \alpha_2 \mid \dots \mid \alpha_n; \quad \xi \rightarrow \alpha_1 + \alpha_2 + \dots + \alpha_n; \quad \xi \rightarrow \{\alpha_1, \alpha_2, \dots, \alpha_n\}.$$

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

Example 1.1 Let $V = \{\xi\}$, $X = \{a, b\}$, $P = \{\xi \rightarrow \xi\xi, \xi \rightarrow a\}$. Then the productions can be written as $\xi \rightarrow \xi\xi + a$.

Example 1.2 Let $V = \{\xi, \xi_a, \xi_b\}$, $X = \{a, b\}$, and the set P given by:

$$\begin{aligned} \xi &\rightarrow 1 + a\xi_a b\xi + b\xi_b a\xi; & \xi_a &\rightarrow 1 + a\xi_a b\xi_a; \\ \xi_b &\rightarrow 1 + b\xi_b a\xi_b. \end{aligned}$$

Let $G = \langle V, X, P \rangle$ be a context-free grammar, and let f, g be in $(V \cup X)^*$. Then we define

$$f \xrightarrow{G} g \quad (1.1)$$

iff there are factorizations $f = u\xi v$, $g = u\alpha v$ with $\xi \in V$, $u, \alpha, v \in (V \cup X)^*$ and $\xi \rightarrow \alpha \in P$. If no confusion can arise, we write $f \rightarrow g$ instead of (1.1). For any $p \geq 0$, define

$$f \xrightarrow[p]{G} g$$

iff there exist $f_0, f_1, \dots, f_p \in (V \cup X)^*$ such that

$$f = f_0, \quad g = f_p, \quad \text{and} \quad f_{i-1} \xrightarrow{G} f_i \quad \text{for} \quad i = 1, \dots, p.$$

(In particular, $f \xrightarrow[0]{G} f$ for any $f \in (V \cup X)^*$). The sequence

$$(f_0, f_1, \dots, f_p)$$

is a derivation from f into g , and p is the length of the derivation. Finally, we define

$$f \xrightarrow{*} g \quad \text{iff} \quad f \xrightarrow[p]{G} g \quad \text{for some} \quad p \geq 0;$$

$$f \xrightarrow{+} g \quad \text{iff} \quad f \xrightarrow[p]{G} g \quad \text{for some} \quad p > 0.$$

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

$$L_G(\xi) = \{w \in X^* \mid \xi \xrightarrow{*} w\}.$$

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

$$L_G(f) = \{w \in X^* \mid f \xrightarrow{*} w\}.$$

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

$$\hat{L}_G(f) = \{w \in (V \cup X)^* \mid f \xrightarrow{*} w\}.$$

Of course,

$$L_G(f) = \hat{L}_G(f) \cap X^*.$$

As noted by M. P. 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 ∂ satisfying

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

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

$$g \in \partial(f) \text{ iff } f \xrightarrow{P} g,$$

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

$$\partial(AB) = \partial(A) \cdot B \cup A \cdot \partial(B).$$

Further

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

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

A context-free grammar $G = \langle V, X, P \rangle$ generates a language $L \subset X^*$ iff $L = L_G(\xi)$ for some $\xi \in V$. Thus a grammar G generates $\text{Card}(V)$ 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 X^* is denoted by $\text{Alg}(X^*)$.

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

Example 1.2 (continued). The language generated by ξ_a is the so-called restricted Dyck language D_1^* over X , 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 X , consisting of all words w such that $|w|_a = |w|_b$.

Let $G = \langle V, X, P \rangle$ be a context-free grammar. The following lemma is very useful.

Lemma 1.1 Let $f_1, f_2, g \in (V \cup X)^*$, and let $p \geq 0$ be an integer. Then

$$f_1 f_2 \xrightarrow{p} g$$

iff there are $g_1, g_2 \in (V \cup X)^*$, $p_1, p_2 \geq 0$ such that

$$f_1 \xrightarrow{p_1} g_1, \quad f_2 \xrightarrow{p_2} g_2, \quad g = g_1 g_2, \quad p = p_1 + p_2.$$

Proof. If $f_1 \xrightarrow{p_1} g_1$ and $f_2 \xrightarrow{p_2} g_2$, then

$$f_1 f_2 \xrightarrow{p_1} g_1 f_2 \xrightarrow{p_2} g_1 g_2, \quad \text{thus } f_1 f_2 \xrightarrow{p} g.$$

Assume conversely $f_1 f_2 \xrightarrow{p} g$. If $p = 0$, there is nothing to prove. Arguing by induction on p , suppose $p > 0$. Then

$$f_1 f_2 \xrightarrow{p-1} h \rightarrow g$$

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

$$h = h_1 h_2 \quad \text{with } f_1 \xrightarrow{q_1} h_1, \quad f_2 \xrightarrow{q_2} h_2, \quad q_1 + q_2 = p - 1.$$

Since $h \rightarrow g$, there are $\xi \rightarrow \alpha \in P$, and words u, v with

$$h = u\xi v, \quad g = u\alpha v.$$

If $|u\xi| \leq |h_1|$, then $h_1 = u\xi\bar{u}$ for some word $\bar{u}$. Thus setting

$$g_1 = u\alpha\bar{u}, \quad g_2 = h_2,$$

we obtain

$$g = g_1 g_2, \quad f_1 \xrightarrow{1+q_1} g_1, \quad f_2 \xrightarrow{q_2} g_2.$$

Otherwise, $|\xi v| \leq |h_2|$, and a symmetric argument achieves the proof. ■

Corollary 1.2 For any $f_1, f_2 \in (V \cup X)^*$, $L_G(f_1 f_2) = L_G(f_1) L_G(f_2)$.

Proof. By the preceding lemma, $w \in L_G(f_1 f_2)$ iff there is a factorization $w = w_1 w_2$ such that $w_1 \in L_G(f_1)$, $w_2 \in L_G(f_2)$. ■

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

Lemma 1.3 Let $G = \langle V, X, P \rangle$ be a context-free grammar, $\xi \in V$. Then

$$L_G(\xi) = \bigcup_{\xi \rightarrow \alpha \in P} L_G(\alpha) = L_G(\{\alpha \mid \xi \rightarrow \alpha \in P\}).$$

Proof. For $\xi \rightarrow \alpha \in P$, clearly $L_G(\alpha) \subset L_G(\xi)$. Conversely, let $w \in L_G(\xi)$. Since $w \in X^*$, we have $\xi \xrightarrow{+} w$. Thus there is a production $\xi \rightarrow \alpha \in P$ such that $\xi \rightarrow \alpha \xrightarrow{+} w$. 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 $V = \{\xi_1, \dots, \xi_N\}$ and X be two disjoint alphabets. A system of algebraic equations is a set

$$\xi_i = P_i \quad i = 1, \dots, N \quad (1.2)$$

of equations, where $P_1, \dots, P_N$ are finite subsets of $(V \cup X)^*$. The letters ξ_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 $Q_i(y_1, y_2, \dots, y_N) = 0$, ($i = 1, \dots, N$). In the case where, in each Q_i , there is a monomial y_i , the system can be written in the form $y_i = Q'_i(y_1, y_2, \dots, y_N)$, 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] and Eilenberg [1978].

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

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

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

$$P = \{\xi_i \rightarrow \alpha \mid \alpha \in P_i, 1 \leq i \leq N\}.$$

We now define a solution of (1.2) as a vector $A = (A_1, \dots, A_N)$ of languages such that the substitution in P_i of the language A_i to each occurrence of ξ_i yields precisely the language A_i .

Formally, given (1.2) let $A = (A_1, \dots, A_N)$ with $A_i \subset (V \cup X)^*$ for $i = 1, \dots, N$. Define a substitution $\underline{A}$ from $(V \cup X)^*$ into itself by

$$\begin{aligned} \underline{A}(x) &= \{x\} & x \in X; \\ \underline{A}(\xi_i) &= A_i & i = 1, \dots, N. \end{aligned}$$

Definition The vector $A = (A_1, \dots, A_N)$ is a solution of the system of equations (1.2) iff

$$\underline{A}(P_i) = A_i \quad i = 1, \dots, N. \quad (1.3)$$

Example 1.1 (continued). The equations $\xi = \xi\xi + a$ has the solution a^+ since $a^+ = a^+a^+ \cup a$ and also the solutions X^* and $(V \cup X)^*$, since $X^* = X^*X^* \cup a$ 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 $A = (A_1, \dots, A_N)$, $B = (B_1, \dots, B_N)$, $A \subset B$ iff $A_i \subset B_i$ for $i = 1, \dots, N$.

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 $L_G = (L_G(\xi_1), \dots, L_G(\xi_N))$ is the minimal solution of (1.2).

This 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 $\underline{L_G}(f) = L_G(f)$ for all $f \in (V \cup X)^*$. We shall verify that the substitution $\underline{L_G}$ satisfies (1.3). Indeed, in view of Lemma 1.3,

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

This shows that $L_G = (L_G(\xi_1), \dots, L_G(\xi_N))$ is a solution of (1.2). Next, let $A = (A_1, \dots, A_N)$ be another solution of (1.2). We show that

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

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

$$f \rightarrow g \xrightarrow{p-1} w,$$

and factorizations $f = u\xi_i v$, $g = uav$ such that $\xi_i \rightarrow \alpha \in P$. Since $w \in \underline{A}(g)$ by

induction, it follows that

$$w \in A(g) = A(u)A(\alpha)A(v) \subset A(u)A(P_i)A(v).$$

Since $A(P_i) = A_i = A(\xi_i)$, we have

$$A(u)A(P_i)A(v) = A(u\xi_i v) = A(f).$$

Thus $w \in A(f)$. From (1.4), we obtain

$$L_G(\xi_i) \subset A(\xi_i) = A_i \quad i = 1, \dots, N. \quad \blacksquare$$

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

Definition An algebraic grammar $G = \langle V, X, P \rangle$ is strict iff for each production $\xi \rightarrow \alpha \in P$, either $\alpha = 1$ or α contains at least one terminal letter, thus iff

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

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 $G = \langle V, X, P \rangle$ 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 to G , and let $A = (A_1, \dots, A_N)$, $B = (B_1, \dots, B_N)$ be two solutions of this system. We prove:

$$\text{for } i = 1, \dots, N, \quad w \in A_i, \quad |w| \leq n \quad \text{implies} \quad w \in B_i \quad (1.5)$$

by induction on n . This shows that $A \subset B$, and $A = B$ by symmetry.

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

$$\alpha = u_0 \xi_i u_1 \cdots u_{r-1} \xi_i u_r,$$

with $r \geq 1$, $u_0, \dots, u_r \in X^*$, $\xi_i, \dots, \xi_i \in V$. Therefore

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

with $v_k \in A(\xi_k) = A_k$ for $k = 1, \dots, r$. Now $u_0 u_1 \cdots u_r \neq 1$ since G is strict. Since $r \geq 1$, $|v_k| < n$ for all $k = 1, \dots, r$, and by the induction hypothesis, $v_k \in B_k = B(\xi_k)$ for $k = 1, \dots, r$. Thus

$$w \in u_0 B(\xi_i) u_1 \cdots u_{r-1} B(\xi_i) u_r = B(\alpha) \subset B_i. \quad \blacksquare$$

Note that the finiteness of the sets P_i was used in none of the proofs of Theorems 1.4 or 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 proof unicity of the solution of equations (Exercise 1.5).

We conclude this section with a result that permits transformations of system 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

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

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

Proposition 1.6 (Substitution Lemma) Let

$$\xi_i = P_i \quad i = 1, \dots, N \quad (1.6)$$

be a system of equation. 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 $i \neq k$, and $Q_k = (P_k \setminus \alpha) \cup uP_j v$. Then (1.6) is equivalent to

$$\xi_i = Q_i \quad i = 1, \dots, N. \quad (1.7)$$

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 $\xi = a + \xi a + \xi\xi\xi$ is the equivalent to the initial one.

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

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

Taking $\alpha = \eta\xi$, and replacing η 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 Y be an alphabet, and let A, B, C, L and M be subsets of Y^* . If

$$L = A \cup BMC \quad \text{and} \quad M = A \cup BLC,$$

then $L = M$.

Proof. If $B = \emptyset$ or $C = \emptyset$, then $L = M = A$. Next, if $1 \in B$ and $1 \in C$, then by the first equation $M \subset BMC \subset L$, and similarly $L \subset M$, hence $L = M$. Thus we

may assume that $1 \notin BC$. Then $1 \in L$ iff $1 \in A$, hence iff $1 \in M$. Arguing by induction on the length of words, consider $w \in Y^*$, $|w| = p > 0$, and assume $w \notin A$. Then $w \in L$ iff $w \in BMC$, hence iff $w = bw'c$ with $b \in B$, $c \in C$, $w' \in M$ and $|w'| < p$. Thus $w' \in L$ and $w \in BLC \subset M$. Similarly, $w \in M$ implies $w \in L$. This proves the lemma. ■

Proof of Proposition 1.6. Let $A = (A_1, \dots, A_N)$ be a solution of (1.6). By definition, $\underline{A}(P_i) = A_i$ for $i = 1, \dots, N$. Thus

$$\begin{aligned}\underline{A}(Q_i) &= A_i \quad i = 1, \dots, N, i \neq k, \\ \underline{A}(Q_k) &= \underline{A}(P_k \setminus \alpha) \cup \underline{A}(u) \underline{A}(P_j) \underline{A}(v) = \underline{A}(P_k \setminus \alpha) \cup \underline{A}(\alpha) = A_k,\end{aligned}$$

showing that A is a solution of (1.7).

Conversely, let $B = (B_1, \dots, B_N)$ be a solution of (1.7). Then

$$\begin{aligned}\underline{B}(P_i) &= B_i \quad i = 1, \dots, N, i \neq k, \\ \underline{B}(P_k) &= \underline{B}(P_k \setminus \alpha) \cup \underline{B}(\alpha) = \underline{B}(P_k \setminus \alpha) \cup \underline{B}(u) \underline{B}(\xi) \underline{B}(v) \\ &= \underline{B}(P_k \setminus \alpha) \cup \underline{B}(u) \underline{B}(Q_j) \underline{B}(v).\end{aligned}\tag{1.8}$$

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

$$\underline{B}(P_k) = \underline{B}(P_k \setminus \alpha \cup u P_j v) = \underline{B}(Q_k) = B_k,$$

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

$$\begin{aligned}\underline{B}(P_k) &= \underline{B}(P_k \setminus \alpha) \cup \underline{B}(u) \underline{B}(Q_k) \underline{B}(v); \\ \underline{B}(Q_k) &= \underline{B}(P_k \setminus \alpha) \cup \underline{B}(u) \underline{B}(P_k) \underline{B}(v)\end{aligned}$$

by definition. In view of Lemma 1.7, we have

$$\underline{B}(P_k) = \underline{B}(Q_k) = B_k;$$

thus B is a solution of (1.6). ■

Exercises

1.1 A context-free grammar $G = \langle V, X, P \rangle$ is called proper if each production $\xi \rightarrow \alpha \in P$ verifies $\alpha \notin 1 \cup V$. A vector $A = (A_1, \dots, A_N)$ of languages is called proper if $1 \notin A_i$ for $i = 1, \dots, N$. 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 $\xi = A \cup \xi B$ has the unique solution AB^* provided $1 \notin B$.

II.2 Closure Properties, Iteration

We recall here some closure properties of the family of context-free languages, and also the 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 $\theta: X^* \rightarrow Y^*$ such that $\theta(x)$ is a context-free language for each $x \in X$.

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

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

$$\psi G = \langle V, Y, \psi P \rangle$$

by $\psi P = \{ \xi \rightarrow \psi(\alpha) \mid \xi \rightarrow \alpha \in P \}$.

Then it 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 $\varphi: Y^* \rightarrow X^*$ be an alphabetic morphism. As above, extend φ to $(V \cup Y)^*$ by setting $\varphi(\xi) = \xi$ for $\xi \in V$. Define $Z = \{ y \in Y \mid \varphi(y) = 1 \}$ and $T = Y \setminus Z$. Finally, let ω be a new letter ($\omega \notin V \cup X \cup Y$). Define a grammar

$$\varphi^{-1} G = \langle \omega \cup V, Y, P' \rangle$$

where $P' = P'' \cup \left\{ \omega \rightarrow 1 + \sum_{z \in Z} \omega z \right\}$

and where P'' is defined as follows: For $\xi \in V$, $k \geq 0$, $y_1, y_2, \dots, y_k \in V \cup T$

$$\xi \rightarrow \omega y_1 \omega y_2 \omega \dots \omega y_k \omega \in P'' \Leftrightarrow \xi \rightarrow \varphi(y_1 y_2 \dots y_k) \in P.$$

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

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

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

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

$$G_K = \langle \hat{\sigma} \cup (Q \times V \times Q), X, P_K \rangle$$

where $P_K = P' \cup P''$,

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

and P' composed of the following productions:

For $k \geq 0$, $\xi, \eta_1, \dots, \eta_k \in V$, $u_0, \dots, u_k \in X^*$, $q, q', q_1, \dots, q_k, q'_1, \dots, q'_k \in Q$,

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

if and only if

$$\xi \rightarrow u_0\eta_1u_1\eta_2 \cdots \eta_ku_k \in P$$

and $q \cdot u_0 = q_1, \quad q'_1 \cdot u_i = q_{i+1} \quad (i = 1, \dots, k-1), \quad q'_k \cdot u_k = q'.$

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 $K_{q,q'} = \{ f \in X^* \mid q \cdot f = q' \}.$

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

d) Context-free substitution Let $\theta: X^* \rightarrow Y^*$ be a context-free substitution. For each $x \in X$, let

$$G_x = \langle V_x, Y, P_x \rangle$$

be a context-free grammar such that $\theta(x) = L_{G_x}(\sigma_x)$ for some $\sigma_x \in V_x$. Clearly the alphabets V_x may be assumed pairwise disjoint and disjoint from V . Define

a copy morphism $\gamma: (V \cup X)^* \rightarrow (V \cup \{\sigma_x : x \in X\})^*$ by $\gamma(\xi) = \xi$ for $\xi \in V$, $\gamma(x) = \sigma_x$ for $x \in X$, and let $\gamma G = \langle V, \{\sigma_x : x \in X\}, \gamma P \rangle$ be defined as in a). Let

$$H = \langle W, Y, Q \rangle$$

be the grammar with $W = V \cup \bigcup_{x \in X} V_x$, $Q = \gamma P \cup \bigcup_{x \in X} P_x$. 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 $L \subset X^*$ be an algebraic language. There exists an integer $N \geq 1$ such that any word $f \in L$ with $|f| \geq N$ admits a factorization $f = aubvc$ ($a, u, b, v, c \in X^*$) satisfying*

(i) $au^n bv^n c \in L$ 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 f 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 I.5.

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

(i) $au^n bv^n c \in L$ for all $n \geq 0$;

(ii) (each of a and u and b) or (each of b and v and c) contains at least one marked position;

(iii) uv contains at most N marked positions.

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

Corollary 2.4 *Let $L \subset X^*$ be an algebraic language. Then there exists an integer N such that for any word $f \in L$, and for any factorization $f = hgh'(h, g, h' \in X^*)$*

with $|g| \geq N$, f admits a factorization $f = aubvc$ ($a, u, b, v, c \in X^*$) satisfying

- (i) $au^n bv^n c \in L$ for all $n \geq 0$;
- (ii) either u is a segment of g and $|u| > 0$ or v is a segment of g 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 $G = \langle V, X, P \rangle$ be an algebraic grammar. Then there exists an integer N such that, for any derivation $\xi \xrightarrow{*} f$ with $\xi \in V$, $f \in (V \cup X)^*$, and for any choice of N marked positions in f , there is a factorization $f = aubvc$ ($a, u, b, v, c \in X^*$) and $\eta \in V$ such that*

- (i) $\xi \xrightarrow{*} a\eta c$, $\eta \xrightarrow{*} u\eta v$, $\eta \xrightarrow{*} b$;
- (ii) (a and u and b) or (b and v and c) contain at least one marked position;
- (iii) uv contains at most N marked positions.

Note that the integer N is independent of the nonterminal ξ . Note also that the lemma is true for sentential forms as well as for words in X^* .

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

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

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

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

We only give the construction. Let $L = L_G(\sigma)$ for some grammar $G = \langle V, X, P \rangle$, 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 $u, v \in X^*$. If $L \neq \emptyset$, then $\sigma \in V'$. Let $G' = \langle V', X, P' \rangle$ where $P' = \{\xi \rightarrow \alpha \in P \mid \xi \in V', \alpha \in (V' \cup X)^*\}$. Then G' is reduced in σ , 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 $G'' = \langle V'', X, P'' \rangle$ as follows. Let $\theta: (V' \cup X)^* \rightarrow (V'' \cup X)^*$ be the substitution given by

$$\theta(x) = x \ (x \in X), \quad \theta(\xi) = \xi \ (\xi \in V^n), \quad \theta(\xi) = L_{G^*}(\xi) \ (\xi \in V^i \setminus V^n),$$

and set

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

If L is infinite, then $\sigma \in V''$, G'' is strictly reduced in σ , 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 $f = hgh'g'h''$ of $f \in L$, of a factorization $f = aubvc$ satisfying (i) and such that both u is a segment of g and v is a segment of g' .

II.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 rational 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 parenthesis. 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

$$(\lceil () () \rceil \{ \} \lceil \rceil) ()$$

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 inverse for each other. A word is considered as "correct" iff successive deletion of factors of associated parentheses (say of the form $x\bar{x}$ and $\bar{x}x$) yields the empty word. Thus

$$\bar{x}x\bar{x}x\bar{y}y\bar{x}x$$

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 $X_n = \{x_1, \dots, x_n\}$, $\bar{X}_n = \{\bar{x}_1, \dots, \bar{x}_n\}$ be two alphabets of n letters. Each couple $x_k, \bar{x}_k$ can be considered as a pair of

parentheses of the same type. Define $Z_n = X_n \cup \bar{X}_n$. We introduce the following useful notation. For $z \in Z_n$, let

$$\bar{z} = \begin{cases} \bar{x}_k & \text{if } z = x_k; \\ x_k & \text{if } z = \bar{x}_k. \end{cases}$$

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

Definition The restricted Dyck congruence δ'_n is the congruence of Z_n^* generated by

$$x_k \bar{x}_k \sim 1 \quad k = 1, \dots, n. \quad (3.1)$$

The Dyck congruence δ_n is the congruence generated by (3.1) and by

$$\bar{x}_k x_k \sim 1 \quad k = 1, \dots, n \quad (3.2)$$

Thus two words w and w' are congruent modulo δ'_n or modulo δ_n , and we write

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

iff w' can be obtained from w by a finite number of insertions or deletions of factors of the form $x_k \bar{x}_k$ (resp. $x_k \bar{x}_k$ or $\bar{x}_k x_k$).

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 Z_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 Z_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 formulation.

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

$$x_k \bar{x}_k \sim 1 \quad (k = 1, \dots, n) \quad \text{and} \quad \bar{x}_i x_i \sim 1 \quad (i \in I).$$

The language D_I^* is the class of the empty word in the congruence δ_I .

Clearly D_I^* is a submonoid of Z_n^* , justifying thus the notation. Anyone of the 2^n subsets of $\{1, \dots, n\}$ defines a "Dyck-like" language. If $I = \emptyset$, then $\delta_I = \delta'_n$ and $D_I^* = D_n'^*$; if $I = \{1, \dots, n\}$, 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 $I \subseteq \{1, \dots, n\}$. For this we first introduce a new relation. Let $u, v \in Z_n^*$, and set $u \vdash_I v$ iff there are $f, g \in Z_n^*$ such that $u = f\alpha g$, $v = fg$, and either $\alpha = x_k \bar{x}_k$ for some $k \in \{1, \dots, n\}$ or $\alpha = \bar{x}_i x_i$ for some $i \in I$. The reflexive and transitive closure $\vdash_I^*$ of $\vdash_I$ is called the Dyck reduction. Clearly, if $u \vdash_I^* v$, then $|u| \geq |v|$, and $|u| = |v|$ implies $u = v$. The congruence δ_I and the reduction $\vdash_I^*$ are linked by

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

iff there are $k \geq 0$, $u_0, \dots, u_k \in Z_n^*$ such that

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

and $(u_p \vdash_I u_{p+1} \text{ or } u_{p+1} \vdash_I u_p) \quad p = 0, \dots, k-1$.

Thus $u \vdash_I^* v$ implies $u \equiv v \pmod{\delta_I}$, but the converse is false.

A word u is reduced mod δ_I iff it contains no factor of the form $x_k \bar{x}_k$ or $\bar{x}_i x_i$, ($i \in I$). Thus u is reduced iff $\{v \mid u \vdash_I v\} = \emptyset$. For any word $w \in Z_n^*$ there is at least one reduced word u congruent to $w \pmod{\delta_I}$. Usually, there are several ways to compute a reduced word which is unique. We follow Autebert and Cousineau [1976] rather than the standard exposition as treated in Magnus, Karrass and Solitar [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 [1970].

Example 3.1 For $n = 2$, $I = \{1, 2\}$, consider the word $w = \bar{x}x\bar{x}y\bar{y}x\bar{x}$. It can be reduced to the empty word in at least the two following fashions:

$$w = \bar{x}x\bar{x}y\bar{y}x\bar{x} \quad w = \bar{x}x\bar{x}y\bar{y}x\bar{x}$$

$$w_1 = \bar{x}x\bar{y}y\bar{x}x \quad w'_1 = \bar{x}x\bar{y}y\bar{x}x$$

$$w_2 = \bar{y}y\bar{x}x \quad w'_2 = \bar{x}x\bar{x}x$$

$$w_3 = \bar{x}x \quad w'_3 = \bar{x}x$$

$$w_4 = 1 \quad w'_4 = 1.$$

From now on, we write $\vdash$ and $\vdash^*$ instead of $\vdash_I$ and $\vdash_I^*$.

Lemma 3.1 (Confluence Lemma) *If $w \vdash^* u_1$ and $w \vdash^* u_2$, then there exists a word v such that $u_1 \vdash^* v$, $u_2 \vdash^* v$.*

Thus the lemma asserts the existence of a word v such that the following diagram holds (Fig. II.1).

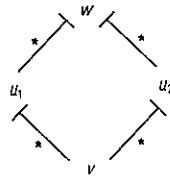


Fig. II.1

We first prove the lemma in a special case.

Lemma 3.2 *If $w \vdash u_1$ and $w \vdash u_2$, then there exists a word v such that $u_1 \vdash^* v$ and $u_2 \vdash^* v$.*

Proof. There are words $f_1, g_1, f_2, g_2 \in Z_n^*$ and $a_1, a_2 \in Z_n^2$ such that

$$w = f_1 a_1 g_1 = f_2 a_2 g_2, \quad u_1 = f_1 g_1, \quad u_2 = f_2 g_2.$$

If $|f_1| = |f_2|$, then $u_1 = u_2$ and there is nothing to prove. Assume for instance $|f_1| < |f_2|$. We distinguish two cases.

a) $|f_1| + 2 \leq |f_2|$. Then $f_2 = f_1 a_1 h$ for some word h , thus $w = f_1 a_1 h a_2 g_2$, and $v = f_1 h g_2$ satisfies $u_1 \vdash v$, $u_2 \vdash v$.

b) $|f_1| + 1 = |f_2|$. Then $f_2 = f_1 z$ for some letter z , hence $a_1 = z \bar{z}$, and $a_2 = \bar{z} z$. (This implies that $z = x_i$ or $z = \bar{x}_i$ with $i \in I$.) Thus $w = f_1 z \bar{z} z g_2$, and $u_1 = f_1 z g_2 = u_2$. 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 is verified 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

$$w \vdash v_1 \vdash^* u_1, \quad w \vdash v_2 \vdash^* u_2.$$

Thus in view of Lemma 3.8, there is a word t such that

$$v_1 \vdash^* t \quad \text{and} \quad v_2 \vdash^* t.$$

Since $v_1 \vdash^* u_1$, $v_1 \vdash^* t$ and $|v_1| < p$, by induction there is a word w_1 such that

$$u_1 \vdash^* w_1, \quad t \vdash^* w_1;$$

similarly, there is a word w_2 such that

$$u_2 \vdash^* w_2, \quad t \vdash^* w_2.$$

Now $t \vdash^* w_1$, $t \vdash^* w_2$ and $|t| < p$. Using the induction hypothesis once more, there exists a word v such that

$$w_1 \vdash^* v, \quad w_2 \vdash^* v.$$

This shows that $u_1 \vdash^* w_1 \vdash^* v$, $u_2 \vdash^* w_2 \vdash^* v$. ■

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

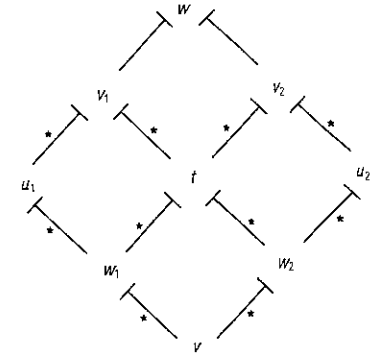


Fig. II.2

Corollary 3.3 *Let $u, v \in Z_n^*$; then $u \equiv v \pmod{\delta_I}$ iff there exists a word w such that $u \vdash^* w$ and $v \vdash^* w$.*

Proof. Assume $u \equiv v \pmod{\delta_I}$. Then there are $k \geq 0$, $u_0, \dots, u_k \in Z_n^*$ such that $u_0 = u$, $u_k = v$ and

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

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

$$u_1 \vdash^* w_1 \quad \text{and} \quad v \vdash^* w_1.$$

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

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

We list two other corollaries.

Corollary 3.4 *If v is reduced and $u \equiv v \pmod{\delta_I}$, then $u \vdash^* v$.*

Proof. By Corollary 3.3, there is a word w such that $u \vdash w$ and $v \vdash w$. Since v is reduced, $v = w$. ■

Corollary 3.5 Any class of the congruence δ_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, $u \vdash v$ and $v \vdash u$, thus $u = v$. ■

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

$$\rho_I(Z_n^*) = Z_n^* \setminus Z_n^* V_I Z_n^*$$

with $V_I = \{x_k \bar{x}_k : k = 1, \dots, n\} \cup \{\bar{x}_i x_i : i \in I\}$.

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 $f, w \in Z_n^*$, $w = z_1 z_2 \dots z_m$ ($z_p \in Z_n^*$). Then

$$f \vdash w$$

iff there exist $d_0, d_1, \dots, d_m \in Z_n^*$ such that

$$f = d_0 z_1 d_1 z_2 \dots d_{m-1} z_m d_m,$$

and $d_0 \vdash 1, d_1 \vdash 1, \dots, d_m \vdash 1$.

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

$$f' = d_0 z_1 d_1 z_2 \dots d_{m-1} z_m d_m$$

for some words d_r with $d_r \vdash 1$, ($r = 0, \dots, m$). Next, there is a factorization

$$f = gah, \text{ with } f' = gh,$$

and $a = x_k \bar{x}_k$ for some $k \in \{1, \dots, n\}$ or $a = \bar{x}_i x_i$ for some $i \in I$. Hence there is an integer j , ($0 \leq j \leq m$) and a factorization $d_i = d' d''$, ($d', d'' \in Z_n^*$) such that

$$g = d_0 z_1 \dots z_j d', \quad h = d'' z_{j+1} \dots z_m d_m.$$

Set $e_j = d' a d''$. Then $e_j \vdash d_i \vdash 1$ and

$$f = d_0 z_1 \dots z_j e_j z_{j+1} \dots z_m d_m. \quad \blacksquare$$

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

$$\xi \rightarrow 1 + \sum_{k=1}^n x_k \xi \bar{x}_k \xi + \sum_{i \in I} \bar{x}_i \xi x_i \xi. \quad (3.3)$$

First, we introduce the notation

$$Y_I = X_n \cup \{\bar{x}_i : i \in I\}.$$

Thus $Y_I = X_n$ if $I = \emptyset$, and $Y_I = Z_n$ if $I = \{1, \dots, n\}$.

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 $w = zw' \bar{z} w''$ with $w' \equiv w'' \equiv 1 \pmod{\delta_I}$ and $z \in Y_I$. Then $w \equiv z \bar{z} \equiv 1 \pmod{\delta_I}$ and $w \in D_I^*$. This shows the inclusion

$$D_I^* \supset 1 \cup \bigcup_{1 \leq k \leq n} x_k D_I^* \bar{x}_k D_I^* \cup \bigcup_{i \in I} \bar{x}_i D_I^* x_i D_I^*.$$

Conversely, let $w \in D_I^*$, $w \neq 1$. Since 1 is reduced, $w \vdash 1$ by Corollary 3.4. Since $w \neq 1$, there is a letter $z \in Y_I$ such that $w \vdash z \bar{z}$. By Lemma 3.6, w factorizes in

$$w = d_0 z d_1 \bar{z} d_2$$

with $d_0, d_1, d_2 \in D_I^*$. If $d_0 = 1$, then $w \in z D_I^* \bar{z} D_I^*$. If $d_0 \neq 1$, then $|d_0| < |w|$, and arguing by induction, $d_0 \in y D_I^* \bar{y} D_I^*$ for some $y \in Y_I$. Thus $w \in y D_I^* \bar{y} D_I^* z D_I^* \bar{z} D_I^* \subset y D_I^* \bar{y} D_I^*$. This achieves the proof. ■

We now investigate the language

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

For $z \in Z_n$, define

$$D_{I,z} = D_I \cap z Z_n^*.$$

Proposition 3.8 (i) The language D_I is bifix;

(ii) $D_{I,z} \neq \emptyset$ iff $z \in Y_I$;

(iii) if $D_{I,z} \neq \emptyset$, then any $w \in D_{I,z}$ admits a unique factorization

$$w = z u_1 u_2 \dots u_m \bar{z} \quad \text{with} \quad m \geq 0, \quad u_1, \dots, u_m \in D_I \setminus D_{I,z}.$$

Proof. (i) Let $w \in D_I$, and assume $w = uv$ with $u \in D_I$, $v \in Z_n^*$. 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 $w \in D_{I,z}$. Then $w = zu$ for some word u . Since $w \vdash 1$, there is a letter $y \in Y_I$ such that $w \vdash y \bar{y}$. In view of Lemma 3.6, w factorizes in $w = d_0 y d_1 \bar{y} d_2$,

with $d_0, d_1, d_2 \in D_I^*$. Since $w \in D_I$, $d_0 = d_2 = 1$ and $y = z$. This proves the assertion, since clearly $D_{I,z} \neq \emptyset$ if $z \in Y_I$.

(iii) We just have seen that a word $w \in D_{I,z}$ factorizes in $w = zd_1\bar{z}$ with $d_1 \in D_I^*$. Thus either $d_1 = 1$, or $d_1 = u_1u_2 \cdots u_m$ with $u_1, \dots, u_m \in D_I$. Assume that $u_p \in D_{I,z}$ for some p . Then $u_p = \bar{z}dz$ for some $d \in D_I^*$, and

$$w = (zu_1 \cdots u_{p-1}\bar{z})d(zu_{p+1} \cdots u_m\bar{z}) \in (D_I^* \setminus 1)^2$$

contrary to the definition of D_I . The unicity is immediate since D_I is a code. ■

By Proposition 3.8,

$$D_I = \bigcup_{z \in Y_I} D_{I,z} \quad (3.4)$$

$$D_{I,z} = z\Delta_{I,z}\bar{z} \quad (z \in Y_I) \quad (3.5)$$

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

$$\Delta_{I,z} = \left(\bigcup_{y \in Y_I \setminus \bar{z}} D_{I,y} \right)^*. \quad (3.6)$$

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

$$D_I^* = 1 \cup D_I D_I^* \quad (3.7)$$

From equations (3.4)–(3.7), we deduce the following grammar $H_I = (V_I, Z_n, P_I)$. Set

$$V_I = \{\xi, \eta\} \cup \{\xi_z, \eta_z : z \in Y_I\},$$

and let P_I contain the productions:

$$\xi \rightarrow 1 + \eta\xi; \quad \eta \rightarrow \sum_{z \in Y_I} \eta_z;$$

$$\eta_z \rightarrow z\xi_z\bar{z}; \quad \xi_z \rightarrow 1 + \left(\sum_{y \in Y_I \setminus \bar{z}} \eta_y \right) \xi_z \quad (z \in Y_I).$$

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

$$\begin{aligned} \xi &= 1 + \sum_{z \in Y_I} z\xi_z\bar{z}; & \xi_z &= 1 + \sum_{y \in Y_I \setminus \bar{z}} y\xi_y\bar{y}\xi_z & (z \in Y_I); \\ \eta &= \sum_{z \in Y_I} \eta_z; & \eta_z &= z\xi_z\bar{z} & (z \in Y_I). \end{aligned} \quad (3.8)$$

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:

$$D_I^* = L_{H_I}(\xi); \quad D_I = L_{H_I}(\eta); \quad D_{I,z} = L_{H_I}(\eta_z), \quad \Delta_{I,z} = L_{H_I}(\xi_z)$$

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

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

$$\xi \rightarrow 1 + \eta\xi; \quad \eta \rightarrow \sum_{k=1}^n x_k \xi \bar{x}_k.$$

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

$$D_n^* = 1 \cup D'_n D_n^*; \quad D'_n = \bigcup_{1 \leq k \leq n} x_k D_n^* \bar{x}_k;$$

$$D_n^* = 1 \cup D_n D_n^*; \quad D_n = \bigcup_{z \in Z_n} D_{n,z};$$

$$D_{n,z} = z\Delta_{n,z}\bar{z}; \quad (z \in Z_n); \quad \Delta_{n,z} = \left(\bigcup_{y \in Z_n \setminus \bar{z}} D_{n,y} \right)^* \quad (z \in Z_n).$$

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

$$\xi \rightarrow \xi\xi + \sum_{k=1}^n x_k \xi \bar{x}_k + 1,$$

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

$$\xi \rightarrow \xi\xi + \sum_{k=1}^n x_k \xi \bar{x}_k + \sum_{k=1}^n \bar{x}_k \xi x_k + 1.$$

Let $X_n^{(*)} = Z_n^* / \delta_n$ be the quotient monoid; we denote by δ_n the canonical morphism from Z_n^* onto $X_n^{(*)}$ defined by $\delta_n(w) = [w]_{\delta_n}$. For $w = z_1 z_2 \cdots z_m \in Z_n^*$, ($z_i \in Z_n$), define $\bar{w} = \bar{z}_m \bar{z}_{m-1} \cdots \bar{z}_1$. Since

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

$X_n^{(*)}$ is a group, and $\delta_n(\bar{w}) = (\delta_n(w))^{-1}$. In particular, $\delta_n(\bar{z}) = (\delta_n(z))^{-1}$ for $z \in Z_n$. It can even be shown that $X_n^{(*)}$ is a free group (see Magnus, Karrass and Solitar [1966]). $X_n^{(*)}$ is called the free group generated by X_n . Since each class $[w]_{\delta_n}$ contains exactly one reduced word $\rho(w)$, there is a bijection from $X_n^{(*)}$ onto $\rho(Z_n^*)$ which associates to any $u \in X_n^{(*)}$ 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 X_n^* is already reduced. Thus $X_n^* \subset \rho(Z_n^*)$. It is sometimes convenient to identify X_n^* with its image in $X_n^{(*)}$. This identification allows use of inverses and may simplify considerably certain formulations. However, it is important not to confuse the product $f^{-1}g$ in $X_n^{(*)}$, where $f, g \in X_n^*$, with the left quotient operation defined in Section I.2: Viewed as an operation in $X_n^{(*)}$, $f^{-1}g$

is always a well defined element of $X_n^{(*)}$, and $f^{-1}g = h \in X_n^*$ iff $fh = g$. Viewed as an operation in X_n^* , $f^{-1}g$ is either the empty set or a word in X_n^* , according to f is not, or is a left factor of g . The embedding of X_n^* into $X_n^{(*)}$ will be used only in Sections IV.2 and IV.6. In all other circumstances, $f^{-1}g$ 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 $L \subset Y^*$ be an algebraic language. Then there are an integer $n \geq 1$, an alphabetic morphism $\varphi: Z_n^* \rightarrow Y^*$, and a local regular language K such that*

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

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 that $1 \notin L$.

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 $G = \langle V, Y, P \rangle$ in quadratic form, i.e. that each production $\xi \rightarrow \alpha \in P$ satisfies $\alpha \in Y \cup V^2$. Such a grammar can always be obtained (see e.g. the books listed in the bibliography). We set

$$V = \{\xi_1, \dots, \xi_N\}, \quad Y = \{y_1, \dots, y_q\},$$

and define

$$X_n = Y \cup \{a_{i,j,k}, b_{i,j,k} \mid i, j, k = 1, \dots, N\} \cup \{d_{i,s} \mid i = 1, \dots, N, s = 1, \dots, q\},$$

where the $a_{i,j,k}, b_{i,j,k}, d_{i,s}$ are new letters. Thus $n = 2N^3 + Nq + q$. Set $\bar{X}_n = \{\bar{x} \mid x \in X_n\}$ and $Z_n = X_n \cup \bar{X}_n$.

Let $H = \langle V, Z_n, Q \rangle$ be the grammar with following productions:

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

$$\xi_i \rightarrow a_{ijk} b_{ijk} \xi_j \bar{\xi}_k \bar{a}_{ijk} \in Q \quad (3.9)$$

if and only if

$$\xi_i \rightarrow \xi_j \bar{\xi}_k \in P.$$

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

$$\xi_i \rightarrow d_{is} y_s \bar{y}_s \bar{d}_{is} \in Q \quad (3.10)$$

if and only if

$$\xi_i \rightarrow y_s \in P.$$

For $i = 1, \dots, N$, set $M_i = L_H(\xi_i)$, and let $\varphi: Z_n^* \rightarrow Y^*$ be the projection. Then clearly

$$\varphi(M_i) = L_G(\xi_i).$$

We shall prove that

$$M_i = D_n^* \cap K_i = D_n'^* \cap K_i = D_n \cap K_i = D_n' \cap K_i \quad i = 1, \dots, N \quad (3.11)$$

where $K_i = (A_i Z_n^* \cap Z_n^* \bar{A}_i) \setminus Z_n^* B Z_n^*$

is the local regular set defined by:

$$A_i = \{a_{ijk} \mid j, k = 1, \dots, N\} \cup \{d_{is} \mid s = 1, \dots, q\}, \quad \bar{A}_i = \{\bar{x} \mid x \in A_i\};$$

$$Z_n^2 \setminus B = W_1 \cup W_2 \cup W_3,$$

$$\text{with } W_1 = \{a_{ijk} b_{ijk} \mid i, j, k = 1, \dots, N\}; \quad (3.12)$$

$$W_2 = \{d_{is} y_s, \bar{y}_s \bar{d}_{is} \mid i = 1, \dots, N, s = 1, \dots, q\} \cup \{y_s \bar{y}_s \mid s = 1, \dots, q\}; \quad (3.13)$$

$$W_3 = \bigcup_{i,j,k} b_{ijk} A_j \cup \bar{b}_{ijk} A_k \cup \bar{A}_j \bar{b}_{ijk} \cup \bar{A}_k \bar{a}_{ijk}. \quad (3.14)$$

a) $M_i \subset D_n^* \cap K_i$, ($i = 1, \dots, N$).

Let indeed $w \in M_i$. Then either, by (3.10),

$$w = d_{is} y_s \bar{y}_s \bar{d}_{is}$$

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

$$w = a_{ijk} b_{ijk} u \bar{b}_{ijk} v \bar{a}_{ijk}$$

for some $j, k \in \{1, \dots, N\}$ 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) $D_n^* \cap K_i \subset D_n' \cap K_i$, ($i = 1, \dots, N$).

First, we verify

$$D_{n,\bar{x}} \cap Z_n^* \setminus Z_n^* B Z_n^* = \emptyset \quad \text{for } \bar{x} \in \bar{X}_n. \quad (3.15)$$

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

Now let $w \in D_n^* \cap K_i$, $w = w_1 w_2 \dots w_r$ with $w_p \in D_n \cap X_n Z_n^* \bar{X}_n$, for $p = 1, \dots, r$ by (3.15). Then $w_1 \in A_i Z_n^* \bar{A}_i$ 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_{is} , then $w = d_{is} y_s \bar{y}_s \bar{d}_{is}$ by (3.13) and $w \in D_n'$. Finally, if w begins with the

letter a_{ijk} , then $w = a_{ijk}u\bar{a}_{ijk}$ for some $u \in D_n^*$, and in view of (3.12), $u = b_{ijk}v_1\bar{b}_{ijk}v_2$ for some $v_1, v_2 \in D_n^*$. In view of (3.14), $v_1 \in K_j$, $v_2 \in K_k$, 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) $D'_n \cap K_i \subset M_i$, ($i = 1, \dots, N$).

Let $w \in D'_n \cap K_i$. If w begins with a letter d_{is} , then by (3.13), $w = d_{is}y_s\bar{y}_s\bar{d}_{is}$ and $w \in M_i$ by (3.10). Otherwise, $w = a_{ijk}u\bar{a}_{ijk}$ for some indices j, k , and $u \in D_n^*$. By (3.12), $u = b_{ijk}v_1\bar{b}_{ijk}v_2$ for some $v_1, v_2 \in D_n^*$. Moreover, $v_1 \in K_j$ and $v_2 \in K_k$. Thus $v_1 \in D'_n \cap K_j \subset D'_n \cap K_i$, 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

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

and (3.11) follows. ■

Exercises

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

$$\xi \rightarrow \xi\xi + \sum_{k=1}^n x_k \xi \bar{x}_k + \sum_{i \in I} \bar{x}_i \xi x_i + 1.$$

3.2 Same question as in 3.1, for the grammar

$$\xi \rightarrow \xi\xi + \sum_{k=1}^n x_k \xi \bar{x}_k + \sum_{i \in I} \bar{x}_i \xi \xi x_i + 1.$$

3.3 (Magnus, Karrass and Solitar [1966]) Define a function $\theta_I : Z_n^* \rightarrow Z_n^*$ inductively as follows: $\theta_I(1) = 1$, $\theta_I(z) = z$ for $z \in Z_n$, and if $\theta_I(w) = z_1 z_2 \dots z_m$, ($z_i \in Z_n$), then

$$\theta_I(wz) = \begin{cases} z_1 z_2 \dots z_m z & \text{if } z_m \in Y_I \text{ and } z_m = \bar{z}; \\ z_1 z_2 \dots z_m z & \text{otherwise.} \end{cases}$$

Show that $\theta_I = \rho_I$.

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

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

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

$$\|w\| = |w|_{x_n} - |w|_{\bar{x}_n} = \sum_{k=1}^n |w|_{x_k} - |w|_{\bar{x}_k}.$$

Show the following assertions:

- $w \in D_n^* \Rightarrow \|w\| = 0$.
- $w \in D_n^* \Rightarrow \|w'\| \geq 0$ for each left factor w' of w .
- $w \in D'_n \Rightarrow \|w'\| > 0$ for each proper non empty left factor w' of w .
- $w \in D'_n \Leftrightarrow \|w\| = 0$.

3.7 (Requires knowledge in ambiguity.) Show that the grammars H_i are unambiguous.

3.8 Assume that the grammar $G = \langle V, Y, P \rangle$ for L in the proof of the Chomsky-Schützenberger Theorem is in Greibach Normal Form, i.e. $\xi \rightarrow \alpha$ implies $\alpha \in Y \cup YV \cup YVV$.

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

b) Replace the productions of the form

$$\xi_i \rightarrow y\xi_j \xi_k \quad \text{by} \quad \xi_i \rightarrow a_{ijk} \xi_j \bar{a}_{ijk} \xi_k$$

$$\xi_i \rightarrow y\xi_j \quad \text{by} \quad \xi_i \rightarrow b_{ij} \bar{b}_{ij} \xi_j$$

$$\xi_i \rightarrow y \quad \text{by} \quad \xi_i \rightarrow d_i \bar{d}_i,$$

and prove that $L = \varphi(D_n^* \cap K)$ where K is a local regular set and where φ 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 $L = \varphi(D_n^* \cap R)$ with R local and φ ε -limited on R (i.e. $k \cdot |\varphi(w)| \geq |w|$ for all w in R and for some $k > 0$).

II.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 $\mathcal{L}$** over $X = \{a, b\}$ is the language generated by the grammar with productions

$$\xi \rightarrow a\xi\xi + b.$$

Thus $\mathcal{L}$ is the unique language satisfying

$$\mathcal{L} = a\mathcal{L}\mathcal{L} \cup b. \quad (4.1)$$

The first words of $\mathcal{L}$ are

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

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 operation, 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 $w \in X^*$, define

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

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

Proposition 4.1 Let $w \in X^*$. Then $w \in \mathcal{L}$ iff w satisfies the two following conditions:

- (i) $\|w\| = -1$;
- (ii) $\|w'\| \geq 0$ for any proper left factor w' of w .

Clearly, Proposition 4.1 implies that $\mathcal{L}$ is prefix.

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

Conversely, let w be a word satisfying (i) and (ii). If $|w| = 1$, then $w = b \in \mathcal{L}$. 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 non empty left factor u of w' such that $\|au\| = 0$. Set $w = auv$. Then $\|u\| = -1$, and for any proper left factor u' of u , $\|u'\| \geq 0$ by the minimality assumption on u . Thus $u \in \mathcal{L}$. Next $\|v\| = \|w\| = -1$, and $\|v'\| = \|auv'\| \geq 0$ for any proper left factor v' of v since w satisfies (ii). Thus $v \in \mathcal{L}$ and $w \in \mathcal{L}$ by (4.1). ■

Proposition 4.1 can be used to draw a pictorial representation of a word w in $\mathcal{L}$. This is given by the graph of the function $w' \mapsto \|w'\|$, where w' ranges over the left factors of w . Thus, for $w = aabaabbabbabaaabbbb$, we obtain Fig. II.3.

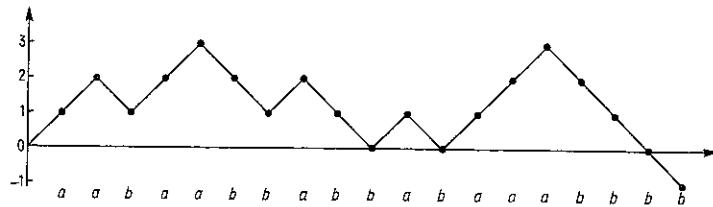


Fig. II.3

Next, consider the restricted Dyck language D_1^* over X , i.e. with $x_1 = a$, $\bar{x}_1 = b$; 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 solution of (4.1), and therefore $D_1^*b \in \mathcal{L}$.

Corollary 4.2 Let $w \in X^*$. Then $w \in D_1^*$ iff w satisfies:

- (i) $\|w\| = 0$;
- (ii) $\|w'\| \geq 0$ for any left factor w' of w .

Recall that u and v are conjugate iff $u = fg$ and $v = gf$ for some words f, g .

Proposition 4.3 Let $u \in X^*$ with $\|u\| = -1$. Then there exists one and only one word v conjugate to u such that $v \in \mathcal{L}$.

Proof. We show first the unicity. Assume $u = fg$, $v = gf \in \mathcal{L}$, $g \neq 1$. Then by Proposition 4.1 $\|f\| \geq 0$, thus $\|u\| = -1 = \|f\| + \|g\| \geq \|g\|$, and g cannot be a proper left factor of v . Thus $f = 1$ and $u = v$.

Next, let $p = \min \{\|u'\| : u' \text{ proper left factor of } u\}$. If $p \geq 0$, then $u \in \mathcal{L}$. Assume $p < 0$, and let f be the shortest left factor of u such that $\|f\| = p$. Write $u = fg$. Then

$$\|f'\| \geq p + 1 \quad \text{for any proper left factor } f' \text{ of } f \quad (4.2)$$

by the minimality of f . Next

$$\|g'\| \geq 0 \quad \text{for any proper left factor } g' \text{ of } g \quad (4.3)$$

since $p \leq \|fg'\| = p + \|g'\|$ by definition of p and

$$\|g\| = -1 - p \geq 0. \quad (4.4)$$

Let $v = gf$. Then $\|v\| = \|u\| = -1$. Let v' be a proper left factor of v . If v' is a left factor of g , then $\|v'\| \geq 0$ by (4.3) and (4.4). Otherwise, $v' = gf'$ where f' is a proper left factor of f , and $\|v'\| = -1 - p + \|f'\| \geq 0$ by (4.2). In view of Proposition 4.1, $v \in \mathcal{L}$. ■

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

$$\xi \rightarrow a\xi b\xi c + d.$$

Thus E is the unique language satisfying

$$E = aEbEc \cup d. \quad (4.5)$$

The first words of E are

$$d, adbd, aadbdc, adbadbdc, aadbdbdc, aadbdcadbdc, \dots$$

The terminology is from M. Nivat [1967]. Write indeed “(” for “ a ”, “)” for “ c ”, “+” for “ b ” and “ i ” for “ d ”. The words listed above become

$$i, (i+i), ((i+i)+i), (i+(i+i)), ((i+i)+(i+i)), \dots$$

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 $\mathcal{L}$ over $\{a, d\}$. 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, non empty left (resp. right) factor 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 η be the congruence over X^* 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, $u = v = d \pmod{\eta}$, thus $w = adbdc \equiv d \pmod{\eta}$. This shows the inclusion $E \subset [d]_\eta$.

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

$$w \in E \Leftrightarrow w' \in E. \quad (4.6)$$

We verify (4.6) by induction on $|w| = |w'| - 4$. If $u = 1$, then $w \in E$ iff $w = d$, and $w' \in E$ iff $w' = adbdc$, 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 $aw'_1bw_2c = w' \in E$ by (4.5). The second case handles in the same way. Conversely, suppose $w' \in E$. Then

$$w' = uadbdcv = aw'_1bw'_2c$$

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 $|dcv| < |w'_2c|$. It suffices to consider the first case. Clearly, it implies that $|uadbdc| \leq |aw'_1|$, 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

$$aw_1bw'_2c = w \in E. \quad \blacksquare$$

Theorem 4.5 admits the following

Corollary 4.6 *Let $u, u' \in E$. Then $fug \in E$ iff $fu'g \in E$.*

Proof. $fug = fu'g \pmod{\eta}$. Thus $fug = d \pmod{\eta}$ iff $fu'g = d \pmod{\eta}$. $\blacksquare$

Exercises

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

4.2 Let $p_n = \text{Card}(X^{2n+1} \cap E)$. Show that $p_n = \frac{1}{n+1} \binom{2n}{n}$. Show that $p_n = q_n$, where $q_n = \text{Card}(X^{4n+1} \cap E)$.

III Rational Transductions

Rational transductions are defined by rational relations, i.e. 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.

III.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 one can try to 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 [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 the 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 second 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 the characterization via a morphism into a finite monoid. This simplifies the exposition.

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

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

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

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

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

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

Example 1.4 Consider the additive group $\mathbb{Z}$ of integers. Let α be a morphism from $\mathbb{Z}$ onto a finite monoid N . Then α 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 $\{0, 1, \dots, n-1\}$, 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 $A \in \text{Rec}(\mathbb{Z})$ iff A 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 $\text{Rec}(M)$ is closed under union, intersection and complementation.

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

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

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

Corollary 1.2 If $A, B \in \text{Rec}(M)$, then $A \setminus B \in \text{Rec}(M)$. ■

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

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

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

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

Corollary 1.4 Let γ be an isomorphism from M onto M' . Then $A \in \text{Rec}(M)$ iff $\gamma(A) \in \text{Rec}(M')$. ■

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

Example 1.5 Let $X = \{x, y\}$, and let $\gamma: X^* \rightarrow \mathbb{Z}$ be the morphism defined by $\gamma(f) = |f|_x - |f|_y$ ($f \in X^*$). Then $\{1\} \in \text{Rec}(X^*)$, and $\gamma(\{1\}) = \{0\}$. In view of Example 1.4, $\{0\} \notin \text{Rec}(\mathbb{Z})$. This can also be seen by applying Proposition 1.3. Assume indeed $\{0\} \in \text{Rec}(\mathbb{Z})$. Then $\gamma^{-1}(\{0\})$ is a recognizable subset of X^* , i.e. a regular language. Since $\gamma^{-1}(0) = D_1^*$, the Dyck language over X (Exercise II.3.6), this yields a contradiction.

In general, the family $\text{Rec}(M)$ 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 ε, a . The set $M = \mathbb{Z} \cup \{\varepsilon, a\}$ is a commutative monoid with addition extended as follows:

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

Thus ε is the neutral element of M . We first show that $\{\varepsilon\}, \{a\} \in \text{Rec}(M)$. 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 $\alpha: M \rightarrow N$ 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 $A \in \text{Rec}(M)$, then $A \cap \mathbb{Z} \in \text{Rec}(\mathbb{Z})$. Let indeed β be a morphism from M onto a finite monoid N' , let β_1 be the restriction of β on $\mathbb{Z}$, and set $N_1 = \beta_1(\mathbb{Z})$.

If $A = \beta^{-1}(P)$ for $P \subset N'$, then

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

Consequently $A \cap \mathbb{Z} \in \text{Rec}(\mathbb{Z})$. Define now $A = \{a\}$. Then $A \in \text{Rec}(M)$, and $A + A = \{0\}$, $A^+ = \{0, a\}$, $A^* = \{0, \varepsilon, a\}$. None of these subsets is in $\text{Rec}(M)$, 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 $B \in \text{Rec}(M)$ iff B is a finite union of sets of the form $A_1 \times A_2$, with $A_1 \in \text{Rec}(M_1)$ and $A_2 \in \text{Rec}(M_2)$.*

Proof. The condition is sufficient. Let indeed $\pi_i: M \rightarrow M_i$, ($i = 1, 2$) be the canonical projections. If $A_1 \subset M_1$, $A_2 \subset M_2$, then

$$A_1 \times A_2 = (A_1 \times M_2) \cap (M_1 \times A_2) = \pi_1^{-1}(A_1) \cap \pi_2^{-1}(A_2).$$

Thus if $A_1 \in \text{Rec}(M_1)$, $A_2 \in \text{Rec}(M_2)$, then $A_1 \times A_2 \in \text{Rec}(M)$ in view of Propositions 1.3 and 1.1. Since $\text{Rec}(M)$ is closed under union, $B \in \text{Rec}(M)$.

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

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

and let $\gamma: M \rightarrow N \times N$ 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 $\gamma(m_1, m_2) \in Q$ iff $\alpha_1(m_1) \alpha_2(m_2) \in P$. Since

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

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

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

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

Exercises

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

1.2 Let M be a monoid. Define a finite automaton $\mathbf{A}$ over M by a finite set of states Q , an initial state q_- , a set of final states Q_+ , and a next state function $Q \times M \rightarrow Q$ 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 $\mathbf{A}$ is by definition $|\mathbf{A}| = \{m \in M \mid q_- \cdot m \in Q_+\}$. Show that $A \in \text{Rec}(M)$ iff A 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 $A \in \text{Rec}(G)$ iff there exists an invariant subgroup H of G of finite index (i.e. G/H is finite) such that A is a union of cosets of H . Show that a subgroup of G is recognizable iff it is of finite index.

1.4 Let M be a monoid, $A \in \text{Rec}(M)$. Show that for any $B \subset M$, $B^{-1}A = \{m \mid Bm \cap A \neq \emptyset\}$ is a recognizable subset of M . (Hint. Use Exercise 1.3.6.)

III.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 $\text{Rat}(M)$ of rational subsets of M is the least family $\mathcal{R}$ of subsets of M satisfying the following conditions:

- (i) $\emptyset \in \mathcal{R}; \{m\} \in \mathcal{R}$ for all $m \in M$; (2.1)
- (ii) if $A, B \in \mathcal{R}$, then $A \cup B, AB \in \mathcal{R}$; (2.2)
- (iii) if $A \in \mathcal{R}$, then $A^+ = \bigcup_{n \geq 1} A^n \in \mathcal{R}$. (2.3)

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

$$(iii') \quad A \in \mathcal{R} \Rightarrow A^* \in \mathcal{R}.$$

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

Any subset A of M obtained from the singletons by a finite number of unions, products and plus or star operations is in $\text{Rat}(M)$. 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 $\text{Rat}(M)$. 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 X be an alphabet, and $X^\oplus$ be the free commutative monoid generated by X . We claim that A is a rational subset of $X^\oplus$ iff A is a finite union of sets of the form

$$ab_1^*b_2^*\cdots b_n^* \quad (n \geq 0, a, b_1, \dots, b_n \in X^\oplus). \quad (2.4)$$

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 $A, B \subset X^\oplus$, then $(A \cup B)^* = A^*B^*$ and $(ab_1^*b_2^*\cdots b_n^*)^* = a^*b_1^*\cdots b_n^*$. This shows that semilinear sets are closed under 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 $X^\oplus$.

Example 2.3 If X 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 X be a (finite) alphabet. Then $\text{Rat}(X^*) = \text{Rec}(X^*)$.*

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 $\alpha: M \rightarrow M'$ be a morphism. If $A \in \text{Rat}(M)$, then $\alpha(A) \in \text{Rat}(M')$. Further if α is surjective, then for any $A' \in \text{Rat}(M')$ there is a set $A \in \text{Rat}(M)$ such that $\alpha(A) = A'$.*

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

$$\alpha(A \cup B) = \alpha(A) \cup \alpha(B), \quad \alpha(AB) = \alpha(A)\alpha(B), \quad \alpha(A^+) = (\alpha(A))^+ \quad (2.5)$$

for any subsets A, B of M . Thus $A, B \in \mathcal{R}$ implies that $A \cup B, AB, A^+ \in \mathcal{R}$. Thus $\mathcal{R}$ satisfies conditions (2.1), (2.2), (2.3). Consequently $\mathcal{R} \supset \text{Rat}(M)$ and the first statement is proved. Consider now the family $\mathcal{S}$ of subsets A' of M' such that $A' = \alpha(A)$ for some $A \in \text{Rat}(M)$. Since α 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 $\mathcal{S} \supset \text{Rat}(M')$. ■

Corollary 2.3 *Let α be an isomorphism from M onto M' . Then $A \in \text{Rat}(M)$ iff $\alpha(A) \in \text{Rat}(M')$.* ■

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

Example 2.4 Consider as in Example 1.5 the alphabet $X = \{x, y\}$ and the morphism $\gamma: X^* \rightarrow \mathbb{Z}$ defined by $\gamma(f) = |f|_x - |f|_y$ ($f \in X^*$). Then $\{0\} \in \text{Rat}(\mathbb{Z})$, and $\gamma^{-1}(0) = \{f \in X^* \mid |f|_x = |f|_y\} = D_1^* \notin \text{Rat}(X^*)$.

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 $\text{Rec}(M) \subset \text{Rat}(M)$.*

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

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

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

Proof. Let $\mathcal{R}$ be the family of subsets A 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 $A, B \in \mathcal{R}$, and let R, S be finite subsets of M such that $A \subset R^*$, $B \subset S^*$. Then $A \cup B, AB \subset (R \cup S)^*$ and $A^* \subset R^*$. Consequently $A \cup B, AB, A^* \in \mathcal{R}$ and $\mathcal{R} \supset \text{Rat}(M)$. ■

Proposition 2.6 *Let M be a monoid. If $A \in \text{Rat}(M)$ and $B \in \text{Rec}(M)$, then $A \cap B \in \text{Rat}(M)$.*

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

$$\alpha(C') = \alpha(A' \cap \alpha^{-1}(B)) = \alpha(A') \cap B = A \cap B,$$

it follows that $A \cap B \in \text{Rat}(M)$. ■

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

Example 2.5 Let $M = \{x\}^* \times \{y, z\}^*$, and consider the sets

$$A = (x, y)^*(1, z)^* = \{(x^n, y^n z^k) : n, k \geq 0\},$$

$$B = (1, y)^*(x, z)^* = \{(x^n, y^k z^n) : n, k \geq 0\}.$$

Clearly, $A, B \in \text{Rat}(M)$. Suppose that

$$C = A \cap B = \{(x^n, y^n z^n) : n \geq 0\}$$

is rational, and define a morphism $\pi : M \rightarrow \{y, z\}^*$ by $\pi(x, 1) = 1$, $\pi(1, y) = y$, $\pi(1, z) = z$. Then $\pi(C) = \{y^n z^n : n \geq 0\}$ would be a rational subset of $\{y, z\}^*$ by Proposition 2.2. Thus C is not rational.

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

$$A \in \text{Rat}_0(M) \text{ iff } A \text{ is a finite subset of } M;$$

$$A \in \text{Rat}_{h+1}(M) \text{ iff } A \text{ is a finite union of sets of the form } B_1 B_2 \dots B_n,$$

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

$$\text{Rat}(M) = \bigcup_{h \geq 0} \text{Rat}_h(M).$$

The sets in $\text{Rat}_h \setminus \text{Rat}_{h-1}$ 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 (Anissimov and Seifert [1975]) *Let G be a group, and let H be a subgroup of G . Then H is finitely generated iff H is a rational subset of G .*

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

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

$$A = x_1 T_1^* x_2 T_2^* \dots x_n T_n^* x_{n+1} \quad (2.6)$$

with $x_1, \dots, x_{n+1} \in G$, $T_1, \dots, T_n \subset G$, and define

$$y_i = x_1 x_2 \dots x_i \quad i = 1, \dots, n+1 \quad (2.7)$$

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

$$A' = y_{n+1} \cup S_1 \cup \dots \cup S_n. \quad (2.8)$$

Then we claim:

$$\langle A \rangle = \langle A' \rangle. \quad (2.9)$$

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

$$S_i = (x_1 \dots x_i T_i x_{i+1} \dots x_{n+1}) y_{n+1}^{-1}.$$

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

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

Since $x_1 = y_1$ and $x_i = y_{i-1}^{-1} y_i$, ($2 \leq i \leq n+1$),

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

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

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

$$R = A_1 \cup A_2 \cup \dots \cup A_r,$$

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

$$R' = A'_1 \cup A'_2 \cup \dots \cup A'_r,$$

where each A'_k is deduced from A_k by (2.7) and (2.8). Then clearly R' has starheight $h-1$. By (2.9), each A_k is contained in $\langle R' \rangle$, and conversely each A'_k is contained in R . Thus $\langle R \rangle = \langle R' \rangle = H$, and R' is a system 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 $X = \{x_1, \dots, x_n\}$, let $\bar{X} = \{\bar{x} \mid x \in X\}$ and set $Z = X \cup \bar{X}$. Let $X^{(*)}$ be the free group generated by X (see Section II.3), and let $\delta : Z^* \rightarrow X^{(*)}$ be the canonical morphism. As already mentioned, there exists an injection $\iota : X^{(*)} \rightarrow Z^*$ which associates to each element $u \in X^{(*)}$ the unique reduced word $\iota(u) = f \in \rho(Z^*)$ such that $\delta(f) = u$. The following result describes a property of the mapping ρ .

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

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

Theorem 2.9 (Benois [1969]) *Let $K \subset X^{(*)}$. Then $K \in \text{Rat}(X^{(*)})$ iff $\iota(K)$ is a regular language.*

Proof. Let $K \in \text{Rat}(X^{(*)})$. In view of Proposition 2.2, there exists a regular language $K' \subset Z^*$ 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 $\iota(K) \in \text{Rat}(Z^*)$. Then the homomorphic image $\delta(\iota(K)) = K$ is in $\text{Rat}(X^{(*)})$ by Proposition 2.2. ■

The following corollary is interesting:

Corollary 2.10 (Fliess [1971]) $\text{Rat}(X^{(*)})$ is closed under intersection and

Proof. It suffices to show closure under complementation. Let $K \in \text{Rat}(X^{(*)})$. Then $\iota(K) \in \text{Rat}(Z^*)$ by Theorem 2.9. Next $\rho(Z^*)$ is regular, thus $\rho(Z^*) \setminus \iota(K)$ is regular. Since $\iota(K) \subset \rho(Z^*)$, it follows that $\delta(\rho(Z^*) \setminus \iota(K)) = X^{(*)} \setminus K \in \text{Rat}(X^{(*)})$ 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 Y , and let $A \subset Y^*$ be an arbitrary language. Define a function λ_A from Y^* into the subsets of Y^* as follows. For $w, w' \in Y^*$, $w' \in \lambda_A(w)$ iff there exists a factorization

$$w = a_0 x_1 a_1 x_2 \cdots a_{r-1} x_r a_r,$$

with $r \geq 0$, $a_0, a_1, \dots, a_r \in A$, $x_1, \dots, x_r \in Y$ such that

$$w' = x_1 x_2 \cdots x_r.$$

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

Lemma 2.11 For any $A \subset Y^*$, and for any regular language $K \subset Y^*$, $\lambda_A(K)$ is a regular language.

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

$$\begin{aligned} q \in p \cdot x & \text{ iff } xA \cap K_{p,q} \neq \emptyset & x \in Y, \quad p, q \in Q; \\ q \in s \cdot x & \text{ iff } Ax \cap K_{q,q} \neq \emptyset & x \in Y, \quad q \in Q. \end{aligned}$$

Next let

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

Then clearly

$$\lambda_A(K) = |B| = \{f \in Y^* \mid s \cdot f \cap Q' \neq \emptyset\}.$$

Proof of Proposition 2.8. Choose in Lemma 2.11 $A = D_n^* = \rho^{-1}(1)$, and $Y = Z$. Then for $f \in Z^*$

$$\rho(f) = \lambda_{D_n^*}(f) \cap \rho(Z^*).$$

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

Exercises

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

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

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 (Anissimov 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 $X^{(*)}$, $\delta^{-1}(K)$ 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, ρ can be replaced by ρ' and in fact by ρ_r as defined in Section II.3.

III.3 Rational Relations

A relation can be considered as a subset of the cartesian product of two sets, or as 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 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 X and Y be alphabets. A rational (resp. recognizable) relation over X and Y is a rational (resp. recognizable) subset of the monoid $X^* \times Y^*$.

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

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

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

Proof. (i) Since $X^* \times Y^*$ is a finitely generated monoid, the inclusion $\text{Rec}(X^* \times Y^*) \subset \text{Rat}(X^* \times Y^*)$ follows from Proposition 2.4. To show that the inclusion is proper, let $x \in X$, $y \in Y$ and consider $A = (x, y)^* = \{(x^n, y^n) : n \geq 0\}$. Clearly A is a rational relation. Assume A is recognizable, let $Z = \{\bar{x}, \bar{y}\}$, and consider the morphism $\gamma : Z^* \rightarrow X^* \times Y^*$ defined by $\gamma(\bar{x}) = (x, 1)$, $\gamma(\bar{y}) = (1, y)$.

Then $\gamma^{-1}A = \{f \in Z^* \mid |f|_x = |f|_y\}$ is recognizable, thus a regular language. This yields the contradiction.

(ii) In view of Mezei's Theorem,

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

with $R_i, R'_j \in \text{Rat}(X^*)$, $S_i, S'_j \in \text{Rat}(Y^*)$. Consequently

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

and $R_i R'_j \in \text{Rat}(X^*)$, $S_i S'_j \in \text{Rat}(Y^*)$. By Mezei's Theorem, $AB \in \text{Rec}(X^* \times Y^*)$. ■

We extend the notion of copy defined in Section I.3 as follows: $X^* \times Y^*$ is a copy of $X'^* \times Y'^*$ if X^* is a copy of X'^* and Y^* is a copy of Y'^* . Then $X^* \times Y^*$ and $X'^* \times Y'^*$ are isomorphic, and recognizable and rational relations are preserved through the 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 monoid, 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 iff it is closed under morphism, inverse morphism and intersection with regular sets.

Theorem 3.2 (Nivat [1968]) *Let X and Y be alphabets. The following conditions are equivalent:*

- (i) $A \in \text{Rat}(X^* \times Y^*)$;
- (ii) *There exist an alphabet Z , two morphisms $\varphi: Z^* \rightarrow X^*$, $\psi: Z^* \rightarrow Y^*$ and a regular language $K \subset Z^*$ such that*

$$A = \{(\varphi h, \psi h) : h \in K\};$$

- (iii) *There exist an alphabet Z , two alphabetic morphisms $\alpha: Z^* \rightarrow X^*$, $\beta: Z^* \rightarrow Y^*$ and a regular language $K \subset Z^*$ such that*

$$A = \{(\alpha h, \beta h) : h \in K\};$$

- (iv) *There exist an alphabet Z , two alphabetic morphisms $\alpha: Z^* \rightarrow X^*$, $\beta: Z^* \rightarrow Y^*$ and a local regular language $K \subset Z^*$ such that*

$$A = \{(\alpha h, \beta h) : h \in K\};$$

if $X \cap Y = \emptyset$, then (i) is equivalent to

- (v) *There exists a regular language $K \subset (X \cup Y)^*$ such that*

$$A = \{(\pi_X h, \pi_Y h) : h \in K\},$$

where π_X and π_Y are the projections of $(X \cup Y)^*$ onto X^* and Y^* respectively.

A couple (φ, ψ) of morphisms $\varphi: Z^* \rightarrow X^*$ and $\psi: Z^* \rightarrow Y^*$ is called a bimorphism.

Proof. The implications (iv) $\Rightarrow$ (iii) $\Rightarrow$ (ii) are obvious. We prove (ii) $\Rightarrow$ (i). Define $\gamma: Z^* \rightarrow X^* \times Y^*$ by $\gamma h = (\varphi h, \psi h)$ ($h \in Z^*$). Then γ is a morphism and $\gamma(K) = A$. Since $K \in \text{Rat}(Z^*)$, $A \in \text{Rat}(X^* \times Y^*)$ by Proposition 2.2. Next, we prove (iii) $\Rightarrow$ (iv). There exist an alphabet Z' , an alphabetic morphism $\gamma: Z'^* \rightarrow Z^*$ and a local regular language $K' \subset Z'^*$ such that $\gamma(K') = K$ (see for instance Section I.4). Thus $A = \{(\alpha(\gamma h'), \beta(\gamma h')) : h' \in K'\}$ and the morphisms $\alpha \circ \gamma, \beta \circ \gamma$ are alphabetic.

Assume now $X \cap Y = \emptyset$, and define $\pi: (X \cup Y)^* \rightarrow X^* \times Y^*$ by $\pi h = (\pi_X h, \pi_Y h)$. Obviously π is a surjective morphism. Thus if $A \in \text{Rat}(X^* \times Y^*)$ there exists, by the second part of Proposition 2.2, a regular language $K \subset (X \cup Y)^*$ such that $\pi(K) = A$. This proves (i) $\Rightarrow$ (v).

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

Finally we prove (i) $\Rightarrow$ (iii). Assume $A \in \text{Rat}(X^* \times Y^*)$. If $X \cap Y = \emptyset$, then (iii) follows from (v). Otherwise, let $X'^* \times Y'^*$ be a copy of $X^* \times Y^*$ with $X' \cap Y' = \emptyset$, let $\omega_X: X^* \rightarrow X'^*$, $\omega_Y: Y^* \rightarrow Y'^*$ be the copy isomorphisms and set $A' = \{(\omega_X f, \omega_Y g) : (f, g) \in A\}$. Then A' is a rational relation, and in view of (v) $A' = \{(\pi_{X'} h, \pi_{Y'} h) : h \in K\}$ for some regular language $K \subset (X' \cup Y')^*$. Consequently, $A = \{((\omega_X^{-1} \circ \pi_X)h, (\omega_Y^{-1} \circ \pi_Y)h) : h \in K\}$. ■

Theorem 3.2 can be used to derive an iteration lemma for rational relations.

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

$$(f, f') = (a, a')(u, u')(b, b') \quad a, u, b \in X^*, \quad a', u', b' \in Y^*$$

such that

- (i) $0 < |u| + |u'| \leq N$;
- (ii) $(a, a')(u, u')^* (b, b') \subset A$.

Proof. After a copy, we may assume $X \cap Y = \emptyset$, and by Theorem 3.2(v), $A = \{(\pi_X h, \pi_Y h) : h \in K\}$ for some regular language K . Since $|h| = |\pi_X h| + |\pi_Y h|$, the 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 holds:

$$|a| + |a'| + |u| + |u'| \leq N.$$

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 subsets 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 A is a rational relation over M and M' iff there exist an alphabet Z , two morphisms $\alpha: Z^* \rightarrow M$, $\beta: Z^* \rightarrow M'$ and a regular language $K \subset Z^*$ such that $A = \{(\alpha h, \beta h) : h \in K\}$.*

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

Exercises

3.1 Let M be a finitely generated, infinite monoid. Show that $A = \{(m, m) : m \in M\}$ is a rational and not recognizable subset of $M \times M$.

3.2 Let X be an alphabet with at least two letters. Show that the relation $R = \{(f, \tilde{f}) : f \in X^*\}$ is not rational.

3.3 Give a counter example to the following version of the Iteration Lemma: For $A \in \text{Rat}(X^* \times Y^*)$ there is an integer $N \geq 1$ such that for any $(g, g') \in A$, and for any factorization

$$(g, g') = (h_1, h'_1)(f, f')(h_2, h'_2) \quad \text{with} \quad |f| + |f'| \geq N,$$

(f, f') admits a factorization $(f, f') = (a, a')(u, u')(b, b')$ such that $0 < |u| + |u'| \leq N$ and

$$(h_1, h'_1)(a, a')(u, u')^*(b, b')(h_2, h'_2) \subset A.$$

3.4 A right linear system of equations over $X^* \times Y^*$ is a system of equations of the form

$$\xi_i = \sum_{j=1}^N C_{ij} \xi_j + B_i \quad i = 1, \dots, N,$$

where $C_{ij}, B_i \subset X^* \times Y^*$. The system is strict iff $(1, 1) \in C_{ij}$ for $j = 1, \dots, N$. A vector $A = (A_1, \dots, A_N)$ of subsets of $X^* \times Y^*$ is a solution of the system iff

$$A_i = \bigcup_{j=1}^N (C_{ij} A_j \cup B_i) \quad i = 1, \dots, N.$$

- Show that a strict right linear system has a unique solution.
- Show that $R \subset X^* \times Y^*$ is a rational relation iff R is a component of the solution of a strict right linear system of equations with C_{ij}, B_i finite. (Hint. Use the fact that a) and b) hold in free monoids and apply Nivat's Theorem.)

III.4 Rational Transductions

The "static" notion of rational relation is now transformed into the "dynamic" notion of rational transduction.

A transduction τ from X^* into Y^* is a function from X^* into the set $\mathfrak{P}(Y^*)$ of subsets of Y^* . For commodity, we write $\tau: X^* \rightarrow Y^*$. The domain $\text{dom}(\tau)$ and the image $\text{im}(\tau)$ are defined by

$$\text{dom}(\tau) = \{f \in X^* : \tau(f) \neq \emptyset\};$$

$$\text{im}(\tau) = \{g \in Y^* \mid \exists f \in X^* : g \in \tau(f)\}.$$

The transduction τ is extended to a mapping from $\mathfrak{P}(X^*)$ into $\mathfrak{P}(Y^*)$ by setting

$$\tau(A) = \bigcup_{f \in A} \tau(f) \quad A \subset X^*.$$

The graph of τ is the relation R defined by

$$R = \{(f, g) \in X^* \times Y^* \mid g \in \tau(f)\}.$$

Conversely, for any relation $R \subset X^* \times Y^*$, the transduction $\tau: X^* \rightarrow Y^*$ defined by R is given by

$$\tau(f) = \{g \in Y^* \mid (f, g) \in R\}.$$

Definition A transduction $\tau: X^* \rightarrow Y^*$ is rational iff its graph R is a rational relation over X and Y .

Let $\tau: X^* \rightarrow Y^*$ be a rational transduction, and let $R \subset X^* \times Y^*$ be the graph of τ . The monoids $X^* \times Y^*$ and $Y^* \times X^*$ are isomorphic. Thus the relation

$$R^{-1} = \{(g, f) \mid (f, g) \in R\}$$

is rational, and the transduction $\tau^{-1}: Y^* \rightarrow X^*$ defined by R^{-1} is rational. τ^{-1} is the inverse transduction of τ . Clearly

$$\tau^{-1}(B) = \{f \in X^* \mid \tau(f) \cap B \neq \emptyset\} \quad B \subset Y^*.$$

In general, $\tau(\tau^{-1}(B)) \neq B$, and $\tau^{-1}(\tau(A)) \neq A$, ($A \subset X^*$). The domain $\text{dom}(\tau)$ and the image $\text{im}(\tau)$ are homomorphic images of the rational relation R , and consequently are regular languages.

Let $\tau_1, \tau_2: X^* \rightarrow Y^*$ be rational transductions and let R_1, R_2 be the graphs of τ_1 and τ_2 . We denote by $\tau_1 \cup \tau_2$, $\tau_1 \tau_2$ and τ_1^+ the transductions with graphs $R_1 \cup R_2$, $R_1 R_2$, R_1^+ . Obviously, these transductions are rational. They verify:

$$(\tau_1 \cup \tau_2)(f) = \tau_1(f) \cup \tau_2(f); \quad (\tau_1 \tau_2)(f) = \bigcup_{f_1 f_2 = f} \tau_1(f_1) \tau_2(f_2);$$

$$\tau_1^+(f) = \bigcup \{\tau_1(f_1) \cdots \tau_1(f_n) \mid n \geq 1, f_1 \cdots f_n = f\}.$$

If $\text{dom}(\tau_1) \cap \text{dom}(\tau_2) = \emptyset$, we also write $\tau_1 + \tau_2$ instead of $\tau_1 \cup \tau_2$. Finally, we associate to $\tau: X^* \rightarrow Y^*$ a transduction $\tilde{\tau}: X^* \rightarrow Y^*$ by setting $\tilde{\tau}(f) = (\tau(f))^-$.

Let R be the graph of τ , and let $\tilde{R}$ be the graph of $\tilde{\tau}$. Then $\tilde{R} = \{(\tilde{f}, \tilde{g}) \mid (f, g) \in R\}$. The formulas

$$(A \cup B)^- = \tilde{A} \cup \tilde{B}; \quad (AB)^- = \tilde{B}\tilde{A}; \quad (A^+)^- = (\tilde{A})^+ \quad (A, B \subset X^* \times Y^*)$$

show that R is rational iff $\tilde{R}$ is rational. Thus the transduction $\tilde{\tau}$, the reversal of τ is rational iff τ is rational.

Nivat's Theorem proved in the preceding section can be formulated as follows for rational transductions.

Theorem 4.1 (Nivat [1968]) *Let X and Y be alphabets. The following conditions are equivalent:*

- (i) $\tau: X^* \rightarrow Y^*$ is a rational transduction;
- (ii) There exist an alphabet Z , two morphisms $\varphi: Z^* \rightarrow X^*$, $\psi: Z^* \rightarrow Y^*$ and a regular language $K \subset Z^*$ such that

$$\tau(f) = \psi(\varphi^{-1}(f) \cap K) \quad f \in X^*; \quad (4.1)$$

- (iii) There exist an alphabet Z , two alphabetic morphisms $\alpha: Z^* \rightarrow X^*$, $\beta: Z^* \rightarrow Y^*$ and a regular language $K \subset Z^*$ such that

$$\tau(f) = \beta(\alpha^{-1}(f) \cap K) \quad (f \in X^*);$$

- (iv) There exist an alphabet Z , two alphabetic morphisms $\alpha: Z^* \rightarrow X^*$, $\beta: Z^* \rightarrow Y^*$ and a local regular language $K \subset Z^*$ such that

$$\tau(f) = \beta(\alpha^{-1}(f) \cap K) \quad f \in X^*;$$

further if $X \cap Y = \emptyset$, then (i) is equivalent to

- (v) There exists a regular language $K \subset (X \cup Y)^*$ such that

$$\tau(f) = \pi_Y(\pi_X^{-1}(f) \cap K) \quad f \in X^*,$$

where π_X and π_Y are the projections of $(X \cup Y)^*$ onto X^* and Y^* respectively. ■

From (4.1), we deduce immediately that

$$\tau^{-1}(g) = \varphi(\psi^{-1}(g) \cap K) \quad g \in Y^*.$$

It follows also from (4.1) that

$$\tau(A) = \psi(\varphi^{-1}(A) \cap K) \quad A \subset X^*.$$

Thus:

Corollary 4.2 *Each rational transduction preserves rational and algebraic languages. That is, for each rational transduction τ , $\tau(A)$ is rational if A is rational, and $\tau(A)$ is algebraic if A is algebraic.* ■

Example 4.1 Let $X = \{x, y\}$, $Y = \{a, b\}$, and consider the transduction $\tau: X^* \rightarrow Y^*$ defined by

$$\tau(f) = \begin{cases} \emptyset & \text{if } f \notin x^+y^*; \\ (a^+b)^n a^{2m}b & \text{if } f = x^n y^m, \quad n \geq 1, \quad m \geq 0. \end{cases}$$

Obviously $\text{dom}(\tau) = x^+y^*$, $\text{im}(\tau) = (a^+b)^+(a^2)^*b$. We claim that the transduction τ is rational. This can be shown in several ways. First, let R be the graph of τ . Then

$$R = (\{x\} \times a^+b)^+(y, a^2)^*(1, b) \in \text{Rat}(X^* \times Y^*).$$

Next let $Z = \{r, s, t, u\}$ and define $\varphi: Z^* \rightarrow X^*$, $\psi: Z^* \rightarrow Y^*$ by

$$\varphi r = x, \quad \varphi s = 1, \quad \varphi t = y, \quad \varphi u = 1;$$

$$\psi r = b, \quad \psi s = a, \quad \psi t = a^2, \quad \psi u = b.$$

Let $K = (s^+r)^+t^*u$. Then $\varphi K = x^+y^*$, $\psi K = (a^+b)^+(a^2)^*b$. Further

$$\varphi^{-1}(x^n y^m) \cap K = (s^+r)^n t^m u \quad n \geq 1, \quad m \geq 0,$$

thus $\tau(f) = \psi(\varphi^{-1}(f) \cap K)$ for all $f \in X^*$.

Finally, since $X \cap Y = \emptyset$, we can represent τ by projections. Consider indeed the regular language

$$K' = xa\{a, bxa\}^*b(ya^2)^*b \subset (X \cup Y)^*.$$

Then $\pi_X(K') = xX^*$. Next if $f = x^n y^m$, ($n \geq 1, m \geq 0$), then

$$\pi_X^{-1}(f) \cap K' = xa(a^*bxa)^{n-1}a^*b(ya^2)^m b,$$

$$\pi_Y(\pi_X^{-1}(f) \cap K') = a(a^*ba)^{n-1}a^*ba^{2m}b = (a^+b)^n a^{2m}b.$$

As for rational relations, the definition of rational transductions can be extended to arbitrary monoids.

Definition Let M, M' be monoids. A rational transduction $\tau: M \rightarrow M'$ is a function from M into $\mathfrak{P}(M')$ such that the graph $R = \{(m, m') \mid m' \in \tau(m)\}$ of τ 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 $\tau: M \rightarrow M'$ is rational iff there exist an alphabet Z , two morphisms $\alpha: Z^* \rightarrow M$, $\beta: Z^* \rightarrow M'$ and a rational language $K \subset Z^*$ such that*

$$\tau(m) = \beta(\alpha^{-1}(m) \cap K) \quad m \in M. \quad \blacksquare$$

If $A \subset M$, then

$$\tau(A) = \beta(\alpha^{-1}(A) \cap K). \quad (4.2)$$

Thus, if A is a recognizable subset of M , then $\alpha^{-1}(A)$ is recognizable, hence regular, $\alpha^{-1}(A) \cap K$ is regular, hence rational, and finally $\tau(A)$ is a rational subset of M' . Note that $\tau(A)$ is not necessarily recognizable, and that $\tau(A)$ is not necessarily rational if A is rational. This follows from Examples 1.5; 2.4, since morphisms and inverse morphisms are particular rational transductions.

We now consider composition of rational transductions. If $\tau: M \rightarrow M'$ and $\tau': M' \rightarrow M''$ are transductions, then the composition $\tau' \circ \tau: M \rightarrow M''$ 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 X, Y, Z be alphabets, and let $\tau: X^* \rightarrow Y^*$ and $\tau': Y^* \rightarrow Z^*$ be rational transductions. Then the transduction $\tau' \circ \tau: X^* \rightarrow Z^*$ is rational.*

We first prove the theorem in a special case. The general case follows then from this special case.

Lemma 4.5 *Let X, Y, Z be three pairwise disjoint alphabets. Set $X' = X \cup Y$, $Z' = Y \cup Z$, $T = X \cup Y \cup Z$ and let*

$$\alpha: X'^* \rightarrow Y^*, \quad \beta: Z'^* \rightarrow Y^*, \quad \alpha': T^* \rightarrow X'^*, \quad \beta': T^* \rightarrow Z'^*$$

be the projections. Then $\beta^{-1} \circ \alpha = \beta' \circ \alpha'^{-1}$.

Lemma 4.5 is represented in Fig. III.1.

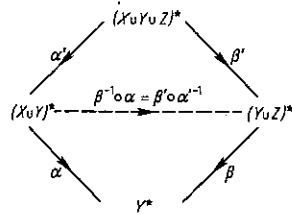


Fig. III.1

Proof. The mappings $\beta^{-1} \circ \alpha$ and $\beta' \circ \alpha'^{-1}$ are morphisms of the semigroup X'^* into the (multiplicative) semigroup $\mathfrak{B}(Y^*)$. Thus it suffices to prove that they are equal on $X' \cup 1$. First

$$\beta^{-1} \circ \alpha(1) = \beta^{-1}(1) = Z^*; \quad \beta' \circ \alpha'^{-1}(1) = \beta'(Z^*) = Z^*.$$

Then for $x \in X$, $\beta^{-1} \circ \alpha(x) = \beta^{-1}(1) = Z^*$ and $\beta' \circ \alpha'^{-1}(x) = \beta'(Z^* x Z^*) = Z^*$. Finally, if $y \in Y$, then $\beta^{-1} \circ \alpha(y) = \beta^{-1}(y) = Z^* y Z^*$ and $\beta' \circ \alpha'^{-1}(y) = \beta'(Z^* y Z^*) = Z^* y Z^*$. This proves the lemma. ■

Proof of Theorem 4.4. After a copy if necessary, we may assume that the alphabets X, Y, Z are pairwise disjoint. Set $X' = X \cup Y$, $Z' = Y \cup Z$. In view of Nivat's Theorem, there exists a regular language $K \subset X'^*$ such that

$$\tau(f) = \alpha(\pi^{-1}(f) \cap K) \quad f \in X^*, \quad (4.3)$$

where $\pi: X'^* \rightarrow X^*$ and $\alpha: X'^* \rightarrow Y^*$ are the projections. Next there is a regular language $M \subset Z'^*$ such that

$$\tau'(g) = \omega(\beta^{-1}(g) \cap M) \quad g \in Y^*, \quad (4.4)$$

where $\beta: Z'^* \rightarrow Y^*$ and $\omega: Z'^* \rightarrow Z^*$ are the projections. Thus we have Fig. III.2. According to Lemma 4.5, $\beta^{-1} \circ \alpha = \beta' \circ \alpha'^{-1}$ where $T = X \cup Y \cup Z$, and

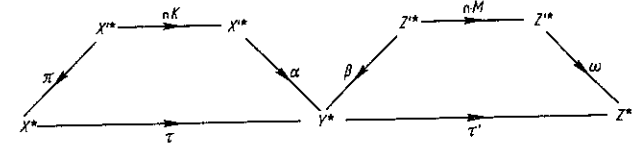


Fig. III.2

β', α' are the projections of T^* onto Z'^* and X'^* respectively. Thus the above diagram can be completed to Fig. III.3.

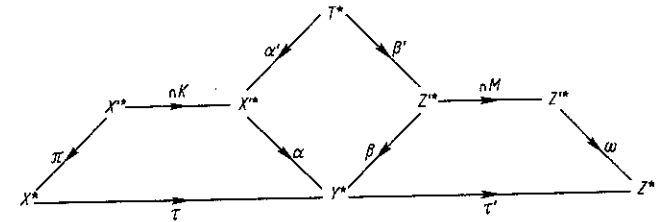


Fig. III.3

Next, setting $\tau'' = \tau' \circ \tau$, we have by (4.3), (4.4), for $f \in X^*$,

$$\tau''(f) = \omega[(\beta^{-1} \circ \alpha)(\pi^{-1}(f) \cap K) \cap M].$$

Since $\beta^{-1} \circ \alpha = \beta' \circ \alpha'^{-1}$,

$$\begin{aligned} \tau''(f) &= \omega[(\beta' \circ \alpha'^{-1})(\pi^{-1}(f) \cap K) \cap M] \\ &= \omega[\beta'((\pi \circ \alpha')^{-1}(f) \cap \alpha'^{-1}(K)) \cap M]. \end{aligned} \quad (4.5)$$

Define $\psi = \omega \circ \beta': T^* \rightarrow Z^*$, $\varphi = \pi \circ \alpha': T^* \rightarrow X^*$, and set $K' = \alpha'^{-1}(K)$, $M' = \beta'^{-1}(M)$, $N = K' \cap M'$. Then (4.5) implies

$$\begin{aligned} \tau''(f) &= \omega[\beta'(\varphi^{-1}(f) \cap K') \cap M] = \omega[\beta'(\varphi^{-1}(f) \cap K' \cap M')] \\ &= \psi(\varphi^{-1}(f) \cap N). \end{aligned} \quad (4.6)$$

Since $N \subset T^*$ is a regular language, the transduction τ'' is rational by (4.6). ■

If M, M', M'' are arbitrary monoids, then the composition of two rational transductions $\tau: M \rightarrow M'$ and $\tau': M' \rightarrow M''$ is not necessarily rational.

