Automata and Profiniteness

Sam van Gool

October/November 2020

About these notes

These are the notes accompanying a short lecture course on *automata and profinitess*, the second part of the course *Automates et modèles de calcul* in the Parisian Master of Research in Computer Science (MPRI) in the year 2020-2021.
A particularity of these lectures, compared to existing courses with comparable aims such as the excellent reference [2][1], to which these notes owe a lot, is that we throw *duality theory* into the mix of automata, monoids and profinite spaces. Duality has many other applications, that we will not be able cover in this course, but we refer the interested reader to our draft [1] of a textbook on Duality[2], co-authored with Mai Gehrke. There is some overlap between these notes and the textbook, which is itself based on a set of handwritten lecture notes of a course on Duality in Computer Science taught by Mai Gehrke in Paris a few years ago.

Disclaimer: this is a draft version, and it is not yet ready for publication or too wide distribution. There may be silly or serious errors; it is meant to be a living document (not literally - I hope) and will therefore grow and change as the course moves along. Comments and corrections are welcome; please send them to vangool@irif.fr or submit a pull request.

Abstract

The overall aim of these lectures is to introduce an algebraic and topological point of view on automata and languages, using the theory of profinite monoids. We will begin by explaining how the syntactic monoid of a regular language is related to a certain Boolean algebra canonically associated to that language. We will then show how these structures play a role in a classical result of Schützenberger, namely, the decidability of the class of star-free languages through a characterization of their syntactic monoids. Duality theory will be introduced as we move along, placing this result in a wider context, namely the correspondence between certain classes of regular languages and certain profinite monoids, yielding the modern point of view on Eilenberg-Reiterman variety theory. Building on this theory, we will make a connection to logic, and, if time permits, we will show some generalizations to the non-regular setting, bringing us to the frontier of current research in this area. Here is a rough outline:

1. Syntactic semigroups as dual spaces; the dual equivalence between monoid quotients and Boolean residuation ideals.

2. Generalization to profinite monoids and Boolean residuation algebras; Eilenberg-Reiterman correspondence theory, and a few particular cases, such as Schützenberger's Theorem: aperiodic = star-free.

3. Connections to logic: monadic second order logic and the power space construction; pro-aperiodic monoids via model theory.

4. Generalizing to non-regular languages: ultrafilter equations and measures.

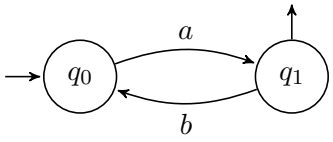
[1] `https://www.irif.fr/~jep/PDF/MPRI/MPRI.pdf`
[2] `https://www.samvangool.net/dualitybook-draft.pdf`

Chapter 1

Syntactic semigroups as dual spaces

1.1 A motivating example

In order to provide a bridge between the more abstract algebraic theory that will follow and the basic automata theory that the reader is likely familiar with, we begin with an example. The aim of this example is to convey the idea that (1) the basic notions of automata theory naturally allow for an algebraic point of view using semigroups; (2) properties of languages (such as "star-freeness") can be detected using recognizing semigroups; (3) there is a need for an intrinsic definition of "semigroup associated to a language". A secondary aim is to (implictly) fix some standard notations. Precise formal definitions of the notions of *semigroup*, *homomorphism*, *recognition*, *star-free* and *aperiodic* will be given later in the text, but are not needed to understand this example.
The set $(ab)^*a = \{(ab)^n a \ : \ n \in \omega\} = \{a, aba, ababa, \dots\}$ is the *language accepted* by the following finite automaton on the *state set* $Q := \{q_0, q_1\}$ and *finite alphabet* $A := \{a, b\}$:



This automaton can be compactly described as a function $\Diamond$ from the finite alphabet A to the set of functions $\mathcal{P}(Q) \to \mathcal{P}(Q)$, as follows. For any letter $x \in \{a, b\}$, the function $\Diamond_x$ sends a set of states $U \subseteq Q$ to the set of states

$$\Diamond_x(U) := \{q \in Q \ \mid \ \text{there is a state } u \in U \text{ and a transition } q \xrightarrow{x} u\}.$$

For example, $\Diamond_a(\{q_1\}) = \Diamond_a(\{q_0, q_1\}) = \{q_0\}$, and $\Diamond_b(\{q_1\} = \emptyset$.
Let us now also write, for any finite word w in A^+, and any set of states $U \subseteq Q$,

$$\Diamond_w(S) := \{q_i \ \mid \ \text{there is a state } u \in U \text{ and a path } q_i \xrightarrow{w} u\}.$$

Note that, if $w = w_1 w_2$ for some $w_1, w_2 \in A^+$, then

$$\Diamond_w(S) = \Diamond_{w_1}(\Diamond_{w_2}(S)). \tag{1.1}$$

Exercise 1.1. This exercise is about the automaton introduced at the beginning of this section.

a. ($\star$) Compute $\Diamond_a$, $\Diamond_b$ and $\Diamond_{ab}$.

b. ($\star\star$) Compute all the elements in $\{\Diamond_w \,:\, w \in A^+\} \subseteq \mathrm{End}(\mathcal{P}(Q))$. How many are there?

Exercise 1.2. ($\star$) Prove (1.1).

This equation (1.1) expresses the fact that the function $w \mapsto \Diamond_w$ is a *homomorphism* from the finitely generated free semigroup A^+ to the finite semigroup $S := \mathrm{End}(\mathcal{P}(Q))$ of functions $\mathcal{P}(Q) \to \mathcal{P}(Q)$, where multiplication in S is functional composition. Let us denote this homomorphism by $\eta\colon A^+ \to S$. The language $(ab)^*a$ consists precisely of those words $w \in A^+$ such that $q_0 \in \eta(w)(\{q_1\})$, that is,

$$(ab)^*a = \eta^{-1}(T) \text{ where } T := \{s \in S \,:\, q_0 \in s(\{q_1\})\}.$$

We say that the homomorphism η *recognizes* the language $(ab)^*a$.
Up to here, our description of the situation does not actually depend on the particular example of a regular language, as we will also see in Definition 1.22 below. A property that is specific to the regular language $(ab)^*a$ is that it may be described alternatively with the *star-free expression*

$$A^*a \cap aA^* \cap (A^*aaA^* \cup A^*bbA^*)^c.$$

The above expression is called star-free because it can be built from single letters and the set A^* of all words using only the operations of concatenation, union (that we denote by $\cup$ instead of $+$) and complementation, $()^c$.
In fact, *every* language recognized by the homomorphism η can be described by a star-free expression, such as for example $(ab)^+$, which is $\eta^{-1}(T')$ for $T' := \{s \in S\colon q_0 \in s(\{q_0\})\}$.

