Efficient Hierarchical Reasoning about Functions over Numerical Domains

Viorica Sofronie-Stokkermans

Max-Planck-Institut für Informatik, Campus E 1.4, D-66123 Saarbrücken, Germany

Abstract. We show that many properties studied in mathematical analysis (monotonicity, boundedness, inverse, Lipschitz properties possibly combined with continuity, derivability) are expressible by formulae in a class for which sound and complete hierarchical proof methods for testing satisfiability of sets of ground clauses exist. The results are useful for automated reasoning in analysis and in the verification of hybrid systems.

1 Introduction

Efficient reasoning about functions over numerical domains subject to certain properties (monotonicity, convexity, continuity or derivability) is a major challenge both in automated reasoning and in symbolic computation. Besides its theoretical interest, it is very important for verification (especially of hybrid systems). The task of automatically reasoning in extensions of numerical domains with function symbols whose properties are expressed by first-order axioms is highly non-trivial: most existing methods are based on heuristics. Very few sound and complete methods or decidability results exist, even for specific fragments: Decidability of problems related to monotone or continuous functions over $\mathbb{R}$ were studied in [3,4,1]. In [3,4] Harvey Friedman and Akos Seress give a 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 ϕ 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 axioms, or about *several* functions is not considered there. In [1], Domenico Cantone, Gianluca Cincotti, and Giovanni Gallo give a decision procedure for the validity of universally quantified sentences over continuous functions satisfying (strict) convexity or concavity conditions and/or monotonicity.

In this paper we apply recent methods for hierarchical reasoning we developed in [8] to the problem of checking the satisfiability of ground formulae involving functions over numerical domains. The main contributions of the paper are:

(1) We extend the notion of locality of theory extensions in [8] to encompass additional axioms and give criteria for recognizing locality of such extensions.
(2) We give several examples, including theories of functions satisfying various monotonicity, convexity, Lipschitz, continuity or derivability conditions and combinations of such extensions. Thus, our results generalize those in [1].

(3) We illustrate the use of hierarchical reasoning to tasks such as deriving constraints between parameters which ensure (un)satisfiability.

Structure of the paper. In Sect. 1.1 we illustrate the ideas on examples. In Sect. 2 local extensions are defined, and hierarchical reasoning in such extensions, as well as ways of recognizing them are discussed. Section 3 provides a large number of examples from analysis with applications to verification.

1.1 Illustration

Assume that $f{:}\mathbb{R}{\rightarrow}\mathbb{R}$ satisfies the bi-Lipschitz condition (BL^λ_f) with constant λ and g is the inverse of f. We want to determine whether g satisfies the bi-Lipschitz condition on the codomain of f, and if so with which constant λ_1, i.e. to determine under which conditions the following holds:

$$\mathbb{R} \cup (\mathsf{BL}^\lambda_f) \cup (\mathbf{Inv}(f, g)) \models \phi, \tag{1}$$

where $\phi : \forall x, x', y, y' (y{=}f(x) \wedge y'{=}f(x') \rightarrow \frac{1}{\lambda_1}|y - y'| {\leq} |g(y) - g(y')| {\leq} \lambda_1 |y - y'|)$;

$$\begin{array}{ll} (\mathsf{BL}^\lambda_f) & \forall x, y(\frac{1}{\lambda}|x - y| \leq |f(x) - f(y)| \leq \lambda |x - y|); \\ \mathsf{Inv}(f, g) & \forall x, y(y = f(x) \rightarrow g(y) = x). \end{array}$$

Entailment (1) is true iff $\mathbb{R} \cup (\mathsf{BL}^\lambda_f) \cup (\mathbf{Inv}(f, g)) \cup G$ is unsatisfiable, where $G = (c_1{=}f(a_1) \wedge c_2{=}f(a_2) \wedge (\frac{1}{\lambda_1}|c_1{-}c_2| > |g(c_1){-}g(c_2)| \vee |g(c_1){-}g(c_2)| > \lambda_1 |c_1{-}c_2|))$ is the formula obtained by Skolemizing the negation of ϕ.

Standard theorem provers for first order logic cannot be used in such situations. Provers for reals do not know about additional functions. The Nelson-Oppen method [7] for reasoning in combinations of theories cannot be used either.

The method we propose reduces the task of checking whether formula (1) holds to the problem of checking the satisfiability of a set of constraints over $\mathbb{R}$. We first note that for any set G of ground clauses with the property that "*if $g(c)$ occurs in G then G also contains a unit clause of the form $f(a) = c$*" every partial model P of G – where (i) f and g are partial and defined exactly on the ground subterms occurring in G and (ii) P satisfies $\mathsf{BL}^\lambda_f \cup \mathbf{Inv}(f, g)$ at all points where f and g are defined – can be completed to a total model of $\mathbb{R} \cup (\mathsf{BL}^\lambda_f) \cup (\mathbf{Inv}(f, g)) \cup G$ (cf. Thm. 8 and Cor. 9). Therefore, problem (1) is equivalent to

$$\mathbb{R} \cup (\mathsf{BL}^\lambda_f \cup \mathbf{Inv}(f, g))[G] \cup G \models \perp,$$

where $(\mathsf{BL}^\lambda_f \cup \mathbf{Inv}(f, g))[G]$ is the set of those instances of $\mathsf{BL}^\lambda_f \cup \mathbf{Inv}(f, g)$ in which the terms starting with g or f are ground terms occurring in G, i.e.