Example 4.2 Let x, y, z be letters, $M = x^*$, $M' = y^* \times z^*$, $M'' = \{y, z\}^*$. Define $\tau: M \rightarrow M'$ and $\tau': M' \rightarrow M''$ by

$$\tau(x^n) = (y^n, z^n), \quad \tau'(y^n, z^k) = y^n z^k \quad (n, k \geq 0).$$

The graphs R and R' of τ and τ' are:

$$R = (x, (y, z))^*, \quad R' = ((y, 1), y)^*((1, z), z)^*,$$

thus τ and τ' are rational. Next

$$(\tau' \circ \tau)(x^n) = y^n z^n \quad n \geq 0.$$

Since the image $\text{im}(\tau' \circ \tau) = \{y^n z^n : n \geq 0\}$ 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 Y be an alphabet. If $\tau: M \rightarrow Y^*$ and $\tau': Y^* \rightarrow M'$ are rational transductions, then $\tau' \circ \tau$ is rational.

Proof. In view of Proposition 4.3,

$$\begin{aligned} \tau(m) &= \beta(\alpha^{-1}(m) \cap K) & m \in M \\ \tau'(g) &= \delta(\gamma^{-1}(g) \cap L) & g \in Y^* \end{aligned}$$

where X, Z are alphabets, $K \in \text{Rat}(X^*)$, $L \in \text{Rat}(Z^*)$, and

$$\alpha: X^* \rightarrow M, \quad \beta: X^* \rightarrow Y^*, \quad \gamma: Z^* \rightarrow Y^*, \quad \delta: Z^* \rightarrow M'$$

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 $\gamma^{-1} \circ \beta: X^* \rightarrow Z^*$ is the composition of two rational transductions, it is a rational transduction by Elgot and Mezei's Theorem. Thus

$$(\gamma^{-1} \circ \beta)(f) = \psi(\varphi^{-1}(f) \cap N) \quad f \in X^*$$

for some alphabet T , morphisms $\varphi: T^* \rightarrow X^*$, $\psi: T^* \rightarrow Z^*$ and some $N \in \text{Rat}(T^*)$. Thus as in the proof of Theorem 4.4,

$$(\tau' \circ \tau)(m) = (\delta \circ \psi)[(\alpha \circ \varphi)^{-1}(m) \cap (\varphi^{-1}(K) \cap N \cap \psi^{-1}(L))] \quad m \in M,$$

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 $\tau: X^* \rightarrow Y^*$ is algebraic if there exist an alphabet Z^* , two morphisms $\alpha: Z^* \rightarrow X^*$, $\beta: Z^* \rightarrow Y^*$ and a context-free language $A \subset Z^*$ such that

$$\tau(f) = \beta(\alpha^{-1}(f) \cap A) \quad f \in X^*.$$

It follows immediately that $\tau(L)$ is context-free if $L \subset X^*$ 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 $\tau: X^* \rightarrow Y^*$ and $\tau': Y^* \rightarrow Z^*$ 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 $\tau: X^* \rightarrow Y^*$, and of subsets $A \subset X^*$, $B \subset Y^*$ such that $\tau^{-1}(\tau(A)) \neq A$ and $\tau(\tau^{-1}(B)) \neq B$.

4.2 Prove Proposition 4.7.

4.3 Give an example of two algebraic transductions τ, τ' such that the composition $\tau' \circ \tau$ is not algebraic.

4.4 Consider the Dyck reduction $\rho: Z_n^* \rightarrow Z_n^*$. Show that ρ is an algebraic transduction. Show that ρ 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 $w' = n_0 \xi'_1 \cdots \xi'_l n_l$ is defined by

$$ww' = m_0 \xi_1 \cdots \xi_k (m_k n_0) \xi'_1 \cdots \xi'_l n_l.$$

An algebraic grammar $G = \langle V, M, P \rangle$ over M is given by a finite subset P of $V \times M[V]$. Derivations are defined as in free monoids. The language $L_G(\xi)$ generated by ξ is the sets of all $m \in M$ derived from ξ . Languages generated by algebraic grammars over M are called algebraic subsets of M .

a) Show that for any algebraic grammar $G = \langle V, M, P \rangle$, there is an algebraic grammar $G_1 = \langle V, M_1, P \rangle$, 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 A is an algebraic subset of M iff there exist an alphabet X , a morphism $\varphi: X^* \rightarrow M$, and a context-free language $L \subset X^*$ such that $\varphi(L) = A$.

c) Show that any rational subset of M is algebraic.

d) Show that a transduction $\tau: X^* \rightarrow Y^*$ is algebraic in the sense given in the text iff its graph is an algebraic subset of $X^* \times Y^*$.

4.6 (continuation of 4.5) Show that in a free commutative monoid $X^{\oplus}$, 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 $\tau: X^* \rightarrow Y^*$ be a rational transduction. Then $\tau = \tau_0 + \tau_{\infty}$, where

$$\tau_0(f) = \tau(f), \quad \tau_{\infty}(f) = \emptyset, \quad \text{if } \text{Card}(\tau f) < \infty;$$

$$\tau_0(f) = \emptyset, \quad \tau_{\infty}(f) = \tau(f), \quad \text{if } \text{Card}(\tau f) = \infty.$$

Show that τ_0, τ_{∞} are rational transductions.

4.9 Let M, M', M'' be finitely generated monoids, and let $\tau: M \rightarrow M', \tau': M' \rightarrow M''$ be transductions. Show that if one of them is recognizable (i.e. its graph is recognizable) and the other is rational, then $\tau' \circ \tau: M \rightarrow M''$ is rational, and even recognizable, provided M, M', M'' are free monoids. Show that if τ and τ' are recognizable, then $\tau' \circ \tau$ is always recognizable.

III.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 there 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 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 $f \mapsto f$ from X^* into itself is a rational transduction. This is straightforward by Nivat's Theorem. The graph of this mapping is

$$\Delta = \{(f, f) : f \in X^*\} = \left(\bigcup_{x \in X} (x, x) \right)^*.$$

5.2 The rational constants $\tau_K: X^* \rightarrow Y^*$ defined for a fixed regular language $K \subset Y^*$ by $\tau_K(f) = K$ are rational. The graph of τ_K is $X^* \times K$.

5.3 Any morphism, any inverse morphism is a rational transduction.

5.4 A rational substitution is a substitution $\sigma: X^* \rightarrow Y^*$ such that $\sigma(x) \in \text{Rat}(Y^*)$ for $x \in X$. The graph of σ is

$$\left(\bigcup_{x \in X} \{x\} \times \sigma(x) \right)^*;$$

thus σ is a rational transduction.

5.5 The union (and of course the intersection) with a regular language is performed by a rational transduction. Let $K \subset X^*$ be a regular language, and consider the transduction $f \mapsto f \cup K$ from X^* into X^* . Then its graph is $\Delta \cup (X^* \times K)$.

5.6 The product with a rational language: let $K \in \text{Rat}(X^*)$ and consider the transduction $f \mapsto Kf$ ($f \in X^*$). Its graph is $(\{1\} \times K)\Delta$.

5.7 The (left or right) quotient by a rational language. Let $K \subset X^*$ be a rational language. The transduction $X^* \rightarrow X^*$ defined by

$$f \mapsto K^{-1}f = \{g \in X^* \mid \exists u \in K: ug = f\}$$

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 $\tau: X^* \rightarrow X^*$ with $\tau(f) = f^{-1}K = \{g \in X^* : fg \in K\}$ is rational if $K \subset X^*$ is a regular language. Consider indeed its graph

$$R = \{(f, g) : fg \in K\}.$$

Let $\bar{X} = \{\bar{x} \mid x \in X\}$ be a copy of X , disjoint from X , set $Z = X \cup \bar{X}$, and define morphisms $\alpha, \beta, \gamma: Z^* \rightarrow X^*$ by

$$\begin{aligned} \alpha(x) &= x, & \beta(x) &= 1, & \gamma(x) &= x & x \in X; \\ \alpha(\bar{x}) &= 1, & \beta(\bar{x}) &= x, & \gamma(\bar{x}) &= x & \bar{x} \in \bar{X}. \end{aligned}$$

Consider the regular language $K' = \gamma^{-1}(K) \cap X^* \bar{X}^* \subset Z^*$. Any word $h \in K'$ factorizes in a unique way into $h = fg$, ($f \in X^*, g \in \bar{X}^*$). It follows that

$$R = \{(\alpha h, \beta h) : h \in K'\}.$$

5.9 The transduction $X^* \rightarrow X^*$ which associates to any word $f \in X^*$ the set of its subwords (resp. factors, left factors, right factors) is a rational relation. Let indeed $\bar{X}, Z, \alpha, \gamma$ be as above. Then the set of subwords of f is $\alpha(\gamma^{-1}(f))$, the set of factors of f is $\alpha(\gamma^{-1}(f) \cap \bar{X}^* X^* \bar{X}^*)$, etc. (Note that the set of left factors of f is $f(X^*)^{-1}$. Thus the rationality of this transduction follows from Example 5.7.)

5.10 Let $\tau: X^* \rightarrow X^*$ be defined for $f = x_1 x_2 \cdots x_n$ ($n \geq 1, x_i \in X$) by $\tau(f) = x_1 x_3 x_5 \dots$, and $\tau(1) = 1$. With the notations of Example 5.8,

$$\tau(f) = \alpha(\gamma^{-1}(f) \cap [(X\bar{X})^* \cup (X\bar{X})^* X]).$$

5.11 The transduction $\tau: x^* \rightarrow \{a, b\}^*$ defined by

$$\tau(x^n) = \begin{cases} a^n & n \text{ even,} \\ b^n & n \text{ odd,} \end{cases}$$

is rational. Indeed, its graph is $(x^2, a^2)^* \cup (x, b)(x^2, b^2)^*$.

5.12 According to Greibach [1973], the "hardest" context-free language is the language $L_0 \subset X^*$, with $X = \{x_1, x_2, \bar{x}_1, \bar{x}_2, \varepsilon, \#\}$ defined in the following way. Set $T = X \setminus \{\#\}$. Then $f \in L_0$ iff either

$$f = 1$$

$$\text{or } f = u_1 | v_1 | w_1 \# u_2 | v_2 | w_2 \# \cdots \# u_n | v_n | w_n,$$

with $u_1, w_1, \dots, u_n, w_n \in T^*$, $v_1, \dots, v_n \in \{x_1, x_2, \bar{x}_1, \bar{x}_2\}^*$ and $v_1 v_2 \cdots v_n \in \varepsilon D_2^*$. In order to show that L_0 is indeed context-free, consider the two transductions $\tau, \tau_1: X^* \rightarrow X^*$:

$$\tau(h) = \# T^* | h | T^* \quad \tau_1(h) = T^* | \varepsilon h | T^* \quad (h \in X^*)$$

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 $X^* \rightarrow X^*$ which associates to any $f \in X^*$ the reversal $\bar{f}$ is not rational if $\text{Card}(X) \geq 2$ since its graph $\{(f, \bar{f}) : f \in X^*\}$ 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 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 $(f, g) \mapsto fg$ from $X^* \times X^*$ into X^* is rational. Its graph is indeed

$$A = \{(x, 1, x) : x \in X\}^* \{(1, x, x) : x \in X\}^*.$$

5.15 The shuffle $f \sqcup g$ of two words $f, g \in X^*$ is defined as

$$f \sqcup g = \{f_1 g_1 \cdots f_n g_n \mid f_1, \dots, f_n, g_1, \dots, g_n \in X^*, f_1 \cdots f_n = f, g_1 \cdots g_n = g\}.$$

The transduction $(f, g) \mapsto f \sqcup g$ is rational, since its graph is A^* , with A 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 $\mathbb{k} = \{0, 1, \dots, k-1\}$. The empty word of $\mathbb{k}^*$ is denoted by ε . For each $f = x_0 x_1 \cdots x_n$ ($x_i \in \mathbb{k}$), let

$$\langle f \rangle = \sum_{i=0}^n x_i k^{n-i}$$

be the integer represented by f in base k . Then $\langle \varepsilon \rangle = 0$, and for any $m \in \mathbb{N}$, there is a unique $f \in \mathbb{k}^* \setminus 0\mathbb{k}^*$ such that $\langle f \rangle = n$. The transduction

$$\oplus : \mathbb{k}^* \times \mathbb{k}^* \rightarrow \mathbb{k}^*$$

which associates to any $(f, g) \in \mathbb{k}^* \times \mathbb{k}^*$ the unique word $h \in \mathbb{k}^* \setminus 0\mathbb{k}^*$ such that $\langle h \rangle = \langle f \rangle + \langle g \rangle$ 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

$$\tau_1 : \mathbb{k}^* \times \mathbb{k}^* \rightarrow (\mathbb{k} \times \mathbb{k})^*.$$

In order to avoid confusion, elements of $\mathbb{k} \times \mathbb{k}$ are noted $[x, y]$. If $f = x_1 x_2 \cdots x_n$, $g = y_1 y_2 \cdots y_m$, ($x_i, y_i \in \mathbb{k}$), $\tau_1(f, g)$ is defined to be equal either to

$$[0, 0]^+ [x_1, 0] \cdots [x_{n-m}, 0] [x_{n-m+1}, y_1] \cdots [x_n, y_m]$$

$$\text{or } [0, 0]^+ [0, y_1] \cdots [0, y_{m-n}] [x_1, y_{m-n+1}] \cdots [x_n, y_m]$$

according to $n \geq m$ or $m \geq n$. Define $R, S, T \subset \mathbb{k}^* \times \mathbb{k}^* \times (\mathbb{k} \times \mathbb{k})^*$ by

$$S = \{(\varepsilon, y, [0, y]) : y \in \mathbb{k}^*\} \cup \{(x, \varepsilon, [x, 0]) : x \in \mathbb{k}^*\},$$

$$T = \{(x, y, [x, y]) : x, y \in \mathbb{k}^*\}, \quad R = (\varepsilon, \varepsilon, [0, 0])^+ S T.$$

Then R is rational and is the graph of τ_1 . Next, we define

$$\tau_2 : (\mathbb{k} \times \mathbb{k})^* \rightarrow \mathbb{k}^*$$

to perform the addition step: For

$$w = [x_0, y_0] \cdots [x_n, y_n], \quad x_0 = y_0 = 0, \quad (5.1)$$

$$f = x_0 \cdots x_n, \quad g = y_0 \cdots y_n,$$

$\tau_2(w)$ will be the word $h = z_0 \cdots z_n$ such that $\langle h \rangle = \langle f \rangle + \langle g \rangle$. For this, we introduce an auxiliary alphabet $\{0, 1\} \times \mathbb{k} \times \mathbb{k} \times \mathbb{k}$ composed of quadruples $[r, z, x, y]$. During the computation, $z + r \cdot k$ represents the number $x + y + 1$ or $x + y + 0$, according to the existence or not of a "carry" from a previous computation. Formally, we define morphisms

$$\varphi : Y^* \rightarrow (\mathbb{k} \times \mathbb{k})^*, \quad \psi : Y^* \rightarrow \mathbb{k}^*$$

$$\text{by } \varphi[r, z, x, y] = [x, y], \quad \psi[r, z, x, y] = z \quad [r, z, x, y] \in Y.$$

Next, we define a local regular language

$$\begin{aligned} K &= (UY^* \cap Y^*V) \setminus Y^*WY^* & U &= \{[0, 1, 0, 0], [0, 0, 0, 0]\} \\ V &= \{[r, z, x, y] : z + rk = x + y\} \\ Y^2 \setminus W &= \{[r, z, x, y][r', z', x', y'] : z + rk = x + y + r'\}. \end{aligned}$$

Then for w given by (5.1),

$$\varphi^{-1}(w) \cap K = [r_0, z_0, x_0, y_0] \cdots [r_n, z_n, x_n, y_n]$$

with $x_n + y_n = z_n + kr_n$, $x_i + y_i + r_{i+1} = z_i + kr_i$, ($i = n-1, \dots, 0, r_0 = 0$). Hence $\psi(\varphi^{-1}(w) \cap K) = \tau_2(w)$ and τ_2 is rational. The final step just deletes initial zeros from the result. It is performed by the transduction

$$\tau_3 : \mathbb{K}^* \rightarrow \mathbb{K}^*, \quad \tau_3(h) = (0^*)^{-1}h \cap \mathbb{K}^* \setminus 0\mathbb{K}^*$$

which is clearly rational. Thus, by Proposition 4.6, the transduction $\oplus = \tau_3 \circ \tau_2 \circ \tau_1$ 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 $X = \{x_1, x_2, \dots, x_k\}$. Define an order on X^* by

$$f \leq g \Leftrightarrow \begin{cases} g = fu & \text{for some } u \in X^+ \text{ or} \\ f = ux_i v, \quad g = ux_j v' & \text{and } i < j; \end{cases}$$

this is the lexicographical order. The "radix" order is defined by

$$f \leq_r g \Leftrightarrow \begin{cases} |f| < |g| \\ |f| = |g| & \text{and } f \leq g. \end{cases}$$

Show that the four transductions from X^* into itself which associate to f the sets

$$\{g \mid g > f\} \quad (\text{resp. } \{g \mid g < f\})$$

are rational for both orders.

5.2 Show that a transduction $\tau : X^* \times Y^* \rightarrow Z^*$ is rational iff there are an alphabet T , three morphisms

$$\alpha_1 : T^* \rightarrow X^*, \quad \alpha_2 : T^* \rightarrow Y^*, \quad \beta : T^* \rightarrow Z^*$$

and a regular language $K \subset T^*$ such that

$$\tau(f, g) = \beta(\alpha_1^{-1}(f) \cap \alpha_2^{-1}(g) \cap K) \quad (f, g) \in X^* \times Y^*.$$

Show that for $R \subset X^*$, the transduction $\tau' : Y^* \rightarrow Z^*$ given by $\tau'(g) = \tau(R \times \{g\})$ ($g \in Y^*$) 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 $\otimes$ 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 fixed $q \geq 1$, the multiplication by $q : \mathbb{K}^* \rightarrow \mathbb{K}^*$ which associates to $f \in \mathbb{K}^*$ the word $f' \in \mathbb{K}^* \setminus 0\mathbb{K}^*$ such that $\langle f' \rangle = q \cdot \langle f \rangle$ is rational.

5.5 Let $X = \{x, y\}$, and let σ be the congruence generated by $yxx \sim xyy$. Show that the transduction $\tau : X^* \rightarrow X^*$ which associates to f the class $[f]_\sigma = \{g \mid g \equiv f \pmod{\sigma}\}$ is rational. (Note that this is not true for all congruences: thus the result does not hold for the Lukasiewicz congruence λ of Section II.4.)

III.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 transducer $T = \langle X, Y, Q, q_-, Q_+, E \rangle$ is composed of an input alphabet X , an output alphabet Y , 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

$$E \subset Q \times X^* \times Y^* \times Q. \quad (6.1)$$

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 iff 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, labelled q and to each transition $e = (q, u, v, q')$ is associated an arrow directed from q to q' and labelled 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 $X = Y = \{x, y\}$, $Q = \{a, b\}$, $q_- = a$, $Q_+ = \{b\}$, $E = \{(a, x^2y, 1, a), (a, 1, 1, b), (b, x, x, b), (b, y, y, b)\}$. Its representation is shown in Fig. III.4.

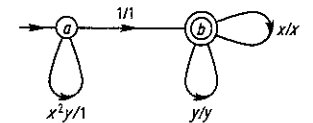


Fig. III.4

We now introduce some supplementary definitions. Consider the free monoid E^* generated by the set E of transitions. The empty word of E^* is denoted by ε . Given a word

$$e = (p_1, u_1, v_1, q_1) \cdots (p_n, u_n, v_n, q_n), \quad (6.2)$$

the label of e is the pair of words $|e| = (f, g)$ defined by $f = u_1 \cdots u_n$, $g = v_1 \cdots v_n$. By convention, $|\varepsilon| = (1, 1)$. Clearly the function $e \mapsto |e|$ is a morphism from E^* into $X^* \times Y^*$ which can be decomposed into two morphisms $\alpha: E^* \rightarrow X^*$, $\beta: E^* \rightarrow Y^*$ defined by $|e| = (\alpha e, \beta e)$. αe and βe are the input label and the output label of e . The word e given by (6.2) is a path or a computation in T from p_1 to q_n iff $q_i = p_{i+1}$, $(i = 1, \dots, n-1)$. 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 this notation by setting

$$\Lambda(p, Q') = \bigcup_{q \in Q'} \Lambda(p, q) \quad Q' \subset Q.$$

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 iff $p = q_-$ and $q \in Q_+$. Thus, the set of all successful paths is $\Lambda(q_-, Q_+)$.

Definition The transduction $|T|: X^* \rightarrow Y^*$ realized by T is defined by

$$|T|(f) = \{g \in Y^* \mid (f, g) \in T(q_-, Q_+)\}. \quad (6.3)$$

Thus $g \in |T|(f)$ iff there exists a successful path in T with label (f, g) . With the morphisms α and β , (6.3) can be reformulated as

$$|T|(f) = \beta(\alpha^{-1}(f) \cap \Lambda(q_-, Q_+)). \quad (6.4)$$

Example 6.1 (continued). The set of successful paths is

$$\Lambda(a, b) = (a, x^2y, 1, a)^*(a, 1, 1, b)\{(b, x, x, b), (b, y, y, b)\}^*.$$

The set of labels of successful paths is

$$T(a, b) = (x^2y, 1)^*\{(x, x), (y, y)\}^*.$$

The transduction τ realized by the transducer is

$$\tau(f) = K^{-1}f, \quad \text{with } K = (x^2y)^*.$$

Theorem 6.1 A transduction $\tau: X^* \rightarrow Y^*$ is rational iff τ is realized by a transducer.

Proof. Let $T = \langle X, Y, Q, q_-, Q_+, E \rangle$ be a transducer. The rationality of $|T|$ 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 $U_p = \{(q_1, u, v, q_2) \in E \mid q_1 = p\}$, $V_q = \{(q_1, u, v, q_2) \in E \mid q_2 = q\}$,

$$W = \{(q_1, u_1, v_1, q'_1)(q_2, u_2, v_2, q'_2) \in E^2 \mid q'_1 \neq q'_2\}, \quad \Omega = \Lambda(p, q) \cap \{\varepsilon\}.$$

Conversely, let $\tau: X^* \rightarrow Y^*$ be a rational transduction. After a copy, we may assume $X \cap Y = \emptyset$. Thus

$$\tau(f) = \pi_Y(\pi_X^{-1}(f) \cap K) \quad f \in X^*,$$

with $K \subset (X \cup Y)^*$ a regular language and π_X, π_Y the projections of $(X \cup Y)^*$ onto X^* and Y^* . Let $A = \langle X \cup Y, Q, q_-, Q_+ \rangle$ be a finite automaton recognizing K , and define a transducer

$$\begin{aligned} T &= \langle X, Y, Q, q_-, Q_+, E \rangle \\ E &= \{(q, \pi_X(z), \pi_Y(z), q \cdot z) \mid q \in Q, z \in X \cup Y\}. \end{aligned} \quad (6.5)$$

Then T realizes τ . ■

We easily obtain the following corollary

Corollary 6.2 Any rational transduction $\tau: X^* \rightarrow Y^*$ can be realized by a transducer $T = \langle X, Y, Q, q_-, Q_+, E \rangle$ such that

$$E \subset Q \times (X \cup \{1\}) \times (Y \cup \{1\}) \times Q \quad (6.6)$$

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 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 $(q^0, 1, 1, q^1)$ if $q_- \in Q_+$.

Let T' be the transducer obtained in this way with initial state q^0 and unique final state q^1 . Then obviously $\tau = |T'|$. ■

Remark. If $\tau(1) = \emptyset$, then (6.6) can be replaced by

$$E \subset (Q \times X \times \{1\} \times Q) \cup (Q \times \{1\} \times Y \times Q).$$

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 a 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 $\bar{Z}$ composed of the three "letters" $x^2y/1$, x/x , y/y . Define morphisms φ, ψ from Z^* into X^* by $\varphi(u/v) = u$, $\psi(u/v) = v$. Then

$$T(a, b) = \{(\varphi h, \psi h) \mid h \in R\} \quad \text{with} \quad R = (x^2y/1)^* \{x/x, y/y\}^*.$$

Example 6.2 Consider the transduction $\tau: X^* \rightarrow Y^*$ with $X = \{x, y\}$, $Y = \{a, b\}$ of Example 4.1 defined by

$$\tau(f) = \begin{cases} \emptyset & \text{if } f \notin x^+y^*; \\ (a^+b)^n a^{2m}b & \text{if } f = x^n y^m \in x^+y^*. \end{cases}$$

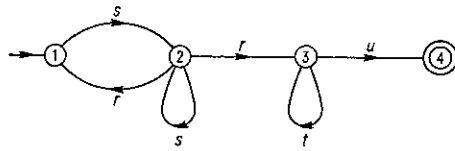


Fig. III.5

With the notations of that example, a finite nondeterministic automaton for $K = (s^+r)^+t^*u$ is given in Fig. III.5. Thus we obtain the following transducer realizing τ (Fig. III.6).

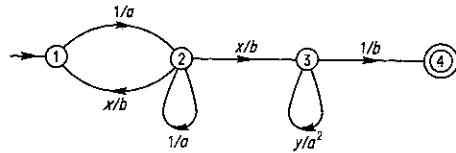


Fig. III.6

Exercise

6.1 Let T be a transducer realizing a transduction τ . Show how finite automata recognizing $\text{dom}(\tau)$ and $\text{im}(\tau)$ can be obtained from T .

III.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 the 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 induced by the operations in S (see Section I.2). The identity matrix is denoted by I .

Let X be an alphabet. A morphism $\mu: X^* \rightarrow S^{Q \times Q}$ is a monoid morphism from X^* into the multiplicative monoid $S^{Q \times Q}$. Thus

$$\mu(fg) = \mu f \cdot \mu g \quad f, g \in X^* \quad (7.1)$$

$$\mu 1 = I. \quad (7.2)$$

If only (7.1) is verified, then μ is a semigroup morphism. In this case, $\mu(X^*) = \{\mu f : f \in X^*\}$ 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 an alphabet Y . Thus the semiring S is $\text{Rat}(Y^*)$. Consequently, the identity matrix I is given by

$$I_{pq} = \begin{cases} 1 & \text{if } p = q; \\ \emptyset & \text{if } p \neq q. \end{cases}$$

For simplicity, we frequently write 0 instead of $\emptyset$.

Definition A matrix representation $M = \langle \mu, Q, q_-, Q_+ \rangle$ from X^* into Y^* is composed of a finite set of states Q , an initial state q_- , a set of final states Q_+ , and a semigroup morphism $\mu: X^* \rightarrow \text{Rat}(Y^*)^{Q \times Q}$. The transduction $|M|: X^* \rightarrow Y^*$ realized by M is defined by

$$|M|(f) = \bigcup_{q \in Q_+} \mu f_{q, q_-}. \quad (7.3)$$

For $p, q \in Q$, note μ_{pq} the transduction $f \mapsto \mu f_{pq}$. Then (7.3) can be written as

$$|M| = \bigcup_{q \in Q_+} \mu_{q, q_-}.$$

Example 7.1 Let X be an alphabet and $x_0 \in X$. Set $Q = \{1, 2\}$, and define a monoid morphism $\mu: X^* \rightarrow \text{Rat}(Y^*)^{2 \times 2}$ by

$$\mu x = \begin{bmatrix} 0 & 0 \\ 0 & x \end{bmatrix} \quad x \in X \setminus x_0, \quad \mu x_0 = \begin{bmatrix} 0 & 1 \\ 0 & x_0 \end{bmatrix}.$$

Then $\mu f = \begin{bmatrix} 0 & 0 \\ 0 & f \end{bmatrix}$ if $f \notin x_0 X^*$, $f \neq 1$,

and $\mu f = \begin{bmatrix} 0 & g \\ 0 & f \end{bmatrix}$ if $f = x_0 g$.

Thus for $M = \langle \mu, Q, 1, \{2\} \rangle$, $|M|(f) = \mu f_{12} = x_0^{-1} f$, ($f \in X^*$).

Theorem 7.1 A transduction $\tau: X^* \rightarrow Y^*$ is rational iff there exists a matrix representation $\mathbf{M} = \langle \mu, Q, q_-, q_+ \rangle$ realizing τ . Then the following hold:

- (i) if $\tau(1) = 0$ or $\tau(1) = 1$, then μ can be chosen to be a monoid morphism;
- (ii) Q_+ can be assumed to consist of a single state $q_+ \neq q_-$, and $\mu f_{q_+q_-} = \mu f_{q_-q_+} = 0$ for all $f \in X^+$, $q \in Q$;
- (iii) if $\tau(1) = 0$, both (i) and (ii) can be satisfied simultaneously.

Note that μ 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 $\mathbf{T} = \langle X, Y, Q, q_-, q_+, E \rangle$ be a transducer realizing τ . In view of Corollary 6.2, we may suppose that $Q_+ = \{q_+\}$, $q_+ \neq q_-$,

$$E \subset Q \times (X \cup \{1\}) \times Y^* \times Q,$$

and moreover $(q, u, v, q') \in E$ implies $q' \neq q_-$, $q \neq q_+$. Let $\alpha: E^* \rightarrow X^*$ and $\beta: E^* \rightarrow Y^*$ be the input and output morphisms as defined in the preceding section. Then

$$\tau(f) = \beta(\alpha^{-1}(f) \cap \Lambda(q_-, q_+)). \quad (7.4)$$

Next note that for $p, q, r \in Q$,

$$\Lambda(p, q) = \bigcup_{r \in Q} \Lambda(p, r) \Lambda(r, q).$$

Since α is an alphabetic morphism by the assumption on E , we have $\alpha^{-1}(fg) = \alpha^{-1}(f)\alpha^{-1}(g)$ for $f, g \in X^*$. Consequently

$$\alpha^{-1}(fg) \cap \Lambda(p, q) = \bigcup_{r \in Q} (\alpha^{-1}(f) \cap \Lambda(p, r))(\alpha^{-1}(g) \cap \Lambda(r, q)). \quad (7.5)$$

Define a mapping $\mu: X^* \rightarrow \mathfrak{R}(Y^*)^{Q \times Q}$ by

$$\mu f_{pq} = \beta(\alpha^{-1}(f) \cap \Lambda(p, q)) \quad p, q \in Q, f \in X^*. \quad (7.6)$$

In view of (7.5), μ is a semigroup morphism, and by (7.6), μf_{pq} is a regular language. Let $\mathbf{M} = \langle \mu, Q, q_-, q_+ \rangle$. Then by (7.4)

$$|\mathbf{M}|(f) = \mu f_{q_-q_+} = \tau(f).$$

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 $\mathbf{T}$, condition (ii)

holds. Next, define the (monoid) morphism $\bar{\mu}$ by

$$\bar{\mu}f = \mu f \quad (f \in X^+), \quad \bar{\mu}1 = I,$$

and $\bar{\mathbf{M}} = \langle \bar{\mu}, Q, q_-, q_+ \rangle$. Since $q_- \neq q_+$, $|\bar{\mathbf{M}}| = \tau$ 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 μ given by (7.6), let $q_0 \notin Q$, set $P = q_0 \cup Q$ and define

$$\mu': X^* \rightarrow \text{Rat}(Y^*)^{P \times P}$$

by $\mu'1 = I$ and

$$\mu'f_{pq} = \begin{cases} \mu f_{pq} & \text{if } p, q \in Q; \\ \mu f_{q_0q} & \text{if } p = q_0, q \in Q; \\ 0 & \text{otherwise.} \end{cases} \quad (f \in X^+)$$

Then μ' is easily seen to be a morphism, and

$$\tau(f) = \mu'f_{q_0q_0} \cup \mu'f_{q_0q_0} \quad (f \in X^*).$$

Thus τ is realized by the matrix representation $\langle \mu', P, q_0, \{q_0, q_+\} \rangle$.

Conversely, let $\tau: X^* \rightarrow Y^*$ be the transduction realized by a matrix representation $\mathbf{M} = \langle \mu, Q, q_-, q_+ \rangle$. In order to prove the rationality of τ , 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 $\nu: X^* \rightarrow \text{Rat}(Y^*)^{P \times P}$ for $u \in 1 \cup X$ by

$$\nu u_{pq} = \mu u_{pq} \quad (p, q \in Q)$$

$$\nu u_{sq} = \nu u_{ss} = 0 \quad (q \in Q)$$

$$\nu u_{qs} = \bigcup_{p \in Q_+} \mu u_{qp} \quad (q \in Q).$$

Then these formulas hold for any word $f \in X^*$. This is obvious for the two first formulas; the third follows by induction from:

$$\nu(fg)_{qs} = \bigcup_{r \in Q} \mu f_{qr} \nu g_{rs} = \bigcup_{p \in Q_+} \bigcup_{r \in Q} \mu f_{qr} \mu g_{rp} = \bigcup_{p \in Q_+} \mu(fg)_{qp}.$$

Thus $\tau(f) = \bigcup_{p \in Q_+} \mu f_{q_+p} = \nu f_{q_+s}$.

Consequently, we assume $Q_+ = \{q_+\}$ and $q_+ \neq q_-$. Next, define the monoid morphism $\bar{\mu}: X^* \rightarrow \text{Rat}(Y^*)^{Q \times Q}$ by $\bar{\mu}x = \mu x$ ($x \in X$). Then $\bar{\mu}f_{q_+q_+} = \mu f_{q_+q_+} = \tau(f)$ for $f \in X^+$, 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 $\tau_1: X^* \rightarrow Y^*$ is defined by $\tau_1(1) = \mu 1_{q_- q_+} \in \text{rat}(Y^*)$ and $\tau_1(f) = \emptyset$ for $f \in X^+$. Since τ_1 is obviously a rational transduction, it suffices to show that $\bar{\tau}$ is rational.

Thus we may assume that μ is a monoid morphism and $\tau(1) = 0$. Let $Z = Q \times X \times Q$ and define the strictly alphabetic morphism $\varphi: Z^* \rightarrow X^*$ by

$$\varphi((p, x, q)) = x.$$

Let $K = [(q_- \times X \times Q)Z^* \cap Z^*(Q \times X \times q_+)] \setminus Z^*WZ^*$

with $W = \{(q, x, q')(p, y, p') \in Z^2 \mid q' \neq p\}$.

Then K is a local regular language, $\varphi^{-1}(1) \cap K = \emptyset$, and for $f = x_1 x_2 \cdots x_n$, ($x_i \in X$),

$$\varphi^{-1}(f) \cap K = \{(q_-, x_1, q_1)(q_1, x_2, q_2) \cdots (q_{n-1}, x_n, q_+) \mid q_1, \dots, q_{n-1} \in Q\}. \quad (7.7)$$

Define a rational substitution $\sigma: Z^* \rightarrow X^*$ by

$$\sigma((p, x, q)) = \mu x_{pq}.$$

Then $\sigma(\varphi^{-1}(1) \cap K) = \emptyset = \tau(1)$ (7.8)

and, in view of (7.7),

$$\sigma(\varphi^{-1}(f) \cap K) = \mu f_{q_- q_+} = \tau(f) \quad (f \in X^+) \quad (7.9)$$

Consequently, τ 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 $\tau: X^* \rightarrow Y^*$ be a transduction with $\tau(1) = 0$ or $\tau(1) = 1$. Then τ is rational iff there exist an alphabet Z , a strictly alphabetic morphism $\varphi: Z^* \rightarrow X^*$, a rational substitution $\sigma: Z^* \rightarrow Y^*$ and a local regular language $K \subset Z^*$ such that*

$$\tau(f) = \sigma(\varphi^{-1}(f) \cap K) \quad (f \in X^*). \quad (7.10)$$

Proof. Let τ be given by (7.10). Then τ is clearly 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 $K \cup 1$. ■

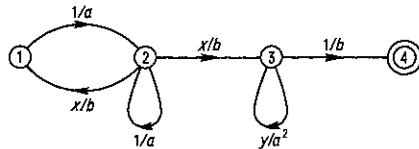


Fig. III.7

Example 7.2 Consider for $X = \{x, y\}$, $Y = \{a, b\}$, the transducer of Example 6.2 (Fig. III.7). Formula (7.6) gives the following semigroup morphism μ :

$$\mu 1 = \begin{bmatrix} 1 & a^+ & 0 & 0 \\ 0 & a^* & 0 & 0 \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \mu x = \begin{bmatrix} a^+ b & a^+ b a^+ & 0 & 0 \\ a^* b & a^* b a^+ & a^* b & a^* b^2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\mu y = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & a^2 & a^2 b \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

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 $\tau: X^* \rightarrow Y^*$ is rational iff the formal power series $\sum_{f \in X^*} \tau(f) \cdot f$ with coefficients in the semiring $\text{Rat}(Y^*)$ is recognizable. The following theorem is the analogue to a well-known characterization of recognizable formal power series.

Proposition 7.3 *A transduction $\tau: X^* \rightarrow Y^*$ is rational iff there exist a finite set Q , a monoid morphism $\mu: X^* \rightarrow \text{Rat}(Y^*)^{Q \times Q}$, a row Q -vector λ , a column Q -vector ρ with entries in $\text{Rat}(Y^*)$ such that*

$$\tau(f) = \lambda \mu f \rho \quad (f \in X^*). \quad (7.11)$$

Proof. Let τ be given by (7.11). Then

$$\tau(f) = \bigcup_{p, q \in Q} \lambda_p \mu f_{pq} \rho_q.$$

By Theorem 7.1, the transductions $\mu_{pq}: f \mapsto \mu f_{pq}$ are rational. Since λ_p, ρ_q are regular languages, the transductions $f \mapsto \lambda_p \mu f_{pq} \rho_q$ are rational. Thus τ is rational.

Conversely, let τ be realized by the matrix representation $\mathbf{M} = \langle v, P, q_-, \{q_+\} \rangle$ with $q_- \neq q_+$. Let $s \notin P$, set $Q = s \cup P$ and define a monoid morphism $\mu: X^* \rightarrow \text{Rat}(Y^*)^{Q \times Q}$ by

$$\begin{aligned} \mu x_{pq} &= v x_{pq} & p, q \in P \\ \mu x_{pq} &= \emptyset & p = s \text{ or } q = s \end{aligned} \quad (x \in X)$$

Then clearly

$$\mu f_{pq} = \begin{cases} v f_{pq} & p, q \in P \\ \emptyset & p = s \text{ or } q = s \end{cases} \quad (f \in X^+)$$

Next define the Q -vectors λ and ρ by

$$\lambda_s = (v1)_{q-q_+}; \quad \rho_s = \{1\}, \quad \lambda_{q_-} = \{1\}, \quad \rho_{q_+} = \{1\}, \\ \lambda_q = \rho_q = \emptyset \text{ otherwise.}$$

Then $\lambda \mu 1 \rho = \lambda \rho = \lambda_s \rho_s = \tau(1)$, $\lambda \mu f \rho = \lambda_{q_-} \mu f_{q_- q_+} \rho_{q_+} = \tau(f)$ $f \in X^+$. ■

Example 7.3 Let $X = \{x\}$, $Y = \{a, b\}$, $Q = \{1, 2, 3, 4\}$, let μ be the monoid morphism defined by

$$\mu x = \begin{bmatrix} 0 & a & 0 & 0 \\ a & 0 & 0 & 0 \\ 0 & 0 & 0 & b \\ 0 & 0 & b & 0 \end{bmatrix} \quad \lambda = [1, 0, 1, 0] \quad \rho = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

A simple computation shows that

$$\lambda \mu x^n = \begin{cases} [a^n, 0, b^n, 0] & \text{if } n \text{ is even;} \\ [0, a^n, 0, b^n] & \text{if } n \text{ is odd.} \end{cases}$$

$$\text{Thus } \lambda \mu x^n \rho = \begin{cases} a^n & n \text{ even;} \\ b^n & n \text{ odd.} \end{cases}$$

We conclude this section by considering a useful technical notion.

Definition Let $M = \langle \mu, Q, q_-, q_+ \rangle$ be a matrix representation from X^* into Y^* . Then M is trim if the following condition is satisfied. For any $q \in Q$, there exist $f, g \in X^*$, $q_+ \in Q_+$, such that

$$\mu f_{q-q_+} \neq \emptyset \quad \text{and} \quad \mu g_{q_+ q_+} \neq \emptyset. \quad (7.12)$$

Proposition 7.4 Let $\tau: X^* \rightarrow Y^*$ be a transduction with $\text{dom}(\tau) \neq \emptyset$, and let $M = \langle \mu, Q, q_-, q_+ \rangle$ with μ a monoid morphism be a matrix representation realizing τ . Then there exists a trim matrix representation $M' = \langle v, P, q_-, q_+ \rangle$ realizing τ 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 $\text{dom}(\tau) \neq \emptyset$ and μ is a monoid morphism, we have $q_- \in P$ and $P_+ = Q_+ \cap P \neq \emptyset$. Moreover, for any $q \in Q_+$, $q \in P_+$ iff $\mu h_{q-q_+} \neq \emptyset$ for at least one word $h \in X^*$. Consequently

$$|M| = \bigcup_{q \in Q_+} \mu_{q-q_+} = \bigcup_{q \in P_+} \mu_{q-q_+} \quad (7.13)$$

Define a monoid morphism $v: X^* \rightarrow \text{Rat}(Y^*)^{P \times P}$ by

$$v x_{pq} = \mu x_{pq} \quad p, q \in P, \quad x \in X.$$

In order to prove the desired result, it suffices to show that

$$v f_{pq} = \mu f_{pq} \quad p, q \in P, \quad f \in X^* \quad (7.14)$$

since then in view of (7.13)

$$|M'| = \bigcup_{q \in P_+} v_{q-q_+} = \bigcup_{q \in P_+} \mu_{q-q_+} = |M|.$$

To show (7.14), we first verify that for $p, q \in P$, $r \in Q \setminus P$,

$$\mu f_{pr} = \emptyset \quad \text{or} \quad \mu g_{rq} = \emptyset \quad (7.15)$$

for any pair of words f, g . Assume the contrary. Then there exist words f, g such that both $\mu f_{pr} \neq \emptyset$ and $\mu g_{rq} \neq \emptyset$. Since $p \in P$, there is a word f' such that $\mu f'_{q-p} \neq \emptyset$, and similarly $\mu g'_{q_+ q_+} \neq \emptyset$ for some word g' and some $q_+ \in Q_+$. But then $\emptyset \neq \mu f'_{q-p} \mu f_{pr} \subset \mu f' f_{q-r}$ and $\emptyset \neq \mu g_{rq} \mu g'_{q_+ q_+} \subset \mu g g'_{r q_+}$ and by (7.12), $r \in P$ contrary to the assumption. This proves (7.15).

Now (7.14) is true if $|f| \leq 1$. Arguing by induction, let $h \in X^*$, $x \in X$. Then for $p, q \in P$,

$$(\mu h x)_{pq} = \bigcup_{r \in Q} \mu h_{pr} \mu x_{rq} = \bigcup_{r \in P} \mu h_{pr} \mu x_{rq}$$

by (7.15). Consequently

$$(\mu h x)_{pq} = \bigcup_{r \in P} v h_{pr} v x_{rq} = (v h x)_{pq}.$$

Exercises

7.1 Show that $M = \langle \mu, Q, q_-, q_+ \rangle$ is trim iff for any $q \in Q$, there exist $q_+ \in Q_+$, and $f, g \in X^*$ with $|f|, |g| \leq \text{card } Q$ such that $\mu f_{q-q_+} \neq \emptyset$ and $\mu g_{q_+ q_+} \neq \emptyset$.

7.2 A transduction $\tau: X^* \rightarrow Y^*$ is faithful if $\tau^{-1}(g)$ is finite for all $g \in Y^*$, and is continuous if $\tau(f) \subset Y^+$ for $f \in X^+$. Show that a rational transduction $\tau: X^* \rightarrow Y^*$ is both faithful and continuous iff

$$\tau(f) = \psi(\varphi^{-1}(f) \cap K) \quad f \in X^*$$

for some alphabet Z , $K \in \text{Rat}(Z^*)$, $\varphi: Z^* \rightarrow X^*$ a morphism and $\psi: Z^* \rightarrow Y^*$ a strictly alphabetic morphism. (Hint. Apply Corollary 7.2 to τ^{-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 $X^* \times Y^*$ closed under union, product and the plus operation, and containing $\emptyset$, $\{(1, 1)\}$, and the relations $\{(u, y)\}$ for $u \in 1 \cup X$, $y \in Y$.

a) Show that $RS, SR \in \mathcal{R}$ for all $R \in \mathcal{R}$ such that $(1, 1) \notin R$, and $S \in \text{Rat}(X^* \times Y^*)$.

b) Show that $R \in \mathcal{R}$ iff the transduction with graph R is rational, faithful and continuous.

III.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 proofs 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 procedure for this property would imply a decision procedure for the Correspondence Problem.

Post's Correspondence Problem *Given an alphabet X with at least two letters, and given two sequences*

$$u_1, u_2, \dots, u_p \quad \text{and} \quad v_1, v_2, \dots, v_p \quad (8.1)$$

of words of X^ , decide whether there exist indices $i_1, i_2, \dots, i_k$, ($k > 0$) such that*

$$u_{i_1} u_{i_2} \cdots u_{i_k} = v_{i_1} v_{i_2} \cdots v_{i_k}. \quad (8.2)$$

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 the two sequences (8.1), and yields as output "yes" or "no" according to the existence or the non-existence of a sequence $i_1, \dots, i_k$ 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 $R \subset X^* \times Y^*$ it is decidable whether R is empty and whether R is finite.*

Proof. R is empty iff one of the two projections $\pi_X(R)$ and $\pi_Y(R)$ on X^* and Y^* are empty, and R is finite iff both projections are finite. Each projection is a regular language, and an explicit description of these languages is readily obtained from any 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 $X = \{a, b\}$, let Y be an alphabet, and let $u_1, u_2, \dots, u_p \in Y^*$. Define

$$U = \{(ab, u_1), (ab^2, u_2), \dots, (ab^p, u_p)\}.$$

Clearly U , hence U^+ is a rational relation over X and Y .

Lemma 8.3 *The relation $(X^* \times Y^*) \setminus U^+$ is rational.*

Usually, $\text{Rat}(X^* \times Y^*)$ is not closed under complementation, thus Lemma 8.3 has to be proved.

Proof. We show that $W = (X^* \times Y^*) \setminus U^+$ is a rational relation by writing W as a union of four rational relations. First the relation H composed of all $(f, g) \in X^* \times Y^*$ such that

$$f \notin \{ab, ab^2, \dots, ab^p\}^+$$

is rational and even recognizable since

$$H = (X^* \setminus \{ab, ab^2, \dots, ab^p\}^+) \times Y^*.$$

Next $(f, g) \in W$ and $(f, g) \notin H$

if and only if

$$f = ab^{i_1} ab^{i_2} \cdots ab^{i_r} \quad \text{for some } r > 0, \quad 1 \leq i_1, \dots, i_r \leq p \quad (8.3)$$

$$\text{and} \quad g \neq u_{i_1} u_{i_2} \cdots u_{i_r}. \quad (8.4)$$

Now (8.4) holds iff one of the three following conditions hold

$$|g| < |u_{i_1} u_{i_2} \cdots u_{i_r}| \quad (8.5)$$

$$|g| > |u_{i_1} u_{i_2} \cdots u_{i_r}| \quad (8.6)$$

$$|g| = |u_{i_1} u_{i_2} \cdots u_{i_r}|, \quad (8.7)$$

and there is a factorization $g = g' h g''$ and $k \in \{1, \dots, p\}$ with

$$|g'| = |u_{i_1} \cdots u_{i_{k-1}}|, \quad |h| = |u_{i_k}|, \quad h \neq u_{i_k}, \quad |g''| = |u_{i_{k+1}} \cdots u_{i_r}|.$$

Define the following relations which are clearly rational:

$$F = \bigcup_{i=1}^p ab^i \times Y^{|u_i|}; \quad G = \bigcup_{i=1}^p ab^i \times (Y^{|u_i|} \setminus u_i) = F \setminus U;$$

$$D = \bigcup_{i=1}^p ab^i \times Y^{|u_i|} Y^+ = F \cdot (1 \times Y^+); \quad C = \bigcup_{i=1}^p ab^i \times Y_i,$$

with $Y_i = \{u \in Y^* : |u| < |u_i|\}$.

Then $CF = FC$, $DF = FD$, and

$$\{(f, g) \mid (f, g) \text{ verifies (8.3) and (8.5)}\} = C^+ F^*;$$

$$\{(f, g) \mid (f, g) \text{ verifies (8.3) and (8.6)}\} = D^+ F^*;$$

$$\{(f, g) \mid (f, g) \text{ verifies (8.3) and (8.7)}\} = F^* G F^*.$$

Thus $W = H \cup C^+ F^* \cup D^+ F^* \cup F^* G F^* \in \text{Rat}(X^* \times Y^*)$. ■

Theorem 8.4 Let X, Y be alphabets with at least two letters. Given rational relations $A, B \subset X^* \times Y^*$, it is undecidable to determine whether

- (i) $A \cap B = \emptyset$;
- (ii) $A \subset B$;
- (iii) $A = B$;
- (iv) $A = X^* \times Y^*$;
- (v) $(X^* \times Y^*) \setminus A$ is finite;
- (vi) A is recognizable.

Proof. We may assume that X contains exactly two letters, and set $X = \{a, b\}$. Consider two sequences

$$u_1, u_2, \dots, u_p \text{ and } v_1, v_2, \dots, v_p \quad (8.8)$$

of words of Y^* and define

$$U = \{(ab, u_1), \dots, (ab^p, u_p)\}, \quad V = \{(ab, v_1), \dots, (ab^p, v_p)\}.$$

Then U^+, V^+ are rational relations, and by the preceding lemma, $\bar{U} = (X^* \times Y^*) \setminus U^+$ and $\bar{V} = (X^* \times Y^*) \setminus V^+$ are rational relations.

- (i) Let $A = U^+, B = V^+$. Then $A \cap B \neq \emptyset$ iff there exist integers $i_1, \dots, i_k$ such that $u_{i_1} \cdots u_{i_k} = v_{i_1} \cdots v_{i_k}$, thus iff the Correspondence Problem (8.8) has a solution. Thus if the emptiness $A \cap B = \emptyset$ would be decidable, Post's Correspondence Problem would be decidable. This proves (i).
- (ii) Let $A = U^+, B = \bar{V}$. Then $A \subset B$ iff $U^+ \cap V^+ = \emptyset$. Thus (ii) follows from (i).
- (iii) is a consequence of (iv) since $X^* \times Y^*$ is rational.
- (iv) Let $A = \bar{U} \cup \bar{V}$. Then $A = X^* \times Y^*$ iff $X^* \times Y^* \setminus A = U^+ \cap V^+ = \emptyset$. Thus (iv) is undecidable by (i).
- (v) Let again $A = \bar{U} \cup \bar{V}$. Then $(m, u) \in X^* \times Y^* \setminus A$ iff there exist $i_1, \dots, i_r$ 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 $(m, u) \in X^* \times Y^* \setminus A$ implies $(m^k, u^k) \in X^* \times Y^* \setminus A$ for any $k \geq 1$. Consequently, $X^* \times Y^* \setminus A$ is finite iff $X^* \times Y^* \setminus A$ is empty, and the last property is undecidable by (iv).
- (vi) Let again $A = \bar{U} \cup \bar{V}$. Then A is recognizable iff $X^* \times Y^* \setminus A = U^+ \cap V^+$ is recognizable since $\text{Rec}(X^* \times Y^*)$ is closed under complementation. We shall see that $U^+ \cap V^+$ is recognizable iff $U^+ \cap V^+ = \emptyset$. Assume $U^+ \cap V^+$ recognizable. Then by Mezei's Theorem,

$$U^+ \cap V^+ = P_1 \times Q_1 \cup \dots \cup P_l \times Q_l$$

for $P_1, \dots, P_l \in \text{Rat}(X^*), Q_1, \dots, Q_l \in \text{Rat}(Y^*)$. 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

$$(m^r, u^r), (m^s, u^s) \in P_i \times Q_j$$

for some j , ($1 \leq j \leq l$). Then $(m^s, u^r) \in P_i \times Q_j$ 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 Show that for a rational relation $A \subset X^* \times Y^*$, the word problem: $(u, v) \in A$ can be solved in $O(n)$ steps, where $n = |u| + |v|$. (For connections with the same problem for linear languages, see Proposition V.6.5.)

8.3 Let $M = \langle \mu, Q, q_-, Q_+ \rangle : X^* \rightarrow Y^*$ be matrix representation. Show that a trim matrix representation realizing $|M|$ can effectively be constructed.

8.4 (continuation of Exercise 4.8) Assume that a rational transduction $\tau : X^* \rightarrow Y^*$ is effectively given. Show that the transductions τ_0 and τ_∞ can be computed effectively.

IV Rational Functions

The present chapter deals with rational functions, i.e. 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 is at most one successful path for each input word. Two different methods for constructing unambiguous representations are given in Section 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 and are used to show that any rational function can be obtained as a 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.

IV.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 Section 4 and 5.

Definition A rational function $\alpha: X^* \rightarrow Y^*$ is a rational transduction which is a partial function, i.e. such that $\text{Card}(\alpha f) \leq 1$ for all $f \in X^*$.

In order to simplify statements and proofs, we first make a general observation. Given any transduction

$$\tau: X^* \rightarrow Y^*$$

define two transductions $\tau_1, \tau_+ : X^* \rightarrow Y^*$ by

$$\begin{aligned} \tau_1(1) &= \tau(1); & \tau_+(1) &= \emptyset; \\ \tau_1(f) &= \emptyset; & \tau_+(f) &= \tau(f) \quad f \in X^+. \end{aligned}$$

Then $\tau = \tau_1 \cup \tau_+$ (and even $\tau = \tau_1 + \tau_+$), and τ is rational iff τ_1 and τ_+ are rational. Further, any transduction $\tau': X^* \rightarrow Y^*$ with $\tau'_+ = \tau_+$ is rational iff τ 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 $\mathbf{M} = \langle \mu, Q, q_-, q_+ \rangle$ realizing τ can always be chosen to be a monoid morphism.

Further, we recall that if $\tau(1) = \emptyset$, then we may assume that $Q_+ = \{q_+\}$ and $q_+ \neq q_-$, and that $\mu f_{q_+q_-} = \mu f_{q_+q} = 0$ for $f \in X^+$, $q \in Q$. 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 $\tau(f) = \mu f_{q_-q_+}$ if $f \in X^+$.

A matrix representation which satisfies the above conditions and which is trim is called normalized. Normalization clearly is effective.

Proposition 1.1 Let $\tau: X^* \rightarrow Y^*$ be the transduction realized by a normalized matrix representation $\mathbf{M} = \langle \mu, Q, q_-, q_+ \rangle$. Then τ is a partial function iff $\text{Card}(\mu f_{pq}) \leq 1$ for any $f \in X^*$, $(p, q \in Q)$.

Proof. If the conclusion holds, then $\text{Card}(\mu f_{q_-q_+}) \leq 1$ for any $f \in X^+$, thus $\text{Card}(\tau(f)) \leq 1$ for $f \in X^*$. Conversely, assume that $\text{Card}(\mu f_{pq}) \geq 2$ for some $f \in X^*$, $(p, q \in Q)$. Then $f \in X^+$ since $\mu 1$ is the identity matrix. Since $\mathbf{M}$ is trim, $\mu h_{q-p} \neq \emptyset$ and $\mu h'_{q_+} \neq \emptyset$ for some $h, h' \in X^*$. Then

$$\tau(hfh') = \mu(hfh')_{q_-q_+} \supset \mu h_{q-p} \mu f_{pq} \mu h'_{q_+},$$

and thus $\text{Card}(\tau(hfh')) \geq 2$. ■

Let $\alpha: X^* \rightarrow Y^*$ be a rational function realized by a normalized matrix representation $\mathbf{M} = \langle \mu, Q, q_-, q_+ \rangle$. Then we associate to $\mathbf{M}$ the transducer $\mathbf{T} = \langle X, Y, Q, q_-, q_+, E \rangle$ with

$$E = \{(p, x, \mu x_{pq}, q) \mid p, q \in Q, x \in X, \mu x_{pq} \neq 0\}.$$

Thus $E \subset Q \times X \times Y^* \times Q$, and for any $(p, x, q) \in Q \times X \times Q$, there is at most one $h \in Y^*$ such that $(p, x, h, q) \in E$. Conversely, if E satisfies these conditions then the formula

$$\mu x_{pq} = \begin{cases} h & \text{if } (p, x, h, q) \in E; \\ 0 & \text{otherwise} \end{cases}$$

defines a matrix representation $\mathbf{M} = \langle \mu, Q, q_-, q_+ \rangle$. The transducer $\mathbf{T}$ and the matrix representation $\mathbf{M}$ are called associated, and we sometimes identify them. Thus we speak of a normalized transducer, of a path in a matrix representation and so on.

Example 1.1 Let $\alpha: x^* \rightarrow \{a, b\}^*$ be given by

$$\alpha(x^n) = \begin{cases} a^n & n \text{ even}; \\ b^n & n \text{ odd}. \end{cases}$$

Then α is a rational transduction (Example III.7.4), hence a rational function.

Example 1.2 Let $X = \{x\}$, $Y = \{b\}$ and consider the transducer in Fig. IV.1

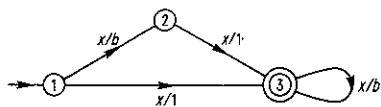


Fig. IV.1

corresponding to the matrix

$$\mu x = \begin{bmatrix} 0 & b & 1 \\ 0 & 0 & 1 \\ 0 & 0 & b \end{bmatrix}.$$

The transduction α realized by this transducer is given by $\alpha(1) = 0$, $\alpha(x^n) = b^{n-1}$, ($n \geq 1$); hence α is a rational function.

Example 1.3 (Choffrut) Let again $X = \{x\}$, $Y = \{b\}$, and consider the transducer in Fig. IV.2. Let α be the transduction realized. It is easy to see that

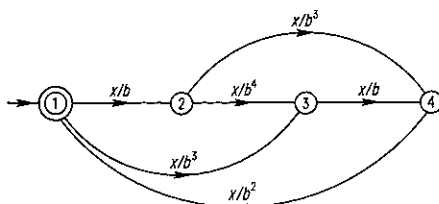


Fig. V.2

there are 3 nonempty paths from state 1 to itself without internal node 1. They are of length 3 and 4 and have labels (x^3, b^6) and (x^4, b^8) . Thus if $\alpha(x^n) \neq 0$, then $\alpha(x^n) = b^{2n}$, and thus, α is a partial function. Further $\text{dom}(\alpha) = 1 \cup x^3 \cup x^4 \cup x^6 x^*$.

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 $\tau: X^* \rightarrow Y^*$ be a transduction realized by a normalized matrix representation $M = \langle \mu, Q, q_-, q_+ \rangle$, and let $m = \text{Card}(Q)$. Then τ is a rational function iff $\text{Card}(\mu f_{pq}) \leq 1$ for all $p, q \in Q$ and all $f \in X^*$ with $|f| \leq 1 + 2m(m-1)$.

Proof. By Proposition 1.1, the condition is necessary. Assume the converse is false. Then, still by Proposition 1.1, $\text{Card}(\mu f_{pq}) \geq 2$ for some $f \in X^+$ and $p, q \in Q$. Choose a word f of minimal length such that $\text{Card}(\mu f_{pq}) \geq 2$ for some $p, q \in Q$. Then $|f| > 1 + 2m(m-1)$. Set $f = x_1 \cdots x_n$ with $x_1, \dots, x_n \in X$. There is a

sequence of $n+1$ pairs of states (q_j, q'_j) , ($j = 0, \dots, n$) such that $q_0 = q'_0 = p$, $q_n = q'_n = q$, and such that with

$$u_j = (\mu x_j)_{q_{j-1}, q_j}, \quad v_j = (\mu x_j)_{q'_{j-1}, q'_j},$$

the words $u = u_1 \cdots u_n$, $v = v_1 \cdots v_n$ are two distinct elements of μf_{pq} . Since f has been chosen of minimal length, $q_j \neq q'_j$ for $j = 1, \dots, n-1$. 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 $1 \leq i < j < k \leq n-1$ such that

$$(q_i, q'_i) = (q_j, q'_j) = (q_k, q'_k). \quad (1.1)$$

Define

$$\begin{aligned} f_1 &= x_1 \cdots x_i, & f_2 &= x_{i+1} \cdots x_j, & f_3 &= x_{j+1} \cdots x_k, & f_4 &= x_{k+1} \cdots x_n; \\ a_1 &= u_1 \cdots u_i, & a_2 &= u_{i+1} \cdots u_j, & a_3 &= u_{j+1} \cdots u_k, & a_4 &= u_{k+1} \cdots u_n; \\ b_1 &= v_1 \cdots v_i, & b_2 &= v_{i+1} \cdots v_j, & b_3 &= v_{j+1} \cdots v_k, & b_4 &= v_{k+1} \cdots v_n. \end{aligned}$$

Then by (1.1)

$$\begin{aligned} a_1 a_4, b_1 b_4 &\in \mu(f_1 f_4)_{pq}; & a_1 a_2 a_4, b_1 b_2 b_4 &\in \mu(f_1 f_2 f_4)_{pq}; \\ a_1 a_3 a_4, b_1 b_3 b_4 &\in \mu(f_1 f_3 f_4)_{pq}. \end{aligned}$$

By the minimality of f , we have

$$a_1 a_4 = b_1 b_4, \quad a_1 a_2 a_4 = b_1 b_2 b_4, \quad a_1 a_3 a_4 = b_1 b_3 b_4. \quad (1.2)$$

We shall deduce from (1.2) that $u = v$, in contradiction with the assumption. By symmetry, we may suppose $|a_1| \leq |b_1|$, hence $b_1 = a_1 w$ for some $w \in Y^*$. Then the first of the equations (1.2) implies $a_4 = w b_4$. Reporting this in the two other equations (1.2) yields: $a_2 w = w b_2$ and $a_3 w = w b_3$. It follows that:

$$u = a_1 a_2 a_3 a_4 = a_1 a_2 a_3 w b_4 = a_1 a_2 w b_3 b_4 = a_1 w b_2 b_3 b_4 = v. \quad \blacksquare$$

Given two rational functions $\alpha, \beta: X^* \rightarrow Y^*$, we write $\alpha \subset \beta$ if $\alpha(f) \neq 0 \Rightarrow \alpha(f) = \beta(f)$, ($f \in X^*$).

Corollary 1.3 Given two rational functions $\alpha, \beta: X^* \rightarrow Y^*$, it is decidable whether $\alpha \subset \beta$, and whether $\alpha = \beta$.

Proof. Clearly $\alpha \subset \beta$ iff the two following conditions hold:

- (i) $\text{dom}(\alpha) \subset \text{dom}(\beta)$;
- (ii) $\alpha \cup \beta$ is a rational function.

Condition (i) is decidable since $\text{dom}(\alpha)$ and $\text{dom}(\beta)$ are regular languages. Condition (ii) is decidable by the previous theorem. Next $\alpha = \beta$ iff $\alpha \subset \beta$ and $\beta \subset \alpha$, thus equality of functions is decidable. $\blacksquare$

Exercises

1.1 Show that it is decidable whether a rational function α is recognizable (i.e. its graph is a recognizable relation).

1.2 Show that it is undecidable, for rational functions $\alpha, \beta: X^* \rightarrow Y^*$, whether there exists a word $f \in X^*$ such that $\alpha(f) = \beta(f)$.

IV.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, the 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 "endmarker". 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 [1977a]. A systematic exposition can be found in Choffrut [1978].

Definition A left sequential transducer (or sequential transducer for short) $\mathbf{L}$ consists of an input alphabet X , an output alphabet Y , a finite set of states Q , an initial state $q_- \in Q$, and of two partial functions

$$\delta: Q \times X \rightarrow Q, \quad \lambda: Q \times X \rightarrow Y^*$$

having the same domain and called the next state function and the output function respectively.

We usually denote δ by a dot, and λ by a star. Thus we write $q \cdot x$ for $\delta(q, x)$ and $q * x$ for $\lambda(q, x)$. Then $\mathbf{L}$ is specified by

$$\mathbf{L} = \langle X, Y, Q, q_- \rangle.$$

With the conventions of Section I.1, Q can be considered as a subset of $\mathfrak{P}(Q)$, and $q \cdot x$ is undefined iff $q \cdot x = \emptyset$ (or $q \cdot x = 0$, by writing 0 for $\emptyset$). Further $0 \cdot x = 0$ for all $x \in X$. Thus, the next state function can also be viewed as a total function from $Q \cup \{0\} \times X$ 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 and the output function are extended to $Q \times X^*$ by setting, for $f \in X^*, x \in X$

$$\begin{aligned} q \cdot 1 &= q; & q \cdot (fx) &= (q \cdot f) \cdot x; \\ q * 1 &= 1; & q * (fx) &= (q * f)((q \cdot f) * x). \end{aligned} \quad (2.1)$$

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 $f, g \in X^*, (q \in Q)$, the following formula hold

$$q \cdot fg = (q \cdot f) \cdot g; \quad (2.2)$$

$$q * fg = (q * f)(q \cdot f * g). \quad (2.3)$$

Indeed (2.2) is clear, and (2.3) is proved by induction on $|g|$: the formula is obvious for $|g|=0$. If $g = hx$ with $h \in X^*, x \in X$, then

$$\begin{aligned} q * fg &= q * fhx = (q * fh)(q \cdot fh * x) \\ &= (q * f)(q \cdot f * h)((q \cdot f) \cdot h * x) = (q * f)(q \cdot f * hx) = (q * f)(q \cdot f * g). \end{aligned}$$

The partial function $|\mathbf{L}|: X^* \rightarrow Y^*$ realized by $\mathbf{L}$ is defined by

$$|\mathbf{L}|(f) = q_- * f \quad (f \in X^*).$$

Definition A partial function $\alpha: X^* \rightarrow Y^*$ is a (left) sequential transduction or (left) sequential function if $\alpha = |\mathbf{L}|$ for some sequential transducer $\mathbf{L}$.

If $\alpha = |\mathbf{L}|$ with $\mathbf{L}$ as above, then

$$\alpha(1) = 1 \quad (2.4)$$

$$\alpha(fg) = \alpha(f)(q_- \cdot f * g). \quad (2.5)$$

By (2.4), $\text{dom}(\alpha)$ is nonempty. Say that a partial function $\alpha: X^* \rightarrow Y^*$ preserves left factors if (2.4) holds and if further

$$\alpha(fg) \neq 0 \Rightarrow \alpha(fg) \in \alpha(f)Y^*.$$

Then by (2.5), a sequential function preserves left factors. Note that this is a rather strong constraint. In particular, the domain of such a function is prefix-closed, i.e. it contains the left factors of its elements. Of course, this is due to the lack of final states.

To each sequential transducer $\mathbf{L} = \langle X, Y, Q, q_- \rangle$ we associate a transducer $\mathbf{T} = \langle X, Y, Q, q_-, Q_+, E \rangle$ by setting $Q_+ = Q$ and

$$E = \{(q, x, q * x, q \cdot x) \mid q \in Q, x \in X, q \cdot x \neq 0\}.$$

Then clearly $|\mathbf{L}| = |\mathbf{T}|$. Thus

Proposition 2.1 Any sequential function is rational. ■

Example 2.1 Any morphism is a sequential function.

Example 2.2 Let $X = \{x, y\}$, $Y = \{a, b\}$, and define $\alpha : X^* \rightarrow Y^*$ by

$$\alpha(f) = \begin{cases} a^{|f|} & \text{if } f \in xX^*, \\ b^{|f|} & \text{otherwise.} \end{cases}$$

Then α is a sequential function realized by the following transducer (Fig. IV.3).

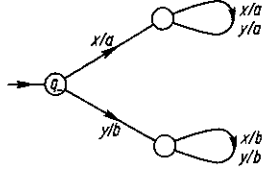


Fig. IV.3

Example 2.3 The function $\tau : x^* \rightarrow \{a, b\}^*$ defined by

$$\tau(x^n) = \begin{cases} a^n & n \text{ even;} \\ b^n & n \text{ odd,} \end{cases}$$

is rational, but not sequential, since it does not preserve left factors. Sometimes, it is useful to have some “reversal” of a left sequential transducer.

Definition A right sequential transducer $R = \langle X, Y, Q, q_- \rangle$ is given by objects X, Y, Q, q_- which have the same meaning as for left sequential transducers, and by two partial functions

$$X \times Q \rightarrow Q; \quad X \times Q \rightarrow Y^*$$

with 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 $X^* \times Q$ by setting

$$\begin{aligned} 1 \cdot q &= q; & xf \cdot q &= x \cdot (f \cdot q); \\ 1 * q &= 1; & xf * q &= (x * f \cdot q)(f * q). \end{aligned}$$

Then the “reversal” of formulas (2.3), (2.4) hold:

$$fg \cdot q = f \cdot (g \cdot q); \quad fg * q = (f * g \cdot q)(g * q). \quad (f, g \in X^*)$$

The partial function $|R|$ realized by R is defined by

$$|R|(f) = f * q_- \quad (f \in X^*),$$

and a partial function realized by a right sequential transducer is called a right sequential transduction or right sequential function.

Proposition 2.2 Let $\alpha : X^* \rightarrow Y^*$ be a partial function, and define $\beta : X^* \rightarrow Y^*$ by $\beta(f) = [\alpha(\tilde{f})]^-$ ($f \in X^*$). Then α is left sequential iff β is right sequential.

Proof. Note first that $\alpha(f) = [\beta(\tilde{f})]^-$, ($f \in X^*$). Thus it suffices to show that if α is right or left sequential, then β is left or right sequential. Assume that α is realized by some right sequential transducer $R = \langle X, Y, Q, q_- \rangle$, and define a left sequential transducer $L = \langle X, Y, Q, q_- \rangle$ by setting

$$q \cdot x = x \cdot q; \quad q * x = (x * q)^-.$$

Then $q \cdot f = \tilde{f} \cdot q$ and $q * f = (\tilde{f} * q)^-$,

since by induction, for $h \in X^*$, $x \in X$,

$$\begin{aligned} q \cdot hx &= (q \cdot h) \cdot x = x \cdot (\tilde{h} \cdot q) = (hx)^- \cdot q, \\ q * hx &= (q * h)(q \cdot h * x) = (\tilde{h} * q)^- (x * \tilde{h} \cdot q)^- \\ &= [(x * \tilde{h} \cdot q)(\tilde{h} * q)]^- = [(hx)^- * q]^- . \end{aligned}$$

Thus $|L|(f) = [|R|(\tilde{f})]^-$ for all $f \in X^*$, and $\beta = |L|$. ■

Corollary 2.3 A right sequential function is rational.

Proof. Let $\alpha : X^* \rightarrow Y^*$ be a right sequential function, and let β be defined by $\beta(f) = [\alpha(\tilde{f})]^-$. Then β is sequential, hence rational, and its graph B is a rational relation. Let A be the graph of α . Then $A = \{(\tilde{f}, g) \mid (f, g) \in B\}$, and A is rational (see Section III.4). ■

Example 2.2 (continued). The function α is not right sequential since it does not preserve right factors.

Example 2.3 (continued). For the same reason, the function τ 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 α which associates, to two words $u, v \in \mathbb{K}^*$ of 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 $u = x_0 x_1 \cdots x_n$, ($x_i \in \mathbb{K}$) either as in Example III.5.16, or by

$$\langle u \rangle = x_0 + x_1 k + \cdots + x_n k^n.$$

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, α can be considered as a function $\alpha : (\mathbb{K} \times \mathbb{K})^* \rightarrow \mathbb{K}^*$. If $v = y_0 y_1 \cdots y_n$, then the argument of α is $f = (x_0, y_0)(x_1, y_1) \cdots (x_n, y_n)$. For simplicity, we write indistinctly $\alpha(u, v)$ or $\alpha(f)$. By Example III.5.16, α is known to be rational, but α is neither left nor right sequential. Consider for instance $k = 2$. Then

$$\alpha(11, 10) = w_1 = 001 \quad \alpha(11111, 10010) = w_2 = 000101.$$

The word $f_1 = (1,1)(1,0)$ is both a left and a right factor of $f_2 = (1,1)(1,0)(1,0)(1,1)(1,0)$, but w_1 is neither a left nor a right factor of w_2 . Now consider the following (left) sequential transducer (Fig. IV.4) and let β be the

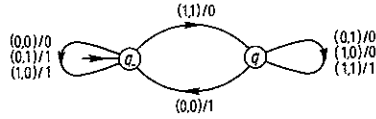


Fig. IV.4

sequential function realized. Then

$$\alpha(f) = \begin{cases} \beta(f) & \text{if } q_- \cdot f = q_-; \\ \beta(f)1 & \text{if } q_- \cdot f = q. \end{cases}$$

Thus α is "almost" a sequential function. This leads to the following definition.

Definition A (left) subsequential transducer $S = \langle X, Y, Q, q_-, \rho \rangle$ is composed of a sequential transducer $\langle X, Y, Q, q_- \rangle$ and of a partial function $\rho: Q \rightarrow Y^*$. The partial function $|S|: X^* \rightarrow Y^*$ realized by S is defined by

$$|S|(f) = (q_- * f)\rho(q_- \cdot f). \quad (2.6)$$

A subsequential function is a partial function realized by some subsequential transducer.

According to the discussion at the beginning of this section, $\rho(q_- \cdot f)$ has the value 0 in (2.6) whenever $q_- \cdot f = 0$.

Example 2.4 (continued). The function α is subsequential with $p(q_-) = \epsilon$, $\rho(q) = 1$.

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 $\alpha: X^* \rightarrow Y^*$ and suppose $\text{dom}(\alpha)$ is finite. We define a subsequential transducer $S = \langle X, Y, Q, q_-, \rho \rangle$ as follows: $Q = \text{dom}(\alpha)(X^*)^{-1}$ is the set of left factors of words in $\text{dom}(\alpha)$; $q_- = 1$. The next state and the output function are defined by

$$u \cdot x = \begin{cases} ux & \text{if } ux \in Q; \\ 0 & \text{otherwise.} \end{cases} \quad u * x = \begin{cases} 1 & \text{if } ux \in Q; \\ 0 & \text{otherwise.} \end{cases}$$

$u \in Q, x \in X.$

Finally,

$$\rho(u) = \begin{cases} \alpha(u) & \text{if } u \in \text{dom}(\alpha) \\ 0 & \text{otherwise.} \end{cases} \quad u \in Q.$$

Then clearly $\alpha = |S|$.

Example 2.7 The function τ of Example 2.3 is not subsequential. Assume indeed that $\tau = |S|$ for S as in the definition and set $K = \max\{|\rho(q)|: \rho(q) \neq 0, q \in Q\}$. Let n be even. Then

$$|S|(x^n) = (q_- * x^n)\rho(q_- \cdot x^n) = a^n$$

$$|S|(x^{n+1}) = (q_- * x^n)(q_- \cdot x^n * x)\rho(q_- \cdot x^{n+1}) = b^{n+1}.$$

If $n > K$, then $w = q_- * x^n$ is not the empty word, and $w \in a^+ \cap b^+$, which is impossible.

Proposition 2.4 A subsequential function is rational.

Proof. Consider a subsequential transducer $S = \langle X, Y, Q, q_-, \rho \rangle$ and define a morphism $\mu: X^* \rightarrow \text{Rat}(Y^*)^{Q \times Q}$ by

$$\mu x_{p,q} = \begin{cases} p * x & \text{if } p \cdot x = q; \\ 0 & \text{otherwise.} \end{cases} \quad (x \in X) \quad (2.7)$$

Then an obvious induction shows that (2.7) still holds if x is replaced by a word $f \in X^*$. Next consider ρ as a column Q -vector, and define a row vector λ by

$$\lambda_q = \begin{cases} 1 & \text{if } q = q_-; \\ 0 & \text{otherwise.} \end{cases}$$

Then: $\lambda \mu f \rho = \bigcup_{q \in Q} \mu f_{q,q} \rho(q) = (q_- * f)\rho(q_- \cdot f) = |S|(f)$.

Thus $|S|$ is rational by Proposition III.7.3. ■

Note that the matrices μf of the preceding proof are row monomial, i.e. for each $p \in Q$, there is at most one $q \in Q$ such that $\mu f_{p,q} \neq 0$. Thus the transductions $f \mapsto \mu f_{q,q}$, ($q \in Q$) have disjoint domains, and the same holds for the transductions $f \mapsto \mu f_{q,q} \rho(q)$.

Proposition 2.5 Let $\alpha: X^* \rightarrow Y^*$ and $\beta: Y^* \rightarrow Z^*$ be subsequential functions. Then $\beta \circ \alpha: X^* \rightarrow Z^*$ is subsequential. If further α and β are sequential (right sequential), then $\beta \circ \alpha$ is sequential (right sequential).

Proof. Consider two subsequential transducers

$$S = \langle X, Y, Q, q_-, \rho \rangle, \quad T = \langle Y, Z, P, p_-, \sigma \rangle$$

realizing α and β respectively. Elements of the product $P \times Q$ are noted $[p, q]$ for easier checking. Define

$$T \circ S = \langle X, Z, P \times Q, [p_-, q_-], \omega \rangle$$

$$[p, q] \cdot x = [p \cdot (q * x), q \cdot x] \quad (2.8)$$

$$[p, q] * x = p * (q * x) \quad p \in P, \quad q \in Q, \quad x \in X \quad (2.9)$$

$$\omega([p, q]) = (p * \rho(q))\sigma(p \cdot \rho(q)). \quad (2.10)$$



We prove that (2.8) and (2.9) remain true if x is replaced by a word $f \in X^*$. This is clear for $f=1$. Arguing by induction, consider $f=hx$, with $h \in X^*$, $x \in X$, and set

$$w = q * h, \quad w' = q \cdot h * x.$$

Then $ww' = q * hx = q * f$ by (2.3). Next

$$\begin{aligned} [p, q] \cdot f &= [p \cdot (q * h), q \cdot h] \cdot x = [p \cdot w, q \cdot h] \cdot x \\ &= [p \cdot w \cdot (q \cdot h * x), q \cdot h \cdot x] \\ &= [p \cdot ww', q \cdot hx] = [p \cdot (q * f), q \cdot f]. \\ [p, q] * f &= ([p, q] * h)([p, q] \cdot h * x) = (p * (q * h))(p \cdot (q * h), q \cdot h * x) \\ &= (p * w)(p \cdot w, q \cdot h * x) \\ &= (p * w)(p \cdot w * (q \cdot h * x)) = (p * w)(p \cdot w * w') = p * ww' \\ &= p * (q * f). \end{aligned}$$

Finally

$$\begin{aligned} \omega([p_-, q_-] \cdot f) &= \omega([p_- \cdot (q_- * f), q_- \cdot f]) \\ &= (p_- \cdot (q_- * f) * \rho(q_- \cdot f)) \sigma(p_- \cdot (q_- * f) \cdot \rho(q_- \cdot f)) \\ &= (p_- \cdot (q_- * f) * \rho(q_- \cdot f)) \sigma(p_- \cdot \alpha(f)). \end{aligned}$$

Consequently

$$\begin{aligned} |T \circ S|(f) &= ([p_-, q_-] * f) \omega([p_-, q_-] \cdot f) \\ &= (p_- * (q_- * f))(p_- \cdot (q_- * f) * \rho(q_- \cdot f)) \sigma(p_- \cdot \alpha(f)) \\ &= (p_- * (q_- * f) \rho(q_- \cdot f)) \sigma(p_- \cdot \alpha(f)) \\ &= (p_- * \alpha(f)) \sigma(p_- \cdot \alpha(f)) = \beta(\alpha(f)). \end{aligned}$$

Thus $|T \circ S| = \beta \circ \alpha$. If both α and β are sequential, then ρ and σ 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 α and β 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 left factors. We show now that a subsequential function which preserves left factors is sequential.

Proposition 2.6 *Let $\alpha : X^* \rightarrow Y^*$ be a partial function. Then α is sequential iff the following conditions hold:*

- (i) α is subsequential;
- (ii) α preserves left factors.

Proof. Clearly the conditions are necessary. Conversely, assume that α satisfies (i) and (ii), and consider a subsequential transducer $S = \langle X, Y, Q, q_-, \rho \rangle$ realizing α . We first put S into some standard form. Consider a state $q \in Q$. If q is not accessible, i.e. 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 $u \in X^*$ such that $q_- \cdot u = q$, and further $\alpha(uv) = 0$ for all $v \in V^*$ since α preserves left factors. Consequently, if the next-state function and the output function are modified by setting $q' \cdot x = 0$, $q' * x = 0$ for all (q', x) such that $q' \cdot x = q$, 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 $q \in Q$, $x \in X$, there exists $\lambda(q, x) \in Y^* \cup \{\emptyset\}$ such that

$$\rho(q) \lambda(q, x) = (q * x) \rho(q \cdot x) \quad (2.11)$$

$$\lambda(q, x) \neq 0 \iff q * x \neq 0. \quad (2.12)$$

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 $q * x \neq 0$, then

$$\alpha(ux) = (q_- * u)(q * x) \rho(q \cdot x) \neq 0,$$

and since α preserves left factors,

$$\alpha(ux) = \alpha(u)g = (q_- * u) \rho(q)g$$

for some word $g \in Y^*$. Thus

$$\rho(q)g = (q * x) \rho(q \cdot x),$$

showing that g is independent of u . We define

$$\lambda(q, x) = \begin{cases} g & \text{if } q * x \neq 0; \\ 0 & \text{otherwise.} \end{cases}$$

Then λ has the same domain as the output function of S .

Consider now the sequential transducer $L = \langle X, Y, Q, q_- \rangle$ with the same next state function as S , and with output function λ . We claim that $\alpha = |L|$, i.e. that $\alpha(f) = \lambda(q_-, f)$ for $f \in X^*$. By (ii), this holds for $f=1$. If $f=hx$, with $h \in X^*$, $x \in X$, then

$$\begin{aligned} \lambda(q_-, f) &= \lambda(q_-, h) \lambda(q_- \cdot h, x) = \alpha(h) \lambda(q_- \cdot h, x) \\ &= (q_- * h) \rho(q_- \cdot h) \lambda(q_- \cdot h, x) \\ &= (q_- * h)(q_- \cdot h * x) \rho(q_- \cdot hx) = \alpha(hx). \end{aligned}$$

Subsequential functions preserve left factors only if they are sequential. However, they satisfy a property which is closely related to the preservation of left factors. Consider indeed a subsequential transducer $S = \langle X, Y, Q, q_-, \rho \rangle$, and

let $\alpha = |S|$. If $u_1, u_2 \in \text{dom}(\alpha)$ are "near" in the sense that $u_1 = uv_1$, $u_2 = uv_2$ and $|v_1| + |v_2|$ is "small", then $\alpha(u_1), \alpha(u_2)$ 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 $u, v \in X^*$, we define

$$u \wedge v = \text{the greatest common left factor of } u \text{ and } v.$$

More generally, if A is a nonempty language, define

$$\bigwedge A = \text{the longest word which is a left factor of all words in } A.$$

The notation is justified by the following remark: Define a relation $\leq$ by: $u \leq v$ iff u is a left factor of v . Then $\leq$ is a partial order, sometimes called the "prefix order". Since $u \leq v$ iff $u \wedge v = u$, X^* 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 left factor of u and v is erased. In order to verify that we get a distance, we first observe that $\|u, v\| = 0$ iff $|u| + |v| = 2|u \wedge v|$. Since $|u \wedge v| \leq |u|, |v|$, this is equivalent to $|u \wedge v| = |u| = |v|$, i.e. to $u = v$. Next we verify that

$$\|u, v\| \leq \|u, w\| + \|w, v\| \quad u, v, w \in X^*.$$

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 left factors of w , either $u \wedge w$ is a left factor of $v \wedge w$, thus of v , and of u , and $|u \wedge w| \leq |u \wedge v|$, or $v \wedge w$ is a left factor 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

$$||u| - |v|| \leq \|u, v\| \quad u, v \in X^*. \quad (2.13)$$

Another useful inequality is the following: if $A \subset X^*$, $A \neq \emptyset$, and $w = \bigwedge A$, then

$$\|w, u\| \leq \max_{f \in A} \|f, g\| \quad u \in A. \quad (2.14)$$

Indeed, for any $u \in A$, there is some $v \in A$ such that $u \wedge v = w$, (since otherwise w would be a proper left factor of all $u' \wedge v$, ($v \in A$) for some $u' \in A$, thus of all $v \in A$). Consequently $\|w, u\| = \|u \wedge v, u\| \leq \|v, u\| \leq \max_{f, g \in A} \|f, g\|$.

Definition A partial function $\alpha: X^* \rightarrow Y^*$ has bounded variation iff for all $k \geq 0$, there exists $K \geq 0$ such that

$$u, v \in \text{dom}(\alpha), \|u, v\| \leq k \Rightarrow \|\alpha(u), \alpha(v)\| \leq K.$$

Example 2.8 A subsequential function has bounded variation. Let indeed $\alpha = |S|$, with $S = \langle X, Y, Q, q_-, \rho \rangle$, and set

$$M = \max\{|q * x| : q \in Q, x \in X, q * x \neq 0\},$$

$$N = \max\{|\rho(q)| : q \in Q, \rho(q) \neq 0\}.$$

If $uv \in \text{dom}(\alpha)$, 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 $u_1, u_2 \in \text{dom}(\alpha)$ 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 the stronger inequality:

$$\|\alpha(u_1), \alpha(u_2)\| \leq M'(1 + \|u_1, u_2\|).$$

The following result gives a characterization of subsequential functions.

Theorem 2.7 (Choffrut [1978]) Let $\alpha: X^* \rightarrow Y^*$ be a partial function. Then α is subsequential iff

- (i) α has bounded variation;
- (ii) for all $L \in \text{Rat}(Y^*)$, $\alpha^{-1}(L) \in \text{Rat}(X^*)$.

This theorem is an extension of a characterization of sequential functions:

Theorem 2.8 (Ginsburg, Rose [1966]) Let $\alpha: X^* \rightarrow Y^*$ be a partial function. Then α is sequential iff

- (i) α preserves left factors;
- (ii) there exists an integer M such that, for all $u \in X^*$, $x \in X$:

$$ux \in \text{dom}(\alpha), \alpha(ux) = \alpha(u)g \text{ imply } |g| \leq M;$$

- (iii) for all rational languages $L \subset Y^*$, $\alpha^{-1}(L)$ is a rational language.

Proof. In order to deduce Theorem 2.8 from Theorem 2.7, it suffices to show that α has bounded variation. The desired conclusion then follows by Proposition 2.6. Let $k \geq 0$, and let $uv_1, uv_2 \in \text{dom}(\alpha)$ be such that $v_1 \wedge v_2 = 1$, and $\|uv_1, uv_2\| = |v_1| + |v_2| \leq k$. Then $\alpha(uv_1) = \alpha(u)g_1$, $\alpha(uv_2) = \alpha(u)g_2$ and, by (ii), $|g_1| < |v_1| M$, $|g_2| < |v_2| M$. Consequently, $\|\alpha(uv_1), \alpha(uv_2)\| \leq |g_1| + |g_2| \leq k \cdot M$. ■

Proof of Theorem 2.7. The 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 α a finite set R of partial functions from X^* into Y^* . We then prove that a certain family A_r ($r \in R$) of subsets of X^* is composed of regular languages. This enables us to construct a machine realizing α , which works like a subsequential transducer excepted that the output function has its values in the free group $Y^{(*)}$ generated by Y . The last step consists in replacing this transducer by a sequential transducer satisfying our definition. We use the following abbreviation:

If Z is an alphabet and $n \geq 0$ is an integer, then

$$Z^{(n)} = 1 \cup Z \cup \dots \cup Z^n = Z^* \setminus Z^n Z^+.$$

Let $\alpha: X^* \rightarrow Y^*$ satisfy (i) and (ii). Then $\text{dom}(\alpha) = \alpha^{-1}(Y^*)$ is a regular language by (ii). Let N be the number of states of a finite automaton recognizing $\text{dom}(\alpha)$. Then we note, for later reference, that

$$uX^* \cap \text{dom}(\alpha) \neq \emptyset \quad \text{iff} \quad uX^{(N-1)} \cap \text{dom}(\alpha) \neq \emptyset. \quad (2.15)$$

Indeed, if $uv \in \text{dom}(\alpha)$ and $|v| \geq N$, then there exists, by the Iteration Lemma for Regular Languages, a word v' such that $|v'| < |v|$ and $uv' \in \text{dom}(\alpha)$.

For $u \in X^*$ define

$$J(u) = \{v \in X^{(N)} \mid \alpha(uv) \neq 0\},$$

and define a partial function $\beta: X^* \rightarrow Y^*$ by

$$\beta(u) = \begin{cases} 0 & \text{if } J(u) = \emptyset; \\ \bigwedge \{\alpha(uv) : v \in J(u)\} & \text{otherwise.} \end{cases}$$

Thus $\beta(u) \neq 0$ iff $J(u) \neq \emptyset$ iff $uX^{(N)} \cap \text{dom}(\alpha) \neq \emptyset$. In this case, there exists, for each $v \in J(u)$, a word $r_u(v) \in Y^*$ such that

$$\alpha(uv) = \beta(u)r_u(v) \quad (2.16)$$

and further there are $v_1, v_2 \in J(u)$ such that

$$r_u(v_1) \wedge r_u(v_2) = 1. \quad (2.17)$$

(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 $v \in X^{(N)} \setminus J(u)$. Thus for any $u \in X^*$, there is a partial function r_u from $X^{(N)}$ into Y^* satisfying (2.16), with $\text{dom}(r_u) = J(u)$. Further $\alpha(u) \neq 0$ iff $1 \in J(u)$ iff $r_u(1) \neq 0$.

a) We prove that there exists an integer M such that $\max\{|r_u(v)| : v \in \text{dom}(r_u)\} \leq M$ for all $u \in X^*$. 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 $X^{(N)} \rightarrow Y^{(M)}$ and the set

$$R = \{r_u : u \in X^*\},$$

as a subset of the finite set of all partial functions from $X^{(N)}$ into $Y^{(M)}$ is itself finite. We note $\mathbf{0}$ the partial function $X^{(N)} \rightarrow Y^{(M)}$ with empty domain.

b) For $r \in R$, define $A_r = \{u \in X^* \mid r_u = r\}$. We claim: the languages A_r are rational. To prove this, define for $i = 0, \dots, 2M$ and $h \in Y^M$:

$$D_{i,h} = \{g \in Y^* : |g| = i \pmod{2M+1} \text{ and } (g \in Y^*h \text{ or } h \in Y^*g)\}.$$

(Note that there is at most one $g \in D_{i,h}$ such that $h \in Y^*g$.) Clearly the languages $D_{i,h}$ are rational. Consider a fixed $r \in R$ and define

$$\begin{aligned} L_{v,i,h} &= [\alpha^{-1}(D_{i,h}r(v))]v^{-1} & \text{for } v \in \text{dom}(r) \\ K_v &= [X^* \setminus \text{dom}(\alpha)]v^{-1} & \text{for } v \in X^{(N)} \setminus \text{dom}(r). \end{aligned}$$

By (ii), these languages are rational. Set

$$K = \bigcap_{v \in X^{(N)} \setminus \text{dom}(r)} K_v; \quad L_{i,h} = \bigcap_{v \in \text{dom}(r)} L_{v,i,h}; \quad B_r = K \cap \left(\bigcup_{i=0}^{2M} \bigcup_{h \in Y^M} L_{i,h} \right).$$

Then B_r is a rational language. We show that $A_r = B_r$, which proves the claim.

