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

- (Σ, 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

$$\mathrm{Pref}(t) = \{s \in \mathbb{M} \mid s \leq t\}$$

- $\mathbb{P}$ set of prime traces, i.e., finite traces having a single maximal vertex.

$$\mathbb{P}\mathrm{ref}(t) = \mathrm{Pref}(t) \cap \mathbb{P}$$

- $\mathbb{R}^1$ 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. $\mathrm{Good} \subseteq \mathbb{M}$ if $\mathrm{Pref}(t) \subseteq \mathrm{Good}$.

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

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

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. $\mathrm{Good} \subseteq \mathbb{M}$ if $\mathrm{Pref}(t) \subseteq \mathrm{Good}$.

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

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

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

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

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

  $$L = \{t \in \mathbb{R} \mid \mathbb{P}\mathrm{ref}(t) \subseteq \mathrm{Good}\}.$$

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. $\mathrm{Good} \subseteq \mathbb{M}$ if $\mathrm{Pref}(t) \subseteq \mathrm{Good}$.

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

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

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

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

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

  $$L = \{t \in \mathbb{R} \mid \mathbb{P}\mathrm{ref}(t) \subseteq \mathrm{Good}\}.$$

- Local safety can be enforced locally.

Safety properties

Example: Local safety

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

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

is a local safety property.

Safety properties

Example: Local safety

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

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

is a local safety property.

Example: Global safety

$\Sigma = \{a, b, c\}$ 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.
- $\mathbb{P}\mathrm{ref}(t)$ is coherent and $t = \sqcup \mathbb{P}\mathrm{ref}(t)$ for all $t \in \mathbb{R}$.
- $\mathrm{Pref}(t)$ is directed and $t = \sqcup \mathrm{Pref}(t)$ for all $t \in \mathbb{R}$.

Local closure

Definition: Local closure

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

$$\mathbb{P}\mathrm{ref}(L) \subseteq L \qquad \text{and} \qquad \sqcup K \in L \quad \text{for all coherent } K \subseteq L$$

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

Local closure

Definition: Local closure

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

$$\mathbb{P}\mathrm{ref}(L) \subseteq L \qquad \text{and} \qquad \sqcup K \in L \quad \text{for all coherent } K \subseteq L$$

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

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

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

Local closure

Definition: Local closure

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

$$\mathbb{P}\mathrm{ref}(L) \subseteq L \qquad \text{and} \qquad \sqcup K \in L \quad \text{for all coherent } K \subseteq L$$

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

- The 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

- $\overline{L}^{\ell} = \{t \in \mathbb{R} \mid \mathbb{P}\mathrm{ref}(t) \subseteq \mathbb{P}\mathrm{ref}(L)\}$.
- $L \subseteq \mathbb{R}$ is a 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:

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

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

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

  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:

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

  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: $\overline{L}^{\sigma} \subseteq \overline{L}^{\ell}$

Proposition: Global closure

- $\overline{L}^{\sigma} = \{t \in \mathbb{R} \mid \mathrm{Pref}(t) \subseteq \mathrm{Pref}(L)\}$.
- $L \subseteq \mathbb{R}$ 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

2 Local temporal logic

Local decomposition of first-order languages

Local liveness

Strong local liveness

Concluding remarks

Local temporal logic

Definition: Syntax of $\mathrm{LocTL}_\Sigma[\mathsf{EX}, \mathsf{U}, \mathsf{EY}, \mathsf{S}]$

$$\varphi ::= \top \mid a \mid \neg\varphi \mid \varphi \vee \varphi \mid \mathsf{EX}\,\varphi \mid \varphi\,\mathsf{U}\,\varphi \mid \mathsf{EY}\,\varphi \mid \varphi\,\mathsf{S}\,\varphi$$

where a ranges over Σ.

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

$$
\begin{array}{lll}
t, x \models a & \text{if} & \lambda(x) = a \\
t, x \models \mathsf{EX}\,\varphi & \text{if} & \exists y \in t\,(x \lessdot y \text{ and } t, y \models \varphi) \\
t, x \models \varphi\,\mathsf{U}\,\psi & \text{if} & \exists z \in t\,(x \leq z \text{ and } t, z \models \psi \text{ and } \forall y \in t\,(x \leq y < z \Rightarrow t, y \models \varphi)) \\
t, x \models \mathsf{EY}\,\varphi & \text{if} & \exists y \in t\,(y \lessdot x \text{ and } t, y \models \varphi) \\
t, x \models \varphi\,\mathsf{S}\,\psi & \text{if} & \exists z \in t\,(z \leq x \text{ and } t, z \models \psi \text{ and } \forall y \in t\,(z < y \leq x \Rightarrow t, y \models \varphi))
\end{array}
$$

