Local safety and local liveness for distributed systems

Paul Gastin & Volker Diekert

LSV, ENS Cachan, CNRS & FMI, Univ. Stuttgart

Developments and New Tracks in Trace Theory
Cremona, 10 October 2008
Motivations

Aim
Define robust notions of local safety and local liveness for distributed system.

- Give topological characterizations
- Establish a decomposition theorem.
- Characterizations by canonical local temporal logic formulae.
Mazurkiewicz traces

Notations

- $(\Sigma, D)$ dependence alphabet.
- $I = \Sigma \times \Sigma \setminus D$ independence relation.
- $t = (V, \leq, \lambda)$ finite or infinite trace.
- $\mathbb{R}$ set of finite or infinite traces.
- $\mathbb{M}$ set of finite traces.
- $s \leq t$ prefix relation over traces
  \[ \text{Pref}(t) = \{ s \in \mathbb{M} \mid s \leq t \} \]
- $\mathbb{P}$ set of prime traces, i.e., finite traces having a single maximal vertex.
  \[ \text{Pref}(t) = \text{Pref}(t) \cap \mathbb{P} \]
- $\mathbb{R}^1$ is the set of nonempty traces having a single minimal vertex.
Plan

1. Local safety

Local temporal logic

Local decomposition of first-order languages

Local liveness

Strong local liveness

Concluding remarks
Safety properties

Definition: Safety

- An execution $t$ is safe if and only if all partial executions of $t$ are Good.
Safety properties

**Definition: Safety**

- An execution $t$ is **safe** if and only if all partial executions of $t$ are **Good**.
- **Global semantics**: a partial execution is a (global) finite prefix.

A trace $t \in \mathbb{R}$ is **globally safe** w.r.t. $\text{Good} \subseteq \mathbb{M}$ if $\text{Pref}(t) \subseteq \text{Good}$.

A language $L$ is a **global safety** if there exists $\text{Good} \subseteq \mathbb{M}$ such that

$$L = \{ t \in \mathbb{R} \mid \text{Pref}(t) \subseteq \text{Good} \}.$$
Safety properties

**Definition: Safety**

- An execution $t$ is **safe** if and only if all partial executions of $t$ are **Good**.
- **Global semantics**: a partial execution is a (global) finite prefix.
  
  A trace $t \in \mathbb{R}$ is **globally safe w.r.t.** $\text{Good} \subseteq \mathbb{M}$ if $\text{Pref}(t) \subseteq \text{Good}$.
  
  A language $L$ is a **global safety** if there exists $\text{Good} \subseteq \mathbb{M}$ such that
  
  $$L = \{ t \in \mathbb{R} \mid \text{Pref}(t) \subseteq \text{Good} \}. $$

- **Local semantics**: a partial execution is a prime prefix.
  
  A trace $t \in \mathbb{R}$ is **locally safe w.r.t.** $\text{Good} \subseteq \mathbb{P}$ if $\text{Pref}(t) \subseteq \text{Good}$.
  
  A language $L$ is a **local safety** if there exists $\text{Good} \subseteq \mathbb{P}$ such that
  
  $$L = \{ t \in \mathbb{R} \mid \text{Pref}(t) \subseteq \text{Good} \}. $$
Safety properties

**Definition: Safety**

- An execution $t$ is safe if and only if all partial executions of $t$ are Good.

- **Global semantics:** a partial execution is a (global) finite prefix.

  A trace $t \in \mathbb{R}$ is globally safe w.r.t. $\text{Good} \subseteq \mathbb{M}$ if $\text{Pref}(t) \subseteq \text{Good}$.

  A language $L$ is a global safety if there exists $\text{Good} \subseteq \mathbb{M}$ such that

  $$L = \{ t \in \mathbb{R} \mid \text{Pref}(t) \subseteq \text{Good} \}.$$  

- **Local semantics:** a partial execution is a prime prefix.

  A trace $t \in \mathbb{R}$ is locally safe w.r.t. $\text{Good} \subseteq \mathbb{P}$ if $\text{Pref}(t) \subseteq \text{Good}$.

  A language $L$ is a local safety if there exists $\text{Good} \subseteq \mathbb{P}$ such that

  $$L = \{ t \in \mathbb{R} \mid \text{Pref}(t) \subseteq \text{Good} \}.$$  

- Local safety can be enforced locally.
Safety properties

Example: Local safety

$\Sigma = \{a, b, c\}$ and $I = \{(a, b), (b, a)\}$.

$L = \{t \in \mathbb{R} \mid t = ucrscev \text{ with } |r|_c = |s|_c = 0 \text{ implies } |r|_a + |r|_b \neq |s|_a + |s|_b \mod 2\}$

is a local safety property.
Safety properties

Example: Local safety

\[ \Sigma = \{a, b, c\} \text{ and } I = \{(a, b), (b, a)\}. \]

\[ L = \{ t \in \mathbb{R} \mid t = ucrsecv \text{ with } |r|_c = |s|_c = 0 \text{ implies } |r|_a + |r|_b \neq |s|_a + |s|_b \mod 2 \} \]

is a local safety property.