Consider first $u \in B_r$. We must show that $r_u = r$. There exist $i \in \{0, \dots, 2M\}$, $h \in Y^M$ such that $u \in K \cap L_{i,h}$. Thus if $v \in \text{dom}(r)$, $\alpha(uv) \in D_{i,h}r(v)$, and if $v \in X^{(N)} \setminus \text{dom}(r)$, then $\alpha(uv) = 0$. Thus $\text{dom}(r) = \text{dom}(r_u)$. If $r = \mathbf{0}$, then $r = r_u$. Next if $\text{dom}(r)$ is a singleton v , then since $r = r_u$ for some $u' \in X^*$, $r(v) = 1$ by the remark following (2.17), and $r = r_u$. Thus assume $\text{Card}(\text{dom}(r)) \geq 2$. Then for each $v \in \text{dom}(r)$, there is a word $g_v \in D_{i,h}$ such that

$$\alpha(uv) = \beta(u)r_u(v) = g_v r(v), \quad (2.18)$$

and it suffices to show that $g_v = \beta(u)$ for $v \in \text{dom}(r)$. Let $v, v' \in \text{dom}(r)$. By (2.13), we have

$$|g_v| - |g_{v'}| = |\alpha(uv)| - |\alpha(uv')| + |r(v')| - |r(v)| \leq \|\alpha(uv), \alpha(uv')\| + M \leq 2M,$$

thus $||g_v| - |g_{v'}|| \leq 2M$. Since further $|g_v| \equiv |g_{v'}| \pmod{2M+1}$, it follows that $|g_v| = |g_{v'}|$ for all $v, v' \in \text{dom}(r)$. Let n be the common length of the words g_v ($v \in \text{dom}(r)$).

Since $r = r_u$ for some $u' \in X^*$, there exist, by (2.17), words $v_1, v_2 \in \text{dom}(r)$ 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 $\text{dom}(r)$ such that $r_u(v_1) \wedge r_u(v_2) = 1$. By

(2.18) there are two words g_1, g_2 of the same length such that

$$r_u(v_1) = g_1 r(v_1), \quad r_u(v_2) = g_2 r(v_2).$$

Therefore $|g_1| = |g_2| \leq M$, and g_1, g_2 are both right factors of h . Thus $g_1 = g_2$. Since $r_u(v_1) \wedge r_u(v_2) = 1$, $g_1 = g_2 = 1$ and $|\beta(u)| = n$. Thus $u \in A_r$.

Conversely, let $u \in A_r$. If $r = r_u = \mathbf{0}$, then $L_{i,h} = X^*$ for all i and all h , and clearly $u \in K$. Thus $u \in B$, in this case. Thus assume $\text{dom}(r) \neq \emptyset$, and let i be the integer such that $0 \leq i \leq 2M$ and $|\beta(u)| = i \pmod{2M+1}$. Next let h be either the unique right factor of length M of $\beta(u)$ if $|\beta(u)| \geq M$, or any word in $Y^M \cap Y^* \beta(u)$ otherwise. Then $\alpha(uv) \in D_{i,h} r(v)$ for all $v \in \text{dom}(r)$, and consequently $u \in L_{i,h}$. Since clearly $u \in K$, we have $u \in B$.

c) Let $S' = \langle X, Q', q_- \rangle$ be an accessible semiautomaton recognizing simultaneously all A_r ($r \in R$) (for the construction, see Section I.4). Then for each $r \in R$, there is a subset Q_r of Q' such that

$$A_r = |S'(Q_r)| = \{u \in X^* \mid q_- \cdot u \in Q_r\}.$$

Clearly the Q_r are pairwise disjoint, and $Q' = \bigcup_{r \in R} Q_r$. Next set

$$R_+ = \{r \in R \mid r(1) \neq 0\}, \quad Q_+ = \bigcup_{r \in R_+} Q_r.$$

Then $\mathbf{0} \notin R_+$ and $\text{dom}(\alpha) = |S'(Q_+)|$. Observe that

$$u \in A_{\mathbf{0}} \Leftrightarrow q_- \cdot u \in Q_{\mathbf{0}} \Leftrightarrow \beta(u) = 0 \quad (2.19)$$

and that further, in view of (2.15)

$$u \in A_{\mathbf{0}} \Leftrightarrow uX^* \cap \text{dom}(\alpha) = \emptyset \Leftrightarrow uX^{(N-1)} \cap \text{dom}(\alpha) = \emptyset. \quad (2.20)$$

Thus $u \in A_{\mathbf{0}}$ implies $uX^* \subset A_{\mathbf{0}}$ (in other terms, $A_{\mathbf{0}}$ is a right ideal). Thus $q \in Q_{\mathbf{0}}$ implies $q \cdot f \in Q_{\mathbf{0}}$ for all $f \in X^*$, and further $q_- \notin Q_{\mathbf{0}}$, since otherwise $\alpha = 0$ and there is nothing to prove.

Define $S = \langle X, Q, q_- \rangle$ by setting $Q = Q' \setminus Q_{\mathbf{0}}$, and by defining the next state function of S to be the partial function obtained by restriction of the next state function of S' to Q . Thus $q \cdot x = 0$ in S iff $q \cdot x \in Q_{\mathbf{0}}$ in S' . Then for $q \in Q_r \subset Q$, $x \in X$:

$$q \cdot x = 0 \quad \text{iff} \quad \text{dom}(r) \cap xX^{(N-1)} = \emptyset. \quad (2.21)$$

Indeed, let $u \in X^*$ be such that $q_- \cdot u = q$. Then by (2.20), $q \cdot x = 0$ iff $uxX^{(N-1)} \cap \text{dom}(\alpha) = \emptyset$, and this holds iff $\text{dom}(r) \cap xX^{(N-1)} = \emptyset$. After these preliminaries, we now construct a subsequential transducer realizing α , but with output function into the free group $Y^{(*)}$ generated by Y . (Since each word of Y^* is reduced, Y^* can be identified with its image in $Y^{(*)}$, and hence Y^* can be viewed as a submonoid of $Y^{(*)}$. In particular, if $u, v \in Y^*$ then $u^{-1}v$ is

always a welldefined element of $Y^{(*)}$, and $u^{-1}v$ is in Y^* iff u is a left factor of v . See also II.3.) Consider a new state q_0 , and extend the next state function of S by setting

$$q_0 \cdot x = q_- \cdot x \quad (x \in X)$$

Next define

$$q_0 * x = \beta(x) \quad (x \in X),$$

and for $q \in Q$, $x \in X$,

$$q * x = \begin{cases} 0 & \text{if } q \cdot x = 0 \\ r(xv)r'(v)^{-1} & \text{if } q \cdot x \in Q_r, \quad v \in \text{dom}(r) \cap xX^{(N-1)}. \end{cases}$$

First we verify that the definition is correct. If $q \cdot x = q' \in Q_r$, then $\text{dom}(r) \cap xX^{(N-1)} \neq \emptyset$ by (2.20). Thus if $u \in X^*$ is such that $q_- \cdot u = q$, then for $v \in \text{dom}(r) \cap xX^{(N-1)}$,

$$0 \neq \alpha(uxv) = \beta(u)r(xv) = \beta(ux)r'(v), \quad (2.22)$$

showing first that $r'(v) \neq 0$, and next that $r(xv)r'(v)^{-1} = \beta(u)^{-1}\beta(ux)$ is an element of $Y^{(*)}$ which is independent of the choice of v in $\text{dom}(r) \cap xX^{(N-1)}$. Thus the next state function and the output function have the same domain. We claim:

$$q_0 * u = \beta(u) \quad u \in X^+. \quad (2.23)$$

This holds for $|u| = 1$. Arguing by induction, consider $u \in X^+$, $x \in X$. If $\beta(u) = 0$, then $u \in A_{\mathbf{0}}$, and $ux \in A_{\mathbf{0}}$. Consequently $q_0 * ux = 0 = \beta(ux)$ 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),

$$q_0 * ux = \beta(u)(q * x) = \begin{cases} 0 & \text{if } q \cdot x = 0 \\ \beta(u)(\beta(u))^{-1}\beta(ux) & \text{otherwise.} \end{cases}$$

Since by (2.19), $q \cdot x = 0$ iff $\beta(ux) = 0$, (2.23) is proved. Finally define $\rho: q_0 \cup Q \rightarrow Y^*$ by $\rho(q_0) = \alpha(1)$, and

$$\rho(q) = \begin{cases} 0 & \text{if } q \notin Q_+ \\ r(1) & \text{if } q \in Q_r \text{ and } r \in R_+. \end{cases} \quad q \in Q$$

Then $(q_0 * u)\rho(q_0 \cdot u) = \alpha(u)$ for all $u \in X^*$.

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

$$U_q = \{u \in X^* \mid q_0 \cdot u = q\}$$

$$\sigma(q) = \text{the longest right factor common to the words } q_0 * u, (u \in U_q).$$

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

$\theta: X^* \rightarrow Y^*$ is a partial function with same domain as β . Let $q \in Q \cup q_0$, and let $u \in U_q$, and suppose there is a letter x such that $q \cdot x \neq 0$. Then

$$q_0 * ux = \theta(u)\sigma(q)(q \cdot x) = \theta(ux)\sigma(q \cdot x).$$

Since $q_0 * u, q_0 * ux \in Y^*$ and $q \cdot x \in Y^{(*)}$, there are words $f, g, h \in Y^*$ such that $\theta(u)\sigma(q) = fh$, $h^{-1}g = q \cdot x$. The last relation shows that h, g are independent of the choice of u in U_q . Thus h is a common right factor to all $q_0 * u (u \in U_q)$. Consequently $\sigma(q) = th$ for some $t \in Y^*$, and $\sigma(q)(q \cdot x) = w \in Y^*$ with $w = thh^{-1}g = tg$. Thus

$$\theta(u)w = \theta(ux)\sigma(q \cdot x) \quad u \in U_q.$$

Assume $|w| < |\sigma(q \cdot x)|$. Then the words $\theta(u)$ have a nonempty common right factor, in contradiction with the definition of $\sigma(q)$. Thus $|w| \geq |\sigma(q \cdot x)|$, and there is a word $\lambda(q, x) \in Y^*$ such that

$$\theta(u)\lambda(q, x) = \theta(ux) \quad (u \in U_q). \quad (2.24)$$

Define $\lambda(q, x) = 0$ whenever $q \cdot x = 0$, and consider S equipped with the output function λ . λ 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 $u \in X^*$. Define $\tau: Q \cup q_0 \rightarrow Y^*$ by $\tau(q) = \sigma(q)\rho(q)$. Then

$$\alpha(u) = \beta(u)\rho(q_0 \cdot u) = \lambda(q_0, u)\tau(q_0 \cdot u) \quad u \in X^*,$$

and α is realized by the subsequential transducer $S = \langle X, Y, Q \cup q_0, q_0, \tau \rangle$ with output function λ . ■

Remark. Consider a partial function $\alpha: X^* \rightarrow Y^*$ realized by a "generalized" sequential transducer defined as a sequential transducer, but with an output function from X^* into the free group $Y^{(*)}$. Such a transducer can erase a right factor 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, i.e. α is subsequential.

Exercises

2.1 Let $\alpha: X^* \rightarrow Y^*$ be a partial function, and let $\#$ be a new symbol. Show that α is subsequential iff there exists a sequential transduction $\beta: (X \cup \#)^* \rightarrow Y^*$ such that $\alpha(u) = \beta(u\#)$ for all $u \in X^*$.

2.2 Let $\alpha_1, \alpha_2: X^* \rightarrow Y^*$ 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 α_1, α_2 are subsequential.

2.3 Let $\alpha: X^* \rightarrow Y^*$ be a subsequential function, and let $R \subset X^*$ be a rational language. Show that the restriction $\alpha|_R$ is subsequential.

IV.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 $\alpha: X^* \rightarrow Y^*$ be a morphism. For any rational language $A \subset X^*$ there exists a rational language $B \subset A$ such that α maps bijectively B onto $\alpha(A)$.*

Set $C = \alpha(A)$. The theorem asserts that in each class $A \cap \alpha^{-1}(f)$, ($f \in C$) a unique word u_f can be chosen in such a way that the language $B = \{u_f \mid f \in C\}$ is rational. The language B is called a cross-section of α on A . We shall see that the proof is effective. Thus given α and A , a cross-section of α on A can be constructed effectively.

Proof. We shall factorize α in morphisms of special form. Therefore we first verify that if $\beta: Y^* \rightarrow Z^*$ is a second morphism, and if the conclusion holds for α and β , it also holds for $\beta \circ \alpha: X^* \rightarrow Z^*$. Indeed, let $A \subset X^*$ be rational, and let B be a rational cross-section of α on A . Set $C = \alpha(A) = \alpha(B)$, and let $D \subset Y^*$ be a rational cross-section of β on C . Define $E = B \cap \alpha^{-1}(D)$. Then E is rational, α is injective on E , and $\alpha(E) = D$. Since β is injective on D , it follows that $\beta \circ \alpha$ is injective on E . Further $\beta \circ \alpha(E) = \beta(D) = \beta(C) = \beta \circ \alpha(A)$. Thus E is a cross-section of $\beta \circ \alpha$ on A .

Next note that if α is injective, the conclusion holds trivially by taking $B = A$. Since any morphism $\alpha: X^* \rightarrow Y^*$ can be factorized into $\alpha = \beta \circ \gamma$, where $\gamma: X^* \rightarrow Z^*$ is injective and $\beta: Z^* \rightarrow Y^*$ is alphabetic, it suffices to consider the case where α is alphabetic. Further, any alphabetic morphism factorizes into projections and strictly alphabetic morphisms. Thus it suffices to consider the following two cases:

$$\begin{aligned} X &= \{x_1, \dots, x_n\} & Y &= \{x_1, \dots, x_{n-1}\} & (n \geq 2) \\ \alpha(x_i) &= x_i & i &= 1, \dots, n-1 \\ \alpha(x_n) &= x_{n-1} & \text{or } \alpha(x_n) &= 1. \end{aligned}$$

Define the lexicographical order on X^* by setting $u < v$ if either of the following cases holds

$$\begin{aligned} v &= uw & \text{with } w \neq 1 \\ u &= fx_i g, \quad v = fx_i g' & \text{with } i < j. \end{aligned}$$

Next define a transduction $\tau: X^* \rightarrow X^*$ by setting

$$\tau(u) = \{v \mid v > u \text{ and } \alpha(v) = \alpha(u)\},$$

and set

$$B = A \setminus \tau(A).$$

Thus for each $u \in A$, the smallest element of $\alpha^{-1}\alpha(u) \cap A$ is selected, and B is the set of all elements so selected. thus B is a cross-section of α on A .

To prove that B is rational, it suffices to show that the transduction τ is rational. This will be done by constructing transducers realizing τ . If $\alpha(x_n) = x_{n-1}$, we define a transducer by Fig. IV.5 with $V = \{x_i/x_i : i = 1, \dots, n\}$. If

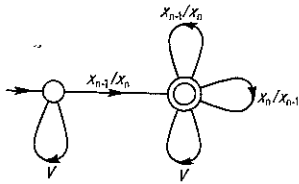


Fig. IV.5

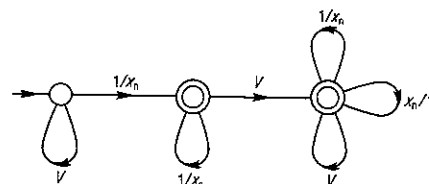


Fig. IV.6

$\alpha(x_n) = 1$, then we consider the transducer in Fig. IV.6. Then it is easily seen that these transducers realize τ . ■

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 $\alpha(x_n) = x_{n-1}$ can be skipped. We conserved it since in the construction of unambiguous representations for rational functions, precisely that case appears, and it is easier to handle directly than through an additional decomposition.

We emphasize the fact that the cross-section B can be obtained effectively from A . Assume $\alpha(x_n) = x_{n-1}$. Then we can proceed as follows. Let y and z be new letters, define $Z = X \cup \{y, z\}$, and let $\varphi, \psi: Z^* \rightarrow X^*$ be the morphisms

$$\begin{aligned} \varphi(x_i) &= \psi(x_i) = x_i & i = 1, \dots, n, \\ \varphi(y) &= \psi(z) = x_{n-1}, & \varphi(z) = \psi(y) = x_n. \end{aligned} \quad (3.1)$$

Then for $A \subset X^*$,

$$\tau(A) = \psi(\varphi^{-1}(A) \cap K) \quad (3.2)$$

where K is the rational language over Z recognized by the automaton in Fig. IV.7. Thus if A is given by a finite automaton, finite automata recognizing $\varphi^{-1}(A)$, $\varphi^{-1}(A) \cap K$, $\tau(A)$ and $A \setminus \tau(A)$ can be effectively constructed.

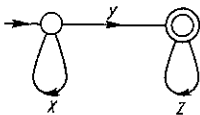


Fig. IV.7

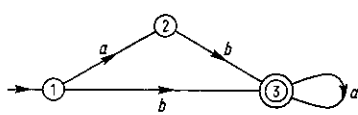


Fig. IV.8

Example 3.1 Let $X = \{a, b\}$ and let $\alpha: X^* \rightarrow a^*$ be the morphism given by $\alpha(a) = \alpha(b) = a$. Further, let $A \subset X^*$ be given by Fig. IV.8. The lexicographical

order is given here by $a < b$. Then

$$\tau(A) = bX^+$$

and the desired cross-section is

$$B = A \setminus \tau(A) = aba^* \cup b.$$

Example 3.2 Let $X = \{a, b, c, d\}$, let $\alpha: X^* \rightarrow a^*$ be the morphism given by $\alpha(X) = a$, and let $A \subset X^*$ be recognized by Fig. IV.9. Thus

$$A = [(bdb \cup bc \cup cb)a]^*.$$

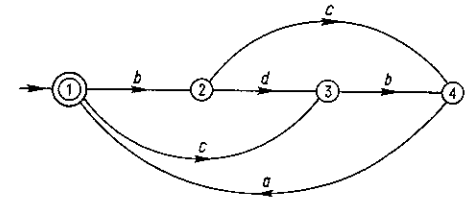


Fig. IV.9

Define a factorization $\alpha = \alpha_3 \circ \alpha_2 \circ \alpha_1$:

$$X^* \xrightarrow{\alpha_1} \{a, b, c\}^* \xrightarrow{\alpha_2} \{a, b\}^* \xrightarrow{\alpha_3} a^*$$

by $\alpha_1(d) = c$, $\alpha_2(c) = b$, $\alpha_3(b) = a$, the other letters being unchanged. We compute a cross-section of α on A .

First $A_1 = \alpha_1(A) = [(bcb \cup bc \cup cb)a]^*$,

and α_1 is injective on A . Next

$$A_2 = \alpha_2(A_1) = [(b^3 \cup b^2)a]^*.$$

We have $b < c$, and

$$A'_1 = [(bcb \cup bc)a]^* \subset A_1$$

is a rational cross-section of α_2 on A_1 . Then

$$A_3 = \alpha_2(A_2) = [a^4 \cup a^3]^*.$$

Since $a < b$, the construction of the proof yields

$$A'_2 = (b^2a)^*(1 \cup b^3a \cup (b^3a)^2)$$

as rational cross-section of α_3 on A_2 . By backward computation

$$A''_1 = A'_1 \cap \alpha_2^{-1}(A'_2) = (bca)^*(1 \cup bcba \cup (bcba)^2)$$

is a rational cross-section of $\alpha_3 \circ \alpha_2$ on A_1 , and

$$B = A \cap \alpha_1^{-1}(A''_1) = (bca)^*(1 \cup bdba \cup (bdba)^2)$$

is a rational cross-section of α on A .

Exercise

3.1 Replace α in Example 3.1 by: $\alpha(a) = \alpha(b) = b$, and compute a cross-section of α on A .

IV.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

$$T = \langle X, Y, Q, q_-, q_+, E \rangle$$

is assumed to satisfy the two conditions

$$E \subset Q \times X \times Y^* \times Q, \quad (4.1)$$

$$(p, x, h, q), (p, x, h', q) \in E \Rightarrow h = h'. \quad (4.2)$$

Definition The transducer T is called **unambiguous** if any word $f \in X^*$ is the input label of at most one successful path e in T .

Let τ be the transduction realized by T . If T is unambiguous and if $f \in \text{dom}(\tau)$, then there exists a successful path e in T with input label f . Let g be the output label of e . Then $\tau(f) = g$. Thus

Proposition 4.1 *The transduction realized by an unambiguous transducer is a partial function.* ■

Conversely, we have

Theorem 4.2 (Eilenberg [1974]) *Let $\tau: X^* \rightarrow Y^*$ be a rational function (with $\tau(1) = 0$ or $\tau(1) = 1$). Then there exists an unambiguous transducer realizing τ .*

Proof. By Corollary III.7.2, there are an alphabet Z , a strictly alphabetic morphism $\alpha: Z^* \rightarrow X^*$, a rational substitution $\sigma: Z^* \rightarrow Y^*$, and a regular language $K \subset Z^*$ such that

$$\tau(f) = \sigma(\alpha^{-1}(f) \cap K) \quad f \in X^*.$$

Clearly we may assume Z minimal, i.e. each letter $z \in Z$ has at least one occurrence in a word in $\alpha^{-1}(X^*) \cap K$. Then σ is a morphism, since τ is a partial function.

Since $\text{dom}(\tau) = \alpha(K)$, there exists, by the Cross-Section Theorem, a rational language $R \subset K$ that maps bijectively R onto $\text{dom}(\tau)$. Let

$$A = \langle Z, Q, q_-, q_+ \rangle$$

be a finite automaton recognizing R , and define

$$T = \langle X, Y, Q, q_-, q_+, E \rangle$$

$$E = \{(q, \alpha z, \sigma z, q \cdot z) \mid q \in Q, z \in Z\}.$$

Note that T satisfies (4.1) and (4.2). Indeed, since α is strictly alphabetic, $\alpha z \in X$ for $z \in Z$. Next consider two successful paths

$$e = (q_-, u_1, v_1, q_1) \cdots (q_{n-1}, u_n, v_n, q)$$

$$e' = (q_-, u'_1, v'_1, q'_1) \cdots (q_{m-1}, u'_m, v'_m, q')$$

and let $z_i, z'_j \in Z$ such that $\alpha z_i = u_i$, $(1 \leq i \leq n)$, $\alpha z'_j = u'_j$, $(1 \leq j \leq m)$. Assume that e and e' have the same input label $f = \alpha h = \alpha h'$ with $h = z_1 \cdots z_n$, $h' = z'_1 \cdots z'_m$. Since $h, h' \in R$ and α is injective on R , it follows that $h = h'$ and $e = e'$. This shows that T is unambiguous. ■

Corollary 4.3 *Let $\tau: X^* \rightarrow Y^*$ be a rational function. Then there exists a normalized unambiguous transducer realizing τ .*

Proof. Let $T = \langle X, Y, Q, q_-, q_+, E \rangle$ be an unambiguous transducer realizing τ . Add two new states q_0, q_1 to Q , and the transitions

$$\{(q_0, x, h, q) \mid (q_-, x, h, q) \in E\} \cup \{(q, x, h, q_1) \mid (q, x, h, q_+) \in E, q_+ \in Q_+\}$$

to E . Take q_0 as 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 $X = \{x\}$, $Y = \{a, b\}$, and consider the transducer in Fig. IV.10

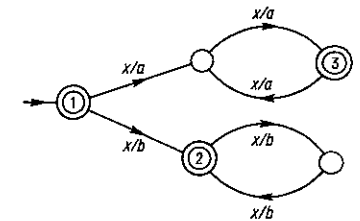


Fig. IV.10

realizing the function

$$\tau(x^n) = \begin{cases} a^n & n \text{ even;} \\ b^n & n \text{ odd.} \end{cases}$$

The transducer is unambiguous since if n is even the only successful 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 (Fig. IV.11). This transducer is ambiguous. Take as alphabet Z the labels of the transitions: $Z = \{(x/b), (x/1)\}$, and consider the morphism $\alpha: Z^* \rightarrow x^*$ defined by

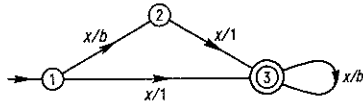


Fig. IV.11

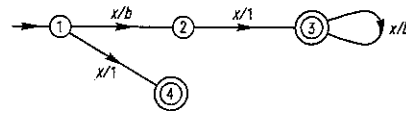


Fig. IV.12

$\alpha((x/b)) = \alpha((x/1)) = x$. Then, up to a renaming, we are in the situation of Example 3.1. Thus $B = (x/b)(x/1)(x/b)^* \cup (x/1)$ is a suitable cross-section, giving the unambiguous transducer in Fig. IV.12.

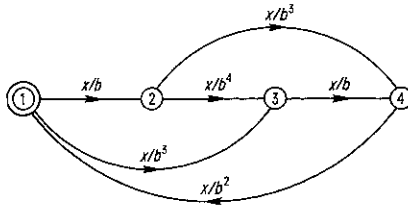


Fig. IV.13

Example 4.4 Consider the ambiguous transducer of Example 1.3 (Fig. IV.13). Take again the alphabet $Z = \{(x/b), (x/b^2), (x/b^3), (x/b^4)\}$ and the morphism α mapping all letters onto x . Then, after a renaming, we are in the situation of Example 3.2. Thus the language

$$B = [(x/b)(x/b^3)(x/b^2)]^* (1 \cup (x/b)(x/b^4)(x/b)(x/b^2) \cup [(x/b)(x/b^4)(x/b)(x/b^2)]^2)$$

is a suitable cross-section. This gives the unambiguous transducer in Fig. IV.14. The simpler transducer in Fig. IV.15 cannot be obtained in that way.

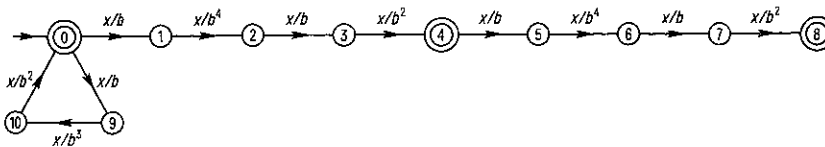


Fig. IV.14

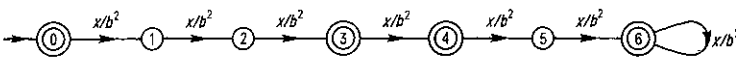


Fig. IV.15

Let $T = \langle X, Y, Q, q_-, Q_+, E \rangle$ be a transducer satisfying (4.1) and (4.2). Define a matrix representation $M = \langle \mu, Q, q_-, Q_+ \rangle$ by

$$\mu x_{pq} = \begin{cases} h & \text{if } (p, x, h, q) \in E; \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 4.4 Assume T trim. Then T is unambiguous iff M satisfies the two conditions:

- (i) For $p, q \in Q$, $f, f' \in X^*$, there is at most one $r \in Q$ such that $\mu f_{pr} \neq 0$ and $\mu f'_{rq} \neq 0$.
- (ii) $\text{dom}(\mu_{q_-, q_1}) \cap \text{dom}(\mu_{q_-, q_2}) = \emptyset$ for $q_1, q_2 \in Q_+$, $q_1 \neq q_2$.

Proof. If T is unambiguous, then (ii) is clearly satisfied. Next, since T is trim, for any $p, q \in Q$, there are $h, h' \in X^*$ such that $\mu h_{q_-, p} \neq 0$, $\mu h'_{q_+, q} \neq 0$ for some $q_+ \in Q_+$. Thus if (i) fails for some $p, q \in Q$, $f, f' \in X^*$, then $hff'h'$ 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 f . Then $q_1 = q_2$ by (ii), and $e_1 = e_2$ by (i). ■

If M is normalized, then (ii) is satisfied by definition. Thus the unambiguity of T is equivalent to condition (i).

Definition A morphism μ satisfying condition (i) of Proposition 4.4 is called unambiguous.

Example 4.5 If the matrices μf , ($f \in X^*$) are row monomial, then μ is unambiguous. Similarly, if the matrices μf , ($f \in X^*$) are column monomial, then μ is unambiguous.

An unambiguous morphism $\mu: X^* \rightarrow \text{Rat}(Y^*)^{Q \times Q}$ is also called a $(0, 1)$ -morphism (Schützenberger [1976], Nivat [1968]) for the following reason. Associate to each matrix μf , ($f \in X^*$) a $Q \times Q$ -matrix $\theta \mu f$ with integral entries by

$$\theta \mu f_{pq} = \begin{cases} 1 & \text{if } \mu f_{pq} \neq 0; \\ 0 & \text{otherwise.} \end{cases}$$

Then θ is a morphism iff μ is unambiguous. Thus a 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 $\mu: X^* \rightarrow \mathfrak{P}(Y^*)^{Q \times Q}$ be a morphism. Then μ is called semimonomial if the set Q is of the form $Q = V \times P$, and if for any $x \in X$, the following hold:

(i) For any $v \in V$, there is at most one $v' \in V$ such that the submatrix

$$(\mu x)_{v \times P, v' \times P} = (\mu x_{(v,p), (v',p')})_{p,p' \in P}$$

is nonzero.

(ii) any submatrix $(\mu x)_{v \times P, v' \times P}$ is column monomial.

Thus the matrix μx , considered as $V \times V$ matrix whose entries are $P \times P$ -matrices, is a row monomial matrix, and each $P \times P$ -block is column monomial. Clearly, the product of two semimonomial matrices with 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

$$\begin{bmatrix} 0 & \begin{matrix} 0 & b & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{matrix} & 0 \\ \hline 0 & 0 & \begin{matrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{matrix} \\ \hline 0 & 0 & \begin{matrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & b \end{matrix} \end{bmatrix}$$

Any semimonomial morphism μ is unambiguous. Consider indeed two words f, f' , and assume

$$\mu f_{(v,p)(v',p')} \neq 0 \quad \text{and} \quad \mu f'_{(v',p')(v'',p'')} \neq 0.$$

Then v' is uniquely determined by v in view of condition (i), and p' is uniquely determined by p'' in view of condition (ii).

The following theorem asserts the existence of a semimonomial representation for any rational function.

Theorem 4.5 (Schützenberger [1976]) *Let $\tau: X^* \rightarrow Y^*$ be a rational function. Then there exists a matrix representation $M = \langle \mu, Q, q_-, q_+ \rangle$ realizing τ such that μ is semimonomial and*

$$\tau = \sum_{q_+ \in Q_+} \mu_{q_- q_+}.$$

(Recall that we use the symbol $\sum$ when the domains $\text{dom}(\mu_{q_- q_+})$ are disjoint.)

Proof. Let $M = \langle \mu, Q, q_-, q_+ \rangle$ be a normalized matrix representation realizing α . The proof is in two steps. First, the usual powerset algorithm for the determinization of an automaton is employed to obtain the set V . Then, “unnecessary” entries in the matrices μx , ($x \in X$) are deleted to get the row monomial part.

Let V be the family of subsets of Q defined by

$$v \in V \Leftrightarrow \text{there exists } f \in X^* \text{ such that } v = \{q \in Q \mid \mu f_{q_-, q} \neq 0\}.$$

Thus, $v \in V$ iff v is the set of states accessible in M by paths starting in q_- and with input label f . A “next state” function $V \times X \rightarrow V$ is defined by

$$v \cdot x = \{q' \in Q \mid \exists q \in v, \mu x_{q, q'} \neq 0\}.$$

This function is extended to $V \times X^*$ by setting, as usual, $v \cdot 1 = v$, $v \cdot fx = (v \cdot f) \cdot x$, ($f \in X^*$, $x \in X$). Then clearly

$$v \cdot fg = (v \cdot f) \cdot g \quad f, g \in X^*.$$

For each $v \in V$, $x \in X$, define a $Q \times Q$ -matrix $\bar{\mu}_v x$ in the following way. Set $v' = v \cdot x$, and for each $q' \in v'$, let $p(q')$ be an arbitrary element of v such that $\mu x_{p(q'), q'} \neq 0$. Then

$$(\bar{\mu}_v x)_{qq'} = 0 \quad q \in Q, \quad q' \notin v'; \quad (4.3)$$

$$(\bar{\mu}_v x)_{qq'} = \begin{cases} \mu x_{p(q'), q'} & \text{if } q = p(q'); \\ 0 & \text{if } q \neq p(q'). \end{cases} \quad q' \in v'. \quad (4.4)$$

By definition, $\bar{\mu}_v x$ is column monomial. It is obtained from μx 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

$$\lambda: X^* \rightarrow \text{Rat}(Y^*)^{S \times S}$$

by blocks for $v, v' \in V, x \in X$:

$$(\lambda x)_{v \times Q, v' \times Q} = \begin{cases} 0 & \text{if } v' \neq v \cdot x; \\ \bar{\mu}_v x & \text{if } v' = v \cdot x. \end{cases}$$

Then the matrices λx are semimonomial. Further, if $f = x_1 x_2 \cdots x_r$, ($r \geq 1$, $x_i \in X$), then clearly

$$(\lambda f)_{v \times Q, v' \times Q} = \begin{cases} 0 & \text{if } v' \neq v \cdot f; \\ \bar{\mu}_v x_1 \bar{\mu}_{v_2} x_2 \cdots \bar{\mu}_{v_r} x_r & \text{if } v' = v \cdot f, \end{cases} \quad (4.5)$$

where $v_2 = v \cdot x_1, \dots, v_r = v_{r-1} \cdot x_{r-1}$ and $v' = v_r \cdot x_r$.

Next, we prove that for $v_- = \{q_-\}$, $f \in X^+$, $v = v_- \cdot f$,

$$\lambda f_{(v_-, q_-), (v, q)} = \mu f_{q_-, q} \quad q \in Q, \quad (4.6)$$

For $|f|=1$, (4.6) results from (4.4). Arguing by induction, let $f=gx$ with $g \in X^+$, $x \in X$, and let $v'=v_- \cdot g$. Then $v=v' \cdot x$ and

$$(\lambda gx)_{(v_-, q_-), (v, q)} = \bigcup_{r \in v'} \mu g_{q_-, r} (\lambda x)_{(v', r), (v, q)},$$

since $(\lambda g)_{(v_-, q_-), (v', r)} = \mu g_{q_-, r} = 0$ for $r \notin v'$. Next if $q \notin v$, then $(\bar{\mu}_v x)_{rq} = \mu x_{rq} = 0$ for $r \in v'$ and $\mu f_{q_-, q} = 0$. Thus (4.6) holds if $q \notin v$. If $q \in v$, then there is a unique $p \in v'$ such that $(\bar{\mu}_v x)_{pq} = \mu x_{pq} \neq 0$. Thus

$$(\lambda f)_{(v_-, q_-), (v, q)} = \mu g_{q_-, p} \mu x_{pq} = \mu f_{q_-, q}.$$

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 $f \in X^+$:

$$(\lambda f)_{(v_-, q_-), S_+} = \bigcup_{v \in V_+} \lambda f_{(v_-, q_-), (v, q_+)} = \mu f_{q_-, q_+}. \quad (4.7)$$

Indeed, (4.7) holds if $v_- \cdot f \in V_+$ (by (4.6)). If $v_- \cdot f \notin V_+$, i.e. if $q_+ \notin v_- \cdot f$, then $\mu f_{q_-, q_+} = 0$ and $(\lambda f)_{(v_-, q_-), S_+} = 0$ by (4.5). Since there is at most one $v \in V_+$ such that $v = v_- \cdot f$ for any $f \in X^+$, the functions $\lambda_{(v_-, q_-), (v, q_+)}$ have disjoint domains. This achieves the proof. ■

Example 4.7 Consider the rational function $\alpha: X^* \rightarrow b^*$ of Example 4.3, with matrix

$$\mu x = \begin{bmatrix} 0 & b & 1 \\ 0 & 0 & 1 \\ 0 & 0 & b \end{bmatrix}$$

We first compute $V: v_1 = v_- = \{1\}$, $v_2 = v_1 \cdot x = \{2, 3\}$, $v_3 = v_2 \cdot x = \{3\} = v_3 \cdot x$. The matrices $\bar{\mu}_i$ (we write $\bar{\mu}_i$ instead of $\bar{\mu}_{v_i}$) are:

$$\begin{aligned} \bar{\mu}_1 x &= \begin{bmatrix} 0 & \overbrace{b \dots 1}^{v_1} \\ 0 & 0 & 0 \\ 0 & \underbrace{0 \dots 0}_{v_2} \end{bmatrix} & \bar{\mu}_2 x &= \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & \overbrace{1}^{v_2} \\ 0 & 0 & \underbrace{0 \dots 0}_{v_3} \end{bmatrix} & \text{or} & \bar{\mu}_2 x &= \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & \overbrace{0}^{v_2} \\ 0 & 0 & \underbrace{b}_{v_3} \end{bmatrix} \\ \bar{\mu}_3 x &= \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \overbrace{b}^{v_3} \end{bmatrix} \end{aligned}$$

Thus, there are two possible choices for $\bar{\mu}_2$; each choice yields another matrix λx :

$$\lambda x = \begin{bmatrix} 0 & \bar{\mu}_1 x & 0 \\ 0 & 0 & \bar{\mu}_2 x \\ 0 & 0 & \bar{\mu}_3 x \end{bmatrix}$$

With the first matrix $\bar{\mu}_2 x$, the matrix λx 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 λ , the row with index $(v_-, 1)$ of λx^n is:

$$(0, 0, 0; 0, b, 1; 0, 0, 0) \quad n=1;$$

$$(0, 0, 0; 0, 0, 0; 0, 0, b^{n-1}) \quad n \geq 2.$$

Note that λ is not trim. The trim transducer associated to λ for the first choice of $\bar{\mu}_2 x$ is given in Fig. IV.16. Thus we get the same transducer as in Example 4.3.

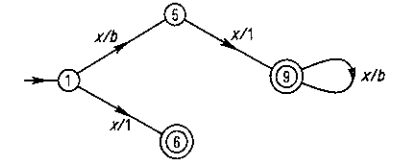


Fig. IV.16

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 $\mu: X^* \rightarrow \text{Rat}(Y^*)^{Q \times Q}$ and $\lambda: X^* \rightarrow \text{Rat}(Y^*)^{S \times S}$ be two morphisms. Then μ is summed up from λ if there exist two functions $l: Q \rightarrow S$ and $c: Q \rightarrow 2^S$ such that

$$\mu f_{pq} = \lambda f_{l(p), c(q)} \quad \left(= \bigcup_{r \in c(q)} \lambda f_{l(p), r} \right) \quad (p, q \in Q, f \in X^+).$$

Thus μ is obtained from λ by conserving just one row of λ 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 $M = \langle \mu, Q, q_-, Q_+ \rangle$ be a trim matrix representation from X^* into Y^* . If μ is unambiguous, then μ is summed up from some semimonomial morphism.

Proof. Assume μ is unambiguous. We shall verify that μ can be extracted from the semimonomial morphism λ constructed in the proof of Theorem 4.5. We keep the notations of that proof. First, we claim that for the matrix $\bar{\mu}_v x$ defined by (4.3) and (4.4), we have

$$(\bar{\mu}_v x)_{qq'} = \begin{cases} \mu x_{qq'} & \text{if } q \in v, \quad q' \in Q; \\ 0 & \text{if } q \notin v, \quad q' \in Q. \end{cases} \quad (4.8)$$

Thus $\bar{\mu}_v x$ and μx have same rows with index $q \in v$. Indeed, $(\bar{\mu}_v x)_{qq'} = 0$ for $q \notin v$ by (4.4), and $(\bar{\mu}_v x)_{qq'} = \mu x_{qq'}$ for $q \in v, q' \in Q \setminus v'$ by definition of $v' = v \cdot x$. Next, for any $q' \in v'$, there exists a unique $p \in v$ such that $\mu x_{pq'} \neq 0$, since for any f such that $v \cdot f = v'$, one has $\mu f_{q-p} \neq 0$ and $\mu x_{pq'} \neq 0$, and thus p is unique by Proposition 4.4(i). Therefore $(\bar{\mu}_v x)_{pq'} = \mu x_{pq'}$ for that p , and $(\bar{\mu}_v x)_{qq'} = \mu x_{qq'} = 0$ for all $q \in v \setminus p$. Thus (4.8) is proved.

Next, we prove that for $f \in X^+, v \in V, v' = v \cdot f$,

$$(\lambda f)_{(v,p),(v',q)} = \begin{cases} \mu f_{pq} & \text{if } p \in v, \quad q \in Q; \\ 0 & \text{if } p \notin v, \quad q \in Q. \end{cases} \quad (4.9)$$

For $|f|=1$, (4.9) holds by (4.8) in view of the definition of λ . Arguing by induction, let $f = gx$ with $g \in X^+, x \in X, v'' = v \cdot g$, thus $v' = v'' \cdot x$. Then clearly

$$(\lambda f)_{(v,p),(v',q)} = 0 \quad \text{if } p \notin v, \quad q \in Q.$$

Thus assume $p \in v$. Then

$$(\lambda f)_{(v,p),(v',q)} = \bigcup_{r \in Q} (\lambda g)_{(v,p),(v'',r)} (\lambda x)_{(v'',r),(v',q)},$$

and since $\lambda x_{(v'',r),(v',q)} = 0$ if $r \notin v''$, it follows from (4.8) that

$$(\lambda f)_{(v,p),(v',q)} = \bigcup_{r \in v''} \mu g_{p,r} \mu x_{r,q} = \mu f_{p,q}.$$

Note that in view of (4.5)

$$\lambda f_{(v,p),(v',q)} = 0 \quad \text{if } v' \neq v \cdot f \quad (p, q \in Q).$$

Thus it follows from (4.9) that

$$\mu f_{p,q} = \bigcup_{v \in V} \lambda f_{(v,p),(v',q)} \quad (p \in v). \quad (4.10)$$

Now define a function $l: Q \rightarrow S$ as follows. For any $p \in Q$, choose a $v \in V$ such that $p \in v$ and set $l(p) = (v, p)$. Such a v exists since μ is trim. Next, define c by

$$c(q) = \{(v', q) : v' \in V\}.$$

Then by (4.10)

$$\mu f_{p,q} = \lambda f_{l(p),c(q)}.$$

For a more exhaustive treatment of related questions, especially in connection with codes, see Boë [1976], Boë, Boyat et al. [1978] Césari [1974], Perrin and Schützenberger [1977].

Exercises

4.1 Compute the trim transducer associated to the second of the two semimonomial morphisms λ 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 $\beta: X^* \rightarrow Z^*$ is length preserving if $\beta f \neq 0$ implies $|f| = |\beta f|$. Show that any rational function $\alpha: X^* \rightarrow Y^*$ can be written in the form $\alpha = \gamma \circ \beta$, where $\beta: X^* \rightarrow Z^*$ is a length preserving rational function and $\gamma: Z^* \rightarrow Y^*$ 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 $A \cup B$ is unambiguous if $A \cap B = \emptyset$. A product AB is unambiguous if $a, a' \in A, b, b' \in B, ab = a'b'$ imply $a = a'$ and $b = b'$. A star A^* is unambiguous if A^* is a free submonoid freely generated by A .)

Show that if $\alpha: X^* \rightarrow Y^*$ is a rational function, then the graph of α is an unambiguous rational subset of $X^* \times Y^*$.

4.5 (Choffrut) Show that for any rational function $\alpha: X^* \rightarrow Y^*$, there is a rational subset C of $\text{dom}(\alpha)$ such that α maps bijectively C onto $\alpha(X^*) = \text{im}(\alpha)$. (This is an extension of the Cross-Section Theorem to rational functions.)

4.6 (Choffrut) Show that for any rational function $\alpha: X^* \rightarrow Y^*$ there exists a rational function $\beta: Y^* \rightarrow X^*$ such that $\alpha \circ \beta: \alpha(X^*) \rightarrow \alpha(X^*)$ is the identity function (Hint. Use Exercise 4.5.)

4.7 (Choffrut) Use the previous exercise to show that if $\alpha: X^* \rightarrow Y^*$ and $\beta: Y^* \rightarrow Z^*$ are partial functions, and if α and $\beta \circ \alpha$ and β are rational, then the restriction $\beta|_{\alpha(X^*)}$ is rational. Show that if $\beta \circ \alpha$ and β are rational, then α needs not to be rational.

IV.5 Bimachines

Bimachines are, in some sense, simultaneously left sequential and right sequential transducers. We show that a partial function is rational iff 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 $B = \langle Q, q_-, P, p_-, \gamma \rangle$ over X and Y 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 $Q \times X \rightarrow Q$ and $X \times P \rightarrow P$ denoted by dots, and a partial output function $\gamma: Q \times X \times P \rightarrow Y^*$.

The next state functions are extended to $Q \times X^*$ and $X^* \times P$ in the usual way by setting:

$$\begin{aligned} q \cdot 1 &= q, & 1 \cdot p &= p \\ q \cdot (fx) &= (q \cdot f) \cdot x, & (xf) \cdot p &= x \cdot (f \cdot p) \end{aligned}$$

for $q \in Q$, $p \in P$, $f \in X^*$, $x \in X$. Next the output function γ is extended to $Q \times X^* \times P$ by

$$\begin{aligned} \gamma(q, 1, p) &= 1; \\ \gamma(q, fx, p) &= \gamma(q, f, x \cdot p) \gamma(q \cdot f, x, p) \end{aligned}$$

for $f \in X^*$, $x \in X$, $q \in Q$, $p \in P$. Then it is easily verified that

$$\gamma(q, fg, p) = \gamma(q, f, g \cdot p) \gamma(q \cdot f, g, p) \quad (f, g \in X^*),$$

and if $f = x_1 x_2 \cdots x_n$, ($x_i \in X$), then

$$\begin{aligned} \gamma(q, f, p) &= \gamma(q, x_1, x_2 \cdots x_n \cdot p) \gamma(q \cdot x_1, x_2, x_3 \cdots x_n \cdot p) \\ &\quad \cdots \gamma(q \cdot x_1 \cdots x_{n-1}, x_n, p). \end{aligned}$$

The partial function $X^* \rightarrow Y^*$ realized by B is defined by

$$|B|(f) = \gamma(q_-, f, p_-).$$

If $P = \{p_-\}$, then B is, up to considerations concerning the domains, a left sequential transducer. Similarly, if $Q = \{q_-\}$, then B is a right sequential transducer.

Bimachines were introduced by Schützenberger [1961b]. See also Nivat [1968].

Example 5.1 Let $\alpha: x^* \rightarrow \{a, b\}^*$ be given by

$$\alpha(x^n) = \begin{cases} a^n & \text{if } n \text{ even;} \\ b^n & \text{if } n \text{ odd.} \end{cases}$$

Consider $P = \{p_-, p_1\}$, $Q = \{q_-, q_1\}$ and define the next state functions by $x \cdot p_- = p_1$, $x \cdot p_1 = p_-$, and $q_- \cdot x = q_1$, $q_1 \cdot x = q_-$. Further, let γ be given by the table

	p_-	p_1
q_-	b	a
q_1	a	b

Then a simple calculation shows that $\alpha(x^n) = \gamma(q_-, x^n, p_-)$ for $n \geq 0$.

Note that in the above definition, no assumption was made about the domains of the next state functions and γ . Call a bimachine state complete if both next state functions $Q \times X \rightarrow Q$ and $X \times P \rightarrow P$ are total functions.

Theorem 5.1 (Eilenberg [1974]) Let $\alpha: X^* \rightarrow Y^*$ be a partial function with $\alpha(1) = 1$. Then α is rational iff it is realized by some bimachine over X and Y .

We shall see that a rational function can always be realized by a state complete bimachine.

Proof. Let $B = \langle Q, q_-, P, p_-, \gamma \rangle$ be a bimachine over X and Y , define $S = Q \times P$, and consider the transducer T with set of states S , and set of transitions $E \subset S \times X \times Y^* \times S$ given by:

$$((q, p), x, h, (q', p')) \in E$$

iff $q \cdot x = q'$, $p = x \cdot p'$, and $h = \gamma(q, x, p') \neq 0$. Consider any path

$$((q_1, p_1), x_1, h_1, (q'_1, p'_1)) \cdots ((q_n, p_n), x_n, h_n, (q'_n, p'_n))$$

in T , with $f = x_1 x_2 \cdots x_n$, $g = h_1 h_2 \cdots h_n$. Then clearly $q_1 \cdot f = q'_n$, $p_1 = f \cdot p'_n$, and $g = \gamma(q_1, f, p'_n)$. For any $q \in Q$, $p \in P$, define the rational transduction $\tau_{q,p}: X^* \rightarrow Y^*$ by

$$\tau_{q,p}(f) = g$$

iff there is a path from (q_-, p) to (q, p_-) with input label f and output label g , and set $\tau_{q,p}(f) = 0$ otherwise. Then $\tau_{q,p}(f) = g \neq 0$ iff $g = \gamma(q_-, f, p_-)$, and

$$\alpha = \sum_{(q,p) \in S} \tau_{q,p}.$$

Thus α is a rational function.

Conversely, let α be realized by an unambiguous normalized matrix representation $M = \langle \mu, Q, q_-, \{q_-, q_+\} \rangle$. Define two families V, W of subsets of Q as follows:

$$\begin{aligned} v \in V &\Leftrightarrow \exists f \in X^*: v = \{q \in Q \mid \mu f_{q,q} \neq 0\}; \\ w \in W &\Leftrightarrow \exists f \in X^*: w = \{q \in Q \mid \mu f_{q,q_+} \neq 0\}. \end{aligned}$$

Then define functions $V \times X \rightarrow V$, $X \times W \rightarrow W$ as follows:

$$\begin{aligned} v \cdot x &= \{q' \in Q \mid \exists q \in v: \mu x_{qq'} \neq 0\} & v \in V; \\ x \cdot w &= \{q' \in Q \mid \exists q \in w: \mu x_{q,q'} \neq 0\} & w \in W. \end{aligned}$$

Extend them to words in the usual way by setting:

$$\begin{aligned} v \cdot 1 &= v, & v \cdot (fx) &= (v \cdot f) \cdot x; \\ 1 \cdot w &= w, & (xf) \cdot w &= x \cdot (f \cdot w) \end{aligned}$$

for $f \in X^*$, $x \in X$. Then clearly for $f \in X^*$

$$\begin{aligned} v \cdot f &= \{q' \in Q \mid \exists q \in v: \mu f_{qq'} \neq 0\} & v \in V; \\ f \cdot w &= \{q' \in Q \mid \exists q \in w: \mu f_{q,q'} \neq 0\} & w \in W. \end{aligned} \tag{5.1}$$

Next we prove

$$\text{Card}(v \cap w) \leq 1 \quad \text{for } v \in V, w \in W. \quad (5.2)$$

Assume indeed $r, r' \in v \cap w$. By definition, there exists a word f such that $\mu f_{q-r} \neq 0$, $\mu f_{q-r'} \neq 0$, and similarly there is a $g \in X^*$ such that $\mu g_{r-q} \neq 0$, $\mu g_{r'-q} \neq 0$. Then $r = r'$ by Proposition 4.4.

Define a partial function

$$\gamma: V \times X^* \times W \rightarrow Y^*$$

$$\text{by } \gamma(v, 1, w) = 1,$$

and for $f \in X^+$,

$$\gamma(v, f, w) = \begin{cases} 0 & \text{if } v \cap f \cdot w = \emptyset \text{ or } v \cdot f \cap w = \emptyset; \\ \mu f_{pq} & \text{if } v \cap f \cdot w = p \text{ and } v \cdot f \cap w = q. \end{cases} \quad (5.3)$$

We claim

$$\gamma(v, hh', w) = \gamma(v, h, h' \cdot w) \gamma(v \cdot h, h', w) \quad h, h' \in X^*. \quad (5.4)$$

Clearly, (5.4) holds if $h = 1$ or $h' = 1$. Thus we may assume $h, h' \in X^+$. Next, if $v \cap hh' \cdot w = \emptyset$ or $v \cdot hh' \cap w = \emptyset$, then both sides of (5.4) are empty. If $p = v \cap hh' \cdot w$ and $q = v \cdot hh' \cap w$, then by definition $\gamma(v, hh', w) = \mu hh'_{pq} \neq 0$. Since μ is unambiguous, there is exactly one $r \in Q$ such that

$$\mu hh'_{pq} = \mu h_{pr} \mu h'_{rq}. \quad (5.5)$$

Thus by (5.1) $r \in v \cdot h$ and $r \in h' \cdot w$. Consequently $r = v \cdot h \cap h' \cdot w$ by (5.2), and therefore $\gamma(v, h, h' \cdot w) = \mu h_{pr}$ and $\gamma(v \cdot h, h', w) = \mu h'_{rq}$. Thus (5.4) follows from (5.5).

Define $v_- = \{q_-\}$, $w_+ = \{q_+\}$. Then in view of (5.4),

$$B = \langle V, v_-, W, w_+, \gamma \rangle$$

is a bimachine over X and Y , and by construction B is state complete. Next let $f \in X^+$. Then by (5.1)

$$q_+ \in v_- \cdot f \Leftrightarrow \mu f_{q_+} \neq 0 \Leftrightarrow q_- \in f \cdot w_+ \Leftrightarrow f \in \text{dom}(\alpha).$$

Thus (5.3) implies

$$\gamma(v_-, f, w_+) = \mu f_{q_+} \quad (f \in X^+).$$

$$\text{Since } \gamma(v_-, 1, w_+) = 1,$$

it follows that $\alpha = |B|$. ■

We conclude this section by the following nice "decomposition theorem".

Theorem 5.2 (Elgot and Mezei [1965]) *Let $\alpha: X^* \rightarrow Y^*$ be a partial function with $\alpha(1) = 1$. Then α is rational iff there are a left sequential function*

$\lambda: X^* \rightarrow Z^*$, and a right sequential function $\rho: Z^* \rightarrow Y^*$ such that $\alpha = \rho \circ \lambda$. Moreover, λ can be chosen to be total and length preserving (i.e. $|\lambda(f)| = |f|$ for all $f \in X^*$).

Thus in order to compute $\alpha(f)$ for some $f \in X^*$, one first reads f sequentially from left to right and transforms it into a word g by some left sequential transducer; then the resulting word g is read from right to left and transformed into $\alpha(f)$ by a right sequential transducer.

Proof. If $\alpha = \rho \circ \lambda$, then α is a partial function and α is rational since the composition of two rational transductions is a rational transduction.

Conversely, consider a bimachine $B = \langle Q, q_-, P, p_-, \gamma \rangle$ over X and Y realizing α . We may assume that B is state complete, i.e. the next state functions $Q \times X \rightarrow Q$ and $X \times P \rightarrow P$ are total. Set $Z = Q \times X$, and define a left sequential transducer

$$L = \langle X, Z, Q, q_- \rangle$$

as follows. The next state function of L is the next state function $Q \times X \rightarrow Q$ of B , and for $q \in Q, x \in X$,

$$q * x = (q, x).$$

Define $\lambda = |L|$. Then λ is length preserving.

Next define a right sequential transducer

$$R = \langle Z, Y, P, p_- \rangle$$

$$\text{by } (q, x) * p = \gamma(q, x, p)$$

$$(q, x) \cdot p = \begin{cases} 0 & \text{if } \gamma(q, x, p) = 0; \\ x \cdot p & \text{otherwise,} \end{cases}$$

where $x \cdot p$ is the next state of p in B . Thus the next state function and the output function of R have same domain. Set $\rho = |R|$.

Let $f = x_1 x_2 \cdots x_n$, ($n \geq 1, x_i \in X$). Then

$$\begin{aligned} \lambda(f) &= (q_- * x_1)(q_- \cdot x_1 * x_2) \cdots (q_- \cdot x_1 x_2 \cdots x_{n-1} * x_n) \\ &= (q_-, x_1)(q_1, x_2) \cdots (q_{n-1}, x_n), \end{aligned}$$

where $q_i = q_- \cdot x_1 x_2 \cdots x_i$ for $i = 1, \dots, n-1$.

Consequently,

$$\begin{aligned} \rho(\lambda(f)) &= \lambda(f) * p_- \\ &= ((q_-, x_1) * p_{n-1})((q_1, x_2) * p_{n-2}) \cdots ((q_{n-2}, x_{n-1}) * p_1)((q_{n-1}, x_n) * p_-) \end{aligned}$$

where $p_i = (q_{n-i}, x_{n-i+1}) \cdots (q_{n-1}, x_n) \cdot p_-$ for $i = 1, \dots, n-1$. Thus

$$\rho(\lambda(f)) = \gamma(q_-, x_1, p_{n-1}) \cdots \gamma(q_{n-1}, x_n, p_-) = \alpha(f).$$

(This computation holds also if $\alpha(f) = 0$ with the usual convention that $x \cdot 0 = 0$.) Thus $\alpha = \rho \circ \lambda$, and the theorem is proved. $\square$

There exists another characterization of rational functions by a property similar to bimachines. See Schützenberger [1977b].

Exercises

5.1 Prove that a partial function $\alpha: X^* \rightarrow Y^*$ is rational iff $\alpha = \lambda \circ \rho$, where $\rho: X^* \rightarrow Z^*$ is a right sequential function and $\lambda: Z^* \rightarrow Y^*$ is left sequential.

5.2 Let x, y be letters. A partial function $\alpha: x^* \rightarrow y^*$ can be viewed as a partial function $\alpha: \mathbb{N} \rightarrow \mathbb{N}$ by identifying a word with its length. Show that $\alpha: \mathbb{N} \rightarrow \mathbb{N}$ is rational iff $\alpha = \alpha_1 + \dots + \alpha_k$, where each α_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 $r'_i, s'_i \in \mathbb{N}$.

IV.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 M from X^* into Y^* , it is decidable whether $|M|$ is subsequential, and whether $|M|$ is sequential.*

According to Proposition III.7.4 (and Exercise III.8.3), M can be supposed to be trim. In view of Theorem 1.2, it is decidable whether $|M|$ is a rational function. Further, the results of Section 4 show that then an unambiguous representation realizing $|M|$ can effectively be constructed. Thus we may assume that the representation M in Theorem 6.1 is unambiguous and normalized.

We use the notations and definitions of Section 2. We consider Y^* as a submonoid of the free group $Y^{(*)}$, according to the discussion of Section II.3. Let $M = \langle \mu, Q, q_-, q_+ \rangle$ be an unambiguous normalized matrix representation from X^* into Y^* , and set $\alpha = |M|$. Then in particular $Q_+ = \{q_-, q_+\}$ or $Q_+ = \{q_+\}$ according to $1 \in \text{dom}(\alpha)$ or $1 \notin \text{dom}(\alpha)$. First we define a property on M which will appear to express that α has bounded variation.

Definition Two states $q_1, q_2 \in Q$ are twinned iff for all $f, u \in X^*$ the following condition holds:

$$\left. \begin{array}{ll} 0 \neq a_1 = \mu f_{q_-, q_1}, & 0 \neq b_1 = \mu u_{q_1, q_1} \\ 0 \neq a_2 = \mu f_{q_-, q_2}, & 0 \neq b_2 = \mu u_{q_2, q_2} \end{array} \right\} \Rightarrow a_1 b_1 a_1^{-1} = a_2 b_2 a_2^{-1} \quad (6.1)$$

M has the twinning property if any two states are twinned.

A pair $f, u \in X^*$ 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 $a_1, a_2, b_1, b_2 \in Y^*$. Then*

$$a_1 b_1 a_1^{-1} = a_2 b_2 a_2^{-1} \quad (6.2)$$

iff one of the following conditions is verified:

- (i) $b_1 = b_2 = 1$;
- (ii) $b_1 \neq 1 \neq b_2$, and there exists $e \in Y^*$ such that either
 - (ii.1) $a_2 = a_1 e$ and $eb_2 = b_1 e$; or
 - (ii.2) $a_1 = a_2 e$ and $eb_1 = b_2 e$.

Proof. Assume (i) holds. Then (6.2) is obvious. Next, suppose for instance (ii.1). Then $a_2 b_2 a_2^{-1} = a_1 e b_2 e^{-1} a_1^{-1} = a_1 b_1 e e^{-1} a_1^{-1} = a_1 b_1 a_1^{-1}$.

Conversely, suppose that (6.2) holds. Then $b_1 = 1$ iff $b_2 = 1$. Thus assume $b_1 \neq 1, b_2 \neq 1$, and let a be the longest left factor common to a_1 and a_2 . Set $a_1 = ac_1, a_2 = ac_2$. Then (6.2) becomes: $c_1 b_1 c_1^{-1} = c_2 b_2 c_2^{-1}$. If $c_1 = 1$, then (ii.1) holds with $e = c_2$; if $c_2 = 1$, then (ii.2) holds with $e = c_1$. If both $c_1, c_2 \neq 1$, then they differ by their initial letter by definition of a . Thus the equation $c_1 b_1 c_1^{-1} = c_2 b_2 c_2^{-1}$ implies $b_1 = b_2 = 1$, contrary to the assumption. $\square$

Example 6.1 Consider the following unambiguous normalized transducer (Fig. IV.17). The function $\alpha: x^* \rightarrow \{y, z, t\}^*$ realized by this transducer is given by

$$\alpha(1) = 1; \quad \alpha(x^{2n}) = t(zy)^n, \quad n \geq 1; \quad \alpha(x^{2n+1}) = t(zy)^{n+1}, \quad n \geq 0.$$

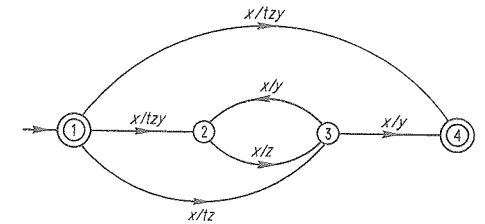


Fig. IV.17

In order to verify that the matrix representation M associated to the transducer has the twinning property, it suffices to show that the states 2 and 3 are twinned. For this, let $f = x^{2n+1}, u = x^{2m}$ be an admissible pair for 2, 3. Then $a_1 = \mu f_{1,2} = t(zy)^n, b_1 = \mu u_{2,2} = (zy)^m$, and $a_2 = \mu f_{1,3} = tz(yz)^n = t(zy)^n z = a_1 e$ with $e = z$, and $b_2 = \mu u_{3,3} = (yz)^m$, whence $eb_2 = b_1 e$. Thus $a_1 b_1 a_1^{-1} = a_2 b_2 a_2^{-1}$ by Proposition 6.2, and 2, 3 are twinned.

We note the following corollary.

Corollary 6.3 *Let $a_1, a_2, b_1, b_2 \in Y^*$. If $a_1 b_1^k a_1^{-1} = a_2 b_2^k a_2^{-1}$ for some $k > 0$, then $a_1 b_1 a_1^{-1} = a_2 b_2 a_2^{-1}$.*

Proof. We may assume $b_1, b_2 \neq 1$ and for instance $|a_2| \geq |a_1|$. Then there exists, in view of Proposition 6.2, a word $e \in Y^*$ such that $a_2 = a_1 e$, and $eb_2^k = b_1^k e$. We prove that this implies $eb_2 = b_1 e$ by induction on $|e|$, the case $|e| = 0$ being immediate. If $|e| \leq |b_1|$, then $b_1 = ef$ for some word f , hence $eb_2^k = (ef)^k e = e(fe)^k$. Therefore $b_2 = fe$ and $eb_2 = efe = b_1 e$. If $|e| > |b_1|$, then $e = b_1 e'$ for some e' . Next $eb_2^k = b_1 e' b_2^k = b_1^k b_1 e'$, thus $e' b_2^k = b_1^k e'$ and $e' b_2 = b_1 e'$ by induction. Thus $eb_2 = b_1 e$. ■

We note also that if $a_1 b_1 a_1^{-1} = a_2 b_2 a_2^{-1}$, then for all c_1, c_2

$$\|a_1 b_1 c_1, a_2 b_2 c_2\| \leq \|a_1 c_1, a_2 c_2\|. \quad (6.3)$$

Indeed, (6.3) is obvious if $b_1 = b_2 = 1$. Otherwise, we may assume by Proposition 6.2 that for instance $a_2 = a_1 e$, and $eb_2 = b_1 e$ for some word e . Then $a_2 b_2 = a_1 b_1 e$, and consequently $|a_1 b_1 c_1 \wedge a_2 b_2 c_2| \geq |a_1 b_1|$. This proves (6.3).

Proposition 6.4 *The two following conditions are equivalent:*

- (i) $\mathcal{M}$ has the twinning property;
- (ii) α 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

$$K = \max\{\|\alpha(f_1), \alpha(f_2)\| : f_1, f_2 \in \text{dom}(\alpha), \|f_1, f_2\| \leq k, |f_1 \wedge f_2| \leq n^2\}.$$

Note that $\|f_1, f_2\| \leq k$ and $|f_1 \wedge f_2| \leq n^2$ imply $|f_1| + |f_2| \leq k + 2n^2$. Thus K is finite. We prove that $\|f_1, f_2\| \leq k$ and $f_1, f_2 \in \text{dom}(\alpha)$ imply: $\|\alpha(f_1), \alpha(f_2)\| \leq K$. This holds by definition if $|f_1 \wedge f_2| \leq n^2$. Arguing by induction on $|f_1 \wedge f_2|$, we assume $|f_1 \wedge f_2| > n^2$. Then there exist words g, h_1, h_2 with $g = f_1 \wedge f_2$, $f_i = gh_i$, $i = 1, 2$, $|g| > n^2$. Consider the successful paths in $\mathcal{M}$ with input labels f_1 and f_2 . Since $|g| > n^2$, there exist a factorization $g = wuv$, $|u| > 0$, and two states q_1, q_2 , such that $\alpha(f_i) = a_i b_i c_i$, where $a_i = \mu w_{q_i q_i}$, $b_i = \mu u_{q_i q_i}$, $c_i = \mu(vh_i)_{q_i q_i}$, ($i = 1, 2$).

Since q_1 and q_2 are twinned, we have by (6.3),

$$\|\alpha(f_1), \alpha(f_2)\| \leq \|a_1 c_1, a_2 c_2\| = \|\alpha(f'_1), \alpha(f'_2)\|$$

where $f'_1 = wvh_1$, $f'_2 = wvh_2 \in \text{dom}(\alpha)$. Further $f'_1 \wedge f'_2 = wv$ is strictly shorter than g . Consequently $\|\alpha(f_1), \alpha(f_2)\| \leq K$ and α has bounded variation.

Conversely, let q_1, q_2 be two states in $\mathcal{M}$, and consider a pair f, u of words which is admissible for q_1, q_2 , i.e. satisfying the hypotheses of (6.1). Since $\mathcal{M}$ is trim, there are words $h_1, h_2 \in X^*$ such that $c_i = (\mu h_i)_{q_i q_i} \neq 0$ for $i = 1, 2$. Consequently $fu^m h_i \in \text{dom}(\alpha)$ for $m \geq 0$, $i = 1, 2$. Next $\|fu^m h_1, fu^m h_2\| = \|h_1, h_2\|$,

and since α has bounded variation, there is an integer K such that

$$\|a_1 b_1^m c_1, a_2 b_2^m c_2\| \leq K \quad m \geq 0.$$

Consequently, there exist words d_1, d_2 , with $|d_1| + |d_2| \leq K$, such that d_i is a right factor of $a_i b_i^m c_i$, ($i = 1, 2$) for an infinity of exponents m . In particular, there are integers $p \geq 0$, $k > 0$ such that:

$$a_1 b_1^p c_1 d_1^{-1} = a_2 b_2^p c_2 d_2^{-1}; \quad (6.4)$$

$$a_1 b_1^{k+p} c_1 d_1^{-1} = a_2 b_2^{k+p} c_2 d_2^{-1}. \quad (6.5)$$

(6.5) can be written as:

$$a_1 b_1^k a_1^{-1} a_1 b_1^p c_1 d_1^{-1} = a_2 b_2^k a_2^{-1} a_2 b_2^p c_2 d_2^{-1}.$$

In view of (6.4), this implies:

$$a_1 b_1^k a_1^{-1} = a_2 b_2^k a_2^{-1},$$

and by Corollary 6.3, $a_1 b_1 a_1^{-1} = a_2 b_2 a_2^{-1}$. Thus q_1 and q_2 twinned. This completes the proof. ■

The following proposition yields the main argument for the proof of Theorem 6.1.

Proposition 6.5 *Let $n = \text{Card}(Q)$. Then $\mathcal{M}$ has the twinning property iff for all $q_1, q_2 \in Q$, (6.1) holds for all pairs $f, u \in X^*$ with $|fu| \leq 2n^2$.*

Proof. We argue by induction on $|fu|$, i.e. we assume that (6.1) holds for all $q_1, q_2 \in Q$ and for all pairs f', u' of words admissible for q_1, q_2 such that $|f'u'| < |fu|$. Consider $q_1, q_2 \in Q$, and consider a pair f, u of words such that the hypotheses of (6.1) hold. Clearly we may assume $|fu| \geq 2n^2$ and $|u| > 0$. Next either $|f| > n^2$ or $|u| > n^2$. If $|f| \geq n^2 + 1$ then there exist a factorization $f = f_1 v f_2$, with $v \neq 1$, and $r_1, r_2 \in Q$, $c_1, d_1, e_1, c_2, d_2, e_2 \in Y^*$ such that $a_1 = c_1 d_1 e_1$, $a_2 = c_2 d_2 e_2$ and

$$c_1 = \mu(f_1)_{q_1 r_1}, \quad d_1 = \mu v_{r_1 r_1}, \quad e_1 = \mu(f_2)_{r_1 q_1},$$

$$c_2 = \mu(f_1)_{q_2 r_2}, \quad d_2 = \mu v_{r_2 r_2}, \quad e_2 = \mu(f_2)_{r_2 q_2}.$$

Thus f_1, v is an admissible pair for r_1, r_2 and $f_1 f_2, u$ is an admissible pair for q_1, q_2 . Consequently by induction

$$c_1 d_1 c_1^{-1} = c_2 d_2 c_2^{-1} \quad \text{and} \quad c_1 e_1 b_1 e_1^{-1} c_1^{-1} = c_2 e_2 b_2 e_2^{-1} c_2^{-1}.$$

$$\begin{aligned} \text{Hence } a_1 b_1 a_1^{-1} &= (c_1 d_1 c_1^{-1})(c_1 e_1 b_1 e_1^{-1} c_1^{-1})(c_1 d_1^{-1} c_1^{-1}) \\ &= c_2 d_2 e_2 b_2 e_2^{-1} d_2^{-1} c_2^{-1} = a_2 b_2 a_2^{-1}. \end{aligned}$$

Next, assume $|u| \geq n^2 + 1$. Then similarly, there exist a factorization $u = u_1 v u_2$, with $v \neq 1$, and $r_1, r_2 \in Q$, $c_1, d_1, e_1, c_2, d_2, e_2 \in Y^*$ such that $b_1 = c_1 d_1 e_1$,

$b_2 = c_2 d_2 e_2$, and

$$\begin{aligned} c_1 &= \mu(u_1)_{q_1 r_1}, & d_1 &= \mu v_{r_1 r_1}, & e_1 &= \mu(u_2)_{r_1 q_1}, \\ c_2 &= \mu(u_1)_{q_2 r_2}, & d_2 &= \mu v_{r_2 r_2}, & e_2 &= \mu(u_2)_{r_2 q_2}. \end{aligned}$$

If $u_2 = 1$, then $r_1 = q_1$, $r_2 = q_2$, $e_1 = e_2 = 1$. Thus (f, u_1) and (f, v) are admissible pairs for q_1 , q_2 , and by induction

$$a_1 c_1 a_1^{-1} = a_2 c_2 a_2^{-1} \quad \text{and} \quad a_1 d_1 a_1^{-1} = a_2 d_2 a_2^{-1}.$$

$$\begin{aligned} \text{Then } a_1 b_1 a_1^{-1} &= a_1 c_1 d_1 a_1^{-1} = (a_1 c_1 a_1^{-1})(a_1 d_1 a_1^{-1}) = (a_2 c_2 a_2^{-1})(a_2 d_2 a_2^{-1}) \\ &= a_2 b_2 a_2^{-1}. \end{aligned}$$

Finally if $u_2 \neq 1$, then $f, u_1 u_2$ is an admissible pair for q_1 , q_2 , and $f u_1, v$ is an admissible pair for r_1 , r_2 . By induction

$$a_1 c_1 e_1 a_1^{-1} = a_2 c_2 e_2 a_2^{-1} \quad \text{and} \quad a_1 c_1 d_1 c_1^{-1} a_1^{-1} = a_2 c_2 d_2 c_2^{-1} a_2^{-1}.$$

It follows that

$$\begin{aligned} a_1 b_1 a_1^{-1} &= a_1 c_1 d_1 e_1 a_1^{-1} = (a_1 c_1 d_1 c_1^{-1} a_1^{-1})(a_1 e_1 a_1^{-1}) \\ &= (a_2 c_2 d_2 c_2^{-1} a_2^{-1})(a_2 e_2 a_2^{-1}) = a_2 c_2 d_2 e_2 a_2^{-1} = a_2 b_2 a_2^{-1}. \end{aligned}$$

Proposition 6.6 *If M has n states and has the twinning property, then α preserves left factors iff $\alpha(1) = 1$ and for any $f \in X^*$ with $|f| \leq n^2$, and for any $x \in X$, $\alpha(fx) \neq 0$ implies $\alpha(fx) \in \alpha(f)Y^*$.*

Proof. The conditions are obviously necessary. Conversely, let $f \in X^*$, $x \in X$ such that $fx \in \text{dom}(\alpha)$. Arguing by induction, we may assume that $|f| > n^2$. There exists a factorization $f = f_1 v f_2$ with $v \neq 1$, and $q_1, q_2 \in Q$, $a_1, b_1, c_1, a_2, b_2, c_2 \in Y^*$ such that

$$\begin{aligned} \alpha(f) &= a_1 b_1 c_1, & \alpha(fx) &= a_2 b_2 c_2, \\ a_1 &= (\mu f_1)_{q_1 q_1}, & b_1 &= \mu v_{q_1 q_1}, & c_1 &= \mu(f_2)_{q_1 q_2}, \\ a_2 &= (\mu f_1)_{q_2 q_2}, & b_2 &= \mu v_{q_2 q_2}, & c_2 &= \mu(f_2 x)_{q_2 q_2}. \end{aligned}$$

It follows that $\alpha(f_1 f_2) = a_1 c_1$, $\alpha(f_1 f_2 x) = a_2 c_2$. Since M has the twinning property, and since f_1, v is an admissible pair for q_1, q_2 ,

$$a_1 b_1 a_1^{-1} = a_2 b_2 a_2^{-1}. \quad (6.6)$$

Next since $|f_1 f_2| < |f|$, there is a word $u \in Y^*$ such that

$$a_2 c_2 = \alpha(f_1 f_2 x) = \alpha(f_1 f_2)u = a_1 c_1 u. \quad (6.7)$$

Combining (6.6) and (6.7), we obtain

$$\alpha(fx) = a_2 b_2 c_2 = a_2 b_2 a_2^{-1} a_2 c_2 = a_1 b_1 a_1^{-1} a_1 c_1 u = a_1 b_1 c_1 u = \alpha(f)u. \quad \blacksquare$$

Proof of Theorem 6.1 Since α is realized by M , α is rational. Consequently $\alpha^{-1}: Y^* \rightarrow X^*$ is a rational transduction and by Corollary III.4.2, α^{-1} preserves rational languages. Thus in view of Theorem 2.7, α is subsequential iff α has bounded variation, and by Proposition 6.4 this holds iff M has the twinning property which is decidable by Proposition 6.5. Thus it is decidable whether α is subsequential. Further α is sequential iff M has the twinning property and α preserves left factors. By Proposition 6.6, this is decidable. Thus the proof is complete. $\blacksquare$

V Families of Languages

This chapter introduces basic notions on families of languages. Rational cones are defined in Section 2, and closure properties of cones are derived from the examples of Chapter III. The second important type of families of languages considered in this book, namely full AFLs, is defined in Section 4. The next section contains basic facts about substitutions in relation with cones and full AFLs. In Section 6, we study the family of linear languages which is shown to be a principal cone, but not a full AFL. In the last section, we prove the incomparability of some special languages.

V.1 Definition

A family of languages should contain all languages having the same, or similar “structure”. This structure does not depend of the alphabet chosen to represent the language. More precisely, if X is an alphabet and $A \subset X^*$, and if A' is a copy of A on an alphabet X' , then A and A' have the same structure. We thus require a family of languages to contain “all” copies of its elements, with the necessary set-theoretic precautions to avoid any paradox. We therefore introduce a fixed infinite alphabet Σ , and restrict alphabets, languages and the above requirements to subsets of Σ and Σ^* .

Let Σ be a fixed, infinite alphabet. In the sequel, an alphabet is a finite, non-empty subset X of Σ . A formal language L is a set $L \subset X^*$, where X is an alphabet. For any language L , we denote by X_L the least alphabet such that $L \subset X_L^*$. If $L = \emptyset$ or $L = \{1\}$, then X_L is an arbitrary alphabet. Whenever, in the sequel, new letters are used or constructed, they will be assumed to be in Σ .

Definition A family of languages $\mathcal{L}$ is a nonempty set of languages, distinct from $\{\emptyset\}$, and satisfying the following property:

if $L \in \mathcal{L}$, and if L' is a copy of L , then $L' \in \mathcal{L}$.

Recall (see Section I.4) that L' is a copy of L if $L' = \alpha(L)$, where α is an isomorphism from X_L^* onto $X_{L'}^*$.

Example 1.1 We introduce some fundamental families of languages. Rat is the family of all regular or rational languages; Alg is the family of context-free or algebraic languages; Lin is the family of linear languages (see Section 6). There are several simple families of languages which will be used to represent some

closure properties by means of substitution. The family Elm consists of all finite subsets of Σ , that is of all alphabets and of the empty set. The family Fin is the family of all finite languages (including $\emptyset$ and $\{1\}$).

Example 1.2 The set of all languages is a family of languages. We denote it by $\hat{\Sigma}$.

Let $\mathcal{L}$ be a family of languages. Then $\mathcal{L}$ is finite if there exist finitely many languages $L_1, \dots, L_n$ such that any language L of $\mathcal{L}$ is a copy of one of the languages $L_1, \dots, L_n$. In this case, we write $\mathcal{L} = \{L_1, \dots, L_n\}$. If all languages of $\mathcal{L}$ are copies of a single language L , that is $\mathcal{L} = \{L\}$, then $\mathcal{L}$ is said to have just one element.

The union of an arbitrary number of families of languages is a family of languages; the same is true for intersection, provided the intersection is nonempty and distinct from $\{\emptyset\}$. Families of languages are ordered by inclusion. Two families $\mathcal{L}$ and $\mathcal{M}$ are incomparable if neither $\mathcal{L} \subset \mathcal{M}$ nor $\mathcal{M} \subset \mathcal{L}$.

Exercise

1.1 Describe the minimal families of languages with respect to the inclusion order.

V.2 Rational Equivalence, Rational Cones

Rational domination and rational equivalence are the basic tools for comparison of formal languages. These relations are transformed into inclusion and equality of families of languages of a special type, called rational cones. Two languages are rationally equivalent if each one can be transformed into the other by a rational transduction. Since these transformations involve only finite memory, the “essential” features of two rationally equivalent languages are the same in a sense which will be precised in Chapter VIII. Rational cones are families of languages closed under morphism, inverse morphism and intersection with regular sets. Further closure properties follow from the properties of rational transductions.

Definition Let L and L' be languages. Then L' is a rational image of L , or L dominates rationally L' iff there exists a rational transduction $\tau: X_L^* \rightarrow X_{L'}^*$ such that $L' = \tau(L)$. We then write $L \geq L'$ or $L' \leq L$.

The composition of two rational transductions is still a rational transduction; thus $\geq$ is a preorder. If $L \geq L'$ and $L' \geq L$, then L and L' are rationally equivalent. We denote this fact by $L \approx L'$, and the contrary by $L \not\approx L'$. We write $L > L'$ when $L \geq L'$ and $L \not\approx L'$ and say that L strictly dominates L' , and we write $L \not\geq L'$ for: not $(L \geq L')$. Finally, L and L' are (rationally) incomparable, if neither $L \geq L'$ nor $L' \geq L$.

Example 2.1 The languages $S_{\leq} = \{a^n b^n \mid n \geq 0\}$ and $A = \{(x^+ y)^n z^n \mid n \geq 0\}$ are rationally equivalent: $S_{\leq} \approx A$. Indeed, A is obtained from $S_{\leq}$ by the rational substitution which maps a into $x^+ y$ and b into z . The converse transformation is performed by the following transducer with initial and final state 1 (Fig. V.1).

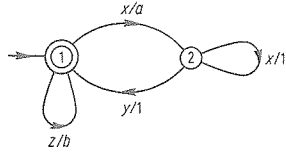


Fig. V.1

Example 2.2 Let $S_{\leq} = \{a^n b^m \mid 0 \leq n \leq m\}$. Then $S_{\leq} > S_{\leq}$. Indeed, $S_{\leq}$ is the image of $S_{\leq}$ under the substitution which substitutes a to a and b^+ to b . The nonequivalence of the two languages will be shown in Section 7.

Example 2.3 Let $S_{\geq} = \{a^n b^m \mid n \geq m \geq 0\}$. The languages $S_{\geq}$ and $S_{\leq}$ are rationally incomparable. This will be proved in Section 7, too.

Definition A family of languages $\mathcal{L}$ is a rational cone, or shorter a cone, if it satisfies the following condition:

$$L \in \mathcal{L}, L \geq L' \text{ imply } L' \in \mathcal{L}.$$

Thus, a rational cone is a family of languages closed under rational transduction. A rational cone is called a “full trio” by Ginsburg [1975], since it is closed under three operations: morphism, inverse morphism, and intersection with regular sets. Conversely, a family of languages closed under these three operations is, by Nivat’s theorem, also closed under rational transduction. Note that in order to prove that a given family of languages is a cone, it suffices to show that it is closed under projection, inverse projection, and intersection with rational languages. This frequently simplifies the verification.

Example 2.4 The families $\hat{\Sigma}$, Rat, Alg, Lin are cones; neither Elm nor Fin is a cone.

The cone Rat is the least cone, since the following property holds

Proposition 2.1 Any rational cone contains Rat.

Proof. Let $\mathcal{L}$ be a cone, and $L \in \mathcal{L}$, $L \neq \emptyset$. Let $K \in \text{Rat}$. The transduction $\tau_K: X_L^* \rightarrow X_K^*$ defined for $w \in X_L^*$ by $\tau_K(w) = K$ is rational (see Example III.5.2). Since $\tau_K(L) = K$ and $\mathcal{L}$ is a cone, it follows that $K \in \mathcal{L}$. ■

By this proposition, the intersection of a family of rational cones is nonempty; it is easily seen to be again a rational cone.

Definition Let $\mathcal{L}$ be a family of languages. The cone generated by $\mathcal{L}$ is the intersection of all cones containing $\mathcal{L}$, that is the least cone containing $\mathcal{L}$. It is denoted by $\mathcal{L}\Gamma$. If $\mathcal{L} = \{L\}$, we write $L\Gamma$ instead of $\{L\}\Gamma$.

Proposition 2.2 Let $\mathcal{L}$ be a family of languages; then

$$\mathcal{L}\Gamma = \{L' \mid L' \leq L \text{ for some } L \in \mathcal{L}\}.$$

Proof. Set $\mathcal{M} = \{L' \mid L' \leq L \text{ for some } L \in \mathcal{L}\}$. Then $\mathcal{M} \subset \mathcal{L}\Gamma$ since $\mathcal{L}\Gamma$ is a cone. In order to show the converse inclusion, it suffices to show that $\mathcal{M}$ is a cone, since $\mathcal{L} \subset \mathcal{M}$. Let $M \in \mathcal{M}$, and M' such that $M \geq M'$. There exists $L \in \mathcal{L}$ such that $L \geq M$, and since $\geq$ is transitive, this implies $L \geq M'$ and thus $M' \in \mathcal{M}$. Thus $\mathcal{M}$ is a cone. ■

Proposition 2.3 Let $\mathcal{L}$ and $\mathcal{L}'$ be two families of languages; then

$$\mathcal{L} \subset \mathcal{L}\Gamma; \quad \mathcal{L} \subset \mathcal{L}' \Rightarrow \mathcal{L}\Gamma \subset \mathcal{L}'\Gamma; \quad \mathcal{L}\Gamma\Gamma = \mathcal{L}\Gamma.$$

We now summarize some closure properties of rational cones.

Proposition 2.4 Let $\mathcal{L}$ be a cone; if $L \in \mathcal{L}$ and $K \in \text{Rat}$, then

$$LK, KL, LK^{-1}, K^{-1}L, L \cup K, L \setminus K \in \mathcal{L}.$$

Proof. Let X be an alphabet such that $L, K \subset X^*$. The transduction $w \mapsto wK$ from X^* into X^* is rational by Example III.5.6; thus $L \geq LK$ and $LK \in \mathcal{L}$. Similarly, $KL \in \mathcal{L}$. The transductions $w \mapsto K^{-1}w$ and $w \mapsto w \cup K$ are also rational (Examples III.5.7 and 5). Finally $L \setminus K = L \cap (X^* \setminus K) \in \mathcal{L}$. ■

We single out a special case of proposition 2.4 which will be of constant use in the sequel.

Corollary 2.5 Let $\mathcal{L}$ be a cone, let L be a language and $\#$ a letter not in X_L ; then

$$L \in \mathcal{L} \Leftrightarrow \#L \in \mathcal{L} \Leftrightarrow L\# \in \mathcal{L}.$$

Definition A rational cone $\mathcal{L}$ is principal if there exists a language $L_0 \in \mathcal{L}$ such that any language of $\mathcal{L}$ is a rational image of L_0 , that is if $\mathcal{L} = L_0\Gamma$. The language L_0 is a cone generator of $\mathcal{L}$.

Two generators of a cone $\mathcal{L}$ are rationally equivalent. More precisely, $L \geq L'$ holds iff $L\Gamma \supset L'\Gamma$, and the languages L and L' are incomparable iff the cones $L\Gamma$ and $L'\Gamma$ are incomparable families of languages.

In general, a cone is not closed under union (Exercise 2.3). For principal cones we have

Proposition 2.6 A principal cone is closed under union.

Proof. Let L_0 be a generator of a principal cone $\mathcal{L}$, and let $L, M \in \mathcal{L}$. Let X be an alphabet such that $L, M \subset X^*$, and set $Y = X_{L_0}$. There exist two rational transductions $\tau, \tau': Y^* \rightarrow X^*$ such that $\tau(L_0) = L$, $\tau'(L_0) = M$. Then the transduction $\tau'' = \tau \cup \tau'$ is also rational, and $\tau''(L_0) = L \cup M$; thus $L \cup M \in L_0\Gamma = \mathcal{L}$. ■

Exercises

2.1 Show that Rat is a principal cone and that any nonempty rational language is a generator of the cone Rat.

2.2 Show that the union of a family of cones is a cone.

2.3 Let $\mathcal{L}$ and $\mathcal{M}$ be two cones, and define

$$\mathcal{L} \vee \mathcal{M} = \{L \cup M \mid L \in \mathcal{L}, M \in \mathcal{M}\}.$$

a) Show that $\mathcal{L} \vee \mathcal{M}$ is a cone, and that $\mathcal{L} \cup \mathcal{M} \subset \mathcal{L} \vee \mathcal{M}$.

b) Show that $\mathcal{L} \cup \mathcal{M} \not\subset \mathcal{L} \vee \mathcal{M}$ if $\mathcal{L}$ and $\mathcal{M}$ are incomparable (Hint. Show that there are languages $L \in \mathcal{L} \setminus \mathcal{M}$ and $M \in \mathcal{M} \setminus \mathcal{L}$ such that $M \subset X_M^+$, $L \subset X_L^+$, $X_M \cap X_L = \emptyset$, and take the language $A = L \cup M$.) Conclude that if $\mathcal{L}$ and $\mathcal{M}$ are incomparable, then $\mathcal{L} \cup \mathcal{M}$ is not closed under union.

c) Assume that $\mathcal{L}$ and $\mathcal{M}$ are principal cones; show that $\mathcal{L} \cup \mathcal{M}$ is principal iff $\mathcal{L}$ and $\mathcal{M}$ are comparable.

2.4 Let $X = \{a, b\}$, and $\Theta = \{=, \neq, \geq, \leq, >, <\}$. The language of Goldstine (from Goldstine [1972]) G_θ is defined, for $\theta \in \Theta$ by:

$$G_\theta = \{a^{n_1} b a^{n_2} b \cdots a^{n_p} b \mid p \geq 1, n_i \geq 0, \exists j, 1 \leq j \leq p : n_j \theta j\}.$$

Let S_+ be as in Example 2.1.

a) Show that $S_+ \geq G_\theta$ for $\theta \in \Theta$. (This shows that G_θ is context-free.)

b) Show that $S_+ \approx G_+$, $G_+ \approx G_{\leq}$, $G_{\leq} \approx G_{\geq}$.

V.3 Rationally Closed Families

The second important class of families of languages is the class of rationally closed families. Rational closure means closure under the three "rational" operations, namely union, product and the star (or the plus) operation. In connection with closure under rational transductions, this leads to the notion of full AFL defined in the next section.

Definition A family of languages $\mathcal{L}$ is rationally closed if the following conditions are satisfied:

- (i) $\emptyset \in \mathcal{L}$, $\{1\} \in \mathcal{L}$;
- (ii) $L, M \in \mathcal{L} \Rightarrow L \cup M, L \cdot M \in \mathcal{L}$;
- (iii) $L \in \mathcal{L} \Rightarrow L^+ \in \mathcal{L}$.

Conditions (i), (ii), (iii) imply that $L^* = \{1\} \cup L^+ \in \mathcal{L}$ for $L \in \mathcal{L}$; conversely, if (ii) holds, then $L, L^* \in \mathcal{L}$ imply $L^+ = LL^* \in \mathcal{L}$.

The above definition slightly differs from the definition of Eilenberg [1974] by the fact that we require the additional condition (i). This difference is not essential but simplifies alternative representations (see Proposition 3.2).

Example 3.1 The families Rat, Alg, $\hat{\Sigma}$ are rationally closed and Lin is not rationally closed (see Section 6).

The intersection of a family of rationally closed families of languages is again a rationally closed family of languages. The rational closure of a family $\mathcal{L}$ is the intersection of all rationally closed families containing $\mathcal{L}$, and thus the least rationally closed family of languages containing $\mathcal{L}$. The rational closure of $\mathcal{L}$ is denoted by $\mathcal{L} \text{ Rat}$. Clearly, we have

Proposition 3.1 Let $\mathcal{L}$ and $\mathcal{L}'$ be two families of languages; then

$$\mathcal{L} \subset \mathcal{L} \text{ Rat}; \quad \mathcal{L} \subset \mathcal{L}' \Rightarrow \mathcal{L} \text{ Rat} \subset \mathcal{L}' \text{ Rat}; \quad \mathcal{L} \text{ Rat Rat} = \mathcal{L} \text{ Rat}. \quad \blacksquare$$

Let $\mathcal{L}$ be a family of languages and let $\sigma : X^* \rightarrow Y^*$ be a substitution. Then σ is a $\mathcal{L}$ -substitution if $\sigma(x) \in \mathcal{L}$ for all $x \in X$. The following result links together rational closure and $\mathcal{L}$ -substitutions.

Proposition 3.2 Let $\mathcal{L}$ be a family of languages; then

$$\mathcal{L} \text{ Rat} = \{\sigma(K) \mid K \in \text{Rat}, \sigma \text{ a } \mathcal{L}\text{-substitution}\}.$$

Proof. Set

$$\mathcal{M} = \{\sigma(K) \mid K \in \text{Rat}, \sigma \text{ a } \mathcal{L}\text{-substitution}\}.$$

We first show the inclusion $\mathcal{L} \text{ Rat} \subset \mathcal{M}$, by proving that $\mathcal{M}$ contains $\mathcal{L}$ and is rationally closed. Let $L \in \mathcal{L}$, let x be a letter, and define $\sigma : x^* \rightarrow X_L^*$ by $\sigma(x) = L$. Then σ is a $\mathcal{L}$ -substitution, and $x \in \text{Rat}$, thus $L = \sigma(x) \in \mathcal{M}$. This shows that $\mathcal{L} \subset \mathcal{M}$.