Exercise 1.3. ($\star$) Give a star-free expression for $(ab)^+$.

Even if we were to change the homomorphism η into a homomorphism $\varphi\colon A^+ \to S$, it would still be the case that $\varphi^{-1}(T)$ is star-free for any $T \subseteq S$. Said otherwise, the property of being star-free *only depends on the finite recognizing semigroup* S. In particular, this semigroup should not contain any groups. For example, contrast the above example with the language

$$(aa)^*a = \{a^{2n+1} \,:\, n \in \omega\},$$

which can *not* be described by a star-free expression.
Schützenberger [3] gave a direct and easily verifiable property for S that is equivalent to its only accepting star-free languages: S has to be *aperiodic*, i.e., S should not contain any groups, except for the trivial, one-element group. We will prove this result later in the course.

Exercise 1.4. ($\star\star$) Prove (using whatever method you like) that the language $(aa)^*a$ cannot be described by a star-free expression.
Remark. This exercise is an immediate consequence of the mentioned result by Schützenberger, but the point of this exercise is to find a direct proof.

The example given at the beginning of this section has at least one important shortcoming, that we will repair in what follows. We started with a particular accepting automaton for a language, and used it to construct a semigroup. Clearly, the presentation of this semigroup depends on the choice of the automaton: if we were unlucky enough to start from an automaton with a number of useless states, say, $n+2$ states total, then the semigroup would be presented as a subsemigroup of the endo-functions on a set of cardinality 2^{n+2}. Even worse, there are infinitely many non-isomorphic finite semigroups that could all be used to recognize this one language! One may thus reasonably wonder if there is an intrinsic, canonical choice of semigroup that can be directly associated to a language, perhaps in analogy with the minimal automaton construction. This is indeed the case, and we will define this semigroup, known as the *syntactic semigroup* of a language, in the next section.

1.2 The syntactic semigroup

Basic notions of semigroup theory

We first give some basic definitions concerning semigroups and monoids.

Definition 1.5. A *semigroup* is a pair $(S, \cdot)$, where S is a set and $\cdot$ is a binary operation on S that satisfies the associative law: for any $s, t, u \in S$, $s \cdot (t \cdot u) = (s \cdot t) \cdot u$.
A *neutral element* in a semigroup S is an element $1 \in S$ such that $1 \cdot s = s = s \cdot 1$ for all $s \in S$; note that a neutral element is unique if it exists. A *monoid* is a tuple $(M, \cdot, 1)$ where $(M, \cdot)$ is a semigroup and 1 is the neutral element in M.
An element m in a monoid $(M, \cdot, 1)$ is *invertible* if there exists an element m^{-1} in M such that $mm^{-1} = 1 = m^{-1}m$; in this case, m^{-1} is called the *(group) inverse* of m. A *group* is a monoid in which every element is invertible.

Exercise 1.6. ($\star$) Show that a neutral element in a semigroup is unique if it exists. Show that an element in a monoid has at most one inverse.

Exercise 1.7. An element m in a monoid M is called *left-invertible* if there exists an element m^l such that $m^l m = 1$, and *right-invertible* if there exists an element m^r such that $mm^r = 1$.

a. ($\star$) Prove that a monoid M is a group if, and only if, every element of M is both left- and right-invertible.

b. ($\star\star$) Prove that a *finite* monoid M is a group if, and only if, every element of M is left-invertible.

We give a few important examples of semigroups and monoids.

Example 1.8. For any set A, the set A^+ of finite non-empty sequences over A with binary concatenation is a semigroup, called the *free semigroup over A* (a justification for this name will be provided below). If we add to A^* the empty sequence, denoted by ϵ, we obtain A^*, the *free monoid over A*.

Example 1.9. For any set X, the set $\mathrm{End}(X)$ of functions $X \to X$ with composition is a monoid with identity element id_X.

Definition 1.10. A subset T of a semigroup S is called a *subsemigroup* if, for any $t, t' \in T$, the element $t \cdot t'$ is also in T. A *submonoid* of a monoid M is a subsemigroup N of M that contains the neutral element. A *subgroup* of a monoid M is a submonoid that is a group.

Exercise 1.11. ($\star$) Prove that the set of invertible elements in a monoid form the largest subgroup of the monoid. Describe what this group is in the monoids given in Examples 1.8 and 1.9.

Example 1.12. Any totally ordered set $(C, \leq)$ is a monoid under the operation of binary minimum. More generally, if S is a set and $\leq$ is a partial order (i.e., a reflexive, transitive, anti-symmetric relation) on S such that any two elements have an infimum (greatest lower bound), then $(S, \inf)$ is a semigroup. Semigroups of the kind $(S, \inf)$ are called *semilattices*. A semigroup $(S, \cdot)$ is a semilattice if, and only if, its multiplication is *commutative* ($a \cdot b = b \cdot a$ for all $a, b \in S$) and *idempotent* ($a^2 = a$ for all $a \in S$).

Exercise 1.13. ($\star$) Prove that a semigroup is a semilattice if and only if it is commutative and idempotent.

Definition 1.14. A *homomorphism* from a semigroup S to a semigroup T is a function $f\colon S \to T$ such that $f(s_1 s_2) = f(s_1) f(s_2)$ for every $s_1, s_2 \in S$. A *homomorphism* from a monoid M to a monoid N is a homomorphism f between the underlying semigroups such that, moreover, $f(1_M) = 1_N$. An *isomorphism* is a bijective homomorphism, and two semigroups are *isomorphic* if there is an isomorphism between them.

Exercise 1.15. ($\star$) Prove that the image of a homomorphism is a subsemigroup. Conclude that if $f\colon S \to T$ is an injective homomorphism, then S is isomorphic to the subsemigroup $f(S)$ of T.

Exercise 1.16. ($\star$) Let G and H be groups and suppose that $f\colon G \to H$ is a homomorphism between the underlying monoids. Prove that f preserves inverses, i.e., $f(g^{-1}) = f(g)^{-1}$ for every $g \in G$.