$$\begin{aligned} (\mathsf{BL}^\lambda_f \cup \mathbf{Inv}(f, g))[G] = {} & \frac{1}{\lambda}|a_1 - a_2| \leq |f(a_1) - f(a_2)| \leq \lambda |a_1 - a_2| \wedge \\ & (c_1 = f(a_1) \rightarrow g(c_1) = a_1) \;\wedge\; (c_2 = f(a_1) \rightarrow g(c_2) = a_1) \wedge \\ & (c_1 = f(a_2) \rightarrow g(c_1) = a_2) \;\wedge\; (c_2 = f(a_2) \rightarrow d(c_2) = a_2). \end{aligned}$$

We separate the numerical symbols from the non-numerical ones by introducing new names for the extension terms, together with their definitions $D = (f(a_1) = e_1 \wedge f(a_2) = e_2 \wedge g(c_1) = d_1 \wedge g(c_2) = d_2)$ and replacing them in $(\mathsf{BL}_f^\lambda \cup \mathbf{Inv}(f,g))[G] \cup G$. The set of formulae obtained this way is $\mathsf{BL}_0 \cup \mathbf{Inv}_0 \cup G_0$. We then use – instead of these definitions – only the instances $\mathsf{Con}[G]_0$ of the congruence axioms for f and g which correspond to these terms. We obtain:

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

Thus, entailment (1) holds iff $\mathsf{BL}_0 \wedge \mathsf{Inv}_0 \wedge G_0 \wedge \mathsf{Con}[G]_0$ is unsatisfiable, i.e. iff

$$\exists a_1, a_2, c_1, c_2, d_1, d_2, e_1, e_2 (\mathsf{BL}_0 \wedge \mathsf{Inv}_0 \wedge G_0 \wedge \mathsf{Con}[G]_0) \text{ is false.}$$

The quantifiers can be eliminated with any QE system for $\mathbb{R}$. We used Redlog [2]; after simplification (w.r.t. $\lambda{>}1, \lambda_1{>}1$ and some consequences) we obtained:

$$\begin{array}{l}
\lambda_1\lambda^2 - \lambda < 0 \ \vee \ \lambda_1\lambda - \lambda^2 < 0 \ \vee \ \lambda_1 - \lambda < 0 \ \vee \ (\lambda_1\lambda - \lambda^2 > 0 \wedge \lambda_1 = \lambda) \ \vee \\
(\lambda_1^2\lambda - \lambda_1 > 0 \ \wedge \ (\lambda_1^2 - \lambda_1\lambda < 0 \ \vee \ (\lambda_1^2 - \lambda_1\lambda > 0 \ \wedge \ \lambda_1 = \lambda))) \ \vee \\
(\lambda_1^2\lambda - \lambda_1 > 0 \ \wedge \ \lambda_1^2 - \lambda_1\lambda < 0 \ \wedge \ \lambda_1 - \lambda > 0) \ \vee \ (\lambda_1^2\lambda - \lambda_1 > 0 \ \wedge \ \lambda_1^2 - \lambda_1\lambda < 0).
\end{array}$$

If $\lambda{>}1, \lambda_1{>}1$, this formula is equivalent to $\lambda_1{<}\lambda$. Hence, if $\lambda{>}1, \lambda_1{>}1$ we have:

$$\mathbb{R} \cup (\mathsf{BL}_f^\lambda) \wedge (\mathbf{Inv}(f,g)) \models \phi, \quad \text{ iff } \lambda_1 \geq \lambda. \tag{2}$$

The constraints we obtain can be used for optimization (e.g. we can show that the smallest value of λ_1 for which g satisfies the bi-Lipschitz condition is λ).

In this paper we investigate situations where this type of reasoning is possible. In Sect. 2 local extensions are defined, and ways of recognizing them, and of hierarchical reasoning in such extensions are discussed. Section 3 provides several examples from analysis with applications to verification.

2 Local Theory Extensions

Let $\mathcal{T}_0$ be a theory with signature $\Pi_0 = (S_0, \Sigma_0, \mathsf{Pred})$, where S_0 is a set of sorts, Σ_0 is a set of function symbols, Pred is a set of predicate symbols. We consider extensions $\mathcal{T}_1$ of $\mathcal{T}_0$ with new sorts and function symbols (i.e. with signature $\Pi = (S_0 \cup S_1, \Sigma_0 \cup \Sigma_1, \mathsf{Pred})$), satisfying a set $\mathcal{K}$ of clauses. We denote such extensions by $\mathcal{T}_0 \subseteq \mathcal{T}_1 = \mathcal{T}_0 \cup \mathcal{K}$. We are interested in disproving ground formulae G in the extension Π^c of Π with new constants Σ_c. This can be done efficiently if we can restrict the number of instances to be taken into account without loss of completeness. In order to describe such situations, we need to refer to "partial models", where only the instances of the problem are defined.

2.1 Total and Partial Models

Partial Π-structures are defined as total ones, with the difference that for every $f \in \Sigma$ with arity n, f_A is a partial function from A^n to A. Evaluating a term t with respect to a variable assignment $\beta : X \to A$ in a partial structure A is the same as for total algebras, except that this evaluation is undefined if $t = f(t_1, \dots, t_n)$ and either one of $\beta(t_i)$ is undefined, or $(\beta(t_1), \dots, \beta(t_n))$ is not in the domain of f_A. For a partial structure A and $\beta : X \to A$, we say that $(A, \beta) \models_w (\neg)P(t_1, \dots, t_n)$ if either (a) some $\beta(t_i)$ is undefined, or (b) $\beta(t_i)$ are all defined and $(\neg)P_A(\beta(t_1), \dots, \beta(t_n))$ holds in A. (A, β) *weakly satisfies a clause* C (notation: $(A, \beta) \models_w C$) if $(A, \beta) \models_w L$ for at least one literal L in C. A *weakly satisfies a set of clauses* $\mathcal{K}$ ($A \models_w \mathcal{K}$) if $(A, \beta) \models_w C$ for all $C \in \mathcal{K}$ and all assignments β.