Next, consider $L, M \in \mathcal{M}$, and let Y be an alphabet such that $L, M \subset Y^*$. There exist two $\mathcal{L}$ -substitutions $\sigma_1 : X_1^* \rightarrow Y^*$ and $\sigma_2 : X_2^* \rightarrow Y^*$ such that $L = \sigma_1(K_1)$, $M = \sigma_2(K_2)$ for some $K_1, K_2 \in \text{Rat}$. After a copy if necessary, we may assume $X_1 \cap X_2 = \emptyset$. Set $X = X_1 \cup X_2$ and define a substitution $\sigma : X^* \rightarrow Y^*$ by

$$\sigma(x) = \begin{cases} \sigma_1(x_1) & \text{if } x_1 \in X_1; \\ \sigma_2(x_2) & \text{if } x_2 \in X_2. \end{cases}$$

Then σ is a $\mathcal{L}$ -substitution, and $L = \sigma(K_1)$, $M = \sigma(K_2)$. This implies

$$L \cup M = \sigma(K_1 \cup K_2), \quad LM = \sigma(K_1 K_2), \quad L^+ = \sigma(K_1^+) \in \mathcal{M}.$$

Since $\emptyset = \sigma(\emptyset)$, $\{1\} = \sigma(1) \in \mathcal{M}$, the family $\mathcal{M}$ is rationally closed. In order to prove the converse inclusion $\mathcal{M} \subset \mathcal{L} \text{ Rat}$, consider the set $\mathcal{N}$ of all languages K such that $\sigma(K) \in \mathcal{L} \text{ Rat}$ for any $\mathcal{L}$ -substitution σ . By definition $\mathcal{L} \text{ Rat} \supset \{\sigma(K) \mid K \in \mathcal{N}, \sigma \text{ a } \mathcal{L}\text{-substitution}\}$ and it suffices to show that $\text{Rat} \subset \mathcal{N}$.

Clearly $\mathcal{N}$ is closed under copy and thus $\mathcal{N}$ is a family of languages. Next $\emptyset, \{1\} \in \mathcal{N}$ and $\{x\} \in \mathcal{N}$ for all $x \in \Sigma$. Assume now $K, K' \in \mathcal{N}$. Set $X = X_K \cup X_{K'}$ and let $\sigma : X^* \rightarrow Y^*$ be an arbitrary $\mathcal{L}$ -substitution. By assumption,

$\sigma(K), \sigma(K') \in \mathcal{L} \text{ Rat}$: thus $K \cup K', K \cdot K', K^+ \in \mathcal{N}$ since $\mathcal{L} \text{ Rat}$ is rationally closed. This shows that $\mathcal{N} \supset \text{Rat}$, and proves the inclusion. ■

Proposition 3.2 is very useful for proving properties of families of languages constructed by substitutions. We give now an example of this fact.

Definition A language A has no infinite rational subset if $K \in \text{Rat}$ and $K \subset A$ imply that K is finite.

Such a language is said to satisfy the IRS-condition by Greibach [1975].

Example 3.2 The language $\{a^{k+n}b^nc^pd^{p+k} \mid k, p, n \geq 1\}$ has no infinite rational subset; on the contrary, the language $S_{<} = \{x^ny^m \mid 0 \leq n < m\}$ contains infinite rational languages, for instance y^+ .

Proposition 3.3 Let A be a language having no infinite rational subset, and let $\mathcal{L}$ be a family of languages; if $A \in \mathcal{L} \text{ Rat}$, then A is a finite union of products of languages in $\mathcal{L}$.

Proof. Since $A \in \mathcal{L} \text{ Rat}$, there exist a rational language K , and a $\mathcal{L}$ -substitution $\sigma: X_K^* \rightarrow X_A^*$ such that $A = \sigma(K)$. We always may assume that $\sigma(x) \neq 1$ for any letter $x \in X_K$. Indeed, let $X_0 = \{x \in X_K : \sigma(x) = 1\}$, set $Y = X_K \setminus X_0$, and let π be the projection of X_K^* onto Y^* ; then $A = \sigma'(\pi(K))$ where σ' is the restriction of σ to Y^* ; $\sigma'(x) \neq 1$ for $x \in Y$ and $\pi(K) \in \text{Rat}$.

We have to prove that K is finite. Assume K infinite; then by the iteration lemma, there exist words a, u, b such that $au^*b \subset K$ and $u \neq 1$. Let $f \in \sigma(a)$, $w \in \sigma(u)$, $g \in \sigma(b)$; since $\sigma(u) \neq 1$, we can choose $w \neq 1$. Then $fw^*g \subset A$, and A contains an infinite rational set, contrary to the hypothesis. ■

Exercises

3.1 Let $\mathcal{L}$ be a family of languages. Show that

$$\{\sigma(K) \mid K \in \text{Elm}, \sigma \text{ a } \mathcal{L}\text{-substitution}\}$$

is the least family of languages containing $\mathcal{L} \cup \{\emptyset\}$ and closed under union. Show that

$$\{\sigma(K) \mid K \in \text{Fin}, \sigma \text{ a } \mathcal{L}\text{-substitution}\}$$

is the least family of languages containing $\mathcal{L} \cup \{\emptyset, \{1\}\}$ and closed under union and product.

3.2 A language A is said to contain no infinite product if for any two languages L, L' such that $LL' \subset A$, either L or L' is finite.

a) Show that a language which contains no infinite product contains no infinite regular set; show that the converse is false.

b) Show that if A contains no infinite product, and if $A \in \mathcal{L} \text{ Rat}$, where $\mathcal{L}$ is a cone, then A is a finite union of languages in $\mathcal{L}$.

V.4 Full AFLs

Families of languages which are both rational cones and rationally closed are called full AFLs. In this section, we prove some general properties of full AFLs. The main “decomposition” theorem stating that any full AFL is equal to the rational closure of a rational cone will be proved in Section VI.4.

Definition A family of languages $\mathcal{L}$ is a full AFL if $\mathcal{L}$ is a cone and is rationally closed, that is:

$$\mathcal{L} = \mathcal{L} \hat{\Gamma} \quad \text{and} \quad \mathcal{L} = \mathcal{L} \text{ Rat}.$$

A family $\mathcal{L}$ is a full AFL iff it is closed under the following six operations: morphism, inverse morphism, intersection with regular sets, union, product, and star or plus operation.

The term AFL is an abbreviation of abstract family of languages. The adjective “full” is used to distinguish these families from AFL which are required to be closed only under continuous (ϵ -free) morphisms instead of arbitrary morphisms. This distinction is necessary for instance if context-sensitive languages have to be included into the general theory, and leads also to further refinements of the theory (see Ginsburg [1975]). In this book, we restrict ourselves to full AFL.

Sometimes, it is convenient to consider a notion which is intermediate between cones and full AFLs:

Definition A family of languages $\mathcal{L}$ is a full semi-AFL if it is a cone and is closed under union.

Example 4.1 The families Rat , Alg , $\hat{\Sigma}$ are full AFLs.

Example 4.2 Any principal rational cone is a full semi-AFL.

The intersection of a family of full AFLs is again a full AFL. The full AFL generated by a family of languages $\mathcal{L}$ is the intersection of all full AFLs containing $\mathcal{L}$, that is the least full AFL containing $\mathcal{L}$. It is denoted by $\mathcal{L} \hat{\Gamma}$.

Proposition 4.1 Let $\mathcal{L}$ and $\mathcal{L}'$ be two families of languages; then

$$\mathcal{L} \subset \mathcal{L} \hat{\Gamma}; \quad \mathcal{L} \subset \mathcal{L}' \Rightarrow \mathcal{L} \hat{\Gamma} \subset \mathcal{L}' \hat{\Gamma}; \quad \mathcal{L} \hat{\Gamma} \hat{\Gamma} = \mathcal{L} \hat{\Gamma}.$$

The six operations defining full AFLs are not independent.

Proposition 4.2 Let $\mathcal{L}$ be a rational cone closed under union and plus-operation; then $\mathcal{L}$ is a full AFL.

Thus a family of languages is closed under product provided it is closed under the other five of the six AFL operations. For other relations between the six axioms for full AFLs see Ginsburg [1975].

Proof. Let L_1, L_2 be languages in $\mathcal{L}$. We have to show that $L_1 L_2 \in \mathcal{L}$. Set $X = X_{L_1} \cup X_{L_2}$ and let $\#, \flat$ be two new letters. Then $L_1 \#, L_2 \flat \in \mathcal{L}$ by Corollary 2.5, and $L_1 \# \cup L_2 \flat, (L_1 \# \cup L_2 \flat)^+ \in \mathcal{L}$ by the assumptions on $\mathcal{L}$. Since $\mathcal{L}$ is a cone, it follows

$$L = (L_1 \# \cup L_2 \flat)^+ \cap X^* \# X^* \flat \in \mathcal{L}.$$

Now $L = L_1 \# L_2 \flat$. Consider the projection $\pi: (X \cup \# \cup \flat)^* \rightarrow X^*$. Then $\pi(L) = L_1 L_2 \in \mathcal{L}$. ■

Definition Let $\mathcal{L}$ be a full AFL. Then $\mathcal{L}$ is a principal full AFL if there exists a language L_0 such that $\mathcal{L} = L_0 \hat{\Gamma}$. The language L_0 is a full AFL generator of $\mathcal{L}$.

Full AFL generators and cone generators must be carefully distinguished. Consider indeed a principal full AFL $\mathcal{L}$, and let L be a full AFL generator of $\mathcal{L}$; thus $L \hat{\Gamma} = \mathcal{L}$. Since $\mathcal{L}$ is a full AFL, it is also a cone.

Consider the cone $L\Gamma$ generated by L . Then $L\Gamma \subset \mathcal{L}$, and in general the inclusion is strict. On the other hand, we shall prove that any full principal AFL $\mathcal{L}$ is also a principal cone (Proposition 4.4 below). Let L' be a cone generator of $\mathcal{L}$: $L'\Gamma = \mathcal{L}$. Then $\mathcal{L} = L'\Gamma \subset L'\hat{\Gamma} = \mathcal{L}$. Thus any cone generator of a principal full AFL is also a full AFL generator. It is quite remarkable that the converse is also true in the special case of substitution-closed full AFL, and thus for the family Alg. This will be shown in Section VII.3.

We first prove the following:

Proposition 4.3 *Let $\mathcal{L}$ be a finite family of languages; then the full AFL $\mathcal{L}\hat{\Gamma}$ generated by $\mathcal{L}$ is principal.*

Proof. Let $\mathcal{L} = \{L_1, L_2, \dots, L_n\}$, set $X = X_{L_1} \cup X_{L_2} \cup \dots \cup X_{L_n}$, and let $\#_1, \#_2, \dots, \#_n \notin X$ be n new letters. Define

$$L = L_1 \#_1 \cup L_2 \#_2 \cup \dots \cup L_n \#_n;$$

Each language $L_i \#_i$ is in $\mathcal{L}\Gamma$ by Corollary 2.5, thus $L \in \mathcal{L}\hat{\Gamma}$ and $L\hat{\Gamma} \subset \mathcal{L}\hat{\Gamma}$. In order to show the converse inclusion, note first that

$$L_i \#_i = L \cap X^* \#_i;$$

thus $L_i \#_i \in L\Gamma$ and $L_i \in L\Gamma$ by Corollary 2.5 for $i = 1, \dots, n$. This implies that $\mathcal{L} \subset L\Gamma$, and hence $\mathcal{L}\hat{\Gamma} \subset L\hat{\Gamma}$. ■

Note that Proposition 4.3 also holds for full semi-AFL, but is false for cones (Exercise 4.1).

Theorem 4.4 (Ginsburg and Greibach [1970]) *Let L be a language, and let $\#$ be a letter not in X_L ; then*

$$L\hat{\Gamma} = (L\#)^+ \Gamma.$$

This theorem supplies explicitly a cone generator for any principal full AFL. For the proof, we need two preliminary results.

Proposition 4.5 *Let L, M be two languages, and let $\#$ be a letter not in $X_L \cup X_M$; if $L \geq M$, then $(L\#)^+ \geq (M\#)^+$.*

Proof. Let $\tau: X_L^* \rightarrow X_M^*$ be a rational transduction such that $\tau(L) = M$, and let $R \in \text{Rat}(X_L^* \times X_M^*)$ be the graph of τ . Consider now the relation

$$S \subset (X_L \cup \#)^* \times (X_M \cup \#)^*$$

defined by $S = R \cdot \{(\#, \#)\}$. Then S is rational. Let

$$\bar{\tau}: (X_L \cup \#)^* \rightarrow (X_M \cup \#)^*$$

be the rational transduction defined by S . Then $\bar{\tau}(w) \neq \emptyset$ only if $w = w'\#$ for some $w' \in X_L^*$, and then

$$\bar{\tau}(w'\#) = \tau(w')\#. \quad (4.1)$$

Consider now the rational transduction $\bar{\tau}^+$ defined by S^+ . Then

$$f \in \bar{\tau}^+(w)$$

iff $w = w_1 \# w_2 \# \dots w_n \#$ for some $n \geq 1$, $w_1, w_2, \dots, w_n \in X_L^*$, and by (4.1):

$$f \in \tau(w_1)\# \tau(w_2)\# \dots \tau(w_n)\#.$$

This shows that $\bar{\tau}^+((L\#)^+) = (M\#)^+$ and achieves the proof. ■

Lemma 4.6 *Let L be a language, and let $\#, \$$ be two letters not in X_L ; then $(L\#)^+ \geq [(L\#)^+ \$]^+$.*

Proof. Set $Y = X_L \cup \#$, consider a third letter $\flat$ not in Y , and define a morphism

$$\theta: (Y \cup \flat)^* \rightarrow Y^*$$

by setting $\theta(y) = y$ ($y \in Y$), $\theta(\flat) = \#$. Then θ is strictly alphabetic, and

$$\theta^{-1}[(L\#)^+] = (L\# \cup L\flat)^+,$$

thus $\theta^{-1}[(L\#)^+] \cap [(X_L^* \#)^* X_L \flat]^+ = [(L\#)^* L\flat]^+$.

Hence $(L\#)^+ \geq [(L\#)^* L\flat]^+$. (4.2)

Consider now the morphism

$$\psi: (Y \cup \flat)^* \rightarrow (Y \cup \$)^*$$

defined by

$$\psi(y) = y(y \in Y), \quad \psi(b) = \#\$$$

$$\text{Then } \psi[(L\#)^*Lb]^+ = [(L\#)^*L\#\$]^+ = [(L\#)^+\$]^+;$$

together with (4.2), this shows that $(L\#)^+ \geq [(L\#)^+\$]^+$.

Proof. of Theorem 4.4 Clearly $(L\#)^+ \in L\hat{F}$, and thus

$$(L\#)^+\Gamma \subset L\hat{F}.$$

In order to prove the converse inclusion, we first note that $L \in (L\#)^+\Gamma$ since

$$(L\#)^+ \geq (L\#)^+ \cap X_L^*\# = L\# \geq L.$$

Thus, it suffices to show that $(L\#)^+\Gamma$ is a full AFL. Now $(L\#)^+\Gamma$ is already a principal cone, and closure under union follows from Proposition 2.6. In view of Proposition 4.2, it suffices to show that $(L\#)^+\Gamma$ is closed under plus operation. Let $M \in (L\#)^+\Gamma$, and let $\$$ be a letter not in $X_L \cup X_M \cup \#$. By Proposition 4.5, we have

$$[(L\#)^+\$]^+ \geq (M\$)^+,$$

and by Lemma 4.6, $(L\#)^+ \geq [(L\#)^+\$]^+$; thus

$$(L\#)^+ \geq (M\$)^+.$$

Clearly $(M\$)^+ \geq M^+$, showing that $M^+ \in (L\#)^+\Gamma$. Thus $(L\#)^+\Gamma$ is a full AFL, and the theorem is proved. ■

Exercises

4.1 Show that Proposition 4.3 remains true for full semi-AFLs, but not for cones.

4.2 Let $\mathcal{L}$ and $\mathcal{M}$ be full AFLs.

- Show that $\mathcal{L} \cup \mathcal{M}$ is closed under plus operation.
- Show that $\mathcal{L} \cup \mathcal{M}$ is a full AFL iff $\mathcal{L}$ and $\mathcal{M}$ are comparable.
- Show that $\mathcal{L} \cup \mathcal{M}$ is closed under product iff $\mathcal{L}$ and $\mathcal{M}$ are comparable.

4.3 Prove the formulas

$$(\mathcal{L}_1 \cup \mathcal{L}_2) \text{Rat} = (\mathcal{L}_1 \text{Rat} \cup \mathcal{L}_2 \text{Rat}) \text{Rat};$$

$$(\mathcal{L}_1 \cup \mathcal{L}_2) \hat{F} = (\mathcal{L}_1 \hat{F} \cup \mathcal{L}_2 \hat{F}) \hat{F}.$$

4.4 Show that the converse of Proposition 4.5 is false.

4.5 Let L_1, L'_1, L_2, L'_2 be languages and let $\#$ be a new letter. Show that if $L_1 \geq L'_1, L_2 \geq L'_2$, then $L_1\#L_2 \geq L'_1\#L'_2$, and give an example showing that the conclusion $L_1L_2 \geq L'_1L'_2$ is in general false.

4.6 Give an example showing that $L_1 \geq L_2$ does not imply $L_1^+ \geq L_2^+$.

V.5 Substitution

Substitutions are a fundamental tool for transformation of languages. They are essentially independent of rational transductions, and can be used to represent other operations such as closure under union or rational closure. Full AFLs closed under substitution (like the family Alg) have quite remarkable properties. Here we give only some basic definitions and results on substitutions. More properties are proved in Chapters VI and VII.

First, we recall the following

Definition Let $\mathcal{M}$ be a family of languages. A $\mathcal{M}$ -substitution is a substitution $\sigma: X^* \rightarrow Y^*$ such that $\sigma(x) \in \mathcal{M}$ for all $x \in X$.

Let $\mathcal{L}$ be a family of languages. Then we denote by $\mathcal{L} \square \mathcal{M}$ the set of all languages obtained from languages in $\mathcal{L}$ by applying $\mathcal{M}$ -substitutions. Thus

$$\mathcal{L} \square \mathcal{M} = \{\sigma(L) \mid L \in \mathcal{L}, \sigma: X_L^* \rightarrow Y^* \text{ a } \mathcal{M}\text{-substitution}\}.$$

Clearly $\mathcal{L} \square \mathcal{M}$ is closed under copy, and thus $\square$ is a binary operation on families of languages. Sometimes, it is convenient to dispose of an unary notation, when one of the two operands $\mathcal{L}$ or $\mathcal{M}$ is some standard family of languages. We introduce the following equivalent notations:

$$\mathcal{L} \square \mathcal{M} = \mathcal{L} \bar{\mathcal{M}} = \mathcal{M} \underline{\mathcal{L}}.$$

Thus $\bar{\mathcal{M}}$ is an operator, parametrized by $\mathcal{M}$, and acting on the family $\mathcal{L}$; and $\underline{\mathcal{L}}$ is an operator acting on $\mathcal{M}$. These notations will be used in the next chapter, where an operator calculus is developed involving only unary operators.

Example 5.1 The notation fits with the notation for rational closure of Section 3. Indeed, in view of Proposition 3.2,

$$\text{Rat} \square \mathcal{L} = \text{Rat } \bar{\mathcal{L}} = \mathcal{L} \text{Rat}$$

is the rational closure of $\mathcal{L}$.

Example 5.2 For any family of languages $\mathcal{L}$,

$$\text{Elm} \square \mathcal{L} = \text{Elm } \bar{\mathcal{L}} = \mathcal{L} \text{Elm} \quad \text{and} \quad \text{Fin} \square \mathcal{L} = \text{Fin } \bar{\mathcal{L}} = \mathcal{L} \text{Fin}$$

are the closure under union and the closure under union and product of $\mathcal{L}$.

Example 5.3 Substitution is not commutative. A Rat-substitution substitutes a rational set to each letter and thus is a rational substitution, a Elm-substitution substitutes a finite set of letters to each letter. In particular, any cone is closed under rational substitution:

$$\mathcal{L} \square \text{Rat} = \mathcal{L} \bar{\text{Rat}} = \text{Rat } \underline{\mathcal{L}} \subset \mathcal{L}\Gamma,$$

but $\text{Rat} \square \mathcal{L}$ usually is not contained in $\mathcal{L}\Gamma$.

Example 5.4 The family Rat is closed under rational substitution, thus

$$\text{Rat} \sqsupset \text{Rat} = \text{Rat};$$

we also have $\text{Alg} \sqsupset \text{Alg} = \text{Alg}$ since Alg is closed under context-free substitution.

The following formulas are clear; let $\mathcal{L}, \mathcal{L}', \mathcal{M}, \mathcal{M}'$ be families of languages:

$$\mathcal{M} \subset \mathcal{M}' \Rightarrow \mathcal{L} \sqsupset \mathcal{M} \subset \mathcal{L} \sqsupset \mathcal{M}' \quad (5.1)$$

$$\mathcal{L} \subset \mathcal{L}' \Rightarrow \mathcal{L} \sqsupset \mathcal{M} \subset \mathcal{L}' \sqsupset \mathcal{M} \quad (5.2)$$

further, if $\{x\} \in \mathcal{L}$ for at least one letter $x \in \Sigma$ (and hence for all letters since $\mathcal{L}$ is a family of languages), then

$$\mathcal{M} \subset \mathcal{L} \sqsupset \mathcal{M}, \quad \mathcal{M} \subset \mathcal{M} \sqsupset \mathcal{L}. \quad (5.3)$$

To see the first of the inclusions (5.3), consider $M \in \mathcal{M}$, $\{x\} \in \mathcal{L}$, and define a $\mathcal{M}$ -substitution $\sigma: x^* \rightarrow X_M^*$ by $\sigma(x) = M$. Then $\sigma(x) = M \in \mathcal{L} \sqsupset \mathcal{M}$. For the second inclusion, define $\sigma': X_M^* \rightarrow X_M^*$ to be the identity. Then $\sigma'(x) = \{x\} \in \mathcal{L}$ for all $x \in X_M$. Thus $\sigma'(M) = M \in \mathcal{M} \sqsupset \mathcal{L}$.

Relation (5.2) can be completed by

$$\left(\bigcup_{\lambda \in \Lambda} \mathcal{L}_\lambda \right) \sqsupset \mathcal{M} = \bigcup_{\lambda \in \Lambda} (\mathcal{L}_\lambda \sqsupset \mathcal{M}), \quad (5.4)$$

where $(\mathcal{L}_\lambda)_{\lambda \in \Lambda}$ is any set of families of languages.

The following theorem is important.

Theorem 5.1 (Associativity) *Let $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3$ be families of languages; then $\mathcal{L}_1 \sqsupset (\mathcal{L}_2 \sqsupset \mathcal{L}_3) = (\mathcal{L}_1 \sqsupset \mathcal{L}_2) \sqsupset \mathcal{L}_3$.*

In unary notations, the associativity relation has the expressions:

$$\mathcal{L}_3(\mathcal{L}_2\mathcal{L}_1) = (\mathcal{L}_3\mathcal{L}_2)\mathcal{L}_1 \quad \text{or} \quad (\mathcal{L}_1\mathcal{L}_2)\mathcal{L}_3 = \mathcal{L}_1(\mathcal{L}_2\mathcal{L}_3).$$

Proof. We show first the inclusion $(\mathcal{L}_1 \sqsupset \mathcal{L}_2) \sqsupset \mathcal{L}_3 \subset \mathcal{L}_1 \sqsupset (\mathcal{L}_2 \sqsupset \mathcal{L}_3)$. Let $A \in (\mathcal{L}_1 \sqsupset \mathcal{L}_2) \sqsupset \mathcal{L}_3$. There exist a language $B \in \mathcal{L}_1 \sqsupset \mathcal{L}_2$, and a $\mathcal{L}_3$ -substitution $\sigma: X_B^* \rightarrow X_A^*$ such that $\sigma(B) = A$. Since $B \in \mathcal{L}_1 \sqsupset \mathcal{L}_2$, there exist a language $C \in \mathcal{L}_1$, and a $\mathcal{L}_2$ -substitution $\tau: X_C^* \rightarrow X_B^*$ such that $\tau(C) = B$. Let $\rho = \sigma \circ \tau: X_C^* \rightarrow X_A^*$. For each letter $z \in X_C$,

$$\rho(z) = \sigma(\tau(z)) \in \mathcal{L}_2 \sqsupset \mathcal{L}_3,$$

thus ρ is a $\mathcal{L}_2 \sqsupset \mathcal{L}_3$ -substitution. Since $A = \rho(C)$, we have $A \in \mathcal{L}_1 \sqsupset (\mathcal{L}_2 \sqsupset \mathcal{L}_3)$. This proves the inclusion.

We now establish the converse inclusion. Let $A \in \mathcal{L}_1 \sqsupset (\mathcal{L}_2 \sqsupset \mathcal{L}_3)$. There exist a language $C \in \mathcal{L}_1$ and a $\mathcal{L}_2 \sqsupset \mathcal{L}_3$ -substitution $\rho: X_C^* \rightarrow X_A^*$ with $\rho(C) = A$. For each $z \in X_C$, $\rho(z) \in \mathcal{L}_2 \sqsupset \mathcal{L}_3$; consequently there is a language $B_z \in \mathcal{L}_2$ and a

$\mathcal{L}_3$ -substitution

$$\sigma_z: X_{B_z}^* \rightarrow X_A^*$$

such that $\rho(z) = \sigma_z(B_z)$. By the closure under copy of $\mathcal{L}_2$, we may assume the alphabets X_{B_z} ($z \in X_C$) pairwise disjoint. Set

$$Y = \bigcup_{z \in X_C} X_{B_z},$$

and define a substitution $\sigma: Y^* \rightarrow X_A^*$ by

$$\sigma(y) = \sigma_z(y) \quad \text{iff} \quad y \in X_{B_z}.$$

Then σ is a $\mathcal{L}_3$ -substitution, and $\rho(z) = \sigma(B_z)$ for all $z \in X_C$. Finally define a substitution $\tau: X_C^* \rightarrow Y^*$ by $\tau(z) = B_z$ for $z \in X_C$. Then τ is a $\mathcal{L}_2$ -substitution, and

$$\rho(z) = \sigma(B_z) = \sigma \circ \tau(z) \quad \text{for all} \quad z \in X_C.$$

Now $\tau(C) \in \mathcal{L}_1 \sqsupset \mathcal{L}_2$, and

$$A = \rho(C) = \sigma(\tau(C)) \in (\mathcal{L}_1 \sqsupset \mathcal{L}_2) \sqsupset \mathcal{L}_3. \quad \blacksquare$$

By induction, we immediately obtain the following

Corollary 5.2 *Let $\mathcal{L}$ and $\mathcal{M}$ be families of languages; then*

$$(\cdots ((\mathcal{L} \sqsupset \mathcal{M}) \sqsupset \mathcal{M}) \sqsupset \cdots \sqsupset \mathcal{M}) = \mathcal{L} \sqsupset (\cdots ((\mathcal{M} \sqsupset \mathcal{M}) \sqsupset \cdots \sqsupset \mathcal{M}))$$

$\underbrace{\hspace{10em}}_{k \text{ times}} \qquad \underbrace{\hspace{10em}}_{k \text{ times}}$

or equivalently $\mathcal{L}(\bar{\mathcal{M}})^k = \mathcal{L}\bar{\mathcal{M}}(\bar{\mathcal{M}})^{k-1}$. ■

Finally we note the following rule

Corollary 5.3 *Let $\mathcal{L}, \mathcal{M}$ and $\mathcal{N}$ be families of languages; then*

$$\mathcal{N}\mathcal{L}\bar{\mathcal{M}} = \mathcal{N}\bar{\mathcal{M}}\mathcal{L}.$$

Proof. $\mathcal{N}\mathcal{L}\bar{\mathcal{M}} = (\mathcal{L} \sqsupset \mathcal{N}) \sqsupset \mathcal{M} = \mathcal{L} \sqsupset (\mathcal{N} \sqsupset \mathcal{M}) = \mathcal{L} \sqsupset (\mathcal{N}\bar{\mathcal{M}}) = \mathcal{N}\bar{\mathcal{M}}\mathcal{L}$. ■

The set of all families of languages equipped with the substitution $\sqsupset$ is a semigroup but not a monoid (Exercise 5.1). The operation $\sqsupset$ is not a binary operation between languages since the result $\sigma(L)$ depends of L and of the $\text{Card}(X_L)$ languages $\sigma(x)$ ($x \in X_L$). There exists a special kind of substitution called syntactic substitution which depends only on two languages. This substitution is very important for two reasons: first, any substitution can be represented as the composition of a syntactic substitution and a rational transduction; in this sense, syntactic substitutions are “generic”. Second, syntactic substitutions lead to “decompositions” of certain families of languages; results of this kind are the converse of closure properties. They will be exposed in Chapter VII.

Definition Let L and M be languages. The syntactic substitution of M in L is the substitution

$$\sigma_M: X_L^* \rightarrow (X_M \cup X_L)^*$$

defined by

$$\sigma_M(x) = Mx \quad (x \in X_L).$$

We use also the symbol $\uparrow$ for syntactic substitution, defined by

$$L\uparrow M = \sigma_M(L).$$

By definition,

$$L\uparrow M = \{m_1x_1m_2x_2 \cdots m_rx_r \mid r \geq 1, m_1, \dots, m_r \in M, x_1, \dots, x_r \in X_L, x_1 \cdots x_r \in L\} \cup (1 \cap L). \quad (5.5)$$

Syntactic substitution is frequently used with the supplementary assumption that the alphabets X_L and X_M are disjoint; sometimes $1 \notin L, 1 \notin M$ are also required. The notation is justified by the following formulas which are similar to formulas for exponentiation:

$$\emptyset \uparrow M = \emptyset; \quad 1 \uparrow M = 1, \quad x \uparrow M = Mx \quad (x \in \Sigma); \quad L \uparrow 1 = L;$$

$$(fg) \uparrow M = (f \uparrow M)(g \uparrow M); \quad L \uparrow M = \bigcup_{f \in L} f \uparrow M;$$

$$(L_1 \cup L_2) \uparrow M = L_1 \uparrow M \cup L_2 \uparrow M; \quad (L_1 L_2) \uparrow M = (L_1 \uparrow M)(L_2 \uparrow M).$$

Note also that

$$c^+ \uparrow M = \bigcup_{n \geq 1} c^n \uparrow M = \bigcup_{n \geq 1} (Mc)^n = (Mc)^+, \quad c \in \Sigma.$$

Thus, Theorem 4.4 may be rewritten in the form

$$L\hat{\Gamma} = (c^+ \uparrow L)\Gamma, \quad \text{for } c \in \Sigma \setminus X_L.$$

Note that σ_M is not a $\{M\}$ -substitution, but if $L \in \mathcal{L}$ and $M \in \mathcal{M}$ and $\mathcal{M}$ is a cone, then $L\uparrow M \in \mathcal{L} \square \mathcal{M}$.

Proposition 5.4 Let $\mathcal{M}$ be a family of languages. Any $\mathcal{M}$ -substitution $\sigma: X^* \rightarrow Y^*$ can be factorized into $\sigma = \tau \circ \sigma_N$ where $\sigma_N: X^* \rightarrow Z^*$ is a syntactic substitution, $N \in \mathcal{M}$ Elm and $\tau: Z^* \rightarrow Y^*$ is a rational transduction.

Proof. For each $x \in X$, set $M_x = \sigma(x)$, and let N_x be a copy of M_x over an alphabet Z_x in bijection with Y by a mapping $\theta_x: Z_x \rightarrow Y$. We choose the alphabets $Z_x, (x \in X)$ pairwise disjoint and disjoint from X . Then set

$$Z = X \cup \bigcup_{x \in X} Z_x$$

and define a morphism $\theta: Z^* \rightarrow Y^*$ by

$$\theta(x) = 1 \quad (x \in X) \quad \theta(z) = \theta_x(z) \quad (z \in Z_x).$$

$$\text{Set } N = \bigcup_{x \in X} N_x. \quad (5.6)$$

Then the syntactic substitution $\sigma_N: X^* \rightarrow Z^*$ satisfies

$$\sigma_N(x) = Nx = \bigcup_{y \in X} N_y x \quad (x \in X).$$

Define the transduction $\tau: Z^* \rightarrow Y^*$ by

$$\tau(f) = \theta(f \cap K) \quad (f \in Z^*)$$

where $K = (\bigcup_{x \in X} Z_x^* x)^* \in \text{Rat}(Z^*)$.

Clearly τ is rational. Further

$$\tau \circ \sigma_N(1) = \tau(1) = 1 = \sigma(1),$$

and for $w = x_1 x_2 \cdots x_r, r \geq 1, x_i \in X$, we have

$$\begin{aligned} \tau \circ \sigma_N(w) &= \theta(Nx_1 Nx_2 \cdots Nx_r \cap K) \\ &= \theta(N_{x_1} x_1 N_{x_2} x_2 \cdots N_{x_r} x_r) = M_{x_1} M_{x_2} \cdots M_{x_r} = \sigma(w). \end{aligned}$$

Thus $\tau \circ \sigma_N = \sigma$. By (5.6), $N \in \mathcal{M}$ Elm. This achieves the proof. ■

This proposition can be used to verify that a full semi-AFL is closed under substitution. First, we give a definition.

Definition Let $\mathcal{L}$ and $\mathcal{M}$ be two families of languages. Then $\mathcal{L}$ is closed under $\mathcal{M}$ -substitution if $\mathcal{L} \square \mathcal{M} \subset \mathcal{L}$, and $\mathcal{L}$ is closed under substitution if $\mathcal{L} \square \mathcal{L} \subset \mathcal{L}$.

Example 5.5 Any cone is closed under rational substitution:

$$\mathcal{L} = \mathcal{L}\Gamma \Rightarrow \mathcal{L} = \mathcal{L} \square \text{Rat}.$$

Example 5.6 The families Rat and Alg are closed under substitution. The family Lin is a rational cone, but not a full AFL (see next section).

Thus Lin is not closed under substitution in view of:

Proposition 5.5 A rational cone closed under substitution is a full AFL.

Proof. Let $\mathcal{L}$ be closed under substitution. Then $\mathcal{L} \square \mathcal{L} \subset \mathcal{L}$. If $\mathcal{L}$ is a rational cone, then $\text{Rat} \subset \mathcal{L}$ by Proposition 2.1. Thus

$$\mathcal{L} \subset \mathcal{L} \text{Rat} = \text{Rat} \square \mathcal{L} \subset \mathcal{L} \square \mathcal{L} \subset \mathcal{L},$$

and $\mathcal{L} = \mathcal{L} \text{Rat}$. ■

Proposition 5.6 Let $\mathcal{L}$ be a full semi-AFL. Then $\mathcal{L}$ is closed under substitution iff $\mathcal{L}$ is closed under syntactic substitution.

Proof. Let $\mathcal{L}$ be closed under substitution, $M \in \mathcal{L}$, and let $\sigma_M: X^* \rightarrow (X_M \cup X)^*$ be a syntactic substitution. Then $\sigma_M(x) = Mx \in \mathcal{L}$ for $x \in X$ since $\mathcal{L}$ is a cone. Thus σ_M is a $\mathcal{L}$ -substitution, and $\mathcal{L}$ is closed under syntactic substitution.

Conversely, let σ be a $\mathcal{L}$ -substitution. In view of Proposition 5.4, there exists a factorization

$$\sigma = \tau \circ \sigma_N,$$

where σ_N is a syntactic substitution, and $N \in \mathcal{L} \text{ Elm} = \mathcal{L}$. Since $\mathcal{L}$ is closed under syntactic substitution, $\sigma_N(L) \in \mathcal{L}$ for $L \in \mathcal{L}$, and $\tau(\sigma_N(L)) = \sigma(L) \in \mathcal{L} \Gamma = \mathcal{L}$. ■

Exercises

5.1 Show that there is no neutral element for the operation $\sqcup$.

5.2 Let L and M be languages over disjoint alphabets and let c be a new letter. Show that

$$L \uparrow (c^+ \uparrow M) \approx (L \uparrow c^+) \uparrow M.$$

5.3 Let L, M, K be languages over disjoint alphabets. Show that $L \uparrow (K \uparrow M) \leq (L \uparrow K) \uparrow M$. Discuss the converse inequality.

5.4 Let L, M, M' be languages over disjoint alphabets. Show that $M \approx M'$ implies $L \uparrow M \approx L \uparrow M'$. Show that the implication $M \approx M' \Rightarrow M \uparrow L \approx M' \uparrow L$ is generally false.

V.6 Example: The Cone of Linear Languages

In this section, we study the family Lin of linear languages. We show that Lin is a principal cone, and we give generators of this cone. We also prove that Lin is not a full AFL.

Definition A context-free grammar $G = \langle V, X, P \rangle$ is linear if the right side of each production contains at most one nonterminal symbol:

$$\xi \rightarrow \alpha \in P \Rightarrow |\alpha|_V \leq 1.$$

A language L is linear if there exists a linear grammar generating L .

We denote by Lin the set of all linear languages. Clearly, Lin is a family of languages.

Example 6.1 The symmetric languages S_n over n letters. They are defined over the alphabet

$$Z_n = X_n \cup \bar{X}_n,$$

where $X_n = \{x_1, \dots, x_n\}$, $\bar{X}_n = \{\bar{x}_1, \dots, \bar{x}_n\}$ are two disjoint alphabets of n letters, and they are generated by the grammars with productions

$$\xi \rightarrow \sum_{k=1}^n x_k \xi \bar{x}_k + 1.$$

Clearly $f \in S_n$ iff $f = g\bar{g}$ where $g = x_{i_1} \cdots x_{i_p} \in X_n^*$ and $\bar{g} = \bar{x}_{i_p} \cdots \bar{x}_{i_1}$.

Example 6.2 Let $X = \{a, b\}$, and $\Theta = \{=, \neq, >, <, \geq, \leq\}$. The language S_θ , ($\theta \in \Theta$) is defined by

$$S_\theta = \{a^n b^m \mid n, m \geq 0 \text{ and } n \theta m\}.$$

All these languages are linear. They are related by

$$\begin{aligned} S_{<} &= S_{=} b^+ = S_{\leq} b; & S_{\leq} &= S_{<} \cup S_{=} = S_{<} b^{-1}; \\ S_{>} &= a^+ S_{=} = a S_{\geq}; & S_{\geq} &= S_{>} \cup S_{=} = a^{-1} S_{>}; \\ S_{\neq} &= S_{>} \cup S_{<}; & S_{=} \cup S_{\neq} &= a^* b^*. \end{aligned}$$

Of course, $S_{=}$ is equal to the symmetric language S_1 .

The following lemma is useful.

Lemma 6.1 For any linear grammar $G = \langle V, X, P \rangle$ there exists a linear grammar $G' = \langle V', X, P' \rangle$ such that $V' \supset V$, further $L_{G'}(\sigma) = L_G(\sigma)$ for all $\sigma \in V$, and all productions of G' are of one of the following forms ($\xi, \eta \in V'$, $x \in V$):

- (i) $\xi \rightarrow x\eta$ or $\xi \rightarrow \eta x$;
- (ii) $\xi \rightarrow x$ or $\xi \rightarrow 1$.

The proof of the lemma is left to the reader. A grammar G' of the above form is said in canonical form.

Theorem 6.2 The family Lin is a rational cone: $\text{Lin } \Gamma = \text{Lin}$.

Proof. Let G be a linear grammar, and consider the constructions of the grammars ψG , $\varphi^{-1} G$, G_K given in Section II.2. By inspection, ψG and G_K are linear grammars and $\varphi^{-1} G$ is not a linear grammar. Thus Lin is closed under morphism and intersection with regular sets. In order to prove closure under inverse projection, a special construction is necessary. Restricting ourselves to inverse projection, we show that the insertion of a new letter can be done just by moving sequentially in the right side of a production by remembering the number of the production in an auxiliary symbol.

Let $L \in \text{Lin}$ be generated by the linear grammar $G = \langle V, X, P \rangle$ in canonical form, let $Y \supset X$ and let π be the projection of Y^* onto X^* . We may assume $\text{Card}(Y \setminus X) = 1$, since the general case results by composition of such projections.

Let $z = Y \setminus X$, and number the productions from 1 to $n = \text{Card } P$. Define a grammar $\bar{G} = \langle \bar{V}, Y, \bar{P} \rangle$ as follows:

$$\bar{V} = V \cup \{\omega_1, \dots, \omega_n\},$$

where the ω_i are new symbols. Further, if the p -th production of G is

$$\xi \rightarrow x\eta \quad (\text{or } \xi \rightarrow \eta x)$$

then put into $\bar{P}$ the productions

$$\begin{aligned} \xi &\rightarrow \omega_p, & \omega_p &\rightarrow z\omega_p + x\eta; \\ (\text{or } \xi &\rightarrow \omega_p, & \omega_p &\rightarrow \omega_p z + \eta x). \end{aligned}$$

If the p -th production of G is

$$\xi \rightarrow x \quad (\text{or } \xi \rightarrow 1)$$

then put into $\bar{P}$ the productions

$$\begin{aligned} \xi &\rightarrow \omega_p, & \omega_p &\rightarrow z\omega_p + \omega_p z + x; \\ (\text{or } \xi &\rightarrow \omega_p, & \omega_p &\rightarrow z\omega_p + 1). \end{aligned}$$

The grammar $\bar{G}$ obtained by this construction is linear, and it is easily seen that

$$L_{\bar{G}}(\xi) = \pi^{-1}(L_G(\xi)) \quad \text{for } \xi \in V.$$

Thus if $L = L_G(\sigma)$ for some $\sigma \in V$, then $\pi^{-1}(L)$ is in Lin . ■

We shall prove that the symmetric languages S_n are generators of the cone Lin for $n \geq 2$. First we prove

Proposition 6.3 *The languages S_n ($n \geq 2$) are rationally equivalent; further $S_2 \geq S_1$.*

We shall prove later that $S_2 > S_1$. A direct proof is possible, but rather long; a simple proof will follow from general properties of iterative pairs developed in Chapter VIII.

Proof. Since

$$S_{n-1} = S_n \cap Z_{n-1}^* \quad (n \geq 2),$$

it follows that $S_n \geq S_{n-1}$ for $n \geq 2$.

Conversely, let $n \geq 1$, and define a morphism

$$\alpha : Z_n^* \rightarrow Z_2^*$$

$$\text{by} \quad \alpha(x_k) = x_1 x_2^k, \quad \alpha(\bar{x}_k) = \bar{x}_2^k \bar{x}_1 \quad 1 \leq k \leq n.$$

Then $f \in S_2 \cap \alpha(Z_n^*)$ iff $f = 1$ or

$$f = x_1 x_2^{k_1} x_1 x_2^{k_2} \cdots x_1 x_2^{k_p} \bar{x}_2^{k_p} \bar{x}_1 \cdots \bar{x}_2^{k_1} \bar{x}_1,$$

with $1 \leq k_i \leq n$ for $i = 1, \dots, p$. Thus

$$\alpha^{-1}(S_2 \cap \alpha(Z_n^*)) = \alpha^{-1}(S_2) = S_n,$$

and $S_2 \geq S_n$ for $n \geq 1$. ■

The method used to prove this proposition is an encoding of the alphabet X_n in an alphabet of two letters. This is a quite general method which will be used several times.

Theorem 6.4 *Lin is a principal cone, and any symmetric language S_n ($n \geq 2$) is a generator of Lin : $\text{Lin} = S_n \Gamma$.*

Proof. Since $S_n \in \text{Lin}$ and Lin is a cone, we have $S_n \Gamma \subset \text{Lin}$ for all $n \geq 2$. Further $S_n \Gamma = S_{n'} \Gamma$ for $n, n' \geq 2$ by the preceding proposition. Thus to prove the theorem it suffices to show that any linear language L belongs to $S_n \Gamma$ for some $n \geq 2$.

Let $L \subset X^*$ be a linear language, and let $G = \langle V, X, P \rangle$ be a linear grammar in canonical form such that $L = L_G(\sigma)$ for some $\sigma \in V$. Number the productions from 1 to $n = \text{Card } P$, and define a morphism $\alpha : Z_n^* \rightarrow X^*$ in the following way:

a) If the p -th production is

$$\xi \rightarrow x\eta \quad (\text{or } \xi \rightarrow \eta x),$$

then set $\alpha(x_p) = x$, $\alpha(\bar{x}_p) = 1$; (or $\alpha(x_p) = 1$, $\alpha(\bar{x}_p) = x$).

b) If the p -th production is

$$\xi \rightarrow x \quad (\text{or } \xi \rightarrow 1),$$

then set $\alpha(x_p) = x$, $\alpha(\bar{x}_p) = 1$ (or $\alpha(x_p) = \alpha(\bar{x}_p) = 1$).

Define the local rational language

$$K = (AX_n^* \cap X_n^* B) \setminus X_n^* C X_n^*$$

by $x_p \in A$ iff the left side of the p -th production is σ

$x_p \in B$ iff the right side of the p -th production is in $X \cup 1$

$x_p x_q \in C$ iff the left side of the q -th production is equal to the unique nonterminal in the right side of p -th production.

We now prove

$$L = \alpha(S_n \cap K \bar{X}_n^*). \quad (6.1)$$

Indeed, consider a derivation

$$\sigma \rightarrow w_1 \rightarrow w_2 \rightarrow \cdots \rightarrow w_r = w \quad (6.2)$$

from σ into $w \in L$ in the grammar G . This derivation is uniquely determined by the sequence $(p_1, p_2, \dots, p_r)$ of the numbers of the productions used in the derivation. By construction, the word $x_{p_1}x_{p_2} \cdots x_{p_r}$ is in K , and $w = \alpha(x_{p_1}x_{p_2} \cdots x_{p_r}\bar{x}_{p_1} \cdots \bar{x}_{p_r})$.

Conversely, if $x_{p_1}x_{p_2} \cdots x_{p_r}\bar{x}_{p_1} \cdots \bar{x}_{p_r} \in S_n \cap K\bar{X}_n^*$, then there exists a derivation (6.2) for which $p_1, p_2, \dots, p_r$ is the sequence of numbers of the productions. Moreover, $w = \alpha(x_{p_1}x_{p_2} \cdots x_{p_r}\bar{x}_{p_1} \cdots \bar{x}_{p_r})$. ■

Note that by formula (6.1), the above construction yields an analogue of the Chomsky-Schützenberger Theorem for linear languages. In fact, a weaker property can be shown for any principal cone (Exercise 6.1).

The rational cone Lin is principal, thus closed under union. We shall see that Lin is not closed under product and thus is not a full AFL. First we show how linear languages are linked to rational relations. The following proposition is in Rosenberg [1967].

Proposition 6.5 A language $L \subset X^*$ is linear iff there exists a rational relation $A \subset X^* \times X^*$ such that

$$L = \{f\bar{g} \mid (f, g) \in A\}.$$

Proof. Let $L \subset X^*$ be a linear language, and consider a linear grammar $G = \langle V, X, P \rangle$ in canonical form such that $L = L_G(\sigma)$ for some $\sigma \in V$.

Define a transducer $T = \langle X, X, Q, \sigma, q_+, E \rangle$ by $Q = V \cup q_+$ with $q_+ \notin V$, and E composed of the transitions

$$\begin{aligned} (\xi, x, 1, \eta) \text{ for } \xi \rightarrow x\eta \in P & \quad (\xi, x, 1, q_+) \text{ for } \xi \rightarrow x \in P \\ (\xi, 1, x, \eta) \text{ for } \xi \rightarrow \eta x \in P & \quad (\xi, 1, 1, q_+) \text{ for } \xi \rightarrow 1 \in P. \end{aligned}$$

It is easily seen that each computation $e = e_1 e_2 \cdots e_n$ from ξ to $\eta \in V$ (resp. to q_+) with label $|e| = (f, g)$ determines a derivation $\xi \xrightarrow{n} f\eta\bar{g}$ (resp. $\xi \xrightarrow{n} f\bar{g}$) and vice-versa. Thus $L = \{f\bar{g} \mid (f, g) \in T(\sigma, q_+)\}$. Conversely, let $\tau: X^* \rightarrow X^*$ be the transduction with graph $A \in \text{Rat}(X^* \times X^*)$ and let $T = \langle X, X, Q, q_-, q_+, E \rangle$ be a transducer realizing τ and satisfying the conditions of Corollary III.6.2. Define $G = \langle V, X, P \rangle$ by $V = Q \setminus q_+$ and

$$P = \{q \rightarrow uq'\bar{v} \mid (q, u, v, q') \in E, q' \neq q_+\} \cup \{q \rightarrow u\bar{v} \mid (q, u, v, q_+) \in E\}.$$

Then G is linear and $L_G(q_-) = \{f\bar{g} \mid (f, g) \in A\}$. ■

Let us comment this proposition. First, we introduce a definition.

Definition For $M \subset X^*$ and $A \subset Y^* \times Z^*$, the bracket of A and M is the language over $X \cup Y \cup Z$ defined by

$$[A, M] = \{fw\bar{g} \mid w \in M, (f, g) \in A\}.$$

Thus $L = \{f\bar{g} \mid (f, g) \in A\}$ can be written as $L = [A, 1]$. Then, Proposition 6.5 states that for any $A \in \text{Rat}(X^* \times X^*)$, the language $[A, 1]$ is linear, and conversely for any $L \in \text{Lin}$, there exists a relation $A \in \text{Rat}(X^* \times X^*)$ such that $L = [A, 1]$. However, if L is linear, and $L = [A, 1]$ for some $A \subset X^* \times X^*$, then A is not necessarily a rational relation (Exercise 6.4). Indeed, a factorization $w = f\bar{g}$ is a “parsing” of w , and any parsing needs not to be linear.

We now prove an iteration lemma for linear languages.

Proposition 6.6 (Iteration lemma for linear languages) Let $L \subset X^*$ be a linear language; then there exists an integer $N \geq 1$ such that any word $f \in L$ of length $|f| \geq N$ admits a factorization

$$f = aubvc \quad (a, u, b, v, c \in X^*)$$

satisfying

$$au^n bv^n c \in L \text{ for } n \geq 0, |uv| \geq 1 \text{ and } |auvc| \leq N.$$

The special feature of this iteration lemma is of course the very last condition which says that the factors u and v can be chosen near to the borders of the word f .

Proof. Let $A \subset X^* \times X^*$ be a rational relation such that $L = \{f\bar{g} \mid (f, g) \in A\}$. Then the proposition is just a reformulation of the iteration lemma for rational relations together with the remark following Lemma III.3.3. ■

Proposition 6.6 can also be proved directly on a linear grammar generating L , without using Proposition 6.5 (Exercise 6.2).

Example 6.3 The language $(S_-)^2 = \{x^n y^n x^m y^m \mid n, m \geq 0\}$ is not linear. Assume the contrary. Then by the iteration lemma, there would exist large enough integers n, m such that $x^{n+\lambda} y^n x^m y^{m+\mu} \in (S_-)^2$ for some integers λ, μ with $0 < \lambda + \mu$, and this is impossible. This example shows that the full AFL generated by S_- is not contained in Lin .

Corollary 6.7 The rational cone Lin is not a full AFL. ■

We give some other examples of nonlinear languages.

Example 6.4 The language $L = \{x^n y^{n+m} x^m \mid n, m \geq 0\}$ is not linear; this is shown as in Example 6.3.

Example 6.5 The Dyck languages are not linear. Consider $D_1^*, D_1^* \subset \{x, \bar{x}\}^*$. Then $D_1^* \cap x^* \bar{x}^* x^* = \{x^n \bar{x}^{n+m} x^n \mid n, m \geq 0\}$ thus $D_1^* \not\supseteq L$, where L is the language of Example 6.4, and the linearity of D_1^* would imply the linearity of L since Lin is a cone. Next

$$D_1^* \cap x^+ \bar{x}^+ x^+ \bar{x}^+ = \{x^{k+n} \bar{x}^n x^p \bar{x}^{p+k} \mid k \geq 0, n, p > 0\}.$$

Let C be the latter language, and assume $C \in \text{Lin}$. Then $x^n \bar{x}^n x^p \bar{x}^p \in C$ for any $n, p > 0$, and by the iteration lemma, there exist λ, μ , $0 < \lambda + \mu$ such that $x^{n-\lambda} \bar{x}^n x^p \bar{x}^{p-\mu} \in C$, provided n, m has been chosen large enough. Thus $D_1^* \notin \text{Lin}$. We shall see later (Chapter VII) that any Dyck language over at least two letters is a generator of the cone Alg and therefore cannot be linear. Further, $D_1 \approx D_1' \approx D_1^{*}$ (Proposition VII.1.3), thus $D_1, D_1' \notin \text{Lin}$.

Exercises

6.1 Let $\mathcal{L} = A\Gamma$ be a principal cone. Show that there exist languages $(A_n)_{n \geq 1}$ in $\mathcal{L}$ such that any $L \in \mathcal{L}$ can be written in the form

$$L = \psi(A_n \cap K)$$

for some $n \geq 1$, where ψ is an alphabetic morphism and K is a regular language.

6.2 Prove the iteration lemma 6.6 directly on a linear grammar for L .

6.3 For $n \geq 1$, let $X_n = \{x_1, \dots, x_n\}$ and define

$$M_n = \{f \in X_n^* \mid f = \bar{f}\}.$$

M_n is the language of palindromes over n letters.

a) Show that M_n is a linear context-free language first by exhibiting a grammar, then by showing that $S_n \geq M_n$.

b) Set $M'_n = \{f \in M_n \mid |f|_{x_n} = 1\}$. Show that $M_n \geq M'_n \geq S_{n-1}$ for $n \geq 2$.

c) Show that any M_n ($n \geq 2$) is a generator of the cone Lin .

6.4 Give an example of a linear language L and an irrational relation A such that $L = [A, 1]$. (For further discussion, see Rosenberg [1967].)

V.7 Examples of Incomparable Languages

It is usually not difficult to prove that a language dominates rationally another language by providing a rational transduction mapping the first onto the second language. It is often much harder to prove nondomination or strict domination.

In some cases, known properties of cones give an easy answer. Thus the fact that the cone of linear languages is not closed under product implies that $\text{Lin} \not\subseteq \text{Alg}$, and thus any generator of the cone of context-free languages strictly dominates all linear languages. On the other hand, there exists a general criterion based on so-called systems of iterative pairs which allows to prove strict domination in a great number of situations. This will be developed in Chapter VIII. For other classes of families of languages, the "syntactic lemma" proved in Chapter VII provides a tool to establish the existence of infinite chains of cones or full AFLs.

Nevertheless, there still remain languages for which strict domination or incomparability can only be shown by a direct proof. The proofs in these cases usually are by contradiction. Assuming the existence of a rational transduction, the pumping lemma is applied to the regular set given by Nivat's theorem in order to obtain a contradiction. In this section we illustrate this technique by two examples, proving the incomparability of the languages $S_{<}, S_{>}, S_{\neq}$.

We first fix some notations. Set

$$S_{<} = \{x^n y^m \mid 0 \leq n < m\}, \quad X = \{x, y\};$$

$$S_{\neq} = \{a^n b^m \mid n, m \geq 0, n \neq m\}, \quad Y = \{a, b\};$$

we may assume $X \cap Y = \emptyset$, and set $Z = X \cup Y$. Finally, let $\alpha: Z^* \rightarrow X^*$ and $\beta: Z^* \rightarrow Y^*$ be the two projections from Z^* onto X^* and Y^* respectively.

Proposition 7.1 *The language $S_{<}$ is not a rational image of $S_{\neq}$.*

Proof. Assume the contrary. Then there exists a rational transduction $\tau: Y^* \rightarrow X^*$ such that $\tau(S_{\neq}) = S_{<}$. By Nivat's Theorem III.4.1, there exists a regular language $R \subset Z^*$ such that

$$\tau(f) = \alpha(\beta^{-1}(f) \cap R) \quad f \in Y^*.$$

Let N be the integer of the pumping lemmas associated with R (N is the number of states of a finite automaton recognizing R), let $r > 2N$, and let $w = x^r y^s \in S_{<}$ for some $s > r$. Then there exists $f = a^n b^m \in S_{\neq}$ such that

$$x^r y^s \in \alpha(\beta^{-1}(a^n b^m) \cap R),$$

and consequently there is a word $h \in R$ such that

$$\alpha h = x^r y^s, \quad \beta h = a^n b^m.$$

Consider an arbitrary factorization

$$h = h_1' h_2' \quad \text{with} \quad \alpha h_1' = x^r \quad \alpha h_2' = y^s.$$

Now $|h_1'|_x = r > 2N$. Thus, marking the letters x in h_1' , we obtain by Ogden's iteration lemma applied twice a factorization $h_1' = v_1 u' v_2 u'' v_3$, with $0 < |u'|_x, |u''|_x \leq N$ and $v_1 u'^* v_2 u''^* v_3 h_2' \subset R$. Since $\beta h_1' \subset a^* b^*$, at least one of the two words $\beta(u')$, $\beta(u'')$ belongs to $a^* \cup b^*$. (This is the reason why we apply the iteration lemma twice!) Denote by u one of the words u' , u'' whose image by β is in a^* or b^* . This provides a factorization

$$h = h_1 u h_2, \quad \text{with} \quad 0 < |u|_x \leq N, \quad \beta(u) \in a^* \cup b^*, \quad h_1 u^* h_2 \subset R.$$

Now $\beta(h_1 u^p h_2) \in a^* b^*$ for $p \geq 0$, thus $\beta(h_1 u^p h_2) \in S_{\neq}$ for all $p \geq 0$ excepted at most one. This implies that

$$h_1 u^p h_2 \in R \cap \beta^{-1}(S_{\neq})$$

for all large enough p , and consequently

$$\alpha(h_1 u^p h_2) = x^{r+(p-1)|\alpha(u)|} y^s \in S_{<}$$

for all large enough p . Since $|\alpha(u)| = |u|_x > 0$, this is impossible. ■

By symmetry, we clearly obtain also the property: $S_{\neq} \not\geq S_{>}$. The next proposition, which is the converse of the previous one, is much more difficult to prove.

Proposition 7.2 *The language $S_{\neq}$ is not a rational image of $S_{<}$.*

There are several consequences of these propositions:

Theorem 7.3 *The languages $S_{<}$, $S_{>}$, $S_{\neq}$ are pairwise incomparable; the language $S_{=}$ strictly dominates the languages $S_{<}$, $S_{>}$, $S_{\neq}$.*

Proof. In view of Propositions 7.1 and 7.2, the languages $S_{\neq}$ and $S_{<}$ are incomparable. By symmetry, the languages $S_{\neq}$ and $S_{>}$ are incomparable. Assume $S_{>} \geq S_{<}$; then $S_{>} \geq S_{<} \cup S_{<} = S_{\neq}$. Thus $S_{>}$ and $S_{<}$ are incomparable. By Example 6.2, $S_{=}$ dominates $S_{>}$, $S_{<}$ and $S_{\neq}$. Assume $S_{\neq} \geq S_{=}$; then $S_{=} \geq S_{<}$ would imply the relation $S_{\neq} \geq S_{<}$, in contradiction to Proposition 7.1. Thus $S_{=} > S_{\neq}$. In the same manner, if $S_{>} \geq S_{=}$, then since $S_{=} \geq S_{\neq}$, it would follow that $S_{>} \geq S_{\neq}$. Thus $S_{=} > S_{>}$ and $S_{=} > S_{<}$. ■

The situation described by Theorem 7.3 can be pictorially represented as in Fig. V. 2.

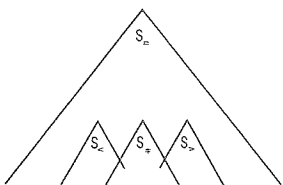


Fig. V.2

The proof of Proposition 7.2 is similar to the proof of 7.1: Assuming the existence of a rational transduction τ such that $\tau(S_{<}) = S_{\neq}$, we obtain a contradiction by showing that in fact $\tau(S_{<}) \not\geq S_{\neq}$. The difficulty of the proof comes from the scarceness of words in $a^*b^* \setminus S_{\neq}$. This implies some complications reflected by the use of factorials.

For $k \geq 2$, define

$$A_k = \{a^{n!k} b^{n!} \mid n \geq 1\}.$$

We first prove a simple lemma.

Lemma 7.4 *There is no regular language K such that $A_k \subset K \subset S_{\neq}$.*

Proof. Assume the contrary. Then K is infinite, and by the pumping lemma, there is an integer p such that $n \geq p$ implies

$$a^{k \cdot n!} b^{n! + \lambda p} \in K \quad \text{for all } \lambda \geq 0.$$

Since $p \leq n$, p divides $n!$, and $\mu = \frac{n!}{p}(k-1)$ is an integer. Thus $a^{kn!} b^{n! + \mu p} \in K$; since $n! + \mu p = kn!$, the language K is not contained in $S_{\neq}$. ■

Proof of Proposition 7.2. We first sketch the proof. Assuming the existence of a rational transduction mapping $S_{<}$ onto $S_{\neq}$, we first show that there are always arbitrarily long words in $S_{\neq}$ which are images, through the transduction, only of very long words in $S_{<}$. This allows us to assume that words h in the intermediate regular language R contain always enough letters of each kind. In a second step, we apply the pumping lemma in a naive fashion. This gives the result excepted in one case. Then we use the pumping lemma in exactly the same way than in the proof of Proposition 7.1. This also gives the result excepted in one special case. Combining now the two factors supplied by the pumping lemma in these two reserved situations yields the contradiction by the use of the factorials. We now proceed to the formal proof.

a) Assume the result is false. Then there exists a rational transduction $\tau: X^* \rightarrow Y^*$ such that $\tau(S_{<}) = S_{\neq}$. Then this transduction verifies:

$$\begin{aligned} &\text{for each } N \text{ there exists a } n \geq N \text{ such that any word} \\ &x^r y^s \in S_{<} \text{ for which } a^{kn!} b^{n!} \in \tau(x^r y^s) \text{ satisfies } r \geq N. \end{aligned} \quad (7.1)$$

Indeed, assume the contrary; then there is an integer N such that, for any $n \geq N$, there exists some word $x^r y^s \in S_{<}$ with $r < N$ and $a^{kn!} b^{n!} \in \tau(x^r y^s)$. This is equivalent to

$$\{a^{kn!} b^{n!} \mid n \geq N\} \subset \tau(B_N),$$

where $B_N = \{x^r y^s \mid r < N, r < s\}$. The language B_N is regular. For $n = 1, \dots, N-1$, let $w_n \in S_{<}$ be a word such that $a^{kn!} b^{n!} \in \tau(w_n)$; then $B = B_N \cup \{w_1, \dots, w_{N-1}\}$ is a regular language contained in $S_{<}$, and

$$A_k \subset \tau(B) \subset \tau(S_{<}) = S_{\neq}. \quad (7.2)$$

The language $\tau(B)$ is regular, and (7.2) is in contradiction with Lemma 7.4. This proves (7.1).

b) By Nivat's Theorem, there is a regular language $R \subset Z^*$ such that

$$\tau(f) = \beta(\alpha^{-1}(f) \cap R) \quad \text{for } f \in X^*.$$

Let q be the number of states of a finite automaton recognizing R , and fix k (k is the index of the language A_k) to be $k = q! + 1$. Finally take N in (7.1) to

satisfy $N \geq 3q$. In view of (7.1), there is an integer $n \geq N$ such that $a^{kn!}b^{n!} \in \tau(x'y^s)$ with $N \leq r < s$. Let $h \in R$ be a word such that

$$\alpha h = x^r y^s, \quad \beta h = a^{kn!} b^{n!}.$$

c) Let h_1 be the right factor of length q of h . Then $h_1 \in \{y, b\}^q$ since both s and $n!$ are greater than q . By the pumping lemma, h_1 has a factor u with $0 < |u| \leq q$ and such that, by setting

$$h = guh', \quad (7.3)$$

$gu^*h' \in R$, and $|uh'| \leq q$. From $u \in \{y, b\}^*$, it follows that $\alpha(u) \in y^*$, $\beta(u) \in b^*$, thus $\alpha(gu^\lambda h') \in S_<$ for all $\lambda \geq 1$, and thus $\beta(gu^\lambda h') \in S_\neq$ for $\lambda \geq 1$. We shall see that $|\beta(u)| = 0$. Assume $t = |\beta(u)| > 0$; then

$$\beta(gu^\lambda h') = a^{kn!} b^{n! + (\lambda-1)t} \in S_\neq \quad \lambda \geq 1,$$

and t divides $n!$ (since $1 \leq t \leq |u| \leq q \leq N \leq n$); thus $\mu = \frac{n!}{t}(k-1) + 1$ is an integer, and $n! + (\mu-1)t = kn!$; this implies $\beta(gu^\mu h') \notin S_\neq$. (Note that this argument was already used for the proof of Lemma 7.4.) Thus $|\beta(u)| = 0$, and we set $p_u = |\alpha(u)| = |u|_y = |u|$. Then $0 < p_u \leq q$.

d) Consider now the left factor g of h given by (7.3). We have $|g|_b \geq |h|_b - q \geq 2q$. Arguing exactly as in the proof of Proposition 7.1 by a double application of Ogden's iteration lemma to the marked b 's of g , there exists a factorization $g = g'vg''$, and thus a factorization

$$h = g'vg''uh', \quad g'v^*g''u^*h' \in R,$$

with $0 < |v|_b \leq q$, $\alpha(v) \in x^* \cup y^*$, $\beta(v) \in b^*$.

e) Set $p_v = |\alpha(v)|$, $q_v = |v|_b = |\beta(v)|$, and define

$$h_{\lambda\mu} = g'v^{1+\lambda}g''u^{1+\mu}h' \quad (\lambda, \mu \geq 0).$$

If $\alpha(v) \in y^*$, then $\alpha(h_{\lambda,\mu}) \in S_<$ for all $\lambda, \mu \geq 0$, thus $\beta(h_{\lambda,0}) = a^{kn!}b^{n!+\lambda q_v} \in S_\neq$ for $\lambda \geq 0$. By $0 < q_v \leq q$, this leads to a contradiction by the same factorial argument as in c). Thus $\alpha(v) \in x^*$, and

$$\alpha(h_{\lambda,\mu}) = x^{r+\lambda p_v} y^{s+\mu p_u}.$$

Consequently, $h_{\lambda p_u, \mu p_v} \in \alpha^{-1}(S_<) \cap R$ for all λ, μ such that $0 \leq \lambda \leq \mu$. On the other hand,

$$\beta(h_{\lambda,\mu}) = a^{kn!} b^{n!+\lambda q_v}$$

since $|\beta(u)| = 0$. Thus

$$\beta(h_{\lambda p_u, \mu p_v}) = a^{kn!} b^{n!+\lambda p_u q_v} \quad (\lambda, \mu \geq 0).$$

We now use once more the factorial argument: since $p_u \leq q$, p_u divides $k-1 = q!$; since $q_v \leq q \leq n$, q_v divides $n!$. Thus the number $t = \frac{(k-1)n!}{p_u q_v}$ is an integer, and

$$\beta(h_{t p_u, t p_v}) = a^{kn!} b^{kn!} \notin S_\neq.$$

Since $\alpha(h_{t p_u, t p_v}) \in S_<$, this gives the final contradiction. ■

Exercises

7.1 (Ginsburg and Greibach [1969]) Assume that the full AFL generated by a language A is equal to the rational closure of the cone generated by A (Theorem VI.4.10): $A\hat{F} = (A\Gamma)\text{Rat}$. Prove that the full AFLs $S_>\hat{F}$ and $S_<\hat{F}$ are incomparable.

7.2 For rational numbers $0 < r \leq s$ define $M(r, s) \subset \{x, y\}^*$ by

$$M(r, s) = 1 \cup \left\{ x^n y^m \mid n, m \in \mathbb{N} \setminus 0, r \leq \frac{m}{n} \leq s \right\}.$$

- Show that $M(r, s) \approx M(kr, ks)$ for any integer $k > 0$.
- Show that $M(r, s) \approx M(qr, qs)$ for any rational number $q > 0$.
- Show that for rational numbers p, q , $0 < q \leq p < 1$ implies $M(q, 1) \leq M(p, 1)$. (Hint. Use the fact that $M(p, 1) \approx M(p^{n+1}, p^n)$ for integers $n \geq 0$, and that $p^{n+1} < q \leq p^n$ for some integer $n \geq 1$.)
- Show that $M(1, 1) \geq M\left(\frac{k}{k+1}, 1\right)$ for any integer $k > 0$.
- Conclude that $M(q, 1) \leq M(p, 1)$ for all rational numbers p, q such that $0 < q \leq p \leq 1$, and that all languages $M(r, s)$ are linear languages.
- Prove that for $0 < q < 1$, $M(q, 1) > S_>, S_\neq, S_<$.

VI Operators

Operators on families of languages are defined as mappings of families of languages satisfying an additional property which links together the languages in the families. All transformations of families of languages introduced in the preceding chapter are operators in this sense. We develop some general properties of operators. In the last two sections of this chapter, operator calculus is used to derive some fundamental results on cones and full AFLs. By this way, we can separate parts of proofs which are only formal calculations from other parts which rely on a few, more or less standard constructions. The exposition follows Lewis [1970] and Nivat [1975].

VI.1 Operators

In the preceding chapter, we introduced several operations on families of languages, such as closure under rational transduction, substitution and so on. These transformations can be considered as mappings which associate a new family of languages to any given family. Then these mappings can be composed, and the result defines a new operation on families of languages. On the other hand, some of the properties of families of languages proved in the previous chapter are in fact results on transformations. Thus, the equality $\mathcal{L}IT = \mathcal{L}I$ (Proposition V.2.3) means that I is idempotent: $II = I$.

These considerations show that it is natural to investigate functions over the set of all families of languages (over some fixed alphabet Σ), with the aim to find relations between these functions. It is to be expected that the consideration of the totality of these mappings will give no information, since all transformations of families of languages defined up to now are related to transformations of the languages themselves. This relation must be expressed on the level of families of languages. Therefore we consider only transformations ω on families which satisfy the following additional property: any language A in the image of the family $\mathcal{L}$ by ω depends only on a finite number of languages in $\mathcal{L}$. In the first three sections of this chapter, we investigate transformations of this kind. A concrete use of these operators will be made in the last two sections.

Let Σ be a fixed infinite alphabet. We denote by $\mathbb{F}$ the set of all families of languages over Σ in the sense defined in the preceding chapter: any language is contained in the free monoid X^* generated by some finite $X \subset \Sigma$. Let ω be a mapping from $\mathbb{F}$ into $\mathbb{F}$. The image of a family $\mathcal{L} \in \mathbb{F}$ under ω is denoted by $\mathcal{L}\omega$.

It is a family of languages, and in particular closed under copy. If ω_1 and ω_2 are two mappings from $\mathbb{F}$ into itself, the composition is denoted by juxtaposition and is defined by

$$\mathcal{L}(\omega_1\omega_2) = (\mathcal{L}\omega_1)\omega_2 \quad (\mathcal{L} \in \mathbb{F}).$$

This composition is associative, and the identity mapping is a neutral element. We denote it by id .

Definition A mapping $\omega: \mathbb{F} \rightarrow \mathbb{F}$ is called monotone if it satisfies the following condition:

$$\text{for any } \mathcal{L}, \mathcal{M} \in \mathbb{F}, \quad \mathcal{L} \subset \mathcal{M} \Rightarrow \mathcal{L}\omega \subset \mathcal{M}\omega \quad (1.1)$$

Further, ω is locally finite if it verifies:

$$\text{for any } \mathcal{L} \in \mathbb{F}, \text{ and for each } A \in \mathcal{L}\omega, \text{ there is a finite family } \mathcal{L}_A \subset \mathcal{L} \text{ such that } A \in \mathcal{L}_A\omega. \quad (1.2)$$

Recall that a family of languages $\mathcal{M}$ is finite (see Section V.1) if there is a finite number of languages $M_1, \dots, M_n \in \mathcal{M}$ such that each $M \in \mathcal{M}$ is a copy of one of the $M_1, \dots, M_n$.

If in (1.2), the family $\mathcal{L}_A$ is always composed of a single language (and its copies), then ω is called unitary.

Definition A mapping ω from $\mathbb{F}$ into itself is an operator on families of languages if it is both monotone and locally finite. The set of all operators over $\mathbb{F}$ is denoted by Ω .

We first show that Ω is a monoid, and that the set of unitary operators is a submonoid of Ω .

Proposition 1.1 *id is an unitary operator; if ω_1, ω_2 are operators, then $\omega_1\omega_2$ is an operator; further, if ω_1, ω_2 are unitary operators, then $\omega_1\omega_2$ is unitary.*

Proof. Clearly, the identity mapping is monotone and unitary. Let ω_1, ω_2 be operators, and let $\mathcal{L}, \mathcal{M}$ be families of languages. If $\mathcal{L} \subset \mathcal{M}$, then $\mathcal{L}\omega_1 \subset \mathcal{M}\omega_1$, and thus $(\mathcal{L}\omega_1)\omega_2 \subset (\mathcal{M}\omega_1)\omega_2$; thus $\omega_1\omega_2$ is monotone. Next set $\mathcal{M} = \mathcal{L}\omega_1$. Let $A \in \mathcal{M}\omega_2$. Since ω_2 is locally finite, there is a finite family $\mathcal{M}_A = \{M_1, \dots, M_n\} \subset \mathcal{M}$ such that $A \in \mathcal{M}_A\omega_2$. For each $M_i \in \mathcal{M}_A$, there exists a finite family $\mathcal{L}_i \subset \mathcal{L}$ such that $M_i \in \mathcal{L}_i\omega_1$. Let $\mathcal{L}' = \mathcal{L}_1 \cup \mathcal{L}_2 \cup \dots \cup \mathcal{L}_n$. Then $\mathcal{L}'$ is a finite family of languages, and $\mathcal{L}_i\omega_1 \subset \mathcal{L}'\omega_1$ for $i = 1, \dots, n$, by the monotonicity of ω_1 . Thus $M_i \in \mathcal{L}'\omega_1$, ($i = 1, \dots, n$), and $\mathcal{M}_A \subset \mathcal{L}'\omega_1$. Since ω_2 is monotone, this implies $\mathcal{M}_A\omega_2 \subset \mathcal{L}'\omega_1\omega_2$; consequently, $A \in \mathcal{L}'\omega_1\omega_2$. Thus $\omega_1\omega_2$ is locally finite. A similar proof shows that if ω_1 and ω_2 are unitary, then $\omega_1\omega_2$ is also unitary. ■

We now define an order on operators by setting:

$$\omega_1 \leq \omega_2 \Leftrightarrow \mathcal{L}\omega_1 \subset \mathcal{L}\omega_2 \quad \text{for all } \mathcal{L} \in \mathbb{F}.$$

Clearly, $\leq$ is an order relation. No confusion seems possible between this order on operators, and the preorder on languages defined by rational transductions in Section V.2.

We note the formula:

$$\omega_1 \leq \omega_2 \Rightarrow \omega_1 \omega \leq \omega_2 \omega \quad \text{and} \quad \omega \omega_1 \leq \omega \omega_2.$$

Indeed, if $\mathcal{L}\omega_1 \subset \mathcal{L}\omega_2$, then $\mathcal{L}\omega_1 \omega \subset \mathcal{L}\omega_2 \omega$ by the monotonicity of ω . The inclusion $(\mathcal{L}\omega)\omega_1 \subset (\mathcal{L}\omega)\omega_2$ is true by definition.

The most interesting operators are closure operators:

Definition An operator ω is called

- (i) extensive if $\text{id} \leq \omega$, thus if $\mathcal{L} \subset \mathcal{L}\omega$ for $\mathcal{L} \in \mathbb{F}$
- (ii) idempotent if $\omega = \omega\omega$, thus if $(\mathcal{L}\omega)\omega = \mathcal{L}\omega$ for $\mathcal{L} \in \mathbb{F}$
- (iii) a closure operator if it is both extensive and idempotent.

Usually, a closure operator with respect to some order is a mapping which is extensive, monotone and idempotent. In the present case, monotonicity is supplied by definition.

Exercises

1.1 Let $\mathcal{L}_0 = \{A_0\}$ be the family consisting of the single language A_0 . Let ω be defined by $\mathcal{L}\omega = \mathcal{L}_0$ for $\mathcal{L} \in \mathbb{F}$. Show that ω is an idempotent, unitary operator which is not extensive.

1.2 Let ω be a closure operator, $\mathcal{L}, \mathcal{M}$ be families of languages. Show that $(\mathcal{L} \cup \mathcal{M})\omega = (\mathcal{L}\omega \cup \mathcal{M}\omega)\omega$.

1.3 Let ω be an unitary operator. Show that for all sets $(\mathcal{L}_i)_{i \in I}$ of families,

$$\left(\bigcup_{i \in I} \mathcal{L}_i \right) \omega = \bigcup_{i \in I} (\mathcal{L}_i \omega).$$

VI.2 Examples of Operators

We list here the principal operators and some simple relations between operators.

2.1 Φ is the “morphism” operator defined by

$$\mathcal{L}\Phi = \{\varphi(L) \mid L \in \mathcal{L}, \varphi: X_L^* \rightarrow Y^* \text{ a morphism}\}.$$

Φ is a unitary closure operator.

2.2 Φ^{-1} is the “inverse morphism” operator defined by

$$\mathcal{L}\Phi^{-1} = \{\varphi^{-1}(L) \mid L \in \mathcal{L}, \varphi: Y^* \rightarrow X_L^* \text{ a morphism}\}.$$

Φ^{-1} also is a unitary closure operator.

2.3 The operators

$$\begin{array}{ll} \Phi_a : \text{alphabetic morphism;} & \Phi_a^{-1} : \text{inverse alphabetic morphism;} \\ \Phi_\pi : \text{projection;} & \Phi_\pi^{-1} : \text{inverse projection} \end{array}$$

are defined as Φ and Φ^{-1} , by replacing morphism by alphabetic morphism and projection. They are all unitary closure operators.

2.4 I_R is the operator “intersection with regular sets” defined by

$$\mathcal{L}I_R = \{L \cap K \mid L \in \mathcal{L}, K \in \text{Rat}\}.$$

Clearly I_R is monotone and unitary. Since the intersection of two regular languages is regular, I_R is a closure operator.

2.5 Γ is the operator of closure under rational transduction:

$$\mathcal{L}\Gamma = \{L' \mid \exists L \in \mathcal{L}, L \geq L'\}.$$

Clearly, Γ is an unitary operator, and Γ is a closure operator by Proposition V.2.3.

Recall (see Section V.5) that if $\mathcal{L}, \mathcal{M}$ are families of languages, we introduced two unary notations for the substitution $\mathcal{L} \square \mathcal{M}$ by setting

$$\mathcal{L} \square \mathcal{M} = \mathcal{L}\bar{\mathcal{M}} = \mathcal{M}\mathcal{L}.$$

This yields two mappings $\bar{\mathcal{M}}$ and $\mathcal{L}$.

2.6 $\bar{\mathcal{M}}$ is an operator for any family $\mathcal{M}$.

Indeed, $\bar{\mathcal{M}}$ is monotone by formula (V.5.2); further, if $A \in \mathcal{L}\bar{\mathcal{M}}$, then $A = \sigma(L)$ for some language $L \in \mathcal{L}$ and some $\mathcal{M}$ -substitution σ . Thus, $A \in \{L\}\bar{\mathcal{M}}$ and $\bar{\mathcal{M}}$ is unitary. In general, $\bar{\mathcal{M}}$ is not a closure operator.

2.7 $\underline{\mathcal{L}}$ is an operator for any family $\mathcal{L}$.

Indeed, $\underline{\mathcal{L}}$ is monotone by formula (V.5.1); and if $A \in \mathcal{M}\underline{\mathcal{L}} = \underline{\mathcal{L}}\bar{\mathcal{M}}$, then $A = \sigma(L)$, where $L \in \mathcal{L}$ and $\sigma: X_L^* \rightarrow Y^*$ is some $\mathcal{M}$ -substitution. Thus $A \in \mathcal{M}_A \underline{\mathcal{L}}$, where $\mathcal{M}_A = \{\sigma(x) : x \in X_L\}$. In general, $\underline{\mathcal{L}}$ is not unitary. This is the reason why we cannot restrict to unitary operators.

2.8 Rat , Fin , Elm are closure operators.

2.9 $\hat{\Gamma}$ is the “full AFL” operator.

Clearly, $\hat{\Gamma}$ is monotone. To show that $\hat{\Gamma}$ is locally finite, consider a family of languages $\mathcal{L}$, and a language $A \in \mathcal{L}\hat{\Gamma}$. Then A has been obtained from languages in $\mathcal{L}$ by a finite number of rational transductions and rational operations. Thus there is a finite family $\mathcal{L}_A \subset \mathcal{L}$ such that $A \in \mathcal{L}_A \hat{\Gamma}$. Thus $\hat{\Gamma}$ is locally finite; moreover $\hat{\Gamma}$ is a closure operator. Note that we shall prove in Section 4 the equality $\hat{\Gamma} = \Gamma \text{Rat}$; this shows a posteriori that $\hat{\Gamma}$ is an operator.

We now give some examples of relations between operators.

1. Nivat's Theorem gives

$$\Gamma = \Phi^{-1} I_R \Phi = \Phi_a^{-1} I_R \Phi_a = \Phi_\pi^{-1} I_R \Phi_\pi.$$

2. The inequalities $\Phi^{-1}, I_R \Phi, \overline{\text{Rat}} \leq \Gamma$ hold since inverse morphisms, morphisms, intersection with regular sets, rational substitutions are special cases of rational transductions.

3. The associativity of the substitution $\mathcal{L} \square \mathcal{M}$ gives the commutativity formula:

$$\mathcal{L} \tilde{\mathcal{M}} = \tilde{\mathcal{M}} \mathcal{L}. \quad (2.1)$$

This is precisely Corollary V.5.3.

4. If $\mathcal{L}_i$, ($i \in I$) are cones, then $\bigcup_{i \in I} \mathcal{L}_i$ is a cone. Indeed, Γ is unitary, and by Exercise 1.3,

$$\left(\bigcup_{i \in I} \mathcal{L}_i \right) \Gamma = \bigcup_{i \in I} (\mathcal{L}_i \Gamma) = \bigcup_{i \in I} \mathcal{L}_i.$$

(This is not true for the full AFL operator $\hat{\Gamma}$, see Exercise V.4.2: $\hat{\Gamma}$ is not unitary.)

Exercises

2.1 Let $\mathcal{M}$ be a family of languages. Show that if $\{x\} \in \mathcal{M}$ for $x \in \Sigma$, then $\underline{\mathcal{M}}$ and $\tilde{\mathcal{M}}$ are extensive.

2.2 Give an example of two closure operators ω_1, ω_2 such that $\omega_1 \omega_2$ is not idempotent, and thus is not a closure operator (this shows that the theorem of Elgot and Mezei about the idempotency of Γ cannot be obtained as a formal consequence of Nivat's Theorem).

VI.3 Closure Operators

Let $\mathcal{L}$ be a family of languages, and let ω be an operator. Suppose $\mathcal{L}$ is not closed under ω (i.e. $\mathcal{L}\omega$ is not contained in $\mathcal{L}$). In some cases, there exists a least family $\mathcal{L}'$ containing $\mathcal{L}$ and closed under ω . This defines a new operator ω^* which associates $\mathcal{L}'$ to $\mathcal{L}$, and ω^* is a closure operator.

In this section, we give an explicit construction of the closure operator ω^* , and more generally of the operator $\{\omega_1, \dots, \omega_k\}^*$ which associates to a family $\mathcal{L}$ the least family of languages containing $\mathcal{L}$ and closed under $\omega_1, \dots, \omega_k$. The main result of this section is a particularly simple expression of $\{\omega_1, \dots, \omega_k\}^*$ which holds provided $\omega_1, \dots, \omega_k$ are closure operators satisfying some relations of commutation.

The reader will observe that the results of this section do not use the fact that the objects under consideration are families of languages. Similarly, the local finiteness of operators is only used to derive a "continuity" property. In fact, all computations are valid in the much more general framework of the lattice of continuous functions over a complete lattice, and lead to rather well-known results in this algebraic structure. We prefer to restrict ourselves to the special case of families of languages and to prove directly the few results necessary in the sequel. (The reader interested in the general theory may consult, e.g. Maeda and Maeda [1974]).

The set $\mathbb{F}$ of all families of languages is a complete semi-lattice for the union. It would be a complete lattice if the empty family would be added. The first lemma shows that operators are upper-continuous mappings.

Lemma 3.1 (Continuity) *Let $\mathcal{L}_1 \subset \mathcal{L}_2 \subset \dots \subset \mathcal{L}_n \subset \dots$ be an increasing sequence of families of languages, and let ω be an operator. Then*

$$\left(\bigcup_{i \geq 1} \mathcal{L}_i \right) \omega = \bigcup_{i \geq 1} (\mathcal{L}_i \omega) \quad (3.1)$$

Proof. Set $\mathcal{L} = \bigcup_{i \geq 1} \mathcal{L}_i$. For any $i \geq 1$, $\mathcal{L}_i \subset \mathcal{L}$; consequently $\mathcal{L}_i \omega \subset \mathcal{L} \omega$ since ω is monotone. Thus $\bigcup_{i \geq 1} \mathcal{L}_i \omega \subset \mathcal{L} \omega$.

Conversely, let $A \in \mathcal{L} \omega$. Since ω is locally finite, there is a finite family $\mathcal{L}_A \subset \mathcal{L}$ such that $A \in \mathcal{L}_A \omega$. Since the sequence $(\mathcal{L}_i)_{i \geq 1}$ is increasing, there is an integer k such that $\mathcal{L}_A \subset \mathcal{L}_k$. Using monotonicity once more, this yields $A \in \mathcal{L}_k \omega$. Thus $\mathcal{L} \omega \subset \bigcup_{i \geq 1} \mathcal{L}_i \omega$. ■

Note that if ω is unitary, then (3.1) holds without the assumption that the sequence is increasing (Exercise 1.3).

Let ω be an operator. A family of languages $\mathcal{L}$ is closed under ω if $\mathcal{L} \omega \subset \mathcal{L}$. If ω is extensive, this is equivalent to $\mathcal{L} \omega = \mathcal{L}$. If ω is a closure operator, then $\mathcal{L} \omega$ is always closed under ω . Our aim is to define the operator of closure under ω .

To any set $(\omega_i)_{i \in I}$ of operators, we associate a mapping denoted by $\bigcup_{i \in I} \omega_i$ and defined by

$$\mathcal{L} \left(\bigcup_{i \in I} \omega_i \right) = \bigcup_{i \in I} (\mathcal{L} \omega_i) \quad \mathcal{L} \in \mathbb{F}.$$

To verify that $\omega = \bigcup_{i \in I} \omega_i$ is an operator, we first observe that ω is clearly monotone. ω is also locally finite. Indeed, let $A \in \mathcal{L} \omega = \bigcup_{i \in I} (\mathcal{L} \omega_i)$. Then there

exists an index $k \in I$ such that $A \in \mathcal{L}\omega_k$. Since ω_k is locally finite, $A \in \mathcal{L}_A\omega_k$ for some finite family $\mathcal{L}_A \subset \mathcal{L}$. Then $A \in \bigcup_{i \in I} (\mathcal{L}_A\omega_i) = \mathcal{L}_A\omega$.

If I is finite, $I = \{i_1, \dots, i_r\}$, we write

$$\bigcup_{i \in I} \omega_i = \omega_{i_1} \cup \omega_{i_2} \cup \dots \cup \omega_{i_r}.$$

In particular, $\omega \leq \omega'$ iff $\omega' = \omega \cup \omega'$.

Definition Let ω be an operator; then ω^* is the operator defined by

$$\omega^* = \bigcup_{n \geq 0} \omega^n,$$

where $\omega^0 = \text{id}$.

Proposition 3.2 Let ω be an extensive operator; then ω^* is a closure operator. For any family of languages $\mathcal{L}$, $\mathcal{L}\omega^*$ is the least family of languages containing $\mathcal{L}$ and closed under ω ; moreover, $\mathcal{L}\omega^*$ is closed under ω^* .

Proof. Let $\mathcal{L}$ be a family of languages. Then

$$\mathcal{L} \subset \bigcup_{n \geq 0} \mathcal{L}\omega^n = \mathcal{L}\omega^*,$$

showing that ω^* is extensive. We show that $\mathcal{L}\omega^*$ is closed under ω . Since ω is extensive, the sequence $(\mathcal{L}\omega^n)_{n \geq 0}$ is increasing. Thus by the continuity lemma,

$$\mathcal{L}\omega^*\omega = \left(\bigcup_{n \geq 0} \mathcal{L}\omega^n \right) \omega = \bigcup_{n \geq 0} \mathcal{L}\omega^n\omega = \bigcup_{n \geq 1} \mathcal{L}\omega^n = \bigcup_{n \geq 0} \mathcal{L}\omega^n = \mathcal{L}\omega^*. \quad (3.2)$$

Next, let $\mathcal{M}$ be a family of languages containing $\mathcal{L}$ and closed under ω . Since ω is monotone, $\mathcal{L}\omega^n \subset \mathcal{M}\omega^n = \mathcal{M}$ for $n \geq 0$, and $\mathcal{L}\omega^* \subset \mathcal{M}$, showing that $\mathcal{L}\omega^*$ is the least family containing $\mathcal{L}$ and closed under ω . Finally, we verify that ω^* is idempotent. By (3.2), $\omega^*\omega = \omega^*$. Therefore, $\omega^*\omega^n = \omega^*$ for any $n \geq 0$. Thus

$$\mathcal{L}\omega^*\omega^* = \bigcup_{n \geq 0} (\mathcal{L}\omega^*)\omega^n = \mathcal{L}\omega^*. \quad \blacksquare$$

Example 3.1 Let $\mathcal{M}$ be a family of languages such that $\{x\} \in \mathcal{M}$ for $x \in \Sigma$. Then $\mathcal{M}$ is extensive (Exercise 2.1). For any family of languages $\mathcal{L}$, the family

$$\mathcal{L}(\bar{\mathcal{M}})^* = \bigcup_{n \geq 0} \mathcal{L}(\bar{\mathcal{M}})^n$$

is the least family of languages containing $\mathcal{L}$ and closed under $\mathcal{M}$ -substitution.

In particular, $\mathcal{M}\bar{\mathcal{M}}^*$ is the least family containing $\mathcal{M}$ and closed under $\mathcal{M}$ -substitution. We prove that $\mathcal{M}\bar{\mathcal{M}}^*$ is closed under substitution, i.e. under $\mathcal{M}\bar{\mathcal{M}}^*$ -substitution. For this, we first extend formula (2.1) and show

$$\bar{\mathcal{M}}^*\bar{\mathcal{N}} = \bar{\mathcal{N}}\bar{\mathcal{M}}^* \quad (\bar{\mathcal{M}} \text{ extensive}). \quad (3.3)$$

Indeed, the formula $\bar{\mathcal{M}}\bar{\mathcal{N}} = \bar{\mathcal{N}}\bar{\mathcal{M}}$ implies, by induction,

$$\bar{\mathcal{M}}^n\bar{\mathcal{N}} = \bar{\mathcal{N}}\bar{\mathcal{M}}^n \quad (n \geq 0).$$

For any family $\mathcal{L}$, $(\mathcal{L}\bar{\mathcal{M}}^n)_{n \geq 0}$ is an increasing sequence since $\bar{\mathcal{M}}$ is extensive; by continuity

$$\mathcal{L}\bar{\mathcal{M}}^*\bar{\mathcal{N}} = \bigcup_{n \geq 0} \mathcal{L}(\bar{\mathcal{M}}^n\bar{\mathcal{N}}) = \bigcup_{n \geq 0} \mathcal{L}\bar{\mathcal{N}}\bar{\mathcal{M}}^n = \mathcal{L}\bar{\mathcal{N}}\bar{\mathcal{M}}^*.$$

This proves (3.3).

Corollary 3.3 Let $\mathcal{M}$ be a family of languages such that $\{x\} \in \mathcal{M}$ for $x \in \Sigma$; then $\mathcal{M}\bar{\mathcal{M}}^*$ is closed under substitution.

Proof. We have

$$\mathcal{M}\bar{\mathcal{M}}^*\bar{\mathcal{M}}\bar{\mathcal{M}}^* = \mathcal{M}\bar{\mathcal{M}}^*\bar{\mathcal{M}}\bar{\mathcal{M}}^* = \mathcal{M}\bar{\mathcal{M}}\bar{\mathcal{M}}^*\bar{\mathcal{M}}^*$$

by (3.3). Further,

$$\mathcal{M}\bar{\mathcal{M}}\bar{\mathcal{M}}^*\bar{\mathcal{M}}^* = \mathcal{M}\bar{\mathcal{M}}^*\bar{\mathcal{M}}\bar{\mathcal{M}}^*.$$

Now $\bar{\mathcal{M}}^*\bar{\mathcal{M}} = \bar{\mathcal{M}}^*\bar{\mathcal{M}}^* = \bar{\mathcal{M}}^*$ by Proposition 3.2, thus

$$\mathcal{M}\bar{\mathcal{M}}^*\bar{\mathcal{M}}\bar{\mathcal{M}}^* = \mathcal{M}\bar{\mathcal{M}}^*. \quad \blacksquare$$

We now extend Proposition 3.2 to the case of several operators. Let $\omega_1, \dots, \omega_k$, ($k \geq 1$) be operators. Define $\mathbb{k} = \{1, 2, \dots, k\}$, and for a word

$$f = i_1 i_2 \dots i_n \in \mathbb{k}^+ \quad (i_1, \dots, i_n \in \mathbb{k}),$$

set $\omega_f = \omega_{i_1} \omega_{i_2} \dots \omega_{i_n}$.

