Linear Time Properties.

Definition 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 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.

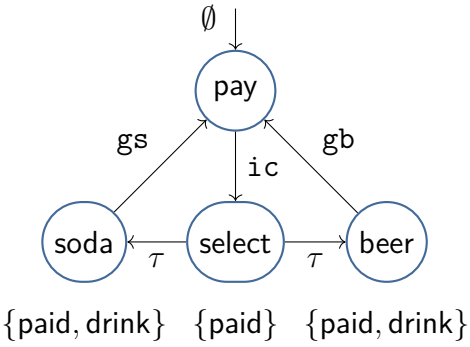

Figure 1 | *Transition system for the BVM with labels*

1 Linear-time properties.

Let AP be a set of *atomic propositions*.

Definition 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 1. For the Beverage vending machine (shown in figure 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 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. 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 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 5 (Satisfaction of a LT property)**.** We say that a transition system TS over AP *satisfies* a LT property P on AP, written $TS \models\!\!\approx P$, when $\mathrm{Tr}^\omega(TS) \subseteq P$.

Example 2. The BVM satisfies all the properties from example 1.

Example 3. We use a different transition system BVM′ to model the beverage vending machine, as seen in figure 2. The two transition systems are equivalent in the sense that:

$$\mathrm{Tr}^\omega(\mathrm{BVM}') = \mathrm{Tr}^\omega(\mathrm{BVM}),$$

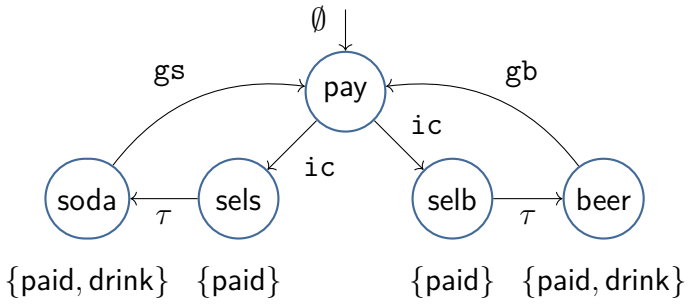

Figure 2 | *Transition system for the alternative BVM*

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

$$\mathrm{BVM}' \approx P \qquad \text{iff} \qquad \mathrm{BVM} \approx P.$$

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

Proposition 1. Given two transition systems TS_1 and TS_2 over AP, then the following are equivalent:

- $\mathrm{Tr}^{\omega}(TS_1) \subseteq \mathrm{Tr}^{\omega}(TS_2)$,
- $\forall P \subseteq (\mathbf{2}^{\mathrm{AP}})^{\omega}$, $TS_2 \approx P \implies TS_1 \approx P$.

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

2.1 Safety properties.

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

Definition 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 4. Considering the examples of LT-properties from example 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 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. An example of a safety property is

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

2.2 Safety properties and trace equivalences.

Example 6. Consider the transition system shown in figure 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 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 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 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.

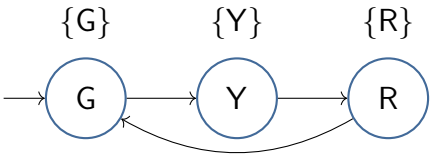

Figure 3 | *Transition system for the traffic light*

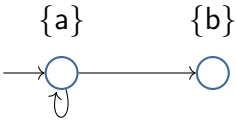

Figure 4 | *Another transition system*

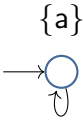

Figure 5 | *One-state transition system*

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

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

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

□

Example 7. Consider the transition system TS from figure 4 (example 6, which has a terminal state), and the transition system TS' from figure 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 8. Consider the transition system TS' shown in figure 7 (page 9) and TS the transition system shown in figure 6. The transition system TS' has terminal states and TS does not. However, we have that

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

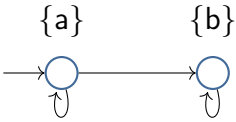

Figure 6 | *A transition system with no terminal state*

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 $L(\pi^n) = \sigma(0) \dots \sigma(n)$.

