

# Efficient hierarchical reasoning about functions over numerical domains

Viorica Sofronie-Stokkermans

Max-Planck-Institut für Informatik

Saarbrücken

KI 2008, Kaiserslautern, September 26, 2008

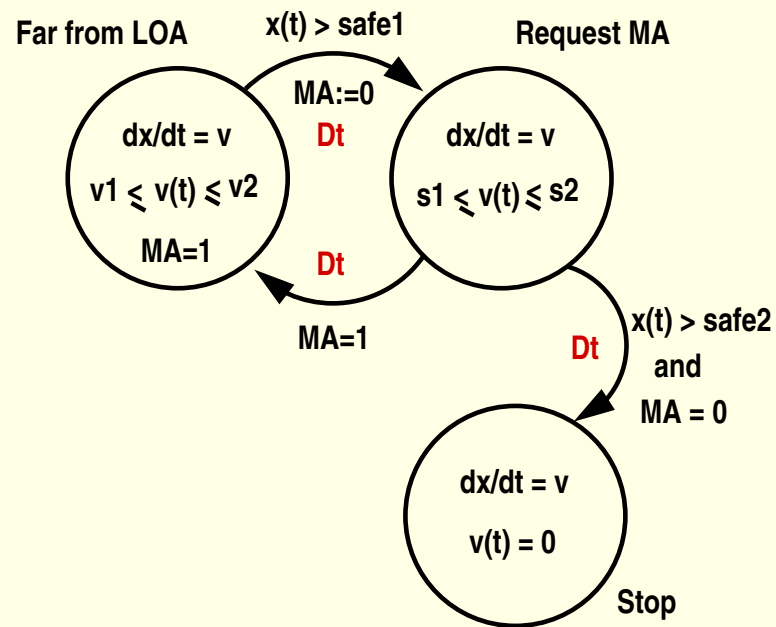
# Goal of the talk

---

- Identify theories from mathematical analysis with the property that:
  - satisfiability of ground sentences is decidable and
  - efficient hierarchical methods exist
  
- Applications

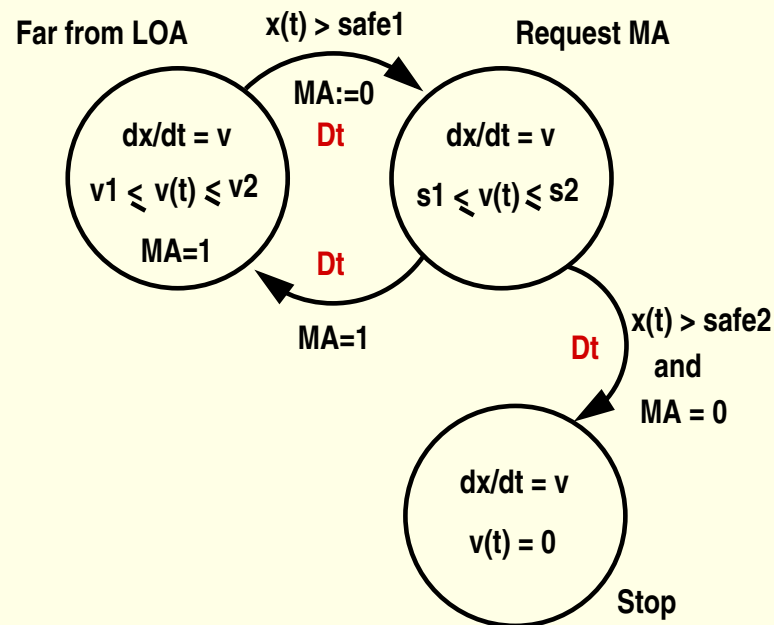
# Motivation

## 1. Verification



# Motivation

## 1. Verification



### Need to have decision procedures involving:

- continuous/derivable functions
- boundedness conditions
- conditions of the form
$$\forall t \leq s, s' \leq t' : a_1 \leq \frac{v(t') - v(t)}{t' - t} \leq a_2$$
- ... perhaps also convexity/concavity conditions, inverse conditions etc.

# Motivation

---

## 2. Mathematics

Automatic reasoning in numerical domains + function symbols whose properties are expressed by first-order axioms: highly non-trivial

- most existing methods are based on heuristics.

# Motivation

---

## 2. Mathematics

Automatic reasoning in numerical domains + function symbols whose properties are expressed by first-order axioms: highly non-trivial

- most existing methods are based on heuristics.

### Existing sound and complete methods:

[Friedman, Seress'90] decision procedure for formulae of the type:

$$(\forall f \in \mathcal{F})\phi(f, x_1, \dots, x_n),$$

where: -  $\mathcal{F}$  is the class of continuous (or differentiable) functions over  $\mathbb{R}$ ,

-  $x_i$  range over  $\mathbb{R}$ , and

-  $\phi$  contains - only existential or only universal quantifiers,

- evaluations of  $f$  and comparisons w.r.t. the order on  $\mathbb{R}$ .

Reasoning about functions which satisfy other types of axioms, or about **several** functions is not considered there.

# Motivation

---

## 2. Mathematics

Automatic reasoning in numerical domains + function symbols whose properties are expressed by first-order axioms: highly non-trivial

- most existing methods are based on heuristics.

### Existing sound and complete methods:

[Cantone et al.'06] decision procedure for the validity of universally quantified sentences over continuous functions satisfying:

- (strict) convexity or concavity conditions, and/or
- monotonicity.