Finally, let ε be the empty word of $\mathbb{k}^*$ and set $\omega_\varepsilon = \text{id}$.

Definition Let $\omega_1, \omega_2, \dots, \omega_k$ be operators; then $\{\omega_1, \omega_2, \dots, \omega_k\}^*$ is the operator defined by

$$\{\omega_1, \omega_2, \dots, \omega_k\}^* = \bigcup_{f \in \mathbb{k}^*} \omega_f.$$

Proposition 3.4 Let $\omega_1, \dots, \omega_k$ be extensive operators; then $\{\omega_1, \dots, \omega_k\}^*$ is a closure operator. For any family of languages $\mathcal{L}$, $\mathcal{L}\{\omega_1, \dots, \omega_k\}^*$ is the least family of languages containing $\mathcal{L}$ and closed under $\omega_1, \dots, \omega_k$; moreover, $\mathcal{L}\{\omega_1, \dots, \omega_k\}^*$ is closed under $\{\omega_1, \dots, \omega_k\}^*$.

Proof. Let $\omega = \{\omega_1, \dots, \omega_k\}^*$. Clearly ω is extensive. We show that $\omega\omega_i = \omega$ for $i = 1, \dots, k$. First note that, since each ω_i is extensive, $\omega_f \leq \omega_g$ for any subword f of g , ($f, g \in \mathbb{k}^*$).

Let $\mathcal{L}$ be a family of languages and define

$$\mathcal{L}^{(n)} = \bigcup_{f \in \mathbb{k}^n} \mathcal{L}\omega_f.$$

The sequence $(\mathcal{L}^{(n)})_{n \geq 0}$ is increasing; thus by continuity

$$\mathcal{L}\omega_i = \left(\bigcup_{n \geq 0} \mathcal{L}^{(n)} \right) \omega_i = \bigcup_{n \geq 0} \mathcal{L}^{(n)} \omega_i \quad i = 1, \dots, k. \quad (3.4)$$

Note that the inclusion $\mathcal{L}^{(n)} \omega_i \subset \mathcal{L}^{(n+1)}$ is not necessarily true except if ω_i is unitary, since in that case ω_i can be passed through the union. Let g be the word of length nk^n obtained by concatenating all words of $\mathbb{K}^n$. Then $\mathcal{L}\omega_f \subset \mathcal{L}\omega_g$ for all $f \in \mathbb{K}^n$, therefore

$$\mathcal{L}^{(n)} \subset \mathcal{L}\omega_g$$

and $\mathcal{L}^{(n)} \omega_i \subset \mathcal{L}\omega_g \omega_i = \mathcal{L}\omega_{gi} \subset \mathcal{L}\omega$. (3.5)

By (3.4) and (3.5), we have $\mathcal{L}\omega_i = \mathcal{L}\omega$ for $i = 1, \dots, k$, showing that $\mathcal{L}\omega$ is closed under $\omega_1, \dots, \omega_k$. Consequently, $\omega\omega_f = \omega$ for all $f \in \mathbb{K}^*$, and

$$\mathcal{L}\omega = \bigcup_{f \in \mathbb{K}^*} \mathcal{L}\omega\omega_f = \mathcal{L}\omega.$$

Thus ω is idempotent. Finally, let $\mathcal{M}$ be a family of languages containing $\mathcal{L}$ and closed under $\omega_1, \dots, \omega_k$. Then $\mathcal{L}\omega_f \subset \mathcal{M}\omega_f = \mathcal{M}$ for $f \in \mathbb{K}^*$, and therefore $\mathcal{L}\omega \subset \mathcal{M}$. This achieves the proof. ■

Example 3.2 Let $\omega_1 = \Gamma$, $\omega_2 = \text{Rat}$. Then $\mathcal{L}\{\Gamma, \text{Rat}\}^*$ is the least family containing $\mathcal{L}$ and closed under Γ and Rat . Thus $\{\Gamma, \text{Rat}\}^* = \hat{\Gamma}$, and

$$\hat{\Gamma} = \bigcup_{n \geq 1} \omega_{i_1} \omega_{i_2} \cdots \omega_{i_n}, \quad \text{with } \omega_{i_i} = \Gamma \text{ or } \omega_{i_i} = \text{Rat}.$$

We now show that the operator $\{\omega_1, \dots, \omega_k\}^*$ has a very simple form, provided certain conditions are verified.

Theorem 3.5 Let $\omega_1, \omega_2, \dots, \omega_k$ be closure operators; if $\omega_i \omega_j \leq \omega_j \omega_i$ for $1 \leq i < j \leq k$, then

$$\{\omega_1, \omega_2, \dots, \omega_k\}^* = \omega_1 \omega_2 \cdots \omega_k.$$

Proof. Clearly $\omega_1 \omega_2 \cdots \omega_k \leq \bigcup_{f \in \mathbb{K}^*} \omega_f$. Conversely, let $f = i_1 i_2 \cdots i_n \in \mathbb{K}^n$.

If $i_1 > i_2$, then $\omega_{i_1} \omega_{i_2} \leq \omega_{i_2} \omega_{i_1}$. Thus $\omega_f \leq \omega_{i_2} \omega_{i_1} \cdots \omega_{i_n}$. Comparing then i_3 to i_1 and so on yields finally

$$\omega_f \leq \omega_{j_1} \omega_{j_2} \cdots \omega_{j_n},$$

where $1 \leq j_1 \leq j_2 \leq \cdots \leq j_n \leq k$ and $(j_1, \dots, j_n)$ is a permutation of $(i_1, \dots, i_n)$. Using the idempotency and the extensivity of $\omega_1, \dots, \omega_k$, we obtain

$$\omega_{j_1} \omega_{j_2} \cdots \omega_{j_n} \leq \omega_1 \cdots \omega_k.$$

Thus $\omega_f \leq \omega_1 \cdots \omega_k$ for any $f \in \mathbb{K}^*$; therefore

$$\{\omega_1, \dots, \omega_k\}^* \leq \omega_1 \omega_2 \cdots \omega_k. \quad \blacksquare$$

Example 3.2 (continued). In order to prove the equality $\hat{\Gamma} = \Gamma \text{Rat}$, it suffices, in view of Theorem 3.5, to show the inequality $\text{Rat} \Gamma \leq \Gamma \text{Rat}$. This will be done in the next section.

Exercises

3.1 Let $\omega_1, \omega_2, \dots, \omega_k$ be extensive operators. Show that

$$\{\omega_1, \dots, \omega_k\}^* = \bar{\omega}^*$$

where $\bar{\omega} = \omega_1 \cup \omega_2 \cup \cdots \cup \omega_k$.

3.2 Let Word be the family of all words of Σ^* . Show that Word is the operator of closure under product. Show that $\text{Elm Word} \leq \text{Word Elm}$, and prove that $\text{Fin} = \text{Word Elm}$.

VI.4 Subcommutative Relations

In this section, we use the results of the preceding section, and especially Theorem 3.5 to derive relations between some frequently appearing operators. As a result, we obtain that the operations defining cones and full AFLs can always be applied in some specific order. For this, we use standard techniques from formal language theory to prove some inequalities between fundamental operators; from these, other relations can then be deduced in a completely formal way.

As an illustration, we first reformulate several results of Chapter III as relations between operators.

Proposition 4.1 $\Gamma = \Phi^{-1} I_R \Phi = \Phi_a^{-1} I_R \Phi_a = \Phi_\pi^{-1} I_R \Phi_\pi$.

This is the theorem of Nivat (Theorem III.4.1).

Proposition 4.2 $\Gamma \Gamma = \Gamma$.

This is the theorem of Elgot and Mezei (Theorem III.4.4). We give the proof of the theorem once more, but using now operators. We need the following three lemmas.

Lemma 4.3 $\Phi_\pi \Phi_\pi^{-1} \leq \Phi_\pi^{-1} \Phi_\pi$.

This is just Lemma III.4.5.

Lemma 4.4 $I_R \Phi^{-1} \leq \Phi^{-1} I_R$, $I_R \Phi_a^{-1} \leq \Phi_a^{-1} I_R$, $I_R \Phi_\pi^{-1} \leq \Phi_\pi^{-1} I_R$.

Proof. We prove the first inequality. Let $\mathcal{L}$ be a family of languages, and let $A \in \mathcal{L} I_R \Phi^{-1}$. Thus there exist a language $L \in \mathcal{L}$, a regular language $K \subset X_L^*$, and a morphism $\varphi: X_A^* \rightarrow X_L^*$ such that $A = \varphi^{-1}(L \cap K)$. Thus $A = \varphi^{-1}(L) \cap \varphi^{-1}(K)$, and since $\varphi^{-1}(L) \in \mathcal{L} \Phi^{-1}$ and $\varphi^{-1}(K) \in \text{Rat}$, we have $A \in \mathcal{L} \Phi^{-1} I_R$, showing that $\mathcal{L} I_R \Phi^{-1} \subset \mathcal{L} \Phi^{-1} I_R$. ■

Lemma 4.5 $\Phi I_R \leq I_R \Phi$; $\Phi_a I_R \leq I_R \Phi_a$; $\Phi_\pi I_R \leq I_R \Phi_\pi$.

Proof. We prove the first inequality. Let $\mathcal{L}$ be a family of languages, and let $A \in \mathcal{L} \Phi I_R$. Thus there exist a language $L \in \mathcal{L}$, a morphism $\varphi: X_L^* \rightarrow X_A^*$ and $K \in \text{Rat}(X_A^*)$ such that $A = \varphi(L) \cap K$. Now

$$A = \varphi(L \cap \varphi^{-1}(K)),$$

and since $\varphi^{-1}(K) \in \text{Rat}(X_L^*)$, we get $A \in \mathcal{L} I_R \Phi$. This shows that $\mathcal{L} \Phi I_R \subset \mathcal{L} I_R \Phi$. ■

The proof of Elgot and Mezei's theorem can now be rewritten as follows:

$$\begin{aligned} \Gamma \Gamma &= \Phi_\pi^{-1} I_R \Phi_\pi \Phi_\pi^{-1} I_R \Phi_\pi && \text{(Nivat's Theorem)} \\ &\leq \Phi_\pi^{-1} I_R \Phi_\pi^{-1} \Phi_\pi I_R \Phi_\pi && \text{(Lemma 4.3)} \\ &\leq \Phi_\pi^{-1} \Phi_\pi^{-1} I_R I_R \Phi_\pi \Phi_\pi && \text{(Lemma 4.4 and 4.5)} \\ &= \Phi_\pi^{-1} I_R \Phi_\pi = \Gamma. && \text{(idempotency)} \end{aligned}$$

Since clearly $\Gamma \Gamma \geq \Gamma$, we finally get $\Gamma = \Gamma \Gamma$.

Remark. The three Lemmas 4.3, 4.4 and 4.5 imply, in view of Theorem 3.5, the equality

$$\{\Phi_\pi^{-1}, I_R, \Phi_\pi\}^* = \Phi_\pi^{-1} I_R \Phi_\pi.$$

Since $\{\Phi_\pi^{-1}, I_R, \Phi_\pi\}^*$ is a closure operator, it is idempotent, and this shows directly that $\Gamma \Gamma = \Gamma$. On the other hand, by the equality $\Gamma = \{\Phi_\pi^{-1}, I_R, \Phi_\pi\}^*$ we see directly that for any family $\mathcal{L}$, $\mathcal{L} \Gamma$ is the least family containing and closed by inverse projection, intersection with rational languages, and projection.

We now investigate similar relations involving substitutions. First, we prove

Lemma 4.6 $\text{Elm } \Gamma \leq \Gamma \text{Elm}$.

Proof. Let $\mathcal{L}$ be a family of languages, and $A \in \mathcal{L} \text{Elm } \Gamma$. Then there exist a language $B \in \mathcal{L} \text{Elm}$ and a rational transduction $\tau: X_B^* \rightarrow X_A^*$ such that $A = \tau(B)$. Since $B \in \mathcal{L} \text{Elm}$, there is an integer $n \geq 0$ such that

$$B = \bigcup_{1 \leq i \leq n} L_i \quad L_i \in \mathcal{L}, \quad i = 1, \dots, n.$$

This implies $\tau(B) = \bigcup_{1 \leq i \leq n} \tau(L_i)$, and since $\tau(L_i) \in \mathcal{L} \Gamma$ for $i = 1, \dots, n$, we finally get $A \in \mathcal{L} \Gamma \text{Elm}$. ■

Theorem 4.7 $\{\Gamma, \text{Elm}\}^* = \Gamma \text{Elm}$, or equivalently: The full semi-AFL generated by a family of languages $\mathcal{L}$ is equal to the closure under union of the rational cone generated by $\mathcal{L}$.

Proof. This follows from Theorem 3.5 in view of the preceding lemma. ■

We now want to show that Theorem 4.7 remains true when Elm is replaced by Rat, and more precisely that the equality $\mathcal{L} \hat{\Gamma} = \mathcal{L} \Gamma \text{Rat}$ holds for any family of

languages $\mathcal{L}$. We need only to prove that $\mathcal{L} \Gamma \text{Rat}$ is a cone, and for this, it suffices to show the inequality $\text{Rat } \Gamma \leq \Gamma \text{Rat}$. Writing $\Gamma = \Phi^{-1} I_R \Phi$, we have to “pass” the operator Rat through the three operators Φ^{-1} , I_R , Φ . This will be done by proving three inequalities, each one involving one of these three operators. It appears that the operator Rat can be replaced, with only minor changes, by any operator of the form $\mathcal{L}$; this gives, as a corollary, another important property of cones. Therefore, we show the more general

Proposition 4.8 Let $\mathcal{L}$ be a family of languages; then

$$\mathcal{L} \Gamma \leq \Gamma \mathcal{L} \Gamma \quad \text{or equivalently} \quad \bar{\mathcal{L}} \Gamma \leq \Gamma \bar{\mathcal{L}} \Gamma.$$

First, we note the following

Corollary 4.9 $\text{Rat } \Gamma \leq \Gamma \text{Rat}$.

Proof. By Proposition 4.8, we have $\text{Rat } \Gamma \leq \Gamma \text{Rat } \Gamma$, and since Rat is a cone, $\text{Rat } \Gamma = \text{Rat}$. ■

Using Theorem 3.5, this corollary implies the following theorem

Theorem 4.10 (Ginsburg and Greibach [1969]) $\hat{\Gamma} = \{\Gamma, \text{Rat}\}^* = \Gamma \text{Rat}$ or equivalently: The full AFL generated by a family of languages $\mathcal{L}$ is equal to the rational closure of the cone generated by $\mathcal{L}$. ■

By this result, AFL-properties can be separated in properties of rational cones, and in properties of rational closure.

For the proof of Proposition 4.8 we need three lemmas. The first lemma involves morphisms.

Lemma 4.11 Let $\mathcal{L}$ be a family of languages; then

$$\mathcal{L} \Phi_\pi = \Phi_\pi \mathcal{L}; \quad \mathcal{L} \Phi_a = \Phi_a \mathcal{L}; \quad \mathcal{L} \Phi = \Phi \mathcal{L}$$

or equivalently

$$\bar{\mathcal{L}} \Phi_\pi = \bar{\mathcal{L}} \Phi_\pi; \quad \bar{\mathcal{L}} \Phi_a = \bar{\mathcal{L}} \Phi_a; \quad \bar{\mathcal{L}} \Phi = \bar{\mathcal{L}} \Phi.$$

Proof. Let $\mathcal{M}$ be a family of languages; then

$$\mathcal{M} \mathcal{L} \Phi = \mathcal{M} \Phi \mathcal{L} \Leftrightarrow \mathcal{L} \bar{\mathcal{M}} \Phi = \mathcal{L} \bar{\mathcal{M}}.$$

Thus the two sequences of formulas are equivalent.

Let $A \in \mathcal{L} \bar{\mathcal{M}} \Phi$. Then there exist a language $B \in \mathcal{L} \bar{\mathcal{M}}$, and a morphism $\varphi: X_B^* \rightarrow X_A^*$ such that $A = \varphi(B)$. Since $B \in \mathcal{L} \bar{\mathcal{M}}$, there are a language $L \in \mathcal{L}$, and a $\mathcal{M}$ -substitution $\sigma: X_L^* \rightarrow X_B^*$ with $B = \sigma(L)$. Thus $A = (\varphi \circ \sigma)(L)$. Now $\varphi \circ \sigma: X_L^* \rightarrow X_A^*$ is a $\mathcal{M} \Phi$ -substitution since $\varphi \sigma(z) \in \mathcal{M} \Phi$ for each $z \in X_L$. This shows that $A \in \mathcal{L} \mathcal{M} \Phi$. Thus $\mathcal{L} \bar{\mathcal{M}} \Phi \subset \mathcal{L} \mathcal{M} \Phi$.

Conversely, let $A \in \mathcal{L} \mathcal{M} \Phi$. Then there exist a language $L \in \mathcal{L}$, and a $\mathcal{M} \Phi$ -substitution $\sigma: X_L^* \rightarrow X_A^*$ with $A = \sigma(L)$. For each $z \in X_L$, there exist an

alphabet Y_z , a language $M_z \subset Y_z^*$, $M_z \in \mathcal{M}$, and a morphism $\varphi_z: Y_z^* \rightarrow X_A^*$ such that $\sigma(z) = \varphi_z(M_z)$. By copying if necessary, we may suppose the alphabets Y_z , ($z \in X_L$) pairwise disjoint. Set

$$Y = \bigcup_{z \in X_L} Y_z,$$

and define a morphism $\varphi: Y^* \rightarrow X_A^*$ by $\varphi(y) = \varphi_z(y)$ iff $y \in Y_z$. Finally, define a substitution

$$\sigma': X_L^* \rightarrow Y^*$$

by $\sigma'(z) = M_z$ for $z \in X_L$. Then $\sigma = \varphi \circ \sigma'$. Since σ' is a $\mathcal{M}$ -substitution, it follows that $A = \varphi(\sigma'(L)) \in \mathcal{L}\bar{\mathcal{M}}\Phi$, and thus $\mathcal{L}\bar{\mathcal{M}}\Phi \subset \mathcal{L}\bar{\mathcal{M}}\Phi$. The proofs of the two other identities are similar. ■

The second lemma handles inverse morphism. The situation is complicated by the fact that inverse morphisms are not substitutions.

Lemma 4.12 *Let $\mathcal{L}$ be a family of languages; then*

$$\mathcal{L}\Phi_\pi^{-1} \leq \mathcal{L}\Phi_a^{-1} \leq \Gamma\mathcal{L}\Phi_\pi^{-1} \quad \text{or equivalently} \quad \bar{\mathcal{L}}\Phi_\pi^{-1} \leq \bar{\mathcal{L}}\Phi_a^{-1} \leq \Phi_\pi^{-1}\bar{\mathcal{L}}\Gamma.$$

Proof. Let $\mathcal{M}$ be a family of languages. Then

$$\mathcal{L}\mathcal{M}\Phi_a^{-1} \subset \mathcal{M}\Gamma\mathcal{L}\Phi_\pi^{-1} \Leftrightarrow \mathcal{L}\bar{\mathcal{M}}\Phi_a^{-1} \subset \mathcal{L}\Phi_\pi^{-1}\bar{\mathcal{M}}\Gamma.$$

This shows that the two sets of inequalities are equivalent. The inequality $\mathcal{L}\Phi_\pi^{-1} \leq \mathcal{L}\Phi_a^{-1}$ is clear, and only the last inequality has to be shown. Let $A \in \mathcal{L}\bar{\mathcal{M}}\Phi_a^{-1}$. Thus there exist a language $B \in \mathcal{L}\mathcal{M}$, and an alphabetic morphism $\varphi: X_A^* \rightarrow X_B^*$ such that $A = \varphi^{-1}(B)$. Further there are a language $L \in \mathcal{L}$, and a $\mathcal{M}$ -substitution $\sigma: X_L^* \rightarrow X_B^*$ such that $B = \sigma(L)$; consequently, we have $A = \varphi^{-1}(\sigma(L))$. Note that $\varphi^{-1} \circ \sigma$ is not a substitution in general, since $\varphi^{-1}(1) \neq \{1\}$. Let y be a new letter not in X_L , set $Y = X_L \cup \{y\}$, and let $\theta: Y^* \rightarrow X_L^*$ be the projection from Y^* onto X_L^* . Set $L' = \theta^{-1}(L)$; then $L' \in \mathcal{L}\Phi_\pi^{-1}$. Define a substitution $\sigma': Y^* \rightarrow X_A^*$ by

$$\sigma'(z) = \varphi^{-1}(\sigma(z)) \quad \text{for } z \in X_L; \quad \sigma'(y) = \varphi^{-1}(1).$$

Then σ' is a $\mathcal{M}\Gamma$ -substitution since $\varphi^{-1}(1) \in \text{Rat} \subset \mathcal{M}\Gamma$. Finally, we have

$$\sigma'(\theta^{-1}(w)) = \varphi^{-1}(\sigma(w)) \quad \text{for all } w \in X_L^*,$$

and thus $\sigma'(L') = \sigma'(\theta^{-1}(L)) = \varphi^{-1}(\sigma(L)) = A$, thus $A \in \mathcal{L}\Phi_\pi^{-1}\bar{\mathcal{M}}\Gamma$. Consequently $\mathcal{L}\bar{\mathcal{M}}\Phi_a^{-1} \subset \mathcal{L}\Phi_\pi^{-1}\bar{\mathcal{M}}\Gamma$. ■

Finally, we investigate intersection with regular sets.

Lemma 4.13 *Let $\mathcal{L}$ be a family of languages; then*

$$\mathcal{L}I_R \leq I_R\mathcal{L}\Gamma \quad \text{or equivalently} \quad \bar{\mathcal{L}}I_R \leq \Gamma\bar{\mathcal{L}}I_R.$$

Proof. Let $\mathcal{M}$ be a family of languages. Then

$$\mathcal{M}\mathcal{L}I_R \subset \mathcal{M}I_R\mathcal{L}\Gamma \Leftrightarrow \mathcal{L}\bar{\mathcal{M}}I_R \subset \mathcal{L}\Gamma\bar{\mathcal{M}}I_R.$$

Therefore, the two inequalities are equivalent. Let $A \in \mathcal{L}\bar{\mathcal{M}}I_R$. Then there exist $K \in \text{Rat}(X_A^*)$ and $B \in \mathcal{L}\bar{\mathcal{M}}$ such that $A = B \cap K$. Next, there exist $L \in \mathcal{L}$, and a $\mathcal{M}$ -substitution $\sigma: X_L^* \rightarrow X_B^*$ such that

$$A = B \cap K = \sigma(L) \cap K.$$

Let $A = \langle X_A, Q, q_-, Q_+ \rangle$ be a finite automaton accepting $K: K = |A|$. For each pair $q, q' \in Q$, define

$$K_{q,q'} = \{f \in X_A^* \mid q \cdot f = q'\}.$$

Clearly, these languages are regular. Next, set

$$Y = Q \times X_A \times Q,$$

and define a transduction $\tau: X_L^* \rightarrow Y^*$ by

$$\tau(1) = \begin{cases} \{1\} & \text{if } 1 \in K; \\ \emptyset & \text{if } 1 \notin K, \end{cases}$$

$\tau(z_1 z_2 \cdots z_n) = \{(q_-, z_1, q_1)(q_1, z_2, q_2) \cdots (q_{n-1}, z_n, q_n) \mid q_i \in Q, q_n \in Q_+\}$ for $n \geq 1, z_1, \dots, z_n \in X_L$. Clearly this transduction is rational, and $\tau(L) \in \mathcal{L}\Gamma$.

Finally, define a substitution $\sigma': Y^* \rightarrow X_A^*$ by

$$\sigma'(q, z, q') = \sigma(z) \cap K_{q,q'} \quad (q, z, q') \in Y.$$

It follows that σ' is a $\mathcal{M}I_R$ -substitution. For any word

$$w = z_1 z_2 \cdots z_n \in X_L^+ \quad (z_i \in X_L)$$

we have

$$\sigma'(\tau(w)) = \bigcup (\sigma(z_1) \cap K_{q_-, q_1})(\sigma(z_2) \cap K_{q_1, q_2}) \cdots (\sigma(z_n) \cap K_{q_{n-1}, q_n}),$$

where the union is over all $(q_1, \dots, q_n) \in Q^n$ with $q_n \in Q_+$. Therefore $\sigma'(\tau(w)) = \sigma(w) \cap K$. Since $\sigma'(\tau(1)) = K \cap \sigma(1)$, we have $A = \sigma'(\tau(L))$, and $A \in \mathcal{L}\Gamma\mathcal{M}I_R$. ■

Now we are ready to prove Proposition 4.8.

Proof of Proposition 4.8. We have

$$\bar{\mathcal{L}}\Gamma = \bar{\mathcal{L}}\Phi_a^{-1}I_R\Phi_a \leq \Phi_\pi^{-1}\bar{\mathcal{L}}\Gamma I_R\Phi_a \quad (\text{Lemma 4.12})$$

$$\leq \Phi_\pi^{-1}\Gamma\bar{\mathcal{L}}\Gamma I_R\Phi_a = \Gamma\bar{\mathcal{L}}\Gamma\Phi_a \quad (\text{Lemma 4.13})$$

$$= \Gamma\bar{\mathcal{L}}\Gamma\Phi_a = \Gamma\bar{\mathcal{L}}\Gamma. \quad (\text{Lemma 4.11}). \quad \blacksquare$$

Remark. A more symmetrical statement of this inequality is the following: $\overline{\mathcal{L}\Gamma} \leq \Gamma \overline{\mathcal{L}\Gamma}$. The converse statement: $\Gamma \overline{\mathcal{L}\Gamma} \leq \overline{\mathcal{L}\Gamma}$ is not true in general (Exercise 4.1).

The following result also is obtained by a simple application of Proposition 4.8.

Theorem 4.14 (Ginsburg and Spanier [1970]). *Let $\mathcal{L}$ be a rational cone (resp. a full semi-AFL, a full AFL) and let $\mathcal{M}$ be a rational cone; then $\mathcal{L}\bar{\mathcal{M}} = \mathcal{L} \circ \mathcal{M}$ is a cone (resp. a full semi-AFL, a full AFL).*

Proof. In view of Proposition 4.8,

$$\mathcal{L}\bar{\mathcal{M}}\Gamma \subset \mathcal{L}\Gamma\bar{\mathcal{M}}\Gamma.$$

Since $\mathcal{L} = \mathcal{L}\Gamma$, $\mathcal{M} = \mathcal{M}\Gamma$, it follows $\mathcal{L}\bar{\mathcal{M}}\Gamma = \mathcal{L}\bar{\mathcal{M}}$, and therefore $\mathcal{L} \circ \mathcal{M}$ is a cone.

Next assume $\mathcal{L}$ is a full semi-AFL. Then by (2.1)

$$\mathcal{L}\bar{\mathcal{M}}\text{Elm} = \mathcal{L}\text{Elm}\bar{\mathcal{M}} = \mathcal{L}\bar{\mathcal{M}},$$

and thus $\mathcal{L}\bar{\mathcal{M}}$ is closed under union. Similarly, if $\mathcal{L}$ is a full AFL,

$$\mathcal{L}\bar{\mathcal{M}}\text{Rat} = \mathcal{L}\text{Rat}\bar{\mathcal{M}} = \mathcal{L}\bar{\mathcal{M}}. \quad \blacksquare$$

We show now that substitution by full AFLs instead of cones do not change the resulting family. We deduce this fact from the following equality.

Lemma 4.15 *Let $\mathcal{L}$ be a family of languages; then*

$$\Gamma \overline{\mathcal{L}\Gamma} = \overline{\Gamma \mathcal{L}\Gamma} \quad \text{or equivalently} \quad \Gamma \underline{\mathcal{L}\Gamma} = \underline{\Gamma \mathcal{L}\Gamma}.$$

Proof. We have $\overline{\Gamma \mathcal{L}\Gamma} = \overline{\Gamma \mathcal{L}\Gamma \text{Rat}} = \overline{\Gamma \text{Rat} \mathcal{L}\Gamma}$.

Now $\text{Rat} \leq \Gamma$ since each rational substitution is a rational transduction; therefore $\overline{\Gamma \text{Rat} \mathcal{L}\Gamma} \leq \overline{\Gamma \Gamma \mathcal{L}\Gamma} = \overline{\Gamma \mathcal{L}\Gamma}$. Thus $\overline{\Gamma \mathcal{L}\Gamma} \leq \overline{\Gamma \mathcal{L}\Gamma}$. The converse inequality is clear. $\blacksquare$

Corollary 4.16 *Let $\mathcal{L}$ and $\mathcal{M}$ be cones; then $\mathcal{L} \circ \mathcal{M} = \mathcal{L} \circ \mathcal{M}\hat{\Gamma}$.*

Proof. Indeed $\mathcal{L}\bar{\mathcal{M}} = \mathcal{L}\Gamma\bar{\mathcal{M}}\Gamma = \mathcal{L}\Gamma\bar{\mathcal{M}}\hat{\Gamma}$ by the preceding lemma. $\blacksquare$

Finally we show that $\mathcal{L}\bar{\mathcal{M}}^*$, the least family containing $\mathcal{L}$ and closed under $\mathcal{M}$ -substitution, is a cone provided $\mathcal{L}$ and $\mathcal{M}$ are cones.

Proposition 4.17 *Let $\mathcal{L}$ and $\mathcal{M}$ be cones; then $\mathcal{L}\bar{\mathcal{M}}^*$ is a cone. Further, if $\mathcal{L}$ is a full AFL, then $\mathcal{L}\bar{\mathcal{M}}^*$ is a full AFL. For any cone $\mathcal{L}$, $\mathcal{L}\bar{\mathcal{L}}^*$ is a full AFL closed under substitution.*

Proof. Assume $\mathcal{L}$ and $\mathcal{M}$ are cones. In view of Theorem 4.14, and arguing by induction, $\mathcal{L}\bar{\mathcal{M}}^k$ is a cone for any integer $k \geq 0$ (with $\bar{\mathcal{M}}^0 = id$). Thus $\mathcal{L}\bar{\mathcal{M}}^* = \bigcup_{k \geq 0} \mathcal{L}\bar{\mathcal{M}}^k$ is a cone, since the union of cones is a cone. Assume $\mathcal{L}$ is a full AFL.

Then by formula (3.3),

$$\mathcal{L}\bar{\mathcal{M}}^* \text{Rat} = \mathcal{L} \text{Rat} \bar{\mathcal{M}}^* = \mathcal{L}\bar{\mathcal{M}}^*,$$

and thus $\mathcal{L}\bar{\mathcal{M}}^*$ is a full AFL.

Finally, $\mathcal{L}\bar{\mathcal{L}}^*$ is a cone and is closed under substitution by Corollary 3.3, thus is a full AFL by Proposition V.5.5. $\blacksquare$

Exercises

4.1 Show that $\overline{\mathcal{L}\Gamma} \neq \overline{\mathcal{L}\Gamma\Gamma}$. (Hint. Apply the operators to Elm.)

4.2 Show that $\Phi_\pi^{-1}\Phi_\pi \leq \Phi_\pi\Phi_\pi^{-1}$, and thus $\Phi_\pi^{-1}\Phi_\pi = \Phi_\pi\Phi_\pi^{-1}$. Discuss the situation for the operators Φ_a and Φ .

4.3 Show that $\Phi^{-1}I_R \neq I_R\Phi^{-1}$.

4.4 (Ginsburg, Greibach and Hopcroft [1969]). Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be two families of languages. The wedge of $\mathcal{L}_1$ and $\mathcal{L}_2$ is the family $\mathcal{L}$ defined by

$$\mathcal{L} = \mathcal{L}_1 \wedge \mathcal{L}_2 = \{L_1 \cap L_2 \mid L_1 \in \mathcal{L}_1, L_2 \in \mathcal{L}_2\}.$$

a) show that if $\mathcal{L}_1$ and $\mathcal{L}_2$ are closed under inverse morphism and intersection with regular sets, then the same holds for $\mathcal{L}$.

b) show that if $\mathcal{L}_1$ and $\mathcal{L}_2$ are rational cones, then $\mathcal{L}\Phi$ is a rational cone (Hint. Apply the operator $\Phi\Gamma$ to $\mathcal{L} = \mathcal{L}\Phi^{-1}I_R$.)

c) show that if $\mathcal{L}_1$ and $\mathcal{L}_2$ are full AFLs, then $\mathcal{L}\Phi$ is a full AFL.

d) show that if $\mathcal{L}_1$ is a cone and $\mathcal{L}_2$ is a full AFL, then $\mathcal{L}_1 \circ \mathcal{L}_2 \subset \mathcal{L}\Phi$ (Hint. Show that $L_1 \uparrow L_2 \in \mathcal{L}_1 \wedge \mathcal{L}_2$ if $L_1 \in \mathcal{L}_1$, $L_2 \in \mathcal{L}_2$ are over disjoint alphabets, and use Proposition V.5.4.)

4.5 Show that $\Gamma \underline{\text{Elm}} = \underline{\text{Elm}} \Gamma$.

VI.5 Marked Substitution

In the preceding section, we showed that $\mathcal{L} \circ \mathcal{M}$ is a rational cone provided $\mathcal{L}$ and $\mathcal{M}$ are cones. In fact, a much more precise result holds: if $\mathcal{L}$ and $\mathcal{M}$ are principal cones (or full AFLs), then $\mathcal{L} \circ \mathcal{M}$ is also principal. Moreover, a generator of $\mathcal{L} \circ \mathcal{M}$ can be given which is explicitly expressed in terms of generators of $\mathcal{L}$ and $\mathcal{M}$ by means of the syntactic substitution. The question of the converse property, namely whether the principality of $\mathcal{L} \circ \mathcal{M}$ implies the principality of $\mathcal{L}$ and/or $\mathcal{M}$ will be considered in the next chapter.

It will appear in the sequel that the proof of the principality of $\mathcal{L} \circ \mathcal{M}$ requires inequalities in operators which are precisely the converses of the inequalities proved in Section 4. Since some of these inequalities are sharp, we have to go through a series of inequalities involving a special type of substitution called marked substitutions. They differ from the general substitutions by the condition that the substituted languages have endmarkers. Marked substitutions are

therefore closely related to, and in fact a generalization of syntactic substitutions.

A language A is said marked if it is of the form $A = Bc$, with c a letter, $c \in X_A \setminus X_B$. A marked language never contains the empty word.

Definition The marking operator $\#$ is the operator which associates, to any family of languages $\mathcal{L}$, the family

$$\mathcal{L}\# = \{Lc \mid L \in \mathcal{L}, c \in \Sigma \setminus X_L\}.$$

Clearly, $\mathcal{L}\#$ is closed under copy and thus is a family of languages. It is also clear that $\#$ is monotone and unitary, and therefore is an operator. Note that $\#$ is neither extensive nor idempotent.

Definition Let $\mathcal{M}$ be a family of languages. A marked $\mathcal{M}$ -substitution is a $\mathcal{M}\#$ -substitution.

Example 5.1 A syntactic substitution is a marked substitution. More precisely, let A, B be languages over disjoint alphabets. Then

$$A \uparrow B = \sigma_B(A)$$

where $\sigma_B(x) = Bx$ for $x \in X_A$. Thus $\sigma_B(x) \in \{B\}\#$, and σ_B is a marked $\{B\}$ -substitution.

Any marked substitution involving only two languages can be reduced to syntactic substitution in the following sense.

Proposition 5.1 Let A and B be languages over disjoint alphabets. Then

$$(\{A\} \sqcup (\{B\}\#))\Gamma = (A \uparrow B)\Gamma.$$

Proof. We just have seen that $A \uparrow B \in \{A\} \sqcup (\{B\}\#)$; thus $(A \uparrow B)\Gamma \subset (\{A\} \sqcup (\{B\}\#))\Gamma$. Conversely, let $L \in \{A\} \sqcup (\{B\}\#)$. Then there exists a $\{B\}\#$ -substitution $\sigma: X_A^* \rightarrow X_L^*$ such that $L = \sigma(A)$. Hence for each $x \in X_A$,

$$\sigma(x) = B_x c_x,$$

where B_x is a copy of B , and $c_x \in X_L \setminus X_{B_x}$. Let $\theta_x: X_B^* \rightarrow X_{B_x}^*$ be the copy isomorphism. Then $\theta_x(B) = B_x$ for each $x \in X_A$. Consider the relation

$$R = \left(\bigcup_{x \in X_A} \{(y, \theta_x(y)) : y \in X_B\}^*(x, c_x) \right)^* \subset (X_A \cup X_B)^* \times X_L^*.$$

Clearly, R is rational, and the transduction $\tau: (X_A \cup X_B)^* \rightarrow X_L^*$ defined by R is rational. Next

$$\text{dom}(\tau) = \left(\bigcup_{x \in X_A} X_{B_x}^* x \right)^*,$$

and for $w_1, w_2, \dots, w_n \in X_B^*, x_1, x_2, \dots, x_n \in X_A$,

$$\tau(w_1 x_1 w_2 x_2 \cdots w_n x_n) = \theta_{x_1}(w_1) c_{x_1} \theta_{x_2}(w_2) c_{x_2} \cdots \theta_{x_n}(w_n) c_{x_n}.$$

Thus $\tau(A \uparrow B) = \sigma(A) = L$.

Consequently, $L \in (A \uparrow B)\Gamma$, and $(\{A\} \sqcup (\{B\}\#))\Gamma \subset (A \uparrow B)\Gamma$. ■

This proposition will be helpful to construct generators of the cone $\mathcal{L} \sqcup \mathcal{M}$ from generators of cones $\mathcal{L}$ and $\mathcal{M}$. We now prove some simple facts on the operator $\#$. First note that $\mathcal{L}\#$ never is a cone, even if $\mathcal{L}$ is a cone, since $\{1\} \notin \mathcal{L}\#$.

Lemma 5.2 $\# \leq \Gamma, \Gamma \# \leq \Gamma, \# \Gamma = \Gamma, \hat{\Gamma} \# \leq \hat{\Gamma}, \# \hat{\Gamma} = \hat{\Gamma}$.

Proof. Let A and B be languages such that $A = Bc$, with $c \notin X_B$. Then $A \approx B$ by Corollary V.2.5. Consequently, $\mathcal{L}\# \Gamma = \mathcal{L}\Gamma$ for any family of languages $\mathcal{L}$. Thus $\# \Gamma = \Gamma$, which implies $\# \leq \# \Gamma = \Gamma$, and $\Gamma \# \leq \Gamma \Gamma = \Gamma$. Next $\hat{\Gamma} \# \leq \hat{\Gamma} \Gamma = \hat{\Gamma}$ and $\# \hat{\Gamma} = \# \Gamma \text{ Rat} = \Gamma \text{ Rat}$. ■

As already noted several times, an inverse alphabetic morphism is not a substitution. By means of the marking operator, inverse alphabetic morphisms can be expressed using rational substitutions.

Lemma 5.3 $\Phi_a^{-1} \leq \# \text{Rat}$.

Proof. Let $\mathcal{L}$ be a family of languages, and let $A \in \mathcal{L} \Phi_a^{-1}$. Then $A = \varphi^{-1}(B)$, where $B \in \mathcal{L}$ and $\varphi: X_A^* \rightarrow X_B^*$ is an alphabetic morphism. Define

$$X_z = \{x \in X_A : \varphi x = z\} \quad (z \in X_B); \quad X_0 = \{x \in X_A : \varphi x = 1\}.$$

Then $\varphi^{-1}(z) = X_0^* X_z X_0^*$ for $z \in X_B$ and $\varphi^{-1}(1) = X_0^*$. Let $c \in \Sigma \setminus X_B$, and define a rational substitution

$$\sigma: (X_B \cup c)^* \rightarrow X_A^* \quad \text{by} \quad \sigma(z) = X_0^* X_z \quad (z \in X_B); \quad \sigma(c) = X_0^*.$$

Then $\sigma(\varphi c) = \varphi^{-1}(f)$ for all $f \in X_B^*$. Hence $A = \sigma(Bc)$. Since $Bc \in \mathcal{L}\#$, $A \in \mathcal{L}\# \text{Rat}$, proving thus the inequality. ■

We now turn to the construction of a set of generators of the cone $\mathcal{L}\Gamma \sqcup \mathcal{M}\Gamma$ in terms of $\mathcal{L}$ and $\mathcal{M}$. We shall prove that $\mathcal{L}\Gamma \sqcup \mathcal{M}\Gamma$ is generated by $\mathcal{L}\# \sqcup \mathcal{M}\hat{\Gamma}$. The inclusion $(\mathcal{L}\# \sqcup \mathcal{M}\hat{\Gamma}) \subset \mathcal{L}\Gamma \sqcup \mathcal{M}\Gamma$ is easy to show. The converse inclusion can be written as an inequality between operators:

$$\Gamma \overline{\mathcal{M}\Gamma} \leq \# \overline{\mathcal{M}\hat{\Gamma}} \Gamma. \quad (5.1)$$

Note that (5.1) is a weak converse of Proposition 4.8. To prove (5.1), we proceed as in the previous section and write

$$\Gamma \overline{\mathcal{M}\Gamma} = \Phi_a^{-1} I_R \Phi_a \overline{\mathcal{M}\Gamma}.$$

We thus have to prove three inequalities involving Φ_a , I_R , Φ_a^{-1} and the operator $\mathcal{M}\Gamma$. Alphabetic morphisms are easy to handle. For intersection with regular sets, we have the following "converse" of Lemma 4.13.

Lemma 5.4 *Let $\mathcal{L}$ be a family of languages; then*

$$I_R \bar{\mathcal{L}} \leq \bar{\mathcal{L}} \# \Gamma \quad \text{or equivalently} \quad \underline{\mathcal{L}} I_R \leq \# \underline{\mathcal{L}} \Gamma.$$

Proof. Let $\mathcal{M}$ be a family of languages. First note that

$$\mathcal{M} I_R \bar{\mathcal{L}} \subset \mathcal{M} \bar{\mathcal{L}} \# \Gamma \Leftrightarrow \mathcal{L} \mathcal{M} I_R \subset \mathcal{L} \# \mathcal{M} \Gamma.$$

Thus the two inequalities are equivalent.

Next, let $A \in \mathcal{M} I_R \bar{\mathcal{L}}$. Then there exist $M \in \mathcal{M}$, $K \in \text{Rat}(X_M^*)$ and a $\mathcal{L}$ -substitution $\sigma: X_M^* \rightarrow X_A^*$ such that $A = \sigma(M \cap K)$. We may assume $X_M \cap X_A = \emptyset$. Define a $\mathcal{L}\#$ -substitution

$$\sigma': X_M^* \rightarrow (X_M \cup X_A)^*$$

by $\sigma'(x) = \sigma(x)x$, $x \in X_M$.

Next, consider the rational substitution

$$\sigma'': X_M^* \rightarrow (X_M \cup X_A)^*$$

defined by

$$\sigma''(x) = X_A^* x, \quad x \in X_M.$$

Then $K' = \sigma''(K)$ is a rational subset of $(X_M \cup X_A)^*$. Further, for $f \in X_M^+$, we have

$$w \in \sigma'(f) \cap K'$$

iff $w = w_1 x_1 w_2 x_2 \cdots w_n x_n$,

with $w_i \in \sigma(x_i)$, $x_i \in X_M$, $f = x_1 x_2 \cdots x_n \in K$. Clearly $\sigma'(1) \cap K' = 1 \cap K$. Let π be the projection from $(X_M \cup X_A)^*$ onto X_A^* . It follows that

$$A = \sigma(M \cap K) = \pi(\sigma'(M) \cap K').$$

Thus $A \in \mathcal{M} \bar{\mathcal{L}} \# \Gamma$, and the inclusion is proved. ■

Inverse morphisms will be treated by Lemma 5.3. Thus we are ready to prove following

Proposition 5.5 *Let $\mathcal{L}$ and $\mathcal{M}$ be families of languages. Then*

- (i) $\mathcal{L}\Gamma \sqcap \mathcal{M}\Gamma = \mathcal{L}\Gamma \sqcap \mathcal{M}\hat{\Gamma} = (\mathcal{L}\# \sqcap \mathcal{M}\hat{\Gamma})\Gamma$;
- (ii) $\mathcal{L}\Gamma \text{Elm} \sqcap \mathcal{M}\Gamma = \mathcal{L}\Gamma \text{Elm} \sqcap \mathcal{M}\hat{\Gamma} = (\mathcal{L}\# \sqcap \mathcal{M}\hat{\Gamma})\Gamma \text{Elm}$;
- (iii) $\mathcal{L}\hat{\Gamma} \sqcap \mathcal{M}\Gamma = \mathcal{L}\hat{\Gamma} \sqcap \mathcal{M}\hat{\Gamma} = (\mathcal{L}\# \sqcap \mathcal{M}\hat{\Gamma})\hat{\Gamma}$.

Proof. We first prove

$$\Gamma \bar{\mathcal{M}}\Gamma = \# \bar{\mathcal{M}}\hat{\Gamma}\Gamma. \quad (5.2)$$

Indeed, $\Gamma \bar{\mathcal{M}}\Gamma = \Phi_a^{-1} I_R \Phi_a \bar{\mathcal{M}}\Gamma \leq \Phi_a^{-1} I_R \text{Rat } \bar{\mathcal{M}}\Gamma$

since a morphism is a rational substitution. In view of $\text{Rat } \bar{\mathcal{M}}\Gamma = \bar{\mathcal{M}}\hat{\Gamma}$, we obtain

$$\begin{aligned} \Gamma \bar{\mathcal{M}}\Gamma &\leq \Phi_a^{-1} I_R \bar{\mathcal{M}}\hat{\Gamma} \\ &\leq \Phi_a^{-1} \bar{\mathcal{M}}\hat{\Gamma} \# \Gamma \quad (\text{by Lemma 5.4}) \\ &\leq \Phi_a^{-1} \bar{\mathcal{M}}\hat{\Gamma}\Gamma \quad (\text{by Lemma 5.2}) \\ &\leq \# \text{Rat } \bar{\mathcal{M}}\hat{\Gamma}\Gamma \quad (\text{by Lemma 5.3}) \\ &= \# \bar{\mathcal{M}}\hat{\Gamma}\Gamma. \end{aligned}$$

Conversely, in view of Proposition 4.8,

$$\# \bar{\mathcal{M}}\hat{\Gamma}\Gamma \leq \# \Gamma \bar{\mathcal{M}}\hat{\Gamma}\Gamma = \# \Gamma \bar{\mathcal{M}}\hat{\Gamma} = \Gamma \bar{\mathcal{M}}\hat{\Gamma}$$

by Lemma 5.2, and in view of Lemma 4.15, $\Gamma \bar{\mathcal{M}}\hat{\Gamma} = \Gamma \bar{\mathcal{M}}\Gamma$. This proves (5.2). Next, since $\mathcal{N}\bar{\mathcal{M}} = \bar{\mathcal{M}}\mathcal{N}$ for any families $\mathcal{N}$ and $\mathcal{M}$, it suffices to prove (i). Now (i) rewrites as

$$\mathcal{L}\Gamma \bar{\mathcal{M}}\Gamma = \mathcal{L}\Gamma \bar{\mathcal{M}}\hat{\Gamma} = \mathcal{L}\# \bar{\mathcal{M}}\hat{\Gamma}\Gamma,$$

and thus follows directly from (5.2) and Lemma 4.15. ■

Proposition 5.5 is not satisfactory, since in the case where $\mathcal{L}$ and $\mathcal{M}$ are singletons, it does not give a single generator for the family $\mathcal{L}\Gamma \sqcap \mathcal{M}\Gamma$. To get this generator, we prove

Lemma 5.6 *Let $\mathcal{L}$ be a family of languages. Then*

$$\bar{\mathcal{L}}\Gamma \leq \bar{\mathcal{L}} \# \Gamma \quad \text{or equivalently} \quad \Gamma \bar{\mathcal{L}} \leq \# \bar{\mathcal{L}}\Gamma.$$

Proof. Let $\mathcal{M}$ be a family of languages. First, observe that

$$\mathcal{M} \bar{\mathcal{L}}\Gamma \subset \mathcal{M} \bar{\mathcal{L}} \# \Gamma \Leftrightarrow \mathcal{L}\Gamma \mathcal{M} \subset \mathcal{L}\# \mathcal{M}\Gamma,$$

thus the inequalities are equivalent.

Next, let $A \in \mathcal{M} \bar{\mathcal{L}}\Gamma$. Then $A = \sigma(B)$, where $B \in \mathcal{M}$ and $\sigma: X_B^* \rightarrow X_A^*$ is a $\mathcal{L}\Gamma$ -substitution. Thus, for each letter $z \in X_B$, $\sigma(z) \in \mathcal{L}\Gamma$, and there exist an alphabet Y_z , a rational transduction $\tau_z: Y_z^* \rightarrow X_A^*$, and a language $L_z \in \mathcal{L}$, $L_z \subset Y_z^*$ such that

$$\sigma(z) = \tau_z(L_z) \quad z \in X_B.$$

We may assume that the alphabets Y_z are pairwise disjoint and disjoint from X_B . Set

$$Y = X_B \cup \bigcup_{z \in X_B} Y_z,$$

and define a substitution $\sigma': X_B^* \rightarrow Y^*$ by

$$\sigma'(z) = L_z z \quad z \in X_B.$$

Thus σ' is a $\mathcal{L}\#$ -substitution. Next, let $\tau: Y^* \rightarrow X_A^*$ be the transduction defined by

$$\begin{aligned} \tau(1) &= 1; \quad \tau(f) = \emptyset \quad \text{if } f \notin (\bigcup Y_z^* z)^*; \\ \tau(f_1 z_1 \cdots f_n z_n) &= \tau_{z_1}(f_1) \cdots \tau_{z_n}(f_n), \quad \text{if } f_i \in Y_{z_i}^*, z_i \in B. \end{aligned}$$

Then $\tau(\sigma'(z)) = \tau(L_z z) = \tau_z(L_z) = \sigma(z) \quad (z \in X_B),$

$$\tau(\sigma'(1)) = \tau(1) = \sigma(1)$$

$$\tau(\sigma'(fg)) = \tau(\sigma'(f)\sigma'(g)) = \sigma(f)\sigma(g) \quad \text{for } f, g \in X_B^*.$$

It follows that $\tau \circ \sigma'$ is a substitution, and $\tau \circ \sigma' = \sigma$. Consequently,

$$A = \sigma(B) = \tau(\sigma'(B)).$$

Now $\sigma'(B) \in \mathcal{ML}\#$, and in order to achieve the proof, it suffices to show that τ is rational. For this, let

$$R_z \subset Y_z^* \times X_A^*$$

be the graph of $\tau_z (z \in X_B)$. Then

$$S = \left(\bigcup_{z \in X_B} R_z \cdot (z, 1) \right)^*$$

is the graph of τ and since each R_z is rational, S is a rational relation. ■

Theorem 5.7 (Ginsburg and Greibach [1970]) *Let $\mathcal{L}$ and $\mathcal{M}$ be principal cones (full AFLs). Then $\mathcal{L} \sqcap \mathcal{M}$ is a principal cone (full AFL). For any cone (full AFL) generators L of $\mathcal{L}$ and M of $\mathcal{M}$ and for any new letters $c, d \notin X_L \cup X_M$, $Ld \uparrow (Mc)^+$ is a cone (full AFL) generators of $\mathcal{L} \sqcap \mathcal{M}$:*

$$L\Gamma \sqcap M\Gamma = (Ld \uparrow (Mc)^+) \Gamma \quad (5.3)$$

$$L\hat{\Gamma} \sqcap M\hat{\Gamma} = (Ld \uparrow (Mc)^+) \hat{\Gamma} \quad (5.4)$$

Further if $L \neq \{1\}$, then

$$L\Gamma \sqcap M\Gamma = (L \uparrow (Mc)^+) \Gamma \quad (5.5)$$

$$L\hat{\Gamma} \sqcap M\hat{\Gamma} = (L \uparrow (Mc)^+) \hat{\Gamma}. \quad (5.6)$$

Proof. By (2.1) and Corollary 4.16, $L\hat{\Gamma} \sqcap M\hat{\Gamma} = (L\Gamma \sqcap M\Gamma) \text{ Rat}$. Thus (5.4) and (5.6) are direct consequences of (5.3) and (5.5) respectively. To show (5.3), we first note that in view of (5.2)

$$\overline{\Gamma M \Gamma} = \# \overline{M \Gamma} \Gamma.$$

Next by Theorem V.4.4, $\overline{M \Gamma} = M_1 \Gamma$, where $M_1 = (Mc)^+$. Consequently

$$\overline{\Gamma M \Gamma} \# \overline{M_1 \Gamma} \Gamma \leq \# \overline{M_1 \Gamma} \Gamma \quad (\text{by Lemma 5.6})$$

$$\leq \# \overline{\Gamma M_1 \Gamma} \Gamma \quad (\text{by Proposition 4.8})$$

$$\leq \overline{\Gamma M_1 \Gamma} \Gamma \quad (\text{by Lemma 5.2})$$

$$= \overline{\Gamma M \Gamma}.$$

Thus $\overline{\Gamma M \Gamma} = \# \overline{M_1 \Gamma} \Gamma$ and by Lemma 4.15, $\overline{\Gamma M \Gamma} = \# \overline{M_1 \Gamma} \Gamma$. Consequently

$$L\Gamma \sqcap M\Gamma = (\{L\} \# \{M_1\} \#) \Gamma = (\{Ld\} \sqcap \{M_1\} \#) \Gamma.$$

By Proposition 5.1, we obtain

$$L\Gamma \sqcap M\Gamma = (Ld \uparrow (Mc)^+) \Gamma.$$

Suppose now $L \neq \{1\}$. To prove (5.5), it suffices to show

$$Ld \uparrow (Mc)^+ \approx L \uparrow (Mc)^+.$$

Set $X = X_L$, $Y = X_M$, $Z = X \cup Y \cup \{c, d\}$. Consider the following rational relations of $Z^* \times Z^*$:

$$R = \{(y, y) : y \in Y^*\} (c, c); \quad I = \left(\bigcup_{x \in X} R^+(x, x) \right)^*; \quad E = Y^* c \times \{1\}.$$

The transduction $Z^* \rightarrow Z^*$ with graph I is the identity on $((Y^* c)^+ X)^*$. Let $\tau_1: Z^* \rightarrow Z^*$ be the rational transduction with graph

$$A = I \cdot E^+ \cdot \{(d, 1)\}.$$

Then for $f_1, \dots, f_{n+1} \in (Y^* c)^+$, $x_1, \dots, x_n \in X$,

$$\tau_1(f_1 x_1 \cdots f_n x_n f_{n+1} d) = f_1 x_1 \cdots f_n x_n.$$

Consequently $\tau_1(Ld \uparrow (Mc)^+) = L \uparrow (Mc)^+$. (The hypothesis $L \neq \{1\}$ was not used.) Conversely, consider the transductions $Z^* \rightarrow Z^*$ with graph

$$S_x = R^+(1, x) R^+(x, d) \quad (x \in X).$$

These transductions map a word $m_1 c \cdots m_k c x$, ($m_i \in Y^*$, $k \geq 2$) into the words $m_1 c \cdots m_i c x m_{i+1} c \cdots m_k c d$, ($1 \leq i < k$). Define a transduction $\tau_2: Z^* \rightarrow Z^*$ with graph

$$B = I \cdot \left(\bigcup_{x \in X} S_x \right).$$

Then $\tau_2((Mc)^+x_1 \cdots (Mc)^+x_n) = (Mc)^+x_1 \cdots (Mc)^+x_n(Mc)^+d$ for $x_1, \dots, x_n \in X$, $n \geq 1$. Consequently, if $1 \notin L$ then

$$\tau_2(L \uparrow (Mc)^+) = Ld \uparrow (Mc)^+.$$

If $1 \in L$, then $Ld \uparrow (Mc)^+ = \tau_2(L \uparrow (Mc)^+) \cup (Mc)^+d$. In this case, consider the rational transduction $\tau_3: Z^* \rightarrow Z^*$ with graph

$$C = \left(\bigcup_{x \in X} E^+(x, 1) \right)^* \left(\bigcup_{x \in X} R^+(x, d) \right).$$

Then for $k \geq 1$, $f_1, \dots, f_k \in (Y^*c)^+$, $x_1, \dots, x_k \in X$,

$$\tau_3(f_1x_1 \cdots f_kx_k) = f_kd.$$

Thus if $L \neq \{1\}$, $\tau_3(L \uparrow (Mc)^+) = (Mc)^+d$. Hence

$$Ld \uparrow (Mc)^+ = (\tau_2 \cup \tau_3)(L \uparrow (Mc)^+).$$

Exercises

5.1 Compute $(Ld \uparrow (Mc)^+)\Gamma$ and $(L \uparrow (Mc)^+)\Gamma$ for $L = \{1\}$.

5.2 Show that for $L \neq \{1\}$, $L\hat{\Gamma} \cap M\hat{\Gamma} = ((Ld)^+ \uparrow (Mc)^+)\Gamma$.

5.3 Let $\mathcal{L}$ and $\mathcal{M}$ be principal cones. Show that there exist $L \in \mathcal{L}$, $M \in \mathcal{M}$ such that $\mathcal{L} \cap \mathcal{M} = (L \uparrow M)\Gamma$. Give an example of languages L , M such that $(L \uparrow M)\Gamma \subsetneq L\Gamma \cap M\Gamma$ (see also Exercises 5.6, 5.7 below).

5.4 (Lewis [1970]) For any family of languages $\mathcal{L}$ define $\hat{\mathcal{L}}$ by

$$\hat{\mathcal{L}} = \{A \mid \{A\} \cap \mathcal{L} \subset \mathcal{L}\}.$$

- Show that $\hat{\hat{\mathcal{L}}} = \mathcal{L}$, and that $\hat{\mathcal{L}}$ is closed under substitution.
- Show that if $\mathcal{L}$ contains at least one language $\{x\}$ with $x \in \Sigma$, then $\hat{\mathcal{L}} \subset \mathcal{L}$.
- Show that if $\mathcal{L}$ is a full AFL, then $\hat{\mathcal{L}}$ is a full AFL.

5.5 (Greibach and Hopcroft [1969]) Let $\mathcal{L}$ be a family of languages closed under rational substitution and intersection with regular sets. Show that if $\mathcal{L}$ contains at least one nonempty language $\neq \{1\}$, then $\mathcal{L}$ is a rational cone. (Hint. Show that $\mathcal{L} \# \subset \mathcal{L}$ and use Lemma 5.3.)

The two following exercises are difficult:

5.6 Show that $S_2 \uparrow (Mc)^+ \approx S_2 \uparrow M$, where S_2 is the symmetric language, S_2 and M are over disjoint alphabets, and c is a new letter. (Hint. Show first that $S_2 \uparrow M \approx S_3 \uparrow M$, and use the third letter of the alphabet of S_3 to create the letter c .)

5.7 Show that $D_1'^* \uparrow (Mc)^+ \approx D_1'^* \uparrow M$, where $D_1'^*$ is the restricted Dyck language, and M , c are as above. Same problem for $D_n'^*$, ($n \geq 2$). (Hint. For $D_1'^*$, consider first a rational transduction which replaces, in words of $D_1'^* \uparrow M$, factors of the form $mxm'\bar{x}$ by mc . For $D_n'^*$, ($n \geq 2$), Proposition VII.1.1 may be useful.)

VII Generators

The first section contains examples of generators of the cone Alg of context-free languages. The Dyck languages over at least two pairs of parentheses and the language E of completely parenthesized arithmetic expressions are shown to be generators. Sections 2 and 3 are concerned with S. Greibach's Syntactic Lemma and its applications. In particular, we prove that in a substitution closed principal full AFL, the nongenerators form a substitution closed full AFL. Next the Syntactic Lemma is used to exhibit infinite ascending chains of cones, and thus nonprincipal cones of context-free languages. In Section 4, we study the family of languages recognized by one counter pushdown automata and we prove this family to be the full AFL generated by $D_1'^*$. The last section deals with the family of quasi-rational or nonexpansive languages. Several characterizations of this family are given.

VII.1 Generators of the Context-Free Languages

The family Alg of context-free or algebraic languages is a full AFL closed under substitution (see Theorem II.2.1.). In this section, we shall see that Alg is a principal cone, by describing some of its generators. Each cone generator is also a full AFL generator of Alg. As a consequence of the Syntactic Lemma, we shall see that conversely, each full AFL generator generates the cone Alg, i.e. $L\hat{\Gamma} = \text{Alg}$ iff $L\Gamma = \text{Alg}$. The family of (full AFL or cone) generators of Alg is the most "powerful" class of context-free languages.

No characterization of the generators of Alg is known. The Chomsky-Schützenberger Theorem implies that the Dyck languages D_n' , $D_n'^*$, D_n , D_n^* are generators for $n \geq 2$. Other examples of generators are related to the language E of completely parenthesized arithmetic expressions introduced in Section II.4. Autebert and Beauquier [1974] observed that these languages are all rationally equivalent to languages of the form $D_n'^* \cap K$, with K rational, and gave a characterization of generators of this form. Let us mention a remarkable property of the generators of Alg proved by Beauquier [1976a, b][1978a]: For any generator L of Alg, there is a regular language K such that $L \cap K$ is still a generator and is an unambiguous language.

Recall that the Dyck languages

$$D_n^*, D_n'^*, D_n, D_n' \quad (n \geq 1)$$

are defined over an alphabet $Z_n = X_n \cup \bar{X}_n$, with $X_n = \{x_1, \dots, x_n\}$, $\bar{X}_n = \{\bar{x}_1, \dots, \bar{x}_n\}$. We first prove:

Proposition 1.1 For $n \geq 2$, $D_n^* \approx D_n'^* \approx D_n \approx D_n' \approx D_2^*$; further $D_2^* \geq D_1^*, D_1'^*, D_1$.

The Dyck languages over one pair of parentheses are not generators. The full AFL generated by D_1^*, D_1, D_1' is the family of one counter languages studied in section 4.

Proof. For $n \geq 1$ we have

$$\begin{aligned} D_n^* &= D_{n+1}^* \cap Z_n^*, & D_n'^* &= D_{n+1}'^* \cap Z_n^*, & D_n &= D_{n+1} \cap Z_n^*, \\ D_n' &= D_{n+1}' \cap Z_n^*, \end{aligned}$$

thus

$$D_{n+1}^* \geq D_n^*, \quad D_{n+1}'^* \geq D_n'^*, \quad D_{n+1} \geq D_n, \quad D_{n+1}' \geq D_n'.$$

Conversely, consider the morphism $\alpha: Z_n^* \rightarrow Z_2^*$ defined by

$$\alpha(x_i) = x_1^i x_2 x_1^i, \quad \alpha(\bar{x}_i) = \bar{x}_1^i \bar{x}_2 \bar{x}_1^i \quad i = 1, \dots, n.$$

Then $U = \alpha(Z_n)$ is a bifix code. We shall verify that

$$\begin{aligned} D_n^* &= \alpha^{-1}(D_2^* \cap U^*), & D_n'^* &= \alpha^{-1}(D_2'^* \cap U^*), \\ D_n &= \alpha^{-1}(D_2 \cap U^*), & D_n' &= \alpha^{-1}(D_2' \cap U^*), \end{aligned}$$

which imply

$$D_n^* \approx D_2^*, \quad D_n'^* \approx D_2'^*, \quad D_n \approx D_2, \quad D_n' \approx D_2'. \quad (1.1)$$

The inclusion $\alpha(D_n^*) \subset D_2^* \cap U^*$ (and similarly for $\alpha(D_n'^*) \subset D_2'^* \cap U^*$, $\alpha(D_n) \subset D_2 \cap U^*$, $\alpha(D_n') \subset D_2' \cap U^*$) is shown by a straightforward induction. To prove conversely $D_n^* \supset \alpha^{-1}(D_2^* \cap U^*)$ we argue by induction on the length of words. Let $f \in \alpha^{-1}(D_2^* \cap U^*)$. If $|f| = 0$, then $f = 1 \in D_n^*$. Assume $|f| > 0$. Then $w = \alpha(f) \neq 1$. Since $w \in D_2^*$, there exists a Dyck reduction

$$w = w_0 \vdash w_1 \vdash w_2 \vdash \dots \vdash w_p = 1.$$

Consider the smallest index i such that $|w_i|_{x_2} < |w|_{x_2}$. Then since $w \vdash^* w_i$, it follows immediately from Lemma II.3.6 that w admits a factorization

$$w = u_0 \bar{x}_2 v x_2 u_1 \quad \text{or} \quad w = u_0 x_2 v \bar{x}_2 u_1$$

with $v \equiv 1 \pmod{\delta_2}$ and $v \in \{x_1, \bar{x}_1\}^*$. Suppose for instance that w has the first of the above factorizations. Since $w \in U^*$, there are integers i, j , ($1 \leq i, j \leq n$) such that

$$w = u' \bar{x}_1^i \bar{x}_2 \bar{x}_1^i x_1^j x_2 x_1^j u''$$

with $u' \bar{x}_1^i = u_0$, $v = \bar{x}_1^i x_1^j$ and $x_1^j u'' = u_1$. Since $v \in D_2^*$, we have $i = j$, and $u', u'' \in U^*$. Consequently there are $f', f'' \in Z_n^*$ such that $\alpha(f') = u'$, $\alpha(f'') = u''$ and $f = f' \bar{x}_i x_i f''$. Next $\alpha(f' f'') = u' u'' \in D_2^* \cap U^*$. By induction, $f' f'' \in D_n^*$, whence $f \in D_n^*$. To prove the inclusion $D_n \supset \alpha^{-1}(D_2 \cap U^*)$, assume that there is a word $f \in \alpha^{-1}(D_2 \cap U^*)$ such that $f \notin D_n$. By the above proof, $f \in D_n^*$, and consequently $f = f_1 f_2$, with $f_1, f_2 \in D_n^* \setminus 1$. But then $\alpha(f_1), \alpha(f_2) \in D_2^* \setminus 1$, and $\alpha(f) \notin D_2$. The proofs for $D_n'^*$ and D_n' are identical.

In view of the Chomsky-Schützenberger Theorem II.3.10 and by (1.1), there are integers $n, m, p, q \geq 2$ such that

$$D_n^* \geq D_2^* \approx D_m'^* \geq D_2 \approx D_p \geq D_2' \approx D_q' \geq D_2^* \approx D_n^*.$$

This concludes the proof. $\blacksquare$

Proposition 1.1 implies immediately

Theorem 1.2 The cone Alg of algebraic languages is principal; any of the languages $D_n^*, D_n'^*, D_n, D_n'$ ($n \geq 2$) is a generator of Alg.

Proof. Let L be an algebraic language; then in view of the Chomsky-Schützenberger Theorem, $D_n^* \geq L$ for some $n \geq 2$. Since $D_n^* \approx D_2^*$ by the previous proposition, $D_2^* \geq L$, whence $\text{Alg} \subset D_2^* \Gamma$. The converse implication is obvious. $\blacksquare$

Proposition 1.3 $D_1 \approx D_1' \approx D_1'^*$.

We shall see later (Proposition VIII.7.1) that none of these languages is a generator of Alg. The situation of D_1^* is particular: Clearly Proposition 1.3 implies

$$D_1^* \hat{\Gamma} \subset D_1 \hat{\Gamma} = D_1' \hat{\Gamma} = D_1'^* \hat{\Gamma}.$$

Thus D_1^* is not a generator of Alg (since otherwise D_1^* would be a generator). In fact, it can be proved (Boasson [1973a]) that the above inclusion is strict, and that further the cones $D_1^* \Gamma$ and $D_1'^* \Gamma$ are incomparable.

Proof. The equalities

$$D_1' = x_1 D_1'^* \bar{x}_1, \quad D_1'^* = x_1^{-1} D_1' \bar{x}_1^{-1}$$

show that D_1' and $D_1'^*$ are rationally equivalent. Define an isomorphism $\beta: Z_1^* \rightarrow Z_1^*$ by

$$\beta(x_1) = \bar{x}_1, \quad \beta(\bar{x}_1) = x_1,$$

and set $\bar{D}_1' = \beta(D_1')$. Then $\bar{D}_1' \approx D_1'$, whence $D_1' \geq D_1' \cup \bar{D}_1'$.

Next we claim that

$$D_1 = D_1' \cup \bar{D}_1'. \quad (1.2)$$

We shall see indeed that, with the notations of Section II.3,

$$D'_1 = D_{1,x_1} = x_1 Z_1^* \bar{x}_1 \cap D_1, \quad \bar{D}'_1 = D_{1,\bar{x}_1} \quad (1.3)$$

The inclusions $D'_1 \subset D_{1,x_1}$ and $\bar{D}'_1 \subset D_{1,\bar{x}_1}$ are clear. Conversely, consider a word w in D_{1,x_1} . Then by formula (II.(3.5), (3.6)), $w = x_1 w_1 w_2 \cdots w_n \bar{x}_1$, where $w_1, \dots, w_n \in D_{1,x_1}$. Thus the conclusion follows by induction. The same proof holds for $\bar{D}'_1$.

By (1.2), $D'_1 \geq D_1$, and in view of (1.3), we have conversely $D_1 \geq D'_1$. ■

There are other generators of Alg, related to the language E of completely parenthesized arithmetic expressions. The first languages of this type have been described by Schützenberger [1973]; other languages were found by Autebert and Beauquier [1974]. A rather complete list was given in Autebert [1973].

For $n \geq 1$, consider the alphabets

$$A_n = \{a_1, \dots, a_n\}, \quad C_n = \{c_1, \dots, c_n\}, \quad Y_n = A_n \cup C_n \cup \{b, d\}.$$

Let E_n be the language generated by the grammar G_n with productions:

$$\xi \rightarrow \sum_{k=1}^n a_k \xi b \xi c_k + d.$$

For $n=1$ we set $a = a_1$, $c = c_1$. Thus $E_1 = E$ is the language introduced in Section II.4. The languages E_n have properties very similar to those of E .

Lemma 1.4 *The language E_n is bifix; more precisely, if $w \in E_n$, then*

$$|w|_{A_n} = |w|_b = |w|_{C_n} = |w|_d - 1,$$

and any nonempty proper left (right) factor w' of w satisfies

$$|w'|_{A_n} > |w'|_{C_n} \quad (|w'|_{A_n} < |w'|_{C_n}).$$

The simple proof is left to the reader.

Lemma 1.5 *The language E_n is equal to the class of d in the congruence η_n generated by the relations*

$$a_k d b d c_k \sim d \quad k = 1, \dots, n.$$

The proof is the same as for Theorem II.4.5 and is also left to the reader.

Lemma 1.6 *Let $w \in E_n$, and $w = u a_k u'$, with $u, u' \in Y_n^*$. Then there exists a unique factorization $u' = w_1 b w_2 c_k u''$ with $w_1, w_2 \in E_n$, $u'' \in Y_n^*$.*

Proof. Let $w = u a_k u'$. Since $w \in E_n$, and $w \neq d$, there exist $w', w'' \in E_n$ such that $w = a_l w' b w'' c_l$ for some l , ($1 \leq l \leq n$). If $u = 1$, then $u' = w' b w'' c_l$ is the desired factorization. If $u \neq 1$, then two possibilities arise. Either $|u a_k| \leq |a_l w'|$, and then w' is of the form $w' = u_1 a_l u'_1$ with $a_l u_1 = u$ and u'_1 a left factor of u' . Otherwise $|a_k u| \leq |w'' c_l|$, and w'' has the form $w'' = u_1 a_l u'_1$, with $u'_1 c_l = u'$ and

u_1 a right factor of u . In both cases, the existence of a factorization follows by induction. The unicity is obvious since E_n is prefix. ■

Theorem 1.7 *The languages E_n ($n \geq 1$) are rationally equivalent.*

Thus, in opposition to the situation for Dyck languages, we also have $E_1 \approx E_n$.

Proof. The proof is in two parts. In the first part we prove the relations $E_n \approx E_2 \geq E_1$ by a standard encoding argument similar to that employed for Proposition 1.1. In the second part we prove $E_1 \geq E_2$ by a more complicated encoding.

First we observe that

$$E_n = E_{n+1} \cap Y_n^*,$$

hence $E_{n+1} \geq E_n$ for $n \geq 1$. Next, we show that $E_2 \geq E_n$. For simplicity, set $a = a_1$, $c = c_1$, $a' = a_2$, $c' = c_2$. Define a morphism

$$\theta: Y_n^* \rightarrow Y_2^*$$

$$\text{by } \theta(a_k) = a(dba')^k; \quad \theta(c_k) = c'^k c \quad k = 1, \dots, n$$

$$\theta(b) = b, \quad \theta(d) = d.$$

The set $U = \theta(Y_n)$ is a code. Further we have the derivations

$$\xi \xrightarrow{*} a(dba')^k \xi b \xi c'^k c \quad k = 1, \dots, n$$

in the grammar G_n . This shows that

$$\theta(E_n) \subset E_2 \cap U^*.$$

To show the converse inclusion $E_n \supset \theta^{-1}(E_2)$ and thereby the relation $E_2 \geq E_n$, we argue by induction on the length of a word $f \in \theta^{-1}(E_2)$. If $|f| = 1$, then $f = d$ and $f \in E_n$. Assume $|f| > 1$ and set $w = \theta(f)$. Then $w \in E_2 \cap U^*$, $|w| > 1$ and consequently $w = a(dba')^k w'$ for some k , ($1 \leq k \leq n$) and some $w' \in U^*$. Applying Lemma 1.6 k times shows the existence of words $u_0, u_1 \in E_2$ such that

$$w = a(dba')^k u_0 b u_1 c'^k c.$$

We verify that $u_0, u_1 \in U^*$. Assume $u_0 \notin U^*$. Then $u_0 b$ is a left factor of a word $v \in U^*$, and by the form of the elements of U , $v \in U^* \theta(a_i)$ for some $i \in \{1, \dots, n\}$. But then either adb or $a'db$ is a right factor of $u_0 b$, and d is a proper right factor of u_0 which is impossible since $u_0 \in E_2$. Thus $u_0 \in U^*$ and similarly $u_1 \in U^*$. Consequently f factorizes into $f = a_k f_0 b f_1 c_k$ with $\theta(f_0) = u_0$, $\theta(f_1) = u_1$. Since $u_0, u_1 \in E_2 \cap U^*$, it follows by induction that $f_0, f_1 \in E_n$, whence $f \in E_n$. This completes the first part of the proof.

In order to prove the relation $E = E_1 \geq E_2$, consider the morphism $\psi: Y_2^* \rightarrow Y^*$

with $Y = Y_1$ defined by

$$\begin{aligned}\psi(a_1) &= \alpha_1 = adba & \psi(c_1) &= \gamma_1 = cc \\ \psi(a_2) &= \alpha_2 = aa & \psi(c_2) &= \gamma_2 = cbdc \\ \psi(b) &= b & \psi(d) &= d.\end{aligned}$$

The set $V = \psi(Y_2)$ is a prefix code. Next

$$\xi \xrightarrow{*} \alpha_i \xi b \xi \gamma_i \quad i = 1, 2$$

in the grammar $G = G_1$ generating E , and therefore

$$\psi(E_2) \subset E \cap V^*.$$

The converse inclusion $\psi^{-1}(E \cap V^*) \subset E_2$ is proved by induction. Let $f \in \psi^{-1}(E \cap V^*)$. If $|f| = 1$, then $f = d \in E_2$. Suppose $|f| > 1$, and set $w = \psi(f)$. Since $w \neq d$, w contains occurrences of α_1 or α_2 , thus f contains occurrences of a_1 , a_2 . We consider the right most occurrence of a letter a_1 or a_2 in f . Then f factorizes into

$$f = ga_k h' \quad k \in \{1, 2\},$$

and $h' \in (Y_2 \setminus \{a_1, a_2\})^*$. Define $u = \psi(g)$, $v' = \psi(h')$. Then $v' \in \{b, d, c\}^*$.

If $k = 1$, then $w = uadbav'$, and in view of Lemma 1.6, there exist words $w_0, w_1 \in E$, such that

$$w = uadbaw_0bw_1ccv, \quad \text{with } v' = w_0bw_1ccv.$$

Since v' contains no occurrence of the letter a , we have $w_0 = w_1 = d$. Thus $v' = dbdccv$, and $v \in V^*$. Therefore

$$f = ga_1dbdc_1h,$$

with $\psi(h) = v$. Consider the word $f' = gdh$. Then $\psi(f') = udv$, and since $w \equiv udv \pmod{\eta_1}$, Lemma 1.5 implies that $udv \in E$. Since also $udv \in V^*$, we have $f' \in E_2$ by induction. Next $f' \equiv f \pmod{\eta_2}$, whence $f \in E_2$.

If $k = 2$, then $w = uaav'$, and in view of Lemma 1.6 there are words $w_0, w_1, w_2 \in E$ such that

$$w = uaaw_0bw_1cbw_2cv, \quad v' = w_0bw_1cbw_2cv.$$

As above, $w_0 = w_1 = w_2 = d$, which implies that $v \in V^*$ and

$$f = ga_2dbdc_2h$$

with $\psi(h) = v$. We conclude as above that $f \in E_2$. Thus $E_2 = \psi^{-1}(E \cap V^*)$ and therefore $E \geq E_2$. ■

Corollary 1.8 *The languages $E_n (n \geq 1)$ are generators of the cone of algebraic languages.*

Proof. We prove that $E_3 \geq D_2^*$. Let indeed $\varphi: Y_3^* \rightarrow Z_2^*$ be the morphism defined by

$$\begin{aligned}\varphi(a_i) &= x_i, & \varphi(c_i) &= \bar{x}_i & i &= 1, 2 \\ \varphi(a_3) &= \varphi(c_3) = \varphi(b) = \varphi(d) = 1.\end{aligned}$$

The language $\varphi(E_3)$ is generated by the grammar $\varphi(G_3)$ with productions:

$$\xi \rightarrow x_1 \xi \xi \bar{x}_1 + x_2 \xi \xi \bar{x}_2 + \xi \xi + 1.$$

It is straightforward (see Exercise II.3.2) that this grammar generates D_2^* . Thus $\varphi(E_3) = D_2^*$. ■

We mention the following consequence of Theorem 1.7:

Corollary 1.9 *Let X be an alphabet, and let $A = \{\alpha, \beta, \gamma, \delta\} \subset X^+$ be a code. Then the language E_A generated by the grammar with productions*

$$\xi \rightarrow \alpha \xi \beta \xi \gamma + \delta$$

is a generator of the cones of algebraic languages.

Proof. Let $Y = \{a, b, c, d\}$ and $E \subset Y^*$ as above. The morphism $\varphi: Y^* \rightarrow X^*$ defined by $\varphi(a) = \alpha$, $\varphi(b) = \beta$, $\varphi(c) = \gamma$, $\varphi(d) = \delta$ clearly satisfies $\varphi(E) = E_A$. Since A is a code, φ is injective. Consequently $E = \varphi^{-1}\varphi(E) = \varphi^{-1}(E_A)$ and $E_A \approx E$. Thus the corollary follows from Theorem 1.7. ■

We now examine some variations of the language E . For a complete classification, the reader is referred to the paper of Autebert [1973] already mentioned.

Proposition 1.10 *The language $E' \subset \{a, c\}^*$ generated by the grammar with productions*

$$\xi \rightarrow a \xi \xi c + 1$$

is a generator of the cone Alg.

Corollary 1.11 *The languages E'_1 and E'_2 defined by the equations*

$$E'_1 = aE'_1bE'_1c \cup 1; \quad E'_2 = aE'_2E'_2c \cup d$$

are generators of the cone Alg.

Proof. The language E' is an obvious homomorphic image of both E'_1 and E'_2 . ■

Proof of Proposition 1.10. Set $X = \{a, c\}$ and define

$$\alpha = aaac, \quad \beta = ca, \quad \gamma = accc, \quad \delta = ac,$$

$$A = \{\alpha, \beta, \gamma, \delta\}, \quad K = (\alpha^* \cup \delta\gamma^*\beta)^*\delta\gamma^*.$$

Clearly K is a regular language, and A is a code.

We shall prove the equality

$$E' \cap K = E_A$$

which proves the assertion in view of Corollary 1.9. For this, define $L = E' \setminus \{1\}$. Since $L \cap K = E' \cap K$, it suffices to show

$$L \cap K = E_A.$$

The language L is generated by the grammar H with productions

$$\xi \rightarrow a\xi\xi c + a\xi c + ac.$$

This implies that L is contained in D'_1 (with $x_1 = a, \bar{x}_1 = c$) by a straightforward induction. Thus L is bifix. The following formulas are easily verified:

$$\xi \xrightarrow{H} \alpha\xi\beta\xi\gamma; \quad \xi \xrightarrow{H} \delta; \quad (1.3)$$

$$\alpha K \beta K \gamma \subset K, \delta \in K; \quad (1.4)$$

$$\alpha w \gamma \in K \Rightarrow w \in K; \quad (1.5)$$

$$awc \in L \Rightarrow w \in 1 \cup L \cup L^2. \quad (1.6)$$

By (1.3) $\alpha L \beta L \gamma \cup \delta \subset L$, whence $L \supset E_A$. By (1.4) we have $K \supset E_A$, and thus $E_A \subset L \cap K$. The converse inclusion $L \cap K \subset E_A$ is proved by induction. Let $w \in L \cap K$. The shortest word in K is δ , and $\delta \in E_A$. Assume $w \neq \delta$. Then w starts with a letter a , and ends with a letter c . Since $w \in A^*$, w starts with α, γ or δ and ends with α, γ or δ . Since $w \in L$ and L is bifix, w cannot start or end with δ . Next, by the form of K , w cannot start with γ nor end with α . Thus

$$w = \alpha g \gamma = aaacgaccc$$

for some $g \in X^*$. By (1.5), $g \in K$. By (1.6),

$$w' = aacgacc \in L \cup L^2.$$

Assume $w' \in L$. Then $w'' = acgac \in L \cup L^2$ by (1.6), and since L is bifix and $ac \in L$, one has $g = 1$ and $w = \alpha\gamma$. But since $\alpha\gamma \notin K$ this is impossible. Thus $w' \in L^2$, and there are words $u, v \in 1 \cup L \cup L^2$ such that

$$w' = aacgacc = aucavc, \quad \text{thus} \quad acgac = ucav.$$

Since $u \neq 1$ and $u \neq a$, ac is a left factor of u and similarly ac is a right factor

of v . Thus $u = ach_1$ and $v = h_2ac$ for some words $h_1, h_2 \in 1 \cup L$. Thus

$$w = \alpha h_1 \beta h_2 \gamma.$$

Next $h_1 \neq 1$ since $\alpha\beta$ is not a left factor of a word of K . Similarly, $h_2 \neq 1$, and $h_1, h_2 \in L$. We claim that

$$h_1, h_2 \in L, \quad h_1 \beta h_2 \in K \Rightarrow h_1, h_2 \in K. \quad (1.7)$$

Taking (1.7) for granted for a moment, we recall that $g = h_1 \beta h_2 \in K$. Thus $h_1, h_2 \in L \cap K$ and $h_1 h_2 \in E_A$ by the induction hypothesis. Consequently $w \in E_A$ which is the desired conclusion.

To prove (1.7), consider the unique factorization

$$g = h_1 \beta h_2 = u_1 u_2 \cdots u_s$$

of g with $u_1, \dots, u_s \in A$. Let n be the least integer such that h_1 is a left factor of $u_1 u_2 \cdots u_n$. If $h_1 = u_1 \cdots u_n$, then $\beta = u_{n+1}$ since β is the only word in A starting with the letter c . Consequently $h_2 = u_{n+2} \cdots u_s \in A^*$, and since $h_1 \beta h_2 \in K$, we have $h_1, h_2 \in K$.

Assume $h_1 \neq u_1 \cdots u_n$. Then $h_1 v = u_1 \cdots u_n$, where $v \neq 1$ is a proper right factor of u_n . Since $\beta = ca$ is a proper factor of none of the words in A , β cannot be a left factor of v . Thus necessarily $v = c$. Since the words in L have even length, $|h_1 c|$ is odd. The length of the words in A^* are even, and consequently $|h_1 c| = |u_1 \cdots u_n|$ is even. This is a contradiction. Thus (1.7) is proved. ■

Exercises

1.1 Define a morphism $\beta: Z_n^* \rightarrow Z_n^*$ by

$$\beta(x_i) = x_2 x_1^i, \quad \beta(\bar{x}_i) = \bar{x}_1 \bar{x}_2 \quad i = 1, \dots, n.$$

Show that $D_n^* = \beta^{-1}(D_2^* \cap \beta(Z_n^*))$, and $D_n^* \not\subseteq \beta^{-1}(D_2^* \cap \beta(Z_n^*))$.

1.2 Show that the language $L \subset \{a, b, c\}^*$ defined by $L = aLbLcL \cup \{1\}$ is a generator of Alg.

1.3 (Schützenberger [1973]) Show that the language $M \subset \{a, \bar{a}\}^*$ defined by $M = aMM\bar{a} \cup a\bar{a}$ is a generator of Alg. (Hint. Show that $M \geq M'$, where M' is given by $M' = aM'M'\bar{a} \cup b\bar{b}$.)

1.4 Let L be defined by $L = aLbL \cup d$. Show that $L \approx D_1^*$. (As already mentioned D_1^* is not a generator of Alg. Thus the letter c cannot be erased in E without losing the generator property of E .)

1.5 Let N be defined by $N = aNNa \cup d$. Show that N is a generator of Alg. (Hint. Proceed as in the proof of Proposition 1.10, with $\alpha = aada, \beta = daaad, \gamma = adaa, \delta = d$.)

1.6 Show that $[w]_{s_n} \approx [w']_{s_n}$ for any $w, w' \in Z_n^*$, and that $[w]_{s_n}$ is a generator of Alg for any $w \in Z_n^*$. Same exercise for δ'_n .

1.7 Prove a Chomsky-Schützenberger like theorem for the family E_n , ($n \geq 1$): For any $L \in \text{Alg}$, there exist an integer n , a morphism φ and a regular language K such that $L = \varphi(E_n \cap K)$.

VII.2 The Syntactic Lemma

For the investigation of families of languages with respect to substitution, the "Syntactic Lemma" due to S. A. Greibach is a basic tool. By means of this lemma, some information about the families $\mathcal{L}$ and $\mathcal{M}$ can be derived from properties of the substitution $\mathcal{L} \square \mathcal{M}$. Further the lemma gives a method to construct infinite ascending chains of cones and full AFLs, and thus of nonprincipal full AFLs. These applications will be given in the next section. The material for this and the next section is from Greibach [1970]. The present statement of the Syntactic Lemma is more precise than the original one. It is due to Beauquier [1978b]. For related topics and extensions, see Boasson, Crestin and Nivat [1973] and Greibach [1972].

Theorem 2.1 (Syntactic Lemma) *Let L and M be languages over disjoint alphabets, and let $\mathcal{L}, \mathcal{M}$ be cones. If $L \uparrow M \in \mathcal{L} \square \mathcal{M}$, then $L \in \mathcal{L}$ or $M \in \mathcal{M}$.*

If $A = L \uparrow M \in \mathcal{L} \square \mathcal{M}$, then $A = \theta(B)$ for some $B \in \mathcal{L}$ and for some $\mathcal{M}$ -substitution θ . Thus $L \uparrow M$ and $\theta(B)$ represent alternative parsings of words in A . The theorem claims that the form of A forces such constraints on the second parsing that either L can be recovered from B or M can be obtained from one of the languages $\theta(x)$, ($x \in X_B$) by a rational transduction.

Note that in the theorem, the conclusion cannot be replaced by: $L \in \mathcal{L}$ and $M \in \mathcal{M}$ (Exercise 2.1).

Proof. Let $L \subset X^*$ and $M \subset Y^*$. First we handle some trivial cases. If $L = \emptyset$ or $M = \emptyset$, then $L \in \mathcal{L}$ or $M \in \mathcal{M}$. If $L = \{1\}$, or $M = \{1\}$, then $L \in \mathcal{L}$ or $M \in \mathcal{M}$. Next $(L \setminus 1) \uparrow (M \setminus 1) = L \uparrow M \cap (Y^+ X)^+$, thus $L \uparrow M \in \mathcal{L} \square \mathcal{M}$ implies $(L \setminus 1) \uparrow (M \setminus 1) \in \mathcal{L} \square \mathcal{M}$. Further, if $L \setminus 1 \in \mathcal{L}$ then $L \in \mathcal{L}$ and similarly for M . Thus it suffices to prove the theorem in the case where $1 \notin L, 1 \notin M$.

Assume $\emptyset \neq L \subset X^+$, $\emptyset \neq M \subset Y^+$. Since $A = L \uparrow M \in \mathcal{L} \square \mathcal{M}$, there exist a language $B \in \mathcal{L}$, and a $\mathcal{M}$ -substitution $\theta: X_B^* \rightarrow (X \cup Y)^*$ such that $A = L \uparrow M = \theta(B)$. Thus any word $f \in A$ has at least two factorizations, a first one of the form

$$f = m_1 x_1 m_2 x_2 \cdots m_p x_p \quad (2.1)$$

with $m_1, \dots, m_p \in M$, $x_1, \dots, x_p \in X$, $x_1 \cdots x_p \in L$, and a second one of the form

$$f = d_1 d_2 \cdots d_q, \quad (2.2)$$

where $d_i \in \theta(z_i)$, $z_i \in X_B$, and $z_1 \cdots z_q \in B$. A factorization (2.2) is a θ -factorization of f . Note that a word $f \in A$ has just one factorization (2.1), but may admit several θ -factorizations.

Let $k \geq 1$ be an integer. We say that the θ -factorization (2.2) splits at order k or k -splits if each d_j , ($1 \leq j \leq q$) contains at most k letters $x \in X$. We now distinguish two cases:

a) There exists an integer $k \geq 1$ such that for each $u = x_1 \cdots x_p \in L$, there are words $m_1, \dots, m_p \in M$ such that $f = m_1 x_1 \cdots m_p x_p$ has a θ -factorization that splits at order k .

b) For all integers $k \geq 1$, there is a word $u = x_1 \cdots x_p \in L$ such that for all $m_1, \dots, m_p \in M$, no θ -factorization of $f = m_1 x_1 \cdots m_p x_p$ splits at order k .

Assume that a) holds and define a substitution $\bar{\theta}: X_B^* \rightarrow (X \cup Y)^*$ by

$$\bar{\theta}(z) = \theta(z) \cap T_k \quad z \in X_B,$$

where $T_k = \{g \in (X \cup Y)^* \mid |g|_X \leq k\}$. Clearly $\bar{\theta}(z) \in \mathcal{M}$ since $\theta(z) \in \mathcal{M}$ and $\mathcal{M}$ is a cone. Further $\bar{\theta}(B) \subset \theta(B) = A$. In fact, $\bar{\theta}(B)$ is precisely the set of words in A that have a k -splitting θ -factorization. Thus by the assumption $\bar{\theta}(B) = A$. Next let $\pi: (X \cup Y)^* \rightarrow X^*$ be the projection. Then for $z \in X_B$, $\pi(\bar{\theta}(z)) \subset 1 \cup X \cup \cdots \cup X^k$. Thus $\sigma = \pi \circ \bar{\theta}: X_B^* \rightarrow X^*$ is a finite substitution, hence a rational transduction, and $\sigma(B) \in \mathcal{L}$. Since

$$\sigma(B) = \pi(\bar{\theta}(B)) = \pi(A) = L,$$

we have $L \in \mathcal{L}$.

Assume now that b) holds. Let $n \geq 1$ be an integer, and define

$$M_n = \{w \in M \mid |w| \leq n\}, \quad k = k_n = \text{Card}(M_n).$$

Let $u = x_1 \cdots x_p \in L$ be a word such that the conclusion of b) holds for the fixed integer $k = k_n$. Then clearly $p \geq k$. Define q, s by $p = qk + s$, ($0 \leq s < k$). Consider any enumeration of the words in M_n :

$$M_n = \{w_1, w_2, \dots, w_k\}$$

and define a word $f = w_1 x_1 \cdots w_p x_p$ by setting $w_j = w_i$ whenever $j \equiv i \pmod{k}$ and $0 < i \leq k$, i.e.

$$f = w_1 x_1 \cdots w_k x_k w_{k+1} x_{k+1} \cdots w_k x_k w_{k+1} x_{k+1} \cdots w_s x_p.$$

Next consider a θ -factorization (2.2) of this word f . By assumption, there is a factor d_j that contains at least $k+1$ letters in X , thus d_j has the form

$$d_j = u' x_r w_t x_{r+1} \cdots w_k x_{jk} w_1 x_{j+1} \cdots w_{t-1} x_{r+k} v' \quad (2.3)$$

for some integers r, t, j , and some words u', v' .

