Yuqi Guo · Yun Liu
Shoufeng Wang

# Topics on Combinatorial Semigroups

Science Press
Beijing

Springer

# Topics on Combinatorial Semigroups

Yuqi Guo • Yun Liu • Shoufeng Wang

# Topics on Combinatorial Semigroups

Springer

Science Press
Beijing

Yuqi Guo
School of Mathematics and Statistics
Lanzhou University
Lanzhou, Gansu, China

Yun Liu
Department of Mathematics
Yuxi Normal University
Yuxi, Yunnan, China

Shoufeng Wang
Department of Mathematics
Yunnan Normal University
Kunming, Yunnan, China

ISBN 978-981-99-9170-9 ISBN 978-981-99-9171-6 (eBook)
https://doi.org/10.1007/978-981-99-9171-6

Mathematics Subject Classification: 20M35, 68Q45, 68Q70, 68R15

Jointly published with Science Press.
The printed edition is not for sale in China Mainland. Customers from China Mainland please order the print book from Science Press.



This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Paper in this product is recyclable.

# Preface

By combinatorial semigroups, we mean a general term of concepts, facts and methods which are produced in investigating of algebraic and combinatorial properties, constructions, classifications and interrelations of formal languages and automata, codes, finite and infinite words by using semigroup theory (including congruences, homomorphisms, quotients and structural theory, etc.) and combinatorial analysis (including word sequence analysis, formal power series, operations of words and languages, etc.). As the main research objects in this field are the elements and subsets of the free semigroups and monoids and many combinatorial properties of these objects are closely related to algebraic theory of semigroups via certain kinds of transformations and congruences (such as syntactic congruences) as the medium, the field is named *combinatorial semigroups* in some literatures.

The research contents of combinatorial semigroups belong to the cross-field of algebra and theoretical computer science, and the idea coincides with the natural languages of human beings and the machine languages of computer systems. This is the fundamental reason why the theory of semigroups can become the theoretical basis of many branches of theoretical computer science such as automata and formal languages, theory of codes, combinatorics of words, symbolic dynamics, and of contemporary artificial intelligence, modern communication technology, big data science and technology and so on.

The systematic study of formal languages began at the beginning of the last century. In the 1940s and 1950s, under the impetus of the newly emerging computer science, it was developed rapidly. The most commonly used tools for studying languages are automata and grammars, both of which are effective tools for expressing languages. The simplest automata are finite automata, and the languages recognized by them are called regular languages. This type of languages is at the bottom of the Chomsky hierarchy of languages, and is one of the most important research objects of formal languages. The semigroup theory of languages started from the classification of regular languages. We know that every language determines a syntactic monoid. A language is a regular language if and only if its syntactic monoid is finite.

With the development of the theory of formal languages and algebraic theory of semigroups, since the early 1970s, some scholars began to use syntactic monoids (or syntactic congruences) to define and study non-regular languages. Among them, the class of disjunctive languages put forward by Professor H. J. Shyr and others is a typical representative [113]. If the syntactic congruence of a language is the equality relation (that is, each congruence class is a singleton set), then the language is called a disjunctive language. For the systematic introduction to the theory of disjunctive languages and its generalizations, it is recommended to refer to Shyr 's book [117].

Over any alphabet, the class of disjunctive languages is disjoint from the class of regular languages. Moreover, it has a certain antithesis to the class of regular languages in terms of definitions and properties. From the perspective of syntactic descriptions, it goes to the other "extreme" as opposed to the class of regular languages. Interestingly, when the alphabet contains only one letter, a language is either regular or disjunctive. When the alphabet contains at least two letters, the two extreme boundaries of disjunctive languages and regular languages will no longer coincide, resulting the occurrences of languages that are neither disjunctive nor regular (called midst-languages in [124]). In order to classify a large number of "midst-languages", many scholars, starting from disjunctive languages and expanding language classes hierarchically, proposed "f-disjunctive languages" with each syntactic congruence class being a finite set, "i-disjunctive language" with each syntactic congruence class being an infix code, and "t-disjunctive language" (also called "nd-disjunctive language") with each syntactic congruence class being a thin (i.e. non-dense) language and "relatively disjunctive language" with a "dense cross-section", and so on.

The organization of the book is as follows: Chap. 1 is a preliminary chapter, in which some basic concepts and notations used throughout the book, including semigroups and monoids, free semigroups (monoids), finite and infinite words, languages, disjunctive (regular) and dense subsets in semigroups, primitive words, are introduced.

The theory of codes takes its origin in the theory of information devised by Shannon in 1950s, which is a branch of theoretical computer science. The algebraic theory of codes, which mainly studies the construction, counting, classification and relations of codes satisfying certain algebraic and combinatorial properties, is closed related to the theory of formal languages, automata and semigroups. This area is not the main subject of the book. However, since many contents involving the constructions of (generalized) disjunctive languages and regular languages are closely related to the algebraic theory of codes, some selected topics are introduced in Chap. 2, including the method of defining codes by using dependence systems, the maximality and completeness of codes, and the detailed discussion of some special kinds of codes such as convex codes, semaphore codes and solid codes. For more information on the theory of codes, the readers are recommended to refer to the book [4] by J. Berstel, D. Perrin and C. Reutenauer, and some parts of the book [51, 57, 117].

The main topics of the book are regular languages and disjunctive languages and their various kinds of generalizations, which covers the contents from Chap. 3

to the last chapter. Regular languages and some generalizations are discussed in Chaps. 3, 6, and 8, and disjunctive languages and some generalizations are discussed in Chaps. 4–7.

Chapter 3 discusses some selected topics of regular languages. The contents of the chapter can be divided into two parts. In Sects. 3.1–3.3, a brief introduction to the theory of regular languages, including the automata theory of regular languages and the equivalence of the three concepts of languages: regularity, recognizability and rationality, are given. This part is classical and elementary and can be found in many books on the theory of formal languages and automata. The second part (Sects. 3.4 and 3.5) introduces some special topics of regular languages such as some decompositions of regular languages and restricted Burnside problem of semigroups (which is related to regular languages).

Chapter 4 mainly involves the disjunctive decompositions of languages. A language is said to be disjunctive decomposable if it can be decomposed into a disjoint union of several disjunctive languages. In 1970–1980s, when the study of disjunctive languages was becoming more popular, many scholars developed in-depth researches on the disjunctive decompositions of languages. In this chapter, we first give a brief introduction to the theory of disjunctive languages, and then, give in detail some kinds of finite and infinite disjunctive decompositions of dense languages.

Chapter 5 is devoted to the theory of f-disjunctive languages. This class of languages is a kind of generalized disjunctive languages which is located in the bottom of the hierarchy of generalized disjunctive languages. In this chapter, systematic characterizations of f-disjunctive languages are given. In particular, f-disjunctive domains and syntactic semigroups of f-disjunctive languages are discussed in detail.

Generalizations of regular languages and disjunctive languages meet in Chap. 6. Relatively regular languages and relatively disjunctive languages are natural generalizations of regular languages and disjunctive languages respectively. Systematic discussions of these two classes of languages are given in the chapter. As mentioned above, when the alphabet contains only one letter, all languages are divided into two disjoint classes: the class of regular languages and the class of disjunctive languages. When the alphabet contains at least two letters, the two extreme boundaries will no longer coincide. One of the main results of the chapter is that "In any finite alphabet, all languages are divided into two disjoint classes: relatively regular languages and relatively disjunctive languages". This is a natural generalization of the classification of languages on one-letter alphabets, and in some sense give a corresponding classification of languages on finite alphabets.

Chapter 7 presents a general theory of generalized disjunctive languages. By using universal algebra, a uniform characterization of syntactic semigroups of various kinds of generalized disjunctive languages is given. Moreover, two kinds of generalized disjunctive languages (i.e. q-disjunctive languages and qf-disjunctive languages) and a hierarchy of generalized disjunctive languages are described in detail.

