Model Checking I
alias
Reactive Systems Verification

Luca Tesei

MSc in Computer Science, University of Camerino

Topics

- Safety Properties and Bad Prefix.
- Prefix Closure.

Material

Reading:

Chapter 3 of the book, pages 111–116.

More:

The slides in the following pages are taken from the material of the course "Introduction to Model Checking" held by Prof. Dr. Ir. Joost-Pieter Katoen at Aachen University.

Introduction

Modelling parallel systems

Linear Time Properties

- state-based and linear time view
- definition of linear time properties
- invariants and safety ⟵
- liveness and fairness

Regular Properties

Linear Temporal Logic

Computation-Tree Logic

Equivalences and Abstraction

Invariant

Invariant

Let E be an LT property over AP.

E is called an invariant if there exists a propositional formula Φ over AP such that

$$E = \left\{ A_0 A_1 A_2 \ldots \in \left(2^{AP}\right)^\omega : \forall i \geq 0.\, A_i \models \Phi \right\}$$

Invariant

Let E be an LT property over AP.

E is called an invariant if there exists a propositional formula Φ over AP such that

$$E = \left\{ A_0 A_1 A_2 \ldots \in \left(2^{AP}\right)^\omega : \forall i \geq 0.\, A_i \models \Phi \right\}$$

Φ is called the invariant condition of E.

Safety properties

state that "nothing bad will happen"

Safety properties

state that "nothing bad will happen"

- mutual exclusion: *never* $crit_1 \wedge crit_2$
- deadlock freedom: e.g., for dining philosophers
  never $\bigwedge_{0 \leq i < n} wait_i$

Safety properties

state that "nothing bad will happen"

- mutual exclusion: *never* $crit_1 \wedge crit_2$
- deadlock freedom: e.g., for dining philosophers
  never $\bigwedge_{0 \leq i < n} wait_i$
- German traffic lights:
  every red phase is preceded by a yellow phase

Safety properties

state that "nothing bad will happen"

- mutual exclusion: *never* $crit_1 \wedge crit_2$
- deadlock freedom: e.g., for dining philosophers
  never $\bigwedge_{0 \leq i < n} wait_i$
- German traffic lights:
  every red phase is preceded by a yellow phase
- beverage machine:
  no drink must be released if the user did not enter a coin before

  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:

- mutual exclusion: *never* $crit_1 \wedge crit_2$
- deadlock freedom: *never* $\bigwedge_{0 \leq i < n} wait_i$

---

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* $crit_1 \wedge crit_2$
- deadlock freedom: *never* $\bigwedge_{0 \leq i < n} wait_i$

---

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* $crit_1 \wedge crit_2$
- deadlock freedom: *never* $\bigwedge_{0 \leq i < n} wait_i$

---

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., $\ldots \{\bullet\}\{\bullet\}$

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., $\ldots \{\bullet\}\{\bullet\}$ (green, red)

- beverage machine:

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

Bad prefixes of safety properties

IS2.5-10B

- 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., $\ldots$ {●} {●}

- 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

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

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

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

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

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.,

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

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

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

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.,

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

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

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

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.,

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

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

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

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.

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

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

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

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.,

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

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

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

↑

briefly: $BadPref$

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

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

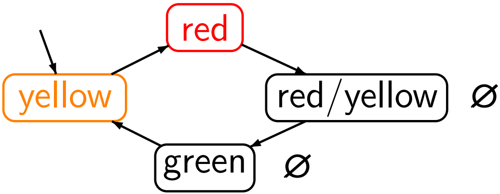
there exists a finite prefix $A_0\, A_1 \ldots A_n$ of σ such that *none* of the words $A_0\, A_1 \ldots A_n\, B_{n+1}\, B_{n+2}\, B_{n+3} \ldots$ belongs to E, i.e.,

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

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

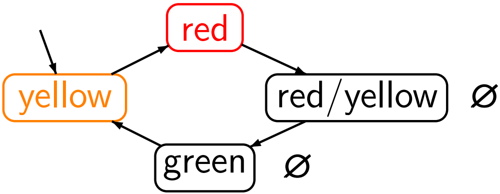
minimal bad prefixes: any word $A_0 \ldots A_i \ldots A_n \in \mathit{BadPref}$ s.t. no proper prefix $A_0 \ldots A_i$ is a bad prefix for E

Safety property for a traffic light



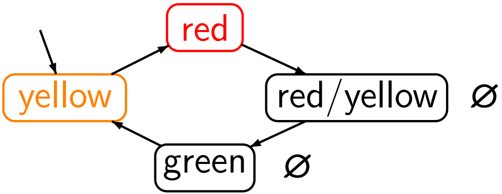
$AP = \{red, yellow\}$

Safety property for a traffic light



"every red phase is preceded by a yellow phase"

Safety property for a traffic light



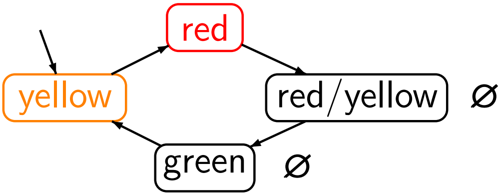
"every red phase is preceded by a yellow phase"

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 $i \in \mathbb{N}$:

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

Safety property for a traffic light

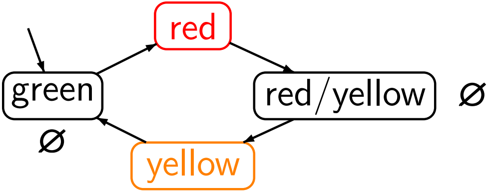


"every red phase is preceded by a yellow phase"

