Semantics & Verification

Course Notes

Colin Riba
ENS de Lyon, Université de Lyon, LIP[*]
`colin.riba@ens-lyon.fr`
http://perso.ens-lyon.fr/colin.riba/

March 5, 2024

[*] Univ Lyon, EnsL, UCBL, CNRS, LIP, F-69342, LYON Cedex 07, France

Contents

1 Introduction 4

1.1 Notational Preliminaries . . . 4

2 Transition Systems 5

3 Linear-Time Properties 6

3.1 Linear-Time Behaviour of Transition Systems . . . 7

3.2 Safety Properties and Invariants . . . 9

3.2.1 Invariants . . . 9

3.2.2 Safety Properties . . . 10

3.2.3 Regular Safety Properties . . . 11

3.2.4 Safety Properties and Trace Equivalence . . . 12

3.2.5 Kőnig's Lemma . . . 15

3.2.6 Proof of Proposition 3.27 . . . 17

3.3 Liveness Properties . . . 18

3.4 Safety vs Liveness . . . 19

4 Topological Approach 20

4.1 Generalities . . . 20

4.1.1 Adherence . . . 22

4.1.2 The Topological Decomposition Theorem . . . 23

4.1.3 Bases and Subbases . . . 23

4.2 Spaces of ω-Words . . . 24

4.2.1 Topological Safety and Liveness . . . 26

5 Partial Orders and Complete Lattices 27

5.1 Partial Orders . . . 27

5.2 Complete Lattices . . . 28

5.3 Closure Operators . . . 30

5.4 Galois Connections . . . 31

5.5 Prefix and Closure . . . 32

5.5.1 Alternative Proof of the Decomposition Theorem 3.42 . . . 33

5.6 Further Properties of Closure Operators and Galois Connections . . . 34

5.6.1 On the Kleisli Construction . . . 36

6 Observable Properties 37

6.1 Observable Properties as Clopen Sets . . . 37

6.2 Compactness . . . 39

6.2.1 The Finite Intersection Property . . . 41

6.3 Compact Hausdorff Spaces . . . 41

7 Linear Temporal Logic 41
7.1 The Logic LML of Observable Properties . . . 42
7.1.1 Syntax and Semantics of LML . . . 42
7.1.2 Logical Equivalence . . . 43
7.1.3 Observable Properties . . . 43
7.2 Extending LML with Fixpoints . . . 46
7.2.1 The "Eventually" and "Always" Modalities . . . 46
7.2.2 Positive and Negative Variables in a Formula . . . 47
7.2.3 The Knaster-Tarski Fixpoint Theorem . . . 48
7.3 The Logic LTL . . . 49
7.3.1 Syntax and Semantics of LTL . . . 50
7.3.2 Fixpoints and Defined Modalities . . . 50
7.3.3 Logical Equivalence . . . 51
7.3.4 Positive Normal Forms . . . 52
7.3.5 Satisfaction of LTL-Formulae by Transition Systems . . . 52

8 Toward Stone Duality 53

9 Bisimulation 55
9.1 Bisimulation (with Actions) . . . 55
9.2 Bisimilarity and Trace Equivalence . . . 56
9.3 The Bisimulation Quotient . . . 57

10 On Modal Logics of Transition Systems 57
10.1 Kripke Frames and Kripke Models . . . 57
10.2 Syntax and Semantics of HML . . . 58
10.3 Logical Equivalence . . . 59
10.3.1 Logical Equivalence on Formulae . . . 59
10.3.2 Logical Equivalence on States and Bisimilarity . . . 60
10.4 The Hennessy-Milner Property . . . 60
10.5 Modal Saturation . . . 62
10.6 Boolean Algebras with Operators . . . 62
10.7 Ultrafilter Extensions of Kripke Models . . . 65

1 Introduction

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

In particular, we refer to [BK08, Chap. 2] for a general introduction to **verification** and **model-checking**.[1]

1.1 Notational Preliminaries

Notation 1.1 (Unions and Intersections)**.** *Let X be a set.*

(1) Given a collection $\mathcal{C} \subseteq \mathcal{P}(X)$, we let $\bigcup \mathcal{C}$ be the unique subset of X such that

$$(\forall x \in X) \left(x \in \bigcup \mathcal{C} \quad \Longleftrightarrow \quad (\exists A \in \mathcal{C})(x \in A) \right)$$

In particular,

$$\bigcup \emptyset \quad = \quad \emptyset$$

Moreover, given a family $(A_i)_{i \in I}$ of subsets of X, we let

$$\textstyle\bigcup_{i \in I} A_i \quad := \quad \bigcup \{A_i \mid i \in I\}$$

(2) Given a collection $\mathcal{C} \subseteq \mathcal{P}(X)$, we let $\bigcap \mathcal{C}$ be the unique subset of X such that

$$(\forall x \in X) \left(x \in \bigcap \mathcal{C} \quad \Longleftrightarrow \quad (\forall A \in \mathcal{C})(x \in A) \right)$$

In particular,

$$\bigcap \emptyset \quad = \quad X$$

Moreover, given a family $(A_i)_{i \in I}$ of subsets of X, we let

$$\textstyle\bigcap_{i \in I} A_i \quad := \quad \bigcap \{A_i \mid i \in I\}$$

Notation 1.2 (Finite and Infinite Words)**.** *Let Σ be an **alphabet** (i.e. a set).*

*(1) We write Σ^ω for the set of **infinite words** (actually ω-words) or **streams** over Σ, i.e. the set of all $\sigma : \mathbb{N} \to \Sigma$.*

*(2) We let $\Sigma^\infty = \Sigma^* \cup \Sigma^\omega$ be the set of **finite or infinite** words over Σ. The **empty word** is denoted ε.*

(3) Given $\sigma \in \Sigma^\infty$ and $\hat{\sigma} \in \Sigma^*$, we write $\hat{\sigma} \subseteq \sigma$ to mean that $\hat{\sigma}$ is a (finite) prefix of σ, i.e. that

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

[1] Until 2008. For a recent project in the subject, see e.g. https://www.aere.iastate.edu/modelchecker/

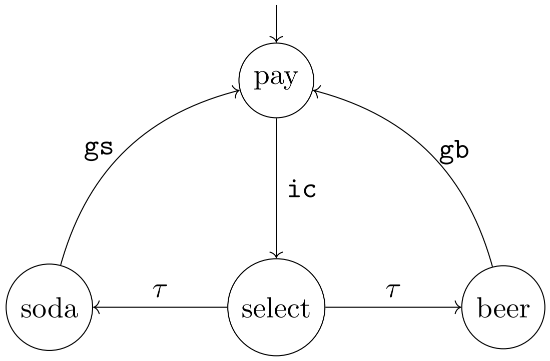


Figure 1: A Beverage Vending Machine (from [BK08]).

(4) Given $\sigma \in \Sigma^\infty$ and $E \subseteq \Sigma^\infty$, we let

$$\begin{array}{lcl} \mathrm{Pref}(\sigma) & := & \{\hat{\sigma} \in \Sigma^* \mid \hat{\sigma} \subseteq \sigma\} \\ \mathrm{Pref}(E) & := & \bigcup_{\sigma \in E} \mathrm{Pref}(\sigma) \quad (= \bigcup\{\mathrm{Pref}(\sigma) \mid \sigma \in E\}) \end{array}$$

Further, we often write σ for an ω-word in Σ^ω and $\hat{\sigma}$ for a finite word Σ^*.

Remark 1.3. *Note that the prefix order $\subseteq$ is a* ***partial*** *order on Σ^*. But given an ω-word $\sigma \in \Sigma^\omega$, the set $\mathrm{Pref}(\sigma)$ is* ***linearly*** *(or* ***totally****) ordered by $\subseteq$.*

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

$$TS \quad = \quad (S, \mathrm{Act}, \to, I, \mathrm{AP}, L)$$

where

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

Example 2.1 (The Beverage Vending Machine of [BK08, Ex. 2.2])**.** *We consider the* ***beverage vending machine*** *(BVM) depicted in Fig. 1. Formally, this transisition system has:*

state set: $S = \{\mathrm{pay}, \mathrm{soda}, \mathrm{beer}\}$, *with* pay *initial;*

action set: $\mathrm{Act} = \{\mathtt{ic}, \mathtt{gs}, \mathtt{gb}, \tau\}$.

The intention is that in state pay *the machine is waiting for the customer to pay. Payment is modelized by the action* `ic` *(short for "insert coin"). Upon payment, the machine goes in state* select, *from which the beverage to be delivered is chosen. This choice is not up to the customer: the two transitions out of the state* select *are labeled with the* ***same action*** τ*. From state* soda *the action* `gs` *(short for "get soda") expresses that the customer will get a soda (and similarly from state* beer*).*

We let the set AP *of atomic propositions be* $\{\mathsf{paid}, \mathsf{drink}\}$*. The labelling function* L *(not drawn in Fig. 1) is given by:*

$$\begin{array}{rclcrcl} L(\mathrm{pay}) & = & \emptyset & \qquad & L(\mathrm{soda}) & = & \{\mathsf{drink}\} \\ L(\mathrm{select}) & = & \{\mathsf{paid}\} & & L(\mathrm{beer}) & = & \{\mathsf{drink}\} \end{array}$$

Remark 2.2 (The Action τ)**.** *It is a quite general convention to use the distinguished name* τ *as in Ex. 2.1 to denote some (possibly non-deterministic) action* ***internal*** *to the system under consideration, where "internal" means that the outside has no information on what is actualy done by the system.*

We refer to [BK08, Chap. 2] for further examples.

3 Linear-Time Properties

We follow the approach of [BK08, Chap. 3] with a few differences in terminology and notation. Recall Notation 1.2 from §1.1.

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

The idea is that an ω-word $\sigma \in (\mathbf{2}^{\mathrm{AP}})^\omega$ is a function

$$\begin{array}{rcccl} \sigma & : & \mathbb{N} & \longrightarrow & \mathbf{2}^{\mathrm{AP}} \\ & & n & \longmapsto & \sigma(n) \end{array}$$

where $\sigma(n) \subseteq \mathrm{AP}$ specifies the set of atomic propositions which σ assumes to hold at time $n \in \mathbb{N}$.

Example 3.2. *Recall the BVM of Ex. 2.1 (§2), with set of atomic propositions* $\mathrm{AP} = \{\mathsf{paid}, \mathsf{drink}\}$*. The following are linear-time properties on this transition system.*

(1) $\sigma \in P$ *iff in* σ*, each* drink *occurs after a* paid*. Formally:*

$$P \quad = \quad \left\{\sigma \in (\mathbf{2}^{\mathrm{AP}})^\omega \mid (\forall n \in \mathbb{N})\,(\mathsf{drink} \in \sigma(n) \implies \exists k < n.\ \mathsf{paid} \in \sigma(k))\right\}$$

(2) $\sigma \in P$ *iff at every moment, there has been at least as many* paid*'s as* drink*'s. Formally:*

$$P \quad = \quad \left\{\sigma \in (\mathbf{2}^{\mathrm{AP}})^\omega \mid \forall \hat{\sigma} \subseteq \sigma,\ \mathrm{Card}\{n \mid \mathsf{drink} \in \hat{\sigma}(n)\} \leq \mathrm{Card}\{n \mid \mathsf{paid} \in \hat{\sigma}(n)\}\right\}$$

(3) $\sigma \in P$ *iff in* σ*, there are infinitely many* paid*'s whenever there are infinitely many* drink*'s. Formally:*

$$P \quad = \quad \left\{\sigma \in (\mathbf{2}^{\mathrm{AP}})^\omega \mid (\exists^\infty t)(\mathsf{drink} \in \sigma(t)) \implies (\exists^\infty t)(\mathsf{paid} \in \sigma(t))\right\}$$

(4) $\sigma \in P$ *iff in* σ*, there are at most finitely many* drink*'s whenever there are at most finitely many* paid*'s. Formally:*

$$P \quad = \quad \left\{\sigma \in (\mathbf{2}^{\mathrm{AP}})^\omega \mid (\forall^\infty t)(\mathsf{paid} \notin \sigma(t)) \implies (\forall^\infty t)(\mathsf{drink} \notin \sigma(t))\right\}$$

Notation 3.3 (The Quantifiers $\exists^\infty$ and $\forall^\infty$)**.** *In Ex. 3.2 we used the quantifiers* $\exists^\infty$ *and* $\forall^\infty$*. These customary notations for linear-time properties stand for the following.*

The "infinitely many" quantifier $(\exists^\infty t)(\cdots t \cdots)$ *unfolds to* $(\forall N \in \mathbb{N})(\exists t \geq N)(\cdots t \cdots)$ *(where* N *is supposed not to occur in* $(\cdots t \cdots)$*). This precisely means that there are infinitely many* $t \in \mathbb{N}$ *such that* $(\cdots t \cdots)$*. For instance,* $(\exists^\infty t)(\mathsf{paid} \in \sigma(t))$ *means that there are infinitely many* $t \in \mathbb{N}$ *such that* $\mathsf{paid} \in \sigma(t)$*.*

The "ultimately all" quantifier $(\forall^\infty t)(\cdots t \cdots)$ *unfolds to* $(\exists N \in \mathbb{N})(\forall t \geq N)(\cdots t \cdots)$ *(where* N *is supposed not to occur in* $(\cdots t \cdots)$*). This means that there are at most finitely many* $t \in \mathbb{N}$ *such that* $(\cdots t \cdots)$ *fails, or equivalently that* $(\cdots t \cdots)$ *holds for ultimately all* $t \in \mathbb{N}$*. For instance,* $(\forall^\infty t)(\mathsf{paid} \notin \sigma(t))$ *means that there are at most finitely many* $t \in \mathbb{N}$ *such that* $\mathsf{paid} \in \sigma(t)$*, equivalently that* $\mathsf{paid} \notin \sigma(t)$ *for ultimately all* $t \in \mathbb{N}$*.*

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

3.1 Linear-Time Behaviour of Transition Systems

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

Definition 3.4 (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* $s_i \xrightarrow{\mathsf{a}} s_{i+1}$ *for some* $\mathsf{a} \in \mathrm{Act}$*.*

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

Definition 3.5 (Trace)**.**

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

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

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

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

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

Example 3.6. *Recall the BVM of Ex. 2.1 (§2). Its unique infinite trace is* $(\emptyset \cdot \{\mathsf{paid}\} \cdot \{\mathsf{drink}\})^\omega$*, while its set of finite traces is* $\mathrm{Pref}\,((\emptyset \cdot \{\mathsf{paid}\} \cdot \{\mathsf{drink}\})^*)$*.*

Remark 3.7 (Differences with [BK08])**.** *Beware that* $\mathrm{Tr}(\mathit{TS})$ *in Def. 3.5 does* ***not*** *coincide with Traces(*TS*) as defined in [BK08, §3.2.2]. However,* $\mathrm{Tr}_{\mathsf{fin}}(\mathit{TS})$ *does coincide with Traces*$_{\mathsf{fin}}$*(*TS*) ([BK08, p. 98 & 96]), and* $\mathrm{Tr}^\omega(\mathit{TS})$ *is the set of infinite traces in Traces(*TS*).*

Definition 3.8 (Satisfaction of Linear-Time Properties)**.** *We say that TS* ***satisfies*** *a LT property* $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$*, notation* $\mathit{TS} \mathrel{|\!\!\approx} P$*, if* $\mathrm{Tr}^\omega(\mathit{TS}) \subseteq P$*.*

Example 3.9. *The BVM of Ex. 2.1 (§2) satisfies all the LT properties of Ex. 3.2.*

Remark 3.10. *Linear time properties do not take into account the branching structure of transition systems.*

Remark 3.11 (Differences with [BK08])**.** *Definition 3.8 coincides with [BK08, Def. 3.11, §3.2.3]. But note our special symbol* $\mathrel{|\!\!\approx}$ *for the satisfaction of LT properties in transition systems, which differs from the notation of [BK08, Def. 3.11]. The reason is that LT properties are properties on the infinite traces of TS's rather than properties on the TS's themselves (see Rem. 3.10), while there are well-known* ***modal logics*** *for describing the latter (see §10).*

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

Proposition 3.12. *Given two transition systems TS and TS′, both over* AP*, we have*

$$\mathrm{Tr}^\omega(\mathit{TS}) \subseteq \mathrm{Tr}^\omega(\mathit{TS}') \qquad \text{if and only if} \qquad \forall P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega, \quad \mathit{TS}' \mathrel{|\!\!\approx} P \quad \Longrightarrow \quad \mathit{TS} \mathrel{|\!\!\approx} P$$

Proof. Assume $\mathrm{Tr}^\omega(\mathit{TS}) \subseteq \mathrm{Tr}^\omega(\mathit{TS}')$. Then for an LT property P such that $\mathit{TS}' \mathrel{|\!\!\approx} P$, we have $\mathrm{Tr}^\omega(\mathit{TS}) \subseteq \mathrm{Tr}^\omega(\mathit{TS}') \subseteq P$, so that $\mathit{TS} \mathrel{|\!\!\approx} P$.

Conversely, let $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ be the LT property $\mathrm{Tr}^\omega(\mathit{TS}')$. Then $\mathit{TS}' \mathrel{|\!\!\approx} P$, but $\mathit{TS} \not\mathrel{|\!\!\approx} P$ unless $\mathrm{Tr}^\omega(\mathit{TS}) \subseteq \mathrm{Tr}^\omega(\mathit{TS}')$. □

Proposition 3.12 is an easy first step in a theme on which we shall come back in §3.2.4 below, namely the comparison of TS's w.r.t. the LT properties they satisfy.

Example 3.13 (Another BVM ([BK08, Ex. 3.19]))**.** *Consider the transition system depicted in Fig. 2, with labelling function*

$$\begin{array}{lcl@{\qquad}lcl@{\qquad}lcl} \mathrm{pay} & \longmapsto & \emptyset & \mathrm{sel.1} & \longmapsto & \{\mathsf{paid}\} & \mathrm{soda} & \longmapsto & \{\mathsf{drink}\} \\ & & & \mathrm{sel.2} & \longmapsto & \{\mathsf{paid}\} & \mathrm{beer} & \longmapsto & \{\mathsf{drink}\} \end{array}$$

This transition system has the same infinite traces as the BVM of Ex. 2.1 (§2) and thus satisfies exactly the same LT properties.

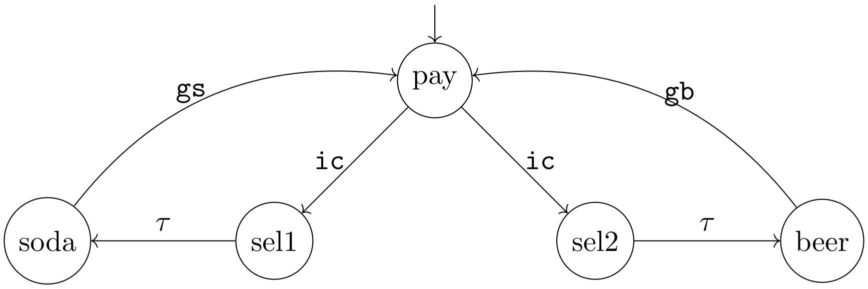


Figure 2: Another Beverage Vending Machine (from [BK08]).

3.2 Safety Properties and Invariants

We now embark in a basic classification of LT properties, which shall be reformulated in §4 with topological notions, and which will be sharpened in §5 using order and lattice theoretic tools. This simple classification considers two families of LT properties:

Safety Properties, discussed in this §3.2;

Liveness Properties, to be discussed in §3.3.

Safety and liveness properties are related by the following important facts (§3.4):

The Decomposition Theorem 3.42: for every LT property P over AP, there is a safety property P_{safe} and a liveness property P_{liveness} (both over AP) such that

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

Proposition 3.41: the only LT property (over AP) which is both a safety and a liveness property is the "true" property $(\mathbf{2}^{\text{AP}})^\omega$.

This classification of LT properties is due to [AS85]. See [BK08, §3.7] for further references.

We fix a set AP of atomic propositions.