# Our approach

---

We apply recent methods for **hierarchical reasoning in local theory extensions** to the problem of checking the satisfiability of ground formulae involving functions over numerical domains

- we extend the notion of locality to encompass additional axioms
- we give criteria for recognizing locality of such extensions
- we give several examples

We show how these ideas can be used for the verification of the abstraction of a simple case study

# Reminder: Local theory extensions

---

Local theory extensions [VS'05]

$\mathcal{K}$  set of equational clauses;  $\mathcal{T}_0$  theory;  $\mathcal{T}_1 = \mathcal{T}_0 \cup \mathcal{K}$

(Loc)  $\mathcal{T}_0 \subseteq \mathcal{T}_1$  is **local**, if for ground clauses  $G$ ,  
 $\mathcal{T}_0 \cup \mathcal{K} \cup G \models \perp$  iff  $\mathcal{T}_0 \cup \mathcal{K}[G] \cup G$  has no (partial) model

Various notions of locality, depending of the instances to be considered  
e.g. stable locality [Ganzinger'01, GSW'04, VS'05], order locality  
[Basin,Ganzinger'96];

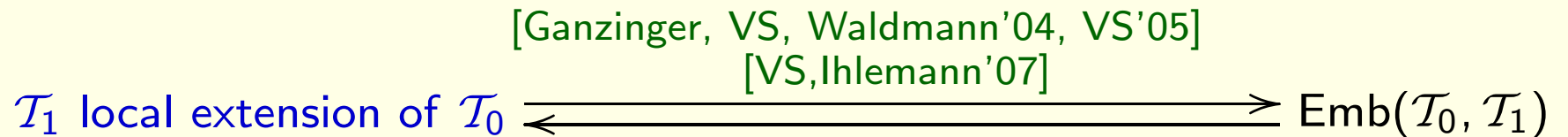
new generalizations of locality: [Ihlemann,Jacobs,VS'08].

# Recognizing local theory extensions

---

**Problem:** Determine if a theory extension is local

**Semantic method:** Embeddability of partial models into total models



# Hierarchical reasoning

---

**Theorem:** Assume that  $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathcal{K}$  is local. The following are equivalent:

- (1)  $\mathcal{T}_0 \cup \mathcal{K} \cup G$  is satisfiable
- (2)  $\mathcal{T}_0 \cup \mathcal{K}[G] \cup G$  has a (partial) model in which all terms in  $G$  are defined
- (3)  $\mathcal{T}_0 \cup \mathcal{K}_0 \cup G_0 \cup \text{Con}[G]_0$  has a (total) model, where  $\text{Con}[G]_0$  is the set of instances of the congruence axioms corresponding to  $D$ :

$$\text{Con}[G]_0 = \left\{ \bigwedge_{i=1}^n c_i = d_i \rightarrow c = d \mid f(c_1, \dots, c_n) = c, f(d_1, \dots, d_n) = d \in D \right\}$$

( $\mathcal{K}_0 \cup G_0 \cup D$  be obtained from  $\mathcal{K}[G] \cup G$  by purification)

**Consequence:** Hierarchical reduction to a satisfiability test in  $\mathcal{T}_0$

# Hierarchical reasoning

**Theorem:** Assume that  $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathcal{K}$  is local. The following are equivalent:

- (1)  $\mathcal{T}_0 \cup \mathcal{K} \cup G$  is satisfiable
- (2)  $\mathcal{T}_0 \cup \mathcal{K}[G] \cup G$  has a (parti
- (3)  $\mathcal{T}_0 \cup \mathcal{K}_0 \cup G_0 \cup \text{Con}[G]_0$   
of instances of the congr

$$\text{Con}[G]_0 = \left\{ \bigwedge_{i=1}^n c_i = d_i \rightarrow \dots \right.$$

( $\mathcal{K}_0 \cup G_0 \cup D$  be obtaine

$$\mathbb{R} \cup \text{Mon}(f) \cup \underbrace{(a < b \wedge f(a) = f(b) + 1)}_G \models \perp$$

$G \cup \text{Mon}(f)$

$$a < b$$

$$f(a) = f(b) + 1$$

$$\forall x (x \leq y \rightarrow f(x) \leq f(y))$$

**Consequence:** Hierarchical reduction to a satisfiability test in  $\mathcal{T}_0$

# Hierarchical reasoning

**Theorem:** Assume that  $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathcal{K}$  is local. The following are equivalent:

- (1)  $\mathcal{T}_0 \cup \mathcal{K} \cup G$  is satisfiable
- (2)  $\mathcal{T}_0 \cup \mathcal{K}[G] \cup G$  has a (parti
- (3)  $\mathcal{T}_0 \cup \mathcal{K}_0 \cup G_0 \cup \text{Con}[G]_0$   
of instances of the congr

$$\text{Con}[G]_0 = \left\{ \bigwedge_{i=1}^n c_i = d_i \rightarrow \dots \right.$$

( $\mathcal{K}_0 \cup G_0 \cup D$  be obtaine

$$\mathbb{R} \cup \text{Mon}(f) \cup \underbrace{(a < b \wedge f(a) = f(b) + 1)}_G \models \perp$$

