Principles of Abstract Interpretation

MIT press

Ch. **14**, Safety and Liveness Trace Properties

Patrick Cousot

pcousot.github.io

PrAbsInt@gmail.com   github.com/PrAbsInt/

These slides are available at
http://github.com/PrAbsInt/slides/slides/slides-14--safety-liveness-PrAbsInt.pdf

Chapter 14

Ch. **14**, Safety and Liveness Trace Properties

A reminder on trace semantics properties

Trace semantics properties

- We have defined the (prefix or maximal) trace semantics as
$$\mathcal{S} \in \mathbb{T}^+ \to \mathbb{T}^{+\infty}$$
since for a given prelude $\pi_0 \in \mathbb{T}^+$, our language has only one continuation $\pi = \mathcal{S}(\pi_0)$
- For a non-deterministic language, we would have
$$\mathcal{S} \in \mathbb{T}^+ \to \wp(\mathbb{T}^{+\infty})$$
- Up to an isomorphism, this is
$$\mathcal{S} \in \wp(\mathbb{T}^+ \times \mathbb{T}^{+\infty})$$
where $\mathcal{S}$ is understood as $\{\langle\pi_0, \pi\rangle \in \mathbb{T}^+ \times \mathbb{T}^{+\infty} \mid \pi \in S(\pi_0)\} \in \wp(\mathbb{T}^+ \times \mathbb{T}^{+\infty})$
- Semantics properties belong to $\wp(\wp(\mathbb{T}^+ \times \mathbb{T}^{+\infty}))$
- Their abstractions by the join abstraction $\alpha^{\mathbb{T}}$ in Section **8.6** are trace properties in $\wp(\mathbb{T}^+ \times \mathbb{T}^{+\infty})$

Safety

Intuition for safety

- Safety properties S of programs are trace properties so $S \in \wp(\mathbb{T}^+ \times \mathbb{T}^{+\infty})$
- The characteristics of a safety property S is that
  "any program execution $\langle \pi_0, \pi \rangle \in \mathcal{S}^{+\infty}[\![\mathsf{P}]\!]$ *(where* $\pi_0 \in \mathbb{T}^+$ *and* $\pi \in \mathbb{T}^{+\infty}$*) that violates* S *has a finite prefix* $\langle \pi_0, \pi' \rangle$ *that violates* S*"*
- runtime checkable, "Nothing bad can happen"

en.wikipedia.org/wiki/Safety_property

Prefix closure

Define the *prefix closure* $\alpha_{\mathsf{pref}}(\Pi)$ of a set of executions (that is of trace properties $\Pi \in \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty})$) as taking all (finite and infinite) prefixes of traces in Π.

$$
\begin{array}{rcll}
\pi \lesssim \pi' & \triangleq & \exists \pi'' \in \mathbb{T}^{*\infty} \,.\, \pi \mathbin{\frown} \pi'' = \pi' & \text{prefix ordering} \qquad (14.3)\\
\pi < \pi' & \triangleq & \pi \lesssim \pi' \wedge \pi \neq \pi' & \text{strict prefix ordering}\\
\langle \pi_0,\, \pi \rangle \lesssim \langle \pi_0',\, \pi' \rangle & \triangleq & \pi_0 = \pi_0' \wedge \pi \lesssim \pi' & \text{extension to executions}
\end{array}
$$

$$
\begin{array}{rcll}
\alpha_{\mathsf{pref}} & \in & \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty}) \mapsto \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty}) & \text{prefix closure}\\
\alpha_{\mathsf{pref}}(\Pi) & \triangleq & \{\langle \pi_0,\, \pi \rangle \in \mathbb{T}^{+} \times \mathbb{T}^{+\infty} \mid \exists \pi' \in \mathbb{T}^{+\infty} \,.\, \langle \pi_0,\, \pi' \rangle \in \Pi \,.\, \pi \lesssim \pi' \} & (14.4)
\end{array}
$$

Prefix closure

Define the *prefix closure* $\alpha_{\mathsf{pref}}(\Pi)$ of a set of executions (that is of trace properties $\Pi \in \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty})$) as taking all (finite and infinite) prefixes of traces in Π.

