Model Checking I
alias
Reactive Systems Verification

Luca Tesei

MSc in Computer Science, University of Camerino

Topics

- Liveness Properties. Definition.
- Examples.

Material

Reading:

Chapter 3 of the book, pages 120–123.

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.

Overview

Liveness

“liveness: something good will happen.”

“liveness: something good will happen.”

“event a will occur eventually”

Liveness

"liveness: something good will happen."

"event a will occur eventually"

e.g., termination for sequential programs

Liveness

"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

"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"

"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

which property type? LF2.6-2

- Each philosopher thinks infinitely often.

which property type?

- Each philosopher thinks infinitely often.

liveness

which property type? LF2.6-2

- Each philosopher thinks infinitely often.

  liveness

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

which property type?

- Each philosopher thinks infinitely often.

  liveness

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

  invariant

which property type?

- 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.

which property type?

- 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

which property type?

LF2.6-2

- 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

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

which property type? LF2.6-2

- 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

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

  liveness

which property type?

- 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

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

  liveness

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

which property type?

- 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

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

  liveness

- Between two eating phases of philosopher $\boldsymbol{i}$ lies at least one eating phase of philosopher $\boldsymbol{i+1}$.

  safety

Liveness

many different formal definitions of liveness
have been suggested in the literature

Liveness

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., $E \subseteq \left(2^{AP}\right)^{\omega}$.

E is called a liveness property if each finite word over AP can be extended to an infinite word in E

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

> E is called a liveness property if each finite word over AP can be extended to an infinite word in E, i.e., if
> $$pref(E) \;=\; \left(2^{AP}\right)^{+}$$

recall: $pref(E) =$ 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

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

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

Examples for liveness properties

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

Examples for $AP = \{crit_i : i = 1, \ldots, n\}$:

Examples for liveness properties

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

Examples for $AP = \{crit_i : i = 1, \ldots, n\}$:

- each process will eventually enter its critical section

Examples for liveness properties

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

Examples for $AP = \{crit_i : i = 1, \ldots, n\}$:

- each process will eventually enter its critical section

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

$$\forall i \in \{1, \ldots, n\}\ \exists k \geq 0.\ crit_i \in A_k$$

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

Examples for $AP = \{crit_i : i = 1, \ldots, n\}$:

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

Examples for $AP = \{crit_i : i = 1, \ldots, n\}$:

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

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

$$\forall i \in \{1, \ldots, n\} \ \overset{\infty}{\exists} k \geq 0. \ crit_i \in A_k$$

Examples for liveness properties

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

Examples for $AP = \{wait_i, crit_i : i = 1, \ldots, n\}$:

- 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

Examples for liveness properties

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

Examples for $AP = \{wait_i, crit_i : i = 1, \ldots, n\}$:

- 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 = set of all infinite words $A_0 A_1 A_2 \ldots$ s.t.

$$\forall i \in \{1, \ldots, n\} \ \forall j \geq 0.\ wait_i \in A_j \longrightarrow \exists k > j.\ crit_i \in A_k$$

Recall: safety properties, prefix closure

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

Recall: safety properties, prefix closure

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

E is a safety property

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

$$\left\{\sigma' \in E : A_0\, A_1 \ldots A_n \in \mathit{pref}(\sigma')\right\} = \varnothing$$

Recall: safety properties, prefix closure

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

E is a safety property

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

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

remind:

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

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

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

E is a safety property

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

$$\left\{\sigma' \in E : A_0 \, A_1 \ldots A_n \in \mathit{pref}(\sigma')\right\} = \varnothing$$

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

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

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

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