$G \cup \text{Mon}(f)[G]$

$$a < b$$

$$f(a) = f(b) + 1$$

$$a \leq b \rightarrow f(a) \leq f(b)$$

$$b \leq a \rightarrow f(b) \leq f(a)$$

**Consequence:** Hierarchical reduction to a satisfiability test in  $\mathcal{T}_0$

# Hierarchical reasoning

**Theorem:** Assume that  $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathcal{K}$  is local. The following are equivalent:

- (1)  $\mathcal{T}_0 \cup \mathcal{K} \cup G$  is satisfiable;
- (2)  $\mathcal{T}_0 \cup \mathcal{K}[G] \cup G$  has a (partial)
- (3)  $\mathcal{T}_0 \cup \mathcal{K}_0 \cup G_0 \cup \text{Con}[G]_0$   
of instances of the congruence

$$\text{Con}[G]_0 = \left\{ \bigwedge_{i=1}^n c_i = d_i \rightarrow c = d \right\}$$

( $\mathcal{K}_0 \cup G_0 \cup D$  be obtained

$$\mathbb{R} \cup \text{Mon}(f) \cup \underbrace{(a < b \wedge f(a) = f(b) + 1)}_G \models \perp$$

Definitions	$G_0 \cup \text{Mon}(f)[G]_0 \cup \text{Con}[G]_0$
$a_1 = f(a)$	$a < b$
$b_1 = f(b)$	$a_1 = b_1 + 1$
	$a \leq b \rightarrow a_1 \leq b_1$
	$b \leq a \rightarrow b_1 \leq a_1$
	$a = b \rightarrow a_1 = b_1$

**Consequence:** Hierarchical reduction to a satisfiability test in  $\mathcal{T}_0$ .

# Examples of local theory extensions

---

## 1. Monotonicity conditions

**Theorem** [VS,Ihlemann'07] Any extension of the theory of reals, rationals or integers with functions satisfying  $\text{Mon}^\sigma(f)$  is local.

$$\text{Mon}^\sigma(f) \quad \bigwedge_{i \in I} x_i \leq_i^{\sigma_i} y_i \wedge \bigwedge_{i \notin I} x_i = y_i \rightarrow f(x_1, \dots, x_n) \leq f(y_1, \dots, y_n)$$

**Theorem.** [Jacobs,VS'06] The extension  $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \text{SMon}(f)$  is local if  $\mathcal{T}_0$  is the theory of reals (and  $f : \mathbb{R} \rightarrow \mathbb{R}$ ) or the disjoint combination of the theories of reals and integers (and  $f : \mathbb{Z} \rightarrow \mathbb{R}$ ).

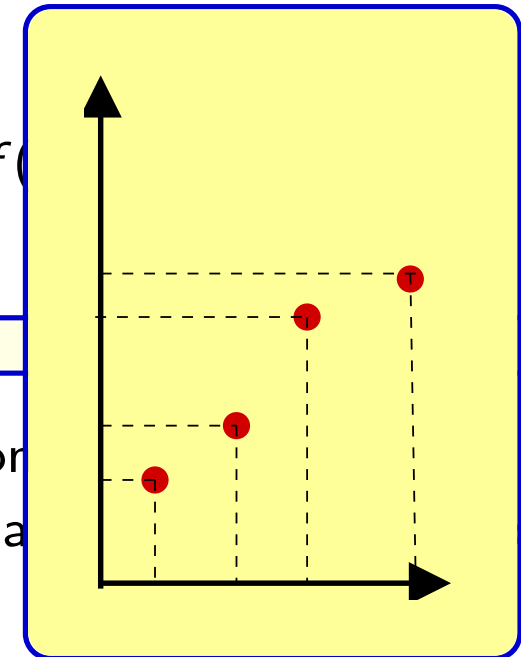
$$\text{SMon}(f) \quad \forall i, j (i < j \rightarrow f(i) < f(j))$$

# Examples of local theory extensions

## 1. Monotonicity conditions

**Theorem** [VS,Ihlemann'07] Any extension of the theory of reals, rationals or integers with functions satisfying  $\text{Mon}^\sigma(f)$  is local.

$$\text{Mon}^\sigma(f) \quad \bigwedge_{i \in I} x_i \leq_i {}^\sigma y_i \wedge \bigwedge_{i \notin I} x_i = y_i \rightarrow f(x_1, \dots, x_n) \leq f(y_1, \dots, y_n)$$



**Theorem.** [Jacobs,VS'06] The extension  $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \text{SMon}(f)$  is local for the theory of reals (and  $f : \mathbb{R} \rightarrow \mathbb{R}$ ) or the disjoint combination of reals and integers (and  $f : \mathbb{Z} \rightarrow \mathbb{R}$ ).

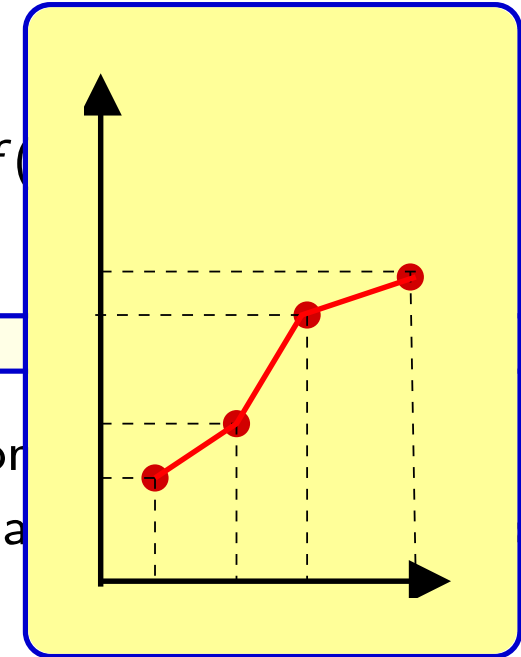
$$\text{SMon}(f) \quad \forall i, j (i < j \rightarrow f(i) < f(j))$$

