Semantics and Verifications

Based on the lectures of Colin Riba
Notes written by Hugo Salou

October 22, 2025

Contents

1 Introduction.

Let us give precisions on the terms in the name of the course, and in the broader space of semantics and verifications.

Verification. Formal techniques to ensure the correctness software or hardware of systems.

Model Checking. "Automatic" checking of the correctness by means of exhaustive exploration.

Exemple 1.1. Consider a program that is 10 lines long, contains 3 booleans variables and 5 integers variables in the range $\{0, \dots, 9\}$. The number of states for this program is:

$$10 \times 2^3 \times 10^5 = 8\,000\,000.$$

The real issue with the state exploration problem is the factor 10^5, coming from the use of 5 integers.

Exemple 1.2. Consider a server and n clients. Clients can make requests to the server and the server can answer a client. The specification of this server should include the following:

- ▷ Each client which makes a request is eventually answered.
- ▷ We *abstract* away from precise quantitative constraints.

We will sometimes reason about an infinite amount of executions. For example, if some client makes infinitely-many requests (then it'll have infinitely-many answers). Infinite sequences are represented by ω-*words*, *i.e.* infinite words indexed by $\mathbb{N}$. Thus, ω-words on some

alphabet Σ are functions $\mathbb{N} \to \Sigma$. We will denote Σ^ω the set of those infinite words on the alphabet Σ.

If $|\Sigma| \geq 2$, then the set Σ^ω is uncountable.

This course will cover the following:

- Transition systems;
- Linear-time properties;
- Topology;
- Orders and Lattices;
- Linear Temporal Logic (LTL);
- Büchi automata;
- **Stone duality** (mostly in homework);
- Bisimilarity/bisimulation;
- Modal Logic.

Ressources from this course include:

- the course notes (available online, non-exhaustive);
- Baier, C. and Katoen, J.-P., Principles of Model Checking, MIT Press, 2008.

Prerequisites for this course include:

- First-order logic (*see* my course notes for the "Logique" L3 course, in french);
- Finite automata ("FDI" L3 course).

Evaluation for this course will be in two parts: the final exam (50 %) and the homework, in two parts (25 % each).

The tutorials will be done by Lison Blondeau-Patissier.

2 Transition systems.

2.1 Transition systems.

Définition 2.1. A transition system is a tuple

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

where

- S is the set of *states*;
- Act is the set of *actions*;
- $\to \subseteq S \times \mathrm{Act} \times S$ the *transition relation*;
- $I \subseteq S$ the set of *initial states*;
- AP is the set of *atomic propositions*;
- $L : S \to \wp(\mathrm{AP}) \cong \mathbf{2}^{\mathrm{AP}}$ is the *state labelling function*.

We will write $s \xrightarrow{\alpha} s'$ when $(s, \alpha, s') \in \to$.

Exemple 2.1 (Beverage Vending Machine, BVM)**.** We can model a beverage vending machine using a diagram like in figure 2.1. Here we have that:

- $S = \{\mathsf{pay}, \mathsf{select}, \mathsf{soda}, \mathsf{beer}\}$,
- $I = \{\mathsf{pay}\}$,
- $\mathrm{Act} = \{\mathtt{ic}, \tau, \mathtt{gb}, \mathtt{gs}\}$.[1]

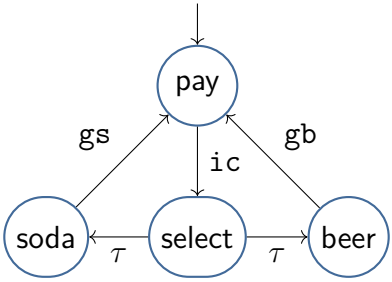

Figure 2.1 | *Transition system for the BVM*

We can define the labels:

$L(\mathsf{pay}) = \emptyset \quad L(\mathsf{soda}) = L(\mathsf{beer}) = \{\mathsf{paid}, \mathsf{drink}\} \quad L(\mathsf{select}) = \{\mathsf{paid}\},$

with $\mathrm{AP} = \{\mathsf{paid}, \mathsf{drink}\}$.

2.2 Program graphs.

The goal is to represent the evaluation of a program.

Définition 2.2 (Typed variables). ▷ A set Var of *variables*.

- ▷ For each variable $x \in \mathrm{Var}$, consider a set $\mathrm{Dom}(x)$.
- ▷ Given $TV = (\mathrm{Var}, (\mathrm{Dom}(x))_{x \in \mathrm{Var}})$, we define

$$\mathrm{Eval}(TV) = \prod_{x \in \mathrm{Var}} \mathrm{Dom}(x),$$

the set of valuations of the form $\eta : x \in \mathrm{Var} \mapsto \eta(x) \in \mathrm{Dom}(x)$ (in the sense of a dependent function type).

[1] The meaning of the actions are the following: `ic` means *insert coin*, `gb` means *get beer* and `gs` for *get soda*.

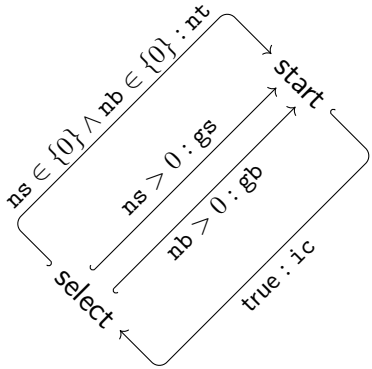

Figure 2.2 | *BVM as a program graph*

Définition 2.3 (Program graph). A *program graph* is a tuple

$$PG = (\text{Loc}, \text{Act}, \text{Effect}, \hookrightarrow, \text{Loc}_0, g_0),$$

where

- ▷ Loc is the set of *locations* (lines of codes);
- ▷ Act is the set of *actions*;
- ▷ $\text{Effect} : \text{Act} \times \text{Eval}(TV) \to \text{Eval}(TV)$;
- ▷ $\hookrightarrow \subseteq \text{Loc} \times \text{Conditions} \times \text{Act} \times \text{Loc}$ where conditions are propositional formula built from atoms of the forms "$x \in D$" for some variable x and some set $D \subseteq \text{Dom}(x)$;
- ▷ $\text{Loc}_0 \subseteq \text{Loc}$ the set of *initial locations*;
- ▷ g_0 is the *initial condition*.

We will write $\ell \xhookrightarrow{g:\alpha} \ell'$ for $(\ell, g, \alpha, \ell') \in \hookrightarrow$.

Exemple 2.2 (BVM as a program graph). In figure 2.2, we use

- ▷ $\text{Loc} = \{\mathsf{start}, \mathsf{select}\}$;

- ▷ $\text{Var} = \{\texttt{ns}, \texttt{nb}\}$;
- ▷ $\text{Act} = \{\texttt{ic}, \texttt{nt}, \texttt{gs}, \texttt{gb}, \texttt{refill}\}$;
- ▷ $\text{Loc}_0 = \{\mathsf{start}\}$;
- ▷ $g_0 = \texttt{ns} \in \{\max\} \wedge \texttt{nb} \in \{\max\}$
- ▷

$$\begin{aligned} \text{Effect} : \text{Act} \times \text{Eval}(TV) &\longrightarrow \text{Eval}(TV) \\ (\texttt{refill}, \eta) &\longmapsto [\texttt{ns} \mapsto \max, \texttt{nb} \mapsto \max] \\ (\texttt{gs}, \eta) &\longmapsto \eta[\texttt{ns} \mapsto \eta(\texttt{ns}) - 1] \\ (\texttt{gb}, \eta) &\longmapsto \eta[\texttt{nb} \mapsto \eta(\texttt{nb}) - 1] \end{aligned}$$

2.3 Transition system of a program graph.

Définition 2.4. Given TV and PG a program graph, we define

$$TS(PG) := (S, \text{Act}, \to, I, \text{AP}, L)$$

where

- ▷ $S = \text{Loc} \times \text{Eval}(TV)$;
- ▷ $\text{AP} = \text{Loc} \cup \text{Conditions}$;
- ▷ $I = \{(\ell_0, \eta) \mid \ell_0 \in \text{Loc}_0, \eta \models g_0\}$;
- ▷ $\to$ is defined by:

$$\frac{\ell \overset{g:\alpha}{\hookrightarrow} \ell' \qquad \eta \models g}{(\ell, \eta) \overset{\alpha}{\to} (\ell', \text{Effect}(\alpha, \eta))},$$

- ▷ and $L(\ell, \eta) = \{\ell\} \cup \{g \mid \eta \models g\}$.

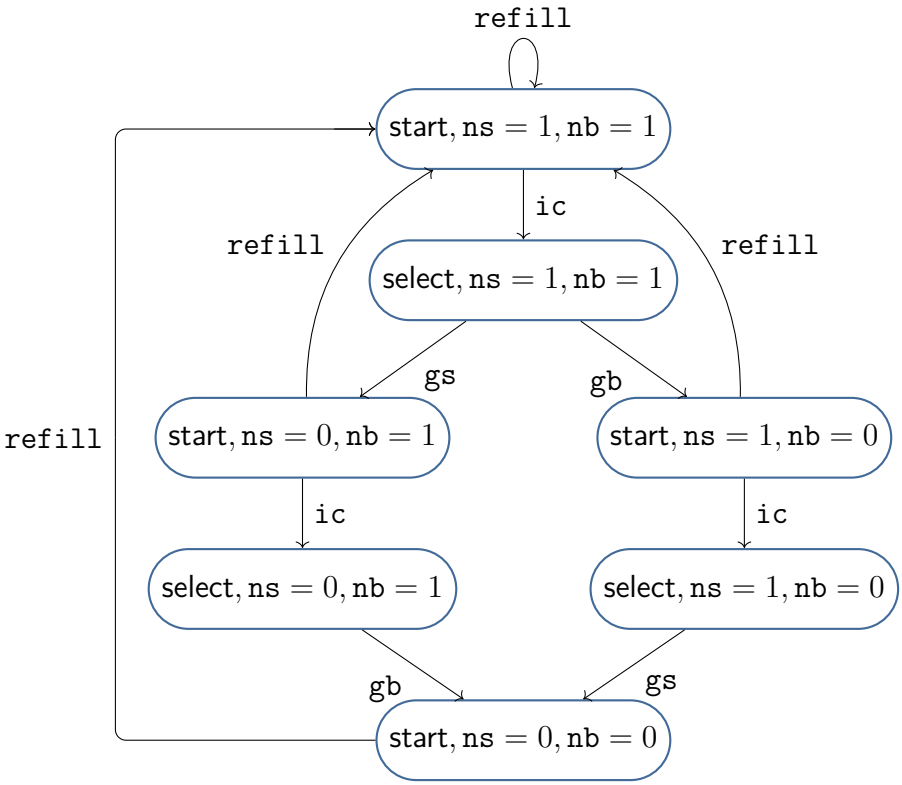

Figure 2.3 | *Transition system of the BVM program graph*

Exemple 2.3. The BVM program graph example seen in the previous example can be transformed as a transition system thanks to the previous definition; it is shown in figure 2.3. To simplify, we assume max = 1.

3 Linear Time Properties.

Definition 3.1. Let Σ be an alphabet (*i.e.* a set).

1. A *ω-word* on Σ is a function $\sigma : \mathbb{N} \to \Sigma$. We denote Σ^ω for the set of ω-words on Σ.
2. We define $\Sigma^\infty := \Sigma^\omega \cup \Sigma^\star$ the set of finite or infinite words.
3. Given $\hat{\sigma} \in \Sigma^\star$ and $\sigma \in \Sigma^\infty$, we say that $\hat{\sigma}$ is a prefix of σ, written $\hat{\sigma} \subseteq \sigma$, whenever
$$\forall i < \mathsf{length}(\hat{\sigma}), \quad \hat{\sigma}(i) = \sigma(i).$$
4. Given $\sigma \in \Sigma^\infty$, we define
$$\mathrm{Pref}(\sigma) := \{\, \hat{\sigma} \in \Sigma^\star \mid \hat{\sigma} \subseteq \sigma \,\},$$
which we extend to sets of words: for $E \subseteq \Sigma^\infty$,
$$\mathrm{Pref}(E) := \bigcup_{\sigma \in E} \mathrm{Pref}(\sigma).$$

Remark 3.1.
- ▷ The prefix order $\subseteq$ on $\Sigma^\star$ is generally[1] a partial order: there are $u, v \in \Sigma^\star$ such that $u \not\subseteq v$ and $v \not\subseteq u$.
- ▷ Given $\sigma \in \Sigma^\infty$, the prefix order $\subseteq$ on $\mathrm{Prefix}(\sigma)$ is a linear (or total order).

[1] As long as the alphabet has at least two letters.

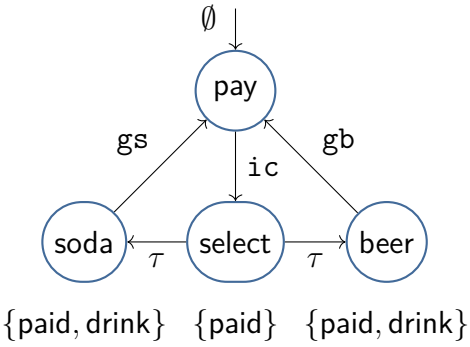

Figure 3.1 | *Transition system for the BVM with labels*

3.1 Linear-time properties.

Let AP be a set of *atomic propositions*.

