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
Safety properties

state that "nothing bad will happen"
Safety properties

state that “nothing bad will happen”

invariants:

• mutual exclusion: never $\text{crit}_1 \land \text{crit}_2$
• deadlock freedom: never $\bigwedge_{0 \leq i < n} \text{wait}_i$

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

Invariants: "no bad state will be reached"

- Mutual exclusion: never $\text{crit}_1 \land \text{crit}_2$
- Deadlock freedom: never $\bigwedge_{0 \leq i < n} \text{wait}_i$

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:  \( \text{never } \text{crit}_1 \land \text{crit}_2 \)
- deadlock freedom:  \( \text{never } \bigwedge_{0 \leq i < n} \text{wait}_i \)

other safety properties:  “no bad prefix”

- German traffic lights:  \( \text{every red phase is preceded by a yellow phase} \)
- beverage machine:  \( \text{the total number of entered coins is never less than the total number of released drinks} \)
Bad prefixes of safety properties

- traffic lights:

  *every red phase is preceded by a yellow phase*

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

  e.g., ... {●} {●} ...
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 \{\textcolor{green}{\circ}\} \{\textcolor{red}{\bullet}\}

- beverage machine:

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

  bad prefix, e.g., \{\textcolor{blue}{\textit{pay}}\} \{\textcolor{blue}{\textit{drink}}\} \{\textcolor{blue}{\textit{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 $\sigma$ 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.,

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

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

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 $\sigma$ 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.,

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

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

$E = \text{ set of all infinite words that do not have a bad prefix}$
Definition of safety properties

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

$E$ is called a safety property if for all words

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

there exists a finite prefix $A_0 A_1 \ldots A_n$ of $\sigma$ 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.,

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

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

$$\text{BadPref}_E \overset{\text{def}}{=} \text{set of bad prefixes for } E$$
Definition of safety properties

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

\( E \) is called a safety property if for all words
\[
\sigma = A_0 A_1 A_2 \ldots \in (2^{\mathcal{AP}})^\omega \setminus E
\]
there exists a finite prefix \( A_0 A_1 \ldots A_n \) of \( \sigma \) 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.,
\[
E \cap \{ \sigma' \in (2^{\mathcal{AP}})^\omega : A_0 \ldots A_n \text{ is a prefix of } \sigma' \} = \emptyset
\]
Such words \( A_0 A_1 \ldots A_n \) are called bad prefixes for \( E \).

\[
\text{BadPref}_E \overset{\text{def}}{=} \text{set of bad prefixes for } E \subseteq (2^{\mathcal{AP}})^+\]
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 \( \sigma \) 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.,

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

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

\[
\text{BadPref}_E \overset{\text{def}}{=} \text{set of bad prefixes for } E \subseteq (2^{AP})^+
\]

briefly: \( \text{BadPref} \)
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 $\sigma$ 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.,

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

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

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

\[ AP = \{ \text{red, yellow} \} \]
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: $\mathcal{T} \models E$

$E = \text{set of all infinite words } A_0 A_1 A_2 \ldots$

over $2^{AP}$ such that for all $i \in \mathbb{N}$:

$\text{red} \in A_i \implies i \geq 1$ and $\text{yellow} \in A_{i-1}$
Safety property for a traffic light

"every red phase is preceded by a yellow phase"

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

\[
E = \text{set of all infinite words } A_0 A_1 A_2 \ldots \text{ over } 2^{AP} \text{ such that for all } i \in \mathbb{N}: \\
\text{red} \in A_i \implies i \geq 1 \text{ and yellow} \in A_{i-1}
\]
Safety property for a traffic light

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

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

“every red phase is preceded by a yellow phase”

hence: $T \models E$
```

```
“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: \( \mathcal{T} \models E \)

\[ E = \text{set of all infinite words } A_0 A_1 A_2 \ldots \]
over \( 2^{AP} \) such that for all \( i \in \mathbb{N} \):
\[ \text{red} \in A_i \implies i \geq 1 \text{ and } \text{yellow} \in A_{i-1} \]

“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: $\mathcal{T} \models E$

$E = \text{set of all infinite words } A_0 A_1 A_2 \ldots$

over $2^{\mathcal{AP}}$ such that for all $i \in \mathbb{N}$:

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

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

bad prefix, e.g.,

$\emptyset \{ \text{red} \} \emptyset \{ \text{yellow} \}$
Safety property for a traffic light

“every red phase is preceded by a yellow phase”

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

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

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

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

minimal bad prefix: $\emptyset \{\text{red}\}$
Safety property for a traffic light

A safety property for a traffic light is:

\[
\text{“every red phase is preceded by a yellow phase”}
\]

hence: \( \mathcal{T} \models E \)

\[
E = \text{set of all infinite words } A_0 A_1 A_2 \ldots \text{ over } 2^{AP} \text{ such that for all } i \in \mathbb{N}:
\]
\[
\text{red} \in A_i \implies i \geq 1 \text{ and } \text{yellow} \in A_{i-1}
\]

is a safety property over \( AP = \{ \text{red}, \text{yellow} \} \) with

\[
\text{BadPref} = \text{set of all finite words } A_0 A_1 \ldots A_n \text{ over } 2^{AP} \text{ s.t. for some } i \in \{0, \ldots, n\}:
\]
\[
\text{red} \in A_i \land (i=0 \lor \text{yellow} \notin A_{i-1})
\]
Satisfaction of safety properties
Let $E \subseteq (2^\text{AP})^\omega$ be a safety property, $\mathcal{T}$ a TS over $\text{AP}$.

