afcs
ALGEBRAIC FOUNDATIONS of COMPUTER SCIENCE
lectures by Ferucio Laurentiu Tiplea

Semigroups and Monoids

Prof.dr. Ferucio Laurențiu Țiplea

Spring 2022

Department of Computer Science
“Alexandru Ioan Cuza” University of Iași
Iași 700506, Romania

e-mail: ferucio.tiplea@uaic.ro

Outline

Definition and examples

Semigroups

Definition 1

A semigroup is a pair $(S, \circ)$ which consists of a set S and an associative binary operation $\circ$ on S.

Definition 2

A semigroup $(S, \circ)$ is called commutative if $\circ$ is a commutative operation.

Remark 3

- *Associativity of a binary operation $\circ$ means that the order of evaluation of an expression $a_1 \circ a_2 \circ a_3$, without changing the order of the terms, is immaterial. In other words, no parenthesis is required for an associative operation;*
- *Commutativity of a binary operation $\circ$ means that the order of the operands in expressions like $a_1 \circ a_2$ is immaterial.*

Examples of semigroups

Example 4

1. $(\mathbb{N},+)$, $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, and $(\mathbb{C},+)$ are (additive) semigroups;
2. $(\mathbb{N},\cdot)$, $(\mathbb{Z},\cdot)$, $(\mathbb{Q},\cdot)$, $(\mathbb{R},\cdot)$, and $(\mathbb{C},\cdot)$ are (multiplicative) semigroups;
3. Let $n \in \mathbb{Z}$ and $n\mathbb{Z} = \{n \cdot x | x \in \mathbb{Z}\}$. Then, $(n\mathbb{Z},+)$ and $(n\mathbb{Z},\cdot)$ are semigroups;
4. Let $m \in \mathbb{Z}$. Then, $(\mathbb{Z}_m,+)$ and $(\mathbb{Z}_m,\cdot)$, where $+$ and $\cdot$ are the addition and multiplication modulo m, are semigroups.

All semigroups in Example 4 are commutative.

Monoids

Definition 5

A monoid is a triple $(M, \circ, e)$ which consists of a set M, an associative binary operation $\circ$ on M, and an element $e \in M$ such that

$$x \circ e = e \circ x = x,$$

for any $x \in M$. e is called the identity element or the unity of M.

Remark 6

The identity of any monoid $(M, \circ, e)$ is unique. For, if we assume that e' is an identity too, then $e = e \circ e' = e'$.

The identity of a monoid $(M, \circ, e)$ is usually denoted by 1_M or even 1.

Definition 7

A monoid $(M, \circ, e)$ is called commutative if its binary operation $\circ$ is commutative.

Examples of monoids

Example 8

1. $(\mathbb{N}, +, 0)$, $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, +, 0)$, and $(\mathbb{R}, +, 0)$ are commutative monoids;
2. $(\mathbb{N}, \cdot, 1)$, $(\mathbb{Z}, \cdot, 1)$, $(\mathbb{Q}, \cdot, 1)$, and $(\mathbb{R}, \cdot, 1)$ are commutative monoids;
3. $(n\mathbb{Z}, +, 0)$ is a commutative monoid and $(n\mathbb{Z}, \cdot)$ is a commutative semigroup. $(n\mathbb{Z}, \cdot)$ has unity only if $n = 0$ or $n = 1$ and, in such a case it becomes commutative monoid;
4. $(\mathbb{Z}_m, +, 0)$ and $(\mathbb{Z}_m, \cdot, 1)$ are commutative monoids. When $m = 1$, $\mathbb{Z}_1 = \{0\}$ and the multiplicative unity of this monoid is 0.

Some basic notations

1. Let $(S, \circ)$ be a semigroup, $A, B \subseteq S$, and $a \in S$. Define:
   - $AB = \{a \circ b | a \in A \ \wedge \ b \in B\}$;
   - $A^1 = A$ and $A^{n+1} = A^n A$, for all $n \geq 1$;
   - $aB = \{a \circ b | b \in B\}$;
   - $a^1 = a$ and $a^{n+1} = a^n \circ a$, for all $n \geq 1$.
2. If $(M, \circ, e)$ is a monoid, $A \subseteq M$, and $a \in M$, we also define:
   - $A^0 = \{e\}$;
   - $a^0 = e$.
3. For any monoid $(M, \circ, e)$ define $S_M = M - \{e\}$.