In the last chapter, by using "permissible subsets", we obtain a kind of generalized principal congruences determined by languages. Applying this kind of generalized principal congruences, we introduce and investigate a class of generalized regular languages, namely, $\mathcal{PS}$-regular languages. By using the properties of this class of languages, some new characterizations of regular languages are given. Furthermore, the relationship among the class of $\mathcal{PS}$-regular languages, context-free languages and context-sensitive languages, is also given in this chapter.

Lanzhou, China — Yuqi Guo
Yuxi, China — Yun Liu
Kunming, China — Shoufeng Wang

# Contents

# Chapter 1
# Basic Concepts and Notations

In this preliminary chapter, we give a short account of some basic concepts and notations which will be used throughout the book. Section 1.1 contains the background knowledge in the general semigroup theory. Section 1.2 covers a short introduction to the theory of languages. In Sect. 1.3, we discuss dense subsets (languages) in semigroups. Dense subsets (languages) will play an important role throughout the book. In Sect. 1.4, we deal with a special but important class of words called primitive words which will be often used in the book. Some elementary properties of infinite words are involved in the last section.

Howie's books [36] and [38] are good references in elementary semigroup theory. The systemic introductions of language theory can be found in [17, 35, 37, 57, 117]. Items not defined in this book can also be found in these books.

## 1.1 Semigroups (Monoids)

A couple $(S, \cdot)$ is called a *semigroup* if $S$ is a nonempty set and "$\cdot$" is a binary operation satisfying *associative law* on $S$. This binary operation is usually called the *multiplication* on $S$. We often simply denote the above semigroup by $S$ and also denote the multiplicative product $a \cdot b$ by $ab$ for any $a, b \in S$ if no ambiguity arises.

Let $S$ be a semigroup. An element 1 (0) of $S$ is called an *identity* (*zero*) of $S$ if

$$(\forall s \in S)\ 1s = s1 = s$$

$$((\forall s \in S)\ 0s = s0 = 0).$$

One can easily show that any semigroup contains at most one identity (zero). A semigroup containing an identity (zero) is called a *monoid* (*semigroup with zero*).



Y. Guo et al., *Topics on Combinatorial Semigroups*,
https://doi.org/10.1007/978-981-99-9171-6_1

For instance, the set $\mathbb{N}$ ($\mathbb{N}^0$) of all positive (nonnegative) integers forms a semigroup (monoid) under the usual integer addition. But, $\mathbb{N}$ ($\mathbb{N}^0$) is a monoid (semigroup with zero) under the usual multiplication.

Let $S \overset{d}{=} (S, \cdot)$ be a semigroup. We can extend $S$ to $S^1 \overset{d}{=} (S^1, *)$ and $S^0 \overset{d}{=} (S^0, \circ)$ as follows.

$$S^1 = \begin{cases} S & \text{if } S \text{ has an identity,} \\ S \cup \{1\} & \text{otherwise,} \end{cases}$$

where $1 \notin S$, and for any $a, b \in S$,

$$a * b = a \cdot b, 1 * a = a * 1 = a, 1 * 1 = 1;$$

and

$$S^0 = \begin{cases} S & \text{if } S \text{ has a zero,} \\ S \cup \{0\} & \text{otherwise,} \end{cases}$$

where $0 \notin S$, and for any $a, b \in S$,

$$a \circ b = a \cdot b, 0 \circ a = a \circ 0 = 0, 0 \circ 0 = 0.$$

If $A$ and $B$ are subsets of semigroup $S$, then we call

$$AB = \{ab | a \in A, b \in B\}$$

the product of $A$ and $B$. Clearly, the *power set* $\mathscr{P}(S)$ of $S$ (the set consisting of all subsets of $S$) forms a semigroup under this operation. Denote

$$A^1 = A, \quad A^{n+1} = AA^n, \quad A^{\leq n} = \bigcup_{i=1}^{n} A^i, \quad A^{\geq n} = \bigcup_{i=n}^{\infty} A^i, \quad n \in \mathbb{N}.$$

If $S$ is a monoid with identity 1, then we also have the notation $A^0 = \{1\}$. For any $A, B \in \mathscr{P}(S)$, we use $A^{-1}B$ and $AB^{-1}$ to denote the set

$$\{x \in S \mid ax \in B \text{ for some } a \in A\}$$

and the set

$$\{x \in S \mid xb \in A \text{ for some } b \in B\}$$

respectively. In addition, we also simply write $aA$, $Aa$, $a^{-1}A$ and $Aa^{-1}$ for $\{a\}A$, $A\{a\}$, $\{a\}^{-1}A$ and $A\{a\}^{-1}$, where $a$ is an element of $S$.

Let $(M, \cdot, 1)$ be a monoid, $a \in M$. An element $a'$ of $M$ is called a *group inverse* of $a$ if $aa' = a'a = 1$. $a \in M$ is called a *unit* of $M$ if $a$ has a group inverse in $M$. It is clear that any unit of $M$ has a unique group inverse in $M$. The set of all units of $M$ forms a group under the operation of $M$, which is called the *group of units* of $M$.

A nonempty subset $T$ of a semigroup $S$ is called a *subsemigroup* of $S$, if $T$ is closed under the semigroup operation of $S$, that is, $T$ forms a semigroup under the induced operation of $S$. If $T$ happens to be a monoid (group) under the operation of $S$, then $T$ is called a *submonoid* (*subgroup*) of $S$. For any nonempty subset $X$ of $S$, the intersection of all subsemigroups of $S$ containing $X$ is clearly a subsemigroup, called the *subsemigroup of $S$ generated by $X$* and denoted by $\langle X \rangle$, which is the minimal subsemigroup containing $X$. If $S = \langle X \rangle$, then say $S$ is *generated* by $X$ or $X$ is a *generating subset* of $S$. A semigroup generated by a singleton is called a *monogenic semigroup*.

A nonempty subset $I$ of a semigroup $S$ is called an *ideal* (*left ideal*, *right ideal*, *quasi-ideal*) of $S$ if $IS \cup SI \subseteq I$ ($SI \subseteq I$, $IS \subseteq I$, $SI \cap IS \subseteq I$). It is easy to show that all subsets above mentioned are subsemigroups of $S$. An (left, right, quasi-) ideal is called a *principal* (*left*, *right*, *quasi-*) *ideal* if it can be generated by one element of $S$. Clearly, $S$ itself is trivially an (left, right, quasi-) ideal of $S$. All other (left, right, quasi-) ideals are said to be *proper*. A semigroup has no proper (left, right, quasi-) ideal is called a (*left*, *right*, *quasi-*) *simple semigroup*. One can easily show that a semigroup is quasi-simple if and only if it is a group.

**The Monoid of Binary Relations**

Let $X$ be a set. A *binary relation* or simply a *relation* on $X$ is a subset of $X \times X$. The set $\mathscr{B}(X)$ of all binary relations on $X$ forms a monoid under the operation of *composition of relations*

$$\rho \circ \sigma = \{(x, y) \in X \times X \mid (\exists z \in X)\ (x, z) \in \rho, (z, y) \in \sigma\}.$$

Obviously, $\iota_X = \{(x, x) \mid x \in X\}$, the *equality relation* is the identity of the monoid. For $\rho \in \mathscr{B}(X)$, we also write $x\rho y$ for $(x, y) \in \rho$.

We list some frequently used notations and notions about binary relations as follows. Let $\rho \in \mathscr{B}(X)$.

(1) $\mathrm{dom}(\rho) = \{x \in X \mid (\exists y \in X)\ (x, y) \in \rho\}$ is the *domain* of $\rho$. Clearly, $x \in \mathrm{dom}(\rho)$ if and only if $x\rho \stackrel{d}{=} \{y \mid (x, y) \in \rho\}$ is not empty.
(2) $\mathrm{im}(\rho) = \{x \in X \mid (\exists y \in X)\ (y, x) \in \rho\}$ is the *image* of $\rho$.
(3) $\rho^{-1} = \{(x, y) \mid (y, x) \in \rho\}$ is the *inverse* of $\rho$. Clearly $\mathrm{dom}(\rho^{-1}) = \mathrm{im}(\rho)$, $\mathrm{im}(\rho^{-1}) = \mathrm{dom}(\rho)$.
(4) $\rho^1 = \rho$, $\rho^{n+1} = \rho \circ \rho^n$, $n \in \mathbb{N}$; $\rho^\infty = \bigcup_{n=1}^{\infty} \rho^n$ is the *transitive closure* of $\rho$.