2.2 Locality

Let Ψ be a closure operator stable under renaming constants, associating with sets $\mathcal{K}$ and T of axioms resp. ground terms, a set $\Psi_{\mathcal{K}}(T)$ of ground terms. We consider condition (Loc^{Ψ}) (cf. also [5]):

(Loc^{Ψ}) for every ground formula G, $\mathcal{T}_1 \cup G \models \perp$ iff $\mathcal{T}_0 \cup \mathcal{K}[\Psi_{\mathcal{K}}(G)] \cup G$ has no weak partial model in which all terms in $\Psi_{\mathcal{K}}(G)$ are defined,

where $\mathcal{K}[\Psi_{\mathcal{K}}(G)]$ consists of all instances of $\mathcal{K}$ in which the terms starting with extension functions are in the set $\Psi_{\mathcal{K}}(G) := \Psi_{\mathcal{K}}(\mathsf{st}(\mathcal{K}, G))$, where $\mathsf{st}(\mathcal{K}, G)$ is the set of ground terms occurring in $\mathcal{K}$ or G. (If Ψ is the identity function, we denote $\mathcal{K}[\Psi_{\mathcal{K}}(G)]$ by $\mathcal{K}[G]$ and the locality condition by (Loc).)

2.3 Hierarchical Reasoning

Assume the extension $\mathcal{T}_0 \subseteq \mathcal{T}_1{=}\mathcal{T}_0{\cup}\mathcal{K}$ satisfies (Loc^{Ψ}). To check if $\mathcal{T}_1{\cup}G \models \perp$ for a set G of ground Π^c-clauses, note that, by locality, $\mathcal{T}_1{\cup}G \models \perp$ iff $\mathcal{T}_0{\cup}\mathcal{K}[\Psi_{\mathcal{K}}(G)]{\cup}G$ has no weak partial model. We *purify* $\mathcal{K}[\Psi_{\mathcal{K}}(G)] \cup G$ by introducing, bottom-up, new constants c_t (from a set Σ_c) for subterms $t = f(g_1, \dots, g_n)$ with $f \in \Sigma_1$, g_i ground $\Sigma_0 \cup \Sigma_c$-terms, together with their definitions $c_t \approx t$. Let D be the set of definitions introduced this way. The formula thus obtained is $\mathcal{K}_0{\cup}G_0{\cup}D$, where $\mathcal{K}_0 \cup G_0$ is obtained from $\mathcal{K}[\Psi_{\mathcal{K}}(G)] \cup G$ by replacing all extension terms with the corresponding constants.

Theorem 1 ([5]) *Assume that $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathcal{K}$ satisfies (Loc^{Ψ}). Let $\mathcal{K}_0 \cup G_0 \cup D$ be obtained from $\mathcal{K}[\Psi_{\mathcal{K}}(G)]{\cup}G$ as explained above. The following are equivalent:*

(1) $\mathcal{T}_0{\cup}\mathcal{K}{\cup}G$ is satisfiable;
(2) $\mathcal{T}_0 \cup \mathcal{K}_0 \cup G_0 \cup \mathsf{Con}[G]_0$ has a (total) model, where $\mathsf{Con}[G]_0$ is the set of instances of the congruence axioms corresponding to D:

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

Thus, if the extension $\mathcal{T}_0 \subseteq \mathcal{T}_1$ satisfies (Loc^{Ψ}) then satisfiability w.r.t. $\mathcal{T}_1$ is decidable for all ground clauses G for which $\mathcal{K}_0 \cup G_0 \cup N_0$ is finite and belongs to a fragment $\mathcal{F}_0$ of $\mathcal{T}_0$ for which checking satisfiability is decidable. Theorem 1 also allows us to give parameterized complexity results for the theory extension:

Theorem 2 *Let $g(m)$ be the complexity of checking the satisfiability w.r.t. $\mathcal{T}_0$ of formulae in $\mathcal{F}_0$ of size m. The complexity of checking satisfiability of a formula G w.r.t. $\mathcal{T}_1$ is of order $g(m)$, where m is a polynomial in $n = |\Psi_{\mathcal{K}}(G)|$ whose degree (≥ 2) depends on the number of extension terms in in $\mathcal{K}$.*

2.4 Recognizing locality

We can recognize local extensions $\mathcal{T}_0 \subseteq \mathcal{T}_1$ by means of flat and linear[1] clauses as follows.

Theorem 3 ([5]) *Assume that $\mathcal{K}$ is flat and linear and $\Psi_{\mathcal{K}}(T)$ is finite for any finite T. If the extension $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathcal{K}$ satisfies condition (Comp_w^{Ψ}) then it satisfies $(\mathsf{Loc})^{\Psi}$, where:*

(Comp_w^{Ψ}) *Every weak partial model A of $\mathcal{T}_1$ with totally defined Σ_0-functions, such that the* definition domains of functions in Σ_1 are finite *and such that the set of terms $f(a_1, \dots, a_n)$ defined in A is closed under Ψ weakly embeds into a total model B of $\mathcal{T}_1$ s.t. $A_{|\Pi_0} \simeq B_{|\Pi_0}$ are isomorphic.*

Theorem 4 (Considering additional axioms.) *Let $\mathcal{A}x_1$ be an additional set of axioms in full first-order logic. Assume that every weak partial model A of $\mathcal{T}_1$ with totally defined Σ_0-functions satisfying the conditions in (Comp_w^{Ψ}) weakly embeds into a total model B of $\mathcal{T}_0 \cup \mathcal{K} \cup \mathcal{A}x_1$. Let G be a set of ground clauses. The following are equivalent:*

