Overview

Safety properties

state that "nothing bad will happen"

Safety properties

state that "nothing bad will happen"

invariants:

- mutual exclusion: *never* $\mathit{crit}_1 \wedge \mathit{crit}_2$
- deadlock freedom: *never* $\bigwedge_{0 \le i < n} \mathit{wait}_i$

---

other safety properties:

- German traffic lights:
  every red phase is preceded by a yellow phase
- beverage machine:
  the total number of entered coins is never less than the total number of released drinks

Safety properties

state that "nothing bad will happen"

invariants: ⟵ "no **bad state** will be reached"

- mutual exclusion: *never* $\mathit{crit}_1 \wedge \mathit{crit}_2$
- deadlock freedom: *never* $\bigwedge_{0 \le i < n} \mathit{wait}_i$

---

other safety properties:

- German traffic lights:
  every red phase is preceded by a yellow phase
- beverage machine:
  the total number of entered coins is never less than the total number of released drinks

Safety properties

state that "nothing bad will happen"

invariants: ⟵ "no **bad state** will be reached"

- mutual exclusion: *never* $\mathit{crit}_1 \wedge \mathit{crit}_2$
- deadlock freedom: *never* $\bigwedge_{0 \leq i < n} \mathit{wait}_i$

---

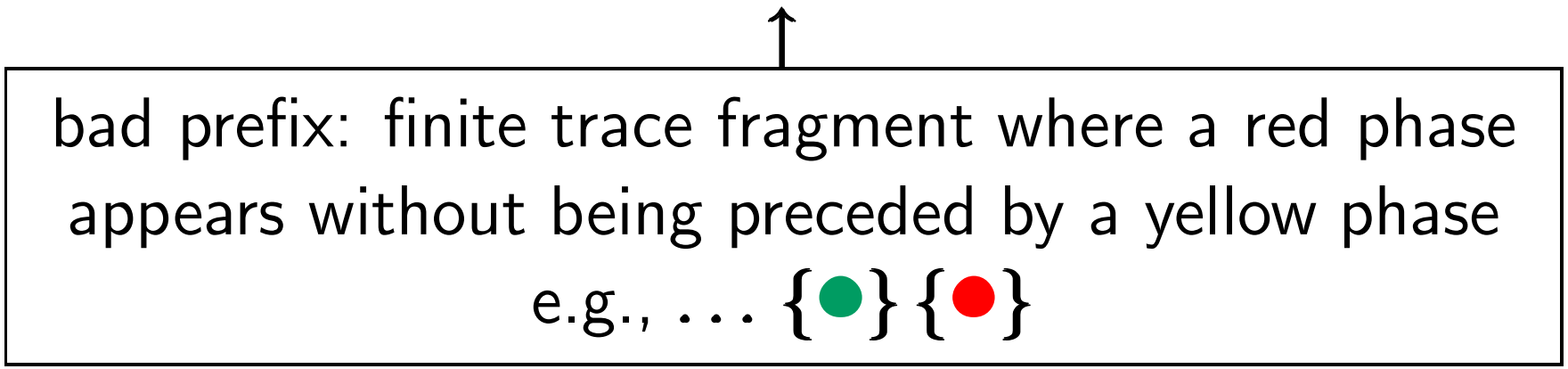
other safety properties: ⟵ "no **bad prefix**"

- German traffic lights:
  every red phase is preceded by a yellow phase
- beverage machine:
  the total number of entered coins is never less than the total number of released drinks

Bad prefixes of safety properties

- traffic lights:

every red phase is preceded by a yellow phase



Bad prefixes of safety properties

- traffic lights:

  every red phase is preceded by a yellow phase

  ↑

  bad prefix: finite trace fragment where a red phase appears without being preceded by a yellow phase

  e.g., ... {●} {●}

- beverage machine:

  the total number of entered coins is never less than the total number of released drinks

  ↑

  bad prefix, e.g., {*pay*} {*drink*} {*drink*}

Definition of safety properties

Let E be a LT property over AP, i.e., $E \subseteq (2^{AP})^{\omega}$.

Definition of safety properties

Let E be a LT property over AP, i.e., $E \subseteq (2^{AP})^\omega$.

E is called a safety property if for all words

$$\sigma = A_0 A_1 A_2 \ldots \in (2^{AP})^\omega \setminus E$$

there exists a finite prefix $A_0 A_1 \ldots A_n$ of σ such that *none* of the words $A_0 A_1 \ldots A_n B_{n+1} B_{n+2} B_{n+3} \ldots$ belongs to E, i.e.,

$$E \cap \{\sigma' \in (2^{AP})^\omega : A_0 \ldots A_n \text{ is a prefix of } \sigma'\} = \varnothing$$

Definition of safety properties

Let E be a LT property over AP, i.e., $E \subseteq (2^{AP})^\omega$.

E is called a safety property if for all words

$$\sigma = A_0 A_1 A_2 \ldots \in (2^{AP})^\omega \setminus E$$

there exists a finite prefix $A_0 A_1 \ldots A_n$ of σ such that *none* of the words $A_0 A_1 \ldots A_n B_{n+1} B_{n+2} B_{n+3} \ldots$ belongs to E, i.e.,

$$E \cap \{\sigma' \in (2^{AP})^\omega : A_0 \ldots A_n \text{ is a prefix of } \sigma'\} = \varnothing$$

Such words $A_0 A_1 \ldots A_n$ are called bad prefixes for E.

Definition of safety properties

Let E be a LT property over AP, i.e., $E \subseteq (2^{AP})^\omega$.

E is called a safety property if for all words

$$\sigma = A_0 A_1 A_2 \ldots \in (2^{AP})^\omega \setminus E$$

there exists a finite prefix $A_0 A_1 \ldots A_n$ of σ such that *none* of the words $A_0 A_1 \ldots A_n B_{n+1} B_{n+2} B_{n+3} \ldots$ belongs to E, i.e.,

$$E \cap \{\sigma' \in (2^{AP})^\omega : A_0 \ldots A_n \text{ is a prefix of } \sigma'\} = \varnothing$$

Such words $A_0 A_1 \ldots A_n$ are called bad prefixes for E.

$E =$ set of all infinite words that do *not* have a bad prefix

Definition of safety properties

Let E be a LT property over AP, i.e., $E \subseteq (2^{AP})^\omega$.

E is called a safety property if for all words

$$\sigma = A_0 A_1 A_2 \ldots \in (2^{AP})^\omega \setminus E$$

there exists a finite prefix $A_0 A_1 \ldots A_n$ of σ such that *none* of the words $A_0 A_1 \ldots A_n B_{n+1} B_{n+2} B_{n+3} \ldots$ belongs to E, i.e.,

$$E \cap \{\sigma' \in (2^{AP})^\omega : A_0 \ldots A_n \text{ is a prefix of } \sigma'\} = \varnothing$$

Such words $A_0 A_1 \ldots A_n$ are called bad prefixes for E.

$BadPref_E \stackrel{\text{def}}{=}$ set of bad prefixes for E

Definition of safety properties

Let E be a LT property over AP, i.e., $E \subseteq (2^{AP})^\omega$.

E is called a safety property if for all words

$$\sigma = A_0 A_1 A_2 \ldots \in (2^{AP})^\omega \setminus E$$

there exists a finite prefix $A_0 A_1 \ldots A_n$ of σ such that *none* of the words $A_0 A_1 \ldots A_n B_{n+1} B_{n+2} B_{n+3} \ldots$ belongs to E, i.e.,

$$E \cap \{\sigma' \in (2^{AP})^\omega : A_0 \ldots A_n \text{ is a prefix of } \sigma'\} = \varnothing$$

Such words $A_0 A_1 \ldots A_n$ are called bad prefixes for E.

$$BadPref_E \stackrel{\text{def}}{=} \text{set of bad prefixes for } E \subseteq (2^{AP})^+$$

Definition of safety properties

Let E be a LT property over AP, i.e., $E \subseteq (2^{AP})^\omega$.

E is called a safety property if for all words

$$\sigma = A_0 A_1 A_2 \ldots \in (2^{AP})^\omega \setminus E$$

there exists a finite prefix $A_0 A_1 \ldots A_n$ of σ such that *none* of the words $A_0 A_1 \ldots A_n B_{n+1} B_{n+2} B_{n+3} \ldots$ belongs to E, i.e.,

$$E \cap \{\sigma' \in (2^{AP})^\omega : A_0 \ldots A_n \text{ is a prefix of } \sigma'\} = \varnothing$$

Such words $A_0 A_1 \ldots A_n$ are called bad prefixes for E.

$BadPref_E \stackrel{\text{def}}{=}$ set of bad prefixes for $E \subseteq (2^{AP})^+$

↑

briefly: $BadPref$

Definition of safety properties

Let E be a LT property over AP, i.e., $E \subseteq (2^{AP})^\omega$.

E is called a safety property if for all words

$$\sigma = A_0 A_1 A_2 \ldots \in (2^{AP})^\omega \setminus E$$

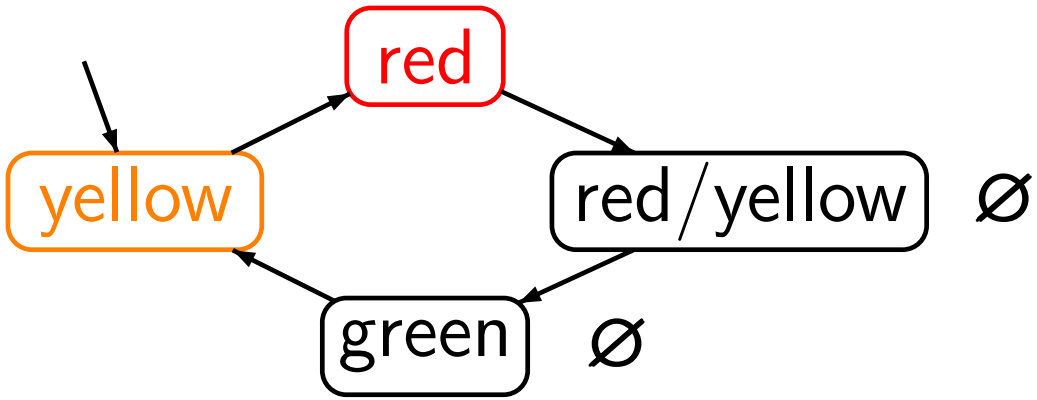
there exists a finite prefix $A_0 A_1 \ldots A_n$ of σ such that *none* of the words $A_0 A_1 \ldots A_n B_{n+1} B_{n+2} B_{n+3} \ldots$ belongs to E, i.e.,

$$E \cap \{\sigma' \in (2^{AP})^\omega : A_0 \ldots A_n \text{ is a prefix of } \sigma'\} = \varnothing$$

Such words $A_0 A_1 \ldots A_n$ are called bad prefixes for E.

