AUTOMATA, LANGUAGES, AND MACHINES

Volume B

SAMUEL EILENBERG

AUTOMATA, LANGUAGES, AND MACHINES

VOLUME B

Pure and Applied Mathematics

A Series of Monographs and Textbooks

RECENT TITLES

T. BENNY RUSHING. Topological Embeddings

JAMES W. VICK. Homology Theory: An Introduction to Algebraic Topology

E. R. KOLCHIN. Differential Algebra and Algebraic Groups

GERALD J. JANUSZ. Algebraic Number Fields

A. S. B. HOLLAND. Introduction to the Theory of Entire Functions

WAYNE ROBERTS AND DALE VARBERG. Convex Functions

A. M. OSTROWSKI. Solution of Equations in Euclidean and Banach Spaces, Third Edition of Solution of Equations and Systems of Equations

H. M. EDWARDS. Riemann's Zeta Function

SAMUEL EILENBERG. Automata, Languages, and Machines: Volumes A and B

MORRIS HIRSCH AND STEPHEN SMALE. Differential Equations, Dynamical Systems, and Linear Algebra

WILHELM MAGNUS. Noneuclidean Tesselations and Their Groups

FRANÇOIS TREVES. Basic Linear Partial Differential Equations

WILLIAM M. BOOTHBY. An Introduction to Differentiable Manifolds and Riemannian Geometry

BRAYTON GRAY. Homotopy Theory: An Introduction to Algebraic Topology

ROBERT A. ADAMS. Sobolev Spaces

JOHN J. BENEDETTO. Spectral Synthesis

D. V. WIDDER. The Heat Equation

IRVING EZRA SEGAL. Mathematical Cosmology and Extragalactic Astronomy

J. DIEUDONNÉ. Treatise on Analysis: Volume II, enlarged and corrected printing; Volume IV

WERNER GREUB, STEPHEN HALPERIN, AND RAY VANSTONE. Connections, Curvature, and Cohomology: Volume III, Cohomology of Principal Bundles and Homogeneous Spaces

In preparation

I. MARTIN ISAACS. Character Theory of Finite Groups

K. D. STROYAN AND W. A. J. LUXEMBURG. Introduction to the Theory of Infinitesimals

JAMES R. BROWN. Ergodic Theory and Topological Dynamics

CLIFFORD A. TRUESDELL. A First Course in Rational Continuum Mechanics: Volume 1, General Concepts

MELVYN BERGER. Nonlinearity and Functional Analysis: Lectures on Nonlinear Problems in Mathematical Analysis

AUTOMATA, LANGUAGES, AND MACHINES

VOLUME B

Samuel Eilenberg

COLUMBIA UNIVERSITY
NEW YORK

With two chapters by

Bret Tilson

CITY UNIVERSITY OF NEW YORK
QUEENS COLLEGE
NEW YORK

ACADEMIC PRESS New York San Francisco London 1976

A Subsidiary of Harcourt Brace Jovanovich, Publishers

ACADEMIC PRESS, INC.
111 Fifth Avenue, New York, New York 10003

United Kingdom Edition published by
ACADEMIC PRESS, INC. (LONDON) LTD.
24/28 Oval Road, London NW1

Library of Congress Cataloging in Publication Data

Eilenberg, Samuel.
Automata, languages, and machines.

(Pure and applied mathematics: a series of monographs and textbooks)
Vol. B includes two chapters by Bret Tilson.
Includes bibliographies.
1. Sequential machine theory. 2. Formal languages. 3. Automata. I. Title. II. Series.
QA3P8 vol. 59 510'.8s [629.8'91] 72-88333
ISBN 0-12-234002-7 (pt. B.)