Now define a transduction $\tau: (X \cup Y)^* \rightarrow Y^*$ by

$$\tau(g) = \{m \in Y^* : g \in (X \cup Y)^* X m X (X \cup Y)^*\} \quad g \in (X \cup Y)^*.$$

Thus $\tau(g)$ is the set of all factors $m \in Y^*$ of g such that xmx' is a factor of g for some letters $x, x' \in X$. The transduction τ is rational since its graph

$$R = [(X \cup Y)^* X \times \{1\}] \{(y, y) : y \in Y\}^* [X(X \cup Y)^* \times \{1\}]$$

is a rational relation. It follows immediately from (2.3) that $\tau(d_j) \supset M_n$. Next obviously $\tau(\theta(z)) \subset M$ for all $z \in X_B$. Combining both inclusions, there exists a letter $z \in X_B$ such that

$$M_n \subset \tau(\theta(z)) \subset M.$$

Thus if b) holds, then for any integer $n \geq 1$, there is a letter $z = z_n \in X_B$ such that

$$M_n \subset \tau(\theta(z_n)). \quad (2.4)$$

This implies that $M = \tau(\theta(\hat{z}))$ for some $\hat{z} \in X_B$. Indeed, assume the contrary. Then there is a word $w \in M$ which is in none of the languages $\tau(\theta(z))$, ($z \in X_B$). Setting $n = |w|$, this contradicts (2.4). Since θ is an M -substitution, $\theta(\hat{z}) \in M$. Further, since M is a cone and τ is rational, $M \in \mathcal{M}$.

Thus we have proved that if a) holds, then $L \in \mathcal{L}$, and if b) holds then $M \in \mathcal{M}$. Since one of these conditions is always satisfied, the proof is complete. ■

There are several useful formulations of the Syntactic Lemma in terms of families of languages.

Corollary 2.2 *Let $\mathcal{L}, \mathcal{L}', \mathcal{M}, \mathcal{M}'$ be cones. If $\mathcal{L}' \setminus \mathcal{L} \neq \emptyset$ and $\mathcal{M}' \setminus \mathcal{M} \neq \emptyset$, then $\mathcal{L}' \sqcup \mathcal{M}' \setminus \mathcal{L} \sqcup \mathcal{M} \neq \emptyset$.*

Proof. Let $L \in \mathcal{L}' \setminus \mathcal{L}$, $M \in \mathcal{M}' \setminus \mathcal{M}$. Since the families are closed under copy, we may assume $X_L \cap X_M = \emptyset$. Next $A = L \uparrow M \in \mathcal{L}' \sqcup \mathcal{M}'$. Suppose that $A \in \mathcal{L} \sqcup \mathcal{M}$. Then by the Syntactic Lemma $L \in \mathcal{L}$ or $M \in \mathcal{M}$. Thus $A \notin \mathcal{L} \sqcup \mathcal{M}$. ■

The property of “factorization” of the Syntactic Lemma appears clearly in the following corollary which is just a reformulation of the above statement.

Corollary 2.3 *Let $\mathcal{L}, \mathcal{L}', \mathcal{M}, \mathcal{M}'$ be cones. If $\mathcal{L} \sqcup \mathcal{M} \subset \mathcal{L}' \sqcup \mathcal{M}'$, then $\mathcal{L} \subset \mathcal{L}'$ or $\mathcal{M} \subset \mathcal{M}'$.*

Proof. Suppose the conclusion is false. Then $\mathcal{L} \setminus \mathcal{L}' \neq \emptyset$ and $\mathcal{M} \setminus \mathcal{M}' \neq \emptyset$. By Corollary 2.2, $\mathcal{L} \sqcup \mathcal{M} \setminus \mathcal{L}' \sqcup \mathcal{M}' \neq \emptyset$. ■

As a first application of the Syntactic Lemma, we prove a weak converse of Theorem V.5.6.

Theorem 2.4 *Let $\mathcal{L}$ be a cone and let $\mathcal{M}$ be a cone closed under union. If $\mathcal{L} \sqcup \mathcal{M}$ is principal, then $\mathcal{L}$ or $\mathcal{M}$ is principal.*

Note that as for the Syntactic Lemma, the conclusion : $\mathcal{L}$ and $\mathcal{M}$ are principal is false (see Exercise 3.1).

Proof. Let A be a generator of $\mathcal{L} \sqcup \mathcal{M} : \mathcal{L} \sqcup \mathcal{M} = A\Gamma$. Then $A = \sigma(L)$ with $L \in \mathcal{L}$ and $\sigma : X_L^* \rightarrow X_A^*$ a M -substitution. By Proposition V.5.4, there is a language $M \in \mathcal{M} \text{ Elm} = \mathcal{M}$ such that $A \leq L \uparrow M$. Since $L \uparrow M \in L\Gamma \sqcup M\Gamma$ and $L\Gamma \sqcup M\Gamma$ is a cone, it follows that $A \in L\Gamma \sqcup M\Gamma$ and consequently $\mathcal{L} \sqcup \mathcal{M} \subset L\Gamma \sqcup M\Gamma$. In view of Corollary 2.3, $\mathcal{L} \subset L\Gamma$ or $\mathcal{M} \subset M\Gamma$. Since $L\Gamma \subset \mathcal{L}$ and $M\Gamma \subset \mathcal{M}$, this implies $\mathcal{L} = L\Gamma$ or $\mathcal{M} = M\Gamma$. ■

Corollary 2.5 *Let $\mathcal{L}$ be a cone closed under union. Then $\mathcal{L}$ is principal iff $\mathcal{L} \sqcup \mathcal{L}$ is principal.* ■

Exercises

2.1 Show that in the Syntactic Lemma, the “or” in the conclusion cannot be replaced by “and”. (Hint. Consider a language A which can be written in two different way as syntactic substitution: $A = L \uparrow M = L' \uparrow M'$ with $L \neq L'$ and $M \neq M'$.)

2.2 Let A_i, B_i be languages with $X_{A_i} \cap X_{B_i} = \emptyset$, ($i = 1, 2$). Show that $A_1 \uparrow B_1 \leq A_2 \uparrow B_2$ implies $A_1 \leq A_2$ or $B_1 \leq B_2$.

2.3 Let $\mathcal{L}$ and $\mathcal{M}$ be incomparable cones. Show that $\mathcal{L} \sqcup \mathcal{M}$ and $\mathcal{M} \sqcup \mathcal{L}$ are incomparable.

VII.3 Substitution Closure

This section contains applications of the Syntactic Lemma both to cones closed under substitution, and to cones not closed under substitution. For principal cones closed under substitution, the existence of a largest full AFL properly contained in it will be proved. Cones not closed under substitution are shown to produce infinite ascending chains of cones and thus nonprincipal cones.

A cone closed under substitution is a full AFL (Proposition V.5.5). Thus cones closed under substitution are idempotent elements in the semigroup of all families of languages with respect to the product $\sqcup$. We first show that such an idempotent cannot be a nontrivial product of two other cones.

Proposition 3.1 *Let $\mathcal{L}$ and $\mathcal{M}$ be cones, and set $\mathcal{N} = \mathcal{L} \sqcup \mathcal{M}$. If $\mathcal{N}$ is closed under substitution, then $\mathcal{N} = \mathcal{L}$ or $\mathcal{N} = \mathcal{M}$.*

Proof. Since $\mathcal{N}$ is closed under substitution, $\mathcal{N} \sqcup \mathcal{N} \subset \mathcal{L} \sqcup \mathcal{M}$. Hence $\mathcal{N} \subset \mathcal{L}$ or $\mathcal{N} \subset \mathcal{M}$ by Corollary 2.3. Since $\mathcal{L} \subset \mathcal{N}$ and $\mathcal{M} \subset \mathcal{N}$, it follows that $\mathcal{N} = \mathcal{L}$ or $\mathcal{N} = \mathcal{M}$. ■

From Proposition 3.1, we obtain:

Proposition 3.2 *Let $\mathcal{L}$ be a substitution closed full AFL, and let $\mathcal{M}$ be a family of languages. If $\mathcal{L} = \mathcal{M}\Gamma$, then $\mathcal{L} = \mathcal{M}\Gamma$.*

Proof. Observe that $\mathcal{L} = M\hat{\Gamma} = M\Gamma \text{ Rat} = \text{Rat} \sqcup M\Gamma$. Thus by Proposition 3.1, $\mathcal{L} = \text{Rat}$ or $\mathcal{L} = M\Gamma$. In the first case $M \subset \text{Rat}$. Thus in both cases, $M\Gamma = M\hat{\Gamma}$. ■

Proposition 3.2 is interesting when $\mathcal{L}$ is principal.

Corollary 3.3 *Let $\mathcal{L}$ be a substitution closed full principal AFL. If $\mathcal{L} = A\hat{\Gamma}$, then $\mathcal{L} = A\Gamma$.* ■

Thus the set of generators of the cone $\mathcal{L}$ is equal to the set of generators of the full AFL $\mathcal{L}$.

Example 3.1 The cone Alg is closed under substitution. Thus any context-free language L such that $L\hat{\Gamma} = \text{Alg}$ also satisfies $\text{Alg} = L\Gamma$.

For any cone $\mathcal{L}$, define the sets of generators and nongenerators of $\mathcal{L}$ as follows:

$$\text{Gen}(\mathcal{L}) = \{L \in \mathcal{L} \mid L\Gamma = \mathcal{L}\} \quad \text{Ng}(\mathcal{L}) = \{L \in \mathcal{L} \mid L\Gamma \subsetneq \mathcal{L}\} = \mathcal{L} \setminus \text{Gen}(\mathcal{L}).$$

Clearly $\text{Gen}(\mathcal{L}) \neq \emptyset$ iff $\mathcal{L}$ is principal, and $\text{Ng}(\mathcal{L}) \neq \{\emptyset\}$ iff $\mathcal{L} \neq \text{Rat}$. If both conditions are satisfied, then $\text{Gen}(\mathcal{L})$ and $\text{Ng}(\mathcal{L})$ are families of languages. In view of the corollary above, if $\mathcal{L}$ is closed under substitution and principal, then $\text{Gen}(\mathcal{L}) = \{L \in \mathcal{L} \mid L\hat{\Gamma} = \mathcal{L}\}$.

Proposition 3.4 *Let $\mathcal{L} \neq \text{Rat}$ be a principal cone. Then $\text{Ng}(\mathcal{L})$ is a cone, and any cone properly contained in $\mathcal{L}$ is contained in $\text{Ng}(\mathcal{L})$.*

Proof. Let $L \in \text{Ng}(\mathcal{L})$, and let M be a language such that $L \geq M$. Then $M\hat{\Gamma} \subset L\hat{\Gamma} \subsetneq \mathcal{L}$, whence $M \in \text{Ng}(\mathcal{L})$. Next let $\mathcal{M}$ be a cone contained in $\mathcal{L}$. If $\mathcal{M}$ is not contained in $\text{Ng}(\mathcal{L})$, then there is a language A in $\mathcal{M} \cap \text{Gen}(\mathcal{L})$. Consequently $\mathcal{L} = A\Gamma \subset \mathcal{M}$, and $\mathcal{M} = \mathcal{L}$. ■

If $\mathcal{L}$ is substitution closed, then a more precise result can be obtained.

Theorem 3.5 *Let $\mathcal{L} \neq \text{Rat}$ be a substitution closed full principal AFL. Then $\text{Ng}(\mathcal{L})$ is a substitution closed full AFL and is the maximal full AFL properly contained in $\mathcal{L}$.*

Proof. In view of the previous proposition, $\text{Ng}(\mathcal{L})$ is the maximal cone properly contained in $\mathcal{L}$. In view of Proposition V.5.5, it suffices to show that $\text{Ng}(\mathcal{L})$ is substitution closed. Define $\mathcal{M} = \text{Ng}(\mathcal{L}) \sqcup \text{Ng}(\mathcal{L})$. Then $\mathcal{M}$ is a cone, and $\mathcal{M} \subset \mathcal{L} \sqcup \mathcal{L} = \mathcal{L}$. Thus either $\mathcal{M} \subset \text{Ng}(\mathcal{L})$ whence $\mathcal{M} = \text{Ng}(\mathcal{L})$, or $\mathcal{M} = \mathcal{L}$. Assume the second case holds, i.e. $\mathcal{L} = \text{Ng}(\mathcal{L}) \sqcup \text{Ng}(\mathcal{L})$. Then Proposition 3.1 implies that $\mathcal{L} = \text{Ng}(\mathcal{L})$, contrary to the definition. Thus $\mathcal{M} = \text{Ng}(\mathcal{L})$ and $\text{Ng}(\mathcal{L})$ is closed under substitution. ■

Example 3.1 (continued). Theorem 3.5 asserts the existence of a maximal full AFL $\text{Ng}(\text{Alg})$ properly contained in Alg. Thus $\text{Lin} \subset \text{Ng}(\text{Alg})$, and since $\text{Ng}(\text{Alg})$ is closed under substitution, $\text{Lin } \overline{\text{Lin}}^*$ is contained in $\text{Ng}(\text{Alg})$. It is not known whether $\text{Ng}(\text{Alg})$ is principal or not (see also below).

We now apply the Syntactic Lemma to the construction of nonprincipal cones or AFLs. This will be done by showing the existence of infinite strictly ascending chains of cones. In the sequel of this section, we use the simplified notation $\mathcal{L}\mathcal{M}$ for $\mathcal{L} \sqcup \mathcal{M}$. Thus in particular

$$\mathcal{L}\mathcal{L} = \mathcal{L} \sqcup \mathcal{L}, \quad \mathcal{L}^n = \mathcal{L} \sqcup \mathcal{L}^{n-1} = \mathcal{L}\mathcal{L}^{n-1} \quad (n \geq 2), \quad \mathcal{L}^1 = \mathcal{L}.$$

Theorem 3.6 *Let $\mathcal{L}$ be a cone. If $\mathcal{L}$ is not closed under substitution, then $\mathcal{L}^k \subsetneq \mathcal{L}^{k+1}$ for any $k \geq 1$ and $\mathcal{L}\overline{\mathcal{L}}^*$ is nonprincipal.*

Since $\mathcal{L}\overline{\mathcal{L}}^*$ is closed under substitution (Corollary VI.3.3) the nonprincipality as a cone or as a full AFL are equivalent by Corollary 3.3.

Proof. By assumption, $\mathcal{L} \subsetneq \mathcal{L}^2$. Suppose that $\mathcal{L}^k = \mathcal{L}^{k+1}$ for some k , and let n be the least integer such that $\mathcal{L}^n = \mathcal{L}^{n+1}$. Then $n \geq 2$. Next $\mathcal{L}^n = \mathcal{L}^{n+l}$ for $l \geq 1$. Thus $\mathcal{L}^n = \mathcal{L}^{2n}$. Hence $\mathcal{L}^n$ is substitution closed. Since $n \geq 2$, $\mathcal{L}^n = \mathcal{L}\mathcal{L}^{n-1}$. In view of Proposition 3.1, $\mathcal{L}^n = \mathcal{L}$ or $\mathcal{L}^n = \mathcal{L}^{n-1}$. The first equality is impossible since $\mathcal{L} \subsetneq \mathcal{L}^2 \subset \mathcal{L}^n$, and the second is ruled out by the minimality assumption on n . Thus $\mathcal{L}^k \subsetneq \mathcal{L}^{k+1}$ for any $k \geq 1$.

Next assume $\mathcal{M} = \mathcal{L}\overline{\mathcal{L}}^* = \bigcup_{k \geq 1} \mathcal{L}^k$ is principal, and let A be a generator of $\mathcal{M}$.

Then $\mathcal{M} = A\hat{\Gamma} = A\Gamma$. There exists an integer k such that $A \in \mathcal{L}^k$. Consequently, $\mathcal{L}^{k+1} \subset \mathcal{M} = A\Gamma \subset \mathcal{L}^k\Gamma = \mathcal{L}^k$, in contradiction with the first part of the proof. Hence $\mathcal{M}$ is nonprincipal. ■

Example 3.2 The cone Lin of linear languages is principal and is not closed under substitution. Consequently, there is an ascending chain

$$\text{Lin} \subsetneq (\text{Lin})^2 \subsetneq \cdots \subsetneq (\text{Lin})^k \subsetneq \cdots$$

of principal cones, and the substitution closure

$$\text{Lin } \overline{\text{Lin}}^* = \bigcup_{k \geq 1} (\text{Lin})^k$$

is not principal. $\text{Lin } \overline{\text{Lin}}^* = \text{Qrt}$ is the family of quasi-rational or standard matching choice or nonexpansive or derivation bounded languages. The cone $(\text{Lin})^k$ is denoted by $\text{Qrt}(k)$ and is called the family of quasi-rational languages of rank k . Quasi-rational languages will be studied in more detail in Section 5.

Example 3.3 In the next section, we shall consider the cone generated by the Dyck language D_1^* . This is the cone of restricted one counter languages. We shall see later that $D_1^*\Gamma$, also denoted Rocl , is not a full AFL. Thus we obtain an ascending chain $\text{Rocl} \subsetneq \cdots \subsetneq (\text{Rocl})^n \subsetneq \cdots$ of principal cones, and the family $\text{Fcl} = \text{Rocl } \overline{\text{Rocl}}^*$ of finite counter languages is not principal and therefore is contained in $\text{Ng}(\text{Alg})$. We note $\text{Fcl}(k)$ the cone $(\text{Rocl})^k$. In Section VIII.7 we prove that Rocl and Lin are incomparable, and even that Rocl is

incomparable with Qrt and symmetrically, that Fcl and Lin are incomparable. These results cannot be derived from the general methods described in this chapter (see also Exercise 3.3). The combination of Lin and Rocl gives another example of a substitution closed full AFL properly contained in Alg. We use the following proposition.

Proposition 3.7 Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be two incomparable cones, and set $\mathcal{L} = \mathcal{L}_1 \cup \mathcal{L}_2$. Then $\mathcal{L}\mathcal{L}^*$ is nonprincipal.

Proof. It suffices to show that the cone $\mathcal{L}$ is not a full AFL, and to apply Theorem 3.6. We verify that $\mathcal{L}$ is not closed under union. Consider indeed languages $L_1 \in \mathcal{L}_1 \setminus \mathcal{L}_2$, and $L_2 \in \mathcal{L}_2 \setminus \mathcal{L}_1$. Since $\mathcal{L}_1$ and $\mathcal{L}_2$ are cones, we may assume $L_1 \subset X_1^+$, $L_2 \subset X_2^+$ for some disjoint alphabets X_1, X_2 . Let $L = L_1 \cup L_2$. Assume $L \in \mathcal{L}_1$. Then $L \cap X_2^* = L_2 \in \mathcal{L}_1$. Thus $L \notin \mathcal{L}_1$ and similarly $L \notin \mathcal{L}_2$. Thus $\mathcal{L}$ is not closed under union. ■

Example 3.4 The family $\text{Gre} = (\text{Rocl} \cup \text{Lin})(\overline{\text{Rocl} \cup \text{Lin}})^*$ is the substitution closure of the restricted one counter languages and the linear languages. By Proposition VIII.7.1, the rational cones Rocl and Lin are incomparable. Thus in view of the previous proposition, Gre is a substitution closed nonprincipal full AFL properly contained in the principal AFL of context-free languages. Greibach [1970] conjectured that $\text{Gre} = \text{Ng}(\text{Alg})$. Boasson [1973b] has proved that the inclusion of Gre in Ng(Alg) is proper. A characterization of Ng(Alg) is still lacking.

Exercises

3.1 Give examples of cones $\mathcal{L}$ and $\mathcal{M}$ such that $\mathcal{L} \sqsubset \mathcal{M}$ is principal and either $\mathcal{L}$ or $\mathcal{M}$ is nonprincipal. (Hint. Take Qrt for $\mathcal{L}$ or $\mathcal{M}$.)

3.2 Let $\mathcal{L}$ be a cone which is not a full AFL. Show that $\mathcal{L}^k \subsetneq \mathcal{L}^k \hat{\Gamma} \subsetneq \mathcal{L}^{k+1}$ for $k \geq 1$.

3.3 Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be two incomparable cones. Show that if none of $\mathcal{L}_1$ and $\mathcal{L}_2$ is substitution closed, then $\mathcal{L}_1^n$ and $\mathcal{L}_2^n$ are incomparable for any $n \geq 2$. (Thus $(\text{Rocl})^n$ and $(\text{Lin})^n$ are incomparable.)

3.4 Let $\mathcal{L}$ be a substitution closed full principal AFL, and let L be a generator of $\mathcal{L}$. Show that for any regular language K , $L \cap K$ or $L \cap (X_L^* \setminus K)$ is a generator of $\mathcal{L}$.

3.5 (Greibach [1970]) Let $\mathcal{L}$ and $\mathcal{M}$ be two incomparable cones not closed under substitution. Assume further that $\mathcal{L} \not\subset \mathcal{M}\mathcal{M}^*$ and $\mathcal{M} \not\subset \mathcal{L}\mathcal{L}^*$. (This situation is realized for $\mathcal{L} = \text{Lin}$, $\mathcal{M} = \text{Rocl}$. See Section VIII.7.)

a) Show that $\mathcal{M}^p \subset \mathcal{M}^n \mathcal{L}^n$ (resp. $\mathcal{M}^p \subset \mathcal{L}^n \mathcal{M}^n$) iff $p \leq q$, ($p, q, n \geq 1$).

b) Show that $\mathcal{L}^n \mathcal{M}^p \subset \mathcal{L}^m \mathcal{M}^q$ iff $n \leq m$ and $p \leq q$, ($p, q, n, m \geq 1$).

For $k \geq 1$, $n_1, n_2, \dots, n_k \geq 1$ define

$$\mathcal{L}(n_1, n_2, \dots, n_k) = \begin{cases} \mathcal{L}^{n_1} \mathcal{M}^{n_2} \dots \mathcal{L}^{n_{k-1}} \mathcal{M}^{n_k} & \text{if } k \text{ even,} \\ \mathcal{L}^{n_1} \mathcal{M}^{n_2} \dots \mathcal{L}^{n_k} & \text{if } k \text{ odd.} \end{cases}$$

c) Show that $\mathcal{L}(n_1, \dots, n_k, 1) \not\subset \mathcal{L}(m_1, \dots, m_k)$, and $\mathcal{M}\mathcal{L}(n_1, \dots, n_k) \not\subset \mathcal{L}(m_1, \dots, m_k)$ for all $n_1, \dots, n_k, m_1, \dots, m_k \geq 1$.

d) Show that $\mathcal{L}(2n_1, 2n_2, \dots, 2n_k) \subset \mathcal{L}(2m_1, 2m_2, \dots, 2m_k)$ iff $n_1 \leq m_1, n_2 \leq m_2, \dots, n_k \leq m_k$. (This yields hierarchies of cones which are order-isomorphic to $\mathbb{N}^k$.)

VII.4 One Counter Languages

We announced in Section 1 that the restricted Dyck language D_1^* is not a generator of the family of context-free languages. This will be proved in the next chapter. The present section is concerned with the study of the cone and the full AFL generated by D_1^* . Indeed, these two families can be characterized by restrictions on the pushdown automata (pda) recognizing them. More precisely, $D_1^* \hat{\Gamma}$ is the family of languages recognized by pda's having just one pushdown symbol. For $D_1^* \hat{\Gamma}$ the condition is slightly weaker.

If a pda has just one pushdown symbol, then only the length of the words on the pushdown store can be used for computations, and the pushdown store works as a counter. Therefore the languages in $D_1^* \hat{\Gamma}$ and $D_1^* \Gamma$ are called one counter and restricted one counter languages. Note that the restriction on pda's defining one counter languages is in some sense dual to the restriction on grammars defining linear languages.

We start with the definition of one counter pda's, introduced by Greibach [1969]. Since in this section we manipulate integers, the empty word will be denoted by ε in order to avoid confusion with the integer 1.

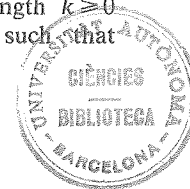
Definition A one counter pushdown automaton $M = \langle X, Q, q_-, Q_+, Y, y_0, \mathfrak{R} \rangle$ is composed of an input alphabet X , a finite set Q of states, an initial state $q_- \in Q$, a set $Q_+ \subset Q$ of final states, an alphabet Y consisting of two pushdown symbols y, y_0 , and a finite set of rules $\mathfrak{R} \subset Q \times (X \cup \varepsilon) \times Y \times Q \times Y^*$. A rule (q, u, z, q', γ) is written $(q, u, z) \rightarrow (q', \gamma)$, and $\mathfrak{R}$ is subject to the following conditions:

$$\begin{aligned} (q, u, y) \rightarrow (q', \gamma) \in \mathfrak{R} &\Rightarrow \gamma \in y^*; \\ (q, u, y_0) \rightarrow (q', \gamma) \in \mathfrak{R} &\Rightarrow \gamma \in y^* y_0. \end{aligned} \quad (4.1)$$

If $(q, u, z) \rightarrow (q', \gamma)$ is a rule, then z is called the pushdown symbol and u is the input symbol of the rule. A configuration is a triple $(q, w, \gamma) \in Q \times X^* \times Y^*$. A move is a couple of configurations denoted by

$$(q_1, w_1, \gamma_1) = (q_2, w_2, \gamma_2)$$

such that there is a rule $(q_1, u, z) \rightarrow (q_2, \gamma)$ in $\mathfrak{R}$ with $w_1 = uw_2$, $\gamma_1 = z\gamma'$, $\gamma_2 = \gamma\gamma'$ for some γ' . Note that $\gamma_1 \neq \varepsilon$. A computation of length $k \geq 0$ is a sequence of $k+1$ configurations (q_i, w_i, γ_i) , ($0 \leq i \leq k$) such that



$(q_{i-1}, w_{i-1}, \gamma_{i-1}) \equiv (q_i, w_i, \gamma_i)$ for $i = 1, \dots, k$. A computation is usually written

$$(q_0, w_0, \gamma_0) \equiv (q_1, w_1, \gamma_1) \equiv \dots \equiv (q_k, w_k, \gamma_k) \quad (4.2)$$

or shorter

$$(q_0, w_0, \gamma_0) \stackrel{k}{\equiv} (q_k, w_k, \gamma_k).$$

As usual, $\stackrel{+}{\equiv}$ and $\stackrel{*}{\equiv}$ denote the transitive and reflexive and transitive closure of $\equiv$. Note that if $\gamma_0 \in y^* y_0$ in (4.2), then $\gamma_1, \dots, \gamma_k \in y^* y_0$ by (4.1), and if $\gamma_0 \in y^+$, then $\gamma_1, \dots, \gamma_{k-1} \in y^+$ and $\gamma_k \in y^*$.

We associate to $\bar{M}$ two languages:

$$\|\bar{M}\| = \{w \in X^* \mid \exists q_+ \in Q_+, (q_-, w, y_0) \stackrel{+}{\equiv} (q_+, \varepsilon, y_0)\};$$

$$|\bar{M}| = \{w \in X^* \mid \exists q_+ \in Q_+, (q_-, w, y) \stackrel{+}{\equiv} (q_+, \varepsilon, \varepsilon)\}.$$

Clearly only rules with pushdown symbol equal to y are involved in computations of words in $|\bar{M}|$. Thus if $\mathfrak{R}$ is the set of rules with pushdown symbol y , then $|\bar{M}| = |\bar{M}'|$, where $\bar{M}' = \langle X, Q, q_-, Q_+, Y, y_0, \mathfrak{R}' \rangle$. Note that $\|\bar{M}\|$ is defined as the set of words which leave y_0 on the pushdown store. The usual definition is rather to consider the words which empty the pushdown store (see the books in the Bibliography). The definition above stems from the cited paper of Greibach. It is easy to see that both definitions are equivalent (Exercise 4.1). The present definition allows reinitialization.

A language L is a one counter language (a restricted one counter language) if $L = \|\bar{M}\|$ ($L = |\bar{M}|$) for some one counter pda $\bar{M}$. The families of one counter languages and of restricted one counter languages are denoted by Ocl and Rocl . Clearly both families are closed under copy.

Example 4.1 The Lukasiewicz language $\mathcal{L} \subset \{a, b\}^*$ is a restricted one counter language. Let $\bar{M}$ be the one counter pda with unique state q , and with rules

$$(q, a, y) \rightarrow (q, y^2), \quad (q, b, y) \rightarrow (q, \varepsilon).$$

Then it is easily seen that $w \in |\bar{M}|$ iff $|w|_a = |w|_b - 1$ and $|w'|_a \geq |w'|_b$ for any proper right factor w' of w . Consequently $|\bar{M}| = \mathcal{L}$ by Proposition II.4.1.

Example 4.2 $D_1^* \subset \{x, \bar{x}\}^*$ is a restricted one counter language. Let indeed $\bar{M}$ be the one counter pda with the two states q_-, q , with final state q and with rules

$$(q_-, x, y) \rightarrow (q_-, y^2), \quad (q_-, \bar{x}, y) \rightarrow (q_-, \varepsilon), \quad (q_-, \varepsilon, y) \rightarrow (q, \varepsilon).$$

Then $|\bar{M}| = D_1^*$ follows immediately from Corollary II.4.2.

Example 4.3 $D_1^* \subset \{x, \bar{x}\}^*$ is a one counter language. Consider indeed the one counter pda $\bar{M}$ with states $q_-, q, \bar{q}$, final state q_- and with following rules:

$$\begin{aligned} (q_-, x, y_0) &\rightarrow (q, yy_0), & (q, x, y) &\rightarrow (q, y^2), & (q, \bar{x}, y) &\rightarrow (q, \varepsilon); \\ (q_-, \bar{x}, y_0) &\rightarrow (\bar{q}, yy_0), & (\bar{q}, \bar{x}, y) &\rightarrow (\bar{q}, y^2), & (\bar{q}, x, y) &\rightarrow (q, \varepsilon); \\ (q, \varepsilon, y_0) &\rightarrow (q_-, y_0), & (\bar{q}, \varepsilon, y_0) &\rightarrow (q_-, y_0). \end{aligned}$$

Then the equality $\|\bar{M}\| = D_1^*$ follows from the relation $D_1^* = (D'_1 \cup \bar{D}'_1)^*$, where $\bar{D}'_1$ is obtained from D'_1 by exchanging x and $\bar{x}$. This relation is a consequence of formula (1.2).

Proposition 4.1 $\text{Rocl} \subset \text{Ocl}$.

Proof. Let $\bar{M} = \langle X, Q, q_-, Q_+, Y, y_0, \mathfrak{R} \rangle$ be a one counter automaton and set $L = |\bar{M}|$. We may assume that all rules of $\bar{M}$ have pushdown symbol y . Let $\bar{q}$ be a new state, and define $\bar{\bar{M}} = \langle X, Q \cup \bar{q}, \bar{q}, Q_+, Y, y, \mathfrak{R} \rangle$ by

$$\mathfrak{R} = \mathfrak{R} \cup \{(\bar{q}, \varepsilon, y_0) \rightarrow (q_-, yy_0)\}.$$

For any computation in $\bar{M}$

$$(q_-, w, y) \equiv (q_1, w_1, y^{n_1}) \equiv \dots \equiv (q_k, w_k, y^{n_k}) \equiv (q_+, \varepsilon, \varepsilon) \quad (4.3)$$

$$\begin{aligned} (\bar{q}, w, y_0) &\equiv (q_-, w, yy_0) \equiv (q_1, w_1, y^{n_1} y_0) \\ &\equiv \dots \equiv (q_k, w_k, y^{n_k} y_0) \equiv (q_+, \varepsilon, y_0) \end{aligned} \quad (4.4)$$

is a computation in $\bar{\bar{M}}$. Conversely, any computation $(\bar{q}, w, y_0) \stackrel{+}{\equiv} (q_+, \varepsilon, y_0)$ in $\bar{\bar{M}}$ factorizes into (4.4), and then (4.3) is a computation in $\bar{M}$. Thus $|\bar{M}| = \|\bar{\bar{M}}\|$. ■

Proposition 4.2 The family Ocl is closed under union, product and the plus operation.

Proof. The closure under union is straightforward. Let $L, L' \subset X^*$ be two one counter languages, and let $L = \|\bar{M}\|$, $L' = \|\bar{M}'\|$ for

$$\bar{M} = \langle X, Q, q_-, Q_+, Y, y_0, \mathfrak{R} \rangle, \quad \bar{M}' = \langle X, Q', q'_-, Q'_+, Y, y_0, \mathfrak{R}' \rangle.$$

Clearly, we may assume $Q \cap Q' = \emptyset$. Define a one counter pda

$$\bar{M}'' = \langle X, Q \cup Q', q_-, Q'_+, Y, y_0, \mathfrak{R}'' \rangle$$

with $\mathfrak{R}'' = \mathfrak{R} \cup \mathfrak{R}' \cup \{(q_+, \varepsilon, y_0) \rightarrow (q'_+, y_0) \mid q_+ \in Q_+\}$.

Then obviously $\|\bar{M}''\| = LL'$. Next let

$$\bar{M}^+ = \langle X, Q, q_-, Q_+, Y, y_0, \mathfrak{R}^+ \rangle$$

with $\mathfrak{R}^+ = \mathfrak{R} \cup \{(q_+, \varepsilon, y_0) \rightarrow (q_-, y_0) \mid q_+ \in Q_+\}$.

Then $\|\bar{M}^+\| = L^+$. ■

Note that these proofs are simplified by the possibility to reinitialize in the definition of $\bar{M}$.

Theorem 4.3 *Ocl is the rational closure of Rocl: $\text{Ocl} = \text{Rocl Rat}$.*

Proof. By Propositions 4.1 and 4.2, we have

$$\text{Rocl Rat} \subset \text{Ocl Rat} \subset \text{Ocl}.$$

To prove conversely $\text{Ocl} \subset \text{Rocl Rat}$, let $\bar{M} = \langle X, Q, q_-, Q_+, Y, y_0, \mathfrak{R} \rangle$ be a one counter automaton. For $p, q \in Q$ and $k \geq 0$, a computation

$$(p, w, y_0) \models (q_1, w_1, \gamma_1) \models \dots \models (q_k, w_k, \gamma_k) \models (q, w', y_0)$$

is called proper if $|\gamma_1|, \dots, |\gamma_k| > 1$, thus if $\gamma_1, \dots, \gamma_k \in y^+ y_0$. Define languages $L_{p,q}$ by

$$p \in L_{p,q} \Leftrightarrow \text{there is a proper computation } (p, w, y_0) \models^+ (q, \varepsilon, y_0).$$

Any computation $(q_-, w, y_0) \models^+ (q_+, \varepsilon, y_0)$ with $q_+ \in Q_+$ factorizes in a sequence of proper computations. Thus there exist states $q_1, q_2, \dots, q_n$, ($n \geq 0$), and a factorization $w = u_0 u_1 u_2 \dots u_n$ such that $u_0 \in L_{q_-, q_1}$, $u_1 \in L_{q_1, q_2}$, $\dots$, $u_n \in L_{q_n, q_+}$. Consider the alphabet $Z = Q \times Q$, and let $K \subset Z^*$ be the local regular language

$$K = (AZ^* \cap Z^*B) \setminus Z^*CZ^*, \\ A = \{q_-\} \times Q, \quad B = Q \times Q_+, \quad C = \{(q_1, q_2)(q'_1, q'_2) \mid q'_1 \neq q'_2\}.$$

Define a substitution $\sigma: Z^* \rightarrow X^*$ by

$$\sigma((p, q)) = L_{p,q}.$$

Then $\sigma(K) = \|\bar{M}\|$, and to prove the theorem, it suffices to show that $L_{p,q} \in \text{Rocl}$. Define a one counter pda

$$\bar{M}_{p,q} = \langle X, Q \cup \bar{p}, \bar{p}, \{q\}, Y, y_0, \mathfrak{R}_{p,q} \rangle$$

where $\bar{p}$ is a new state, by

$$\mathfrak{R}_{p,q} = \mathfrak{R} \cup \{(\bar{p}, u, y) \rightarrow (q', \gamma) \mid (p, u, y_0) \rightarrow (q', \gamma y_0) \in \mathfrak{R}\}.$$

Then it is easily seen that $\|\bar{M}_{p,q}\| = L_{p,q}$. ■

For the rest of this section, we only consider restricted one counter languages. We therefore introduce some simplified notations. First, since the symbol y_0 will no longer be relevant, a one counter pda will be denoted by $\bar{M} = \langle X, Q, q_-, Q_+, \mathfrak{R} \rangle$. Next, all rules in $\mathfrak{R}$ are assumed to have pushdown symbol y , and we write

$$(q, u) \rightarrow (q', m) \quad \text{instead of} \quad (q, u, y) \rightarrow (q', y^{1+m}) \quad (m \geq -1)$$

Thus m denotes the increase or decrease of the pushdown store. With these notations, the computation (4.3) takes the form:

$$(q_-, w, 1) \models (q, w_1, n_1) \models \dots \models (q_k, w_k, n_k) \models (q_+, \varepsilon, 0).$$

Theorem 4.4 *The family Rocl is a rational cone and Ocl is a full AFL.*

Proof. The second part of the statement follows from the first part by the previous theorem. Thus it suffices to show that Rocl is a cone. Let $\bar{M} = \langle X, Q, q_-, Q_+, \mathfrak{R} \rangle$ be a one counter automaton and $L = \|\bar{M}\|$.

a) Let $\varphi: X^* \rightarrow Y^*$ be an alphabetic morphism. Define a pda $\varphi\bar{M} = \langle Y, Q, q_-, Q_+, \varphi\mathfrak{R} \rangle$ by

$$\varphi\mathfrak{R} = \{(q, \varphi u) \rightarrow (q', m) \mid (q, u) \rightarrow (q', m) \in \mathfrak{R}\}.$$

Then clearly $\|\varphi\bar{M}\| = \varphi\|\bar{M}\|$.

b) Let $K \subset X^*$ be a rational language, and let $\bar{A} = \langle X, P, p_-, P_+ \rangle$ be a finite automaton recognizing K . Define $\bar{M}_K = \langle X, Q \times P, (q_-, p_-), Q_+ \times P_+, \mathfrak{R}_K \rangle$ by

$$\mathfrak{R}_K = \{((q, p), u) \rightarrow ((q', p'), m) \mid (q, u) \rightarrow (q', m) \in \mathfrak{R} \text{ and } p \cdot u = p'\}.$$

Then one has $\|\bar{M}_K\| = L \cap K$.

c) Let $Z = X \cup z$, with $z \notin X$, and let $\pi: Z^* \rightarrow X^*$ be the projection. The first idea for the construction of a one counter pda $\bar{M}'$ with $\|\bar{M}'\| = \pi^{-1}(L)$ is to add to $\mathfrak{R}$ the rules $(q, z) \rightarrow (q, 0)$ for $q \in Q$. This method does not work. Indeed, consider for instance a word $w = w'z$ with $w' \in L$. Then w would not be accepted by $\bar{M}'$ since the pushdown store is empty after the lecture of w' . Therefore the presence of letters z has to be anticipated. This yields the following construction. For each $(q, u) \in Q \times (X \cup \varepsilon)$, let q_u be a new state. Then define $Q' = \{q_u \mid (q, u) \in Q \times (X \cup \varepsilon)\}$ and $\pi^{-1}\bar{M} = \langle Z, Q \cup Q', q_-, Q_+, \mathfrak{R}' \rangle$, where $\mathfrak{R}'$ is given by

$$\mathfrak{R}' = \{(q_-, z) \rightarrow (q_-, 0)\} \cup \mathfrak{R}''$$

$$\mathfrak{R}'' = \{(q, u) \rightarrow (q_u, 0), (q_u, z) \rightarrow (q_u, 0), (q_u, \varepsilon) \rightarrow (q', m) \mid (q, u) \rightarrow (q', m) \in \mathfrak{R}\}.$$

A straightforward verification shows that $\|\pi^{-1}\bar{M}\| = \pi^{-1}L$.

By the previous constructions, Rocl is closed under alphabetic morphism, inverse projection and intersection with rational languages. Thus Rocl is a rational cone. ■

In order to prove that Rocl is a principal cone, a “normal form” of one counter pda's will appear to be useful. A one counter pda $\bar{M} = \langle X, Q, q_-, Q_+, \mathfrak{R} \rangle$ is called normalized iff for any rule $(q, u) \rightarrow (q', m) \in \mathfrak{R}$, either $m = 1$ or $m = -1$. Thus the length of the pushdown store always increases or decreases by 1.

Lemma 4.5 For any one counter pda M , there is a normalized one counter pda M' such that $|M| = |M'|$.

Proof. Let $M = \langle X, Q, q_-, Q_+, \mathfrak{R} \rangle$, and define $M' = \langle X, Q', q_-, Q_+, \mathfrak{R}' \rangle$ with $Q' \supset Q$ as follows. Let $(q, u) \rightarrow (p, m) \in \mathfrak{R}$ be a rule. Then (i) if $m = 1$ or $m = -1$, then $(q, u) \rightarrow (p, m) \in \mathfrak{R}'$; (ii) if $m = 0$, then let $\bar{q}$ be a new state and add to $\mathfrak{R}'$ the two rules $(q, u) \rightarrow (\bar{q}, 1)$, $(\bar{q}, \varepsilon) \rightarrow (p, -1)$; (iii) if $m \geq 2$, then let $\bar{q}_1, \bar{q}_2, \dots, \bar{q}_{m-1}$ be new states and add to $\mathfrak{R}'$ the rules $(q, u) \rightarrow (\bar{q}_1, 1)$, $(\bar{q}_1, \varepsilon) \rightarrow (\bar{q}_2, 1)$, $\dots$, $(\bar{q}_{m-2}, \varepsilon) \rightarrow (\bar{q}_{m-1}, 1)$, $(\bar{q}_{m-1}, \varepsilon) \rightarrow (p, 1)$. Such a "factorization" of the rules of $\mathfrak{R}$ yields a normalized pda M' , and clearly $|M'| = |M|$. ■

Theorem 4.6 The rational cone Rocl is principal. D_1^* , D_1' , D_1 , $\bar{L}$ are generators of the cone Rocl .

Proof. By Proposition 1.3, $D_1^* \approx D_1' \approx D_1$. Next if $D_1^*, \bar{L} \subset \{a, b\}^*$ then we noted in Section II.4 that $D_1^*b = \bar{L}$. Thus $D_1^* \approx \bar{L}$, and the four languages are rationally equivalent. All these languages are restricted one counter languages, and since Rocl is a rational cone, we have $\bar{L} \Gamma \subset \text{Rocl}$. Thus it suffices to show the converse inclusion, or $\bar{L} \geq L$ for any $L \in \text{Rocl}$.

Let $L \subset X^*$, $L \in \text{Rocl}$, and let $M = \langle X, Q, q_-, Q_+, \mathfrak{R} \rangle$ be a normalized one counter automaton with $L = |M|$. The proof is in several steps. Note that only minor changes will be made with respect to a proof showing that the languages recognized by general pda's are context-free.

a) First we prove that L is the homomorphic image of a language recognized by a "deterministic" one counter pda. Number the rules of $\mathfrak{R}$ from 1 to $N = \text{Card}(\mathfrak{R})$. Let π_i , $(1 \leq i \leq N)$ be the i -th rule. Then $\mathfrak{R} = \{\pi_1, \dots, \pi_N\}$. Let $T = \{t_1, \dots, t_N\}$ be an alphabet and define a one counter pda $M' = \langle T, Q, q_-, Q_+, \mathfrak{R}' \rangle$ by

$$(q, t_i) \rightarrow (q', m) \in \mathfrak{R}' \Leftrightarrow \pi_i = (q, u) \rightarrow (q', m) \quad 1 \leq i \leq N.$$

Then clearly M' is normalized, and M' is deterministic in the sense that there is no rule with left side of the form (q, ε) , and

$$\text{each } t \in T \text{ is the input symbol of exactly one rule in } \mathfrak{R}' \quad (4.5)$$

Let $\alpha: T^* \rightarrow X^*$ be the morphism defined by $\alpha(t_i) = u$ iff u is the input symbol of the i -th rule in $\mathfrak{R}$. Let $L' = |M'|$. We prove that $L = \alpha(L')$. Consider indeed a computation in M' :

$$(q_-, t_{i_1} \cdots t_{i_k}, 1) \models (q_1, t_{i_2} \cdots t_{i_k}, n_1) \models \cdots \models (q_{k-1}, t_{i_k}, n_k) \models (q_+, \varepsilon, 0).$$

Since $\pi_{i_1} = (q_-, \alpha(t_{i_1})) \rightarrow (q_1, n_1 - 1)$, $\pi_{i_r} = (q_{r-1}, \alpha(t_{i_r})) \rightarrow (q_r, n_r - n_{r-1})$, $(2 \leq r \leq k-1)$ and $\pi_{i_k} = (q_{k-1}, \alpha(t_{i_k})) \rightarrow (q_+, -n_k)$, it follows that $\alpha(t_{i_1} \cdots t_{i_k}) \in L$. Thus $\alpha(L') \subset L$. Conversely, let $w \in L$ and consider a computation in $M: (q_-, w, 1) \models^k (q_+, \varepsilon, 0)$ of length k and let $\pi_{i_1}, \dots, \pi_{i_k}$ be the sequence of rules

used in this computation. Then each π_{i_r} is of the form $\pi_{i_r} = (q, \alpha(t_{i_r})) \rightarrow (q', m)$ for some $t_{i_r} \in T$, and $(q, t_{i_r}) \rightarrow (q', m)$ is in $\mathfrak{R}'$. Therefore $\alpha(t_{i_1} \cdots t_{i_k}) = w$ and $t_{i_1} \cdots t_{i_k} \in L'$. Thus $L \subset \alpha(L')$.

b) Next we show that $L' = |M'| \cap K$ where $K \subset T^*$ is a regular language and M'' has just one state. Define a one counter pda $M'' = \langle T, \{p\}, p, \{p\}, \mathfrak{R}'' \rangle$ and a finite state automaton $A = \langle T, Q, q_-, Q_+ \rangle$ by

$$\left. \begin{array}{l} (p, t) \rightarrow (p, m) \in \mathfrak{R}'' \\ q \cdot t = q' \end{array} \right\} \Leftrightarrow (q, t) \rightarrow (q', m) \in \mathfrak{R}'$$

Then it is easily seen by induction that

$$(q_-, w, 1) \models^k (q_+, \varepsilon, 0) \text{ in } M'$$

$$\text{iff } (p, w, 1) \models^k (p, \varepsilon, 0) \text{ in } M'' \text{ and } q_- \cdot w = q_+.$$

Consequently $L' = L'' \cap K$, with $L'' = |M''|$ and $K = |A|$.

c) The set $\mathfrak{R}''$ of rules of M'' defines a morphism v from T^* into the additive group $\mathbb{Z}$ by

$$v(t) = m \Leftrightarrow (p, t) \rightarrow (p, m) \in \mathfrak{R}'' \quad (t \in T). \quad (4.6)$$

Note that v is well defined in view of (4.5).

Let $w = z_1 \cdots z_k \in T^*$, $(z_i \in T)$. Assume $w \in L''$. Then there is a computation in M'' :

$$(p, z_1, \dots, z_k, n_0) \models (p, z_2 \cdots z_k, n_1) \models \cdots \models (p, z_k, n_{k-1}) \models (p, \varepsilon, n_k) \quad (4.7)$$

with $n_0 = 1$, $n_k = 0$. By (4.6), $v(z_i) = n_i - n_{i-1}$ for $i = 1, \dots, k$, whence $v(z_1 \cdots z_i) = n_i - 1$ for $i = 0, \dots, k$. Since $n_i > 0$ for $i = 0, \dots, k-1$, we have:

$$v(w) = -1 \text{ and } v(w') \geq 0 \text{ for any proper left factor } w' \text{ of } w. \quad (4.8)$$

Assume conversely that (4.8) holds and define $n_i = 1 + v(z_1 \cdots z_i)$ for $i = 0, \dots, k$. Then by (4.6), (4.7) is a computation for w and therefore $w \in L''$. This proves that $w \in L''$ iff (4.8) holds. Finally let $\bar{L} \subset \{a, b\}^*$ and let $\beta: T^* \rightarrow \{a, b\}^*$ be the morphism defined by

$$\beta(t) = \begin{cases} a & \text{if } v(t) = 1 \\ b & \text{if } v(t) = -1 \end{cases} \quad (t \in T)$$

(Recall that the integer m in (4.6) is equal to 1 or -1 since the automaton M was supposed to be normalized.) Then Proposition II.4.1 and (4.8) show that $w \in L''$ iff $\beta(w) \in \bar{L}$. Consequently $L'' = \beta^{-1}(\bar{L})$. The three steps of the proof

show that

$$L = \alpha(L') = \alpha(L'' \cap K) = \alpha(\beta^{-1}(\mathcal{L}) \cap K).$$

Thus $L \leq \mathcal{L}$. ■

We shall see in the next chapter that the principal cones Rocl and Lin are incomparable. A direct proof of this fact is long and tedious. A short proof uses results on iterative pairs.

The language $S_- = \{x^n y^n \mid n \geq 0\}$ is both a linear and a one counter language. Thus $S_- \Gamma \subset \text{Rocl} \cap \text{Lin}$. It is an open question whether this inclusion is strict. A related open problem is the following: Is the intersection of two principal cones a principal cone?

Exercises

4.1 (Greibach [1969]) Show that a language is context-free iff it is of the form $\|M\| = \{w \in X^* \mid \exists q_+ \in Q_+ : (q_-, w, y_0) \stackrel{+}{\vdash} (q_+, \varepsilon, y_0)\}$, where M is a general pda (as defined for instance in Ginsburg [1966]).

4.2 Let $X_n = \{x_0, x_1, \dots, x_n\}$, ($n \geq 1$). Define $L_n \subset X_n^*$ by

$$L_n = \bigcup_{k=1}^n x_k (L_n)^k \cup x_0.$$

Show that the languages L_n , ($n \geq 2$) are generators of the cone Rocl .

4.3 (Greibach [1969]) Let $M = \langle X, Q, q_-, Q_+, Y, y_0, \delta \rangle$ be a pda. Define $P(M) = \{h \in Y^* \mid \exists w \in X^*, \exists q \in Q \mid (q_-, w, y_0) \stackrel{+}{\vdash} (q, \varepsilon, h)\}$ to be the set of all words appearing on the push-down store during computations. Then M is an n -counter pda iff

$$P(M) \subset y_0 y_1^* \cdots y_n^*, (y_1, \dots, y_n \in Y).$$

Show that $L \in \text{Fcl}(n)\hat{\Gamma}$ iff $L = \|M\| = \{w \in X^* \mid \exists q_+ \in Q, (q_-, w, y_0) \stackrel{+}{\vdash} (q, \varepsilon, y_0)\}$ for some n -counter pda M .

VII.5 Quasi-Rational Languages

The family of quasi-rational languages is the closure under substitution of the family of linear languages. This remarkable family admits several quite different characterizations and therefore has also several denominations: quasi-rational languages are known as standard matching choice, or nonexpansive, or derivation bounded languages.

In this section, we prove the equivalence of some of these definitions. Papers on quasi-rational languages include Yntema [1967], Nivat [1967], Ginsburg and Spanier [1968], Salomaa [1969a], Gruska [1971a, b]. Results concerning subfamilies have been proved in Boasson, Crestin and Nivat [1973], Crestin [1978].

Definition The family $\text{Qrt}(k)$ of quasi-rational languages of rank $k \geq 1$ is defined inductively by:

$$\text{Qrt}(1) = \text{Lin}, \quad \text{Qrt}(k+1) = \text{Lin} \circ \text{Qrt}(k) \quad (k \geq 1).$$

The family of quasi-rational languages is

$$\text{Qrt} = \bigcup_{k \geq 1} \text{Qrt}(k).$$

In view of the associativity of substitution (Theorem V.5.1),

$$\text{Qrt}(k) = \text{Qrt}(k-1) \circ \text{Lin} = \text{Qrt}(n) \circ \text{Qrt}(m)$$

for all $k \geq 2$, $n, m \geq 1$ with $k = n + m$. By Theorem VI.5.7, $\text{Qrt}(k)$ is a principal cone, hence closed under union. In view of Example 3.2 and Exercise 3.2,

$$\text{Qrt}(k) \subsetneq \text{Qrt}(k) \hat{\Gamma} \subsetneq \text{Qrt}(k+1) \quad k \geq 1. \quad (5.1)$$

Example 5.1 Let $X = \{x, y, z\}$, let $S_- = \{x^n y^n : n \geq 0\}$, and consider the language

$$L = \{x^{n_1} y^{n_1} x^{n_2} y^{n_2} \cdots x^{n_p} y^{n_p} z^p : p \geq 0, n_1, \dots, n_p \geq 0\}.$$

Then $L = \theta(S_-)$, where $\theta : \{x, y\}^* \rightarrow X^*$ is given by $\theta(x) = S_-$, $\theta(y) = z$. Thus $L \in \text{Qrt}(2)$. The iteration lemma for linear languages (Proposition V.6.6) easily shows that L is not linear.

Example 5.2 No generator of the cone Alg is quasi-rational since otherwise it would belong to $\text{Qrt}(k)$ for some $k \geq 1$, and (5.1) would be violated. It is much harder to prove that D_1^* (and consequently also $\mathcal{L}$, D_1' , D_1) are not quasi-rational. This will be done in the next chapter (Theorem VIII.7.14).

We now give a first characterization of the quasi-rational languages. For this we need a definition.

Definition A context-free grammar $G = \langle V, X, P \rangle$ is nonexpansive if for every $\xi \in V$, and $w \in (V \cup X)^*$, $\xi \xrightarrow{*} w$ implies that w contains at most one occurrence of ξ . A language L is nonexpansive if there exists a nonexpansive context-free grammar generating L .

Let Nexp denote the family of nonexpansive languages.

Theorem 5.1 $\text{Nexp} = \text{Qrt}$.

Proof. In order to verify the inclusion $\text{Qrt} \subset \text{Nexp}$, we show that $\text{Qrt}(k) \subset \text{Nexp}$ by induction on k . Clearly any linear grammar is nonexpansive. Thus $\text{Qrt}(1) \subset \text{Nexp}$. Next let $L \subset Y^*$, $L \in \text{Qrt}(k+1) = \text{Lin} \circ \text{Qrt}(k)$. Then there are a linear language $A \subset X^*$, and a $\text{Qrt}(k)$ -substitution $\theta : X^* \rightarrow Y^*$ such that $\theta(A) = L$. Let $G = \langle V, X, P \rangle$ be a linear grammar such that $A = L_G(\sigma)$ for a

$\sigma \in V$. By induction, there are nonexpansive grammars $G_x = \langle V_x, Y, P_x \rangle$ such that $\theta(x) = L_{G_x}(\sigma_x)$ with $\sigma_x \in V_x$ for each $x \in X$. Let $H = \langle W, Y, Q \rangle$ be the grammar generating L constructed in Section II.2. We claim that H is nonexpansive. Otherwise there is a $\xi \in W = V \cup \bigcup_{x \in X} V_x$ such that

$$\xi \xrightarrow{H}^* a\xi b\xi c \quad (5.2)$$

for some words a, b, c . The variable ξ is in none of the sets V_x , since otherwise (5.2) would hold in G_x , and G_x would be expansive. Thus $\xi \in V$. But then (5.2) cannot hold since G is linear. Thus H is nonexpansive and $L \in \text{Nexp}$. Conversely, let L be a nonexpansive language. Let $G = \langle V, X, P \rangle$ be a nonexpansive grammar with $L = L_G(\sigma)$ for some $\sigma \in V$. We prove that L is quasi-rational by induction on $n = \text{Card}(V)$. If $n = 1$, then G is linear and L is quasi-rational. Thus assume $n \geq 2$, and that the conclusion holds for all nonexpansive grammars with less than n variables. Clearly G is still nonexpansive if it reduced in σ (in the sense of Section II.2). Thus we assume that G is reduced in σ . Define $V' \subset V$ to be the set of variables ξ such that $\xi \xrightarrow{*} a\sigma b$ for some $a, b \in (V \cup X)^*$. Since $\sigma \in V'$, V' is nonempty. Define a grammar

$$G' = \langle V', X \cup (V \setminus V'), P' \rangle, \quad P' = \{\xi \rightarrow \alpha \in P \mid \xi \in V'\}.$$

We claim that G' is linear. Assume the contrary. Then there exists a production $\xi \rightarrow f\eta_1 g\eta_2 h$ in P' with $\xi, \eta_1, \eta_2 \in V'$. Consequently $\eta_1 \xrightarrow{*} a_1\sigma b_1$, $\eta_2 \xrightarrow{*} a_2\sigma b_2$ for some words a_1, b_1, a_2, b_2 , and since G is reduced, $\sigma \xrightarrow{*} u\xi v$ for some words u, v . Combining these derivations, we obtain

$$\sigma \xrightarrow{*} u\xi v \xrightarrow{*} uf\eta_1 g\eta_2 hv \xrightarrow{*} ufa_1\sigma b_1 ga_2\sigma b_2 hv,$$

and G is expansive, contrary to the assumption. Thus G' is linear. If $V' = V$, then $G = G'$ is linear and L is quasi-rational. Thus suppose $V' \neq V$ and consider the grammar

$$\bar{G} = \langle V \setminus V', X, P \setminus P' \rangle.$$

Note that $\bar{G}$ is indeed a grammar, i.e. $\eta \rightarrow \alpha \in P \setminus P'$ implies $\alpha \in (X \cup V \setminus V')^*$, since otherwise $\alpha = a\xi b$ for some $\xi \in V'$, hence $\alpha \rightarrow a'\sigma b'$ for some a', b' , and $\eta \in V'$. Since $\sigma \in V'$, $\bar{G}$ has less than n variables, and obviously is nonexpansive. Thus by induction $L_{\bar{G}} = L_{\bar{G}}(\xi)$ is quasi-rational for each $\xi \in V \setminus V'$. Next $L = \theta(L_G(\sigma))$, where $\theta: (X \cup V \setminus V')^* \rightarrow X^*$ is the substitution defined by $\theta(x) = x$ for $x \in X$, and $\theta(\xi) = L_{\bar{G}}(\xi)$ for $\xi \in V \setminus V'$. Thus $L \in \text{Lin} \square \text{Qrt} = \text{Qrt}$ and L is quasi-rational. ■

We now consider another property of grammars which will appear to give a characterization of the quasi-rational languages of rank k . Let $G = \langle V, X, P \rangle$ be a context-free grammar. The index of a derivation

$$w_0 \rightarrow w_1 \rightarrow \cdots \rightarrow w_n$$

is the maximum number of occurrences of variables in $w_0, \dots, w_n$, i.e. the greatest of the numbers $|w_0|_V, \dots, |w_n|_V$. Given a word $w \in (V \cup X)^*$ such that $\xi \xrightarrow{*} w$, the index of w with respect to $\xi \in V$ is the least of the indices of all derivations $\xi \xrightarrow{*} w$. Denote this number by $\text{ind}(\xi, w)$. Clearly $\text{ind}(\xi, w) \geq 1$. Next define

$$L_G^{(k)}(\xi) = \{w \in X^* \mid \text{ind}(\xi, w) \leq k\}.$$

Thus $L_G^{(k)}(\xi)$ is the set of all words $w \in X^*$ for which there exists a derivation $\xi \xrightarrow{*} w$ with index at most k . Obviously

$$L_G^{(k)}(\xi) \subset L_G^{(k+1)}(\xi), \quad L_G(\xi) = \bigcup_{k \geq 1} L_G^{(k)}(\xi).$$

The grammar G has index k in ξ if k is the least integer such that $L_G(\xi) = L_G^{(k)}(\xi)$, and G has infinite index in ξ if $L_G(\xi) \neq L_G^{(k)}(\xi)$ for all $k \geq 1$. Let $\text{ind}(G, \xi)$ denote the index of G in ξ . Thus $\text{ind}(G, \xi)$ is either a positive integer or infinite.

Definition Let L be an algebraic language. Then the index of L is defined as

$$\text{ind}(L) = \min \text{ind}(G, \xi)$$

where (G, ξ) ranges over all algebraic grammars such that $L = L_G(\xi)$. Thus the index of L is either a positive integer or infinite. Let $\text{Ind}(k)$ be the family of all algebraic languages of index $\leq k$, ($k \geq 1$).

Example 5.3 Any linear language has index 1, since any linear grammar has index 1 in all its variables.

Example 5.4 Let $\mathcal{L} \subset \{a, b\}^*$ be the Lukasiewicz language. $\mathcal{L}$ is generated by the grammar with productions $\xi \rightarrow a\xi\xi + b$. We claim that this grammar has infinite index.

Define indeed a sequence of words $(f_m)_{m \geq 1}$ by $f_1 = b$, $f_{m+1} = af_m f_m$. We verify that $\text{ind}(\xi, f_m) = m$. Since $\xi \rightarrow b$, we have $\text{ind}(\xi, f_1) = 1$. Arguing by induction, assume $\text{ind}(\xi, f_m) = m$. Then there exists a derivation

$$\xi = w_0 \rightarrow w_1 \rightarrow \cdots \rightarrow w_r = f_m$$

of index m . Consequently the derivation

$$\xi \rightarrow a\xi\xi \rightarrow aw_1\xi \rightarrow \cdots \rightarrow aw_r\xi \rightarrow aw_r w_1 \rightarrow \cdots \rightarrow aw_r w_r = f_{m+1}$$

has index $m+1$, and $\text{ind}(\xi, f_{m+1}) \leq m+1$. Conversely, consider a derivation

$$\xi = w_0 \rightarrow w_1 \rightarrow \cdots \rightarrow w_p = f_{m+1}.$$

Then $w_1 = a\xi\xi$, and by Lemma II.1.1, each w_i admits a factorization $w_i = au_i v_i$ such that

$$\xi = u_1 \xrightarrow{k_1} u_2 \rightarrow \cdots \rightarrow u_{p-1} \xrightarrow{k_p} u_p$$

$$\xi = v_1 \xrightarrow{l_1} v_2 \rightarrow \cdots \rightarrow v_{p-1} \xrightarrow{l_p} v_p$$

with $k_i + l_i = 1$ for $i = 2, \dots, p$. Since $f_{m+1} = au_p v_p$, and $u_p, v_p \in \mathcal{L}$, and since $\mathcal{L}$ is prefix (Proposition II.4.1), it follows that $u_p = v_p = f_m$. Next either $k_p = 0$ or $l_p = 0$. Assume $k_p = 0$, then $l_p = 1$, and $|v_{p-1}|_\xi = 1$. Consequently $|v_i|_\xi \geq 1$ for each $i = 1, \dots, p-1$. Next $u_{p-1} = u_p = f_m$, and by induction, there is an integer i , ($1 \leq i \leq p-1$) such that $|u_i|_\xi \geq m$. Thus $|w_i|_\xi \geq m+1$, showing that $\text{ind}(\xi, f_{m+1}) \geq m+1$.

Note that we did not prove that the language $\mathcal{L}$ has infinite index. We only proved that a particular grammar generating $\mathcal{L}$ has infinite index. The proof that $\mathcal{L}$ has infinite index is much more difficult. It is a consequence of Theorem VIII.7.14 in view of the following result.

Theorem 5.2 For any $k \geq 1$, $\text{Ind}(k) = \text{Qrt}(k)$.

The proof of this theorem is in two parts. First we prove

Lemma 5.3 For any $k \geq 1$, $\text{Qrt}(k) \subset \text{Ind}(k)$.

Proof. The proof is by induction on k . Any linear grammar has index 1. Hence $\text{Lin} \subset \text{Ind}(1)$. Since by induction

$$\text{Qrt}(k+1) = \text{Lin} \circ \text{Qrt}(k) \subset \text{Lin} \circ \text{Ind}(k),$$

it suffices to show the inclusion $\text{Lin} \circ \text{Ind}(k) \subset \text{Ind}(k+1)$. For this, consider a language $L \subset Y^*$ in $\text{Lin} \circ \text{Ind}(k)$. Then $L = \theta(A)$, where $A \subset X^*$ is linear, and $\theta: X^* \rightarrow Y^*$ is a $\text{Ind}(k)$ -substitution. Let $G = \langle V, X, P \rangle$ be a linear grammar in canonical form (as defined in Section V.6), and let $\sigma \in V$ be such that $A = L_G(\sigma)$. Next for each $x \in X$, let $G_x = \langle V_x, Y, P_x \rangle$ be a grammar such that $\theta(x) = L_{G_x}(\sigma_x)$, and having index $\leq k$ in σ_x . Let $H = \langle W, Y, Q \rangle$ be the grammar such that $L = L_H(\sigma)$ deduced from G and the G_x , as given in Section II.2.

Observe that for each production $\xi \rightarrow x\eta$ in P , the production $\xi \rightarrow \sigma_x \eta$ is in Q . Thus for all $w \in \theta(x)$, there is a derivation $\xi \xrightarrow{*} w\eta$ of index at most $k+1$ in H . The same conclusion holds for the other types of productions in P . Consequently, for each derivation $\sigma \xrightarrow{*} f$ in G , and for each $w \in \theta(f)$, there exists a derivation $\sigma \xrightarrow{*} w$ of index at most $k+1$ in H . Thus $L \in \text{Ind}(k+1)$. ■

The proof of the converse inclusion, namely $\text{Ind}(k) \subset \text{Qrt}(k)$, is more involved and requires some investigations of the index of derivations. For this, we first introduce an auxiliary notation: Given a grammar G and words u, v , we write

$$u \mapsto v$$

as an abbreviation for

$$u = v \quad \text{or} \quad u \rightarrow v.$$

Thus $u \mapsto v$ iff $u \xrightarrow{n} v$ with $n = 0$ or $n = 1$.

We now prove a general lemma concerning decompositions of derivations, and their relation to the notion of index. Let $G = \langle V, X, P \rangle$ be a context-free grammar, and consider a derivation in G :

$$w_1 \rightarrow w_2 \rightarrow \cdots \rightarrow w_n \quad (5.3)$$

with $w_n \in X^*$. Assume further that

$$w_1 = u_0 \xi_1 u_1 \cdots u_{s-1} \xi_s u_s, \quad \xi_1, \dots, \xi_s \in V, \quad u_0, \dots, u_s \in X^*.$$

In view of Lemma II.1.1, each word w_i admits a factorization

$$w_i = u_0 h_1^{(i)} u_1 h_2^{(i)} \cdots u_{s-1} h_s^{(i)} u_s$$

such that

$$\begin{aligned} \xi_1 &= h_1^{(1)} \mapsto h_1^{(2)} \mapsto \cdots \mapsto h_1^{(n)} \\ \xi_2 &= h_2^{(1)} \mapsto h_2^{(2)} \mapsto \cdots \mapsto h_2^{(n)} \\ &\vdots \\ \xi_s &= h_s^{(1)} \mapsto h_s^{(2)} \mapsto \cdots \mapsto h_s^{(n)} \end{aligned} \quad (5.4)$$

and further for each $i = 1, \dots, n-1$, $h_t^{(i)} \mapsto h_t^{(i+1)}$ for exactly one t . The derivations (5.4) are said to be induced by (5.3).

The following lemma is an extension of the argument used in Example 5.4.

Lemma 5.4 Assume that the derivation (5.3) has index $\leq p$. Then for $t = 1, \dots, s$, at least t of the induced derivations (5.4) have index $\leq p-s+t$.

Proof. Assume the contrary. Then there is some t such that less than t induced derivations have index $\leq p-s+t$. Since the index of the other derivations is greater than $p-s+t$, this means that there exist $r = s-t+1$ induced derivations which all have an index at least $p-s+t+1 = p-r+2$. For simplicity, we assume that these derivations are the first ones in (5.4). Next, since $h_1^{(1)}, \dots, h_r^{(1)} \in V$, and $h_1^{(n)}, \dots, h_r^{(n)} \in X^*$, there is a largest integer $m < n$ such that

$$|h_1^{(m)}|_V \geq 1, \quad |h_2^{(m)}|_V \geq 1, \dots, |h_r^{(m)}|_V \geq 1,$$

and there is some $j \in \{1, \dots, r\}$ such that $h_i^{(m+1)} \in X^*$. Consider this j , and the corresponding induced derivation $\xi_j \xrightarrow{*} h_j^{(n)}$ in (5.4). The index of this derivation is $\geq p-r+2$. Thus there is some exponent l with $1 \leq l \leq m$ and such that

$$|h_i^{(l)}|_V \geq p-r+2.$$

Since $|h_i^{(l)}|_V \geq 1$ for $i=1, \dots, r$, $i \neq j$, we have

$$|w_l|_V \geq (p-r+2) + (r-1) = p+1.$$

Thus the index of the derivation (5.3) is $\geq p+1$, and this is a contradiction. ■

Proposition 5.5 (Ginsburg and Spanier [1968]) *Let $G = \langle V, X, P \rangle$ be a context-free grammar. Then $L_G^{(k)}(\xi)$ is a quasi-rational language of rank k for all $\xi \in V$ and $k \geq 1$.*

The proposition claims that the languages $L_G^{(k)}(\xi)$ are context-free. Ginsburg and Spanier [1968] show that this holds even if G is an arbitrary phrase-structure grammar.

Proof. Let $k \geq 1$ be fixed. We first construct a context-free grammar H generating $L_G^{(k)}(\xi)$, which proves that these languages are context-free. The analysis of the grammar H then shows that the languages are quasi-rational of rank k .

Define a grammar

$$H = \langle W, X, Q \rangle$$

as follows: $W = V \times \{1, \dots, k\}$. (An element of W is noted $[\xi, p]$ instead of (ξ, p) .) Next, for each production

$$\xi \rightarrow u_0 \xi_1 u_1 \xi_2 \cdots u_{s-1} \xi_s u_s \in P, \quad (5.5)$$

with $\xi_1, \dots, \xi_s \in V$, $u_0, \dots, u_s \in X^*$ and $s \leq k$, the productions

$$[\xi, p] \rightarrow u_0 [\xi_1, p_1] u_1 [\xi_2, p_2] \cdots u_{s-1} [\xi_s, p_s] u_s$$

are in Q for all $p \geq s$, and for all permutations $(p_1, p_2, \dots, p_s)$ of $(p-s+1, \dots, p)$.

Note that the p_i 's are distincts, and that $\{p_1, \dots, p_s\} = \{p-s+1, \dots, p\}$. Note also that if $s > k$ in (5.5), then this production gives no contribution to Q . Finally, observe that if $s=0$, then $[\xi, p] \rightarrow u_0 \in Q$ for all $p=1, \dots, k$. We claim:

$$L_H([\xi, p]) = L_G^{(p)}(\xi) \quad \text{for } \xi \in V, \quad 1 \leq p \leq k.$$

(i) We first prove the inclusion $L_G^{(p)}(\xi) \subset L_H([\xi, p])$ by induction on the length of derivations. Let $w \in L_G^{(p)}(\xi)$, and consider a derivation of index $\leq p$:

$$\xi \rightarrow w_1 \rightarrow w_2 \rightarrow \cdots \rightarrow w_n = w \quad \text{in } G.$$

If $n=1$, then $\xi \rightarrow w \in P$, and, in view of a previous remark, $[\xi, p] \rightarrow w \in Q$ for $p=1, \dots, k$. Thus $w \in L_H([\xi, p])$.

Assume $n > 1$, and set

$$w_1 = u_0 \xi_1 u_1 \xi_2 \cdots \xi_s u_s, \quad \xi_1, \dots, \xi_s \in V, \quad u_0, \dots, u_s \in X^*.$$

Obviously $s \leq p$, since the derivation has index $\leq p$.

In view of Lemma 5.4, there is at least one induced derivation with index $\leq p-s+1$. Next, there is at least one other derivation which has index $\leq p-s+2$. Continuing in this way, one determines, for each $j=1, \dots, s$, an integer $\pi(j) \in \{1, \dots, s\}$, distinct from the previous ones, such that the induced derivation $\xi_{\pi(j)} \xrightarrow{*} h_{\pi(j)}^{(n)}$ has index at most $p-s+j$. Since the length of the induced derivations is smaller than n , it follows by induction that

$$h_{\pi(j)}^{(n)} \in L_H([\xi_{\pi(j)}, p-s+j]) \quad j=1, \dots, s.$$

Note that π is a permutation of $\{1, \dots, s\}$. Setting $p_i = p-s+\pi^{-1}(i)$ for $i=1, \dots, s$ we get a permutation $(p_1, \dots, p_s)$ of $(p-s+1, \dots, p)$, and

$$h_i^{(n)} \in L_H([\xi_i, p_i]) \quad i=1, \dots, s.$$

Finally

$$[\xi, p] \rightarrow u_0 [\xi_1, p_1] u_1 \cdots u_{s-1} [\xi_s, p_s] u_s \in Q,$$

and consequently $w \in L_H([\xi, p])$.

(ii) We now prove the inclusion $L_H([\xi, p]) \subset L_G^{(p)}(\xi)$, by induction on the length of derivations. Let $w \in L_H([\xi, p])$, and consider a derivation

$$[\xi, p] \rightarrow w_1 \rightarrow w_2 \rightarrow \cdots \rightarrow w_n = w \quad \text{in } H.$$

If $n=1$, then $\xi \rightarrow w \in P$, and $w \in L_G^{(1)}(\xi)$. Otherwise

$$w_1 = u_0 [\xi_1, p_1] u_1 [\xi_2, p_2] \cdots u_{s-1} [\xi_s, p_s] u_s,$$

with $s \leq p$, and with $(p_1, \dots, p_s)$ a permutation of $(p-s+1, \dots, p)$. There is no loss of generality in assuming $p_1 = p-s+1, \dots, p_s = p$. By Lemma II.1.1,

$$w = u_0 h_1 u_1 h_2 \cdots u_{s-1} h_s u_s,$$

with

$$[\xi_j, p_j] \xrightarrow{*}_H h_j \quad j=1, \dots, s.$$

By induction, $h_j \in L_G^{(p_j)}(\xi_j)$ for $j=1, \dots, s$, and therefore there are derivations

$$\xi_j \xrightarrow{*}_G h_j \quad (5.6)$$

with index $\leq p_i = p - s + j$ for $j = 1, \dots, s$. Consider now the derivation

$$\begin{aligned}
 \xi &\xrightarrow{G} u_0 \xi_1 u_1 \xi_2 \cdots u_{s-1} \xi_s u_s \\
 &\xrightarrow{G}^* u_0 h_1 u_1 \xi_2 \cdots u_{s-1} \xi_s u_s \\
 &\xrightarrow{G}^* u_0 h_1 u_1 h_2 \cdots u_{s-1} \xi_s u_s \\
 &\quad \vdots \\
 &\xrightarrow{G}^* u_0 h_1 u_1 h_2 \cdots u_{s-1} h_s u_s = w,
 \end{aligned} \tag{5.7}$$

obtained by concatenating the derivations (5.6) in increasing order. The j -th derivation (5.6) contributes in (5.7) to words containing at most $p_i + (s - j) = p$ nonterminals. Thus (5.7) has index at most p . This shows that w is in $L_G^{(p)}(\xi)$.

(iii) It remains to prove that $L_H([\xi, p]) \in \text{Qrt}(p)$. Observe first that for each production $[\xi, p] \rightarrow \alpha \in Q$, and for each nonterminal $[\eta, q]$ appearing in α , we have $q \leq p$. Thus the grammar

$$H_p = \langle W_p, X, Q_p \rangle$$

with

$$W_p = V \times \{1, \dots, p\}, \quad Q_p = \{[\xi, q] \rightarrow \alpha \in Q \mid q \leq p\}$$

is well-defined, and further

$$L_{H_p}([\xi, q]) = L_H([\xi, q]) \quad \text{for } q \leq p.$$

For $p = 1$, the grammar L_{H_1} is linear by construction. Thus $L_H([\xi, 1]) \in \text{Lin}$.

Assume $p > 1$, and consider the grammar

$$\bar{H}_p = \langle W_p \setminus W_{p-1}, X \cup W_{p-1}, Q_p \setminus Q_{p-1} \rangle.$$

By the previous remark, $\bar{H}_p$ is well-defined and by the construction of H , $\bar{H}_p$ is linear. Further, it is easily seen that

$$L_H([\xi, p]) = \theta(L_{\bar{H}_p}([\xi, p])),$$

where $\theta: (W_{p-1} \cup X)^* \rightarrow X^*$ is the substitution defined by

$$\theta(x) = x \quad (x \in X);$$

$$\theta([\xi, q]) = L_H([\xi, q]) \quad q < p.$$

Arguing by induction, θ is a $\text{Qrt}(p-1)$ -substitution, and $L_H([\xi, p]) \in \text{Qrt}(p)$. ■

Proof of Theorem 5.2 The inclusion $\text{Qrt}(k) \subset \text{Ind}(k)$ holds by Lemma 5.3. Conversely, let $L \in \text{Ind}(k)$. Then $L = L_G(\xi) = L_G^{(k)}(\xi)$ for some grammar G . By Proposition 5.5, $L_G^{(k)}(\xi) \in \text{Qrt}(k)$. Thus $L \in \text{Qrt}(k)$, and $\text{Qrt}(k) = \text{Ind}(k)$. ■

There is another characterization of quasi-rational languages using the bracket operation defined in Section V.6, due to Nivat [1967] and Yntema [1967]. See the following exercises.

Exercises

5.1 Show that for a rational relation R , and for a quasi-rational language L of rank k , the language $[R, L]$ is quasi-rational of the rank k . (The bracket $[R, L]$ was defined in Section V.6.)

5.2 (Yntema [1967], Nivat [1967]) The set of quasi-rational relations of rank k over X and Y is the least family of subsets of $X^* \times Y^*$ containing the relations $L \times L'$, ($L \subset X^*$, $L' \in Y^*$) with $L, L' \in \text{Qrt}(k)$ and closed under union, product and the star operation.

a) Show that for any quasi-rational relation R of rank k , and for any quasi-rational language L of rank k , $[R, L]$ is in $\text{Qrt}(k+1)$.

b) Show that conversely any language $A \in \text{Qrt}(k+1)$ can be written as $A = [R, 1]$, where R is a quasi-rational relation of rank k . Give such a relation of rank 1 for the language of Example 5.1.

VIII Iterative Pairs

In Chapter V it was shown that languages like $S_{<} = \{x^n y^m \mid 0 \leq n < m\}$ and $S_{>} = \{x^n y^m \mid 0 \leq m < n\}$ are rationally incomparable. In the previous chapter, the Syntactic Lemma gave infinite chains of rational cones which appear to be of increasing "complexity". Thus rational transductions classify languages according to some measure of complexity. In the present chapter, we give a description of this complexity measure in so far as context-free languages are concerned.

Since any algebraic language is a rational image of D_2^* , it is obtained by adjoining additional restrictions to that language. The resulting language is then subjected to two types of constraints, some of "context-free" nature, the other of "regular" nature. The algebraic constraints are expressed by counting restrictions or by restriction on parenthesization. The rational constraints concern repetition and transcription. Rational transductions should ignore rational constraints, and detect modification of algebraic constraints.

The concepts introduced by Boasson [1976] and Beauquier [1978a] to describe the algebraic constraints are the notions of iterative pair and of system of iterative pairs. The central theorem of this chapter (Theorem 6.1) can be rephrased informally as follows: if A and B are algebraic languages and if $A \geq B$, then A has systems of iterative pairs of greater complexity than those of B .

The systems of iterative pairs in a language L are defined by a combinatorial property of L . But if L is context-free, then these systems are closely related to some nesting of the self-embedding variables of any algebraic grammar generating L . Thus systems of iterative pairs give, through a property of the words of a language, a description of a "structural" feature common to all grammars for this language. In view of this relationship, the types of systems of iterative pairs can really be considered as a good measure of complexity. By the way, these facts constitute a justification a posteriori of the use of rational transductions as a tool for comparison of languages.

The first three sections of this chapter are concerned with iterative pairs and the Transfer Theorem for these pairs. As an illustration, we easily obtain most of the results of Section V.7, and we show a new infinite chain of rational cones. Sections 4-7 contain the generalization of the results to systems of iterative pairs and applications. The material for this chapter is from Boasson [1976] and Beauquier [1978a]. The second author gives, in Beauquier

[1977] another generalization, not included here, of iterative pairs, which he calls "multipairs".

VIII.1 Types of Iterative Pairs

This section contains the definition and examples of iterative pairs. A classification of iterative pairs is given and some simple lemmas are proved.

Definition Let X be an alphabet, and let $L \subset X^*$ be a language. A sequence

$$\pi = (a, u, b, v, c)$$

of words of X^* is an iterative pair in L if

- (i) $au^n bv^n c \in L$ for $n \geq 0$;
- (ii) $|uv| > 0$.

The words u and v are the iterating elements of π .

In view of (i) the word $w = au^0 bv^0 c$ belongs to L . Then π is called an iterative pair of w in L , and w is said to admit the iterative pair π in L . We are interested in the language $L \cap au^* bv^* c$ or equivalently in the set of integers k, l such that $au^k bv^l c \in L$. Therefore we define the set of exponents of π in L by

$$\text{Exp}(\pi, L) = \{(k, l) \in \mathbb{N}^2 : au^k bv^l c \in L\}.$$

This set describes the local constraint of L on the factorization π of w . By definition, $\text{Exp}(\pi, L)$ contains the diagonal $\Delta = \{(n, n) : n \in \mathbb{N}\}$. If π is an iterative pair in L , and if $L \subset L'$, then clearly π is also an iterative pair in L' and $\text{Exp}(\pi, L) \subset \text{Exp}(\pi, L')$. Note that

$$\text{Exp}(\pi, L) = \text{Exp}(\pi, L \cap au^* bv^* c).$$

Example 1.1 Let $L \subset X^*$ be context-free. The iteration lemmas assert that any long enough word w in L admits an iterative pair in L .

Example 1.2 Let $X = \{x, y\}$ and $S_{\leq} = \{x^n y^m \mid 0 \leq n \leq m\}$. Then $\pi = (1, x, 1, y, 1)$ is an iterative pair of xy in $S_{\leq}$, and $\text{Exp}(\pi, S_{\leq}) = \{(n, m) \mid 0 \leq n \leq m\}$.

Example 1.3 Let $L = \{x^n y^m \mid 0 \leq n \leq m \leq n+3\}$. The word xy admits the iterative pair $\pi = (1, x, 1, y, 1)$ in L . The word $x^4 y^4$ admits the iterative pair $\pi' = (1, x^4, 1, x^4, 1)$ in L , and $\text{Exp}(\pi', L) = \Delta$.

Example 1.4 Consider the language

$$L = \{x^k y^p \bar{y}^q z^n \bar{z}^m \bar{x}^k \mid 0 \leq k, 0 \leq p \leq q, 0 \leq m \leq n\}.$$

The word $w = xy\bar{y}z\bar{z}\bar{x}$ admits at least the following iterative pairs in L :

$$\begin{aligned}\pi_1 &= (1, x, y\bar{y}z\bar{z}, \bar{x}, 1); & \pi_2 &= (x, y, 1, \bar{y}, z\bar{z}\bar{x}); & \pi_3 &= (xy\bar{y}, z, 1, \bar{z}, \bar{x}); \\ \pi_4 &= (xy, \bar{y}, 1, 1, z\bar{z}\bar{x}); & \pi_5 &= (xy, 1, 1, \bar{y}, z\bar{z}\bar{x}); & \dots\end{aligned}$$

Example 1.5 The language $\{x^n y^n z^n \mid n \geq 0\}$ has no iterative pairs.

We now introduce a classification of iterative pairs according to the nature of the set of exponents. Let

$$\pi = (a, u, b, v, c)$$

be an iterative pair in L , and define for $k, l \geq 0$:

$$G(l) = \{k : au^k bv^l c \in L\}; \quad D(k) = \{l : au^k bv^l c \in L\}.$$

Definition The iterative pair π in L is called:

left strict if $G(l)$ is finite for any $l \geq 0$;
right strict if $D(k)$ is finite for any $k \geq 0$;
strict if it is both left strict and right strict;
very strict if $\text{Exp}(\pi, L) = \Delta$;
nondegenerated if it is left strict or right strict.

Thus the following implications hold:

$$\text{very strict} \Rightarrow \text{strict} \begin{matrix} \nearrow \text{left strict} \\ \searrow \text{right strict} \end{matrix} \Rightarrow \text{nondegenerated}.$$

This terminology does not fit exactly with the terminology of Boasson and Beauquier. For Boasson [1976], a very strict pair satisfies a somewhat weaker condition, and Beauquier [1978a] calls strict the pairs we call very strict.

Note that if $\pi = (a, u, b, v, c)$ is nondegenerated in L , then both $u \neq 1$ and $v \neq 1$. Indeed, assume for instance that $u = 1$. Then clearly $au^l bv^l c \in L$ for any $l \geq 0$ and thus π is not left strict. Further $aubv^l c = au^l bv^l c \in L$ for $l \geq 0$ and consequently π is not right strict.

We now define the type $\chi(\pi, L)$ of a nondegenerated iterative pair π in L as a word of length 2 over a fixed alphabet $\Xi = \{e, \bar{e}, s, \bar{s}, l, \bar{l}, r, \bar{r}\}$:

$$\chi(\pi, L) = \begin{cases} e\bar{e} & \text{if } \pi \text{ is very strict ("e" for equal);} \\ s\bar{s} & \text{if } \pi \text{ is strict, but not very strict;} \\ l\bar{l} & \text{if } \pi \text{ is left strict, but not right strict;} \\ r\bar{r} & \text{if } \pi \text{ is right strict, but not left strict.} \end{cases}$$

Types are ordered by $e\bar{e} > s\bar{s} > l\bar{l}, s\bar{s} > r\bar{r}$.

This rather lengthy definition will be useful in later sections where we consider systems of iterative pairs.

Example 1.2 (continued). The pair π is left strict, but not right strict in $S_{\leq}$. Thus $\chi(\pi, S_{\leq}) = l\bar{l}$.

Example 1.3 (continued). The pair π is strict, but not very strict. The pair π' is very strict.

Example 1.4 (continued). $\chi(\pi_1) = e\bar{e}$, $\chi(\pi_2) = l\bar{l}$, $\chi(\pi_3) = r\bar{r}$.

The pairs π_4 and π_5 are degenerated. The iterative pairs π_1, π_2, π_3 can be considered to form a "system". The type of this "system" will be defined as $ell\bar{r}\bar{r}\bar{e}$. This is the reason for our notation for types.

Example 1.6 Any iterative pair in a regular language is degenerated.

Example 1.7 The equation $S_2 = xS_2\bar{x} \cup yS_2\bar{y} \cup 1$ defines the symmetric language S_2 over the alphabet $Z = X \cup \bar{X}$, with $X = \{x, y\}$, $\bar{X} = \{\bar{x}, \bar{y}\}$. We claim that any iterative pair in S_2 is very strict. Let indeed

$$\pi = (a, u, b, v, c)$$

be an iterative pair in S_2 . Since $au^n bv^n c \in S_2$ for any $n \geq 0$, and $S_2 \subset X^* \bar{X}^*$, it follows that $u, v \in X^* \cup \bar{X}^*$. Next $f \in S_2$ implies $|f|_X = |f|_{\bar{X}}$. Thus if $u \in \bar{X}^*$ then $u = v = 1$ and π is not an iterative pair. Consequently $u \in X^*$, and similarly $v \in \bar{X}^*$. Therefore $|u| = |v| > 0$ and

$$\text{Exp}(\pi, S_2) = \Delta.$$

Example 1.8 Any iterative pair in the restricted Dyck language $D_1^* \subset \{x, \bar{x}\}^*$ is either degenerated or very strict. Define indeed $\|f\| = |f|_x - |f|_{\bar{x}}$ for $f \in \{x, \bar{x}\}^*$ and consider an iterative pair

$$\pi = (a, u, b, v, c)$$

in D_1^* . In view of the characterization of D_1^* given by Corollary II.4.2, we have $0 = \|aubvc\| = \|abc\| + \|u\| + \|v\| = \|u\| + \|v\|$, whence $\|u\| = -\|v\|$. Next $\|u\| \geq 0$, since otherwise $\|au^n\| = \|a\| + n\|u\| < 0$ for sufficiently large n , contrary to the fact that $au^n bv^n c \in D_1^*$. If $\|u\| = 0 = \|v\|$, then $0 \leq \|au^n\| = \|au^n u'\|$ for any left factor u' of u , and $0 \leq \|aubv^n\| = \|au^n bv^n v'\|$ for any left factor v' of v . Thus $au^* bv^* c \in D_1^*$ and π is degenerated. Otherwise $\|u\| > 0$ and $\|v\| < 0$ and $\|au^n bv^m c\| = (n - m)\|u\|$. Thus $au^n bv^m c \in D_1^*$ iff $n = m$. Consequently π is very strict.

We conclude this section by some simple lemmas concerning the transfer of iterative pairs.

Lemma 1.1 Let π be an iterative pair in $L \cap K$, where L is a language and K is a local regular language. Then π is an iterative pair in L , and $\text{Exp}(\pi, L) = \text{Exp}(\pi, L \cap K)$.

Proof. Let $\pi = (a, u, b, v, c)$. Since $L \cap K \subset L$, $\text{Exp}(\pi, L \cap K) \subset \text{Exp}(\pi, L)$. Next $au^n bv^n c \in K$ for all $n \geq 0$. Since K is local, this implies $au^* bv^* c \in K$ (see Exercise I.4.1). Thus $L \cap K \supset L \cap au^* bv^* c$ and

$$\text{Exp}(\pi, L) = \text{Exp}(\pi, L \cap au^* bv^* c) \subset \text{Exp}(\pi, L \cap K). \quad \blacksquare$$

Let $\varphi: X^* \rightarrow Y^*$ be a morphism. For a sequence

$$\pi = (a, u, b, v, c)$$

of words of X^* , define

$$\varphi\pi = (\varphi a, \varphi u, \varphi b, \varphi v, \varphi c).$$

Lemma 1.2 Let $M \subset Y^*$, $L = \varphi^{-1}(M)$. If π is a nondegenerated iterative pair in L , then $\varphi\pi$ is an iterative pair in M and $\text{Exp}(\pi, L) = \text{Exp}(\varphi\pi, M)$.

Proof. Let $\pi = (a, u, b, v, c)$. If $au^k bv^l c \in L$, then $\varphi(au^k bv^l c) \in M$. Thus $\text{Exp}(\pi, L) \subset \text{Exp}(\varphi\pi, M)$. Conversely, if $\varphi(au^k bv^l c) \in M$, then $au^k bv^l c \in \varphi^{-1}(M) = L$. Consequently $\text{Exp}(\pi, L) = \text{Exp}(\varphi\pi, M)$. It remains to show that $|\varphi u \varphi v| > 0$. Suppose the contrary. Then $\text{Exp}(\varphi\pi, M) = \mathbb{N}^2$ and π is degenerated, contrary to the assumption. $\blacksquare$

There is a lack of a lemma of the following kind: If $L \subset X^*$ and $M = \varphi(L)$, and if π' is an iterative pair in M , then there is an iterative pair π in L such that $\varphi\pi = \pi'$. Such a lemma does not exist.

Example 1.7 Let $L = \{x^n y^n z^n : n \geq 0\}$ and let $\varphi: \{x, y, z\}^* \rightarrow \{x, y\}^*$ be the projection. Then $M = \varphi(L) = \{x^n y^n : n \geq 0\}$ has iterative pairs but L has no iterative pairs.

The next section will be concerned with a strengthened notion of iterative pairs for the case of algebraic languages.

Exercises

1.1 Let $\pi = (a, u, b, v, c)$ be an iterative pair in L . Show that $\pi^N = (a, u^N, b, v^N, c)$ is an iterative pair in L for any $N \geq 1$. Show that $\chi(\pi^N, L) \geq \chi(\pi, L)$, and give an example where this inequality is strict.

1.2 Let $\pi = (a, u, b, v, c)$ be a nondegenerated iterative pair in $L \subset X^*$. Show that the mapping $(k, l) \mapsto au^k bv^l c$ from $\mathbb{N}^2$ into X^* is injective. (Hint. Use Exercise I.2.6.)

1.3 (Beauquier [1977]) An iterative pair $\pi = (a, u, b, v, c)$ is bounded in L iff there is an integer K such that $G(l)$ and $D(k)$ have at most K elements for any $l, k \geq 0$. Show that if L is context-free and π is bounded in L , then there exists an iterative pair π' which is very strict in L . (Hint. Use the fact, proved for instance in Ginsburg [1966], that $\text{Exp}(\pi, L)$ is a rational subset of $\mathbb{N}^2$ for context-free L .)

1.4 Let $\pi = (a, u, b, v, c)$ be an iterative pair in L . Show that if $L \cap au^* bv^* c$ is a regular language, then π is degenerated (the converse is false).