# Examples of local theory extensions

## 1. Monotonicity conditions

**Theorem** [VS,Ihlemann'07] Any extension of the theory of reals, rationals or integers with functions satisfying  $\text{Mon}^\sigma(f)$  is local.

$$\text{Mon}^\sigma(f) \quad \bigwedge_{i \in I} x_i \leq_i^{\sigma_i} y_i \wedge \bigwedge_{i \notin I} x_i = y_i \rightarrow f(x_1, \dots, x_n) \leq f(y_1, \dots, y_n)$$



**Theorem.** [Jacobs,VS'06] The extension  $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \text{SMon}(f)$  is local for the theory of reals (and  $f : \mathbb{R} \rightarrow \mathbb{R}$ ) or the disjoint combination of reals and integers (and  $f : \mathbb{Z} \rightarrow \mathbb{R}$ ).

$$\text{SMon}(f) \quad \forall i, j (i < j \rightarrow f(i) < f(j))$$

# Examples of local theory extensions

## 2. Boundedness

**Theorem.**  $\mathcal{T}_0$  contains reflexive binary predicate  $\leq$ , and  $f \notin \Sigma_0$ .

$t_1, \dots, t_m, s_1, \dots, s_m$ :  $\Sigma_0$ -terms;  $\phi_1, \dots, \phi_m$ :  $\Pi_0$ -formulae s.t.

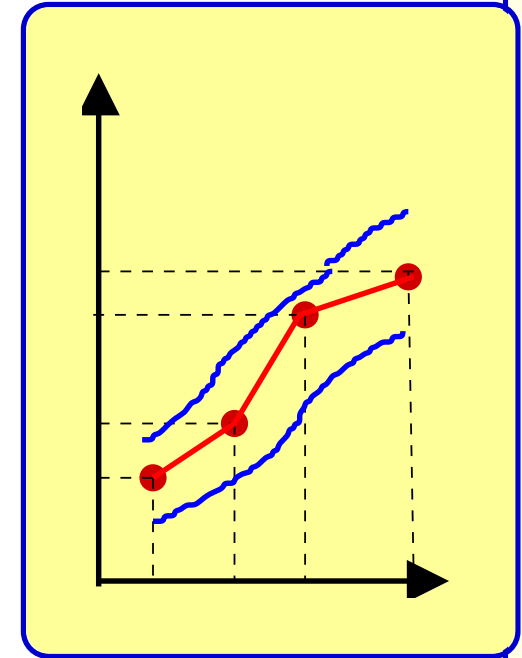
(i)  $\mathcal{T}_0 \models \forall \bar{x}(\phi_i(\bar{x}) \rightarrow s_i(\bar{x}) \leq t_i(\bar{x}))$ ;

(ii) if  $i \neq j$ ,  $\phi_i \wedge \phi_j \models_{\mathcal{T}_0} \perp$ .

$$\text{GB}(f) = \begin{cases} \forall \bar{x}(\phi_1(\bar{x}) \rightarrow s_1(\bar{x}) \leq f(\bar{x}) \leq t_1(\bar{x})) \\ \dots \\ \forall \bar{x}(\phi_m(\bar{x}) \rightarrow s_m(\bar{x}) \leq f(\bar{x}) \leq t_m(\bar{x})) \end{cases}$$

$$\text{Def}(f) = \begin{cases} \forall \bar{x}(\phi_1(\bar{x}) \rightarrow f(\bar{x}) = t_1(\bar{x})) \\ \dots \\ \forall \bar{x}(\phi_m(\bar{x}) \rightarrow f(\bar{x}) = t_m(\bar{x})) \end{cases}$$

The extensions  $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \text{GB}(f)$  and  $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \text{Def}(f)$  are both local.



# Examples of local theory extensions

---

## 2. Boundedness for monotone functions

**Theorem.** Any extension of a theory for which  $\leq$  is a partial order (or at least reflexive) with functions satisfying  $\text{Mon}^\sigma(f)$  and  $\text{Bound}^t(f)$  is local.

$$\text{Bound}^t(f) \quad \forall x_1, \dots, x_n (f(x_1, \dots, x_n) \leq t(x_1, \dots, x_n))$$

where  $t(x_1, \dots, x_n)$  is a  $\Pi_0$ -term whose associated function has the same monotonicity as  $f$  in any model.

Similar results hold for strictly monotone functions.

# Examples of local theory extensions

---

## 3. Injectivity

An extension  $\mathcal{T}_0 \subseteq \mathcal{T}_1 = \mathcal{T}_0 \cup \text{Inj}(f)$  with a function  $f$  of arity  $i \rightarrow e$  satisfying  $\text{Inj}(f)$  is local provided that in all models of  $\mathcal{T}_1$  the cardinality of the support of sort  $i$  is lower or equal to the cardinality of the support of sort  $e$ .

$$\text{Inj}(f) \quad \forall i, j (i \neq j \rightarrow f(i) \neq f(j)).$$

## 4. Inverse conditions

Consider the following inverse condition:

$$\text{Inv}(f, g) \quad \forall x, y (y = f(x) \rightarrow g(y) = x).$$

Let  $\mathcal{T}_0$  be a theory with signature  $\Pi_0 = (S_0, \Sigma_0, \text{Pred})$ . Assume that  $f \in \Sigma_0$  and  $\mathcal{T}_0 \models \text{Inj}(f)$ . Let  $g \notin \Sigma_0$ . The extension  $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \text{Inv}(f, g)$  is local.