PRINTED IN THE UNITED STATES OF AMERICA

Contents

CHAPTER III

Transformation Semigroups (continued)

CHAPTER IV

Primes

CHAPTER V

Semigroups and Varieties

CHAPTER VI

Decomposition of Sequential Functions

CHAPTER VII

Varieties of Sets

CHAPTER VIII

Examples of Varieties of Sets

CHAPTER IX

Aperiodicity

CHAPTER X

Unitary-Prefix Decompositions

CHAPTER XI

Depth Decomposition Theorem

by Bret Tilson

CHAPTER XII

Complexity of Semigroups and Morphisms

by Bret Tilson

This Page Intentionally Left Blank

Preface

The objective of this volume is to study, by algebraic methods, the properties of recognizable sets (i.e. sets recognized by finite state automata) and of sequential functions. The algebra is introduced by means of the following device. Let A be a recognizable subset of Σ^* where Σ is a finite alphabet, and let $\mathscr{A} = (Q_A, i, T)$ be the minimal automaton of A. Each letter $\sigma \in \Sigma$ defines a partial function (the automaton need not be complete!) $Q_A \to Q_A$. These partial functions generate a subsemigroup S_A of the finite monoid of all partial functions $Q_A \to Q_A$. This semigroup S_A is called the *syntactic semigroup* of A and the pair $TS_A = (Q_A, S_A)$ is called the *syntactic transformation semigroup* of A. If we adjoin the identity transformation of Q_A to S_A, we obtain the *syntactic monoid* M_A and the *syntactic transformation monoid* $TM_A = (Q_A, M_A)$.

If we start with a sequential function f: $\Sigma^* \to \Gamma^*$, we apply the same procedure to the minimal sequential machine $\mathscr{M} = (Q_f, i, \lambda)$: $\Sigma \to \Gamma$ of f. This yields syntactic invariants of f. Clearly, if interesting information about A and f is to be gleaned out of the syntactic invariants, we must know a good deal about these algebraic objects. This puts the spotlight on transformation semigroups and transformation monoids and also on semigroups and monoids, with everything in sight assumed to be finite.

As expected, a good deal of more or less new algebra will have to be used, and this algebra is developed in Chapters I–V. Chapter I introduces ts's (i.e. transformation semigroups) and tm's (i.e. transformation monoids) and defines basic concepts for dealing with them. Among these are

$X \prec Y$	inequality
$X \times Y$	direct product
$X \circ Y$	wreath product

Chapter II deals with decompositions of the form

(i) $$X \prec X_1 \circ \ldots \circ X_n$$

where X is a given ts and $X_1, \ldots, X_n$ are chosen to be in some sense as small as possible. The key result here is the Krohn–Rhodes Decomposition Theorem. We give two proofs of this important theorem. The second one utilizes a result that we call the Holonomy Decomposition Theorem and which gives an elegant algorithm for the decomposition.

Chapter III studies classes of ts's. This chapter is somewhat technical and paves the way for the applications.

A ts X is said to be a prime if $X \prec Y \circ Z$ implies $X \prec Y$ or $X \prec Z$. Such ts's are studied (and actually are enumerated) in Chapter IV. Each such prime X defines a class $\langle X \rangle$ of those Y for which $X \prec Y$ fails. It turns out that these classes $\langle X \rangle$ are very interesting and occur in many applications.

Chapter V studies monoids and semigroups (as opposed to transformation monoids and transformation semigroups). The wreath product is replaced by the semidirect product. The important notions of a variety (of finite monoids or finite semigroups) are introduced and studied. This completes the block of five algebraic chapters.

The next five chapters deal with applications. Chapter VI deals with sequential functions. It is shown that factoring a sequential function f into a series composition $f_n \ldots f_1$ is essentially equivalent to decomposing the syntactic ts TS_f as in (i). Thus any decomposition theorem for ts's has a companion theorem for decomposing sequential functions.

Chapter VII introduces the notions of $*$-varieties and $+$-varieties of recognizable sets. The key Theorems VII,3.4 and VII,3.4s show that these varieties of sets are in a 1–1 correspondence with the varieties of finite monoids and finite semigroups. Chapters VIII–X exploit this 1–1 correspondence in applying it under various circumstances. Despite the large number of situations considered, many interesting open questions remain.