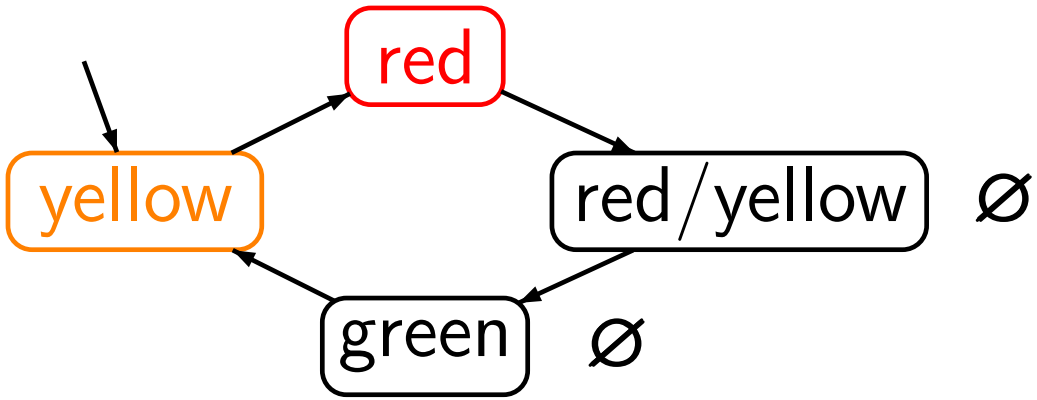
minimal bad prefixes: any word $A_0 \ldots A_i \ldots A_n \in BadPref$ s.t. no proper prefix $A_0 \ldots A_i$ is a bad prefix for E

Safety property for a traffic light



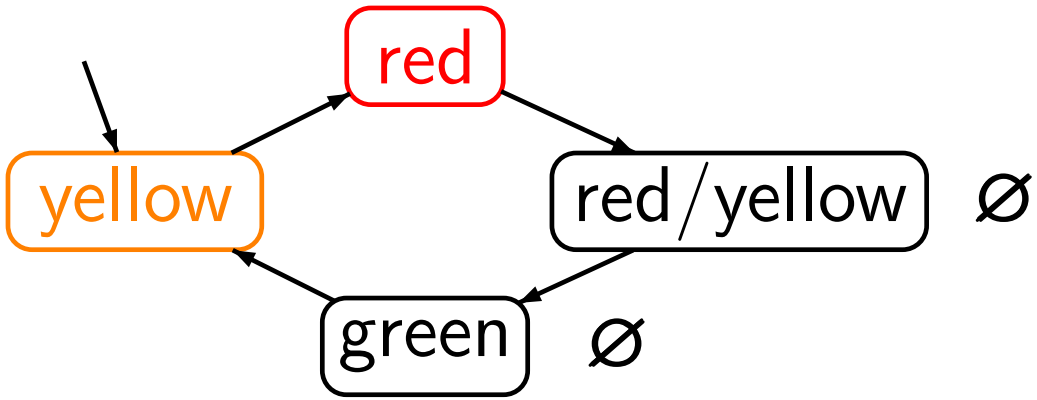
$AP = \{red, yellow\}$

Safety property for a traffic light



"every red phase is preceded by a yellow phase"

Safety property for a traffic light



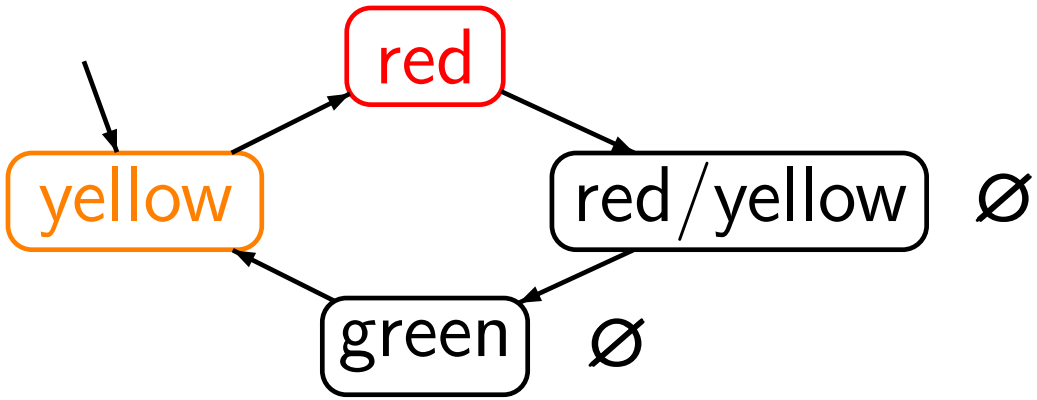
"every red phase is preceded by a yellow phase"

hence: $\mathcal{T} \models E$

E = set of all infinite words $A_0 A_1 A_2 \ldots$ over 2^{AP} such that for all $i \in \mathbb{N}$:

$$\mathit{red} \in A_i \implies i \geq 1 \text{ and } \mathit{yellow} \in A_{i-1}$$

Safety property for a traffic light

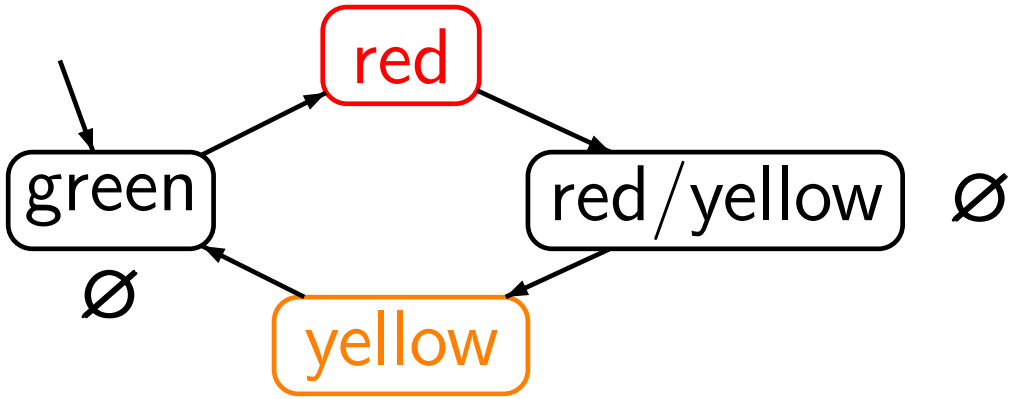


"every red phase is preceded by a yellow phase"

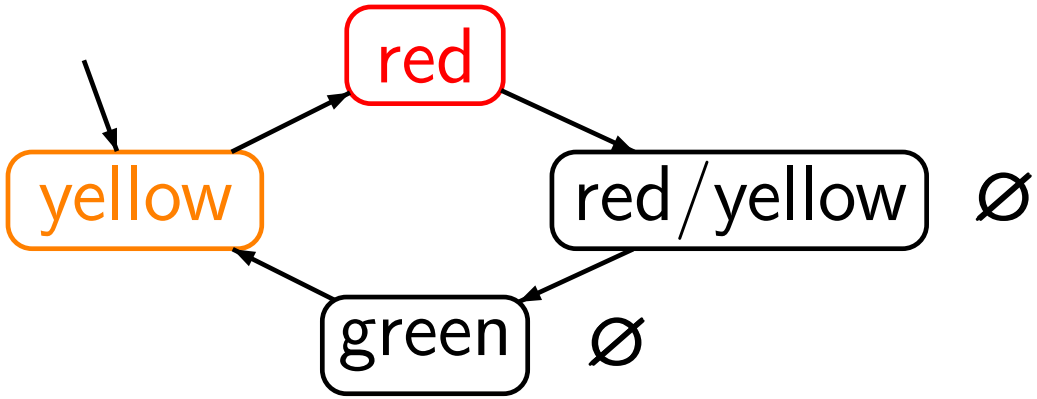
hence: $\mathcal{T} \models E$

E = set of all infinite words $A_0 A_1 A_2 \ldots$ over 2^{AP} such that for all $i \in \mathbb{N}$:

$$\mathit{red} \in A_i \implies i \geq 1 \text{ and } \mathit{yellow} \in A_{i-1}$$



Safety property for a traffic light

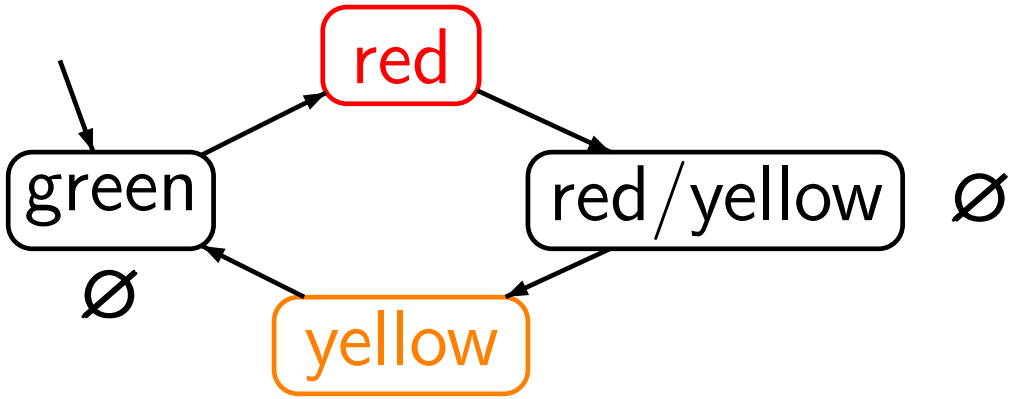


"every red phase is preceded by a yellow phase"

hence: $\mathcal{T} \models E$

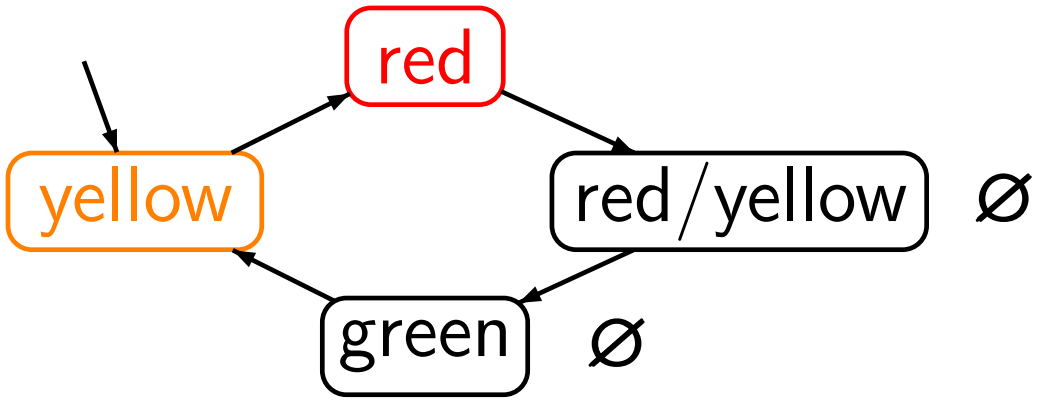
E = set of all infinite words $A_0 A_1 A_2 \ldots$ over 2^{AP} such that for all $i \in \mathbb{N}$:

$$\mathit{red} \in A_i \implies i \geq 1 \text{ and } \mathit{yellow} \in A_{i-1}$$



"there is a red phase that is not preceded by a yellow phase"

Safety property for a traffic light

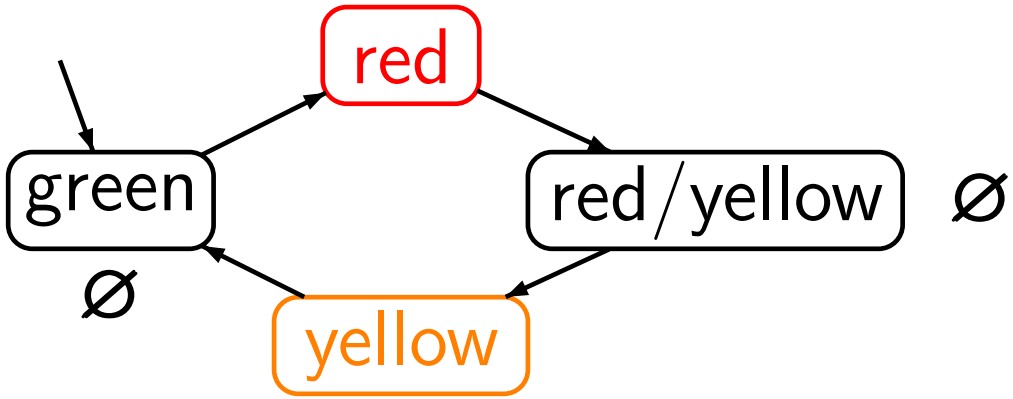


"every red phase is preceded by a yellow phase"

hence: $\mathcal{T} \models E$

E = set of all infinite words $A_0 A_1 A_2 \ldots$ over 2^{AP} such that for all $i \in \mathbb{N}$:

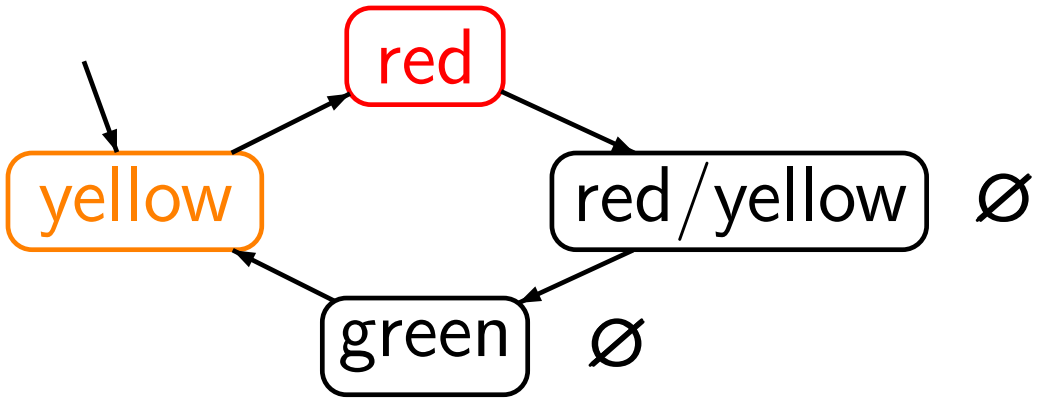
$$\mathit{red} \in A_i \implies i \geq 1 \text{ and } \mathit{yellow} \in A_{i-1}$$



"there is a red phase that is not preceded by a yellow phase"

hence: $\mathcal{T} \not\models E$

Safety property for a traffic light

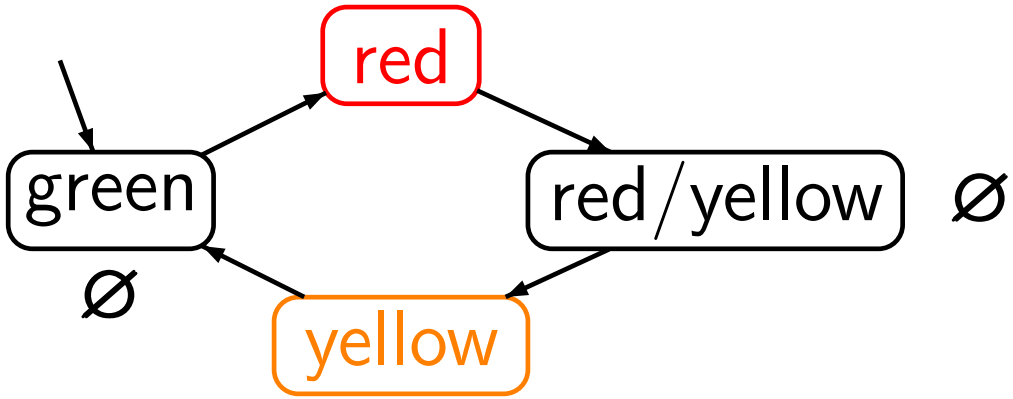


"every red phase is preceded by a yellow phase"

hence: $\mathcal{T} \models E$

E = set of all infinite words $A_0 A_1 A_2 \ldots$ over 2^{AP} such that for all $i \in \mathbb{N}$:

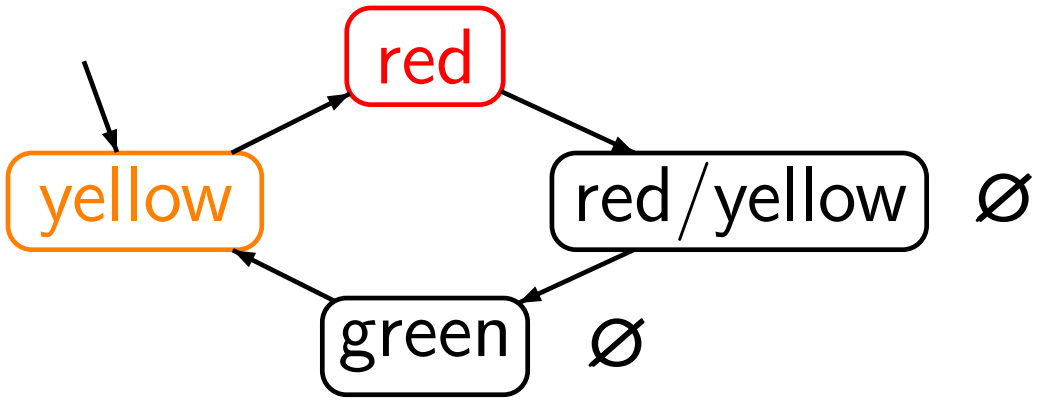
$$\mathit{red} \in A_i \implies i \geq 1 \text{ and } \mathit{yellow} \in A_{i-1}$$



$\mathcal{T} \not\models E$

bad prefix, e.g., $\varnothing \{\mathit{red}\} \varnothing \{\mathit{yellow}\}$

Safety property for a traffic light

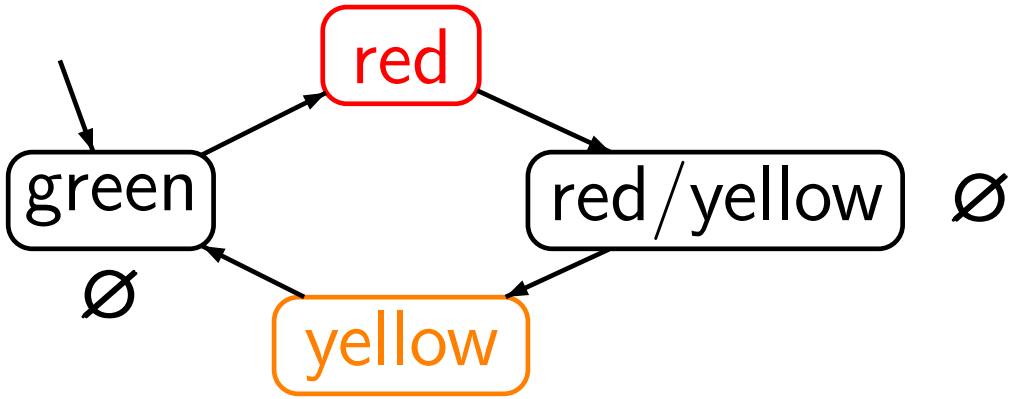


"every red phase is preceded by a yellow phase"

hence: $\mathcal{T} \models E$

E = set of all infinite words $A_0 A_1 A_2 \ldots$ over 2^{AP} such that for all $i \in \mathbb{N}$:

$$\mathit{red} \in A_i \implies i \geq 1 \text{ and } \mathit{yellow} \in A_{i-1}$$

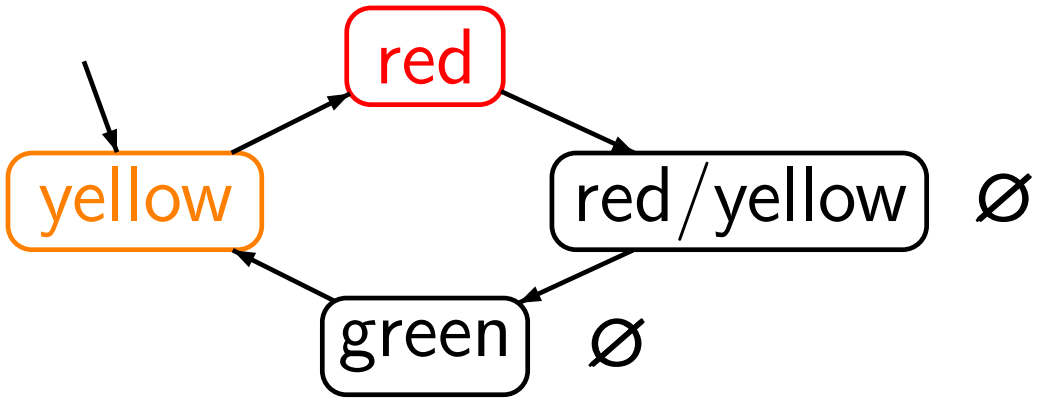


$\mathcal{T} \not\models E$

minimal bad prefix:

$\varnothing\,\{\mathit{red}\}$

Safety property for a traffic light



"every red phase is preceded by a yellow phase"

hence: $\mathcal{T} \models E$

E = set of all infinite words $A_0 A_1 A_2 \ldots$ over 2^{AP} such that for all $i \in \mathbb{N}$:

$$\mathit{red} \in A_i \implies i \geq 1 \text{ and } \mathit{yellow} \in A_{i-1}$$

is a safety property over $AP = \{\mathit{red}, \mathit{yellow}\}$ with

$\mathit{BadPref}$ = set of all finite words $A_0 A_1 \ldots A_n$ over 2^{AP} s.t. for some $i \in \{0, \ldots, n\}$:

$$\mathit{red} \in A_i \wedge (i{=}0 \vee \mathit{yellow} \notin A_{i-1})$$

Satisfaction of safety properties

Satisfaction of safety properties

Let $E \subseteq (2^{AP})^{\omega}$ be a safety property, $\mathcal{T}$ a TS over AP.

$$\mathcal{T} \models E \quad \text{iff} \quad \mathit{Traces}(\mathcal{T}) \subseteq E$$

$\mathit{Traces}(\mathcal{T})$ = set of traces of $\mathcal{T}$

Satisfaction of safety properties

Let $E \subseteq (2^{AP})^\omega$ be a safety property, $\mathcal{T}$ a TS over AP.

$$\mathcal{T} \models E \quad \text{iff} \quad Traces(\mathcal{T}) \subseteq E$$
$$\text{iff} \quad Traces_{fin}(\mathcal{T}) \cap BadPref = \varnothing$$

$BadPref$ = set of all bad prefixes of E

$Traces(\mathcal{T})$ = set of traces of $\mathcal{T}$

$Traces_{fin}(\mathcal{T})$ = set of finite traces of $\mathcal{T}$

$= \{ trace(\hat{\pi}) : \hat{\pi}$ is an initial, finite path fragment of $\mathcal{T} \}$

Satisfaction of safety properties

Let $E \subseteq (2^{AP})^\omega$ be a safety property, $\mathcal{T}$ a TS over AP.

$$
\begin{aligned}
\mathcal{T} \models E \quad &\text{iff} \quad Traces(\mathcal{T}) \subseteq E \\
&\text{iff} \quad Traces_{fin}(\mathcal{T}) \cap BadPref = \varnothing \\
&\text{iff} \quad Traces_{fin}(\mathcal{T}) \cap MinBadPref = \varnothing
\end{aligned}
$$

$BadPref$ = set of all bad prefixes of E

$MinBadPref$ = set of all minimal bad prefixes of E

$Traces(\mathcal{T})$ = set of traces of $\mathcal{T}$

$Traces_{fin}(\mathcal{T})$ = set of finite traces of $\mathcal{T}$

$= \{ trace(\hat{\pi}) : \hat{\pi}$ is an initial, finite path fragment of $\mathcal{T} \}$

Correct or wrong?

Every invariant is a safety property.

Correct or wrong?

> Every invariant is a safety property.

correct.

Correct or wrong?

> Every invariant is a safety property.

correct.

Let E be an invariant with invariant condition Φ.

Correct or wrong?

> Every invariant is a safety property.

correct.

Let E be an invariant with invariant condition Φ.

- bad prefixes for E: finite words $A_0 \ldots A_i \ldots A_n$ s.t.

$$A_i \not\models \Phi \text{ for some } i \in \{0, 1, \ldots, n\}$$

Correct or wrong?

Every invariant is a safety property.

correct.

Let E be an invariant with invariant condition Φ.

- bad prefixes for E: finite words $A_0 \ldots A_i \ldots A_n$ s.t.
$$A_i \not\models \Phi \text{ for some } i \in \{0, 1, \ldots, n\}$$
- minimal bad prefixes for E:
finite words $A_0\, A_1 \ldots A_{n-1}\, A_n$ such that
$$A_i \models \Phi \text{ for } i = 0, 1, \ldots, n-1, \text{ and } A_n \not\models \Phi$$

Correct or wrong?