Definition 9

Let $(S, \circ)$ be a semigroup and I a non-empty subset of S.

1. I is called a left ideal of $(S, \circ)$ if $SI \subseteq I$.
2. I is called a right ideal of $(S, \circ)$ if $IS \subseteq I$.
3. I is called an ideal of $(S, \circ)$ if I is a left and a right ideal of $(S, \circ)$.
4. The least (left, right) ideal of $(S, \circ)$ which includes I is called the (left, right) ideal of $(S, \circ)$ generated by I. It is denoted by $\langle I \rangle$.
5. If $I = \{a\}$, then $\langle I \rangle$ is called a (left, right) principal ideal of $(S, \circ)$. It is also denoted by $\langle a \rangle$.

(Left, Right) Ideals of monoids are defined in a similar way.

Example 10

The principal ideal of $(\mathbb{Z}, \cdot, 1)$ generated by $n \in \mathbb{Z}$ is $n\mathbb{Z}$.

Sub-semigroups and generators

Definition 11

1. A semigroup $(S', \circ')$ is a sub-semigroup of a semigroup $(S, \circ)$, denoted $(S', \circ') \leq (S, \circ)$, if $S' \subseteq S$ and $\circ' = \circ|_{S'}$.
2. A monoid $(M', \circ', e')$ is a sub-monoid of a monoid $(M, \circ, e)$, denoted $(M', \circ', e') \leq (M, \circ, e)$, if $M' \subseteq M$ and $\circ' = \circ|_{M'}$ and $e' = e$.
3. The least subsemigroup (monoid) of a semigroup (monoid) which includes a given subset A, denoted $\langle A \rangle$, is called the sub-semigroup (sub-monoid) generated by A.
4. A semigroup (monoid) is generated by a subset A of it if it coincides with the sub-semigroup (sub-monoid) generated by A.

The set A in Definition 11(3)(4) is called a set of generators and its elements are called generators.

Sub-semigroups and closures

Remark 12

The sub-semigroup (sub-monoid) of a semigroup (monoid), generated by a subset A, is the closure of A under the operation(s) of the host semigroup (monoid):

- *If $(S, \circ)$ is a semigroup and $A \subseteq S$, then the sub-semigroup generated by A is the set of all products*

$$a_1 \circ \cdots \circ a_n,$$

  where $n \geq 1$ and $a_1, \ldots, a_n \in A$;
- *If $(M, \circ, e)$ is a monoid and $A \subseteq M$, then the sub-monoid generated by A is obtained as above by including supplementary the unity e of the monoid.*

Examples of sub-semigroups

Example 13

- $(\mathbb{N}, +) \leq (\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$;
- $(\mathbb{N}, +, 0) \leq (\mathbb{Z}, +, 0) \leq (\mathbb{Q}, +, 0) \leq (\mathbb{R}, +, 0)$;
- $(\mathbb{N}, \cdot) \leq (\mathbb{Z}, \cdot) \leq (\mathbb{Q}, \cdot) \leq (\mathbb{R}, \cdot)$;
- $(\mathbb{N}, \cdot, 1) \leq (\mathbb{Z}, \cdot, 1) \leq (\mathbb{Q}, \cdot, 1) \leq (\mathbb{R}, \cdot, 1)$;
- The sub-monoid of $(\mathbb{Z}, +, 0)$, generated by $n \in \mathbb{Z}$, is $(n\mathbb{N}, +, 0)$;
- A semigroup (monoid) may have more than one set of generators. For instance, $(\mathbb{Z}, +, 0)$ can be generated by $\{-1, 1\}$ and by $\{-3, 2\}$.

Order of an element

Definition 14

1. The order of a semigroup (monoid) is the number of its elements if the semigroup (monoid) is finite, and ∞, otherwise.
2. The order of an element a of a semigroup (monoid) is the order of the sub-semigroup (sub-monoid) generated by a.

Example 15

- $(\mathbb{Z}, +, 0)$ has the order ∞;
- $(\mathbb{Z}_m, +, 0)$ has the order m, if $m \neq 0$. For $m = 0$, $(\mathbb{Z}_m, +, 0)$ has the order ∞.