A *transformation* (*partial transformation*) $\varphi$ on $X$ is a relation such that for any $x \in X$, $|x\varphi| = 1$ ($|x\varphi| \leq 1$). The set of all transformation (partial transformation) is denoted by $\mathscr{T}(X)$ ($\mathscr{PT}(X)$). Obviously, $\mathscr{T}(X)$ is a submonoid of $\mathscr{PT}(X)$ and $\mathscr{PT}(X)$ is a submonoid of $\mathscr{B}(X)$.

An *equivalence* $\rho$ on $X$ is a relation which is reflexive (i.e., $\iota_X \subseteq \rho$), symmetric (i.e., $\rho^{-1} = \rho$) and transitive (i.e., $\rho^2 \subseteq \rho$). The set of all equivalences on $X$ is denoted by $\mathscr{E}(X)$.

A *partition* $\pi$ of $X$ is a subset of $\mathscr{P}(X)$ satisfying the following three conditions:

(1) For any $X' \in \pi$, $X' \neq \emptyset$;
(2) For any $X', X'' \in \pi$, $X' \cap X'' \neq \emptyset$ implies $X' = X''$;
(3) $\bigcup_{X' \in \pi} X' = X$.

The set of all partitions of $X$ is denoted by $\Pi(X)$.

For any equivalence $\rho$ on $X$, the *quotient set* $X/\rho = \{x\rho \mid x \in X\}$ constitutes a partition $\pi_\rho$ of $X$. We call such $x\rho$ a $\rho$*-class* of $X$. Clearly,

$$\eta : \mathscr{E}(X) \to \Pi(X)$$
$$\rho \mapsto X/\rho$$

is a bijection. An equivalence $\rho$ *saturates* a subset $L$ of $X$ means $L$ is the union of some $\rho$-classes.

A (*partial*) *order* $\leq$ on $X$ is a relation which is reflexive, antisymmetric (i.e. $\leq \cap \leq^{-1} \subseteq \iota_X$) and transitive. A *total order* (or *linear order*) $\leq$ on $X$ is a partial order which satisfies that any pairs of elements in $X$ are comparable, that is, for any $x, y \in X$, $x \leq y$ or $y \leq x$ holds. $x \in X$ is called a *minimal element* of $X$ if for all $y \in X$, $y \leq x$ implies $y = x$; $x$ is called a *minimum element* of $X$ if $x \leq y$ for all $y \in X$. Similarly we can define concepts of the *maximal element* and the *maximum element*. Clearly, by antisymmetry of the relation, the minimum element (maximum element) is unique whenever it exists. A *well-order* $\leq$ on $X$ is a total order which satisfies that any nonempty subset of $X$ contains a minimal element. A set with a order (total order, well-order) is called an *ordered* (*totally ordered*, *well-ordered*) *set*. A totally ordered subset $Y$ of an ordered set $X$ is usually called a *chain*. In an ordered set $X$, we used $x < y$ to stand for $x \leq y$ but $x \neq y$.

**Congruences, Quotients and Homomorphisms**

In the rest of this section, let $S$ and $T$ be semigroups (monoids with identity $1_S$ and $1_T$ respectively).

A *left congruence* (*right congruence*) $\rho$ on $S$ is an equivalence which is left (right) compatible with respect to the semigroup operation, that is,

$$(\forall a, b, c \in S)\ \text{“}a\rho b \Rightarrow ca\rho cb\text{”}$$

$$((\forall a, b, c \in S)\ \text{“}a\rho b \Rightarrow ac\rho bc\text{”}).$$

A *congruence* $\rho$ on $S$ is both a left congruence and a right congruence, which is equivalent to $\rho \in \mathscr{E}(X)$ and $\rho$ is *compatible*, that is

$$(\forall a, b, c, d \in S)\ \text{“}a\rho b, c\rho d \Rightarrow ac\rho bd\text{”}.$$

If $\rho$ is a congruence on $S$, then the quotient set $S/\rho$ is a semigroup under the following multiplication:

$$(\forall x, y \in S)\ x\rho \cdot y\rho = (xy)\rho.$$

$S/\rho$ is called the *quotient semigroup* of $S$ with respect to $\rho$. Let $S/\rho = \{S_i | i \in I\}$. Then $C = \{c_i \in S_i | i \in I\}$ is called a *cross-section* of $\rho$.

A mapping $\varphi : S \to T$ is called a semigroup (monoid) *homomorphism* from $S$ to $T$ if $\varphi$ preserves the operations on two semigroups, that is,

$$\varphi(ab) = \varphi(a)\varphi(b) \text{ for all } a, b \in S$$

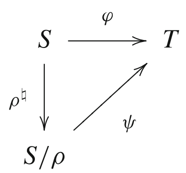
$$(\varphi(ab) = \varphi(a)\varphi(b) \text{ for all } a, b \in S \text{ and } \varphi(1_S) = 1_T).$$

An injective (surjective, bijective) homomorphism is called a *monomorphism* (*epimorphism*, *isomorphism*). A homomorphism (isomorphism) from $S$ to itself is called an *endomorphism* (*automorphism*). The set of all endomorphism is denoted by $\mathrm{End}(S)$.

Let $\rho$ be a congruence on $S$. Then $x \mapsto x\rho$ is an epimorphism from $S$ to $S/\rho$, which is called the *natural homomorphism* induced by $\rho$ and denoted by $\rho^\natural$. Let $\varphi$ be a homomorphism from $S$ to $T$. Then $\{(x, y) \in S \times S \mid \varphi(x) = \varphi(y)\}$ is a congruence on $S$, which is called the *kernel* of $\varphi$ and denoted by $\ker\varphi$.

The following theorems are well-known.

**Theorem 1.1.1 ([36])** *Let $\rho$ be a congruence on a semigroup (monoid) $S$. If $\varphi : S \to T$ is a homomorphism such that $\rho \subseteq \ker\varphi$. Then there is a unique homomorphism $\psi : S/\rho \to T$ such that $\mathrm{im}(\psi) = \mathrm{im}(\varphi)$ and the diagram*




*commutes. Moreover, $\psi$ is injective if and only if $\rho = \ker\varphi$.*

***Proof*** Define $\psi : S/\rho \to T$ by

$$\psi(s\rho) = \varphi(s) \quad (s\rho \in S/\rho). \tag{1.1.1}$$

Then $\psi$ is well-defined, since for all $s, s' \in S$,

$$s\rho = s'\rho \iff (s, s') \in \rho \Rightarrow (s, s') \in \ker\varphi \iff s\varphi = s'\varphi.$$

It is now a routine matter to verify that $\psi$ is a homomorphism, $\mathrm{im}(\psi) = \mathrm{im}(\varphi)$ and $\rho^\natural \circ \psi = \varphi$. The uniqueness of $\psi$ is also obvious, since any homomorphism $\psi$ satisfying $\rho^\natural \circ \psi = \varphi$ must be defined by the rule (1.1.1).