3.2.1 Invariants

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

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

3.2.2 Safety Properties

The idea of **safety properties** is to specify "bad behaviours" that should not occur. Otherwise said, a safety property expresses that "something bad does not occur". This is formalized as follows for LT properties.

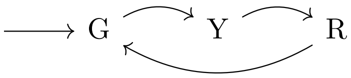
Definition 3.14 (Safety Property)**.** *We say that $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ is a **safety property** if there is a (possibly infinite) set of finite words $P_{\mathrm{bad}} \subseteq (\mathbf{2}^{\mathrm{AP}})^*$ such that P is the set of ω-words which avoid P_{bad}, in the sense that*

$$P \quad = \quad \{\sigma \in (\mathbf{2}^{\mathrm{AP}})^\omega \mid \forall \hat{\sigma} \subseteq \sigma,\ \hat{\sigma} \notin P_{\mathrm{bad}}\}$$

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

Example 3.15. *The LT properties of Ex. 3.2.(1) and (2) are safety properties. The properties of Ex. 3.2.(3) and (4) are not.*

Example 3.16 (A Traffic Light ([BK08, Ex. 3.23]))**.** *Consider the following transition system*



with exactly one action, with set of atomic propositions $\mathrm{AP} = \{\mathsf{G}, \mathsf{Y}, \mathsf{R}\}$, and whose labelling function is given by

$$\mathrm{G} \mapsto \{\mathsf{G}\} \qquad\qquad \mathrm{Y} \mapsto \{\mathsf{Y}\} \qquad\qquad \mathrm{R} \mapsto \{\mathsf{R}\}$$

A typical safety property on this transition system is "every R is the immediate successor of a Y", which can be formalized as

$$\big\{\sigma \in (\mathbf{2}^{\mathrm{AP}})^\omega \mid (\forall n \in \mathbb{N})\,\big(\mathsf{R} \in \sigma(n) \implies \big[n > 0 \textit{ and } \mathsf{Y} \in \sigma(n-1)\big]\big)\big\}$$

Safety properties have a partly finitary nature, since they a generated from sets of **finite** words P_{bad}. This suggests to check the satisfaction of safety properties via some inspection of the **finite** traces of a TS. This is possible under a mild assumption, which is given by the following definition.

Definition 3.17. *A state $s \in S$ of a transition system TS is called **terminal** if there are no state $s' \in S$ and no action $\mathsf{a} \in \mathrm{Act}$ such that $s \xrightarrow{\mathsf{a}} s'$.*

Proposition 3.18 (Satisfaction of Safety Properties)**.** *Let $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ be a safety property induced by P_{bad}. Given a transition system TS over AP and without terminal states, we have*

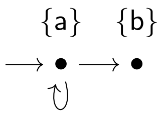
$$TS \mid\!\!\approx P \qquad \textit{iff} \qquad \mathrm{Tr}_{\mathrm{fin}}(TS) \cap P_{\mathrm{bad}} = \emptyset$$

Proof. Assume first that $\mathrm{Tr}_{\mathrm{fin}}(TS) \cap P_{\mathrm{bad}} = \emptyset$. and let $\sigma \in \mathrm{Tr}^\omega(TS)$. Then for any $\hat{\sigma} \subseteq \sigma$, since $\hat{\sigma} \in \mathrm{Tr}_{\mathrm{fin}}(TS)$ we have $\hat{\sigma} \notin P_{\mathrm{bad}}$. It follows that $\sigma \in P$.

Conversely, let $\hat{\sigma} \in \mathrm{Tr}_{\mathrm{fin}}(TS) \cap P_{\mathrm{bad}}$. Let $\hat{\pi}$ be a finite initial path in TS such that $\hat{\sigma} = L(\hat{\pi})$. Then since TS has no terminal state, there is an infinite (initial) path π in TS with $\hat{\pi} \subseteq \pi$. But then $TS \not\mid\!\!\approx P$ since $\hat{\sigma} \subseteq L(\pi)$. □

The assumption that TS has no terminal state is unavoidable in Prop. 3.18.

Example 3.19. *Consider the following transition system TS (with exactly one action):*



Let P be the safety property induced by $P_{\text{bad}} = \{\mathsf{a}\}^*\{\mathsf{b}\}$. Then TS satisfies P since the only infinite trace of TS is $\{\mathsf{a}\}^\omega$. But $\{\mathsf{a}\}\{\mathsf{b}\}$ is a finite trace in TS which belongs to P_{bad}.

3.2.3 Regular Safety Properties

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

Definition 3.20 (Regular Safety Property)**.** *A safety property $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ is* ***regular*** *if it is induced by a regular set $P_{\text{bad}} \subseteq (\mathbf{2}^{\mathrm{AP}})^*$.*

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

$$(\mathcal{A} : \mathbf{2}^{\mathrm{AP}}) \quad = \quad (Q, \Delta, Q_0, F)$$

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

Consider now a transition system TS over AP:

$$TS \quad = \quad (S, \mathrm{Act}, \rightarrow, I, \mathrm{AP}, L)$$

We define the product transition system

$$TS \otimes \mathcal{A} \quad := \quad (S_\otimes, \mathrm{Act}, \rightarrow_\otimes, I_\otimes, \mathrm{AP}_\otimes, L_\otimes)$$

as follows:

- The set of states is $S_\otimes := S \times Q$.
- The transition relation $\rightarrow_\otimes$ is defined by the rule

  $$\frac{s \xrightarrow{\mathsf{a}} s' \qquad (q, L(s'), q') \in \Delta}{(s, q) \xrightarrow{\mathsf{a}} (s', q')}$$

  Note that it is the label of the **target** state s' of $s \xrightarrow{\mathsf{a}} s'$ 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

$$\varphi_{\mathcal{A}} \quad := \quad \bigwedge_{q \in F} \neg q$$

Note that if TS has no terminal states, then it follows from Prop. 3.18 that we have

$$TS \models P \qquad \text{iff} \qquad \mathrm{Tr}_{\mathrm{fin}}(TS) \cap \mathcal{L}(\mathcal{A}) = \emptyset$$

Proposition 3.21. *Assume that TS has no terminal states. Then $TS \models P$ iff the transition system $TS \otimes \mathcal{A}$ satisfies the invariant induced by $\varphi_{\mathcal{A}}$.*

Proof. Exercise! □

Remark 3.22. *An immediate consequence of Prop. 3.21 is that it is decidable whether a given **finite** TS satisfies a given **regular** safety property. This actually extends (in a non-trivial way) to (sufficiently regularly generated) infinite TS's. We refer to [Wal16] for an overview (outside the scope of this course).*

3.2.4 Safety Properties and Trace Equivalence

We now continue the task began in Prop. 3.12 (§3.1), and compare transition systems w.r.t. the safety properties they satisfy.

We begin with the following direct consequence of Prop. 3.18 (§3.2.2) for **finite** traces.

Lemma 3.23. *Consider TS and TS', both over AP and both without terminal states. We have*

$$\mathrm{Tr}_{\mathrm{fin}}(TS) \subseteq \mathrm{Tr}_{\mathrm{fin}}(TS') \qquad \textit{iff} \qquad \forall P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega \textit{ safety}, \quad TS' \models P \quad \Longrightarrow \quad TS \models P$$

Proof. Assume first that $\mathrm{Tr}_{\mathrm{fin}}(TS) \subseteq \mathrm{Tr}_{\mathrm{fin}}(TS')$. Let P be induced by P_{bad} and such that $TS' \models P$. Then by Prop. 3.18 we have $\mathrm{Tr}_{\mathrm{fin}}(TS') \cap P_{\mathrm{bad}} = \emptyset$, from which we get $\mathrm{Tr}_{\mathrm{fin}}(TS) \cap P_{\mathrm{bad}} = \emptyset$, and the result follows, again by Prop. 3.18.

For the converse, let P be the safety property induced by

$$P_{\mathrm{bad}} \quad := \quad (\mathbf{2}^{\mathrm{AP}})^* \setminus \mathrm{Tr}_{\mathrm{fin}}(TS')$$

Then $TS' \models P$ by definition. But then by Prop. 3.18 we have $\mathrm{Tr}_{\mathrm{fin}}(TS) \subseteq \mathrm{Tr}_{\mathrm{fin}}(TS')$ whenever $TS \models P$. □

It is fairly easy to see that TS must have no terminal state in Lem. 3.23.

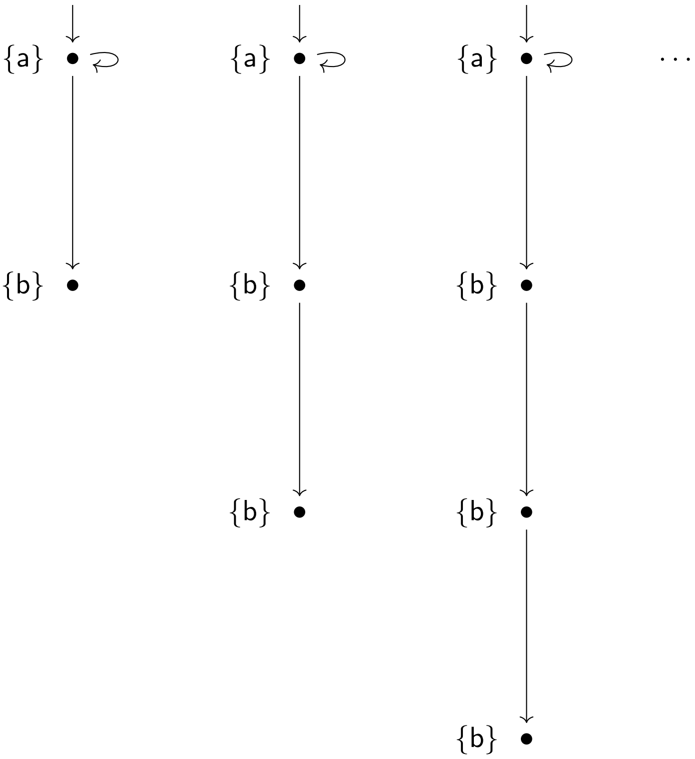
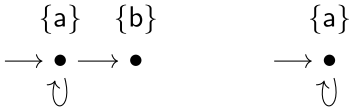


Figure 3: A transition system with infinitely many initial states for Ex. 3.25.

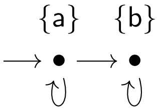
Example 3.24. *Consider the following two transition systems:*



These TS's satisfy the same LT properties (and in particular the same safety properties) since they have the same infinite traces (Prop. 3.12, §3.1). But the TS on the left-hand side has finite traces that the other one does not have.

The following shows that the assumption on TS' in Lem. 3.23 cannot be omitted neither.

Example 3.25. *Let TS be the following transition system:*



Let TS' be the transition system depicted in Fig. 3 (with infinitely many initial states). Then both TS and TS' have set of finite traces $\{\mathsf{a}\}^* \cup \{\mathsf{a}\}^+\{\mathsf{b}\}^*$. *Note that TS has the* *infinite trace* $\{\mathsf{a}\}\{\mathsf{b}\}^\omega$*, while the only infinite trace of* TS' *is* $\{\mathsf{a}\}^\omega$*. In particular,* TS' *satisfies the safety property induced by* $P_{\mathrm{bad}} = \{\mathsf{a}\}^+\{\mathsf{b}\}$*, but this property is not satisfied by* TS*.*

We now look for an analogue of Prop. 3.12 (§3.1) for safety properties. To this end, we shall forbid transition systems which (as the TS' of Ex. 3.25) have infinitely many initial states. This actually lead to the following assumption.

Definition 3.26 (Finitely Branching TS)**.** *A transition system* $\mathit{TS} = (S, \mathrm{Act}, \to, I, \mathrm{AP}, L)$ *is **finitely branching** when the two following conditions are satisfied:*

(i) I *is finite, and*

(ii) for every $s \in S$*, there are at most finitely many* $s' \in S$ *such that* $s \xrightarrow{\mathsf{a}} s'$ *for some* $\mathsf{a} \in \mathrm{Act}$*.*

Proposition 3.27. *Consider* TS *and* TS'*, both over* AP*. Assume that* TS *has no terminal state and that* TS' *is finitely branching. Then*

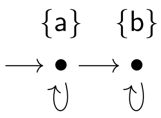
$$\mathrm{Tr}^\omega(\mathit{TS}) \subseteq \mathrm{Tr}^\omega(\mathit{TS}') \qquad \textit{iff} \qquad \mathrm{Tr}_{\mathrm{fin}}(\mathit{TS}) \subseteq \mathrm{Tr}_{\mathrm{fin}}(\mathit{TS}')$$

Corollary 3.28. *Consider finitely branching* TS *and* TS'*, both over* AP *and both without terminal states. Then we have*

$$\mathrm{Tr}^\omega(\mathit{TS}) = \mathrm{Tr}^\omega(\mathit{TS}') \qquad \textit{iff} \qquad \forall P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega \ \textit{safety}, \quad \mathit{TS}' \mathrel{|\!\!\approx} P \quad \Longleftrightarrow \quad \mathit{TS} \mathrel{|\!\!\approx} P$$

Example 3.24 shows that the assumption on TS cannot be omitted in Prop. 3.27. As for the assumption on TS', one can consider the following mild modification of Ex. 3.25.

Example 3.29. *Let* TS *be the following transition system:*



Let TS' *be the transition system depicted in Fig. 4 (with infinitely many initial states). Then both* TS *and* TS' *have set of finite traces* $\{\mathsf{a}\}^* \cup \{\mathsf{a}\}^+\{\mathsf{b}\}^*$*. But* TS *has the infinite trace* $\{\mathsf{a}\}^\omega$*, while all infinite traces of* TS' *have the form* $\{\mathsf{a}\}^+\{\mathsf{b}\}^\omega$*.*

Since both TS *and* TS' *have no terminal states, they satisfy the same safety properties (Lem. 3.23). Hence, we cannot omit the assumption that* TS *and* TS' *are finitely branching in Cor. 3.28.*

Remark 3.30. *For Ex. 3.25 and Ex. 3.29, the transition systems of Fig. 3 and Fig. 4 could have been replaced by (non finitely branching) transition systems with exactly one initial state.*

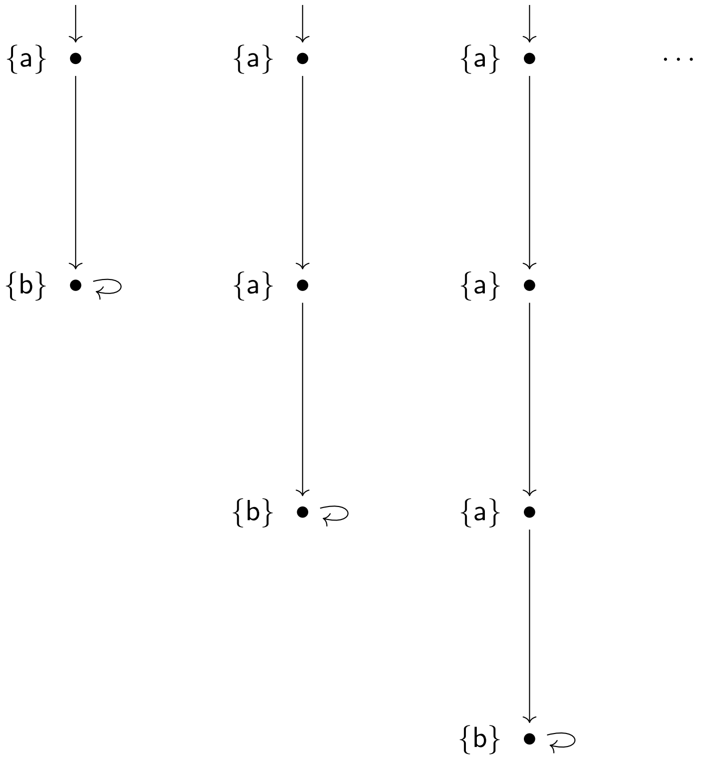


Figure 4: A transition system with infinitely many initial states for Ex. 3.29.

3.2.5 Kőnig's Lemma

Proposition 3.27 relies on a principle of infinite combinatorics known as **Kőnig's Lemma**. It basically says that if an infinite tree is finitely branching, then it has an infinite path.

We first define the required notions.

Definition 3.31.

*(1) A **tree** over 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 over A is **finitely branching** if for each $u \in T$, 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 ω-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 3.32 (Kőnig'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 $T{\restriction}u$ for the **subtree** of T at u:

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

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 $T{\restriction}a$ for $a \in A$. Since T is infinite and finitely branching, by the infinite pigeonhole principle there is some $a \in A$ such that $T{\restriction}a$ 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 $n \in \mathbb{N}$,
- $T{\restriction}(a_0 \cdots a_n)$ is infinite for all $n \in \mathbb{N}$.

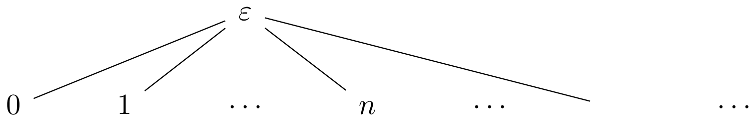
Assuming $a_0, \ldots, a_n$ defined, since

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

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 $T{\restriction}(a_0 \cdots a_n a)$ is infinite. We let $a_{n+1} := a$. □

No assumption of Kőnig's Lemma 3.32 can be omitted. First, T trivially needs be infinite to have an infinite path. Finite branching is also easy to observe.

Example 3.33. *The following tree over $\mathbb{N}$ is infinite but has no infinite path:*



Why T is required to be a tree is not too difficult to see neither, but perhaps more subtle. We come back on this in Ex. 4.18 (§4.2).

Example 3.34. *The set $T_0 := 0^*1 \subseteq \{0,1\}^*$ is infinite, finitely branching but is not a tree: T_0 is not closed under prefix since it is prefix-free (if $u \in T_0$ then no proper prefix of u belongs to T_0). In particular, it is clear that T_0 has no infinite path.*

On the other hand, the tree $T := \mathrm{Pref}(T_0)$ has a unique infinite path, namely 0^ω. But note that no prefix of 0^ω belongs to T_0! See Fig. 5 (in which nodes are the $v \in T$).

Remark 3.35 (On Definition 3.31)**.** *The notion of tree in Def. 3.31 formally differs from the graph-theoretic one. See e.g. [Kec95, 4.13 (§4B)] for a comparison.*

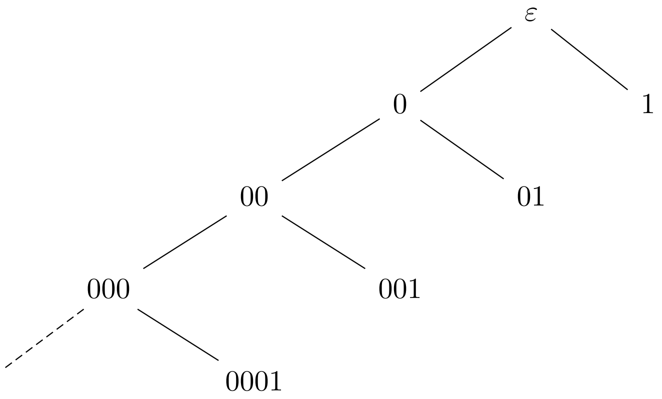


Figure 5: The tree T of Ex. 3.34.

Remark 3.36 (References). *A striking aspect of Kőnig's Lemma 3.32 is that there are recursive infinite trees $T \subseteq \{0,1\}^*$ with no recursive infinite path (see e.g. [TvD88, Chap. 4, §7.6] or [Sim10, Lem. VIII.2.15]). We refer to [Sim10, I.8.8 and §III.7] for the axiomatic strength of Kőnig's Lemma (outside the scope of this course).*

Kőnig's Lemma 3.32 is an important tool for various topics related to this course. First, see [BBJ07, §26.2] for an approach based on logic and an application to graphs (namely Ramsey's Theorem). Moreover, Kőnig's Lemma 3.32 has important applications in the theory of automata on ω-words, see e.g. [GTW02, §3] (also [PP04, §I.9]) or [VW08, §2.2.1] (outside the scope of this course). Last but not least, Kőnig's Lemma 3.32 is strongly related to topological compactness. We come back on this in §6.2 (Prop. 6.12, Rem. 6.13 and *Rem. 6.14).*

3.2.6 Proof of Proposition 3.27

We can now prove Prop. 3.27.