Abbreviations

- $\mathsf{F}\,\varphi = \top\,\mathsf{U}\,\varphi$
- $\mathsf{G}\,\varphi = \neg\,\mathsf{F}\,\neg\varphi$

Local temporal logic

Definition: Future formulae

Future formulae: $\mathrm{LocTL}_\Sigma[\mathsf{EX}, \mathsf{U}]$

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

$$t, x \models \varphi \qquad \text{iff} \qquad {\uparrow}x, x \models \varphi$$

Theorem: Diekert & G., IC 06

Let $L \subseteq \mathbb{R}$ be a first-order definable real trace language.
Then there is a future formula $\varphi \in \mathrm{LocTL}_\Sigma[\mathsf{EX}, \mathsf{U}]$ 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: $\mathrm{LocTL}_\Sigma[\mathsf{EY}, \mathsf{S}]$

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

$$t, x \models \varphi \qquad \text{iff} \qquad \downarrow x, x \models \varphi$$

Corollary: Diekert & G., IC 06

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

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

Plan

F and G formulae

Definition: Direct semantics for F and G

$$\begin{array}{lll} t \models_\ell \mathsf{F}\,\varphi & \text{if} & \exists x \in t,\ t, x \models \varphi \\ t \models_\ell \mathsf{G}\,\psi & \text{if} & \forall x \in t,\ t, x \models \psi. \end{array}$$

Remark: $1 \models \mathsf{G}\,\varphi$ but $1 \not\models \mathsf{F}\,\varphi$ for all $\varphi \in \mathrm{LocTL}_\Sigma$

F and G formulae

Definition: Direct semantics for F and G

$$\begin{array}{lll} t \models_\ell \mathsf{F}\,\varphi & \text{if} & \exists x \in t,\ t, x \models \varphi \\ t \models_\ell \mathsf{G}\,\psi & \text{if} & \forall x \in t,\ t, x \models \psi. \end{array}$$

Remark: $1 \models \mathsf{G}\,\varphi$ but $1 \not\models \mathsf{F}\,\varphi$ for all $\varphi \in \mathrm{LocTL}_\Sigma$

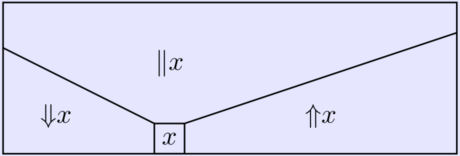
Extension to any boolean combination γ of F and G formulae.

$$\mathcal{L}(\gamma) = \{t \in \mathbb{R} \mid t \models_\ell \gamma\}$$

Concurrent modality

Definition: Local decompotion of traces

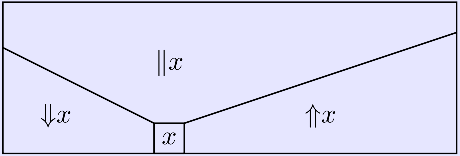
Let $t = [V, \leq, \lambda] \in \mathbb{R}$ and $x \in t$



Concurrent modality

Definition: Local decompotion of traces

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



Definition: Concurrent modality

Let γ be any Boolean combination of F and G formulae.
Then, $\mathsf{CO}\,\gamma$ is a concurrent formula with semantics

$$t, x \models \mathsf{CO}\,\gamma \quad \text{if} \quad \| x \models_{\ell} \gamma.$$

Decomposition formulae

Definition:

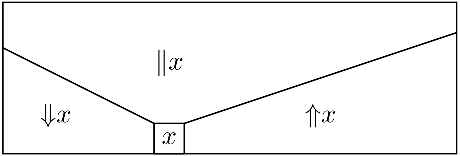
A decomposition formula is a disjunction

$$\delta = \bigvee_{j \in J} a_j \wedge \psi_j \wedge \varphi_j \wedge \mathsf{CO}\, \gamma_j$$

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

- $a_j \in \Sigma$
- $\psi_j \in \mathrm{LocTL}_\Sigma(\mathsf{EY}, \mathsf{S})$ is a past formula
- $\varphi_j \in \mathrm{LocTL}_\Sigma(\mathsf{EX}, \mathsf{U})$ is a future formula
- γ_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*

$$\delta = \bigvee_{j \in J} a_j \wedge \psi_j \wedge \varphi_j \wedge \mathsf{CO}\, \gamma_j$$

such that

1. $L \cup \{1\} = \mathcal{L}(\mathsf{G}\, \delta)$,
2. $L \setminus \{1\} = \mathcal{L}(\mathsf{F}\, \delta)$,
3. $\mathbb{P}\mathrm{ref}(L) = \{r \in \mathbb{P} \mid r, \max(r) \models \bigvee_{j \in J} a_j \wedge \psi_j\}$,
4. for each $j \in J$, the formula $a_j \wedge \psi_j \wedge \varphi_j \wedge \mathsf{CO}\, \gamma_j$ is satisfiable.

