1 Introduction

While the course is mostly based on the book [BK08], we depart from it in several occasions. These notes cover material which is either not presented in [BK08], or on which we substantially differ from [BK08].

2 Transition Systems

Fix a set $AP$ of atomic propositions. Recall from [BK08, Def. 2.1] that a transition system over $AP$ is a tuple

$$TS = (S, Act, \to, I, AP, L)$$

where

- $S$ is the set of states,
- $I \subseteq S$ is the set of initial states,
- $Act$ is the set of actions,
- $\to \subseteq S \times Act \times S$ is the transition relation,
- $L : S \to P(AP)$ is the labelling function.

We refer to [BK08, Chap. 2] for examples.
3 Linear-Time Properties

We follow the approach of [BK08, Chap. 3] with a few differences in terminology and notation.

**Definition 3.1.** A linear-time (LT) property over a set $AP$ of atomic propositions is a set of $\omega$-words $P \subseteq (2^{AP})^\omega$.

We refer to [BK08, Chap. 3] for examples.

**Notation 3.2.** We often write $\sigma$ for an $\omega$-word in $\Sigma^\omega$ and $\hat{\sigma}$ for a finite word $\Sigma^*$. Given $\sigma$ and $\hat{\sigma}$, we write $\hat{\sigma} \subseteq \sigma$ to mean that $\hat{\sigma}$ is a (finite) prefix of $\sigma$, i.e. that

$$\forall i < \text{length}(\hat{\sigma}), \hat{\sigma}(i) = \sigma(i)$$

Moreover, we let $\text{Pref}(\sigma) := \{ \hat{\sigma} | \hat{\sigma} \subseteq \sigma \}$

### 3.1 Linear-Time Behaviour of Transition Systems

Fix a transition system $TS = (S, \text{Act}, \rightarrow, I, AP, L)$ over $AP$.

**Definition 3.3 (Path).** A (finite or infinite) path in $TS$ is a finite or infinite sequence of states $\pi = (s_i)_{i < n}$ with $n \leq \omega$ which respects the transitions of $TS$ in the sense that for all $i$ such that $i + 1 < n$, we have $s_i \xrightarrow{a} s_{i+1}$ for some $a \in \text{Act}$.

A path $\pi = (s_i)_{i < n}$ is initial if $s_0$ is initial (i.e. if $s_0 \in I$).

**Definition 3.4 (Trace).**

(1) Let $\pi = (s_i)_{i < n}$ be finite or infinite path. The trace of $\pi$ is the finite or infinite word

$$L(\pi) := (L(s_i))_{i < n}$$

(2) The set of traces of $TS$ is

$$\text{Tr}(TS) := \{ L(\pi) | \pi \text{ finite or infinite initial path of } TS \}$$

We shall write $\text{Tr}^\omega(TS)$ (resp. $\text{Tr}_{\text{fin}}(TS)$) for the set of infinite (resp. finite) traces of $TS$.

**Definition 3.5 (Satisfaction of Linear-Time Properties).** We say that $TS$ satisfies a LT property $P \subseteq (2^{AP})^\omega$, notation $TS \models P$, if $\text{Tr}^\omega(TS) \subseteq P$.

Two transition systems have the same infinite traces if and only if they satisfy the same LT properties.

**Proposition 3.6.** Given two transition systems $TS$ and $TS'$, both over $AP$, we have

$$\text{Tr}^\omega(TS) \subseteq \text{Tr}^\omega(TS') \iff \forall P \subseteq (2^{AP})^\omega, \text{ TS' } \models P \implies \text{ TS } \models P$$

*Proof.* Assume $\text{Tr}^\omega(TS) \subseteq \text{Tr}^\omega(TS')$. Then for an LT property $P$ such that $TS' \models P$, we have $\text{Tr}^\omega(TS) \subseteq \text{Tr}^\omega(TS') \subseteq P$, so that $TS \models P$.

Conversely, let $P \subseteq (2^{AP})^\omega$ be the LT property $\text{Tr}^\omega(TS')$. Then $TS' \models P$, but $TS \not\models P$ unless $\text{Tr}^\omega(TS) \subseteq \text{Tr}^\omega(TS')$. 

\[\Box\]
3.2 Safety Properties and Invariants

Fix a set AP of atomic propositions.

3.2.1 Invariants

An invariant is an LT property $P \subseteq (2^{AP})^\omega$ such that for some propositional formula $\varphi$ over AP, we have

$$P = \{ \sigma \in (2^{AP})^\omega | \forall i \in \mathbb{N}, \sigma(i) \models \varphi \}$$

3.2.2 Safety Properties

**Definition 3.7 (Safety Property).** We say that $P \subseteq (2^{AP})^\omega$ is a safety property if there is a (possibly infinite) set of finite words $P_{bad} \subseteq (2^{AP})^*$ such that $P$ is the set of $\omega$-words which avoid $P_{bad}$, in the sense that

$$P = \{ \sigma \in (2^{AP})^\omega | \forall \hat{\sigma} \subseteq \sigma, \hat{\sigma} /\in P_{bad} \}$$

In this case we say that $P$ is induced by $P_{bad}$.

A state $s \in S$ of a transition system $TS$ is called terminal if there are no state $s' \in S$ and no action $a \in Act$ such that $s \xrightarrow{a} s'$.

**Proposition 3.8 (Satisfaction of Safety Properties).** Let $P \subseteq (2^{AP})^\omega$ be a safety property induced by $P_{bad}$. Given a transition system $TS$ over AP and without terminal states, we have

$$TS \models P \iff \text{Tr}_{\text{fin}}(TS) \cap P_{bad} = \emptyset$$

*Proof.* Exercise!

3.2.3 Regular Safety Properties

We essentially follow here [BK08, §4.2], hence momentarily jumping to Chapter 4 (Regular Properties).

**Definition 3.9 (Regular Safety Property).** A safety property $P \subseteq (2^{AP})^\omega$ is regular if it is induced by a regular set $P_{bad} \subseteq (2^{AP})^*$.

Let $P \subseteq (2^{AP})^\omega$ be the regular safety property induced by the regular set $P_{bad} \subseteq (2^{AP})^*$. Fix an NFA

$$\langle A : 2^{AP} \rangle = (Q, \Delta, Q_0, F)$$

which recognizes $P_{bad}$. Note that we can assume $P_{bad}$ to be suffix-closed, and that for $q \in F$ and $A \in 2^{AP}$ we have $(q, A, q') \in \Delta$ iff $q' = q$.

Consider now a transition system $TS$ over AP:

$$TS = (S, Act, \rightarrow, I, AP, L)$$

We define the product transition system

$$TS \otimes A := (S_\otimes, Act, \rightarrow_\otimes, I_\otimes, AP_\otimes, L_\otimes)$$

as follows:
• The set of states is \( S_\otimes := S \times Q \).

• The transition relation \( \rightarrow_\otimes \) is defined by the rule

\[
\frac{s \xrightarrow{a} s'}{(q, L(s'), q') \in \Delta} \quad (s, q) \xrightarrow{a} (s', q')
\]

Note that it is the label of the target state \( s' \) of \( s \xrightarrow{a} s' \) which is used as input letter of \( \mathcal{A} \).

• The set of initial states \( I_\otimes \) is the set of all pairs \((s_0, q)\) such that \( s_0 \) is initial in \( TS \) \((s_0 \in I)\) and such that we have \((q_0, L(s_0), q)\) for some initial \( q_0 \in Q_0 \).

• \( \mathcal{A}_\otimes := Q \).

• \( L_\otimes(s, q) := \{ q \} \).

Since the accepting states \( F \) of \( \mathcal{A} \) are assumed to be sink states, we can reduce checking \( TS \models P \) to checking that \( TS \otimes \mathcal{A} \) satisfies the invariant property induced by

\[
\varphi_\mathcal{A} := \bigwedge_{q \in F} \neg q
\]

Note that if \( TS \) has no terminal states, then it follows from Prop. 3.8 that we have \( TS \models P \iff \text{Tr}_{\text{fin}}(TS) \cap L(\mathcal{A}) = \emptyset \)

**Proposition 3.10.** Assume that \( TS \) has no terminal states. Then \( TS \models P \iff \text{the transition system } TS \otimes \mathcal{A} \text{ satisfies the invariant induced by } \varphi_\mathcal{A} \).

*Proof.* Exercise! \( \square \)

### 3.2.4 Safety Properties and Trace Equivalence

Proposition 3.8 directly gives the following.

**Lemma 3.11.** Consider \( TS \) and \( TS' \), both over \( \text{AP} \) and both without terminal states. We have

\[
\text{Tr}_{\text{fin}}(TS) \subseteq \text{Tr}_{\text{fin}}(TS') \iff \forall P \subseteq (2^{\text{AP}})^\omega \text{ safety, } TS' \models P \implies TS \models P
\]

*Proof.* Exercise! \( \square \)

**Definition 3.12** (Finitely Branching TS). A transition system \( TS = (S, \text{Act}, \rightarrow, I, \text{AP}, L) \) is **finitely branching** when the two following conditions are satisfied:

• \( I \) is finite, and

• for every \( s \in S \), there are at most finitely many \( s' \in S \) such that \( s \xrightarrow{a} s' \) for some \( a \in \text{Act} \).

**Proposition 3.13.** Consider \( TS \) and \( TS' \), both over \( \text{AP} \) and both finitely branching and without terminal states. Then

\[
\text{Tr}(TS) \subseteq \text{Tr}(TS') \iff \text{Tr}_{\text{fin}}(TS) \subseteq \text{Tr}_{\text{fin}}(TS')
\]

**Corollary 3.14.** Consider finitely branching \( TS \) and \( TS' \), both over \( \text{AP} \) and both without terminal states. Then we have

\[
\text{Tr}(TS) \subseteq \text{Tr}(TS') \iff \forall P \subseteq (2^{\text{AP}})^\omega \text{ safety, } TS' \models P \implies TS \models P
\]
3.2.5 Proof of Proposition 3.13

Proposition 3.13 relies on a principle of infinite combinatorics known as König’s Lemma. It basically says that if an infinite tree is finitely branching, then it has an infinite path.

Definition 3.15.

(1) A tree on a set $A$ is a set $T \subseteq A^*$ which is closed under prefix: if $u \in T$ and $v \subseteq u$ then $v \in T$.

(2) A tree $T$ is finitely branching if for all $u \in T$, there are at most finitely many $a \in A$ such that $u.a \in T$.

(3) An infinite path in a tree $T$ over $A$ is an $\omega$-word $\pi \in A^\omega$ whose finite prefixes belong all to $T$: 

$$\forall n \in \mathbb{N}, \quad \pi(0)\cdots\pi(n) \in T$$

Note that a tree $T$ over $A$ is automatically finitely branching if $A$ is finite.

Lemma 3.16 (König’s Lemma). If $T$ is an infinite tree which is finitely-branching, then $T$ has an infinite path.

Proof. Given a tree $T \subseteq A^*$ and $u \in A^*$, we write $T|u$ for the subtree of $T$ at $u$:

$$T|u := \{ v \in T \mid u \subseteq v \text{ or } v \subseteq u \}$$

Fix a tree $T \subseteq A^*$, and assume that $T$ is infinite and finitely branching. We build an infinite path $\pi = (a_n)_{n \in \mathbb{N}}$ by induction on $n \in \mathbb{N}$ as follows. First, note that $T$ is the union of the $T|a$ for $a \in A$. Since $T$ is infinite and finitely branching, by the infinite pigeonhole principle there is some $a \in A$ such that $T|a$ is infinite. We let $a_0 := a$. Iterating this process, we obtain a sequence $(a_n)_{n \in \mathbb{N}}$ such that

- $a_0 \cdots a_n \in T$ for all $n \in \mathbb{N}$,
- $T|(a_0 \cdots a_n)$ is infinite for all $n \in \mathbb{N}$.

Assuming $a_0, \ldots, a_n$ defined, since

$$T|(a_0 \cdots a_n) = \bigcup_{\substack{a \in A \\ (a_0 \cdots a_n a) \in T}} T|(a_0 \cdots a_n a)$$

is infinite and finitely branching, by the infinite pigeonhole principle there is some $a \in A$ such that $a_0 \cdots a_n a \in T$ and $T|(a_0 \cdots a_n a)$ is infinite. We let $a_{n+1} := a$.

We can now prove Prop. 3.13.

Proof of Proposition 3.13. Assume first that $\text{Tr}^\omega(TS) \subseteq \text{Tr}^\omega(TS')$. Then given $\hat{\sigma} \in \text{Tr}_{\text{fin}}(TS)$, since $TS$ has no terminal states we have $\hat{\sigma} \subseteq \sigma$ for some $\sigma \in \text{Tr}^\omega(TS) \subseteq \text{Tr}^\omega(TS')$, and it follows that $\hat{\sigma} \in \text{Tr}_{\text{fin}}(TS')$.

For the converse, assume $\text{Tr}_{\text{fin}}(TS) \subseteq \text{Tr}_{\text{fin}}(TS')$ and let $\sigma \in \text{Tr}^\omega(TS)$. Then for all $\hat{\sigma} \subseteq \sigma$ we have $\hat{\sigma} \in \text{Tr}_{\text{fin}}(TS) \subseteq \text{Tr}_{\text{fin}}(TS')$. As a consequence, for all $n \in \mathbb{N}$ there is in $TS'$ a finite initial path

$$\pi_n = s_0^n \cdots s_n^n$$
such that

\[ L'(\pi_n) \subseteq \sigma \]

But note that we may not have \( \pi_n \subseteq \pi_{n+1} \). We therefore apply König’s Lemma 3.16 to build a suitable infinite path in \( TS' \). Consider the tree \( T \subseteq (S')^* \) defined as

\[ T := \{ u \in (S')^* \mid u \text{ is a finite initial path in } TS' \text{ and } L'(u) \subseteq \sigma \} \]

Then \( T \) is evidently a tree. It is finitely branching since \( TS' \) is finitely branching. Moreover \( T \) is infinite: for all \( \hat{\sigma} \subseteq \sigma \) we have \( \hat{\sigma} \in \text{Tr}_{\text{fin}}(TS) \subseteq \text{Tr}_{\text{fin}}(TS') \), so there is a finite initial path \( u \) in \( TS' \) such that \( L'(u) = \hat{\sigma} \). By König’s Lemma 3.16, \( T \) has an infinite path \( \pi \). We have \( L'(\pi) = \sigma \) since \( L'(\pi(0) \cdots \pi(n)) \subseteq \sigma \) for all \( n \in \mathbb{N} \). Moreover, \( \pi \) is an initial path in \( TS' \) by construction of \( T \).

We can nevertheless give a direct proof of Prop. 3.13.

**Direct Proof of Proposition 3.13.** Assume first that \( \text{Tr}^\omega(TS) \subseteq \text{Tr}^\omega(TS') \). Then given \( \hat{\sigma} \in \text{Tr}_{\text{fin}}(TS) \), since \( TS \) has no terminal states we have \( \hat{\sigma} \subseteq \sigma \) for some \( \sigma \in \text{Tr}^\omega(TS) \subseteq \text{Tr}^\omega(TS') \), and it follows that \( \hat{\sigma} \in \text{Tr}_{\text{fin}}(TS') \).

For the converse, assume \( \text{Tr}_{\text{fin}}(TS) \subseteq \text{Tr}_{\text{fin}}(TS') \) and let \( \sigma \in \text{Tr}^\omega(TS) \). Then for all \( \hat{\sigma} \subseteq \sigma \) we have \( \hat{\sigma} \in \text{Tr}_{\text{fin}}(TS) \subseteq \text{Tr}_{\text{fin}}(TS') \). As a consequence, for all \( n \in \mathbb{N} \) there is in \( TS' \) a finite initial path

\[ \pi_n = s_0^n \cdots s_n^n \]

such that

\[ L'(\pi_n) \subseteq \sigma \]

But note that we may not have \( \pi_n \subseteq \pi_{n+1} \). However, since \( TS' \) is finitely branching, by the infinite pigeonhole principle there is some state \( s \in S' \) such that \( s_0^n = s \) for infinitely many \( n \in \mathbb{N} \). This induces an infinite subsequence \( (\pi_n^k)_{n \in \mathbb{N}} \) of \( (\pi_n)_{n \in \mathbb{N}} \) with \( \pi_n^k(0) = s \) for all \( n \in \mathbb{N} \). Iterating this process, we get for each \( k \in \mathbb{N} \) an infinite sequence \( (\pi_n^k)_{n \in \mathbb{N}} \) such that

- each \( \pi_n^k \) has length at least \( n \),
- \( (\pi_n^{k+1})_{n \in \mathbb{N}} \) is an infinite subsequence of \( (\pi_n^k)_{n \in \mathbb{N}} \),
- and for each \( k \in \mathbb{N} \), all the

\[ \pi_n^k := \pi_n^k(0) \cdots \pi_n^k(k) \]

agree for \( n \geq k \).

It follows that \( (\pi_n^k)_{k \in \mathbb{N}} \) forms an infinite strictly increasing sequence in \( (S')^* \). Then its limit \( \pi \) in \( (S')^\omega \) is an infinite initial path in \( TS' \) such that \( L'(\pi) = \sigma \). Hence \( \sigma \in \text{Tr}^\omega(TS') \) and we are done.

### 3.3 Liveness Properties

**Definition 3.17** (Liveness Property). We say that \( P \subseteq (2^{AP})^\omega \) is a liveness property if for every \( \hat{\sigma} \in (2^{AP})^* \) there is some \( \sigma \in P \) such that \( \hat{\sigma} \subseteq \sigma \).
3.4 Safety vs Liveness

Proposition 3.18 ([BK08, Lem. 3.35]). The only LT property which is both a safety and a liveness property is the “true” property \((2^{\text{AP}})^\omega\).

Proof. First, note that \((2^{\text{AP}})^\omega\) is evidently a liveness property. It is also the safety property induced by \(P_{\text{bad}} := \emptyset\).

Conversely, let \(P \subseteq (2^{\text{AP}})^\omega\) be both a liveness property and a safety property, say induced by \(P_{\text{bad}}\). Then for every \(\hat{\sigma} \in P_{\text{bad}}\) there must be some \(\sigma \in P\) such that \(\hat{\sigma} \subseteq \sigma\). But this implies \(P_{\text{bad}} = \emptyset\). \(\square\)

Theorem 3.19 (Decomposition ([BK08, Thm. 3.37])). For every LT property \(P \subseteq (2^{\text{AP}})^\omega\), there is a safety property \(P_{\text{safe}}\) and a liveness property \(P_{\text{liveness}}\) such that

\[ P = P_{\text{safe}} \cap P_{\text{liveness}} \]

The Decomposition Theorem 3.19 is be proved in §4.2 as a corollary of a topological decomposition theorem. An alternative proof, based on closure operators and Galois connections and actually following [BK08, Thm. 3.37], is presented in §5.5.1.

4 Topological Approach

The goal of this Section is to present (and prove) the Decomposition Theorem 3.19 in its natural topological context.

4.1 Generalities

We expose some basic fundamental concepts and facts on general (or set-theoretic) topological spaces. We refer to [Wil70, Chap. 2] and [Run05, Chap. 3] for most of the material.

Definition 4.1. A topological space is a pair \((X, \Omega X)\) where \(X\) is a set and \(\Omega X \subseteq \mathcal{P}(X)\) is a family of subsets of \(X\), called the open subsets of \(X\), and such that

- \(\Omega X\) is closed under unions: given a family \((U_i)_{i \in I}\) of open sets, the set \(\bigcup_{i \in I} U_i\) is open as well, and
- \(\Omega X\) is closed under finite intersections: given a finite family \((U_i)_{i \in I}\) of open sets, the set \(\bigcap_{i \in I} U_i\) is open.

The complements of open sets, i.e. the sets of the form \(X \setminus U\) for \(U\) open, are called closed.

Note that \(\emptyset\) and \(X\) (as resp. the empty union and the empty intersection) are always open (and thus closed) in \((X, \Omega X)\). Moreover, closed sets are closed under arbitrary intersections and finite unions.

Lemma 4.2. Let \((X, \Omega X)\) be a topological space.

- Given a family \((C_i)_{i \in I}\) of closed sets, the set \(\bigcap_{i \in I} C_i\) is closed as well.
- Given a finite family \((C_i)_{i \in I}\) of closed sets, the set \(\bigcup_{i \in I} C_i\) is closed.

In order to show that a particular subset of a topological space is open (resp. closed), one usually proceeds by the following basic fact.
Lemma 4.3. Let \((X, \Omega_X)\) be a topological space.

(1) A set \(A \subseteq X\) is open iff for every \(x \in A\) there is an open set \(U \in \Omega_X\) such that \(x \in U\) and \(U \subseteq A\).

(2) A set \(A \subseteq X\) is closed iff for every \(x \notin A\) there is an open set \(U \in \Omega_X\) such that \(x \in U\) and \(U \cap A = \emptyset\).

Proof. Exercise! 

Every subset \(A\) of topological space \((X, \Omega_X)\) is contained in a least closed set \(\overline{A}\).

Definition 4.4 (Closure of a set). Given a topological space \((X, \Omega_X)\) and a set \(A \subseteq X\), the closure \(\overline{A}\) of \(A\) is defined as

\[
\overline{A} := \bigcap\{C \subseteq X \mid A \subseteq C \text{ and } C \text{ is closed}\}
\]

Note that \(\overline{A}\) is closed as an intersection of closed sets. Moreover, \(\overline{A}\) is the least closed set containing \(A\):

- if \(A \subseteq C\) with \(C\) closed, then \(\overline{A} \subseteq C\).

In particular, a set \(A \subseteq X\) is closed iff \(\overline{A} = A\). The following is [Wil70, Thm. 3.7]. See also [Run05, Def. 3.1.19 & Thm. 3.1.20].

Lemma 4.5. Given subsets \(A, B \subseteq X\) of a topological space \((X, \Omega_X)\), we have

(1) \(A \subseteq B\) implies \(\overline{A} \subseteq \overline{B}\),

(2) \(A \subseteq \overline{A}\),

(3) \(\overline{(A)} = \overline{A}\),

(4) \(\overline{\emptyset} = \emptyset\),

(5) \(\overline{A} \cup \overline{B} = \overline{A \cup B}\).

Proof. Exercise! 

Remark 4.6. Given a set \(A\), an operator \((\overline{-}) : \mathcal{P}(A) \to \mathcal{P}(A)\) satisfying all the conditions of Lem. 4.5 is called a Kuratowski closure operator. Closure operators, which are only required to satisfy the first three conditions of Lem. 4.5 are further discussed in the context of complete lattices in §5.3. It in particular follows from Lem. 5.16 that a Kuratowski closure operator \((\overline{-}) : \mathcal{P}(X) \to \mathcal{P}(X)\) induces a topology on \(X\), with \(C \subseteq X\) closed iff \(\overline{C} = C\).

4.1.1 Adherence

The following notion is useful to reason on the closure of a set. We refer to [Bou07, Chap. 1] for developments.

Definition 4.7 (Adherent Point). Consider a topological space \((X, \Omega_X)\) and some \(A \subseteq X\). We say that \(x \in X\) is adherent to \(A\) (or that \(x\) is an adherent point of \(A\)) if \(A\) intersects any open set which contains \(x\):

\[
\forall U \in \Omega_X, \quad x \in U \implies A \cap U \neq \emptyset
\]
Remark 4.8 (Terminology). In the English terminology, adherent points are also called **points of closure**.

Adherent points provide a handy characterization of the closure of a set.

**Lemma 4.9.** Consider a topological space \((X, \Omega X)\) and some \(A \subseteq X\). Then \(x\) is adherent to \(A\) if and only if \(x \in \overline{A}\).

**Proof.** Exercise! \(\square\)

### 4.1.2 The Topological Decomposition Theorem

**Definition 4.10** (Dense Set). Let \((X, \Omega X)\) be a topological space. A set \(D \subseteq X\) is **dense** if \(D \cap U \neq \emptyset\) for all non-empty open \(U\).

**Theorem 4.11** (Topological Decomposition Theorem). Let \((X, \Omega X)\) be a topological space. Then for any \(A \subseteq X\), there is some closed set \(C\) and some dense set \(D\) such that \(A = C \cap D\).