Homomorphisms

Definition 16

1. A function $f : S \to S'$ is a homomorphism from a semigroup $(S, \circ)$ to a semigroup $(S', \circ')$ if
   - $f(a \circ b) = f(a) \circ' f(b)$, for any $a, b \in S$.
2. A function $f : M \to M'$ is a homomorphism from a monoid $(M, \circ, e)$ to a monoid $(M', \circ', e')$ if
   - $f(a \circ b) = f(a) \circ' f(b)$, for any $a, b \in M$;
   - $f(e) = e'$.

Related concepts:

- injective homomorphism = monomorphism;
- surjective homomorphism = epimorphism;
- bijective homomorphism = isomorphism;

Homomorphisms

- Homomorphism from a semigroup (monoid) to the same semigroup (monoid) = endomorphism;
- Isomorphism from a semigroup (monoid) to the same semigroup (monoid) = automorphism.

Example 17

- The function $f(x) = 2^x$, for any $x \in \mathbb{N}$, is a homomorphism from $(\mathbb{N}, +, 0)$ to $(\mathbb{N}, \cdot, 1)$. Indeed,
  - $f(0) = 2^0 = 1$;
  - $f(x+y) = 2^{x+y} = 2^x \cdot 2^y = f(x) \cdot f(y)$, for any x, y.

  Moreover, f is injective but not surjective. Therefore, f is a monomorphism (but not an epimorphism).

Word semigroups

Alphabet

Definition 18

An alphabet is any non-empty set. The elements of an alphabet are called letters or symbols.

Example 19

The following sets are alphabets:

- $\Sigma_1 = \{a, b, c\}$;
- $\Sigma_2 = \{0, 1, 2, 3\}$;
- $\Sigma_3 = \{\mathtt{begin}, \mathtt{end}, \mathtt{if}, \mathtt{then}, \mathtt{else}, \mathtt{while}, \mathtt{do}\}$.

All letters of an alphabet are assumed indivisible.

Words

Definition 20

Let Σ be an alphabet. A word of length $k \geq 1$ over Σ is any function $w : \{1, \ldots, k\} \to \Sigma$. The empty function from $\emptyset$ into Σ is called the empty word over Σ and its length is 0.

We usually denote the word w by $w = w(1) \cdots w(k)$, if $k > 0$, and its length k by $|w|$. The empty word is usually denoted by λ.

Example 21

- $w = abaa$ is a word of length 4 over $\Sigma_1 = \{a, b, c\}$;
- 011033 is a word of length 6 over $\Sigma_2 = \{0, 1, 2, 3\}$;
- `begin end` is a word of length 2 over $\Sigma_3 = \{\mathtt{begin}, \mathtt{end}, \mathtt{if}, \mathtt{then}, \mathtt{else}, \mathtt{while}, \mathtt{do}\}$.

Word equality

Let Σ be an alphabet. Denote:

- $\Sigma^0 = \{\lambda\}$;
- $\Sigma^+ = \bigcup_{k\geq 1} \Sigma^k$,
- $\Sigma^* = \bigcup_{k\geq 0} \Sigma^k = \Sigma^+ \cup \{\lambda\}$.

Words of length 1 are usually identified with letters. Therefore, we may write $\Sigma^1 = \Sigma$.

Definition 22

Two words u and v over the same alphabet Σ are called equal if they have the same length k and $u(i) = v(i)$, for each $1 \leq i \leq k$.

Concatenation of words

Definition 23

Let Σ be an alphabet. The binary operation $\cdot : \Sigma^* \times \Sigma^* \to \Sigma^*$ given by

$$w_1 \cdot w_2 : \{i | 1 \leq i \leq |w_1| + |w_2|\} \to \Sigma$$

where

$$(w_1 \cdot w_2)(i) = \begin{cases} w_1(i), & \text{if } 1 \leq i \leq |w_1| \\ w_2(i - |w_1|), & \text{otherwise,} \end{cases}$$

for any i, is called the concatenation or catenation operation on Σ^*.

Example 24

- $abba \cdot bbaa = abbabbaa$;
- $\lambda \cdot w = w \cdot \lambda = w$, for any w.

The concatenation operation symbol is usually omitted. That is, we write uv instead of $u \cdot v$.