Local decomposition: proof sketch

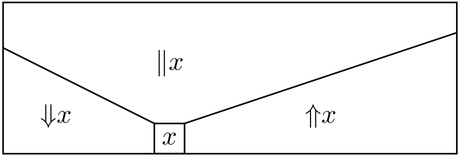
The proof uses

Theorem: Ebinger & Muscholl, TCS 96

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

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

$$t \in [\Downarrow x] \cdot \lambda(x) \cdot [\| x] \cdot [\Uparrow x] \subseteq L$$



Local decomposition: proof sketch

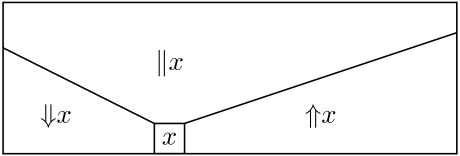
The proof uses

Theorem: Ebinger & Muscholl, TCS 96

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

Let $h : \mathbb{M}(\Sigma, D) \to S$ 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 $h : \mathbb{M}(\Sigma, D) \to S$ 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.

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 φ_j and a past formula ψ_j such that

$$\begin{aligned} a_j \cdot L_j^{\Uparrow} \cap \mathbb{R}^1 &= \{s \in \mathbb{R}^1 \mid s, \min(s) \models \varphi_j\} \\ L_j^{\Downarrow} \cdot a_j \cap \mathbb{P} &= \{r \in \mathbb{P} \mid r, \max(r) \models \psi_j\}. \end{aligned}$$

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 φ_j and a past formula ψ_j such that

$$\begin{aligned} a_j \cdot L_j^{\Uparrow} \cap \mathbb{R}^1 &= \{s \in \mathbb{R}^1 \mid s, \min(s) \models \varphi_j\} \\ L_j^{\Downarrow} \cdot a_j \cap \mathbb{P} &= \{r \in \mathbb{P} \mid r, \max(r) \models \psi_j\}. \end{aligned}$$

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

Let $\gamma_j = \begin{cases} \mathsf{G}\,\delta_j & \text{if } 1 \in L_j^{\|} \\ \mathsf{F}\,\delta_j & \text{otherwise.} \end{cases}$

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 φ_j and a past formula ψ_j such that

$$\begin{aligned} a_j \cdot L_j^{\Uparrow} \cap \mathbb{R}^1 &= \{s \in \mathbb{R}^1 \mid s, \min(s) \models \varphi_j\} \\ L_j^{\Downarrow} \cdot a_j \cap \mathbb{P} &= \{r \in \mathbb{P} \mid r, \max(r) \models \psi_j\}. \end{aligned}$$

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

Let $\gamma_j = \begin{cases} \mathsf{G}\,\delta_j & \text{if } 1 \in L_j^{\|} \\ \mathsf{F}\,\delta_j & \text{otherwise.} \end{cases}$

Claim: the decomposition formula $\delta = \bigvee_{j \in J} a_j \wedge \psi_j \wedge \varphi_j \wedge \mathsf{CO}\,\gamma_j$

satisfies statements (1–4) of the decomposition theorem.

Canonical local safety formulae

Definition:

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

Canonical local safety formulae

Definition:

A *canonical local safety formula* is a formula of type $\mathsf{G}\,\psi$ where $\psi \in \mathrm{LocTL}_\Sigma[\mathsf{EY}, \mathsf{S}]$ 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 $\psi \in \mathrm{LocTL}_\Sigma[\mathsf{EY}, \mathsf{S}]$. Then, $\mathcal{L}(\mathsf{G}\,\psi)$ is locally closed.