**Proof.** Let \(C := \overline{A}\) and \(D := A \cup (X \setminus \overline{A})\). The set \(C\) is trivially closed. Moreover,

\[
C \cap D = (\overline{A} \cap A) \cup (\overline{A} \cap (X \setminus \overline{A})) = A
\]

It thus remains to show that \(D\) is dense. So let \(U\) be a non-empty open set. If \(U \cap A = \emptyset\), then \(A\) is included in the closed set \(X \setminus U\). But this implies \(\overline{A} \subseteq X \setminus U\), so that \(U \subseteq X \setminus \overline{A}\). \(\square\)

Let us finally mention a useful property on dense sets.

**Lemma 4.12.** Let \((X, \Omega X)\) be a topological space. A set \(D \subseteq X\) is dense if and only if \(\overline{D} = X\).

**Proof.** Exercise! \(\square\)

**Remark 4.13** (Alternative Proof of Thm. 4.11). Lemma 4.12, together with the fact that \((\cdot)\) is a Kuratowski closure operator (see Lem. 4.5 and Rem. 4.6) gives a more direct proof of the Topological Decomposition Theorem 4.11, similar in spirit to the proof of [BK08, Thm. 3.37] (see §5.5.1). The argument goes as follows. Taking \(D := A \cup (X \setminus \overline{A})\) as in the proof of Thm. 4.11, by Lem. 4.5 we have

\[
\overline{D} = \overline{A} \cup (X \setminus \overline{A})
\]

It follows that \(\overline{D} = X\), and thus that \(D\) is dense by Lem. 4.12.

### 4.1.3 Bases and Subbases

It is often convenient to define a topology from more atomic data than the direct description of open sets.

**Lemma 4.14** (Base). Consider a set \(X\) together with a family of sets \(\mathcal{B} \subseteq \mathcal{P}(X)\) which is closed under finite intersections. Let \(\Omega X\) consist of all the \(\bigcup_{i \in I} U_i\) for \((U_i)_{i \in I}\) a family of elements of \(\mathcal{B}\). Then \((X, \Omega X)\) is a topological space.

**Proof.** Exercise! \(\square\)

A family \(\mathcal{B}\) as in Lem. 4.14 is a base of the topology \(\Omega X\). In practice, it is often more convenient to generate a base as the closure under finite intersections of an arbitrary family \(\mathcal{B}_0\) subsets of \(X\). Such \(\mathcal{B}_0\) are the called subbases of \(\Omega X\).
4.2 Spaces of \( \omega \)-Words

**Definition 4.15** (The Topology on Streams). Given a non-empty set \( A \), we equip \( A^\omega \) with the topology induced by the subbase \( (\text{ext}(u))_{u \in A^*} \), where

\[
\text{ext}(u) := \{ \sigma \in A^\omega \mid u \subseteq \sigma \}
\]

Note that \( A^\omega = \text{ext}(\varepsilon) \). Also, if \( u, v \in A^* \) are incomparable w.r.t. the prefix order then \( \text{ext}(u) \cap \text{ext}(v) = \emptyset \). Moreover:

**Lemma 4.16.** Given \( u, v \in A^* \) we have

\[
\text{ext}(u) \subseteq \text{ext}(v) \quad \text{iff} \quad v \subseteq u
\]

**Proof.** Exercise! \( \square \)

As a consequence, every open of \( A^\omega \) is a union of sets of the form \( \text{ext}(u) \) for \( u \in A^* \). Lemma 4.3 gives a quite useful characterization of the open (resp. closed) subsets of \( A^\omega \).

**Lemma 4.17.** Let \( A \) be a non-empty set.

1. A set \( P \subseteq A^\omega \) is open iff for every \( \sigma \in P \) there is a finite word \( \hat{\sigma} \in A^* \) such that \( \hat{\sigma} \subseteq \sigma \) and \( \beta \in P \) for all \( \beta \in A^\omega \) such that \( \hat{\sigma} \subseteq \beta \).

2. A set \( P \subseteq A^\omega \) is closed iff for every \( \sigma \notin P \) there is a finite word \( \hat{\sigma} \in A^* \) such that \( \hat{\sigma} \subseteq \sigma \) and \( \beta \notin P \) for all \( \beta \in A^\omega \) such that \( \hat{\sigma} \subseteq \beta \).

In particular, if \( C \subseteq A^\omega \) is closed, then given \( \sigma \in A^\omega \), we have \( \sigma \in C \) whenever for all \( \hat{\sigma} \subseteq \sigma \) there is some \( \beta \in C \) with \( \hat{\sigma} \subseteq \beta \).

**Notation 4.18.** Given \( U \subseteq A \) we let

\[
\begin{align*}
\text{ext}(u) & := \{ \sigma \in A^\omega \mid u \subseteq \sigma \} \\
\text{ext}(U) & := \bigcup_{u \in U} \text{ext}(u)
\end{align*}
\]

**Remark 4.19** (A Base on Streams). Note that we have \( \text{ext}(\emptyset) = \emptyset \). Moreover, sets of streams the form \( \text{ext}(U) \) for \( U \subseteq A^* \) are closed under finite intersections. Since \( A^\omega = \text{ext}(\{\varepsilon\}) \in \mathcal{B}_A \), we just have to consider the case of binary intersections. But for \( U, V \subseteq A^* \) we have

\[
\text{ext}(U) \cap \text{ext}(V) = (\bigcup_{u \in U} \text{ext}(u)) \cap (\bigcup_{v \in V} \text{ext}(v)) = \bigcup_{u \in U, v \in V} \text{ext}(u) \cap \text{ext}(v)
\]

Now \( \text{ext}(u) \cap \text{ext}(v) \) is either empty or equal to \( \text{ext}(u) \) or \( \text{ext}(v) \), so that \( \bigcup_{u \in U, v \in V} \text{ext}(u) \cap \text{ext}(v) \) is indeed of the form \( \text{ext}(W) \) for some \( W \subseteq A^* \). Moreover \( W \) is finite whenever so are \( U, V \).

As a consequence the set \( \mathcal{B}_A \subseteq \mathcal{P}(A^\omega) \) consist of all sets of the form \( \text{ext}(U) \) for \( U \subseteq A^* \) finite can be used as base for a topology on \( A^\omega \). It easy to show that it coincides with that of Def. 4.15.
4.2.1 Topological Safety and Liveness

**Lemma 4.20.** An LT property is closed if and only if it is a safety property.

*Proof.* Exercise!

**Lemma 4.21.** An LT property is dense if and only if it is a liveness property.

*Proof.* Exercise!

The Decomposition Theorem 3.19 is thus a direct consequence of the Topological Decomposition Theorem 4.11.

**Corollary 4.22** (Decomposition (Thm. 3.19)). For every LT property $P \subseteq (2^{\mathcal{AP}})^\omega$, there is a safety property $P_{\text{safe}}$ and a liveness property $P_{\text{liveness}}$ such that

$$P = P_{\text{safe}} \cap P_{\text{liveness}}$$

Let us finally mention the following alternative characterization of liveness properties.

**Corollary 4.23.** An LT property $P \subseteq (2^{\mathcal{AP}})^\omega$ is a liveness property if and only if $P = (2^{\mathcal{AP}})^\omega$.

Corollary 4.23 is a direct consequence of Lem. 4.21 and Lem. 4.12.

5 Partial Orders and Complete Lattices

In this Section, we target the proof of the Decomposition Theorem 3.19 given as [BK08, Thm. 3.37]. This is the occasion to introduce some basic concepts and facts on partial orders and complete lattices, for which mainly refer to [DP02]. We indicate differences in notation and terminology whenever possible.

5.1 Partial Orders

**Definition 5.1** ([DP02, Def. 1.2]). A partial order is a pair $(A, \leq)$ where $A$ is a set and $\leq$ is a binary relation on $A$ which is

- reflexive: $a \leq a$ for all $a \in L$,
- transitive: $a \leq c$ whenever $a \leq b$ and $b \leq c$,
- antisymmetric: $a = b$ whenever $a \leq b$ and $b \leq a$.

**Definition 5.2.** The opposite of a partial order $(A, \leq)$ is the partial order $(A, \geq)^{\text{op}} := (A, \geq)$ where $a \geq b$ iff $b \leq a$.

We often just write $A^{\text{op}}$ for the opposite of $(A, \leq)$. Opposites are called duals in [DP02] and are denoted $(A, \leq)^{\varnothing}$. We refer to [DP02, §1.19 & §1.20] for further comments on opposites.

**Definition 5.3** (Monotone Function). Consider partial orders $(A, \leq_A)$ and $(B, \leq_B)$ and a function $f : A \to B$.

(a) We say that $f$ is monotone if $f(a) \leq_B f(a')$ whenever $a \leq_A a'$.

(b) We say that $f$ is antimonotone if $f(a') \leq_B f(a)$ whenever $a \leq_A a'$. 

11
In other words, a function $A \to B$ is antimonotone iff it is monotone as a function $A^\text{op} \to B$.

**Definition 5.4.** Let $(A, \leq)$ be a partial order and consider some set $S \subseteq A$.

(1) An upper bound of $S$ is some $b \in A$ such that $s \leq b$ for all $s \in S$.

(2) A least upper bound (or join) of $S$ is an upper bound $\bigvee S$ such that $\bigvee S \leq b$ for every upper bound $b$ of $S$.

A lower bound of $S$ is an upper bound of $S \cap A$. A greatest lower bound (or meet) $\bigwedge S$ of $S$ is a least upper bound of $S$ in $(A, \leq)^\text{op}$.

In words, $b \in A$ is a lower bound of $S$ iff $b \leq s$ for all $s \in S$, and $\bigwedge S$ is a lower bound of $S$ such that $b \leq \bigwedge S$ for all lower bound $b$ of $S$. Note that by antisymmetry, joins and meets are unique whenever they exist. We refer to [DP02, Def. 2.1] for a slightly more elaborated definition of (least) upper and (greatest) lower bounds.

### 5.2 Complete Lattices

**Definition 5.5.** A complete lattice is a partial order $(L, \leq)$ such that every subset $S \subseteq L$ has both a join (i.e. least upper bound) $\bigvee S \in L$ and a meet (i.e. greatest lower bound) $\bigwedge S \in L$.

Note that a complete lattice $(L, \leq)$ has in particular a least element $\bot = \bigvee \emptyset \in L$ and a greatest element $\top = \bigwedge \emptyset \in L$. We repeat that by antisymmetry, joins and meets are unique.

**Example 5.6.** Given a set $A$, the set $(\mathcal{P}(A), \subseteq)$ is a complete lattice.

The notion of complete lattice of [DP02, Def. 2.4] relies on the following, which can be rephrased as a consequence of [DP02, Thm. 2.31].

**Lemma 5.7.** The following are equivalent for a partial order $(L, \leq)$:

1. $(L, \leq)$ is a complete lattice,
2. every subset $S \subseteq L$ has a join $\bigvee S \in L$,
3. every subset $S \subseteq L$ has a meet $\bigwedge S \in L$.

**Proof.** It is obvious that the first condition implies the other two. Let $(L, \leq)$ be a partial order with all joins. Given $S \subseteq L$, define:

$$B := \{ b \in L \mid \forall s \in S, b \leq s \}$$

We claim that $\bigvee B$ is the greatest lower bound of $S$. Indeed, given $s \in S$, we have $b \leq s$ for all $b \in B$, so that $\bigvee B \leq s$. Moreover, given a lower bound $b$ of $S$, we have $b \in B$, and thus $b \leq \bigvee B$.

The proof that having all meets implies having all joins is similar. □

A particular case of complete lattices are the frames. They simply abstract the lattice structure of open sets. This apparently candid notion is the basis of considerable developments, see e.g. [Joh86].

**Definition 5.8.** A frame is a partial order $(L, \leq)$ which has finite meets and all joins, and which satisfies the following infinite distributive law, where $S$ is an arbitrary subset of $L$:

$$a \wedge \bigvee S = \bigvee \{ a \wedge s \mid s \in S \}$$
Corollary 5.9. Every frame \((L, \leq)\) is a complete lattice.

Example 5.10. For a topological space \((X, \Omega_X)\), the partial order \((\Omega_X, \subseteq)\) is a frame where finite meets are given by finite intersections and joins are given by unions.

Recall that by antisymmetry, meets (and joins) in a partial order are unique whenever they exist. In particular, for a frame \((L, \leq, \wedge, \vee)\), we have

\[ a \wedge b = \vee \{ c \in L | c \leq a \text{ and } c \leq b \} \]

Corollary 5.11. For a topological space \((X, \Omega_X)\), the partial order \((\Omega_X, \subseteq)\) is a complete lattice.

Beware that meets of open sets are in general not given by intersections!

Example 5.12. Consider the space \(A^\omega\) for \(A = \{a, b\}\). The set \(S = \bigcap_{n \in \mathbb{N}} \text{ext}(a^n)\) is not open. Indeed, assume \(S = \bigcup_{u \in W} \text{ext}(u)\) for some \(W \subseteq A^*\). Then since \(S\) contains the \(\omega\)-word \(a^\omega\), we must have \(a^\omega \in \text{ext}(u)\) for some \(u \in W\). But this implies \(u = a^n\) for some \(n\) while \(\text{ext}(a^n)\) is not a subset of \(S\) since \(a^n b^\omega \in \text{ext}(a^n) \setminus \text{ext}(a^{n+1})\)

Given a topological space \((X, \Omega_X)\), following the proof of Lem. 5.7, the meet in \(\Omega_X\) of a family of open sets \(S \subseteq \Omega_X\) is given by

\[ \wedge S := \bigcup \{ U \in \Omega_X | \forall V \in S, U \subseteq V \} \]

In other words, \(\wedge S\) is the largest open set contained in \(\bigcap S\). This generalizes to the following usual notion.

Definition 5.13 (Interior (see e.g. [Wil70, Def. 3.9] or [Run05, Def. 2.2.22])). Given a topological space \((X, \Omega_X)\), the interior of a set \(A \subseteq X\) is

\[ \hat{A} := \bigcup \{ U \in \Omega_X | U \subseteq A \} \]

We state the following obvious fact, and refer to [Wil70, §3.9–12] for further material.

Lemma 5.14. Given a topological space \((X, \Omega_X)\), the interior \(\hat{A}\) of \(A \subseteq X\) is the largest open set contained in \(A\).

5.3 Closure Operators

Definition 5.15 ([DP02, Def. 7.1]). A closure operator on a partial order \((L, \leq)\) is a function \(c : L \rightarrow L\) which is

- monotone: \(a \leq b\) implies \(c(a) \leq c(b)\),
- expansive: \(a \leq c(a)\),
- idempotent: \(c(c(a)) = c(a)\).

We say that an element \(a \in L\) is closed when \(c(a) = a\). We write \(L^c\) for the set of closed elements of \(L\).
Lemma 5.16 ([DP02, Prop. 7.2]). Consider a closure operator $c$ on a complete lattice $(L, \leq)$. Then $L^c$ is a complete lattice with meets $\bigwedge S$ and joins $\bigvee S$ given resp. by

$$\bigwedge S = \bigwedge S \quad \text{and} \quad \bigvee S = c(\bigvee S)$$

Proof. Exercise! \hfill \Box

Closure operator are in particular an abstraction of the closure operation on subsets of a topological space.

Example 5.17. Given a topological space $(X, \Omega X)$, the operation $(-)$ is a closure operator on $\mathcal{P}(X)$.

We note the following, for the sake of sharpening our intuitions.

Lemma 5.18. Consider a closure operator $c$ on a complete lattice $(L, \leq)$. Then for all $a \in L$ we have

$$c(a) = \bigwedge \{c(b) \mid a \leq c(b)\}$$

Proof. Exercise! \hfill \Box

5.4 Galois Connections

Galois connections are the subject of [DP02, §7.23–35]. We differ on notation.

Definition 5.19. Given partial orders $(A, \leq_A)$ and $(B, \leq_B)$, a Galois connection $g \dashv f : A \to B$ is given by a pair of functions

$$g : A \to B \quad f : B \to A$$

such that for all $a \in A$ and all $b \in B$ we have

$$g(a) \leq_B b \iff a \leq_A f(b)$$

In a Galois connection $g \dashv f$, $g$ (resp. $f$) is called the lower adjoint (resp. upper adjoint).

Lemma 5.20 ([DP02, Lem. 7.26]). If $g \dashv f : A \to B$ form a Galois connection, then both $f$ and $g$ are monotone.

Proof. Exercise! \hfill \Box

Lemma 5.21 ([DP02, Prop. 7.27]). If $g \dashv f : A \to B$ is a Galois connection, then $f \circ g : A \to A$ is a closure operator.

Proof. Exercise! \hfill \Box

We refer to §5.6 for further general properties of Galois connections and closure operators.
5.5 Prefix and Closure

We now describe the closed subsets of $A^\omega$ by a closure operator induced by a Galois connection. This in particular gives another proof of the Decomposition Theorem 3.19 (see §5.5.1). We loosely follow the approach [BK08, Chap. 3]. Recall the definition of $\text{Pref}(\sigma)$ from Notation 3.2.

Given a non-empty set $A$, define

\[
\begin{align*}
\text{Pref} : \mathcal{P}(A^\omega) & \rightarrow \mathcal{P}(A^*) \\
P & \mapsto \bigcup \{\text{Pref}(\sigma) \mid \sigma \in P\}
\end{align*}
\]

\[
\begin{align*}
\text{cl} : \mathcal{P}(A^*) & \rightarrow \mathcal{P}(A^\omega) \\
W & \mapsto \{\sigma \in \Sigma^\omega \mid \text{Pref}(\sigma) \subseteq W\}
\end{align*}
\]

It is easy to see that these maps form a Galois connection $\text{Pref} \dashv \text{cl} : \mathcal{P}(A^\omega) \rightarrow \mathcal{P}(A^*)$.

**Lemma 5.22.** For all $P \subseteq A^\omega$ and all $W \subseteq A^*$ we have

\[
\text{Pref}(P) \subseteq W \iff P \subseteq \text{cl}(W)
\]

**Proof.** Exercise!

It thus follows from Lem. 5.21 that

\[
\text{cl} \circ \text{Pref} : \mathcal{P}(A^\omega) \rightarrow \mathcal{P}(A^\omega)
\]

is a closure operator. Note that

\[
\text{cl}(\text{Pref}(P)) = \{\sigma \in A^\omega \mid \text{Pref}(\sigma) \subseteq \text{Pref}(P)\}
\]

\[
= \{\sigma \in A^\omega \mid \forall \hat{\sigma} \subseteq \sigma, \exists \beta \in P, \hat{\sigma} \subseteq \beta\}
\]

**Proposition 5.23.** Given $P \subseteq A^\omega$, we have

\[
\overline{P} = \text{cl}(\text{Pref}(P))
\]

**Proof.** Exercise!

**Notation 5.24.** Given $P \subseteq A^\omega$ we often write $\text{cl}(P)$ for $\text{cl}(\text{Pref}(P))$. With this notation, $\text{cl}(P)$ is closure($P$) in the sense of [BK08, Def. 3.26].

Proposition 5.23, together with the fact that safety properties $P \subseteq (2^{AP})^\omega$ are the topologically closed subsets of $(2^{AP})^\omega$ (Lem. 4.20), gives the following. A direct proof is nevertheless possible.

**Corollary 5.25.** An LT property $P \subseteq (2^{AP})^\omega$ is a safety property if and only if $P = \text{cl}(P)$.

Together with Corollary 4.23, Prop. 5.23 gives the following.

**Corollary 5.26.** An LT property $P \subseteq (2^{AP})^\omega$ is a liveness property iff $\text{cl}(P) = (2^{AP})^\omega$.

We moreover have the following.

**Proposition 5.27.** An LT property $P \subseteq (2^{AP})^\omega$ is a liveness property iff $\text{Pref}(P) = (2^{AP})^*$.

**Proof.** Exercise!
5.5.1 Alternative Proof of the Decomposition Theorem 3.19

The Galois connection $\text{Pref} \dashv \text{cl} : \mathcal{P}(A^\omega) \to \mathcal{P}(A^*)$ gives an alternative, more combinatorial proof of Thm. 3.19, following the lines of [BK08, Thm. 3.37]. The combinatorial content of the argument is contained in the following.

**Lemma 5.28** ([BK08, Lem. 3.36]). Given $P, Q \subseteq A^\omega$, we have

$$\text{cl}(P \cup Q) = \text{cl}(P) \cup \text{cl}(Q)$$

Lemma 5.28 directly follows from Lem. 4.5 and Prop. 5.23. A direct (more combinatorial) proof is nevertheless possible.

**Remark 5.29.** As a consequence, $\text{cl} : \mathcal{P}(A^\omega) \to \mathcal{P}(A^\omega)$ is a Kuratowski closure operator (see Rem. 4.6).

The proof of Thm. 3.19 given in [BK08] then proceeds by the following. The decomposition has the same shape as in the general topological Thm. 4.11.

**Corollary 5.30** ([BK08, Thm. 3.37]). For every LT property $P \subseteq (2^{AP})^\omega$, we have

$$P = \text{cl}(P) \cap (P \cup ((2^{AP})^\omega \setminus \text{cl}(P)))$$

where $\text{cl}(P)$ is a safety property and $P \cup ((2^{AP})^\omega \setminus \text{cl}(P))$ is a liveness property.

5.6 Further Properties of Closure Operators and Galois Connections

We gather here some further properties of Galois connections and closure operators. These properties come from the fact that Galois connections and closure operators are particular cases of general notions in category theory, the notions resp. of adjunction and monad. We generally refer to [ML98] for categorical material, and give references to the corresponding statements.

We begin with the usual join and (resp. meet) preservation of lower (resp. upper adjoints).

**Lemma 5.31** ([DP02, Prop. 7.31]). If $g \dashv f : A \to B$ is a Galois connection, then $g$ preserves any join which exists in $A$ and $f$ preserves any meet which exists in $B$.

**Proof.** Exercise!

Lemma 5.31 thus implies that $g$ (resp. $f$) preserves joins (resp. meets) whenever it has a lower adjoint (resp. an upper adjoint). This is actually a particular case of a general property of adjoints in category theory (see e.g. [Awo10, §9.5] or [ML98, §V.5]), where we speak of left and right adjoints for the generalized form of resp. lower and upper adjoints. In various occasions, one is more interested in knowing the existence of an adjoint, so as to deduce preservation properties, rather than in the adjoint in itself.

Interestingly, Lem. 5.31 has a converse.

**Lemma 5.32** ([DP02, Prop. 7.34]). Assume that $(A, \leq_A)$ and $(B, \leq_B)$ are complete lattices.

1. If $f : B \to A$ preserves meets (and is thus monotone), then $f$ has a lower adjoint $g : A \to B$.
2. If $g : A \to B$ preserves joins (and is thus monotone), then $g$ has an upper adjoint $f : B \to A$.

**Proof.** Exercise!
The categorical generalization of Lem. 5.32 actually involves more complex conditions. See e.g. [ML98, §V.6] and [Awo10, §9.8].

We have seen in Lem. 5.21 that Galois connections induce closure operators. The converse, namely that every Galois connections arises from a closure operator is also true. The categorical generalization of closure operators are monads. See e.g. [ML98, Chap VI].

Given a closure operator $c : A \to A$, we already have looked at the set $A^c$ of closed elements in §5.3.

**Lemma 5.33** ([DP02, §7.28]). Let $c : A \to A$ be a closure operator. Then $c : A \to A^c$ is part of a Galois connection $c \dashv \iota : A \to A^c$, where $\iota(a) := a$.

*Proof.* Exercise!

We of course have $c = \iota \circ c$. The Galois connection of Lem. 5.33 generalizes to the well-known adjunction between a category $\mathcal{C}$ and the Eilenberg-Moore category $\mathcal{C}^T$ of a monad $T$ on $\mathcal{C}$, see e.g. [ML98, §VI.2].

### 5.6.1 On the Kleisli Construction

The notion of closure operator on a partial order of Def. 5.15 can be generalized to preorders. A preorder on a set $A$ is a binary relation which is reflexive and transitive. So the difference with a partial order is that antisymmetry is not required, i.e. we can have $a \leq b$ and $b \leq a$ with $a \neq b$. If $(A, \leq)$ is a preorder, we say that $c : A \to A$ is a closure operator if $c$ is monotone, expansive and such that $c(c(a)) \leq c(a)$ for all $a \in A$. The definition of Galois connections between preorders is the same as for partial orders (Def. 5.19), and all properties seen in §5.4 and the present §5.6 generalize to preorders.