$\psi$ is injective if and only if "for any $s\rho, s'\rho \in S/\rho$, $\psi(s\rho) = \psi(s'\rho)$ implies $s\rho = s'\rho$", and if and only if "for any $s, s' \in S$, $\varphi(s) = \varphi(s')$ implies $(s, s') \in \rho$", which is equivalent to $\rho \supseteq \ker\varphi$, and hence $\rho = \ker\varphi$. □

One application of this theorem is to the situation where $\rho$ and $\sigma$ are congruences on $S$ with $\rho \subseteq \sigma$. The theorem implies that there is a homomorphism $\psi$ from $S/\rho$ onto $S/\sigma$ such that the diagram

$$\begin{array}{ccc} S & \xrightarrow{\sigma^\natural} & S/\sigma \\ {\scriptstyle\rho^\natural}\downarrow & \nearrow{\scriptstyle\psi} & \\ S/\rho & & \end{array}$$

commutes. The homomorphism $\psi$ is given by

$$\psi(a\rho) = a\sigma \quad (a\rho \in S/\rho),$$

and the congruence $\ker\psi$ on $S$ is given by

$$\ker\psi = \{(a\rho, b\rho) \in S/\rho \times S/\rho \mid (a, b) \in \sigma\}.$$

It is usual to write $\ker\psi$ as $\sigma/\rho$. From Theorem 1.1.1, it follows that there is an isomorphism $\theta : (S/\rho)/(\sigma/\rho) \to S/\sigma$ defined by

$$\theta((s\rho)(\sigma/\rho)) = s\sigma \quad (s \in S),$$

and such that the diagram

$$\begin{array}{ccc} S & \xrightarrow{\sigma^\natural} & S/\sigma \\ {\scriptstyle\rho^\natural}\downarrow & & \uparrow{\scriptstyle\theta} \\ S/\rho & \xrightarrow[(\sigma/\rho)^\natural]{} & (S/\rho)/(\sigma/\rho) \end{array}$$

commutes. We summarize in a theorem:

**Theorem 1.1.2 ([36])** *Let $\rho$, $\sigma$ be congruences on a semigroup (monoid) $S$ such that $\rho \subseteq \sigma$. Then*

$$\sigma/\rho = \{(a\rho, b\rho) \in S/\rho \times S/\rho \mid (a, b) \in \sigma\}$$

*is a congruence on $S/\rho$, and $(S/\rho)/(\sigma/\rho) \simeq S/\sigma$.*

Let $I$ be an ideal of $S$. Then $\rho_I = \iota_S \cup (I \times I)$ is a congruence on $S$, which is called the *Rees congruence* with respect to $I$. We always write $S/I$ rather than $S/\rho_I$ and call it the *Rees quotient* with respect to $I$.

**Typical Classes of Semigroups**

We now introduce some typical classes of semigroups which are often used in this book. Let $S$ be a semigroup. $S$ is called

(1) a *band* if $a^2 = a$ for all $a \in S$;
(2) a *left zero semigroup* if $ab = a$ for all $a, b \in S$;
(3) a *right zero semigroup* if $ab = b$ for all $a, b \in S$;
(4) a *rectangular band* if $a^2 = a$ and $aba = a$ for all $a, b \in S$;
(5) a *semilattice* if $a^2 = a$ and $ab = ba$ for all $a, b \in S$;
(6) a *null semigroup* (or *zero semigroup*) if $S$ contains the zero element 0 and $ab = 0$ for all $a, b \in S$;
(7) a *nilpotent semigroup* if $S$ contains the zero element 0 and there is an $n \in \mathbb{N}$ such that $a_1 a_2 \cdots a_n = 0$ for all $a_i \in S$, $i = 1, 2, \ldots, n$;
(8) a *nil-semigroup* if $S$ contains the zero element 0 and every elements of $S$ is nilpotent, that is,

$$(\forall a \in S)(\exists n \in \mathbb{N}) a^n = 0.$$

The elements of $S$ satisfying the equality $a^2 = a$ are called *idempotents* and the set of all idempotents of $S$ is denoted by $E(S)$.

In a semigroup $S$, the relations $\mathscr{L}$, $\mathscr{R}$ and $\mathscr{J}$ are defined as follows:

$$\begin{aligned}
(\forall a, b \in S)\ a \mathscr{L} b &\text{ if and only if } \quad S^1 a = S^1 b, \\
(\forall a, b \in S)\ a \mathscr{R} b &\text{ if and only if } \quad a S^1 = b S^1, \\
(\forall a, b \in S)\ a \mathscr{J} b &\text{ if and only if } S^1 a S^1 = S^1 b S^1,
\end{aligned}$$

and define $\mathscr{H} = \mathscr{L} \wedge \mathscr{R}$, $\mathscr{D} = \mathscr{L} \vee \mathscr{R}$. All the above relations are equivalences on $S$, called the *Green's relations* on $S$. We denote the $\mathscr{J}$ ($\mathscr{L}$, $\mathscr{R}$, $\mathscr{H}$, $\mathscr{D}$)-class containing $a$ by $J_a$ ($L_a$, $R_a$, $H_a$, $D_a$).

An element $a$ of $S$ is said to be *regular* if $axa = a$ for some $x \in S$. Denote the set of all regular elements of $S$ by $\mathrm{Reg}(S)$. $S$ is said to be *regular* if every element of $S$ is regular. $a' \in S$ is called an *inverse* of $a \in S$ if $aa'a = a$ and $a'aa' = a'$. The set of all inverses of $a$ is denoted by $V(a)$. Then it is clear that $a \in \mathrm{Reg}(S)$ if and only if $V(a) \neq \emptyset$. An element $a$ of $S$ is said to be *completely regular* if $axa = a$ and $ax = xa$ for some $x \in S$. $S$ is said to be *completely regular* if every element of $S$ is completely regular. A completely regular simple semigroup is called a *completely simple semigroup*. The readers are referred to Howie's book [36] for systemic introduction to the theory of Green's relations and regular semigroups.

The concepts such as substructures, generating sets, congruences, homomorphisms defined above can also be similarly defined in monoids, groups and other algebraic systems.

In this book, we use $|X|$ to represent the cardinality of set $X$, $|X| < \infty$ to represent $X$ is finite and $|X| = \infty$ to represent $X$ is infinite. For a subset $L$ of a set $X$, we use $L^c$ to represent $X \setminus L = \{x \in X \mid x \notin L\}$, call it the complement of $L$ in $X$. If $L^c$ is finite, then we call $L$ is *cofinite*.

## 1.2 Free Semigroups (Monoids) and Languages

Let $A$ be a nonempty set, which we call an *alphabet*.

$$A^+ \stackrel{d}{=} \{a_1a_2\cdots a_n | a_i \in A, i = 1, 2, \ldots, n, n \in \mathbb{N}\}$$

is a semigroup with respect to "·" as follows

$$(a_1a_2\cdots a_n)\cdot(b_1b_2\cdots b_m) = a_1a_2\cdots a_nb_1b_2\cdots b_m.$$

$A^+$ is called the *free semigroup* generated by $A$. $A^* \stackrel{d}{=} (A^+)^1$ is the *free monoid* generated by $A$. The elements of $A$ are called *letters*. The elements of $A^*$ are called *words* over $A$. 1 is called the *empty word* over $A$ (we may regard it to be a word without letter). Any subset of a free monoid $A^*$ is called a *language* over $A$.

The *length* $lg(w)$ of a word $w = a_1a_2\cdots a_n$ with $a_i \in A$ is $n$, the number of letters occurring in $w$. We often denote the number of occurrences of $a \in A$ in $w$ by $w_a$. Then we have $lg(w) = \sum_{a\in A} w_a$. The set of letters occurring in $w$ is denoted by $\mathrm{alph}(w)$. For any $L \subseteq A^*$, $\mathrm{alph}(L) = \bigcup_{w\in L} \mathrm{alph}(w)$.

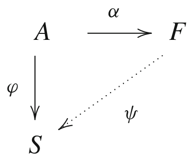
A word $u$ is called a *prefix* of a word $w$ if $u$ is a *left factor* of $w$, that is, $w = uv$ for some $v \in A^*$. *Suffixes* are defined dually. $u$ is called an *infix* of $w$ if $u$ is a *factor* of $w$, that is, $w = xuy$ for some $x, y \in A^*$. It is clear that the relation

$$\leq_{\mathrm{P}} \stackrel{d}{=} \left\{(x, y) \in A^* \times A^* \mid x \text{ is a prefix of } y\right\}$$

on $A^*$ is a partial order called the *prefix order*. Similarly, we can define the *suffix order* $\leq_{\mathrm{S}}$ and *infix order* $\leq_{\mathrm{I}}$. Denote the set of all prefixes (suffixes, infixes) of $w$ by $P(w)$ ($S(w)$, $I(w)$). For a language $L$ over $A$, we define $P(L) = \bigcup_{w\in L} P(w)$, $S(L) = \bigcup_{w\in L} S(w)$ and $I(L) = \bigcup_{w\in L} I(w)$. $L$ is said to be *prefix-closed* (*suffix-closed*, *infix-closed*) if $P(L) \subseteq L$ ($S(L) \subseteq L$, $I(L) \subseteq L$). Indeed, these "$\subseteq$" are "$=$", because $w \in P(L)$ ($S(L)$, $I(L)$) for all $w \in L$.