Definition 1.17. A *congruence* on a semigroup S is an equivalence relation $\sim$ on S such that, for any $s, s', t \in S$, if $s \sim s'$, then $st \sim s't$ and $ts \sim ts'$. A congruence on a monoid S is a congruence on the underlying semigroup.
The *quotient* of the semigroup S under the congruence $\sim$ is the semigroup on $S/\!\sim$ obtained by defining $[s]_\sim [t]_\sim := [st]_\sim$, for any $s, t \in S$. The fact that $\sim$ is a congruence ensures that multiplication in $S/\!\sim$ is well-defined. If $1 \in S$ is a neutral element, then so is $[1]_\sim \in S/\!\sim$. Note that the function $p_\sim\colon S \to S/\!\sim$ which sends s to $[s]_\sim$ is a surjective homomorphism.

Exercise 1.18. Let G be a group. For any congruence $\sim$ on (the semigroup underlying) G, define $N_\sim := \{n \in G : \ n \sim 1_G\}$.

a. ($\star$) Prove that $N_\sim$ is a normal subgroup of G (i.e., a subgroup such that $n \in N_\sim$ implies $gng^{-1} \in N_\sim$ for all $g \in G$).

b. ($\star$) Prove that $G/\!\sim$ as defined in Definition 1.17 is isomorphic to the group G/N as usually defined in group theory using cosets of N.

c. ($\star\star$) Prove that the assignment $\sim \mapsto N_\sim$ is a bijection between the congruences on G and the normal subgroups of G.

Proposition 1.19 (Homomorphism theorem for semigroups)**.** *Let S and T be semigroups, and let $f\colon S \to T$ be a homomorphism between semigroups. The* kernel *of f,*

$$\ker(f) := \{(s, s') \in S \times S \ :\ f(s) = f(s')\},$$

is a congruence on S, and there is a unique injective homomorphism $i\colon S/\ker(f) \to T$ such that $f = i \circ p_{\ker(f)}$.

Exercise 1.20. ($\star\star$) Prove Proposition 1.19.

Free and syntactic semigroups

Let A be a finite set of symbols. The set, A^+, of *finite words over the alphabet A*, i.e., finite non-empty sequences[1] over A, is a semigroup under concatenation. Every element $a \in A$ is identified with the corresponding sequence of length 1 in A^+, also denoted a.

Proposition 1.21. *The semigroup A^+ is* free *over its set of generators A. That is, for any semigroup S and any function $f\colon A \to S$, there exists a unique homomorphism $\bar{f}\colon A^+ \to S$ such that $\bar{f}(a) = f(a)$ for every $a \in A$.*

Proof. By induction on the length of $w \in A^+$, define $\bar{f}(wa) := \bar{f}(w)f(a)$. It is straightforward to verify that $\bar{f}$ is a homomorphism with the required property, and that is the unique such. □

We now make precise the definition of (finite, non-deterministic, word) automaton that we alluded to in the first section.

Definition 1.22. An *automaton* is a tuple $\mathcal{A} = (Q, A, \delta, I, F)$, where Q is a finite set, A is a finite alphabet, δ is a function $Q \times A \to \mathcal{P}(Q)$, and I and F are subsets of Q. The *reachability function* of $\mathcal{A}$, $\Diamond_-^{\mathcal{A}}$, is the unique homomorphism $A^+ \to \mathrm{End}(\mathcal{P}(Q))$ defined by the condition $\Diamond_a^{\mathcal{A}}(U) = \{q \in Q \ :\ U \cap \delta(q, a) \neq \emptyset\}$ for $a \in A$ and $U \in \mathcal{P}(Q)$. The automaton $\mathcal{A}$ *accepts* a word $w \in A^+$ if $\Diamond_w^{\mathcal{A}}(F) \cap I \neq \emptyset$. The *language accepted by* $\mathcal{A}$ is denoted $L(\mathcal{A})$.

Exercise 1.23. ($\star$) Verify that the above definition of automata is equivalent to the one you are familiar with. Prove in particular that, for any $w \in A^+$ and $U \in \mathcal{P}(Q)$, $\Diamond_w(U)$ is the set of states q such that there exists a path $q \xrightarrow{w} u$ for some $u \in U$.

We will return to automata at the end of the next section, but we first introduce the *syntactic congruence*.

Definition 1.24. Let L be a subset of A^+. The *syntactic preorder* of L is the relation $\preceq_L$ on A^+ defined by

$$u \preceq_L v \iff \text{for any } x, y \in A^*, \text{ if } xuy \in L, \text{ then } xvy \in L.$$

The *syntactic congruence* of L is the relation $\sim_L$ on A^+ defined by

$$u \sim_L v \iff u \preceq_L v \text{ and } v \preceq_L u.$$

[1] We will always use enough notation to ensure that words be *uniquely parsable*. If for example $A = \{|, ||, |||\}$, then '|||' is *not* uniquely parsable: we will need to specify explicitly whether we mean a word of length 1, (|||), or one of the words of length 2, (|, ||) or (||, |). We will thus take care to avoid such ambiguous alphabets.

The *syntactic semigroup* of L is the semigroup quotient $A^+/{\sim_L}$. We denote this semigroup by $S(L)$.[2]

Recall that, if $\equiv$ is an equivalence relation on a set X, and L is a subset of X, then $\equiv$ *saturates* L if, for any $u \in L$, $v \in X$, $u \equiv v$ implies $v \in L$. Equivalently, $\equiv$ saturates L if L is a union of $\equiv$-classes.

Proposition 1.25. *The syntactic congruence $\sim_L$ of L is the largest congruence on A^+ saturating L.*

Proof. It is left as Exercise 1.26 to verify that $\sim_L$ is indeed a congruence on A^+. Note that, if $u \in L$ and $u \sim_L v$, then also $v \in L$, applying the definition of $u \preceq_L v$ in the case $x = y = \epsilon$. Thus, $\sim_L$ saturates L. Now suppose that ϑ is any congruence on A^+ saturating L; we show that $\vartheta \subseteq \sim_L$. Suppose that $u \vartheta v$. Let $x, y \in A^*$ be such that $xuy \in L$. Since ϑ is a congruence, $xuy \;\vartheta\; xvy$. Since ϑ saturates L, we get that $xvy \in L$. Thus, $u \preceq_L v$. The proof that $v \preceq_L u$ is symmetric. □

Exercise 1.26. ($\star$) Prove that, for any $L \subseteq A^+$, $\sim_L$ is a congruence on A^+.

Exercise 1.27. ($\star\star$) Give the multiplication table of the (finite) syntactic semigroup of the language $L = (ab)^*a$, which we considered at the beginning of this chapter. Verify that this semigroup is isomorphic to the one you found in Exercise 1.1.b. Is that the case for any automaton recognizing L?