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

$\text{Traces}(\mathcal{T}) = \text{set of traces of } \mathcal{T}$
Satisfaction of safety properties

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

\[ T \models E \quad \text{iff} \quad \text{Traces}(T) \subseteq E \]
\[ \quad \text{iff} \quad \text{Traces}_{\text{fin}}(T) \cap \text{BadPref} = \emptyset \]

**BadPref** = set of all bad prefixes of $E$

**Traces** ($T$) = set of traces of $T$

**Traces**$_{\text{fin}}$ ($T$) = set of finite traces of $T$

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

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

\[
\begin{align*}
T \models E & \iff \text{Traces}(T) \subseteq E \\
& \iff \text{Traces}_{\text{fin}}(T) \cap \text{BadPref} = \emptyset \\
& \iff \text{Traces}_{\text{fin}}(T) \cap \text{MinBadPref} = \emptyset
\end{align*}
\]

**BadPref** = set of all bad prefixes of $E$

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

**Traces(T)** = set of traces of $T$

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

= \{ \text{trace}(\pi) : \pi \text{ is an initial, finite path fragment of } 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 $\Phi$. 
Correct or wrong?

Every invariant is a safety property.

correct.

Let $E$ be an invariant with invariant condition $\Phi$.

- bad prefixes for $E$: finite words $A_0 \ldots A_i \ldots A_n$ s.t. $A_i \not\models \Phi$ 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 $\Phi$.

- bad prefixes for $E$: finite words $A_0 \ldots A_i \ldots A_n$ s.t. $A_i \not\models \Phi$ 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 $A_i \models \Phi$ for $i = 0, 1, \ldots, n-1$, and $A_n \not\models \Phi$
Correct or wrong?

∅ is a safety property
Correct or wrong?

Ø is a safety property

correct
Correct or wrong?

∅ is a safety property

correct

• all finite words $A_0 \ldots A_n \in (2^{AP})^+$ are bad prefixes
Correct or wrong?

∅ is a safety property

correct

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

• ∅ is even an invariant (invariant condition false)
Correct or wrong?

\[ \emptyset \text{ is a safety property} \]

**Correct**

- All finite words \( A_0 \ldots A_n \in (2^{AP})^+ \) are bad prefixes.
- \( \emptyset \) is even an invariant (invariant condition \textit{false}).

\[ (2^{AP})^\omega \text{ is a safety property} \]
Correct or wrong?

∅ is a safety property

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

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

**correct**
Correct or wrong?

∅ is a safety property

**Correct**

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

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

**Correct**

“For all words $\in (2^{AP})^\omega \setminus (2^{AP})^\omega \ldots$”

$\equiv \emptyset$
Prefix closure
Prefix closure

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

\[
pref(\sigma) \overset{\text{def}}{=} \text{set of all nonempty, finite prefixes of } \sigma
\]

\[= \{ A_0 A_1 \ldots A_n : n \geq 0 \}\]
Prefix closure

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

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

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

For $E \subseteq (2^A)^\omega$, let $\text{pref}(E) \overset{\text{def}}{=} \bigcup_{\sigma \in E} \text{pref}(\sigma)$
For a given infinite word $\sigma = A_0 A_1 A_2 \ldots$, let

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

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

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

$$\text{pref}(E) \overset{\text{def}}{=} \bigcup_{\sigma \in E} \text{pref}(\sigma)$$

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

$$\text{cl}(E) \overset{\text{def}}{=} \{ \sigma \in (2^{AP})^\omega : \text{pref}(\sigma) \subseteq \text{pref}(E) \}$$
Prefix closure and safety

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

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

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

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

$$\text{cl}(E) = \{ \sigma \in (2^{AP})^\omega : \text{pref}(\sigma) \subseteq \text{pref}(E) \}$$
Prefix closure and safety

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

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

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

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

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

**Theorem:**

$E$ is a safety property iff $\text{cl}(E) = E$
Safety and finite trace inclusion

**remind**: LT properties and trace inclusion:

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

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

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

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

\[
\text{Traces}(\mathcal{T}_1) \subseteq \text{Traces}(\mathcal{T}_2)
\]

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:

\[
\text{Traces}_{\text{fin}}(\mathcal{T}_1) \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2)
\]

iff for all safety properties \( E: \mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E \)
Safety and finite trace inclusion

\[ \text{Traces}_{\text{fin}}(\mathcal{T}_1) \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2) \]

iff for all safety properties \( E \): \( \mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E \)
Safety and finite trace inclusion

\[ \text{Traces}_{\text{fin}}(\mathcal{T}_1) \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2) \]

iff for all safety properties \( E \):

\[ \mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E \]

Proof “\( \implies \)” : obvious, as for safety property \( E \):

\[ \mathcal{T} \models E \iff \text{Traces}_{\text{fin}}(\mathcal{T}) \cap \text{BadPref} = \emptyset \]
Safety and finite trace inclusion

\[
\text{Traces}_\text{fin}(\mathcal{T}_1) \subseteq \text{Traces}_\text{fin}(\mathcal{T}_2)
\]

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

Proof \( \implies \): obvious, as for safety property \( E \):

\[
\mathcal{T} \models E \iff \text{Traces}_\text{fin}(\mathcal{T}) \cap \text{BadPref} = \emptyset
\]

Hence:

If \( \mathcal{T}_2 \models E \) and \( \text{Traces}_\text{fin}(\mathcal{T}_1) \subseteq \text{Traces}_\text{fin}(\mathcal{T}_2) \) then:
Safety and finite trace inclusion

\[
\text{Traces}_{\text{fin}}(\mathcal{T}_1) \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2)
\]

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

Proof “\( \implies \)” : obvious, as for safety property \( E \):

\[
\mathcal{T} \models E \quad \text{iff} \quad \text{Traces}_{\text{fin}}(\mathcal{T}) \cap \text{BadPref} = \emptyset
\]

Hence:

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

\[
\text{Traces}_{\text{fin}}(\mathcal{T}_1) \cap \text{BadPref} \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2) \cap \text{BadPref} = \emptyset
\]
Safety and finite trace inclusion

\[ \text{Traces}_{\text{fin}}(\mathcal{T}_1) \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2) \]

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

**Proof “\( \implies \)”:** obvious, as for safety property \( E \):

\[ \mathcal{T} \models E \text{ iff } \text{Traces}_{\text{fin}}(\mathcal{T}) \cap \text{BadPref} = \emptyset \]

Hence:

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

\[ \text{Traces}_{\text{fin}}(\mathcal{T}_1) \cap \text{BadPref} \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2) \cap \text{BadPref} = \emptyset \]

and therefore \( \mathcal{T}_1 \models E \)
Safety and finite trace inclusion

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

iff for all safety properties \( E \): \( \mathcal{T}_2 \models E \) \( \Rightarrow \) \( \mathcal{T}_1 \models E \)

**Proof “\( \iff \)”**: consider the LT property

\( E = \text{cl}(\text{Traces}(\mathcal{T}_2)) \)
Safety and finite trace inclusion

\[
\text{Traces}_{\text{fin}}(\mathcal{T}_1) \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2)
\]

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

Proof “\(\iff\)” : consider the LT property

\[
E = \text{cl}(\text{Traces}(\mathcal{T}_2)) = \{ \sigma : \text{pref}(\sigma) \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2) \} 
\]
Safety and finite trace inclusion

\[ \text{Traces}_{\text{fin}}(\mathcal{T}_1) \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2) \]

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

Proof "\( \iff \)" : consider the LT property

\[ E = \text{cl}(\text{Traces}(\mathcal{T}_2)) = \{ \sigma : \text{pref}(\sigma) \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2) \} \]

for each transition system \( \mathcal{T} \):

\[ \text{pref}(\text{Traces}(\mathcal{T})) = \text{Traces}_{\text{fin}}(\mathcal{T}) \]
Safety and finite trace inclusion

\begin{align*}
\text{Traces}_{\text{fin}}(\mathcal{T}_1) & \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2) \\
\text{iff} & \text{ for all safety properties } E: \quad \mathcal{T}_2 \models E \implies \mathcal{T}_1 \models E
\end{align*}

Proof “\(\iff\)” : consider the LT property

\[ E = cl(\text{Traces}(\mathcal{T}_2)) = \{ \sigma : \text{pref}(\sigma) \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2) \} \]

Then, \( E \) is a safety property
Safety and finite trace inclusion

\[ \text{Traces}_{\text{fin}}(T_1) \subseteq \text{Traces}_{\text{fin}}(T_2) \]

iff for all safety properties \( E : T_2 \models E \Rightarrow T_1 \models E \)

Proof “\( \iff \)”: consider the LT property

\[ E = \text{cl}(\text{Traces}(T_2)) = \{ \sigma : \text{pref} (\sigma) \subseteq \text{Traces}_{\text{fin}}(T_2) \} \]

Then, \( E \) is a safety property

as \( \text{cl}(E) = E \)
Safety and finite trace inclusion

\[ \text{Traces}_{\text{fin}}(T_1) \subseteq \text{Traces}_{\text{fin}}(T_2) \]

iff for all safety properties \( E: T_2 \models E \Rightarrow T_1 \models E \)

**Proof “\( \Leftarrow \)”**: consider the LT property

\[ E = \text{cl}(\text{Traces}(T_2)) = \{ \sigma : \text{pref}(\sigma) \subseteq \text{Traces}_{\text{fin}}(T_2) \} \]

Then, \( E \) is a safety property

as \( \text{cl}(E) = E \)

set of bad prefixes: \((2^{AP})^+ \setminus \text{Traces}_{\text{fin}}(T_2)\)
Safety and finite trace inclusion

\[ \text{Traces}_{\text{fin}}(\mathcal{T}_1) \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2) \]

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

Proof “\( \Leftarrow \)” : consider the LT property

\[ E = \text{cl}(\text{Traces}(\mathcal{T}_2)) = \{ \sigma : \text{pref}(\sigma) \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2) \} \]

Then, \( E \) is a safety property and \( \mathcal{T}_2 \models E \).
Safety and finite trace inclusion

\[ \text{Traces}_{\text{fin}}(\mathcal{T}_1) \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2) \]

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

Proof “\( \iff \)” : consider the LT property

\[ E = \text{cl}(\text{Traces}(\mathcal{T}_2)) = \{ \sigma : \text{pref}(\sigma) \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2) \} \]

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

By assumption: \( \mathcal{T}_1 \models E \)
Safety and finite trace inclusion

\[ \text{Traces}_{\text{fin}}(\mathcal{T}_1) \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2) \]

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

Proof “\( \Leftarrow \)”: consider the LT property

\[ E = \text{cl}(\text{Traces}(\mathcal{T}_2)) = \{ \sigma : \text{pref}(\sigma) \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2) \} \]

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

By assumption: \( \mathcal{T}_1 \models E \) and therefore \( \text{Traces}(\mathcal{T}_1) \subseteq E \).
Safety and finite trace inclusion

\[
\text{Traces}_{\text{fin}}(\mathcal{T}_1) \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2)
\]

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

Proof “\(\leftarrow\)” : consider the LT property

\[
E = \text{cl}(\text{Traces}(\mathcal{T}_2)) = \{ \sigma : \text{pref}(\sigma) \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2) \}
\]

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

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

Hence: \( \text{Traces}_{\text{fin}}(\mathcal{T}_1) = \text{pref}(\text{Traces}(\mathcal{T}_1)) \)
Safety and finite trace inclusion

\[ \text{Traces}_{\text{fin}}(\mathcal{T}_1) \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2) \]