# Examples of local theory extensions

---

## 4. Inverse conditions

$\mathcal{T}_0$  theory and  $f, g \notin \Sigma_0$ .  $\mathcal{K}(f)$  set of clauses over  $(\Sigma_0 \cup \{f\}, \text{Pred})$ .

Assume that:

- (1)  $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathcal{K}(f)$  local;
- (2)  $\mathcal{T}_0 \cup \mathcal{K}(f) \models \text{Inj}(f)$ .

Then the following are equivalent:

- (1)  $\mathcal{T}_0 \cup (\mathcal{K}(f) \cup \text{Inv}(f, g)) \cup G \models \perp$ ;
- (2)  $\mathcal{T}_0 \cup (\mathcal{K}(f) \cup \text{Inv}(f, g))[G] \cup G \models \perp$

for all sets  $G$  of ground clauses with the property that if  $g(c)$  occurs in  $G$  then also some  $f(a) = c$  occurs in  $G$ .

# Examples of local theory extensions

---

## 5. Convexity/Concavity

Let  $f$  be a unary function, and  $I = [a, b]$  a subset of the domain of definition of  $f$ . We consider the axiom:

$$\text{Conv}^I(f) \quad \forall x, y, z \left( x, y \in I \wedge x \leq z \leq y \rightarrow \frac{f(z) - f(x)}{z - x} \leq \frac{f(y) - f(x)}{y - x} \right).$$

**Theorem.** The extensions  $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \text{Conv}^I(f)$  and  $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \text{Conc}^I(f)$  are local in each of the following situations:

- (i)  $\mathcal{T}_0 = \mathbb{R}$ , the theory of real numbers, and  $f$  is a new unary function;
- (ii)  $\mathcal{T}_0 = \mathbb{Z}$ , the theory of integers, and  $f$  is a new unary function;
- (iii)  $\mathcal{T}_0$  is the many-sorted combination of the theories of reals (sort real) and integers (sort int) and  $f$  has arity  $\text{int} \rightarrow \text{real}$ .

# Examples of local theory extensions

---

## 6. Lipschitz conditions

Consider the following conditions:

$(L_f^\lambda(c_0))$	$\forall x ( f(x) - f(c_0)  \leq \lambda x - c_0 )$	Lipschitz condition at $c_0$
$(L_f^\lambda)$	$\forall x, y ( f(x) - f(y)  \leq \lambda x - y )$	(uniform) Lipschitz condition
$(BL_f^\lambda)$	$\forall x, y (\frac{1}{\lambda} x - y  \leq  f(x) - f(y)  \leq \lambda x - y )$	bi-Lipschitz condition

**Theorem.** The extensions  $\mathbb{R} \subseteq \mathbb{R} \cup (L_f^\lambda(c_0))$ ,  $\mathbb{R} \subseteq \mathbb{R} \cup (L_f^\lambda)$ , and  $\mathbb{R} \subseteq \mathbb{R} \cup (BL_f^\lambda)$  are local.

Also local are extensions with axioms of the form:

$$(Bd_a^b(f)) \quad \forall x, y (y < x \rightarrow (a * (x - y) \leq f(x) - f(y) \leq b * (x - y)))$$

# Example

---

Illustrate hierarchical reasoning in local extensions of  $\mathbb{R}$

**Main feature:** We do not restrict to proof tasks.

- consider problems with parameters
- the hierarchical reduction to proof tasks in base theory can be used
  - (together with QE): for obtaining constraints on parameters which guarantee (un)satisfiability
  - for model building

# Example

**Given:**  $f : \mathbb{R} \rightarrow \mathbb{R}$  satisfying the bi-Lipschitz condition  $(BL_f^\lambda)$   
 $g : \mathbb{R} \rightarrow \mathbb{R}$ , the inverse of  $f$ , i.e. satisfies  $\text{Inv}(f, g)$

$$(BL_f^\lambda) \quad \forall x, y \left( \frac{1}{\lambda} |x - y| \leq |f(x) - f(y)| \leq \lambda |x - y| \right);$$

$$\text{Inv}(f, g) \quad \forall x, y (y = f(x) \rightarrow g(y) = x).$$

**Task:** Determine whether  $g$  satisfies a bi-Lipschitz condition on the codomain of  $f$ , and if so with which constant.

i.e.: determine under which conditions the following holds:

$$\mathbb{R} \cup BL_f^\lambda \cup \text{Inv}(f, g) \models \underbrace{\forall x, x', y, y' (y = f(x) \wedge y' = f(x') \rightarrow \frac{1}{\lambda_1} |y - y'| \leq |g(y) - g(y')| \leq \lambda_1 |y - y'|)}_{BLG^{\lambda_1}(f, g)}$$