Let $L$ be a language over $A$. We use $lg(L)$ and $Lg(L)$ to represent the minimal and maximal length of words in $L$ respectively. If the above maximal length does not exist, then let $Lg(L) = \infty$. $L$ is called *bounded* if $Lg(L) < \infty$, otherwise $L$ is called *unbounded*. Finite languages are clearly bounded. If $A$ is finite, then $L \subseteq A^*$ is bounded if and only if $L$ is finite.

An abstract definition of "a free semigroup on $A$" can be given as follows: $F$ is a free semigroup on $A$ if there is an injection $\alpha : A \to F$ satisfying for every semigroup $S$ and every homomorphism $\varphi : A \to S$, there exists a unique homomorphism $\psi : F \to S$ such that the diagram




commutes.

The following proposition shows that why we call $A^+(A^*)$ the free semigroup (monoid) over $A$.

**Proposition 1.2.1 ([36, 57])** *Let $A$ be an alphabet, $S$ $(M)$ a semigroup (monoid), $\varphi$ a mapping from $A$ to $S$ $(M)$. Then there exists a unique homomorphism $\overline{\varphi}$ from $A^+$ $(A^*)$ to $S$ $(M)$ such that $\overline{\varphi}|_A = \varphi$. Furthermore, $\overline{\varphi}$ is surjective if and only if $\varphi(A)$ generates $S$ $(M)$.*

***Proof*** If $\overline{\varphi}$ is a homomorphism from $A^+$ $(A^*)$ to $S$ $(M)$, then for any $w = a_1a_2\cdots a_n, a_i \in A, i = 1, 2, \ldots, n, n \in \mathbb{N}$ $(\mathbb{N}^0)$,

$$\begin{aligned} \overline{\varphi}(w) &= \varphi(a_1)\varphi(a_2)\cdots\varphi(a_n), \\ (\overline{\varphi}(w) &= \varphi(a_1)\varphi(a_2)\cdots\varphi(a_n), \\ \overline{\varphi}(w) &= 1_M, \quad n = 0). \end{aligned} \tag{1.2.1}$$

And the mapping $\overline{\varphi}$ from $A^+$ $(A^*)$ to $S$ $(M)$ satisfying (1.2.1) is indeed a homomorphism from $A^+$ $(A^*)$ to $S$ $(M)$. This shows the existence and uniqueness of the homomorphism we require.

The set $\varphi(A)$ generates $S$ $(M)$ if and only if for every $s \in S$ $(m \in M)$, $s$ $(m)$ $= \varphi(b_1)\varphi(b_2)\cdots\varphi(b_n) = \overline{\varphi}(b_1b_2\cdots b_n)$ for some $b_1, b_2, \ldots, b_n \in A, n \in \mathbb{N}$ $(\mathbb{N}^0)$. This is equivalent to $\overline{\varphi}$ is surjective. □

The property above is called the *universal mapping property*. See any book on universal algebras, such as [10], for details.

Usually, a semigroup (monoid) is said to be free if it is isomorphic to $A^+$ $(A^*)$ for some alphabet $A$.

Take $A$ as a generating subset of a semigroup (monoid) $S$ $(M)$ and $\varphi$ as the equality relation $\iota_A$ on $A$, we have

**Corollary 1.2.2** *Any semigroup (monoid) is a homomorphic image of a free semigroup (monoid).*

Next, we discuss some algebraic properties of free semigroups.

**Proposition 1.2.3 ([3, 57, 84])** *A semigroup $S$ is free if and only if every element of $S$ has a unique factorization as a product of elements of $A = S \setminus S^2$.*

***Proof*** The necessity is clear. Conversely, let $\iota : A \to S$ be the inclusion mapping (i.e. $\iota(a) = a$ for any $a \in A$). Extend $\iota$ to an epimorphism $\varphi : A^+ \to S$. Then by the unique factorization property of $S$, $\varphi$ is injective and hence an isomorphism. □

For a free semigroup $S$, the set $A = S \setminus S^2$, the minimum generating set of $S$, is called the *base* of $S$.

A semigroup $S$ is said to be *equidivisible* if for any $a, b, c, d \in S$, $ab = cd$ implies $a = cu$, $ub = d$ or $c = au$, $ud = b$ for some $u \in S^1$.

Clearly, any free semigroup is equidivisible. Moreover, we have the following proposition.

**Proposition 1.2.4 ([57])** *A semigroup $S$ is free if and only if it is equidivisible and $\bigcap_{n=1}^{\infty} S^n = \emptyset$.*

***Proof*** The necessity is obviously. Conversely, since $\bigcap_{n=1}^{\infty} S^n = \emptyset$, we have the chain $S \supseteq S^2 \supseteq \cdots \supseteq S^n \supseteq \cdots$ is strictly descending. Then for any $s \in S$, there exists an integer $k$ such that $s \in S^k \setminus S^{k+1}$ (otherwise $s \in \bigcap_{n=1}^{\infty} S^n$, a contradiction). Thus $s = a_1 a_2 \cdots a_k$ for some $a_i \in A = S \setminus S^2$, $i = 1, 2, \ldots, k$. This shows the existence of factorizations for any $s \in S$. To prove the uniqueness, for any two factorization of $s = a_1 a_2 \cdots a_k = b_1 b_2 \cdots b_l$ of $s$ as products of elements of $A$, we put $n = \min(k, l)$ and proceed by induction on $n$. For $n = 1$ we have $s = a_1 = b_1$ by definition of $A$. For $n > 1$, equidivisibility yields either $a_1 = b_1 u$, $u a_2 a_3 \cdots a_k = b_2 b_3 \cdots b_l$ or $a_1 u = b_1$, $a_2 a_3 \cdots a_k = u b_2 b_3 \cdots b_l$ for some $u \in S^1$. The definition of $A$ gives that $u = 1$, $a_1 = b_1$ and $a_2 a_3 \cdots a_k = b_2 b_3 \cdots b_l$. Then the uniqueness follows from the induction hypothesis applied to $a_2 a_3 \cdots a_k = b_2 b_3 \cdots b_l$. Therefore, by Proposition 1.2.3, $S$ is free. □

The following corollary is known as the Levi's Theorem.

**Corollary 1.2.5 (Levi's Theorem, [62])** *A semigroup $S$ is free if and only if it is equidivisible and there exists a homomorphism $l$ from $S$ to semigroup $\mathbb{N}$ under integer addition.*

***Proof*** We need only to show the sufficiency. For any $s \in S$, if $s \in S^k$, then $s = s_1 s_2 \cdots s_k$ for some $s_i \in S$, $i = 1, 2, \ldots, k$, which implies $l(s) = \sum_{i=1}^{k} l(s_i) \geq k$. Hence $s \notin S^{l(s)+1}$ for any $s \in S$, which implies $\bigcap_{n=1}^{\infty} S^n = \emptyset$. Then by Proposition 1.2.4, $S$ is free. □

The mapping $l$ in the above corollary is called the *length function* on $S$. If there exists a length function on $S$, then $S$ is called a *semigroup with length*.