$\varnothing$ is a safety property

Correct or wrong?

$\varnothing$ is a safety property

correct

Correct or wrong?

$\varnothing$ is a safety property

correct

- all finite words $A_0 \dots A_n \in (2^{AP})^+$ are bad prefixes

Correct or wrong?

$\varnothing$ is a safety property

correct

- all finite words $A_0 \dots A_n \in (2^{AP})^+$ are bad prefixes
- $\varnothing$ is even an invariant (invariant condition ***false***)

Correct or wrong?

$\varnothing$ is a safety property

correct

- all finite words $A_0 \dots A_n \in (2^{AP})^+$ are bad prefixes
- $\varnothing$ is even an invariant (invariant condition ***false***)

$(2^{AP})^\omega$ is a safety property

Correct or wrong?

$\varnothing$ is a safety property

correct

- all finite words $A_0 \dots A_n \in (2^{AP})^+$ are bad prefixes
- $\varnothing$ is even an invariant (invariant condition ***false***)

$(2^{AP})^\omega$ is a safety property

correct

Correct or wrong?

$\varnothing$ is a safety property

correct

- all finite words $A_0 \dots A_n \in (2^{AP})^+$ are bad prefixes
- $\varnothing$ is even an invariant (invariant condition ***false***)

$(2^{AP})^\omega$ is a safety property

correct

"For all words $\in \underbrace{(2^{AP})^\omega \setminus (2^{AP})^\omega}_{=\varnothing}$ ..."

Prefix closure

Prefix closure

For a given infinite word $\sigma = A_0 A_1 A_2 \ldots$, let

$$\begin{aligned} \mathit{pref}(\sigma) &\stackrel{\text{def}}{=} \text{set of all nonempty, finite prefixes of } \sigma \\ &= \left\{ A_0 A_1 \ldots A_n : n \geq 0 \right\} \end{aligned}$$

Prefix closure

For a given infinite word $\sigma = A_0 A_1 A_2 \ldots$, let

$$pref(\sigma) \stackrel{\text{def}}{=} \text{set of all nonempty, finite prefixes of } \sigma$$

$$= \{ A_0 A_1 \ldots A_n : n \geq 0 \}$$

For $E \subseteq (2^{AP})^\omega$, let $pref(E) \stackrel{\text{def}}{=} \bigcup_{\sigma \in E} pref(\sigma)$

Prefix closure

For a given infinite word $\sigma = A_0 A_1 A_2 \ldots$, let

$$pref(\sigma) \stackrel{\text{def}}{=} \text{set of all nonempty, finite prefixes of } \sigma$$

$$= \{ A_0 A_1 \ldots A_n : n \geq 0 \}$$

For $E \subseteq (2^{AP})^\omega$, let $pref(E) \stackrel{\text{def}}{=} \bigcup_{\sigma \in E} pref(\sigma)$

Given an LT property E, the prefix closure of E is:

$$cl(E) \stackrel{\text{def}}{=} \{\sigma \in (2^{AP})^\omega : pref(\sigma) \subseteq pref(E)\}$$

Prefix closure and safety

For any infinite word $\sigma \in (2^{AP})^\omega$, let

$$pref(\sigma) \quad = \quad \text{set of all nonempty, finite prefixes of } \sigma$$

For any LT property $E \subseteq (2^{AP})^\omega$, let

$$pref(E) \quad = \quad \bigcup_{\sigma \in E} pref(\sigma) \text{ and}$$

$$cl(E) \quad = \quad \{\sigma \in (2^{AP})^\omega : pref(\sigma) \subseteq pref(E)\}$$

Prefix closure and safety

For any infinite word $\sigma \in (2^{AP})^\omega$, let

$$pref(\sigma) \quad = \quad \text{set of all nonempty, finite prefixes of } \sigma$$

For any LT property $E \subseteq (2^{AP})^\omega$, let

$$pref(E) \quad = \quad \bigcup_{\sigma \in E} pref(\sigma) \text{ and}$$

$$cl(E) \quad = \quad \{\sigma \in (2^{AP})^\omega : pref(\sigma) \subseteq pref(E)\}$$

Theorem:

E is a safety property iff $cl(E) = E$

Safety and finite trace inclusion

remind: LT properties and trace inclusion:

If $\mathcal{T}_1$ and $\mathcal{T}_2$ are TS over AP then:

$$Traces(\mathcal{T}_1) \subseteq Traces(\mathcal{T}_2)$$

iff for all LT properties E: $\mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E$

Safety and finite trace inclusion

remind: LT properties and trace inclusion:

If $\mathcal{T}_1$ and $\mathcal{T}_2$ are TS over AP then:

$$Traces(\mathcal{T}_1) \subseteq Traces(\mathcal{T}_2)$$

iff for all LT properties E: $\mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E$

safety properties and finite trace inclusion:

If $\mathcal{T}_1$ and $\mathcal{T}_2$ are TS over AP then:

$$Traces_{fin}(\mathcal{T}_1) \subseteq Traces_{fin}(\mathcal{T}_2)$$

iff for all safety properties E: $\mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E$

Safety and finite trace inclusion

$$Traces_{fin}(\mathcal{T}_1) \subseteq Traces_{fin}(\mathcal{T}_2)$$

iff for all safety properties E: $\mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E$

Safety and finite trace inclusion

$$\mathit{Traces}_{\mathit{fin}}(\mathcal{T}_1) \subseteq \mathit{Traces}_{\mathit{fin}}(\mathcal{T}_2)$$

iff for all safety properties E: $\mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E$

Proof "$\Longrightarrow$": obvious, as for safety property E:

$$\mathcal{T} \models E \quad \text{iff} \quad \mathit{Traces}_{\mathit{fin}}(\mathcal{T}) \cap \mathit{BadPref} = \varnothing$$

Safety and finite trace inclusion

$$\mathit{Traces}_{\mathit{fin}}(\mathcal{T}_1) \subseteq \mathit{Traces}_{\mathit{fin}}(\mathcal{T}_2)$$

iff for all safety properties E: $\mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E$

Proof "$\Longrightarrow$": obvious, as for safety property E:

$$\mathcal{T} \models E \quad \text{iff} \quad \mathit{Traces}_{\mathit{fin}}(\mathcal{T}) \cap \mathit{BadPref} = \varnothing$$

Hence:

If $\mathcal{T}_2 \models E$ and $\mathit{Traces}_{\mathit{fin}}(\mathcal{T}_1) \subseteq \mathit{Traces}_{\mathit{fin}}(\mathcal{T}_2)$ then:

Safety and finite trace inclusion

$$Traces_{fin}(\mathcal{T}_1) \subseteq Traces_{fin}(\mathcal{T}_2)$$

iff for all safety properties E: $\mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E$

Proof "$\Longrightarrow$": obvious, as for safety property E:

$$\mathcal{T} \models E \quad \text{iff} \quad Traces_{fin}(\mathcal{T}) \cap BadPref = \varnothing$$

Hence:

If $\mathcal{T}_2 \models E$ and $Traces_{fin}(\mathcal{T}_1) \subseteq Traces_{fin}(\mathcal{T}_2)$ then:

$$Traces_{fin}(\mathcal{T}_1) \cap BadPref$$
$$\subseteq \; Traces_{fin}(\mathcal{T}_2) \cap BadPref = \varnothing$$

Safety and finite trace inclusion

$$\mathit{Traces}_{\mathit{fin}}(\mathcal{T}_1) \subseteq \mathit{Traces}_{\mathit{fin}}(\mathcal{T}_2)$$

iff for all safety properties E: $\mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E$

Proof "$\Longrightarrow$": obvious, as for safety property E:

$$\mathcal{T} \models E \quad \text{iff} \quad \mathit{Traces}_{\mathit{fin}}(\mathcal{T}) \cap \mathit{BadPref} = \varnothing$$

Hence:

If $\mathcal{T}_2 \models E$ and $\mathit{Traces}_{\mathit{fin}}(\mathcal{T}_1) \subseteq \mathit{Traces}_{\mathit{fin}}(\mathcal{T}_2)$ then:

$$\mathit{Traces}_{\mathit{fin}}(\mathcal{T}_1) \cap \mathit{BadPref}$$
$$\subseteq \mathit{Traces}_{\mathit{fin}}(\mathcal{T}_2) \cap \mathit{BadPref} = \varnothing$$

and therefore $\mathcal{T}_1 \models E$

Safety and finite trace inclusion

$$\mathit{Traces}_{\mathit{fin}}(\mathcal{T}_1) \subseteq \mathit{Traces}_{\mathit{fin}}(\mathcal{T}_2)$$

iff for all safety properties E: $\mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E$

Proof "$\Longleftarrow$": consider the LT property

$$E = \mathit{cl}(\mathit{Traces}(\mathcal{T}_2))$$

Safety and finite trace inclusion

$$Traces_{fin}(\mathcal{T}_1) \subseteq Traces_{fin}(\mathcal{T}_2)$$

iff for all safety properties E: $\mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E$

Proof "$\Longleftarrow$": consider the LT property

$$E = cl(Traces(\mathcal{T}_2)) = \{\sigma : pref(\sigma) \subseteq Traces_{fin}(\mathcal{T}_2)\}$$

Safety and finite trace inclusion

$$Traces_{fin}(\mathcal{T}_1) \subseteq Traces_{fin}(\mathcal{T}_2)$$

iff for all safety properties E: $\mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E$

Proof "$\Longleftarrow$": consider the LT property

$$E = cl(Traces(\mathcal{T}_2)) = \{\sigma : pref(\sigma) \subseteq Traces_{fin}(\mathcal{T}_2)\}$$

↑

for each transition system $\mathcal{T}$:

$$pref\big(Traces(\mathcal{T})\big) = Traces_{fin}(\mathcal{T})$$

Safety and finite trace inclusion

$$Traces_{fin}(\mathcal{T}_1) \subseteq Traces_{fin}(\mathcal{T}_2)$$

iff for all safety properties E: $\mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E$

Proof "$\Longleftarrow$": consider the LT property

$$E = cl(Traces(\mathcal{T}_2)) = \{\sigma : pref(\sigma) \subseteq Traces_{fin}(\mathcal{T}_2)\}$$

Then, E is a safety property

Safety and finite trace inclusion

$$Traces_{fin}(\mathcal{T}_1) \subseteq Traces_{fin}(\mathcal{T}_2)$$

iff for all safety properties E: $\mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E$

Proof "$\Longleftarrow$": consider the LT property

$$E = cl(Traces(\mathcal{T}_2)) = \{\sigma : pref(\sigma) \subseteq Traces_{fin}(\mathcal{T}_2)\}$$

Then, E is a safety property

$\uparrow$

as $cl(E) = E$

Safety and finite trace inclusion

$$Traces_{fin}(\mathcal{T}_1) \subseteq Traces_{fin}(\mathcal{T}_2)$$

iff for all safety properties E: $\mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E$

Proof "$\Longleftarrow$": consider the LT property

$$E = cl(Traces(\mathcal{T}_2)) = \{\sigma : pref(\sigma) \subseteq Traces_{fin}(\mathcal{T}_2)\}$$

Then, E is a safety property

↑

as $cl(E) = E$

set of bad prefixes: $(2^{AP})^+ \setminus Traces_{fin}(\mathcal{T}_2)$

Safety and finite trace inclusion

$$Traces_{fin}(\mathcal{T}_1) \subseteq Traces_{fin}(\mathcal{T}_2)$$

iff for all safety properties E: $\mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E$

Proof "$\Longleftarrow$": consider the LT property

$$E = cl(Traces(\mathcal{T}_2)) = \{\sigma : pref(\sigma) \subseteq Traces_{fin}(\mathcal{T}_2)\}$$

Then, E is a safety property and $\mathcal{T}_2 \models E$.