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

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

$$\pi_n \quad = \quad s_0^n \cdots s_n^n$$

such that

$$L'(\pi_n) \subseteq \sigma$$

But note that we may not have $\pi_n \subseteq \pi_{n+1}$. We therefore apply Kőnig's Lemma 3.32 to build a suitable infinite path in TS'. Consider the tree $T \subseteq (S')^*$ defined as

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

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 $\hat{\sigma} \in \mathrm{Tr}_{\mathrm{fin}}(TS) \subseteq \mathrm{Tr}_{\mathrm{fin}}(TS')$, so there is a finite initial path u in TS' such that $L'(u) = \hat{\sigma}$. By Kőnig's Lemma 3.32, T has an infinite path π. We have $L'(\pi) = \sigma$ since $L'(\pi(0) \cdots \pi(n)) \subseteq \sigma$ for all $n \in \mathbb{N}$. Moreover, π is an initial path in TS' by construction of T. □

Direct Proof of Proposition 3.27. We can nevertheless give a direct proof of Prop. 3.27.

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

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

$$\pi_n \quad = \quad s_0^n \cdots s_n^n$$

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 $(\pi_n^0)_{n \in \mathbb{N}}$ of $(\pi_n)_{n \in \mathbb{N}}$ with $\pi_n^0(0) = s$ 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 π_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

  $$\tilde{\pi}_n^k \quad := \quad \pi_n^k(0) \cdots \pi_n^k(k)$$

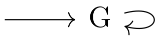
  agree for $n \geq k$.

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

3.3 Liveness Properties

While safety properties specify that "nothing wrong can happen", a given safety property may vacuously hold in a "sufficiently inactive" system.

Example 3.37. *Recall Ex. 3.16 (§3.2.2) and consider the following "traffic light":*



with AP $= \{\mathsf{G}, \mathsf{Y}, \mathsf{R}\}$ *and state labelling* G $\mapsto \{\mathsf{G}\}$. *This system trivially satisfies the safety property of Ex. 3.16 ("every* R *is the immediate successor of a* Y*").*

Liveness properties, which form the second part of the classification mentioned in §3.2, specify that "something good will happen".

Definition 3.38 (Liveness Property)**.** *We say that $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ is a **liveness property** if for every $\hat{\sigma} \in (\mathbf{2}^{\mathrm{AP}})^*$ there is some $\sigma \in P$ such that $\hat{\sigma} \subseteq \sigma$.*

Liveness properties are typically conditions on infinite behaviours.

Example 3.39. *A typical liveness property which can be used to ensure that the safety property of Ex. 3.37 holds in a non-trivial way is: "*R *occurs infinitely often". Formally:*

$$\left\{\sigma \in (\mathbf{2}^{\mathrm{AP}})^\omega \mid (\exists^\infty t)(\mathsf{R} \in \sigma(t))\right\}$$

This property is satisfied by the transition system of Ex. 3.16 but not by the one of Ex. 3.37.

Example 3.39 suggests to consider the conjunction of a safety property with a liveness property. This is no special case: the Decomposition Theorem 3.42 (in §3.4 below) states that **every** LT property is the conjunction of a safety property with a liveness property.

Example 3.40. *Recall the BVM of Ex. 2.1 (§2). The following two properties from Ex. 3.2 are liveness properties:*

- *$\sigma \in P$ iff in σ, there are infinitely many* paid*'s whenever there are infinitely many* drink*'s:*

$$P \quad = \quad \left\{\sigma \in (\mathbf{2}^{\mathrm{AP}})^\omega \mid (\exists^\infty t)(\mathsf{drink} \in \sigma(t)) \implies (\exists^\infty t)(\mathsf{paid} \in \sigma(t))\right\}$$

- *$\sigma \in P$ iff in σ, there are at most finitely many* drink*'s whenever there are at most finitely many* paid*'s:*

$$P \quad = \quad \left\{\sigma \in (\mathbf{2}^{\mathrm{AP}})^\omega \mid (\forall^\infty t)(\mathsf{paid} \notin \sigma(t)) \implies (\forall^\infty t)(\mathsf{drink} \notin \sigma(t))\right\}$$

See [BK08, §3.5] for more.

3.4 Safety vs Liveness

We now turn to the two results relating safety and liveness which were mentioned in §3.2.

Proposition 3.41 ([BK08, Lem. 3.35])**.** *The only LT property which is both a safety and a liveness property is the "true" property $(\mathbf{2}^{\mathrm{AP}})^\omega$.*

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

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

Theorem 3.42 (Decomposition ([BK08, Thm. 3.37]))**.** *For every LT property $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$, there is a safety property P_{safe} and a liveness property $P_{liveness}$ such that*

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

The Decomposition Theorem 3.42 will 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

Topology has different purposes in this course.

First, we shall see that Σ^ω (the set of ω-words over Σ) can be equipped with a nice notion of topology. In the case of LT properties over AP, the topology on $(\mathbf{2}^{\mathrm{AP}})^\omega$ provides clean characterizations of safety and liveness, and exhibits the Decomposition Theorem 3.42 as a basic topological fact.

Second, as we shall see in §6 and §7.1, the topology on $(\mathbf{2}^{\mathrm{AP}})^\omega$ will give us a strong ground on how to build **logics** (*i.e.* syntaxes) to describe LT properties. This will be sharpened in §8, with **Stone's Representation Theorem** which establishes a deep connection between Boolean algebras on the one hand, and the so called **Stone's spaces** on the hand, of which Σ^ω (for Σ finite) is an important example.

Further, in §10 we shall consider (Hennessy-Milner) **modal logic**, which allows us to reason on the **branching structure** of transitions systems, and whose model theory rests on Stone's Representation Theorem.

To keep things simple, the exposition of this Section is oriented toward presenting (and proving) the Decomposition Theorem 3.42 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*

- *ΩX 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*
- *ΩX 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.

(1) If A is open, then A is itself an open set contained in A and containing each of its points. Conversely, if for each $x \in A$ there is an open U_x such that $x \in U_x \subseteq A$ then $A = \bigcup_{x \in A} U_x$ is open.

(2) Since $A \subseteq X$ is closed iff $X \setminus A$ is open. □

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*

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

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

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

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

PROOF.

(1) Assume $A \subseteq B$ and let C be closed set such that $B \subseteq C$. We then have $A \subseteq C$, and thus $\overline{A} \subseteq C$.

(2) Trivial.

(3) We just have to show $\overline{(\overline{A})} \subseteq \overline{A}$. But $\overline{A}$ is a closed set containing $\overline{A}$, so that $\overline{A} \in \{C \subseteq X \mid \overline{A} \subseteq C \text{ and } C \text{ is closed}\}$ and $\overline{(\overline{A})} \subseteq \overline{A}$.

(4) Since the empty set is itself closed.

(5) We have $\overline{A} \cup \overline{B} \subseteq \overline{A \cup B}$ by monotonicity of $\overline{(-)}$. For the converse, note that $\overline{A} \cup \overline{B}$ is a closed set which contains $A \cup B$, so it contains $\overline{A \cup B}$. □

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 partial orders in §5.3 (Ex. 5.19). It in particular follows from Lem. 5.20 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:*

$$\forall U \in \Omega X, \quad x \in U \quad \Longrightarrow \quad A \cap U \neq \emptyset$$

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. Assume first that x is adherent to A. If C is a closed set which contains A but not x, then x belongs to the open $X \setminus C$. But the latter cannot intersect A as $A \subseteq C$.

Conversely, if $x \in \overline{A}$ and $x \in U$ with U open, then $A \cap U$ empty would imply $A \subseteq X \setminus U$ and thus $x \notin U$, a contradiction. □

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,

$$C \cap D \quad = \quad (\overline{A} \cap A) \cup (\overline{A} \cap (X \setminus \overline{A})) \quad = \quad A$$

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 $U \subseteq X \setminus \overline{A}$.

Note that the density of $D = A \cup (X \setminus \overline{A})$ may be easier to see via the notion of **adherence** (§4.1.1). Indeed consider a non-empty open U such that $U \cap (X \setminus \overline{A})$ is empty. This means that U is included in $\overline{A}$ and since U is non-empty, there is some $x \in \overline{A}$ such that $x \in U$. Now, by Lem. 4.9, x is adherent to A since $x \in \overline{A}$, which implies $U \cap A \neq \emptyset$ since $x \in U$ with U open. □

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. Assume first that D is a dense subset of X. We claim that X is the only closed set C such that $D \subseteq C$. So assume C is a proper closed subset of X such that $D \subseteq C$. But then $X \setminus C$ is a non-empty open set, so that we must have $D \cap (X \setminus C) \neq \emptyset$, contradicting $D \subseteq C$.

Conversely, assume $\overline{D} = X$ and consider some non-empty open U. If $U \cap D$ is empty then $D \subseteq X \setminus U$, so that $X \subseteq X \setminus U$, contradicting that U is non-empty. □

Remark 4.13 (Alternative Proof of Thm. 4.11)**.** *Lemma 4.12, together with the fact that $\overline{(-)}$ 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*

$$\overline{D} \quad = \quad \overline{A} \cup \overline{(X \setminus \overline{A})}$$

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 ΩX 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. First, ΩX is obviously closed under unions. As for closure under finite intersections, we have $X \in \Omega X$ as $X \in \mathcal{B}$ (since $\mathcal{B}$ is closed under finite intersections). It thus remains to show that ΩX is closed under binary intersections. Consider families $(U_i)_{i \in I}$ and $(V_j)_{j \in J}$ of elements of $\mathcal{B}$. Since finite intersections distribute over unions, we have

$$(\bigcup_i U_i) \cap (\bigcup_j V_j) \quad = \quad \bigcup_{i,j} U_i \cap V_j$$

so that $(\bigcup_i U_i) \cap (\bigcup_j V_j) \in \Omega X$ as $\mathcal{B}$ is closed under finite intersections. □

A family $\mathcal{B}$ as in Lem. 4.14 is a **base** of the topology ΩX. 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 ΩX.

4.2 Spaces of ω-Words

Definition 4.15 (The Topology on ω-Words)**.** *Given a non-empty set Σ, we equip Σ^ω with the topology induced by the subbase $(\mathsf{ext}(u))_{u \in \Sigma^*}$, where*

$$\mathsf{ext}(u) \quad := \quad \{\sigma \in \Sigma^\omega \mid u \subseteq \sigma\}$$

Note that $\Sigma^\omega = \mathsf{ext}(\varepsilon)$. Also, if $u, v \in \Sigma^*$ are incomparable w.r.t. the prefix order then $\mathsf{ext}(u) \cap \mathsf{ext}(v) = \emptyset$. Moreover, $v \subseteq u$ obviously implies $\mathsf{ext}(u) \subseteq \mathsf{ext}(v)$. We actually have the following.

Lemma 4.16. *Assume that Σ has at least two elements. Given $u, v \in \Sigma^*$ we have*

$$\mathsf{ext}(u) \subseteq \mathsf{ext}(v) \qquad \textit{iff} \qquad v \subseteq u$$

Proof. If $v \subseteq u$ and $u \subseteq \sigma$, then we obviously have $v \subseteq \sigma$. Hence $\mathsf{ext}(u) \subseteq \mathsf{ext}(v)$.

Conversely, let $\mathsf{ext}(u) \subseteq \mathsf{ext}(v)$. Recall that Σ has at least two elements. If $\text{length}(u) = \text{length}(v)$, then we must have $u = v$. If $\text{length}(u) < \text{length}(v)$, then given σ such that $u \subseteq \sigma$, we have $v \subseteq \sigma$ by assumption, so u must be a strict prefix of v. Hence $u.a$ is a prefix of v for some $a \in \Sigma$. Then for $b \neq a$ let σ such that $u \subseteq u.b \subseteq \sigma$. But we cannot have $u.a \subseteq \sigma$, and in particular $\sigma \notin \mathsf{ext}(v)$, a contradiction. Hence $\text{length}(v) < \text{length}(u)$ and v must be a prefix of u. □

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

Lemma 4.17. *Let Σ be a non-empty set.*

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

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

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

Example 4.18 (Closed Sets from Trees (§3.2.5))**.** *Recall Def. 3.31. Given a tree $T \subseteq \Sigma^*$, the set $\mathrm{cl}(T)$ of infinite paths of T is a **closed** subset of Σ^ω. For instance, the closed set $\mathrm{cl}(\mathrm{Pref}(0^*1)) \subseteq \{0,1\}^\omega$ is the singleton $\{0^\omega\}$ (Ex. 3.34). Actually, we shall see in §5.5 (Cor. 5.28) that the closed subsets of Σ^ω are exactly the $\mathrm{cl}(T)$ for trees $T \subseteq \Sigma^*$. See e.g. [Kec95, §2B] for more.*

Notation 4.19. *Given $U \subseteq \Sigma^*$ we let*

$$\begin{array}{lcl} \mathsf{ext}(u) & := & \{\sigma \in \Sigma^\omega \mid u \subseteq \sigma\} \\ \mathsf{ext}(U) & := & \bigcup_{u \in U} \mathsf{ext}(u) \end{array}$$

Remark 4.20 (A Base on Streams)**.** *The set $\mathcal{B}_\Sigma \subseteq \mathcal{P}(\Sigma^\omega)$ consisting of all sets of the form $\mathsf{ext}(U)$ for $U \subseteq \Sigma^*$ **finite** can be used as a base for a topology on Σ^ω. It is easy to see that this topology coincides with that of Def. 4.15.*

Proof. Note that we have $\mathsf{ext}(\emptyset) = \emptyset$. Moreover, sets of streams the form $\mathsf{ext}(U)$ for $U \subseteq \Sigma^*$ are closed under finite intersections. Since $\Sigma^\omega = \mathsf{ext}(\{\varepsilon\})$, we just have to consider the case of binary intersections. But for $U, V \subseteq \Sigma^*$ we have

$$\begin{array}{lcl} \mathsf{ext}(U) \cap \mathsf{ext}(V) & = & \left(\bigcup_{u \in U} \mathsf{ext}(u)\right) \cap \left(\bigcup_{v \in V} \mathsf{ext}(v)\right) \\ & = & \bigcup_{\substack{u \in U \\ v \in V}} \mathsf{ext}(u) \cap \mathsf{ext}(v) \end{array}$$

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

As a consequence, the set $\mathcal{B}_\Sigma \subseteq \mathcal{P}(\Sigma^\omega)$ consisting of all sets of the form $\mathsf{ext}(U)$ for $U \subseteq \Sigma^*$ **finite** can be used as a base for a topology on Σ^ω. It is easy to see that it coincides with that of Def. 4.15. □

Remark 4.21 (On Finite or Infinite Words)**.** *While we focus on infinite words $\sigma \in \Sigma^\omega$, it is sometimes useful to topologize the set Σ^∞ of finite or infinite words (see Notation 1.2, §1.1). A good (advanced) example in the context of this course is [VVK05]. We refer to [PP04, §III.4] for a detailed account of Σ^∞ as a topological space.*

Remark 4.22 (An Informal Analogy with Recursively Enumerable Sets)**.** *Given a finite word $u \in \Sigma^*$ and an ω-word $\sigma \in \Sigma^\omega$, we can check whether $\sigma \in \mathsf{ext}(u)$ by only inspecting a finite prefix of σ. Consider now an open set $\mathsf{ext}(W)$ with $W \subseteq \Sigma^*$, and assume that we want to check whether $\sigma \in \mathsf{ext}(W)$. If it happens that $\sigma \in \mathsf{ext}(W)$, then we can know this after checking whether $\sigma \in \mathsf{ext}(w)$ for only finitely many $w \in W$. But if $\sigma \notin \mathsf{ext}(W)$, then we might have to check whether $\sigma \in \mathsf{ext}(w)$ for infinitely many $w \in W$.*

This suggests an analogy between membership of an ω-word to a given open subset of Σ^ω on the one hand, and membership of a natural number to a given recursively enumerable set on the other hand. This mere analogy can actually be made formal, as detailed in [Mos09, Chap. 3] (outside the scope of this course).

4.2.1 Topological Safety and Liveness

Lemma 4.23. *An LT property is closed if and only if it is a safety property.*

Proof. Assume first that $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ is the safety property induced by $P_{\mathrm{bad}} \subseteq (\mathbf{2}^{\mathrm{AP}})^*$. Then P is closed as

$$P \quad = \quad (\mathbf{2}^{\mathrm{AP}})^\omega \setminus \bigcup_{u \in P_{\mathrm{bad}}} \mathsf{ext}(u)$$

Conversely, if P is closed then $(\mathbf{2}^{\mathrm{AP}})^\omega \setminus P$ is open, say

$$(\mathbf{2}^{\mathrm{AP}})^\omega \setminus P \quad = \quad \bigcup_{u \in P_{\mathrm{bad}}} \mathsf{ext}(u)$$

for some $P_{\mathrm{bad}} \subseteq (\mathbf{2}^{\mathrm{AP}})^*$. But then P is the safety property induced by P_{bad}. □

Lemma 4.24. *An LT property is dense if and only if it is a liveness property.*

Proof. Assume first that $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ is a liveness property. Let U be a non-empty open set. Then $\mathsf{ext}(u) \subseteq U$ for some $u \in (\mathbf{2}^{\mathrm{AP}})^*$. But since P is a liveness property, we have $\sigma \in P$ for some $\sigma \in \mathsf{ext}(u)$. Hence $\sigma \in P \cap U$.

Conversely, assume that P is dense. Given $u \in (\mathbf{2}^{\mathrm{AP}})^*$, we have $P \cap \mathsf{ext}(u) \neq \emptyset$. Hence there is some $\sigma \in P$ such that $u \subseteq \sigma$. It follows that P is a liveness property. □

The Decomposition Theorem 3.42 is thus a direct consequence of the Topological Decomposition Theorem 4.11.

Corollary 4.25 (Decomposition (Thm. 3.42))**.** *For every LT property $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$, there is a safety property P_{safe} and a liveness property P_{liveness} such that*

$$P \quad = \quad P_{\mathit{safe}} \cap P_{\mathit{liveness}}$$

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

Corollary 4.26. *An LT property $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ is a liveness property if and only if $\overline{P} = (\mathbf{2}^{\mathrm{AP}})^\omega$.*

Corollary 4.26 is a direct consequence of Lem. 4.24 and Lem. 4.12.

5 Partial Orders and Complete Lattices

In this Section, we introduce some basic concepts and facts pertaining to partial orders and complete lattices. These will be used for different purposes in this course.

First, these tools provide a purely order-theoretic proof of the Decomposition Theorem 3.42 (essentially as in [BK08, Thm. 3.37]). Moreover, some order-theoretic notions which are good generalizations of topological ones can serve as useful abstractions for the latter. Further, some basic order-theoretic notions presented here lay the ground to lattice-theoretic concepts which are important for Stone's Representation Theorem (§8).

Second, complete lattices have a nicely behaved notion of **fixpoint** on which we rely to define (and reason on) the logic LTL in §7.

We mainly refer to [DP02], and 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 $b \leq a$.*

Example 5.2. *The following are simple but important examples of partial orders which are not **linear** (i.e. in which $a \not\leq b$ may **not** imply $b \leq a$):*

(1) $(\Sigma^*, \subseteq)$ where Σ has at least two elements.

(2) $(\mathcal{P}(X), \subseteq)$ for a set X.

(3) $(\Omega X, \subseteq)$ for a topological space $(X, \Omega X)$.

Definition 5.3. *The **opposite** of a partial order $(A, \leq)$ is the partial order $(A, \leq)^{\mathrm{op}} := (A, \geq)$ where $a \geq b$ iff $b \leq a$.*

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

Definition 5.4 (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 $a \leq_A a'$.*

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

5.2 Complete Lattices

Definition 5.5. *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 in $(A, \leq)^{\mathrm{op}}$. A **greatest lower bound** (or **meet**) $\bigwedge S$ of S is a least upper bound of S in $(A, \leq)^{\mathrm{op}}$.*

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. We refer to [DP02, Def. 2.1] for a slightly more elaborated definition of (least) upper and (greatest) lower bounds.

