System Specification, Verification and Synthesis (SSVS) – CS 4830/7485, Fall 2019

10: Formal Specification: Safety and Liveness

Stavros Tripakis

Northeastern University
Khoury College of Computer Sciences

SAFETY and LIVENESS

Safety and Liveness

Two important classes of properties.

- **Safety** property: *something "bad" does not happen*.
  - E.g., system never crashes, division by zero never happens, voltage stays always $\leq K$ (never exceeds K), etc.
  - Finite length error trace.

- **Liveness** property: *something "good" must happen*.
  - E.g., every request must eventually receive a response.
  - Infinite length error trace.

Safety and Liveness

Are these LTL properties safety, liveness, or something else?

- $\mathbf{G}p$:

Safety and Liveness

Are these LTL properties safety, liveness, or something else?

- $\mathbf{G}p$: safety.
- $\mathbf{F}p$:

Safety and Liveness

Are these LTL properties safety, liveness, or something else?

- $\mathbf{G}p$: safety.
- $\mathbf{F}p$: liveness.
- $\mathbf{X}p$:

Safety and Liveness

Are these LTL properties safety, liveness, or something else?

- $\mathbf{G}p$: safety.
- $\mathbf{F}p$: liveness.
- $\mathbf{X}p$: safety.
- $p\,\mathbf{U}\,q$:

Safety and Liveness

Are these LTL properties safety, liveness, or something else?

- $\mathbf{G}p$: safety.
- $\mathbf{F}p$: liveness.
- $\mathbf{X}p$: safety.
- $p \, \mathbf{U} \, q$: a "mix" of both!
- $\mathbf{GF}p$:

Safety and Liveness

Are these LTL properties safety, liveness, or something else?

- $\mathbf{G}p$: safety.
- $\mathbf{F}p$: liveness.
- $\mathbf{X}p$: safety.
- $p \, \mathbf{U} \, q$: a "mix" of both!
- $\mathbf{GF}p$: liveness.
- $\mathbf{G}(p \rightarrow \mathbf{F}q)$:

Safety and Liveness

Are these LTL properties safety, liveness, or something else?

- $\mathbf{G}p$: safety.
- $\mathbf{F}p$: liveness.
- $\mathbf{X}p$: safety.
- $p \, \mathbf{U} \, q$: a “mix” of both!
- $\mathbf{GF}p$: liveness.
- $\mathbf{G}(p \rightarrow \mathbf{F}q)$: liveness.
- $\mathbf{G}(p \rightarrow \mathbf{X}q)$:

Safety and Liveness

Are these LTL properties safety, liveness, or something else?

- $\mathbf{G}p$: safety.
- $\mathbf{F}p$: liveness.
- $\mathbf{X}p$: safety.
- $p\,\mathbf{U}\,q$: a "mix" of both!
- $\mathbf{GF}p$: liveness.
- $\mathbf{G}(p \rightarrow \mathbf{F}q)$: liveness.
- $\mathbf{G}(p \rightarrow \mathbf{X}q)$: safety.

Safety and Liveness

Are these LTL properties safety, liveness, or something else?

- $\mathbf{G}p$: safety.
- $\mathbf{F}p$: liveness.
- $\mathbf{X}p$: safety.
- $p \,\mathbf{U}\, q$: a "mix" of both!
- $\mathbf{GF}p$: liveness.
- $\mathbf{G}(p \rightarrow \mathbf{F}q)$: liveness.
- $\mathbf{G}(p \rightarrow \mathbf{X}q)$: safety.

Let's formalize all this.

Finite and infinite sequences over a set

Let Σ be a set.

- Σ^* is the set of all finite sequences (also called finite *words*) over Σ.
- Σ^ω is the set of all infinite sequences (also called infinite *words*) over Σ.

The empty sequence is often denoted ϵ.

Example: let $\Sigma = \{a, b\}$

- $\Sigma^* = \{\epsilon, a, b, aa, ab, ba, bb, aaa, aab, ...\}$
- $\Sigma^\omega = \{aaa\cdots, bbb\cdots, baa\cdots, abb\cdots, ababab\cdots, ...\}$

Notes:

- Regular and ω-regular expression notation:
  - a^*: a finite sequence of a's, zero, one, or more
  - a^ω: an infinite sequence of a's, $a^\omega = aaa\cdots$
- Note: a^* is a set of (finite) words, but a^ω is just one (infinite) word
- Note: some infinite words are not periodic, e.g., $aabaabaaab\cdots \in \Sigma^\omega$

Properties – Formally

What is a *property*, formally?