# Example

---

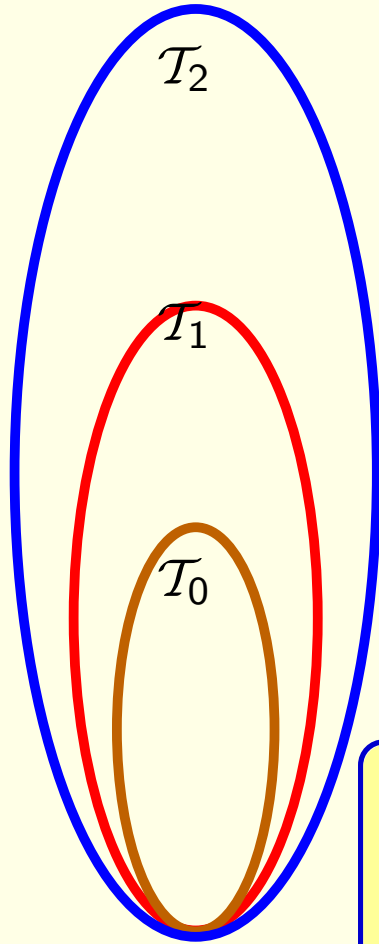
The following are equivalent:

$$(1) \mathbb{R} \cup (\mathbf{BL}_f^\lambda) \cup \mathbf{Inv}(f, g) \models \mathbf{BLG}^{\lambda_1}(f, g)$$

$$(2) c_1=f(a_1) \wedge c_2=f(a_2) \wedge \left( \frac{|c_1-c_2|}{\lambda_1} > |g(c_1)-g(c_2)| \vee |g(c_1)-g(c_2)| > \lambda_1|c_1-c_2| \right) \models_{\mathcal{T}} \perp$$

$$\text{where } \mathcal{T} = \mathbb{R} \cup \mathbf{BL}_f^\lambda \cup \mathbf{Inv}(f, g)$$

# Example



$$\mathcal{T}_2 = \mathcal{T}_1 \cup \text{Inv}(f, g)$$

$$\mathcal{T}_2 \cup \underbrace{\neg \text{BLG}^{\lambda_1}(f, g)}_{G(f, g)} \models \perp$$

$$\Downarrow$$

$$\mathcal{T}_1 = \mathcal{T}_0 \cup \text{BL}^\lambda(f)$$

$$\mathcal{T}_1 \cup \underbrace{\text{Inv}(f, g)[G]_0 \cup G_0 \cup \text{Con}[G]_0}_{G'(f)} \models \perp$$

$$\Downarrow$$

$$\mathcal{T}_0 = \mathbb{R}$$

$$\mathcal{T}_0 \cup \underbrace{\text{BL}^\lambda(f)[G']_0 \cup G'_0}_{G''} \models \perp$$

$$G'' : \begin{cases} \text{BL}_0 : & \frac{1}{\lambda} |a_1 - a_2| \leq |e_1 - e_2| \leq \lambda |a_1 - a_2| \\ \text{Inv}_0 : & (c_1 = e_1 \rightarrow d_1 = a_1) \wedge (c_2 = e_1 \rightarrow d_2 = a_1) \wedge \\ & (c_1 = e_2 \rightarrow d_1 = a_2) \wedge (c_2 = e_2 \rightarrow d_2 = a_2) \\ G_0 : & c_1 = e_1 \wedge c_2 = e_2 \wedge \\ & (|d_1 - d_2| < \frac{|c_1 - c_2|}{\lambda_1} \vee |d_1 - d_2| > \lambda_1 |c_1 - c_2|) \\ \text{Con}[G]_0 : & c_1 = c_2 \rightarrow d_1 = d_2 \wedge a_1 = a_2 \rightarrow e_1 = e_2 \end{cases}$$

(where  $e_i = f(a_i)$ ,  $d_i = g(c_i)$ )

# Example

The following are equivalent:

- (1)  $\models_{\mathcal{T}} \text{BLG}^{\lambda_1}(f, g)$  where  $\mathcal{T} = \mathbb{R} \cup \text{BL}^{\lambda}(f) \cup \text{Inv}(f, g)$ .
- (2)  $\exists a_1, a_2, c_1, c_2, d_1, d_2, e_1, e_2 (\text{BL}_0 \wedge \text{Inv}_0 \wedge G_0 \wedge \text{Con}[G]_0)$  is false.
- (3)  $\lambda_1 \lambda^2 - \lambda < 0 \vee \lambda_1 \lambda - \lambda^2 < 0 \vee \lambda_1 - \lambda < 0 \vee (\lambda_1 \lambda - \lambda^2 > 0 \wedge \lambda_1 = \lambda) \vee$   
 $(\lambda_1^2 \lambda - \lambda_1 > 0 \wedge (\lambda_1^2 - \lambda_1 \lambda < 0 \vee (\lambda_1^2 - \lambda_1 \lambda > 0 \wedge \lambda_1 = \lambda))) \vee$   
 $(\lambda_1^2 \lambda - \lambda_1 > 0 \wedge \lambda_1^2 - \lambda_1 \lambda < 0 \wedge \lambda_1 - \lambda > 0) \vee (\lambda_1^2 \lambda - \lambda_1 > 0 \wedge \lambda_1^2 - \lambda_1 \lambda < 0)$

(obtained by QE (using Redlog) + simplification (interactive))

is false.