In the litterature, a least upper bound is sometimes also called a **lub** or a **sup**. Similarly, greatest lower bounds are sometimes called **glb**'s of **infs**.

Remark 5.6. *By antisymmetry, joins and meets are unique whenever they exist.*

Remark 5.7 (On $\mathcal{P}(X)$ and ΩX)**.** *It is easy to see that $(\mathcal{P}(X), \subseteq)$ has all meets and joins, given respectively by intersections and unions.*

For $(X, \Omega X)$ a topological space, it follows from the definition that $(\Omega X, \subseteq)$ has all joins. But does it have all meets? This question may be seen as a motivation for the following definition.

Definition 5.8. *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 5.9. *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 5.10. *The following are equivalent for a partial order $(L, \leq)$:*

(i) $(L, \leq)$ is a complete lattice,

(ii) every subset $S \subseteq L$ has a join $\bigvee S \in L$,

(iii) 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:

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

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. [Joh82].

Definition 5.11. *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:*

$$a \wedge \bigvee S \quad = \quad \bigvee \{a \wedge s \mid s \in S\}$$

Corollary 5.12. *Every frame $(L, \leq)$ is a complete lattice.*

Example 5.13. *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 exists. In particular, for a frame $(L, \leq, \wedge, \bigvee)$, we have

$$a \wedge b \quad = \quad \bigvee \{c \in L \mid c \leq a \text{ and } c \leq b\}$$

Corollary 5.14. *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 5.15. *Consider the space Σ^ω for $\Sigma = \{a, b\}$. The set $S = \bigcap_{n \in \mathbb{N}} \mathsf{ext}(a^n)$ is not open.*

Proof. Indeed, assume $S = \bigcup_{u \in W} \mathsf{ext}(u)$ for some $W \subseteq \Sigma^*$. Then since S contains the ω-word a^ω, we must have $a^\omega \in \mathsf{ext}(u)$ for some $u \in W$. But this implies $u = a^n$ for some $n \in \mathbb{N}$, while $\mathsf{ext}(a^n)$ is not a subset of S since

$$a^n b^\omega \in \mathsf{ext}(a^n) \setminus \mathsf{ext}(a^{n+1})$$

□

Given a topological space $(X, \Omega X)$, following the proof of Lem. 5.10, the meet in ΩX of a family of open sets $S \subseteq \Omega X$ is given by

$$\bigwedge S \quad := \quad \bigcup \{U \in \Omega X \mid \forall V \in S,\ U \subseteq V\}$$

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

Definition 5.16 (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*

$$\mathring{A} \quad := \quad \bigcup\{U \in \Omega X \mid U \subseteq A\}$$

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

Lemma 5.17. *Given a topological space $(X, \Omega X)$, the interior $\mathring{A}$ of $A \subseteq X$ is the largest open set contained in A.*

5.3 Closure Operators

Definition 5.18 ([DP02, Def. 7.1])**.** *A closure operator on a partial order $(L, \leq)$ is a function $c : L \to L$ 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.*

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

Example 5.19. *Given a topological space $(X, \Omega X)$, the operation $\overline{(-)}$ is a closure operator on $\mathcal{P}(X)$ (see Rem. 4.6, §4.1).*

Lemma 5.20 ([DP02, Prop. 7.2])**.** *Consider a closure operator c on a complete lattice $(L, \leq)$. Then L^c is a complete lattice with meets $\bigsqcap$ and joins $\bigsqcup$ given resp. by*

$$\bigsqcap S = \bigwedge S \qquad \text{and} \qquad \bigsqcup S = c(\bigvee S)$$

Proof. Fix a set $S \subseteq L^c$ of closed elements.

We first prove that $\bigwedge S$ is closed. Indeed, for all $s \in S$, we have $\bigwedge S \leq s$, and thus $c(\bigwedge S) \leq s$ since s is closed. It follows that $c(\bigwedge S) \leq \bigwedge S$ and thus $c(\bigwedge S) = \bigwedge S$ since c is expansive. We now show that $\bigwedge S$ is the meet of S **in** L^c. But given $b \in L^c$ such that $b \leq s$ for all $s \in S$, we of course have $b \leq \bigwedge S$.

We now turn to the case of joins. We have to show that $c(\bigvee S)$ is the join of S in L^c. Let $b \in L^c$ such that $s \leq b$ for all $s \in S$. We then of course have $\bigvee S \leq b$, and thus $c(\bigvee S) \leq c(b) = b$. □

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

Lemma 5.21. *Consider a closure operator c on a complete lattice $(L, \leq)$. Then for all $a \in L$ we have*

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

Proof. Fix $a \in L$. Given b such that $a \leq c(b)$, we have $c(a) \leq c(b)$. It follows that $c(a) \leq \bigwedge\{c(b) \mid a \leq c(b)\}$. For the reverse direction, note that $a \leq c(a)$, so that $\bigwedge\{c(b) \mid a \leq c(b)\} \leq c(a)$ as $c(a) \in \{c(b) \mid a \leq c(b)\}$. □

5.4 Galois Connections

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

Definition 5.22. *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*

$$\begin{array}{rcccl} g & : & A & \longrightarrow & B \\ f & : & B & \longrightarrow & A \end{array}$$

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

$$g(a) \leq_B b \qquad \text{iff} \qquad a \leq_A f(b)$$

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

Remark 5.23. *It immediately follows from Def. 5.22 that in a Galois connection $g \dashv f$, f is uniquely determined by g and g is uniquely determined by f.*

Proof. Assume $g \dashv f$ and $g \dashv f'$ with $g : A \to B$. Given $b \in B$ we have $f'(b) \leq_A f(b)$ since $g(f'(b)) \leq_B b$, which itself follows from $f'(b) \leq_A f'(b)$. We similarly get $f(b) \leq_A f'(b)$. The case of $g \dashv f$ and $g' \dashv f$ is similar. □

Lemma 5.24 ([DP02, Lem. 7.26])**.** *If $g \dashv f : A \to B$ form a Galois connection, then both f and g are monotone.*

Proof. First note that for all $a \in A$ and all $b \in B$, since $g(a) \leq_B g(a)$ and $f(b) \leq_A f(b)$, we have

$$a \leq_A (f \circ g)(a) \qquad \text{and} \qquad (g \circ f)(b) \leq_B b$$

Then for $a \leq_A a'$ and $b \leq_B b'$ we have

$$a \leq_A a' \leq_A (f \circ g)(a') \qquad \text{and} \qquad (g \circ f)(b) \leq_B b \leq_B b'$$

and thus

$$g(a) \leq_B g(a') \qquad \text{and} \qquad f(b) \leq_A f(b')$$

□

Lemma 5.25 ([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. Let $c : A \to A$ be $f \circ g$. First, c is monotone as a composite of two monotone maps. Second, we have $a \leq c(a)$ since

$$g(a) \leq_B g(a) \qquad \Longleftrightarrow \qquad a \leq_A (f \circ g)(a)$$

Finally, we have $c(c(a)) \leq_A c(a)$ since $(g \circ f \circ g)(a) \leq_A g(a)$, the latter being given by

$$(g \circ f \circ g)(a) \leq_B g(a) \qquad \Longleftrightarrow \qquad (f \circ g)(a) \leq_A (f \circ g)(a)$$

□

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 Σ^ω by a closure operator induced by a Galois connection. This in particular gives another proof of the Decomposition Theorem 3.42 (see §5.5.1). We loosely follow the approach [BK08, Chap. 3]. Recall the definition of $\mathrm{Pref}(\sigma)$ from Notation 1.2 (§1.1).

Given a non-empty set Σ, define

$$\begin{array}{rcrcl} \mathrm{Pref} & : & \mathcal{P}(\Sigma^\omega) & \longrightarrow & \mathcal{P}(\Sigma^*) \\ & & P & \longmapsto & \bigcup\{\mathrm{Pref}(\sigma) \mid \sigma \in P\} \end{array}$$

$$\begin{array}{rcrcl} \mathrm{cl} & : & \mathcal{P}(\Sigma^*) & \longrightarrow & \mathcal{P}(\Sigma^\omega) \\ & & W & \longmapsto & \{\sigma \in \Sigma^\omega \mid \mathrm{Pref}(\sigma) \subseteq W\} \end{array}$$

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

Lemma 5.26. *For all $P \subseteq \Sigma^\omega$ and all $W \subseteq \Sigma^*$ we have*

$$\mathrm{Pref}(P) \subseteq W \qquad \textit{iff} \qquad P \subseteq \mathrm{cl}(W)$$

Proof. Exercise! □

It thus follows from Lem. 5.25 that

$$\mathrm{cl} \circ \mathrm{Pref} \quad : \quad \mathcal{P}(\Sigma^\omega) \quad \longrightarrow \quad \mathcal{P}(\Sigma^\omega)$$

is a closure operator. Note that

$$\begin{array}{rcl} \mathrm{cl}(\mathrm{Pref}(P)) & = & \{\sigma \in \Sigma^\omega \mid \mathrm{Pref}(\sigma) \subseteq \mathrm{Pref}(P)\} \\ & = & \{\sigma \in \Sigma^\omega \mid \forall \hat{\sigma} \subseteq \sigma,\ \exists \beta \in P,\ \hat{\sigma} \subseteq \beta\} \end{array}$$

Proposition 5.27. *Given $P \subseteq \Sigma^\omega$, we have*

$$\overline{P} \quad = \quad \mathrm{cl}(\mathrm{Pref}(P))$$

Proof. Exercise! □

Recall Def. 3.31 (§3.2.5). Note that for a tree $T \subseteq \Sigma^*$, the set $\mathrm{cl}(T)$ defined above is exactly the set of infinite paths of T (see Ex. 4.18, §4.2). We thus obtain the following.

Corollary 5.28. *A subset C of Σ^ω is closed if and only if C is the set of infinite paths of some tree $T \subseteq \Sigma^*$.*

Notation 5.29. *Given $P \subseteq \Sigma^\omega$ we often write* $\mathrm{cl}(P)$ *for* $\mathrm{cl}(\mathrm{Pref}(P))$. *With this notation,* $\mathrm{cl}(P)$ *is* $\mathrm{closure}(P)$ *in the sense of [BK08, Def. 3.26].*

Proposition 5.27, together with the fact that safety properties $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ are the topologically closed subsets of $(\mathbf{2}^{\mathrm{AP}})^\omega$ (Lem. 4.23), gives the following. A direct proof is nevertheless possible.

Corollary 5.30. *An LT property* $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ *is a safety property if and only if* $P = \mathrm{cl}(P)$*.*

Together with Corollary 4.26, Prop. 5.27 gives the following.

Corollary 5.31. *An LT property* $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ *is a liveness property iff* $\mathrm{cl}(P) = (\mathbf{2}^{\mathrm{AP}})^\omega$*.*

We moreover have the following.

Proposition 5.32. *An LT property* $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ *is a liveness property iff* $\mathrm{Pref}(P) = (\mathbf{2}^{\mathrm{AP}})^*$*.*

Proof. Exercise! □

5.5.1 Alternative Proof of the Decomposition Theorem 3.42

The Galois connection $\mathrm{Pref} \dashv \mathrm{cl} : \mathcal{P}(\Sigma^\omega) \to \mathcal{P}(\Sigma^*)$ gives an alternative, more combinatorial proof of Thm. 3.42, following the lines of [BK08, Thm. 3.37]. The combinatorial content of the argument is contained in the following.

Lemma 5.33 ([BK08, Lem. 3.36])**.** *Given* $P, Q \subseteq \Sigma^\omega$*, we have*

$$\mathrm{cl}(P \cup Q) \quad = \quad \mathrm{cl}(P) \cup \mathrm{cl}(Q)$$

Lemma 5.33 directly follows from Lem. 4.5 and Prop. 5.27. A direct (more combinatorial) proof is nevertheless possible.

Direct Proof of Lemma 5.33. We have $\mathrm{cl}(P) \cup \mathrm{cl}(Q) \subseteq \mathrm{cl}(P \cup Q)$ by monotonicity of $\mathrm{cl}(-)$. For the converse inclusion, let $\sigma \in \mathrm{cl}(P \cup Q)$. Hence for every $n \in \mathbb{N}$ there is some $\beta_n \in \Sigma^\omega$ such that $\sigma(0) \cdots \sigma(n) \subseteq \beta$ and $\beta_n \in P \cup Q$. By the infinite pigeonhole principle, we have (say) $\beta_n \in P$ for infinitely many $n \in \mathbb{N}$. Hence, given $\beta_k \notin P$, there is some $n > k$ such that $\beta_n \in P$. But we have

$$\sigma(0) \cdots \sigma(k) \subseteq \sigma(0) \cdots \sigma(n) \subseteq \beta_n$$

In other words, β_n is an extension of $\sigma(0) \cdots \sigma(k)$ which is in P. As a consequence, each $\sigma(0) \cdots \sigma(n)$ has an extension in P, and $\sigma \in \mathrm{cl}(P)$. □

Remark 5.34. *As a consequence,* $\mathrm{cl} : \mathcal{P}(\Sigma^\omega) \to \mathcal{P}(\Sigma^\omega)$ *is a Kuratowski closure operator (see Rem. 4.6).*

The proof of Thm. 3.42 given in [BK08] then proceeds by the following. The decomposition has the same shape as in the general topological Thm. 4.11.

Corollary 5.35 ([BK08, Thm. 3.37])**.** *For every LT property* $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$*, we have*

$$P \quad = \quad \mathrm{cl}(P) \quad \cap \quad \big(P \cup \big((\mathbf{2}^{\mathrm{AP}})^\omega \setminus \mathrm{cl}(P)\big)\big)$$

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

Proof. We obviously have

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

The set $\mathrm{cl}(P)$ is evidently closed. So to conclude, we show that

$$D \quad := \quad P \cup ((\mathbf{2}^{\mathrm{AP}})^\omega \setminus \mathrm{cl}(P))$$

is dense. In view of Cor. 5.31 we have to show that $\mathrm{cl}(D) = (\mathbf{2}^{\mathrm{AP}})^\omega$. But by Lem. 5.33 we have

$$\mathrm{cl}(D) \quad = \quad \mathrm{cl}(P) \cup \mathrm{cl}\big((\mathbf{2}^{\mathrm{AP}})^\omega \setminus \mathrm{cl}(P)\big)$$

The result then follows from the fact that

$$(\mathbf{2}^{\mathrm{AP}})^\omega \setminus \mathrm{cl}(P) \quad \subseteq \quad \mathrm{cl}\big((\mathbf{2}^{\mathrm{AP}})^\omega \setminus \mathrm{cl}(P)\big)$$

□

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 5.36 ([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. Consider first some $S \subseteq A$ such that $\bigvee S$ exists in A. We claim that $g(\bigvee S)$ is the least upper bound in B of

$$g(S) \quad := \quad \{g(s) \mid s \in S\}$$

It is clear from the monotonicity of g that $g(\bigvee S)$ is an upper bound of $g(S)$. It remains to show that $g(\bigvee S)$ is the **least** upper bound of $g(S)$. Consider now some $b \in B$ such that $g(s) \leq_B b$ for all $s \in S$. Then for all $s \in S$ we have $s \leq_A f(b)$. But this implies $\bigvee S \leq_A f(b)$ and thus $g(\bigvee S) \leq b$.

The case of $\bigwedge S$ for $S \subseteq A$ is dual (since a meet in L is a join in L^{op}). We detail it for the sake of completeness. We thus show that $f(\bigwedge S)$ is the greatest lower bound of $f(S)$ in A. It is certainly a lower bound by monotonicity of f. So consider some a such that $a \leq_A f(s)$ for all $s \in S$. This implies that $g(a) \leq_B s$ for all $s \in S$ and thus that $g(a) \leq_B \bigwedge S$. We then deduce that $a \leq_A f(\bigwedge S)$. □

Lemma 5.36 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. 5.36 has a converse.

Lemma 5.37 ([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. By duality, we only discuss the case of $f : B \to A$. Assuming that f preserves meets, we define $g : A \to B$ as

$$g(a) \quad := \quad \bigwedge\{b \mid a \leq_A f(b)\}$$

Assume that $a \leq_A f(b)$. Then we have

$$g(a) \quad = \quad \bigwedge\{b' \mid a \leq_A f(b')\} \quad \leq_B \quad b$$

Conversely, assume that $g(a) \leq_B b$. Then by assumption on f we have

$$a \quad \leq_A \quad \bigwedge\{f(b') \mid a \leq_A f(b')\} \quad = \quad f\left(\bigwedge\{b' \mid a \leq_A f(b')\}\right) \quad = \quad f(g(a)) \quad \leq_A \quad f(b)$$

□

The categorical generalization of Lem. 5.37 actually involves more complex conditions. See e.g. [ML98, §V.6] and [Awo10, §9.8].

Example 5.38 ((Complete) Heyting Algebras)**.** *Let $(A, \leq)$ be a complete lattice. Given $a \in A$, consider the map*

$$\begin{array}{rcrcl} (-) \wedge a & : & A & \longrightarrow & A \\ & & b & \longmapsto & b \wedge a \end{array}$$

It follows from Lem. 5.36 and Lem. 5.37 that $(-) \wedge a$ has an upper adjoint if and only if $(-) \wedge a$ preserves all joins. Note that the latter exactly means that for all $S \subseteq A$, we have

$$\left(\bigvee S\right) \wedge a \quad = \quad \bigvee\{s \wedge a \mid s \in S\}$$

Hence, A is a frame (Def. 5.11, §5.2) if and only if each map $(-) \wedge a$ (for $a \in A$) has an upper adjoint.

Upper adjoints to $(-) \wedge a$ are often denoted $a \Rightarrow (-)$, since $(-) \wedge a \dashv a \Rightarrow (-)$ means

$$(b \wedge a) \leq c \qquad \textit{iff} \qquad b \leq (a \Rightarrow c)$$

so that $a \Rightarrow c$ is reminiscent from a logical implication.

*Frames are also called **complete Heyting algebras**. Anticipating on the terminology of §**??**, a **Heyting algebra** is a lattice A (i.e. a partial order in which has all **finite** joins and all **finite** meets) such that each map $(-) \wedge a$ (for $a \in A$) has an upper adjoint $a \Rightarrow (-)$. Note that this implies (by Lem. 5.36) that a Heyting algebra is automatically **distributive**, in the sense that for all $a, b, c \in A$ we have*

$$(c \vee b) \wedge a \quad = \quad (c \wedge a) \vee (b \wedge a)$$

Note also that what we called a "complete Heyting algebra" is nothing else but a Heyting algebra which happens to be complete as a lattice.

*Heyting algebras are the appropriate notion of truth values for **intuitionistic** propositional logic (see e.g. [SU06, §2.4] or [Awo10, §6.3], outside the scope of this course).*

We have seen in Lem. 5.25 that Galois connections induce closure operators. The converse, namely that every Galois connection 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 5.39 ([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. 5.39 generalizes to the well-known adjunction between a category $\mathbb{C}$ and the Eilenberg-Moore category $\mathbb{C}^T$ of a monad T on $\mathbb{C}$, see e.g. [ML98, §VI.2].

5.6.1 On the Kleisli Construction

The notion of closure operator on a partial order of Def. 5.18 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. 5.22), 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 $\mathbb{C}$, namely the adjunction between $\mathbb{C}$ and its Kleisli category $\mathbb{C}_T$. We refer to e.g. [ML98, §VI.5] for details.