A **property** L over Σ is a set of infinite sequences over Σ:[1]

$$L \subseteq \Sigma^\omega$$

Examples:

- $L = \Sigma^\omega$: L holds on all traces (every trace is in L, i.e., every trace satisfies property L).
- $L = \emptyset$: no trace satisfies L.
- $L =$ the set of all traces satisfying $\mathbf{GF}p$.
- $L =$ the set of all traces such that p holds at every odd step in the trace.

[1] In our case, $\Sigma = 2^{\mathsf{AP}}$, where AP is a set of atomic propositions, and 2^{AP} is the powerset (set of all subsets) of AP.

Prefixes

- Let $\sigma \in \Sigma^\omega$ and let $\rho \in \Sigma^*$: ρ is called a **prefix of** σ if

$$\exists \sigma' \in \Sigma^\omega : \sigma = \rho \cdot \sigma'$$

  i.e., the concatenation of ρ and σ' gives σ.
- If $\sigma = \alpha_1\alpha_2\alpha_3\cdots$, and ρ is a prefix of σ, then there must be some $k \in \mathbb{N}$ such that $\rho = \alpha_1 \cdots \alpha_k$. We denote the finite prefix $\alpha_1 \cdots \alpha_k$ by $\sigma[1..k]$.
- When $k = 0$ we get the **empty** prefix, denoted ϵ.
- Let $L \subseteq \Sigma^\omega$ be a property over Σ. $\mathit{Prefixes}(L)$ denotes the set of all finite prefixes of all words in L:

$$\mathit{Prefixes}(L) = \{\rho \in \Sigma^* \mid \exists \sigma \in L : \rho \text{ is a prefix of } \sigma\}$$

Safety – Formally

Let L be a property = set of (infinite) traces.

- L is a **safety property** if

$$\forall \sigma \notin L : \exists k \in \mathbb{N} : \forall \rho \in \Sigma^\omega : \sigma[1..k] \cdot \rho \notin L$$

Safety – Formally

Let L be a property = set of (infinite) traces.

- L is a **safety property** if

$$\forall \sigma \notin L : \exists k \in \mathbb{N} : \forall \rho \in \Sigma^\omega : \sigma[1..k] \cdot \rho \notin L$$

i.e., *for any σ violating the safety property, there exists a* **bad prefix** $\sigma[1..k]$*, such that no matter how we extend this prefix we can no longer satisfy the safety property*.

Liveness – Formally

Let L be a property = set of (infinite) traces.

- L is a **liveness property** if

$$\forall \sigma \in \Sigma^* : \exists \rho \in \Sigma^\omega : \sigma \cdot \rho \in L$$

Liveness – Formally

Let L be a property = set of (infinite) traces.

- L is a **liveness property** if

$$\forall \sigma \in \Sigma^* : \exists \rho \in \Sigma^\omega : \sigma \cdot \rho \in L$$

i.e., *every finite trace can be extended, by appending a* **good suffix**, *into an infinite trace which satisfies the liveness property*.

Liveness – Formally

Let L be a property = set of (infinite) traces.

- L is a **liveness property** if

$$\forall \sigma \in \Sigma^* : \exists \rho \in \Sigma^\omega : \sigma \cdot \rho \in L$$

  i.e., *every finite trace can be extended, by appending a* **good suffix**, *into an infinite trace which satisfies the liveness property*.

- Equivalently, L is a liveness property iff

$$Prefixes(L) = \Sigma^*$$

Safety and Liveness – Topological Characterization

Theorem ([Alpern and Schneider, 1985] and others)

Every property is the intersection of a safety property and a liveness property.

This follows from a topological characterization of subsets of Σ^ω:

- Safety properties are the *closed* sets
- Liveness properties are the *dense* sets
- The *open* sets of the topology are the sets of all traces that share a common prefix.

Examples

Let $\Sigma = \{a, b\}$, or $\Sigma = 2^{\mathsf{AP}}$ with AP $= \{p, q\}$, as appropriate for each example below.

For each of the following sets: is it a safety property? a liveness property?

Hint: think of the **violating** traces!