Example: Global safety

\[ \Sigma = \{a, b, c\} \text{ and } I = \{(a, b), (b, a)\}. \]

\[ L = \{ t \in \mathbb{R} \mid t = ucrv \text{ with } |r|_c = 0 \text{ implies } |r|_a + |r|_b \leq 3 \} \]

is a global safety property but not a local safety property.
Some Poset properties

Definitions and notations

- \((E, \leq)\) Poset
- \(X \subseteq E\) is coherent if for all \(x, y \in X\) there exists \(z \in E\) with \(x \leq z\) and \(y \leq z\).
- \(X \subseteq E\) is directed if \(X \neq \emptyset\) and for all \(x, y \in X\) there exists \(z \in X\) with \(x \leq z\) and \(y \leq z\).
- \(\sqcup X\) least upper bound of \(X\) when it exists.

Theorem: G. & Rozoy, TCS 93

- \((\mathbb{R}, \leq)\) is coherently complete, i.e., any coherent set has a lub.
- \(\text{Pref}(t)\) is coherent and \(t = \sqcup \text{Pref}(t)\) for all \(t \in \mathbb{R}\).
- \(\text{Pref}(t)\) is directed and \(t = \sqcup \text{Pref}(t)\) for all \(t \in \mathbb{R}\).
Definition: Local closure

- $L \subseteq \mathbb{R}$ is **locally closed** if it is closed under prime prefixes and lub of coherent subsets:

$$\text{Pref}(L) \subseteq L \quad \text{and} \quad \sqcup K \in L \quad \text{for all coherent } K \subseteq L$$

Remark: if $L$ is locally closed then $\text{Pref}(L) \subseteq L$. 
Local closure

**Definition: Local closure**

- \( L \subseteq \mathbb{R} \) is **locally closed** if it is closed under prime prefixes and lub of coherent subsets:

\[
\text{Pref}(L) \subseteq L \quad \text{and} \quad \biguplus K \in L \quad \text{for all coherent} \ K \subseteq L
\]

**Remark:** if \( L \) is locally closed then \( \text{Pref}(L) \subseteq L \).

- The **local closure** \( \overline{L}^l \) is the smallest set which is locally closed and contains \( L \).

**Remark:** \( 1 = \biguplus \emptyset \in \overline{L}^l \)
Definition: Local closure

- \( L \subseteq \mathbb{R} \) is \textbf{locally closed} if it is closed under \textbf{prime prefixes} and \textbf{lub of coherent subsets}:

\[
\text{Pref}(L) \subseteq L \quad \text{and} \quad \sqcup K \in L \quad \text{for all coherent } K \subseteq L
\]

Remark: if \( L \) is locally closed then \( \text{Pref}(L) \subseteq L \).

- The \textbf{local closure} \( \overline{L}^\ell \) is the smallest set which is locally closed and contains \( L \).

Remark: \( 1 = \sqcup \emptyset \in \overline{L}^\ell \)

Proposition: Local closure

- \( \overline{L}^\ell = \{ t \in \mathbb{R} \mid \text{Pref}(t) \subseteq \text{Pref}(L) \} \).
- \( L \subseteq \mathbb{R} \) is a \textbf{local safety property} if and only if it is locally closed.
Global closure

Definition: Global closure = Scott closure

- $L \subseteq \mathbb{R}$ is Scott closed if it is closed under prefixes and lub of directed subsets:

  \[ \text{Pref}(L) \subseteq L \quad \text{and} \quad \sqcup K \in L \quad \text{for all directed } K \subseteq L \]

Remark: if $L$ is locally closed then it is Scott closed.
Definition: Global closure $\equiv$ Scott closure

- $L \subseteq \mathbb{R}$ is Scott closed if it is closed under prefixes and lub of directed subsets:

$$\text{Pref}(L) \subseteq L \quad \text{and} \quad \sqcup K \in L \quad \text{for all directed } K \subseteq L$$

Remark: if $L$ is locally closed then it is Scott closed.

- The Scott closure $\overline{L}^\sigma$ is the smallest set which is Scott closed and contains $L$.

Remark: $\overline{L}^\sigma \subseteq \overline{L}^\ell$
**Global closure**

**Definition: Global closure = Scott closure**

- $L \subseteq \mathbb{R}$ is **Scott closed** if it is closed under prefixes and lub of directed subsets:

  \[
  \text{Pref}(L) \subseteq L \quad \text{and} \quad \bigcup K \in L \quad \text{for all directed } K \subseteq L
  \]

  Remark: if $L$ is locally closed then it is Scott closed.

- The **Scott closure** $L^\sigma$ is the smallest set which is Scott closed and contains $L$.