$$G'' : \left\{ \begin{array}{l} \text{BL}_0 : \quad \frac{1}{\lambda} |a_1 - a_2| \leq |e_1 - e_2| \leq \lambda |a_1 - a_2| \\ \text{Inv}_0 : \quad (c_1 = e_1 \rightarrow d_1 = a_1) \wedge (c_2 = e_1 \rightarrow d_2 = a_1) \wedge \\ \quad (c_1 = e_2 \rightarrow d_1 = a_2) \wedge (c_2 = e_2 \rightarrow d_2 = a_2) \\ G_0 : \quad c_1 = e_1 \wedge c_2 = e_2 \wedge \\ \quad (|d_1 - d_2| < \frac{|c_1 - c_2|}{\lambda_1} \vee |d_1 - d_2| > \lambda_1 |c_1 - c_2|) \\ \text{Con}[G]_0 : \quad c_1 = c_2 \rightarrow d_1 = d_2 \wedge a_1 = a_2 \rightarrow e_1 = e_2 \end{array} \right.$$

(where  $e_i = f(a_i)$ ,  $d_i = g(c_i)$ )

# Example

---

The following are equivalent:

- (1)  $\models_{\mathcal{T}} \text{BLG}^{\lambda_1}(f, g)$  where  $\mathcal{T} = \mathbb{R} \cup \text{BL}^{\lambda}(f) \cup \text{Inv}(f, g)$ .
- (2)  $\exists a_1, a_2, c_1, c_2, d_1, d_2, e_1, e_2 (\text{BL}_0 \wedge \text{Inv}_0 \wedge G_0 \wedge \text{Con}[G]_0)$  is false.
- (3)  $\lambda_1 \lambda^2 - \lambda < 0 \vee \lambda_1 \lambda - \lambda^2 < 0 \vee \lambda_1 - \lambda < 0 \vee (\lambda_1 \lambda - \lambda^2 > 0 \wedge \lambda_1 = \lambda) \vee$   
 $(\lambda_1^2 \lambda - \lambda_1 > 0 \wedge (\lambda_1^2 - \lambda_1 \lambda < 0 \vee (\lambda_1^2 - \lambda_1 \lambda > 0 \wedge \lambda_1 = \lambda))) \vee$   
 $(\lambda_1^2 \lambda - \lambda_1 > 0 \wedge \lambda_1^2 - \lambda_1 \lambda < 0 \wedge \lambda_1 - \lambda > 0) \vee (\lambda_1^2 \lambda - \lambda_1 > 0 \wedge \lambda_1^2 - \lambda_1 \lambda < 0)$

(obtained by QE (using Redlog) + simplification (interactive))

is false.

If  $\lambda > 1, \lambda_1 > 1$ , formula (3) is equivalent to  $\lambda_1 < \lambda$ .

**Consequence:** If  $\lambda > 1, \lambda_1 > 1$  we have:

$$\mathbb{R} \cup (\text{BL}_f^{\lambda}) \wedge (\text{Inv}(f, g)) \models \text{BLG}^{\lambda_1}(f, g) \quad \text{iff} \quad \lambda_1 \geq \lambda.$$

# Taking additional axioms into account

**Theorem.** Assume that  $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathcal{K}$  is local.

Let  $Ax$  be an additional set of axioms such that every weak partial model  $A$  of  $\mathcal{T}_1$  with totally defined  $\Sigma_0$ -functions weakly embeds into a total model  $B$  of  $\mathcal{T}_0 \cup \mathcal{K} \cup Ax$ .

The following are equivalent:

- (1)  $\mathcal{T}_0 \cup \mathcal{K} \cup Ax \cup G \models \perp$ .
- (2)  $\mathcal{T}_0 \cup \mathcal{K}[G] \cup G$  has a (partial) model in which all terms in  $G$  are defined.
- (3)  $\mathcal{T}_0 \cup \mathcal{K}_0 \cup G_0 \cup \text{Con}[G]_0$  has a (total) model, where  $\text{Con}[G]_0$  is the set of instances of the congruence axioms corresponding to  $D$ :

$$\text{Con}[G]_0 = \left\{ \bigwedge_{i=1}^n c_i = d_i \rightarrow c = d \mid f(c_1, \dots, c_n) = c, f(d_1, \dots, d_n) = d \in D \right\}.$$

( $\mathcal{K}_0 \cup G_0 \cup D$  be obtained from  $\mathcal{K}[G] \cup G$  by purification.)

# Examples

---

## 7. Continuity

We consider the following continuity conditions for a function  $f : \mathbb{R} \rightarrow \mathbb{R}$ :

$$\begin{array}{lll} \text{Cont}_f(c_0) & \forall \epsilon (\epsilon > 0 \rightarrow \exists \delta (\delta > 0 \wedge \forall x (|x - c_0| < \delta \rightarrow |f(x) - f(c_0)| < \epsilon))) & \text{continuity at } c_0 \\ \text{Cont}_f & \forall x (\text{Cont}_f(x)) & \text{continuity} \end{array}$$

Any partial function over the reals with a finite domain of definition extends to a total continuous function over the reals.

**Theorem.**  $\mathbb{R} \cup \text{Cont}_f(c_0)$  and  $\mathbb{R} \cup \text{Cont}_f$  are local extensions of  $\mathbb{R}$ .