Lemma 5.40. *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 $\mathsf{ext}(V)$, for a **finite** $V \subseteq (\mathbf{2}^{\mathrm{AP}})^*$, 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

$$\begin{array}{rcll} f^{-1} & : & \mathcal{P}(Y) & \longrightarrow & \mathcal{P}(X) \\ & & B & \longmapsto & \{x \mid f(x) \in B\} \end{array}$$

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 $(\mathcal{P}(Y), \bigcap, \bigcup, Y \setminus (-), Y, \emptyset)$ to $(\mathcal{P}(X), \bigcap, \bigcup, X \setminus (-), X, \emptyset)$.*

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. Consider some $S \subseteq \mathcal{P}(Y)$. Then for $x \in X$ we have

$$\begin{array}{lll} x \in f^{-1}(\bigcap S) & \text{iff} & \forall B \in S,\ x \in f^{-1}(B) \\ x \in f^{-1}(\bigcup S) & \text{iff} & \exists B \in S,\ x \in f^{-1}(B) \end{array}$$

Moreover,

$$\begin{array}{lll} f^{-1}(Y) & = & X \\ f^{-1}(\emptyset) & = & \emptyset \end{array}$$

□

Definition 6.2 (Continuous Function)**.** *Consider topological spaces $(X, \Omega X)$ and $(Y, \Omega Y)$.*

(1) 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.*

(2) We say that $f : X \to Y$ is an ***homeomorphism*** *if f is a continuous bijection with continuous inverse $Y \to X$.*

Lemma 6.3. *A function $f : \Sigma^\omega \to \Gamma^\omega$ is continuous iff*

$$\forall n \in \mathbb{N},\ \forall \alpha \in \Sigma^\omega,\ \exists k \in \mathbb{N},\ \forall \beta \in \Sigma^\omega \Big(\beta(0) \cdots \beta(k) = \alpha(0) \cdots \alpha(k) \implies \\ f(\beta)(0) \cdots f(\beta)(n) = f(\alpha)(0) \cdots f(\alpha)(n) \Big)$$

Proof. Assume first that f is continuous. Given $\alpha \in \Sigma^\omega$ and $n \in \mathbb{N}$, let $v := f(\alpha)(0) \cdots f(\alpha)(n)$. The set

$$U \quad := \quad f^{-1}(\mathsf{ext}(v))$$

is open in Σ^ω, and since $\alpha \in U$, there is some $k \in \mathbb{N}$ such that $\mathsf{ext}(\alpha(0) \cdots \alpha(k)) \subseteq U$.

For the converse, let V be an open of Γ^ω. If $f^{-1}(\Gamma)$ is empty then the result is trivial. Otherwise, let $\alpha \in f^{-1}(\Gamma)$. We are done if we show that $\mathsf{ext}(\alpha(0) \cdots \alpha(k)) \subseteq f^{-1}(\Gamma)$ for some $k \in \mathbb{N}$. Since $f(\alpha) \in \Gamma$ with Γ open, there is some $n \in \mathbb{N}$ such that with $v := f(\alpha)(0) \cdots f(\alpha)(n)$ we have $\mathsf{ext}(v) \subseteq \Gamma$. But by assumption on f, we indeed have $\mathsf{ext}(\alpha(0) \cdots \alpha(k)) \subseteq f^{-1}(\mathsf{ext}(v))$ for some $k \in \mathbb{N}$. □

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 $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ to be decidable is to have a continuous characteristic function

$$\begin{array}{rcccl} \chi_P & : & (\mathbf{2}^{\mathrm{AP}})^\omega & \longrightarrow & \mathbf{2} \\ & & \alpha & \longmapsto & \begin{cases} 1 & \text{if } \alpha \in P \\ 0 & \text{otherwise} \end{cases} \end{array}$$

where $\mathbf{2}$ is endowed with the **discrete** topology, with which every subset is open. This amounts to ask that both P and $(\mathbf{2}^{\mathrm{AP}})^\omega \setminus P$ 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. □

Definition 6.6 (Observable Property). *An LT property $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ is* ***observable*** *if P is a clopen subset of $(\mathbf{2}^{\mathrm{AP}})^\omega$.*

Let us look more precisely at the observable properties.

Lemma 6.7. *In Σ^ω, each set of the form $\mathsf{ext}(u)$ for $u \in \Sigma^*$ is clopen.*

Proof. Exercise! □

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

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

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

is obviously open. It is also closed as being the complement of $\mathsf{ext}(0)$*. But P cannot be presented as the extension of a finite set $U \subseteq \mathbb{N}^*$.*

We shall see in Prop. 6.15 that when AP is finite, the observable $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ are **exactly** the sets of the form $\bigcup_{u \in U} \mathsf{ext}(u)$ for a finite $U \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$. This relies on a strong topological property of $(\mathbf{2}^{\mathrm{AP}})^\omega$ 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 contains a finite cover of A, in the sense that 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.*

A metric space is compact in the sense of Definition 6.9 precisely when it is sequentially compact (every sequence has a convergent subsequence), see e.g. [Run05, Theorem 2.5.10]. Beware however that in general, the two notions differ (see e.g. [Run05, Example 3.3.22]).

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. 6.20).

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

Proof. Exercise! □

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

Lemma 6.11. *Consider the space of ω-words Σ^ω for some non-empty set Σ. If Σ is infinite, then Σ^ω is not compact.*

Proof. Indeed, we have

$$\Sigma^\omega \quad = \quad \bigcup_{a \in \Sigma} \mathsf{ext}(a)$$

But if Σ is infinite, one cannot extract a finite subcover of Σ^ω from $(\mathsf{ext}(a))_{a \in \Sigma}$. □

We now show that Σ^ω is compact when Σ is finite. We rely on Kőnig's Lemma 3.32 (§3.2.5).

Proposition 6.12. *Let Σ be a* ***finite*** *non-empty set. Then Σ^ω is compact.*

Proof. Consider an open covering $(U_i)_{i\in I}$ of Σ^ω. Note that each U_i is of the form $\bigcup_{v\in V_i}\mathsf{ext}(v)$ for some $V_i \subseteq \Sigma^*$. 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 $u \in \Sigma^*$ 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 $\mathsf{ext}(v) \subseteq \mathsf{ext}(w)$ (Lem. 4.16), W induces a cover of Σ^ω as

$$\Sigma^\omega \quad = \quad \bigcup_{v\in V}\mathsf{ext}(v) \quad = \quad \bigcup_{w\in W}\mathsf{ext}(w)$$

Hence we are done if W is finite. Assume toward a contradiction that W is infinite. Let $T \subseteq \Sigma^*$ 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 Σ is finite, and T is infinite as W is infinite. Hence, by Kőnig's Lemma 3.32, T has a path π. Since W induces a cover of Σ^ω, we have $w \subseteq \pi$ for some $w \in W$. Since π is a path in T, we have $w.a \subseteq \pi$ for some $w.a \in T$ with $a \in \Sigma$. 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 Σ^ω is the product topology in the usual sense (taking Σ 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. In the simple case of Σ^ω, we used Kőnig's Lemma 3.32, a much weaker principle of infinite combinatorics (see e.g. [Sim10, Ex. I.8.8]).*

Remark 6.14. *It is possible to prove Prop. 6.12 without explicitly relying on Kőnig's Lemma 3.32 (see e.g. [PP04, §III.3.5]). Actually, one can obtain Kőnig's Lemma 3.32 from a strengthening of Prop. 6.12 stating the relative compactness of subspaces of Σ^ω (with Σ possibly infinite). See e.g. [PP04, Ex. III.8.6] (outside the scope of this course).*

Proposition 6.15 (Observable Property – The Compact Case)**.** *If AP is finite, then $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ is observable iff $P = \bigcup_{u\in U}\mathsf{ext}(u)$ for some* ***finite*** *$U \subseteq (\mathbf{2}^{\mathrm{AP}})^*$.*

Proof. We already know from Lem. 6.7 and Lem. 6.5 that the condition is sufficient.

Let $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ be clopen, hence compact open. Then $P = \bigcup_{u\in U}\mathsf{ext}(u)$ for some $U \subseteq (\mathbf{2}^{\mathrm{AP}})^*$. Since P is compact, there is a finite subset $V \subseteq U$ such that $P \subseteq \bigcup_{u\in V}\mathsf{ext}(u)$. But this implies $P = \bigcup_{u\in V}\mathsf{ext}(u)$ as $V \subseteq U$. □

6.2.1 The Finite Intersection Property

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

Definition 6.16 (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 6.17. *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! □

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 6.18 (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 6.19. *Spaces of ω-words Σ^ω 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 6.20. *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 $C \subseteq V_{y_1} \cup \cdots \cup V_{y_n}$. □

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.

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 $(\mathbf{2}^{\mathrm{AP}})^\omega$.

7.1.1 Syntax and Semantics of LML

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

$$\begin{array}{lll} \varphi, \psi & ::= & \top \quad | \quad \bot \quad | \quad X \quad | \quad \mathsf{a} \qquad\qquad \text{(where } X \in \mathcal{X} \text{ and } \mathsf{a} \in \mathrm{AP}) \\ & | & \varphi \wedge \psi \quad | \quad \varphi \vee \psi \quad | \quad \neg\varphi \\ & | & \bigcirc\varphi \end{array}$$

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

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

*(1) A **valuation** of a set of variables $V \subseteq \mathcal{X}$ is a function $\rho : V \to \mathcal{P}((\mathbf{2}^{\mathrm{AP}})^\omega)$.*

*(2) A **formula with parameters** is a pair (φ, ρ) of a formula φ and a valuation $\rho : V \to \mathcal{P}((\mathbf{2}^{\mathrm{AP}})^\omega)$ where V contains all the variables of φ.*

*We often speak of a **formula φ with parameters** ρ for the pair (φ, ρ).*

Consider a formula φ with parameters ρ. We define the interpretation $[\![\varphi]\!]_\rho \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ by induction on φ as follows:

$$\begin{array}{rcl} [\![X]\!]_\rho & := & \rho(X) \\ [\![\mathsf{a}]\!]_\rho & := & \big\{\sigma \in (\mathbf{2}^{\mathrm{AP}})^\omega \mid \mathsf{a} \in \sigma(0)\big\} \\ [\![\top]\!]_\rho & := & (\mathbf{2}^{\mathrm{AP}})^\omega \\ [\![\bot]\!]_\rho & := & \emptyset \\ [\![\varphi \wedge \psi]\!]_\rho & := & [\![\varphi]\!]_\rho \cap [\![\psi]\!]_\rho \\ [\![\varphi \vee \psi]\!]_\rho & := & [\![\varphi]\!]_\rho \cup [\![\psi]\!]_\rho \\ [\![\neg\varphi]\!]_\rho & := & (\mathbf{2}^{\mathrm{AP}})^\omega \setminus [\![\varphi]\!]_\rho \\ [\![\bigcirc\varphi]\!]_\rho & := & \big\{\sigma \in (\mathbf{2}^{\mathrm{AP}})^\omega \mid \sigma{\upharpoonright}1 \in [\![\varphi]\!]_\rho\big\} \end{array}$$

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

$$\begin{array}{rcl} \sigma & = & \sigma(0) \cdot \sigma(1) \cdot \dots \cdot \sigma(n) \cdot \ \dots \\ \sigma{\upharpoonright}1 & = & \sigma(1) \cdot \sigma(2) \cdot \dots \cdot \sigma(n+1) \cdot \ \dots \end{array}$$

Notation 7.2. *Other propositional connectives are defined as usual:*

$$\begin{array}{rcl} \varphi \to \psi & := & \neg\varphi \vee \psi \\ \varphi \leftrightarrow \psi & := & (\varphi \to \psi) \wedge (\psi \to \varphi) \end{array}$$

Definition 7.3. *We say that $\sigma \in (\mathbf{2}^{\mathrm{AP}})^\omega$ **satisfies** a formula φ with parameters ρ if $\sigma \in [\![\varphi]\!]_\rho$.*

Lemma 7.4. *If $\rho(X) = \rho'(X)$ for all variables X which actually occur in φ, then $[\![\varphi]\!]_\rho = [\![\varphi]\!]_{\rho'}$*

In particular, if φ is **closed**, *i.e.* contains no free variable, then $[\![\varphi]\!]_\rho$ does not depend on ρ. In this case, we just write $[\![\varphi]\!]$ for $[\![\varphi]\!]_\rho$.

Notation 7.5. *For a closed φ, we write $\sigma \Vdash \varphi$ for $\sigma \in [\![\varphi]\!]$.*

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

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

$$\begin{array}{lll}
\sigma \Vdash \mathsf{a} & \textit{iff} & \mathsf{a} \in \sigma(0) \\
\sigma \Vdash \top & & \\
\sigma \nVdash \bot & & \\
\sigma \Vdash \varphi \wedge \psi & \textit{iff} & \sigma \Vdash \varphi \textit{ and } \sigma \Vdash \psi \\
\sigma \Vdash \varphi \vee \psi & \textit{iff} & \sigma \Vdash \varphi \textit{ or } \sigma \Vdash \psi \\
\sigma \Vdash \neg\varphi & \textit{iff} & \sigma \nVdash \varphi \\
\sigma \Vdash \bigcirc\varphi & \textit{iff} & \sigma{\upharpoonright}1 \Vdash \varphi
\end{array}$$

7.1.2 Logical Equivalence

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

$$[\![\varphi]\!]_\rho \quad = \quad [\![\psi]\!]_\rho$$

Lemma 7.8. *All the equivalences of Fig. 6 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 $(\mathbf{2}^{\mathrm{AP}})^\omega$. Recall from Prop. 6.15 that when AP is finite, the clopen subsets of $(\mathbf{2}^{\mathrm{AP}})^\omega$ are exactly the finite unions of sets of the form $\mathsf{ext}(\hat{\sigma})$ for $\hat{\sigma} \in (\mathbf{2}^{\mathrm{AP}})^*$. Recall moreover from Lem. 6.5 that clopen sets are closed under complements, finite unions and finite intersections.

Semilattices Laws:

$$\begin{array}{rcl@{\qquad}rcl}
\varphi \vee \varphi & \equiv & \varphi & \varphi \wedge \varphi & \equiv & \varphi \\
\varphi \vee \psi & \equiv & \psi \vee \varphi & \varphi \wedge \psi & \equiv & \psi \wedge \varphi \\
\varphi \vee \bot & \equiv & \varphi & \varphi \wedge \top & \equiv & \varphi \\
\varphi \vee (\psi \vee \theta) & \equiv & (\varphi \vee \psi) \vee \theta & \varphi \wedge (\psi \wedge \theta) & \equiv & (\varphi \wedge \psi) \wedge \theta
\end{array}$$

Absorptive Laws (Lattice Laws):

$$\begin{array}{rcl}
\varphi \vee (\varphi \wedge \psi) & \equiv & \varphi \\
\varphi \wedge (\varphi \vee \psi) & \equiv & \varphi
\end{array}$$

Distributive Laws:

$$\begin{array}{rcl}
\varphi \vee (\psi \wedge \theta) & \equiv & (\varphi \vee \psi) \wedge (\varphi \vee \theta) \\
\varphi \wedge (\psi \vee \theta) & \equiv & (\varphi \wedge \psi) \vee (\varphi \wedge \theta)
\end{array}$$

Boolean Algebra Laws:

$$\varphi \wedge \neg\varphi \equiv \bot \qquad \varphi \vee \neg\varphi \equiv \top$$

Duality (De Morgan) Laws:

$$\varphi \wedge \psi \equiv \neg(\neg\varphi \vee \neg\psi) \qquad \varphi \vee \psi \equiv \neg(\neg\varphi \wedge \neg\psi) \qquad \varphi \equiv \neg\neg\varphi$$

Modal Laws:

$$\begin{array}{rcl@{\qquad}rcl}
\bigcirc(\varphi \wedge \psi) & \equiv & \bigcirc\varphi \wedge \bigcirc\psi & \bigcirc\top & \equiv & \top \\
\bigcirc(\varphi \vee \psi) & \equiv & \bigcirc\varphi \vee \bigcirc\psi & \bigcirc\bot & \equiv & \bot \\
\bigcirc(\neg\varphi) & \equiv & \neg\bigcirc\varphi & & &
\end{array}$$

Figure 6: Some Usual Laws.

Proposition 7.10. *For each closed* LML*-formula* φ*,* $[\![\varphi]\!]$ *is a clopen subset of* $(\mathbf{2}^{\mathrm{AP}})^{\omega}$*.*

Proof. By induction on φ.

Case of $\mathsf{a} \in \mathrm{AP}$**.** We have

$$[\![\mathsf{a}]\!] \quad = \quad \bigcup\{\mathsf{ext}(A) \mid A \in \mathbf{2}^{\mathrm{AP}} \text{ and } \mathsf{a} \in A\}$$

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

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

Cases of $\top$**,** $\bot$**,** $\neg\varphi$**,** $\varphi \wedge \psi$ **and** $\varphi \vee \psi$**.** By Lem. 6.5.

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

$$[\![\bigcirc\varphi]\!] \quad = \quad \bigcup\{\mathsf{ext}(A.u) \mid u \in U \text{ and } A \in \mathbf{2}^{\mathrm{AP}}\}$$

If AP is finite, then by Prop. 6.15 we can further assume that U is finite, and we are done by Lem. 6.7 and Lem. 6.5 since $\mathbf{2}^{\mathrm{AP}}$ is also finite.

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

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

Proof. We know from Prop. 6.15 that $P = \mathsf{ext}(U)$ for some finite $U \subseteq (\mathbf{2}^{\mathrm{AP}})^*$. We show that $\mathsf{ext}(u)$ 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 $A \in \mathbf{2}^{\mathrm{AP}}$, we have $\mathsf{ext}(A) = [\![\varphi_A]\!]$ where

$$\varphi_A \quad := \quad \left(\bigwedge_{\mathsf{a} \in A} \mathsf{a}\right) \wedge \left(\bigwedge_{\mathsf{a} \in \mathrm{AP} \setminus A} \neg\mathsf{a}\right)$$

Consider now some finite word $u = A_n \cdots A_1 \in (\mathbf{2}^{\mathrm{AP}})^*$. We show by induction on $n \in \mathbb{N}$ that $\mathsf{ext}(u)$ is definable in LML. The base case follows from the fact that $\mathsf{ext}(\varepsilon) = [\![\top]\!]$. As for the induction step, assume that u is definable by ψ_u. Then $A.u$ is definable by $\varphi_A \wedge \bigcirc\psi_u$. □

Proposition 7.11 may not hold when AP is infinite.