  Remark: $L^\sigma \subseteq L^\ell$

**Proposition: Global closure**

- $L^\sigma = \{ t \in \mathbb{R} \mid \text{Pref}(t) \subseteq \text{Pref}(L) \}$.
- $L \subseteq \mathbb{R}$ is a global safety property if and only if it is Scott closed.
- Every local safety property is also a global safety property.
Plan

Local safety

Local temporal logic

Local decomposition of first-order languages

Local liveness

Strong local liveness

Concluding remarks
### Local temporal logic

**Definition: Syntax of \( \text{LocTL}_\Sigma[\text{EX}, \text{U}, \text{EY}, \text{S}] \)**

\[
\varphi ::= \top \mid a \mid \neg \varphi \mid \varphi \lor \varphi \mid \text{EX} \, \varphi \mid \varphi \, \text{U} \, \varphi \mid \text{EY} \, \varphi \mid \varphi \, \text{S} \, \varphi
\]

where \( a \) ranges over \( \Sigma \).

**Definition: Semantics:** \( t = [V, \leq, \lambda] \in \mathbb{R} \setminus \{1\} \) and \( x \in V \)

- \( t, x \models a \) if \( \lambda(x) = a \)
- \( t, x \models \text{EX} \, \varphi \) if \( \exists y \in t \ (x < y \text{ and } t, y \models \varphi) \)
- \( t, x \models \varphi \, \text{U} \, \psi \) if \( \exists z \in t \ (x \leq z \text{ and } t, z \models \psi \text{ and } \forall y \in t \ (x \leq y < z \Rightarrow t, y \models \varphi)) \)
- \( t, x \models \text{EY} \, \varphi \) if \( \exists y \in t \ (y < x \text{ and } t, y \models \varphi) \)
- \( t, x \models \varphi \, \text{S} \, \psi \) if \( \exists z \in t \ (z \leq x \text{ and } t, z \models \psi \text{ and } \forall y \in t \ (z < y \leq x \Rightarrow t, y \models \varphi)) \)

**Abbreviations**

- \( \text{F} \, \varphi = \top \, \text{U} \, \varphi \)
- \( \text{G} \, \varphi = \neg \text{F} \, \neg \varphi \)
Local temporal logic

**Definition: Future formulae**

Future formulae: \( \text{LocTL}_\Sigma[\text{EX}, \text{U}] \)

**Remark:** if \( \varphi \in \text{LocTL}_\Sigma[\text{EX}, \text{U}] \) then for all \( t \in \mathbb{R} \setminus \{1\} \) and \( x \in t \) we have

\[
 t, x \models \varphi \quad \text{iff} \quad \uparrow x, x \models \varphi
\]

**Theorem: Diekert & G., IC 06**

Let \( L \subseteq \mathbb{R} \) be a first-order definable real trace language. Then there is a **future formula** \( \varphi \in \text{LocTL}_\Sigma[\text{EX}, \text{U}] \) such that

\[
 L \cap \mathbb{R}^1 = \{ t \in \mathbb{R}^1 \mid t, \min(t) \models \varphi \}
\]
Local temporal logic

**Definition: Past formulae**

Past formulae: $\text{LocTL}_\Sigma[\text{EY}, S]$

Remark: if $\varphi \in \text{LocTL}_\Sigma[\text{EY}, S]$ then for all $t \in \mathbb{R} \setminus \{1\}$ and $x \in t$ we have

$$t, x \models \varphi \iff \downarrow x, x \models \varphi$$

**Corollary: Diekert & G., IC 06**

Let $L \subseteq \mathbb{R}$ be a first-order definable real trace language. Then there is a past formula $\varphi \in \text{LocTL}_\Sigma[\text{EY}, S]$ such that

$$L \cap \mathbb{P} = \{t \in \mathbb{P} | t, \max(t) \models \psi\}$$
Plan

Local safety

Local temporal logic

Local decomposition of first-order languages

Local liveness

Strong local liveness

Concluding remarks
Definition: Direct semantics for F and G

\[ t \models_{\ell} F \varphi \quad \text{if} \quad \exists x \in t, \ t, x \models \varphi \]
\[ t \models_{\ell} G \psi \quad \text{if} \quad \forall x \in t, \ t, x \models \psi. \]

Remark: 1 \models G \varphi \text{ but } 1 \not\models F \varphi \text{ for all } \varphi \in \text{LocTL}_\Sigma
Definition: Direct semantics for $F$ and $G$

\[
\begin{align*}
t \models_{\ell} F \varphi & \quad \text{if} \quad \exists x \in t, \ t, x \models \varphi \\
t \models_{\ell} G \psi & \quad \text{if} \quad \forall x \in t, \ t, x \models \psi.
\end{align*}
\]

Remark: $1 \models G \varphi$ but $1 \not\models F \varphi$ for all $\varphi \in \text{LocTL}_\Sigma$.