$$
\begin{array}{rcll}
\pi \preceq \pi' & \triangleq & \exists \pi'' \in \mathbb{T}^{*\infty} \,.\, \pi \frown \pi'' = \pi' & \text{prefix ordering} \qquad (14.3)\\
\pi \prec \pi' & \triangleq & \pi \preceq \pi' \wedge \pi \neq \pi' & \text{strict prefix ordering}\\
\langle \pi_0,\, \pi \rangle \preceq \langle \pi_0',\, \pi' \rangle & \triangleq & \pi_0 = \pi_0' \wedge \pi \preceq \pi' & \text{extension to executions}
\end{array}
$$

$$
\begin{array}{rcll}
\alpha_{\mathsf{pref}} & \in & \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty}) \mapsto \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty}) & \text{prefix closure}\\
\alpha_{\mathsf{pref}}(\Pi) & \triangleq & \{\langle \pi_0,\, \pi \rangle \in \mathbb{T}^{+} \times \mathbb{T}^{+\infty} \mid \exists \pi' \in \mathbb{T}^{+\infty} \,.\, \langle \pi_0,\, \pi' \rangle \in \Pi \,.\, \pi \preceq \pi' \} & (14.4)
\end{array}
$$

Theorem α_{pref} is a topological closure on $\wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty})$.

Limit closure

Define the *limit closure* $\alpha_{\mathsf{limit}}(\Pi)$ of a set of traces (that is on trace properties Π) as taking all infinite traces which prefixes are in Π.

$$\begin{array}{rcl}\alpha_{\mathsf{limit}} & \in & \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty}) \mapsto \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty}) \\ \alpha_{\mathsf{limit}}(\Pi) & \triangleq & \Pi \cup \{\langle \pi_0,\, \pi\rangle \in \mathbb{T}^{+} \times \mathbb{T}^{\infty} \mid \forall \pi' \lessdot \pi \,.\, \langle \pi_0,\, \pi'\rangle \in \Pi\}\end{array}$$

limit closure

Limit closure

Define the *limit closure* $\alpha_{\text{limit}}(\Pi)$ of a set of traces (that is on trace properties Π) as taking all infinite traces which prefixes are in Π.

$$\begin{array}{rcll}\alpha_{\text{limit}} & \in & \wp(\mathbb{T}^+ \times \mathbb{T}^{+\infty}) \mapsto \wp(\mathbb{T}^+ \times \mathbb{T}^{+\infty}) & \text{limit closure}\\ \alpha_{\text{limit}}(\Pi) & \triangleq & \Pi \cup \{\langle \pi_0,\ \pi\rangle \in \mathbb{T}^+ \times \mathbb{T}^{\infty} \mid \forall \pi' \lessdot \pi \mathrel{.} \langle \pi_0,\ \pi'\rangle \in \Pi\} & \end{array}$$

Theorem α_{limit} is a topological closure on $\wp(\mathbb{T}^+ \times \mathbb{T}^{+\infty})$.

Safety closure

Define the *safety closure* α_{safety} on sets of traces (that is on trace properties $\Pi \in \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty})$) such that $\alpha_{\text{safety}}(\Pi)$ is the set of limits of prefixes of Π.

$$
\begin{array}{rcl}
\alpha_{\text{safety}} & \in & \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty}) \mapsto \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty}) \\
\alpha_{\text{safety}} & \triangleq & \alpha_{\text{limit}} \circ \alpha_{\text{pref}}
\end{array} \tag{14.8}
$$

Safety closure

Define the *safety closure* α_{safety} on sets of traces (that is on trace properties $\Pi \in \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty})$) such that $\alpha_{\mathsf{safety}}(\Pi)$ is the set of limits of prefixes of Π.

$$\begin{array}{rcl}
\alpha_{\mathsf{safety}} & \in & \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty}) \mapsto \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty}) \\
\alpha_{\mathsf{safety}} & \triangleq & \alpha_{\mathsf{limit}} \circ \alpha_{\mathsf{pref}}
\end{array} \tag{14.8}$$

Theorem 14.10 α_{safety} is a topological closure on $\wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty})$.