In this setting, for a closure operator $c : A \to A$, let $\leq_c \subseteq A \times A$ be such that $a \leq_c a'$ iff $a \leq c(a')$. The following is a particular case of a second way to generate an adjunction from a monad $T$ on a category $\mathcal{C}$, namely the adjunction between $\mathcal{C}$ and its Kleisli category $\mathcal{C}^T$. We refer to e.g. [ML98, §VI.5] for details.

**Lemma 5.34.** Let $c : A \to A$ be a closure operator on a preorder. Then $c : A \to A$ is part of a Galois connection $\iota \dashv c : (A, \leq) \to (A, \leq_c)$, where $\iota(a) := a$.

*Proof.* Exercise!

### 6 Observable Properties

This Section refines the topological approach of §4, with the aim of isolating a natural notion of “observable” linear-time property. This lays the ground to logics for linear-time properties. An important point is that, when AP is finite, LT properties of the form $\text{ext}(V)$, for a finite $V \subseteq (2^{\text{AP}})^*$, form a Boolean algebra.

#### 6.1 Observable Properties as Clopen Sets

Given sets $X$ and $Y$, a function $f : X \to Y$ induces a function

$$f^{-1} : \mathcal{P}(Y) \longrightarrow \mathcal{P}(X)$$

$$B \mapsto \{x \mid f(x) \in B\}$$
Lemma 6.1. Given a function \( f : X \to Y \), the function \( f^{-1} : \mathcal{P}(Y) \to \mathcal{P}(X) \) is a map of complete Boolean algebras from \((\mathcal{P}(Y), \cap, \cup, Y \setminus (-), Y, \emptyset)\) to \((\mathcal{P}(X), \cap, \cup, X \setminus (-), X, \emptyset)\).

Note that if \( f^{-1} \) preserves unions and intersections, then it also preserves complements, as the complement of \( A \in \mathcal{P}(X) \) is the unique \( B \in \mathcal{P}(X) \) such that \( A \cup B = X \) and \( A \cap B = \emptyset \).

Proof. Exercise!

\[
\square
\]

Definition 6.2 (Continuous Function). Consider topological spaces \((X, \Omega_X)\) and \((Y, \Omega_Y)\). A function \( f : X \to Y \) is continuous if \( f^{-1} : \mathcal{P}(Y) \to \mathcal{P}(X) \) restricts to a function \( \Omega_Y \to \Omega_X \), i.e. if \( f^{-1}(V) \) is open in \( X \) whenever \( V \) is open in \( Y \).

Lemma 6.3. A function \( f : A^\omega \to B^\omega \) is continuous iff

\[
\forall n \in \mathbb{N}, \forall \alpha \in A^\omega, \exists k \in \mathbb{N}, \forall \beta \in A^\omega \big( \beta(0) \cdots \beta(k) = \alpha(0) \cdots \alpha(k) \implies f(\beta)(0) \cdots f(\beta)(n) = f(\alpha)(0) \cdots f(\alpha)(n) \big)
\]

Proof. Exercise!

In words, a continuous stream function must be able to produce a finite part of its output from a finite part of its input. It is generally admitted that a computable function on streams must be continuous. In particular, a necessary condition for an LT property \( P \subseteq (2^\mathbb{A})^\omega \) to be decidable is to have a continuous characteristic function

\[
\chi_P : (2^\mathbb{A})^\omega \to 2
\]

\[
\alpha \mapsto \begin{cases} 1 & \text{if } \alpha \in P \\ 0 & \text{otherwise} \end{cases}
\]

where 2 is endowed with the discrete topology, with which every subset is open. This amounts to ask that both \( P \) and \((2^\mathbb{A})^\omega \setminus P\) are open, or equivalently that \( P \) is both open and closed.

Definition 6.4 (Clopen Set). A subset of a topological space is clopen if it is both open and closed.

Lemma 6.5 (The Boolean Algebra of Clopens). Let \((X, \Omega_X)\) be a topological space. The clopens of \( X \) form a sub-Boolean algebra of \((\mathcal{P}(X), (-) \cap (-), (-) \cup (-), X \setminus (-), X, \emptyset)\).

Proof. First, clopens are evidently closed under complements. Furthermore, both \( \emptyset \) and \( X \) are clopens. Finally, the open subsets and the closed subsets of \( X \) are closed under binary intersections and binary unions.

\[
\square
\]

Definition 6.6 (Observable Property). An LT property \( P \subseteq (2^\mathbb{A})^\omega \) is observable if \( P \) is a clopen subset of \((2^\mathbb{A})^\omega \).

Let us look more precisely at the observable properties.

Lemma 6.7. In \( A^\omega \), each set of the form \( \text{ext}(u) \) for \( u \in A^* \) is clopen.

Proof. We reason by induction on \( u \). If \( u = \varepsilon \) then \( \text{ext}(u) = A^\omega \) is evidently clopen. Otherwise, \( u = v.a \) and

\[
A^\omega \setminus \text{ext}(v.a) = \bigcup_{b \neq a} \text{ext}(v.b) \cup (A^\omega \setminus \text{ext}(v))
\]

Since \( \text{ext}(v) \) is clopen by induction hypothesis and since each \( \text{ext}(v.b) \) is open, we get that \((2^\mathbb{A})^\omega \setminus \text{ext}(v.a) \) is open, so that \( \text{ext}(v.a) \) is clopen.

\[
\square
\]
As a consequence, each finite subset $U \subseteq A^*$ induces a clopen set $\text{ext}(U) = \bigcup_{u \in U} \text{ext}(u)$. However, the converse is not true in general.

**Example 6.8.** Consider the Baire space $N := \mathbb{N}^\omega$. The subset $P \subseteq \mathbb{N}^\omega$ given by

$$P := \bigcup_{n>0} \text{ext}(n)$$

is obviously open. It is also closed as being the complement of $\text{ext}(0)$. But $P$ cannot be presented as the extension of a finite set $U \subseteq \mathbb{N}^*$. We shall see in Prop. 6.19 that when AP is finite, the observable $P \subseteq (2^{AP})^\omega$ are exactly the sets of the form $\bigcup_{u \in U} \text{ext}(u)$ for a finite $U \subseteq (2^{AP})^\omega$. This relies on a strong topological properties of $(2^{AP})^\omega$ for finite AP, known as compactness, and whose most basic aspects are presented in §6.2 and §6.3.

### 6.2 Compactness

We follow here parts of the presentation of [Run05].

**Definition 6.9.** Let $(X, \Omega_X)$ be a topological space.

- An **open cover** of a set $A \subseteq X$ is a family of open sets $(U_i)_{i \in I}$ such that $A \subseteq \bigcup_{i \in I} U_i$.
- A set $A \subseteq X$ is **compact** in $X$ if every open cover $(U_i)_{i \in I}$ of $A$, i.e. there is a finite set $J \subseteq I$ such that $A \subseteq \bigcup_{j \in J} U_j$.
- The space $(X, \Omega_X)$ is **compact** if $X$ is itself a compact subset of $X$.

The following is a simple consequence of the definitions. In the case of compact Hausdorff spaces (§6.3) it becomes part of a powerful characterization of the compact sets (see Prop. 6.18).

**Lemma 6.10.** A closed subset of a compact space is compact.

**Proof.** Let $(X, \Omega_X)$ be a compact space and let $C \subseteq X$ be closed. Given an open covering $U = (U_i)_{i \in I}$ of $C$, we obtain with $U \cup \{X \setminus C\}$ an open covering of $X$. Since $X$ is compact, it has a finite subcover $V \cup \{X \setminus C\}$ where $V = (U_j)_{j \in J}$ for some finite $J \subseteq I$. But then $V$ covers $C$. \qed

In the case of $\omega$-words, the space $A^\omega$ is compact if and only if $A$ is finite. First, it is easy to see that $A^\omega$ is not be compact when $A$ is infinite.

**Lemma 6.11.** Consider the space of $\omega$-words $A^\omega$ for some non-empty set $A$. If $A$ is infinite, then $A^\omega$ is not compact.

**Proof.** Indeed, we have

$$A^\omega = \bigcup_{a \in A} \text{ext}(a)$$

But if $A$ is infinite, one cannot extract a finite subcover of $A^\omega$ from $(\text{ext}(a))_{a \in A}$. \qed

We now show that $A^\omega$ is compact when $A$ is finite. We rely on König’s Lemma 3.16 (§3.2.5).

**Proposition 6.12.** Let $A$ be a finite non-empty set. Then $A^\omega$ is compact.

**Proof.** Consider an open covering $(U_i)_{i \in I}$ of $A^\omega$. Note that each $U_i$ is of the form $\bigcup_{v \in V_i} \text{ext}(v)$ for some $V_i \subseteq A^*$. Let $V := \bigcup_{i \in I} V_i$. We build a prefix-free $W \subseteq V$ as $W = \bigcup_{n \in \mathbb{N}} W_n$, where
• \( \varepsilon \in W_0 \) iff \( \varepsilon \in V \).

• Given \( u \in A^* \) of length \( n + 1 \), we let \( u \in W_{n+1} \) if \( u \in V \) and \( u \) has no prefix in \( \bigcup_{k \leq n} W_k \).

It is clear that \( W \) is prefix-free, in the sense that if \( u \in W \) then \( u \) has no strict prefix in \( W \). Moreover, each \( v \in V \) has a prefix in \( W \). Hence, recalling that \( w \subseteq v \) implies \( \text{ext}(v) \subseteq \text{ext}(w) \) (Lem. 4.16), \( W \) induces a cover of \( A^\omega \) as

\[
A^\omega = \bigcup_{v \in V} \text{ext}(v) = \bigcup_{w \in W} \text{ext}(w)
\]

Hence we are done if \( W \) is finite. Assume toward a contradiction that \( W \) is infinite. Let \( T \subseteq A^* \) be the prefix-closure of \( W \) (i.e. \( u \in T \) iff \( u \subseteq w \) for some \( w \in W \)). Then \( T \) is finitely branching as \( A \) is finite, and \( T \) is infinite as \( W \) is infinite. Hence, by König’s Lemma 3.16, \( T \) has a path \( \pi \). Since \( W \) induces a cover of \( A^\omega \), we have \( w \subseteq \pi \) for some \( w \in W \). Since \( \pi \) is a path in \( T \), we have \( w.a \subseteq \pi \) for some \( w.a \in T \) with \( a \in A \). By definition of \( T \), we must have \( w.a \subseteq v \) for some \( v \in W \), but this is impossible since \( v \in W \) would then have a strict prefix \( w \in W \).

**Remark 6.13** (Tychonoff Theorem – Compactness of Product Spaces). The conjunction of Lem. 6.11 with Prop. 6.12 is an instance of Tychonoff Theorem. We refer to [Wil70, Thm. 17.8] and to [Run05, Thm. 3.3.21]. It is an easy exercise to show that “our” topology on \( A^\omega \) is the product topology in the usual sense (taking \( A \) discrete), see e.g. [Wil70, Chap. 3, §8] or [Run05, Def. 3.3.19]. Tychonoff Theorem is known to be equivalent to the Axiom of Choice.

**6.2.1 The Finite Intersection Property**

The following characterization of compact spaces is useful in practice. It directly follows from the definitions.

**Definition 6.14** (Finite Intersection Property). Given a set \( A \), a family of sets \( \mathcal{F} \subseteq \mathcal{P}(A) \) has the finite intersection property for every finite \( F \subseteq \mathcal{F} \), we have \( \bigcap F \neq \emptyset \).

**Lemma 6.15.** A space \((X, \Omega_X)\) is compact iff for every family of closed sets \( \mathcal{F} \) with the finite intersection property, we have \( \bigcap \mathcal{F} \neq \emptyset \).

**Proof.** Exercise! \( \square \)

**6.3 Compact Hausdorff Spaces**

Compact spaces with the following separation property enjoy a particularly simple characterization of their compact subsets. See e.g. [Wil70, Chap. 5, §13] or [Run05, Def. 3.13].

**Definition 6.16** (Hausdorff Space). A topological space \((X, \Omega_X)\) is Hausdorff (or \( T_2 \)) if for any distinct points \( x, y \in X \), there are disjoint opens \( U, V \) such that \( x \in U \) and \( y \in V \).

**Example 6.17.** Spaces of \( \omega \)-words \( A^\omega \) are Hausdorff.

Here comes the announced characterization of the compacts subsets of a compact Hausdorff space. Recall from Lem. 6.10 that the closed subsets of a compact spaces are always compact.

**Proposition 6.18.** In an Hausdorff space, each compact set is closed.
Proof. Consider an Hausdorff space \((X, \Omega X)\) and fix a compact set \(C \subseteq X\). We show that \(C\) is closed using Lem. 4.3. So let \(x \notin C\). Since \(X\) is Hausdorff, for each \(y \in C\) there are disjoint open sets \(U_y, V_y\) such that \(x \in U_y\) and \(y \in V_y\). Hence \((V_y)_{y \in C}\) is an open cover of \(C\). Since \(C\) is compact, \((V_y)_{y \in C}\) has a finite subcover, say \(V_{y_1}, \ldots, V_{y_n}\). But then \(x\) belongs to the open set \(U := U_{y_1} \cap \cdots \cap U_{y_n}\). Moreover, since each \(U_{y_i}\) is disjoint from \(V_{y_i}\), it follows that \(U\) is disjoint from each \(V_{y_i}\) and thus from \(C \subseteq V_{y_1} \cup \cdots \cup V_{y_n}\). \(\square\)

As a consequence, in a compact Hausdorff space, the compact sets are exactly the closed sets, and the clopen sets are exactly the compact open sets.

**Proposition 6.19** (Observable Property – The Compact Case). If \(AP\) is finite, then \(P \subseteq (2^{AP})^\omega\) is observable iff \(P = \bigcup_{u \in U} \text{ext}(u)\) for some finite \(U \subseteq (2^{AP})^\ast\).

**Proof.** We already know from Lem. 6.7 and Lem. 6.5 that the condition is sufficient. Let \(P \subseteq (2^{AP})^\omega\) be clopen, hence compact open. Then \(P = \bigcup_{u \in U} \text{ext}(u)\) for some \(U \subseteq (2^{AP})^\ast\). Since \(P\) is compact, there is a finite subset \(V \subseteq U\) such that \(P \subseteq \bigcup_{u \in V} \text{ext}(u)\). But this implies \(P = \bigcup_{u \in V} \text{ext}(u)\) as \(V \subseteq U\). \(\square\)

### 7 Linear Temporal Logic

Linear Temporal Logic (LTL) is a modal logic to express linear-time properties. In the field of computer science, temporal logics for linear-times properties were introduced by [Pnu77]. We refer to [BdRV02] for a comprehensive introduction to modal logic.

This Section presents LTL in a step-wise manner, starting from the notion of observable property drawn in §6. We mostly build from [BK08, Chap. 5], but differ in various aspects. In particular, we discuss standard material on the computation of fixpoints in complete lattices which goes beyond [BK08] and for which we mainly refer to [DP02].

#### 7.1 The Logic LML of Observable Properties

Fix a set \(AP\) of atomic propositions. We are going to define a linear-time modal logic \(LML\) such that, when \(AP\) is finite, the formulae of \(LML\) describe exactly the clopens of \((2^{AP})^\omega\).

**7.1.1 Syntax and Semantics of LML**

We assume given a countably infinite set \(\mathcal{X} = \{X, Y, Z, \ldots\}\) of variables. The formulae of \(LML\) are given by the following grammar:

\[
\varphi, \psi ::= \top \mid \bot \mid X \mid a \quad \text{(where } X \in \mathcal{X} \text{ and } a \in AP) \\
\quad \mid \varphi \land \psi \mid \varphi \lor \psi \mid \neg \varphi \\
\quad \mid \diamond \varphi
\]

The formulae of \(LML\) are to be interpreted as subsets of \((2^{AP})^\omega\). In particular, the interpretation of a formula \(\varphi\) with variables among \(X_1, \ldots, X_n\) depends on a valuation of the \(X_i\)'s as sets \(A_i \subseteq (2^{AP})^\omega\).

**Definition 7.1** (Valuations and Formulae with Parameters).

(1) A valuation of a set of variables \(V \subseteq \mathcal{X}\) is a function \(\rho: V \to \mathcal{P}((2^{AP})^\omega)\).
A formula with parameters is a pair $(\varphi, \rho)$ of a formula $\varphi$ and a valuation $\rho : V \to \mathcal{P}((2\text{AP})^\omega)$ where $V$ contains all the variables of $\varphi$.

We often speak of a formula $\varphi$ with parameters $\rho$ for the pair $(\varphi, \rho)$.

Consider a formula $\varphi$ with parameters $\rho$. We define the interpretation $\llbracket \varphi \rrbracket_\rho \subseteq (2\text{AP})^\omega$ by induction on $\varphi$ as follows:

\[
\begin{align*}
\llbracket X \rrbracket_\rho & := \rho(X) \\
\llbracket a \rrbracket_\rho & := \{ \sigma \in (2\text{AP})^\omega \mid a \in \sigma(0) \} \\
\llbracket \top \rrbracket_\rho & := (2\text{AP})^\omega \\
\llbracket \bot \rrbracket_\rho & := \emptyset \\
\llbracket \varphi \land \psi \rrbracket_\rho & := \llbracket \varphi \rrbracket_\rho \cap \llbracket \psi \rrbracket_\rho \\
\llbracket \varphi \lor \psi \rrbracket_\rho & := \llbracket \varphi \rrbracket_\rho \cup \llbracket \psi \rrbracket_\rho \\
\llbracket \neg \varphi \rrbracket_\rho & := (2\text{AP})^\omega \setminus \llbracket \varphi \rrbracket_\rho \\
\llbracket \circ \varphi \rrbracket_\rho & := \{ \sigma \in (2\text{AP})^\omega \mid \sigma|1 \in \llbracket \varphi \rrbracket_\rho \}
\end{align*}
\]

where, for $i \in \mathbb{N}$, $\sigma|1 \in (2\text{AP})^\omega$ is the function which takes $k \in \mathbb{N}$ to $\sigma(i+k) \in 2\text{AP}$, e.g.

\[
\sigma = \sigma(0) \cdot \sigma(1) \cdot \ldots \cdot \sigma(n) \cdot \ldots
\]

\[
\sigma|1 = \sigma(1) \cdot \sigma(2) \cdot \ldots \cdot \sigma(n+1) \cdot \ldots
\]

Notation 7.2. Other propositional connectives are defined as usual:

\[
\begin{align*}
\varphi \rightarrow \psi & := \neg \varphi \lor \psi \\
\varphi \leftrightarrow \psi & := (\varphi \rightarrow \psi) \land (\psi \rightarrow \varphi)
\end{align*}
\]

Definition 7.3. We say that $\sigma \in (2\text{AP})^\omega$ satisfies a formula $\varphi$ with parameters $\rho$ if $\sigma \in \llbracket \varphi \rrbracket_\rho$.

Lemma 7.4. If $\rho = \rho'$ for all variables which actually occur in $\varphi$, then $\llbracket \varphi \rrbracket_\rho = \llbracket \varphi \rrbracket_{\rho'}$.

In particular, if $\varphi$ is closed, i.e., contains no free variable, then $\llbracket \varphi \rrbracket_\rho$ does not depend on $\rho$. In this case, we just write $\llbracket \varphi \rrbracket$ for $\llbracket \varphi \rrbracket_\rho$.

Notation 7.5. For a closed $\varphi$, we write $\sigma \vdash \varphi$ for $\sigma \in \llbracket \varphi \rrbracket$.

The relation $\sigma \vdash \varphi$ (for $\varphi$ closed) can be given an inductive definition.

Remark 7.6. The relation $\sigma \vdash \varphi$ is the least relation such that

\[
\begin{align*}
\sigma \vdash a & \iff a \in \sigma(0) \\
\sigma \vdash \top & \\
\sigma \not\vdash \bot & \\
\sigma \vdash \varphi \land \psi & \iff \sigma \vdash \varphi \text{ and } \sigma \vdash \psi \\
\sigma \vdash \varphi \lor \psi & \iff \sigma \vdash \varphi \text{ or } \sigma \vdash \psi \\
\sigma \vdash \neg \varphi & \iff \sigma \not\vdash \varphi \\
\sigma \vdash \circ \varphi & \iff \sigma|1 \vdash \varphi
\end{align*}
\]

7.1.2 Logical Equivalence

Definition 7.7 (Logical Equivalence). Given formulae $\varphi$ and $\psi$ with free variables in $V \subseteq X$, we say that $\varphi$ and $\psi$ are logically equivalent (notation $\varphi \equiv \psi$) if for all valuation $\rho : V \to \mathcal{P}((2\text{AP})^\omega)$ we have

\[
\llbracket \varphi \rrbracket_\rho = \llbracket \psi \rrbracket_\rho
\]
Semilattices Laws:

\[
\begin{align*}
\varphi \lor \varphi & \equiv \varphi \\
\varphi \lor \psi & \equiv \psi \lor \varphi \\
\varphi \lor \bot & \equiv \varphi \\
\varphi \lor (\psi \lor \theta) & \equiv (\varphi \lor \psi) \lor \theta \\
\end{align*}
\]

\[
\begin{align*}
\varphi \land \varphi & \equiv \varphi \\
\varphi \land \psi & \equiv \psi \land \varphi \\
\varphi \land \top & \equiv \varphi \\
\varphi \land (\psi \land \theta) & \equiv (\varphi \land \psi) \land \theta
\end{align*}
\]

Absorptive Laws (Lattice Laws):

\[
\begin{align*}
\varphi \lor (\varphi \land \psi) & \equiv \varphi \\
\varphi \land (\varphi \lor \psi) & \equiv \varphi
\end{align*}
\]

Distributive Laws:

\[
\begin{align*}
\varphi \lor (\psi \land \theta) & \equiv (\varphi \lor \psi) \land \varphi \\
\varphi \land (\psi \lor \theta) & \equiv (\varphi \land \psi) \lor \varphi
\end{align*}
\]

Boolean Algebra Laws:

\[
\begin{align*}
\varphi \land \neg \varphi & \equiv \bot \\
\varphi \lor \neg \varphi & \equiv \top
\end{align*}
\]

Duality (De Morgan) Laws:

\[
\begin{align*}
\varphi \land \psi & \equiv \neg (\neg \varphi \lor \neg \psi) \\
\varphi \lor \psi & \equiv \neg (\neg \varphi \land \neg \psi) \\
\varphi & \equiv \neg \neg \varphi
\end{align*}
\]

Modal Laws:

\[
\begin{align*}
\Box (\varphi \land \psi) & \equiv \Box \varphi \land \Box \psi \\
\Box (\varphi \lor \psi) & \equiv \Box \varphi \lor \Box \psi \\
\Box \top & \equiv \top \\
\Box \bot & \equiv \bot \\
\Box (\neg \varphi) & \equiv \neg \Box \varphi
\end{align*}
\]

Figure 1: Some Usual Laws.

Lemma 7.8. All the equivalences of Fig. 1 hold.

Remark 7.9. The notion of logical equivalence \(\equiv\) given in Def. 7.7, for which we follow [BK08, Def. 5.17], is not the usual one (see e.g. [BdRV02, Def. 5.29]). In Def. 7.7 as well as in [BK08, Def. 5.17], logical equivalence is defined as a semantic equivalence, whereas [BdRV02, Def. 5.29] defines \(\equiv\) as provable equivalence in a given axiomatic system.

While the “right” notion of logical equivalence is that of [BdRV02, Def. 5.29] (see also e.g. [DP02, §11.11–16]), we stick to the semantic notion of [BK08, Def. 5.17] since the present notes do not cover axiomatic and deductive approaches to logic.

7.1.3 Observable Properties

We now turn to the promised fact that when \(AP\) is finite, the closed formulae of \(LML\) exactly correspond to the observable (i.e. clopen) properties on \((2^{AP})^\omega\). Recall from Prop. 6.19 that when \(AP\) is finite, the clopen subsets of \((2^{AP})^\omega\) are exactly the finite unions of sets of the form \(\text{ext}(\hat{\sigma})\) for \(\hat{\sigma} \in (2^{AP})^*\). Recall moreover from Lem. 6.5 that clopen sets are closed under complements, finite unions and finite intersections.

Proposition 7.10. For each closed \(LML\)-formula \(\varphi\), \(\llbracket \varphi \rrbracket\) is a clopen subset of \((2^{AP})^\omega\).
We thus have for all \( \beta \):

\[
[\beta] = \bigcup \{ \text{ext}(A) \mid A \in 2^{\text{AP}} \text{ and } \beta \in A \}
\]

and we are done by Lem. 6.7 and Lem. 6.5 if AP is finite.