Word semigroups

Theorem 25

Let Σ be an alphabet. Then:

1. $(\Sigma^+, \cdot)$ *is a semigroup generated by* Σ*;*
2. $(\Sigma^*, \cdot, \lambda)$ *is a monoid generated by* Σ*;*
3. $(\Sigma^*, \cdot, \lambda)$ *is a monoid with simplification;*
4. $l : \Sigma^* \to \mathbb{N}$ *given by* $l(w) = |w|$*, for any* $w \in \Sigma^*$*, is a homomorphism from* $(\Sigma^*, \cdot, \lambda)$ *to the additive monoid* $(\mathbb{N}, +, 0)$*. Moreover,* $l^{-1}(0) = \{\lambda\}$*;*
5. *The group of units of the monoid* $(\Sigma^*, \cdot, \lambda)$ *is trivial.*

It is a good exercise for you to prove Theorem 25 (textbook [1], page 212).

Sub-words

Definition 26

Let Σ be an alphabet and $u, v \in \Sigma^*$.

1. u is called a prefix or left factor of v if $v = uw$ for some word w.
2. u is called a suffix or right factor of v if $v = wu$ for some word w.
3. u is called a sub-word of v if $v = xuy$ for some words x and y.

Theorem 27 (Levi's Theorem)

Let x, y, u, and v be words over Σ such that $xy = uv$.

1. *If $|x| < |u|$, then there exists a unique $z \in \Sigma^*$ such that $u = xz$.*
2. *If $|x| = |u|$, then $x = u$ and $y = v$.*
3. *If $|x| > |u|$, then there exists a unique $z \in \Sigma^*$ such that $x = uz$.*

It is a good exercise for you to prove Theorem 27 (textbook [1], page 212).

Lexicographic order on words

Definition 28

(1) A pair $(\Sigma, \prec)$ which consists of an alphabet Σ and a total order $\prec$ on Σ is called an ordered alphabet.

(2) Let $(\Sigma, \prec)$ be an ordered alphabet. The binary relation $\leq_{(\Sigma,\prec)}$ given by

$$x \leq_{(\Sigma,\prec)} y$$

iff

- x is a prefix of y, or
- $x = uav$, $y = ubw$, and $a \prec b$, for some $u, v, w \in \Sigma^*$ and $a, b \in \Sigma$ with $a \neq b$,

is called the direct lexicographic order on $(\Sigma, \prec)$.

In a similar way one can define the inverse lexicographic order on ordered alphabets.

Lexicographic order on words

a)	b)
λ	λ
a	a
aa	b
aaa	aa
$\cdots$	ab
$aaaab$	ba
$aaab$	bb
aab	aaa
ab	aab
$\cdots$	$\cdots$
b	bbb

a) Lexicographic order

b) Lexicographic order on words of the same length.

Cyclic semigroups

Cyclic semigroups

If $\mathbb{S} = (S, \circ)$ is a semigroup and $a \in S$, then

$$\langle a \rangle_{\mathbb{S}} = \{a, a^2, \ldots, a^n, \ldots\}$$

If $\mathbb{M} = (M, \circ, e)$ is a monoid $a \in M$, then

$$\langle a \rangle_{\mathbb{M}} = \{e = a^0, a, a^2, \ldots, a^n, \ldots\}$$

Definition 29

A semigroup (monoid) generated by one of its elements is called a cyclic semigroup (cyclic monoid).

$\mathbb{S}$ cyclic semigroup $\Rightarrow S = \{a, a^2, \ldots, a^n, \ldots\}$, for some $a \in S$.

$\mathbb{M}$ cyclic monoid $\Rightarrow M = \{e = a^0, a, a^2, \ldots, a^n, \ldots\}$, for some $a \in M$.

Theorem of cyclic semigroups

Theorem 30

Let a be an element of a semigroup $(S, \circ)$. Then, exactly one of the following two properties is satisfied:

(1) $a^n \neq a^m$ *for any* $n \neq m$*, and the semigroup generated by* a *is isomorphic with* $(\mathbb{N} - \{0\}, +)$*;*

(2) *there exists* $m > 0$ *and* $r > 0$ *such that :*

  (a) $a^m = a^{m+r}$*;*

  (b) $a^{m+u} = a^{m+v}$ *iff* $u \equiv v \mod r$*, for any* $u, v \in \mathbb{N}$*;*

  (c) $\langle a \rangle = \{a, a^2, \ldots, a^{m+r-1}\}$ *has exactly* $m + r - 1$ *elements;*

  (d) $K(a) = \{a^m, \ldots, a^{m+r-1}\}$ *is a cyclic subgroup of* $\langle a \rangle$*.*

Proof.