Extension to any boolean combination $\gamma$ of $F$ and $G$ formulae.

\[
\mathcal{L}(\gamma) = \{ t \in \mathbb{R} \mid t \models_{\ell} \gamma \}
\]
Concurrent modality

**Definition: Local decompotion of traces**

Let $t = [V, \leq, \lambda] \in \mathbb{R}$ and $x \in t$
**Definition: Local decomposition of traces**

Let \( t = [V, \leq, \lambda] \in \mathbb{R} \) and \( x \in t \)

**Definition: Concurrent modality**

Let \( \gamma \) be any Boolean combination of F and G formulae. Then, **CO \( \gamma \) is a concurrent formula** with semantics

\[
\text{if } \llbracket x \rrbracket \models \ell \gamma.
\]
A decomposition formula is a disjunction

\[ \delta = \bigvee_{j \in J} a_j \land \psi_j \land \varphi_j \land \text{CO} \gamma_j \]

where \( J \) is some finite index set, and for each \( j \in J \)

- \( a_j \in \Sigma \)
- \( \psi_j \in \text{LocTL}_\Sigma(\text{EY}, S) \) is a past formula
- \( \varphi_j \in \text{LocTL}_\Sigma(\text{EX}, U) \) is a future formula
- \( \gamma_j \) is an \( F \) or \( G \) formula

Note that, if \( J = \emptyset \) then we get \( \delta = \bot \) by convention.
Local decomposition

**Theorem: Decomposition**

Let \( L \subseteq \mathbb{R} \) be a first-order definable real trace language. There exists a *decomposition formula*

\[
\delta = \bigvee_{j \in J} a_j \land \psi_j \land \varphi_j \land \text{CO} \gamma_j
\]

such that

1. \( L \cup \{1\} = \mathcal{L}(G \delta) \),
2. \( L \setminus \{1\} = \mathcal{L}(F \delta) \),
3. \( \text{Pref}(L) = \{ r \in P \mid r, \max(r) \models \bigvee_{j \in J} a_j \land \psi_j \} \),
4. for each \( j \in J \), the formula \( a_j \land \psi_j \land \varphi_j \land \text{CO} \gamma_j \) is satisfiable.
The proof uses

**Theorem: Ebinger & Muscholl, TCS 96**

A language $L \subseteq \mathbb{R}$ is a first-order definable if and only if it is **aperiodic**.

Let $h : \mathbb{M}(\Sigma, D) \rightarrow S$ be a morphism **recognizing** $L$ with $S$ finite **aperiodic** monoid. Assume $h$ **alphabetic**.

Let $t \in L \setminus \{1\}$ and $x \in t$. Then,

$$t \in [\downarrow x] \cdot \lambda(x) \cdot [\parallel x] \cdot [\uparrow x] \subseteq L$$
Local decomposition: proof sketch

The proof uses

Theorem: Ebinger & Muscholl, TCS 96

A language \( L \subseteq \mathbb{R} \) is a first-order definable if and only if it is aperiodic.

Let \( h : \mathbb{M}(\Sigma, D) \rightarrow S \) be a morphism recognizing \( L \) with \( S \) finite aperiodic monoid. Assume \( h \) alphabetic.

Let \( t \in L \setminus \{1\} \) and \( x \in t \). Then,

\[
t \in [\downarrow x] \cdot \lambda(x) \cdot [\| x ] \cdot [\uparrow x] \subseteq L
\]

Let \( J = \{(\lambda(x), [\downarrow x], [\| x], [\uparrow x]) \mid t \in L \setminus \{1\} \text{ and } x \in t\} \) finite index set.
Local decomposition: proof sketch

Let $h : \mathcal{M}(\Sigma, D) \to S$ be a morphism recognizing $L$ with $S$ finite aperiodic monoid. Let $t \in L \setminus \{1\}$ and $x \in t$. Then,

$$t \in [\downarrow x] \cdot \lambda(x) \cdot [\|x] \cdot [\uparrow x] \subseteq L$$

Let $J = \{(\lambda(x), [\downarrow x], [\|x], [\uparrow x]) \mid t \in L \setminus \{1\} \text{ and } x \in t\}$ finite index set.
Local decomposition: proof sketch

Let $h : \mathbb{M}(\Sigma, D) \to S$ be a morphism recognizing $L$ with $S$ finite aperiodic monoid. Let $t \in L \setminus \{1\}$ and $x \in t$. Then,

$$t \in [\downarrow x] \cdot \lambda(x) \cdot [\parallel x] \cdot [\uparrow x] \subseteq L$$

Let $J = \{ (\lambda(x), [\downarrow x], [\parallel x], [\uparrow x]) \mid t \in L \setminus \{1\} \text{ and } x \in t \}$ finite index set.

Fix $j = (a_j, L_j^{\downarrow}, L_j^{\parallel}, L_j^{\uparrow}) \in J$.