Assume now that AP is infinite. If \( \sigma \notin [\beta] \), we have \( \sigma \notin \sigma(0) \). But then \( \text{ext}(\sigma(0)) \) is an open set containing \( \sigma \) and disjoint from \([\beta]\). Hence \([\beta]\) is closed and thus clopen.

Cases of \( T, \bot, \varphi \land \psi \) and \( \varphi \lor \psi \). By Lem. 6.5.

Case of \( \bigcirc \varphi \). By induction hypothesis, \([\varphi]\) is clopen and thus open. Hence \([\varphi] = \text{ext}(U)\) for some set \( U \subseteq (2^{\text{AP}})^{\ast} \). Then we have

\[
[\bigcirc \varphi] = \bigcup \{ \text{ext}(A.u) \mid u \in U \text{ and } A \in 2^{\text{AP}} \}
\]

If AP is finite, then by Prop. 6.19 we can further assume that \( U \) is finite, and we are done by Lem. 6.7 and Lem. 6.5 since \( 2^{\text{AP}} \) is also finite.

Assume now that AP is infinite. If \( \sigma \notin [\bigcirc \varphi] \), then we have \( \sigma[1] \notin [\varphi] \). Hence by induction hypothesis there is some \( w \in (2^{\text{AP}})^{\ast} \) such that \( \sigma[1] \in \text{ext}(w) \) and \( \text{ext}(w) \cap [\varphi] = \emptyset \). But then it follows that \( \text{ext}(\sigma(0).w) \cap [\bigcirc \varphi] = \emptyset \) while \( \sigma \in \text{ext}(\sigma(0).w) \). Hence \([\bigcirc \varphi]\) is closed and we are done. \( \square \)

**Proposition 7.11.** Assume that AP is finite. Then for any clopen \( P \subseteq (2^{\text{AP}})^{\omega} \) there is a closed LML-formula \( \varphi \) such that \( P = [\varphi] \).

**Proof.** We know from Prop. 6.19 that \( P = \text{ext}(U) \) for some finite \( U \subseteq (2^{\text{AP}})^{\ast} \). We show that \( \text{ext}(u) \) is definable in LML for each \( u \in U \) and then conclude by Lem. 6.5. First note that since AP is finite, for each set \( A \in 2^{\text{AP}} \), we have \( \text{ext}(A) = [\varphi_A] \) where

\[
\varphi_A := \left( \bigwedge_{a \in A} a \right) \land \left( \bigwedge_{a \in \text{AP}\setminus A} \neg a \right)
\]

Consider some finite word \( u = A_n \cdots A_1 \in (2^{\text{AP}})^{\ast} \). We show by induction on \( n \in \mathbb{N} \) that \( \text{ext}(u) \) is definable in LML. The base case follows from the fact that \( \text{ext}(\varepsilon) = [\top] \). As for the induction step, assume that \( u \) is definable by \( \psi_u \). Then \( A.u \) is definable by \( \varphi_A \land \bigcirc \psi_u \). \( \square \)

Proposition 7.11 does not hold when AP is infinite.

**Example 7.12.** Let AP := \( \mathbb{N} \) and let \( 2\mathbb{N} \subseteq \text{AP} \) consist of the even numbers. Note that \( \sigma \in \text{ext}(2\mathbb{N}) \) iff \( \sigma(0) = 2\mathbb{N} \) and that \( \text{ext}(2\mathbb{N}) \) is clopen by Lem. 6.7. It is easy to see that there is no closed formula \( \varphi \) such that \( \text{ext}(2\mathbb{N}) = [\varphi] \).

**Proof.** Assume toward a contradiction that such a \( \varphi \) exists. Using the laws of Fig. 1, we have

\[
\varphi := \bigvee_{i \in I} \bigwedge_{j \in J_i} \bigcirc n_{i,j} \lambda_{i,j}
\]

where \( I \) and the \( J_i \)’s are finite sets and each \( \lambda_{i,j} \) is either of the form \( n \) or \( \neg n \) with \( n \in \mathbb{N} \). Note that we can always assume \( n_{i,j} = 0 \) (i.e. \( \bigcirc n_{i,j} \lambda_{i,j} = \lambda_{i,j} \)) since \( \sigma \in \text{ext}(2\mathbb{N}) \) iff \( (\sigma(0) \cdot \beta) \in \text{ext}(2\mathbb{N}) \) for all \( \beta \in (2^{\text{AP}})^{\omega} \).

Let \( \sigma \models \varphi \), with say \( \sigma \models \bigwedge_{j \in J_i} \lambda_{i,j} \). Let \( n \) be the least odd number not occurring in \( \bigwedge_{j \in J_i} \lambda_{i,j} \). We thus have \( \beta := (\sigma(0) \cup \{ n \}) \cdot \sigma[1] \models \varphi \), a contradiction since \( \beta \notin \text{ext}(2\mathbb{N}) \) as \( n \) is odd. \( \square \)
7.2 Extending LML with Fixpoints

As seen in Prop. 7.10, the logic LML has a very limited expressive power. In particular, it can only express few safety properties, and it follows from Prop. 3.18 that the only expressible liveness property is the “true property” \((2^{\text{AP}})^\omega\). We shall therefore look for extensions of LML.

7.2.1 The “Eventually” and “Always” Modalities

Typical logical constructs one may wish to add to LML are the **Eventually** and **Always** modalities, noted resp. \(\Diamond \varphi\) and \(\Box \varphi\), and with

\[
\begin{align*}
[\Diamond \varphi]_{\rho} & := \{ \sigma \in (2^{\text{AP}})^\omega | \exists i \in \mathbb{N}, \sigma|i \models \varphi \}_{\rho} \\
[\Box \varphi]_{\rho} & := \{ \sigma \in (2^{\text{AP}})^\omega | \forall i \in \mathbb{N}, \sigma|i \models \varphi \}_{\rho}
\end{align*}
\]

In the spirit of Notation 7.5, for a closed \(\varphi\) we write

\[
\sigma \models \Diamond \varphi \iff \exists i \in \mathbb{N}, \sigma|i \models \varphi
\]

\[
\sigma \models \Box \varphi \iff \forall i \in \mathbb{N}, \sigma|i \models \varphi
\]

**Example 7.13.** Let \(a \in \text{AP}\).

1. \(\sigma \models \Diamond a\) iff \(a \in \sigma(i)\) for some \(i \in \mathbb{N}\).
   
   The formula \(\Diamond a\) defines an open liveness property \([\Diamond a] \subseteq (2^{\text{AP}})^\omega\).

2. \(\sigma \models \Box a\) iff \(a \in \sigma(i)\) for all \(i \in \mathbb{N}\).
   
   The formula \(\Box a\) defines a safety property \([\Box a] \subseteq (2^{\text{AP}})^\omega\).

3. \(\sigma \models \Diamond \Diamond a\) iff \(a \in \sigma(i)\) for infinitely many \(i \in \mathbb{N}\).

4. \(\sigma \models \Box \Box a\) iff \(a \notin \sigma(i)\) for at most finitely many \(i \in \mathbb{N}\), or equivalently iff there is some \(n \in \mathbb{N}\) such that \(a \in \sigma(i)\) for all \(i \geq n\).

Note that \(\Diamond \Box \varphi \rightarrow \Box \Diamond \varphi\) is always true. The formulae \(\Diamond a\) and \(\Box \Diamond a\) define liveness properties \([\Diamond a], [\Box a] \subseteq (2^{\text{AP}})^\omega\) which are not closed nor open.

Let us investigate the semantics of \(\Diamond \varphi\) and \(\Box \varphi\), with the aim of looking for behaviour which could be easily generalized. First note the following basic equivalences, where \(\equiv\) stands for the obvious extension of Def. 7.7.

**Lemma 7.14.** We have

\[
\begin{align*}
\Diamond \varphi & \equiv \neg \Box \neg \varphi \\
\Box \varphi & \equiv \neg \Diamond \neg \varphi \\
\Diamond \Diamond \varphi & \equiv \varphi \lor \Diamond \Diamond \varphi \\
\Box \Box \varphi & \equiv \varphi \land \Box \Box \varphi
\end{align*}
\]

Intuitively, the first two equivalences of Lem. 7.14 say that \(\Diamond\) and \(\Box\) can be seen as De Morgan duals of each other. The last two could be rephrased as follows.

- \(\Diamond \varphi\) holds at the current time step iff **either** \(\varphi\) holds at the current time step **or** \(\Diamond \varphi\) holds at the next time step.

- \(\Box \varphi\) holds at the current time step iff \(\varphi\) holds at the current time step **and** \(\Box \varphi\) holds at the next time step.
If we allowed for formulae with infinite disjunctions and conjunctions, we could state

$$\Diamond \varphi \equiv \varphi \lor \bigcirc \varphi \lor \bigcirc \bigcirc \varphi \lor \cdots \equiv \bigvee_{n \in \mathbb{N}} \bigwedge_{n \in \mathbb{N}}^n \varphi$$

$$\Box \varphi \equiv \varphi \land \bigcirc \varphi \land \bigcirc \bigcirc \varphi \land \cdots \equiv \bigwedge_{n \in \mathbb{N}} \bigvee_{n \in \mathbb{N}}^n \varphi$$

We shall rather look for finitary representations of such infinite behaviors, with extensions of LML with fixpoints of functions $P((2^{AP})^\omega) \to P((2^{AP})^\omega)$ induced by formulae as follows.

**Notation 7.15.** Given a formula $\varphi$ with parameters $\rho$ and a variable $X$, we write $[\varphi]_\rho(X)$ for the function

$$[\varphi]_\rho(X) : P((2^{AP})^\omega) \to P((2^{AP})^\omega)$$

Lemma 7.16. Let $\varphi$ be a formula with parameters $\rho$. Consider the formulae

$$\varphi_\Diamond(X) := \varphi \lor \bigcirc X \quad \varphi_\Box(X) := \varphi \land \bigcirc X$$

Then we have:

1. $[\varphi_\Diamond]_\rho$ is the least element of $(P((2^{AP})^\omega), \subseteq)$ such that

$$[\varphi_\Diamond]_\rho = [\varphi]_\rho([\varphi_\Diamond]_\rho)$$

2. $[\varphi_\Box]_\rho$ is the greatest element of $(P((2^{AP})^\omega), \subseteq)$ such that

$$[\varphi_\Box]_\rho = [\varphi]_\rho([\varphi_\Box]_\rho)$$

Proof. Both equations are clear from Lem. 7.14.

(1) Consider some $P \subseteq (2^{AP})^\omega$ such that $P = [\varphi_\Diamond](P)$. We show that $[\varphi_\Diamond] \subseteq P$. Note that for all $k \in \mathbb{N}$ we have $\sigma \upharpoonright k \in [\varphi_\Diamond](P) = P$ whenever $\sigma \upharpoonright k+1 \in P$.

Assume that $\sigma \not\vdash \Diamond \varphi$ and let $i \in \mathbb{N}$ such that $\sigma \upharpoonright i \not\models \varphi$. We thus have $\sigma \upharpoonright i \in [\varphi_\Diamond](P) = P$. By (reverse) induction, we obtain $\sigma \upharpoonright k \in [\varphi_\Diamond](P) = P$ for all $k \leq i$, and so in particular $\sigma \in P$.

(2) Consider some $P \subseteq (2^{AP})^\omega$ such that $P = [\varphi_\Box](P)$. We show that $P \subseteq [\varphi_\Box]$. Note that for all $k \in \mathbb{N}$, if $\sigma \upharpoonright k \in P = [\varphi_\Box](P)$, then we have $\sigma \upharpoonright k \in [\varphi]$ and $\sigma \upharpoonright k+1 \in P$. Hence, given $\sigma \in P$, it follows by induction that $\sigma \upharpoonright i \in [\varphi]$ and $\sigma \upharpoonright i+1 \in P$ for all $i \in \mathbb{N}$, and so in particular $\sigma \in [\varphi_\Box]$.

7.2.2 Positive and Negative Variables in a Formula

We note here the simple fact that if the variable $X$ occurs under an even (resp. odd) number of negations in $\varphi$, then $[\varphi]_\rho(X)$ is a monotone (resp. antimonotone) function of $(P((2^{AP})^\omega), \subseteq)$.

We use the following inductive notions of positive (resp. negative) variable in a formula $\varphi$ in order to express that a variable occurs under an even (resp. odd) number of negations in $\varphi$.

**Definition 7.17** (Positive Negative Variables). Given an LML-formula $\varphi$ and a variable $X$, the relations $X$ Pos $\varphi$ ($X$ is positive in $\varphi$) and $X$ Neg $\varphi$ ($X$ is negative in $\varphi$) are defined by induction on Fig. 2.

Lemma 7.18. Consider a formula $\varphi$ with parameters $\rho$ and a variable $X$.

1. If $X$ Pos $\varphi$, then $[\varphi](X)$ is a monotone function on $(P((2^{AP})^\omega), \subseteq)$.

2. If $X$ Neg $\varphi$, then $[\varphi](X)$ is an antimonotone function on $(P((2^{AP})^\omega), \subseteq)$. 

26
7.2.3 The Knaster-Tarski Fixpoint Theorem

Definition 7.19 (Fixpoints ([DP02, Def. 8.14])).

(1) A fixpoint of a function $f : X \to X$ is an $x \in X$ such that $f(x) = x$.

(2) Let $L$ be a partial order and let $f : L \to L$ be monotone. We say that $a \in L$ is a pre-fixpoint of $f$ if $f(a) \leq a$, and that $a \in L$ is a post-fixpoint of $f$ if $a \leq f(a)$.

A monotone function $f : L \to L$ on a complete lattice has always a least fixpoint $\mu(f) \in L$ and a greatest fixpoint $\nu(f) \in L$. Intuitively, the least fixpoint $\mu(f)$ can always be obtained as the least pre-fixpoint of $f$. Dually, the greatest fixpoint of $\nu(f)$ can always be obtained as the greatest post-fixpoint of $f$.

Theorem 7.20 (Knaster-Tarski Fixpoint Theorem ([DP02, Thm. 2.35])). Let $L$ be a complete lattice and let $f : L \to L$ be a monotone. Then the least fixpoint $\mu(f)$ and the greatest fixpoint $\nu(f)$ are given resp. by

$$
\mu(f) = \bigwedge \{ a \in L \mid f(a) \leq a \}
$$

$$
\nu(f) = \bigvee \{ a \in L \mid a \leq f(a) \}
$$

Proof. Exercise! \qed

Remark 7.21 (On the Modal $\mu$-Calculus). The full extension of LML with fixpoints is the (linear-time) modal $\mu$-calculus, a powerful logic, due to [Koz83], whose study would lead us too far for this course. We refer to e.g. [VW08, §6] and [GTW02, BW18] and references therein for more material on the modal $\mu$-calculus. At the semantic level, we refer to [DP02, §8.27–31] for reasoning principles with least and greatest fixpoints.

We finally note the following duality between least and greatest fixpoints.

Lemma 7.22. Let $\phi$ be a formula with parameters $\rho$ and assume that $X \text{ Pos } \phi$. Let $\psi(X) := \neg \phi(\neg X)$. Then

$$
\nu([\phi]_\rho(X)) = (2^{\text{AP}})^\omega \setminus \mu([\psi]_\rho(X))
$$

$$
\mu([\phi]_\rho(X)) = (2^{\text{AP}})^\omega \setminus \nu([\psi]_\rho(X))
$$

Figure 2: Positive and Negative Occurrences in a Formula.
Proof. We rely on the Knaster-Tarski Fixpoint Theorem 7.20. We have
\[
(2\text{AP})^\omega \setminus \mu([\psi]) = (2\text{AP})^\omega \setminus \bigcap \{A \subseteq (2\text{AP})^\omega \mid [\psi](A) \subseteq A\}
\]
\[
= \bigcup \{(2\text{AP})^\omega \setminus A \mid [\psi](A) \subseteq A\}
\]
\[
= \bigcup \{(2\text{AP})^\omega \setminus A \mid (2\text{AP})^\omega \setminus [\varphi](2\text{AP})^\omega \setminus A\} \subseteq A\}
\]
\[
= \bigcup \{B \subseteq (2\text{AP})^\omega \mid B \subseteq [\varphi](B)\}
\]
Dually,
\[
(2\text{AP})^\omega \setminus \nu([\psi]) = (2\text{AP})^\omega \setminus \bigcap \{A \subseteq (2\text{AP})^\omega \mid A \subseteq [\psi](A)\}
\]
\[
= \bigcup \{(2\text{AP})^\omega \setminus A \mid A \subseteq [\psi](A)\}
\]
\[
= \bigcup \{(2\text{AP})^\omega \setminus A \mid A \subseteq (2\text{AP})^\omega \setminus [\varphi](2\text{AP})^\omega \setminus A\} \subseteq A\}
\]
\[
= \bigcup \{B \subseteq (2\text{AP})^\omega \mid [\varphi](B) \subseteq B\}
\]
\[
= \nu([\varphi])
\]
\qed

7.3 The Logic LTL

The logic LTL is the extension of LML with a limited form of fixpoints, which can be presented as follows. Consider a formula \(\theta(X)\) with \(X\) Pos \(\theta\). Then using the laws of Fig. 1, we can put \(\theta(X)\) in disjunctive normal form, and obtain
\[
\theta(X) \equiv \psi \lor \bigvee_{i \in I} (\varphi_i \land \bigwedge_{j \in J} \circ^{n_{i,j}} X)
\]
where \(X\) does not occur in \(\psi\) nor in the \(\varphi_i\)’s. If we further assume that in \(\theta\), \(X\) occurs under exactly one \(\circ\), then we have
\[
\theta(X) \equiv \psi \lor \bigvee_{i \in I} (\varphi_i \land \circ X)
\]
\[
\equiv \psi \lor (\varphi \land \circ X)
\]
where \(X\) does not occur in \(\psi\) nor in \(\varphi\).

The logic LTL is the extension of LML with least (and greatest by the duality of Lem. 7.22) fixpoints of formulae of the form \(\theta(X) = \psi \lor (\varphi \land \circ X)\). Concretely, we extend the formulae of LML with a modality \(\varphi \circ \psi\) (pronounced \(\varphi\) until \(\psi\)), whose semantics is the least fixpoint of \(\theta(X) = \psi \lor (\varphi \land \circ X)\).

Our order of presentation does not follow [BK08].

7.3.1 Syntax and Semantics of LTL

The formulae of LTL are given by the following grammar:
\[
\varphi, \psi ::= T \mid \bot \mid X \mid a \mid (\varphi \land \psi) \mid (\varphi \lor \psi) \mid \neg \varphi \mid \circ \varphi \mid \varphi \circ \psi
\]
(\text{where} \(X \in \mathcal{X}\) and \(a \in \text{AP}\))

The semantics of LTL-formulae extends that of LML with the clause:
\[
[\varphi \circ \psi]_\rho := \{\sigma \in (2\text{AP})^\omega \mid \exists i \in \mathbb{N}, \ \sigma|\iota \models [\psi]_\rho \text{ and } \forall j < i, \ \sigma|j \models [\varphi]_\rho\}
\]
We extend the notation \(\sigma \models \varphi\) of Notation 7.5. This gives, for closed \(\varphi, \psi\),
\[
\sigma \models \varphi \circ \psi \text{ iff } \exists i \in \mathbb{N}, \ \sigma|\iota \models \psi \text{ and } \forall j < i, \ \sigma|j \models \varphi
\]
7.3.2 Fixpoints and Defined Modalities

It is now time to check that \( \varphi \mathrel{\Box} \psi \) is indeed the least fixpoint of \( \theta(X) = \psi \lor (\varphi \land \bigcirc X) \).

**Lemma 7.23** ([BK08, Lem. 5.18]). Given formulae \( \varphi, \psi \) with parameters \( \rho \), \( \llbracket \varphi \mathrel{\Box} \psi \rrbracket_\rho \) is the least fixpoint of \( \theta(X) : \mathcal{P}((2 \mathbf{AP})^\omega) \to \mathcal{P}((2 \mathbf{AP})^\omega) \), where

\[
\theta(X) := \psi \lor (\varphi \land \bigcirc X)
\]

**Proof.** Exercise! \( \Box \)

With the notations of §7.2.3, Lem. 7.23 says that for \( \varphi, \psi \) with parameters \( \rho \) and with \( \theta(X) \) as in Lem. 7.23 we have

\[
\llbracket \varphi \mathrel{\Box} \psi \rrbracket_\rho = \mu X. \llbracket \theta \rrbracket_\rho(X)
\]

Using the duality of Lem. 7.22, we can obtain a syntactic representation of the greatest fixpoint of \( \theta(X) \), known as the weak until modality. It follows from Lem. 7.22 that the greatest fixpoint \( \nu X. \llbracket \theta \rrbracket_\rho(X) \) of \( \llbracket \theta \rrbracket_\rho(X) \) is given by

\[
\nu X. \llbracket \theta \rrbracket_\rho(X) = (2 \mathbf{AP})^\omega \setminus \mu X. \llbracket \neg \neg X/X \rrbracket_\rho(X)
\]

By using the laws of Fig. 1, we have

\[
\neg \llbracket \neg X/X \rrbracket = \neg (\psi \lor (\varphi \land \bigcirc X)) \\
= \neg \psi \land \neg (\varphi \land \bigcirc X) \\
= \neg \psi \land (\neg \varphi \lor \bigcirc X) \\
= (\neg \psi \land \neg \varphi) \lor (\neg \psi \land \bigcirc X)
\]

It thus follows from Lem. 7.23 that

\[
\mu X. \llbracket \neg \neg X/X \rrbracket_\rho(X) = \llbracket \neg \psi \lor (\psi \lor \varphi) \rrbracket_\rho
\]

so that

\[
\nu X. \llbracket \theta \rrbracket_\rho(X) = \llbracket \neg (\psi \lor (\psi \lor \varphi)) \rrbracket_\rho
\]

**Notation 7.24** (Weak Until). Given formulae \( \varphi \) and \( \psi \), we let

\[
\varphi \mathrel{\Box} \psi := \neg (\neg \psi \lor (\psi \lor \varphi))
\]

The above discussion leads us to the expected:

**Lemma 7.25.** Given formulae \( \varphi, \psi \) with parameters \( \rho \), \( \llbracket \varphi \mathrel{\mathcal{E}} \psi \rrbracket_\rho \) is the greatest fixpoint of \( \theta(X) : \mathcal{P}((2 \mathbf{AP})^\omega) \to \mathcal{P}((2 \mathbf{AP})^\omega) \), where

\[
\theta(X) := \psi \lor (\varphi \land \bigcirc X)
\]

It is then direct to define the modalities \( \Diamond \) and \( \square \) discussed in §7.2.1. Recall from Lem. 7.16 that \( \Diamond \varphi \) and \( \square \varphi \) are respectively the least and greatest fixpoints of

\[
\varphi \Diamond(X) := \varphi \lor \bigcirc X \quad \varphi \Box(X) := \varphi \land \bigcirc X
\]

**Notation 7.26** (Eventually and Always). Given a formula \( \varphi \), we let

\[
\Diamond \varphi := \top \lor \varphi \quad \square \varphi := \varphi \mathrel{\mathcal{E}} \bot
\]
Finally, note that while we have presented LTL as the extension of LML with least (and greatest) fixpoints of formulae of the form $\theta(X) = \psi \lor (\varphi \land \Box \Box X)$, there are quite simple (positive and guarded) fixpoints which are not definable in LTL.

**Proposition 7.27.** Let $a \in \mathcal{P}$. There is no closed LTL-formula $\varphi$ such that $[\varphi]$ is the greatest fixpoint of $\theta(X) := a \land \Box \Box X$.

Proposition 7.27 is part of a non-trivial theory. We refer to e.g. [PP04, Chap. VIII] and references therein for details.

### 7.3.3 Logical Equivalence

The notion of logical equivalence for LTL is exactly that of LML (Def. 7.7) extended to the formulae of LTL. In addition to the rules of Fig. 1, we have the equivalences for LTL-formulae of Fig. 3.

**Lemma 7.28.** All the equivalences of Fig. 1 and Fig. 3 hold.

We refer to [BK08, Fig. 5.7, p. 248] and [BK08, §5.1.5] for further equivalences. We nevertheless note the two following facts. First, there is a simple direct description of $\varphi W \psi$.