Proof Composition of topological closures. □

Safety properties

Definition 14.11 The *safety properties* are the trace properties $P \in \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty})$ such that $\alpha_{\mathsf{safety}}(P) = P$. $\square$

Safety properties

Definition 14.11 The *safety properties* are the trace properties $P \in \wp(\mathbb{T}^+ \times \mathbb{T}^{+\infty})$ such that $\alpha_{\text{safety}}(P) = P$. $\square$

Theorem The safety properties are the closed sets of the topology defined by α_{safety} on $\mathbb{T}^+ \times \mathbb{T}^{+\infty}$.

Safety properties

Definition 14.11 The *safety properties* are the trace properties $P \in \wp(\mathbb{T}^+ \times \mathbb{T}^{+\infty})$ such that $\alpha_{\text{safety}}(P) = P$. $\square$

Theorem The safety properties are the closed sets of the topology defined by α_{safety} on $\mathbb{T}^+ \times \mathbb{T}^{+\infty}$.

Theorem 14.15 The poset $\langle \alpha_{\text{safety}}(\wp(\mathbb{T}^+ \times \mathbb{T}^{+\infty})), \subseteq \rangle$ (*i.e.* the post-image of $\wp(\mathbb{T}^+ \times \mathbb{T}^{+\infty})$ by α_{safety}) of safety properties is a complete lattice.

Runtime checks of safety violation

Theorem 14.20 If $\alpha_{\mathsf{safety}}(\Pi) = \Pi$ then $\forall \langle \pi_0, \pi \rangle \notin \Pi \,.\, \exists \pi' \in \mathbb{T}^+ \,.\, \langle \pi_0, \pi' \rangle \preceq \langle \pi_0, \pi \rangle \wedge \langle \pi_0, \pi' \rangle \notin \Pi$

This explains the common explanation of safety as "nothing bad can happen".

Runtime checks of safety violation

Theorem 14.20 If $\alpha_{\text{safety}}(\Pi) = \Pi$ then $\forall \langle \pi_0, \pi\rangle \notin \Pi \,.\, \exists \pi' \in \mathbb{T}^+ \,.\, \langle \pi_0, \pi'\rangle \preceq \langle \pi_0, \pi\rangle \wedge \langle \pi_0, \pi'\rangle \notin \Pi$

Proof — If $\pi \in \mathbb{T}^+$ then choosing $\pi' = \pi$, we have $\langle \pi_0, \pi'\rangle \preceq \langle \pi_0, \pi\rangle$ by reflexivity of $\preceq$ and $\langle \pi_0, \pi'\rangle \notin \Pi$ by hypothesis.

— Otherwise, $\pi \in \mathbb{T}^\infty$. For all $\langle \pi_0, \pi'\rangle \prec \langle \pi_0, \pi\rangle$, $\pi' \in \mathbb{T}^+$ and $\langle \pi_0, \pi'\rangle \in \Pi$ by prefix closure.

— Therefore $\langle \pi_0, \pi\rangle \in \{\langle \pi_0, \pi\rangle \in \mathbb{T}^+ \times \mathbb{T}^\infty \mid \forall \langle \pi_0, \pi'\rangle \prec \langle \pi_0, \pi\rangle \,.\, \langle \pi_0, \pi'\rangle \in \Pi\} \subseteq \alpha_{\text{limit}}(\Pi) = \alpha_{\text{limit}}(\alpha_{\text{safety}}(\Pi)) = \alpha_{\text{limit}}(\alpha_{\text{limit}} \circ \alpha_{\text{pref}}(\Pi)) = \alpha_{\text{limit}} \circ \alpha_{\text{pref}}(\Pi) = \alpha_{\text{safety}}(\Pi) = \Pi$ since α_{limit} is idempotent.