Definition 3.2. A *linear-time property* (sometimes written LT property) on AP is a set $P \subseteq (\mathbf{2}^{\mathrm{AP}})^{\omega}$.

The idea is that a linear-time property $A : \mathbb{N} \to \mathbf{2}^{\mathrm{AP}}$ specifies, for each $i \in \mathbb{N}$, a set $\sigma(i) \subseteq \mathrm{AP}$ of all atomic propositions are assumed at time i.

Example 3.1. For the Beverage vending machine (shown in figure 3.1), we can have the following linear-time properties:

- $\{\sigma \in (\mathbf{2}^{\mathrm{AP}})^{\omega} \mid \forall n \in \mathbb{N}, \mathsf{drink} \in \sigma(n) \implies \exists k < n, \mathsf{paid} \in \sigma(k)\}$,
- $\{\sigma \in (\mathbf{2}^{\mathrm{AP}})^{\omega} \mid \forall n \in \mathbb{N}, \#\{k \leq n \mid \mathsf{drink} \in \sigma(k)\} \leq \#\{k \leq n \mid \mathsf{paid} \in \sigma(k)\}\}$,
- $\{\sigma \in (\mathbf{2}^{\mathrm{AP}})^{\omega} \mid (\exists^{\infty} t, \mathsf{paid} \in \sigma(i)) \implies (\exists^{\infty} t, \mathsf{drink} \in \sigma(t))\}$,
- $\{\sigma \in (\mathbf{2}^{\mathrm{AP}})^{\omega} \mid (\forall^{\infty} t, \mathsf{paid} \notin \sigma(t)) \implies (\forall^{\infty} t, \mathsf{drink} \notin \sigma(t))\}$.

Remark 3.2. The notations $\exists^{\infty}$ and $\forall^{\infty}$ are "infinitely many" and "ultimately all" quantifiers:

- $\exists^{\infty} t, P(t)$ is, by definition, $\forall N \in \mathbb{N}, \exists t \geq N, P(t)$;

▷ $\forall^\infty t, P(t)$ is, by definition, $\exists N \in \mathbb{N}, \forall t \geq N, P(t)$.

Definition 3.3. A (finite or infinite) *path* in TS is a finite or infinite sequence $\pi = (s_i)_i \in S^\infty$ which respects transitions: for all i, we have $s_i \xrightarrow{\mathtt{a}} s_{i+1}$ for some $\mathtt{a} \in \mathrm{Act}$.

A path $\pi = (s_i)_i$ is *initial* if $s_0 \in I$.

Definition 3.4 (Trace).

1. The *trace* of a path $\pi = (s_i)_i$ is the (finite or infinite) word
$$L(\pi) := \big(L(s_i)\big)_i \in L^\infty.$$
2. We define
   - ▷ $\mathrm{Tr}(TS) := \{L(\pi) \mid \pi \text{ is a finite or infinite path in } TS\}$;
   - ▷ $\mathrm{Tr}^\omega(TS) := \{L(\pi) \mid \pi \text{ is a infinite path in } TS\}$;
   - ▷ $\mathrm{Tr}_{\mathrm{fin}}(TS) := \{L(\pi) \mid \pi \text{ is a finite path in } TS\}$.

Definition 3.5 (Satisfaction of a LT property). We say that a transition system TS over AP *satisfies* a LT property P on AP, written $TS \models P$, when $\mathrm{Tr}^\omega(TS) \subseteq P$.

Example 3.2. The BVM satisfies all the properties from example 3.1.

Example 3.3. We use a different transition system BVM′ to model the beverage vending machine, as seen in figure 3.2. The two transition systems are equivalent in the sense that:
$$\mathrm{Tr}^\omega(\mathrm{BVM}') = \mathrm{Tr}^\omega(\mathrm{BVM}),$$

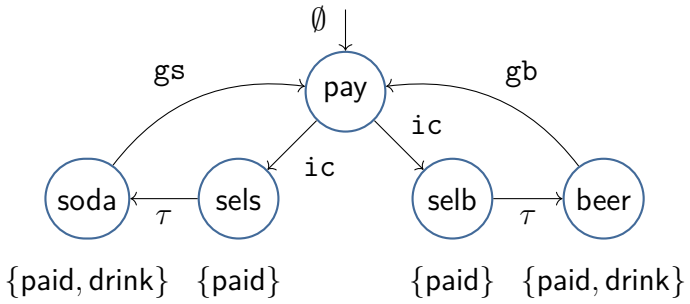

Figure 3.2 | *Transition system for the alternative BVM*

so, for any LT Property $P \subseteq (\mathbf{2}^{\mathrm{AP}})^{\omega}$,

$$\mathrm{BVM}' \not\approx P \qquad \text{iff} \qquad \mathrm{BVM} \not\approx P.$$

We have a very simple result, which we will (probably) prove in the tutorials.

Proposition 3.1. Given two transition systems TS_1 and TS_2 over AP, then the following are equivalent:

- $\mathrm{Tr}^{\omega}(TS_1) \subseteq \mathrm{Tr}^{\omega}(TS_2)$,
- $\forall P \subseteq (\mathbf{2}^{\mathrm{AP}})^{\omega}$, $TS_2 \not\approx P \implies TS_1 \not\approx P$.

3.2 Decomposition of a linear-time property.

In this section, we introduce the notions of a "safety property" and a "liveness property" such that, for any LT property P,

1. there exists a safety property P_{safe} and a liveness property P_{liveness} such that
$$P = P_{\mathrm{safe}} \cap P_{\mathrm{liveness}};$$
2. P is a liveness and a safety property if and only if $P = (\mathbf{2}^{\mathrm{AP}})^{\omega}$.

3.2.1 Safety properties.

The idea of a safety property is to ensure that "nothing bad is going to happen."

Definition 3.6. We say that $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ is a *safety property* if there exists a set $P_{\mathrm{bad}} \subseteq (\mathbf{2}^{\mathrm{AP}})^\star$ such that

$$\sigma \in P \iff \mathrm{Pref}(\sigma) \cap P_{\mathrm{bad}} = \emptyset.$$

Example 3.4. Considering the examples of LT-properties from example 3.1,

- ▷ Property (1) is a safety property: we can consider

$$P_{\mathrm{bad}}^{(1)} = \{\hat{\sigma} \in \Sigma^\star \mid \mathsf{drink} \in \hat{\sigma}(n) \wedge \forall i < n, \mathsf{paid} \notin \hat{\sigma}(i)\},$$

  where n is the length of $\hat{\sigma}$.

- ▷ Property (2) is a safety property: we can consider

$$P_{\mathrm{bad}}^{(2)} = \{\hat{\sigma} \in \Sigma^\star \mid \#\{t \mid \mathsf{paid} \in \hat{\sigma}(t)\} < \#\{t \mid \mathsf{drink} \in \hat{\sigma}(t)\}\}.$$

- ▷ Properties (3) and (4) are not safety properties: for any finite word $\hat{\sigma} \in (\mathbf{2}^{\mathrm{AP}})^\omega$, there exists $\sigma \in (\mathbf{2}^{\mathrm{AP}})^\omega$ such that $\hat{\sigma} \subseteq \sigma$ and $\sigma \in P$.

Example 3.5 (Traffic Light)**.** We consider a traffic light as a transition system over $\mathrm{AP} = \{\mathsf{G}, \mathsf{Y}, \mathsf{R}\}$, as shown in figure 3.3. An example of a safety property is

$$\forall n, \mathsf{R} \in \sigma(n) \implies n > 0 \text{ and } \mathsf{Y} \in \sigma(n-1).$$

3.2.2 Safety properties and trace equivalences.

Example 3.6. Consider the transition system shown in figure 3.4, a safety property P with $P_{\text{bad}} = \{\mathsf{a}\}^\star\{\mathsf{b}\}$ is satisfied: $TS \not\approx P$. This is true since $\text{Tr}^\omega(TS) = \{\mathsf{a}\}^\omega$. However, when we consider *finite* (instead of infinites) traces, we have that $\text{Tr}_{\text{fin}}(TS) \cap P_{\text{bad}} \neq \emptyset$.

Definition 3.7 (Terminal state)**.** A state $s \in S$ of a transition system TS is *terminal* if

$$\forall s' \in S, \quad \forall \alpha \in \text{Act}, \quad s \overset{\alpha}{\not\to} s'.$$

Proposition 3.2. Let TS be a transition system without terminal states, and a safety property P with P_{bad} the set of "bad behaviours". Then,

$$TS \not\approx P \qquad \text{if and only if} \qquad \text{Tr}_{\text{fin}}(TS) \cap P_{\text{bad}} = \emptyset.$$

Proof. See the course notes in § 3.2.3. □

Lemma 3.1. Let TS and TS' be two transition systems over AP without terminal states. Then, the following are equivalent:

- $\text{Tr}_{\text{fin}}(TS) \subseteq \text{Tr}_{\text{fin}}(TS')$;
- for any safety property P, $TS' \not\approx P$ implies $TS \not\approx P$.

Proof. ▷ " $\Longrightarrow$ ". This is true by the last proposition.

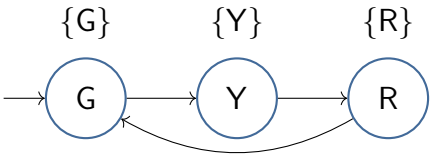

Figure 3.3 | *Transition system for the traffic light*

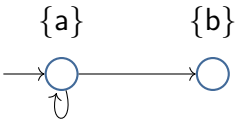

Figure 3.4 | *Another transition system*

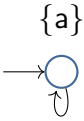

Figure 3.5 | *One-state transition system*

▷ " $\Longleftarrow$ ". Let P be a safety property with

$$P_{\text{bad}} = (\mathbf{2}^{\text{AP}})^\star \setminus \text{Tr}_{\text{fin}}(TS').$$

So, $TS' \not\models P$ hence $TS \not\models P$ by assumption. Therefore, $\text{Tr}_{\text{fin}}(TS) \subseteq \text{Tr}_{\text{fin}}(TS')$ by the last proposition.

□

Example 3.7. Consider the transition system TS from figure 3.4 (example 3.6, which has a terminal state), and the transition system TS' from figure 3.5. Safety properties satisfied in TS' are satisfied in TS. However, $\text{Tr}_{\text{fin}}(TS) \not\subseteq \text{Tr}_{\text{fin}}(TS')$ (even though the sets of infinite traces are equal).

Example 3.8. Consider the transition system TS' shown in figure 3.7 (page 20) and TS the transition system shown in figure 3.6. The transition system TS' has terminal states and TS does not. However, we have that

$$\text{Tr}_{\text{fin}}(TS) = \text{Tr}_{\text{fin}}(TS').$$

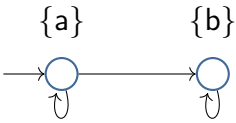

Figure 3.6 | *A transition system with no terminal state*

We also have that

$$\mathrm{Tr}^\omega(TS') = \{\mathsf{a}\}^\omega \quad \text{and} \quad \mathrm{Tr}^\omega(TS) = \{\mathsf{a}\}^\omega \cup \{\mathsf{a}\}^+ \cdot \{b\}^\omega.$$

Thus giving a counter example to the previous lemma if one of the transition system has terminal states: consider a linear-time property P with the set of "bad behaviors" as $P_{\text{bad}} = \{\mathsf{a}\}^+ \cdot \{\mathsf{b}\}$, then $TS' \not\approx P$ but $TS \not\approx P$.

The rest of the course will be done in french.

L'objectif est de trouver des conditions sur TS et TS' telles que l'on ait l'équivalence entre :

- $\mathrm{Tr}^\omega(TS) \subseteq \mathrm{Tr}^\omega(TS')$;
- pour toute propriété de sûreté P, $TS' \not\approx P$ implique $TS \not\approx P$.

On commence par trouver des conditions sur TS et TS' telles que l'on ait l'équivalence :

$$\mathrm{Tr}^\omega(TS) \subseteq \mathrm{Tr}^\omega(TS') \iff \mathrm{Tr}_{\text{fin}}(TS) \subseteq \mathrm{Tr}_{\text{fin}}(TS').$$

Pour que l'on ait « $\implies$ », il est nécessaire que TS soit sans état terminal. En effet, si TS est sans état terminal, alors pour tout $\hat{\sigma} \in \mathrm{Tr}_{\text{fin}}(TS)$, il existe $\sigma \in \mathrm{Tr}^\omega(TS)$ tel que $\hat{\sigma} \subseteq \sigma$.

Dans l'autre sens, supposons que $\mathrm{Tr}_{\text{fin}}(TS) \subseteq \mathrm{Tr}_{\text{fin}}(TS')$. Soit $\sigma \in \mathrm{Tr}^\omega(TS)$. Alors, pour tout $\hat{\sigma} \subseteq \sigma$, on a $\hat{\sigma} \in \mathrm{Tr}_{\text{fin}}(TS) \subseteq \mathrm{Tr}_{\text{fin}}(TS')$. Ainsi, pour tout $n \in \mathbb{N}$, on a qu'il existe un chemin $\pi^n := (\pi_i^n)_{i \leq n}$ initial dans TS' tel que $L(\pi^n) = \sigma(0) \dots \sigma(n)$.