**Lemma 7.29** ([BK08, Lem. 5.19]). We have

$$\varphi W \psi \equiv (\varphi U \psi) \lor \Box \varphi$$

**Proof.** Exercise!

Second, Lem. 7.22 gives the following dualities.

**Lemma 7.30.** We have

$$\neg (\varphi W \psi) \equiv \neg \psi U (\neg \varphi \land \neg \psi)$$

$$\neg (\varphi U \psi) \equiv \neg \psi W (\neg \varphi \land \neg \psi)$$

**Proof.** Exercise!

### 7.3.4 Positive Normal Forms

By extending the syntax of LTL with the weak until modality $\varphi W \psi$, the equivalences of §7.3.3 allow us to “reduce” each formula to a formula in positive normal form, i.e. to a formula in which negations are only allowed on atomic formulae $a \in \mathcal{P}$ and on variables $X \in X$. This, however, comes with an exponential blow-up if one uses the equivalences of Lem. 7.30. A solution for this is, instead of extending the syntax of LTL with $W$, to extend it with the formal dual $R$ of $U$, called **release** and such that

$$\varphi R \psi \equiv \neg (\neg \varphi U \neg \psi)$$

$$\varphi U \psi \equiv \neg (\neg \varphi R \neg \psi)$$

We refer to [BK08, §5.1.5] for details.
Modal Duality Laws:
\[ \Diamond \varphi \equiv \neg \Box \neg \varphi \quad \Box \varphi \equiv \neg \Diamond \neg \varphi \]

Modal Operators Laws:
\[ \Diamond (\varphi \lor \psi) \equiv \Diamond \varphi \lor \Diamond \psi \quad \Diamond \bot \equiv \bot \]
\[ \Box (\varphi \land \psi) \equiv \Box \varphi \land \Box \psi \quad \Box \top \equiv \top \]

Distributive \( \Diamond / \lor \top \) Law:
\[ \Diamond (\varphi \lor \psi) \equiv \Diamond \varphi \lor \Diamond \psi \]

 Expansion Laws:
\[ \varphi \lor \psi \equiv \psi \lor (\varphi \land \Diamond \psi) \]
\[ \Diamond \varphi \equiv \varphi \lor \Diamond \Diamond \varphi \]
\[ \Box \varphi \equiv \varphi \land \Diamond \Diamond \varphi \]

Figure 3: Some Usual LTL Laws.

7.3.5 Satisfaction of LTL-Formulae by Transition Systems
Consider a transition system \( TS = (S, \text{Act}, \rightarrow, I, \text{AP}, L) \) over AP. A (closed) LTL-formula \( \varphi \) defines a linear-time property \( \llbracket \varphi \rrbracket \subseteq (2^{\text{AP}})^\omega \). Hence, we can specialize the notion of satisfaction of LT properties (Def. 3.5) to the following.

Definition 7.31. Given \( TS \) and \( \varphi \) as above, we say that \( TS \) satisfies \( \varphi \) (notation \( TS \models \varphi \)) if \( TS \models \llbracket \varphi \rrbracket \) (i.e. if \( \text{Tr}^\omega(TS) \subseteq \llbracket \varphi \rrbracket \)).

Definition 7.31 corresponds to [BK08, Def. 5.7]. We refer to [BK08, §5.1.2 & 5.1.3] for examples.

7.4 Fixpoints of Scott-Continuous Functions
While the Knaster-Tarski Fixpoint Theorem 7.20 gives a general method for computing least and greatest fixpoints, it gives few hints on the actual values of these fixpoints. In particular, using Thm. 7.20 to compute the fixpoint interpretations of \( \Diamond \varphi \) and \( \Box \varphi \) given by Lem. 7.16 does not seem to help to recover the intuitions behind the ideal descriptions presented in §7.2.1:
\[ \Diamond \varphi \equiv \varphi \lor \Diamond \varphi \lor \Diamond \Diamond \varphi \lor \cdots \equiv \bigvee_{n \in \mathbb{N}} \Diamond^n \varphi \]
\[ \Box \varphi \equiv \varphi \land \Box \varphi \land \Box \Diamond \varphi \land \cdots \equiv \bigwedge_{n \in \mathbb{N}} \Box^n \varphi \]

In this Section, we shall see general conditions under which the least and greatest fixpoints of a function \( f : L \rightarrow L \) can be computed as follows:
\[ \mu(f) = \bigvee_{n \in \mathbb{N}} f^n(\bot) \quad \nu(f) = \bigwedge_{n \in \mathbb{N}} f^n(\top) \]
As we shall see, these conditions do apply to the formulae of Lem. 7.16
\[ \varphi \Diamond (X) := \varphi \lor \Diamond X \quad \varphi \Box (X) := \varphi \land \Diamond X \]
As a consequence, we obtain
\[ \llbracket \Diamond \varphi \rrbracket_\rho = \bigvee_{n \in \mathbb{N}} \llbracket \varphi \Diamond^n (\bot) \rrbracket_\rho \quad \llbracket \Box \varphi \rrbracket_\rho = \bigwedge_{n \in \mathbb{N}} \llbracket \varphi \Box^n (\top) \rrbracket_\rho \]

31
and since
\[ \phi^{n+1}(\bot) \equiv \bigvee_{k \leq n} \phi^n \phi \quad \phi^{n+1}(\top) \equiv \bigwedge_{k \leq n} \phi^n \phi \]
we indeed have
\[ \llbracket \phi \rrbracket_\rho = \bigvee_{n \in \mathbb{N}} \llbracket \phi^n \phi \rrbracket_\rho \quad \llbracket \phi \downarrow \rrbracket_\rho = \bigwedge_{n \in \mathbb{N}} \llbracket \phi^n \phi \rrbracket_\rho \]
This relies on some structure that we make explicit first.

### 7.4.1 Scott-Continuity

**Definition 7.32 ((Co)Directed Set).** Let \((L, \leq)\) be a partial order.

1. A subset \(D \subseteq L\) of \(L\) is **directed** if it is non-empty and if for all \(a, b \in D\) there is some \(c \in D\) such that \(a \leq c\) and \(a \leq d\).
2. A subset \(D \subseteq L\) of \(L\) is **codirected** if it is a directed subset of \(L^{\text{op}}\).

In words, \(D \subseteq L\) is codirected if it is non-empty and if for all \(a, b \in D\) there is some \(c \in D\) such that \(c \leq a\) and \(c \leq b\).

The notions of **directed set** and **Scott-continuous functions** are standard. We refer e.g. to [DP02, Def. 7.7 & §8.6]. See also the book [AC98] for a more comprehensive reference on the use of these notions for the denotational semantics of programming languages.

**Definition 7.33 (Scott (Co)Continuous Function).** Let \((L, \leq), (L', \leq')\) be complete lattices.

1. A function \(f : L \to L'\) is **Scott-continuous** if it is monotone and if for each directed \(D \subseteq L\), we have
   \[ f(\bigvee D) = \bigvee_{d \in D} f(d) \]
2. A function \(f : L \to L'\) is **Scott-cocontinuous** if it is a Scott-continuous function \(L^{\text{op}} \to (L')^{\text{op}}\).

In words, \(f : L \to L'\) is Scott-cocontinuous if it is monotone, and if for each codirected \(D \subseteq L\) we have \(f(\bigwedge D) = \bigwedge_{d \in D} f(d)\). Note that if \(f\) is monotone and \(D\) is (co)directed, then \(\{f(d) \mid d \in D\}\) is also (co)directed. The notion of Scott-continuous function is usually defined for structures weaker than complete lattices, namely (directed-)complete partial orders ((D)CPOs).

See e.g. [DP02, Chap. 8] or [AC98].

Fixpoints of Scott-(co)continuous functions \(f : L \to L\) are particularly simple to compute. The case of least fixpoints of Scott-continuous functions is standard, see e.g. [DP02, Thm. 8.15] or [AC98]. Given a function \(f : L \to L\) and some \(a \in L\), we let \(f^0(a) := a\) and \(f^{n+1}(a) := f(f^n(a))\).

**Proposition 7.34.** Let \((L, \leq)\) be a complete lattice.

1. If \(f : L \to L\) is Scott-continuous then its least fixpoint is given by
   \[ \mu(f) = \bigvee_{n \in \mathbb{N}} f^n(\bot) \]
2. If \(f : L \to L\) is Scott-cocontinuous then its greatest fixpoint is given by
   \[ \nu(f) = \bigwedge_{n \in \mathbb{N}} f^n(\top) \]
Proof. Exercise! \[ \square \]

In order to apply Prop. 7.34 to functions defined by LML-formulae, we shall need to show that given a formula $\varphi$ with parameters $\rho$ and a variable $X$, if $X \text{ Pos } \varphi$ then

$$\llbracket \varphi \rrbracket_\rho(X) : \mathcal{P}((2^{AP})^\omega) \to \mathcal{P}((2^{AP})^\omega)$$

is a Scott-continuous function. This relies on the following fundamental property. Recall from Def. 5.8 ($\S$5.2) that a formula $\varphi$ with parameters $\rho$ and a variable $X$, if $X \text{ Pos } \varphi$ then

$$\llbracket \varphi \rrbracket_\rho(X) : \mathcal{P}((2^{AP})^\omega) \to \mathcal{P}((2^{AP})^\omega)$$

Proof. Exercise! \[ \square \]

**Corollary 7.36.** Let $X$ be a set and let $(D, \subseteq)$ be a partial order. If $D$ is directed and $f, g : D \to L$ are monotone then

1. If $D$ is directed and $f, g : (D, \subseteq) \to (\mathcal{P}(X), \subseteq)$ are monotone then

$$\left( \bigvee_{d \in D} f(d) \right) \cup \left( \bigvee_{d \in D} g(d) \right) = \bigvee_{d \in D} f(d) \cup g(d)$$

$$\left( \bigvee_{d \in D} f(d) \right) \cap \left( \bigvee_{d \in D} g(d) \right) = \bigvee_{d \in D} f(d) \cap g(d)$$

2. If $C$ is codirected and $f, g : (C, \subseteq) \to (\mathcal{P}(X), \subseteq)$ are monotone then

$$\left( \bigcap_{c \in C} f(c) \right) \cap \left( \bigcap_{c \in C} g(c) \right) = \bigcap_{c \in C} f(c) \cap g(c)$$

$$\left( \bigcap_{c \in C} f(c) \right) \cup \left( \bigcap_{c \in C} g(c) \right) = \bigcap_{c \in C} f(c) \cup g(c)$$

Proof. Exercise! \[ \square \]

### 7.4.2 Application to LML

We can now show, with the help of Cor. 7.36, that we can indeed apply Prop. 7.34 to fixpoints of LML-formulae, i.e. that an LML-formula of a positive variable indeed induces a Scott-continuous function. Similarly as for monotonicity in Lem. 7.18, this requires to also handle the case of negative variables.

**Lemma 7.37.** The function $\llbracket \bigcirc X \rrbracket(X)$ is a map of complete Boolean algebras.

Lemma 7.37 amounts to the fact that $\llbracket \bigcirc X \rrbracket(X)$ preserves all unions and intersections, which is easy to observe. It then follows that it also preserves complements since the complement of $P$ is the unique $Q$ such that $P \cup Q = (2^{AP})^\omega$ and $P \cap Q = \emptyset$.

**Proposition 7.38.** Consider a formula $\varphi$ with parameters $\rho$ and a variable $X$.

1. If $X \text{ Pos } \varphi$, then

$$\llbracket \varphi \rrbracket_\rho(X) : (\mathcal{P}((2^{AP})^\omega), \subseteq) \to (\mathcal{P}((2^{AP})^\omega), \subseteq)$$

is Scott-continuous as well as Scott-cocontinuous.
(2) If $X \neg \varphi$, then

$$[[\varphi]]_\rho(X) : (P((2^{AP})^\omega), \subseteq) \to (P((2^{AP})^\omega), \subseteq)^\text{op}$$

is Scott-continuous as well as Scott-cocontinuous.

Let us explicit the case of $X \neg \varphi$ in Prop. 7.38. First note that a Scott-(co)continuous

$$[[\varphi]]_\rho(X) : (P((2^{AP})^\omega), \subseteq) \to (P((2^{AP})^\omega), \subseteq)^\text{op}$$

is antimonotone ($[[\varphi]]_\rho(B) \subseteq [[\varphi]]_\rho(A)$ whenever $A \subseteq B$). Second, since directed joins (resp. codirected meets) in $(P((2^{AP})^\omega), \subseteq)^\text{op}$ are codirected meets (resp. directed joins) in $(P((2^{AP})^\omega), \subseteq)$, we have, for directed $D \subseteq P((2^{AP})^\omega)$ and codirected $C \subseteq P((2^{AP})^\omega)$,

$$[[\varphi]]_\rho(\bigcup_{D \in D} D) = \bigcap_{D \in D} [[\varphi]]_\rho(D)
$$

$$[[\varphi]]_\rho(\bigcap_{C \in C} C) = \bigcup_{C \in C} [[\varphi]]_\rho(C)$$

where, by antimonotonicity of $[[\varphi]]_\rho(X)$,

$$\{[[\varphi]]_\rho(D) \mid D \in D\} \text{ is codirected}
$$

$$\{[[\varphi]]_\rho(C) \mid C \in C\} \text{ is directed}$$

Proof. Exercise! \qed

We therefore have obtained the expected fact that for $\varphi(X)$ with parameters $\rho$, if $X \text{ Pos } \varphi$ then

$$\mu X. [[\varphi]]_\rho(X) = \bigcup_{n \in \mathbb{N}} [[\varphi^n(\bot)]]_\rho
$$

$$\nu X. [[\varphi]]_\rho(X) = \bigcap_{n \in \mathbb{N}} [[\varphi^n(\top)]]_\rho$$

**Example 7.39** (The Fixpoint of Prop. 7.27). Proposition 7.27 states that given $a \in AP$, the greatest fixpoint of $\theta(X) := a \land \bigcirc \bigcirc X$ is not definable by a closed LTL formula. Proposition 7.38 (together with Prop. 7.34) implies that

$$\nu X. [[\theta]](X) = \bigcap_{n \in \mathbb{N}} [[\theta^n(\top)]]$$

But note that

$$\theta^{n+1}(\top) \equiv \bigwedge_{k \leq n} \bigcirc^{2k} a$$

It follows that

$$\nu X. [[\theta]](X) = \{\sigma \in (2^{AP})^\omega \mid \forall n \in \mathbb{N}, \ a \in \sigma(2n)\}$$

**7.4.3 A Warning on Scott-Continuity for LML-Formulae**

A few words of caution are required when applying Prop. 7.38. The **linear-time** modal $\mu$-calculus alluded to in Rem. 7.21 is the extension of LML with least and greatest fixpoints $\mu X. \varphi$ and $\nu X. \varphi$ for each formula $\varphi$ such that $X \text{ Pos } \varphi$. Assuming that we also have $Y \text{ Pos } \varphi$, $Y$ is again positive in both $\mu X. \varphi$ and $\nu X. \varphi$, and in the modal $\mu$-calculus we can further form the fixpoints

$$\mu Y. \mu X. \varphi \quad \nu Y. \mu X. \varphi \quad \mu Y. \nu X. \varphi \quad \nu Y. \nu X. \varphi$$

However, the functions (of $Y$) induced by $(\mu X. \varphi)(Y)$ and $(\nu X. \varphi)(Y)$ are in general **not** Scott-(co)continuous.
A well-known restriction of the modal $\mu$-calculus is its \textbf{alternation-free} (see e.g. [BW18, p. 37]) or \textbf{flat} [SV10] fragment, in which fixpoints $\mu X. \varphi$ and $\nu X. \varphi$ are not allowed when $X$ occurs free in a subformula of $\varphi$ of the form $\mu Y. \psi$ or $\nu Y. \psi$. In this fragment, least and greatest fixpoints can always be computed as in Prop. 7.34.

In the specific case of the \textbf{linear-time} $\mu$-calculus, \textit{i.e.} the extension of LML with fixpoints, it turns out that the alternation-free fragment has the same expressive power as the full $\mu$-calculus (combine [BW18, Thm. 20 & Thm. 21] with [Tho97, Cor. 5.12]). This is a consequence of McNaughton’s Theorem (see e.g. [Tho97, Thm. 5.4]), a non-trivial result on automata over $\omega$-words.

Finally, note that the fixpoint of Prop. 7.27 (see Ex. 7.39) is alternation-free (or flat).

\section{Toward Stone Duality}

\textbf{Warning (On AP). In this section we always assume that AP is a finite non-empty set.}
In §6, we devised a topological notion of “observable properties”, which consist of the Boolean algebra of clopen sets of a topological space. For spaces $(2^{AP})^\omega$, this amounts to the Boolean algebra of sets of the form $\text{ext}(W)$ for some finite $W \subseteq (2^{AP})^*$. In §7, we devised LML, a base modal logic for linear-time properties, whose formulae define exactly the observable properties on $(2^{AP})^\omega$. We noted that LML is very weak w.r.t. the linear-time properties discussed in §3, and considered LTL, and extension of LML with a restricted form of least and greatest fixpoints.

In this Section, we shall discuss further topological properties of spaces $(2^{AP})^\omega$, which allow for recovering the whole set $(2^{AP})^\omega$ from the Boolean algebra of clopen sets of its topology, \textit{i.e.} from LML.

We use the following notation.

\textbf{Notation 8.1.} Given a compact Hausdorff space $(X, \Omega)$, we let $K\Omega$ be the set of compact open subsets of $X$.

Recall from Lem. 6.10 and Prop. 6.18 that for $(X, \Omega)$ compact Hausdorff, $K\Omega$ coincides with the set of clopen subsets of $X$. By Prop. 6.12 and Prop. 6.19, we in particular have $K\Omega((2^{AP})^\omega) = \{\text{ext}(W) \mid W \subseteq (2^{AP})^* \text{ is finite}\}$

Given an $\omega$-word $\sigma \in (2^{AP})^\omega$, let

$$F_\sigma := \{\text{ext}(W) \in K\Omega((2^{AP})^\omega) \mid \sigma \in \text{ext}(W)\}$$

The following observations are easy. Recall that $\text{ext}(\varepsilon) = (2^{AP})^\omega$ and that $\text{ext}(\emptyset) = \emptyset$.

(1) $(2^{AP})^\omega \in F_\sigma$ and $\emptyset \notin F_\sigma$.

(2) If $U \in F_\sigma$ and $U \subseteq V$ with $V \in K\Omega((2^{AP})^\omega)$ then $V \in F_\sigma$.

(3) If $U \in F_\sigma$ and $V \in F_\sigma$, then $U \cap V \in F_\sigma$.

(4) If $U \cup V \in F_\sigma$ with $U, V \in K\Omega((2^{AP})^\omega)$, then either $U \in F_\sigma$ or $V \in F_\sigma$.

Given a Boolean algebra $B$, subsets $F \in B$ satisfying the above conditions are called \textbf{prime filters} on $B$.

Note that for $\sigma, \beta \in (2^{AP})^\omega$, we evidently have $F_\sigma \neq F_\beta$ whenever $\sigma \neq \beta$. Hence $(2^{AP})^\omega$ can be embedded into the set of prime filters on $K\Omega((2^{AP})^\omega)$. Actually, $(2^{AP})^\omega$ is in bijection with the set of prime filters on $K\Omega((2^{AP})^\omega)$. This fact, which is part of \textbf{Stone’s Representation Theorem}, holds for any \textbf{Stone space}.
Definition 8.2 (Stone Space). A Stone space is a topological space \((X, \Omega)\) which is compact (see Def. 6.9), and satisfies the two following conditions:

\((X, \Omega)\) is \(T_0\): for any distinct points \(x, y \in X\), there is an open containing one and not the other, i.e. there is some \(U \in \Omega\) such that either \((x \in U \text{ and } y \notin U)\) or \((x \notin U \text{ and } y \in U)\).

\((X, \Omega)\) is zero-dimensional: the clopen subsets of \(X\) form a base for the topology.

Note that every Stone space \((X, \Omega)\) is Hausdorff (Def. 6.16).

Example 8.3. It follows from Lem. 6.7 that \(A^\omega\) is zero-dimensional, whether or not \(A\) is finite. Hence \((2^{AP})^\omega\) is a Stone space by Prop. 6.12.

We shall target the two following instances of Stone’s Representation Theorem:

- Every Boolean algebra \(B\) is isomorphic to the Boolean algebra \(K\Omega(\text{Sp}(B))\) for some Stone space \((\text{Sp}(B), \Omega(\text{Sp}(B)))\), called the spectrum of \(B\).
- Every Stone space \((X, \Omega)\) is homeomorphic to the spectrum of the Boolean algebra \(K\Omega\).

We refer to [Joh86, Cor. II.4.4] for the full statement of Stone’s Representation Theorem.

Let us finally illustrate the logical relevance of these matters in our context.

Definition 8.4.

(1) Let \(\Sigma(LML)\) be the set of closed LML-formulae quotiented by logical equivalence \(\equiv\) (in the sense of Def. 7.7 and Fig. 1, §7.1.2).

(2) Let \(\Sigma(LTL)\) be the set of closed LTL-formulae quotiented by logical equivalence \(\equiv\) (in the sense of §7.3.3).

Notation 8.5. In this Section 8, \(L\) stands for either LML or LTL.

We shall always notationally confuse a closed \(L\)-formula \(\varphi\) with its quotient \([\varphi]_\equiv \in \Sigma(L)\), where, as usual

\[
[\varphi]_\equiv = \{ \psi \mid \psi \text{ is a closed } L \text{-formula such that } \varphi \equiv \psi \}
\]

We equip \(\Sigma(L)\) with the partial order

\[
\varphi \leq \psi := (\varphi \rightarrow \psi) \equiv \top
\]

Note that

\[
\varphi \leq \psi \iff \varphi \equiv (\varphi \land \psi) \iff (\varphi \lor \psi) \equiv \psi
\]

and that \(\leq\) is indeed a partial order on \(\Sigma(L)\) (i.e. \(\varphi \equiv \psi\) if \(\varphi \leq \psi\) and \(\psi \leq \varphi\)).

It follows from Prop. 7.10 and Prop. 7.11 (§7.1.3) that we can identify \(K\Omega((2^{AP})^\omega)\) with \(\Sigma(LML)\). The properties of prime filters underlined above can then be rephrased as follows, for a set \(\mathcal{F} \subseteq \Sigma(LML)\):

- \(\mathcal{F}\) is non-empty (\(\top \in \mathcal{F}\)) and coherent (\(\bot \notin \mathcal{F}\)).
- \(\mathcal{F}\) is a theory:
  - \(\varphi \in \mathcal{F}\) and \(\varphi \leq \psi\) imply \(\psi \in \mathcal{F}\),
  - \(\varphi, \psi \in \mathcal{F}\) implies \(\varphi \land \psi \in \mathcal{F}\).
• \( F \) is complete (\( \varphi \lor \psi \in F \) implies either \( \varphi \in F \) or \( \psi \in F \), so that for every \( \varphi \) we have either \( \varphi \in F \) or \( \neg \varphi \in F \)).

Then, the existence of a bijection between \( (2^{AP})^\omega \) and the set of prime filters over \( K\Omega((2^{AP})^\omega) \) can be read as a completeness theorem:

• Every complete consistent theory \( F \subseteq L(LML) \) has a model, i.e. there is some \( \sigma \in (2^{AP})^\omega \) such that for all \( \varphi \in L(LML) \), we have \( \sigma \models \varphi \) iff \( \varphi \in F \).

Remark 8.6 (On Lindenbaum-Tarski Algebras). The set \( \mathfrak{L}(L) \) defined in Def. 8.4 is reminiscent from Lindenbaum-Tarski algebras (see e.g. [BdRV02, Def. 5.31]). However, Lindenbaum-Tarski algebras are usually defined as the quotient of formulae w.r.t. provable logical equivalence (see also Rem. 7.9).

8.1 A Short Path Toward a Simplified Result

We present here a short path toward a simplified form of Stone’s Duality, namely that for every Stone space \((X, \Omega)\), the set of points \( X \) is in bijection with the set of prime filters over the Boolean algebra \( K\Omega \).

Warning. The notions and results discussed in this §8.1 are not presented in their usual generality.

8.1.1 From Lattices to Boolean Algebras

Definition 8.7 (Lattice). A lattice is a partial order having all finite joins and all finite meets.