- Σ^ω:

Examples

Let $\Sigma = \{a, b\}$, or $\Sigma = 2^{\mathsf{AP}}$ with AP $= \{p, q\}$, as appropriate for each example below.

For each of the following sets: is it a safety property? a liveness property?

Hint: think of the **violating** traces!

- Σ^ω: both!
- $\emptyset$:

Examples

Let $\Sigma = \{a, b\}$, or $\Sigma = 2^{\mathsf{AP}}$ with AP $= \{p, q\}$, as appropriate for each example below.

For each of the following sets: is it a safety property? a liveness property?

Hint: think of the **violating** traces!

- Σ^ω: both!
- $\emptyset$: safety.
- $(ab)^\omega$:

Examples

Let $\Sigma = \{a, b\}$, or $\Sigma = 2^{\mathsf{AP}}$ with $\mathsf{AP} = \{p, q\}$, as appropriate for each example below.

For each of the following sets: is it a safety property? a liveness property?

Hint: think of the **violating** traces!

- Σ^ω: both!
- $\emptyset$: safety.
- $(ab)^\omega$: safety.
- $\mathbf{F}q$:

Examples

Let $\Sigma = \{a, b\}$, or $\Sigma = 2^{\mathsf{AP}}$ with AP $= \{p, q\}$, as appropriate for each example below.
For each of the following sets: is it a safety property? a liveness property?
Hint: think of the **violating** traces!

- Σ^ω: both!
- $\emptyset$: safety.
- $(ab)^\omega$: safety.
- $\mathbf{F}q$: liveness.
- ba *appears at least three times in the trace*:

Examples

Let $\Sigma = \{a, b\}$, or $\Sigma = 2^{\mathsf{AP}}$ with AP $= \{p, q\}$, as appropriate for each example below.

For each of the following sets: is it a safety property? a liveness property?

Hint: think of the **violating** traces!

- Σ^ω: both!
- $\emptyset$: safety.
- $(ab)^\omega$: safety.
- $\mathbf{F}q$: liveness.
- ba *appears at least three times in the trace*: liveness.
- $p\,\mathbf{U}\,q$:

Examples

Let $\Sigma = \{a, b\}$, or $\Sigma = 2^{\mathsf{AP}}$ with AP $= \{p, q\}$, as appropriate for each example below.
For each of the following sets: is it a safety property? a liveness property?
Hint: think of the **violating** traces!

- Σ^ω: both!
- $\emptyset$: safety.
- $(ab)^\omega$: safety.
- $\mathbf{F}q$: liveness.
- ba *appears at least three times in the trace*: liveness.
- $p\,\mathbf{U}\,q$: neither! Can we define $p\,\mathbf{U}\,q$ as the intersection of a safety and a liveness property? Hint: start with the liveness part.

Examples

Let $\Sigma = \{a, b\}$, or $\Sigma = 2^{\mathsf{AP}}$ with AP $= \{p, q\}$, as appropriate for each example below.
For each of the following sets: is it a safety property? a liveness property?
Hint: think of the **violating** traces!

- Σ^ω: both!
- $\emptyset$: safety.
- $(ab)^\omega$: safety.
- $\mathbf{F}q$: liveness.
- ba *appears at least three times in the trace*: liveness.
- $p\,\mathbf{U}\,q$: neither! Can we define $p\,\mathbf{U}\,q$ as the intersection of a safety and a liveness property? Hint: start with the liveness part.

$$p\,\mathbf{U}\,q = (\mathbf{F}q) \wedge (p\,\mathbf{W}\,q)$$

where $p\,\mathbf{W}\,q$ (p "weak until" q) is the safety property that says that p must continuously hold (no "gap") until q holds, if q ever holds.

Safety and Liveness – Closure Properties

- Safety properties are closed under union and intersection.
- I.e., if L_1 and L_2 are both safety, then so are $L_1 \cup L_2$ and $L_1 \cap L_2$.
- Liveness properties are closed under union, but generally not under intersection.
- Neither safety nor liveness properties are closed under set complement.

Homework: find examples and counter-examples to the above closure and non-closure claims.

Bibliography

Alpern, B. and Schneider, F. B. (1985).
Defining liveness.
Information Processing Letters, 21(4):181 – 185.

Baier, C. and Katoen, J.-P. (2008).
Principles of Model Checking.
MIT Press.

Clarke, E., Grumberg, O., and Peled, D. (2000).
Model Checking.
MIT Press.