A nonempty language $C$ over $A$ is called a *code* if

$$x_1 x_2 \cdots x_m = y_1 y_2 \cdots y_n, x_i, y_j \in C, i = 1, 2, \ldots, m, j = 1, 2, \ldots, n$$

implies

$$m = n \quad \text{and} \quad x_i = y_i, \quad i = 1, 2, \ldots, n.$$

A nonempty language $L$ is called a *prefix* (*suffix*, *infix*) *language* over $A$, if no word in $L$ is a prefix (suffix, infix) of another word in $L$, that is, any two different words of $L$ are incomparable with respect to the prefix (suffix, infix) ordering $\leq_P$ ($\leq_S$, $\leq_I$). It is clear that any prefix (suffix, infix) language expect $\{1\}$ is a code, so a prefix (suffix, infix) language expect $\{1\}$ is also called a *prefix* (*suffix*, *infix*) *code*. A *bifix code* is both a prefix code and a suffix code.

We denote the sets of all codes, prefix codes, suffix codes, bifix codes and infix codes over $A$ by $\mathbf{C}(A)$, $\mathbf{P}(A)$, $\mathbf{S}(A)$, $\mathbf{B}(A)$ and $\mathbf{I}(A)$, respectively. Usually, we just discuss codes over alphabet containing at least two letters, since a language $L$ over an one-letter alphabet $A$ is a code if and only if it is a singleton of $A^+$. One can easily show that if $|A| \geq 2$, then

$$\mathbf{I}(A) \subsetneq \mathbf{B}(A) \subsetneq \begin{matrix}\mathbf{P}(A)\\ \mathbf{S}(A)\end{matrix} \subsetneq \mathbf{C}(A).$$

If $S$ is a subsemigroup of $A^+$, then $X = S \setminus S^2$ is the minimal generating set of $S$. Clearly, by Proposition 1.2.3, $S$ is free if and only if $X$ is a code over $A$.

A subset $T$ of a semigroup $S$ is said to be *unitary* (*left unitary*, *right unitary*, *weakly unitary*) if $T^{-1}T \cup TT^{-1} \subseteq T^1$ ($T^{-1}T \subseteq T^1$, $TT^{-1} \subseteq T^1$, $T^{-1}T \cap TT^{-1} \subseteq T^1$).

**Proposition 1.2.6 ([3, 57, 84])** *A subsemigroup $S$ of $A^+$ is free if and only if it is weakly unitary in $A^+$. Moreover, $X \subseteq A^+$ is a code (prefix code, suffix code, bifix code) if and only if $X^+$ is a weakly unitary (left unitary, right unitary, unitary) subsemigroup of $A^+$.*

***Proof*** We only show that a subsemigroup $S$ of $A^+$ is free if and only if it is weakly unitary in $A^+$ (or equivalently, $X$ is a code if and only if $X^+$ is a weakly unitary subsemigroup of $A^+$). The other statements are left to the readers.

Suppose that $S$ is a free subsemigroup of $A^+$. Let $w \in S^{-1}S \cap SS^{-1}$. Then there exist $u, v \in S$ such that $uw, wv \in S$. Since $S$ is free, by equidivisibility, $u(wv) = (uw)v$ implies that there exist $x \in S^1$ such that $u = uwx$ or $ux = uw$. $u = uwx$ implies $w = 1$; $ux = uw$ implies $w = x \in S^1$. Thus $S^{-1}S \cap SS^{-1} \subseteq S^1$ and $S$ is weakly unitary.

Conversely, to prove $S$ is free, by Levi's Theorem, we need only show that $S$ is equidivisible, because any subsemigroup of $A^+$ is with length. Suppose that $ab = cd$, $a, b, c, d \in S$. Then by equidivisibility of $A^+$, there exists $u \in A^*$ such that $a = cu, ub = d$ or $c = au, ud = b$. In either case, $u$ is in $S^{-1}S \cap SS^{-1}$. By the fact that $S$ is weakly unitary, $u \in S^1$. Thus $S$ is equidivisible and hence free. □

**Corollary 1.2.7 ([3, 57, 84])** *The intersection of free subsemigroups of $A^+$ is free if the intersection is not empty.*

For any $X \subseteq A^+$, the intersection of all free subsemigroups of $A^+$ containing $X$ is the minimum free subsemigroup of $A^+$ containing $X$, that is, it is the free semigroup generated by $X$, which is called the *free hull* of $X$.

**Theorem 1.2.8 (Defect Theorem, [84])** *Let $X$ be a finite nonempty language over $A$, and $Y$ the base of the free hull of $X$. If $X$ is not a code, then $|Y| \leq |X| - 1$.*

***Proof*** Consider the mapping $\alpha : X \to Y$ associating to $x \in X$ the word $y \in Y$ such that $x \in yY^*$. Since $Y$ is a code, the mapping $\alpha$ is well defined.

As $X$ is not a code, there exists an equality $x_1 x_2 \cdots x_m = x'_1 x'_2 \cdots x'_n$ with $x_i, x'_j \in X$, $x_1 \neq x'_1$, $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$. Hence $\alpha(x_1) = \alpha(x'_1)$ and $\alpha$ can not be injective.

Now we show that $\alpha$ is surjective. If it is not the case, let $z \in Y$ be such that $z \notin \alpha(X)$. Consider the set $Z = (Y \setminus z)z^*$. One can check that $Z$ is a code over $A$. However, $X \subseteq Z^+ \subsetneq Y^+$, which contradicts the fact that $Y^+$ is the free hull of $X$. □

**Corollary 1.2.9 ([3, 57, 84, 117])** *$X = \{x, y\} \subseteq A^+$ is a code if and only if $x$ and $y$ are not powers of a common word.*

***Proof*** If $x = w^m$ and $y = w^n$ are powers of a common word $w$, then clearly $xy = w^{m+n} = yx$, and hence $X$ is not a code. Conversely, if $X$ is not a code, then by the Defect Theorem, the base of the free hull of $X$ contains only one word, say $w$, which implies $x$ and $y$ are powers of $w$. □

The algebraic properties, generalizations and related topics of free semigroups and monoids have been investigated in many literatures. The researches on Hua semigroups are one of them.

In 1949, L. K. Hua has shown that if $h$ is a mapping from a ring $R$ to a ring $R'$ such that for any $a, b \in R$,

$$h(a + b) = h(a) + h(b), \tag{1.2.2}$$

$$h(ab) = h(a)h(b) \text{ or } h(b)h(a), \tag{1.2.3}$$

then $h$ is either a homomorphism or an anti-homomorphism (see [39]). This result has been included in some texts of algebra as an exercise, for example Jacobson [47, p. 74], where, it is called Hua Theorem.

In 1977, C. M. Reis and H. J. Shyr translated the above result from rings to free semigroups (see [102]). They showed that if $h$ is a mapping from a free semigroup $S$ to itself such that Condition (1.2.3) holds for any $a, b \in S$, then $h$ is either a homomorphism or an anti-homomorphism.

In 2003, K. P. Shum and Y. Q. Guo gave a new proof of Hua Theorem by using group theory, and gave an example which shows that Reis and Shyr's result does not hold generally for arbitrary semigroups (see [112]).

In [80], we have generalized the above Reis and Shyr's result and give some systematic studies of the semigroups in which Reis and Shyr's result holds. We call such semigroups *Hua semigroups* and show that every cancellative semigroup (which is a generalization of free semigroups and monoids) is a Hua semigroup.

## 1.3 Disjunctive (Regular) and Dense Subsets of Semigroups

Let $L$ be a subset of semigroup $S$. For $x \in S$, we define the set of all *contexts of $x$ with respect to $L$* by

$$\mathrm{Cont}_L(x) = \Big\{(u, v) \in S^1 \times S^1 \mid uxv \in L\Big\}.$$

Define the binary relation $P_L$ (or $P_L(S)$) as follows:

$$x P_L y \text{ if and only if } \mathrm{Cont}_L(x) = \mathrm{Cont}_L(y),$$

that is,

$$P_L = \Big\{(x, y) \in S \times S \mid (\forall u, v \in S^1)\ uxv \in L \text{ if and only if } uyv \in L\Big\}.$$

It is easy to see that $P_L$ is a congruence on $S$. We call it *syntactic congruence (or principal congruence) on $S$ determined by* $L$. The *index* of $P_L$ is the number of $P_L$-classes, denoted by $|P_L|$. The natural homomorphism $P_L^{\natural}$ is usually called *the syntactic homomorphism* determined by $L$ and denoted by $\varphi_L$. The $P_L$-class containing $x$ is denoted by $[x]_L$ for any $x \in S$.