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

Proof “\( \iff \)” : consider the LT property

\[ E = \text{cl}(\text{Traces}(\mathcal{T}_2)) = \{ \sigma: \text{pref}(\sigma) \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2) \} \]

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

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

Hence: \( \text{Traces}_{\text{fin}}(\mathcal{T}_1) = \text{pref}(\text{Traces}(\mathcal{T}_1)) \subseteq \text{pref}(E) \)
Safety and finite trace inclusion

\[ \text{Traces}_{\text{fin}}(\mathcal{T}_1) \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2) \]

iff for all safety properties \( E : \mathcal{T}_2 \models E \Rightarrow \mathcal{T}_1 \models E \)

**Proof** “\( \Leftarrow \)” : consider the LT property

\[ E = \text{cl}(\text{Traces}(\mathcal{T}_2)) = \{ \sigma : \text{pref}(\sigma) \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2) \} \]

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

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

Hence:

\[ \text{Traces}_{\text{fin}}(\mathcal{T}_1) = \text{pref}(\text{Traces}(\mathcal{T}_1)) \]

\[ \subseteq \text{pref}(E) = \text{pref}(\text{cl}(\text{Traces}(\mathcal{T}_2))) \]
Safety and finite trace inclusion

\[ \text{Traces}_{\text{fin}}(\mathcal{T}_1) \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2) \]

iff for all safety properties \( E \): \( \mathcal{T}_2 \models E \Rightarrow \mathcal{T}_1 \models E \)

**Proof** “\( \iff \)” : consider the LT property

\[ E = \text{cl}(\text{Traces}(\mathcal{T}_2)) = \{ \sigma : \text{pref}(\sigma) \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}_2) \} \]

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

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

Hence:

\[ \text{Traces}_{\text{fin}}(\mathcal{T}_1) = \text{pref}(\text{Traces}(\mathcal{T}_1)) \]

\[ \subseteq \text{pref}(E) = \text{pref}(\text{cl}(\text{Traces}(\mathcal{T}_2))) \]

\[ = \text{Traces}_{\text{fin}}(\mathcal{T}_2) \]
Safety and finite trace equivalence
Safety and finite trace equivalence

safety properties and finite trace inclusion:

If $T_1$ and $T_2$ are TS over $AP$ then:

$$\text{Traces}_{\text{fin}}(T_1) \subseteq \text{Traces}_{\text{fin}}(T_2)$$

iff for all safety properties $E$: $T_2 \models E \implies T_1 \models E$
Safety and finite trace equivalence

safety properties and finite trace inclusion:

If $T_1$ and $T_2$ are TS over $AP$ then:

$\text{Traces}_{\text{fin}}(T_1) \subseteq \text{Traces}_{\text{fin}}(T_2)$

iff for all safety properties $E$: $T_2 \models E \implies T_1 \models E$

safety properties and finite trace equivalence:

If $T_1$ and $T_2$ are TS over $AP$ then:

$\text{Traces}_{\text{fin}}(T_1) = \text{Traces}_{\text{fin}}(T_2)$

iff $T_1$ and $T_2$ satisfy the same safety properties
trace inclusion

\[ \text{Traces}(\mathcal{T}) \subseteq \text{Traces}(\mathcal{T}') \text{ iff } \]

for all LT properties \( E : \mathcal{T}' \models E \implies \mathcal{T} \models E \)

finite trace inclusion

\[ \text{Traces}_{\text{fin}}(\mathcal{T}) \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}') \text{ iff } \]

for all safety properties \( E : \mathcal{T}' \models E \implies \mathcal{T} \models E \)
trace equivalence

\[ \text{Traces}(T) = \text{Traces}(T') \text{ iff } T \text{ and } T' \text{ satisfy the same LT properties} \]

finite trace equivalence

\[ \text{Traces}_{\text{fin}}(T) = \text{Traces}_{\text{fin}}(T') \text{ iff } T \text{ and } T' \text{ satisfy the same safety properties} \]
correct or wrong?

If \( \text{Traces}(T) \subseteq \text{Traces}(T') \)
then \( \text{Traces}_{\text{fin}}(T) \subseteq \text{Traces}_{\text{fin}}(T') \).
correct or wrong?

If \( \text{Traces}(T) \subseteq \text{Traces}(T') \)
then \( \text{Traces}_{\text{fin}}(T) \subseteq \text{Traces}_{\text{fin}}(T') \).

**correct**, since

\[
\text{Traces}_{\text{fin}}(T) = \text{set of all finite nonempty prefixes of words in } \text{Traces}(T)
\]
\[
= \text{pref}(\text{Traces}(T))
\]
correct or wrong?

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

correct, since

$\text{Traces}_{\text{fin}}(T) = \text{set of all finite nonempty prefixes of words in } \text{Traces}(T)$

$= \text{pref} (\text{Traces}(T))$

$\text{Traces}(T) = \{{}\{a\}^\omega\}$

$\text{Traces}_{\text{fin}}(T) = \{{}\{a\}^n : n \geq 1\}$
Finite trace relations versus trace relations

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

answer: no
Finite trace relations versus trace relations

\[ \mathcal{T} \]

\[ \mathcal{T}' \]

set of propositions

\[ AP = \{ b \} \]
Finite trace relations versus trace relations

\[ \mathcal{T} \]

\[ \mathcal{T}' \]

\[ \text{Traces}(\mathcal{T}) = \{ \emptyset^\omega \} \]

set of propositions

\[ AP = \{ b \} \]
Finite trace relations versus trace relations

\[ \mathcal{T} \]

\( \mathcal{T}' \)

\( \text{Traces}(\mathcal{T}) = \{\emptyset^\omega\} \)

\( \text{Traces}_{\text{fin}}(\mathcal{T}) = \{\emptyset^n : n \geq 0\} \)