Canonical local safety formulae

Definition:

A *canonical local safety formula* is a formula of type $\mathsf{G}\,\psi$ where $\psi \in \mathrm{LocTL}_\Sigma[\mathsf{EY}, \mathsf{S}]$ 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 $\psi \in \mathrm{LocTL}_\Sigma[\mathsf{EY}, \mathsf{S}]$. Then, $\mathcal{L}(\mathsf{G}\,\psi)$ is locally closed.
2. Let $L \subseteq \mathbb{R}$ be a first-order definable language.
   Let $\delta = \bigvee_{j \in J} a_j \wedge \psi_j \wedge \varphi_j \wedge \mathsf{CO}\,\gamma_j$ be a decomposition formula for L.
   Then,

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

Canonical local safety formulae

Example:

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

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

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

Canonical local safety formulae

Example:

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

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

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

Example:

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

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

$$\mathsf{G}\big(c \wedge \mathsf{EY}(\top \mathbin{\mathsf{S}} c) \longrightarrow \neg \mathsf{EY}(a \wedge \mathsf{EY}(a \wedge \mathsf{EY}\, a)) \wedge \neg \mathsf{EY}(b \wedge \mathsf{EY}(b \wedge \mathsf{EY}\, b))\big)$$

Plan

Local safety

Local temporal logic

Local decomposition of first-order languages

4 Local liveness

Strong local liveness

Concluding remarks

Liveness properties

Definition: Liveness

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

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

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

$$\mathrm{Pref}(L) = \mathbb{M}$$

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

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

  $$\mathrm{Pref}(L) = \mathbb{M}$$

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

  A trace $r \in \mathbb{P}$ is locally live w.r.t. $\mathrm{Good} \subseteq \mathbb{R}$ if $r \in \mathbb{P}\mathrm{ref}(\mathrm{Good})$.

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

  $$\mathbb{P}\mathrm{ref}(L) = \mathbb{P}$$

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

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

  $$\mathrm{Pref}(L) = \mathbb{M}$$

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

  A trace $r \in \mathbb{P}$ is locally live w.r.t. $\mathrm{Good} \subseteq \mathbb{R}$ if $r \in \mathbb{P}\mathrm{ref}(\mathrm{Good})$.

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

  $$\mathbb{P}\mathrm{ref}(L) = \mathbb{P}$$

- Any global liveness property is also a local liveness property.

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

$$\mathbb{P} = a^+ \cup b^+ = \mathbb{P}\mathrm{ref}(L)$$

But L is not a global liveness property since

$$\mathrm{Pref}(L) = \mathbb{P}\mathrm{ref}(L) \neq \mathbb{M}$$

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

$$\mathbb{P} = a^+ \cup b^+ = \mathbb{P}\mathrm{ref}(L)$$

But L is not a global liveness property since

$$\mathrm{Pref}(L) = \mathbb{P}\mathrm{ref}(L) \neq \mathbb{M}$$

Example: Global liveness

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

Local density

Definition: Local density

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

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

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

$$\overline{L}^{\ell} = \{t \in \mathbb{R} \mid \mathbb{P}\mathrm{ref}(t) \subseteq \mathbb{P}\mathrm{ref}(L)\}$$

Proposition: local density

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

Canonical local liveness formulae

Definition:

A canonical local liveness formula is of the form $\mathsf{F}\,\delta$ where

$$\delta = \bigvee_{j \in J} a_j \wedge \psi_j \wedge \varphi_j \wedge \mathsf{CO}\,\gamma_j$$

is a decompotion formula such that

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

Canonical local liveness formulae

Definition:

A canonical local liveness formula is of the form $\mathsf{F}\,\delta$ where

$$\delta = \bigvee_{j \in J} a_j \wedge \psi_j \wedge \varphi_j \wedge \mathsf{CO}\,\gamma_j$$

is a decompotion formula such that

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

Proposition: local liveness

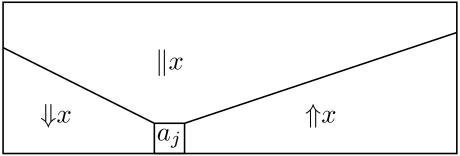
Let $\mathsf{F}\,\delta$ be a canonical local liveness formula.
Then the language $L = \mathcal{L}(\mathsf{F}\,\delta)$ is a local liveness property.

Canonical local liveness formulae

Proof: Sketch

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

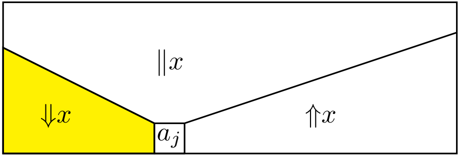
$t =$



Canonical local liveness formulae

Proof: Sketch

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

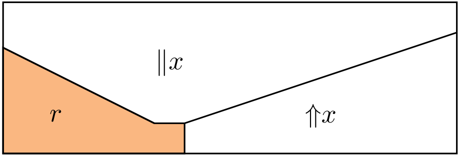
$t =$ 

Canonical local liveness formulae

Proof: Sketch

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

Then, $r \cdot \|x \cdot \Uparrow x \models \mathsf{F}\,\delta$.