The *left* (*right*) *principal congruence* determined by $L$, denoted by $P_L^{(l)}$ ($P_L^{(r)}$), is defined similarly by using left (right) contexts of elements of $S$ with respect to $L$. For example,

$$P_L^{(l)} = \Big\{(x, y) \in S \times S \mid (\forall u \in S^1)\ ux \in L \text{ if and only if } uy \in L\Big\}.$$

Clearly, $P_L = P_{L^c}$, and $P_L \subseteq P_L^{(l)}$ ($P_L^{(r)}$). In fact, we have

**Proposition 1.3.1** *$P_L$ ($P_L^{(l)}$, $P_L^{(r)}$) is the largest congruence (left congruence, right congruence) on $S$ saturating $L$.*

***Proof*** Immediate. □

Let $L$ be any subset of a semigroup $S$. Then $L$ is said to be *disjunctive* in $S$ (or a *disjunctive subset* of $S$) if $P_L = \iota_S$, the equality on $S$. Denote all disjunctive subsets of $S$ by $\mathbf{D}(S)$. $L$ is said to be *regular* in $S$ (or a *regular subset* of $S$) if the index of $P_L$ is finite. Denote all regular subsets of $S$ by $\mathbf{R}(S)$.

Let $L \subseteq A^+$ ($L \subseteq A^*$), $P_L$ the syntactic congruence of $L$ on $A^+$ ($A^*$). We call $A^+/P_L$ ($A^*/P_L$) the *syntactic semigroup* (*syntactic monoid*) of $L$ and denoted by $\mathbf{S}(L)$ ($\mathbf{M}(L)$). A semigroup (monoid) is said to be *syntactic* if it is isomorphic to the syntactic semigroup (monoid) of some language.

In the rest of this section, we only deal with free semigroups. The corresponding properties for free monoids can be similarly obtained.

**Lemma 1.3.2 ([3, 57])** *Let $A$ be an alphabet, $S$ a semigroup.*

(1) *For any epimorphism $\theta : A^+ \to S$, $P \subseteq S$ and $L = \theta^{-1}(P)$, there exists a unique epimorphism $\sigma : S \to \mathbf{S}(L)$ such that the diagram*

$$\begin{array}{ccc} L = \theta^{-1}(P) \subseteq A^+ & \xrightarrow{\ \theta\ } & S \supseteq P \\ \varphi_L \big\downarrow & \swarrow_{\sigma} & \\ \mathbf{S}(L) & & \end{array}$$

*commutes, where $\varphi_L$ is the syntactic homomorphism of $L$.*

(2) *Conversely, if for some $L \subseteq A^+$, $\sigma : S \to \mathbf{S}(L)$ is an epimorphism, then there exist a homomorphism $\theta : A^+ \to S$ and $P \subseteq S$ such that $L = \theta^{-1}(P)$ and $\varphi_L = \sigma \circ \theta$, that is, the diagram*

$$\begin{array}{ccc} L = \theta^{-1}(P) \subseteq A^+ & \xrightarrow{\ \theta\ } & S \supseteq P \\ \varphi_L \big\downarrow & \swarrow_{\sigma} & \\ \mathbf{S}(L) & & \end{array}$$

*commutes.*

***Proof***

(1) By Theorem 1.1.1, we need only show that $\ker\theta \subseteq P_L$, which is true by Proposition 1.3.1 since $\ker\theta$ saturates $L$.

(2) For any $a \in A$, we choose $s_a \in S$ such that $\sigma(s_a) = \varphi_L(a)$. This is possible, since $\sigma$ is surjective. Putting $\theta(a) = s_a$, we extend $\theta$ to a homomorphism from $A^+$ to $S$ and also denote it by $\theta$. Then by definition of $\theta$, $\sigma \circ \theta = \varphi_L$. Let $P = \sigma^{-1}\varphi_L(L)$. Then we have

$$\theta^{-1}(P) = \theta^{-1}\sigma^{-1}\varphi_L(L) = \varphi_L^{-1}\varphi_L(L) = L.$$

□

The following proposition encourages us more or less to study disjunctive subsets of general semigroups (especially the existence problem).

**Proposition 1.3.3 ([57])** *A semigroup is syntactic if and only if it contains a disjunctive subset.*

***Proof*** Let $L \subseteq A^+$ and $\varphi_L : A^+ \to \mathbf{S}(L) = A^+/P_L$ be the syntactic homomorphism, $X = \varphi_L(L)$. Since $\varphi_L = P_L^\natural$ and $P_L$ saturates $L$, $\varphi^{-1}(X) = L$. We show that $X$ is disjunctive in $\mathbf{S}(L)$. In fact, suppose that $(s_1, s_2) \in P_X$, then $xs_1y \in X$ if and only if $xs_2y \in X$ for all $x, y \in \mathbf{S}(L)^1$. Let $w_1, w_2 \in A^+$ be such that

$\varphi_L(w_i) = s_i$, $i = 1, 2$. Then we have for any $u, v \in A^*$,

$$uw_1v \in L \Leftrightarrow \varphi_L(u)s_1\varphi_L(v) \in X \Leftrightarrow \varphi_L(u)s_2\varphi_L(v) \in X \Leftrightarrow uw_2v \in L.$$

It follows that $(w_1, w_2) \in P_L$, that is, $s_1 = s_2$.

Conversely, in view of Corollary 1.2.2, let $\theta$ be an epimorphism from $A^+$ to $S$. If $X \subseteq S$ is disjunctive in $S$ and $L = \theta^{-1}(X)$, then by Lemma 1.3.2, there exists an epimorphism $\sigma : S \to \mathbf{S}(L)$ such that $\varphi_L = \sigma \circ \theta$. For $s_1, s_2 \in S$, assume that $\sigma(s_1) = \sigma(s_2)$, or equivalently that $\varphi_L(w_1) = \varphi_L(w_2)$ for some $w_1, w_2 \in A^+$ such that $\theta(w_i) = s_i$, $i = 1, 2$. For any $x, y \in S^1$, if $xs_1y \in X$, then there are $u, v \in A^*$ such that $\theta(u) = x$, $\theta(v) = y$ and $\theta(uw_1v) \in X$, so $uw_1v \in L$. But $\varphi_L(uw_1v) = \varphi_L(uw_2v)$, it follows that $uw_2v \in L$ and $xs_2y \in \theta(L) = X$. Similarly, $xs_2y \in X$ implies $xs_1y \in X$. Since $X$ is disjunctive in $S$, $s_1 = s_2$. This shows that $\sigma$ is injective and hence an isomorphism. □

Let $S$ be a semigroup, $L \subseteq S$. An element $x \in S$ is called *completable* (*left completable*, *right completable*) in $L$ if

$$(\exists u, v \in S^1)\ uxv \in L$$

$$((\exists u \in S^1)\ ux \in L, (\exists u \in S^1)\ xu \in L).$$

An element which is not [left, right] completable in $L$ is called [*left*, *right*] *incompletable*. $L$ is said to be *dense* in $S$ if every element of $S$ is completable in $L$ (or equivalently, for any $x \in S$, $S^1xS^1 \cap L \neq \emptyset$). Otherwise, we call it *thin* (or *non-dense*). Similarly we can define *left* (*right*) *dense* and *left* (*right*) *thin subsets* of $S$. If a [left, right] dense subset $L$ is a singleton, the unique element of $L$ is called a [*left*, *right*] *dense element* of $S$. If the subsemigroup generated by $L$ is [left, right] dense, then $L$ is said to be [*left*, *right*] *complete*, otherwise, $L$ is said to be [*left*, *right*] *incomplete*.

A disjunctive (regular, dense, left dense, right dense, thin, left thin, right thin) subset of a free semigroup $A^+$ is usually called a *disjunctive* (*regular*, *dense*, *left dense*, *right dense*, *thin*, *left thin* , *right thin) language* over $A$.