The quotient $A^+/{\sim_L}$ is *finite* if, and only if, there is a finite automaton accepting L. In this case, L is called a *regular* language. This fundamental result shows that the study of regular languages is, in a sense, equivalent to the study of finite semigroups (with a distinguished finite set of generators). Many elementary proofs of this equivalence exist; we will give a proof below that illustrates a basic use of duality theory, and, crucially, makes a connection with the theory of *Boolean residuation algebras*, see Theorem 1.65 below. Before doing so, we formally introduce the notion of *recognition* by a semigroup, and we show in what sense the syntactic semigroup of a language is its *smallest* recognizer.

Definition 1.28. Let S and T be semigroups and let $L \subseteq T$. We say that a homomorphism $f\colon S \to T$ *recognizes* L if there exists a subset $P \subseteq T$ such that $L = f^{-1}(P)$. We also say that T *recognizes* L if there exists a homomorphism $f\colon S \to T$ recognizing L.

Exercise 1.29. ($\star$) Prove that a surjective homomorphism $f\colon S \to T$ recognizes $L \subseteq S$ if, and only if, $L = f^{-1}(f(L))$.

The syntactic semigroup is a *smallest* recognizer for L, where 'smallness' is measured according to the notion of *division* of semigroups. We will say more about division when we talk about varieties later in this course. For now, we just give the basic definition and result connecting syntactic semigroups, recognition, and division.

Definition 1.30. Let S and T be semigroups. We say that S *divides* T if there exist a subsemigroup T' of T and congruence ϑ on T' such that S is isomorphic to T'/ϑ.

[2] To familiarize yourself with this definition, it is instructive to compute a few examples, also see Exercise 1.27 below. A useful tool to check your calculations, programmed by Charles Paperman, is available at `https://paperman.name/semigroup/`.

Exercise 1.31. ($\star$) Prove that S divides T if, and only if, there exist a semigroup U, an injective homomorphism $i\colon U \to T$, and a surjective homomorphism $g\colon U \to S$.

Proposition 1.32. *Let $L \subseteq A^+$. A semigroup T recognizes L if, and only if, the syntactic semigroup of L divides T.*

Proof. Let T be a semigroup recognizing L. Pick a homomorphism $f\colon A^+ \to T$ and $P \subseteq T$ such that $L = f^{-1}(P)$. Let U be the semigroup $A^+/\ker(f)$, and $i\colon U \to T$ the injective homomorphism given by Proposition 1.19. The congruence $\ker(f)$ on A^+ saturates L, so $\ker(f) \subseteq \sim_L$ by Proposition 1.25. Thus, the function $g\colon U \to S(L)$ defined by $g([w]_{\ker f}) = [w]_{\sim_L}$ is well-defined, and g is clearly surjective. By Exercise 1.31, $S(L)$ divides T.
Conversely, suppose that $S(L)$ divides a semigroup T; let T' be a subsemigroup of T, and $g\colon T' \to S(L)$ a surjective homomorphism. For any $a \in A$, choose $f(a) \in T'$ such that $g(f(a)) = [a]_{\sim_L}$. Denote by $\bar{f}\colon A^+ \to T$ the homomorphism extending f, which exists by Proposition 1.21. Then, applying the uniqueness part of Proposition 1.21, we have $g \circ \bar{f} = p_{\sim_L}$, since $g(\bar{f}(a)) = g(f(a)) = [a]_{\sim_L}$ for every $a \in A$. Hence, $L = (\bar{f})^{-1}(P)$, where $P := g^{-1}(p_{\sim_L}(L))$. Thus, $\bar{f}\colon A^+ \to T$ recognizes L. □

1.3 Discrete duality for regular languages

The aim of this section is to prove the following theorem.

Theorem. *Let A be a finite alphabet, and let $L \subseteq A^+$. The following are equivalent:*

a. the syntactic congruence $\sim_L$ has finite index;

b. there is a finite automaton accepting L;

c. the residuation ideal $B(L)$ generated by L is finite.

A language L satisfying these properties is a *regular* language.[3] To understand the statement of this theorem, we first need to define what 'the residuation ideal $B(L)$' is, and what it has to do with the syntactic congruence introduced in the previous section. To do so, we need to explain the basics of *duality theory*, for now in *discrete* form; i.e., topology does not yet play a role.

Basics on lattices and Boolean algebras

Definition 1.33. A *(bounded) lattice* is a partially ordered set L in which every finite subset has a supremum and an infimum. A *complete lattice* C is a partially ordered set in which every subset has a supremum and an infimum.

Exercise 1.34. ($\star$) Prove that a partially ordered set L is a bounded lattice if, and only if, any subset S of cardinality at most 2 has a supremum and infimum.
Prove that a partially ordered set C is a complete lattice if, and only if, any subset S of C has a supremum.

[3] As the reader may know from a basic course in automata theory, regularity of L is also equivalent to: *d.* there is a regular expression describing L. We will not talk much about regular expressions here.

An interesting equivalent definition of lattices is the following. A *lattice* is a tuple $(L, \vee, \wedge, \bot, \top)$, such that $(L, \vee, \bot)$ and $(L, \wedge, \top)$ are semilattices with neutral elements, and the *absorption laws* $a \wedge (a \vee b) = a$ and $a \vee (a \wedge b) = a$ hold for all $a, b \in L$. Given a lattice $(L, \vee, \wedge, \bot, \top)$ according to this algebraic definition, define

$$a \leq_L b \iff a \wedge b = a.$$

Then $\leq_L$ defines a partial order on the set L which makes L into a lattice according to the order-theoretic definition.

Exercise 1.35. ($\star$) Given a lattice $(L, \leq)$ according to the order-theoretic definition, prove that the operations of binary supremum ($\vee$), binary infimum ($\wedge$), and the maximum ($\top$) and minimum ($\bot$) make L into a lattice according to the algebraic definition.

Exercise 1.36. ($\star\star$) Taking inspiration from the definitions for semigroups in Section 1.2, write down the appropriate definitions of (bounded) *sublattice*, *lattice homomorphism*, *congruence on a lattice*, and *quotient lattice*. Formulate and prove the *homomorphism theorem for lattices*. In case of doubt, refer to, e.g., p. 11 of [1].

Exercise 1.37. ($\star\star$) Prove that the set of congruences on a semigroup S is a complete lattice under the inclusion order.

The first kind of duality we introduce in this course is trivial, but important.