Safety and finite trace inclusion

$$Traces_{fin}(\mathcal{T}_1) \subseteq Traces_{fin}(\mathcal{T}_2)$$

iff for all safety properties E: $\mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E$

Proof "$\Longleftarrow$": consider the LT property

$$E = cl(Traces(\mathcal{T}_2)) = \{\sigma : pref(\sigma) \subseteq Traces_{fin}(\mathcal{T}_2)\}$$

Then, E is a safety property and $\mathcal{T}_2 \models E$.

By assumption: $\mathcal{T}_1 \models E$

Safety and finite trace inclusion

$$Traces_{fin}(\mathcal{T}_1) \subseteq Traces_{fin}(\mathcal{T}_2)$$

iff for all safety properties E: $\mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E$

Proof "$\Longleftarrow$": consider the LT property

$$E = cl(Traces(\mathcal{T}_2)) = \{\sigma : pref(\sigma) \subseteq Traces_{fin}(\mathcal{T}_2)\}$$

Then, E is a safety property and $\mathcal{T}_2 \models E$.

By assumption: $\mathcal{T}_1 \models E$ and therefore $Traces(\mathcal{T}_1) \subseteq E$.

Safety and finite trace inclusion

$$Traces_{fin}(\mathcal{T}_1) \subseteq Traces_{fin}(\mathcal{T}_2)$$

iff for all safety properties E: $\mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E$

Proof "$\Longleftarrow$": consider the LT property

$$E = cl(Traces(\mathcal{T}_2)) = \{\sigma : pref(\sigma) \subseteq Traces_{fin}(\mathcal{T}_2)\}$$

Then, E is a safety property and $\mathcal{T}_2 \models E$.

By assumption: $\mathcal{T}_1 \models E$ and therefore $Traces(\mathcal{T}_1) \subseteq E$.

Hence: $Traces_{fin}(\mathcal{T}_1) = pref(Traces(\mathcal{T}_1))$

Safety and finite trace inclusion

$$Traces_{fin}(\mathcal{T}_1) \subseteq Traces_{fin}(\mathcal{T}_2)$$

iff for all safety properties E: $\mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E$

Proof "$\Longleftarrow$": consider the LT property

$$E = cl(Traces(\mathcal{T}_2)) = \{\sigma : pref(\sigma) \subseteq Traces_{fin}(\mathcal{T}_2)\}$$

Then, E is a safety property and $\mathcal{T}_2 \models E$.

By assumption: $\mathcal{T}_1 \models E$ and therefore $Traces(\mathcal{T}_1) \subseteq E$.

Hence: $Traces_{fin}(\mathcal{T}_1) = pref(Traces(\mathcal{T}_1))$

$$\subseteq pref(E)$$

Safety and finite trace inclusion

$$\mathit{Traces}_{\mathit{fin}}(\mathcal{T}_1) \subseteq \mathit{Traces}_{\mathit{fin}}(\mathcal{T}_2)$$

iff for all safety properties E: $\mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E$

Proof "$\Longleftarrow$": consider the LT property

$$E = \mathit{cl}(\mathit{Traces}(\mathcal{T}_2)) = \{\sigma : \mathit{pref}(\sigma) \subseteq \mathit{Traces}_{\mathit{fin}}(\mathcal{T}_2)\}$$

Then, E is a safety property and $\mathcal{T}_2 \models E$.

By assumption: $\mathcal{T}_1 \models E$ and therefore $\mathit{Traces}(\mathcal{T}_1) \subseteq E$.

Hence: $\mathit{Traces}_{\mathit{fin}}(\mathcal{T}_1) = \mathit{pref}(\mathit{Traces}(\mathcal{T}_1))$

$$\subseteq \mathit{pref}(E) = \mathit{pref}(\mathit{cl}(\mathit{Traces}(\mathcal{T}_2)))$$

Safety and finite trace inclusion

$$Traces_{fin}(\mathcal{T}_1) \subseteq Traces_{fin}(\mathcal{T}_2)$$

iff for all safety properties E: $\mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E$

Proof "$\Longleftarrow$": consider the LT property

$$E = cl(Traces(\mathcal{T}_2)) = \{\sigma : pref(\sigma) \subseteq Traces_{fin}(\mathcal{T}_2)\}$$

Then, E is a safety property and $\mathcal{T}_2 \models E$.

By assumption: $\mathcal{T}_1 \models E$ and therefore $Traces(\mathcal{T}_1) \subseteq E$.

Hence: $Traces_{fin}(\mathcal{T}_1) = pref(Traces(\mathcal{T}_1))$

$$\subseteq pref(E) = pref(cl(Traces(\mathcal{T}_2)))$$

$$= Traces_{fin}(\mathcal{T}_2)$$

Safety and finite trace equivalence

Safety and finite trace equivalence

safety properties and finite trace inclusion:

If $\mathcal{T}_1$ and $\mathcal{T}_2$ are TS over AP then:

$$Traces_{fin}(\mathcal{T}_1) \subseteq Traces_{fin}(\mathcal{T}_2)$$

iff for all safety properties E: $\mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E$

Safety and finite trace equivalence

safety properties and finite trace inclusion:

If $\mathcal{T}_1$ and $\mathcal{T}_2$ are TS over AP then:

$$Traces_{fin}(\mathcal{T}_1) \subseteq Traces_{fin}(\mathcal{T}_2)$$

iff for all safety properties E: $\mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E$

safety properties and finite trace equivalence:

If $\mathcal{T}_1$ and $\mathcal{T}_2$ are TS over AP then:

$$Traces_{fin}(\mathcal{T}_1) = Traces_{fin}(\mathcal{T}_2)$$

iff $\mathcal{T}_1$ and $\mathcal{T}_2$ satisfy the same safety properties

Summary: trace relations and properties

trace inclusion

$Traces(\mathcal{T}) \subseteq Traces(\mathcal{T}')$ iff

for all LT properties E: $\mathcal{T}' \models E \Longrightarrow \mathcal{T} \models E$

finite trace inclusion

$Traces_{fin}(\mathcal{T}) \subseteq Traces_{fin}(\mathcal{T}')$ iff

for all safety properties E: $\mathcal{T}' \models E \Longrightarrow \mathcal{T} \models E$

Summary: trace relations and properties

trace equivalence

$\mathit{Traces}(\mathcal{T}) = \mathit{Traces}(\mathcal{T}')$ iff

$\mathcal{T}$ and $\mathcal{T}'$ satisfy the same LT properties

finite trace equivalence

$\mathit{Traces}_{\mathit{fin}}(\mathcal{T}) = \mathit{Traces}_{\mathit{fin}}(\mathcal{T}')$ iff

$\mathcal{T}$ and $\mathcal{T}'$ satisfy the same safety properties

correct or wrong?

If $\mathit{Traces}(\mathcal{T}) \subseteq \mathit{Traces}(\mathcal{T}')$
then $\mathit{Traces}_{\mathit{fin}}(\mathcal{T}) \subseteq \mathit{Traces}_{\mathit{fin}}(\mathcal{T}')$.

correct or wrong?

If $\mathit{Traces}(\mathcal{T}) \subseteq \mathit{Traces}(\mathcal{T}')$
then $\mathit{Traces}_{\mathit{fin}}(\mathcal{T}) \subseteq \mathit{Traces}_{\mathit{fin}}(\mathcal{T}')$.

correct, since

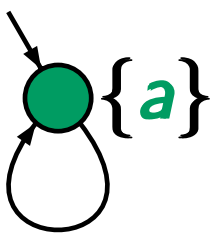
$$\begin{aligned} \mathit{Traces}_{\mathit{fin}}(\mathcal{T}) &= \text{set of all finite nonempty prefixes of words in } \mathit{Traces}(\mathcal{T}) \\ &= \mathit{pref}(\mathit{Traces}(\mathcal{T})) \end{aligned}$$

correct or wrong?

If $\mathit{Traces}(\mathcal{T}) \subseteq \mathit{Traces}(\mathcal{T}')$
then $\mathit{Traces}_{\mathit{fin}}(\mathcal{T}) \subseteq \mathit{Traces}_{\mathit{fin}}(\mathcal{T}')$.

correct, since

$$\begin{aligned} \mathit{Traces}_{\mathit{fin}}(\mathcal{T}) &= \text{set of all finite nonempty prefixes of words in } \mathit{Traces}(\mathcal{T}) \\ &= \mathit{pref}(\mathit{Traces}(\mathcal{T})) \end{aligned}$$



$$\begin{aligned} \mathit{Traces}(\mathcal{T}) &= \{ \{a\}^\omega \} \\ \mathit{Traces}_{\mathit{fin}}(\mathcal{T}) &= \{ \{a\}^n : n \geq 1 \} \end{aligned}$$

Finite trace relations versus trace relations

is trace equivalence the same as
finite trace equivalence **?**

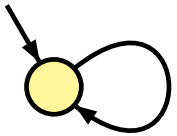
Finite trace relations versus trace relations

is trace equivalence the same as
finite trace equivalence **?**

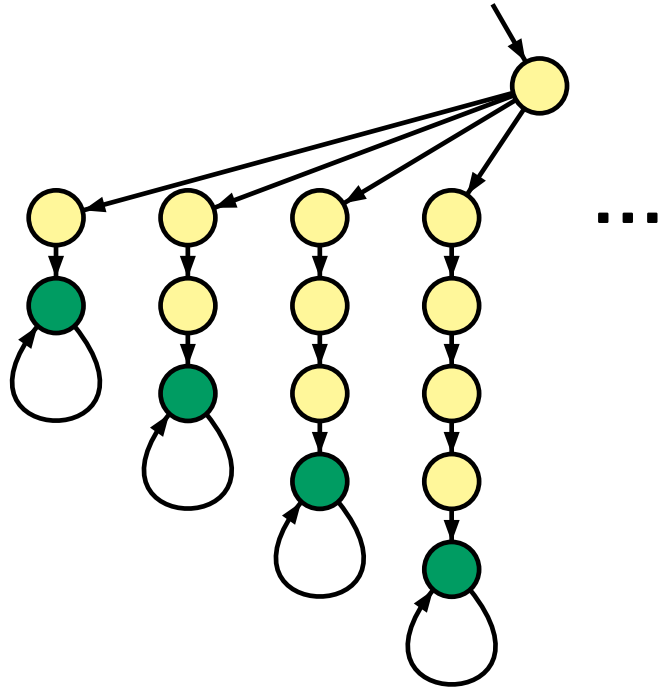
answer: **no**

Finite trace relations versus trace relations

$\mathcal{T}$



$\mathcal{T}'$

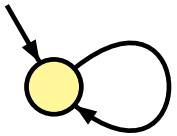


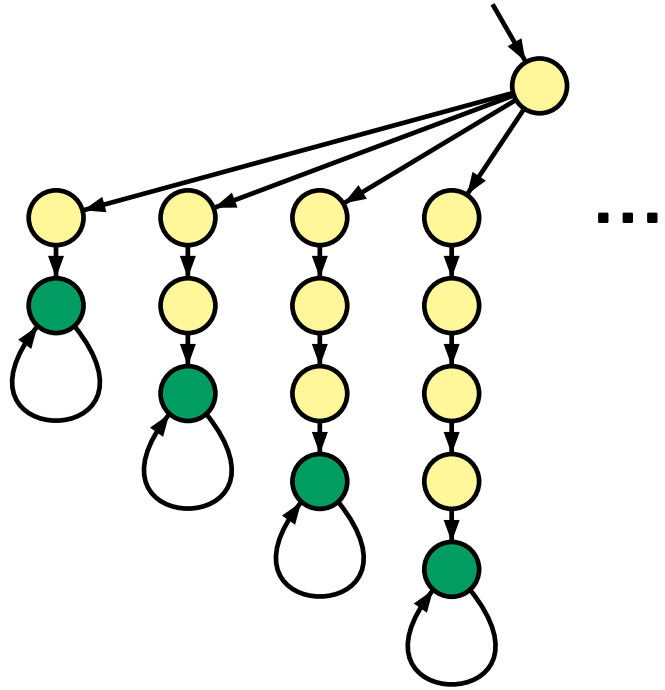
$\bigcirc \mathrel{\widehat{=}} \varnothing \qquad \bullet \mathrel{\widehat{=}} \{b\}$