(1) $\mathcal{T}_0 \cup \mathcal{K} \cup \mathcal{A}x_1 \cup G \models \perp$.
(2) $\mathcal{T}_0 \cup \mathcal{K}[\Psi_{\mathcal{K}}(G)] \cup G$ *has no partial model in which all ground subterms in* $\mathcal{K}[\Psi_{\mathcal{K}}(G)] \cup G$ *are defined.*

3 Examples of Local Extensions

We give several examples of local extensions of numerical domains. Besides axioms already considered in [8,10,6] (Sect. 3.1) we now look at extensions with functions satisfying inverse conditions, convexity/concavity, continuity and derivability. For the sake of simplicity, we here restrict to unary functions, but most of the results also hold for functions $f : \mathbb{R}^n \to \mathbb{R}^m$.

[1] A *non-ground formula* is Σ_1-*flat* if function symbols (also constants) do not occur as arguments of functions in Σ_1. A Σ_1-flat non-ground formula is called Σ_1-*linear* if whenever a universally quantified variable occurs in two terms which start with functions in Σ_1, the two terms are identical, and if no term which starts with a function in Σ_1 contains two occurrences of the same universal variable.

3.1 Monotonicity and Boundedness Conditions

Any extension of a theory with free function symbols is local. In addition the following theory extensions have been proved to be local in [8,10,6]:

Monotonicity. Any extension of the theory of reals, rationals or integers with functions satisfying $\mathsf{Mon}^\sigma(f)$ is local (($\mathsf{Comp_w}$) holds [8,10]) [2]:

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

The extension $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathsf{SMon}(f)$ is local if $\mathcal{T}_0$ is the theory of reals (and $f : \mathbb{R} \to \mathbb{R}$) or the disjoint combination of the theories of reals and integers (and $f : \mathbb{Z} \to \mathbb{R}$) [5]. The extension of the theory of integers with ($\mathsf{SMon}_\mathbb{Z}(f)$) is local.

$\mathsf{SMon}(f) \quad \forall i,j (i{<}j \rightarrow f(i){<}f(j)) \qquad \mathsf{SMon}_\mathbb{Z}(f) \quad \forall i,j (i{<}j \rightarrow (j{-}i) < f(j){-}f(i)).$

Boundedness. Assume $\mathcal{T}_0$ contains a reflexive binary predicate $\leq$, and $f \notin \Sigma_0$. Let $m \in \mathbb{N}$. For $1 \leq i \leq m$ let $t_i(x_1,\dots,x_n)$ and $s_i(x_1,\dots,x_n)$ be terms in the signature Π_0 and $\phi_i(x_1,\dots,x_n)$ be Π_0-formulae with (free) variables among $x_1,\dots,x_n$, such that $\mathcal{T}_0 \models \forall \overline{x}(\phi_i(\overline{x}) \rightarrow s_i(\overline{x}) \leq t_i(\overline{x}))$, and if $i \neq j$, $\phi_i \wedge \phi_j \models_{\mathcal{T}_0} \perp$. Let $\mathsf{GB}(f){=}\bigwedge_{i=1}^m \mathsf{GB}^{\phi_i}(f)$ and $\mathsf{Def}(f){=}\bigwedge_{i=1}^n \mathsf{Def}^{\phi_i}(f)$, where:

$\mathsf{GB}^{\phi_i}(f) \quad \forall \overline{x}(\phi_i(\overline{x}) \rightarrow s_i(\overline{x}) \leq f(\overline{x}) \leq t_i(\overline{x})) \qquad \mathsf{Def}^{\phi_i}(f) \quad \forall \overline{x}(\phi_i(\overline{x}) \rightarrow f(\overline{x}) = t_i(\overline{x}))$

(i) The extensions $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathsf{GB}(f)$ and $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathsf{Def}(f)$ are both local [10,5].

(ii) Any extension of a theory for which $\leq$ is a partial order (or at least reflexive) with functions satisfying $\mathsf{Mon}^\sigma(f)$ and $\mathsf{Bound}^t(f)$ is local [10,5].

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

where $t(x_1,\dots,x_n)$ is a Π_0-term with variables among $x_1, \dots, x_n$ whose associated function has the same monotonicity as f in any model. Similar results hold for strictly monotone functions.

Injectivity. An extension $\mathcal{T}_0 \subseteq \mathcal{T}_1 = \mathcal{T}_0 \cup \mathsf{Inj}(f)$ with a function f of arity $\mathsf{i} \rightarrow \mathsf{e}$ satisfying $\mathsf{Inj}(f)$ 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.

$$\mathsf{Inj}(f) \;\; \forall i,j (i \neq j \rightarrow f(i) \neq f(j)).$$

3.2 Inverse conditions

Consider the following inverse condition:

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

Such conditions often occur in mathematics and are important in verification (e.g. to model direct and inverse links between certain objects).

[2] For $i \in I$, $\sigma_i {\in} \{-,+\}$, and for $i \notin I$, $\sigma_i{=}0$; $\leq^+ = \leq, \leq^- = \geq$.