Definition 1.38 (Formal duality)**.** The *formal dual* or *opposite* of a lattice $(L, \vee, \wedge, \bot, \top)$ is the lattice $L^{\mathrm{op}} := (L, \wedge, \vee, \top, \bot)$. Said otherwise, L^{op} is given by equipping the same set L with the *reverse* of the partial order $\leq_L$. An *antitone* or *contravariant* map from a lattice L to a lattice M is a map that is monotone from L^{op} to M. A *dual isomorphism* between L and M is an isomorphism between L^{op} and M.

We now define distributive lattices and Boolean algebras.

Definition 1.39. A lattice L is called *distributive* if

$$\text{for all } a, b, c \in L, \quad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c), \tag{1.2}$$

and

$$\text{for all } a, b, c \in L, \quad a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c). \tag{1.3}$$

If a is an element in a lattice, an element b is called a *complement* of a if $a \wedge b = \bot$ and $a \vee b = \top$. A *Boolean algebra* is a distributive lattice in which each element has a complement. If L is a Boolean algebra, we denote by $\neg a$ the unique complement of an element a. A *subalgebra* of a Boolean algebra is a sublattice which moreover contains the complement of any of its elements.

Exercise 1.40. ($\star$) This exercise asks you to establish some properties and give some examples of lattices and Boolean algebras.

a. Prove that, in any lattice, (1.2) holds if, and only if, (1.3) holds.

b. Prove that any sublattice and any quotient of a lattice is distributive.

c. Give two examples of lattices that are not distributive.

d. Prove that any element of a distributive lattice has at most one complement.

e. Give an example of a sublattice of a Boolean algebra that is not a subalgebra.

f. Prove that a lattice homomorphism between Boolean algebras must preserve complements.

g. Prove that, in a complete Boolean algebra, the complement of a supremum is equal to the infimum of the complements, i.e., for any subset U, $\neg(\bigvee U) = \bigwedge_{u\in U} \neg u$.

h. Prove that a function between Boolean algebras that preserves $\wedge$ and $\neg$ is a homomorphism.

The definition of Boolean algebras that we gave above was order-theoretic; as for lattices, there exist several equivalent *equational* definitions. The simplest equational definition, and most useful for our purposes, is that a *Boolean algebra* is a tuple $(B, \wedge, \vee, \bot, \top, \neg)$ such that $(B, \wedge, \vee, \bot, \top)$ is a distributive lattice, and for all $a \in B$, $a \wedge \neg a = \bot$ and $a \vee \neg a = \top$. The *terminology* 'Boolean algebra' comes from another (the original) equational definition: a Boolean algebra is the same thing as a commutative ring with unit in which all elements are idempotent.

Exercise 1.41. ($\star$) Let $(B, +, \cdot, 0, 1)$ be a commutative ring with unit in which $a^2 = a$ for all $a \in B$. Define $a \leq b$ if, and only if, $a \cdot b = a$. Prove that $\leq$ is a distributive lattice order on B, and that every element of B has a complement with respect to $\leq$. *Hint:* first show that $a + a = 0$ for all $a \in B$.
Conversely, let $(B, \wedge, \vee, \bot, \top, \neg)$ be a Boolean algebra. Define, for any $a, b \in B$, $a + b := (a \wedge \neg b) \vee (\neg a \wedge b)$, $a \cdot b := a \wedge b$, $0 := \bot$ and $1 := \top$. Prove that $(B, +, \cdot, 0, 1)$ is a commutative ring with unit in which $a^2 = a$ for all $a \in B$.

Example 1.42. For any partially ordered set P, the collection $\mathcal{D}(P)$ of *downward closed* subsets of P is a distributive lattice under the operations of intersection $\cap$ and union $\cup$, with bounds $\emptyset$ and P. In general, $\mathcal{D}(P)$ is not a Boolean algebra, except when the order on P is trivial (i.e., $p \leq q$ implies $p = q$). In this case, we obtain the *power set Boolean algebra*, $\mathcal{P}(P)$. The operation $\neg$ in this Boolean algebra is given by $\neg u := P \setminus u$, for any $u \in \mathcal{P}(P)$.

Example 1.42 covers every *finite* distributive lattice and Boolean algebra, as we will see shortly. However, *infinite* lattices and Boolean algebras may be more complicated. We give just one example here, which the reader may be familiar with from a topology and/or logic course – more examples follow later in the course.

Example 1.43. Let B be the collection of *clopen* (closed-and-open) subsets of the Cantor space, $\{0,1\}^\omega$, where $\{0,1\}$ has the discrete topology, and $\{0,1\}^\omega$ carries the product topology, generated by the sets $U_{n,i} := \{x \in \{0,1\}^\omega : \ x_n = i\}$, for $n \in \omega, i \in \{0,1\}$. Then B is a Boolean algebra. Indeed, B is a subalgebra of the power set algebra $\mathcal{P}(\{0,1\}^\omega)$.

Exercise 1.44. ($\star$) Prove that, for the Boolean algebra B of Example 1.43, there is no set X such that B is isomorphic to $\mathcal{P}(X)$. *Hint.* Show that B is not complete.

Exercise 1.45. ($\star\star$) Prove that the Boolean algebra B of Example 1.43 is isomorphic to the Boolean algebra of equivalence classes of formulas of propositional logic over a countable set of variables. (The latter algebra is known as the *Lindenbaum-Tarski algebra* of propositional logic.)

We will now characterize (Theorem 1.48) the Boolean algebras that are of the form $\mathcal{P}(X)$ for some set X.

Definition 1.46. An *atom* in a Boolean algebra is a minimal element above $\bot$. That is, $x \in B$ is an atom if $x \neq \bot$ and, for any $b \in B$, if $b < x$ then $b = \bot$. A Boolean algebra B is called *atomic* if, for every element $b \in B$, if $b \neq \bot$, then there exists an atom $x \in B$ with $x \leq b$.