There exists a future formula $\varphi_j$ and a past formula $\psi_j$ such that

$$a_j \cdot L_j^{\uparrow} \cap \mathbb{R}^1 = \{ s \in \mathbb{R}^1 \mid s, \min(s) \models \varphi_j \}$$

$$L_j^{\downarrow} \cdot a_j \cap \mathbb{P} = \{ r \in \mathbb{P} \mid r, \max(r) \models \psi_j \}.$$
Local decomposition: proof sketch

Let $h : \mathbb{M}(\Sigma, D) \to S$ be a morphism recognizing $L$ with $S$ finite aperiodic monoid. Let $t \in L \setminus \{1\}$ and $x \in t$. Then,

$$t \in [\downarrow x] \cdot \lambda(x) \cdot [\| x] \cdot [\uparrow x] \subseteq L$$

Let $J = \{ (\lambda(x), [\downarrow x], [\| x], [\uparrow x]) \mid t \in L \setminus \{1\} \text{ and } x \in t \}$ finite index set.

Fix $j = (a_j, L_j^\downarrow, L_j^\|, L_j^\uparrow) \in J$.

There exists a future formula $\varphi_j$ and a past formula $\psi_j$ such that

$$a_j \cdot L_j^\uparrow \cap \mathbb{R}^1 = \{ s \in \mathbb{R}^1 \mid s, \min(s) \models \varphi_j \}$$
$$L_j^\downarrow \cdot a_j \cap \mathbb{P} = \{ r \in \mathbb{P} \mid r, \max(r) \models \psi_j \}.$$ 

By induction on the alphabet, we find a decomposition formula $\delta_j$ for $L_j^\|$.

Let $\gamma_j = \begin{cases} G \delta_j & \text{if } 1 \in L_j^\| \\ F \delta_j & \text{otherwise.} \end{cases}$
Local decomposition: proof sketch

Let \( h : \mathbb{M}(\Sigma, D) \rightarrow S \) be a morphism recognizing \( L \) with \( S \) finite aperiodic monoid. Let \( t \in L \setminus \{1\} \) and \( x \in t \). Then,

\[
 t \in \downarrow x \cdot \lambda(x) \cdot \uparrow x \subseteq L
\]

Let \( J = \{ (\lambda(x), \downarrow x, \parallel x, \uparrow x) \mid t \in L \setminus \{1\} \text{ and } x \in t \} \) finite index set.

Fix \( j = (a_j, L_j^\downarrow, L_j^\parallel, L_j^\uparrow) \in J \).

There exists a future formula \( \varphi_j \) and a past formula \( \psi_j \) such that

\[
 a_j \cdot L_j^\uparrow \cap \mathbb{R}^1 = \{ s \in \mathbb{R}^1 \mid s, \min(s) \models \varphi_j \}
\]

\[
 L_j^\downarrow \cdot a_j \cap \mathbb{P} = \{ r \in \mathbb{P} \mid r, \max(r) \models \psi_j \}.
\]

By induction on the alphabet, we find a decomposition formula \( \delta_j \) for \( L_j^\parallel \).

Let \( \gamma_j = \begin{cases} G \delta_j & \text{if } 1 \in L_j^\parallel \\ F \delta_j & \text{otherwise.} \end{cases} \)

Claim: the decomposition formula \( \delta = \bigvee_{j \in J} a_j \land \psi_j \land \varphi_j \land \text{CO} \gamma_j \) satisfies statements (1–4) of the decomposition theorem.
Definition:
A canonical local safety formula is a formula of type $G \psi$ where $\psi \in \text{LocTL}_\Sigma[EY, S]$ is a past formula.

Theorem: local safety
A first-order definable language is a local safety property if and only if it can be expressed by a canonical local safety formula.
Definition:
A canonical local safety formula is a formula of type $G \psi$ where $\psi \in \text{LocTL}_\Sigma[EY, S]$ is a past formula.

Theorem: local safety
A first-order definable language is a local safety property if and only if it can be expressed by a canonical local safety formula.

More precisely:
1. Let $\psi \in \text{LocTL}_\Sigma[EY, S]$. Then, $\mathcal{L}(G \psi)$ is locally closed.
**Definition:**

A *canonical local safety formula* is a formula of type $G \psi$ where $\psi \in \text{LocTL}_\Sigma[\text{EY}, S]$ is a past formula.

**Theorem: local safety**

A first-order definable language is a local safety property if and only if it can be expressed by a canonical local safety formula.