Lemma 8.8. In a lattice \((L, \lor, \land, \bot, \top)\), the following two distributive laws are equivalent:

\[
\forall a, b, c \in L, \quad a \land (b \lor c) = (a \land b) \lor (a \land c) \\
\forall a, b, c \in L, \quad a \lor (b \land c) = (a \lor b) \land (a \lor c)
\]

Proof. Exercise!

Definition 8.9 (Distributive Lattice). A lattice is distributive if it satisfies either of the distributive laws of Lem. 8.8.

Definition 8.10. Let \((L, \lor, \land, \bot, \top)\) be a lattice. Given \( a \in L \), we say that \( c \in L \) is a complement of \( a \) whenever both \( a \lor c = \top \) and \( a \land c = \bot \) hold.

Lemma 8.11. If \((L, \leq)\) is a distributive lattice, then \( a \in L \) has at most one complement.

Proof. Exercise!

Definition 8.12 (Boolean Algebra). A Boolean algebra is a distributive lattice in which every element \( b \) has a (necessarily unique) complement \( \neg b \).

Lemma 8.13 (De Morgan Laws). Every Boolean algebra \((B, \lor, \land, \bot, \top)\) satisfies the following De Morgan Laws:

\[
a \land b = \neg(\neg a \lor \neg b) \quad a \lor b = \neg(\neg a \land \neg b) \quad a = \neg \neg a
\]

Proof. Exercise!
8.1.2 Filters and Ultrafilters

Definition 8.14 (Filters). Let \((L, \leq)\) be a lattice.

1. A set \(F \subseteq L\) is a filter if
   - \(F\) is upward-closed (\(b \in F\) whenever \(b \geq a\) for some \(a \in F\)), and
   - \(\top \in F\), and
   - \(a \land b \in F\) whenever \(a \in F\) and \(b \in F\).

2. A filter \(F \subseteq L\) is prime if
   - \(\bot \not\in F\), and
   - if \(a \lor b \in F\) then either \(a \in F\) or \(b \in F\).

Definition 8.15 (Finite Intersection Property). Let \((L, \leq)\) be a lattice. A family of sets \(F \subseteq L\) is said to have the finite intersection property if \(\bigwedge S \neq \bot\) for all finite \(S \subseteq F\).

Lemma 8.16 (Ultrafilter Lemma). Let \((L, \leq)\) be a distributive lattice. If \(F \subseteq L\) has the finite intersection property, then \(F \subseteq F^*\) for some prime filter \(F^*\) on \(L\).

The Ultrafilter Lemma 8.16 is discussed in §8.1.4 as a consequence of Zorn’s Lemma (an equivalent formulation of the Axiom of Choice).

8.1.3 The Spectrum of a Boolean Algebra

Definition 8.17 (Spectrum of a Boolean Algebra (1/2)). Given a Boolean algebra \(B\), we let \(\text{Sp}(B)\) be the set of prime filters on \(B\).

Definition 8.18. Given a Boolean algebra \(B\) and \(a \in B\) we let

\[
\text{ext}(a) := \{F \in \text{Sp}(B) \mid a \in F\}
\]

Lemma 8.19. Let \((B, \leq)\) be a Boolean algebra. Then we have

\[
\begin{align*}
\text{ext}(a \land b) &= \text{ext}(a) \cap \text{ext}(b) \\
\text{ext}(a \lor b) &= \text{ext}(a) \cup \text{ext}(b) \\
\text{ext}(\lnot a) &= \text{Sp}(B) \setminus \text{ext}(a) \\
\text{ext}(\top) &= \text{Sp}(B) \\
\text{ext}(\bot) &= \emptyset
\end{align*}
\]

Proof. Exercise! □

Definition 8.20 (Spectrum of a Boolean Algebra (2/2)). Given a Boolean algebra \(B\), we equip \(\text{Sp}(B)\) with the topology \(\Omega(\text{Sp}(B))\) induced by the base \(B := \{\text{ext}(a) \mid a \in B\}\). The space \((\text{Sp}(B), \Omega(\text{Sp}(B)))\) is the spectrum of \(B\).

As expected, \(\text{Sp}(B)\) is always a Stone space.

Lemma 8.21. The spectrum of a Boolean algebra \(B\) is \(T_0\) and zero-dimensional.

It remains to show that \(\text{Sp}(B)\) is compact. For this, we rely on the Ultrafilter Lemma 8.16.

Proposition 8.22. The spectrum \((\text{Sp}(B), \Omega(\text{Sp}(B)))\) of a Boolean algebra \(B\) is compact.
We can now state a simplified version of Stone’s Representation Theorem. We refer to [Joh86, Cor. II.4.4] for the full statement of Stone’s Representation Theorem.

**Theorem 8.23.** If \((X, \Omega)\) is a Stone space, then the following function is a bijection:

\[
\eta : X \rightarrow \text{Sp}(K\Omega) \\
x \mapsto \{U \in K\Omega \mid x \in U\}
\]

8.1.4 Proof of the Ultrafilter Lemma 8.16

The Ultrafilter Lemma 8.16 follows from a formulation of the Axiom of Choice known as Zorn’s Lemma. A chain in a partial order \((L, \leq)\) is a set \(C \subseteq L\) such that for all \(a, b \in C\), we have either \(a \leq b\) or \(b \leq a\). Zorn’s Lemma is equivalent to the Axiom of Choice.

**Lemma 8.24** (Zorn’s Lemma). Let \((L, \leq)\) be a partial order. If every chain in \(L\) has an upper bound in \(L\), then \(L\) has a maximal element (i.e. some \(a \in L\) such that \(b \leq a\) whenever \(a \leq b\)).

A filter \(F\) on a lattice \((L, \leq)\) is proper if \(\perp \not\in F\). Note that if \(F \subseteq L\) has the finite intersection property, then

\[
\text{Filt}(F) := \{a \in L \mid a \geq \bigwedge S \text{ for some finite } S \subseteq F\}
\]

is a proper filter.

**Proof of the Ultrafilter Lemma 8.16.** Exercise!

8.2 Lattices and Boolean Algebras

In this Section, we discuss an algebraic presentation of (semi)lattices, distributive lattices and Boolean algebras, which is mostly based on [Joh86, §I.1]. Most of the material presented here can also be found in [DP02], but is more scattered in that source.

8.2.1 Semilattices

A lattice is a partial order \((L, \leq)\), which, similarly to a complete lattice, has joins and meets. But in contrast with complete lattices, only finite joins and meets are required to exists in a lattice. This obviously amounts to ask for binary joins and meets as well as for a least and a greatest element. As a consequence, and again in contrast with complete lattices, we must assume joins and meets separately. This leads to the notions of meet and join semilattices.

**Definition 8.25** (Semilattices).

(1) A meet semilattice is a partial order having all finite meets (i.e. greatest lower bounds \(\land, \top\)).

(2) A join semilattice is a partial order having all finite joins (i.e. least upper bounds \(\lor, \bot\)).

**Example 8.26.** Given a set \(X\), \((\mathcal{P}(X), \subseteq)\) is a meet semilattice (with meets given by intersections) and a join semilattice (with joins given by unions).

**Example 8.27.** Given a topological space \((X, \Omega)\), \((\Omega, \subseteq)\) is a meet semilattice (with meets given by intersections) and a join semilattice (with joins given by unions).
A meet semilattice can equivalently be defined as a partial order \((L, \leq)\) equipped with binary meets \(\wedge : L \times L \to L\) and a greatest element \(\top \in L\). Similarly, a join semilattice is a partial order \((L, \leq)\) equipped with binary joins \(\vee : L \times L \to L\) and a least element \(\bot \in L\). In each case, the order \(\leq\) can be recovered from equational axioms on \((L, \wedge, \top)\) and \((L, \vee, \bot)\).

**Definition 8.28.**

(1) A **monoid** is a set \(A\) equipped with a binary operation \(\odot : A \times A \to A\) and a constant \(I \in A\) such that for all \(a, b, c \in A\) we have

\[
a \odot (b \odot c) = (a \odot b) \odot c \quad a \odot I = a \quad I \odot a = a
\]

(2) A **commutative monoid** is a monoid \((A, \odot, I)\) such that for all \(a, b \in A\) we have

\[
a \odot b = b \odot a
\]

(3) An element \(a \in A\) of a monoid \((A, \odot, I)\) is **idempotent** if

\[
a \odot a = a
\]

**Lemma 8.29.**

(1) Let \((L, \leq)\) be a meet semilattice. Then \((L, \wedge, \top)\) is a commutative monoid in which every element is idempotent. Moreover, we have \(a \leq b\) iff \(a = a \wedge b\).

(2) Let \((L, \leq)\) be a join semilattice. Then \((L, \vee, \bot)\) is a commutative monoid in which every element is idempotent. Moreover, we have \(a \leq b\) iff \(a \vee b = b\).

**Proof.** Exercise!

Conversely,

**Lemma 8.30.**

(1) Given a commutative monoid \((L, \wedge, \top)\) in which every element is idempotent, let \(a \leq \wedge b\) iff \(a = a \wedge b\). Then \((L, \leq \wedge)\) is a meet semilattice with binary meets given by \(\wedge\) and with greatest element \(\top\).

(2) Given a commutative monoid \((L, \vee, \bot)\) in which every element is idempotent, let \(a \leq \vee b\) iff \(a \vee b = b\). Then \((L, \leq \vee)\) is a join semilattice with binary joins given by \(\vee\) and with least element \(\bot\).

**Proof.** Exercise!

**Corollary 8.31.** Let \((L, \leq)\) be a partial order.

(1) The following are equivalent:

- \((L, \leq)\) is a meet semilattice.
- \(L\) is equipped with the structure \((L, \wedge, \top)\) of a commutative monoid in which every element is idempotent and such that \(a \leq b\) iff \(a = a \wedge b\).

Moreover, if either of the above conditions holds, the binary meets of \((L, \leq)\) are given by \(\wedge\) and \(\top\) is the greatest element of \(L\).
(2) The following are equivalent:
- \((L, \leq)\) is a join semilattice.
- \(L\) is equipped with the structure \((L, \lor, \bot)\) of a commutative monoid in which every element is idempotent and such that \(a \leq b\) iff \(a \lor b = b\).

Moreover, if either of the above conditions holds, the binary joins of \((L, \leq)\) are given by \(\lor\) and \(\bot\) is the least element of \(L\).

**Example 8.32.** Consider the partial order \((\mathcal{L}(L), \leq)\).

(1) \((\mathcal{L}(L), \leq)\) is a meet semilattice with greatest element \(\top\) and with binary meets given by

\[
(-) \land (-) : \mathcal{L}(L) \times \mathcal{L}(L) \to \mathcal{L}(L)
\]

\[
(\varphi, \psi) \mapsto \varphi \land \psi
\]

(2) \((\mathcal{L}(L), \leq)\) is a join semilattice with least element \(\bot\) and with binary joins given by

\[
(-) \lor (-) : \mathcal{L}(L) \times \mathcal{L}(L) \to \mathcal{L}(L)
\]

\[
(\varphi, \psi) \mapsto \varphi \lor \psi
\]

**Proof.** Exercise! 

**Definition 8.33 (Semilattice Morphism).** Let \((L, \leq)\) and \((L', \leq')\) be partial orders and let \(f : L \to L'\) be a function.

(1) If \((L, \leq)\) and \((L', \leq')\) are meet semilattices, then \(f\) is a map of meet semilattices if it preserves finite meets, i.e. if for all finite \(S \subseteq L\) we have

\[
f(\bigwedge S) = \bigwedge' \{f(s) \mid s \in S\}
\]

(2) If \((L, \leq)\) and \((L', \leq')\) are join semilattices, then \(f\) is a map of join semilattices if it preserves finite joins, i.e. if for all finite \(S \subseteq L\) we have

\[
f(\bigvee S) = \bigvee' \{f(s) \mid s \in S\}
\]

Note that it follows from Lem. 8.29 that a map of semilattices is automatically monotone. Moreover, if follows from Lem. 8.29 and Lem. 8.30 that \(f : L \to L'\) is a map of meet (resp. join) semilattices iff \(f(\top) = \top'\) and \(f(a \land b) = f(a) \land' f(b)\) (resp. \(f(\bot) = \bot'\) and \(f(a \lor b) = f(a) \lor' f(b)\)).

**Example 8.34.** Given sets \(X\) and \(Y\), each function \(f : X \to Y\) induces a map of join and meet semilattices \(f^{-1} : (\mathcal{P}(Y), \subseteq) \to (\mathcal{P}(X), \subseteq)\) (see §6.1).

**Example 8.35.** Given topological spaces \((X, \Omega_X)\) and \((Y, \Omega_Y)\), each continuous function \(f : X \to Y\) (Def. 6.2) induces a map of join and meet semilattices \(f^{-1} : (\Omega_Y, \subseteq) \to (\Omega_X, \subseteq)\).

**Example 8.36.** Consider the partial order \((\mathcal{L}(\text{LTL}), \leq)\).

(1) The function

\[
\Box : \mathcal{L}(\text{LTL}) \to \mathcal{L}(\text{LTL})
\]

\[
\varphi \mapsto \Box \varphi
\]

is a map of meet semilattices.
The function
\[ \diamond : \mathcal{L}(\text{LTL}) \rightarrow \mathcal{L}(\text{LTL}) \]
\[ \varphi \mapsto \diamond \varphi \]
is a map of join semilattices.

Proof. Exercise!

The following is a general algebraic property, which leads to the usual notion of isomorphic algebra (see e.g. [BS81, §I.2 & §II.2] and also [DP02, §2.16 & §2.17]).

Lemma 8.37. Given meet (resp. join) semilattices \( L, L' \) and a bijective meet (resp. join) semilattice morphism \( f : L \rightarrow L' \), the inverse of \( f \) is map of meet (resp. join) semilattices from \( L' \) to \( L \).

Proof. Exercise!

Definition 8.38 (Semilattice Isomorphism). A map of meet (resp. join) semilattices \( f : L \rightarrow L' \) is an **isomorphism** if \( f \) is a bijection.

8.2.2 Lattices

Definition 8.39 (Lattice). A **lattice** is a partial order having all finite joins and all finite meets.

Example 8.40. Given a set \( X \), \( (\mathcal{P}(X), \subseteq) \) is a lattice in which meets are given by intersections and joins are given by unions.

Example 8.41. Given a topological space \( (X, \Omega) \), \( (\Omega, \subseteq) \) is a lattice in which meets are given by intersections and joins are given by unions.

Of course, a finite join (resp. meet) semilattice has all joins (resp. all meets), and is thus a (complete) lattice by Lem. 5.7. But this does not hold for infinite semilattices.

Example 8.42. Consider the partial order \( (L, \sqsubseteq) \) where
\[ L := \mathbb{N} \cup \{\alpha, \beta, \top\} \]
and where \( \sqsubseteq \) is the reflexive-transitive closure of \( \sqsubseteq \), where
\[ a \sqsubseteq b \iff \begin{cases} a < b \text{ in } \mathbb{N}, & \text{or} \\ a \in \mathbb{N} \text{ and } b \in \{\alpha, \beta\}, & \text{or} \\ a \in \{\alpha, \beta\} \text{ and } b = \top \end{cases} \]

Then \( (L, \sqsubseteq) \) is a join semilattice but not a lattice.

Proof. Exercise!

Consider a lattice \( (L, \leq) \) with finite meets given by \( (\land, \top) \) and finite joins given by \( (\lor, \bot) \). Then \( (L, \leq, \land, \top) \) and \( (L, \leq, \lor, \bot) \) are resp. a meet and a join semilattice. Hence the partial orders \( \leq_{\land} \) and \( \leq_{\lor} \) of Lem. 8.30 coincide since by Lem. 8.29 we have
\[ a \leq b \iff a = a \land b \quad \text{iff} \quad b = a \lor b \]

This gives a purely algebraic characterization of lattices.
Lemma 8.43. Consider a set $L$ equipped with two binary operations $\land, \lor : L \times L \to L$ and two constants $\top, \bot \in L$. Assume that $(L, \land, \top)$ and $(L, \lor, \bot)$ are commutative monoids in which every element is idempotent. Then the following are equivalent:

(a) The partial order $\leq \lor$ induced by $(L, \lor, \bot)$ coincides with the partial order $\leq \land$ induced by $(L, \land, \top)$.

(b) $(L, \lor, \land, \bot, \top)$ satisfies the two following absorptive laws:

$$a \lor (a \land b) = a$$
$$a \land (a \lor b) = a$$

Proof. Exercise! \qed

As a consequence, if $(L, \lor, \land, \bot, \top)$ satisfies either of the equivalent conditions of Lem. 8.43, then, for $\leq = \leq \land = \leq \lor$, $(L, \leq)$ is a lattice with finite meets given by $(\land, \top)$ and with finite joins given by $(\lor, \bot)$.

Example 8.44. The partial order $(\mathcal{L}(L), \leq)$ is a lattice.

Proof. Exercise! \qed

Definition 8.45 (Lattice (Iso)Morphism). Given lattices $(L, \leq)$ and $(L', \leq')$, a function $f : L \to L'$ is a map of lattices if $f$ is both a map of meet and join semilattices from $(L, \leq)$ to $(L', \leq')$. If moreover $f$ is a bijection then we say that $f$ is an isomorphism of lattices.

Remark 8.46. It directly follows from Lem. 8.37 that $f : L \to L'$ is an isomorphism of lattices if and only if there is a lattice morphism $g : L \to L'$ such that

$$g(f(a)) = a \quad \text{and} \quad f(g(a')) = a' \quad \text{(for all} \ a \in L \ \text{and all} \ a' \in L')$$

Example 8.47. Given a function $f : X \to Y$, the function $f^{-1} : (\mathcal{P}(Y), \subseteq) \to (\mathcal{P}(X), \subseteq)$ of §6.1 is a lattice morphism.

Example 8.48. Given a continuous function $f : (X, \Omega_X) \to (Y, \Omega_Y)$ (Def. 6.2), the function $f^{-1} : (\Omega_Y, \subseteq) \to (\Omega_X, \subseteq)$ is a lattice morphism.

Example 8.49. The function

$$\bigcirc : \mathcal{L}(L) \to \mathcal{L}(L)$$

$$\varphi \mapsto \bigcirc \varphi$$

is a lattice morphism.

Proof. Exercise! \qed

8.2.3 Distributive Lattices

Lemma 8.50. In a lattice $(L, \lor, \land, \bot, \top)$, the following two distributive laws are equivalent:

$$\forall a, b, c \in L, \quad a \land (b \lor c) = (a \land b) \lor (a \land c)$$
$$\forall a, b, c \in L, \quad a \lor (b \land c) = (a \lor b) \land (a \lor c)$$

Proof. Exercise! \qed

43
Definition 8.51 (Distributive Lattice). A lattice is distributive if it satisfies either of the distributive laws of Lem. 8.50.

Example 8.52. Given a set $X$, $(\mathcal{P}(X), \subseteq)$ is a distributive lattice.

Example 8.53. Given a topological space $(X, \Omega)$, $(\Omega, \subseteq)$ is a distributive lattice.

Lemma 8.54. The partial order $(\mathcal{L}(L), \leq)$ is a distributive lattice.

Proof. Exercise!

Definition 8.55 (Distributive Lattice (Iso)Morphism). Given distributive lattices $(L, \leq)$, $(L', \leq')$, a function $f : L \rightarrow L'$ is a map of distributive lattices if $f$ is a map of lattices from $(L, \leq)$ to $(L', \leq')$. If moreover $f$ is a bijection then we say that $f$ is an isomorphism of distributive lattices.

Example 8.56. Given a function $f : X \rightarrow Y$, the function $f^{-1} : (\mathcal{P}(Y), \subseteq) \rightarrow (\mathcal{P}(X), \subseteq)$ of §6.1 is a morphism of distributive lattices.

Example 8.57. Given a continuous function $f : (X, \Omega_X) \rightarrow (Y, \Omega_Y)$ (Def. 6.2), the function $f^{-1} : (\Omega_Y, \subseteq) \rightarrow (\Omega_X, \subseteq)$ is a morphism of distributive lattices.

Example 8.58. The function $\bigcirc : \mathcal{L}(L) \rightarrow \mathcal{L}(L)$ of Ex. 8.49 is a map of distributive lattices.

Definition 8.59. Let $(L, \lor, \land, \bot, \top)$ be a lattice. Given $a \in L$, we say that $c \in L$ is a complement of $a$ whenever both $a \lor c = \top$ and $a \land c = \bot$ hold.

Lemma 8.60. If $(L, \leq)$ is a distributive lattice, then $a \in L$ has at most one complement.

Proof. Exercise!

8.2.4 Boolean Algebras

Definition 8.61 (Boolean Algebra). A Boolean algebra is a distributive lattice in which every element $b$ has a (necessarily unique) complement $\neg b$.

Example 8.62. Given a set $X$, $(\mathcal{P}(X), \subseteq)$ is a Boolean algebra.

As expected, the clopens of a topological space $(X, \Omega)$ form a Boolean algebra. This was the content of Lem. 6.5. We reformulate it in Ex. 8.68 below, using a proper notion of “sub-Boolean algebra”, which essentially corresponds to the usual algebraic notion of “sub-algebra” (see e.g. [BS81, Def. 2.2]).

Example 8.63. The partial order $(\mathcal{L}(L), \leq)$ is a Boolean algebra.

Lemma 8.64 (De Morgan Laws). Every Boolean algebra $(B, \lor, \land, \bot, \top)$ satisfies the following De Morgan Laws:

$$a \land b = \neg (\neg a \lor \neg b) \quad a \lor b = \neg (\neg a \land \neg b) \quad a = \neg \neg a$$

Proof. Exercise!

It would be natural to ask morphisms of Boolean algebra to preserve all the structure (finite meets, joins and complements). But since complements are uniquely determined by finite meets and joins, it they are preserved by lattice morphisms.
Definition 8.65 (Boolean Algebra (Iso)Morphism). Given Boolean algebras \((B, \leq)\) and \((B', \leq')\), a function \(f : B \to B'\) is a map of Boolean algebras if \(f\) is a map of lattices from \((B, \leq)\) to \((B', \leq')\). If moreover \(f\) is a bijection then we say that \(f\) is an isomorphism of Boolean algebras.

Lemma 8.66. If \(f\) is a map of Boolean algebras from \((B, \leq)\) to \((B', \leq')\) then \(f\) preserves complements.

We can now give better statements to Lem. 6.1 and Lem. 6.5 of §6.1.

Example 8.67 (Lem. 6.1). Given a function \(f : X \to Y\), the function \(f^{-1} : (\mathcal{P}(Y), \subseteq) \to (\mathcal{P}(X), \subseteq)\) is a morphism of Boolean algebras.

Example 8.68. Let \((X, \Omega)\) be a topological space.

1. The clopen subsets of \(X\) (ordered by inclusion) form a sub-Boolean algebra of \((\mathcal{P}(X), \subseteq)\) (Lem. 6.5).

2. In particular, if \((X, \Omega)\) is compact Hausdorff, then it follows from Lem. 6.10 and Prop. 6.18 that \((K\Omega, \subseteq)\) is a sub-Boolean algebra of \((\mathcal{P}(X), \subseteq)\).

Example 8.69 (Compact-Open Sets of \(\omega\)-Words). Recall from Lem. 6.10 and Prop. 6.18 that \(K\Omega((2^{AP})^{\omega})\) coincides with the set of clopen subsets of \((2^{AP})^{\omega}\). Hence \(K\Omega((2^{AP})^{\omega})\) is a sub-Boolean algebra of \(\mathcal{P}((2^{AP})^{\omega})\).

Moreover, it follows from Prop. 6.12 and Prop. 6.19 that \([\cdot] : \mathfrak{L}(LML) \to K\Omega((2^{AP})^{\omega}) \varphi \mapsto [\varphi]\) is bijection. It is easy to see that \([\cdot]\) is actually an isomorphism of Boolean algebras.

8.3 Representation of Boolean Algebras

We already know that \(\mathfrak{L}(LML)\) is isomorphic a sub-Boolean algebra of sets, namely as a sub-Boolean algebra of \(\mathcal{P}((2^{AP})^{\omega})\). As alluded to in the introduction of this Section 8, the space \((2^{AP})^{\omega}\) can be exactly described as a space of prime filter over \(\mathfrak{L}(LML)\). This generalizes to any Stone space. We present some basic definitions and facts about filters in §8.3.1 and then turn to the representation of Boolean algebras in §8.3.2.