# Example

$$\mathbb{R} \cup \text{Cont}(f)(c_0) \stackrel{?}{\models} L_f^\lambda(c_0).$$

The following are equivalent:

(1)  $\mathbb{R} \cup \text{Cont}(f)(c_0) \wedge G \models \perp$

(2)  $\mathbb{R} \cup \text{Free}(f) \wedge G \models \perp$

where  $G = |f(c_1) - f(c_0)| > \lambda|c_1 - c_0|$

(3)  $\mathbb{R} \cup \wedge G_0 \wedge D \models \perp$

where  $D : f(c_1) = d_1 \wedge f(c_0) = d_0,$

$$G_0 = |d_1 - d_0| > \lambda|c_1 - c_0|$$

(4)  $\mathbb{R} \cup G_0 \cup \{c_1 = c_0 \rightarrow d_1 = d_0\} \models \perp$

It can easily be checked that the last problem is satisfiable in  $\mathbb{R}$  ( $\forall \lambda > 0$ ).

**Model generation.** From any satisfying valuation for this problem we can construct a model for  $\mathbb{R} \cup (\text{Cont}(f)(c_0)) \cup \neg(L_f^\lambda(c_0))$  by noticing that we extend every partial function to a total continuous function  $f : \mathbb{R} \rightarrow \mathbb{R}$

# Examples

## 8. Derivability

Consider the following derivability conditions for a (continuous) function  $f$ :

$$\text{Der}(f, f')(c_0) : \quad \forall \epsilon (\epsilon > 0 \rightarrow \exists \delta (\delta > 0 \wedge \forall x (|x - c_0| < \delta \rightarrow |\frac{f(x) - f(c_0)}{x - c_0} - f'(c_0)| < \epsilon)).$$

$$\text{Der}(f, f') : \quad \forall x \text{Der}(f, f')(x).$$

$$\text{Der}^{\leq n}(f, f^1 \dots f^n) : \quad \forall x \text{Der}^{\leq n}(f, f^1, \dots, f^n)(x) \quad (f^0 = f; f^i \text{ } i\text{-th derivative of } f).$$

**Theorem.**  $\mathbb{R} \cup \text{Cont}_f(c_0) \cup \text{Der}(f, f')(c_0)$  and  $\mathbb{R} \cup \text{Cont}_f \cup \text{Der}(f, f')$  are  $\Psi$ -local extensions of  $\mathbb{R}$ , where  $\Psi(T) = T \cup \{f(c) \mid f'(c) \in T\} \cup \{f'(c) \mid f(c) \in T\}$ .

**Theorem.**  $\mathbb{R} \subseteq \mathbb{R} \cup \text{Der}^{\leq n}(f, f^1 \dots f^n)(c_0)$  and  $\mathbb{R} \subseteq \mathbb{R} \cup \text{Der}^{\leq n}(f, f^1 \dots f^n)$  are  $\Psi^n$ -local extensions, where  $\Psi^n(T) = T \cup \{f^k(c) \mid 0 \leq k \leq n \text{ if } f^i(c) \in T \text{ for some } 0 \leq i \leq n\}$ .

# Combinations of axioms

---

Analyzing the previous locality proofs, we notice that the same completion for the partial functions can be used for

- (i) monotone, strictly monotone, convex/concave, Lipschitz and continuous functions over  $\mathbb{R}$ .

The same completion (possibly different from that in (i)) is used

- (ii) for Lipschitz, and for (uniformly) continuous and  $n$ -derivable functions over  $\mathbb{R}$ .

**Theorem.** The following axiom combinations define local extensions of  $\mathbb{R}$ :

- (1) Arbitrary combinations of  $[S]Mon(f)$ ,  $Conv_f$ ,  $L_f^\lambda[(c_0)]$ ,  $BL_f^\lambda$ ,  $Cont_f[(c_0)]$ ;
- (2) Arbitrary combinations of  $L_f^\lambda[(c_0)]$ ,  $BL_f^\lambda$ ,  $Cont_f[(c_0)]$ ,  $Cont_f[(c_0)] \wedge Der(f, f')[(c_0)]$ ,  $Der^{\leq n}(f, f^1, \dots, f^n)(c_0)$ , and  $Der^{\leq n}(f, f^1, \dots, f^n)$ .

# Combinations of axioms

---

However, care is needed when combining  $\text{Der}(f, f')$  with boundedness or monotonicity conditions on  $f'$ , or with convexity/concavity conditions on  $f$  or  $f'$ .

# Combinations of axioms

---

The types of extensions considered before can be combined:

**Theorem.** Let:

- $\{f_1, \dots, f_n\}$  be unary function symbols, and
- $\mathcal{K}_1, \dots, \mathcal{K}_n$  be systems of axioms such that:  
 $\mathcal{K}_i$  is a set of formulae over the signature of  $\mathbb{R}$  augmented with  $f_i$ .

Assume that for every  $i \in \{1, \dots, n\}$ ,  $\mathcal{K}_i$  is in one of the classes considered on the previous slide.

Then  $\mathbb{R} \subseteq \mathbb{R} \cup \mathcal{K}_1 \cup \dots \cup \mathcal{K}_n$  is a local extension.

# Conclusions

---

We applied **hierarchical reasoning in local theory extensions** for reducing

- satisfiability tests for ground formulae with functions over  $\mathbb{R}, \mathbb{Z}$  to
- satisfiability tests in the numerical domains.

## By-products:

- test satisfiability (sound and complete decision procedures in many cases)
- counterexample generation / model building
- inferring constraints on parameters

We have an efficient implementation of hierarchical reasoning (joint work with C. Ihlemann) which can be used for these tasks.

**Ongoing/Future work:** First steps towards identifying types of abstractions of hybrid systems where this method can be used.