More precisely:

1. Let $\psi \in \text{LocTL}_\Sigma[\text{EY}, S]$. Then, $\mathcal{L}(G \psi)$ is locally closed.

2. Let $L \subseteq \mathbb{R}$ be a first-order definable language. Let $\delta = \bigvee_{j \in J} a_j \land \psi_j \land \varphi_j \land \text{CO} \gamma_j$ be a decomposition formula for $L$. Then,

$$\overline{L}^\ell = \mathcal{L} \left( G \bigvee_{j \in J} a_j \land \psi_j \right)$$
Example:

Let $\Sigma = \{a, b, c\}$ and $I = \{(a, b), (b, a)\}$.

$$L = \{t \in \mathbb{R} \mid t = ucrscsv \text{ with } |r|_c = |s|_c = 0 \text{ implies } |r|_a + |r|_b \neq |s|_a + |s|_b \mod 2\}$$

is a local safety property but is not first-order definable.
Canonical local safety formulae

Example:
Let $\Sigma = \{a, b, c\}$ and $I = \{(a, b), (b, a)\}$.

$$L = \{t \in \mathbb{R} \mid t = ucrscev \text{ with } |r|_c = |s|_c = 0 \text{ implies } |r|_a + |r|_b \neq |s|_a + |s|_b \mod 2\}$$

is a local safety property but is not first-order definable.

Example:

$$L = \{t \in \mathbb{R} \mid t = ucrscev \text{ with } |r|_c = 0 \text{ implies } |r|_a \leq 2 \land |r|_b \leq 2\}$$

is a local safety property which is first-order definable. It is defined by the canonical local safety formula

$$G(c \land EY(\top S c) \longrightarrow \neg EY(a \land EY(a \land EY a)) \land \neg EY(b \land EY(b \land EY b)))$$
Plan

Local safety

Local temporal logic

Local decomposition of first-order languages

Local liveness

Strong local liveness

Concluding remarks
Definition: Liveness

- A partial execution $r$ is live if it can be extended to some Good execution.
Definition: Liveness

- A partial execution $r$ is live if it can be extended to some Good execution.
- Global semantics: a partial execution is a (global) finite prefix.

A trace $r \in M$ is globally live w.r.t. $\text{Good} \subseteq \mathbb{R}$ if $r \in \text{Pref}(\text{Good})$.

$L \subseteq \mathbb{R}$ is a global liveness property if all partial executions are live w.r.t. $L$:

$$\text{Pref}(L) = M$$
Liveness properties

**Definition: Liveness**

- A partial execution \( r \) is **live** if it can be extended to some \( \text{Good} \) execution.
- **Global semantics**: a partial execution is a (global) finite prefix.
  
  A trace \( r \in \mathbb{M} \) is **globally live w.r.t.** \( \text{Good} \subseteq \mathbb{R} \) if \( r \in \text{Pref}(\text{Good}) \).

  \( L \subseteq \mathbb{R} \) is a **global liveness property** if all partial executions are live w.r.t. \( L \):

  \[
  \text{Pref}(L) = \mathbb{M}
  \]

- **Local semantics**: a partial execution is a **prime prefix**.

  A trace \( r \in \mathbb{P} \) is **locally live w.r.t.** \( \text{Good} \subseteq \mathbb{R} \) if \( r \in \text{Pref}(\text{Good}) \).

  \( L \subseteq \mathbb{R} \) is a **local liveness property** if all partial executions are live w.r.t. \( L \):

  \[
  \text{Pref}(L) = \mathbb{P}
  \]
Liveness properties

Definition: Liveness

- A partial execution \( r \) is live if it can be extended to some Good execution.
- Global semantics: a partial execution is a (global) finite prefix.
  
  A trace \( r \in M \) is globally live w.r.t. \( \text{Good} \subseteq R \) if \( r \in \text{Pref}(\text{Good}) \).
  
  \( L \subseteq R \) is a global liveness property if all partial executions are live w.r.t. \( L \):
  
  \[
  \text{Pref}(L) = M
  \]

- Local semantics: a partial execution is a prime prefix.
  
  A trace \( r \in P \) is locally live w.r.t. \( \text{Good} \subseteq R \) if \( r \in \text{Pref}(\text{Good}) \).
  
  \( L \subseteq R \) is a local liveness property if all partial executions are live w.r.t. \( L \):
  
  \[
  \text{Pref}(L) = P
  \]

- Any global liveness property is also a local liveness property.
Example: Local liveness

Let $\Sigma = \{a, b\}$ with $(a, b) \in I$. The language $L = \{a^\omega, b^\omega\}$ is a local liveness property since

$$\mathbb{P} = a^+ \cup b^+ = \text{Pref}(L)$$

But $L$ is not a global liveness property since

$$\text{Pref}(L) = \text{Pref}(L) \neq \mathbb{M}$$
Liveness properties

Example: Local liveness

Let $\Sigma = \{a, b\}$ with $(a, b) \in I$. The language $L = \{a^\omega, b^\omega\}$ is a local liveness property since

$$P = a^+ \cup b^+ = \text{Pref}(L)$$

But $L$ is not a global liveness property since

$$\text{Pref}(L) = \text{Pref}(L) \neq \mathbb{M}$$

Example: Global liveness

The language $L = \{(ab)^\omega\}$ is a global liveness property, hence also a local liveness property.
**Definition: Local density**