The volume is enriched by two algebraic chapters contributed by Bret Tilson. Both aim at the complexity theory in the sense of Rhodes. Chapter XI established a decomposition theorem for semigroups inspired by complexity theory, while Chapter XII develops the main facts of complexity.

The algebraic chapters I–V, XI, and XII are totally independent of Volume A. Chapter VI has some references to A,XI and A,XII (i.e.

Chapters XI and XII of Volume A). Chapter VII has some references to A,III and Chapter X uses A,IV fairly heavily.

In addition to Chapters XI and XII Bret Tilson made other contributions which are explicitly acknowledged in the reference sections to the various chapters. In addition Tilson helped with criticism and useful suggestions.

M. P. Schützenberger made valuable contributions which are specifically acknowledged in the reference sections.

This Page Intentionally Left Blank

CHAPTER I

Transformation Semigroups

This chapter introduces the basic concept of a transformation semigroup. Various unary and binary operations on these objects are defined. Techniques for comparisons between transformation semigroups are studied.

1. Semigroups, Monoids, and Groups

A *semigroup* S is a set equipped with an associative multiplication. A subset S' of S such that $S'S' \subset S'$ is called a *subsemigroup* of S. The product $S \times T$ of two semigroups has its multiplication defined by the formula $(s, t)(s', t') = (ss', tt')$. The empty set $\emptyset$ is a semigroup.

A relation φ: $S \twoheadrightarrow T$ is a *relation of semigroups* if its graph is a subsemigroup of $S \times T$. In terms of φ itself this is equivalent with

$$(s\varphi)(s'\varphi) \subset (ss')\varphi$$

If further φ is a function, then the inclusion above becomes

$$(s\varphi)(s'\varphi) = (ss')\varphi$$

and we say that φ: $S \to T$ is a *morphism* of semigroups.

A *congruence relation* in a semigroup S is an equivalence relation $\sim$ in S such that $s_1 \sim s_1'$ and $s_2 \sim s_2'$ imply $s_1 s_2 \sim s_1' s_2'$. The quotient set $S' = S/\sim$ then acquires the structure of a semigroup such that the factorization mapping π: $S \to S'$ is a surjective morphism of semigroups.

A *monoid* is a semigroup that has a two-sided unit element. Such an element is necessarily unique and is usually denoted by 1. Thus a monoid is never empty. For a *morphism* φ: $S \to T$ *of monoids* we require that $1\varphi = 1$.

Let S be a semigroup and S' a subsemigroup of S. If S' is a monoid, then we say that S' is a *monoid in* S. The term *submonoid* is used only if both S and S' are monoids with the *same unit element*. Groups are treated as special cases of monoids.

Let S be a monoid. An element s of S is said to be *invertible* if there exists an element $s' \in S$ such that $ss' = 1 = s's$. Then s' is unique and is usually denoted by s^{-1}. The invertible elements of S form a group G which is the *maximal subgroup* of S. This maximal subgroup may be trivial (i.e. $G = 1$) if 1 is the only invertible element of S.

For any semigroup S we define a monoid S^{I} by adjoining a new element e to S and extending the multiplication from S to $S \cup e$ by setting $es = s = se$ for all $s \in S \cup e$. This operation is defined even if S is a monoid. If this is the case, then the unit element 1 of S ceases to be the unit element of S^{I} and e becomes the new unit element of S^{I}.

PROPOSITION 1.1. *A finite semigroup is a monoid if and only if*

$$(1.1) \qquad Ss = S, \qquad tS = S$$

holds for some elements $s, t \in S$. *Further,* S *is a group if and only if* $Ss = S$ *holds for every* $s \in S$, *while* $tS = S$ *holds for some* $t \in S$.