set of propositions

$AP = \{b\}$

Finite trace relations versus trace relations

$\mathcal{T}$ 

$\mathcal{T}'$ 

$Traces(\mathcal{T}) = \{\varnothing^\omega\}$

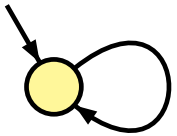
$\bigcirc \mathrel{\widehat{=}} \varnothing \quad \bullet \mathrel{\widehat{=}} \{b\}$

set of propositions

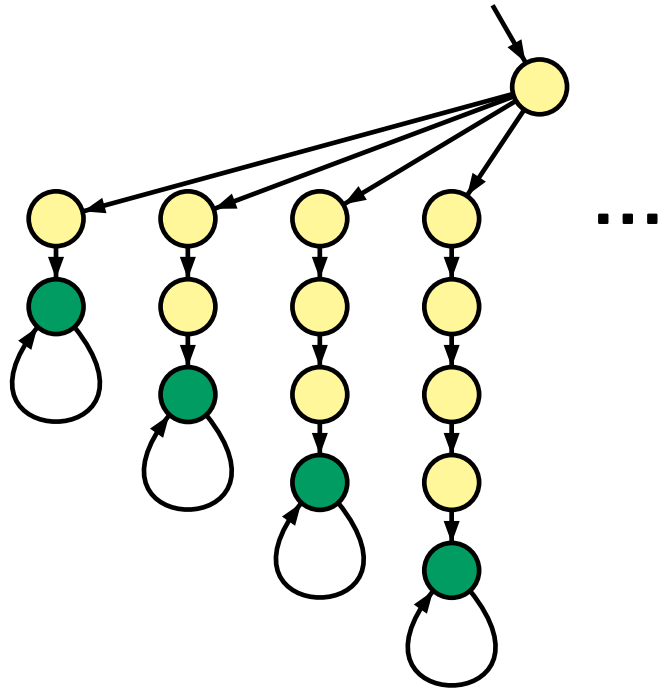
$AP = \{b\}$

Finite trace relations versus trace relations

$\mathcal{T}$



$\mathcal{T}'$



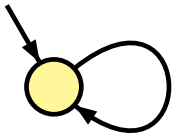
$$\mathit{Traces}(\mathcal{T}) = \{\varnothing^\omega\}$$
$$\mathit{Traces}_{\mathit{fin}}(\mathcal{T}) = \{\varnothing^n : n \geq 0\}$$

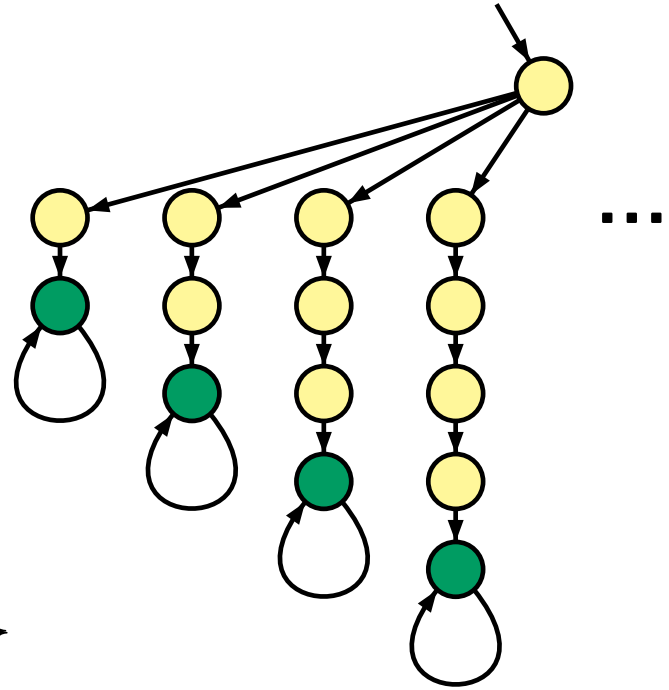
$\widehat{=}\varnothing$ $\widehat{=}\{b\}$

set of propositions

$$AP = \{b\}$$

Finite trace relations versus trace relations

$\mathcal{T}$ 

$\mathcal{T}'$ 

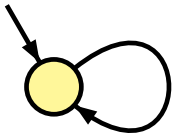
$$\begin{aligned} \mathit{Traces}(\mathcal{T}) &= \{\varnothing^\omega\} \\ \mathit{Traces}_{\mathit{fin}}(\mathcal{T}) &= \{\varnothing^n : n \geq 0\} \\ \mathit{Traces}(\mathcal{T}') &= \{\varnothing^n \{b\}^\omega : n \geq 2\} \end{aligned}$$

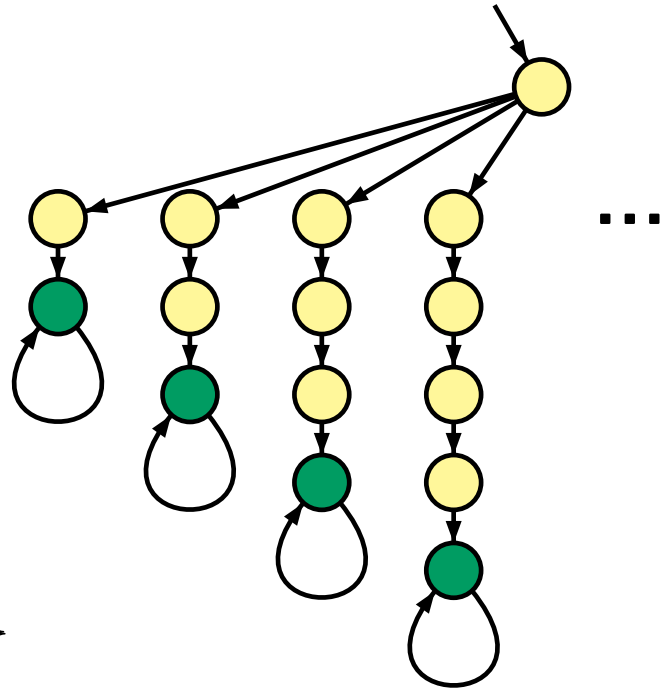
$\bigcirc \mathrel{\widehat{=}} \varnothing \quad \bullet \mathrel{\widehat{=}} \{b\}$

set of propositions

$$AP = \{b\}$$

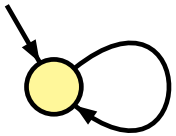
Finite trace relations versus trace relations

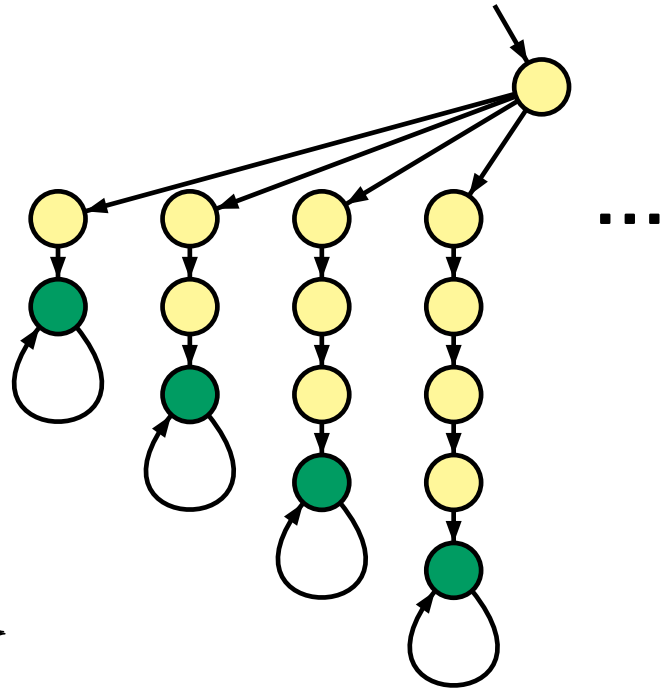
$\mathcal{T}$ 

$\mathcal{T}'$ 

$$
\begin{aligned}
\mathit{Traces}(\mathcal{T}) &= \{\varnothing^{\omega}\} \\
\mathit{Traces}_{\mathit{fin}}(\mathcal{T}) &= \{\varnothing^{n} : n \geq 0\} \\
\mathit{Traces}(\mathcal{T}') &= \{\varnothing^{n}\{b\}^{\omega} : n \geq 2\} \\
\mathit{Traces}_{\mathit{fin}}(\mathcal{T}') &= \{\varnothing^{n} : n \geq 0\} \ \cup \\
&\quad \{\varnothing^{n}\{b\}^{m} : n \geq 2 \wedge m \geq 1\}
\end{aligned}
$$

Finite trace relations versus trace relations

$\mathcal{T}$ 

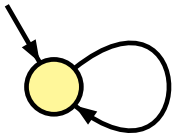
$\mathcal{T}'$ 

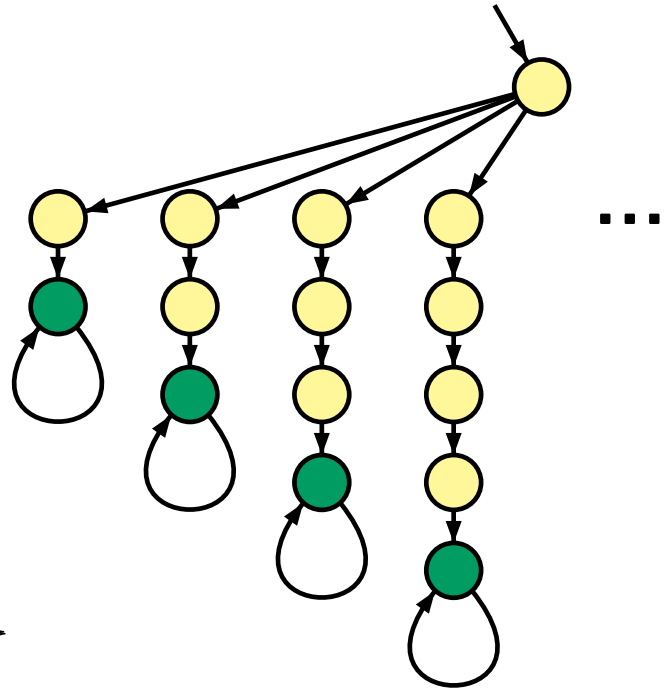
$$
\begin{aligned}
\mathit{Traces}(\mathcal{T}) &= \{\varnothing^{\omega}\} \\
\mathit{Traces}_{\mathit{fin}}(\mathcal{T}) &= \{\varnothing^{n} : n \geq 0\} \\
\mathit{Traces}(\mathcal{T}') &= \{\varnothing^{n}\{b\}^{\omega} : n \geq 2\} \\
\mathit{Traces}_{\mathit{fin}}(\mathcal{T}') &= \{\varnothing^{n} : n \geq 0\} \ \cup \\
&\quad \{\varnothing^{n}\{b\}^{m} : n \geq 2 \wedge m \geq 1\}
\end{aligned}
$$

$\mathit{Traces}(\mathcal{T}) \not\subseteq \mathit{Traces}(\mathcal{T}')$, but

$\mathit{Traces}_{\mathit{fin}}(\mathcal{T}) \subseteq \mathit{Traces}_{\mathit{fin}}(\mathcal{T}')$

Finite trace relations versus trace relations

$\mathcal{T}$ 

$\mathcal{T}'$ 

$$
\begin{aligned}
\mathit{Traces}(\mathcal{T}) &= \{\varnothing^{\omega}\} \\
\mathit{Traces}_{\mathit{fin}}(\mathcal{T}) &= \{\varnothing^{n} : n \geq 0\} \\
\mathit{Traces}(\mathcal{T}') &= \{\varnothing^{n}\{b\}^{\omega} : n \geq 2\} \\
\mathit{Traces}_{\mathit{fin}}(\mathcal{T}') &= \{\varnothing^{n} : n \geq 0\} \ \cup \\
&\quad \{\varnothing^{n}\{b\}^{m} : n \geq 2 \wedge m \geq 1\}
\end{aligned}
$$

$\mathit{Traces}(\mathcal{T}) \not\subseteq \mathit{Traces}(\mathcal{T}')$, but

$\mathit{Traces}_{\mathit{fin}}(\mathcal{T}) \subseteq \mathit{Traces}_{\mathit{fin}}(\mathcal{T}')$

LT property

$E \mathrel{\widehat{=}}$ "eventually b"

$\mathcal{T} \not\models E, \quad \mathcal{T}' \models E$

Finite trace and trace inclusion

Suppose that $\mathcal{T}$ and $\mathcal{T}'$ are TS over AP such that

(1) $\mathcal{T}$ has no terminal states,

(2) $\mathcal{T}'$ is finite.