\( \hat{\mathcal{T}} = \emptyset \)

\( \hat{\mathcal{T}}' = \{b\} \)

set of propositions

\( \text{AP} = \{b\} \)
Finite trace relations versus trace relations

\[ \mathcal{T} \quad \rightarrow \quad \mathcal{T}' \]

\[
\begin{align*}
\text{Traces}(\mathcal{T}) &= \{ \emptyset^\omega \} \\
\text{Traces}_{\text{fin}}(\mathcal{T}) &= \{ \emptyset^n : n \geq 0 \} \\
\text{Traces}(\mathcal{T}') &= \{ \emptyset^n \{b\}^\omega : n \geq 2 \}
\end{align*}
\]

set of propositions

\[ AP = \{ b \} \]
Finite trace relations versus trace relations

\[
\text{Traces}(T) = \{\emptyset^\omega\}
\]

\[
\text{Traces}_{\text{fin}}(T) = \{\emptyset^n : n \geq 0\}
\]

\[
\text{Traces}(T') = \{\emptyset^n\{b\}^\omega : n \geq 2\}
\]

\[
\text{Traces}_{\text{fin}}(T') = \{\emptyset^n : n \geq 0\} \cup \{\emptyset^n\{b\}^m : n \geq 2 \land m \geq 1\}
\]
Finite trace relations versus trace relations

\[ \text{Traces}(T) = \{ \emptyset^\omega \} \]
\[ \text{Traces}_{\text{fin}}(T) = \{ \emptyset^n : n \geq 0 \} \]
\[ \text{Traces}(T') = \{ \emptyset^n \{b\}^\omega : n \geq 2 \} \]
\[ \text{Traces}_{\text{fin}}(T') = \{ \emptyset^n : n \geq 0 \} \cup \{ \emptyset^n \{b\}^m : n \geq 2 \land m \geq 1 \} \]

\[ \text{Traces}(T) \nsubseteq \text{Traces}(T') \], but
\[ \text{Traces}_{\text{fin}}(T) \subseteq \text{Traces}_{\text{fin}}(T') \]
Finite trace relations versus trace relations

\( \text{Traces}(T) \subseteq \{\emptyset^\omega\} \)

\( \text{Traces}_{\text{fin}}(T) = \{\emptyset^n : n \geq 0\} \)

\( \text{Traces}(T') = \{\emptyset^n\{b\}^\omega : n \geq 2\} \)

\( \text{Traces}_{\text{fin}}(T') = \{\emptyset^n : n \geq 0\} \cup \{\emptyset^n\{b\}^m : n \geq 2 \land m \geq 1\} \)

\( \text{Traces}(T) \not\subseteq \text{Traces}(T') \), but

\( \text{Traces}_{\text{fin}}(T) \subseteq \text{Traces}_{\text{fin}}(T') \)

LT property

\( E \equiv \text{“eventually } b\text{”} \)

\( T \not\models E, \quad T' \models E \)
Finite trace and trace inclusion

Suppose that $T$ and $T'$ are TS over $AP$ such that

(1) $T$ has no terminal states,

(2) $T'$ is finite.
Suppose that $\mathcal{T}$ and $\mathcal{T}'$ are TS over $\mathcal{AP}$ such that

1. $\mathcal{T}$ has no terminal states, i.e., all paths of $\mathcal{T}$ are infinite
2. $\mathcal{T}'$ is finite.
Suppose that $T$ and $T'$ are TS over $AP$ such that

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

(2) $T'$ is finite.

Then:

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

iff

$$
\text{Traces}_{\text{fin}}(T) \subseteq \text{Traces}_{\text{fin}}(T')
$$
Finite trace and trace inclusion

Suppose that $T$ and $T'$ are TS over $AP$ such that

1. $T$ has no terminal states, i.e., all paths of $T$ are infinite
2. $T'$ is finite.

Then:

\[ \text{Traces}(T) \subseteq \text{Traces}(T') \]

iff

\[ \text{Traces}_{\text{fin}}(T) \subseteq \text{Traces}_{\text{fin}}(T') \]

“$\implies$” holds for all transition systems, no matter whether (1) and (2) hold.
Finite trace and trace inclusion

Suppose that $T$ and $T'$ are TS over $AP$ such that

1. $T$ has no terminal states, i.e., all paths of $T$ are infinite
2. $T'$ is finite.

Then:

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

iff

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

“$\Rightarrow$” holds for all transition systems

“$\Leftarrow$”: suppose that (1) and (2) hold and that

3. $\text{Traces}_{\text{fin}}(T) \subseteq \text{Traces}_{\text{fin}}(T')$

Show that $\text{Traces}(T) \subseteq \text{Traces}(T')$
Suppose that $T$ and $T'$ are TS over $AP$ such that

1. $T$ has no terminal states
2. $T'$ is finite
3. $\text{Traces}_{\text{fin}}(T) \subseteq \text{Traces}_{\text{fin}}(T')$

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

*Proof:*
Finite trace and trace inclusion

Suppose that $T$ and $T'$ are TS over $AP$ such that

1. $T$ has no terminal states
2. $T'$ is finite
3. $\text{Traces}_{\text{fin}}(T) \subseteq \text{Traces}_{\text{fin}}(T')$

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

Proof: Pick some path $\pi = s_0 s_1 s_2 \ldots$ in $T$ and show that there exists a path $\pi' = t_0 t_1 t_2 \ldots$ in $T'$ such that $\text{trace}(\pi) = \text{trace}(\pi')$
finite TS $\mathcal{T}'$

paths from state $t_0$
(unfolded into a tree)
Traces fin versus traces

finite TS $T'$
paths from state $t_0$
(unfolded into a tree)

finite until depth $\leq n$
Traces fin 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 $\leq n$
Traces in 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 $\leq n$
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
$t_n s_{n+1}^{m} \ldots s_{m}^{m}$
Traces fin 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: $t_0 t_1 \ldots t_n$