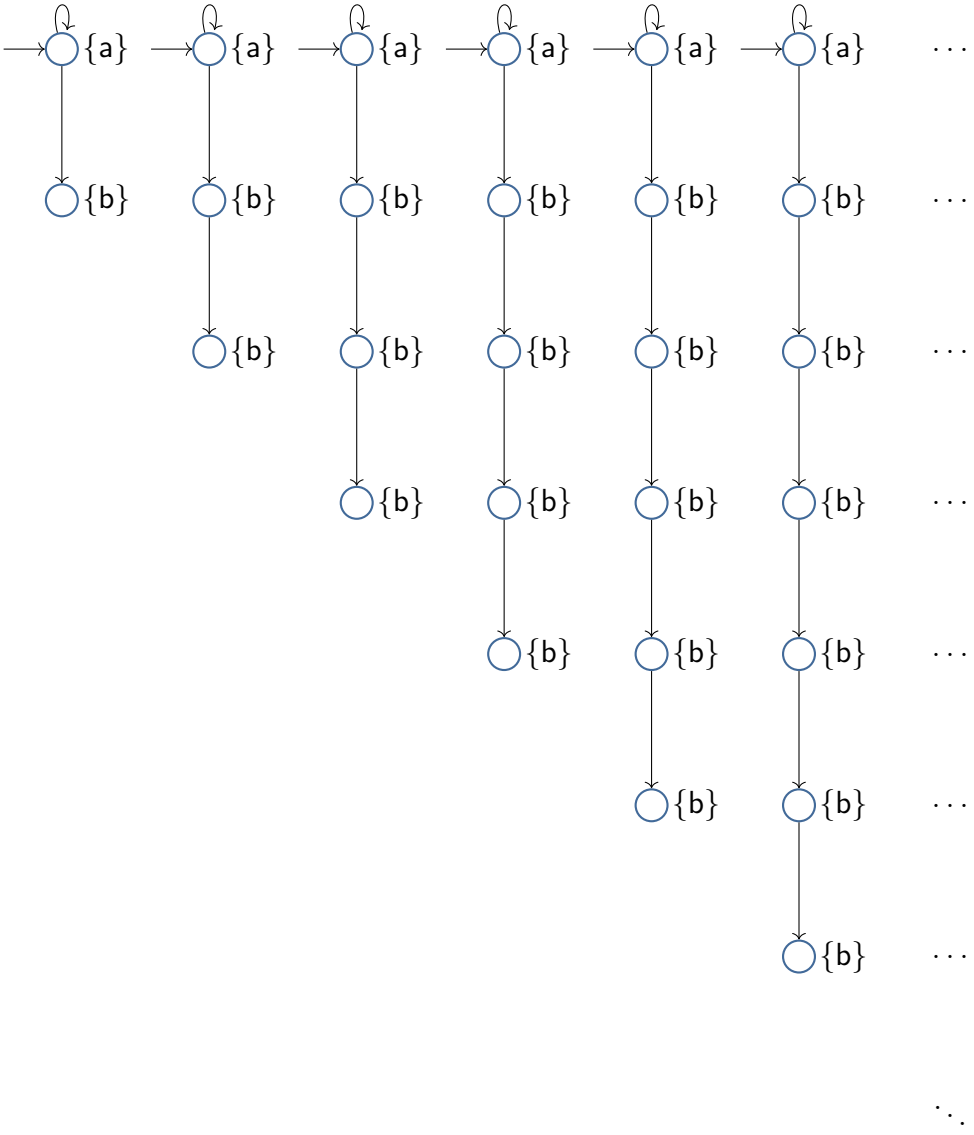

Figure 7 | *An infinite transition system*

Exemple 1. On considère TS comme celui représenté en figure 6 et TS' comme représenté en figure 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 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 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 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.