Lemma 1.47. *Let x be an atom in a Boolean algebra B. Then, for any $b \in B$, $x \leq b$ if, and only if, $x \not\leq \neg b$.*

Proof. If $x \leq b$, then necessarily $x \not\leq \neg b$ because $b \wedge \neg b = \bot$ and $x \neq \bot$. Conversely, note that if $x \not\leq \neg b$, then $x \wedge \neg b < x$, and thus $x \wedge \neg b = \bot$, since x is an atom. Thus,

$$x = x \wedge \top = x \wedge (b \vee \neg b) = (x \wedge b) \vee (x \wedge \neg b) = x \wedge b,$$

so that $x \leq b$. □

Theorem 1.48 (Discrete duality for Boolean algebras, objects)**.** *A Boolean algebra B is complete and atomic if, and only if, B is isomorphic to $\mathcal{P}(X)$, where X is the set of atoms of B.*

Proof. In a Boolean algebra of the form $\mathcal{P}(X)$, any singleton set is an atom, and any supremum is given by union, so $\mathcal{P}(X)$ is certainly complete and atomic. For the converse, suppose that B is a complete and atomic Boolean algebra, write X for the set of atoms of B, and define the function

$$\varphi\colon B \to \mathcal{P}(X), \quad \varphi(b) := \{x \in X \,:\, x \leq b\}.$$

We show that the function φ is an isomorphism.
Firstly, if $b, c \in B$, then $x \leq b \wedge c$ if, and only if, $x \leq b$ and $x \leq c$, so that $\varphi(b \wedge c) = \varphi(b) \cap \varphi(c)$. Secondly, $\varphi(\neg b) = X \setminus \varphi(b)$ by Lemma 1.47. Thus, φ preserves $\neg$ and $\wedge$, and therefore is a homomorphism by the last item of Exercise 1.40.
We show that φ is injective. If $b, b' \in B$ are such that $b \neq b'$, then either $b \wedge \neg b' \neq \bot$ or $b' \wedge \neg b \neq \bot$. Without loss of generality, assume the first. Since B is atomic, pick an atom $x \in B$ such that $x \leq b \wedge \neg b'$. Then $x \in \varphi(b)$ and $x \notin \varphi(b')$, so $\varphi(b) \neq \varphi(b')$.
Finally, for surjectivity, we show that, for any set $u \subseteq X$, we have $\varphi(\bigvee u) = u$. Write $b_u := \bigvee u$. Indeed, if $x \in u$ then certainly $x \leq b_u$. Conversely, if $x \leq b_u$, then by Lemma 1.47, $x \not\leq \neg b_u$, which is equal to the infimum of the set $\{\neg y \,:\, y \in u\}$, see Exercise 1.40. Thus, pick $y \in u$ such that $x \not\leq \neg y$. Again by Lemma 1.47, $x \leq y$. Since y is an atom and $x \neq \bot$, we get $x = y$, so $x \in u$. □

We note an immediate consequence of Theorem 1.48 in the *finite* case.

Corollary 1.49. *Any finite Boolean algebra B is isomorphic to $\mathcal{P}(X)$, where X is the set of atoms of B.*

Proof. Let B be a finite Boolean algebra. Clearly, B is complete. It is also atomic, because for any $b \in B$, the set $\{c \in B : \bot \neq c \leq b\}$ is finite, and therefore contains a minimal element, which must be an atom. □

Exercise 1.50. ($\star\star$) Prove that every finite distributive lattice L is isomorphic to $\mathcal{D}(X)$, where X is the partially ordered set of join-irreducible elements of L, i.e., the elements $x \in L$ for which $x \neq \bot$ and $x = a \vee b$ implies $x = a$ or $x = b$ for any $a, b \in L$. *Hint.* If you are stuck, see, e.g., Section 1.3 of [1].

Theorem 1.48 shows that complete and atomic Boolean algebras are completely determined by their sets of atoms. The set of atoms of a complete and atomic Boolean algebra B is sometimes called the *discrete dual space* of B, and if X is a set then the Boolean algebra $\mathcal{P}(X)$ is sometimes called the *discrete dual algebra* of X. Later in this course, we will see how to modify Theorems 1.48, and also Theorem 1.53 below, to obtain a *duality* (dual equivalence) between the category of *all* Boolean algebras and the category of compact Hausdorff zero-dimensional (a.k.a. *profinite*) topological spaces. This involves (1) using ultrafilters to extend the above object correspondence to Boolean algebras that are not complete or atomic; (2) establishing a correspondence at the level of *all homomorphisms* between Boolean algebras. Duality theory becomes powerful when considering additional structure on Boolean algebras or their corresponding dual spaces. We end this subsection with a first result in that direction: a correspondence between complete subalgebras of a discrete Boolean algebra and equivalence relations on its set of atoms. We will build on this correspondence when we throw semigroups into the mix in the next subsection.

Definition 1.51. A *subalgebra* of a Boolean algebra B is a subset I of B such that, for any $a, a' \in I$, we have $a \vee a' \in I$ and $\neg a \in I$ (and hence also $a \wedge a' \in I$, and $\bot, \top \in I$). If B is moreover complete, then by a *complete subalgebra* we mean a subalgebra I of B which moreover has the property that $\bigvee U \in I$ for any $U \subseteq I$ (and hence also $\bigwedge U \in I$ for any $U \subseteq I$).

Exercise 1.52. ($\star\star$) Show that a complete Boolean algebra B may have a subalgebra I which is by itself a complete Boolean algebra, but is not a complete subalgebra of B according to the above definition.

Theorem 1.53 (Discrete duality for Boolean algebras, subalgebras and quotients)**.** *Let X be a set and $B := \mathcal{P}(X)$ the dual complete and atomic Boolean algebra. The complete lattice of equivalence relations on X is dually isomorphic to the complete lattice of complete subalgebras of B.*

Proof. For any relation R on X, define $I_R \subseteq B$ by

$$I_R := \{a \in B : \quad \text{for any } (x, x') \in R, \quad x \in a \text{ if, and only if, } x' \in a\},$$

and for any subset J of B, define $\sim_J \subseteq X^2$ by

$$x \sim_J x' \iff \text{for any } a \in J, \quad x \in a \text{ if, and only if, } x' \in a.$$

Note that, for any relation R on X and any subset J of B, we have

$$J \subseteq I_R \iff R \subseteq \sim_J,$$

and that both assignments are antitone. It follows that, for any $J \subseteq B$, $J \subseteq I_{\sim_J}$, and for any $R \subseteq X^2$, we have $R \subseteq \sim_{I_R}$, and that the assignments $R \mapsto I_R$ and $J \mapsto \sim_J$ restrict to anti-isomorphisms between their respective images (see Exercise 1.54). We prove that the relations on X that are of the form $\sim_J$ for some $J \subseteq B$ are exactly the equivalence relations, and that the subsets of the form I_R for some $R \subseteq X^2$ are exactly the complete subalgebras.
It is easy to see that $\sim_J$ is always an equivalence relation, for any $J \subseteq B$. Conversely, if $\sim$ is an equivalence relation, and $x \sim_{J_\sim} x'$, then in particular $x' \in [x]_\sim$ since $x \in [x]_\sim$, so $x \sim x'$. Thus, $\sim_{J_\sim} = \sim$.
It is again easy to see that I_R is always a complete subalgebra, for any relation R. Conversely, if I is a complete subalgebra of B, then for any $a \in I_{\sim_I}$, note that $a = \bigvee_{x \in a} [x]_{\sim_I}$, so we are done if we can show that $[x]_{\sim_I} \in I$ for every $x \in X$. Note that $[x]_{\sim_I} = \bigwedge_{b \in I, x \in b} b \wedge \bigwedge_{c \in I, x \notin c} \neg c$, which is an element of I since I is a complete subalgebra. □