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

there exists $t_{n+1} \in \text{Post}(t_n)$
s.t. $t_{n+1} = s_{n+1}^m$ for
infinitely many $m$
Finite trace and trace inclusion

Suppose that \( T \) and \( T' \) are TS over \( AP \) such that

1. \( T \) has no terminal states
2. \( T' \) is finite
3. \( \text{Traces}_{\text{fin}}(T) \subseteq \text{Traces}_{\text{fin}}(T') \)

Then \( \text{Traces}(T) \subseteq \text{Traces}(T') \)

image-finiteness is sufficient
Finite trace and trace inclusion

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

1. $\mathcal{T}$ has no terminal states
2. $\mathcal{T}'$ is finite
3. $\text{Traces}_{\text{fin}}(\mathcal{T}) \subseteq \text{Traces}_{\text{fin}}(\mathcal{T}')$

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

image-finiteness of $\mathcal{T}' = (S', \text{Act}, \rightarrow, S'_0, \mathit{AP}, L')$: 
Finite trace and trace inclusion

Suppose that $T$ and $T'$ are TS over $AP$ such that

1. $T$ has no terminal states
2. $T'$ is finite
3. $\text{Traces}_{\text{fin}}(T) \subseteq \text{Traces}_{\text{fin}}(T')$

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

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

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

  $\{ t \in \text{Post}(s) : L'(t) = A \}$ is finite
Finite trace and trace inclusion

Suppose that $T$ and $T'$ are TS over $AP$ such that

1. $T$ has no terminal states
2. $T'$ is finite
3. $\text{Traces}_{\text{fin}}(T) \subseteq \text{Traces}_{\text{fin}}(T')$

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

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

- for each $A \in 2^{AP}$ and state $s \in S'$:
  \[ \{ t \in \text{Post}(s) : L'(t) = A \} \text{ is finite} \]
- for each $A \in 2^{AP}$:
  \[ \{ s_0 \in S'_0 : L'(s_0) = A \} \text{ is finite} \]
Whenever $\text{Traces}(T) = \text{Traces}(T')$ then $\text{Traces}_{\text{fin}}(T) = \text{Traces}_{\text{fin}}(T')$
Trace equivalence vs. finite trace equivalence

Whenever \( \text{Traces}(T) = \text{Traces}(T') \) then

\[
\text{Traces}_{\text{fin}}(T) = \text{Traces}_{\text{fin}}(T')
\]

while the reverse direction does not hold in general (even not for finite transition systems)
Whenever \( \text{Traces}(T) = \text{Traces}(T') \) then
\[
\text{Traces}_{\text{fin}}(T) = \text{Traces}_{\text{fin}}(T')
\]
while the reverse direction does not hold in general
(even not for finite transition systems)
Trace equivalence vs. finite trace equivalence

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

while the reverse direction does not hold in general (even not for finite transition systems)

finite trace equivalent, but not trace equivalent
Whenever $\text{Traces}(\mathcal{T}) = \text{Traces}(\mathcal{T}')$ then

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

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 $\text{AP}$-deterministic
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
“liveness: something good will happen.”

“event \( a \) will occur eventually”

e.g., termination for sequential programs

“event \( a \) will occur infinitely many times”

e.g., starvation freedom for dining philosophers

“whenever event \( b \) occurs then event \( a \) will occur sometimes in the future”

e.g., every waiting process enters eventually its critical section
● Each philosopher thinks infinitely often.
• Each philosopher thinks infinitely often.
which property type?

- Each philosopher thinks infinitely often.
- Two philosophers next to each other never eat at the same time.
Each philosopher thinks infinitely often.

Two philosophers next to each other never eat at the same time.
Each philosopher thinks infinitely often. 

Two philosophers next to each other never eat at the same time.

Whenever a philosopher eats then he has been thinking at some time before.
Each philosopher thinks infinitely often.  \- liveness
Two philosophers next to each other never eat at the same time. \- invariant
Whenever a philosopher eats then he has been thinking at some time before. \- safety
Each philosopher thinks infinitely often.

Two philosophers next to each other never eat at the same time.

Whenever a philosopher eats then he has been thinking at some time before.

Whenever a philosopher eats then he will think some time afterwards.
Each philosopher thinks infinitely often.

Two philosophers next to each other never eat at the same time.

Whenever a philosopher eats then he has been thinking at some time before.

Whenever a philosopher eats then he will think some time afterwards.
Each philosopher thinks infinitely often.

Two philosophers next to each other never eat at the same time.

Whenever a philosopher eats then he has been thinking at some time before.

Whenever a philosopher eats then he will think some time afterwards.

Between two eating phases of philosopher $i$ lies at least one eating phase of philosopher $i+1$. 

Liveness

Invariant

Safety
which property type?

- Each philosopher thinks infinitely often.  
  \textit{liveness}

- Two philosophers next to each other never eat at the same time.  
  \textit{invariant}

- Whenever a philosopher eats then he has been thinking at some time before.  
  \textit{safety}

- Whenever a philosopher eats then he will think some time afterwards.  
  \textit{liveness}

- Between two eating phases of philosopher $i$ lies at least one eating phase of philosopher $i+1$.  
  \textit{safety}
many different formal definitions of liveness have been suggested in the literature
many different formal definitions of liveness have been suggested in the literature

*here:* one just example for a formal definition of liveness
Definition of liveness properties
Definition of liveness properties

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

$E$ is called a liveness property if each finite word over $AP$ can be extended to an infinite word in $E$. 
Definition of liveness properties