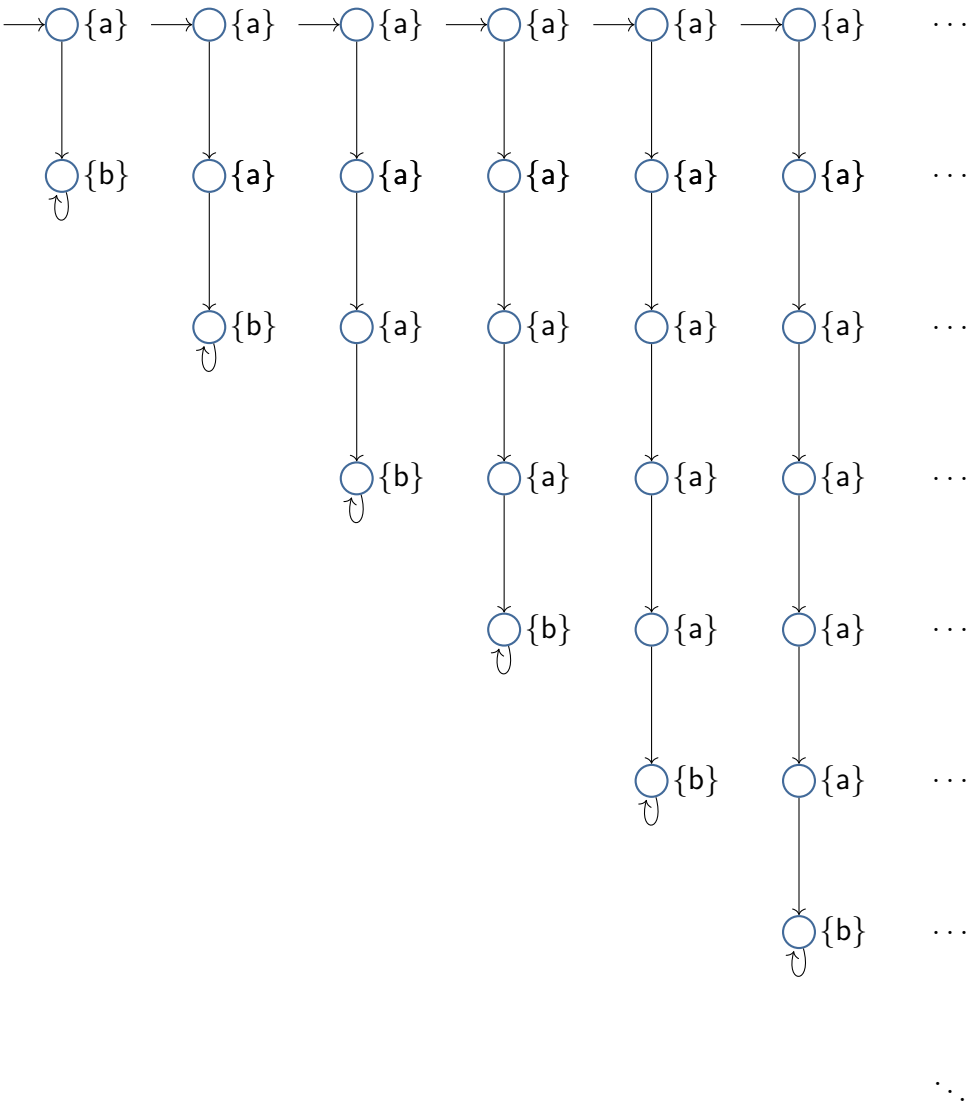

Fig. 8 | *Un système de transition infini*

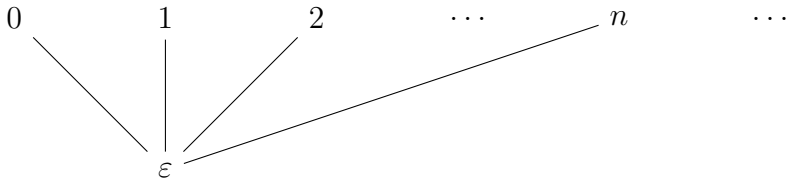

Fig. 9 | *Arbre* $\{\varepsilon\} \cup \mathbb{N}$ *sur* $\mathbb{N}$

Exemple 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 9).

Lemme 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 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 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 1. Si TS et TS' sont deux systèmes de transitions sans états terminaux et à branchement fini alors les deux propriétés suivantes sont équivalentes :

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

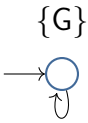

Fig. 10 | *Un feu tricolore un peu dangereux*

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

2.3 Propriétés de vivacité.

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

Exemple 3. Avec $\mathrm{AP} = \{\mathsf{G}, \mathsf{Y}, \mathsf{R}\}$ et TS défini comme en figure 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 (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 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 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 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 $P = \mathsf{True}$.

□