8.3.1 Filters and Ultrafilters

Definition 8.70 (Filter on a Partial Order). Let \((A, \leq)\) be a partial order. Then \(\mathcal{F} \subseteq A\) is a filter if \(\mathcal{F}\) is:

- upward-closed: if \(a \in \mathcal{F}\) and \(a \leq b\) then \(b \in \mathcal{F}\), and

- codirected: \(\mathcal{F}\) is non-empty and for all \(a, b \in \mathcal{F}\) there is some \(c \in \mathcal{F}\) such that \(c \leq a\) and \(c \leq b\).

Lemma 8.71 (Filter on a Meet Semilattice). Let \((L, \land, \top)\) be a meet semilattice. Then \(\mathcal{F} \subseteq L\) is a filter iff
• $\mathcal{F}$ is upward-closed, and
• $\top \in \mathcal{F}$, and
• $a \land b \in \mathcal{F}$ whenever $a \in \mathcal{F}$ and $b \in \mathcal{F}$.

The notion of prime filter is standard, see e.g. [Joh86, §I.2.1 & I.2.2] or [DP02, Def. 10.7]. Note that [AC98, Def. 10.1.4] uses the terminology “coprime” filter. We stick to the terminology of [DP02, Joh86].

**Definition 8.72** (Prime Filter). Let $(L, \lor, \bot)$ be a join semilattice. A filter $\mathcal{F}$ on $(L, \leq)$ is **prime** if

• $\bot \notin \mathcal{F}$, and
• if $a \lor b \in \mathcal{F}$ then either $a \in \mathcal{F}$ or $b \in \mathcal{F}$.

In other words a filter $\mathcal{F}$ on a lattice $L$ is prime iff for every finite $S \subseteq L$ such that $\bigvee S \in \mathcal{F}$, there is some $s \in S$ such that $s \in \mathcal{F}$.

A filter $\mathcal{F}$ on a lattice $(L, \leq)$ is **proper** if $\bot \notin \mathcal{F}$.

**Definition 8.73** (Ultrafilter). An **ultrafilter** $\mathcal{F}$ on a lattice $L$ is a maximal proper filter, in the sense that for any proper filter $\mathcal{H}$ on $L$ such that $\mathcal{F} \subseteq \mathcal{H}$, we have $\mathcal{H} = \mathcal{F}$.

**Definition 8.74** (Finite Intersection Property). Let $(L, \leq)$ be a lattice. A family of sets $F \subseteq L$ is said to have the **finite intersection property** if $\bigwedge S \neq \bot$ for all finite $S \subseteq F$.

Note that if $F \subseteq L$ has the finite intersection property, then

$$\text{Filt}(F) := \{ a \in L \mid a \geq \bigwedge S \text{ for some finite } S \subseteq F \}$$

is a proper filter containing. Indeed, we cannot have $\bot \in \text{Filt}(F)$ since $F$ has the finite intersection property. Moreover, $\text{Filt}(F)$ is upward-closed. Finally, if $a \geq \bigwedge S_a$ and $b \geq \bigwedge S_b$ for finite $S_a, S_b \subseteq F$, then $a \land b \geq \bigwedge (S_a \cup S_b)$, hence $a \land b \in \text{Filt}(F)$.

The following is [DP02, Thm. 10.11].

**Lemma 8.75.** Let $\mathcal{F}$ be a filter on a distributive lattice. If $\mathcal{F}$ is an ultrafilter, then $\mathcal{F}$ is prime.

**Proof.** Exercise! □

In the case of Boolean algebras, we have the following neat characterization of ultrafilters (see e.g. [DP02, Thm. 10.12]).

**Proposition 8.76.** Let $(B, \leq)$ be a Boolean algebra and let $\mathcal{F} \subseteq B$ be a filter. The following are equivalent:

(a) $\mathcal{F}$ is an ultrafilter.
(b) $\mathcal{F}$ is prime.
(c) for each $a \in B$, we have $\neg a \in \mathcal{F}$ if $a \notin \mathcal{F}$.

**Proof.** Exercise! □
8.3.2 The Spectrum of a Boolean Algebra

Definition 8.77 (Spectrum of a Boolean Algebra (1/2)). Given a Boolean algebra \( B \), we let \( \text{Sp}(B) \) be the set of prime filters on \( B \).

Definition 8.78. Given a Boolean algebra \( B \) and \( a \in B \) we let
\[
\text{ext}(a) := \{ F \in \text{Sp}(B) \mid a \in F \}
\]

Lemma 8.79. Let \((B, \leq)\) be a Boolean algebra. Then we have
\[
\text{ext}(a \land b) = \text{ext}(a) \cap \text{ext}(b)
\]
\[
\text{ext}(a \lor b) = \text{ext}(a) \cup \text{ext}(b)
\]
\[
\text{ext}(\neg a) = \text{Sp}(B) \setminus \text{ext}(a)
\]
\[
\text{ext}(\top) = \text{Sp}(B)
\]
\[
\text{ext}(\bot) = \emptyset
\]

Proof. Exercise! \( \square \)

Definition 8.80 (Spectrum of a Boolean Algebra (2/2)). Given a Boolean algebra \( B \), we equip \( \text{Sp}(B) \) with the topology \( \Omega(\text{Sp}(B)) \) induced by the base \( \mathcal{B} := \{ \text{ext}(a) \mid a \in B \} \). The space \( (\text{Sp}(B), \Omega(\text{Sp}(B))) \) is the spectrum of \( B \).

It follows from Lem. 8.79 that \( \mathcal{B} \) is a sub-Boolean algebra of \( \mathcal{P}(\text{Sp}(B)) \), and that \( \mathcal{B} \) is isomorphic to \( B \). Moreover, since for each \( U \in \mathcal{B} \) we have \( \text{Sp}(B) \setminus U \in \mathcal{B} \), the space \( (\text{Sp}(B), \Omega(\text{Sp}(B))) \) has a basis of clopen sets.

As expected, \( \text{Sp}(B) \) is always a Stone space.

Lemma 8.81. The spectrum \((\text{Sp}(B), \Omega(\text{Sp}(B)))\) of a Boolean algebra \( B \) is \( T_0 \) and zero-dimensional. 

Proof. Exercise! \( \square \)

It remains to show that \( \text{Sp}(B) \) is compact. For this, we rely on the following, sometimes referred to as the ultrafilter lemma.

Lemma 8.82 (Ultrafilter Lemma). Let \((L, \leq)\) be a lattice. If \( F \subseteq L \) has the finite intersection property, then \( F \subseteq F \) for some ultrafilter \( F \) on \( L \).

The Ultrafilter Lemma 8.82 is discussed in §8.3.3 as a consequence of Zorn’s Lemma (an equivalent formulation of the Axiom of Choice).

Lemma 8.83. The spectrum \((\text{Sp}(B), \Omega(\text{Sp}(B)))\) of a Boolean algebra \( B \) is compact. 

Proof. Exercise! \( \square \)

We now state the simplified version of Stone’s Representation Theorem alluded to in the introduction of this Section 8. We refer to [Joh86, Cor. II.4.4] for the full statement of Stone’s Representation Theorem. Recall that it follows from Lem. 6.10, Prop. 6.18 and Lem. 6.5 that for a Stone space \((X, \Omega)\), the set \( K\Omega \) of compacts opens is a sub-Boolean algebra of \( \mathcal{P}(X) \).

Theorem 8.84 (Stone).

(1) Given a Boolean algebra \( B \), the space \((\text{Sp}(B), \Omega(\text{Sp}(B)))\) is a Stone space, and \( B \) is isomorphic to \( K\Omega(\text{Sp}(B)) \) (as Boolean algebras).

(2) Each Stone space \((X, \Omega)\) is homeomorphic to \((\text{Sp}(K\Omega), \Omega(\text{Sp}(K\Omega)))\).

Corollary 8.85. \((2^{\mathcal{P}})^{\omega} \) is homeomorphic to \( \text{Sp}(\mathcal{E}(LML)) \).
8.3.3 On the Proof of The Ultrafilter Lemma 8.82

The Ultrafilter Lemma 8.82 follows from a formulation of the Axiom of Choice known as Zorn’s Lemma. We consider Zorn’s Lemma in the form of [DP02, (ZL), §10.2]. A chain (see e.g. [DP02, §1.3]) in a partial order \((L, \leq)\) is a set \(C \subseteq L\) such that for all \(a, b \in C\), we have \(a \leq b\) or \(b \leq a\).

**Lemma 8.86** (Zorn’s Lemma). Let \((L, \leq)\) be a partial order. If every chain in \(L\) has an upper bound in \(L\), then \(L\) has a maximal element (i.e. some \(a \in L\) such that \(b \leq a\) whenever \(a \leq b\)).

Zorn’s Lemma is equivalent to the Axiom of Choice (see e.g. [DP02, Thm. 10.3]).

**Proof of the Ultrafilter Lemma 8.82.** Exercise!

9 Bisimulation

We essentially follow here [BK08, §7.1], with a few slight changes in notation.

9.1 Bisimulation (with Actions)

We begin with the usual notion.

**Definition 9.1** (Bisimulation). Consider t.s. \(TS_0\) and \(TS_1\) with \(TS_i = (S_i, \text{Act}, \rightarrow_i, I_i, \text{AP}, L_i)\). A bisimulation between \(TS_0\) and \(TS_1\) is a relation \(R \subseteq S_0 \times S_1\) such that for all \((s_0, s_1) \in R\) we have

- \(L_0(s_0) = L_1(s_1)\), and
- for each \(i \in \{0, 1\}\) and each \(\alpha \in \text{Act}_i\), if \(s_i \overset{\alpha_i}{\rightarrow} s'_i\) in \(TS_i\) then there is \(s'_{1-i}\) in \(TS_{1-i}\) such that \(s_{1-i} \overset{\alpha_{1-i}}{\rightarrow} s'_{1-i}\) and \((s'_0, s'_1) \in R\).

Note that in Def. 9.1, \(TS_0\) and \(TS_1\) are required to be over the same sets \(\text{Act}\) and \(\text{AP}\) of actions and atomic propositions.

**Definition 9.2.** We write \(TS_0 \approx TS_1\) if there is a bisimulation \(R \subseteq S_0 \times S_1\) such that moreover

- for each \(i \in \{0, 1\}\), for all \(s_i \in I_i\) there is \(s_{1-i} \in I_{1-i}\) such that \((s_0, s_1) \in R\).

Definition 9.2 corresponds to [BK08, Def. 7.1] (but with a slightly different notation).

**Definition 9.3** (Bisimilarity). Consider transition systems \(TS_0\) and \(TS_1\) as in Def. 9.1. We say that \(s_0 \in S_0\) and \(s_1 \in S_1\) are bisimilar (notation \(s_0 \sim s_1\)) if there is a bisimulation \(R \subseteq S_0 \times S_1\) such that \((s_0, s_1) \in R\). The relation \(\sim\) is called the bisimilarity relation over \(TS_0\) and \(TS_1\).

We now turn to the basic properties of bisimulations.

**Lemma 9.4.**

1. Given a transition system \(TS\), we have \(s \sim s\) for each state \(s\) of \(TS\).

2. Given transition systems \(TS_0\) and \(TS_1\), if \(R\) is a bisimulation between \(TS_0\) and \(TS_1\), then \(R^{-1} = \{(s_1, s_0) \mid (s_0, s_1) \in R\}\) is a bisimulation between \(TS_1\) and \(TS_0\).
(3) Given transitions systems TS$_0$, TS$_1$ and TS$_2$, if $\mathcal{R}$ is a bisimulation between TS$_0$ and TS$_1$ and $\mathcal{T}$ is a bisimulation between TS$_1$ and TS$_2$, then $\mathcal{T} \circ \mathcal{R}$ is a bisimulation between TS$_0$ and TS$_2$, where

$$ \mathcal{T} \circ \mathcal{R} = \{(s_0, s_2) \mid \exists s_1, (s_0, s_1) \in \mathcal{R} \text{ and } (s_1, s_2) \in \mathcal{T}\} $$

Proof. Exercise! \qed

Lemma 9.5.

(1) Given TS$_0$ and TS$_1$, the bisimilarity relation $\sim$ over TS$_0$ and TS$_1$ is a bisimulation between TS$_0$ and TS$_1$.

(2) Given TS$_0$ and TS$_1$, the bisimilarity relation $\sim$ is the coarsest bisimulation between TS$_0$ and TS$_1$ (i.e. given any bisimulation $\mathcal{R}$ between TS$_0$ and TS$_1$, we have $\mathcal{R} \subseteq \sim$).

(3) For every TS, the bisimilarity relation $\sim$ over TS and itself is an equivalence relation.

Proof. Exercise! \qed

9.2 Bisimilarity and Trace Equivalence

It follows from the definition that we have.

Proposition 9.6 ([BK08, Thm. 7.6]). Given TS$_0$ and TS$_1$ over both over AP and Act, if $TS_0 \approx TS_1$ then $Tr^\omega(TS_0) = Tr^\omega(TS_1)$.

Corollary 9.7. Given TS$_0$ and TS$_1$ over both over AP and Act, if $TS_0 \approx TS_1$ then for all LT property $P \subseteq (2^{AP})^\omega$, we have

$$ TS_0 \models P \text{ if and only if } TS_1 \models P $$

In particular, if $TS_0 \approx TS_1$, then for every LTL-formula $\varphi$ we have

$$ TS_0 \models \varphi \text{ if and only if } TS_1 \models \varphi $$

9.3 The Bisimulation Quotient

Given a transition system TS, let $TS_{\sim}$ be the transition system with

- as states the equivalence classes $[s]_{\sim}$ of $\sim$,
- as initial states the equivalence classes of initial states of TS,
- as transitions, we let $[s]_{\sim} \xrightarrow{\alpha} [s']_{\sim}$ if $s \xrightarrow{\alpha} s'$,
- as labeling, note that if $s \sim t$ then $L(s) = L(t)$, so that we can put $L([s]_{\sim}) := L(s)$.

Lemma 9.8. $TS \approx TS_{/\sim}$.

Proof. Exercise! \qed
10 On Modal Logics of Transition Systems

In this Section, we study a modal logic on transition systems (in the sense of §2 and [BK08, Def. 2.1]) which properly deals with their transition structure. We consider here the Hennessy-Milner Logic (HML). We loosely follow [Sti11] for the presentation of HML and [BdRV02] for the general theory of modal logic.

Kripke Frames and Models

The tradition of modal logic (in the sense of e.g. [BdRV02, Chap. 1]) leads us to distinguish the following structure in a transition system $TS = (S, \text{Act}, \rightarrow, I, \text{AP}, L)$:

- a transition structure given by $(S, (\overset{\alpha}{\rightarrow})_{\alpha \in \text{Act}})$,
- a logical (model) structure given by the state labelling $L : S \rightarrow \mathcal{P}(\text{AP})$,
- a “pointed” structure given by the initial states $I \subseteq S$.

We use the following adaptation of the notions of [BdRV02, Chap. 1].

**Definition 10.1** (Kripke Frame and Model). Fix Act and AP.

- A Kripke frame over Act is given by a set of states $S$ together with a relation $\rightarrow \subseteq S \times \text{Act} \times S$.
- A Kripke model over Act and AP is given by a Kripke frame $(S, \text{Act}, \rightarrow)$ together with a state labelling $L : S \rightarrow \mathcal{P}(\text{AP})$.

A t.s. is thus a Kripke model $(S, \text{Act}, \rightarrow, \text{AP}, L)$ equipped with a set of initial states $I \subseteq S$.

10.1 Syntax and Semantics of HML

Fix a set AP of atomic propositions and a set Act of actions. The formulae of HML are given by the following grammar:

$$
\varphi, \psi ::= \top \mid \bot \mid a \quad (\text{where } a \in \text{AP}) \\
\mid \varphi \land \psi \mid \varphi \lor \psi \mid \neg \varphi \\
\mid [\alpha] \varphi \mid \langle \alpha \rangle \varphi \quad (\text{where } \alpha \in \text{Act})
$$

**Notation 10.2.** Other propositional connectives are defined as usual (see also Notation 7.2, §7.1.1):

$$
\varphi \rightarrow \psi ::= \neg \varphi \lor \psi \\
\varphi \leftrightarrow \psi ::= (\varphi \rightarrow \psi) \land (\psi \rightarrow \varphi)
$$

Consider a transition system $TS = (S, \text{Act}, \rightarrow, I, \text{AP}, L)$. The interpretation $[\varphi] \in \mathcal{P}(S)$ of an HML-formula $\varphi$ is defined by induction on $\varphi$ as follows:

$$
[\top] ::= S \\
[\bot] ::= \emptyset \\
[\varphi \land \psi] ::= [\varphi] \cap [\psi] \\
[\varphi \lor \psi] ::= [\varphi] \cup [\psi] \\
[\neg \varphi] ::= S \setminus [\varphi] \\
[\alpha] \varphi ::= \{ s \in S \mid \forall s' \in S, \text{ if } s \overset{\alpha}{\rightarrow} s' \text{ then } s' \in [\varphi] \} \\
\langle \alpha \rangle \varphi ::= \{ s \in S \mid \exists s' \in S, \text{ if } s \overset{\alpha}{\rightarrow} s' \text{ and } s' \in [\varphi] \}
$$

50
The following usual notions are presented e.g. in [BdRV02, §1.3] (with slight variations in notation).

**Definition 10.3** (Modal Satisfaction Relations). Consider a t.s. $TS = (S, \text{Act}, \rightarrow, I, \text{AP}, L)$ and an HML-formula $\varphi$.

1. We say that a state $s \in S$ satisfies $\varphi$ (notation $s \models \varphi$) if $s \in \llbracket \varphi \rrbracket$ ([BdRV02, Def. 1.20]).
2. We say that $TS$ satisfies $\varphi$ (notation $TS \models \varphi$) if $s \in \llbracket \varphi \rrbracket$ for all $s \in S$ ([BdRV02, Def. 1.21]).

We say that $\varphi$ is valid (notation $\models \varphi$) is $TS \models \varphi$ for every transition system $TS$ (over Act and AP).

**Remark 10.4.** We shall be mostly concerned with the local satisfaction relation $\models$. The notion of satisfaction in a given t.s. ($TS \models \varphi$) only interests us as a means to define logical validity $\models \varphi$. As a consequence, we shall not bother in seriously considering the possible notion $TS \models \varphi$ iff $\forall s \in I, s \models \varphi$ since it would induce the same notion of logical validity (by changing initial states of t.s.'s).

**Remark 10.5.** Similarly as with LML (Rem. 7.6, §7.1.1) and LTL (§7.3.1), we can give an inductive characterization of the relation $s \models \varphi$ (s forces $\varphi$):

\[
\begin{align*}
s \models a & \quad \text{iff} \quad a \in L(s) \\
s \models \top & \\
s \not\models \bot & \\
s \models \varphi \land \psi & \quad \text{iff} \quad s \models \varphi \text{ and } s \models \psi \\
s \models \varphi \lor \psi & \quad \text{iff} \quad s \models \varphi \text{ or } s \models \psi \\
s \models \neg \varphi & \quad \text{iff} \quad s \not\models \varphi \\
s \models [\alpha] \varphi & \quad \text{iff} \quad \text{for all } s' \in S \text{ such that } s \xrightarrow{\alpha} s', \text{ we have } s' \models \varphi \\
s \models \langle \alpha \rangle \varphi & \quad \text{iff} \quad \text{there is some } s' \in S \text{ such that } s \xrightarrow{\alpha} s' \text{ and } s' \models \varphi
\end{align*}
\]

**Remark 10.6.** One gets the usual basic modal logic by taking $\text{Act} = 1$ (see e.g. [BdRV02, Def. 1.9]).

**Example 10.7** (LML as an instance of HML). Fix $\text{Act} = \{\bullet\}$. We define the following Kripke model $M((2^{\text{AP}})^\omega)$ on streams:

\[
M((2^{\text{AP}})^\omega) := ((2^{\text{AP}})^\omega, \text{Act}, \rightarrow, \text{AP}, L)
\]

where

\[
\begin{align*}
\sigma \xrightarrow{\bullet} \beta & \quad \text{iff} \quad \beta = \sigma[1] \\
\alpha \in L(\sigma) & \quad \text{iff} \quad a \in \sigma(0)
\end{align*}
\]

Then for all HML-formula $\varphi$ and each $\sigma \in (2^{\text{AP}})^\omega$, we have

\[
\sigma \models \langle \bullet \rangle \varphi \quad \text{iff} \quad \sigma[1] \models \varphi
\]

Hence both modalities $\langle \bullet \rangle$ and $[\bullet]$ collapse to the $\circ$ modality of LML. It is then easy to see that HML and LML have the same expressive power over $M((2^{\text{AP}})^\omega)$.

Moreover, two streams $\sigma, \beta \in (2^{\text{AP}})^\omega$ are bisimilar iff they are equal.

**Proof.** Exercise!
10.2 Logical Equivalence

We shall consider two notions of logical equivalence with HML, first the logical equivalence of formulae, similar to that of LML and LTL seen in §7, and second the logical equivalence of states of transition systems.

10.2.1 Logical Equivalence on Formulae

Similarly as with LML and LTL, HML has a notion of logical equivalence on formulae.

**Definition 10.8 (Logical Equivalence on Formulae).** Two HML-formulae \( \varphi \) and \( \psi \) are logically equivalent (notation \( \varphi \equiv \psi \)), if \( \models \varphi \leftrightarrow \psi \).

Hence \( \varphi \equiv \psi \) iff \( TS \models \varphi \leftrightarrow \psi \) for every t.s. \( TS \). But this is equivalent to \( \left[ \varphi \right] = \left[ \psi \right] \) within every transition system \( TS \).

**Lemma 10.9.** We have \( \varphi \equiv \psi \) iff for every t.s. \( TS = (S, \text{Act}, \rightarrow, I, \text{AP}, L) \) and all \( s \in S \),

\[
 s \models \varphi \iff s \models \psi 
\]

*Proof.* Exercise!

**Lemma 10.10.** We have, for \( \alpha \in \text{Act} \),

\[
\langle \alpha \rangle \varphi \equiv \neg[\alpha] \neg \varphi \\
[\alpha] \varphi \equiv \neg(\alpha) \neg \varphi
\]

as well as

\[
\langle \alpha \rangle (\varphi \lor \psi) \equiv \langle \alpha \rangle \varphi \lor \langle \alpha \rangle \psi \\
[\alpha] (\varphi \land \psi) \equiv [\alpha] \varphi \land [\alpha] \psi
\]

10.2.2 Logical Equivalence on States and Bisimilarity

In HML, it is pertinent to consider a notion of logical equivalence on states of transition systems.

**Definition 10.11.** Consider \( TS_0 \) and \( TS_1 \) with \( TS_i = (S_i, \text{Act}, \rightarrow_i, I_i, \text{AP}, L_i) \). We say that \( s_0 \in S_0 \) and \( s_1 \in S_1 \) are logically equivalent (notation \( s_0 \equiv s_1 \)) if for all HML-formula \( \varphi \) we have

\[
 s_0 \models \varphi \iff s_1 \models \varphi 
\]

As expected for a modal logic, bisimilarity of states implies logical equivalence w.r.t. HML.

**Theorem 10.12 ([BdRV02, Thm. 2.20 p. 67]).** If \( s_0 \sim s_1 \), then \( s_0 \equiv s_1 \).

*Proof.* Exercise!

10.3 The Hennessy-Milner Property

We shall look for (partial) converses to Thm. 10.12, i.e. for sufficient conditions on a class \( \mathcal{M} \) of t.s.'s (over fixed Act and AP) such that given \( TS_0, TS_1 \in \mathcal{M} \) and \( s_0 \in S_0, s_1 \in S_1 \), we have

\[
 s_0 \sim s_1 \iff s_0 \equiv s_1 
\]

This property is called the Hennessy-Milner property for \( \mathcal{M} \) (see e.g. [BdRV02, Def. 2.52 p. 92] or [Sti11]). As the shown by Ex. 10.13 below, the class \( \mathcal{T} \) of all transition systems (over fixed Act and AP) does not have the Hennessy-Milner property.
Example 10.13 ([BdRV02, Ex. 2.23 & Fig. 2.5]). Assume Act = 1 and AP = \{a\}. Consider the transition system

Then we have \( s_0 \equiv s_1 \) but \( s_0 \not\sim s_1 \).

Note that the Hennessy-Milner property for a class \( \mathcal{M} \) of t.s.'s is equivalent to the following condition:

- Given \( TS_0, TS_1 \in \mathcal{M} \), the logical equivalence relation on states \( \equiv \subseteq S_0 \times S_1 \) is a bisimulation.