Theorem 5 *Let $\mathcal{T}_0$ be a theory with signature $\Pi_0 = (S_0, \Sigma_0, \mathsf{Pred})$. Assume that $f \in \Sigma_0$ and $\mathcal{T}_0 \models \mathsf{Inj}(f)$. Let $g \notin \Sigma_0$. The extension $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathsf{Inv}(f, g)$ is local.*

Proof: Let P be a weak partial model of $\mathcal{T}_0 \cup \mathsf{Inv}(f, g)$. Then $P_{|\Pi_0}$ is a total model of $\mathcal{T}_0$ (hence $f_P : P \to P$ is total and injective) and $g_P : P \to P$ is a partial function such that whenever $b = f(a)$ and $g_P(b)$ is defined, $g_P(b) = a$. Let $c_0 \in P$ be arbitrary but fixed. We define $\overline{g}_P : P \to P$ by:

$$\overline{g}_P(b) = \begin{cases} a & \text{if } b = f_P(a) \text{ for some } a \in P, \\ g(b) & \text{if } g(b) \text{ defined}, \\ c_0 & \text{if } b \notin f_P(P) \text{ and } g(b) \text{ is not defined.} \end{cases}$$

By the injectivity of f_P, $\overline{g}_P$ is well-defined and extends g_P. Thus $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathsf{Inv}(f, g)$ satisfies Comp_w, so it is local. □

Theorem 6 *Let $\mathcal{T}_0$ be a theory and $f, g \notin \Sigma_0$. Let $\mathcal{K}(f)$ be a set of clauses over the signature $(\Sigma_0 \cup \{f\}, \mathsf{Pred})$. Assume that $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathcal{K}(f)$ satisfies Comp_w, and that $\mathcal{T}_0 \cup \mathcal{K}(f) \models \mathsf{Inj}(f)$. Then the following are equivalent:*

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

Proof: Let P be a partial model of $\mathcal{T}_0 \cup (\mathcal{K}(f) \cup \mathsf{Inv}(f, g))[G] \cup G$ in which all ground subterms in $\mathcal{K}(f)$ and G are defined (and no other terms). We use the fact that $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathcal{K}(f)$ satisfies Comp_w to extend f_P to a total function $\overline{f}$. We now extend g_P to a total function $\overline{g} : P \to P$ as follows. Let $p \in P$. If there exists $q \in P$ such that $\overline{f}(q) = p$ we define $\overline{g}(p) = q$. $\overline{g}$ is defined arbitrarily otherwise. As before it is easy to see that $\overline{g}$ is well-defined and extends g_P. □

3.3 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:

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

Theorem 7 *The extensions $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathsf{Conv}^I_f$ and $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathsf{Conc}^I_f$ 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 $\mathsf{int} \to \mathsf{real}$.

Proof: Let P be a partial algebra which weakly satisfies Conv^I_f in which f has a finite definition domain. Let $p_1, \dots, p_n \in \mathbb{R}$ be the points at which f is defined. Let $\overline{f} : \mathbb{R} \to \mathbb{R}$ be obtained by linear interpolation from f. Then $\overline{f}$ is convex. All other cases are proved similarly. □

3.4 Lipschitz Conditions

Consider the following conditions:

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

Such conditions occur in the verification of hybrid systems when specifying (by universal axioms) that the derivative of a function is bounded by a given value.

Theorem 8 *The extensions* $\mathbb{R} \subseteq \mathbb{R} \cup (\mathsf{L}_f^\lambda(c_0))$, $\mathbb{R} \subseteq \mathbb{R} \cup (\mathsf{L}_f^\lambda)$, *and* $\mathbb{R} \subseteq \mathbb{R} \cup (\mathsf{BL}_f^\lambda)$ *satisfy* Comp_w*, hence are local.*

Proof: To prove that $\mathbb{R} \subseteq \mathbb{R} \cup (\mathsf{L}_f^\lambda(c_0))$ satisfies Comp_w it is sufficient to define, for every partial model P, $f_P(p) := c_0$ whenever it is not defined. To prove that $\mathbb{R} \subseteq \mathbb{R} \cup (\mathsf{L}_f^\lambda)$ and $\mathbb{R} \subseteq \mathbb{R} \cup (\mathsf{BL}_f^\lambda)$ satisfy Comp_w, let P be a partial algebra in which f has a finite definition domain. Let $p_1, \dots, p_n \in \mathbb{R}$ be the points at which f is defined. Let $\overline{f} : \mathbb{R} \to \mathbb{R}$ be obtained by linear interpolation from f. It is easy to check that if f satisfies condition L_f^λ then $\overline{f}$ also satisfies L_f^λ, and if f satisfies condition BL_f^λ then $\overline{f}$ also satisfies BL_f^λ. $\square$

From Thms. 6 and 8 we obtain the result used in the illustration in Sect. 1.

Corollary 9 *The extension* $\mathbb{R} \cup \mathsf{BL}_f^\lambda \cup \mathsf{Inv}(f, g)$ *of* $\mathbb{R}$ *has the property that for all sets* G *of ground clauses such that if* $g(c)$ *occurs in* G *then also* $f(a) = c$ *occurs in* G, $\mathbb{R} \cup (\mathsf{BL}_f^\lambda \cup \mathsf{Inv}(f, g)) \cup G \models \perp$ *iff* $\mathbb{R} \cup (\mathsf{BL}_f^\lambda \cup \mathsf{Inv}(f, g))[G] \cup G$ *has no weak partial model in which all subterms of* G *are defined (and only those).*

3.5 Continuity, Derivability

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

$\mathsf{Cont}_f(c_0)$	$\forall \epsilon(\epsilon{>}0 {\to} \exists \delta(\delta{>}0 \wedge \forall x(\lvert x{-}c_0\rvert{<}\delta {\to} \lvert f(x){-}f(c_0)\rvert{<}\epsilon)))$	continuity at c_0
Cont_f	$\forall x(\mathsf{Cont}_f(x))$	continuity

