Model Checking I
alias
Reactive Systems Verification

Luca Tesei

MSc in Computer Science, University of Camerino

Topics

- Decomposition Theorem.
- Examples.

Material

Reading:

Chapter 3 of the book, pages 123–126.

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.

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 $SAFE$ and a liveness property $LIVE$ s.t.

$$E = SAFE \cap LIVE$$

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

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

---

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

$pref(\sigma)$ = set of all finite, nonempty prefixes of σ

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

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 $SAFE \stackrel{\text{def}}{=} cl(E)$

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

---

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

$pref(\sigma)$ = set of all finite, nonempty prefixes of σ

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

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

$$E = SAFE \cap LIVE$$

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

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

Show that:

- $E = SAFE \cap LIVE$
- $SAFE$ is a safety property
- $LIVE$ 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 $SAFE \stackrel{\text{def}}{=} cl(E)$

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

Show that:

- $E = SAFE \cap LIVE$ $\quad\surd$
- $SAFE$ is a safety property
- $LIVE$ 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 $SAFE \overset{\text{def}}{=} cl(E)$

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

Show that:

- $E = SAFE \cap LIVE$ $\surd$
- $SAFE$ 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 $SAFE \stackrel{\text{def}}{=} cl(E)$

$$LIVE \stackrel{\text{def}}{=} E \cup \big((2^{AP})^{\omega} \setminus cl(E) \big)$$

Show that:

- $E = SAFE \cap LIVE$ $\quad\surd$
- $SAFE$ is a safety property as $cl(SAFE) = SAFE$
- $LIVE$ is a liveness property, i.e., $pref(LIVE) = (2^{AP})^{+}$

Being safe and live

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 $\left(2^{AP}\right)^{\omega}$ 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: $\surd$

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

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

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

$$\mathit{pref}(E) = (2^{AP})^+$$
$$\Longrightarrow \quad cl(E) = (2^{AP})^\omega$$

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

$$pref(E) = (2^{AP})^+$$
$$\Longrightarrow \quad cl(E) = (2^{AP})^\omega$$

If E is a safety property too, then $cl(E) = E$.

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

$$pref(E) = (2^{AP})^{+}$$
$$\Longrightarrow \quad cl(E) = (2^{AP})^{\omega}$$

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