

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

LF2.6-DECOMP-THM

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

$$E = SAFE \cap LIVE$$

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

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

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

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

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

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

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

Show that:

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

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

Show that:

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

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

Show that:

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

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

Show that:

- $E = SAFE \cap LIVE$ ✓
- $SAFE$ 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?

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 $(2^{AP})^\omega$ 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

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

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

$$\begin{aligned} \text{pref}(E) &= (2^{AP})^+ \\ \implies \text{cl}(E) &= (2^{AP})^\omega \end{aligned}$$

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

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

$$\implies \text{cl}(E) = (2^{AP})^\omega$$

If E is a **safety** property too, then $\text{cl}(E) = E$.

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

$$\begin{aligned} \text{pref}(E) &= (2^{AP})^+ \\ \implies \text{cl}(E) &= (2^{AP})^\omega \end{aligned}$$

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