Proof. If S is a monoid, then $S1 = S = 1S$. Conversely, assume that $Ss = S$ for some $s \in S$. Consequently the transformation $S \to S$ defined by $x \to xs$ is surjective. Since S is finite, it follows that this transformation is a permutation of S. Consequently some power s^n $(n > 1)$ of s is the identity and hence is a right unit element for S. Since $tS = S$, it follows similarly that there exists a left unit element for S. It follows that S is a monoid with s^n as unit element. Further s is invertible with s^{n-1} as inverse. Thus if $Ss = S$ for all $s \in S$, then all elements of S are invertible and S is a group ▌

PROPOSITION 1.2. *Every non-empty subsemigroup* S *of a finite group* G *is a subgroup.*

Proof. Let $s \in S$. Then $s^n = 1$ for some $n > 1$. Consequently $1 \in S$ and $s^{-1} = s^{n-1} \in S$. Thus S is a subgroup ▌

2. Transformation Semigroups

Given a finite set Q we denote by $PF(Q)$ the monoid of all partial functions $Q \to Q$ with composition of partial functions as multiplication. The identity transformation 1_Q is the unit element. This monoid has a zero, namely the empty partial function $\emptyset\colon Q \to Q$. The letter $\emptyset$ will be used exclusively for this purpose. Clearly $\emptyset s = \emptyset = s\emptyset$ for all $s \in PF(Q)$.

A *transformation semigroup* (abbreviation: ts)

$$X = (Q, S)$$

consists of a finite set Q and a subsemigroup S of $PF(Q)$. The elements of Q are called *states*, and Q itself is called the *underlying set* of X. The elements of S are called *transformations* of X, while S itself is called the *action semigroup* of X. If several ts's are involved in an argument, we shall write Q_X and S_X instead of Q and S, to make recognition easier.

Frequently the semigroup S is given abstractly, i.e., outside of $PF(Q)$. To imbed S in $PF(Q)$, we must give a partial function (called the *action*)

$$\alpha\colon Q \times S \to Q$$

satisfying the following conditions

(2.1) $((q, s)\alpha, s')\alpha = (q, ss')\alpha$

(2.2) $s \neq s'$ implies $(q, s)\alpha \neq (q, s')\alpha$ for some $q \in Q$.

We usually write qs instead of $(q, s)\alpha$. Conditions (2.1) and (2.2) then take on the easier form

(2.1′) $(qs)s' = q(ss')$

(2.2′) $s \neq s'$ implies $qs \neq qs'$ for some $q \in Q$.

Condition (2.1′) is called the *associativity* condition. Note that both sides of (2.1′) may be $\emptyset$. This will take place if either $qs = \emptyset$ or $qs = q'$ and $q's' = \emptyset$. Condition (2.2′) is called the *faithfulness* condition. In the next section we shall discuss it in greater detail.

The ts $X = (Q, S)$ is called a *transformation monoid* (abbreviation: tm) if the identity transformation 1_Q is in S. Thus S in this case is a monoid. Note that S being a monoid is not sufficient to ensure that X is a tm; we must insist that S be a submonoid of $PF(Q)$, i.e., that S contain the unit element of $PF(Q)$, namely 1_Q.

With each ts $X = (Q, S)$ we may associate the tm $X^{\bullet} = (Q, S \cup 1_Q)$. Clearly $X^{\bullet} = X$ iff X is a tm. Thus $X^{\bullet\bullet} = X^{\bullet}$.

A ts $X = (Q, S)$ is said to be *complete* (abbreviation: cts) if the following two conditions hold

(2.3) $Q \neq \emptyset$

(2.4) $qs \neq \emptyset$ for all $q \in Q, s \in S$.

In a cts X, the transformations of X are functions rather than partial functions. Note that if $Q \neq \emptyset$ and $S = \emptyset$, then X is complete. If X is complete, so is $X^{\bullet}$.