— We proved $\forall \pi_0 \in \mathbb{T}^+, \pi \in \mathbb{T}^\infty \,.\, ((\forall \pi' \in \mathbb{T}^{+\infty} \,.\, \langle \pi_0, \pi'\rangle \preceq \langle \pi_0, \pi\rangle) \Rightarrow (\langle \pi_0, \pi'\rangle \in \Pi))$ implies $\langle \pi_0, \pi\rangle \in \Pi$ and so by contraposition, $\langle \pi_0, \pi\rangle \notin \Pi$ implies $\exists \pi' \in \mathbb{T}^{+\infty} \,.\, (\langle \pi_0, \pi'\rangle \preceq \langle \pi_0, \pi\rangle) \wedge (\langle \pi_0, \pi'\rangle \notin \Pi)$. $\square$

Liveness

Liveness properties

Definition 14.26 The *liveness properties* are the dense sets of the topology defined by α_{safety}
(hence, by Lemma 13.11, such that $\text{live}(P) = P$ where $\text{live}(P) \triangleq \neg\alpha_{\text{safety}}(P) \cup P$. $\square$

live is extensive and idempotent but not increasing to that $\text{live}(P)$ need not be the least liveness property implied by P

en.wikipedia.org/wiki/Liveness

Liveness properties

By 14.26, the *liveness properties* are characterized by $\text{live}(P) = P$ where $\text{live}(P) \triangleq \neg\alpha_{\text{safety}}(P) \cup P$.

Theorem 14.27 $P \in \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty})$ is a liveness property if and only if $\neg P \subseteq \alpha_{\text{safety}}(P)$.

Proof

$$
\begin{array}{lll}
 & \text{live}(P) = P & \\
\Leftrightarrow & \neg\alpha_{\text{safety}}(P) \cup P = P & \wr \text{Definition 14.26 of live}(P) \int \\
\Leftrightarrow & \neg(\neg\alpha_{\text{safety}}(P) \cup P) = \neg P & \wr \text{def. complement } \neg \int \\
\Leftrightarrow & \alpha_{\text{safety}}(P) \cap \neg P = \neg P & \wr \text{De Morgan laws} \int \\
\Leftrightarrow & \neg P \subseteq \alpha_{\text{safety}}(P) & \wr \text{def. glb} \int \quad \square
\end{array}
$$

Impossible runtime checks of liveness violation

Theorem 14.29 For all $P \in \wp(\mathbb{T}^+ \times \mathbb{T}^{+\infty})$, we have $\mathsf{live}(P) = P$ if and only if $\forall \pi_0 \in \mathbb{T}^+ \,.\, \forall \pi \in \mathbb{T}^{+\infty} \,.\, \exists \pi' \in \mathbb{T}^{+\infty} \,.\, \langle \pi_0, \pi \frown \pi' \rangle \in P$.

Liveness properties cannot be checked at runtime (since if the property is not satisfied after a finite time, there is always the possibility that it will be satisfied later).

Proof of Theorem 14.29

P is a dense set of the topology defined by α_{safety}

$\Leftrightarrow \quad \alpha_{\text{safety}}(P) = \mathbb{T}^{+} \times \mathbb{T}^{+\infty}$ $\qquad$ ⦃Definition 13.9 of dense sets⦄

$\Leftrightarrow \quad \mathbb{T}^{+} \times \mathbb{T}^{+\infty} \subseteq \alpha_{\text{safety}}(P)$ $\qquad$ ⦃since $\alpha_{\text{safety}} \in \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty}) \mapsto \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty})$⦄

$\Leftrightarrow \quad \forall\langle\pi_0, \pi\rangle \in \mathbb{T}^{+} \times \mathbb{T}^{+\infty} \,.\, \langle\pi_0, \pi\rangle \in \alpha_{\text{limit}} \circ \alpha_{\text{pref}}(P)$ $\qquad$ ⦃def. $\subseteq$ and α_{safety}⦄

$\Leftrightarrow \quad \forall\langle\pi_0, \pi\rangle \in \mathbb{T}^{+} \times \mathbb{T}^{+\infty} \,.\, \langle\pi_0, \pi\rangle \in (\alpha_{\text{pref}}(P) \cup \{\langle\pi_0', \pi\rangle \in \mathbb{T}^{+} \times \mathbb{T}^{\infty} \mid \forall\langle\pi_0', \pi'\rangle \lessdot \langle\pi_0', \pi\rangle \,.\, \langle\pi_0', \pi'\rangle \in \alpha_{\text{pref}}(P)\})$ $\qquad$ ⦃def. α_{limit}⦄