Exercise 1.54. ($\star$) Let C and D be complete lattices, and suppose that $f \colon C \leftrightarrows D \colon g$ are a pair of antitone maps between them such that, for any $c \in C$ and $d \in D$, $d \leq f(c)$ if, and only if, $c \leq g(d)$. (Such a pair is called a *Galois connection* between C and D.) Prove that $f \circ g \circ f = f$ and $g \circ f \circ g = g$. Deduce that the restrictions $f \colon g(D) \leftrightarrows f(C) \colon g$ are anti-isomorphisms between $g(D)$ and $f(C)$.

Semigroup quotients and residuation ideals

We use discrete duality to associate a Boolean algebra with additional operations to any semigroup. For any semigroup S, the Boolean algebra $\mathcal{P}(S)$ also carries a *complex multiplication*, $\cdot$, defined by

$$s \cdot t := \{\, mn \mid m \in s, n \in t \,\}.$$

There exist two operations, $\backslash, / \colon \mathcal{P}(S)^2 \to \mathcal{P}(S)$, which are uniquely determined by the property that they are *left and right residuals* of $\cdot$, i.e., for any $r, s, t \in \mathcal{P}(S)$,

$$r \cdot s \subseteq t \iff s \subseteq r \backslash t \iff r \subseteq t / s. \tag{1.4}$$

More explicitly, $\backslash$ and $/$ are given by the following formulas:

$$r \backslash t = \{m \in S \mid km \in t \text{ for all } k \in r\}, \tag{1.5}$$
$$t / s = \{m \in S \mid m\ell \in t \text{ for all } \ell \in s\}. \tag{1.6}$$

Exercise 1.55. ($\star$) Prove that the formulas (1.5) and (1.6) indeed define the unique operations satisfying (1.4).

Definition 1.56. Let S be a semigroup. We call the Boolean algebra with three additional operations $(\mathcal{P}(S), \cdot, \backslash, /)$ the *(discrete) dual residuated Boolean algebra* of M.
A sublattice I of $\mathcal{P}(S)$ is a *residuation ideal* if, for any $r \in \mathcal{P}(S)$ and $s \in I$, both $r \backslash s \in I$ and $s / r \in I$. A residuation ideal I is said to be *Boolean* provided the underlying sublattice is a Boolean algebra. A residuation ideal is called *complete* provided the underlying sublattice is a complete sublattice of $\mathcal{P}(S)$, i.e., for any $U \subseteq I$, we have $\bigcup U \in I$.
For a subset $U \subseteq \mathcal{P}(S)$, we denote by $B(U)$ the *Boolean residuation ideal generated by* U, that is, the smallest Boolean residuation ideal containing U. If $U = \{u\}$ for a single element $u \in \mathcal{P}(S)$, we write $B(u)$ instead of $B(\{u\})$.

We are now ready to prove the discrete duality theorem for semigroups which we will need in order to characterize regularity. Recall from Exercise 1.37 that the congruences on a semigroup S form a complete lattice under the inclusion order.

Theorem 1.57 (Discrete duality for semigroups, quotients and subs)**.** *Let S be a semigroup and $(\mathcal{P}(S), \cdot, \backslash, /)$ its discrete dual residuated Boolean algebra. The congruence lattice of S is dually isomorphic to the lattice of complete Boolean residuation ideals of $\mathcal{P}(S)$.*

Proof. It suffices to show that the dual isomorphism given in the proof of Theorem 1.53 restricts to semigroup congruences and complete Boolean residuation ideals. Using the same notation as in that proof, suppose first that $\sim$ is a congruence on S; we show that $I_\sim$ is a residuation ideal. Indeed, let $r \in \mathcal{P}(S)$ and $s \in I_\sim$. We need to show that s/r and $r\backslash s$ are both $\sim$-saturated. We only show the former, the proof of the latter is the same. Suppose that $m \in s/r$ and that $m \sim m'$. Let $n \in r$ be arbitrary. Since $\sim$ is a congruence, we have $mn \sim m'n$. Since $m \in s/r$, we have $mn \in s$. Since s is R-saturated, we get $m'n \in s$, as required.
Now suppose that I is a residuation ideal in $\mathcal{P}(S)$; we show that $\sim_I$ is a congruence. Suppose that $m \sim_I m'$ and let $n \in S$ be arbitrary. For every $a \in I$, if $mn \in a$, then $m \in a/\{n\}$, and $a/\{n\} \in I$ because I is a residuation ideal. Therefore, $m' \in a/\{n\}$, since $m \sim_I m'$. Thus, $m'n \in a$, and we conclude that $mn \sim_I m'n$. The proof that $nm \sim_I nm'$ is similar, using that $\{n\}\backslash a \in I$. □

Definition 1.58. Let S be a semigroup, $m \in S$, and $s \in \mathcal{P}(S)$. Then we denote $\{m\}\backslash s$ by $m^{-1}s$ and we denote $s/\{m\}$ by sm^{-1} and we call these the *left and right quotients* of s by m, respectively.

Exercise 1.59. ($\star$) Prove that a complete subalgebra A of $\mathcal{P}(S)$ is a residuation ideal if, and only if, for any $s \in A$ and $n \in S$, $sn^{-1} \in A$ and $n^{-1}s \in A$. *Hint.* Inspect the proof of Theorem 1.57.

Exercise 1.60. ($\star$) Let S be a semigroup and $m \in S$. Prove that the maps

$$m^{-1}(\ ) \colon \mathcal{P}(S) \to \mathcal{P}(S) \quad \text{and} \quad (\ )m^{-1} \colon \mathcal{P}(S) \to \mathcal{P}(S)$$

are Boolean algebra homomorphisms.