VIII.2 Grammatical Pairs

The iteration lemma for context-free languages shows the existence of iterative pairs for any infinite context-free language L . The iterative pairs obtained in that way depend on the grammar $G = \langle V, X, P \rangle$ generating L . More precisely, if $L = L_G(\xi_0)$, then the iteration lemma gives an iterative pair $\pi = (a, u, b, v, c)$ together with a variable $\xi \in V$ such that

$$\xi_0 \xrightarrow{*} a\xi c, \quad \xi \xrightarrow{*} u\xi v, \quad \xi \xrightarrow{*} b.$$

It follows that two different grammars for a same language can give two distinct iterative pairs of the same word. This raises the question how an iterative pair π of a word w in L is linked to the iterative pairs of w which are supplied by the grammars generating L . A rather precise answer to this question will be given in this section. It shows how a "combinatorial" property of the language L , described by the iterative pair, is related to a common "generative" property of all grammars generating L . We first give a definition.

Definition Let $L \subset X^*$ be an algebraic language, let $G = \langle V, X, P \rangle$ be an algebraic grammar such that $L = L_G(\xi_0)$ for $\xi_0 \in V$. An iterative pair $\pi = (a, u, b, v, c)$ in L is grammatical with respect to G if there exists a variable $\xi \in V$ such that

$$\xi_0 \xrightarrow{*} a\xi c, \quad \xi \xrightarrow{*} u\xi v, \quad \xi \xrightarrow{*} b.$$

The variable ξ is called the pivot of π in G .

Example 2.1 Let $X = \{x, y, z\}$, and let

$$L = \{x^{3n} zy^{3n} \mid n \geq 0\}.$$

The word $w = x^6 zy^6$ admits the three iterative pairs in L :

$$\begin{aligned} \pi_1 &= (1, x^6, z, y^6, 1), & \pi_2 &= (x^2, x^3, xzy, y^3, y^2), \\ \pi_3 &= (x, x^3, x^2zy, y^3, y^2). \end{aligned}$$

Next consider the grammar G with productions

$$\xi_0 \rightarrow x^3 \xi y^3 + \xi; \quad \xi \rightarrow x^6 \xi y^6 + z.$$

Then π_1 is grammatical with respect to G , and neither π_2 nor π_3 are grammatical in G .

The example shows however that π_2 and π_3 can be transformed into grammatical pairs first by taking a power of the iterating elements and then by "shifting" these new iterating elements. We shall see that this procedure is valid in the general case. First we prove some lemmas concerning transfer of grammatical pairs.

Lemma 2.1 Let $L \subset X^*$ be generated by an algebraic grammar G , and let $K \subset X^*$ be a rational language. If π is an iterative pair in $L \cap K$ grammatical with respect to G_K , then π is grammatical with respect to G .

Recall that G_K is the grammar generating $L \cap K$ defined in Section II.2.

Proof. Let $\pi = (a, u, b, v, c)$. Assume that G and G_K are as in Section II.2. Then there exist derivations in G_K :

$$\hat{\sigma} \xrightarrow{*} a(q, \xi, q')c; \quad (q, \xi, q') \xrightarrow{*} u(q, \xi, q')v; \quad (q, \xi, q') \xrightarrow{*} b.$$

The first derivation factorizes into

$$\hat{\sigma} \rightarrow (q_-, \sigma, q_+) \xrightarrow{*} a(q, \xi, q')c$$

for some q_+ . Consequently there exist, in the grammar G , derivations

$$\sigma \xrightarrow{*} a\xi c; \quad \xi \xrightarrow{*} u\xi v; \quad \xi \xrightarrow{*} b,$$

showing that π is grammatical with respect to G . ■

Lemma 2.2 Let $\varphi: X^* \rightarrow Y^*$ be an alphabetic morphism, let $M \subset Y^*$ be generated by some algebraic grammar G , and let $L = \varphi^{-1}(M)$. If π is a nondegenerated iterative pair in L grammatical with respect to $\varphi^{-1}(G)$, then $\varphi\pi$ is grammatical with respect to G .

Proof. Let $\pi = (a, u, b, v, c)$. In view of Lemma 1.2, $\varphi\pi$ is an iterative pair in M . With the notations of Section II.2, there are in the grammar $\varphi^{-1}G$ derivations

$$\sigma \xrightarrow{*} a\eta c, \quad \eta \xrightarrow{*} u\eta v, \quad \eta \xrightarrow{*} b.$$

In order to show that there are derivations

$$\sigma \xrightarrow{*} \varphi(a)\eta\varphi(c), \quad \eta \xrightarrow{*} \varphi(u)\eta\varphi(v), \quad \eta \xrightarrow{*} \varphi(b)$$

in G , it suffices to show that the nonterminal η is distinct from ω . Now if $\eta = \omega$, then $\varphi u = \varphi v = 1$, and $\varphi\pi$ is not an iterative pair. This achieves the proof. ■

The following lemma is important and will be used in the next section.

Lemma 2.3 Let $\psi: X^* \rightarrow Y^*$ be a morphism, let $L \subset X^*$ be generated by an algebraic grammar G , and let $M = \psi(L)$. If π is an iterative pair in L grammatical with respect to ψG , then there exists an iterative pair π' in L grammatical with respect to G , such that $\psi\pi' = \pi$. Further $\text{Exp}(\pi', L) \subset \text{Exp}(\pi, M)$.

This lemma shows that iterative pairs can be transferred through a morphism, provided they are grammatical with respect to some specific grammar.

Proof. Let $\pi = (a, u, b, v, c)$. By assumption there are in the grammar ψG derivations

$$\sigma \xrightarrow{*} a\xi c, \quad \xi \xrightarrow{*} u\xi v, \quad \xi \xrightarrow{*} b.$$

Consequently there are words a', u', b', v', c' in X^* such that $\psi a' = a$, $\psi u' = u$, $\psi b' = b$, $\psi v' = v$, $\psi c' = c$, and

$$\sigma \xrightarrow{*} a'\xi c', \quad \xi \xrightarrow{*} u'\xi v', \quad \xi \rightarrow b'$$

in the grammar G . Thus $\pi' = (a', u', b', v', c')$ is an iterative pair in L grammatical with respect to G . The inclusion $\text{Exp}(\pi', L) \subset \text{Exp}(\pi, M)$ is obvious. ■

We now rely nondegenerated pairs to grammatical pairs. First we need a definition.

Definition Let $\pi = (a, u, b, v, c)$ and $\bar{\pi} = (\bar{a}, \bar{u}, \bar{b}, \bar{v}, \bar{c})$ be two sequences of words. Then $\bar{\pi}$ is deduced from π if the two following conditions hold:

(i) there is an integer $N \geq 1$ such that

$$\bar{a}\bar{u}\bar{b}\bar{v}\bar{c} = au^Nbv^Nc;$$

(ii) there are integers $p, q \geq 0$, and factorizations $u = u_1u_2$, $v = v_1v_2$ such that

$$\bar{a} \in au^*u_1, \quad \bar{u} = (u_2u_1)^p, \quad \bar{b} \in u_2u^*bv^*v_1, \quad \bar{v} = (v_2v_1)^q, \quad \bar{c} \in v_2v^*c.$$

Condition (ii) implies that

$$\bar{a}\bar{u}^{k+1}\bar{b}\bar{v}^{l+1}\bar{c} = au^{N+pk}bv^{N+ql}c \quad \text{for } k+1, l+1 \geq 0.$$

Assume next that π and $\bar{\pi}$ are iterative pairs in some language L . Then

$$(k, l) \in \text{Exp}(\bar{\pi}, L) \Leftrightarrow (N+p(k-1), N+q(l-1)) \in \text{Exp}(\pi, L). \quad (2.1)$$

This implies immediately

Lemma 2.4 Let π and $\bar{\pi}$ be iterative pairs in L , and assume that $\bar{\pi}$ is deduced from π . If π is nondegenerated, then $\bar{\pi}$ is nondegenerated and $\chi(\bar{\pi}, L) \geq \chi(\pi, L)$. ■

Example 2.1 (continued). The pair $\bar{\pi} = (x^3, x^6, x^3zy^3, y^6, y^3)$ is deduced from π_2 , and is deduced from π_3 . It is grammatical with respect to G .

Theorem 2.5 Let $L \subset X^*$ be an algebraic language, and let π be a nondegenerated iterative pair in L . For any algebraic grammar generating L there exists an iterative pair $\bar{\pi}$ deduced from π and grammatical with respect to G .

Proof. We first prove the theorem for iterative pairs of a special kind and derive then the general case from this special case.

Assume $X = Z \cup \{t, x, y\}$, with $t, x, y \notin Z$, and suppose that π has the form

$$\pi = (at, xu, tbt, yv, tc)$$

with $a, u, b, v, c \in Z^*$. Define

$$L' = L \cap K, \quad K = at(xu)^*tbt(yv)^*tc.$$

Recall that $\text{Exp}(\pi, L) = \text{Exp}(\pi, L')$. Next let $H = G_K$ be the grammar generating L' . By Lemma 2.1, it suffices to prove the existence of an iterative pair grammatical with respect to H . Let N be the integer associated to H by Ogden's Iteration Lemma II.2.5, and define

$$g = at(xu)^Ntbt(yv)^Ntc.$$

Since π is nondegenerated, it is left strict or right strict. Suppose first π left strict and mark the N occurrences of the letter x in g . In view of Lemma II.2.5, g admits in L' an iterative pair

$$\bar{\pi} = (\bar{a}, \bar{u}, \bar{b}, \bar{v}, \bar{c})$$

which is grammatical with respect to H , and $\bar{a}, \bar{u}, \bar{b}$ or $\bar{b}, \bar{v}, \bar{c}$ contain occurrences of x . We have to prove that $\bar{\pi}$ is deduced from π . First note that neither $\bar{u}$ nor $\bar{v}$ contain a letter t since otherwise $\bar{a}\bar{u}^2\bar{b}\bar{v}^2\bar{c} \notin K$. Next neither $\bar{u}$ nor $\bar{v}$ can be nonempty factors of a or b or c . We prove that $\bar{v}$ contains no occurrence of x . Assume indeed $|\bar{v}|_x > 0$. Then $\bar{v}$ is a segment of $(xu)^N$. This implies that $\bar{a}\bar{u}^k\bar{b}\bar{v}^k \in at(xu)^*$ for $k \geq 0$. Hence the number of x 's in the words $\bar{a}\bar{u}^k\bar{b}\bar{v}^k\bar{c}$ increases with k , and the number of y 's remains constant equal to N . This is in contradiction with the fact that π is left strict in L , hence in L' . Thus $|\bar{v}|_x = 0$.

Since $\bar{v}$ contains no occurrences of the letter x , $\bar{u}$ contains occurrences of x , and $\bar{u}$ is a segment of $(xu)^N$ and similarly $\bar{v}$ is a segment of $(yv)^N$. Thus there are integers $p, q \geq 0$ such that

$$\bar{u} = u_2(xu)^p xu_1, \quad \bar{v} = v_2(yv)^q yv_1$$

for words $u_1, u_2, v_1, v_2 \in Z^*$. Since $\bar{a}\bar{u}^2\bar{b}\bar{v}^2\bar{c} \in K$, this implies that $u = u_1 u_2$, $v = v_1 v_2$. It follows immediately that $\bar{\pi}$ is deduced from π . This proves the special case for left strict pairs. The case of right strict pairs is proved in the same manner by marking the occurrences of y in g .

Consider now the general case of a nondegenerated iterative pair $\pi = (a, u, b, v, c)$ in $L \subset X^*$. Let t, x, y be new letters, set $Y = X \cup \{t, x, y\}$, and let $\varphi: Y^* \rightarrow X^*$ be the projection. Let $L' = \varphi^{-1}(L)$ and $K = at(xu)^*tbt(yv)^*tc$,

$$\pi' = (at, xu, tbt, yv, tc).$$

Then $\varphi\pi' = \pi$, and obviously $\text{Exp}(\pi', L') = \text{Exp}(\pi, L)$. By the first part of the proof, there exists a pair $\hat{\pi}$ deduced from π' which is grammatical with respect to the grammar $\varphi^{-1}(G)$. Then $\bar{\pi} = \varphi\hat{\pi}$ is deduced from $\pi = \varphi\pi'$, and is grammatical with respect to the grammar G in view of Lemma 2.2. ■

VIII.3. Transfer of Iterative Pairs

We are now ready for the proof of the main theorem concerning transfer of iterative pairs through rational transductions.

Theorem 3.1 (Transfer Theorem) *Let A and B be algebraic languages such that $A \geq B$. For any nondegenerated iterative pair π in B , there is a nondegenerated iterative pair π' in A such that $\chi(\pi', A) \geq \chi(\pi, B)$.*

As already noted, this theorem is false for nonalgebraic languages. The result gives a necessary condition for rational domination of algebraic languages. But the Transfer Theorem can also be regarded as a result on rational transductions: Rational transductions only decrease and never increase the types of iteration pairs occurring in algebraic languages. Thus rational transductions decrease the "complexity" of context-free languages in so far as the type of the iterative pairs of a language is considered as a measure of its complexity.

Let $A \subset X^*$, $B \subset Y^*$, and assume $A \geq B$. Then by Nivat's Theorem, there is an alphabet Z such that

$$B = \psi(\varphi^{-1}(A) \cap K)$$

where $\psi: Z^* \rightarrow Y^*$ is a morphism, $\varphi: Z^* \rightarrow X^*$ can be chosen to be an alphabetic morphism and $K \subset Z^*$ is a regular language which we may suppose to be local. We first prove

Proposition 3.2 *Let G be an algebraic grammar generating A . For any nondegenerated iterative pair $\pi = (a, u, b, v, c)$ in B grammatical with respect to the grammar $\psi[\varphi^{-1}(G)_K]$, there is an iterative pair $\pi' = (a', u', b', v', c')$ in A grammatical with respect to G such that $\text{Exp}(\pi', A) \subset \text{Exp}(\pi, B)$. Moreover*

$$au^k bv^l c \in \psi[\varphi^{-1}(a'u'^k b'v'^l c') \cap K] \quad \text{for } k, l \geq 0.$$

Proof. Set $C = \varphi^{-1}(A) \cap K$. In view of Lemma 2.3, there exists an iterative pair $\pi_1 = (a_1, u_1, b_1, v_1, c_1)$ in C , grammatical with respect to $(\varphi^{-1}G)_K$, such that $\psi\pi_1 = \pi$. Further $\text{Exp}(\pi_1, C) \subset \text{Exp}(\pi, B)$. Since K is local $\text{Exp}(\pi_1, C) = \text{Exp}(\pi_1, \varphi^{-1}(A))$ by Lemma 1.1. Next π_1 is grammatical with respect to $\varphi^{-1}G$ by Lemma 2.1. Define $\pi' = \varphi\pi_1$. Since π_1 is nondegenerated, π' is an iterative pair in A , and $\text{Exp}(\pi_1, \varphi^{-1}(A)) = \text{Exp}(\pi', A)$ by Lemma 1.2. Finally π' is grammatical with respect to G in view of Lemma 2.2. Further $\text{Exp}(\pi', A) \subset \text{Exp}(\pi, B)$. Now consider a word $w = a'u'^k b'v'^l c'$. Then $w_1 = a_1 u_1^k b_1 v_1^l c_1 \in \varphi^{-1}(w)$ and since $K \supset a_1 u_1^* b_1 v_1^* c_1$, $w_1 \in \varphi^{-1}(w) \cap K$. Consequently $\psi w_1 = au^k bv^l c \in \psi(\varphi^{-1}(w) \cap K)$. ■

Proof of Theorem 3.1. Let φ, ψ, K, Z be as above, and let G be a grammar generating A . Let π be a nondegenerated iterative pair in B . In view of Theorem 2.5, there exists an iterative pair $\bar{\pi}$ deduced from π , and grammatical

with respect to the grammar $\psi[\varphi^{-1}(G)_K]$. Further $\chi(\tilde{\pi}, B) \geq \chi(\pi, B)$ by Lemma 2.4. In view of the Proposition 3.2 above, there is an iterative pair π' in A such that $\text{Exp}(\pi', A) \subset \text{Exp}(\tilde{\pi}, B)$. Consequently $\chi(\pi', A) \geq \chi(\tilde{\pi}, B) \geq \chi(\pi, B)$. ■

The Transfer Theorem can be strengthened in the following way.

Corollary 3.3. *Let A and B be algebraic languages. If $A \geq B$, then for any nondegenerated iterative pair π in B , there are a nondegenerated iterative pair π' in A , and integers $N, p, q \geq 1$ such that*

$$(k, l) \in \text{Exp}(\pi', A) \Rightarrow (N + p(k-1), N + q(l-1)) \in \text{Exp}(\pi, B).$$

Proof. With the notations of the proof of Theorem 3.1, the grammatical iterative pair $\tilde{\pi}$ deduced from π satisfies formula (2.1). The corollary follows then immediately from Proposition 3.2. ■

As an illustration, we show that some of the results of Section V.7 are simple applications of the Transfer Theorem.

Example 3.1 The languages $S_>$ and $S_<$ are incomparable. Indeed, the language $S_>$ has right strict iterative pairs and $S_<$ has no right strict iterative pair. Thus $S_<$ does not dominate $S_>$. The symmetric result is obtained by considering left strict pairs in $S_<$.

Example 3.2 S_* dominates none of the languages $S_-, S_>, S_<$. Indeed, the languages $S_-, S_>, S_<$ all have nondegenerated iterative pairs. On the contrary, all iterative pairs in S_* are degenerated.

Note that the Transfer Theorem cannot be used to prove that $S_>$ and $S_<$ do not dominate S_* (Proposition V.7.2), since S_* only has degenerated pairs.

Example 3.3 Any generator of the cone Alg or of Lin or Rocl has at least one very strict iterative pair. Indeed, any generator of one of these cones must dominate S_- .

There is an interesting interpretation of this example: It has been proved (Alt [1977], Alt and Mehlhorn [1976]) that if L is a context-free language which admits a nondegenerated iterative pair, then the membership problem for L (i.e. the problem to decide whether $u \in L$ or not) requires $\log n$ space ($n = |u|$) infinitely many often on a nondeterministic Turing machine. Thus the languages of Example 3.3 all have space complexity at least $\log n$. On the other hand, languages like the Dyck languages can be analyzed in space $\log n$ (see Hotz and Messerschmidt [1974]).

As an illustration of the more precise version of the Transfer Theorem formulated in Corollary 3.3, we now give another infinite chain of rational cones which all lie in $\text{Rocl} \cap \text{Lin}$. Moreover we prove the existence of infinitely many pairwise incomparable rational cones.

Let $X = \{x, y\}$. For rational numbers $0 < r \leq s$ define a language $M(r, s) \subset x^*y^*$ by

$$M(r, s) = 1 \cup \left\{ x^n y^m \mid n, m \in \mathbb{N} \setminus 0, r \leq \frac{m}{n} \leq s \right\}.$$

Thus $M(1, 1) = S_-$. In Exercise V.7.2, it is stated that $M(r, s) \approx M(qr, qs)$ for any rational number $q > 0$, whence $M(r, s) \approx M(r/s, 1)$. Thus only languages of the form $M(q, 1)$, ($0 < q \leq 1$), q rational have to be considered.

Proposition 3.4 (Berstel [1973]) *Let q, q' be rational numbers with $0 < q, q' \leq 1$. If $M(q', 1) \geq M(q, 1)$, then $q' \geq q$.*

The converse property, namely $q' \geq q \Rightarrow M(q', 1) \geq M(q, 1)$ is stated in Exercise V.7.2. Thus

Corollary 3.5 *For rational numbers $0 < q, q' \leq 1$, $M(q', 1) \geq M(q, 1)$ iff $q' \geq q$.* ■

In particular, $q' > q$ implies $M(q', 1) \not\approx M(q, 1) \Gamma$. Hence the rational cones $M(q, 1) \Gamma$ ($0 < q \leq 1$) form an infinite chain of principal cones which is order-isomorphic to the interval $0 < q \leq 1$ of rational numbers. In particular, for any two rational numbers $1 \geq q' > q > 0$, there exist infinitely many cones $\mathcal{L}$ such that $M(q', 1) \Gamma \not\approx \mathcal{L} \not\approx M(q, 1) \Gamma$.

Proof. Assume $M(q', 1) \geq M(q, 1)$. The word xy admits in $M(q, 1)$ the strict iterative pair $\pi = (1, x, 1, y, 1)$, and

$$\text{Exp}(\pi, M(q, 1)) = \{(0, 0)\} \cup \left\{ (n, m) \in (\mathbb{N} \setminus 0)^2 \mid q \leq \frac{m}{n} \leq 1 \right\}.$$

By Corollary 3.3, there exist an iterative pair π' in $M(q', 1)$, and integers $N, a, b \geq 1$ such that

$$(n, m) \in \text{Exp}(\pi', M(q', 1)) \Rightarrow (N + (n-1)a, N + (m-1)b) \in \text{Exp}(\pi, M(q, 1)). \quad (3.1)$$

Since π' is strict, it has the form

$$\pi' = (x^{a'}, x^{a'}, x^{n_2} y^{m_1}, y^{b'}, y^{m_2}) \quad n_1, n_2, m_1, m_2 \geq 0, \quad a', b' \geq 1.$$

Set $c = N - a$, $d = N - b$, $c' = n_1 + n_2$, $d' = m_1 + m_2$. Then

$$\text{Exp}(\pi', M(q', 1)) \supset \left\{ (n, m) \in (\mathbb{N} \setminus 0)^2 \mid q' \leq \frac{d' + mb'}{c' + na'} \leq 1 \right\} \neq \emptyset,$$

and by (3.1)

$$q' \leq \frac{d' + mb'}{c' + na'} \leq 1 \Rightarrow q \leq \frac{d + mb}{c + na} \leq 1 \quad (n, m > 0). \quad (3.2)$$

In order to exploit this relation, define functions γ_r, γ'_r for rational r by

$$\gamma_r(n) = nr \frac{a}{b} + \frac{rc-d}{b}; \quad \gamma'_r(n) = nr \frac{a'}{b'} + \frac{rc'-d'}{b'}. \quad (3.3)$$

A straightforward computation shows that

$$q \leq \frac{d+mb}{c+na} \leq 1 \quad \text{iff} \quad \gamma_q(n) \leq m \leq \gamma_1(n)$$

and similarly for γ'_q . Thus (3.2) is equivalent to

$$\gamma'_q(n) \leq m \leq \gamma'_1(n) \Rightarrow \gamma_q(n) \leq m \leq \gamma_1(n) \quad (n > 0). \quad (3.4)$$

The values of the functions γ, γ' are rational, not necessarily integral numbers. Hence (3.4) implies

$$\gamma'_q(n) \geq \gamma_q(n) - 1; \quad \gamma'_1(n) \leq \gamma_1(n) + 1 \quad (n > 0).$$

In view of (3.3), it follows that $q' \frac{a'}{b'} \geq q \frac{a}{b}$ and $\frac{a'}{b'} \leq \frac{a}{b}$, whence $q' \geq q$. ■

For rational numbers $0 < r < s < t < 1$, define

$$K(r, s, t) = M(r, s) \cup M(t, 1).$$

Lemma 3.6 If $K(r', s', t') \geq K(r, s, t)$, and $t = t', \frac{r}{s} = \frac{r'}{s'}$, then $r = r', s = s'$.

Proof. By the same argument as in the preceding proof, the inequality $K(r', s', t) \geq K(r, s, t)$ implies for $n, m > 0$:

$$\begin{aligned} \text{if} \quad & \gamma'_r(n) \leq m \leq \gamma'_s(n) \quad \text{or} \quad \gamma'_t(n) \leq m \leq \gamma'_1(n) \\ \text{then} \quad & \gamma_r(n) \leq m \leq \gamma_s(n) \quad \text{or} \quad \gamma_t(n) \leq m \leq \gamma_1(n) \end{aligned} \quad (3.5)$$

As above, this implies the inequalities

$$r' \frac{a'}{b'} \geq r \frac{a}{b}, \quad \frac{a'}{b'} \leq \frac{a}{b} \quad (3.6)$$

whence $r \leq r', s \leq s'$. In order to derive the equality, we claim that there exists an integer n_0 such that

$$\gamma'_r(n) \leq m \leq \gamma'_s(n) \Rightarrow \gamma_r(n) \leq m \leq \gamma_s(n) \quad n \geq n_0 \quad (3.7)$$

$$\gamma'_t(n) \leq m \leq \gamma'_1(n) \Rightarrow \gamma_t(n) \leq m \leq \gamma_1(n) \quad n \geq n_0. \quad (3.8)$$

Note first that for rational numbers $z, z', \gamma_z(n) \leq \gamma_{z'}(n)$ implies

$$n \left(z \frac{a}{b} - z' \frac{a'}{b'} \right) \leq \frac{z'c' - d'}{b'} - \frac{zc - d}{b},$$

thus if n is sufficiently large,

$$\gamma_z(n) \leq \gamma_{z'}(n) \Rightarrow z \frac{a}{b} \leq z' \frac{a'}{b'} \quad \text{and} \quad \gamma_z(n) \geq \gamma_{z'}(n) \Rightarrow z \frac{a}{b} \geq z' \frac{a'}{b'}. \quad (3.9)$$

Let n_1 be such that (3.9) holds for $z \in \{r, s, t, 1\}, z' \in \{r', s', t', 1\}$. Next since $r' < s', \gamma'_s(n) - \gamma'_r(n) \geq 1$ for sufficiently large n , and consequently there is an integer m such that $\gamma'_r(n) \leq m \leq \gamma'_s(n)$. Let n_2 be such that $\gamma'_s(n) - \gamma'_t(n) \geq 1$ and $\gamma'_1(n) - \gamma'_t(n) \geq 1$ for all $n \geq n_2$, and set $n_0 = \max(n_1, n_2)$.

Assume now that (3.7) is false. Then there are integers $n \geq n_0, m$ such that, by (3.5),

$$m \leq \gamma'_s(n) \quad \text{and} \quad \gamma_t(n) \leq m,$$

whence $\gamma_t(n) \leq \gamma'_s(n)$ and by (3.9), $t \frac{a}{b} \leq s' \frac{a'}{b'}$. Since $t = t'$, (3.6) implies $t' \leq s'$ which is impossible. Thus (3.7) holds. Consequently $\gamma'_s(n) \leq \gamma_s(n) + 1$ for all $n \geq n_0$, and therefore $s' \frac{a'}{b'} \leq s \frac{a}{b}$. In view of (3.6) and since $\frac{r}{s} = \frac{r'}{s'}$,

$$r \frac{a}{b} = r' \frac{a'}{b'}, \quad s \frac{a}{b} = s' \frac{a'}{b'} \quad (3.10)$$

Next assume (3.8) is false. Then as above there is an integer $n \geq n_0$ such that $\gamma'_t(n) \leq \gamma_s(n)$, and by (3.9) it follows that $t' \frac{a'}{b'} \leq s \frac{a}{b}$. By (3.10), this again implies $t' \leq s'$, which is impossible. This proves (3.8). (3.8) implies $\gamma'_t(n) \geq \gamma_t(n) - 1$ for $n \geq n_0$, whence $t' \frac{a'}{b'} \geq t \frac{a}{b} = t' \frac{a}{b}$. Thus $\frac{a'}{b'} \geq \frac{a}{b}$. By (3.6), we obtain $\frac{a'}{b'} = \frac{a}{b}$, and by (3.10), it follows that $r = r', s = s'$. ■

Proposition 3.7 (Berstel [1973]) Let $0 < r < s < t < 1$. For any two rational numbers $q \neq q'$ with $0 < q, q' < 1$, the rational cones generated by $K(qr, qs, t)$ and $K(q'r, q's, t)$ are incomparable.

Proof. Assume for instance that $K(q'r, q's, t) \geq K(qr, qs, t)$. Then by Lemma 3.6, $q'r = qr$, whence $q = q'$. ■

Proposition 3.7 shows the existence of an infinity of pairwise incomparable rational cones all contained in $\text{RocI} \cap \text{Lin}$, since all languages $K(r, s, t)$ are dominated by S_- . It can be shown (Exercise 3.1) that the full AFLs generated by $K(qr, qs, t)$ and $K(q'r, q's, t)$ are also incomparable.

Exercise

3.1 (Berstel [1974]) Let $L, M \subset x^*y^*$ be two context-free languages. Show that $LF \subset MF$ iff $L\hat{F} \subset M\hat{F}$. Prove that the full AFLs $K(qr, qs, t)\hat{F}$ and $K(q'r, q's, t)\hat{F}$ are incomparable for $q \neq q'$.

VIII.4 Systems of Iterative Pairs

The Transfer Theorem for iterative pairs proved in the preceding section gives a first criterion for rational domination, but the notion of iterative pairs is not powerful enough to allow comparison of languages whose words admit simultaneously several iterative pairs. Consider for instance the languages

$$A = \{x^n y^n z^p t^p : n, p \geq 0\} \quad \text{and} \quad B = \{x^n y^p z^p t^n : n, p \geq 0\}.$$

All iterative pairs in these two languages are very strict, so the Transfer Theorem gives no information. We shall see that A and B are incomparable. This will follow from the consideration of "systems" of iterative pairs. In the present example, systems for A are formed of two consecutive pairs, and systems for B are formed of nested pairs. Thus the types of systems are incomparable, and in view of a Transfer Theorem to be proved, the languages are rationally incomparable.

The present section contains the definition and examples of systems of iterative pairs. Section 5 is concerned with grammatical systems, and Section 6 contains the proof of the Transfer Theorem for systems.

We shall be concerned in the sequel with sequences of words of the form

$$\theta = (a_0, u_1, a_1, \dots, a_{m-1}, u_m, a_m) \quad (4.1)$$

and with sequences derived from (4.1) by concatenating some of its terms. A typical sequence related to (4.1) is

$$\theta' = (a_0 u_1 a_1 \dots a_{i_1-1}, u_{i_1}, a_{i_1}, u_{i_1+1} \dots a_{i_2-1}, u_{i_2}, \dots, u_{i_r}, a_{i_r} \dots u_m a_m) \quad (4.2)$$

with $1 \leq i_1 < \dots < i_r \leq m$. For sake of simplicity, we introduce the notation

$$\theta' = \langle u_{i_1}, u_{i_2}, \dots, u_{i_r} \rangle \quad (4.3)$$

for (4.2). Thus $\langle u_1, u_2, \dots, u_m \rangle$ is equivalent to (4.1), and $\pi = \langle u, v \rangle$ is an equivalent notation for $\pi = (a, u, b, v, c)$.

Next if L is a language we define

$$\text{Exp}(\theta, L) = \{(k_1, \dots, k_m) \in \mathbb{N}^m \mid a_0 u_1^{k_1} a_2 \dots a_{m-1} u_m^{k_m} a_m \in L\}.$$

Finally we introduce the following notation: For $P \subset \mathbb{N}^2$, $Q \subset \mathbb{N}^q$,

$$P * Q = \{(p, k_1, \dots, k_q, p') \mid (p, p') \in P, (k_1, \dots, k_q) \in Q\}.$$

Thus, with $\Delta = \{(n, n) : n \geq 0\}$ we have for instance

$$\Delta * \Delta = \{(n, m, m, n) : n, m \geq 0\}$$

while $\Delta \times \Delta = \{(n, n, m, m) : n, m \geq 0\}$.

Definition Let X be an alphabet, and let $L \subset X^*$ be a language. A sequence of words of X^*

$$\theta = (a_0, u_1, a_1, \dots, a_{2n-1}, u_{2n}, a_{2n})$$

is a system of iterative pairs of length n in L if one of the following conditions is satisfied:

- (i) $n = 1$ and θ is a nondegenerated iterative pair in L ;
- (ii) $n > 1$ and
 - (ii.1) $\pi = \langle u_1, u_{2n} \rangle$ is a nondegenerated iterative pair in L ,
 - (ii.2) $\theta' = \langle u_2, \dots, u_{2n-1} \rangle$ is a system of iterative pairs in L ,
 - (ii.3) $\text{Exp}(\theta, L) \supset \text{Diag}(\theta, L)$, where $\text{Diag}(\theta, L) = \Delta * \text{Diag}(\theta', L)$.
- (iii) $n > 1$ and there is some integer p , ($1 \leq p < n$) such that
 - (iii.1) $\theta_1 = \langle u_1, \dots, u_{2p} \rangle$ and $\theta_2 = \langle u_{2p+1}, \dots, u_{2n} \rangle$ are systems of iterative pairs in L ,
 - (iii.2) $\text{Exp}(\theta, L) \supset \text{Diag}(\theta, L)$, where $\text{Diag}(\theta, L) = \text{Diag}(\theta_1, L) \times \text{Diag}(\theta_2, L)$.

θ is called a system of iterative pairs of the word $w = a_0 u_1 \dots u_{2n} a_{2n}$ in L , and w is said to admit the system θ in L .

Notation. If θ is defined by condition (ii), then we write $\theta = \pi * \theta'$; if θ is defined by (iii), then we write $\theta = \theta_1 \times \theta_2$.

With this notation, any system of iterative pairs θ of length n of a word w has an expression as a combination of n nondegenerated iterative pairs $\pi_1, \dots, \pi_n$ of w , which are combined by the operations $*$ and $\times$. The pairs $\pi_1, \dots, \pi_n$ are called the underlying pairs of θ . Note that the operation $\times$ is associative.

Definition The type $\chi(\theta, L)$ of a system θ of iterative pairs in L is

$$\chi(\theta, L) = \begin{cases} \chi(\pi, L) & \text{if } \theta = \pi \text{ is an iterative pair;} \\ z\chi(\theta', L)\bar{z} & \text{if } \theta = \pi * \theta' \text{ and } \chi(\pi, L) = z\bar{z}; \\ \chi(\theta_1, L)\chi(\theta_2, L) & \text{if } \theta = \theta_1 \times \theta_2. \end{cases}$$

The type is clearly a word of the restricted Dyck language D_4^* over the alphabet Ξ . Types of the same length are ordered by the following conventions:

$$e > s > r, s > l; \quad \bar{e} > \bar{s} > \bar{r}, \bar{s} > \bar{l};$$

if $h, h' \in \Xi^*$ and $|h| = |h'|$, then $h \geq h'$ iff

$$h_1 \geq h'_1, \quad h_2 \geq h'_2$$

for all factorizations $h = h_1 h_2$, $h' = h'_1 h'_2$ such that $0 < |h_1| = |h'_1| < |h|$. This definition agrees with the order on types of iterative pairs given in Section 1.

Definition A system θ of iterative pairs in L is independent if the following conditions (ii.4) and (iii.3) hold instead of (ii.3) and (iii.2) for all steps of the definition of θ :

$$(ii.4) \quad \text{Exp}(\theta, L) = \text{Exp}(\pi, L) * \text{Exp}(\theta', L);$$

$$(iii.3) \quad \text{Exp}(\theta, L) = \text{Exp}(\theta_1, L) \times \text{Exp}(\theta_2, L).$$

These conditions express the property that simultaneous iteration of some of the underlying iterative pairs of θ does not create new elements in $\text{Exp}(\theta, L)$.

Note that there may exist systems θ_1, θ_2 in L such that $\text{Exp}(\theta_1, L) = \text{Exp}(\theta_2, L)$ and $\chi(\theta_1, L) \neq \chi(\theta_2, L)$ (see Example 4.3 below). In other terms, a system of iterative pairs θ is completely specified only when the expression in its underlying iterative pairs is supplied. This expression is described by the type $\chi(\theta, L)$. Nevertheless, if θ is a system of iterative pairs in L , and if $\theta' = (a'_0, u'_1, \dots, u'_{2n}, a'_{2n})$ is a sequence of words such that $\text{Exp}(\theta, L) = \text{Exp}(\theta', L)$, then an expression in iterative pairs in L' can be given for θ' which is the same as the expression of θ in L , i.e. such that $\chi(\theta, L) = \chi(\theta', L)$.

Independent systems of iterative pairs have the useful property that their expression in iterative pairs is determined by the set of exponents. Thus the situation described above cannot occur for independent systems. More precisely we claim: If $\theta = (a_0, u_1, \dots, u_{2n}, a_{2n})$ and $\bar{\theta} = (\bar{a}_0, \bar{u}_1, \dots, \bar{u}_{2n}, \bar{a}_{2n})$ are systems of iterative pairs in L with $\text{Exp}(\theta, L) = \text{Exp}(\bar{\theta}, L)$, and if θ is independent in L , then $\chi(\theta, L) = \chi(\bar{\theta}, L)$ (then $\bar{\theta}$ is also independent). Assume indeed the contrary. Then there is an underlying pair $\bar{\pi} = \langle \bar{u}_i, \bar{u}_j \rangle$ of $\bar{\theta}$ such that $\langle u_i, u_j \rangle$ is not an underlying pair of θ . Consequently there is an integer $k \neq j$ such that either $\pi = \langle u_k, u_i \rangle$ or $\pi = \langle u_i, u_k \rangle$ is an underlying pair of θ , according to $k < i$ or $i < k$. By conditions (ii.3) and (iii.2) applied to $\bar{\theta}$, we have

$$(q, \dots, q, p, q, \dots, q, p, q, \dots, q) \in \text{Exp}(\bar{\theta}, L)$$

for all $q, p \geq 0$, where the p 's occur at the entries i, j . Since θ is independent, conditions (ii.4) and (iii.3) imply that either $(q, p) \in \text{Exp}(\pi, L)$ or $(p, q) \in \text{Exp}(\pi, L)$, according to $k < i$ or $i < k$. Thus in both cases, $\text{Exp}(\pi, L) = \mathbb{N}^2$, and θ has an underlying pair which is degenerated, contrary to the definition.

Example 4.1 Let $A = \{x^n y^n z^p t^p : n, p \geq 0\}$. Then

$$\theta = (1, x, 1, y, 1, z, 1, t, 1)$$

is a system of iterative pairs of $w = xyzt$ in A . The underlying iterative pairs are $\pi_1 = \langle x, y \rangle$ and $\pi_2 = \langle z, t \rangle$; thus $\theta = \pi_1 \times \pi_2$. Further

$$\text{Exp}(\theta, A) = \text{Diag}(\theta, A) = \Delta \times \Delta.$$

Thus θ is independent, and $\chi(\theta, A) = e\bar{e}e\bar{e}$.

Example 4.2 Let $B = \{x^n y^p z^p t^n : n, p \geq 0\}$. Then

$$\theta' = (1, x, 1, y, 1, z, 1, t, 1)$$

is a system of iterative pairs in B , whose underlying iterative pairs are $\pi_3 = \langle x, t \rangle$ and $\pi_4 = \langle y, z \rangle$. Thus $\theta' = \pi_3 * \pi_4$. Since

$$\text{Exp}(\theta', B) = \text{Diag}(\theta', B) = \Delta * \Delta,$$

θ' is independent in B , and $\chi(\theta', B) = e\bar{e}e\bar{e}$. The types $\chi(\theta, A)$ and $\chi(\theta', B)$ are incomparable.

Example 4.3 Let $C = A \cup B$, with A, B as above. Then the word $xyzt$ admits the two systems $\theta = \pi_1 \times \pi_2$ and $\theta' = \pi_3 * \pi_4$ in C . But now

$$\text{Exp}(\theta, C) = \text{Exp}(\theta', C) = \Delta \times \Delta \cup \Delta * \Delta.$$

Hence neither θ nor θ' is independent in C .

Example 4.4 Let $L = \{xyz^p t^p \mid p \geq 0\} \cup \{x^n y^n zt \mid n \geq 0\}$. The word $w = xyzt$ admits in L the two very strict iterative pairs

$$\pi_1 = (xy, z, 1, t, 1) \quad \text{and} \quad \pi_2 = (1, x, 1, y, zt).$$

But $\theta = \pi_1 \times \pi_2 = (1, x, 1, y, 1, z, 1, t, 1)$

is not a system of iterative pairs in L , since

$$\text{Exp}(\theta, L) = \Delta \times \{(1, 1)\} \cup \{(1, 1)\} \times \Delta \not\supset \text{Diag}(\theta, L) = \Delta \times \Delta.$$

Example 4.5 Let $L = \{x^k y^p \bar{y}^q z^n \bar{z}^m \bar{x}^k \mid 0 \leq k, 0 \leq p \leq q, 0 \leq m \leq n\}$ be the language of Example 1.4. Then

$$\theta = (1, x, 1, y, 1, \bar{y}, 1, z, 1, \bar{z}, 1, \bar{x}, 1) = \pi_1 * (\pi_2 \times \pi_3)$$

with $\pi_1 = \langle x, \bar{x} \rangle$, $\pi_2 = \langle y, \bar{y} \rangle$, $\pi_3 = \langle z, \bar{z} \rangle$ is a system of iterative pairs in L . $\text{Diag}(\theta, L) = \{k, p, p, n, n, k\} \in \mathbb{N}^6 \mid k, p, n \geq 0\}$; further θ is easily seen to be independent in L . Finally

$$\chi(\theta, L) = e\bar{e}\bar{l}r\bar{r}\bar{e}.$$

Example 4.6 Let S_2 be the symmetric language over $Z = X \cup \bar{X}$, with $X = \{x, y\}$, $\bar{X} = \{\bar{x}, \bar{y}\}$ defined by

$$S_2 = xS_2\bar{x} \cup yS_2\bar{y} \cup 1.$$

We claim that any system of iterative pairs θ in S_2 is of the form

$$\theta = \pi_1 * \pi_2 * \cdots * \pi_n, \quad (4.4)$$

where $\pi_1, \dots, \pi_n$ are iterative pairs. Indeed θ cannot be of the form $\theta = \theta_1 \times \theta_2$, since otherwise at least one of the underlying iterative pairs of θ would have its iterating elements both in X^* or in $\bar{X}^*$, contrary to Example 1.7. Next all iterative pairs in (4.4) are very strict, thus θ has type $e^n \bar{e}^n$. θ may be dependent, but there exist independent systems of type $e^n \bar{e}^n$ in S_2 for any $n \geq 1$. Thus the systems

$$\theta = \langle xy, xy^2, \dots, xy^n, \bar{y}^n \bar{x}, \dots, \bar{y}^2 \bar{x}, \bar{y} \bar{x} \rangle$$

$$\text{or } \theta = \langle x, y, x, y, \dots, x, y, \bar{y}, \bar{x}, \dots, \bar{y}, \bar{x}, \bar{y}, \bar{x} \rangle$$

are independent.

Example 4.7 Let D_1^* be the restricted Dyck language over $X = \{x, \bar{x}\}$. We claim that any independent system of iterative pairs in D_1^* is of length 1, i.e. is a (nondegenerated) iterative pair in D_1^* . Consider indeed a system of iterative pairs of length 2 in D_1^* :

$$\theta = (a_0, u_1, a_1, u_2, a_2, u_3, a_3, u_4, a_4).$$

Two possibilities arise:

(i) $\theta = \pi_1 \times \pi_2$, with $\pi_1 = \langle u_1, u_2 \rangle$, $\pi_2 = \langle u_3, u_4 \rangle$.

By Example 1.8, these pairs are very strict. Set $k = \|u_1\| = -\|u_2\|$, $l = \|u_3\| = -\|u_4\|$. Then $k, l > 0$. Next

$$f = a_0 u_1^{1+l} a_1 u_2 a_2 u_3 a_3 u_4^{1+k} a_4 \in D_1^*.$$

Indeed $\|f\| = l \|u_1\| + k \|u_4\| = 0$. Further if f' is a left factor of $a_0 u_1^{1+l} a_1 u_2 a_2 u_3 a_3$, then $\|f'\| > 0$. Finally, if $f' = a_0 u_1^{1+l} a_1 u_2 a_2 u_3 a_3 u_4^m u'$ with $0 \leq m \leq k$ and u' a left factor of u_4 , then $\|f'\| = l \|u_1\| + m \|u_4\| + \|a_0 u_1 a_1 u_2 a_2 u_3 a_3 u'\| \geq l \|u_1\| + m \|u_4\| \geq 0$. Consequently

$$(1+l, 1, 1, 1+k) \in \text{Exp}(\theta, D_1^*)$$

and $\text{Exp}(\theta, D_1^*) \not\supseteq \Delta \times \Delta$.

(ii) $\theta = \pi_1 * \pi_2$, with $\pi_1 = \langle u_1, u_4 \rangle$, $\pi_2 = \langle u_2, u_3 \rangle$.

Setting $k = \|u_1\| = -\|u_4\|$, $l = \|u_2\| = -\|u_3\|$, an identical argument shows that $f = a_0 u_1^{1+l} a_1 u_2 a_2 u_3^{1+k} a_3 u_4 a_4$ is in D_1^* , which proves that $\Delta * \Delta$ is strictly contained in $\text{Exp}(\theta, D_1^*)$.

Note that there exist in D_1^* systems of iterative pairs of any length and of any type (in $\{e, \bar{e}\}^*$) (Exercise 4.1). The above proof shows that these systems are not independent.

We conclude this section by the analog of Lemmas 1.1 and 1.2.

Lemma 4.1 Let θ be system of iterative pairs in $L \cap K$ where L is a language and K is a local regular language. Then θ is a system of iterative pairs of the same type in L , and $\text{Exp}(\theta, L) = \text{Exp}(\theta, L \cap K)$.

Proof. Let $\theta = (a_0, u_1, \dots, u_{2n}, a_{2n})$. By conditions (ii.3) and (iii.2) of the definition, $a_0 u_1^k \cdots u_{2n}^k a_{2n} \in K$ for $k \geq 0$. Since K is local, $a_0 u_1^* \cdots u_{2n}^* a_{2n} \subset K$. Thus

$$\text{Exp}(\theta, L) = \text{Exp}(\theta, L \cap a_0 u_1^* \cdots u_{2n}^* a_{2n}) \subset \text{Exp}(\theta, L \cap K).$$

The converse inclusion is obvious. ■

Let $\varphi: X^* \rightarrow Y^*$ be a morphism, and let

$$\theta = (a_0, u_1, \dots, u_{2n}, a_{2n}) \quad (4.5)$$

be a sequence of words of X^* . Define

$$\varphi(\theta) = (\varphi a_0, \varphi u_1, \dots, \varphi u_{2n}, \varphi a_{2n}).$$

Lemma 4.2 Let $M \subset Y^*$, $L = \varphi^{-1}(M)$. If θ is a system of iterative pairs in L , then $\varphi(\theta)$ is a system of the same type in M and $\text{Exp}(\theta, L) = \text{Exp}(\varphi(\theta), M)$.

Proof. It suffices to prove the last equality. Let θ be given by (4.5). Clearly $\text{Exp}(\theta, L) \subset \text{Exp}(\varphi(\theta), M)$. Next if $\varphi(a_0 u_1^k \cdots u_{2n}^k a_{2n}) \in M$, then $a_0 u_1^k \cdots u_{2n}^k a_{2n} \in \varphi^{-1}(M) = L$. Thus $\text{Exp}(\varphi(\theta), M) \subset \text{Exp}(\theta, L)$. ■

Exercises

4.1 Show that in D_1^* there exist systems of iterative pairs of any length and of any type contained in $\{e, \bar{e}\}^*$.

4.2 (Beauquier [1977]) Show that the underlying iterative pairs of any system in D_n^* ($n \geq 1$) are all very strict. Show that in D_n^* ($n \geq 2$) there exist independent systems of iterative pairs of any length and of any type contained in $\{e, \bar{e}\}^*$.

VIII.5 Grammatical Systems

This section contains the extension of the notion of grammatical pairs to systems of iterative pairs. Such a system is formed of grammatical iterative pairs with the additional requirement that the pivots of the iterative pairs are simultaneously derivable from the nonterminal generating the language.

Definition Let $L \subset X^*$ be an algebraic language, and let $G = \langle V, X, P \rangle$ be an algebraic grammar such that $L = L_G(\sigma)$ for $\sigma \in V$. Let

$$\theta = (a_0, u_1, \dots, u_{2n}, a_{2n})$$

be a system of iterative pairs in L . Then θ is grammatical with respect to G and has pivot $w \in (V \cup X)^*$ if

- (i) $n = 1$, and θ is a grammatical iterative pair with pivot w ,
- (ii) $\theta = \pi * \theta'$, where π is a grammatical pair with pivot w , θ' is a grammatical system with pivot w' , and

$$w \xrightarrow{*G} a_1 w' a_{2n-1};$$

- (iii) $\theta = \theta_1 \times \theta_2$, where θ_1 is a grammatical system of length k and pivot w_1 , θ_2 is a grammatical system with pivot w_2 , and

$$w = w_1 a_{2k} w_2 \quad \text{and} \quad \sigma \xrightarrow{*G} a_0 w a_{2n}.$$

It is easily seen by induction that the pivot w is a word of $V(X^*V)^*$.

Example 5.1 Let

$$\theta = (a_0, u_1, \dots, u_{2n}, a_{2n}) = \pi_1 * \pi_2 * \dots * \pi_n,$$

and assume θ is grammatical with respect to G . Then there are variables $\xi_1, \xi_2, \dots, \xi_n \in V$ such that

$$\sigma \xrightarrow{*} a_0 \xi_1 a_{2n}; \quad \xi_1 \xrightarrow{*} u_1 \xi_1 u_{2n};$$

$$\xi_1 \xrightarrow{*} a_1 \xi_2 a_{2n-1}; \quad \xi_2 \xrightarrow{*} u_2 \xi_2 u_{2n-1};$$

$$\vdots \quad \vdots$$

$$\xi_{n-1} \xrightarrow{*} a_{n-1} \xi_n a_{n+1}; \quad \xi_n \xrightarrow{*} u_n \xi_n u_{n+1}; \quad \xi_n \xrightarrow{*} a_n.$$

The pivot of θ is ξ_1 .

Example 5.2 Assume that θ is of the form

$$\theta = \pi_1 \times \pi_2 \times \dots \times \pi_n.$$

If θ is grammatical with respect to G , then there are variables $\xi_1, \dots, \xi_n \in V$ such that

$$\sigma \xrightarrow{*} a_0 \xi_1 a_2 \xi_2 a_4 \dots a_{2n-2} \xi_n a_{2n};$$

$$\xi_i \xrightarrow{*} u_{2i-1} \xi_i u_{2i}; \quad \xi_i \xrightarrow{*} a_{2i-1} \quad (i = 1, \dots, n).$$

The pivot of θ is $\xi_1 a_2 \xi_2 a_4 \dots \xi_n$.

Example 5.3 Let $D_1^* \subset \{x, \bar{x}\}^*$. Then

$$\theta = (1, x, 1, \bar{x}, 1, x, 1, \bar{x}, 1) = \pi_1 \times \pi_2,$$

with $\pi_1 = (1, x, 1, \bar{x}, x\bar{x})$, $\pi_2 = (x\bar{x}, x, 1, \bar{x}, 1)$ is a (dependent) system of iterative pairs in D_1^* . θ is grammatical with respect to the grammar with rules $\xi \rightarrow \xi\xi + x\xi\bar{x} + 1$. Indeed ξ is pivot of both π_1 and π_2 , and $\xi\xi$ is the pivot of θ .

We now prove the analogues of Lemmas 2.1–2.3.

Lemma 5.1 Let $L \subset X^*$ be generated by an algebraic grammar G , and let $K \subset X^*$ be a rational language. If θ is a system of iterative pairs in $L \cap K$ grammatical with respect to G_K , then θ is grammatical with respect to G .

Proof. By induction on the length n of $\theta = (a_0, u_1, \dots, u_{2n}, a_{2n})$. For $n = 1$, the result is Lemma 2.1. We assume that G and G_K are as in Section II.2. Assume $\theta = \pi * \theta'$. Then in G_K :

$$\hat{\sigma} \rightarrow (q_-, \sigma, q_+) \xrightarrow{*} a_0(q, \xi, q') a_{2n};$$

$$(q, \xi, q') \xrightarrow{*} u_1(q, \xi, q') u_{2n}; \quad (q, \xi, q') \xrightarrow{*} a_1 w' a_{2n-1},$$

where w' is the pivot of θ' in G_K . Now w' is of the form $w' = (q_1, \xi_1, q'_1) v_1 \dots v_{r-1} (q_r, \xi_r, q'_r)$ with $v_1, \dots, v_{r-1} \in X^*$. Assuming by induction that $w'' = \xi_1 v_1 \dots v_{r-1} \xi_r$ is the pivot of θ' in G , we have, in G ,

$$\sigma \xrightarrow{*} a_0 \xi a_{2n}, \quad \xi \xrightarrow{*} u_1 \xi u_{2n}, \quad \xi \xrightarrow{*} a_1 w'' a_{2n-1}.$$

Thus θ is grammatical in G with pivot ξ . The case $\theta = \theta_1 \times \theta_2$ is proved in the same way. $\blacksquare$

Lemma 5.2 Let $\varphi: X^* \rightarrow Y^*$ be an alphabetic morphism, let $M \subset Y^*$ be generated by an algebraic grammar G , and set $L = \varphi^{-1}(M)$. If θ is a system of iterative pairs in L grammatical with respect to $\varphi^{-1}(G)$, then $\varphi(\theta)$ is grammatical with respect to G .

Proof. By induction on the length n of $\theta = (a_0, u_1, \dots, u_{2n}, a_{2n})$. For $n = 1$, the result is Lemma 2.2. Let G and $\varphi^{-1}(G)$ be as in Section II.2, and suppose first $\theta = \theta_1 \times \theta_2$. Let k be the length of θ_1 , and let w, w_1, w_2 be the pivots of $\theta, \theta_1, \theta_2$ in $\varphi^{-1}(G)$ respectively. Suppose by induction that no variable in w_1 and w_2 is equal to the variable ω of $\varphi^{-1}(G)$. Then the same is true for $w = w_1 a_{2k} w_2$. Suppose next by induction that $\varphi(w_1)$ and $\varphi(w_2)$ are the pivots in G of $\varphi(\theta_1)$ and $\varphi(\theta_2)$. Then in G

$$\sigma \xrightarrow{*} \varphi(a_0) \varphi(w) \varphi(a_{2n})$$

and $\varphi(w)$ is the pivot of $\varphi(\theta)$ in G . Thus the lemma is proved in this case.

Suppose next $\theta = \pi * \theta'$. Then in $\varphi^{-1}G$:

$$\sigma \xrightarrow{*} a_0 \eta a_{2n}; \quad \eta \xrightarrow{*} u_1 \eta u_{2n}; \quad \eta \xrightarrow{*} a_1 w' a_{2n-1},$$

where w' is the pivot in $\varphi^{-1}G$ of θ' . Since π is nondegenerated, η is not the variable ω . Assuming by induction that $\varphi w'$ is the pivot of $\varphi(\theta')$ in G , it follows that

$$\sigma \xrightarrow{*} \varphi(a_0) \eta \varphi(a_{2n}); \quad \eta \xrightarrow{*} \varphi(u_1) \eta \varphi(u_{2n}); \quad \eta \xrightarrow{*} \varphi(a_1) \varphi(w') \varphi(a_{2n-1})$$

in G , thus $\varphi\eta = \eta$ is the pivot of $\varphi(\theta)$ in G . ■

Lemma 5.3 Let $\psi: X^* \rightarrow Y^*$ be a morphism, let $L \subset X^*$ be generated by an algebraic grammar G , and let $M = \psi(L)$. If θ is a system of iterative pairs in M grammatical with respect to ψG , then there exists a system of iterative pairs $\hat{\theta}$ in L , grammatical with respect to G , such that $\psi(\hat{\theta}) = \theta$. Further $\text{Exp}(\hat{\theta}, L) \subset \text{Exp}(\theta, M)$ and $\chi(\hat{\theta}, L) \geq \chi(\theta, M)$.

Proof. The inclusion $\text{Exp}(\hat{\theta}, L) \subset \text{Exp}(\theta, M)$ is immediate. The inequality $\chi(\hat{\theta}, L) \geq \chi(\theta, M)$ is a consequence of the fact that for any iterative pair $\hat{\pi}$ underlying to $\hat{\theta}$, $\pi = \psi(\hat{\pi})$ is underlying to θ and therefore $\chi(\hat{\pi}, L) \geq \chi(\pi, M)$ in view of Lemma 2.3. For simplicity, set $m = 2n$. Assume first $\theta = \pi * \theta'$, and let ξ and w' be the pivots of π and θ' in ψG . Then in ψG :

$$\sigma \xrightarrow{*} a_0 \xi a_m, \quad \xi \xrightarrow{*} u_1 \xi u_m, \quad \xi \xrightarrow{*} a_1 w' a_{m-1}.$$

Thus there exist $\hat{a}_0, \hat{a}_m, \hat{u}_1, \hat{u}_m, \hat{a}_1, \hat{a}_{m-1}, \hat{w}'$ with $\psi \hat{a}_0 = a_0, \psi \hat{a}_m = a_m, \psi \hat{u}_1 = u_1, \psi \hat{u}_m = u_m, \psi \hat{a}_1 = a_1, \psi \hat{a}_{m-1} = a_{m-1}, \psi \hat{w}' = w'$ such that in G :

$$\sigma \xrightarrow{*} \hat{a}_0 \xi \hat{a}_m; \quad \xi \xrightarrow{*} \hat{u}_1 \xi \hat{u}_m; \quad \xi \xrightarrow{*} \hat{a}_1 \hat{w}' \hat{a}_{m-1}.$$

Next by induction there exists a grammatical system $\bar{\theta}'$ in G with $\psi \bar{\theta}' = \theta'$ and with pivot $\bar{w}'$ verifying $\psi(\bar{w}') = w'$. w' has the form

$$w' = \xi_1 b_1 \cdots b_{r-1} \xi_r,$$

where $\xi_1, \dots, \xi_r$ are variables and $b_1, \dots, b_{r-1}$ are among the a_i 's. Consequently

$$\bar{w}' = \xi_1 \bar{b}_1 \cdots \bar{b}_{r-1} \xi_r, \quad \bar{w}' = \xi_1 \hat{b}_1 \cdots \hat{b}_{r-1} \xi_r,$$

with $\psi \bar{b}_i = \psi \hat{b}_i = b_i$ for $i = 1, \dots, r-1$. Since $\bar{w}'$ is the pivot of $\bar{\theta}'$, it follows that $\hat{w}'$ is the pivot of the system $\hat{\theta}'$ obtained by replacing $\bar{b}_i$ by $\hat{b}_i$ in $\bar{\theta}'$. This proves the lemma when $\theta = \pi * \theta'$. The case where $\theta = \theta_1 \times \theta_2$ is similar. ■

Note that if θ is independent, it does not follow that $\hat{\theta}$ is independent (see Example 6.4).

The main result of this section is the generalization of Theorem 2.5 to systems of iterative pairs. We therefore define:

Definition Let

$$\theta = (a_0, u_1, a_1, \dots, u_m, a_m) \quad \text{and} \quad \bar{\theta} = (\bar{a}_0, \bar{u}_1, \bar{a}_1, \dots, \bar{u}_m, \bar{a}_m) \quad (5.1)$$

be sequences of words. Then $\bar{\theta}$ is deduced from θ if

(i) there is an integer $N \geq 1$ such that

$$\bar{a}_0 \bar{u}_1 \bar{a}_1 \bar{u}_2 \cdots \bar{u}_m \bar{a}_m = a_0 u_1^N a_1 u_2^N \cdots u_m^N a_m;$$

(ii) there exist factorizations

$$u_1 = u'_1 u''_1, \dots, u_m = u'_m u''_m,$$

words $c_1, \dots, c_m, d_1, \dots, d_m$ and integers $p_1, \dots, p_m$, ($1 \leq p_i \leq N$) with

$$u_i^N = c_i \bar{u}_i d_i; \quad \bar{u}_i = (u'_i u''_i)^{p_i}; \quad i = 1, \dots, m \quad (5.2)$$

$$\bar{a}_0 = a_0 c_1; \quad \bar{a}_i = d_i a_i c_{i+1} \quad (1 \leq i < m); \quad \bar{a}_m = d_m a_m. \quad (5.3)$$

Example 5.4 Let $\theta = (a_0, u_1, a_1, u_2, a_2, u_3, a_3, u_4, a_4) = \pi_1 \times \pi_2$ be a system of iterative pairs in some language L , with $\pi_1 = \langle u_1, u_2 \rangle$, $\pi_2 = \langle u_3, u_4 \rangle$. Then $\bar{\theta} = (a_0, u_1^2, a_1, u_2^2, a_2, u_3^2, a_3, u_4^2, a_4)$ is deduced from θ . Set

$$\bar{\pi}_1 = (a_0, u_1^2, a_1, u_2^2, a_2 u_3^2 a_3 u_4^2 a_4),$$

$$\bar{\pi}_2 = (a_0 u_1^2 a_1 u_2^2 a_2, u_3^2, a_3, u_4^2, a_4).$$

Then $\bar{\pi}_1$ and $\bar{\pi}_2$ are iterative pairs in L , but note that they are not deduced from π_1 and π_2 . Next if both $\bar{\pi}_1$ and $\bar{\pi}_2$ are nondegenerated (this is not necessarily true, see the following example), then $\bar{\theta} = \bar{\pi}_1 \times \bar{\pi}_2$.

Example 5.5 Let $L = \{x^n y^n z^p t^p \mid n, p \geq 0\} \cup x^* y^* z^2 t^2$. Then

$$\theta = (1, x, 1, y, 1, z, 1, t, 1) = \pi_1 \times \pi_2$$

is a system of iterative pairs, and $\pi_1 = \langle x, y \rangle$, $\pi_2 = \langle z, t \rangle$ are very strict iterative pairs. Next

$$\bar{\theta} = (1, x^2, 1, y^2, 1, z^2, 1, t^2, 1)$$

is deduced from θ , but $\bar{\pi} = (1, x^2, 1, y^2, z^2 t^2)$ is a degenerated iterative pair in L .

Since we will deal now with several systems of iterative pairs simultaneously, we precise the notation (4.3) and write

$$\theta' = \langle u_i, \dots, u_i \rangle_\theta$$

if θ' is a subsequence of a sequence θ .

Proposition 5.4 Let θ be a system of iterative pairs in L and let $\bar{\theta}$ be deduced from θ . If θ is independent, then $\bar{\theta}$ is an independent system of iterative pairs in L , and $\chi(\bar{\theta}, L) \geq \chi(\theta, L)$.

Proof. Let n be the length of θ , and let $\theta, \bar{\theta}$ be as in (5.1) with $m = 2n$. First note that

$$(k_1, \dots, k_m) \in \text{Exp}(\bar{\theta}, L) \Leftrightarrow (N + p_1(k_1 - 1), \dots, N + p_m(k_m - 1)) \in \text{Exp}(\theta, L). \quad (5.4)$$

Then the proposition is true for $n = 1$. Arguing by induction, assume $\theta = \pi * \theta'$ and define

$$\bar{\pi} = \langle \bar{u}_1, \bar{u}_m \rangle_{\bar{\theta}}, \quad \bar{\theta}' = \langle \bar{u}_2, \dots, \bar{u}_{m-1} \rangle_{\bar{\theta}}.$$

Note that $\bar{\pi}$ and $\bar{\theta}'$ are not deduced from π and θ . But from the independence of θ , it follows that

$$\begin{aligned} (k_1, k_m) \in \text{Exp}(\bar{\pi}, L) &\Leftrightarrow (N + p_1(k_1 - 1), N + p_m(k_m - 1)) \in \text{Exp}(\pi, L) \\ (k_2, \dots, k_{m-1}) \in \text{Exp}(\bar{\theta}', L) &\Leftrightarrow (N + p_2(k_2 - 1), \dots, N + p_{m-1}(k_{m-1} - 1)) \in \text{Exp}(\theta', L). \end{aligned}$$

Thus, by (5.4),

$$\text{Exp}(\bar{\theta}, L) = \text{Exp}(\bar{\pi}, L) * \text{Exp}(\bar{\theta}', L). \quad (5.5)$$

Consider next

$$\begin{aligned} \pi_1 &= (a_0 c_1, \bar{u}_1, d_1 a_1 u_2 \cdots u_{m-1} a_{m-1} c_m, \bar{u}_m, d_m a_m) \\ \theta_1 &= (a_0 u_1 c_2, \bar{u}_2, \bar{a}_2, \dots, \bar{u}_{m-1}, d_{m-1} u_m a_m). \end{aligned}$$

Then π_1 and θ_1 are deduced from π and θ' . By induction θ_1 is an independent system in L and by Lemma 2.4 and by induction, $\chi(\pi_1, L) \geq \chi(\pi, L)$ and $\chi(\theta_1, L) \geq \chi(\theta', L)$. The independence of θ implies that

$$\text{Exp}(\pi_1, L) = \text{Exp}(\bar{\pi}, L), \quad \text{Exp}(\theta_1, L) = \text{Exp}(\bar{\theta}', L).$$

Thus $\bar{\theta}$ is an independent system by (5.5) and $\chi(\bar{\theta}, L) \geq \chi(\theta, L)$. The proof is quite similar in the case where $\theta = \theta_1 \times \theta_2$. ■

Note that (5.4) is a precise description of $\text{Exp}(\bar{\theta}, L)$ in terms of $\text{Exp}(\theta, L)$. We give a more compact formulation of (5.4) by introducing first two vectors of $\mathbb{N}^m$

$$\vec{p} = (p_1, \dots, p_m), \quad \vec{q} = (N - p_1, \dots, N - p_m).$$

Then we agree to define the product of two vectors $\vec{a} = (a_1, \dots, a_m)$ and $\vec{b} = (b_1, \dots, b_m)$ of $\mathbb{N}^m$ by

$$\vec{a}\vec{b} = (a_1 b_1, \dots, a_m b_m).$$

Then (5.4) is equivalent to

$$\vec{q} + \vec{p} \text{Exp}(\bar{\theta}, L) = \text{Exp}(\theta, L) \cap (\vec{q} + \vec{p}\mathbb{N}^{2n}). \quad (5.6)$$

We are now ready for the analogue of Theorem 2.5.

Theorem 5.5 Let $L \subset X^*$ be an algebraic language, and let θ be an independent system of iterative pairs in L . For any algebraic grammar G generating L , there exists a system $\bar{\theta}$ deduced from θ which is grammatical with respect to G .

Proof. As for Theorem 2.5, the proof is in two parts. We first prove the theorem in a special case, and then reduce the general case to this special case. Let

$$\theta = (a_0, u_1, \dots, u_{2n}, a_{2n})$$

and set $m = 2n$. In the first part, we assume that X is the disjoint union of an alphabet Z and of letters $t, x_1, \dots, x_m$ such that

$$\begin{aligned} a_0 &\in Z^* t, & a_i &\in tZ^* t \quad (i = 1, \dots, m-1), & a_m &\in tZ^*, \\ u_i &\in x_i Z^* \quad (i = 1, \dots, m). \end{aligned}$$

Let $\pi_1, \dots, \pi_n$ be the iterative pairs underlying to θ . For each π_i , there are integers l_i, r_i with $1 \leq l_i < r_i \leq m$ such that $\pi_i = \langle u_{l_i}, u_{r_i} \rangle$. Renumber the π_i 's in such a way that $l_1 < l_2 < \dots < l_n$. Then there is a sequence $\theta_n, \dots, \theta_1$ of independent systems of iterative pairs such that

$$\theta_n = \pi_n, \quad \theta_1 = \theta$$

and for $i = 1, \dots, n-1$, one of the three following possibilities hold:

$$\begin{aligned} \theta_i &= \pi_i * \theta_{i+1}; & \theta_i &= \pi_i \times \theta_{i+1}; \\ \theta_i &= (\pi_i * \theta^{(1)}) \times \theta^{(2)}, & \theta_{i+1} &= \theta^{(1)} \times \theta^{(2)} \end{aligned}$$

where $\theta^{(1)}$ and $\theta^{(2)}$ are systems of iterative pairs. (Note that the two first cases could be considered as a special case of the third one, arising when one of the two systems $\theta^{(1)}$ or $\theta^{(2)}$ is the "empty system" of length 0.)

Let $K = a_0 u_1^* a_1 u_2^* \cdots u_m^* a_m$ and let $H = G_K = \langle V, X, P \rangle$ be the grammar generating $L \cap K$ obtained from G . Let $\sigma \in V$ be such that $L \cap K = L_H(\sigma)$. In view of Lemma 5.1, it suffices to prove the result for the grammar H . Let N be the integer associated to H by Ogden's Iteration Lemma II.2.5, and define

$$g = a_0 v_1 a_1 v_2 \cdots v_m a_m \quad \text{with } v_i = u_i^N \quad (1 \leq i \leq m).$$

We proceed by induction on $i = n, n-1, \dots, 1$. Consider first $i = n$. Then $\pi_n = \langle u_k, u_{k+1} \rangle$ for some k . By the proof of Theorem 2.5, there exists a variable

ξ_n such that

$$\sigma \xrightarrow{*} g_n = a_0 v_1 \cdots a_{k-1} c_k \xi_n d_{k+1} v_{k+2} \cdots v_m,$$

$$\xi_n \xrightarrow{*} \bar{u}_k \xi_n \bar{u}_{k+1}, \quad \xi_n \xrightarrow{*} d_k a_k c_{k+1},$$

where $c_k, d_k, c_{k+1}, d_{k+1}, \bar{u}_k, \bar{u}_{k+1}$ are as in (5.2), (5.3). Thus the word g admits a grammatical pair θ_n with pivot ξ_n . Suppose now $n > i$, and assume

$$\theta_i = (\pi_i * \theta^{(1)}) \times \theta^{(2)}, \quad \theta_{i+1} = \theta^{(1)} \times \theta^{(2)}.$$

(The two other cases are only simplified versions of the present one.) Let $\pi_i = \langle u_i, u_r \rangle$. The order on the π_i 's implies that

$$\theta^{(1)} = \langle u_{i+1}, \dots, u_{r-1} \rangle, \quad \theta^{(2)} = \langle u_{q_1}, \dots, u_{q_h} \rangle$$

for some $r < q_1 < q_2 < \dots < q_h$. We now make the following induction hypotheses:

a) There exists a grammatical system of iterative pairs $\bar{\theta}_{i+1} = \bar{\theta}^{(1)} \times \bar{\theta}^{(2)}$ where

$$\bar{\theta}^{(1)} = (a_0 v_1 \cdots v_l a_l c_{l+1}, \bar{u}_{l+1}, \bar{a}_{l+1}, \dots, \bar{u}_{r-1}, d_{r-1} a_{r-1} v_r \cdots v_m a_m)$$

$$\bar{\theta}^{(2)} = (a_0 v_1 \cdots a_{q_1} c_{q_1}, \bar{u}_{q_1}, d_{q_1}, \dots, c_{q_2}, \bar{u}_{q_2}, \dots, \bar{u}_{q_h}, d_{q_h} a_{q_h} \cdots v_m a_m)$$

such that if $w^{(1)}$ and $w^{(2)}$ are the pivots of $\theta^{(1)}$ and $\theta^{(2)}$, then

$$\sigma \xrightarrow{*} g_{i+1} = a_0 v_1 \cdots v_l a_l c_{l+1} w^{(1)} d_{r-1} a_{r-1} v_r \cdots c_{q_1} w^{(2)} d_{q_h} a_{q_h} \cdots v_m a_m.$$

This implies the existence of derivations

$$\begin{aligned} c_{l+1} w^{(1)} d_{r-1} &\xrightarrow{*} v_{l+1} a_{l+1} \cdots v_{r-1}; \\ c_{q_1} w^{(2)} d_{q_h} &\xrightarrow{*} v_{q_1} a_{q_1} v_{q_1+1} \cdots a_{q_h-1} v_{q_h}. \end{aligned} \quad (5.7)$$

b) Any variable occurring in $w^{(1)}$ and $w^{(2)}$ derives in a word having at least one a_i as factor.

These induction hypotheses are clearly satisfied by $\bar{\theta}_n$. Next we proceed as in the proof of Theorem 2.5 and distinguish two cases according to whether π_i is left strict or right strict. Suppose that π_i is right strict and mark the positions of the letter x_r in the word g_{i+1} (and not in g !). Then g_{i+1} admits a grammatical iterative pair

$$\bar{\pi}_i = (\bar{a}, \bar{u}, \bar{b}, \bar{v}, \bar{c}).$$

Consequently $g_{i+1} = \bar{a} \bar{u} \bar{b} \bar{v} \bar{c}$ and there are, in H , the derivations

$$\sigma \xrightarrow{*} \bar{a} \bar{\xi}_i \bar{c}, \quad \bar{\xi}_i \xrightarrow{*} \bar{u} \bar{\xi}_i \bar{v}, \quad \bar{\xi}_i \xrightarrow{*} \bar{b},$$

whence

$$\sigma \xrightarrow{*} \bar{a} \bar{\xi}_i \bar{c} \rightarrow \bar{a} \bar{u}^k \bar{b} \bar{v}^k \bar{c} \quad (k \geq 0). \quad (5.8)$$

Further $\bar{u}$ or $\bar{v}$ contains occurrences of the letter x_r . First we note that neither $\bar{u}$ nor $\bar{v}$ contains the letter t since otherwise, by (5.8), the number of letters t in the words of $L \cap K$ would not be bounded. Next in view of hypothesis b), neither $\bar{u}$ nor $\bar{v}$ contains an occurrence of a variable. By the form of K , neither $\bar{u}$ nor $\bar{v}$, if they are nonempty, occur as factors in one of the a_i 's. Thus $\bar{u}$ and $\bar{v}$ are factors either of some v_j 's or of $c_{l+1}, d_{r-1}, c_{q_1}, d_{q_h}$. Assume now that $\bar{u}$ contains an occurrence of the letter x_r . Then $\bar{u}$ is a factor of v_r , and $\bar{v}$ is a factor of v_r , or of some $v_j (j > r)$ or of c_{q_1} or d_{q_h} . If $\bar{v}$ is not a factor of v_r , there is some factorization

$$v_r = c' \bar{u} d',$$

and in view of (5.7)

$$\bar{a} \bar{u}^k \bar{b} \bar{v}^k \bar{c} \xrightarrow{*} a_0 v_1 a_1 v_2 \cdots a_{r-1} c' \bar{u}^k d' a_r f^{(k)} \in L \cap K$$

where $f^{(k)}$ is some word in $u_{r+1}^* a_{r+1} \cdots u_m^* a_m$, ($k \geq 0$). Thus $\bar{u}$ is of the form $\bar{u} = (u'' u')^p$ for some factorization $u_r = u' u''$, and the independence of θ implies that

$$(N, N + p(k-1)) \in \text{Exp}(\pi_i, L \cap K) \quad \text{for } k \geq 0.$$

This is impossible since π_i is right strict. Similarly if $\bar{v}$ is also a factor of v_r , then there is a factorization

$$v_r = c'' \bar{u} \bar{e} \bar{v} d''$$

and $\bar{a} \bar{u}^k \bar{b} \bar{v}^k \bar{c} \xrightarrow{*} a_0 v_1 \cdots a_{r-1} c'' \bar{u}^k \bar{e} \bar{v}^k d'' a_r v_{r+1} \cdots v_m a_m \in L \cap K$

and the independence of θ leads to a contradiction. Thus $\bar{u}$ contains no occurrence of the letter x_r , therefore $\bar{v}$ is a factor of v_r , and by the same argument as above one proves that $\bar{u}$ is a nonempty factor of v_l . This gives factorizations

$$v_l = u_l^N = c_l \bar{u} d_l, \quad v_r = u_r^N = c_r \bar{v} d_r, \quad u_l = u_l' u_l'', \quad u_r = u_r' u_r'',$$

such that $\bar{u} = (u_l' u_l'')^{p_l}$, $\bar{v} = (u_r' u_r'')^{p_r}$ for some $p_l, p_r \geq 1$.

The same conclusion holds if π_i is left strict by marking the positions of x_l instead of x_r .

Thus there are derivations

$$\sigma \xrightarrow{*} g_i = a_0 v_1 \cdots a_{l-1} c_l \bar{\xi}_i d_l a_r \cdots c_{q_1} w^{(2)} d_{q_h} \cdots v_m a_m,$$

$$\bar{\xi}_i \xrightarrow{*} \bar{u} \bar{\xi}_i \bar{v}, \quad \bar{\xi}_i \xrightarrow{*} d_l a_l c_{l+1} w^{(1)} d_{r-1} a_{r-1} c_r.$$

This shows that the induction hypotheses a) and b) are satisfied by the system of iterative pairs

$$\bar{\theta}_i = (a_0 \cdots a_{l-1} c_l, \bar{u}_l, \bar{a}_l, \dots, \bar{u}_r, d_r a_r \cdots v_m a_m) \times \bar{\theta}^{(2)}.$$

Thus the proof is complete in the case where θ has the special form described at the beginning.

Finally, and as in the proof of Theorem 2.5, consider the general case of an independent system of iterative pairs

$$\theta = (a_0, u_1, \dots, u_{2n}, a_{2n}).$$

Let $t, x_1, \dots, x_m$ ($m=2n$) be new letters, set $Y = X \cup \{t, x_1, \dots, x_m\}$ and let $\varphi: Y^* \rightarrow X^*$ be the projection. Set $M = \varphi^{-1}(L)$ and

$$K = a_0 t (x_1 u_1)^* t a_1 t (x_2 u_2)^* \dots (x_m u_m)^* t a_m,$$

$$\theta' = (a_0 t, x_1 u_1, t a_1 t, \dots, t a_m).$$

Then $\varphi(\theta') = \theta$ and $\text{Exp}(\theta', M) = \text{Exp}(\theta, L)$. By the first part of the proof, there is a system of iterative pairs $\hat{\theta}$ deduced from θ which is grammatical with respect to the grammar $\varphi^{-1}(G)$. Then $\bar{\theta} = \varphi(\hat{\theta})$ is deduced from $\theta = \varphi(\theta')$ and $\bar{\theta}$ is grammatical with respect to the grammar G in view of Lemma 5.2. ■

VIII.6 Transfer of Systems

The following theorem was proved by Boasson [1976] for systems of length 2, and by Beauquier [1978a] in the general case.

Theorem 6.1 (Transfer Theorem for Systems of Iterative Pairs) *Let A and B be algebraic languages such that $A \geq B$. For any independent system θ of iterative pairs in B , there exists a system θ' of iterative pairs in A of the same length such that $\chi(\theta', A) \geq \chi(\theta, B)$.*

Note that θ' is not claimed to be independent, and in fact the theorem is false with this additional condition. We shall give some "substantial" counterexample below (Example 6.4). This restriction makes the theorem difficult to apply in its present form since dependent systems of great length or "complexity" are in general easily constructed in languages which have only simple independent systems. This was seen for instance for D_1^* in Example 4.7. We therefore state below several variations or special cases of the Transfer Theorem.

Let $A \subset X^*$, $B \subset Y^*$ and assume $A \geq B$. Then by Nivat's Theorem, there is an alphabet Z such that

$$B = \psi(\varphi^{-1}(A) \cap K)$$

where $\psi: Z^* \rightarrow Y^*$ is a morphism, $\varphi: Z^* \rightarrow X^*$ is an alphabetic morphism and $K \subset Z^*$ is a local regular language. With these notations, we first prove

Proposition 6.2 *Let A and B be algebraic languages such that $A \geq B$, and let G be an algebraic grammar generating A . For any system of iterative pairs*

$$\theta = (a_0, u_1, \dots, u_{2n}, a_{2n})$$

in B grammatical with respect to the grammar $\psi[\varphi^{-1}(G)_K]$, there exists a system of iterative pairs

$$\theta' = (a'_0, u'_1, \dots, u'_{2n}, a'_{2n})$$

in A grammatical with respect to G such that $\chi(\theta', A) \geq \chi(\theta, B)$ and $\text{Exp}(\theta', A) \subset \text{Exp}(\theta, B)$. Further

$$a_0 u_1^{k_1} \dots u_{2n}^{k_{2n}} a_{2n} \in \psi[\varphi^{-1}(a'_0 u_1'^{k_1} \dots u_{2n}'^{k_{2n}} a'_{2n}) \cap K], \text{ for } k_1, \dots, k_{2n} \geq 0.$$

Proof. Set $C = \varphi^{-1}(A) \cap K$. Then $B = \psi(C)$. In view of Lemma 5.3 there exists a system of iterative pairs $\bar{\theta} = (\bar{a}_0, \bar{u}_1, \dots, \bar{u}_{2n}, \bar{a}_{2n})$ in C , grammatical with respect to $(\varphi^{-1}G)_K$, such that $\psi(\bar{\theta}) = \theta$. Further $\text{Exp}(\bar{\theta}, C) \subset \text{Exp}(\theta, B)$. Since K is local, $\text{Exp}(\bar{\theta}, C) = \text{Exp}(\bar{\theta}, \varphi^{-1}(A))$ by Lemma 4.1, and $\bar{\theta}$ is grammatical with respect to $\varphi^{-1}(G)$ by Lemma 5.1. Define $\theta' = \varphi(\bar{\theta})$. Then θ' is a system of iterative pairs in A and $\text{Exp}(\theta', A) = \text{Exp}(\bar{\theta}, \varphi^{-1}(A))$ by Lemma 4.2, and θ' is grammatical with respect to G by Lemma 5.2. Thus $\text{Exp}(\theta', A) \subset \text{Exp}(\theta, B)$. Next if $w = a'_0 u_1'^{k_1} \dots u_{2n}'^{k_{2n}} a'_{2n}$, let $\bar{w} = \bar{a}_0 \bar{u}_1^{k_1} \dots \bar{u}_{2n}^{k_{2n}} \bar{a}_{2n}$. Then $\bar{w} \in \varphi^{-1}(w)$, and $\bar{w} \in K$ since $K \supset \bar{a}_0 \bar{u}_1^* \dots \bar{u}_{2n}^* \bar{a}_{2n}$. Consequently $\psi \bar{w} = a_0 u_1^{k_1} \dots u_{2n}^{k_{2n}} a_{2n} \in \psi[\varphi^{-1}(w) \cap K]$. ■

Proof of Theorem 6.1. Let φ, ψ, K, Z be as above, and let G be a grammar generating A . In view of Theorem 5.5 there exists an (independent) system of iterative pairs $\bar{\theta}$ deduced from θ which is grammatical with respect to the grammar $\psi[\varphi^{-1}(G)_K]$. Further $\chi(\bar{\theta}, B) \geq \chi(\theta, B)$ by Lemma 5.4. In view of the proposition above, there is a system of iterative pairs θ' in A such that $\text{Exp}(\theta', A) \subset \text{Exp}(\bar{\theta}, B)$. Consequently $\chi(\theta', A) \geq \chi(\bar{\theta}, B) \geq \chi(\theta, B)$. ■

We now prove the following more precise version of Theorem 6.1.

Proposition 6.3 *Let A and B be algebraic languages such that $A \geq B$. For any independent system of iterative pairs θ in B of length n , there exists a system of iterative pairs θ' in A of the same length, and two vectors $\vec{q}, \vec{p} \in \mathbb{N}^{2n}$ such that*

$$\vec{q} + \vec{p} \text{Exp}(\theta', A) \subset \text{Exp}(\theta, B) \cap (\vec{q} + \vec{p}\mathbb{N}^{2n}). \quad (6.1)$$

Proof. With the notations of the proof of Theorem 6.1, we have by (5.6)

$$\vec{q} + \vec{p} \text{Exp}(\bar{\theta}, B) = \text{Exp}(\theta, B) \cap (\vec{q} + \vec{p}\mathbb{N}^{2n}).$$

Since $\text{Exp}(\theta', A) \subset \text{Exp}(\bar{\theta}, B)$, the conclusion follows. ■

There is another formulation of Proposition 6.2 which can be used for proving nondomination.

Corollary 6.4 Let A and B be algebraic languages such that $A \geq B$, and let α be a type of a system of iterative pairs (i.e. a word in D_4^* over Ξ). If for any algebraic grammar G' generating B , there is a system θ' of iterative pairs in B grammatical with respect to G' and of type $\chi(\theta', B) \geq \alpha$, then for any algebraic grammar G generating A , there exists a system θ of iterative pairs in A grammatical with respect to G such that $\chi(\theta, A) \geq \alpha$.

Proof. Assume that there is a grammar G for A , such that any system θ of iterative pairs in A grammatical with respect to G satisfies $\chi(\theta, A) \not\geq \alpha$. Then with the notations of Proposition 6.2, let $G' = \psi[\varphi^{-1}(G)_K]$. There is a system θ' in B grammatical with respect to G' such that $\chi(\theta', B) \geq \alpha$. By Proposition 6.2, there exists a system θ in A , grammatical with respect to G , such that $\chi(\theta, A) \geq \chi(\theta', B) \geq \alpha$. This yields the contradiction. ■

There is a more striking statement of the previous corollary. Define the grammatical type $\gamma(A)$ of an algebraic language to be the following subset of D_4^* over Ξ : $\alpha \in \gamma(A)$ iff for any algebraic grammar G generating A , there exists a system θ of iterative pairs in A grammatical with respect to G such that $\chi(\theta, A) \geq \alpha$. Then Corollary 6.4 can be restated as:

Corollary 6.5 Let A and B be algebraic languages. If $A \geq B$ then $\gamma(A) \supset \gamma(B)$. ■

This corollary expressed the influence of rational domination on the "structural" description of the languages. Indeed, the "complexity" of a context-free language A can be defined as the features which are common to all grammars generating A . The types of grammatical systems shared by all grammars for A reflect in some sense these common features since they described restrictions in the use of nonterminals which are common to all grammars. Thus the corollary says that if A dominates B , the grammars for B are not as rich in structure as the grammars for A .

However, the meaning of results like Corollary 6.5 concerning grammatical systems of iterative pairs must not be overestimated. Indeed, the converse of the corollary is false, since for instance $\gamma(S_-) = \gamma(S_2)$, where S_2 is the symmetric language and $S_- = \{x^n y^n \mid n \geq 0\}$. This is a consequence of the fact (Exercise 6.1) that whenever a context-free language L has a grammatical iterative pair of type $e\bar{e}$ with respect to some grammar G , then it has also grammatical systems of iterative pairs of type $e^n \bar{e}^n$ with respect to G for any $n \geq 2$. (Of course, these systems are not independent in general.) Thus the sets $\gamma(L)$ are not a satisfactory measure of complexity, since a language like S_2 is intuitively regarded as, and proved by rational domination to be more "complex" than S_- . Consequently, the consideration of grammatical systems of iterative pair is not sufficient, even if they are very useful in some cases (see for instance Theorem 7.14).

Results like Proposition 6.2 or Corollary 6.5 may be delicate to apply since they require some knowledge about all grammars generating a given language. Thus the description of special cases of the Transfer Theorem or of Proposition 6.2 may provide helpful results for comparison of languages. Such a special case is realized when all the underlying iterative pairs of a given system are very strict, and when further this system is independent. Therefore we define:

Definition Let θ be a system of iterative pairs in L . Then θ is called very strict if all underlying iterative pairs of θ are very strict.

Thus θ is very strict in L iff $\chi(\theta, L) \in \{e, \bar{e}\}^*$. We first give a characterization of independence for very strict systems.

Lemma 6.6 Let θ be a very strict system of iterative pairs in L . Then θ is independent iff $\text{Exp}(\theta, L) = \text{Diag}(\theta, L)$.

Proof. We first prove that the condition is necessary by induction on the length n of θ . For $n = 1$ there is nothing to prove. Assume $\theta = \pi * \theta'$. Then $\text{Exp}(\pi, L) = \Delta$ since θ is very strict. Next $\text{Exp}(\theta, L) = \Delta * \text{Exp}(\theta', L)$ since θ is independent. By induction, $\text{Exp}(\theta', L) = \text{Diag}(\theta', L)$ and therefore $\text{Exp}(\theta, L) = \Delta * \text{Diag}(\theta', L) = \text{Diag}(\theta, L)$. Next assume $\theta = \theta_1 \times \theta_2$. Then $\text{Exp}(\theta, L) = \text{Exp}(\theta_1, L) \times \text{Exp}(\theta_2, L)$ since θ is independent. By induction, $\text{Exp}(\theta_i, L) = \text{Diag}(\theta_i, L)$ $i = 1, 2$. Thus $\text{Exp}(\theta, L) = \text{Diag}(\theta_1, L) \times \text{Diag}(\theta_2, L) = \text{Diag}(\theta, L)$.

Conversely, assume $\text{Exp}(\theta, L) = \text{Diag}(\theta, L)$. If $n = 1$ there is nothing to prove. If $\theta = \pi * \theta'$, then $\text{Exp}(\pi, L) = \Delta$ since θ is very strict. Next $\text{Exp}(\theta, L) = \Delta * \text{Diag}(\theta', L)$ and $\text{Exp}(\theta, L) \supset \{(1, 1)\} * \text{Exp}(\theta', L)$. Thus $\{(1, 1)\} * \text{Exp}(\theta', L) \subset \{(1, 1)\} * \text{Diag}(\theta', L)$, whence $\text{Diag}(\theta', L) = \text{Exp}(\theta', L)$. Thus θ' is independent by induction, and since $\text{Exp}(\theta, L) = \Delta * \text{Exp}(\theta', L)$, θ is independent. If $\theta = \theta_1 \times \theta_2$, then $\text{Exp}(\theta, L) = \text{Diag}(\theta_1, L) \times \text{Diag}(\theta_2, L)$; Let k be the length of θ_1 and let $\bar{1}_k = (1, 1, \dots, 1) \in \mathbb{N}^{2k}$. Then $\bar{1}_k \times \text{Exp}(\theta_2, L) \subset \text{Exp}(\theta, L)$, thus $\text{Exp}(\theta_2, L) = \text{Diag}(\theta_2, L)$. Similarly $\text{Exp}(\theta_1, L) = \text{Diag}(\theta_1, L)$. Consequently θ_1 and θ_2 are independent by induction, and $\text{Exp}(\theta, L) = \text{Exp}(\theta_1, L) \times \text{Exp}(\theta_2, L)$. Thus θ is independent. ■

Corollary 6.7 Let A and B be algebraic languages such that $A \geq B$. For any independent very strict system θ of iterative pairs in B , there exists an independent very strict system $\bar{\theta}$ of iterative pairs of the same type in A .

Proof. The only new assertion is the independence of $\bar{\theta}$. Let n be the length of θ and set $m = 2n$. Then in view of (6.1) and of the previous lemma, there is a very strict system $\bar{\theta}$ in A of same type as θ such that

$$\bar{q} + \bar{p} \text{Exp}(\bar{\theta}, A) \subset \text{Diag}(\bar{\theta}, B), \quad (6.2)$$

where as in Section 5:

$$\bar{p} = (p_1, \dots, p_m), \quad \bar{q} = (N - p_1, \dots, N - p_m).$$

We prove by induction on n that (6.2) implies:

$$\text{Exp}(\bar{\theta}, A) = \text{Diag}(\bar{\theta}, A). \quad (6.3)$$

The corollary follows then by the previous lemma. If $n = 1$, then (6.3) holds by definition. Thus assume $n > 1$, and suppose first $\theta = \theta_1 \times \theta_2$, for some independent very strict systems θ_1 and θ_2 . Let l be the length of θ_1 . Since θ and $\bar{\theta}$ have the same type, $\bar{\theta} = \bar{\theta}_1 \times \bar{\theta}_2$, where $\bar{\theta}_1$ and $\bar{\theta}_2$ are of the same type as θ_1 and θ_2 respectively. Next $(k_1, \dots, k_{2l}) \in \text{Exp}(\bar{\theta}_1, A)$ implies that

$$\bar{q} + \bar{p}(k_1, \dots, k_{2l}, 1, \dots, 1) \in \text{Diag}(\theta, B) = \text{Diag}(\theta_1, B) \times \text{Diag}(\theta_2, B).$$

Thus (6.2) is verified for $\bar{\theta}_1$ and θ_1 , and similarly for $\bar{\theta}_2$ and θ_2 . By induction, $\text{Exp}(\bar{\theta}_i, A) = \text{Diag}(\bar{\theta}_i, A)$, ($i = 1, 2$). Now let $(k_1, \dots, k_m) \in \text{Exp}(\bar{\theta}, A)$. Then by (6.2)

$$(N + (k_1 - 1)p_1, \dots, N + (k_{2l} - 1)p_{2l}) \in \text{Diag}(\theta_1, B)$$

$$(N + (k_{2l+1} - 1)p_{2l+1}, \dots, N + (k_m - 1)p_m) \in \text{Diag}(\theta_2, B).$$

Consequently $(k_1, \dots, k_m) \in \text{Diag}(\bar{\theta}_1, A) \times \text{Diag}(\bar{\theta}_2, A)$, whence

$$\text{Exp}(\bar{\theta}, A) \subset \text{Diag}(\bar{\theta}_1, A) \times \text{Diag}(\bar{\theta}_2, A).$$

Suppose now $\theta = \pi * \theta'$. Then $\bar{\theta} = \bar{\pi} * \bar{\theta}'$. Since $\bar{\theta}$ is very strict, $\text{Exp}(\bar{\pi}, A) = \Delta$. By the same argument as above, it is seen that $\text{Exp}(\bar{\theta}', A) = \text{Diag}(\bar{\theta}', A)$. It follows in the same way that

$$\text{Exp}(\bar{\theta}, A) \subset \Delta * \text{Diag}(\bar{\theta}, A). \quad \blacksquare$$

We now give some examples of the use of the Transfer Theorem and of its variations. Further applications are given in the next section.