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

$E$ is called a liveness property if each finite word over $AP$ can be extended to an infinite word in $E$, i.e., if

$$\text{pref}(E) = (2^{AP})^+$$

recall: $\text{pref}(E) =$ set of all finite, nonempty prefixes of words in $E$
Definition of liveness properties

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

$E$ is called a liveness property if each finite word over $AP$ can be extended to an infinite word in $E$, i.e., if

$$\text{pref}(E) = (2^{AP})^+$$

Examples:

- each process will eventually enter its critical section
- each process will enter its critical section infinitely often
- whenever a process has requested its critical section then it will eventually enter its critical section
An LT property $E$ over $AP$ is called a liveness property if $\text{pref}(E) = (2^{AP})^+$

Examples for $AP = \{\text{crit}_i : i = 1, \ldots, n\}$:
Examples for liveness properties

An LT property $E$ over $AP$ is called a liveness property if $\text{pref}(E) = (2^{AP})^+$

Examples for $AP = \{\text{crit}_i : i = 1, \ldots, n\}$:

- each process will eventually enter its critical section
Examples for liveness properties

An LT property $E$ over $AP$ is called a liveness property if $\text{pref}(E) = (2^{2AP})^+$

Examples for $AP = \{\text{crit}_i : i = 1, \ldots, n\}$:
- each process will eventually enter its critical section

$E$ = set of all infinite words $A_0A_1A_2\ldots$ s.t.

$\forall i \in \{1, \ldots, n\} \ \exists k \geq 0. \ \text{crit}_i \in A_k$
Examples for liveness properties

An LT property $E$ over $AP$ is called a liveness property if

$\text{pref}(E) = (2^{AP})^+$

Examples for $AP = \{\text{crit}_i : i = 1, \ldots, n\}$:

- each process will eventually enter its critical section
- each process will enter its critical section infinitely often
Examples for liveness properties

An LT property $E$ over $AP$ is called a liveness property if $\text{pref}(E) = (2^{\text{AP}})^+$

Examples for $AP = \{\text{crit}_i : i = 1, \ldots, n\}$:

- each process will eventually enter its critical section
- each process will enter its critical section infinitely often

$E = \text{set of all infinite words } A_0 A_1 A_2 \ldots \text{ s.t. }$

$\forall i \in \{1, \ldots, n\} \exists k \geq 0. \text{crit}_i \in A_k$
Examples for liveness properties

An LT property $E$ over $AP$ is called a liveness property if $\text{pref}(E) = (2^{\text{AP}})^+$

Examples for $AP = \{\text{wait}_i, \text{crit}_i : i = 1, \ldots, n\}$:

- each process will eventually enter its critical section
- each process will enter its crit. section \(\text{inf. often}\)
- whenever a process is waiting then it will eventually enter its critical section
Examples for liveness properties

An LT property $E$ over $AP$ is called a liveness property if $\text{pref}(E) = (2^{\text{AP}})^+$

Examples for $AP = \{\text{wait}_i, \text{crit}_i : i = 1, \ldots, n\}$:

- each process will eventually enter its critical section
- each process will enter its crit. section inf. often
- whenever a process is waiting then it will eventually enter its critical section

$E = \text{set of all infinite words } A_0 A_1 A_2 \ldots \text{ s.t. }$

\[
\forall i \in \{1, \ldots, n\} \forall j \geq 0. \text{ wait}_i \in A_j \quad \rightarrow \quad \exists k > j. \text{ crit}_i \in A_k
\]
Let $E$ be an LT-property, i.e., $E \subseteq (2^{\mathcal{AP}})^\omega$
Recall: safety properties, prefix closure

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

$E$ is a safety property

iff \[ \forall \sigma \in (2^\mathcal{AP})^\omega \setminus E \ \exists A_0 A_1 \ldots A_n \in \text{pref}(\sigma) \ \text{s.t.} \]

\[ \{ \sigma' \in E : A_0 A_1 \ldots A_n \in \text{pref}(\sigma') \} = \emptyset \]
Recall: safety properties, prefix closure

Let \( E \) be an LT-property, i.e., \( E \subseteq (2^{AP})^\omega \)

\[ E \text{ is a safety property} \]

\[ \text{iff } \forall \sigma \in (2^{AP})^\omega \setminus E \exists A_0 A_1 \ldots A_n \in \text{pref} (\sigma) \text{ s.t.} \]

\[ \{ \sigma' \in E : A_0 A_1 \ldots A_n \in \text{pref} (\sigma') \} = \emptyset \]

remind:

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

\[ \text{pref}(E) = \bigcup_{\sigma \in E} \text{pref}(\sigma) \]
Recall: safety properties, prefix closure

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

$E$ is a safety property

iff $\forall \sigma \in (2^\text{AP})^\omega \setminus E \\exists A_0 A_1 \ldots A_n \in \text{pref}(\sigma)$ s.t.

$$\left\{ \sigma' \in E : A_0 A_1 \ldots A_n \in \text{pref}(\sigma') \right\} = \emptyset$$

iff $\text{cl}(E) = E$

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

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

$\text{pref}(E) = \bigcup_{\sigma \in E} \text{pref}(\sigma)$
Decomposition theorem
Decomposition theorem

For each LT-property $E$, there exists a safety property $SAFE$ and a liveness property $LIVE$ s.t.

$$E = SAFE \cap LIVE$$
Decomposition theorem

For each LT-property $E$, there exists a safety property $SAFE$ and a liveness property $LIVE$ s.t.

$$E \ = \ SAFE \cap LIVE$$

Proof:
Decomposition theorem

For each LT-property $E$, there exists a safety property $\text{SAFE}$ and a liveness property $\text{LIVE}$ s.t.

$$E = \text{SAFE} \cap \text{LIVE}$$

Proof: Let $\text{SAFE} \overset{\text{def}}{=} cl(E)$
Decomposition theorem

For each LT-property $E$, there exists a safety property $SAFE$ and a liveness property $LIVE$ s.t.