$\Leftrightarrow \quad \forall\langle\pi_0, \pi\rangle \in \mathbb{T}^{+} \times \mathbb{T}^{+\infty} \,.\, \langle\pi_0, \pi\rangle \in \alpha_{\text{pref}}(P) \vee (\langle\pi_0, \pi\rangle \in \mathbb{T}^{+} \times \mathbb{T}^{\infty} \wedge \forall\langle\pi_0, \pi'\rangle \lessdot \langle\pi_0, \pi\rangle \,.\, \langle\pi_0, \pi'\rangle \in \alpha_{\text{pref}}(P)\})$ $\qquad$ ⦃def. $\cup$⦄

$\Leftrightarrow \quad \forall\langle\pi_0, \pi\rangle \in \mathbb{T}^{+} \times \mathbb{T}^{+} \,.\, \langle\pi_0, \pi\rangle \in \alpha_{\text{pref}}(P)$

⦃($\Rightarrow$) $\mathbb{T}^{+} \cap \mathbb{T}^{\infty} = \varnothing$
($\Leftarrow$) $\langle\pi_0, \pi\rangle \in \mathbb{T}^{+} \times \mathbb{T}^{\infty} \wedge \langle\pi_0, \pi'\rangle \lessdot \langle\pi_0, \pi\rangle$ implies $\langle\pi_0, \pi'\rangle \in \mathbb{T}^{+}$ and so $\langle\pi_0, \pi'\rangle \in \alpha_{\text{pref}}(P)$⦄

$\Leftrightarrow \quad \forall\langle\pi_0, \pi\rangle \in \mathbb{T}^{+} \times \mathbb{T}^{+} \,.\, \langle\pi_0, \pi\rangle \in \{\langle\pi_0', \pi\rangle \in \mathbb{T}^{+} \times \mathbb{T}^{+\infty} \mid \exists\pi' \in \mathbb{T}^{+\infty} \,.\, \langle\pi_0', \pi \frown \pi'\rangle \in P\}$ $\qquad$ ⦃def. α_{pref}⦄

$\Leftrightarrow \quad \forall\pi_0.\pi \in \mathbb{T}^{+} \,.\, \exists\pi' \in \mathbb{T}^{+\infty} \,.\, \langle\pi_0, \pi \frown \pi'\rangle \in P$ $\qquad$ ⦃def. $\in$⦄ $\qquad \square$

Safety/liveness decomposition of trace properties

Finally, any trace property is the intersection of a safety (closed) and liveness (dense) property.

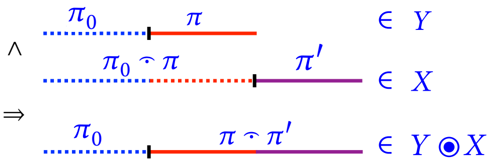
Theorem ([Alpern and Schneider, 1985, Th. 1])
$\forall P \in \wp(\mathbb{T}^+ \times \mathbb{T}^{+\infty}) \;.\; P = \alpha_{\mathsf{safety}}(P) \cap \mathsf{live}(P)$.

Proof By Lemma 13.12. $\square$

Guarantee

Guarantee properties

$$\begin{array}{rcll}
\alpha_{\text{guarantee}} & \in & \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty}) \mapsto \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty}) & \text{guarantee closure} \\
\alpha_{\text{guarantee}}(X) & \triangleq & (\mathbb{T}^{+} \times \mathbb{T}^{*}) \circledbullet X \qquad \text{where} & \\
Y \circledbullet X & \triangleq & \{\langle \pi_0,\ \pi \frown \pi' \rangle \mid \langle \pi_0,\ \pi \rangle \in Y \wedge \langle \pi_0 \frown \pi,\ \pi' \rangle \in X\} & \text{concatenation}
\end{array}$$



