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 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 Linear-time properties.

Let AP be a set of *atomic propositions*.

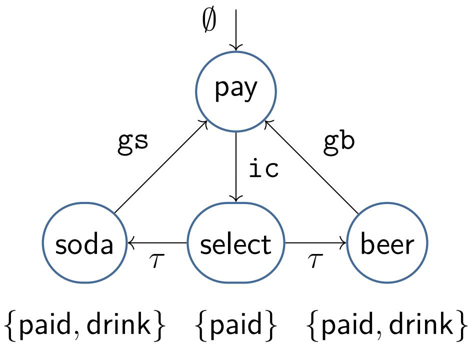

Figure 1 | *Transition system for the BVM with labels*

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:

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

Remark 2. The notations $\exists^\infty$ and $\forall^\infty$ are "infinitely many" and "ultimately all" quantifiers:

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

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 $TS \mathrel{|\!\!\approx} P$, 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:
$$\mathrm{Tr}^\omega(\mathrm{BVM}') = \mathrm{Tr}^\omega(\mathrm{BVM}),$$
so, for any LT Property $P \subseteq (\mathbf{2}^{\mathrm{AP}})^\omega$,
$$\mathrm{BVM}' \mathrel{|\!\!\approx} P \qquad \text{iff} \qquad \mathrm{BVM} \mathrel{|\!\!\approx} P.$$

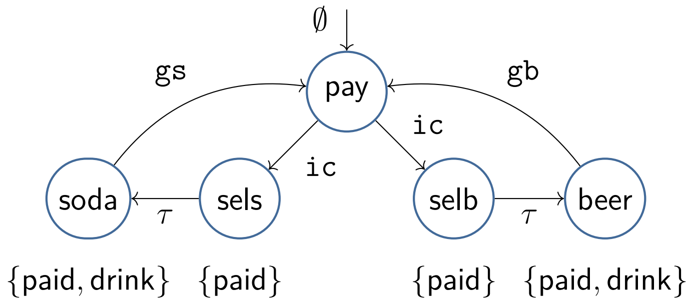

Figure 2 | *Transition system for the alternative BVM*

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:

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

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
$$P = P_{\text{safe}} \cap P_{\text{liveness}};$$
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 $P_{\text{bad}} \subseteq (\mathbf{2}^{\mathrm{AP}})^\star$ such that

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

Example 4. Considering the examples of LT-properties from example 1,

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

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

  where n is the length of $\hat{\sigma}$.
- Property (2) is a safety property: we can consider

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

- 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

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

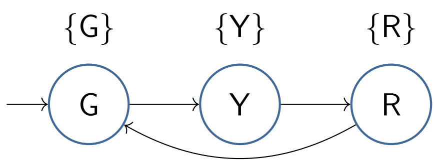

Figure 3 | *Transition system for the traffic light*

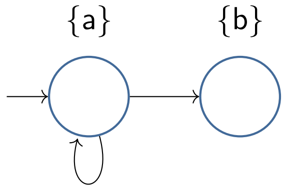

Figure 4 | *Transition system for the traffic light*

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: $TS \approx P$. This is true since $\operatorname{Tr}^\omega(TS) = \{\mathsf{a}\}^\omega$. However, when we consider *finite* (instead of infinites) traces, we have that $\operatorname{Tr}_{\text{fin}}(TS) \cap P_{\text{bad}} \neq \emptyset$.

Definition 7 (Terminal state). A state $s \in S$ of a transition system TS is *terminal* if

$$\forall s' \in S, \quad \forall \alpha \in \text{Act}, \quad s \overset{\alpha}{\nrightarrow} s'.$$

Proposition 2. Let TS be a transition system without terminal states, and a safety property P with the set of "bad behaviours" is written P_{bad}. Then,

$$TS \approx P \qquad \text{if and only if } \operatorname{Tr}_{\text{fin}}(TS) \cap P_{\text{bad}} = \emptyset.$$

Proof. See the course notes in section § 3.2.3. □

2.2 Safety properties and trace equivalences.

Lemma 1. Let TS and TS' be two transition systems over AP without terminal states. Then, the following are equivalent:

- ▷ $\operatorname{Tr}_{\text{fin}}(TS) \subseteq \operatorname{Tr}_{\text{fin}}(TS')$;
- ▷ for any safety property P, $TS' \approx P$ implies $TS \approx P$.

Proof.

- ▷ “ $\Longrightarrow$ ”. This is true by the last proposition.
- ▷ “ $\Longleftarrow$ ”. Let P be a safety property with

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

So, $TS' \models P$ hence $TS \models P$ by assumption. Therefore, $\operatorname{Tr}_{\text{fin}}(TS) \subseteq \operatorname{Tr}_{\text{fin}}(TS')$ by the last proposition.

□