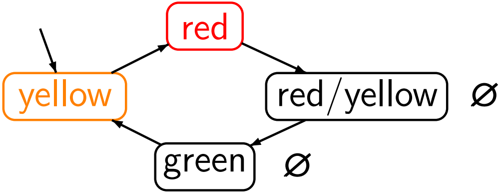
hence: $\mathcal{T} \not\models E$

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

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



Safety property for a traffic light

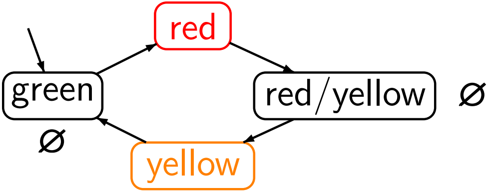


"every red phase is preceded by a yellow phase"

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

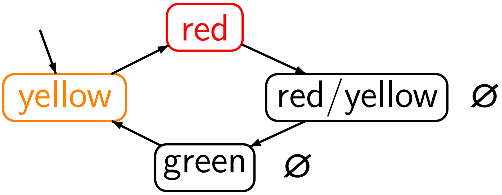
E = set of all infinite words $A_0 A_1 A_2 \ldots$ over 2^{AP} such that for all $i \in \mathbb{N}$:

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



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

Safety property for a traffic light

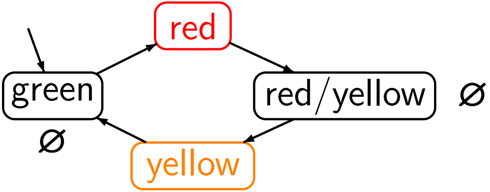


"every red phase is preceded by a yellow phase"

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 $i \in \mathbb{N}$:

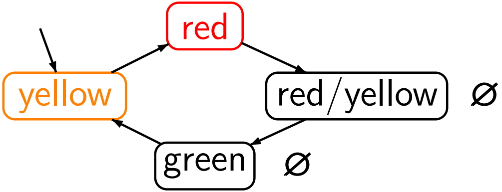
$$red \in A_i \implies i \geq 1 \text{ and } yellow \in A_{i-1}$$



"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

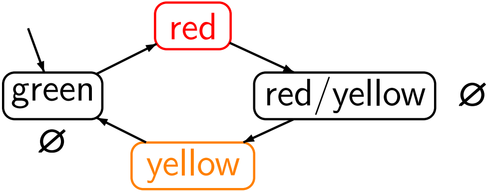


"every red phase is preceded by a yellow phase"

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

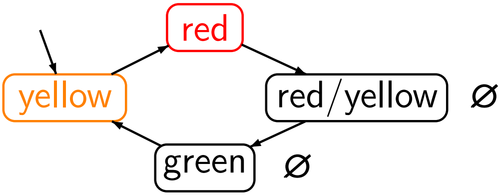
E = set of all infinite words $A_0\, A_1\, A_2 \ldots$ over 2^{AP} such that for all $i \in \mathbb{N}$:

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



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

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

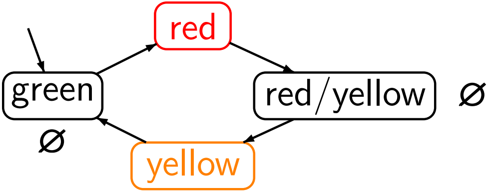


"every red phase is preceded by a yellow phase"

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 $i \in \mathbb{N}$:

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

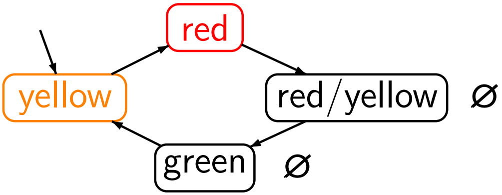


$\mathcal{T} \not\models E$

minimal bad prefix:

$\varnothing \{red\}$

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 $i \in \mathbb{N}$:

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

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

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

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

Satisfaction of safety properties

IS2.5-11A

Satisfaction of safety properties

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

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

$\mathit{Traces}(\mathcal{T}) \quad = \quad$ 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.

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

$BadPref$ = 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 $\mathcal{T}$

$= \{\, trace(\widehat{\pi}) : \widehat{\pi}$ 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.

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

$\mathit{BadPref}$ = set of all bad prefixes of E

$\mathit{MinBadPref}$ = set of all minimal bad prefixes of E

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

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

$= \{ \, \mathit{trace}(\widehat{\pi}) : \widehat{\pi}$ 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.

Every invariant is a safety property.

correct.

Let E be an invariant with invariant condition Φ.

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.

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

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

$\varnothing$ is a safety property

correct

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

Correct or wrong?

$\varnothing$ is a safety property

correct

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

Correct or wrong?

$\varnothing$ is a safety property

correct

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

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

correct

$\varnothing$ 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

$$\text{“For all words} \in \underbrace{(2^{AP})^\omega \setminus (2^{AP})^\omega}_{= \varnothing} \dots\text{”}$$

Prefix closure

Prefix closure

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

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

Prefix closure

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

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

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

Prefix closure

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

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

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

Prefix closure

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

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

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

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

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

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

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

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

Prefix closure and safety

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

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

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

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

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

Prefix closure and safety

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

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

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

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

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

Theorem:

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