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

$\mathsf{Der}(f, f')(c_0)$: $\quad \forall \epsilon(\epsilon{>}0 {\to} \exists \delta(\delta{>}0 \wedge \forall x(\lvert x{-}c_0\rvert{<}\delta {\to} \lvert \frac{f(x)-f(c_0)}{x-c_0} {-} f'(c_0)\rvert{<}\epsilon)))$

$\mathsf{Der}^{\leq n}(f, f^1, \dots, f^n)(c_0)$: $\quad \bigwedge_{i=1}^{n} \mathsf{Cont}_{f^{i-1}}(c_0) \wedge \mathsf{Der}(f^{i-1}, f^i)(c_0)$

$\mathsf{Der}(f, f') := \forall x \mathsf{Der}(f, f')(x)$; $\mathsf{Der}^{\leq n}(f, f^1, \dots, f^n) = \forall x \mathsf{Der}^{\leq n}(f, f^1, \dots, f^n)(x)$ (axiomatizing derivability – resp. n-times derivability – at every point, where $n \in \mathbb{N} \cup \{\infty\}$, $f^0 = f$ and f^i is the i-th derivative of f).

Theorem 10 *Any partial function over the reals with a finite domain of definition extends to a total continuous function over the reals.*

Proof: For $\mathbb{R} \cup \mathsf{Cont}_f(c_0)$ we can extend any partial model to a total one by defining $\overline{f}(x) := f(x)$ whenever $f(x)$ is defined and $\overline{f}(x) := f(c_0)$ otherwise. For showing that $\mathbb{R} \subseteq \mathbb{R} \cup \mathsf{Cont}_f$ satisfies condition Comp_w we extend any partial model to a total one by taking $\overline{f}$ to be the function obtained by (e.g. linear) interpolation from the partially defined function f_P. We prove that $\mathbb{R} \subseteq \mathbb{R} \cup \mathsf{UCont}_f$ satisfies condition Comp_w as follows: if P is a weak partial model of $\mathbb{R} \cup \mathsf{UCont}_f$, and f_P has a finite definition domain, we use a polynomial interpolation procedure for extending f_P to a *polynomial function* $\overline{f}$ which then is uniformly continuous. $\square$

Theorem 11 *$\mathbb{R} \cup \mathsf{Cont}_f(c_0) \cup \mathsf{Der}(f, f')(c_0)$ and $\mathbb{R} \cup \mathsf{Cont}_f \cup \mathsf{Der}(f, f')$ are Ψ-local extensions of $\mathbb{R}$, where $\Psi(T) = T \cup \{f(c) \mid f'(c) \in T\} \cup \{f'(c) \mid f(c) \in T\}$. $\mathbb{R} \subseteq \mathbb{R} \cup \mathsf{Der}^{\leq n}(f, f^1, \dots, f^n)(c_0)$ and $\mathbb{R} \subseteq \mathbb{R} \cup \mathsf{Der}^{\leq n}(f, f^1, \dots, f^n)$ are Ψ^n-local extensions, where $\Psi^n(T) = T \cup \{f^k(c) \mid 0 \leq k \leq n \text{ if } f^i(c) \in T \text{ for some } 0 \leq i \leq n\}$.*

Proof: We can use any polynomial interpolation theorem to compute a total model from any partial model (e.g. the Hermite interpolation theorem). $\square$

Example 12 We want to check whether $\mathbb{R} \cup \mathsf{Cont}(f)(c_0) \models \mathsf{L}_\mathsf{f}^\lambda(c_0)$. This holds iff $\mathbb{R} \cup \mathsf{Cont}(f)(c_0) \wedge G \models \perp$, where $G = |f(c_1) - f(c_0)| > \lambda |c_1 - c_0|$ is the formula obtained from $\neg \mathsf{L}_\mathsf{f}^\lambda(c_0)$ after Skolemization. We proceed as follows.

Step 1: By Theorem 11, $\mathbb{R} \cup \mathsf{Cont}(f)(c_0) \wedge G \models \perp$ iff $\mathbb{R} \cup \mathsf{Free}(f) \wedge G \models \perp$.

Step 2: We purify G replacing the ground terms starting with f with new constants and replacing the definitions $D = \{f(c_0){=}d_0, f(c_1){=}d_1\}$ with corresponding instances of the congruence axioms, and obtain:

$$\mathsf{Con}[G]_0 \wedge (\mathsf{Free}(f) \wedge G)_0 : \; c_1{=}c_0 {\rightarrow} d_1{=}d_0 \wedge |d_1 - d_0| > \lambda |c_1 - c_0|$$

It can easily be checked that the problem is satisfiable in $\mathbb{R}$. A solution (i.e. real values for c_0, c_1, d_1, λ for which the formula above becomes true) can easily be found by any solver for the reals. An example is the valuation β which assigns c_1 the value $c_0 + 1$, and d_1 the value $d_0 + \lambda + 1$.

Model generation. From any satisfying valuation for this problem, $\beta : X {\rightarrow} \mathbb{R}$ with $\beta(c_0){=}\overline{c}_0, \beta(c_1){=}\overline{c}_1, \beta(d_0){=}\overline{d}_0$, $\beta(d_1){=}\overline{d}_1$, we can construct a model for $\mathbb{R} \cup (\mathsf{Cont}(f)(c_0)) \cup \neg(\mathsf{L}_f^\lambda(c_0))$ by noticing that we extend every partial function with $f(\overline{c}_0) = \overline{d}_0$ and $f(\overline{c}_1) = \overline{d}_1$ to a total continuous function $f : \mathbb{R} \rightarrow \mathbb{R}$ (e.g. a linear function with $f(\overline{c}_0) = \overline{d}_0$ if $\overline{c}_1 = \overline{c}_0$ and $f(x) = \overline{d}_0 + \frac{\overline{d}_1 - \overline{d}_0}{\overline{c}_1 - \overline{c}_0}(x - \overline{c}_0)$ if $\overline{c}_1 \neq \overline{c}_0$).