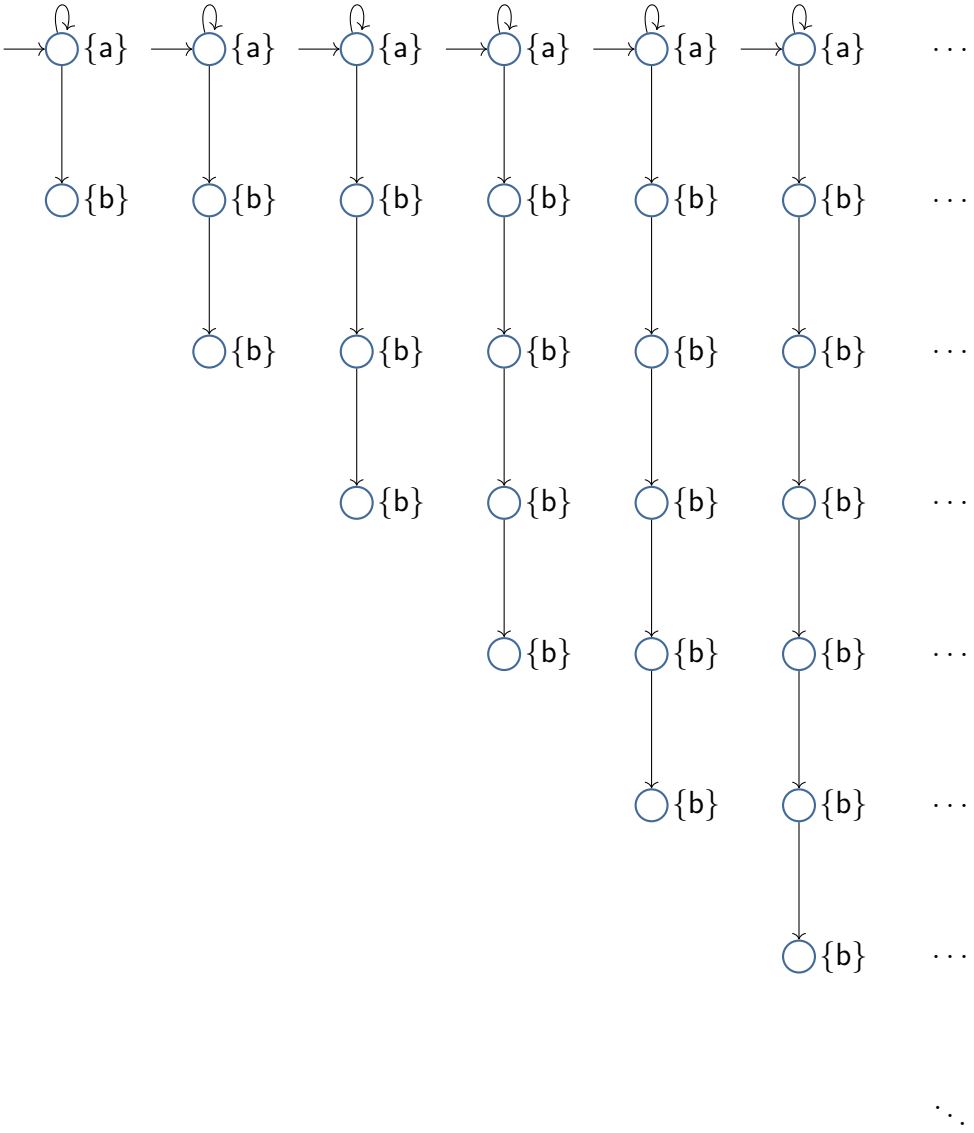

Figure 3.7 | *An infinite transition system*

Exemple 3.1. On considère TS comme celui représenté en figure 3.6 et TS' comme représenté en figure 3.8. On a que

$$\mathrm{Tr}_{\mathrm{fin}}(TS) = \mathrm{Tr}_{\mathrm{fin}}(TS') = \{\mathsf{a}\}^\star \cup \{\mathsf{a}\}^+\{\mathsf{b}\}^\star,$$

et

$$\mathrm{Tr}^\omega(TS) = \{\mathsf{a}\}^\omega \cup \{\mathsf{a}\}^+\{\mathsf{b}\}^\omega \neq \{\mathsf{a}\}^+\{\mathsf{b}\}^\omega = \mathrm{Tr}^\omega(TS').$$

Dans notre cas, on a $\{\mathsf{a}\}^n \subseteq \mathrm{Tr}_{\mathrm{fin}}(TS')$ mais on n'a pas $\{\mathsf{a}\}^\omega \subseteq \mathrm{Tr}^\omega(TS')$.

Définition 3.1 (Branchement fini)**.** Un système de transition $TS = (S, \mathrm{Act}, \to, I, \mathrm{AP}, L)$ est à *branchement fini* si

1. I est fini ;
2. pour tout $s \in S$, l'ensemble $\{s' \mid \exists \alpha \in \mathrm{Act}, s \xrightarrow{\alpha} s'\}$ est fini.

Interlude. Le lemme de Kőnig.

Définition 3.2. Soit A un ensemble.

1. Un *arbre* sur A est un ensemble $T \subseteq A^\star$ clos par préfixe, c'est-à-dire que si $u \in T$ alors pour tout préfixe $v \subseteq u$, on a $v \in T$.
2. Un chemin infini dans un arbre $T \subseteq A^\star$ est un mot $\pi \in A^\omega$ tel que, pour tout $n \in \mathbb{N}$, $\pi(0) \dots \pi(n) \in T$.
3. Un arbre est à *branchement fini* si, pour tout $u \in T$, l'ensemble $\{ua \mid a \in A \text{ et } ua \in T\}$ est fini.

Remarque 3.1. Si A est fini, alors tout arbre sur A est à branchement fini.

Aussi, si T est fini alors T n'as pas de chemin infini.

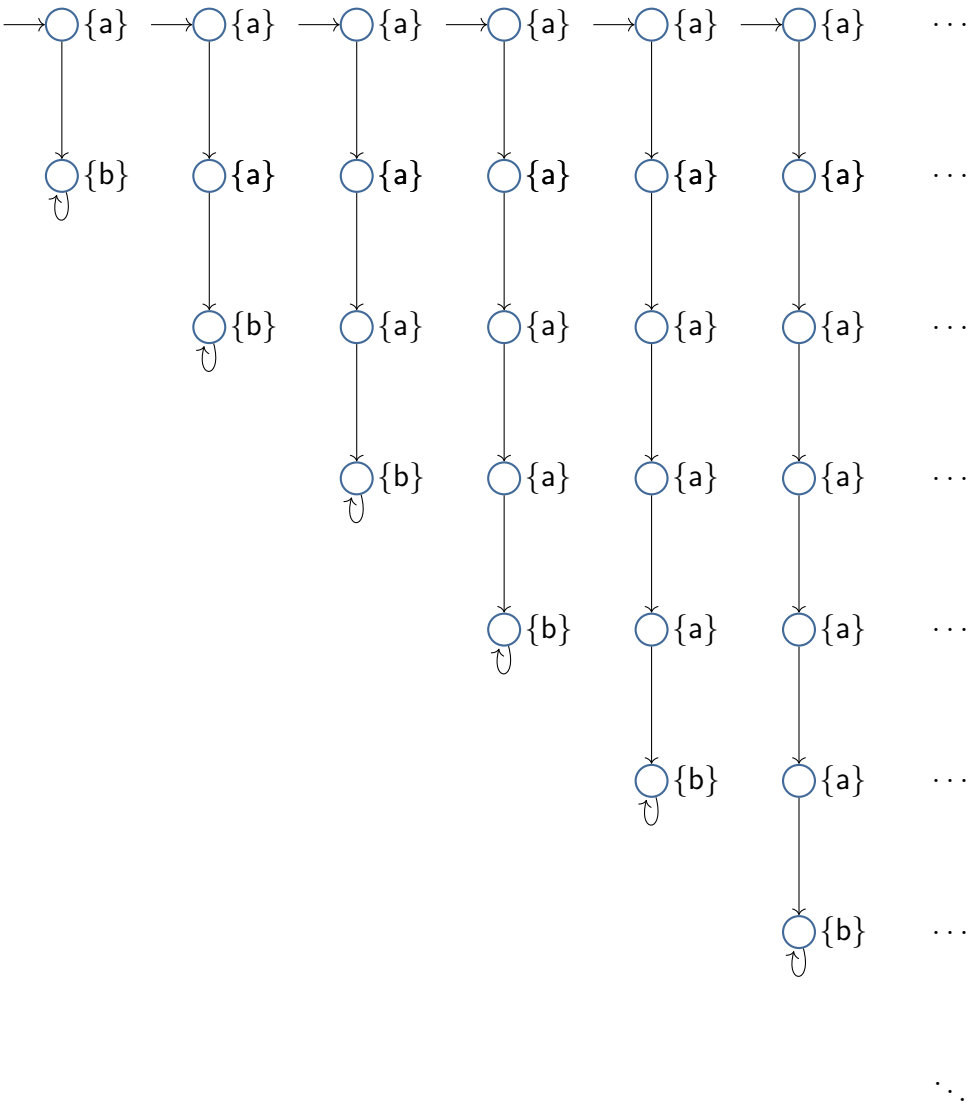

Fig. 3.8 | *Un système de transition infini*

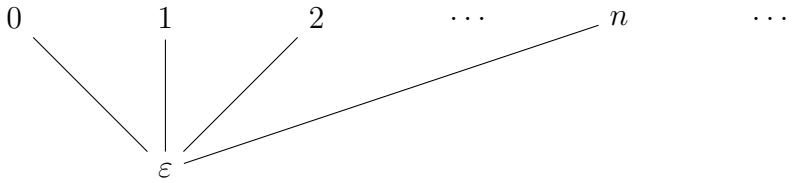

Fig. 3.9 | *Arbre* $\{\varepsilon\} \cup \mathbb{N}$ *sur* $\mathbb{N}$

Exemple 3.2. Avec $T \subseteq \mathbb{N}^\star$ défini par $T = \{\varepsilon\} \cup \mathbb{N}$ alors T est sans chemin infini et à branchement infini (figure 3.9).

Lemme 3.1 (Lemme de Kőnig). Si T est un arbre infini et à branchement fini alors T a un chemin infini.

Preuve. Soit $T \subseteq A^\star$ un arbre infini à branchement fini. Si $u \in T$ on note $T \restriction u$ l'arbre

$$\{v \in T \mid u \subseteq v \text{ ou } v \subseteq u\}.$$

On remarque que $T = T \restriction \varepsilon$ et $T \restriction u = \bigcup_{a \in A\ ua \in T} T \restriction ua$. Alors, comme que T est infini et $T = \bigcup_{a \in A \cap T} T \restriction a$, par e lemme des tiroirs infini, il existe $a \in A \cap T$ tel que $T \restriction a$ est infini. On a donc

$$T \restriction a = \bigcup_{b \in A\ ab \in T} T \restriction ab.$$

Par induction sur $n \in \mathbb{N}$, on définit $a_0, \ldots, a_n \in A$ (en étendant) tel que $a_0 \ldots a_n \in T$ et $T \restriction a_0 \ldots a_n$ est infini. On obtient donc $\pi = (a_i)_{i \in \mathbb{N}}$ qui est un chemin infini dans T. □

Remarque 3.2 (Attention !). On doit manipuler un arbre !

En considérant $A = \{0, 1\}$ avec $T_0 = \{0\}^\star\{1\} \subseteq A^\star$, on a que :

- T_0 est infini ;

- ▷ T_0 est à branchement fini ;
- ▷ MAIS, ce n'est pas un arbre.

On considère donc $T = \mathrm{Pref}(T_0)$ qui est un arbre infini et à branchement fini. Alors, par le lemme de Kőnig, on a que T a un chemin infini $\pi \in \{0\}^\omega$ (il n'y a qu'un seul choix possible). Et, on a $\mathrm{Pref}(\pi) \subseteq T$ sauf que $\mathrm{Pref}(\pi) \cap T_0 = \emptyset$.

On peut maintenant revenir à notre objectif de caractériser les propriétés de sûreté par les traces.

Proposition 3.1. Si TS est sans état terminal et TS' est à branchement fini, on a que

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

Preuve.

- ▷ « $\Longrightarrow$ ». On l'a déjà vu précédemment.
- ▷ « $\Longleftarrow$ ». Supposons $\mathrm{Tr}_{\mathrm{fin}}(TS) \subseteq \mathrm{Tr}_{\mathrm{fin}}(TS')$. Considérons un mot $\sigma \in \mathrm{Tr}^\omega(TS)$. Soit $T' \subseteq (S')^\star$ (où S' est l'ensemble des états de TS') défini par

  $$T' = \{u \in (S')^\star \mid u \text{ chemin initial fini de } TS' \text{ et } L'(u) \subseteq \sigma\}.$$

  On a que T' est un arbre, qui est infini (car $\mathrm{Tr}_{\mathrm{fin}}(TS) \subseteq \mathrm{Tr}_{\mathrm{fin}}(TS')$. Aussi, on a que T' est à branchement fini car TS' est à branchement fini. Par le lemme de Kőnig, on a que T' a un chemin infini π. On a aussi $L'(\pi) = \sigma$ et donc $\sigma \in \mathrm{Tr}^\omega(TS')$.