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

Proof. Exercise! □

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. 3.41 that the only expressible liveness property is the "true property" $(\mathbf{2}^{\mathrm{AP}})^\omega$. 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

$$\begin{array}{lcl} [\![\Diamond\varphi]\!]_\rho & := & \{\sigma \in (\mathbf{2}^{\mathrm{AP}})^\omega \mid \exists i \in \mathbb{N},\ \sigma{\restriction}i \in [\![\varphi]\!]_\rho\} \\ [\![\Box\varphi]\!]_\rho & := & \{\sigma \in (\mathbf{2}^{\mathrm{AP}})^\omega \mid \forall i \in \mathbb{N},\ \sigma{\restriction}i \in [\![\varphi]\!]_\rho\} \end{array}$$

In the spirit of Notation 7.5, for a closed φ we write

$$\begin{array}{lcl} \sigma \Vdash \Diamond\varphi & \text{iff} & \exists i \in \mathbb{N},\ \sigma{\restriction}i \Vdash \varphi \\ \sigma \Vdash \Box\varphi & \text{iff} & \forall i \in \mathbb{N},\ \sigma{\restriction}i \Vdash \varphi \end{array}$$

Example 7.13. *Let* $\mathsf{a} \in \mathrm{AP}$*.*

(1) $\sigma \Vdash \Diamond\mathsf{a}$ *iff* $\mathsf{a} \in \sigma(i)$ *for some* $i \in \mathbb{N}$*.*

The formula $\Diamond\mathsf{a}$ *defines an open liveness property* $[\![\Diamond\mathsf{a}]\!] \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$*.*

(2) $\sigma \Vdash \Box\mathsf{a}$ *iff* $\mathsf{a} \in \sigma(i)$ *for all* $i \in \mathbb{N}$*.*

The formula $\Box\mathsf{a}$ *defines a safety property* $[\![\Box\mathsf{a}]\!] \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$*.*

(3) $\sigma \Vdash \Box\Diamond\mathsf{a}$ *iff* $\mathsf{a} \in \sigma(i)$ *for infinitely many* $i \in \mathbb{N}$*.*

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

Note that $\Diamond\Box\varphi \to \Box\Diamond\varphi$ *is always true. The formulae* $\Diamond\Box\mathsf{a}$ *and* $\Box\Diamond\mathsf{a}$ *define liveness properties* $[\![\Diamond\Box\mathsf{a}]\!], [\![\Box\Diamond\mathsf{a}]\!] \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ *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*

$$\begin{array}{lcl} \Diamond\varphi & \equiv & \neg\Box\neg\varphi \\ \Box\varphi & \equiv & \neg\Diamond\neg\varphi \\ \Diamond\varphi & \equiv & \varphi \vee \bigcirc\Diamond\varphi \\ \Box\varphi & \equiv & \varphi \wedge \bigcirc\Box\varphi \end{array}$$

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** φ holds at the current time step **or** $\Diamond\varphi$ holds at the next time step.
- $\Box\varphi$ holds at the current time step iff φ 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

$$\begin{array}{lcl} \Diamond\varphi & \equiv & \varphi \vee \bigcirc\varphi \vee \bigcirc\bigcirc\varphi \vee \cdots & \equiv & \bigvee_{n\in\mathbb{N}} \bigcirc^n\varphi \\ \Box\varphi & \equiv & \varphi \wedge \bigcirc\varphi \wedge \bigcirc\bigcirc\varphi \wedge \cdots & \equiv & \bigwedge_{n\in\mathbb{N}} \bigcirc^n\varphi \end{array}$$

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

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

$$\begin{array}{lcccl} [\![\varphi]\!]_\rho(X) & : & \mathcal{P}((\mathbf{2}^{\mathrm{AP}})^\omega) & \longrightarrow & \mathcal{P}((\mathbf{2}^{\mathrm{AP}})^\omega) \\ & & S & \longmapsto & [\![\varphi]\!]_{\rho[S/X]} \end{array}$$

Lemma 7.16. *Let φ be a formula with parameters ρ. Consider the formulae*

$$\varphi_\Diamond(X) \quad := \quad \varphi \vee \bigcirc X \qquad\qquad \varphi_\Box(X) \quad := \quad \varphi \wedge \bigcirc X$$

where X does not occur in φ. Then we have:

(1) $[\![\Diamond\varphi]\!]_\rho$ is the least element of $(\mathcal{P}((\mathbf{2}^{\mathrm{AP}})^\omega), \subseteq)$ such that

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

(2) $[\![\Box\varphi]\!]_\rho$ is the greatest element of $(\mathcal{P}((\mathbf{2}^{\mathrm{AP}})^\omega), \subseteq)$ such that

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

PROOF. Exercise! □

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 φ, then $[\![\varphi]\!]_\rho(X)$ is a monotone (resp. antimonotone) function of $(\mathcal{P}((\mathbf{2}^{\mathrm{AP}})^\omega), \subseteq)$.

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

Definition 7.17 (Positive Negative Variables)**.** *Given an LML-formula φ and a variable X, the relations $X \operatorname{Pos} \varphi$ (X is **positive** in φ) and $X \operatorname{Neg} \varphi$ (X is **negative** in φ) are defined by induction on Fig. 7.*

Lemma 7.18. *Consider a formula φ with parameters ρ and a variable X.*

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

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

$$\frac{}{X \mathrel{\mathrm{Pos}} X} \qquad \frac{X \neq Y}{X \mathrel{\mathrm{Pos}} Y} \qquad \frac{}{X \mathrel{\mathrm{Pos}} \mathsf{a}} \qquad \frac{}{X \mathrel{\mathrm{Pos}} \top} \qquad \frac{}{X \mathrel{\mathrm{Pos}} \bot} \qquad \frac{X \mathrel{\mathrm{Pos}} \varphi}{X \mathrel{\mathrm{Pos}} \bigcirc\varphi}$$

$$\frac{X \mathrel{\mathrm{Pos}} \varphi \qquad X \mathrel{\mathrm{Pos}} \psi}{X \mathrel{\mathrm{Pos}} \varphi \vee \psi} \qquad \frac{X \mathrel{\mathrm{Pos}} \varphi \qquad X \mathrel{\mathrm{Pos}} \psi}{X \mathrel{\mathrm{Pos}} \varphi \wedge \psi} \qquad \frac{X \mathrel{\mathrm{Neg}} \varphi}{X \mathrel{\mathrm{Pos}} \neg\varphi}$$

$$\frac{Y \neq X}{X \mathrel{\mathrm{Neg}} Y} \qquad \frac{}{X \mathrel{\mathrm{Neg}} \mathsf{a}} \qquad \frac{}{X \mathrel{\mathrm{Neg}} \top} \qquad \frac{}{X \mathrel{\mathrm{Neg}} \bot} \qquad \frac{X \mathrel{\mathrm{Neg}} \varphi}{X \mathrel{\mathrm{Neg}} \bigcirc\varphi}$$

$$\frac{X \mathrel{\mathrm{Neg}} \varphi \qquad X \mathrel{\mathrm{Neg}} \psi}{X \mathrel{\mathrm{Neg}} \varphi \vee \psi} \qquad \frac{X \mathrel{\mathrm{Neg}} \varphi \qquad X \mathrel{\mathrm{Neg}} \psi}{X \mathrel{\mathrm{Neg}} \varphi \wedge \psi} \qquad \frac{X \mathrel{\mathrm{Pos}} \varphi}{X \mathrel{\mathrm{Neg}} \neg\varphi}$$

Figure 7: Positive and Negative Occurrences in a Formula.

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 function. Then the **least fixpoint** $\mu(f)$ and the **greatest fixpoint** $\nu(f)$ are given resp. by*

$$\begin{array}{rcl} \mu(f) & = & \bigwedge\{a \in L \mid f(a) \leq a\} \\ \nu(f) & = & \bigvee\{a \in L \mid a \leq f(a)\} \end{array}$$

Proof. Exercise! □

Remark 7.21 (On the Modal μ-Calculus)**.** *The full extension of* LML *with fixpoints is the (linear-time) modal μ-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 μ-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 φ be a formula with parameters ρ and assume that X Pos φ. Let $\psi(X) := \neg\varphi(\neg X)$. Then*

$$\nu([\![\varphi]\!]_\rho(X)) \quad = \quad (\mathbf{2}^{\mathrm{AP}})^\omega \setminus \mu([\![\psi]\!]_\rho(X)) \qquad\qquad \mu([\![\varphi]\!]_\rho(X)) \quad = \quad (\mathbf{2}^{\mathrm{AP}})^\omega \setminus \nu([\![\psi]\!]_\rho(X))$$

Proof. We rely on the Knaster-Tarski Fixpoint Theorem 7.20. We have

$$\begin{array}{rcl}
(\mathbf{2}^{\mathrm{AP}})^\omega \setminus \mu([\![\psi]\!]) & = & (\mathbf{2}^{\mathrm{AP}})^\omega \setminus \bigcap\{A \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega \mid [\![\psi]\!](A) \subseteq A\} \\
& = & \bigcup\{(\mathbf{2}^{\mathrm{AP}})^\omega \setminus A \mid [\![\psi]\!](A) \subseteq A\} \\
& = & \bigcup\{(\mathbf{2}^{\mathrm{AP}})^\omega \setminus A \mid (\mathbf{2}^{\mathrm{AP}})^\omega \setminus [\![\varphi]\!]((\mathbf{2}^{\mathrm{AP}})^\omega \setminus A) \subseteq A\} \\
& = & \bigcup\{(\mathbf{2}^{\mathrm{AP}})^\omega \setminus A \mid (\mathbf{2}^{\mathrm{AP}})^\omega \setminus A \subseteq [\![\varphi]\!]((\mathbf{2}^{\mathrm{AP}})^\omega \setminus A)\} \\
& = & \bigcup\{B \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega \mid B \subseteq [\![\varphi]\!](B)\} \\
& = & \nu([\![\varphi]\!])
\end{array}$$

Dually,

$$\begin{array}{rcl}
(\mathbf{2}^{\mathrm{AP}})^\omega \setminus \nu([\![\psi]\!]) & = & (\mathbf{2}^{\mathrm{AP}})^\omega \setminus \bigcup\{A \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega \mid A \subseteq [\![\psi]\!](A)\} \\
& = & \bigcap\{(\mathbf{2}^{\mathrm{AP}})^\omega \setminus A \mid A \subseteq [\![\psi]\!](A)\} \\
& = & \bigcap\{(\mathbf{2}^{\mathrm{AP}})^\omega \setminus A \mid A \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega \setminus [\![\varphi]\!]((\mathbf{2}^{\mathrm{AP}})^\omega \setminus A)\} \\
& = & \bigcap\{(\mathbf{2}^{\mathrm{AP}})^\omega \setminus A \mid [\![\varphi]\!]((\mathbf{2}^{\mathrm{AP}})^\omega \setminus A) \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega \setminus A\} \\
& = & \bigcap\{B \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega \mid [\![\varphi]\!](B) \subseteq B\} \\
& = & \mu([\![\varphi]\!])
\end{array}$$

□

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 θ. Then using the laws of Fig. 6, we can put $\theta(X)$ in disjunctive normal form, and obtain

$$\theta(X) \quad \equiv \quad \psi \vee \bigvee_{i \in I} \left(\varphi_i \wedge \bigwedge_{j \in J} \bigcirc^{n_{i,j}} X\right)$$

where X does not occur in ψ nor in the φ_i's. If we further assume that **in θ, X occurs under exactly one $\bigcirc$**, then we have

$$\begin{array}{rcl}
\theta(X) & \equiv & \psi \vee \bigvee_{i \in I} (\varphi_i \wedge \bigcirc X) \\
& \equiv & \psi \vee (\varphi \wedge \bigcirc X)
\end{array}$$

where X does not occur in ψ nor in φ.

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 $\theta(X) = \psi \vee (\varphi \wedge \bigcirc X)$. Concretely, we extend the formulae of LML with a modality φ U ψ (pronounced φ **until** ψ), whose semantics is the least fixpoint of $\theta(X) = \psi \vee (\varphi \wedge \bigcirc X)$.

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:

$$\begin{array}{rcl} \varphi, \psi & ::= & \top \quad | \quad \bot \quad | \quad X \quad | \quad \mathsf{a} \qquad\qquad (\text{where } X \in \mathcal{X} \text{ and } \mathsf{a} \in \mathrm{AP}) \\ & | & \varphi \wedge \psi \quad | \quad \varphi \vee \psi \quad | \quad \neg\varphi \\ & | & \bigcirc\varphi \quad | \quad \varphi \,\mathsf{U}\, \psi \end{array}$$

The semantics of LTL-formulae extends that of LML with the clause:

$$[\![\varphi \,\mathsf{U}\, \psi]\!]_\rho \quad := \quad \{\sigma \in (\mathbf{2}^{\mathrm{AP}})^\omega \mid \exists i \in \mathbb{N},\ \sigma{\restriction}i \in [\![\psi]\!]_\rho \text{ and } \forall j < i,\ \sigma{\restriction}j \in [\![\varphi]\!]_\rho\}$$

We extend the notation $\sigma \Vdash$ of Notation 7.5. This gives, for closed φ, ψ,

$$\sigma \Vdash \varphi \,\mathsf{U}\, \psi \quad \text{iff} \quad \exists i \in \mathbb{N},\ \sigma{\restriction}i \Vdash \psi \text{ and } \forall j < i,\ \sigma{\restriction}j \Vdash \varphi$$

7.3.2 Fixpoints and Defined Modalities

It is now time to check that $\varphi \,\mathsf{U}\, \psi$ is indeed the least fixpoint of $\theta(X) = \psi \vee (\varphi \wedge \bigcirc X)$.

Lemma 7.23 ([BK08, Lem. 5.18]). *Given formulae φ, ψ with parameters ρ, $[\![\varphi \,\mathsf{U}\, \psi]\!]_\rho$ is the least fixpoint of $[\![\theta]\!]_\rho(X) : \mathcal{P}((\mathbf{2}^{\mathrm{AP}})^\omega) \to \mathcal{P}((\mathbf{2}^{\mathrm{AP}})^\omega)$, where*

$$\theta(X) \quad := \quad \psi \vee (\varphi \wedge \bigcirc X)$$

Proof. Exercise! □

With the notations of §7.2.3, Lem. 7.23 says that for φ, ψ with parameters ρ and with $\theta(X)$ as in Lem. 7.23 we have

$$[\![\varphi \,\mathsf{U}\, \psi]\!]_\rho \quad = \quad \mu X.[\![\theta]\!]_\rho(X)$$

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 $\nu X.[\![\theta]\!]_\rho(X)$ of $[\![\theta]\!]_\rho(X)$ is given by

$$\nu X.[\![\theta]\!]_\rho(X) \quad = \quad (\mathbf{2}^{\mathrm{AP}})^\omega \setminus \mu X.[\![\neg\theta[\neg X/X]]\!]_\rho(X)$$

By using the laws of Fig. 6, we have

$$\begin{array}{rcl} \neg\theta[\neg X/X] & \equiv & \neg\big(\psi \vee (\varphi \wedge \bigcirc\neg X)\big) \\ & \equiv & \neg\psi \wedge \neg(\varphi \wedge \neg\bigcirc X) \\ & \equiv & \neg\psi \wedge (\neg\varphi \vee \bigcirc X) \\ & \equiv & (\neg\psi \wedge \neg\varphi) \vee (\neg\psi \wedge \bigcirc X) \end{array}$$

It thus follows from Lem. 7.23 that

$$\mu X.[\![\neg\theta[\neg X/X]]\!]_\rho(X) \quad = \quad [\![\neg\psi \,\mathsf{U}\, \neg(\psi \vee \varphi)]\!]_\rho$$

so that

$$\nu X.[\![\theta]\!]_\rho(X) \quad = \quad [\![\neg(\neg\psi \,\mathsf{U}\, \neg(\psi \vee \varphi))]\!]_\rho$$

Notation 7.24 (Weak Until)**.** *Given formulae φ and ψ, we let*

$$\varphi \mathsf{W} \psi \quad := \quad \neg(\neg\psi \mathsf{U} \neg(\psi \vee \varphi))$$

The above discussion leads us to the expected:

Lemma 7.25. *Given formulae φ, ψ with parameters ρ, $[\![\varphi \mathsf{W} \psi]\!]_\rho$ is the greatest fixpoint of $[\![\theta]\!]_\rho(X) : \mathcal{P}((\mathbf{2}^{\mathrm{AP}})^\omega) \to \mathcal{P}((\mathbf{2}^{\mathrm{AP}})^\omega)$, where*

$$\theta(X) \quad := \quad \psi \vee (\varphi \wedge \bigcirc X)$$

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

$$\varphi_\Diamond(X) \quad := \quad \varphi \vee \bigcirc X \qquad\qquad \varphi_\Box(X) \quad := \quad \varphi \wedge \bigcirc X$$

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

$$\begin{array}{rcl} \Diamond\varphi & := & \top \mathsf{U} \varphi \\ \Box\varphi & := & \varphi \mathsf{W} \bot \end{array}$$

Finally, note that while we have presented LTL as the extension of LML with least (and greatest) fixpoints of formulae of the form $\theta(X) = \psi \vee (\varphi \wedge \bigcirc X)$, there are quite simple (positive and guarded) fixpoints which are not definable in LTL.

Proposition 7.27. *Let $\mathsf{a} \in \mathrm{AP}$. There is no closed LTL-formula φ such that $[\![\varphi]\!]$ is the greatest fixpoint of $\theta(X) := \mathsf{a} \wedge \bigcirc\bigcirc X$.*

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. 6, we have the equivalences for LTL-formulae of Fig. 8.

Lemma 7.28. *All the equivalences of Fig. 6 and Fig. 8 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 $\varphi \mathsf{W} \psi$.

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

$$\varphi \mathsf{W} \psi \quad \equiv \quad (\varphi \mathsf{U} \psi) \vee \Box\varphi$$

Proof. Exercise! □

Second, Lem. 7.22 gives the following dualities.

Lemma 7.30. *We have*

$$\begin{array}{rcl} \neg(\varphi \mathsf{W} \psi) & \equiv & \neg\psi \mathsf{U} (\neg\varphi \wedge \neg\psi) \\ \neg(\varphi \mathsf{U} \psi) & \equiv & \neg\psi \mathsf{W} (\neg\varphi \wedge \neg\psi) \end{array}$$

Proof. Exercise! □

Modal Duality Laws:

$$\Diamond\varphi \quad\equiv\quad \neg\Box\neg\varphi \qquad\qquad \Box\varphi \quad\equiv\quad \neg\Diamond\neg\varphi$$

Modal Operators Laws:

$$\begin{array}{rcl@{\qquad\qquad}rcl}
\Diamond(\varphi \lor \psi) & \equiv & \Diamond\varphi \lor \Diamond\psi & \Diamond\bot & \equiv & \bot \\
\Box(\varphi \land \psi) & \equiv & \Box\varphi \land \Box\psi & \Box\top & \equiv & \top
\end{array}$$

Distributive $\bigcirc/\,\mathsf{U}$ Law:

$$\bigcirc(\varphi \mathbin{\mathsf{U}} \psi) \quad\equiv\quad \bigcirc\varphi \mathbin{\mathsf{U}} \bigcirc\psi$$

Expansion Laws:

$$\begin{array}{rcl}
\varphi \mathbin{\mathsf{U}} \psi & \equiv & \psi \lor (\varphi \land \bigcirc\psi) \\
\Diamond\varphi & \equiv & \varphi \lor \bigcirc\Diamond\varphi \\
\Box\varphi & \equiv & \varphi \land \bigcirc\Box\varphi
\end{array}$$

Figure 8: Some Usual LTL Laws.

7.3.4 Positive Normal Forms

By extending the syntax of LTL with the weak until modality $\varphi \mathbin{\mathsf{W}} \psi$, 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 $\mathsf{a} \in \mathrm{AP}$ and on variables $X \in \mathcal{X}$. 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

$$\begin{array}{rcl}
\varphi \mathbin{\mathsf{R}} \psi & \equiv & \neg(\neg\varphi \mathbin{\mathsf{U}} \neg\psi) \\
\varphi \mathbin{\mathsf{U}} \psi & \equiv & \neg(\neg\varphi \mathbin{\mathsf{R}} \neg\psi)
\end{array}$$

We refer to [BK08, §5.1.5] for details.

7.3.5 Satisfaction of LTL-Formulae by Transition Systems

Consider a transition system $TS = (S, \mathrm{Act}, \rightarrow, I, \mathrm{AP}, L)$ over AP. A (closed) LTL-formula φ defines a linear-time property $[\![\varphi]\!] \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$. Hence, we can specialize the notion of satisfaction of LT properties (Def. 3.8) to the following.

Definition 7.31. *Given TS and φ as above, we say that TS **satisfies** φ (notation $TS \mathrel{|\!\!\approx} \varphi$) if $TS \mathrel{|\!\!\approx} [\![\varphi]\!]$ (i.e. if $\mathrm{Tr}^\omega(TS) \subseteq [\![\varphi]\!]$).*

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

8 Toward Stone Duality

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 $(\mathbf{2}^{\mathrm{AP}})^\omega$, this amounts to the Boolean algebra of sets of the form $\mathsf{ext}(W)$ for some **finite** $W \subseteq (\mathbf{2}^{\mathrm{AP}})^*$. In §7, we devised LML, a base modal logic for linear-time properties, whose formulae define exactly the observable properties on $(\mathbf{2}^{\mathrm{AP}})^\omega$. 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 $(\mathbf{2}^{\mathrm{AP}})^\omega$, which allow for recovering the whole set $(\mathbf{2}^{\mathrm{AP}})^\omega$ from the Boolean algebra of clopen sets of its topology, *i.e.* from LML.

We use the following notation.