In the following proposition, we list some basic properties about dense subsets, which will be used in this book.

**Proposition 1.3.4** *Let $S$ be a semigroup, $X, Y \subseteq S$. Then*

(1) *$S$ is dense in itself, $\emptyset$ is thin in $S$;*
(2) *If $X$ is dense in $S$, $Y \supseteq X$, then $Y$ is dense in $S$;*
(3) *$X \cup Y$ is dense in $S$ if and only if at least one of $X$ and $Y$ is dense in $S$;*
(4) *At least one of $X$ and its complement is dense in $S$;*
(5) *If $X$ and $Y$ are nonempty and at least one of them is dense in $S$, then $XY$ is dense in $S$;*
(6) *The intersection of a dense subset and an ideal of $S$ is dense in $S$.*

***Proof*** (1) and (2) are direct consequences of the definition of density.

(3) If one of $X$ and $Y$ is dense, then by (2), $X \cup Y$ is dense. Conversely, If both $X$ and $Y$ are thin, then there are $x, y \in S$ such that $S^1xS^1 \cap X = \emptyset$ and $S^1yS^1 \cap Y = \emptyset$. Then $S^1xyS^1 \cap (X \cup Y) = \emptyset$. That is $X \cup Y$ is thin.

(4) is a direct consequence of (1) and (3).

(5) Suppose, without loss of generality, that $X$ is dense. Then for any $x \in S$, $S^1xS^1 \cap X \neq \emptyset$. Since $Y$ is not empty, we have $S^1xS^1 \cap XY \supseteq (S^1xS^1 \cap X)Y \neq \emptyset$. Thus $XY$ is dense.

(6) Let $D$ be a dense subset and $I$ be an ideal of $S$. Then for any $x \in S$, $y \in I$, there are $u, v \in S^1$ such that $uxyv \in D$. Clearly, $uxyv \in I$. Hence $uxyv \in D \cap I$. That is, $D \cap I$ is a dense subset of $S$. □

**Proposition 1.3.5** *Let $S$ be a semigroup with zero $0$, $L \subseteq S$. Then*

(1) *$L$ is dense if and only if $0 \in L$;*
(2) *$L$ is dense if and only if $L^c$ is thin;*
(3) *If $L$ is disjunctive, then $S$ contains both dense and thin disjunctive subsets.*

***Proof***

(1) Since 0 is a dense element of $S$, the sufficiency is a direct consequence of Proposition 1.3.4.
    On the other hand, suppose that $0 \notin L$. Then 0 is incompletable in $L$. Hence $L$ is not dense.
(2) Which can be directly derived from (1).
(3) Since the complement of disjunctive subsets of $S$ is also disjunctive, by Proposition 1.3.4 and (2), the statement is clear.

□

**Proposition 1.3.6** *Let $S$ be a semigroup without zero. Then any disjunctive subset of $S$ is dense.*

***Proof*** Suppose that $L \subseteq S$ is disjunctive, but not dense. Then there exists $w \in S$ such that $S^1wS^1 \cap L = \emptyset$. Since $S^1uwvS^1 \subseteq S^1wS^1$, we have $S^1uwvS^1 \cap L = \emptyset$ for any $u, v \in S^1$. Hence $S^1wS^1 \subseteq [w]_L = \{w\}$. This shows that $w$ is the zero element of $S$, a contradiction. □

For any subset $L$ of a semigroup $S$, the *residue* of $L$ is the set

$$\mathbf{W}(L) = \left\{x \in S \mid S^1xS^1 \cap L = \emptyset\right\}.$$

Clearly, $L$ is dense in $S$ if and only if $\mathbf{W}(L) = \emptyset$. If $\mathbf{W}(L)$ is not empty, then it is an ideal as well as a $P_L$-class of $S$. Thus it is the zero element of $S/P_L$. Furthermore, we have

**Proposition 1.3.7** *For any subset $L$ of a semigroup $S$, the following statements are equivalent:*

(1) *Both $L$ and $L^c$ are dense;*
(2) *$\mathbf{W}(L) = \mathbf{W}(L^c) = \emptyset$;*

(3) *$S/P_L$ has not the zero element;*
(4) *Either $S$ contains no dense $P_L$-class, or contains at least two.*

***Proof*** The equivalence of (1) and (2) is a direct consequence of the definition of $\mathbf{W}(L)$.

(2) $\Rightarrow$ (3). If $Z$ is the zero element of $S/P_L$, then $S^1ZS^1 \subseteq Z$. Let $w \in Z$. If $w \notin L$, then, since $Z$ is a $P_L$-class and $P_L$ saturates $L$, we have $Z \cap L = \emptyset$, and hence $S^1wS^1 \cap L = \emptyset$. This implies that $w \in \mathbf{W}(L)$, which contradicts to $\mathbf{W}(L) = \emptyset$. If $w \notin L^c$, then, similarly, we have $w \in \mathbf{W}(L^c)$, which contradicts to $\mathbf{W}(L^c) = \emptyset$. Thus $S/P_L$ has not the zero element.

(3) $\Rightarrow$ (4). Suppose that $S$ contains exactly one dense $P_L$-class $Z = [z]_L$. Then for any $w \in S$, we have $wZ \subseteq [wz]_L$ and $Zw \subseteq [zw]_L$. By Proposition 1.3.4, we know that $wZ$ ($Zw$) and hence $[wz]_L$ ($[zw]_L$) is dense in $S$. Thus $[wz]_L = [zw]_L = Z$, which implies $Z = [z]_L$ is the zero element of $S/P_L$.

(4) $\Rightarrow$ (2). If $\mathbf{W}(L) \neq \emptyset$, then $\mathbf{W}(L)$ is a dense $P_L$-class. Since $\mathbf{W}(L)$ is an ideal, by Proposition 1.3.4, $\mathbf{W}(L)^c$ is not dense. Hence $S$ contains only one dense $P_L$-class, a contradiction. Similarly, $\mathbf{W}(L^c) \neq \emptyset$ is impossible either. □

**Proposition 1.3.8** *Let $S$ and $T$ be two semigroups, $\varphi : S \to T$ an epimorphism, $X \subseteq S$ and $Y \subseteq T$.*

(1) *If $X$ is dense then so is $\varphi(X)$.*
(2) *If $Y$ is dense then so is $\varphi^{-1}(Y)$.*

***Proof***

(1) Let $y$ be any element in $T$. Since $\varphi$ is surjective, there exists $x \in S$ such that $\varphi(x) = y$. Now by the density of $X$, there exist $u, v \in S$ such that $uxv \in X$. Then $\varphi(u)y\varphi(v) = \varphi(uxv) \in \varphi(X)$. Hence $\varphi(X)$ is dense.
(2) Let $x$ be any element in $S$ and $y = \varphi(x)$. Then by the density of $Y$, there exist $s, t \in T$ such that $syt \in Y$. Since $\varphi$ is surjective, we have $s = \varphi(u)$ and $t = \varphi(v)$ for some $u, v \in S$. Then $\varphi(uxv) = \varphi(u)\varphi(x)\varphi(v) = syt \in Y$. That is $uxv \in \varphi^{-1}(Y)$. Hence $\varphi^{-1}(Y)$ is dense.

□

At the end of this section, we give a description of dense elements in a semigroup.

**Proposition 1.3.9** *Let $S$ be a semigroup. Then the set of all dense elements is*

$$K(S) = \bigcap \{I \mid I \text{ is an ideal of } S\}.$$

*Therefore, $S$ contains dense elements if and only if $S$ has the minimum ideal.*

***Proof*** By the definition of density, $L \subseteq S$ is a dense subset of $S$ if and only if $L$ intersects with every ideal of $S$. Hence $x \in S$ is a dense element of $S$ if and only if $x$ is contained in every ideal of $S$, that is, if and only if $x \in K(S)$. Thus $K(S)$ is the set of all dense elements of $S$. Clearly, $K(S)$, if nonempty then, is the minimum ideal of $S$. Thus, $S$ contains dense elements if and only if $S$ has the minimum ideal. □