See textbook [1], pages 219-220. □

order = index + period - 1

The number m in Theorem 30(2) is called the index of a, and r is called the period of a, in $(S, \circ)$. The following property holds true:

$$order(\mathrm{a}) = index(\mathrm{a}) + period(\mathrm{a}) - 1$$

Definition 31

A semigroup (monoid) is called periodic if each element of it has a finite order.

Clearly, finite semigroups (monoids) are periodic.

Free semigroups and monoids

Free semigroups and monoids

Remark 32

- *The monoid* $(\mathbb{N}, +, 0)$ *can be generated by* $\{1\}$*. Moreover, any number* $n \in \mathbb{N} - \{0\}$ *can uniquely be written as a finite combination of* 1*'s under* $+$*, namely,*

$$n = \underbrace{1 + 1 + \cdots + 1}_{n \ \textit{times}}.$$

We say that $\{1\}$ *freely generates the monoid.*

Definition 33

A semigroup $(S, \circ)$ is freely generated by a subset $X \subseteq S$ if any element $s \in S$ can uniquely be written as a finite combination of elements in X,

$$s = x_1 \circ \cdots \circ x_n,$$

where $x_1, \ldots, x_n \in X$ and $n \geq 1$.

Free generators

Definition 34

A monoid $(M, \circ, e)$ is freely generated by a subset $X \subseteq M$ if $(S_M, \circ)$ is freely generated by X.

Definition 35

A free semigrup (free monoid) is a semigroup (monoid) which can be freely generated by some subset of it.

If X freely generates a semigroup, then it is called a set of free generators of the semigroup (monoid).

Example 36

- $(\mathbb{N}, +, 0)$ is a free monoid.
- X^+ (X^*) together with the concatenation operation is a free semigroup (monoid), for any non-empty set X.
- $(\mathbb{Z}, +, 0)$ is not a free monoid.

The universality property

Theorem 37 (The universality property)

If $(S, \circ)$ is a semigroup freely generated by X, then for any semigroup $(T, *)$ and any function $f : X \to T$, there exists a unique homomorphism $h : S \to T$ which extends f (that is, $h(x) = f(x)$, for any $x \in X$).

Proof.

See textbook [1], page 225. □

The universality property can be similarly formulated for free monoids.

Corollary 38

Any free semigroup (monoid) is isomorphic with a word semigroup (monoid).

Proof.

See textbook [1], page 225. □

The universality property allows us to define homomorphisms from free semigroups $(S, \circ)$ to semigroups $(T, *)$ just by defining them on sets of free generators of $(S, \circ)$.

Example 39

To define a homomorphism from $(\mathbb{N}, +, 0)$ to $(\mathbb{N}, \cdot, 1)$ it is sufficient to consider an arbitrary function from $\{1\}$, which freely generates $(\mathbb{N}, +, 0)$, to $(\mathbb{N}, \cdot, 1)$. For example, if we consider the function $f(1) = 10$, then the unique homomorphism induced by f is:

- $h(0) = 1$;
- $h(1) = f(1) = 10$;
- $h(2) = h(1 + 1) = h(1) \cdot h(1) = 10^2$;
- $h(3) = h(1 + 1 + 1) = h(1) \cdot h(1) \cdot h(1) = 10^3$;
- $h(n) = 10^n$, for any $n \geq 0$.

Free semigroups and monoids

How many sets of free generators may have a free semigroup or monoid?

Proposition 40

If a semigroup $(S, \circ)$ (monoid $(M, \circ, e)$) is free, then it has a unique set of free generates, and this set is $S - S^2$ ($S_M - S_M^2$).

Proof.

First, show that any set of generators should include $S - S^2$ ($S_M - S_M^2$).

Then, show that any set X of generators should be a subset of $S - S^2$ ($S_M - S_M^2$). □

Reading and exercise guide

Reading and exercise guide

It is highly recommended that you do all the exercises marked in red from the slides.

Course readings:

1. Pages 203-235 from textbook [1].

References

[1] Ferucio Laurențiu Țiplea. *Algebraic Foundations of Computer Science*. “Alexandru Ioan Cuza” University Publishing House, Iași, Romania, second edition, 2021.