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

Recall from Lem. 6.10 and Prop. 6.20 that for (X, Ω) compact Hausdorff, $\mathbf{K}\Omega$ coincides with the set of clopen subsets of X. By Prop. 6.12 and Prop. 6.15, we in particular have

$$\mathbf{K}\Omega((\mathbf{2}^{\mathrm{AP}})^\omega) \quad = \quad \{\mathsf{ext}(W) \mid W \subseteq (\mathbf{2}^{\mathrm{AP}})^* \text{ is finite}\}$$

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

$$\mathcal{F}_\sigma \quad := \quad \{\mathsf{ext}(W) \in \mathbf{K}\Omega((\mathbf{2}^{\mathrm{AP}})^\omega) \mid \sigma \in \mathsf{ext}(W)\}$$

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

(1) $(\mathbf{2}^{\mathrm{AP}})^\omega \in \mathcal{F}_\sigma$ and $\emptyset \notin \mathcal{F}_\sigma$.

(2) If $U \in \mathcal{F}_\sigma$ and $U \subseteq V$ with $V \in \mathbf{K}\Omega((\mathbf{2}^{\mathrm{AP}})^\omega)$ then $V \in \mathcal{F}_\sigma$.

(3) If $U \in \mathcal{F}_\sigma$ and $V \in \mathcal{F}_\sigma$ then $U \cap V \in \mathcal{F}_\sigma$.

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

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

Note that for $\sigma, \beta \in (\mathbf{2}^{\mathrm{AP}})^\omega$, we evidently have $\mathcal{F}_\sigma \neq \mathcal{F}_\beta$ whenever $\sigma \neq \beta$. Hence $(\mathbf{2}^{\mathrm{AP}})^\omega$ can be embedded into the set of prime filters on $\mathbf{K}\Omega((\mathbf{2}^{\mathrm{AP}})^\omega)$. Actually, $(\mathbf{2}^{\mathrm{AP}})^\omega$ is in bijection with the set of prime filters on $\mathbf{K}\Omega((\mathbf{2}^{\mathrm{AP}})^\omega)$. This fact, which is part of **Stone's Representation Theorem**, holds for any **Stone space**.

Definition 8.2 (Stone Space)**.** *A **Stone space** is a topological space (X, Ω) which is compact (see Def. 6.9), and satisfies the two following conditions:*

(X, Ω) **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 ($x \in U$ and $y \notin U$) or ($x \notin U$ and $y \in U$).*

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

Note that every Stone space (X, Ω) is Hausdorff (Def. 6.18).

Example 8.3. *It follows from Lem. 6.7 that A^ω is zero-dimensional, whether or not A is finite. Hence $(\mathbf{2}^{\mathrm{AP}})^\omega$ 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 $\mathbf{K}\Omega(\mathbf{Sp}(B))$ for some Stone space $(\mathbf{Sp}(B), \Omega(\mathbf{Sp}(B)))$, called the **spectrum** of B.
- Every Stone space (X, Ω) is homeomorphic to the spectrum of the Boolean algebra $\mathbf{K}\Omega$.

We refer to [Joh82, 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 $\mathfrak{L}(\mathsf{LML})$ be the set of closed LML-formulae quotiented by logical equivalence $\equiv$ (in the sense of Def. 7.7 and Fig. 6, §7.1.2).

(2) Let $\mathfrak{L}(\mathsf{LTL})$ 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 notationaly confuse a closed L-formula φ with its quotient $[\varphi]_\equiv \in \mathfrak{L}(\mathsf{L})$, where, as usual

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

We equip $\mathfrak{L}(\mathsf{L})$ with the partial order

$$\varphi \leq \psi \quad := \quad (\varphi \to \psi) \equiv \top$$

Note that

$$\varphi \leq \psi \quad \text{iff} \quad \varphi \equiv (\varphi \wedge \psi) \quad \text{iff} \quad (\varphi \vee \psi) \equiv \psi$$

and that $\leq$ is indeed a partial order on $\mathfrak{L}(\mathsf{L})$ (*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 $\mathbf{K}\Omega((\mathbf{2}^{\mathrm{AP}})^\omega)$ with $\mathfrak{L}(\mathsf{LML})$. The properties of prime filters underlined above can then be rephrased as follows, for a set $\mathcal{F} \subseteq \mathfrak{L}(\mathsf{LML})$:

- $\mathcal{F}$ 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 $\varphi \wedge \psi \in \mathcal{F}$.
- $\mathcal{F}$ is complete ($\varphi \vee \psi \in \mathcal{F}$ implies either $\varphi \in \mathcal{F}$ or $\psi \in \mathcal{F}$, so that for every φ we have either $\varphi \in \mathcal{F}$ or $\neg\varphi \in \mathcal{F}$).

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

- Every complete consistent theory $\mathcal{F} \subseteq \mathfrak{L}(\mathsf{LML})$ has a model, *i.e.* there is some $\sigma \in (\mathbf{2}^{\mathrm{AP}})^\omega$ such that for all $\varphi \in \mathfrak{L}(\mathsf{LML})$, we have $\sigma \Vdash \varphi$ iff $\varphi \in \mathcal{F}$.

Remark 8.6 (On Lindenbaum-Tarski Algebras)**.** *The set $\mathfrak{L}(\mathsf{L})$ 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).*

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 $TS_i = (S_i, \mathrm{Act}, \rightarrow_i, I_i, \mathrm{AP}, L_i)$. A **bisimulation** between TS_0 and TS_1 is a relation $\mathcal{R} \subseteq S_0 \times S_1$ such that for all $(s_0, s_1) \in \mathcal{R}$ we have*

(i) *$L_0(s_0) = L_1(s_1)$, and*

(ii) *for each $i \in \{0,1\}$ and each $\alpha \in \mathrm{Act}$, if $s_i \xrightarrow{\alpha}_i s'_i$ in TS_i then there is s'_{1-i} in TS_{1-i} such that $s_{1-i} \xrightarrow{\alpha}_{1-i} s'_{1-i}$ and $(s'_0, s'_1) \in \mathcal{R}$.*

Note that in Def. 9.1, TS_0 and TS_1 are required to be over the **same** sets Act and AP of actions and atomic propositions.

Definition 9.2. *We write $TS_0 \approx TS_1$ if there is a bisimulation $\mathcal{R}$ between TS_0 and TS_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 $(s_0, s_1) \in \mathcal{R}$.*

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 $\mathcal{R} \subseteq S_0 \times S_1$ such that $(s_0, s_1) \in \mathcal{R}$. 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 $\mathcal{R}$ is a bisimulation between TS_0 and TS_1, then $\mathcal{R}^{-1} = \{(s_1, s_0) \mid (s_0, s_1) \in \mathcal{R}\}$ 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

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

Proof. Exercise! □

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! □

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 $\mathrm{Tr}^\omega(TS_0) = \mathrm{Tr}^\omega(TS_1)$.*

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 $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$, we have*

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

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

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

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! □

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.

10.1 Kripke Frames and Kripke 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 $TS = (S, \mathrm{Act}, \to, I, \mathrm{AP}, L)$:

- **a transition structure** given by $(S, (\xrightarrow{\alpha})_{\alpha\in\mathrm{Act}})$,
- **a logical (model) structure** given by the state labelling $L : S \to \mathcal{P}(\mathrm{AP})$,
- **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 $\to\ \subseteq S \times \mathrm{Act} \times S$.*
- *A **Kripke model** over* Act *and* AP *is given by a Kripke frame $(S, \mathrm{Act}, \to)$ together with a state labelling $L : S \to \mathcal{P}(\mathrm{AP})$.*

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

10.2 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:

$$\begin{array}{lllr} \varphi, \psi & ::= & \top \mid \bot \mid \mathsf{a} & (\text{where } \mathsf{a} \in \mathrm{AP}) \\ & \mid & \varphi \wedge \psi \mid \varphi \vee \psi \mid \neg\varphi & \\ & \mid & [\alpha]\varphi \mid \langle\alpha\rangle\varphi & (\text{where } \alpha \in \mathrm{Act}) \end{array}$$

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

$$\begin{array}{lll} \varphi \to \psi & := & \neg\varphi \vee \psi \\ \varphi \leftrightarrow \psi & := & (\varphi \to \psi) \wedge (\psi \to \varphi) \end{array}$$

Consider a Kripke model $M = (S, \mathrm{Act}, \to, \mathrm{AP}, L)$. The interpretation $[\![\varphi]\!] \in \mathcal{P}(S)$ of an HML-formula φ is defined by induction on φ as follows:

$$\begin{array}{rcl} [\![\mathsf{a}]\!] & := & \{s \in S \mid \mathsf{a} \in L(s)\} \\ [\![\top]\!] & := & S \\ [\![\bot]\!] & := & \emptyset \\ [\![\varphi \wedge \psi]\!] & := & [\![\varphi]\!] \cap [\![\psi]\!] \\ [\![\varphi \vee \psi]\!] & := & [\![\varphi]\!] \cup [\![\psi]\!] \\ [\![\neg\varphi]\!] & := & S \setminus [\![\varphi]\!] \\ [\![[\alpha]\varphi]\!] & := & \left\{ s \in S \mid \forall s' \in S,\ \text{if } s \xrightarrow{\alpha} s' \text{ then } s' \in [\![\varphi]\!] \right\} \\ [\![\langle\alpha\rangle\varphi]\!] & := & \left\{ s \in S \mid \exists s' \in S,\ s \xrightarrow{\alpha} s' \text{ and } s' \in [\![\varphi]\!] \right\} \end{array}$$

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

Definition 10.3 (Modal Satisfaction)**.** *Consider a Kripke model $M = (S, \mathrm{Act}, \to, \mathrm{AP}, L)$ and an* HML*-formula φ.*

*(1) We say that a state $s \in S$ **satisfies** φ (notation $s \Vdash \varphi$) if $s \in [\![\varphi]\!]$ ([BdRV02, Def. 1.20]).*

*(2) We say that M **satisfies** φ (notation $M \models \varphi$) if $s \in [\![\varphi]\!]$ for all $s \in S$ ([BdRV02, Def. 1.21]).*

*We say that φ is **valid** (notation $\models \varphi$) is $M \models \varphi$ for every Kripke model M (over* Act *and* AP*).*

Remark 10.4. *We shall be mostly concerned with the local satisfaction relation $\Vdash$. The notion of satisfaction in a given Kripke model ($M \models \varphi$) 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 for **transition systems***

$$TS \models^{\imath} \varphi \quad \text{iff} \quad \forall s \in I,\ s \Vdash \varphi$$

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* $s \Vdash \varphi$ *(s* ***forces*** φ*):*

$$\begin{array}{lll}
s \Vdash \mathsf{a} & \textit{iff} & \mathsf{a} \in L(s) \\
s \Vdash \top & & \\
s \not\Vdash \bot & & \\
s \Vdash \varphi \wedge \psi & \textit{iff} & s \Vdash \varphi \textit{ and } s \Vdash \psi \\
s \Vdash \varphi \vee \psi & \textit{iff} & s \Vdash \varphi \textit{ or } s \Vdash \psi \\
s \Vdash \neg\varphi & \textit{iff} & s \not\Vdash \varphi \\
s \Vdash [\alpha]\varphi & \textit{iff} & \textit{for all } s' \in S \textit{ such that } s \xrightarrow{\alpha} s', \textit{ we have } s' \Vdash \varphi \\
s \Vdash \langle\alpha\rangle\varphi & \textit{iff} & \textit{there is some } s' \in S \textit{ such that } s \xrightarrow{\alpha} s' \textit{ and } s' \Vdash \varphi
\end{array}$$

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

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

$$M\left((\mathbf{2}^{\mathrm{AP}})^\omega\right) \quad := \quad \left((\mathbf{2}^{\mathrm{AP}})^\omega, \mathrm{Act}, \to, \mathrm{AP}, L\right)$$

where

$$\begin{array}{lll}
\sigma \xrightarrow{\bullet} \beta & \textit{iff} & \beta = \sigma{\upharpoonright}1 \\
\mathsf{a} \in L(\sigma) & \textit{iff} & \mathsf{a} \in \sigma(0)
\end{array}$$

Then for all HML*-formula* φ *and each* $\sigma \in (\mathbf{2}^{\mathrm{AP}})^\omega$*, we have*

$$\begin{array}{lll}
\sigma \Vdash \langle\bullet\rangle\varphi & \textit{iff} & \sigma{\upharpoonright}1 \Vdash \varphi \\
& \textit{iff} & \sigma \Vdash [\bullet]\varphi
\end{array}$$

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

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

Proof. Exercise! □

10.3 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 Kripke models.

10.3.1 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* φ *and* ψ *are* ***logically equivalent*** *(notation* $\varphi \equiv \psi$*), if* $\models \varphi \leftrightarrow \psi$*.*

Hence $\varphi \equiv \psi$ iff $M \models \varphi \leftrightarrow \psi$ for every Kripke model M. But this is equivalent to $[\![\varphi]\!] = [\![\psi]\!]$ within every Kripke model M.

Lemma 10.9. *We have $\varphi \equiv \psi$ iff for every Kripke model $M = (S, \mathrm{Act}, \rightarrow, \mathrm{AP}, L)$ and all $s \in S$,*

$$s \Vdash \varphi \quad \textit{iff} \quad s \Vdash \psi$$

Proof. Exercise! □

Lemma 10.10. *We have, for $\alpha \in \mathrm{Act}$,*

$$\begin{array}{rcl} \langle\alpha\rangle\varphi & \equiv & \neg[\alpha]\neg\varphi \\ [\alpha]\varphi & \equiv & \neg\langle\alpha\rangle\neg\varphi \end{array}$$

as well as

$$\begin{array}{rclcrcl} \langle\alpha\rangle(\varphi \vee \psi) & \equiv & \langle\alpha\rangle\varphi \vee \langle\alpha\rangle\psi & \qquad & \langle\alpha\rangle\bot & \equiv & \bot \\ [\alpha](\varphi \wedge \psi) & \equiv & [\alpha]\varphi \wedge [\alpha]\psi & \qquad & [\alpha]\top & \equiv & \top \end{array}$$

10.3.2 Logical Equivalence on States and Bisimilarity

In HML, it is pertinent to consider a notion of logical equivalence on **states** of Kripke models.

Definition 10.11. *Consider M_0 and M_1 with $M_i = (S_i, \mathrm{Act}, \rightarrow_i, \mathrm{AP}, L_i)$. 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 φ we have*

$$s_0 \Vdash \varphi \quad \textit{iff} \quad s_1 \Vdash \varphi$$

It is expected that for a modal logic, bisimilarity of states implies logical equivalence.

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

Proof. Exercise! □

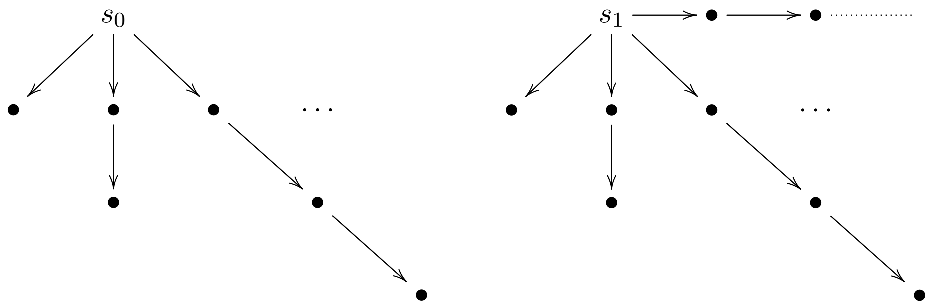
10.4 The Hennessy-Milner Property

We shall look for (partial) converses to Thm. 10.12, *i.e.* for sufficient conditions on a class $\mathfrak{M}$ of Kripke models (over fixed Act and AP) such that given $M_0, M_1 \in \mathfrak{M}$ and $s_0 \in S_0$, $s_1 \in S_1$, we have

$$s_0 \sim s_1 \quad \text{iff} \quad s_0 \equiv s_1$$

This property is called the **Hennessy-Milner property** for $\mathfrak{M}$ (see e.g. [BdRV02, Def. 2.52 p. 92] or [Sti11]). As shown by Ex. 10.13 below, the class $\mathfrak{K}$ of all Kripke models (over fixed Act and AP) does not have the Hennessy-Milner property.

Example 10.13 ([BdRV02, Ex. 2.23 & Fig. 2.5])**.** *Assume* Act $= \mathbf{1}$ *and* AP $= \{\mathtt{a}\}$*. Consider the Kripke models*



(where all states have label $\mathtt{a}$*). Then we have* $s_0 \equiv s_1$ *but* $s_0 \not\sim s_1$*.*

Remark 10.14. *Showing that* $s_0 \equiv s_1$ *in Ex. 10.13 can be done directly (see [BdRV02, Ex. 2.23 & Fig. 2.5]). But it is convenient for such tasks to use appropriate tools (e.g. [BdRV02, Prop. 2.31 & Lem. 2.33]) providing suitable induction principles on formulae (actually quite similar to those for Prop. 7.27, namely variants of the* ***Ehrenfeucht-Faïssé*** *method, see e.g. [PP04, Chap. VIII]).*

Note that the Hennessy-Milner property for a class $\mathfrak{M}$ of Kripke models is equivalent to the following condition:

- Given $M_0, M_1 \in \mathfrak{M}$, 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** Kripke models 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 10.15 (Image Finite T.S.)**.** *We say that* M *is* ***image finite*** *if for every* $s \in S$ *and* $\alpha \in$ Act*, the set*

$$\mathrm{Succ}^{\alpha}(s) \quad := \quad \{s' \in S \mid s \xrightarrow{\alpha} s'\}$$

of α***-successors*** *of* s *is finite.*

Proposition 10.16 (Hennessy-Milner Theorem)**.** *If* M_0 *and* M_1 *(both over* AP *and* Act*) are* ***image finite****, then for all* $(s_0, s_1) \in S_0 \times S_1$ *we have*

$$s_0 \sim s_1 \quad \textit{iff} \quad s_0 \equiv s_1$$

We refer to e.g. [Sti11, Thm. 1.2.4] for a direct proof of Prop. 10.16. In §10.5 we prove Prop. 10.16 using the model-theoretic notion of **modal saturation**. This notion paves the way toward the main construction and result of this §10, namely that for each Kripke model M there is a (modally saturated) Kripke model $\mathfrak{Uf}(M)$ (called the **ultrafilter extension** of M) and a function $\pi : S_M \to S_{\mathfrak{Uf}(M)}$ such that

$$s_0 \equiv s_1 \quad \text{iff} \quad \pi(s_0) \sim \pi(s_1)$$

10.5 Modal Saturation

We follow [BdRV02, §2.5 p. 91].

Definition 10.17. *Let $M = (S, \mathrm{Act}, \to, \mathrm{AP}, L)$.*

*(1) Given a set of states $T \subseteq S$, a set of formulae Φ is **satisfiable** in T if there is a state $s \in T$ such that $s \Vdash \varphi$ for all $\varphi \in \Phi$.*

*(2) Given a set of states $T \subseteq S$, a set of formulae Φ is **finitely satisfiable** in T if every finite subset of Φ is satisfiable in T.*

*(3) M is **modally saturated** if for every state s, every $\alpha \in \mathrm{Act}$, and every set of formulae Φ, if Φ is finitely satisfiable in the set of α-successors of s, then Φ is satisfiable in the set of α-successors of s.*

Proposition 10.18. *If M is image finite, then M is modally saturated.*

Proof. Exercise! □

The following Prop. 10.19 and Cor. 10.20 are gathered in [BdRV02, Prop. 2.54, p. 93].

Proposition 10.19. *If M_0 and M_1 are modally saturated, then $\equiv$ is a bisimulation between M_0 and M_1.*

Proof. Exercise! □

Corollary 10.20. *If M_0 and M_1 are modally saturated, then for every $(s_0, s_1) \in S_0 \times S_1$, we have*

$$s_0 \sim s_1 \quad \textit{iff} \quad s_0 \equiv s_1$$

Proposition 10.16 is a direct consequence of Prop. 10.18 and Cor. 10.20.