□

Corollaire 3.1. Si TS et TS' sont deux systèmes de transitions sans états terminaux et à branchement fini alors les deux propriétés suivantes sont équivalentes :

- ▷ $\mathrm{Tr}^\omega(TS) = \mathrm{Tr}^\omega(TS')$;

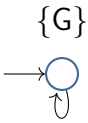

Fig. 3.10 | *Un feu tricolore un peu dangereux*

▷ pour toute propriété de sûreté P, $TS' \not\approx P$ ssi $TS \not\approx P$. □

3.2.3 Propriétés de vivacité.

L'idée est de s'assurer que « quelque chose de bon peut toujours arriver ».

Exemple 3.3. Avec $\mathrm{AP} = \{\mathsf{G}, \mathsf{Y}, \mathsf{R}\}$ et TS défini comme en figure 3.10. On a que TS satisfait « si R à un instant donné alors Y à l'instant précédent » (on note cette propriété P_{safe}). Cependant TS ne satisfait pas $P_{\text{live}} := \{\sigma \mid \exists^{\infty} t, \mathsf{R} \in \sigma(t)\}$.

Définition 3.3 (Vivacité). On dit que $P \subseteq (\mathbf{2}^{\mathrm{AP}})^{\omega}$ est une propriété de *vivacité* si, pour tout mot fini $\hat{\sigma} \in (\mathbf{2}^{\mathrm{AP}})^{\star}$, il existe $\sigma \in (\mathbf{2}^{\mathrm{AP}})^{\omega}$ tel que $\hat{\sigma} \subseteq \sigma$ et $\sigma \in P$.

Exemple 3.4. Avec l'exemple de la BVM, les propriétés (3) et (4) sont des propriétés de vivacité.

Dans la suite, on montrera le théorème de décomposition suivant en passant au point de vue topologique.

Théorème 3.1. Pour toute propriété $P \subseteq (\mathbf{2}^{\mathrm{AP}})^{\omega}$, il existe

- ▷ P_{safe} une propriété de sûreté,
- ▷ P_{live} une propriété de vivacité,

tels que $P = P_{\text{safe}} \cap P_{\text{live}}$.

Proposition 3.2. La propriété $\mathsf{True} := (\mathbf{2}^{\mathrm{AP}})^{\omega} \subseteq (\mathbf{2}^{\mathrm{AP}})^{\omega}$ est l'unique LT-property sur AP qui est une propriété de sûreté et de vivacité.

Preuve.

▷ On a que True est une propriété de sûreté en posant l'ensemble des « mauvais comportements » comme $\mathsf{True}_{\mathrm{bad}} := \emptyset$.

▷ On a que True est une propriété de vivacité car, pour tout mot fini $\hat{\sigma} \in (\mathbf{2}^{\mathrm{AP}})^{\star}$, il existe $\sigma \in (\mathbf{2}^{\mathrm{AP}})^{\omega}$ tel que $\hat{\sigma} \subseteq \sigma$.

▷ **Unicité.** Soit $P \subseteq (\mathbf{2}^{\mathrm{AP}})^{\omega}$ de sûreté pour $P_{\mathrm{bad}} \subseteq (\mathbf{2}^{\mathrm{AP}})^{\star}$. Si P est une propriété de vivacité alors pour tout $\hat{\sigma} \in P_{\mathrm{bad}}$ alors il existe $\sigma \in P$ tel que $\hat{\sigma} \subseteq \sigma$. Donc, on a que $P_{\mathrm{bad}} = \emptyset$ et donc $P = \mathsf{True}$.

□

4 L'approche topologique.

Définition 4.1. Un *espace topologique* est une paire $(X, \Omega X)$ où X est un ensemble et $\Omega X \subseteq \wp(X)$ que l'on appelle *ensemble des ouverts* telle que

- si $\mathcal{S} \subseteq_{\text{fin}} \Omega X$ alors $\bigcap \mathcal{S} = \bigcap_{V \in \mathcal{S}} V \in \Omega X$;
- si $\mathcal{S} \subseteq \Omega X$ alors $\bigcup \mathcal{S} = \bigcup_{V \in \mathcal{S}} V \in \Omega X$.

Remarque 4.1. On a toujours $\emptyset, X \in \Omega X$ avec $\emptyset = \bigcup \emptyset$ et $X = \bigcap \emptyset$.

Exemple 4.1 (Topologie sur Σ^ω et intuition)**.** On peut voir les ouverts comme « analogues » aux ensembles récursivement énumérables.

On définit une topologie sur Σ^ω où les ouverts sont $\mathsf{ext}(W)$ où $W \subseteq \Sigma^\star$ et $\mathsf{ext}(W) = \bigcup_{u \in W} \mathsf{ext}(u)$ et

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

Ainsi, si on a une manière d'énumérer W, on peut tester si $u \in \mathsf{ext}(W)$ en temps fini, mais il n'est pas forcément possible de vérifier que $u \notin \mathsf{ext}(W)$.

Définition 4.2. Soit $(X, \Omega X)$ un espace topologique. Alors, on appelle *fermé* un sous-ensemble $C \subseteq X$ tel que $X \setminus C \in \Omega X$.

Remarque 4.2. On a donc que $\emptyset$ et X sont toujours fermés.

Remarque 4.3. L'ensemble des fermés sur $(X, \Omega X)$ est stable par

- ▷ intersections arbitraire ;
- ▷ unions finies.

Ce sont les « duales » des propriétés de stabilité des ouverts.

Avec quelques manipulations « simples », on peut arriver à la caractérisation suivante.

Lemme 4.1. Soit $(X, \Omega X)$ un espace topologique.

- ▷ On a que $A \subseteq X$ est un ouvert ssi $\forall x \in X$ on a l'équivalence suivante

$$x \in A \iff \exists U \in \Omega X, \quad x \in U \subseteq A.$$

- ▷ On a que $A \subseteq X$ est un fermé ssi $\forall x \in X$ on a l'équivalence suivante

$$x \in A \iff \forall U \in \Omega X, \quad (x \in U \implies A \cap U \neq \emptyset).$$

Lemme 4.2 (Avec Σ^ω).

- ▷ Sur Σ^ω, on a que $A \subseteq \Sigma^\omega$ est ouvert ssi $\forall \sigma \in \Sigma^\omega$, on a l'équivalence suivante

$$\sigma \in A \iff \exists \hat{\sigma} \subseteq \sigma, \mathsf{ext}(\hat{\sigma}) \subseteq A.$$

- ▷ Sur Σ^ω, on a que $A \subseteq \Sigma^\omega$ est fermé ssi $\forall \sigma \in \Sigma^\omega$, on a l'équivalence suivante

$$\sigma \in A \iff \forall \hat{\sigma} \subseteq \sigma, \mathsf{ext}(\hat{\sigma}) \cap A \neq \emptyset,$$

autrement dit,

$$\sigma \in A \iff \forall n \in \mathbb{N}, \begin{cases} \mathsf{ext}(\sigma(0)\dots\sigma(n)) \cap A \neq \emptyset \\ \Updownarrow \\ \forall \hat{\sigma} \subseteq \sigma, \exists \beta \supseteq \hat{\sigma}, \beta \in A. \end{cases}$$

Exemple 4.2. L'ensemble $\{\mathsf{a}\}^\omega$ est un fermé mais pas un ouvert. En effet, si $\hat{\sigma} \subseteq \mathsf{a}^\omega$ alors $\hat{\sigma} = \mathsf{a}^n$, mais, si $|\Sigma| \geq 2$,

$$\mathsf{ext}(\mathsf{a}^n) \not\subseteq \{\mathsf{a}^\omega\}.$$

Corollaire 4.1. Une propriété $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ est de sûreté ssi P est un fermé.

Preuve. L'idée est que $\mathsf{ext}(P_{\mathrm{bad}})$ est un ouvert et que

$$P = (\mathbf{2}^{\mathrm{AP}})^\omega \setminus \mathsf{ext}(P_{\mathrm{bad}}).$$

□

Proposition 4.1 (Clôture). Soit $A \subseteq X$ où $(X, \Omega X)$ est un espace topologique. Alors,

$$\bar{A} := \bigcap_{A \subseteq C \text{ où } C \text{ fermé}} C$$

est un fermé.

Remarque 4.4. On a que A est un fermé ssi $\bar{A} = A$.

4.1 Théorème de décomposition.

Définition 4.3. Pour $(X, \Omega X)$ un espace topologique, on dit que $A \subseteq X$ est *dense* si

$$\forall U \in \Omega X, \quad U \neq \emptyset \implies U \cap A \neq \emptyset.$$

Exemple 4.3. Une partie $A \subseteq \Sigma^\omega$ est dense ssi

$$\forall u \in \Sigma^\star \quad \mathsf{ext}(u) \cap A \neq \emptyset,$$

autrement dit, pour tout mot fini $u \in \Sigma^\star$, il existe $\sigma \in \Sigma^\omega$ qui étend u (*i.e.* $u \subseteq \sigma$) et tel que $\sigma \in A$.

Lemme 4.3. On a que $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ est une propriété de vivacité ssi P est dense.

Théorème 4.1 (Décomposition). Soit $(X, \Omega X)$ un espace et $A \subseteq X$. Alors il existe $C \subseteq X$ un fermé et $D \subseteq X$ dense tel que

$$A = C \cap D.$$

Preuve. On pose $C := \bar{A}$ et $D := A \cup (X \setminus \bar{A})$. Ainsi, on a bien que $A = C \cap D$. On a aussi que C est fermé. Montrons que D est dense.

Soit $U \in \Omega X$ non vide. Si $U \cap A = \emptyset$ alors $A \subseteq X \setminus U$, qui est un fermé. Donc $\bar{A} \subseteq X \setminus U$ et $U \subseteq X \setminus \bar{A}$. □

4.2 Bases.

Définition 4.4. Soit X un ensemble et $\mathscr{B} \subseteq \wp(X)$ tel que $\mathscr{B}$ est stable par intersections finies. Alors,

$$\Omega := \left\{ \bigcup_{i \in I} B_i \;\middle|\; \forall i \in I, B_i \in \mathscr{B} \right\}$$

est une topologie sur X et $\mathscr{B}$ est appelée *base* de Ω. Autrement dit, on a défini

$$\Omega := \left\{ \bigcup \mathscr{F} \;\middle|\; \mathscr{F} \subseteq \mathscr{B} \right\}.$$

Lemme 4.4 (Quelques propriétés).
- ▷ Si $u \subseteq v$ alors $\mathsf{ext}(v) \subseteq \mathsf{ext}(u)$.
- ▷ Si $|\Sigma| \geq 2$ et $\mathsf{ext}(v) \subseteq \mathsf{ext}(u)$ alors $u \subseteq v$.

(Attention à la contravariance !)

- ▷ Pour $u, v \in \Sigma^\star$, on a

$$\mathsf{ext}(u) \cap \mathsf{ext}(v) = \begin{cases} \mathsf{ext}(v) & \text{si } u \subseteq v \\ \mathsf{ext}(u) & \text{si } v \subseteq u \\ \emptyset & \text{sinon.} \end{cases}$$

Remarque 4.5. Sur Σ^ω, on a que pour tout ouvert U, il existe $W \subseteq \Sigma^\star$ tel que $U = \bigcup_{v \in W} \mathsf{ext}(v)$. Avec le lemme précédent, on a que $\Omega\Sigma^\omega$ a pour base

$$\{\mathsf{ext}(u) \mid u \in \Sigma^\star\} \cup \{\emptyset\}.$$

Remarque 4.6. On a $\mathsf{ext}(\varepsilon) = \Sigma^\omega$.

Remarque 4.7. L'ensemble Σ^ω est un *espace métrique complet* pour la distance

$$\begin{aligned} d : \Sigma^\omega \times \Sigma^\omega &\longrightarrow [0,1] \\ \alpha, \beta &\longmapsto \begin{cases} 0 & \text{si } \alpha = \beta \\ 1/2^{\min n \mid \alpha(n) \neq \beta(n)} & \text{sinon.} \end{cases} \end{aligned}$$

On a que $d(\alpha, \gamma) \leq \max\big(d(\alpha, \beta), d(\beta, \gamma)\big)$.

5 Ordres partiels et treillis.

5.1 Ordres partiels.

Définition 5.1. Un *ordre partiel* (ou *poset* en anglais) est une paire $(P, \leq)$ où $\leq$ est une relation binaire sur P telle que

- ▷ (*reflexivité*) $\forall x \in P, x \leq x$;
- ▷ (*transitivité*) $\forall x, y \in P, x \leq y \implies y \leq z \implies x \leq z$;
- ▷ (*antisymétrie*) $\forall x, y \in P, x \leq y \implies y \leq x \implies x = y$.