$t =$ 

Local liveness

Theorem: Local liveness

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

$$\delta = \bigvee_{j \in J} a_j \wedge \psi_j \wedge \varphi_j \wedge \mathsf{CO}\, \gamma_j$$

be a decomposition formula for L.
Let also $\psi = \bigvee_{j \in J} a_j \wedge \psi_j$. Then,

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

Local liveness

Theorem: Local liveness

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

$$\delta = \bigvee_{j \in J} a_j \wedge \psi_j \wedge \varphi_j \wedge \mathsf{CO}\,\gamma_j$$

be a decomposition formula for L.
Let also $\psi = \bigvee_{j \in J} a_j \wedge \psi_j$. Then,

1. $\overline{L}^{\ell} = \mathcal{L}(\mathsf{G}\,\psi)$.
2. If L is a local liveness property, then ψ is a valid formula and $L \setminus \{1\} = \mathcal{L}(\mathsf{F}\,\delta)$ 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

$$\delta = \bigvee_{j \in J} a_j \wedge \psi_j \wedge \varphi_j \wedge \mathsf{CO}\,\gamma_j$$

be a decomposition formula for L.
Let also $\psi = \bigvee_{j \in J} a_j \wedge \psi_j$. Then,

1. $\overline{L}^{\ell} = \mathcal{L}(\mathsf{G}\,\psi)$.
2. If L is a local liveness property, then ψ is a valid formula and $L \setminus \{1\} = \mathcal{L}(\mathsf{F}\,\delta)$ is defined by a canonical local liveness formula.
3. $\mathsf{F}(\neg\psi \vee \delta)$ is a canonical local liveness formula.
   $\widetilde{L} = \mathcal{L}(\mathsf{F}(\neg\psi \vee \delta)) = (L \setminus \{1\}) \cup (\mathbb{R} \setminus \overline{L}^{\ell})$ 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

5 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.

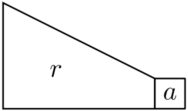
Consider the global partial execution $a^3 b^2$.

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

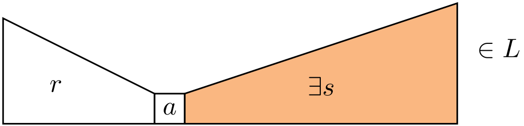
Both local partial execution are locally live.

But the global partial execution is not live.

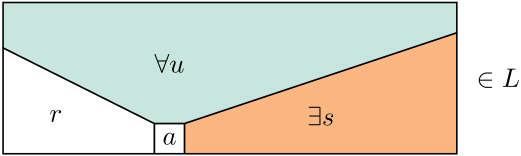
Strong local liveness



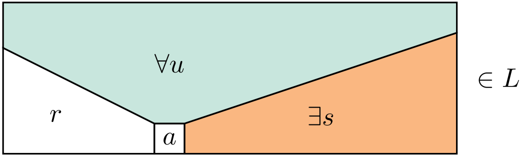
Strong local liveness



Strong local liveness



Strong local liveness



Definition: Strong local liveness

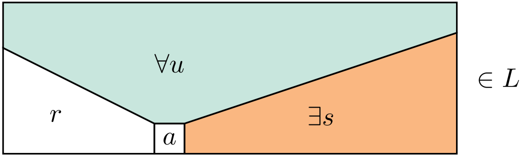
$L \subseteq \mathbb{R}$ is a strong local liveness property (SLLP) if

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

$$raus \in L \qquad \Longleftrightarrow \qquad ras \in L$$

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

Strong local liveness



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 $ra \in \mathbb{P}$, $a \in \Sigma$, $as \in \mathbb{R}^1$ and $\mathrm{alph}(u) \subseteq I(a)$,

$$raus \in L \qquad \Longleftrightarrow \qquad ras \in L$$

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

Proposition: Various liveness

$$\mathrm{SLLP} \subsetneq \mathrm{GLP} \subsetneq \mathrm{LLP}.$$

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

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

such that

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

and such that

$$L \setminus \{1\} = \mathcal{L}(\mathsf{F}\,\delta) \qquad \text{and} \qquad L \cup \{1\} = \mathcal{L}(\mathsf{G}\,\delta)$$

Plan

Local safety

Local temporal logic

Local decomposition of first-order languages

Local liveness

Strong local liveness

6 Concluding remarks

Strong or not?

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

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

Strong or not?

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

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

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.

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

Strong or not?

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

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

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.

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

Proof:

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

Local separation

With a proof similar to the decomposition theorem, we obtain

Theorem: Separation

Let φ be a first-order formula with one free variable.
Then there exists a decomposition formula

$$\delta = \bigvee_{j \in J} a_j \wedge \psi_j \wedge \varphi_j \wedge \mathsf{CO}\, \gamma_j$$

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

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