Finite trace and trace inclusion

Suppose that $\mathcal{T}$ and $\mathcal{T}'$ are TS over AP such that

(1) $\mathcal{T}$ has no terminal states,
i.e., all paths of $\mathcal{T}$ are infinite

(2) $\mathcal{T}'$ is finite.

Finite trace and trace inclusion

Suppose that $\mathcal{T}$ and $\mathcal{T}'$ are TS over AP such that

(1) $\mathcal{T}$ has no terminal states,
i.e., all paths of $\mathcal{T}$ are infinite

(2) $\mathcal{T}'$ is finite.

Then:

$$Traces(\mathcal{T}) \subseteq Traces(\mathcal{T}')$$

$$\text{iff} \quad Traces_{fin}(\mathcal{T}) \subseteq Traces_{fin}(\mathcal{T}')$$

Finite trace and trace inclusion

Suppose that $\mathcal{T}$ and $\mathcal{T}'$ are TS over AP such that

(1) $\mathcal{T}$ has no terminal states,
i.e., all paths of $\mathcal{T}$ are infinite

(2) $\mathcal{T}'$ is finite.

Then:

$$Traces(\mathcal{T}) \subseteq Traces(\mathcal{T}')$$

$$\text{iff} \quad Traces_{fin}(\mathcal{T}) \subseteq Traces_{fin}(\mathcal{T}')$$

"$\Longrightarrow$": holds for all transition systems,
no matter whether (1) and (2) hold

Finite trace and trace inclusion

Suppose that $\mathcal{T}$ and $\mathcal{T}'$ are TS over AP such that

(1) $\mathcal{T}$ has no terminal states,
i.e., all paths of $\mathcal{T}$ are infinite

(2) $\mathcal{T}'$ is finite.

Then:

$$Traces(\mathcal{T}) \subseteq Traces(\mathcal{T}')$$

iff

$$Traces_{fin}(\mathcal{T}) \subseteq Traces_{fin}(\mathcal{T}')$$

"$\Longrightarrow$": holds for all transition systems

"$\Longleftarrow$": suppose that (1) and (2) hold and that

(3) $Traces_{fin}(\mathcal{T}) \subseteq Traces_{fin}(\mathcal{T}')$

Show that $Traces(\mathcal{T}) \subseteq Traces(\mathcal{T}')$

Finite trace and trace inclusion

Suppose that $\mathcal{T}$ and $\mathcal{T}'$ are TS over AP such that

(1) $\mathcal{T}$ has no terminal states

(2) $\mathcal{T}'$ is finite

(3) $Traces_{fin}(\mathcal{T}) \subseteq Traces_{fin}(\mathcal{T}')$

Then $Traces(\mathcal{T}) \subseteq Traces(\mathcal{T}')$

Proof:

Finite trace and trace inclusion

Suppose that $\mathcal{T}$ and $\mathcal{T}'$ are TS over AP such that

(1) $\mathcal{T}$ has no terminal states

(2) $\mathcal{T}'$ is finite

(3) $Traces_{fin}(\mathcal{T}) \subseteq Traces_{fin}(\mathcal{T}')$

Then $Traces(\mathcal{T}) \subseteq Traces(\mathcal{T}')$

Proof: Pick some path $\pi = s_0\, s_1\, s_2 \ldots$ in $\mathcal{T}$ and show that there exists a path

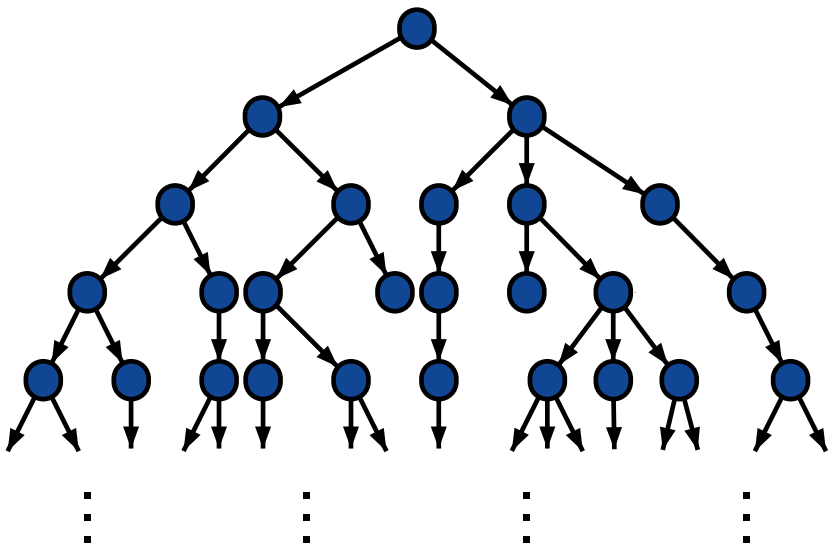
$$\pi' = t_0\, t_1\, t_2 \ldots \text{ in } \mathcal{T}'$$

such that $trace(\pi) = trace(\pi')$

Tracesfin versus traces

finite TS $\mathcal{T}'$

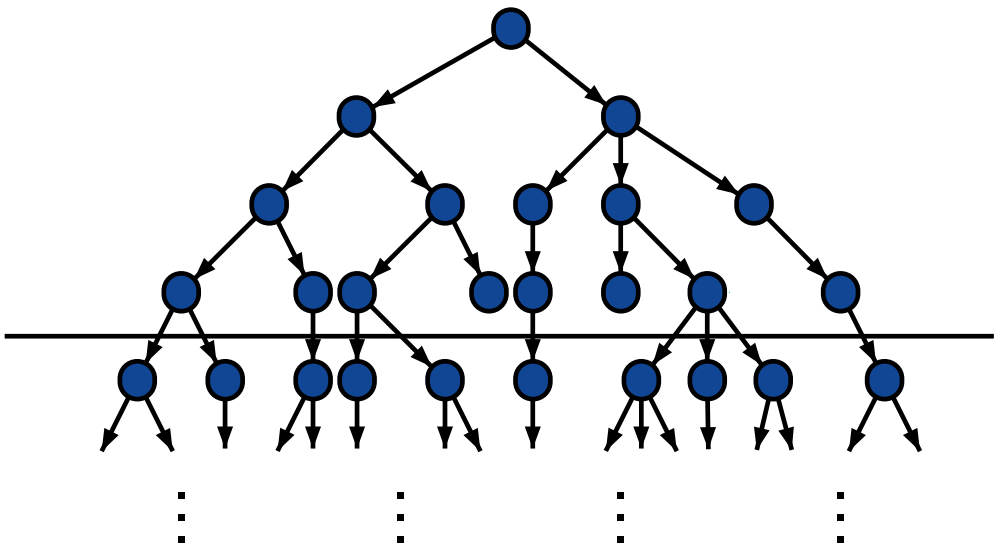
paths from state t_0
(unfolded into a tree)



Tracesfin versus traces

finite TS $\mathcal{T}'$

paths from state t_0
(unfolded into a tree)



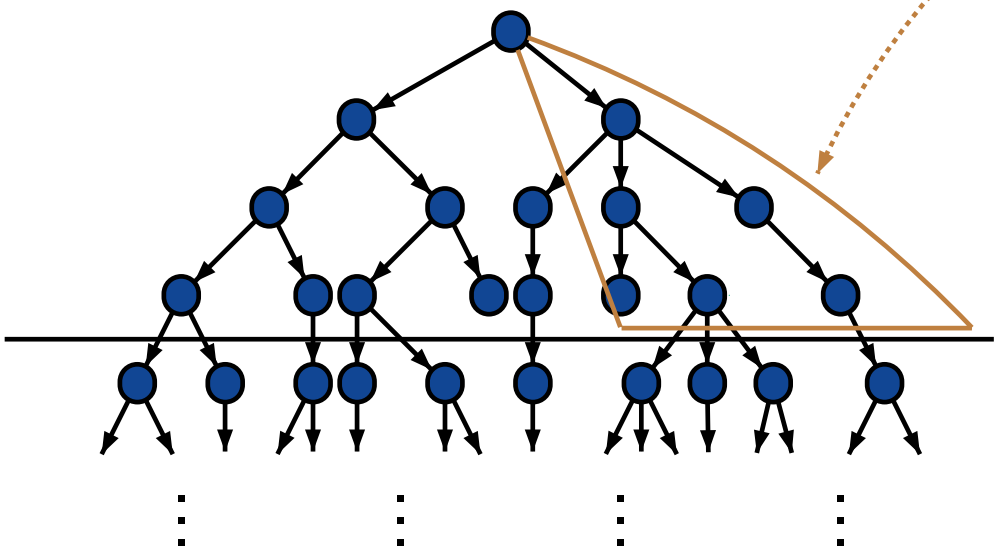
finite until
depth $\leq n$

Tracesfin versus traces

finite TS $\mathcal{T}'$

paths from state t_0
(unfolded into a tree)

contains all path fragments
with trace $A_0\, A_1 \ldots A_n$



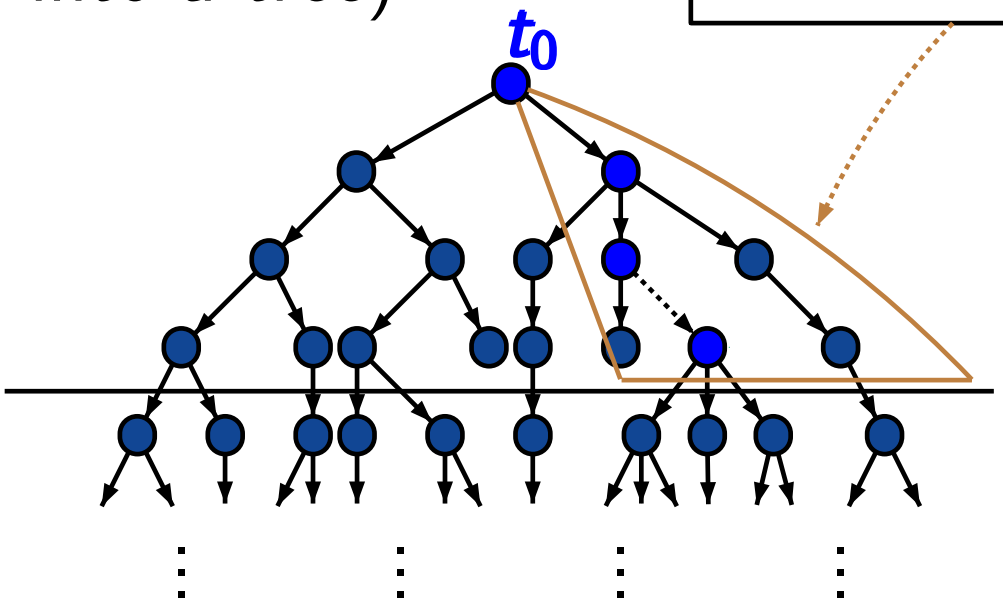
finite until
depth $\leq n$

Tracesfin versus traces

finite TS $\mathcal{T}'$

paths from state t_0
(unfolded into a tree)

contains all path fragments
with trace $A_0\, A_1 \ldots A_n$
in particular: $t_0\, t_1 \ldots t_n$