Un préodre est une relation binaire reflexive et transitive.

Exemple 5.1. On donne quelques exemples de poset :

1. $(\wp(X), \subseteq)$, l'inclusion dans les parties de X
2. $(\Omega X, \subseteq)$, l'inclusion dans les ouverts de X
3. $(\Sigma^\star, \subseteq)$, la relation préfixe dans les mots sur Σ

Attention, dans les trois exemples, il existe deux éléments u, v où

$$u \not\leq v \quad \text{et} \quad v \not\leq u.$$

Définition 5.2 (Dual)**.** Soit $(P, \leq)$ un poset. Le *dual* de P est $(P, \leq)^{\text{op}} := (P, \geq)$ où

$$a \geq b \iff b \leq a.$$

Définition 5.3 (Fonction (anti)monotone)**.** Soit $(P, \leq_P)$ et $(L, \leq_L)$ deux posets. Une fonction $f : P \to L$ est *monotone* si pour tout $a, b \in P$ on a

$$a \leq_P b \implies f(a) \leq_L f(b).$$

On dit que $f : (P, \leq) \to (L, \leq)$ est *antimonotone* si $f : (P, \text{¬}\geq) = (P, \leq_P)^{\text{op}} \to (L, \leq_L)$ est monotone, autrement dit pour tout $a, b \in P$ on a

$$a \leq_P b \implies f(a) \geq_L f(b).$$

5.2 Treillis complet.

Définition 5.4. Soit $(A, \leq)$ un poset et $S \subseteq A$.

- ▷ Un *upper bound* de S est un élément $a \in A$ tel que $\forall s \in S$, $s \leq a$.
- ▷ Un *least upper bound* (*lub*, *join* ou *sup*) de S est un upper bound $a \in A$ de S tel que, pour tout upper bound $b \in A$ de S, on a $a \leq b$.

Par dualité, on a les définitions suivantes.

- ▷ Un élément $a \in A$ est un *lower bound* de S ssi a est un upper bound de S dans A^{op}.
- ▷ Un élément $a \in A$ est un *greatest lower bound* (*glb*, *meet*, *inf*) de S ssi a est un least upper bound de S dans A^{op}.

On note $\bigvee S$ le least upper bound de S. On note $\bigwedge S$ le greatest lower bound de S.

Exemple 5.2. Soit $S \subseteq \wp(X)$ alors le least upper bound de S dans $(\wp(X), \subseteq)$ est $\bigcup S \in \wp(X)$. Le greatest lower bound de S dans $(\wp(X), \subseteq)$ est $\bigcap S \in \wp(X)$.

Exemple 5.3. Soit $S \subseteq \Omega X$ alors le least upper bound dans $(\Omega X, \subseteq)$ est $\bigcup S \in \Omega X$. Le greatest lower bound dans $(\Omega X, \subseteq)$ n'est pas évident. En effet,

$$\{\mathsf{ext}(\mathsf{a}^n) \mid n \in \mathbb{N}\} \subseteq \Omega\Sigma^\omega,$$

mais $\bigcap_{n\in\mathbb{N}} \mathsf{ext}(\mathsf{a}^n) = \{\mathsf{a}^\omega\} \notin \Omega\Sigma^\omega$.

Exemple 5.4. Dans $(\Sigma^\star, \subseteq)$ (la relation « préfixe de »), une partie $S \subseteq \Sigma^\star$ n'a pas forcément de sup.

Définition 5.5. Un poset $(L, \leq)$ est un *treillis complet* si

- ▷ tout $S \subseteq L$ a un sup $\bigvee S \in L$;
- ▷ tout $S \subseteq L$ a un inf $\bigwedge S \in L$.

Remarque 5.1 (Unicité du lub/glb)**.** Par antisymétrie, si a et b sont deux least upper bound (ou greatest lower bound) alors $a = b$.

En conséquence on a que tout treillis complet a

- ▷ un plus petit élément $\bot := \bigvee \emptyset \in L$;
- ▷ un plus grand élément $\top := \bigwedge \emptyset \in L$.

Remarque 5.2 (Non-exemple)**.** Le poset $(\Sigma^\star, \subseteq)$ (avec la relation « préfixe de ») n'est ***pas*** un treillis complet, car il n'a pas de plus grand élément $\top$.

Exemple 5.5. Le poset $(\wp(X), \subseteq)$ (avec la relation d'inclusion ensembliste) est un treillis complet.

Lemme 5.1. Les conditions suivantes sont équivalentes pour un poset $(L, \leq)$:

1. $(L, \leq)$ est un treillis complet ;
2. tout $S \subseteq L$ a un sup $\bigvee S \in L$;
3. tout $S \subseteq L$ a un inf $\bigwedge S \in L$;

Preuve. Pour montrer l'implication « 2. $\implies$ 3. », on peut définir

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

et montrer que c'est bien un inf. □

Exemple 5.6. En revenant sur $(\Omega X, \subseteq)$, c'est un treillis complet dont l'inf de $S \subseteq \Omega X$ est

$$\bigwedge S = \bigcup \{V \in \Omega X \mid V \subseteq \bigcap S\}.$$

Il s'agit de $\overset{\circ}{\bigcap} S$ qui est l'*intérieur* de $\bigcap S$.

Par exemple, dans $(\Omega\Sigma^\omega, \subseteq)$, on a

$$\bigwedge \{\mathsf{ext}(\mathsf{a}^n) \mid n \in \mathbb{N}\} = \overset{\circ}{\{\mathsf{a}^\omega\}} = \emptyset.$$

5.3 Opérateur de clôture.

Définition 5.6. Soit $(A, \leq)$ un poset. Un *opérateur de clôture* suer $(A, \leq)$ est une fonction

$$c : A \to A$$

telle que

- ▷ c est monotone ;

- ▷ c est « *expansive* » : pour tout $a \in A$, $a \leq c(a)$;
- ▷ c est *idempotent* : $c(c(a)) = c(a)$ pour tout $a \in A$.

Exemple 5.7. Soit $(X, \Omega X)$ un espace topologique. Alors

$$\wp(X) \ni A \mapsto \bar{A} \in \wp(X)$$

est un opérateur de clôture sur $(\wp(X), \subseteq)$.

Lemme 5.2. Soit c un opérateur de clôture sur $(L, \leq)$. On pose

$$L^c := \{a \in L \mid \underbrace{c(a) = a}_{a \in \operatorname{im} c}\}.$$

Si $(L, \leq)$ est un treillis complet alors $(L^c, \leq)$ est un treillis complet avec

$$\forall S \subseteq L^c, \qquad \bigwedge^{L^c} S = \bigwedge^{L} S.$$

Exemple 5.8. Pour $\overline{(-)} : \wp(X) \to \wp(X)$ où $(X, \Omega X)$ est un espace topologique, on a

$$\big(\wp(X)\big)^{\overline{(-)}} = \{F \in \wp(X) \mid F \text{ fermé}\}.$$

Dans ce treillis complet :

$$\bigwedge \mathscr{F} = \bigcap \mathscr{F} \qquad \text{et} \qquad \bigvee \mathscr{F} = \overline{\bigcup \mathscr{F}},$$

où $\mathscr{F}$ est un ensemble de fermés.

5.4 Connexion de Galois.

Définition 5.7. Considérons deux posets $(A, \leq_A)$ et $(B, \leq_B)$. Une *connexion de Galois* $g \dashv f : A \to B$ est une paire (f, g) de

fonctions :

$$f : B \to A \qquad \text{et} \qquad g : A \to B$$

telle que

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

Exemple 5.9. Soit $f : X \to Y$ une fonction. On possède deux « lifts » de f sur les powersets :

- ▷ le lift covariant $f_! : \begin{array}{ccc} \wp(X) & \longrightarrow & \wp(Y) \\ A & \longmapsto & \{f(a) \mid a \in A\} \end{array}$;
- ▷ le lift contravariant $f^\bullet : \begin{array}{ccc} \wp(Y) & \longrightarrow & \wp(X) \\ B & \longmapsto & \{x \in X \mid f(x) \in B\} \end{array}$.[1]

On a que $f_! \dashv f^\bullet$. En effet, pour tout $A \in \wp(X)$ et $B \in \wp(Y)$,

$$\begin{aligned} f_!(A) \subseteq B &\iff \forall x \in X, (x \in A \implies f(x) \in B) \\ &\iff A \subseteq f^\bullet(B). \end{aligned}$$

Exemple 5.10. Soit Σ un alphabet. On a, d'une part,

$$\begin{aligned} \mathrm{Pref} : \wp(\Sigma^\omega) &\longrightarrow \wp(\Sigma^\star) \\ A &\longmapsto \underbrace{\{\hat{\sigma} \in \Sigma^\star \mid \exists \sigma \in A, \hat{\sigma} \subseteq \sigma\}}_{\bigcup_{\sigma \in A} \mathrm{Pref}(\sigma)}. \end{aligned}$$

D'autre part, on a

$$\begin{aligned} \mathrm{cl} : \wp(\Sigma^\star) &\longrightarrow \wp(\Sigma^\omega) \\ W &\longmapsto \{\sigma \in \Sigma^\omega \mid \mathrm{Pref}(\sigma) \subseteq W\}. \end{aligned}$$

Attention, ce n'est pas le cl vu en TD. On a que

$$\mathrm{Pref}(-) \dashv \mathrm{cl}(-).$$

[1] On note habituellement f^* et non $f^\bullet$, mais vu qu'on utilise souvent « $*$ » dans le cours, on change de notation.

Lemme 5.3. ▷ Si $g \dashv f$ et $g' \dashv f$ alors $g = g'$.

▷ Si $g \dashv f$ et $g \dashv f'$ alors $f = f'$.

▷ Si $g \dashv f$ alors g et f sont monotones.

Preuve. Vu en TD. □

Dans $g \dashv f$, on dit que

- ▷ g est un *adjoint à gauche* de f ;
- ▷ f est un *adjoint à droite* de g.

Lemme 5.4. Si $g \dashv f : (A, \leq_A) \to (B, \leq_B)$ alors

$$f \circ g : A \xrightarrow{g} B \xrightarrow{f} A$$

est un opérateur de clôture sur $(A, \leq_A)$.[2]

Preuve. Vu en TD. □

Exemple 5.11. Pour $\mathrm{Pref}(-) \dashv \mathrm{cl}(-) : \wp(\Sigma^\omega) \to \wp(\Sigma^\star)$, le lemme précédent nous donne l'opérateur de clôture

$$\begin{aligned} \mathrm{cl} \circ \mathrm{Pref} : \wp(\Sigma^\omega) &\longrightarrow \wp(\Sigma^\omega) \\ A &\longmapsto \{\sigma \in \Sigma^\omega \mid \mathrm{Pref}(\sigma) \subseteq \mathrm{Pref}(A)\} \end{aligned}$$

(c'est le $\mathrm{cl}(-)$ vu en TD) est la clôture topologique pour $(\Sigma^\omega, \Omega\Sigma^\omega)$.

Remarque 5.3. En particulier, $A \subseteq \Sigma^\omega$ est un fermé si et seulement s'il existe un arbre $T \subseteq \Sigma^\star$ tel que

$$A = \{\pi \in \Sigma^\omega \mid \pi \text{ chemin infini dans } T\}.$$

On a que $\mathrm{cl} \circ \mathrm{Pref}(A)$ qui est un arbre sur Σ.

[2] Attention à ne pas se tromper sur le sens de la composition !

Corollaire 5.1. ▷ Une propriété $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ est de sûreté si et seulement si on a $P = \mathrm{cl}(\mathrm{Pref}(P))$.

▷ Une propriété $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ est de vivacité si et seulement si on a $(\mathbf{2}^{\mathrm{AP}})^\omega = \mathrm{cl}(\mathrm{Pref}(P))$.

Preuve. (Déjà) vu en TD. Ceci correspond exactement au fait que

▷ P est de sûreté ssi P est fermé dans $(\Sigma^\omega, \Omega\Sigma^\omega)$;

▷ P est de vivacité ssi P est dense dans $(\Sigma^\omega, \Omega\Sigma^\omega)$;

▷ $\mathrm{cl} \circ \mathrm{Pref}$ est exactement $\overline{(-)}$ dans $(\Sigma^\omega, \Omega\Sigma^\omega)$.

□

Proposition 5.1. Une propriété $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ est de vivacité si et seulement si $\mathrm{Pref}(P) = (\mathbf{2}^{\mathrm{AP}})^\star$.

Preuve. En effet, par adjonction (connexion de Galois), on a

$$(\mathbf{2}^{\mathrm{AP}})^\star = \mathrm{Pref}((\mathbf{2}^{\mathrm{AP}})^\omega) \subseteq \mathrm{Pref}(P) \iff (\mathbf{2}^{\mathrm{AP}})^\omega \subseteq \mathrm{cl}(\mathrm{Pref}(P)).$$

□

Quelques propriétés des connexions de Galois.

Lemme 5.5. Soit $g \dashv f : A \to B$ une connexion de Galois.

1. pour tout $S \subseteq A$ tel que $\bigvee S \in A$ alors $g(\bigvee S) = \bigvee g_!(S)$;
2. pour tout $S \subseteq B$ tel que $\bigwedge S \in B$ alors $f(\bigwedge S) = \bigwedge f_!(S)$.