3.6 Combinations

Analyzing the proofs in the previous sections 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 13 *The following axiom combinations define local extensions of* $\mathbb{R}$*:*

(1) Arbitrary combinations of $[\mathsf{S}]\mathsf{Mon})(f)$, Conv_f, $\mathsf{L}^\lambda_f[(c_0)]$, BL^λ_f, $\mathsf{Cont}_f[(c_0)]$*;*

(2) Arbitrary combinations of $\mathsf{L}^\lambda_f[(c_0)]$, BL^λ_f, $\mathsf{Cont}_f[(c_0)]$, $\mathsf{Cont}_f[(c_0)] \wedge \mathsf{Der}(f, f')[(c_0)]$, $\mathsf{Der}^{\leq n}(f, f^1, .., f^n)(c_0)$*, and* $\mathsf{Der}^{\leq n}(f, f^1, .., f^n)$.

However, care is needed when combining $\mathsf{Der}(f, f')$ with boundedness or monotonicity conditions on f', or with convexity/concavity conditions on f or f'. The types of extensions considered before can be combined up to a certain extent.

Theorem 14 *Let* $\{f_1, \dots, f_n\}$ *be unary function symbols, and* $\mathcal{K}_1, \dots, \mathcal{K}_n$ *be systems of axioms such that for every* i*,* $\mathcal{K}_i$ *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 in Thm. 13. Then* $\mathbb{R} \subseteq \mathbb{R} \cup \mathcal{K}_1 \cup \cdots \cup \mathcal{K}_n$ *is a local extension.*

Proof: Analogous to the proof in [9]. □

The constructions in the previous sections can be relativized to a subinterval I of the domain of definition of the function. We denote this by adding the index I to the corresponding axiom. Locality is preserved for families $\{C^I_f \mid I \in \mathcal{J}\}$ of axioms in the class above relativized over a family of mutually disjoint intervals.

Example 15 We want to determine which constraints on $\lambda, \lambda_1, \lambda_2$ guarantee that if f, g satisfy the Lipschitz conditions at c_0 with coefficients $\lambda_1 > 0, \lambda_2 > 0$ then $f + g$ satisfies the Lipschitz condition at c_0 with coefficient λ, i.e.:

$$\mathbb{R} \cup (\mathsf{L}^{\lambda_1}_{\mathsf{f}}(c_0)) \cup (\mathsf{L}^{\lambda_2}_{\mathsf{g}}(c_0)) \models \mathsf{L}^{\lambda}_{\mathsf{f+g}}(c_0) \tag{3}$$

or, equivalently, that $\mathbb{R} \cup (\mathsf{L}^{\lambda_1}_{\mathsf{f}}(c_0)) \cup (\mathsf{L}^{\lambda_2}_{\mathsf{g}}(c_0)) \cup G \models \perp$, where $G = |f(c) + g(c) - (f(c_0) + g(c_0))| \not\leq \lambda \cdot |c - c_0|$ is the set of ground clauses obtained from $\neg \mathsf{L}^{\lambda}_{\mathsf{f+g}}(c_0)$ by Skolemization.

Step 1. By Theorem 14, $\mathbb{R} \cup (\mathsf{L}^{\lambda_1}_{\mathsf{f}}(c_0)) \cup (\mathsf{L}^{\lambda_2}_{\mathsf{g}}(c_0))$ is a local extension of $\mathbb{R}$, so $\mathbb{R} \cup (\mathsf{L}^{\lambda_1}_{\mathsf{f}}(c_0)) \cup (\mathsf{L}^{\lambda_2}_{\mathsf{g}}(c_0)) \cup G$ is satisfiable iff $\mathbb{R} \cup (\mathsf{L}^{\lambda_1}_{\mathsf{f}}(c_0)) \cup (\mathsf{L}^{\lambda_2}_{\mathsf{g}}(c_0))[G] \cup G$ has a partial model in which $\{c_0, f(c_0), g(c_0), c, f(c), g(c)\}$ (all ground subterms occurring in all terms in $(\mathsf{L}^{\lambda_1}_{\mathsf{f}}(c_0)) \cup (\mathsf{L}^{\lambda_2}_{\mathsf{g}}(c_0))$ or in G) are defined.

Step 2. We purify the new problem by replacing the ground terms starting with f or g with new constants, and obtain a set of definitions $D = \{f(c) \approx d, f(c_0) \approx d_0, g(c) \approx e, g(c_0) \approx e_0\}$ and a set of constraints over $\mathbb{R}$ (we omitted those in which x, y are instantiated with the same constant):

$$|d - d_0| \leq \lambda_1 |c - c_0| \ \wedge \ |e - e_0| \leq \lambda_2 |c - c_0| \ \wedge \ |(d + e) - (d_0 + e_0)| \leq \lambda |c - c_0|$$