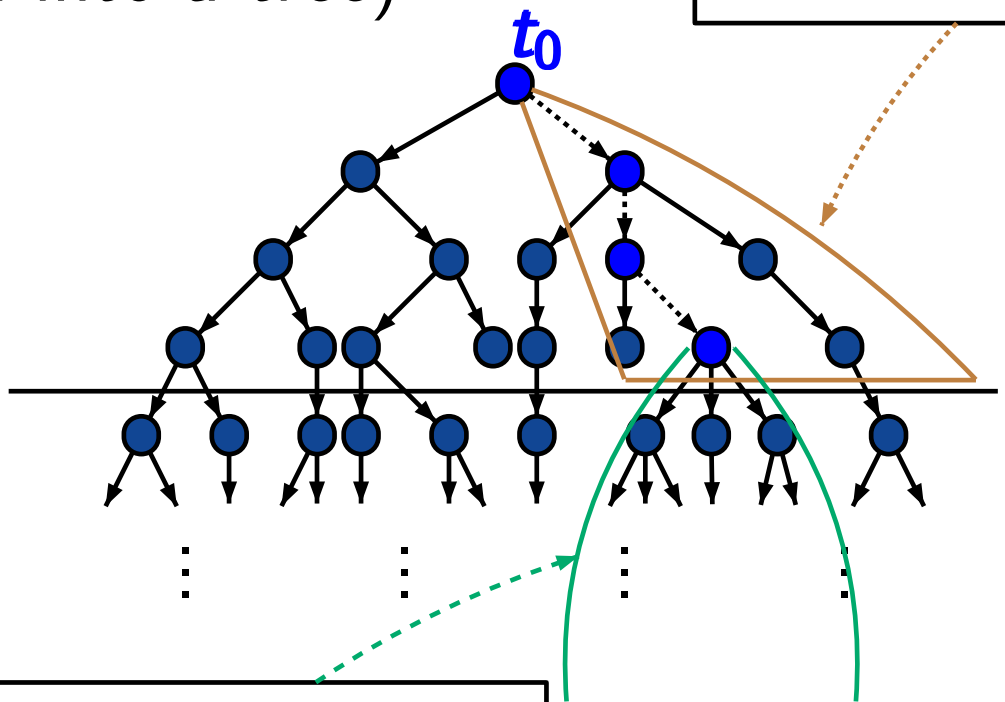
finite until
depth $\leq n$

Tracesfin versus traces

finite TS $\mathcal{T}'$

paths from state t_0
(unfolded into a tree)

contains all path fragments
with trace $A_0\, A_1 \ldots A_n$
in particular: $t_0\, t_1 \ldots t_n$



finite until
depth $\leq n$

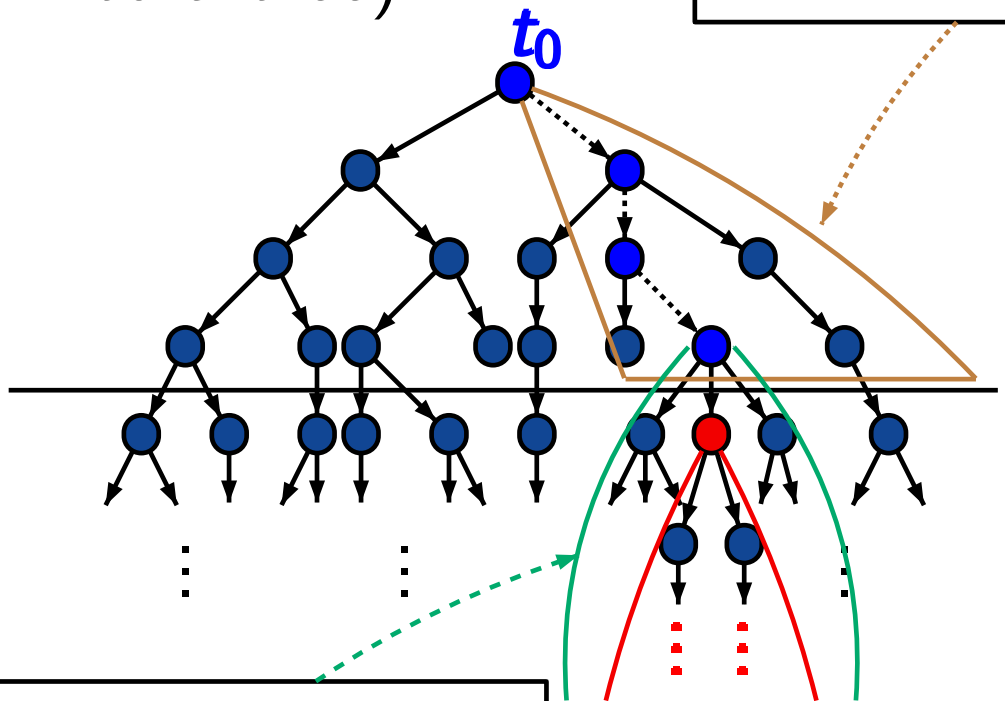
contains infinitely
many path fragments
$t_n\, s_{n+1}^m \cdots s_m^m$

Tracesfin versus traces

finite TS $\mathcal{T}'$

paths from state t_0
(unfolded into a tree)

contains all path fragments
with trace $A_0\, A_1 \ldots A_n$
in particular: $t_0\, t_1 \ldots t_n$



finite until
depth $\leq n$

contains infinitely
many path fragments
$t_n\, s^m_{n+1} \cdots s^m_m$

there exists $t_{n+1} \in Post(t_n)$
s.t. $t_{n+1} = s^m_{n+1}$ for
infinitely many m

Finite trace and trace inclusion

Suppose that $\mathcal{T}$ and $\mathcal{T}'$ are TS over AP such that

(1) $\mathcal{T}$ has no terminal states

(2) $\mathcal{T}'$ is finite

(3) $Traces_{fin}(\mathcal{T}) \subseteq Traces_{fin}(\mathcal{T}')$

Then $Traces(\mathcal{T}) \subseteq Traces(\mathcal{T}')$

$\longleftarrow$ image-finiteness is sufficient

Finite trace and trace inclusion

Suppose that $\mathcal{T}$ and $\mathcal{T}'$ are TS over AP such that

(1) $\mathcal{T}$ has no terminal states

(2) $\mathcal{T}'$ is finite

(3) $Traces_{fin}(\mathcal{T}) \subseteq Traces_{fin}(\mathcal{T}')$

Then $Traces(\mathcal{T}) \subseteq Traces(\mathcal{T}')$

$\longleftarrow$ image-finiteness is sufficient

image-finiteness of $\mathcal{T}' = (S', Act, \rightarrow, S'_0, AP, L')$:

Finite trace and trace inclusion

Suppose that $\mathcal{T}$ and $\mathcal{T}'$ are TS over AP such that

(1) $\mathcal{T}$ has no terminal states

(2) $\mathcal{T}'$ is finite

(3) $Traces_{fin}(\mathcal{T}) \subseteq Traces_{fin}(\mathcal{T}')$

Then $Traces(\mathcal{T}) \subseteq Traces(\mathcal{T}')$

$\longleftarrow$ image-finiteness is sufficient

image-finiteness of $\mathcal{T}' = (S', Act, \rightarrow, S'_0, AP, L')$:

- for each $A \in 2^{AP}$ and state $s \in S'$:

  $\{t \in Post(s) : L'(t) = A\}$ is finite

Finite trace and trace inclusion

Suppose that $\mathcal{T}$ and $\mathcal{T}'$ are TS over AP such that

(1) $\mathcal{T}$ has no terminal states

(2) $\mathcal{T}'$ is finite

(3) $Traces_{fin}(\mathcal{T}) \subseteq Traces_{fin}(\mathcal{T}')$

Then $Traces(\mathcal{T}) \subseteq Traces(\mathcal{T}')$

$\longleftarrow$ image-finiteness is sufficient

image-finiteness of $\mathcal{T}' = (S', Act, \rightarrow, S'_0, AP, L')$:

- for each $A \in 2^{AP}$ and state $s \in S'$:

  $\{t \in Post(s) : L'(t) = A\}$ is finite

- for each $A \in 2^{AP}$: $\{s_0 \in S'_0 : L'(s_0) = A\}$ is finite

Trace equivalence vs. finite trace equivalence

Whenever $\mathit{Traces}(\mathcal{T}) = \mathit{Traces}(\mathcal{T}')$ then

$\mathit{Traces}_{\mathit{fin}}(\mathcal{T}) = \mathit{Traces}_{\mathit{fin}}(\mathcal{T}')$

Trace equivalence vs. finite trace equivalence

Whenever $\mathit{Traces}(\mathcal{T}) = \mathit{Traces}(\mathcal{T}')$ then

$\mathit{Traces}_{\mathit{fin}}(\mathcal{T}) = \mathit{Traces}_{\mathit{fin}}(\mathcal{T}')$

while the reverse direction does not hold in general

(even not for finite transition systems)

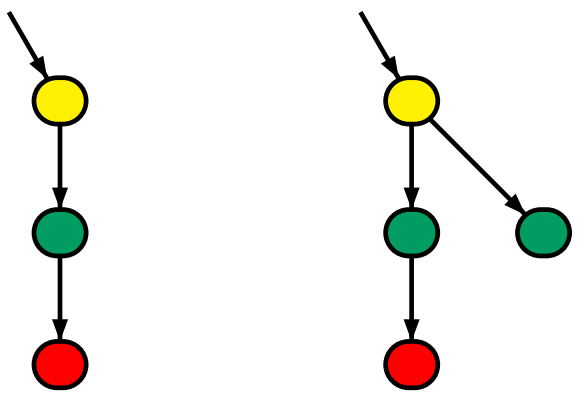
Trace equivalence vs. finite trace equivalence

Whenever $\mathit{Traces}(\mathcal{T}) = \mathit{Traces}(\mathcal{T}')$ then

$\mathit{Traces}_{\mathit{fin}}(\mathcal{T}) = \mathit{Traces}_{\mathit{fin}}(\mathcal{T}')$

while the reverse direction does not hold in general

(even not for finite transition systems)



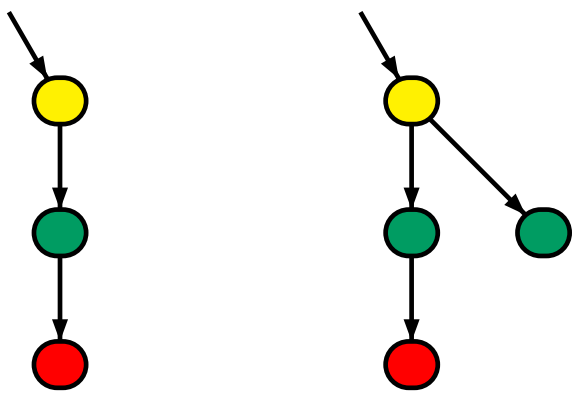
Trace equivalence vs. finite trace equivalence

Whenever $\mathit{Traces}(\mathcal{T}) = \mathit{Traces}(\mathcal{T}')$ then

$\mathit{Traces}_{\mathit{fin}}(\mathcal{T}) = \mathit{Traces}_{\mathit{fin}}(\mathcal{T}')$

while the reverse direction does not hold in general

(even not for finite transition systems)



finite trace equivalent,

but *not* trace equivalent

Trace equivalence vs. finite trace equivalence

Whenever $\mathit{Traces}(\mathcal{T}) = \mathit{Traces}(\mathcal{T}')$ then
$\mathit{Traces}_{\mathit{fin}}(\mathcal{T}) = \mathit{Traces}_{\mathit{fin}}(\mathcal{T}')$

The reverse implication holds under additional assumptions, e.g.,

- if $\mathcal{T}$ and $\mathcal{T}'$ are finite and have no terminal states
- or, if $\mathcal{T}$ and $\mathcal{T}'$ are AP-deterministic