A language $L \subseteq \mathbb{R}$ is **locally dense** if

$$\overline{L}^l = \mathbb{R}$$

Recall that $\overline{L}^l$ is the smallest set which is locally closed and contains $L$:

$$\overline{L}^l = \{ t \in \mathbb{R} | \text{Pref}(t) \subseteq \text{Pref}(L) \}$$

**Proposition: Local density**

A trace language $L \subseteq \mathbb{R}$ is a **local liveness property** if and only if it is locally dense.
Definition:

A canonical local liveness formula is of the form $F \delta$ where

$$\delta = \bigvee_{j \in J} a_j \land \psi_j \land \varphi_j \land CO \gamma_j$$

is a decomposition formula such that

- $\psi = \bigvee_{j \in J} a_j \land \psi_j$ is valid,
- $a_j \land \varphi_j \land CO \gamma_j$ is satisfiable for all $j \in J$. 
Definition:

A canonical local liveness formula is of the form $F\delta$ where

$$\delta = \bigvee_{j \in J} a_j \land \psi_j \land \varphi_j \land \text{CO} \gamma_j$$

is a decomposition formula such that

- $\psi = \bigvee_{j \in J} a_j \land \psi_j$ is valid,
- $a_j \land \varphi_j \land \text{CO} \gamma_j$ is satisfiable for all $j \in J$.

Proposition: local liveness

Let $F\delta$ be a canonical local liveness formula. Then the language $L = \mathcal{L}(F\delta)$ is a local liveness property.
Proof: Sketch

Let $r \in \mathbb{P}$. Let $j \in J$ with $r, \max(r) \models a_j \land \psi_j$ Let $t \in \mathbb{R} \setminus \{1\}$ and $x \in t$ such that $t, x \models a_j \land \varphi_j \land \text{CO } \gamma_j$ (valid) (satisfiable)

\[
t = \begin{array}{c}
\downarrow x \\
\quad a_j \\
\uparrow x
\end{array}
\]

|| x
Proof: Sketch

Let $r \in P$.
Let $j \in J$ with $r, \max(r) \models a_j \land \psi_j$
Let $t \in \mathbb{R} \setminus \{1\}$ and $x \in t$ such that $t, x \models a_j \land \varphi_j \land \text{CO } \gamma_j$

($\psi$ valid)
(satisfiable)
Canonical local liveness formulae

Proof: Sketch

Let \( r \in \mathbb{P} \).

Let \( j \in J \) with \( r, \max(r) \models a_j \land \psi_j \)

Let \( t \in \mathbb{R} \setminus \{1\} \) and \( x \in t \) such that \( t, x \models a_j \land \varphi_j \land \text{CO} \gamma_j \) \hspace{1cm} (\psi \text{ valid})

(satisfiable)

Then,

\[
    r \cdot \|x\cdot \uparrow x \models F \delta.
\]
Theorem: Local liveness

Let $L \subseteq \mathbb{R}$ be a first-order definable real trace language and let

$$\delta = \bigvee_{j \in J} a_j \land \psi_j \land \varphi_j \land \text{CO} \gamma_j$$

be a decomposition formula for $L$.

Let also $\psi = \bigvee_{j \in J} a_j \land \psi_j$. Then,

1. $\overline{L}^\ell = \mathcal{L}(G\psi)$. 

Theorem: Local liveness

Let $L \subseteq \mathbb{R}$ be a first-order definable real trace language and let

$$
\delta = \bigvee_{j \in J} a_j \land \psi_j \land \varphi_j \land \text{CO} \gamma_j
$$

be a decomposition formula for $L$.

Let also $\psi = \bigvee_{j \in J} a_j \land \psi_j$. Then,

1. $\overline{L}^\ell = \mathcal{L}(G \psi)$.

2. If $L$ is a local liveness property, then $\psi$ is a valid formula and $L \setminus \{1\} = \mathcal{L}(F \delta)$ is defined by a canonical local liveness formula.
Local liveness

Theorem: Local liveness

Let $L \subseteq \mathbb{R}$ be a first-order definable real trace language and let

$$\delta = \bigvee_{j \in J} a_j \land \psi_j \land \varphi_j \land \text{CO} \gamma_j$$

be a decomposition formula for $L$.

Let also $\psi = \bigvee_{j \in J} a_j \land \psi_j$. Then,

1. $\overline{L}^\ell = L(G\psi)$.

2. If $L$ is a local liveness property, then $\psi$ is a valid formula and $L \setminus \{1\} = L(F\delta)$ is defined by a canonical local liveness formula.