With each ts $X = (Q, S)$ we associate a cts X^c called the *completion* of X, which is defined as follows: $X^c = X$ if X already is complete; if X is not complete, then $X^c = (Q^c, S)$ where Q^c is obtained from Q by adjoining to it a new state $\square$ (called the *sink* state). The action of S on Q^c is defined as follows

$$q \cdot s = \begin{cases} qs & \text{if } q \in Q \text{ and } qs \neq \emptyset \\ \square & \text{in all other cases} \end{cases}$$

Thus in particular $\square \cdot s = \square$ for all $s \in S$. The reader should note the close analogy with the completion of an automaton.

If X is a tm, then so is its completion X^c. Thus in this case X^c is a *complete transformation monoid* (abbreviation: ctm).

A tx $X = (Q, S)$ is called a *transformation group* (abbreviation: tg) if

(2.5) $Q \neq \emptyset$

(2.6) S is a group

(2.7) $1_Q \in S$.

If s is a transformation in the tg X, then so is s^{-1} and $ss^{-1} = 1_Q = s^{-1}s$. It follows that s is a bijection of Q, i.e. a permutation, and that s^{-1} is its inverse. Thus each tg is a ctm. Conversely, if $X = (Q, S)$ is a ts, if $Q \neq \emptyset$, $S \neq \emptyset$, and if each transformation s of X is a permutation, then X is a tg.

Given a finite set Q and an element $q \in Q$, the constant function $Q \to Q$ with value q will be denoted by $\bar{q}$. Thus $q'\bar{q} = q$ for all $q' \in Q$. The semigroup of all these constant functions will be denoted by $\bar{Q}$. The ts $X = (Q, S)$ will be said to be *closed* if all the constants are transformations of X, i.e., if $\bar{Q} \subset S$. The *closure* of a ts $X = (Q, S)$ is defined as $\bar{X} = (Q, S')$ where S' is the least subsemigroup of $PF(Q)$ containing $S \cup \tilde{Q}$. If X is complete, then so is $\bar{X}$.

Given $s, t \in PF(Q)$, we write as usual $s \subset t$ provided $qs \subset qt$ for all $q \in Q$. Equivalently, $s \subset t$ signifies that $qs = qt$ whenever $qs \neq \emptyset$. This defines a partial ordering on S for any ts $X = (Q, S)$. If $s \in S$ and $s \subset 1_Q$, then we say that s is a *subidentity*. If $s \subset \tilde{q}$ for some $q \in Q$, then we say that s is a *subconstant*. If $Q \neq \emptyset$, then θ is a subconstant. By abuse of language, we shall call θ a subconstant even if $Q = \emptyset$.

EXERCISE 2.1. *Verify that*

$$(\overline{X^{\cdot}}) = (\bar{X})^{\cdot}, \qquad (X^{\cdot})^{c} = (X^{c})^{\cdot}$$

for any ts X.

EXERCISE 2.2. *Let $X = (Q, S)$ be a ts and let $\bar{X} = (Q, S')$ be its closure. Verify that either*

$$S' = S \cup \tilde{Q}$$

or

$$S' = S \cup \tilde{Q} \cup S\tilde{Q} \cup \theta$$

The first case holds if X is complete or $Q = \emptyset$, while the second case holds if X is not complete and $Q \neq \emptyset$.

3. Examples of Transformation Semigroups

For any (finite) set Q, the pair $(Q, \emptyset)$ is a ts which we shall denote by Q. Thus

$$Q = (Q, \emptyset)$$

This is not to be confused with the ts (Q, θ) in which the action semigroup consists of the empty transformation.

For each integer $k \geq 0$ we denote by $\mathbf{k}$ the set

$$\mathbf{k} = \{n \mid 0 \leq n \leq k - 1\}$$

of digits at the base k. In particular $\mathbf{0}$ is the empty set, $\mathbf{1}$ has a single element 0, and $\mathbf{2}$ consists of the digits 0 and 1. As explained above we shall regard $\mathbf{k}$ as a ts with an empty action semigroup. In particular $\mathbf{0}$ is the "smallest" ts, while $\mathbf{0}^{\cdot} = (\mathbf{0}, \theta)$ is the smallest tm. Also $\mathbf{1} = \mathbf{0}^{c}$ is