10.6 Boolean Algebras with Operators

Similarly as in Def. 8.4 (§8) we write $\mathfrak{L}(\mathsf{HML})$ for the set of HML-formulae (over fixed Act and AP) quotiented by the logical equivalence relation $\equiv$ of Def. 10.8 (§10.2). Then writing φ for $[\varphi]_\equiv \in \mathfrak{L}(\mathsf{HML})$ (as in Notation 8.5), the relation

$$\varphi \leq \psi \quad := \quad (\varphi \to \psi) \equiv \top$$

(see §8) is a partial order on $\mathfrak{L}(\mathsf{HML})$, and moreover $(\mathfrak{L}(\mathsf{HML}), \leq)$ is a Boolean algebra. Similarly as in §8, for a Kripke model $M = (S, \mathrm{Act}, \to, \mathrm{AP}, L)$ the map

$$\begin{array}{rcccc} [\![-]\!] & : & \mathfrak{L}(\mathsf{HML}) & \longrightarrow & \mathcal{P}(S) \\ & & \varphi & \longmapsto & [\![\varphi]\!] \end{array}$$

is a morphism of Boolean algebras.

We shall now see an algebraic approach to HML via the notion of **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.

Definition 10.21. *Given a Kripke frame $K = (S, \mathrm{Act}, \to)$ and $\alpha \in \mathrm{Act}$, define*

$$\begin{array}{rcccl} [\![\langle\alpha\rangle]\!] & : & \mathcal{P}(S) & \longrightarrow & \mathcal{P}(S) \\ & & A & \longmapsto & \{s \in S \mid \exists s' \in \mathrm{Succ}^{\alpha}(s),\ s' \in A\} \\ [\![[\alpha]]\!] & : & \mathcal{P}(S) & \longrightarrow & \mathcal{P}(S) \\ & & A & \longmapsto & \{s \in S \mid \forall s' \in \mathrm{Succ}^{\alpha}(s),\ s' \in A\} \end{array}$$

In the case of a Kripke model M, we of course have

$$\begin{array}{rcl} [\![\langle\alpha\rangle\varphi]\!] & = & [\![\langle\alpha\rangle]\!]([\![\varphi]\!]) \\ [\![[\alpha]\varphi]\!] & = & [\![[\alpha]]\!]([\![\varphi]\!]) \end{array}$$

Moreover:

Lemma 10.22. *Consider a Kripke frame $K = (S, \mathrm{Act}, \to)$ and let $\alpha \in \mathrm{Act}$.*

(1) The function $[\![\langle\alpha\rangle]\!] : \mathcal{P}(S) \to \mathcal{P}(S)$ is a map of join semilattices.

(2) The function $[\![[\alpha]]\!] : \mathcal{P}(S) \to \mathcal{P}(S)$ is a map of meet semilattices.

Proof. Exercise! □

Lemma 10.10 gives a similar situation for $\mathfrak{L}(\mathsf{HML})$.

Lemma 10.23. *Fix some $\alpha \in \mathrm{Act}$.*

(1) The function

$$\begin{array}{rcccl} \langle\alpha\rangle & : & \mathfrak{L}(\mathsf{HML}) & \longrightarrow & \mathfrak{L}(\mathsf{HML}) \\ & & \varphi & \longmapsto & \langle\alpha\rangle\varphi \end{array}$$

is a map of join semilattices.

(2) The function

$$\begin{array}{rcccl} [\alpha] & : & \mathfrak{L}(\mathsf{HML}) & \longrightarrow & \mathfrak{L}(\mathsf{HML}) \\ & & \varphi & \longmapsto & [\alpha]\varphi \end{array}$$

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 $\mathfrak{L}(\mathsf{HML})$) are interdefinable. Let us elaborate a bit on this.

Definition 10.24. *Given Boolean algebras B, B' and a function $f : B \to B'$, the **dual** of f is the function*

$$\begin{array}{rcccl} f^{\partial} & : & B & \longrightarrow & B' \\ & & b & \longmapsto & \neg' f(\neg b) \end{array}$$

Lemma 10.25. *Consider a Kripke frame $K = (S, \mathrm{Act}, \to)$ and let $\alpha \in \mathrm{Act}$. Then*

$$\begin{array}{rcl} [\![[\alpha]]\!] & = & [\![\langle\alpha\rangle]\!]^{\partial} \\ [\![\langle\alpha\rangle]\!] & = & [\![[\alpha]]\!]^{\partial} \end{array}$$

PROOF. Exercise! □

Lemma 10.26. *Given $\alpha \in \mathrm{Act}$, in $(\mathfrak{L}(\mathsf{HML}), \leq)$ we have*

$$\begin{array}{rcl} [\alpha] & = & \langle\alpha\rangle^{\partial} \\ \langle\alpha\rangle & = & [\alpha]^{\partial} \end{array}$$

PROOF. Exercise! □

Lemma 10.27. *Let B, B' be Boolean algebras, and consider a function $f : B \to B'$.*

(1) We have $f^{\partial\partial} = f$.

(2) If f is a map of join (resp. meet) semilattices, then f^{∂} is a map of meet (resp. join) semilattices.

(3) If f is a map of lattices, then $f^{\partial} = f$.

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. 10.27. 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 10.28 (Boolean Algebra with Operators)**.** *A **Boolean algebra with operators** (BAO) B^+ of type Act is a Boolean algebra B equipped with a family $(f_\alpha)_{\alpha \in \mathrm{Act}}$ of join semilattice morphisms $f_\alpha : B \to B$.*

Example 10.29. $\mathfrak{L}(\mathsf{HML})^+ := (\mathfrak{L}(\mathsf{HML}), (\langle\alpha\rangle)_{\alpha \in \mathrm{Act}})$ *is a BAO of type Act.*

Example 10.30. *Given a Kripke frame $K = (S, \mathrm{Act}, \to)$, $K^+ := (\mathcal{P}(S), ([\![\langle\alpha\rangle]\!])_{\alpha \in \mathrm{Act}})$ is a BAO of type 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 10.31 (Ultrafilter Frames)**.** *Given a BAO $B^+ = (B, (f_\alpha)_{\alpha \in \mathrm{Act}})$, the **ultrafilter frame** $\mathfrak{Uf}(B)$ is defined as*

$$\mathfrak{Uf}(B^+) \quad := \quad (\mathbf{Sp}(B), \mathrm{Act}, \to)$$

where:

- *$\mathbf{Sp}(B)$ is the set of ultrafilters (or equivalently prime filters) over B (see §**??**),*
- *given $\mathcal{F}, \mathcal{H} \in \mathbf{Sp}(B)$ and $\alpha \in \mathrm{Act}$, we have*

$$\mathcal{F} \xrightarrow{\alpha} \mathcal{H} \quad \text{iff} \quad \forall b \in B,\ b \in \mathcal{H} \implies f_\alpha(b) \in \mathcal{F}$$

Lemma 10.32. *Consider a BAO $B^+ = (B, (f_\alpha)_{\alpha \in \mathrm{Act}})$. In the ultrafilter frame $\mathfrak{Uf}(B^+)$, given $\alpha \in \mathrm{Act}$ and $\mathcal{F}, \mathcal{H} \in \mathbf{Sp}(B)$ we have*

$$\mathcal{F} \xrightarrow{\alpha} \mathcal{H} \quad \textit{iff} \quad \forall b \in B,\ f^{\partial}_{\alpha}(b) \in \mathcal{F} \implies b \in \mathcal{H}$$

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 §10.7 how this construction, applied to the BAO $(\mathcal{P}(S), ([\![\langle\alpha\rangle]\!])_{\alpha \in \mathrm{Act}})$ of a Kripke model $M = (S, \mathrm{Act}, \to, \mathrm{AP}, L)$, induces a Kripke model with the Hennessy-Milner property.

10.7 Ultrafilter Extensions of Kripke Models

The ultrafilter frame construction of Def. 10.31 turns a BAO into a frame. If one starts from the BAO K^+ induced by the frame structure K of a Kripke model M, we can extend $\mathfrak{Uf}(K^+)$ to a Kripke model $\mathfrak{Uf}(M)$, the **ultrafilter extension** of M, which is modally saturated (and in particular satisfies the Hennessy-Milner property). We essentially follow [BdRV02, §2.5].

We take the material of §**??** for granted. We begin by specializing it to ultrafilters over powerset algebras.

Definition 10.33. *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 $\mathfrak{Uf}(X)$ for the set of ultrafilters on X.*

Hence $\mathfrak{Uf}(X) = \mathbf{Sp}(\mathcal{P}(X), \subseteq)$.

Lemma 10.34. *Let X be a set. If $G \subseteq \mathcal{P}(X)$ has the finite intersection property, then*

$$F \quad := \quad \bigcap\{E \mid E \textit{ is a proper filter} \supseteq G\}$$

is a proper filter.

Note that if there is some $G \subseteq \mathcal{P}(X)$ with the finite intersection property, we necessarily have X non empty, since otherwise the intersection of the empty family, which is the top element of $(\mathcal{P}(X), \subseteq)$ (*i.e.* X), would be empty.

Proof. Exercise! □

Example 10.35.

*(1) For each $x \in X$, the **principal ultrafilter** on x is the ultrafilter*

$$\pi(x) \quad := \quad \{A \in \mathcal{P}(X) \mid x \in A\}$$

(2) If X is a finite set, then the ultrafilters on X are exactly the principal filters on X. In particular, $\mathfrak{Uf}(X)$ is in bijection with X.

PROOF. Exercise! □

(3) It follows from the Ultrafilter Lemma **??** *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 $\mathcal{F}$ containing all $A \subseteq X$ such that $X \setminus A$ is finite.*

We shall now use the **ultrafilter extension** of a Kripke model M in order to produce modally saturated models. In the following, we assume that the labelings $L : S \to \mathcal{P}(\mathrm{AP})$ are described by their transpose $V : \mathrm{AP} \to \mathcal{P}(S)$ (where $s \in V(\mathsf{a})$ iff $\mathsf{a} \in L(s)$).

Definition 10.36 (Ultrafilter Extension of a Kripke Model)**.** *Consider a Kripke model $M = (S, \mathrm{Act}, \to, \mathrm{AP}, L)$. The* ***ultrafilter extension of*** *M is the Kripke model $\mathfrak{Uf}(M)$ over* AP *and* Act *with*

- *as state set the set $\mathfrak{Uf}(S)$ of ultrafilters on S,*
- *as transition relation, $\mathcal{F} \xrightarrow{\alpha} \mathcal{H}$ iff $[\![\langle\alpha\rangle]\!](A) \in \mathcal{F}$ whenever $A \in \mathcal{H}$,*
- *as state labelling, the map taking $\mathsf{a} \in \mathrm{AP}$ to the set of ultrafilters $\mathcal{F}$ such that $V(\mathsf{a}) \in \mathcal{F}$,*

In the case of as t.s. $TS = (S, \mathrm{Act}, \to, I, \mathrm{AP}, L)$, $\mathfrak{Uf}(TS)$ has underlying Kripke model $\mathfrak{Uf}(S, \mathrm{Act}, \to, \mathrm{AP}, L)$ and initial states $\{\pi(s) \mid s \in I\}$.

Hence the Kripke frame part of $\mathfrak{Uf}(M)$ is the ultrafilter frame $\mathfrak{Uf}(S, \mathrm{Act}, \to)$ in the sense of Def. 10.31. In particular, Lem. 10.32 specializes to the following.

Lemma 10.37. *Consider a Kripke model $M = (S, \mathrm{Act}, \to, \mathrm{AP}, L)$. Then, in $\mathfrak{Uf}(M)$ we have*

$$\mathcal{F} \xrightarrow{\alpha} \mathcal{H} \quad \textit{iff} \quad \forall A \in \mathcal{P}(S),\ [\![[\alpha]]\!](A) \in \mathcal{F} \implies A \in \mathcal{H}$$

PROOF. Exercise! □

Example 10.38. *Consider a Kripke model $M = (S, \mathrm{Act}, \to, \mathrm{AP}, L)$ with* ***finite*** *set of states S. It follows from Ex. 10.35.(2) that $\mathfrak{Uf}(M)$ has a finite set of states $\mathfrak{Uf}(S) \simeq S$ (via π). Moreover:*

- *Given $s \in S$ and $\mathsf{a} \in \mathrm{AP}$, we have $\mathsf{a} \in L(s)$ in M if and only if $\mathsf{a} \in L(\pi(s))$ in $\mathfrak{Uf}(M)$.*

  PROOF. Exercise! □

- *Given $s, s' \in S$ and $\alpha \in \mathrm{Act}$, we have $s \xrightarrow{\alpha} s'$ in M if and only if $\pi(s) \xrightarrow{\alpha} \pi(s')$ in $\mathfrak{Uf}(M)$.*

Proof. Exercise! □

Notation 10.39. *In the following, given a transition system M and its ultrafilter extension $\mathfrak{Uf}(M)$, with $[\![-]\!]$ we always refer to the semantics of* HML *in M rather than in $\mathfrak{Uf}(M)$.*

Recall the map ext of Def. **??** (§**??**). In the case of a Boolean algebra of the form $(\mathcal{P}(X), \subseteq)$ for some set X, we have

$$\begin{array}{rcrcl} \mathsf{ext} & : & \mathcal{P}(X) & \longrightarrow & \mathcal{P}(\mathfrak{Uf}(X)) \\ & & A & \longmapsto & \{\mathcal{F} \in \mathfrak{Uf}(X) \mid A \in \mathcal{F}\} \end{array}$$

In particular, given a Kripke model M with state set S, $\mathsf{ext}([\![\varphi]\!]) \in \mathcal{P}(\mathfrak{Uf}(S))$ for each HML-formula φ.

Proposition 10.40. *Let $M = (S, \mathrm{Act}, \to, \mathrm{AP}, L)$. Then, for all $\mathcal{F} \in \mathfrak{Uf}(S)$ and all* HML*-formula φ, we have*

$$\mathcal{F} \Vdash \varphi \quad \Longleftrightarrow \quad \mathcal{F} \in \mathsf{ext}([\![\varphi]\!])$$

Proof. Exercise! □

Corollary 10.41. *Let $M = (S, \mathrm{Act}, \to, \mathrm{AP}, L)$. Then, for every* HML*-formula φ we have*

$$\begin{array}{rcl} (\forall s \in S)\big(s \Vdash \varphi & \Longleftrightarrow & \pi(s) \Vdash \varphi\big) \\ M \models \varphi & \Longleftrightarrow & \mathfrak{Uf}(M) \models \varphi \end{array}$$

Proof. Exercise! □

Remark 10.42. *Since the initial states of $\mathfrak{Uf}(TS)$ are exactly the $\pi(s)$ for s initial in TS, Cor. 10.41 extends to the notion $\models^{\imath}$ of Rem. 10.4 as*

$$TS \models^{\imath} \varphi \quad \Longleftrightarrow \quad \mathfrak{Uf}(TS) \models^{\imath} \varphi$$

Proposition 10.43. *Let $M = (S, \mathrm{Act}, \to, \mathrm{AP}, L)$. Then $\mathfrak{Uf}(M)$ is modally saturated.*

Proof. Exercise! □

Corollary 10.44. *Given Kripke models M_0 and M_1, both over* AP *and* Act*, for all $(s_0, s_1) \in S_0 \times S_1$ we have*

$$s_0 \equiv s_1 \quad \Longleftrightarrow \quad \pi(s_0) \sim \pi(s_1)$$

References

[AS85] B. Alpern and F. B. Schneider. Defining liveness. *Information Processing Letters*, 21(4):181–185, 1985. 9

[Awo10] S. Awodey. *Category Theory*. Oxford University Press, Inc., USA, 2nd edition, 2010. 35, 36

[BBJ07] G. S. Boolos, J. P. Burgess, and R. C. Jeffrey. *Computability and Logic*. Cambridge University Press, fifth edition, 2007. 17

[BdRV02] P. Blackburn, M. de Rijke, and Y. Venema. *Modal Logic*. Cambridge Tracts in Theoretical Computer Science. Cambridge University Press, 2002. 41, 43, 55, 57, 58, 59, 60, 61, 62, 64, 65

[BK08] C. Baier and J.-P. Katoen. *Principles of Model Checking*. MIT Press, 2008. 4, 5, 6, 7, 8, 9, 10, 11, 19, 20, 23, 27, 32, 33, 41, 43, 49, 50, 51, 52, 55, 56, 57

[Bou07] N. Bourbaki. *Topologie générale: Chapitres 1 à 4*. Springer Berlin Heidelberg, 2007. Reprint of the original 1971 edition. 22

[BW18] J. C. Bradfield and I. Walukiewicz. The mu-calculus and Model Checking. In E. M. Clarke, T. A. Henzinger, H. Veith, and R. Bloem, editors, *Handbook of Model Checking*, pages 871–919. Springer, 2018. 48

[DP02] B.A. Davey and H.A. Priestley. *Introduction to Lattices and Order*. CUP, 2nd edition, 2002. 27, 28, 30, 31, 34, 35, 36, 41, 43, 48

[GTW02] E. Grädel, W. Thomas, and T. Wilke, editors. *Automata, Logics, and Infinite Games: A Guide to Current Research*, volume 2500 of *LNCS*. Springer, 2002. 17, 48

[Joh82] P.T. Johnstone. *Stone Spaces*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1982. 29, 54

[Kec95] A. S. Kechris. *Classical Descriptive Set Theory*, volume 156 of *Graduate Texts in Mathematics*. Springer, 1995. 16, 25

[Koz83] D. Kozen. Results on the propositional μ-calculus. *Theoretical Computer Science*, 27(3):333 – 354, 1983. Special Issue Ninth International Colloquium on Automata, Languages and Programming (ICALP) Aarhus, Summer 1982. 48

[ML98] S. Mac Lane. *Categories for the Working Mathematician*. Springer, 2nd edition, 1998. 34, 35, 36

[Mos09] Y. N. Moschovakis. *Descriptive Set Theory*, volume 155 of *Mathematical Surveys and Monographs*. American Mathematical Soc., second edition, 2009. 26

[Pnu77] A. Pnueli. The temporal logic of programms. In *Proceedings of the 18th Annual Symposium on Foundations of Computer Science*, SFCS '77, pages 46–57. IEEE Computer Society, 1977. 41

[PP04] D. Perrin and J.-É. Pin. *Infinite Words: Automata, Semigroups, Logic and Games*. Pure and Applied Mathematics. Elsevier, 2004. 17, 25, 40, 51, 61

[Run05] V. Runde. *A Taste of Topology*. Universitext. Springer New York, 2005. 20, 21, 30, 39, 40, 41

[Sim10] S.G. Simpson. *Subsystems of Second Order Arithmetic*. Perspectives in Logic. Cambridge University Press, 2nd edition, 2010. 17, 40

[Sti11] C. Stirling. Bisimulation and logic. In D. Sangiorgi and J. Rutten, editors, *Advanced Topics in Bisimulation and Coinduction*, Cambridge Tracts in Theoretical Computer Science, pages 173–196. Cambridge University Press, 2011. 57, 60, 61

[SU06] M. H. Sørensen and P. Urzyczyn. *Lectures on the Curry-Howard Isomorphism*, volume 149 of *Studies in Logic and the Foundations of Mathematics*. Elsevier Science Inc., 2006. 36

[TvD88] A. S. Troelstra and D. van Dalen. *Constructivism in Mathematics, Volume 1*, volume 121 of *Studies in Logic and the Foundations of Mathematics*. Elsevier, 1988. 17

[VVK05] H. Völzer, D. Varacca, and E. Kindler. Defining Fairness. In Martín Abadi and Luca de Alfaro, editors, *CONCUR 2005 - Concurrency Theory, 16th International Conference, CONCUR 2005, San Francisco, CA, USA, August 23-26, 2005, Proceedings*, volume 3653 of *Lecture Notes in Computer Science*, pages 458–472. Springer, 2005. 25

[VW08] M. Y. Vardi and T. Wilke. Automata: from logics to algorithms. In *Logic and Automata*, volume 2 of *Texts in Logic and Games*, pages 629–736. Amsterdam University Press, 2008. 17, 48

[Wal16] I. Walukiewicz. Automata theory and higher-order model-checking. *ACM SIGLOG News*, 3(4):13–31, October 2016. 12

[Wil70] S. Willard. *General Topology*. Addison-Wesley, 1970. 20, 21, 30, 40, 41