3. $F(\neg \psi \lor \delta)$ is a canonical local liveness formula.

$$\widetilde{L} = L(F(\neg \psi \lor \delta)) = (L \setminus \{1\}) \cup (\mathbb{R} \setminus \overline{L}^\ell)$$

is a local liveness property. Moreover, $\widetilde{L}$ is the largest set $K$ such that $L \setminus \{1\} = \overline{L}^\ell \cap K$. 
Plan

Local safety

Local temporal logic

Local decomposition of first-order languages

Local liveness

Strong local liveness

Concluding remarks
Local liveness

Example: Motivation

Let $\Sigma = \{a, b\}$ with $(a, b) \in I$.

The language $L = \{a^\omega, b^\omega\}$ is a local liveness property.

Consider the global partial execution $a^3 b^2$.

The local partial executions are $a^3$ and $b^2$.

Both local partial execution are locally live.

But the global partial execution is not live.
Strong local liveness
Strong local liveness

\[ r \quad a \quad \exists s \quad \in L \]
Strong local liveness

\[ \exists s \in L \]
Definition: Strong local liveness

$L \subseteq \mathbb{R}$ is a strong local liveness property (SLLP) if
- $L$ is a local liveness property (LLP)
- for all $t = raus \in \mathbb{R} \setminus \{1\}$ with $ra \in P$, $a \in \Sigma$, $as \in \mathbb{R}^1$ and $\text{alph}(u) \subseteq I(a)$,

$$raus \in L \iff ras \in L$$

If $(a, b) \in I$ then $L = a^\omega b^\infty \cup a^\infty b^\omega$ is a SLLP.
Definition: Strong local liveness

$L \subseteq \mathbb{R}$ is a strong local liveness property (SLLP) if

- $L$ is a local liveness property (LLP)
- for all $t = raus \in \mathbb{R} \setminus \{1\}$ with $ra \in P$, $a \in \Sigma$, $as \in \mathbb{R}^1$ and $\text{alph}(u) \subseteq I(a)$,

$$raus \in L \iff ras \in L$$

If $(a,b) \in I$ then $L = a^\omega b^\infty \cup a^\infty b^\omega$ is a SLLP.

Proposition: Various liveness

SLLP $\subsetneq$ GLP $\subsetneq$ LLP.

If $(a,b) \in I$ then $L = (ab)^\omega$ is a GLP but not a SLLP.
Strong local liveness

Theorem: Canonical formulae

$L \subseteq \mathbb{R}$ is a first-order definable strong local liveness property if and only if there is a finite decomposition formula with no concurrent part

$$\delta = \bigvee_{j \in J} a_j \land \psi_j \land \varphi_j$$

such that

- $\psi = \bigvee_{j \in J} a_j \land \psi_j$ valid,
- $a_j \land \psi_j \land \varphi_j$ satisfiable for each $j \in J$

and such that

$$L \setminus \{1\} = \mathcal{L}(F \delta) \quad \text{and} \quad L \cup \{1\} = \mathcal{L}(G \delta)$$
Plan

Local safety

Local temporal logic

Local decomposition of first-order languages

Local liveness

Strong local liveness

Concluding remarks
Strong or not?

Any property $L \subseteq \mathbb{R}$ is the intersection of a local safety and a local liveness:

$$L = \overline{L}^\ell \cap (L \cup \mathbb{R} \setminus \overline{L}^\ell)$$
Any property $L \subseteq \mathbb{R}$ is the intersection of a local safety and a local liveness:

$$L = \overline{L}^l \cap (L \cup \mathbb{R} \setminus \overline{L}^l)$$

**Remark:**

If we wish that every language is the intersection of a local safety property and a liveness property then each locally dense language must be a liveness property.

$$SLLP \subsetneq GLP \subsetneq LLP = LD$$
Strong or not?

Any property $L \subseteq \mathbb{R}$ is the intersection of a local safety and a local liveness:

$$L = \overline{L}^l \cap (L \cup \mathbb{R} \setminus \overline{L}^l)$$

Remark:
If we wish that every language is the intersection of a local safety property and a liveness property then each locally dense language must be a liveness property.

$$\text{SLLP} \subsetneq \text{GLP} \subsetneq \text{LLP} = \text{LD}$$

Proof:
Let $L$ be locally dense. Assume that $L = K_1 \cap K_2$ with $K_1$ local safety and $K_2$ liveness. Then $\mathbb{R} = \overline{L}^l \subseteq \overline{K_1}^l = K_1$. We deduce $L = K_2$ is a liveness property.
Local separation

With a proof similar to the decomposition theorem, we obtain

**Theorem: Separation**

Let \( \varphi \) be a first-order formula with one free variable. Then there exists a decomposition formula

\[
\delta = \bigvee_{j \in J} a_j \land \psi_j \land \varphi_j \land \text{CO} \gamma_j
\]

such that for all \( t \in \mathbb{R} \setminus \{1\} \) and all \( x \in t \) we have

\[
t, x \models \varphi(x) \quad \text{if and only if} \quad t, x \models \delta
\]