Remarque 5.4. Dans le lemme précédent, il est important de remarquer que l'on a une implication « cachée » : $\bigvee S$ existe dans A implique $\bigvee g_!(S)$ existe dans B (et idem pour $\bigwedge$ et f).

Lemme 5.6. Soient $(A, \leq_A)$ et $(B, \leq_B)$ deux treillis complets.

1. Si $g : A \to B$ préserve les sups (*i.e.* $g(\bigvee S) = \bigvee g_!(S)$) alors il existe une fonction $f : B \to A$ telle que $g \dashv f$. Cette fonction est :
$$f(b) := \bigvee \{a \in A \mid g(a) \leq_B b\}.$$

2. Si $f : B \to A$ préserve les infs alors il existe une fonction $g : A \to B$ telle que $g \dashv f$. Cette fonction est :
$$g(a) := \bigwedge \{b \in B \mid a \leq_A f(b)\}.$$

Exemple 5.12 (Algèbres de Heyting complètes)**.** Soit $(L, \leq)$ un treillis complet. Soit $a \in L$. On a une fonction
$$\begin{aligned} - \wedge a : L &\longrightarrow L \\ b &\longmapsto b \wedge a = \bigwedge \{a, b\}. \end{aligned}$$

On dit que $(L, \leq)$ est une *algèbre de Heyting complète* si, pour tout $a \in A$, la fonction $- \wedge a$ a un adjoint à gauche. Si cet adjoint existe, on le note $a \Rightarrow -$. Ceci nous donne que
$$\forall a, b, c \in L, \qquad b \wedge a \leq c \iff b \leq a \Rightarrow c.$$

On a l'équivalence entre :

- $(L, \leq)$ est une algèbre de Heyting complète ;
- pour tout $a \in L$, $- \wedge a : L \to L$ préserve les sups, autrement dit pour tout $S \subseteq L$,
$$\left(\bigvee S\right) \wedge a = \bigvee \{s \wedge a \mid s \in S\}.$$
C'est une sorte de distributivité.

Dans ce cas, on a que

$$a \Rightarrow c = \bigvee \{b \mid b \wedge a \leq c\}.$$

6 Propriétés « observables ».

La terminologie « propriété observable » n'est pas utilisée dans la littérature, mais c'est en réalité la compacité.

Remarque 6.1 (Rappel). Si $f : X \to Y$ alors

$$f_! \dashv f^\bullet : \wp(X) \to \wp(Y),$$

où $f_!$ est l'image directe, et $f^\bullet$ est l'image réciproque.

Ainsi, $f^\bullet : \wp(Y) \to \wp(X)$ préserve les intersections (*i.e.* si $\mathcal{S} \subseteq \wp(Y)$ alors on a que$f^\bullet(\bigcap \mathcal{S}) = \bigcap_{S \in \mathcal{S}} f^\bullet(S)$).

De plus, $f^\bullet$ préserve les unions car $f^\bullet \dashv f_\bullet : \wp(Y) \to \wp(X)$ où

$$\begin{aligned} f_\bullet : \wp(X) &\longrightarrow \wp(Y) \\ A &\longmapsto \bigcup \{B \subseteq Y \mid f^\bullet(B) \subseteq A\}. \end{aligned}$$

Définition 6.1. Soient $(X, \Omega X)$ et $(Y, \Omega Y)$ deux espaces topologiques. Une fonction $f : X \to Y$ est *continue* si $f^\bullet : \wp(Y) \to \wp(X)$ se restreint en une fonction $f^\bullet : \Omega Y \to \Omega X$, autrement dit

$$\forall V \in \Omega Y, \qquad f^\bullet(V) = \{x \in X \mid f(x) \in V\} \in \Omega(X).$$

On définie ainsi une catégorie d'espaces topologiques.

Un *homéomorphisme* $f : X \to Y$ est une bijection continue telle que

$$f^{-1} : Y \to X$$

est continue.[1]

Lemme 6.1. Une fonction $f : \Sigma^\omega \to \Gamma^\omega$ est continue si et seulement si

$$\begin{gathered}\forall \alpha \in \Sigma^\omega, \forall n \in \mathbb{N}, \exists k \in \mathbb{N}, \forall \beta \in \Sigma^\omega, \\ \beta(0)\dots\beta(k) = \alpha(0)\dots\alpha(k) \\ \Downarrow \\ f(\beta)(0)\dots f(\beta)(n) = f(\alpha)(0)\dots f(\alpha)(n).\end{gathered}$$

Autrement dit, f est continue ssi on peut déterminer une partie finie de sa sortie à partir d'une partie finie de son entrée.

Soit $P \subseteq \Sigma^\omega$, et on définit la *fonction caractéristique* de P :

$$\begin{aligned}\chi_P : \Sigma^\omega &\longrightarrow \mathbf{2} = \{0,1\} \\ \alpha &\longmapsto \begin{cases}1 & \text{si } \alpha \in P \\ 0 & \text{si } \alpha \notin P\end{cases}.\end{aligned}$$

Avec $\Omega\mathbf{2} = \wp(\mathbf{2}) = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$ (ce qui est cohérent avec l'idée que $\mathbf{2}$ représente les booléens), on a que χ_P est continue ssi

- $\chi_P^\bullet\{0\} = \Sigma^\omega \setminus P$ est un ouvert ;
- $\chi_P^\bullet\{1\} = P$ est un ouvert.

On arrive donc à la notion de *clopen*.

Définition 6.2. Soit $(X, \Omega X)$ un espace topologique. Une partie $P \subseteq X$ est *clopen* (*ouvert fermé* en français) si P et $X \setminus P$ sont ouverts.

[1] Ce n'est pas évident : par exemple, il y a une bijection $[0,1] \to \mathbb{S}^1$ (où $\mathbb{S}^1$ est le cercle unité de $\mathbb{R}^2$) continue mais la réciproque ne l'est pas.

Remarque 6.2.
1. On a $\emptyset$ est clopen, et que, si A et B sont clopen alors $A \cup B$ est clopen.
2. On a X est clopen, et que, si A et B sont clopen alors $A \cap B$ est clopen (dual du point précédent).
3. Si A est clopen alors $X \setminus A$ est clopen.

Exemple 6.1. Soit $u \in \Sigma^\star$, on a que $\mathsf{ext}(u)$ est ouvert. Mais, on a aussi que $\Sigma^\omega \setminus \mathsf{ext}(u)$ est ouvert :

$$\Sigma^\omega \setminus \mathsf{ext}(u) = \bigcup \{\mathsf{ext}(v) \mid v \neq u \text{ et } \mathsf{length}(v) = \mathsf{length}(u)\}.$$

Remarque 6.3. Sur $(\Sigma^\omega, \Omega\Sigma^\omega)$, tous les $\mathsf{ext}(W)$ où $W \subseteq \Sigma^\star$ est ***fini*** sont clopen. La réciproque est fausse, comme le montre le lemme suivant.

Lemme 6.2. Si Σ est infini et $a \in \Sigma$, alors

$$\Sigma^\omega \setminus \mathsf{ext}(a) = \bigcup_{\Sigma \ni b \neq a} \mathsf{ext}(b)$$

est clopen mais ***pas*** de la forme $\mathsf{ext}(W)$ avec W fini.

6.1 Compacité.

Définition 6.3. Soit $(X, \Omega X)$ un espace topologique.
1. Une partie $A \subseteq X$ est *compacte* si, pour toute famille $(V_i)_{i \in I} \in \Omega X^I$ telle que $A \subseteq \bigcup_{i \in I} V_i$, il existe $J \subseteq I$ ***fini*** tel que $A \subseteq \bigcup_{j \in J} V_j$.
2. On dit que $(X, \Omega X)$ est *compact* si X est une partie compacte.

Remarque 6.4 (Non-exemple). Si Σ est infini alors Σ^ω n'est pas compact :

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

Proposition 6.1. Si Σ est ***fini*** alors Σ^ω est compact.

Preuve. On procède à l'aide du lemme de Kőnig. Supposons que $\Sigma^\omega = \bigcup_{i\in I} U_i$ où $U_i \in \Omega\Sigma^\omega$. On a que $U_i = \mathsf{ext}(V_i)$ pour un $V_i \subseteq \Sigma^\star$ (en général, V_i est infini). Soit $V = \bigcup_{i\in I} V_i \subseteq \Sigma^\star$, et on vérifie que $\mathsf{ext}(V) = \Sigma^\omega$. Pour chaque $n \in \mathbb{N}$, on définit $W_n \subseteq \Sigma^n$ par récurrence :

- ▷ On pose $W_0 := \{\varepsilon\}$ si $\varepsilon \in V$ et $W_0 := \emptyset$ sinon.
- ▷ On pose

$$W_{n+1} := \left\{ u \in V \;\middle|\; u \text{ n'a pas de préfixe dans } \bigcup_{k\leq n} W_k \right\}.$$

On pose enfin $W = \bigcup_{n\in\mathbb{N}} W_n$. On a que $\mathsf{ext}(W) = \mathsf{ext}(V)$ (car, pour tout $v \in V$, il existe $w \in W$ tel que $w \subseteq v$), et W est « prefix-free » (c'est-à-dire que, pour $w, w' \in W$, on a $w \not\subseteq w'$ ssi $w \neq w'$).

Si W est fini alors on s'arrête.

Par l'absurde, supposons W infini, et posons $T = \mathrm{Pref}(W)$ qui est un arbre par définition. L'arbre T est à branchement fini (car Σ est fini), et T est infini (car W l'est) Par le lemme de Kőnig, il existe un chemin infini $\pi \in \Sigma^\omega$ dans T. Comme $\Sigma^\omega = \mathsf{ext}(W)$, il existe $u \in W$ tel que $u \subseteq \pi$. De plus, il existe $a \in \Sigma$ tel que $ua \subseteq \pi$ et donc $ua \in T = \mathrm{Pref}(W)$.

On arrive à une contradiction car $u \in W$ et W est prefix-free. □

Corollaire 6.1. On a que Σ^ω est compact ssi Σ fini. □

Lemme 6.3. Si $(X, \Sigma X)$ est compact et $C \subseteq X$ est fermé alors C est compact.

Preuve. L'idée est que si $C \subseteq \bigcup_{i\in I} V_i$ alors $X \subseteq (X \setminus C) \cup \bigcup_{i\in I} V_i$. □

Corollaire 6.2. Si Σ est fini alors $A \subseteq \Sigma^\omega$ est clopen ss'il existe $W \subseteq \Sigma^\star$ ***fini*** tel que $A = \mathsf{ext}(W)$. □

6.2 Espace Hausdorff.

Définition 6.4. On dit que $(X, \Omega X)$ est *Hausdorff* (ou T_2) lorsque, pour tout $x \neq y \in X$, alors il existe $U, V \in \Omega X$ tels que

$$U \cap V = \emptyset \qquad x \in U \quad \text{et} \quad y \in V.$$

Exemple 6.2. L'espace $(\Sigma^\omega, \Omega\Sigma^\omega)$ est Hausdorff. Soient $\alpha \neq \beta$. Il existe $u \subseteq \alpha$ et $v \subseteq \beta$ tels que $\mathsf{ext}(u) \cap \mathsf{ext}(v)$.

(On peut choisir $u = p\alpha(\mathsf{length}(p))$ et $v = p\beta(\mathsf{length}(p))$ où p est le plus long préfixe commun à α et β.)

Proposition 6.2. Si (X, Ω) est compact Hausdorff et $C \subseteq X$ est compact alors C est fermé.

Preuve. Soit $C \subseteq X$ est compact et $x \notin C$. Pour tout $y \in C$, il existe U_y, V_y tels que $U_y \cap V_y = \emptyset$ et $x \in U_y$ et $y \in V_y$. Donc, on a $C \subseteq \bigcup_{y\in C} V_y$. Comme C est compact, il existe $y_1, \ldots, y_n \in C$ tels que $C \subseteq V_{y_1} \cup V_{y_2} \cup \cdots \cup V_{y_n}$. On a que $x \in U_{y_1} \cup \cdots \cup U_{y_n} =: U \in \Omega X$. Et, $U \subseteq X \setminus C$ car, $U \cap (V_{y_1} \cup \cdots \cup V_{y_n}) = \emptyset$. □

Corollaire 6.3. Si $(X, \Omega X)$ est compact Hausdorff et $C \subseteq X$,

$$C \text{ compact} \iff C \text{ fermé}.$$

7 Logique temporelle linéaire.

7.1 La logique LML.

Remarque 7.1 (Idée). La signification de LML est *linear-time modal logic*. L'idée est de définir une logique pour une propriété LT $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ telle que, pour AP fini, les formules correspondent aux clopens.

Soit AP un ensemble de proposition atomiques.

Définition 7.1. Les formules de LML sont

$$\begin{aligned} \phi, \psi ::= {} & \mathsf{a} && \mathsf{a} \in \mathrm{AP} \\ | \ & \mathsf{True} && (\text{parfois notée } \top) \\ | \ & \mathsf{False} && (\text{parfois notée } \bot) \\ | \ & \phi \wedge \psi \\ | \ & \phi \vee \psi \\ | \ & \neg\phi \\ | \ & \bigcirc \phi \\ & . \end{aligned}$$

La *modalité* $\bigcirc$ est appelée *later* ou *next*.