Guarantee properties

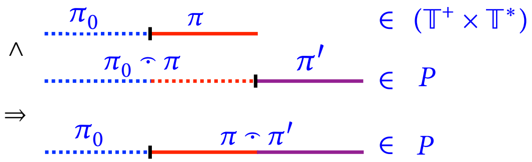
$$\begin{array}{rcll}
\alpha_{\text{guarantee}} & \in & \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty}) \mapsto \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty}) & \text{guarantee closure} \\
\alpha_{\text{guarantee}}(X) & \triangleq & (\mathbb{T}^{+} \times \mathbb{T}^{*}) \circledcirc X \qquad \text{where} & \\
Y \circledcirc X & \triangleq & \{\langle \pi_0,\ \pi \frown \pi' \rangle \mid \langle \pi_0,\ \pi \rangle \in Y \wedge \langle \pi_0 \frown \pi,\ \pi' \rangle \in X\} & \text{concatenation}
\end{array}$$

Definition 14.34 (guarantee) The *guarantee properties* are the trace properties $P \in \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty})$ such that $\alpha_{\text{guarantee}}(P) = P$.

Guarantee properties

$$\begin{array}{rcll}
\alpha_{\text{guarantee}} & \in & \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty}) \mapsto \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty}) & \text{guarantee closure} \\
\alpha_{\text{guarantee}}(X) & \triangleq & (\mathbb{T}^{+} \times \mathbb{T}^{*}) \odot X \qquad \text{where} & \\
Y \odot X & \triangleq & \{\langle \pi_0,\, \pi \frown \pi' \rangle \mid \langle \pi_0,\, \pi \rangle \in Y \wedge \langle \pi_0 \frown \pi,\, \pi' \rangle \in X\} & \text{concatenation}
\end{array}$$

Definition 14.34 (guarantee) The *guarantee properties* are the trace properties $P \in \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty})$ such that $\alpha_{\text{guarantee}}(P) = P$.



Guarantee properties

$$
\begin{array}{rcll}
\alpha_{\text{guarantee}} & \in & \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty}) \mapsto \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty}) & \text{guarantee closure} \\
\alpha_{\text{guarantee}}(X) & \triangleq & (\mathbb{T}^{+} \times \mathbb{T}^{*}) \circledcirc X \qquad \text{where} & \\
Y \circledcirc X & \triangleq & \{\langle \pi_0,\, \pi \frown \pi' \rangle \mid \langle \pi_0,\, \pi \rangle \in Y \wedge \langle \pi_0 \frown \pi,\, \pi' \rangle \in X\} & \text{concatenation}
\end{array}
$$

Definition 14.34 (guarantee) The *guarantee properties* are the trace properties $P \in \wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty})$ such that $\alpha_{\text{guarantee}}(P) = P$.

This is the intuition that “something good must happen”.

Example Termination is a guarantee property since $\alpha_{\text{guarantee}}(\mathbb{T}^{+} \times \mathbb{T}^{+}) = ((\mathbb{T}^{+} \times \mathbb{T}^{*}) \circledcirc (\mathbb{T}^{+} \times \mathbb{T}^{+})) = \mathbb{T}^{+} \times \mathbb{T}^{+}$.

Guarantee is liveness but liveness is not guarantee

Theorem [1]**14.36** Any guarantee property is a liveness property.

Theorem 14.38 The poset $\langle\alpha_{\text{guarantee}}(\wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty})), \subseteq\rangle$ of guarantee properties is a complete lattice $\langle\alpha_{\text{guarantee}}(\wp(\mathbb{T}^{+} \times \mathbb{T}^{+\infty})), \subseteq, \emptyset, \mathbb{T}^{+\infty}, \cup, \cap\rangle$.

Not all liveness properties are a guarantee that "something good must happen"!

Example Consider a program P on the web with guarantee property $G \triangleq$"questions are always answered in finite time".
The availability property that "an attacker cannot delay a response for ever" is a liveness property but not a guarantee property (it is necessary for P to guarantee G).

[1] proofs in the book

Conclusion

Take out

- Safety and guarantee are (upper closure/Galois connection-based) abstractions of trace properties
- Liveness is not
- Any trace property is the intersection of a safety and a liveness trace property
- This book is mainly concerned with safety properties

Bibliography I

Alpern, Bowen and Fred B. Schneider (1985). "Defining Liveness". *Inf. Process. Lett.* 21.4, pp. 181–185.

Home work

- Read Ch. **14** "Safety and Liveness Trace Properties" of

  Principles of Abstract Interpretation
  Patrick Cousot
  MIT Press

The End, Thank you