This problem is satisfiable iff the problem obtained by replacing D with the corresponding instances $\mathsf{Con}[G]_0$ of the congruence axioms for f, g is satisfiable:

$$\begin{array}{l} c = c_0 \rightarrow d = d_0 \quad \wedge \quad c = c_0 \rightarrow e = e_0 \\ |d - d_0| \leq \lambda_1 |c - c_0| \ \ \wedge \ \ |e - e_0| \leq \lambda_2 |c - c_0| \ \ \wedge \ \ |(d + e) - (d_0 + e_0)| \leq \lambda |c - c_0| \end{array}$$

i.e. iff the following formula is satisfiable (in $\mathbb{R}$):

$$\phi(\lambda_1, \lambda_2, \lambda) = \exists c_0 \exists c \exists d_0 \exists d \exists e_0 \exists e (\lambda_1{>}0 \wedge \lambda_2{>}0 \wedge \lambda{>}0 \wedge (c{\approx}c_0 \rightarrow d{\approx}d_0) \wedge (c{\approx}c_0 \rightarrow e{\approx}e_0) \\ \wedge |d{-}d_0| {\leq} \lambda_1 |c{-}c_0| \wedge |e{-}e_0| {\leq} \lambda_2 |c{-}c_0| \wedge |(d+e) - (d_0 + e_0)| \not\leq \lambda |c - c_0|).$$

After eliminating the quantifiers in ϕ with REDLOG [2] and simplifying the result taking into account that $\lambda_i > 0, \lambda > 0$ we obtain the following equivalent formula:

$$\lambda > 0 \wedge \lambda_1 > 0 \wedge \lambda_2 > 0 \wedge ((\lambda{-}\lambda_1{+}\lambda_2{<}0 \wedge \lambda_1{-}\lambda_2{\geq}0) \vee \\ (\lambda{+}\lambda_1{-}\lambda_2{<}0 \wedge \lambda_1{-}\lambda_2{<}0) \vee (\lambda{+}\lambda_1{-}\lambda_2{<}0 \wedge \lambda_1{-}\lambda_2{\leq}0) \vee \\ \lambda{-}\lambda_2 < 0 \vee \lambda{-}\lambda_1 < 0 \vee (\lambda{-}\lambda_1{-}\lambda_2 < 0 \wedge \lambda_1{+}\lambda_2{\geq}0))$$

which is equivalent to $\lambda < \lambda_1 + \lambda_2 \wedge \lambda_1 > 0 \wedge \lambda_2 > 0 \wedge \lambda > 0$. We thus proved that for $\lambda_1 > 0, \lambda_2 > 0$, and $\lambda > 0$:

$$\mathbb{R} \cup (\mathsf{L}_{\mathsf{f}}^{\lambda_1}) \wedge (\mathsf{L}_{\mathsf{g}}^{\lambda_2}) \models (\mathsf{L}_{\mathsf{f+g}}^{\lambda}) \quad \text{iff} \quad \lambda \geq \lambda_1 + \lambda_2.$$

4 Conclusions

We presented a class of extensions of numerical domains with additional functions for which sound and complete proof methods exist, which allow to reduce testing satisfiability of quantifier-free formulae, hierarchically, to a satisfiability problem in the "base", numerical domain.[3] These results can be applied for automated reasoning in mathematical analysis as well as in verification. An example we considered in the frame of AVACS involved train control systems [6]. We used hierarchical reasoning to determine constraints between the parameters of such control systems which guarantee safety. The new results we present here open new possibilities for efficient verification, since Lipschitz conditions, as well as continuity and derivability conditions occur naturally in the verification of (parametric) hybrid systems (Lipschitz conditions can model e.g. boundedness of derivatives). For tests we used an implementation (cf. also [5]) of the method for hierarchical reasoning in local theory extensions described in [8,5]. All tests and experiments are very encouraging. In the future we will also consider problems involving satisfiability tests for formulae with (alternations) of quantifiers.

Acknowledgments. We thank Thomas Sturm for advise in using REDLOG. This work was partly supported by the German Research Council (DFG) as part of the Transregional Collaborative Research Center "Automatic Verification and Analysis of Complex Systems" (SFB/TR 14 AVACS, `www.avacs.org`).

References

1. D. Cantone, G. Cincotti, and G. Gallo. Decision algorithms for fragments of real analysis. I. Continuous functions with strict convexity and concavity predicates. *Journal of Symbolic Computation*, 41:763–789, 2006.

[3] Note that the hierarchical reduction method we use is sound even for non-local extensions. Locality guarantees completeness for proving validity of universal sentences.

2. A. Dolzmann and T. Sturm. Redlog: Computer algebra meets computer logic. *ACM SIGSAM Bulletin*, 31(2):2–9, 1997.
3. H. Friedman and A. Serres. Decidability in elementary analysis, I. *Adv. in Mathematics*, 76(1):94–115, 1989.
4. H. Friedman and A. Serres. Decidability in elementary analysis, II. *Adv. in Mathematics*, 70(2):1–17, 1990.
5. C. Ihlemann, S. Jacobs, and V. Sofronie-Stokkermans. On local reasoning in verification. In *Proceedings of TACAS 2008, LNCS 4963*, pages 265-281, 2008.
6. S. Jacobs and V. Sofronie-Stokkermans. Applications of hierarchical reasoning in the verification of complex systems. *Electronic Notes in Theoretical Computer Science*, 174(8):39–54, 2007.
7. G. Nelson and D.C. Oppen. Simplification by cooperating decision procedures. *ACM Transactions on Programming Languages and Systems*, 1979.
8. V. Sofronie-Stokkermans. Hierarchic reasoning in local theory extensions. In *20th Int. Conf. on Automated Deduction (CADE-20), LNAI 3632*, pp. 219–234. Springer, 2005.
9. V. Sofronie-Stokkermans. Hierarchical and modular reasoning in complex theories: The case of local theory extensions. In *Proc. 6th Int. Symp. Frontiers of Combining Systems* (FroCos 2007)*, LNCS 4720*, pp. 47–71. Springer, 2007. Invited paper.
10. V. Sofronie-Stokkermans and C. Ihlemann. Automated reasoning in some local extensions of ordered structures. *Journal of Multiple-Valued Logics and Soft Computing* 13(4–6):397–414, 2007.