Définition 7.2. L'*interprétation* $[\![\phi]\!] \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ est définie par :

- $[\![\mathsf{a}]\!] := \{\sigma \mid \mathsf{a} \in \sigma(0)\}$;

- $[\![\mathsf{True}]\!] := (\mathbf{2}^{\mathrm{AP}})^{\omega}$;
- $[\![\phi \wedge \psi]\!] := [\![\varphi]\!] \cap [\![\psi]\!]$;
- $[\![\mathsf{False}]\!] := \emptyset$;
- $[\![\phi \vee \psi]\!] := [\![\varphi]\!] \cup [\![\psi]\!]$;
- $[\![\neg\phi]\!] := (\mathbf{2}^{\mathrm{AP}})^{\omega} \setminus [\![\phi]\!]$;
- $[\![\bigcirc \phi]\!] := \{\sigma \mid \sigma \restriction 1 \in [\![\phi]\!]\}$ où, pour $\sigma \in (\mathbf{2}^{\mathrm{AP}})^{\omega}$, on note

$$\begin{aligned} \sigma \restriction i : \mathbb{N} &\longrightarrow \mathbf{2}^{\mathrm{AP}} \\ k &\longmapsto \sigma \restriction \sigma(k+i), \end{aligned}$$

(c'est un décalage d'indices).

Exemple 7.1. Quelques exemples de mots tels que $\sigma \in [\![\mathsf{a} \vee \bigcirc \mathsf{b}]\!]$:

- $\sigma = \{\mathsf{a}\}\emptyset^{\omega}$,
- $\sigma = \{\mathsf{b}\}\{\mathsf{a},\mathsf{b}\}^{\omega}$,
- $\sigma = \emptyset\{\mathsf{a},\mathsf{b}\}\emptyset^{\omega}$.

Proposition 7.1. Pour ϕ une formule de LML, on a que $[\![\phi]\!]$ est clopen dans $(\mathbf{2}^{\mathrm{AP}})^{\omega}$.

Preuve. Par induction sur ϕ, on a les cas suivants.

- On a que $[\![\mathsf{a}]\!] = \bigcup_{\mathsf{a} \in A \subseteq \mathrm{AP}} \mathsf{ext}(A)$[1] est un ouvert. De plus, on a que $(\mathbf{2}^{\mathrm{AP}})^{\omega} \setminus [\![\mathsf{a}]\!] = \bigcup_{a \notin B \subseteq \mathrm{AP}} \mathsf{ext}(B)$ est un ouvert.
- On a que
  - $[\![\bigcirc \phi]\!] = \bigcup_{u \in W, A \subseteq \mathrm{AP}} \mathsf{ext}(Au)$
  - $(\mathbf{2}^{\mathrm{AP}})^{\omega} \setminus [\![\bigcirc \phi]\!] = \bigcup_{v \in V, A \subseteq \mathrm{AP}} \mathsf{ext}(Av)$

  où par hypothèse d'induction, il existe $V, W \subseteq \Sigma^{\star}$ tels que $[\![\phi]\!] = \mathsf{ext}(W)$ et $(\mathbf{2}^{\mathrm{AP}})^{\omega} \setminus [\![\phi]\!] = \mathsf{ext}(V)$.

▷ De même pour les autres cas.

□

Proposition 7.2. Si AP est ***fini*** et $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ est clopen alors il existe ϕ une formule LML telle que $P = [\![\phi]\!]$.

Preuve. On a que $P = \mathsf{ext}(W)$ où $W \subseteq (\mathbf{2}^{\mathrm{AP}})^\star$ est ***fini***. On a montrer par récurrence sur la taille du mot u que :

$$\forall u \in (\mathbf{2}^{\mathrm{AP}})^\star, \quad \exists \phi_u \text{ une formule LML}, \quad [\![\phi_u]\!] = \mathsf{ext}(u).$$

▷ *Cas de base.* Soit $A \subseteq \mathrm{AP}$, on peut prendre

$$\phi_A := \Big(\bigwedge_{\mathsf{a} \in A} \mathsf{a}\Big) \wedge \Big(\bigwedge_{\mathsf{b} \notin A} \neg \mathsf{b}\Big).$$

▷ *Récurrence.* Soit $u = Av$ où $A \subseteq \mathrm{AP}$ et $v \in (\mathbf{2}^{\mathrm{AP}})^\star$. On peut poser

$$\phi_{Av} := \phi_A \wedge \bigcirc \phi_v.$$

On peut aussi faire le cas de base pour ε, en posant $\phi_\varepsilon := \mathsf{True}$.

□

Corollaire 7.1. Si AP est ***fini*** et $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$ alors

$$P \text{ clopen} \iff \text{il existe } \phi \text{ telle que } [\![\phi]\!] = P.$$

□

7.1.1 Équivalences logiques.

Définition 7.3. On note $\phi \equiv \psi$ lorsque $[\![\phi]\!] = [\![\psi]\!]$. On dit que ϕ et ψ sont *(logiquement) équivalentes*.

[1] On rappelle que $\mathsf{ext}(A) = \{\sigma \mid \sigma(0) = A \subseteq \mathrm{AP}\}$.

On a les équivalences suivantes :

- $\phi \equiv \phi \wedge \phi$
- $\phi \equiv \mathsf{True} \wedge \phi$
- $\mathsf{True} \equiv \phi \vee \neg\phi$
- $\mathsf{False} \equiv \phi \wedge \neg\phi$
- $\phi \equiv \neg\neg\phi$
- $\bigcirc(\phi \vee \psi) \equiv \bigcirc\phi \vee \bigcirc\psi$
- $\bigcirc\mathsf{False} \equiv \mathsf{False}$
- $\bigcirc(\phi \wedge \psi) \equiv \bigcirc\phi \wedge \bigcirc\psi$
- $\bigcirc\mathsf{True} \equiv \mathsf{True}$

d'autres équivalences sont possibles (*c.f.* figure 6 des notes de cours).

7.1.2 *Homework* : Dualité de Stone.

L'idée est de motiver le DM, et de donner quelques bases sur ce que l'on va montrer.

On se place dans le cas où AP est un ensemble fini. Considérons un mot $\sigma \in (\mathbf{2}^{\mathrm{AP}})^\omega$, on pose

$$\mathscr{F}_\sigma := \{[\phi]_\equiv \mid \sigma \in [\![\phi]\!]\},$$

où $[\phi]_\equiv$ est la classe d'équivalence de $\equiv$. Par les résultats précédents, on a que

$$\mathscr{F}_\sigma \cong \{C \mid \sigma \in C \text{ clopen}\}.$$

On a $\sigma \neq \beta$ implique $\mathscr{F}_\sigma \neq \mathscr{F}_\beta$. De plus, on a les propriétés suivantes :

1. si $C \in \mathscr{F}_\sigma$ et $C \subseteq D$ clopen alors $D \in \mathscr{F}_\sigma$;
2. si $C, D \in \mathscr{F}_\sigma$ alors $C \cap D \in \mathscr{F}_\sigma$;
3. $(\mathbf{2}^{\mathrm{AP}})^\omega \in \mathscr{F}_\sigma$;

4. si C, D sont clopen tels que $C \cup D \in \mathscr{F}_\sigma$ alors $C \in \mathscr{F}_\sigma$ ou $D \in \mathscr{F}_\sigma$;
5. $\emptyset \in \mathscr{F}_\sigma$.

Ces cinq propriétés caractérisent totalement les mots infinis, comme le montre le théorème suivant.

Théorème 7.1. Si $\mathscr{F}$ est un ensemble de clopens dans $(\mathbf{2}^{\mathrm{AP}})^\omega$ vérifiant les cinq propriétés, alors il existe $\sigma \in (\mathbf{2}^{\mathrm{AP}})^\omega$ tel que $\mathscr{F} = \mathscr{F}_\sigma$.

Ce théorème est une spécialisation de la *dualité de Stone*.

Définition 7.4. On dit que $(X, \Omega X)$ est un *espace de Stone* s'il est compact, Hausdorff et qu'il admet une base de clopens.

Théorème 7.2. Si $(X, \Omega X)$ est un espace de Stone alors

$$(X, \Omega X) \cong \mathbf{Sp}\big(\underbrace{\{C \mid C \text{ clopen}\}, \subseteq}_{\text{algèbre de Boole}}\big).$$

On va définir le *spectre* $\mathbf{Sp}(B)$ où B est une algèbre de Boole, à l'aide des ultrafiltres sur B et les filtres premiers (*c.f.* les cinq propriétés ci-dessus).

Remarque 7.2 (Idée). Si $\mathscr{F} \subseteq B$ alors c'est une « théorie consistante et complète » où

- ▷ *théorie* : stable par implication, *c.f.* 1.–3.
- ▷ *consistante* : sans contradiction, 5.
- ▷ *complète* : 4., $\forall C$ clopen, si $C \notin \mathscr{F}_\sigma$ alors $(\mathbf{2}^{\mathrm{AP}})^\omega \setminus C \in \mathscr{F}_\sigma$.

7.1.3 Extension de LML avec $\Box$ et $\Diamond$.

Remarque 7.3. Avec LML, on ne définit que des clopens. Ainsi, les propriétés de sécurité ne sont que « finitaires » et il n'y a que $(\mathbf{2}^{\mathrm{AP}})^{\omega}$ comme propriété de vivacité.

Définition 7.5. On ajoute à LML les modalités

- $\Box\,\phi$ qui signifie « always » (notée parfois $\mathrm{A}\phi$) ;
- $\Diamond\,\phi$ qui signifie « eventually » (notée parfois $\mathrm{E}\phi$) ;

où

- $[\![\Box\,\phi]\!] := \{\,\sigma \in (\mathbf{2}^{\mathrm{AP}})^{\omega} \mid \forall n \in \mathbb{N}, \sigma \upharpoonright n \in [\![\phi]\!]\,\}$;
- $[\![\Diamond\,\phi]\!] := \{\,\sigma \mid \exists n \in \mathbb{N}, \sigma \upharpoonright n \in [\![\phi]\!]\,\}$.

Dans la suite, les preuves se termineront par « **QED** » au lieu du symbole usuel « $\square$ », pour enlever l'ambigüité avec la modalité.

Notation. On note $\sigma \Vdash \phi$ pour $\sigma \in [\![\phi]\!]$.

Exemple 7.2. On a

1. $\sigma \Vdash \Diamond\,\mathsf{a}$ ssi $\exists n \in \mathbb{N}, \mathsf{a} \in \sigma(n)$, l'ensemble $[\![\Diamond\,a]\!]$ est ouvert mais pas compact, donc pas un clopen car
$$[\![\Diamond\,\mathsf{a}]\!] = \bigcup_{u \in (\mathbf{2}^{\mathrm{AP}})^{\star}, \mathsf{a} \in A} \mathsf{ext}(uA);$$
2. $\sigma \Vdash \Box\,\mathsf{a}$ ssi $\forall n \in \mathbb{N}, \mathsf{a} \in \sigma(n)$ (l'ensemble $[\![\Box\,\mathsf{a}]\!]$ est un fermé non clopen) ;
3. $\sigma \Vdash \Box\,\Diamond\,\mathsf{a}$ ssi $\exists^{\infty} n, \mathsf{a} \in \sigma(n)$ (c'est une propriété de vivacité) ;
4. $\sigma \Vdash \Diamond\,\Box\,\mathsf{a}$ ssi $\forall^{\infty} n, \mathsf{a} \in \sigma(n)$ (c'est une propriété de vivacité).

Lemme 7.1. On a que :

1. $\Box\,\phi \equiv \neg\Diamond\,\neg\phi$;
2. $\Diamond\,\phi \equiv \neg\Box\,\neg\phi$;
3. $\Box\,\phi \equiv \phi \wedge \bigcirc\,\Box\,\phi$;
4. $\Diamond\,\phi \equiv \phi \vee \bigcirc\,\Diamond\,\phi$.

Avec des $\wedge$ et des $\vee$ infinis, on aurait :

$$\Box\,\phi \equiv \phi \wedge \bigcirc\phi \wedge \bigcirc\bigcirc\phi \wedge \cdots \equiv \bigwedge_{n\in\mathbb{N}} \bigcirc^n\phi$$

et

$$\Diamond\,\phi \equiv \phi \vee \bigcirc\phi \vee \bigcirc\bigcirc\phi \vee \cdots \equiv \bigvee_{n\in\mathbb{N}} \bigcirc^n\phi.$$

Définition 7.6. On étend ensuite LML par variables :

$$\phi, \psi ::= X \mid \cdots,$$

où $X, Y, \ldots \in \mathfrak{X}$. Une *valuation* de $\mathfrak{X}$ est une fonction

$$\rho : \mathfrak{X} \to \wp\big((\mathbf{2}^{\mathrm{AP}})^\omega\big),$$

où la sémantique $[\![\phi]\!]_\rho$ est définie de manière très similaire à $[\![\phi]\!]$ en ajoutant

$$[\![X]\!]_\rho := \rho(X).$$

Notation. Soient ϕ, ρ, X, on pose

$$\begin{aligned}[\![\phi]\!]_\rho(X) : \wp\big((\mathbf{2}^{\mathrm{AP}})^\omega\big) &\longrightarrow \wp\big((\mathbf{2}^{\mathrm{AP}})^\omega\big)\\ A &\longmapsto [\![\phi]\!]_\rho[A/X],\end{aligned}$$

où $\rho[A/X](X) = A$ et $\rho[A/X](Y) = \rho(Y)$ si $Y \neq X$.