$$E = SAFE \cap LIVE$$

Proof: Let $SAFE \overset{\text{def}}{=} cl(E)$

\[cl(E) = \{ \sigma \in (2^AP)^\omega : \text{pref}(\sigma) \subseteq \text{pref}(E) \}\]

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

$\text{pref}(E) = \bigcup_{\sigma \in E} \text{pref}(\sigma)$
Decomposition theorem

For each LT-property $E$, there exists a safety property $SAFE$ and a liveness property $LIVE$ s.t.

$$E = SAFE \cap LIVE$$

**Proof:** Let $SAFE \overset{\text{def}}{=} cl(E)$

$$LIVE \overset{\text{def}}{=} E \cup \left( (2^{AP})^\omega \setminus cl(E) \right)$$

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

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

$\text{pref}(E) = \bigcup_{\sigma \in E} \text{pref}(\sigma)$
Decomposition theorem

For each LT-property \( E \), there exists a safety property \( \text{SAFE} \) and a liveness property \( \text{LIVE} \) s.t.

\[
E = \text{SAFE} \cap \text{LIVE}
\]

**Proof:** Let \( \text{SAFE} \) \( \overset{\text{def}}{=} \) \( \text{cl}(E) \)

\( \text{LIVE} \) \( \overset{\text{def}}{=} \) \( E \cup \left( (2^{\text{AP}})^\omega \setminus \text{cl}(E) \right) \)

Show that:

- \( E = \text{SAFE} \cap \text{LIVE} \)
- \( \text{SAFE} \) is a safety property
- \( \text{LIVE} \) is a liveness property
Decomposition theorem

For each LT-property $E$, there exists a safety property $\textit{SAFE}$ and a liveness property $\textit{LIVE}$ s.t.

$$E = \textit{SAFE} \cap \textit{LIVE}$$

Proof: Let

\begin{align*}
\textit{SAFE} & \overset{\text{def}}{=} cl(E) \\
\textit{LIVE} & \overset{\text{def}}{=} E \cup ( (2^{AP})^\omega \setminus cl(E) )
\end{align*}

Show that:

- $E = \textit{SAFE} \cap \textit{LIVE}$ \checkmark
- $\textit{SAFE}$ is a safety property
- $\textit{LIVE}$ is a liveness property
For each LT-property $E$, there exists a safety property $SAFE$ and a liveness property $LIVE$ s.t.

$$E = SAFE \cap LIVE$$

### Proof:
Let $SAFE \overset{\text{def}}{=} cl(E)$

$LIVE \overset{\text{def}}{=} E \cup (\left((2^{AP})^\omega \ \backslash \ cl(E)\right))$

Show that:

- $E = SAFE \cap LIVE \quad \checkmark$
- $SAFE$ is a safety property as $cl(SAFE) = SAFE$
- $LIVE$ is a liveness property
Decomposition theorem

For each LT-property $E$, there exists a safety property $SAFE$ and a liveness property $LIVE$ s.t.

$$E = SAFE \cap LIVE$$

Proof: Let $SAFE \overset{\text{def}}{=} cl(E)$

$$LIVE \overset{\text{def}}{=} E \cup \left( (2^{AP})^\omega \setminus cl(E) \right)$$

Show that:

- $E = SAFE \cap LIVE$ \checkmark
- $SAFE$ is a safety property as $cl(SAFE) = SAFE$
- $LIVE$ is a liveness property, i.e., $pref(LIVE) = (2^{AP})^+$
Which LT properties are both a safety and a liveness property?
Being safe and live

Which LT properties are both a safety and a liveness property?

**answer:** The set \((2^{AP})^\omega\) is the only LT property which is a safety property and a liveness property.
Which LT properties are both a safety and a liveness property?

**Answer:** The set \((2^{AP})^\omega\) is the only LT property which is a safety property and a liveness property.

- \((2^{AP})^\omega\) is a safety and a liveness property: √
Which LT properties are both a safety and a liveness property?

**answer:** The set $\left(2^{AP}\right)^\omega$ is the only LT property which is a safety property and a liveness property.

- $\left(2^{AP}\right)^\omega$ is a safety and a liveness property: ✔
- If $E$ is a liveness property then $\text{pref}(E) = \left(2^{AP}\right)^+$
Which LT properties are both a safety and a liveness property?

**Answer:** The set $(2^{AP})^\omega$ is the only LT property which is a safety property and a liveness property.

- $(2^{AP})^\omega$ is a safety and a liveness property: ✓
- If $E$ is a liveness property then
  
  $\text{pref}(E) = (2^{AP})^+$
  
  $\implies \text{cl}(E) = (2^{AP})^\omega$
answer: The set \((2^{AP})^\omega\) is the only LT property which is a safety property and a liveness property.

- \((2^{AP})^\omega\) is a safety and a liveness property: √
- If \(E\) is a liveness property then
  \[
  \text{pref}(E) = (2^{AP})^+
  \]
  \[
  \implies \text{cl}(E) = (2^{AP})^\omega
  \]
  If \(E\) is a safety property too, then \(\text{cl}(E) = E\).
Being safe and live

Which LT properties are both a safety and a liveness property?

answer: The set \((2^{AP})^\omega\) is the only LT property which is a safety property and a liveness property.

- \((2^{AP})^\omega\) is a safety and a liveness property: \(\surd\)
- If \(E\) is a liveness property then
  
  \[
  \text{pref}(E) = (2^{AP})^+
  \]

  \[\implies cl(E) = (2^{AP})^\omega\]

If \(E\) is a safety property too, then \(cl(E) = E\).
Hence \(E = cl(E) = (2^{AP})^\omega\).