It is well-known that the class of image finite transition systems has the Hennessy-Milner property. This is result is known as the Hennessy-Milner Theorem (see e.g. [BdRV02, Thm. 2.24, p. 69] or [Sti11, Thm. 1.2.3 & Thm. 1.2.4]).

Definition 10.14 (Image Finite T.S.). We say that \( TS \) is image finite if for every \( s \in S \) and \( \alpha \in \text{Act} \), the set

\[
\text{Succ}^\alpha(s) := \{ s' \in S \mid s \xrightarrow{\alpha} s' \}
\]

of \( \alpha \)-successors of \( s \) is finite.

Proposition 10.15 (Hennessy-Milner Theorem). If \( TS_0 \) and \( TS_1 \) (both over \( \text{AP} \) and \( \text{Act} \)) are image finite, then for all \( (s_0, s_1) \in S_0 \times S_1 \) we have

\[
s_0 \sim s_1 \iff s_0 \equiv s_1
\]

We refer to e.g. [Sti11, Thm. 1.2.4] for a direct proof of Prop. 10.15. In §10.4 we prove Prop. 10.15 using the model-theoretic notion of modal saturation. This notion paves the way toward the main construction and result of this Section 10, namely that for each transition system \( TS \), there is a (modally saturated) transition system \( \text{uf}(TS) \) (called the ultrafilter extension of \( TS \)) and a function \( \pi : S_{TS} \to S_{\text{uf}(TS)} \) such that

\[
s_0 \equiv s_1 \iff \pi(s_0) \sim \pi(s_1)
\]

10.4 Modal Saturation

We follow [BdRV02, §2.5 p. 91].

Definition 10.16. Let \( TS = (S, \text{Act}, \xrightarrow{\cdot}, I, \text{AP}, L) \).

(1) Given a set of states \( T \subseteq S \), a set of formulae \( \Phi \) is satisfiable in \( T \) if there is a state \( s \in T \) such that \( s \models \varphi \) for all \( \varphi \in \Phi \).
Given a set of states $T \subseteq S$, a set of formulae $\Phi$ is \textbf{finitely satisfiable} in $T$ if every finite subset of $\Phi$ is satisfiable in $T$.

$TS$ is \textbf{modally saturated} if for every state $s$, every $\alpha \in \text{Act}$, and every set of formulae $\Phi$, if $\Phi$ is finitely satisfiable in the set of $\alpha$-successors of $s$, then $\Phi$ is satisfiable in the set of $\alpha$-successors of $s$.

\textbf{Proposition 10.17.} If $TS$ is image finite, then $TS$ is modally saturated.

\textit{Proof.} Exercise! \hfill $\square$

The following Prop. 10.18 and Cor. 10.19 are gathered in [BdRV02, Prop. 2.54, p. 93].

\textbf{Proposition 10.18.} If $TS_0$ and $TS_1$ are modally saturated, then $\equiv$ is a bisimulation between $TS_0$ and $TS_1$.

\textit{Proof.} Exercise! \hfill $\square$

\textbf{Corollary 10.19.} If $TS_0$ and $TS_1$ are modally saturated, then for every $(s_0, s_1) \in S_0 \times S_1$, we have

$$s_0 \sim s_1 \iff s_0 \equiv s_1$$

Proposition 10.15 is a direct consequence of Prop. 10.17 and Cor. 10.19.

## 10.5 Boolean Algebras with Operators

Similarly as in Def. 8.4 (§8) we write $\mathcal{L}(HML)$ for the set of HML-formulae (over fixed Act and AP) quotiented by the logical equivalence relation $\equiv$ of Def. 10.8 (§10.1). Then writing $\varphi$ for $[\varphi] \equiv \in \mathcal{L}(HML)$ (as in Notation 8.5), the relation

$$\varphi \leq \psi \coloneqq (\varphi \rightarrow \psi) \equiv \top$$

(see §8) is a partial order on $\mathcal{L}(HML)$, and moreover $(\mathcal{L}(HML), \leq)$ is a Boolean algebra. Similarly as in §8, for a transition system $TS = (S, \text{Act, } \rightarrow, I, \text{AP}, L)$ the map

$$[-] : \mathcal{L}(HML) \rightarrow \mathcal{P}(S) \quad \varphi \mapsto [\varphi]$$

is a morphism of Boolean algebras.

We shall now see an algebraic approach to HML via the notion of \textbf{Boolean Algebra with Operators} (BAO). While this fits quite well in the general setting of Stone Duality (see e.g. [BdRV02, Chap. 5]), we follow here a more naive approach.

\textbf{Definition 10.20.} Given a transition system $TS = (S, \text{Act, } \rightarrow, I, \text{AP, } L)$ and $\alpha \in \text{Act}$, define

$$[[\langle \alpha \rangle ]] : \mathcal{P}(S) \rightarrow \mathcal{P}(S)$$

$$A \mapsto \{ s \in S \mid \exists s' \in \text{Succ}^\alpha(s), \ s' \in A \}$$

$$[[[\alpha]]] : \mathcal{P}(S) \rightarrow \mathcal{P}(S)$$

$$A \mapsto \{ s \in S \mid \forall s' \in \text{Succ}^\alpha(s), \ s' \in A \}$$

Then we of course have

$$[[\langle \alpha \rangle \varphi]] = [[\langle \alpha \rangle] [[\varphi]]]$$

$$[[[\alpha] \varphi]] = [[[\alpha]] [[\varphi]]]$$

Moreover:
Lemma 10.21. Consider a transition system $TS = (S, Act, \rightarrow, I, AP, L)$ and let $\alpha \in Act$.

1. The function $[[\alpha]] : \mathcal{P}(S) \rightarrow \mathcal{P}(S)$ is a map of join semilattices.
2. The function $[\alpha] : \mathcal{P}(S) \rightarrow \mathcal{P}(S)$ is a map of meet semilattices.

Proof. Exercise!

Lemma 10.10 gives a similar situation for $\mathcal{L}(HML)$.

Lemma 10.22. Fix some $\alpha \in Act$.

1. The function $\langle \alpha \rangle : \mathcal{L}(HML) \rightarrow \mathcal{L}(HML)$
   
   $\varphi \mapsto \langle \alpha \rangle \varphi$

   is a map of join semilattices.

2. The function $[\alpha] : \mathcal{L}(HML) \rightarrow \mathcal{L}(HML)$
   
   $\varphi \mapsto [\alpha] \varphi$

   is a map of meet semilattices.

Proof. Exercise!

Of course, the maps $[[\langle \alpha \rangle]]$ and $[[[\alpha]]]$ (as well as $\langle \alpha \rangle$ and $[\alpha]$ over $\mathcal{L}(HML)$) are interdefinable. Let us elaborate a bit on this.

Definition 10.23. Given Boolean algebras $B, B'$ and a function $f : B \rightarrow B'$, the dual of $f$ is the function

$f^\partial : B \rightarrow B'$

$b \mapsto \lnot f(\lnot b)$

Lemma 10.24. Consider a transition system $TS = (S, Act, \rightarrow, I, AP, L)$ and let $\alpha \in Act$. Then

$[[[\alpha]]] = [[\langle \alpha \rangle]]^\partial$

$[[\langle \alpha \rangle]] = [[[\alpha]]]^{\partial}$

Proof. Exercise!

Lemma 10.25. Given $\alpha \in Act$, in $(\mathcal{L}(HML), \leq)$ we have

$[\alpha] = \langle \alpha \rangle^{\partial}$

$\langle \alpha \rangle = [\alpha]^{\partial}$

Proof. Exercise!


1. We have $f^{\partial \partial} = f$.

2. If $f$ is a map of join (resp. meet) semilattices, then $f^\partial$ is a map of meet (resp. join) semilattices.

3. If $f$ is a map of lattices, then $f^\partial = f$. 55
Proof. Exercise!

There are two equivalent presentations of Boolean Algebra with Operators (BAO) in the literature. The first one consists of a Boolean algebra $B$ together with maps of join semilattices $B \to B$. The second one consists of a Boolean algebra $B$ together with maps of meet semilattices $B \to B$. These two notions are equivalent by Lem. 10.26. We choose the first option as it is the one adopted in [BdRV02]. In the context of HML, this leads to the following notion.

**Definition 10.27** (Boolean Algebra with Operators). A Boolean algebra with operators (BAO) $B^+$ of type $\text{Act}$ is a Boolean algebra $B$ equipped with a family $(f_\alpha)_{\alpha \in \text{Act}}$ of join semilattice morphisms $f_\alpha : B \to B$.

**Example 10.28.** $L(HML)^+ := (L(HML), (\langle \alpha \rangle)_{\alpha \in \text{Act}})$ is a BAO of type $\text{Act}$.

**Example 10.29.** Given a Kripke frame $K = (S, \text{Act}, \to)$, $K^+ := (P(S), (\langle \langle \alpha \rangle \rangle)_{\alpha \in \text{Act}})$ is a BAO of type $\text{Act}$.

The crux of the algebraic approach to modal logic is that one can go the other way around. The following is the adaptation of [BdRV02, Def. 5.40, §5.3] to HML.

**Definition 10.30** (Ultrafilter Frames). Given a BAO $B^+ = (B, (f_\alpha)_{\alpha \in \text{Act}})$, the ultrafilter frame $\mathcal{Uf}(B)$ is defined as

$$\mathcal{Uf}(B^+) := (\text{Sp}(B), \text{Act}, \to)$$

where:

- $\text{Sp}(B)$ is the set of ultrafilters (or equivalently prime filters) over $B$ (see §8.3.1),
- given $\mathcal{F}, \mathcal{H} \in \text{Sp}(B)$ and $\alpha \in \text{Act}$, we have

$$\mathcal{F} \xrightarrow{\alpha} \mathcal{H} \iff \forall b \in B, b \in \mathcal{H} \implies f_\alpha(b) \in \mathcal{F}$$

**Lemma 10.31.** Consider a BAO $B^+ = (B, (f_\alpha)_{\alpha \in \text{Act}})$. In the ultrafilter frame $\mathcal{Uf}(B^+)$, given $\alpha \in \text{Act}$ and $\mathcal{F}, \mathcal{H} \in \text{Sp}(B)$ we have

$$\mathcal{F} \xrightarrow{\alpha} \mathcal{H} \iff \forall b \in B, f_\alpha^0(b) \in \mathcal{F} \implies b \in \mathcal{H}$$

**Proof.** Exercise! □

We refer to e.g. [BdRV02] (and in particular to [BdRV02, Chap. 5]) for uses of this construction (and in particular in the context of Stone duality). We shall just see in §10.6 how this construction, applied to the BAO $(\mathcal{P}(S), (\langle \alpha \rangle)_{\alpha \in \text{Act}})$ of a transition system $TS = (S, \text{Act}, \to, I, \text{AP}, L)$, induces a transition system with the Hennessy-Milner property.

### 10.6 Ultrafilter Extensions of Transition Systems

The ultrafilter frame construction of Def. 10.30 turns a BAO into a frame. If one starts from the BAO $K^+$ induced by the frame structure $K$ of a transition system $TS$, we can extend $\mathcal{Uf}(K^+)$ to a transition system $\mathcal{Uf}(TS)$, the ultrafilter extension of $TS$, which is modally saturated (and in particular satisfies the Hennessy-Milner property). We essentially follow [BdRV02, §2.5].

We take the material of §8.3.1 for granted. We begin by specializing it to ultrafilters over powerset algebras.
Definition 10.32. Let $X$ be a set.

(1) A (proper) filter on $X$ is a (proper) filter on $(\mathcal{P}(X), \subseteq)$.

(2) An ultrafilter on $X$ is an ultrafilter (or equivalently a prime filter) on $(\mathcal{P}(X), \subseteq)$. We write $\mathcal{Uf}(X)$ for the set of ultrafilters on $X$.

Hence $\mathcal{Uf}(X) = \text{Sp}(\mathcal{P}(X), \subseteq)$.

Lemma 10.33. Let $X$ be a set. If $G \subseteq \mathcal{P}(X)$ has the finite intersection property, then

$$F := \bigcap \{E \mid E \text{ is a proper filter } \supseteq G\}$$

is a proper filter.

Proof. Exercise! \hfill \square

Example 10.34.

(1) For each $x \in X$, the principal ultrafilter on $x$ is the ultrafilter

$$\pi(x) := \{A \in \mathcal{P}(X) \mid x \in A\}$$

(2) If $X$ is a finite set, then the ultrafilters on $X$ are exactly the principal filters on $X$. In particular, $\mathcal{Uf}(X)$ is in bijection with $X$.

Proof. Exercise! \hfill \square

(3) It follows from the Ultrafilter Lemma 8.82 that every family $G \subseteq \mathcal{P}(X)$ with the finite intersection property is contained in an ultrafilter.

(4) This in particular gives ultrafilters of co-finite sets (for $X$ infinite), namely ultrafilters $F$ containing all $A \subseteq X$ such that $X \setminus A$ is finite.

We now use the technique of ultrafilter extension of a transition system $TS$ in order to produce modally saturated models. In the following, we assume that the labelings $L : S \to \mathcal{P}(\text{AP})$ are described by their transpose $V : \text{AP} \to \mathcal{P}(S)$ (where $s \in V(a)$ iff $a \in L(s)$).

Definition 10.35 (Ultrafilter Extension of a TS). Consider a t.s. $TS = (S, \text{Act}, \to, I, \text{AP}, L)$. The ultrafilter extension of $TS$ is the transition system $\mathcal{Uf}(TS)$ over $\text{AP}$ and $\text{Act}$ with

- as state set the set $\mathcal{Uf}(S)$ of ultrafilters on $S$,
- as transition relation, $\mathcal{F} \xrightarrow{\alpha} \mathcal{H}$ iff $\llbracket (\alpha) \rrbracket(A) \in \mathcal{F}$ whenever $A \in \mathcal{H}$,
- as state labelling, the map taking $a \in \text{AP}$ to the set of ultrafilters $\mathcal{F}$ such that $V(a) \in \mathcal{F}$,
- as initial states the set $\{\pi(s) \mid s \in I\}$.

Hence the Kripke frame part of $\mathcal{Uf}(TS)$ is the ultrafilter frame $\mathcal{Uf}(S, \text{Act}, \to)$ in the sense of Def. 10.30. In particular, Lem. 10.31 specializes to the following.

Lemma 10.36. Consider a t.s. $TS = (S, \text{Act}, \to, I, \text{AP}, L)$. Then, in $\mathcal{Uf}(TS)$ we have

$$\mathcal{F} \xrightarrow{\alpha} \mathcal{H} \iff \forall A \in \mathcal{P}(S), \llbracket (\alpha) \rrbracket(A) \in \mathcal{F} \implies A \in \mathcal{H}$$
Proof. By Lem. 10.31 and Lem. 10.24.

Example 10.37. Consider a transition system $TS = (S, \text{Act}, \rightarrow, I, \text{AP}, L)$ with finite set of states $S$. It follows from Ex. 10.34.(2) that $Uf(TS)$ has a finite set of states $Uf(S) \simeq S$ (via $\pi$).

Moreover:

- Given $s \in S$ and $a \in \text{AP}$, we have $a \in L(s)$ in $TS$ if and only if $a \in L(\pi(s))$ in $Uf(TS)$.
  
  Proof. Exercise!

- Given $s, s' \in S$ and $\alpha \in \text{Act}$, we have $s \overset{\alpha}{\rightarrow} s'$ in $TS$ if and only if $\pi(s) \overset{\alpha}{\rightarrow} \pi(s')$ in $Uf(TS)$.
  
  Proof. Exercise!

Notation 10.38. In the following, given a transition system $TS$ and its ultrafilter extension $Uf(TS)$, with $J - K$ we always refer to the semantics of HML in $TS$ rather than in $Uf(TS)$.

Recall the map $\text{ext}$ of Def. 8.78 (§8.3.2). In the case of a Boolean algebra of the form $(\mathcal{P}(X), \subseteq)$ for some set $X$, we have

$$\text{ext} : \mathcal{P}(X) \rightarrow \mathcal{P}(Uf(X))$$

In particular, given a transition system $TS$ with state set $S$, $\text{ext}(\varphi) \in \mathcal{P}(Uf(S))$ for each HML-formula $\varphi$.

Proposition 10.39. Let $TS = (S, \text{Act}, \rightarrow, I, \text{AP}, L)$. Then, for all $F \in Uf(S)$ and all HML-formula $\varphi$, we have

$$F \models \varphi \iff F \in \text{ext}(\varphi)$$

Proof. Exercise!

Corollary 10.40. Let $TS = (S, \text{Act}, \rightarrow, I, \text{AP}, L)$. Then, for every HML-formula $\varphi$ we have

$$\forall s \in S (s \models \varphi \iff \pi(s) \models \varphi)$$

$$TS \models \varphi \iff Uf(TS) \models \varphi$$

Proof. Exercise!

Remark 10.41. Since the initial states of $Uf(TS)$ are exactly the $\pi(s)$ for $s$ initial in $TS$, Cor. 10.40 extends to the notion $\models^1$ of Rem. 10.4 as

$$TS \models^1 \varphi \iff Uf(TS) \models^1 \varphi$$

Proposition 10.42. Let $TS = (S, \text{Act}, \rightarrow, I, \text{AP}, L)$. Then $Uf(TS)$ is modally saturated.

Proof. Exercise!

Corollary 10.43. Given transition systems $TS_0$ and $TS_1$, both over AP and Act, for all $(s_0, s_1) \in S_0 \times S_1$ we have

$$s_0 \equiv s_1 \iff \pi(s_0) \sim \pi(s_1)$$
References


Contents

1 Introduction 1

2 Transition Systems 1

3 Linear-Time Properties 2
  3.1 Linear-Time Behaviour of Transition Systems ................. 2
  3.2 Safety Properties and Invariants ................................. 3
    3.2.1 Invariants .................................................. 3
    3.2.2 Safety Properties .............................................. 3
    3.2.3 Regular Safety Properties .................................... 3
    3.2.4 Safety Properties and Trace Equivalence ..................... 4
    3.2.5 Proof of Proposition 3.13 ................................... 5
  3.3 Liveness Properties ................................................ 6
  3.4 Safety vs Liveness .................................................. 7

4 Topological Approach 7
  4.1 Generalities ......................................................... 7
    4.1.1 Adherence ....................................................... 8
    4.1.2 The Topological Decomposition Theorem ....................... 9
    4.1.3 Bases and Subbases .......................................... 9
  4.2 Spaces of $\omega$-Words ........................................... 10
    4.2.1 Topological Safety and Liveness ............................ 11

5 Partial Orders and Complete Lattices 11
  5.1 Partial Orders ...................................................... 11
  5.2 Complete Lattices ................................................. 12
  5.3 Closure Operators .................................................. 13
  5.4 Galois Connections ................................................ 14
  5.5 Prefix and Closure ................................................. 15
    5.5.1 Alternative Proof of the Decomposition Theorem 3.19 ....... 16
  5.6 Further Properties of Closure Operators and Galois Connections .. 16
    5.6.1 On the Kleisli Construction ................................ 17

6 Observable Properties 17
  6.1 Observable Properties as Clopen Sets ............................ 17
  6.2 Compactness ........................................................ 19
    6.2.1 The Finite Intersection Property ............................ 20
  6.3 Compact Hausdorff Spaces ....................................... 20

7 Linear Temporal Logic 21
  7.1 The Logic LML of Observable Properties .......................... 21
    7.1.1 Syntax and Semantics of LML ................................. 21
    7.1.2 Logical Equivalence ........................................ 22
    7.1.3 Observable Properties ....................................... 23
  7.2 Extending LML with Fixpoints .................................... 25
    7.2.1 The “Eventually” and “Always” Modalities ................... 25
    7.2.2 Positive and Negative Variables in a Formula .............. 26
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.2.3</td>
<td>The Knaster-Tarski Fixpoint Theorem</td>
<td>27</td>
</tr>
<tr>
<td>7.3</td>
<td>The Logic LTL</td>
<td>28</td>
</tr>
<tr>
<td>7.3.1</td>
<td>Syntax and Semantics of LTL</td>
<td>28</td>
</tr>
<tr>
<td>7.3.2</td>
<td>Fixpoints and Defined Modalities</td>
<td>29</td>
</tr>
<tr>
<td>7.3.3</td>
<td>Logical Equivalence</td>
<td>30</td>
</tr>
<tr>
<td>7.3.4</td>
<td>Positive Normal Forms</td>
<td>30</td>
</tr>
<tr>
<td>7.3.5</td>
<td>Satisfaction of LTL-Formulae by Transition Systems</td>
<td>31</td>
</tr>
<tr>
<td>7.4</td>
<td>Fixpoints of Scott-Continuous Functions</td>
<td>31</td>
</tr>
<tr>
<td>7.4.1</td>
<td>Scott-Continuity</td>
<td>32</td>
</tr>
<tr>
<td>7.4.2</td>
<td>Application to LML</td>
<td>33</td>
</tr>
<tr>
<td>7.4.3</td>
<td>A Warning on Scott-Continuity for LML-Formulae</td>
<td>34</td>
</tr>
<tr>
<td>8</td>
<td>Toward Stone Duality</td>
<td>35</td>
</tr>
<tr>
<td>8.1</td>
<td>A Short Path Toward a Simplified Result</td>
<td>37</td>
</tr>
<tr>
<td>8.1.1</td>
<td>From Lattices to Boolean Algebras</td>
<td>37</td>
</tr>
<tr>
<td>8.1.2</td>
<td>Filters and Ultrafilters</td>
<td>38</td>
</tr>
<tr>
<td>8.1.3</td>
<td>The Spectrum of a Boolean Algebra</td>
<td>38</td>
</tr>
<tr>
<td>8.1.4</td>
<td>Proof of the Ultrafilter Lemma 8.16</td>
<td>39</td>
</tr>
<tr>
<td>8.2</td>
<td>Lattices and Boolean Algebras</td>
<td>39</td>
</tr>
<tr>
<td>8.2.1</td>
<td>Semilattices</td>
<td>39</td>
</tr>
<tr>
<td>8.2.2</td>
<td>Lattices</td>
<td>42</td>
</tr>
<tr>
<td>8.2.3</td>
<td>Distributive Lattices</td>
<td>43</td>
</tr>
<tr>
<td>8.2.4</td>
<td>Boolean Algebras</td>
<td>44</td>
</tr>
<tr>
<td>8.3</td>
<td>Representation of Boolean Algebras</td>
<td>45</td>
</tr>
<tr>
<td>8.3.1</td>
<td>Filters and Ultrafilters</td>
<td>45</td>
</tr>
<tr>
<td>8.3.2</td>
<td>The Spectrum of a Boolean Algebra</td>
<td>47</td>
</tr>
<tr>
<td>8.3.3</td>
<td>On the Proof of The Ultrafilter Lemma 8.82</td>
<td>48</td>
</tr>
<tr>
<td>9</td>
<td>Bisimulation</td>
<td>48</td>
</tr>
<tr>
<td>9.1</td>
<td>Bisimulation (with Actions)</td>
<td>48</td>
</tr>
<tr>
<td>9.2</td>
<td>Bisimilarity and Trace Equivalence</td>
<td>49</td>
</tr>
<tr>
<td>9.3</td>
<td>The Bisimulation Quotient</td>
<td>49</td>
</tr>
<tr>
<td>10</td>
<td>On Modal Logics of Transition Systems</td>
<td>50</td>
</tr>
<tr>
<td>10.1</td>
<td>Syntax and Semantics of HML</td>
<td>50</td>
</tr>
<tr>
<td>10.2</td>
<td>Logical Equivalence</td>
<td>52</td>
</tr>
<tr>
<td>10.2.1</td>
<td>Logical Equivalence on Formulae</td>
<td>52</td>
</tr>
<tr>
<td>10.2.2</td>
<td>Logical Equivalence on States and Bisimilarity</td>
<td>52</td>
</tr>
<tr>
<td>10.3</td>
<td>The Hennessy-Milner Property</td>
<td>52</td>
</tr>
<tr>
<td>10.4</td>
<td>Modal Saturation</td>
<td>53</td>
</tr>
<tr>
<td>10.5</td>
<td>Boolean Algebras with Operators</td>
<td>54</td>
</tr>
<tr>
<td>10.6</td>
<td>Ultrafilter Extensions of Transition Systems</td>
<td>56</td>
</tr>
</tbody>
</table>