Example 6.1 The language $A = \{x^n y^n z^p t^p \mid n, p \geq 0\} (\approx (S_-)^2)$ strictly dominates $S_- = \{x^n y^n \mid n \geq 0\}$. Obviously A dominates S_- . To prove that the domination is strict, we observe that there exists in A an independent very strict system θ of type $e\bar{e}e\bar{e}$, namely $\theta = (1, x, 1, y, 1, z, 1, t, 1)$. Clearly no word of S_- admits an independent system of length 2. Thus by Corollary 6.7, S_- does not dominate A . (Note that S_- has very strict systems of type $ee\bar{e}\bar{e}$, for instance $(1, x, 1, x, 1, y, 1, y, 1)$, but these systems clearly are dependent.)

Example 6.2 The languages $A = \{x^n y^n z^p t^p \mid n, p \geq 0\}$ and $B = \{x^n y^p t^p z^n \mid n, p \geq 0\}$ are rationally incomparable. Indeed, the independent very strict systems of length 2 have all type $e\bar{e}e\bar{e}$ in A , and type $ee\bar{e}\bar{e}$ in B . These types are distinct, so by Corollary 6.7, the languages A and B are incomparable.

Example 6.3 Consider the languages

$$L = \{x^n y^m z^p t^q \mid n \geq m \geq 0, 0 \leq p \leq q\} \approx S_{\geq} \cdot S_{\leq},$$

$$M = \{x^n y^m z^p t^q \mid m \geq n \geq 0, 0 \leq q \leq p\} \approx S_{\leq} \cdot S_{\geq}.$$

We claim that L and M are incomparable. Assume for instance that M dominates L . Clearly $xyzt$ admits, in L an independent system of iterative pairs of type $r\bar{r}l\bar{l}$. Then the Transfer Theorem asserts the existence of a system of iterative pairs of length 2 in M , of type $\geq r\bar{r}l\bar{l}$. This system is necessarily of the form $\pi_1 \times \pi_2$, where π_1 and π_2 are (nondegenerated) iterative pairs. Clearly any such system has type $l\bar{l}r\bar{r}$. This yields the contradiction.

Example 6.4 (Lattaux [1977]) The restricted Dyck language $D_1^* \subset \{x, \bar{x}\}^*$ strictly dominates the language L of the preceding example. The fact that L does not dominate D_1^* follows from the Transfer Theorem for iterative pairs, since D_1^* has very strict pairs and obviously L has no pair of this type. The remarkable feature of this example is that D_1^* dominates L , whereas L has independent systems of length 2, and D_1^* has none such system (Example 4.7). To prove $D_1^* \geq L$, we first note that

$$D_1^* \geq D_1^* \cap x^* \bar{x}^* x^* \bar{x}^* \approx N$$

with $N = \{x^n y^m z^p t^q \mid n \geq m \geq 0, 0 \leq p \leq q, n + p = m + q\}$.

Next we verify that $L = x^* N t^*$ which gives the desired conclusion. Obviously $x^* N t^* \subset L$. Conversely, let $w = x^n y^m z^p t^q \in L$. Then $n \geq m$, $p \leq q$. If $k = (n - m - (q - p)) \geq 0$, let $r = n - k$. Then $r = m + q - p \geq 0$, and $r - m = q - p \geq 0$. Thus $w = x^k w'$ with $w' = x^r y^m z^p t^q \in N$, whence $w \in x^* N$. Symmetrically, $k \leq 0$ implies $w \in N t^*$.

Exercise

6.1 Suppose that a context-free language L has an iterative pair of type $e\bar{e}$. Show that for any context-free grammar G generating L , there is in L a system of iterative pairs of type $e''\bar{e}''$ grammatical with respect to G , for any $n \geq 2$.

VIII.7 Applications

In this section, we apply the Transfer Theorem and its corollaries to continue the classifications of context-free languages. Several infinite chains of cones are constructed. The main results are: The cone of restricted one counter languages and the cone of quasi-rational languages are incomparable; the cone of finite counter languages and the cone of linear languages are incomparable. We first prove a weaker result used later.

Proposition 7.1 *The cones Rocl and Lin are incomparable. Neither Rocl nor Lin is closed under product.*

Thus in particular D_1^* is not a generator of Alg.

Proof. In view of Examples 4.6 and 4.7, neither D_1^* nor S_2 has an independent system of iterative pairs of type $(e\bar{e})^2$. Thus by Corollary 6.5 the language

$(S_-)^2$ is neither in Rocl nor in Lin . This proves the second part of the proposition. We already know that D_1^* is not a linear language (Example V.6.5). To show that Lin is not contained in Rocl , consider the language $L = \{x^n y^p z^q t^n \mid n, p \geq 0\}$. Clearly L is linear and there is an independent system of type $e^2 \bar{e}^2$ in L . Thus in view of Corollary 6.7 and Example 4.7, L is not a restricted one counter language. ■

The next proposition extends Example 6.1 and shows the existence of an ascending chain of rational cones which are all contained in the least full AFL $\text{Lin } \hat{\Gamma}$ containing the linear languages and which are all, excepted the first, neither contained in Rocl nor in Lin .

Proposition 7.2 *The rational cones $(S_-)^n \Gamma$ ($n \geq 1$) form a strictly increasing chain of cones.*

Proof. Obviously $(S_-)^{n+1} \supseteq (S_-)^n$ for $n \geq 1$. Next $(S_-)^n$ has an independent system of iterative pairs of type $(e\bar{e})^n$, but has no such system of type $(e\bar{e})^{n+1}$. Thus by Corollary 6.7, $(S_-)^{n+1}$ does not dominate $(S_-)^n$. ■

There is another interesting chain built of cones of linear languages. Define $A_n \subset (X_n \cup \bar{X}_n)^*$, where $X_n = \{x_1, \dots, x_n\}$ and $\bar{X}_n = \{\bar{x}_1, \dots, \bar{x}_n\}$ by

$$A_n = \{x_1^{k_1} \cdots x_n^{k_n} \bar{x}_n^{k_n} \cdots \bar{x}_1^{k_1} \mid k_1, \dots, k_n \geq 0\}.$$

Clearly

$$A_n = S_n \cap x_1^* \cdots x_n^* \bar{x}_n^* \cdots \bar{x}_1^*,$$

where S_n is the symmetric language over $X_n \cup \bar{X}_n$.

Proposition 7.3 *The cones $A_n \Gamma$, ($n \geq 1$) form a strictly increasing chain of rational cones.*

Proof. Clearly A_n has independent very strict systems of iterative pairs of type $e^n \bar{e}^n$, but none of type $e^{n+1} \bar{e}^{n+1}$. Thus the conclusion follows from Corollary 6.7. ■

The rational cone $\mathcal{L} = \bigcup_{n \geq 1} A_n \Gamma$ is not principal, thus $\mathcal{L}$ is strictly contained in

Lin . It can even be shown that $\mathcal{L} \subsetneq \text{Ng}(\text{Lin}) = \{L \in \text{Lin} \mid L\Gamma \neq \text{Lin}\}$ (see Exercise 7.1). The cones $A_n \Gamma$ and $(S_-)^m \Gamma$, ($n, m \geq 2$) are pairwise incomparable. For a generalization, see Exercise 7.2. In order to pursue the classification of families of languages, we now consider systems of iterative pairs in principal full AFLs, and in the syntactic substitution of two languages. We need a definition.

Definition A system of iterative pairs θ in a language L is called prime if either θ is an iterative pair or $\theta = \pi * \theta'$.

Clearly θ is prime iff its type $\chi(\theta, L)$ is a Dyck prime in the language D_4^* over Ξ . Thus any system θ can be written in the form

$$\theta = \theta^{(1)} \times \cdots \times \theta^{(r)}$$

where $\theta^{(1)}, \dots, \theta^{(r)}$ are prime systems.

Proposition 7.4 *Let L be a language, $d \notin X_L$. If θ is a prime system of iterative pairs in $(Ld)^+$, then there is a prime system $\bar{\theta}$ of iterative pairs in L such that $\text{Exp}(\bar{\theta}, L) = \text{Exp}(\theta, (Ld)^+)$.*

Proof. We consider first iterative pairs. Let $\pi = (a, u, b, v, c)$ be a nondegenerated iterative pair of a word

$$w = h_1 d h_2 d \cdots h_m d \quad (h_i \in L)$$

in L . Then $w = aubvc$. We claim that neither u nor v contains an occurrence of the letter d . Assume indeed for instance that $|u|_d > 0$. Then there are integers $i < j$, and factorizations

$$h_i = h'_i h''_i, \quad h_j = h'_j h''_j$$

such that

$$a = h_1 d \cdots h_{i-1} d h'_i, \quad u = h''_i d h_{i+1} d \cdots h_{j-1} d h'_j.$$

Since $au^p b v^q c \in (Ld)^+$, necessarily $h'_i h''_i \in L$, $h'_j h''_j \in L$. Consequently, $au^p b v^q c \in (Ld)^+$ implies $au^p b v^q c \in (Ld)^+$ for all $p \geq 0$, whence $au^* b v^* c \in (Ld)^+$ and π is degenerated contrary to the assumption. Thus there is an index i , ($1 \leq i \leq m$) and a factorization

$$h_i = \bar{a} u h'_i, \quad \text{with} \quad a = h_1 d \cdots h_{i-1} d \bar{a}.$$

Then two cases are possible: a) There is an index $j > i$ such that $h_j = h'_j v h''_j$, and $b = h'_j d \cdots h_{j-1} d h'_j$. But then $au^p b v^q c \in (Ld)^+$ implies $\bar{a} u^p h'_j \in L$, $h'_j v^q h''_j \in L$, whence again $au^* b v^* c \in (Ld)^+$. Therefore we have: b) h'_i factorizes into $h'_i = b v \bar{c}$ (and $\bar{c} d h_{i+1} d \cdots h_m d = c$). Then $au^p b v^q c \in (Ld)^+$ iff $\bar{a} u^p b v^q \bar{c} \in L$, thus $\pi = (\bar{a}, u, b, v, \bar{c})$ is an iterative pair of h_i in L , and $\text{Exp}(\bar{\pi}, L) = \text{Exp}(\pi, (Ld)^+)$.

Consider next a prime system

$$\theta = (a_0, u_1, a_1, \dots, u_{2n}, a_{2n})$$

of iterative pairs of w in $(Ld)^+$, and let $\theta = \pi * \theta'$, with $\pi = \langle u_1, u_{2n} \rangle$. Then by the first part of the proof, there are factorizations $a_0 = w' \bar{a}_0$, $a_{2n} = \bar{a}_{2n} w''$ with $w', w'' \in (Ld)^*$, such that $\bar{a}_0 u_1 a_1 \cdots u_{2n} \bar{a}_{2n} \in L$. Thus

$$\bar{\theta} = (\bar{a}_0, u_1, a_1, \dots, u_{2n}, \bar{a}_{2n})$$

is a system of iterative pairs in L and clearly $\text{Exp}(\bar{\theta}, L) = \text{Exp}(\theta, (Ld)^+)$. ■

Example 7.1 The symmetric language S_2 is not in $\text{Ocl} = D_1^* \hat{\Gamma}$. Assume indeed that $(D_1^* d)^+$ dominates S_2 . Since by Example 4.6, S_2 has independent very

strict systems of type $e^p \bar{e}^p$ for any $p \geq 1$, the language $(D_1^* d)^+$ must have independent systems of these types by Corollary 6.7. But then Proposition 7.4 implies that D_1^* itself has independent systems of these types, and this contradicts Example 4.7.

We now extend the previous result to the syntactic substitution $L \uparrow M$, with the aim to prove that S_2 is not in the substitution closure of the one counter languages. Consider two disjoint alphabets X, Y , and let $L \subset X^*, M \subset Y^*$. Let φ be the projection $(X \cup Y)^* \rightarrow X^*$.

We first consider two special cases.

Lemma 7.5 Let $\theta = (a_0, u_1, \dots, u_{2n}, a_{2n})$ be a system of iterative pairs in $L \uparrow M$, and suppose that $u_1 a_1 \dots a_{2n-1} u_{2n} \in Y^*$. Then there exists a system of iterative pairs $\bar{\theta}$ in M with $\text{Exp}(\bar{\theta}, M) = \text{Exp}(\theta, L \uparrow M)$.

Proof. Set $w = a_0 u_1 \dots u_{2n} a_{2n}$. Since $w \in L \uparrow M$, $w = h_1 x_1 \dots h_p x_p$ for some $h_1, \dots, h_p \in M, x_1, \dots, x_p \in X, x_1 \dots x_p \in L$. The assumption implies that there is an index i , ($1 \leq i \leq p$) and a factorization

$$h_i = \bar{a}_0 u_1 a_1 \dots u_{2n} \bar{a}_{2n} \\ a_0 = h_1 x_1 \dots x_{i-1} \bar{a}_0, \quad a_{2n} = \bar{a}_{2n} x_i h_{i+1} x_{i+1} \dots h_p x_p.$$

Then $\bar{\theta} = (\bar{a}_0, u_1, a_1, \dots, u_{2n}, \bar{a}_{2n})$ clearly satisfies $\text{Exp}(\bar{\theta}, M) = \text{Exp}(\theta, L \uparrow M)$. $\blacksquare$

Lemma 7.6 Let $\theta = (a_0, u_1, \dots, u_{2n}, a_{2n})$ be a system of iterative pairs in $L \uparrow M$, and suppose that $|u_i|_X > 0$, ($i = 1, \dots, 2n$) and $|a_i|_X > 0$, ($i = 1, \dots, 2n-1$). Then $\varphi(\theta)$ is a system of iterative pairs in L and $\text{Exp}(\varphi(\theta), L) = \text{Exp}(\theta, L \uparrow M)$.

Proof. Clearly $\text{Exp}(\theta, L \uparrow M) \subset \text{Exp}(\varphi(\theta), L)$. In order to prove the converse inclusion, observe first that $L \uparrow M = \varphi^{-1}(L) \cap (MX)^*$. Next $\text{Exp}(\varphi(\theta), L) = \text{Exp}(\theta, \varphi^{-1}(L))$. Set $K = a_0 u_1^* a_1 \dots u_{2n}^* a_{2n}$. Suppose proved already that $K \subset (MX)^*$. Then

$$\text{Exp}(\theta, \varphi^{-1}(L)) = \text{Exp}(\theta, \varphi^{-1}(L) \cap K) \subset \text{Exp}(\theta, L \uparrow M),$$

whence $\text{Exp}(\varphi(\theta), L) = \text{Exp}(\theta, L \uparrow M)$ as desired. Thus it suffices to verify the inclusion $K \subset (MX)^*$. For this, set $m = 2n$,

$$w = a_0 u_1 \dots u_m a_m = h_1 x_1 \dots h_p x_p,$$

with $h_1, \dots, h_p \in M, x_1, \dots, x_p \in L$. The conditions $\varphi(u_i) \neq 1, \varphi(a_i) \neq 0$ imply that there exist indices $1 \leq r(1) < s(1) < r(2) < \dots < r(m) < s(m) \leq p$ such that

$$u_i = h_{r(i)}'' x_{r(i)} \dots x_{s(i)-1} h_{s(i)}' \quad i = 1, \dots, m \\ a_i = h_{s(i)}'' x_{s(i)} \dots x_{r(i+1)-1} h_{r(i+1)}' \quad i = 1, \dots, m-1 \\ a_0 = h_1 x_1 \dots x_{r(1)} h_{r(1)}', \quad a_m = h_{s(m)}'' x_m \dots h_p x_p$$

for factorizations $h_{r(i)} = h_{r(i)}' h_{r(i)}'', h_{s(i)} = h_{s(i)}' h_{s(i)}'', (i = 1, \dots, m)$. Since $a_0 a_1 a_2 \dots a_m \in L \uparrow M$, we have $h_{r(i)}' h_{s(i)}'' \in M$ for $i = 1, \dots, m$. Similarly, since $a_0 u_1^* a_1 u_2^* \dots a_{m-1} u_m^* a_m \in L \uparrow M$, we have $h_{s(i)}' h_{r(i)}'' \in M$ for $i = 1, \dots, m$. Consequently $a_0 u_1^* a_1 \in (MX)^* h_{r(2)}'$ for all $k_1 \geq 0$, and by induction

$$a_0 u_1^* a_1 u_2^{k_2} a_2 \dots u_i^{k_i} a_i \in (MX)^+ h_{r(i+1)}' \\ \text{for } i \leq m-1 \text{ and } k_1, \dots, k_i \geq 0,$$

and the desired result follows. $\blacksquare$

Proposition 7.7 Let $\pi = (a, u, b, v, c)$ be a nondegenerated iterative pair in $L \uparrow M$. Then

- (i) either $|u|_X > 0, |v|_X > 0$ and $\varphi(\pi)$ is an iterative pair in L ;
- (ii) or $ubv \in Y^+$, and there is an iterative pair $\bar{\pi}$ in M such that $\text{Exp}(\bar{\pi}, M) = \text{Exp}(\pi, L \uparrow M)$.

Note that we do not claim that $\varphi(\pi)$ is nondegenerated. Indeed this stronger result is false in general.

Example 7.2 Let $X = \{x, y\}, Y = \{a, b, c\}, L = x^* y \cup S_{\leq}$, and $M = \{1, a, bc, c, ab\}$. Consider the iterative pair $\pi = (a, x, b, cy, y)$ in $L \uparrow M$. Then $\text{Exp}(\pi, L \uparrow M) = \{(n, m) \mid 0 \leq n \leq m\}$. Next $\varphi(\pi) = (1, x, 1, y, y)$ and $\text{Exp}(\varphi(\pi), L) = \mathbb{N} \times \{0\} \cup \{(n, m) \mid 0 \leq n \leq m\}$. Thus π is left strict and $\varphi(\pi)$ is degenerated.

However, the previous example is somewhat artificial as is shown by the

Corollary 7.8 Let $\pi = (a, u, b, v, c)$ be a nondegenerated iterative pair in $L \uparrow M$ and suppose $|u|_X > 0, |v|_X > 0$. Then $\pi' = (a, u, ub, v, vc)$ is an iterative pair in $L \uparrow M$ with $\chi(\pi', L \uparrow M) \geq \chi(\pi, L \uparrow M)$, and $\varphi(\pi')$ is an iterative pair in L satisfying $\text{Exp}(\varphi(\pi'), L) = \text{Exp}(\pi', L \uparrow M)$.

Proof. Clearly $(k, l) \in \text{Exp}(\pi', L \uparrow M)$ iff $(1+k, 1+l) \in \text{Exp}(\pi', L \uparrow M)$. Thus $\chi(\pi', L \uparrow M) \geq \chi(\pi, L \uparrow M)$. Next by Proposition 7.7, $\varphi(\pi')$ is an iterative pair in L . Finally π' satisfies the conditions of Lemma 7.6, and this lemma gives the required equality. $\blacksquare$

Proof of Proposition 7.7. If $|u|_X > 0$ and $|v|_X > 0$, then $\varphi(\pi)$ is an iterative pair in L since $|\varphi(uv)| > 0$ and $\text{Exp}(\pi, L \uparrow M) \subset \text{Exp}(\varphi(\pi), L)$. Next if $ubv \in Y^+$, then the conclusion follows from Lemma 7.5. Thus it remains only to prove that no other possibilities arise. For this, we show that $u \in Y^+$ implies $ubv \in Y^+$. The symmetrical implication: $v \in Y^+ \Rightarrow ubv \in Y^+$ is proved in the same way. Set

$$w = aubvc = h_1 x_1 \dots h_p x_p,$$

with $h_1, \dots, h_p \in M, x_1, \dots, x_p \in X, x_1 \dots x_p \in L$. If $u \in Y^+$, then there is an index i , ($0 \leq i \leq p$) such that

$$a = h_1 x_1 \dots h_{i-1} x_{i-1} h_i', \quad h_i = h_i' u h_i'', \quad bvc = h_i'' x_i \dots h_p x_p.$$

We claim that bu is a left factor of h''_i , showing thus that ubv is in Y^+ . Assume the contrary. Then h''_i is a proper left factor of bu , and for $n \geq 1$,

$$au^n bu^n c = h_1 x_1 \cdots h_{i-1} x_{i-1} h'_i u^n h''_i x_i f_n,$$

where $f_n \in (MX)^*$ is such that $x_1 \cdots x_i \varphi(f_n) \in L$. Since $h'_i u^n h''_i \in M$ for all $n \geq 1$, we also have

$$h_1 x_1 \cdots h_{i-1} x_{i-1} h'_i u^m h''_i x_i f_n = au^m bu^n c \in L \uparrow M$$

for all $m, n > 0$. Thus π is degenerated, contrary to the assumption. ■

Theorem 7.9 *The symmetric language S_2 is not a finite counter language. The cones Fcl and Lin are incomparable.*

Thus the relation $\text{Lin} \not\subseteq \text{Rocl}$ of Proposition 7.1 is strengthened to: $\text{Lin} \not\subseteq \text{Fcl}$. The “dual” result, namely $\text{Rocl} \not\subseteq \text{Qrt}$, will be proved below. Recall that $\text{Fcl} = \bigcup_{n \geq 1} \text{Fcl}(n)$, where $\text{Fcl}(1) = \text{Rocl}$ and $\text{Fcl}(n+1) = \text{Rocl} \circ \text{Fcl}(n)$ for $n \geq 1$.

The theorem is a direct consequence of the following proposition.

Proposition 7.10 *Let $A \in \text{Fcl}(n)$ and suppose that A has an independent system of iterative pairs of type $e^p \bar{e}^p$. Then $p \leq n$.*

Proof of Theorem 7.9. The symmetric language S_2 has independent systems of iterative pairs of type $e^p \bar{e}^p$ for any $p \geq 1$ (Example 4.6). Thus by the previous proposition, S_2 is not in $\text{Fcl}(n)$ for any $n \geq 1$. Thus $\text{Lin} \not\subseteq \text{Fcl}$. Since $\text{Rocl} \not\subseteq \text{Lin}$, the converse relation is obvious. ■

Proof of Proposition 7.10. (i) We first consider the following situation: Let $A = D_1^* \uparrow M$, where $D_1^* \subset X^*$ with $X = \{x, \bar{x}\}$, $M \subset Y^*$, $X \cap Y = \emptyset$, and φ is the projection of $(X \cup Y)^*$ onto X^* . Suppose that

$$\theta = (a_0, u_1, a_1, u_2, a_2, u_3, a_3, u_4, a_4) = \pi_1 * \pi_2$$

is an independent system of type $e^2 \bar{e}^2$ in A . We claim that then $|u_1|_X = 0$ or $|u_2|_X = 0$. Indeed, assume the contrary. Then by Proposition 7.7, $|u_3|_X > 0$ and $|u_4|_X > 0$. Consider the system

$$\theta' = (a_0, u_1, u_1 a_1, u_2, u_2 a_2, u_3, u_3 a_3, u_4, u_4 a_4).$$

Since $\text{Exp}(\theta, A) = \Delta * \Delta$, we have $\text{Exp}(\theta', A) = \Delta * \Delta$. In view of Lemma 7.6, $\varphi(\theta')$ is an independent system of iterative pairs of type $e^2 \bar{e}^2$ in D_1^* which is impossible by Example 4.7.

(ii) Next we claim that if $A = D_1^* \uparrow M$ has an independent system of type $e^p \bar{e}^p$ with $p \geq 2$, then M has an independent system of type $e^{p-1} \bar{e}^{p-1}$. Let indeed

$$\theta = (a_0, u_1, \dots, u_{2p}, a_{2p}) = \pi_1 * \pi_2 * \cdots * \pi_p$$

be an independent system of type $e^p \bar{e}^p$ in A . Then $\pi_1 * \pi_2$ is an independent system of type $e^2 \bar{e}^2$ in A , and by part (i), we have $u_1 a_1 \cdots a_{2p-1} u_{2p} \in Y^+$. In

view of Lemma 7.5, there is an independent system of type $e^{p-1} \bar{e}^{p-1}$ in M .

(iii) We now define languages A_n , ($n \geq 1$) as follows: $A_1 = D_1^*$, $A_{n+1} = D_1^* \uparrow (A'_n d_n)^+$, where A'_n is a copy of A_n over an alphabet disjoint from X , and where d_n is a new letter. By Theorem VI.5.7, A_n is a generator of the rational cone $\text{Fcl}(n)$. (Note that the use of Exercise VI.5.7 would supply generators of simpler form.) If $A \in \text{Fcl}(n)$, then $A_n \geq A$, and by Corollary 6.7, A_n has an independent system of iterative pairs of type $e^p \bar{e}^p$. Thus we have to prove that if A_n has an independent system of type $e^n \bar{e}^n$, then $p \leq n$. This will be done by induction, the case $n = 1$ being true in view of Example 4.7. Thus suppose $n > 1$ and $p > 1$. Then by part (ii), the language $(A'_{n-1} d_{n-1})^+$ has an independent system of type $e^{p-1} \bar{e}^{p-1}$. Since this system is prime, we apply Proposition 7.4. Consequently, A'_{n-1} , whence also A_{n-1} , has an independent system of type $e^{p-1} \bar{e}^{p-1}$. By induction, $n-1 \geq p-1$. ■

We now want to prove a result “dual” to Theorem 7.9, namely that D_1^* is not a quasi-rational language. The proof cannot use independent systems of iterative pairs, since such systems in D_1^* are all of type $e\bar{e}$. Instead of independent systems, we shall use grammatical systems and apply Proposition 6.2. Recall that

$$\text{Qrt} = \bigcup_{n \geq 1} \text{Qrt}(n),$$

where

$$\text{Qrt}(1) = \text{Lin}, \quad \text{Qrt}(n+1) = \text{Lin} \circ \text{Qrt}(n).$$

The idea of the proof is the following: We observe first that for a fixed grammar generating a fixed generator of the cone $\text{Qrt}(n)$, any grammatical system of iterative pairs of some special type satisfies an additional constraint (Proposition 7.12). Then we construct a restricted one counter language having systems violating this constraint, whatever is the grammar generating it (Lemma 7.13. This is the main part of the proof). By an application of Proposition 6.2, we conclude that this language is not in $\text{Qrt}(n)$. Consequently, the cone Rocl is contained in none of the cones $\text{Qrt}(n)$, and therefore D_1^* is in none of the $\text{Qrt}(n)$.

We begin with construction of an algebraic grammar generating the language $S_2 \uparrow (Md)^+$, where $S_2 \subset Z_2^*$ is the symmetric language, $M \subset Y^*$ is some algebraic language, $Z_2 \cap Y = \emptyset$ and $d \notin Z_2 \cup Y$ is a new letter. This will be used below with M a generator of $\text{Qrt}(n)$, and thus yields a grammar for a generator of $\text{Qrt}(n+1)$. As for the Dyck language D_1^* , the application of Exercise VI.5.6 could simplify the construction.

Let G_1 be the grammar generating S_2 with productions

$$\xi \rightarrow x_1 \xi \bar{x}_1 + x_2 \xi \bar{x}_2 + 1,$$

and let $G = \langle V, Y, P \rangle$ be an algebraic grammar such that $L_G(\sigma) = M$ for some $\sigma \in V$. We assume $\xi \notin V$, and consider a new symbol σ_+ . Define a grammar

$$G_1 \uparrow G = \langle \xi \cup \sigma_+ \cup V, Z_2 \cup Y \cup d, P \cup P' \rangle$$

by $P' = \{ \xi \rightarrow \sigma_+ x_1 \xi \sigma_+ \bar{x}_1, \xi \rightarrow \sigma_+ x_2 \xi \sigma_+ \bar{x}_2, \xi \rightarrow 1, \sigma_+ \rightarrow \sigma d \sigma_+, \sigma_+ \rightarrow \sigma d \}$.

Then a straightforward verification shows that

$$L_{G_1 \uparrow G}(\xi) = S_2 \uparrow (Md)^+.$$

Lemma 7.11 *If $S_2 \uparrow (Md)^+$ has a system of iterative pairs grammatical with respect to $G_1 \uparrow G$ of type $\beta = e\alpha\alpha\bar{e}$, where $\alpha \in \{e, \bar{e}\}^+$ is the type of a prime system of iterative pairs, then M has a system of iterative pairs of type α grammatical with respect to G .*

Proof. Let $\theta = (a_0, u_1, \dots, u_{2n}, a_{2n})$ be a grammatical system of type β . Then by definition, there are variables $\eta, \eta_1, \eta_2 \in V \cup \xi \cup \sigma_+$ such that, in $G_1 \uparrow G$,

$$\xi \xrightarrow{*} a_0 \eta a_{2n}, \quad \eta \xrightarrow{*} u_1 \eta u_{2n}, \quad \eta \xrightarrow{*} a_1 \eta_1 a_n \eta_2 a_{2n-1} \quad (7.1)$$

and since α is a Dyck-prime

$$\eta_1 \xrightarrow{*} u_2 \eta_1 u_n, \quad \eta_2 \xrightarrow{*} u_{n+1} \eta_2 u_{2n-1} \quad (7.2)$$

Observe that $\eta_1 \neq \sigma_+$ since the iterative pair $\langle u_2, u_n \rangle$ is nondegenerated and consequently $u_n \neq 1$. Similarly $\eta_2 \neq \sigma_+$. Thus $\eta_1, \eta_2 \in V \cup \xi$. If $\eta_1 = \eta_2 = \xi$, then by (7.1), $\xi \xrightarrow{*} a_0 a_1 \xi a_n \xi a_{2n-1} a_{2n}$. This is impossible since ξ appears at most once in the right side of each production of $G_1 \uparrow G$. Thus either $\eta_1 \in V$ or $\eta_2 \in V$. In the first case, the first of the derivations (7.2) holds also in G , and $\langle u_2, \dots, u_n \rangle$ is a system of iterative pairs of type α grammatical with respect to G . In the second case, $\langle u_{n+1}, \dots, u_{2n-1} \rangle$ is grammatical with respect to G . (Note that we do not claim that both η_1, η_2 are in V .) ■

We now define languages B_n , ($n \geq 1$) as follows:

$$B_1 = S_2, \quad B_{n+1} = S_2 \uparrow (B'_n d_n)^+ \quad (n \geq 1),$$

where B'_n is a copy of B_n over an alphabet disjoint from Z_2 , and where d_n is a new letter. Next let $G_{n+1} = G_1 \uparrow G'_n$, where G'_n is the grammar generating B'_n derived from G_n in the obvious way. Then $L_{G_n}(\xi) = B_n$, ($n \geq 1$). Define a sequence (α_n) of types by

$$\alpha_1 = e\bar{e}, \quad \alpha_{n+1} = e\alpha_n \alpha_n \bar{e} \quad (n \geq 1).$$

Proposition 7.12 *If B_n has a system of iterative pairs of type α_p grammatical with respect to G_n , then $p \leq n$.*

Actually, it is easy to show that B_n has systems of type α_n , grammatical with respect to G_n (Exercise 7.3).

Proof. The result is true for $n = 1$ by Example 4.6. Assume that B_n has a system of iterative pairs of type $\alpha_p = e\alpha_{p-1}\alpha_{p-1}\bar{e}$, ($p \geq 2$) grammatical with respect to G_n . Then by the previous lemma, B_{n-1} has a grammatical system with respect to G_{n-1} of type $p-1$. By induction $p-1 \leq n-1$. ■

The main lemma for the proof of the announced result is the following:

Lemma 7.13 *Define $L(k) = D_1^{*k} \cap (x^+ \bar{x}^+)^{2^{k-1}}$, ($k \geq 1$). For any grammar H generating $L(k)$, there exists a system of iterative pairs in $L(k)$ of type α_k which is grammatical with respect to H .*

Take the lemma for granted for a moment. Then we can prove

Theorem 7.14 (Yntema [1967]) *The language D_1^{*k} is not quasi-rational. The cones Rocl and Qrt are incomparable.*

Proof. If $D_1^{*k} \notin \text{Qrt}$, then $\text{Rocl} \not\subseteq \text{Qrt}$. Since $\text{Lin} \not\subseteq \text{Rocl}$ by Proposition 7.1, the cones Rocl and Qrt are incomparable. Thus it suffices to show that D_1^{*k} is not quasi-rational. Assume the contrary. Then $D_1^{*k} \in \text{Qrt}(n)$ for some $n \geq 1$. Let $k > n$. Since $D_1^{*k} \geq L(k)$ and $\text{Qrt}(n)$ is a cone, we have $L(k) \in \text{Qrt}(n)$, whence $L(k) \leq B_n$. Next in view of Lemma 7.13 and of Corollary 6.4, there is a system of iterative pairs θ in B_n grammatical with respect to G_n and such that $\chi(\theta, B_n) \geq \alpha_k$, whence $\chi(\theta, B_n) = \alpha_k$. By Proposition 7.12, we have $k \leq n$. This yields the desired contradiction. ■

Thus it remains to prove Lemma 7.13. The proof which follows is similar to a proof given by Gruska [1971b]. Fix an integer $k \geq 1$, set $X = \{x, \bar{x}\}$, $L = L(k)$, $K = (x^+ \bar{x}^+)^{2^{k-1}}$, and let $H = \langle V, X, P \rangle$ be a grammar such that $L = L_H(\sigma)$ for some $\sigma \in V$. We first give two preliminary lemmas.

Lemma 7.15 *One can assume that H is strictly reduced in σ , i.e. satisfies the two following conditions:*

(i) *For any $\xi \in V$, there are $a, b \in X^*$ such that $\sigma \xrightarrow{*} a\xi b$.* (7.3)

(ii) *For any $\xi \in V$, $L_H(\xi)$ is infinite.* (7.4)

Proof. In view of Lemma II.2.6, a strictly reduced grammar H' generating L exists. By the construction given in Section II.2, it is straightforward that any system of iterative pairs which is grammatical with respect to H' is also grammatical with respect to the original grammars, since all pivots satisfy condition (ii). ■

For the rest of the proof, we assume that H satisfies (7.3) and (7.4). Then we have

- Lemma 7.16** (i) For all $\xi \in V$, $u, v \in L_H(\xi)$ implies $\|u\| = \|v\|$.
(ii) For all $\xi \in V$, $L_H(\xi) \not\subset x^* \cup \bar{x}^*$.
(iii) If $\eta \xrightarrow{*} u\eta v$ for $u, v \in (V \cup X)^+$, then $u = x^p$, $v = \bar{x}^p$ for some $p > 0$.

By (i), there is an integer $\delta(\xi)$ for each $\xi \in V$ such that $\|u\| = \delta(\xi)$ for all $u \in L_H(\xi)$.

Proof. (i) By (7.3), there are $a, b \in X^*$ such that $\sigma \rightarrow a\xi b$. Thus $aub, avb \in D_1^*$, whence $0 = \|aub\| = \|avb\|$. Consequently $\|u\| = \|v\|$.
(ii) If $L_H(\xi) \subset x^* \cup \bar{x}^*$, then $L_H(\xi)$ consists of a single word $x^{\delta(\xi)}$ or $\bar{x}^{-\delta(\xi)}$ according to $\delta(\xi)$ being positive or negative. This contradicts (7.4).
(iii) In view of (7.3) and (7.4), there are $a, b, c \in X^*$ such that $\sigma \xrightarrow{*} a\eta c$, $\eta \xrightarrow{*} b$. Further $\sigma \xrightarrow{*} au^nbv^nc$ for $n \geq 0$. If $u \notin X^+$, then $|u|_\xi > 0$ for some $\xi \in V$. By (ii) $L_H(\xi)$ contains a word in $X^*(x\bar{x} \cup \bar{x}x)X^*$. Consequently $u \xrightarrow{*} u'$ for some $u' \in X^*(x\bar{x} \cup \bar{x}x)X^*$. Then $u'^n \in X^*(x\bar{x})^n X^* \cup X^*(\bar{x}x)^n X^* \subset X^*(x\bar{x})^{n-1} X^*$, and au^nbv^nc derives into a word which is not in K for sufficiently large n . Thus $u \in X^*$ and by the same argument as above $u \in x^+ \cup \bar{x}^+$. Since au^n is left factor of a word in D_1^* for $n \geq 0$, we have $\|au^n\| = \|a\| + n\|u\| \geq 0$ for all n whence $\|u\| \geq 0$. Thus $u \in x^+$. Symmetrically $v \in \bar{x}^+$. Finally $\|u\| + \|v\| = 0$. ■

Now let T be the integer associated to the grammar H by Ogden's Lemma II.2.5, set $D = \max\{|d(\xi)| : \xi \in V\}$ and set $N = D + T$. The two main lemmas of the proof are the following.

Lemma 7.17 Suppose that $\sigma \xrightarrow{*} w = gx^N \bar{x}^N h$ for some $g, h \in (V \cup X)^*$. Then there exist $\xi \in V$, and integers $r, s \geq 0$, $p > 0$ such that

- (i) $r + p, s + p \leq N$;
(ii) $\sigma \xrightarrow{*} g\xi^r \bar{\xi}^s h$, $\xi \rightarrow x^p \xi \bar{x}^p$, $x^{p+r} \xi \bar{x}^{p+s} \xrightarrow{*} x^N \bar{x}^N$.

Thus the lemma asserts that w admits an iterative pair (in the language $\hat{L}_H(\sigma)$ of sentential forms) such that both iterating elements are in the central factor $x^N \bar{x}^N$ of w .

Proof. Mark the T rightmost positions in the left factor $gx^N \bar{x}^N$ of w , and apply Ogden's Lemma II.2.5 to w . Then there exist a factorization $w = aubvc$, and a variable ξ such that $\sigma \xrightarrow{*} a\xi c$, $\xi \xrightarrow{*} u\xi v$, $\xi \xrightarrow{*} b$. By Lemma 7.16 (iii), $u = x^p$, $v = \bar{x}^p$ for some $p > 0$. Further $c = \bar{x}^s h$ for some $s \geq 0$, and $p + s \leq T \leq N$. Two localizations are possible for the iterating element u :

- (i) $|a| \geq |g|$. Then $a = gx^r$ for some $r \geq 0$, and clearly $r + p \leq N$. Further $b = x^{N-p-r} \bar{x}^{N-p-s}$.
(ii) $|a| < |g|$. Then $w' = ubv = g'x^N \bar{x}^{N-s}$, where g' is some right factor of g . Mark the T left most positions in the right factor $x^N \bar{x}^{N-s}$ of w' , and apply

Ogden's Lemma, noting that $\xi \xrightarrow{*} w'$. Then there are a factorization $w' = a'u'b'v'c'$ and a variable η such that $\xi \xrightarrow{*} a'\eta c'$, $\eta \xrightarrow{*} u'\eta v'$, $\eta \xrightarrow{*} b'$. As above, $u' = x^q$, $v' = \bar{x}^q$ for some $q > 0$, and $a' = g'x^{r'}$ for some $r' \geq 0$. Moreover $r' + q \leq T$. Further $c' = \bar{x}^{s'}$ for some s' such that $q + s' \leq N - s$, whence $(s' + s) + q \leq N$. Since $\sigma \xrightarrow{*} aa'\eta c'c = gx^{r'} \eta \bar{x}^{s'+s} h$ and $b' = x^{N-r'} \bar{x}^{N-(s'+s)}$, the lemma is verified also in this case. ■

Lemma 7.18 Suppose that

$$\sigma \xrightarrow{*} w = gx^{N+r_1} \eta_1 \bar{x}^{s_1} x^{r_2} \eta_2 \bar{x}^{s_2+N} h$$

for some $g, h \in (V \cup X)^*$, and that further

- (i) $r_1, r_2, s_1, s_2 \leq N$;
(ii) $x^{r_1} \eta_1 \bar{x}^{s_1} \xrightarrow{*} x^N u_1 \bar{x}^N$, $x^{r_2} \eta_2 \bar{x}^{s_2} \xrightarrow{*} x^N u_2 \bar{x}^N$ for some $u_1, u_2 \in D_1^*$.

Then there exist $\xi \in V$, $t_1, t_2 \geq 0$, $p > 0$ such that

- (iii) $t_1 + p, t_2 + p \leq N$;
(iv) $\sigma \xrightarrow{*} g\xi^{t_1} \bar{\xi}^{t_2} h$; $\xi \xrightarrow{*} x^p \xi \bar{x}^p$, $x^{t_1+p} \xi \bar{x}^{t_2+p} \xrightarrow{*} x^{N+r_1} \eta_1 \bar{x}^{s_1} x^{r_2} \eta_2 \bar{x}^{s_2+N}$;
(v) $x^{t_1+p} \xi \bar{x}^{t_2+p} \xrightarrow{*} x^N u_3 \bar{x}^N$ for some $u_3 \in D_1^*$.

The lemma claims the existence of an iterative pair of w whose iterating elements are contained in the N first x 's of the block x^{N+r_1} and in the N last $\bar{x}$'s of the block $\bar{x}^{s_2+N}$ of w respectively.

Proof. The conclusion (v) is a direct consequence of (iv) and (ii), since $x^{t_1+p} \xi \bar{x}^{t_2+p} \xrightarrow{*} x^N u_1 \bar{x}^N x^N u_2 \bar{x}^N \bar{x}^N$, whence $u_3 = x^N u_1 \bar{x}^N x^N u_2 \bar{x}^N \in D_1^*$. We proceed as in the proof of the previous lemma: Mark the T rightmost positions of the left factor $gx^{N+r_1} \eta_1 \bar{x}^{s_1} x^{r_2} \eta_2 \bar{x}^{s_2+N}$ of w , and apply Ogden's Lemma to w . Then there are a factorization $w = aubvc$, and a variable ξ such that $\sigma \xrightarrow{*} a\xi c$, $\xi \xrightarrow{*} u\xi v$, $\xi \xrightarrow{*} b$. By Lemma 7.16, $u = x^p$, $v = \bar{x}^p$ for some $p > 0$, and $c = \bar{x}^{t_2} h$ for some t_2 such that $t_2 + p \leq T \leq N$. Three localizations are possible for the iterating element u :

- a) $|a| \geq |gx^{N+r_1} \eta_1 \bar{x}^{s_1}|$ and $|bvc| \geq |\eta_2 \bar{x}^{s_2+N} h|$.
b) $|a| \geq |g|$ and $|au| \leq |gx^{N+r_1}|$.
c) $|a| < |g|$.

We first verify that case a) is impossible. Assume the contrary. Then $ubv = x^r \eta_2 \bar{x}^{s_2+N-t_2}$ for some $r \leq r_2$. Next, by (ii), $ubv \xrightarrow{*} x^{r-r_2+N} u_2 \bar{x}^{2N-t_2}$. Since $\xi \xrightarrow{*} ubv$, we have $-D \leq d(\xi) = r - r_2 - N + t_2 \leq -N + t_2 < -N + T$, whence $N < D + T = N$.

Consider now case b). Then $a = gx^{t_1}$ for some $t_1 \geq 0$, whence $ubv = x^{N+r_1-t_1} \eta_1 \bar{x}^{s_1} x^{r_2} \eta_2 \bar{x}^{N+s_2-t_2}$. Since

$$\xi \xrightarrow{*} ubv \xrightarrow{*} x^{2N-t_1} u_1 \bar{x}^N x^N u_2 \bar{x}^{2N-t_2},$$

$-D \leq d(\xi) = t_2 - t_1 \leq T - (t_1 + p)$, whence $t_1 + p \leq T + D = N$.

Finally assume that c) holds. Then $ubv = w' = g' x^{N+r_1} \eta_1 \bar{x}^{s_1} x^{r_2} \eta_2 \bar{x}^{s_2-t_2+N}$, where g' is a right factor of g . Mark the T leftmost positions of the right factor $x^{N+r_1} \eta_1 \bar{x}^{s_1} x^{r_2} \eta_2 \bar{x}^{s_2-t_2+N}$ of w' , and apply Ogden's Lemma to w' . Remembering that $\xi \xrightarrow{*} w'$, we obtain a factorization $w' = a' u' b' v' c'$ and a variable η such that $\xi \xrightarrow{*} a' \eta c'$, $\eta \xrightarrow{*} u' \eta v'$, $\eta \xrightarrow{*} b'$. Then $a' = g' x^{t'}$, and $u' = x^q$, $v' = \bar{x}^q$ for $t' \geq 0$, $q > 0$ and $t' + q \leq T$. Next either $|c'| \geq |x^{r_2} \eta_2 \bar{x}^{s_2-t_2+N}|$ or $c' = \bar{x}^l$ for some l . In the first case, $u' b' v' = x^{N+r_1-t'} \eta_1 \bar{x}^{s_1}$ for some $s_1' \leq s_1$, and since $\eta \xrightarrow{*} u' b' v' \xrightarrow{*} x^{2N-t'} u_1 \bar{x}^{N+s_1'-s_1}$, we obtain $d(\eta) = N - t' - (s_1' - s_1)$. Consequently $N = d(\eta) + t' + s_1' - s_1 \leq d(\eta) + t' < D + T = N$, which is impossible. Thus the second case holds. Then

$$\sigma \xrightarrow{*} aa' \eta c' = g x^{t'} \eta \bar{x}^{l+t_2} h,$$

$$x^{t'+q} \eta \bar{x}^{q+l+t_2} = x^{t'} u' \eta v' \bar{x}^{l+t_2} \xrightarrow{*} x^{N+r_1} \eta_1 \bar{x}^{s_1} x^{r_2} \eta_2 \bar{x}^{s_2+N}.$$

Since $t' + q \leq T \leq N$, it remains only to show that $q + l + t_2 \leq N$.

By (ii), $\eta \xrightarrow{*} u' b' v' \xrightarrow{*} x^{2N-t'} u_1 \bar{x}^N x^N u_2 \bar{x}^{2N-(l+t_2)}$. Thus $d(\eta) = l + t_2 - t'$, whence $q + l + t_2 = d(\eta) + q + t' \leq D + T = N$. ■

Proof of Lemma 7.13. Define a sequence f_n , ($n = 1, \dots, k$) of words by

$$f_1 = x^N \bar{x}^N, \quad f_{n+1} = x^N f_n f_n \bar{x}^N, \quad n = 1, \dots, k-1.$$

Then $f_1 \in x^+ \bar{x}^+ = (x^+ \bar{x}^+)^{2^0}$, and assuming by induction that $f_n \in (x^+ \bar{x}^+)^{2^{n-1}}$, we have $f_{n+1} \in x^+ (x^+ \bar{x}^+)^{2^n} \bar{x}^+ = (x^+ \bar{x}^+)^{2^n}$. Thus $f_k \in L (= L(k))$. We shall prove by induction on n that f_k admits a grammatical system of iterative pairs of type $(\alpha_n)^{2^{k-n}}$. The desired conclusion results for $n = k$.

For sake of simplicity, we set $z(n) = 2^{k-n}$. Then for $n = 1, \dots, k$, f_k can be written as

$$f_k = g_{n,0} f_n g_{n,1} f_n \cdots g_{n,z(n)-1} f_n g_{n,z(n)} \quad (7.5)$$

where the words $g_{n,i}$ are defined by:

$$g_{k,0} = g_{k,1} = 1,$$

and for $1 \leq n \leq k-1$:

$$g_{n,0} = g_{n+1,0} x^N, \quad g_{n,z(n)} = \bar{x}^N g_{n+1,z(n+1)}; \quad (7.6)$$

$$g_{n,2i} = \bar{x}^N g_{n+1,i} x^N \quad (0 < 2i < z(n)); \quad (7.7)$$

$$g_{n,2i+1} = 1 \quad (0 < 2i+1 < z(n)).$$

The verification of these formulas is straightforward. We claim that for $n = 1, \dots, k$,

$$\sigma \xrightarrow{*} h_n = g_{n,0} w_{n,1} g_{n,1} w_{n,2} \cdots g_{n,z(n)-1} w_{n,z(n)} g_{n,z(n)}, \quad (7.8)$$

where for $i = 1, \dots, z(n)$, $w_{n,i}$ has the form

$$w_{n,i} = x^{r(n,i)} \xi_{n,i} \bar{x}^{s(n,i)}, \quad (7.9)$$

with $r(n,i), s(n,i) \leq N$, and where $\xi_{n,i}$ is the pivot of a grammatical system of iterative pairs of type α_n of the word f_k . If this assertion holds, then by (7.8), f_k admits a system of type $(\alpha_n)^{z(n)}$ as desired. We verify first the assertion for $n = 1$, by induction on $i = 1, \dots, z(1)$. Assume that

$$\sigma \xrightarrow{*} w = g_{1,0} w_{1,1} \cdots w_{1,i-1} g_{1,i-1} f_1 g_{1,i} f_1 \cdots f_1 g_{1,z(1)},$$

where $w_{1,1}, \dots, w_{1,i-1}$ have the form (7.9). Since $f_1 = x^N \bar{x}^N$, Lemma 7.17 applies to w , and consequently

$$\sigma \xrightarrow{*} g_{1,0} \cdots g_{1,i-1} w_{1,i} g_{1,i} f_1 \cdots f_1 g_{1,z(1)},$$

where $w_{1,i}$ has the form (7.9), and further $\xi_{1,i}$ is the pivot of an iterative pair (of type $e\bar{e} = \alpha_1$) of f_k . This proves the case $n = 1$.

Suppose now that the assertion is true for some $n < k$, and consider the case $n+1$. By the induction hypothesis, (7.8) holds.

Write $h_n = h' h''$, with $h' = g_{n,0} w_{n,1} g_{n,1} w_{n,2} g_{n,2}$. Then in view of (7.6), (7.7) and (7.9),

$$h_n = g_{n+1,0} x^{N+r(n,1)} \xi_{n,1} \bar{x}^{s(n,1)} x^{r(n,1)} \xi_{n,2} \bar{x}^{s(n,2)+N} g_{n+1,1} h'' \quad (7.10)$$

with $h'' = x^N h''$ if $n+1 < k$, and $h'' = h'' (= 1)$ if $n+1 = k$. By (7.10), Lemma 7.17 applies to h_n , and consequently

$$\sigma \xrightarrow{*} g_{n+1,0} w_{n+1,1} g_{n+1,1} h''$$

with $w_{n+1,1}$ described by (7.9). Assume now that

$$\sigma \xrightarrow{*} h = g_{n+1,0} w_{n+1,1} \cdots w_{n+1,i-1} g_{n+1,i-1} x^N w_{n,2i-1} g_{n,2i-1} \cdots w_{n,z(n)} g_{z(n)},$$

for some $i \leq z(n+1)$. Then $h = h' w' h''$, with

$$h' = g_{n+1,0} \cdots g_{n+1,i-1}, \quad w' = x^N w_{n,2i-1} w_{n,2i} \bar{x}^N \quad (7.11)$$

$$h'' = g_{n+1,i} x^N w_{n,2i+1} \cdots w_{n,z(n)} g_{z(n)} \quad \text{or} \quad h'' = 1,$$

according to $i < z(n+1)$ or $i = z(n+1)$. In view of (7.11) and (7.9), Lemma 7.17 can be applied to h , and consequently

$$\sigma \xrightarrow{*} g_{n+1,0} \cdots g_{n+1,i} w_{n+1,i} h'',$$

where $w_{n+1,i}$ satisfies (7.9). Thus the induction step is verified and the proof is achieved. ■

Exercises

7.1 (Boasson) Let S_2 be the symmetric language over $Z = X \cup \bar{X}$, where $X = \{x, y\}$, $\bar{X} = \{\bar{x}, \bar{y}\}$. Let $\sigma: Z^* \rightarrow Z^*$ be the rational substitution defined by $\sigma(x) = x$, $\sigma(y) = y$, $\sigma(\bar{x}) = \bar{x}\bar{X}^*$, $\sigma(\bar{y}) = \bar{y}\bar{X}^*$ and let $\hat{S}_2 = \sigma(S_2)$.

- Show that any nondegenerated iterative pair in $\hat{S}_2$ is left strict but not right strict.
- Show that there are independent systems of iterative pairs of type $I^p \bar{I}^p$ in $\hat{S}_2$ for any $p \geq 1$.
- Show that $\hat{S}_2$ is not a generator of Lin, and that $\hat{S}_2 \notin \bigcup_{n \geq 1} A_n \Gamma$, where the A_n are the

languages of the text. (A similar argument is used in Boasson [1973b] to show that the family Gre is properly contained in Ng(Alg).)

7.2 Let $S = \{x^n y^n \mid n \geq 1\}$. For two languages A, B , define $A \circ B = A'B$, where A' is a copy of A such that $X_{A'} \cap X_B = \emptyset$. Define $S * A = \{x_1^n h x_2^n \mid n \geq 1, h \in A\}$, where x_1, x_2 are letters not in X_A . Let $\mathcal{R}$ be the least family of languages containing S and closed under the operations $\circ$ and $*$. Next define a mapping $\alpha: \mathcal{R} \rightarrow D_1^+ \subset \{e, \bar{e}\}^*$ by: $\alpha(S) = e\bar{e}$, $\alpha(A \circ B) = \alpha(A)\alpha(B)$, $\alpha(S * A) = e\alpha(A)\bar{e}$.

- Show that $A \in \mathcal{R}$ has an independent system of iterative pairs of type $\alpha(A)$. Let $w', w \in D_1^+$. Say that w' is a Dyck-subword of w if $w' = x_1 \cdots x_r$, $w = u_0 x_1 u_1 \cdots u_{r-1} x_r u_r$, $x_1, \dots, x_r \in \{e, \bar{e}\}$, $u_0, \dots, u_r \in \{e, \bar{e}\}^*$ and if for $1 \leq i < j \leq r$, $x_i x_{i+1} \cdots x_j \in D_1^+ \Rightarrow x_i u_i x_{i+1} \cdots u_{j-1} x_j \in D_1^+$.
- Show that for $A, B \in \mathcal{R}$, $A \leq B$ iff $\alpha(A)$ is a Dyck-subword of $\alpha(B)$.

7.3 Show that the language B_n has independent systems of very strict iterative pairs of type α_n .

7.4 Define languages A_k , ($k \geq 1$) by $A_1 = S_2$, and $A_{k+1} = [(a_k, b_k)^*, A_k A'_k]$, where A'_k is a disjoint copy of A_k , and a_k, b_k are new letters. Show that $A_k \in \text{Qrt}(k) \setminus \text{Qrt}(k-1)$ for $k \geq 2$.

7.5 For $k \geq 1$, let $\text{Lin}^{(k)}$ be the family of all languages which are finite unions of products of at most k linear languages.

- Show that $\text{Lin}^{(k)}$ is a principal cone for $k \geq 1$.
- Show that $\text{Lin}^{(k)} \not\subseteq \text{Lin}^{(k+1)}$ for $k \geq 1$, and that the cone $\text{Mlin} = \bigcup_{k \geq 1} \text{Lin}^{(k)}$ is nonprincipal (Mlin is the family of metalinear languages).
- Show that $\text{Mlin} \not\subseteq \text{Lin} \hat{I}$, and that $\text{Mlin} \not\subseteq \text{Ng}(\text{Lin} \hat{I})$. (Hint. Show that $(S_{\leq \#})^+$ is not in Mlin.)

IX Open Problems, Further Developments

Fig. IX.1 summarizes the results concerning cones of context-free languages proved in the preceding chapters. Inclusion is represented by containment. A principal cone is represented by a sharp peak, a nonprincipal one by a rounded peak. There are several question marks in the figure. They refer to open problems which we are going to discuss now:

1. It is unknown whether the full AFL $\text{Ng}(\text{Alg})$ of nongenerators of Alg is principal or not. A positive answer to this question would imply, by Theorem VII.3.5, that $\text{Ng}(\text{Ng}(\text{Alg}))$ is a full AFL closed under substitution. Thus the same question would hold for that full AFL. Thus there may exist a finite or infinite decreasing chain of substitution closed full principal AFLs $\text{Alg} \supsetneq \text{Ng}(\text{Alg}) \supsetneq \text{Ng}(\text{Ng}(\text{Alg})) \supsetneq \dots$, having some similarity with the sequence of powers of the maximal ideal in a local ring. However, it is conjectured (Greibach [1970]) that $\text{Ng}(\text{Alg})$ is nonprincipal.

2. Is there a cone $\mathcal{L}$ of context-free languages containing no nonregular linear (or one counter) language, i.e. such that $\mathcal{L} \cap \text{Lin} = \text{Rat}$ (resp. $\mathcal{L} \cap \text{Roc} = \text{Rat}$)? More generally, say that two cones $\mathcal{L}$ and $\mathcal{M}$ are disjoint if $\mathcal{L} \cap \mathcal{M} = \text{Rat}$. Then the question is: Are there disjoint cones of context-free languages?

3. Call a cone $\mathcal{L}$ minimal if Rat is the only cone properly contained in $\mathcal{L}$. A minimal cone is principal, and $\text{Ng}(\mathcal{L}) = \text{Rat}$. Are there minimal cones of context-free languages? Note that two distinct minimal cones are disjoint. Only a few partial results concerning this question are known. Thus Latteux [1978] proves that the cone generated by $\bar{D}_1^+ = \{x, \bar{x}\}^* \setminus D_1^+$ is minimal among all cones generated by commutative languages. See also Berstel and Boasson [1974].

4. The previous question is closely related to the following. Say that a cone $\mathcal{L}$ covers a cone $\mathcal{M}$ if $\mathcal{M}$ is the maximal cone properly contained in $\mathcal{L}$. Thus a cone is minimal iff it covers Rat. For a principal cone $\mathcal{L}$, $\mathcal{L}$ covers $\text{Ng}(\mathcal{L})$. Are there principal cones $\mathcal{L}$ and $\mathcal{M}$ such that $\mathcal{L}$ covers $\mathcal{M}$? In other terms, is there a principal cone $\mathcal{L}$ such that $\text{Ng}(\mathcal{L})$ is principal? A negative answer would imply a negative answer to both problems 1 and 3. A related question is: Is there a cone $\mathcal{L}$ which contains only finitely many incomparable principal cones?

There are other open problems which are even more closely related to context-free languages.

5. Is the cone S_Γ properly contained in the intersection $\text{Lin} \cap \text{Rocl}$? A related question is: Is the intersection of two principal cones of context-free languages always a principal cone? (For a negative answer to a related problem, see Ullian [1971].) Another question is: Is there a least principal cone containing a given family of context-free languages?

6. Consider a language L which dominates all quasi-rational languages. Is L a generator of Alg ? In other terms, let $\mathcal{L}$ be a principal cone containing Qrt . Is it true that then $\mathcal{L}$ contains Alg ? Same question for the family Fcl of finite counter languages.

There are some results concerning the modification of the hierarchies represented in Fig. IX.1 when the attention is restricted to some cutset of the

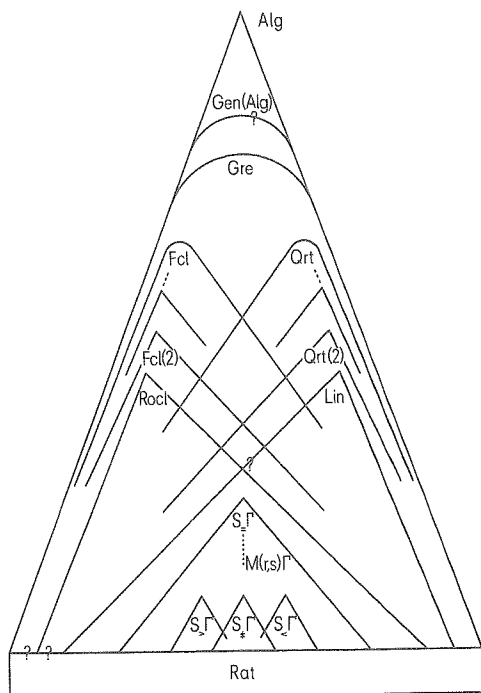


Fig. IX.1

context-free languages characterized by an additional restriction. Thus consider the family Irs of context-free languages that contain no infinite regular set (i.e. satisfying the IRS-condition described in Section V.3). S. Greibach [1975] proves that $\text{Irs} \cap \text{Gre} = \text{Irs} \cap \text{Qrt}$. This implies in particular that any generator

of Rocl contains an infinite regular set (since such a generator is not quasi-rational by Theorem VIII.7.14). Along these lines, let Idk be the family of these languages which are rationally equivalent to a language of the form $D_n^* \cap K$ for some $n \geq 1$, and some regular language K . Then Beauquier [1973] shows that for $L \in \text{Idk}$, either $\text{Rocl} \subseteq L\Gamma$ or $L\Gamma \subseteq \text{Qrt}$. Note that this result is related to problem 6.

We now discuss some developments which were not included in the preceding chapters, and which are closely related to the topics we are concerned with. Observe that the classification of context-free languages via cones and full AFLs is a classification of languages, in opposition to a classification of machines (acceptors) or of generating devices (grammars). In fact, there exists a theory of AFAs (Abstract Families of Acceptors) which is entirely parallel to the theory of full AFLs. For these results, the reader is referred to the book of Ginsburg [1975]. Up to now, no characterization of the family of context-free grammars generating the languages of a cone is known. The notions of grammar form and of family of grammars introduced in Cremers and Ginsburg [1974] mainly apply to subfamilies of quasi-rational languages.

For some purposes, the concept of cone is too large. Thus the deterministic and the unambiguous context-free languages are closed under inverse morphism and intersection with regular sets, but are not closed under morphism. Therefore, these important families are not cones. This leads to the following weakened version of a cone: A cylinder is a family of languages closed under inverse morphism and intersection with regular languages. There is another reason why cylinders are interesting: cylinders preserve complexity of recognition. More precisely, consider a language L . If one has an algorithm A for deciding membership in L (say on a nondeterministic Turing machine) then for a language L' of the form $L' = \varphi^{-1}(L)$ or $L' = L \cap K$, where φ is a morphism and K is a regular language, one can easily obtain an algorithm A' for deciding membership in L' such that the order of running time of A' is the same as the order of running time of A . (Thus for $L' = \varphi^{-1}(L)$, A' is simply the following algorithm: For a word f' , compute first $f = \varphi(f')$ and then apply A to f .) Similar considerations hold for space complexity. In this sense, L is "harder" to analyze than L' (since there may exist other algorithms for L' which are faster than A'). In other terms, the language L is the "hardest" language in the cylinder generated by L . The question whether a given cylinder $\mathcal{L}$ is principal thus is equivalent to whether there exists a "hardest" language in $\mathcal{L}$. Greibach [1973] has given a hardest context-free language. Autebert [1977b] and Boasson and Nivat [1977] have proved that neither the cone of restricted one counter languages, nor the cone of linear languages is a principal cylinder. For a general method, see Autebert [1977a]. The techniques are similar to those exposed in the previous chapters. Thus the theory of transductions and of abstract families of languages serves as starting point for further developments.

Bibliography

Expository texts on formal languages include Aho and Ullman [1972], Autebert and Cousineau [1976], Becker and Walter [1977], Eilenberg [1974], Ginsburg [1966], Hopcroft and Ullman [1969], Hotz and Walter [1968/1969], Hotz and Claus [1972], Maurer [1977], Salomaa [1969a], [1973]. Salomaa [1973] contains a list of books on formal languages and automata theory up to March 1972. Ginsburg [1975] is a treatise on AFL theory. For rational transductions and rational functions, see Eilenberg [1974].

Aho, A. V.; Ullman, J. D. [1972]: *The Theory of Parsing, Translation and Compiling*, Vol. I. Englewood Cliffs, N.J. 1972

Alt, H. [1977]: Eine untere Schranke für den Platzbedarf bei der Analyse beschränkter kontextfreier Sprachen. In: *Theoretical Computer Science*, 3rd GI Conference. Berlin-Heidelberg-New York 1977. = *Lecture Notes in Computer Science*, vol. 48, 123-131

Alt, H.; Mehlhorn, K. [1976]: Lower bounds for the space complexity of context-free recognition. In: Michaelson, S.; Milner, R. (eds.): *Automata, Languages and Programming*, Third International Colloquium, Edinburgh 1976, 338-354

Amar, V.; Putzolu, G. [1965]: Generalizations of regular events. *Inform. and Control* 8 (1965) 56-63

Anissimov, A. W.; Seifert, F. D. [1975]: Zur algebraischen Charakteristik der durch kontext-freie Sprachen definierten Gruppen. *Elektron. Inform. Verarb. u. Kybern.* 11 (1975) 695-702

Autebert, J. M. [1973]: Quelques générateurs des langages algébriques. In: Böhlting, K. H.; Indermark, K. (eds.): 1. Fachtagung über Automatentheorie und Formale Sprachen, Bonn. Berlin-Heidelberg-New York 1977. = *Lecture Notes in Computer Science*, vol. 2, 124-131

— [1977a]: Push-down automata and families of languages generating cylinders. In: Gruska, J. (ed.): *Mathematical Foundations of Computer Science 1977*. Berlin-Heidelberg-New York 1977. = *Lecture Notes in Computer Science*, vol. 53, 231-239

— [1977b]: Non-principalité du cylindre des langages à compteur. *Math. Syst. Theory* 11 (1977), 157-167

Autebert, J. M.; Beauquier, J. [1974]: Une caractérisation des

générateurs standard. *Rev. franç. d'Automat. Informat. et Rech. Opérationn.* 8è Ann. (1974) R-1, 63-83

Autebert, J. M.; Cousineau, G. [1976]: *Théorie des automates et des langages formels: I. Les langages algébriques*. Institut de Programmation, Université de Paris 1976

Beauquier, J. [1973]: Une caractérisation des langages quasi-rationnels standards. In: Böhlting, K. H.; Indermark, K. (eds.): 1. Fachtagung über Automatentheorie und Formale Sprachen, Bonn. Berlin-Heidelberg-New York 1977. = *Lecture Notes in Computer Science*, vol. 2, 132-138

— [1976a]: Une propriété de non-ambiguïté des générateurs algébriques. *C. R. Acad. Sci. Paris. Sér. A*, 282 (1976) 1203-1205

— [1976b]: Générateurs algébriques non-ambigus. In: Michaelson, S.; Milner, R. (eds.): *Automata, Languages and Programming*. Third International Colloquium, Edinburgh 1976, 66-73

— [1977]: Contribution à l'étude de la complexité structurelle des langages algébriques. Thèse d'Etat, Université Paris VII, 1977

— [1978a]: Générateurs algébriques et systèmes de paires itérantes. *Theor. Comput. Sci.* (to appear)

— [1978b]: A remark about the syntactic lemma (submitted for publication)

Becker, H., Walter, H. [1977]: *Formale Sprachen*. Braunschweig-Wiesbaden 1977

Benois, M. [1969]: Parties rationnelles du groupe libre. *C. R. Acad. Sci. Paris, Sér. A*, 269 (1969) 1188-1190

Benois, M.; Nivat, M. [1972]: Congruences parfaites et quasi-parfaites. *Sémin. Dubreil*, 25è Ann., 1971/1972, Université de Paris

Berstel, J. [1973]: Une hiérarchie des parties rationnelles de N^2 . *Math. Syst. Theory* 7 (1973) 114-137

— [1974]: Sur une conjecture de S. Greibach. *Acta Informatica* 3 (1974) 293-295

Berstel, J.; Boasson, L. [1974]: Une suite décroissante de cônes rationnels. In: Loeckx, J. (ed.): *Automata, Languages and Programming*, 2nd Colloquium. Berlin-Heidelberg-New York 1974. = *Lecture Notes in Computer Science*, vol. 14, 383-397

Blattner, M.; Head, T. [1977]: Single valued a -transducers. *J. of Comput. and Syst. Sci.* 15 (1977) 310-327

Boasson, L. [1973a]: Two iteration theorems for some families of languages. *J. Comput. and Syst. Sci.* 7 (1973) 583-596

— [1973b]: The inclusion of the substitution closure of linear and one-counter languages in the largest sub AFL of the family of CFL's is proper. *Inform. Process. Lett* 2 (1973) 135-140

- [1976]: *Langages algébriques, paires itérantes et transductions rationnelles*. *Theor. Comput. Sci.* **2** (1976) 209–223
- Boasson, L.; Crestin, J. P.; Nivat, M. [1973]: Familles de langages translatables et fermées par crochet. *Acta Informatica* **2** (1973) 383–393
- Boasson, L.; Nivat, M. [1977]: Le cylindre des langages linéaires. *Math. Syst. Theory* **11** (1977) 147–155
- Boë, J. M. [1976]: Représentations des monoïdes: Applications à la théorie des codes. Thèse 3e cycle, Montpellier 1976
- Boë, J. M.; Boyat, J.; Cesari, Y.; Lacheney, A.; Vincent, M. [1978]: Automates et monoïdes syntaxiques des sous-monoïdes libres. *Inform. and Control* (to appear)
- Cesari, Y. [1974]: Sur l'application du théorème de Suschkewitsch à l'étude des codes rationnels complets. In: Loeckx, J. (ed.): *Automata, Languages and Programming*, 2nd Colloquium. Berlin-Heidelberg-New York 1974. = *Lecture Notes in Computer Science*, vol. 14, 342–350
- Choffrut, Ch. [1977]: Une caractérisation des fonctions séquentielles et des fonctions sous-séquentielles en tant que relations rationnelles. *Theor. Comput. Sci.* **5** (1977), 325–338
- [1978]: Contribution à l'étude de quelques familles remarquables de fonctions rationnelles, Thèse d'Etat, Université Paris VII, Paris 1978
- Cochet, Y.; Nivat, M. [1971]: Une généralisation des ensembles de Dyck. *Israel J. of Math.* **9** (1971) 389–395
- Conway, J. H. [1971]: *Regular Algebra and Finite Machines*. London 1971
- Cremers, A.; Ginsburg, S. [1975]: Context-free grammar forms. *J. Comput. and Syst. Sci.* **11** (1975) 86–117
- Crestin, J. P. [1978]: *Langages quasi-rationnels*. In: Crestin, J. P.; Nivat, M. (eds.): *Langages algébriques*, Ecole Nationale Supérieure des Techniques Avancées, Paris, 1978, 123–166
- Davis, M. [1958]: *Computability and Unsolvability*. New York 1958
- Eilenberg, S. [1967]: *Algèbre catégorique et théorie des automates*. Institut H. Poincaré, Université de Paris, 1967
- [1974]: *Automata, Languages and Machines*, vol. A. New York-San Francisco-London 1974
- [1978]: *Automata, Languages and Machines*, vol. C (in preparation).
- Elgot, C. C.; Mezei, G. [1965]: On relations defined by generalized finite automata. *IBM J. of Res. and Dev.* **9** (1965) 47–65
- Fischer, P. C.; Rosenberg, A. L. [1968]: Multitape one-way nonwriting automata. *J. of Comput. and Syst. Sci.* **2** (1968) 88–101
- Fliess, M. [1971]: Deux applications de la représentation matricielle d'une série rationnelle non commutative. *J. of Algebra* **19** (1971) 344–353

- Ginsburg, S. [1966]: *The Mathematical Theory of Context-Free Languages*. New York 1966
- [1975]: *Algebraic and Automata-Theoretic Properties of Formal Languages*. Amsterdam-New York-Oxford 1975
- Ginsburg, S.; Greibach, S. A. [1969]: Abstract families of languages. In: *Studies in Abstract Families of Languages*. *Mem. of the Amer. Math. Soc.* **87** (1969) 1–32
- [1970]: Principal AFL. *J. of Comput. and Syst. Sci.* **4** (1970) 308–338
- Ginsburg, S.; Greibach, S. A.; Hopcroft, J. E. [1969]: Pre-AFL. In: *Studies in Abstract Families of Languages*. *Mem. of the Amer. Math. Soc.* **87** (1969) 41–51
- Ginsburg, S.; Rose, G. F. [1966]: A characterization of machine mappings. *Can. J. of Math.* **18** (1966) 381–388
- Ginsburg, S.; Spanier, E. H. [1968]: Derivation-bounded languages. *J. of Comput. and Syst. Sci.* **2** (1968) 228–250
- [1970]: Substitutions in families of languages. *Inform. Sci.* **2** (1970) 83–110
- Goldstine, J. [1972]: Substitution and bounded AFLs. *J. of Comput. and Syst. Sci.* **6** (1972) 9–29
- Greibach, S. A. [1969]: An infinite hierarchy of context-free languages. *J. of the Assoc. of Comput. Mach.* **16** (1969) 91–106
- [1970]: Chains of full AFLs. *Math. Syst. Theory* **4** (1970) 231–242
- [1972]: Syntactic operators on full semi-AFLs. *J. of Comput. and Syst. Sci.* **6** (1972) 30–76
- [1973]: The hardest context-free language. *SIAM J. of Computing* **2** (1973) 304–310
- [1975]: One-counter languages and the IRS condition. *J. of Comput. and Syst. Sci.* **10** (1975) 237–247
- Greibach, S. A.; Hopcroft, J. E. [1969]: Independence of AFL operations. In: *Studies in Abstract Families of Languages*. *Mem. of the Amer. Math. Soc.* **87** (1969) 33–40
- Gruska, J. [1971a]: A characterization of context-free languages. *J. of Comp. and Syst. Sci.* **5** (1971) 353–364
- [1971b]: A few remarks on the index of context-free grammars and languages. *Inform. and Control* **19** (1971) 216–223
- Hopcroft, J.; Ullman, J. [1969]: *Formal Languages and Their Relation to Automata*. Reading, MA-Don Mills, Ont.-London-Amsterdam-Sydney 1969
- Hotz, G.; Claus, V. [1972]: *Automatentheorie und formale Sprachen III*. Mannheim-Wien-Zürich 1972. = B.I. Hochschultaschenbücher, vol. 823
- Hotz, G.; Messerschmidt, J. [1974]: Dyck-Sprachen sind in Bandkomplexität $\log n$ analysierbar. *Tech. Ber. Universität des Saarlandes*, 1974.

- Hotz, G.; Walter, H. [1968/69] *Automatentheorie und formale Sprachen I, II*. Mannheim 1968, 1969. = B. I. Hochschultaschenbücher, vol. 821, 822
- Kleene, S. C. [1956]: Representation of events in nerve nets and finite automata. In: Shannon, C. E.; McCarthy, J. (eds.): *Automata Studies*. Princeton, N.J. 1956, 3-40
- McKnight Jr., J. D. [1964]: Kleene quotient theorems. *Pac. J. of Math.* **14** (1964) 1343-1352
- McKnight Jr., J. D.; Storey, A. J. [1969]: Equidivisible semigroups. *J. of Algebra* **12** (1969) 24-48
- Latteux, M. [1977]: Produit dans le cône rationnel engendré par D_1^* . *Theor. Comput. Sci.* **5** (1977) 129-134
- [1978]: Cônes rationnels commutatifs. *J. of Comput. and Syst. Sci.* (to appear)
- Lewis, D. J. [1970]: Closure of families of languages under substitution operators. In: *Proc. of the 2nd Annual ACM Symp. on Theory of Computing* 1970, 100-108
- Maeda, F.; Maeda, S. [1974]: *Theory of Symmetric Lattices*. Berlin-Heidelberg-New York 1974. = *Grundlehren der math. Wiss.*, vol. 173
- Magnus, W.; Karrass, A.; Solitar, D. [1966]: *Combinatorial Group Theory*. New York-London-Sydney 1966
- Maurer, H. [1977]: *Theoretische Grundlagen der Programmiersprachen*. Repr. Mannheim-Wien-Zürich 1977
- Nivat, M. [1967]: *Transductions des langages de Chomsky*. Thèse d'Etat, Université de Paris, 1967
- [1968]: Transductions des langages de Chomsky. *Ann. de l'Inst. Fourier* **18** (1968) 339-456
- [1970]: On some families of languages related to the Dyck language. In: *Proc. of the 2nd Annual ACM Symp. on Theory of Computing*, 1970, 221-225
- [1975]: Opérateurs sur les familles de langages. *Rapp.* 106, IRIA, France, 1975
- Ogden, W. [1968]: A helpful result for proving inherent ambiguity. *Math. Syst. Theory* **2** (1968) 191-194
- Perrin, D.; Schützenberger, M. P. [1977]: Codes et sous-monoïdes possédant des mots neutres. In: *Theoretical Computer Science*, 3rd GI Conference. Berlin-Heidelberg-New York 1977. = *Lecture Notes in Computer Science*, vol. 48, 270-281
- Perrot, J. F.; Sakarovitch, J. [1977]: A theory of syntactic monoids for context-free languages. In: Gilchrist, B. (ed.): *Information Processing 77*, IFIP. Amsterdam-New York-Oxford 1977, 69-72

- Rosenberg, A. L. [1967]: A machine realization of the linear context-free languages. *Inform. and Control* **10** (1967) 175-188
- Sakarovitch, J. [1977]: Sur les groupes infinis, considérés comme monoïdes syntaxiques des langages formels. In: *Séminaire P. Dubreil 1975/76*. Berlin-Heidelberg-New York 1977. = *Lecture Notes in Mathematics*, vol. 586, 168-179
- Salomaa, A. [1969a]: *Theory of Automata*. Oxford-New York-Toronto-Sydney 1969
- [1969b]: On the index of a context-free grammar and language. *Inform. and Control* **14** (1969) 474-477
- [1973]: *Formal Languages*. New York-San-Francisco-London 1973
- Salomaa, A.; Soittola, M. [1978]: *Automata-Theoretic Aspects of Formal Power Series*. Berlin-Heidelberg-New York 1978
- Schnorr, C. P. [1974]: *Rekursive Funktionen und ihre Komplexität*. Stuttgart 1974. = *Teubner Studienbücher Informatik. Leitfäden der angewandten Mathematik und Mechanik*, vol. 24
- Schützenberger, M. P. [1961a]: Some remarks on Chomsky's context-free languages. *M.I.T. Res. Lab. Electron. Quart. Prog. Rept.* 63, 1961
- [1961b]: A remark on finite transducers. *Inform. and Control* **4** (1961) 185-196
- [1973]: Sur un langage équivalent au langage de Dyck. In: Suppes, P. et al. (ed.): *Logic, Methodology and Philosophy of Science IV*. Amsterdam-New York-Oxford 1973, 197-203
- [1975]: Sur les relations rationnelles. In: Brakhage, H. (ed.): *Automata Theory and Formal Languages*, 2nd GI Conference. Berlin-Heidelberg-New York 1975. = *Lecture Notes in Computer Science*, vol. 33, 209-213
- [1976]: Sur les relations rationnelles entre monoïdes libres. *Theor. Comput. Sci.* **3** (1976) 243-259
- [1977a]: Sur une variante des fonctions séquentielles. *Theor. Comput. Sci.* **4** (1977) 47-57
- [1977b]: Une propriété de Hankel des relations fonctionnelles entre monoïdes libres. *Advances in Math.* **24** (1977) 274-280
- Ullian, J. S. [1971]: Three theorems concerning principal AFL. *J. of Comput. and Syst. Sci.* **5** (1971) 304-314
- Vogel, H. [1972]: *Zur Theorie der rationalen und deterministischen Mengen*. *Mitt. der Gesell. f. Math. Datenverarb.* **18** (1972)
- Walljasper, S. J. [1970]: *Nondeterministic automata and effective languages*. Ph. D. Thesis, University of Iowa, 1970
- Yntema, M. K. [1967]: Inclusion relations among families of context-free languages. *Inform. and Control* **10** (1967) 572-597

List of Symbols

$\mathbb{N}, \mathbb{Z}$	9	G_θ	9
$\mathfrak{P}(E)$	9	S_n	9
$A \setminus B$	9	$S_-, S_<, S_\leq,$	
$P * Q$	232	$S_>, S_\geq, S_\neq$	
$ u , u _x, u _Y$	10	$\rightarrow, \xrightarrow{p}, \Rightarrow, \rightarrowtail$	
$\tilde{u}$	10	$\vdash_T, \vdash_T^*$	
$u \wedge v, \bigwedge A$	104	$=$	
$\ u, v\ $	104	$\stackrel{k}{=}, \stackrel{\pm}{=}$	
$\oplus$	75	$L_G, \hat{L}_G$	
$\ k$	75, 169	$\psi(G), \varphi^{-1}(G)$	
$\sqcup$	74	G_K	
A^+, A^*	10	Δ	
$B^{-1}A$	11	$\text{Exp}(\pi, L)$	
$X^\oplus$	15	$\chi(\pi, L)$	
$X_n^{(*)}$	43	$\text{Exp}(\theta, L)$	
$[A, M]$	154	$\chi(\theta, L)$	
$L \uparrow M$	148	$\text{Diag}(\theta, L)$	
$A \geq B, A > B,$		$\pi * \theta, \theta_1 \times \theta_2$	
$A \approx B$	135	Γ	
$\delta_n, \delta'_n, \delta_I$	36	$\hat{\Gamma}$	
$D_n, D'_n, D_n^*, D_n'^*$	36	Φ, Φ^{-1}	
D_I, D_I^*	36	$\Phi_a, \Phi_a^{-1}, \Phi_\pi, \Phi_\pi^{-1}$	
$\mathcal{L}$	47	I_R	
E	49	$\bar{M}, \underline{\mathcal{L}}$	
E_n	188	$\underline{\text{Rat}}$	

138	$\mathcal{L} \sqcap \mathcal{M}$	145
151	$\mathcal{L} \vee \mathcal{M}$	138
	$\mathcal{L} \wedge \mathcal{M}$	177
151	$\hat{\mathcal{L}}$	184
23	$\text{Gen}(\mathcal{L}), \text{Ng}(\mathcal{L})$	198
37	$\text{Rec}(M)$	52
201	$\text{Rat}(M)$	55
202	Σ	134
23	$\hat{\Sigma}$	135
31	$\mathbb{F}$	162
32	Alg	134
219	Elm	134
219	$\text{Fcl}, \text{Fcl}(k)$	199
220	Fin	134
233	Gre	200
233	$\text{Ind}(k)$	211
233	Irs	266
233	Lin	150
136	Mlin	264
145	Nexp	209
164	Ocl	202
165	$\text{Qrt}, \text{Qrt}(k)$	209
165	Rat	134
145	Rocl	202
139		

Index

abstract family of languages (AFL)	context-free language 24
141	— — substitution 31
accessible state 18	continuous morphism 13
addition 74, 99	— transduction 87
algebraic grammar 22, 71	copy 13, 62
— language 24	cross-section 111
— subset 71	cylinder 267
— transduction 71	
alphabet 10, 134	deduced iterative pair 225
alphabetic morphism 13	— system of iterative pairs 241
automaton, accessible part 18	derivation 23
—, finite 16, 55	— bounded language 199, 208
—, minimal 18	—, index of a 211
—, nondeterministic 17	—, length of a 23
—, semi- 18, 108	—, proper 23
bifix code 11	diagonal 219
bimachine 123	distance of languages 15
—, state complete 124	— of words 104
bimorphism 62	domination, rational 135
bounded variation 105	—, strict 135
bracket 154, 217	Dyck congruence 36
	— language 36, 187, 203, 228
closure operator 164	— —, restricted 36, 184, 199, 221,
code, prefix, suffix, bifix 11	233, 236, 251, 259
computation 78, 201	— primes 36
cone, disjoint 265	— reduction 37
—, generator 137, 198	— -subword 264
—, minimal 265	
—, nongenerators 198	equations, algebraic 26
—, principal 137	—, equivalent 29
—, rational 136	—, right linear 64
configuration 201	—, solution of 27
congruence 14	—, system of 26
—, saturated 52	extensive operator 164
—, syntactic 15	
context-free grammar 22	factor, left, right, proper 11
	faithful transduction 87

- family of languages 134
 - — —, abstract (AFL) 141
 - — —, finite 135
 - — —, incomparable 135
 - — —, rationally closed 138
- finite counter language 199
- free commutative monoid 15
 - group 43
 - monoid 10
- full AFL 141
 - — generator 142
 - —, principal 142
 - semi-AFL 141
 - trio 136
- function, (left) sequential 97
 - , length preserving 123, 127
 - , rational 92
 - , right sequential 98
 - , subsequential 100
 - with bounded variation 105
- generator of a cone 137, 198
 - — — full AFL 142
- grammar, algebraic, context-free 22, 71
 - , index of a 211
 - , linear 150
 - , proper 30
 - , reduced 34
 - , strict 28
 - , strictly reduced 34
- grammatical iterative pair 223
 - system of iterative pairs 238
 - type 248
- idempotent operator 164
- incomparable families of languages 135
- independent system of iterative pairs 234
- index of a derivation 211
 - — — grammar 211
 - — — language 211
- input label 78
- inverse transduction 65
- IRS-condition 140, 266
- Iteration lemma for algebraic grammars 34
 - — — — languages 33
 - — — linear languages 155
 - — — rational relations 63
 - — — regular languages 20
- iterative pair, bounded 222
 - —, deduced 225
 - —, degenerated 220
 - —, grammatical 223
 - —, pivot of an 223
 - —, strict, left strict, right strict 220
 - —, underlying 233
 - —, very strict 220
- label 78
 - , input 78
 - , output 78
- language 10, 134
 - , algebraic, context-free 24
 - , derivation bounded 199, 208
 - , finite counter 199
 - , index of a 211
 - , linear 150
 - , local regular 18
 - , Lukasiewicz 47, 202
 - , marked 178
 - , metalinear 264
 - , nonexpansive 199, 209
 - of arithmetic expressions 49, 188
 - — palindromes 156
 - — sentential forms 23
 - , one counter 202
 - , quasi-rational 199, 209
 - , rational 56
 - , recognizable 16
 - , regular 16
 - , restricted one counter 199, 202
 - , standard matching choice 199, 208

- language, symmetric 151, 184, 221, 235, 256
- length of a system of iterative pairs 233
 - — — word 10
 - preserving function 123, 127
- linear grammar 150
 - language 150
- local regular language 18
- locally finite 163
- Lukasiewicz language 47, 202
- marked language 178
 - $\mathcal{M}$ -substitution 178
- marking operator 178
- matrix representation 81
 - , normalised 93
 - , trim 86
 - with twinning property 128
- metalinear language 264
- minimal automaton 18
 - cone 265
- morphism 12
 - , alphabetic 13
 - , continuous, ε -free 13
 - , semigroup 12, 81
 - , semimonomial 117
 - , strictly alphabetic 13
 - , summed up 121
 - , unambiguous 117
 - , (0, 1)- 117
- $\mathcal{M}$ -substitution 145
- nondeterministic automaton 17
- nonexpansive language 199, 209
- nongenerators 198
- norm of a language 15
- normalized matrix representation 93
- one counter language 202
- operator 163
 - , closure 164
 - , extensive 164
 - , idempotent 164
- operator, marking 178
- output label 78
- path, successful 78
- pivot of an iterative pair 223
 - — a system of iterative pairs 238
- prefix code 11
- prime system of iterative pairs 252
- principal cone 137
 - full AFL 142
- production 22
- projection 13
- pushdown automaton, one counter 201
- quasi-rational language 199, 209
 - — relation 217
- quotient, left, right 11
- rank of a quasi-rational language 199, 209
- rational domination 135
 - expression 55
 - function 92
 - image 135
 - relation 61, 63
 - subset 55
 - transduction 65, 67
- recognizable language 16
 - relation 61
 - subset 52
 - transduction 72
- reduced grammar 34
- regular language 16
 - substitution 17
- relation 14
 - , quasi-rational 217
 - , rational 61, 63
 - , recognizable 61
- restricted Dyck language 36, 184, 199, 221, 233, 236, 251, 259
- one counter language 199, 202
- reversal of a transduction 66



- right linear system of equations 64
 - sequential function 98
 - — transducer 98
 - — transduction 98
- rule 201
- segment 11
- semiautomaton 18, 108
- semigroup 9
- semilinear subset 56
- semimonomial morphism 117
- semiring 11
- sequential function 97
 - transducer 96
 - transduction 97
- set of exponents 219
- shuffle 74
- standard matching choice language
 - 199, 208
- starheight 58
- strict grammar 28
- strictly alphabetic morphism 13
 - reduced grammar 34
- subsequential function 100
 - transducer 100
- subset, algebraic 71
 - , rational 55
 - , recognizable 52
 - , semilinear 56
 - , unambiguous rational 123
- substitution 13
 - , context-free 31
 - , $\mathcal{M}$ - 145
 - , marked $\mathcal{M}$ - 178
 - , regular 17
 - , syntactic 148
- subword 11
- successful path 78
- suffix code 11
- symmetric language 151, 184, 221, 235, 256
- syntactic congruence 15
 - monoid 15
- syntactic substitution 148
- system, deduced 241
 - , grammatical 238
 - , independent 234
 - , length of a 233
 - , of iterative pairs 233
 - , pivot of a 238
 - , prime 252
 - , type of a 233
 - , very strict 249
- transducer 77
 - , right sequential 98
 - , sequential 96
 - , subsequential 100
 - , unambiguous 114
- transduction 65
 - , algebraic 71
 - , continuous 87
 - , faithful 87
 - , inverse 65
 - , recognizable 72
 - , reversal 66
 - , right sequential 97
 - , sequential 98
- transition, authorized, forbidden 19
- trim matrix representation 86
- twinned states 128
- twinning property 128
- type of an iterative pair 220
 - — a system of iterative pairs 233
- unambiguous morphism 117
 - rational subset 123
 - transducer 114
- underlying pair 233
- unitary operator 163
- variable 22
- very strict system of iterative pairs
 - 249
- word 10
 - , conjugate 12
 - , primitive- 12

Mathematik

Ahlsweide/Wegener: **Suchprobleme**

328 Seiten. DM 28,80

Ansorge: **Differenzenapproximationen partieller Anfangswertaufgaben**

298 Seiten. DM 29,80 (LAMM)

Böhmer: **Spline-Funktionen**

Theorie und Anwendungen. 340 Seiten. DM 28,80

Clegg: **Variationsrechnung**

138 Seiten. DM 17,80

Collatz: **Differentialgleichungen**

Eine Einführung unter besonderer Berücksichtigung der Anwendungen

5. Aufl. 226 Seiten. DM 24,80 (LAMM)

Collatz/Krabs: **Approximationstheorie**

Tschebyscheffsche Approximation mit Anwendungen. 208 Seiten. DM 28,—

Constantinescu: **Distributionen und ihre Anwendung in der Physik**

144 Seiten. DM 18,80

Fischer/Sacher: **Einführung in die Algebra**

2. Aufl. 240 Seiten. DM 18,80

Grigorieff: **Numerik gewöhnlicher Differentialgleichungen**

Band 1: Einschrittverfahren. 202 Seiten. DM 16,80

Band 2: Mehrschrittverfahren. 411 Seiten. DM 29,80

Hainzl: **Mathematik für Naturwissenschaftler**

2. Aufl. 311 Seiten. DM 29,— (LAMM)

Hässig: **Graphentheoretische Methoden des Operations Research**

160 Seiten. DM 26,80 (LAMM)

Hilbert: **Grundlagen der Geometrie**

12. Aufl. VII, 271 Seiten. DM 24,80

Jaeger/Wenke: **Lineare Wirtschaftsalgebra**

Eine Einführung

Band 1: vergriffen

Band 2: IV, 160 Seiten. DM 19,80 (LAMM)

Jeggle: **Nichtlineare Funktionalanalysis**

Existenz von Lösungen nichtlinearer Gleichungen. 255 Seiten. DM 24,80

Kall: **Mathematische Methoden des Operations Research**

Eine Einführung. 176 Seiten. DM 22,80 (LAMM)

Kochendörffer: **Determinanten und Matrizen**

IV, 148 Seiten. DM 17,80

Kohlas: **Stochastische Methoden des Operations Research**

192 Seiten. DM 24,80 (LAMM)

Krabs: **Optimierung und Approximation**

208 Seiten. DM 25,80

Fortsetzung auf der 3. Umschlagseite

Mathematik Fortsetzung

Rauhut/Schmitz/Zachow: **Spieltheorie**

Eine Einführung in die mathematische Theorie strategischer Spiele

400 Seiten. DM 28,80 (LAMM)

Stiefel: **Einführung in die numerische Mathematik**

5. Aufl. 292 Seiten. DM 26,80 (LAMM)

Stiefel/Fässler: **Gruppentheoretische Methoden und ihre Anwendung**

Eine Einführung mit typischen Beispielen aus Natur- und Ingenieurwissenschaften

256 Seiten. DM 25,80 (LAMM)

Stummel/Hainer: **Praktische Mathematik**

299 Seiten. DM 28,80

Topsøe: **Informationstheorie**

Eine Einführung. 88 Seiten. DM 12,80

Velte: **Direkte Methoden der Variationsrechnung**

Eine Einführung unter Berücksichtigung von Randwertaufgaben bei partiellen

Differentialgleichungen. 198 Seiten. DM 25,80 (LAMM)

Walter: **Biomathematik für Mediziner**

148 Seiten. DM 15,80

Witting: **Mathematische Statistik**

Eine Einführung in Theorie und Methoden. 3. Aufl. 223 Seiten. DM 26,80 (LAMM)

Preisänderungen vorbehalten



REG. 18.345

SIG. 519.7 Ber