Lemme 7.2. Soit ϕ et X n'apparaissant pas dans ϕ. On pose

$$\phi_{\Diamond}(X) := \phi \wedge \bigcirc X \qquad \phi_{\Box}(X) := \phi \wedge \bigcirc X.$$

Alors, pour tout ρ,

- $[\![\Diamond \phi]\!]_\rho$ est le plus petit point fixe de $[\![\phi_{\Diamond}]\!]_\rho(X)$;
- $[\![\Box \phi]\!]_\rho$ est le plus grand point fixe de $[\![\phi_{\Box}]\!]_\rho(X)$.

Preuve. Pour le premier point, on doit montrer les deux propriétés suivantes :

1. $[\![\Diamond \phi]\!]_\rho = [\![\phi_{\Diamond}]\!]([\![\Diamond \phi]\!])$;
2. $\forall P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega,\ P = [\![\phi_{\Diamond}]\!]_\rho(P) \implies [\![\Diamond \phi]\!]_\rho \subseteq P$.

Pour la première propriété, c'est la loi d'expansion de $\Diamond$. Pour la seconde, soit P tel que $P = [\![\phi \vee \bigcirc X]\!](P)$ et $\sigma \in [\![\Diamond \phi]\!]$, et montrons que $\sigma \in P$. Soit $n \in \mathbb{N}$ tel que $\sigma \restriction n \in [\![\phi]\!]$. Alors, on a que $\sigma \restriction n \in [\![\phi \vee \bigcirc X]\!](P)$ et donc $\sigma \restriction n \in P$. Donc $\sigma \restriction (n-1) \in [\![\phi \vee \bigcirc \phi]\!](P) = P$, donc pour tout $i \leq n$, $\sigma \restriction i \in [\![\phi \vee \bigcirc X]\!](P) = P$ et en particulier $\sigma = \sigma \restriction 0 \in P$. **QED**

Définition 7.7. On dit qu'une variable X est *positive* dans ϕ si toutes les occurrences de X dans ϕ sont sous un nombre pair de $\neg$. (On peut donner une définition inductive de « X est positive dans ϕ » et de « ϕ est négative dans ϕ ».)

Exemple 7.3. Dans les exemples ci-dessous, on a que X est positive dans ϕ :

$$\mathsf{a} \wedge \bigcirc X \qquad \mathsf{a} \vee \bigcirc X \qquad \text{et } \neg(\neg \mathsf{a} \wedge \bigcirc \neg X),$$

mais, dans les exemples ci-dessous, X n'est pas positive dans ϕ :

$$\neg X \qquad \text{et} \qquad \neg X \vee (\mathsf{a} \wedge \bigcirc X).$$

Lemme 7.3. Si X est positive dans ϕ alors

$$[\![\phi]\!](X) : \big(\wp\big((\mathbf{2}^{\mathrm{AP}})^\omega\big), \subseteq\big) \longrightarrow \big(\wp\big((\mathbf{2}^{\mathrm{AP}})^\omega\big), \subseteq\big)$$

est monotone. **QED**

7.1.4 Théorème de Knaster-Tarski.

Définition 7.8. Soient $(L, \leq)$ un poset et $f : L \to L$.

1. On dit que $a \in L$ est un *pré-pointfixe* de f si $f(a) \leq a$.
2. On dit que $a \in L$ est un *post-pointfixe* de f si $a \leq f(a)$.

Théorème 7.3 (Knaster-Tarski)**.** Soit $f : L \to L$ une fonction monotone où $(L, \leq)$ est un treillis complet. Alors

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

est le plus petit point fixe de f, et

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

est le plus grand point fixe de f.

Preuve. Vu en TD. **QED**

Lemme 7.4. Soit $f : (\wp(X), \subseteq) \to (\wp(X), \subseteq)$ monotone. On pose

$$\begin{aligned} g : \wp(X) &\longrightarrow \wp(X) \\ A &\longmapsto g(A) = X \setminus f(X \setminus A). \end{aligned}$$

On a alors que

$$\mu(f) = X \setminus \nu(g) \qquad \nu(f) = X \setminus \mu(g).$$

Preuve.

$$\begin{aligned} X \setminus \nu(g) &= X \setminus \bigcup \{ A \mid A \subseteq g(a) \} \\ &= \bigcap \{ X \setminus A \mid A \subseteq g(A) \} \\ &= \bigcap \{ X \setminus A \mid A \subseteq X \setminus f(X \setminus A) \} \\ &= \bigcap \{ X \setminus A \mid f(X \setminus A) \subseteq X \setminus A \} \\ &= \bigcap \{ B \mid f(B) \subseteq B \} \\ &= \nu(f). \end{aligned}$$

QED

7.2 La logique LTL.

La logique LTL est une extension de LML par certains points fixes. Soit $\theta(X)$ avec X positive dans θ. On peut écrire

$$\theta(X) \equiv \psi \vee \Big(\bigwedge_{i \in I} \Big(\phi_i \wedge \bigwedge_{j \in J_i} \bigcirc^{n_{i,j}} X \Big) \Big),$$

où X n'apparait pas dans ψ ni dans ϕ_i pour tout $i \in I$.

Dans LTL, on va avoir les points fixes de θ si $n_{i,j} = 1$. Dans ce cas, on pourra écrire

$$\theta(X) \equiv \psi \vee (\phi \wedge \bigcirc X),$$

où X n'apparait pas dans ψ ni dans ϕ.

Définition 7.9. On définit la syntaxe de LTL par

$$\begin{aligned} \phi, \psi ::= & \ \mathsf{a} && \mathsf{a} \in \mathrm{AP} \\ & \mid \phi \wedge \psi \\ & \mid \phi \vee \psi \\ & \mid \mathsf{False} \\ & \mid \mathsf{True} \\ & \mid \neg \phi \\ & \mid \bigcirc \phi \\ & \mid \phi \ \mathsf{Until} \ \psi \\ & . \end{aligned}$$

La modalité ϕ Until ψ est notée ϕ U ψ dans les notes de cours.

La sémantique pour LTL est définie de manière identique à la sémantique de LML en ajoutant

$$[\![\phi \ \mathsf{Until} \ \psi]\!] = \left\{ \sigma \in (\mathbf{2}^{\mathrm{AP}})^{\omega} \;\middle|\; \exists i \in \mathbb{N}, \begin{array}{r} \sigma \upharpoonright i \in [\![\psi]\!] \\ \forall j < i, \sigma \upharpoonright j \in [\![\phi]\!] \end{array} \right\}.$$

7.2.1 Points fixes dans LTL.

On étend, dans cette sous-section uniquement, LTL avec des variables (comme pour LML).

Lemme 7.5. Soit X n'apparaissant pas dans ϕ ni ψ. Alors, on a que $[\![\phi \ \mathsf{Until} \ \psi]\!]$ est le plus petit point fixe de $[\![\theta]\!](X)$.

Preuve. On a

$$\phi \ \mathsf{Until} \ \psi \equiv \psi \vee (\phi \wedge \bigcirc (\phi \ \mathsf{Until} \ \psi)).$$

Soit P tel que $P = [\![\theta]\!](P)$. Soit $\sigma \in [\![\phi \ \mathsf{Until} \ \psi]\!]$. Soit $i \in \mathbb{N}$ tel que $\sigma \upharpoonright i \in [\![\psi]\!]$ et $\sigma \upharpoonright 0, \ldots, \sigma \upharpoonright (i-1) \in [\![\phi]\!]$. On a $\sigma \upharpoonright i \in [\![\theta]\!](P) = P$, et comme $\sigma \upharpoonright (i-1) \in [\![\phi]\!]$, on a que $\sigma \upharpoonright (i-1) \in [\![\theta]\!](P) = P$.

Ainsi, pour tout $k \in \{i-1, \dots, 0\}$, on a $\sigma \restriction k \in [\![\theta]\!](P) = P$, donc $\sigma = \sigma \restriction 0 \in P$. **QED**

Remarque 7.4. Si X est (positive et) sous exactement un $\bigcirc$ dans $\theta(X)$ alors c'est le cas aussi dans $\neg\theta[\neg X/X]$.

On a

$$\begin{aligned}\neg\theta[\neg X/X] &= \neg\big(\phi \vee (\psi \wedge \bigcirc(\neg X))\big) \\ &\equiv \neg\psi \wedge (\neg\phi \vee \bigcirc X) \\ &\equiv (\neg\psi \wedge \neg\phi) \vee (\neg\psi \wedge \bigcirc X)\end{aligned}$$

,

donc

$$\mu[\![\neg\theta[\neg X/X]]\!](X) = [\![\neg\psi \text{ Until } (\neg\psi \wedge \neg\phi]\!].$$

Lemme 7.6. Soit X n'apparaissant pas dans ϕ, ψ. Alors

$$[\![\neg(\neg\psi \text{ Until } (\neg\psi \wedge \neg\phi))]\!]$$

qui est un plus petit point fixe de $[\![\theta]\!](X)$ pour $\theta(X) = \psi \vee (\phi \wedge \bigcirc X)$.

Notation. On note

$$\phi \text{ WUntil } \psi := \neg(\neg\psi \text{ Until } (\neg\psi \wedge \neg\phi)),$$

pour *weak until*.

Notation. On note

$$\Diamond\,\phi := \text{True Until } \phi \qquad \Box\,\phi := \phi \text{ WUntil False},$$

et ont la même sémantique que pour LML.

Remarque 7.5. On peut montrer que le plus grand point fixe de $\theta(X) = \mathsf{a} \wedge \bigcirc\bigcirc X$ n'est pas définissable dans LTL.

7.2.2 Équivalences logiques pour LTL.

On note, comme avant, $\phi \equiv \psi$ si $[\![\phi]\!] = [\![\psi]\!]$. On a des lois, comme pour LML, *c.f.* figure 8 dans les notes de cours (section 7.3.3).

Exemple 7.4. On a

$$\Diamond \mathsf{False} \equiv \mathsf{False}$$
$$\Diamond(\phi \vee \psi) \equiv \Diamond\phi \vee \Diamond\psi$$
$$\Box \mathsf{True} \equiv \mathsf{True}$$
$$\Box(\phi \wedge \psi) \equiv \Box\phi \wedge \Box\psi$$
$$\bigcirc(\phi \ \mathsf{Until}\ \psi) \equiv \bigcirc\phi \ \mathsf{Until}\ \bigcirc\psi$$

Lemme 7.7. On a

1. $\neg(\phi \ \mathsf{WUntil}\ \psi) \equiv \neg\psi \ \mathsf{Until}\ (\neg\psi \wedge \neg\phi)$;
2. $\neg(\phi \ \mathsf{Until}\ \psi) \equiv \neg\psi \ \mathsf{WUntil}\ (\neg\psi \wedge \neg\phi)$.

QED

Lemme 7.8. On a

$$\phi \ \mathsf{WUntil}\ \psi \equiv (\phi \ \mathsf{Until}\ \psi) \vee \Box\phi.$$

Preuve. Soit $P = [\![(\phi \ \mathsf{Until}\ \psi) \vee \Box\phi]\!]$. On va montrer que $P = \nu\big([\![\theta]\!](X)\big)$ où $\theta = \psi \vee (\phi \wedge \bigcirc X)$. On a que $P = [\![\theta]\!](P)$ (c'est « facile »). Soit Q tel que $Q = [\![\theta]\!](Q)$ et on va montrer que $Q \subseteq P$. Soit $\sigma \in Q$.

- ▷ Si $\sigma \in [\![\Box\phi]\!]$ alors $\sigma \in P$ par définition de P.

▷ Sinon soit i le plus petit tel que $\sigma \upharpoonright i \notin [\![\phi]\!]$. Ainsi, par définition, $\sigma \upharpoonright j \in \phi$ pour $j < i$. On montre qu'il existe un certain $k \leq i$ tel que $\sigma \upharpoonright k \in [\![\psi]\!]$. Par l'absurde, supposons que $\sigma \upharpoonright k \notin [\![\psi]\!]$ pour tout $k \leq i$. On voit que pour tout $k < i$, on a $\sigma \upharpoonright k \in [\![\theta]\!](Q) = Q$ donc $\sigma \upharpoonright (i-1) \in [\![\theta]\!](Q) = Q$, et donc $\sigma \upharpoonright (i-1) \notin [\![\psi]\!]$, ce qui implique $\sigma \upharpoonright i \in Q$, ce qui contredit la définition de i (car $\sigma \upharpoonright i \notin [\![\psi]\!]$ et $\sigma \upharpoonright i \notin [\![\phi]\!]$).

QED