CS 512, Spring 2018, Handout 04

Regular Safety Properties

Assaf Kfoury

30 January 2018 (Last modified: 1 February 2018)

safety properties in general (once more)

- LT property P over AP is a safety property if for every bad ω-trace $\sigma \in \left((2^{\mathsf{AP}})^{\omega} - P\right)$ there is a finite prefix σ' of σ such that:

$$P \cap \left\{ \sigma'' \in (2^{\mathsf{AP}})^{\omega} \;\middle|\; \sigma' \text{ is a prefix of } \sigma'' \right\} = \varnothing$$

i.e., every ω-extension σ'' of the prefix σ' is a bad ω-trace .

safety properties in general (once more)

- LT property P over AP is a safety property if for every bad ω-trace $\sigma \in \left((2^{\mathsf{AP}})^{\omega} - P\right)$ there is a finite prefix σ' of σ such that:

$$P \cap \left\{ \sigma'' \in (2^{\mathsf{AP}})^{\omega} \;\middle|\; \sigma' \text{ is a prefix of } \sigma'' \right\} = \varnothing$$

i.e., every ω-extension σ'' of the prefix σ' is a bad ω-trace .

- **Equivalently:** LT property P over AP is a safety property if there is a set of finite words $\mathsf{BadPref}(P) \subseteq (2^{\mathsf{AP}})^{*}$ such that:
    1. For every finite $\sigma \in \mathsf{BadPref}(P)$ and every infinite $\sigma' \in (2^{\mathsf{AP}})^{\omega}$, it holds that $\sigma\,\sigma'$ is a bad ω-trace , *i.e.*, $\sigma\,\sigma' \in \left((2^{\mathsf{AP}})^{\omega} - P\right)$.
    2. For every bad ω-trace $\sigma'' \in \left((2^{\mathsf{AP}})^{\omega} - P\right)$, there is a $\sigma \in \mathsf{BadPref}(P)$ such that σ is a prefix of σ''.

safety properties in general (once more)

- LT property P over AP is a safety property if for every bad ω-trace $\sigma \in \left((2^{\mathsf{AP}})^{\omega} - P\right)$ there is a finite prefix σ' of σ such that:

$$P \cap \left\{ \sigma'' \in (2^{\mathsf{AP}})^{\omega} \;\middle|\; \sigma' \text{ is a prefix of } \sigma'' \right\} = \varnothing$$

i.e., every ω-extension σ'' of the prefix σ' is a bad ω-trace .

- **Equivalently:** LT property P over AP is a safety property if there is a set of finite words $\mathsf{BadPref}(P) \subseteq (2^{\mathsf{AP}})^*$ such that:
  1. For every finite $\sigma \in \mathsf{BadPref}(P)$ and every infinite $\sigma' \in (2^{\mathsf{AP}})^{\omega}$, it holds that $\sigma\,\sigma'$ is a bad ω-trace , *i.e.*, $\sigma\,\sigma' \in \left((2^{\mathsf{AP}})^{\omega} - P\right)$.
  2. For every bad ω-trace $\sigma'' \in \left((2^{\mathsf{AP}})^{\omega} - P\right)$, there is a $\sigma \in \mathsf{BadPref}(P)$ such that σ is a prefix of σ''.

- Instead of $\mathsf{BadPref}(P)$ (not unique) use $\mathsf{MinBadPref}(P)$ (uniquely defined).
(See [PMC, Definition3.22, page 112] for how to pass from $\mathsf{BadPref}(P)$ to $\mathsf{MinBadPref}(P)$.)

More on the preceding in the handout "*Properties of Transition Systems*" click here and in the book [PMC].

regular safety properties

- **Definition:** safety property P over AP is a regular safety property iff a set $\mathsf{BadPref}(P)$ of bad prefixes is a regular language over 2^{AP}.

- **Fact:** safety property P over AP is a regular safety property $\Leftrightarrow$ the set $\mathsf{MinBadPref}(P)$ of minimal bad prefixes is a regular language over 2^{AP} [PMC, Lemma 4.12, page 161].

- **Fact:** every invariant property P over AP is a regular safety property [PMC, page 159-160].

- **Fact:** not every LT safety property P over AP is regular [PMC, Example 4.15, page 163].

- **Fact:** verifying whether transition system TS satisfies regular safety property P, *i.e.*, TS $\models P$, can be reduced to a reachability problem in the product TS $\otimes \mathscr{A}$ where $\mathscr{A}$ is an appropriately defined NFA $\mathscr{A}$ from $\mathsf{MinBadPref}(P)$. [PMC, Definition 4.16, page 165, Theorem 4.19, page 167].

(THIS PAGE INTENTIONALLY LEFT BLANK)