The duality of Theorem 1.57 allows us to make a first observation that links residuation ideals to the syntactic congruence. Recall from Proposition 1.25 that $\sim_L$ is the largest congruence saturating L. It therefore follows from the dual isomorphism of Theorem 1.57 that the corresponding complete Boolean residuation ideal is the smallest one that contains L. We will now show that this residuation ideal is finite if, and only if, L is accepted by an automaton.

Definition 1.61. Let $\mathcal{A} = (Q, A, \delta, I_0, F_0)$ be an automaton and let $L = L(\mathcal{A})$ be the language accepted by $\mathcal{A}$. For any pair of subsets $(I, F) \in \mathcal{P}(Q)^2$, denote by $L(I, F)$ the language accepted by the automaton (Q, A, δ, I, F); in particular, $L(\mathcal{A}) = L(I_0, F_0)$. We denote by $B(\mathcal{A})$ the Boolean subalgebra of $\mathcal{P}(A^+)$ generated by the languages $L(I, F)$, for $(I, F) \in \mathcal{P}(Q)^2$.

Exercise 1.62. This exercise is about the example automaton $\mathcal{A}$ given at the beginning of Section 1.1.

a. ($\star$) List the languages $L(I,F)$ for $(I,F) \in \mathcal{P}(Q)^2$. How many different ones are there?

b. ($\star\star$) What algebraic properties does the function $(I,F) \mapsto L(I,F)$ seem to have, viewed as a function from the lattice $\mathcal{P}(Q)^2$ to $\mathcal{P}(A^+)$? Prove that it always has these properties.

c. ($\star\star$) How many elements does $B(\mathcal{A})$ have in this case? What is the best way to describe them?

We will prove (Proposition 1.64) that $B(\mathcal{A})$ is a residuation ideal in $\mathcal{P}(A^+)$. Note that the generating set for $B(\mathcal{A})$ has at most $2^{2|Q|}$ elements and is thus in particular *finite*. Hence, $B(\mathcal{A})$ is also finite.
Recall from Definition 1.22 the definition of the (backward) *reachability function* $\Diamond$ for an automaton $\mathcal{A}$. There is also a *forward reachability function*, $\blacklozenge$, where, for any $U \subseteq Q$, $\blacklozenge_w(U)$ is the set of states $q \in Q$ such that there exists a path $u \xrightarrow{w} q$ for some $u \in U$.

Lemma 1.63. *For any $x \in A^+$, $(I,F) \in \mathcal{P}(Q)^2$, we have*

$$x^{-1}L(I,F) = L(\blacklozenge_x(I), F), \quad L(I,F)x^{-1} = L(I, \Diamond_x(F)).$$

Proof. Recall that, for any $x, w \in A^+$, $wx \in L(I,F)$ if, and only if, $\Diamond_{wx}(F) \cap I \neq \emptyset$. This is the case if, and only if, $\Diamond_w(\Diamond_x(F)) \cap I \neq \emptyset$, which establishes the second equality. The first equality follows similarly, noting that $xw \in L(I,F)$ if, and only if $\blacklozenge_{xw}(I) \cap F \neq \emptyset$. □

Proposition 1.64. *For any automaton $\mathcal{A}$, $B(\mathcal{A})$ is a finite (hence complete) Boolean residuation ideal in $\mathcal{P}(A^+)$.*

Proof. Let $x \in A^*$. By Lemma 1.63, the generating set of $B(\mathcal{A})$ is closed under the quotient operations $x^{-1}(\ )$ and $(\ )x^{-1}$. Also, by Exercise 1.60, these operations are homomorphisms, and thus the Boolean algebra generated by this set remains closed under these operations. Since $B(\mathcal{A})$ is finite, it is complete. By Exercise 1.59, $B(\mathcal{A})$ is a residuation ideal. □

We are now ready to prove the main theorem of the chapter.

Theorem 1.65. *Let A be a finite alphabet, and let $L \subseteq A^+$. The following are equivalent:*

a. the syntactic congruence $\sim_L$ has finite index;

b. there is a finite automaton accepting L;

c. the residuation ideal $B(L)$ generated by L is finite.

Proof. If $\sim_L$ has finite index, then L is easily seen to be accepted by the deterministic finite automaton with state set $A^+/{\sim_L} \cup \{\epsilon\}$, alphabet A, transitions defined by $[w]_{\sim_L} \xrightarrow{a} [wa]_{\sim_L}$, $\epsilon \xrightarrow{a} [a]_{\sim_L}$, initial state ϵ and final states $\{[w]_{\sim_L} : w \in L\}$. If some finite automaton $\mathcal{A}$ accepts L, then $L \in B(\mathcal{A})$, and $B(\mathcal{A})$ is a finite Boolean residuation ideal, so by definition of $B(L)$, we obtain $B(L) \subseteq B(\mathcal{A})$, so that $B(L)$ is finite as well. Finally, if $B(L)$ is finite, then it is complete. By Theorem 1.57, its corresponding congruence is the largest congruence which saturates L. By Proposition 1.25, this is $\sim_L$, which must have finite index, because its corresponding residuation ideal $B(L) = A_{\sim_L}$ is finite. □

Exercise 1.66. a. ($\star\star$) Verify, in the case of the example automaton given at the beginning of this chapter, that $B(L)$ is equal to $B(\mathcal{A})$ (which you calculated in Exercise 1.62), and isomorphic to the power semigroup of $A^+/\sim_L$ (which you calculated in Exercise 1.27).

b. ($\star$) Give an example of an automaton $\mathcal{A}'$ that recognizes L but has $B(\mathcal{A})$ strictly bigger than $B(L)$.

c. ($\star\star\star$) Formulate a conjecture about when $B(\mathcal{A})$ is equal to $B(L)$, and prove it.

The title of this chapter was 'Syntactic semigroups as dual spaces'. But why 'spaces'? We barely mentioned topology in this chapter, so for now the word 'space' may just seem like a hollow name to make things sound fancy. In the next chapter, we will show that this is not the case, and we will become more serious about topology.

Bibliography

[1] M. Gehrke and S.J. v. Gool, *Duality*, Textbook draft, available online at `https://www.samvangool.net/dualitybook-draft.pdf`, 2020.

[2] J.-É. Pin, *Mathematical foundations of automata theory*, Lecture notes, available online at `https://www.irif.fr/~jep/PDF/MPRI/MPRI.pdf`, 2020.

[3] M. P. Schützenberger, *On finite monoids having only trivial subgroups*, Information and Control **8** (1965), no. 2, 190–194.