Foundations for Natural Proofs and Quantifier Instantiation

CHRISTOF LÖDING, RWTH Aachen University
P. MADHUSUDAN, University of Illinois at Urbana-Champaign
LUCAS PEÑA, University of Illinois at Urbana-Champaign

We give foundational results that explain the efficacy of heuristics used for dealing with quantified formulas and recursive definitions. We develop a framework for first order logic (FOL) over an uninterpreted combination of background theories. Our central technical result is that systematic term instantiation is complete for a fragment of FOL that we call safe. Coupled with the fact that unfolding recursive definitions is essentially term instantiation and with the observation that heap verification engines generate verification conditions in the safe fragment explains the efficacy of verification engines like natural proofs that resort to such heuristics. Furthermore, we study recursive definitions with least fixpoint semantics and show that though they are not amenable to complete procedures, we can systematically introduce induction principles that in practice bridge the divide between FOL and FOL with recursive definitions.

ACM Reference format:
Christof Löding, P. Madhusudan, and Lucas Peña. 2017. Foundations for Natural Proofs and Quantifier Instantiation. 1, 1, Article 1 (July 2017), 31 pages.
https://doi.org/10.1145/nnnnnn.nnnnnn

1 INTRODUCTION

Automated reasoning for quantified logics is an important and integral component of program verification. Automated engines for checking validity and satisfiability of quantifier-free logics for combinations of several important theories has made a significant impact in systems verification, especially through their efficient realization in SMT solvers, resulting in robust and scalable engines both for verification and finding bugs using symbolic execution. However, automated quantified reasoning remains mostly driven by heuristics, resulting in tools that are extremely fragile and unpredictable [27, 54, 57]. Furthermore, software verification requires reasoning in logics that are even beyond FOL, especially for reasoning with recursive/inductive definitions, which are not expressible in first-order logic.

The goal of this paper is to provide foundations for a class of heuristics currently used to reason with quantified logics in practice that are based on two paradigms— quantifier instantiation using terms for FOL and the unfold-and-match paradigm to deal with recursive definitions. In particular, we are interested in settings where we can show these heuristics in fact lead to sound and complete reasoning, even though the logics are undecidable.

We work in a reasoning framework that is refutation-based, where, in order to prove a formula \( \varphi \) valid, under some theory \( T \), we build procedures that show that \( \neg \varphi \) is not \( T \)-satisfiable.

Given a formula in FOL that we need to show unsatisfiable, we can write the formula, after Skolemizing, as a universally quantified formula \( \forall \bar{x} \; \psi \). By Herbrand’s Theorem and compactness

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

© 2017 Association for Computing Machinery.

XXXX-XXXX/2017/7-ART1 $15.00
https://doi.org/10.1145/nnnnnn.nnnnnn

, Vol. 1, No. 1, Article 1. Publication date: July 2017.
Uninterpreted Combination of Theories

A primary motivation of our work is to build reasoning for FOL and recursive definitions that can utilize the efficient solvers for quantifier free theories realized as SMT solvers available today. Consequently, we work with a framework called Uninterpreted Combination of Theories (UCT) that explicitly allows reasoning modulo background theories. A UCT is a many-sorted universe where there is a special sort that is declared to be a foreground sort, while the other sorts are declared background sorts. The signature allows functions and relations of any type on the underlying sorts. Furthermore, we allow arbitrary background theories for the various individual background sorts (these will mention only functions and relations that are restricted to the particular background sort, of course). And we insist the foreground sort to be entirely uninterpreted.

Formulas over a UCT can, of course, include any finite axiomatization of the foreground sort; hence any finite axiomatizations are permitted. UCTs can hence be seen as a combination of the background theories that communicate through uninterpreted functions and relations and a new foreground type.

We seek procedures that are both sound and complete for checking unsatisfiability of formulas over UCTs. More precisely, given a formula $\forall \bar{x} \psi$, the goals of this paper are to perform term instantiation for universally quantified variables over the foreground sort, resulting in a sequence of formulas $\phi_1, \phi_2, \phi_3, \ldots$ corresponding to each level of instantiation so that each $\phi_i$ has no foreground quantification and hence is over the combined theory of uninterpreted functions and the background theories. This term instantiation is sound if each $\phi_i$ is implied by $\phi$ and complete if whenever $\forall \bar{x} \psi$ is unsatisfiable, there is some $i \in \mathbb{N}$ such that $\phi_i$ is unsatisfiable.

When the instantiated formulas fall into a class that has a decidable satisfiability problem, a sound and complete term instantiation coupled by checking satisfiability of the formulas at each level of instantiation results in a recursively enumerable procedure for unsatisfiability, and hence for validity.

The Safe Fragment and Completeness

One technique for term instantiation that is followed by many practical tools today is to simply instantiate using the terms (of the appropriate type) occurring in the formula at the previous level of instantiation (i.e., where $\phi_{i+1}$ has variables instantiated with ground terms occurring in $\phi_i$, where $i \geq 0$ and $\phi_0$ is interpreted to be $\forall \bar{x} \psi$). This kind of term instantiation is often effective in practice as it is targeted towards the formula being verified, and is used by the $E$-matching and pattern-based quantification in SMT solvers as well as in the work on natural proofs [33, 46, 49, 56].

Our first result shows that when there are no background theories present, such a term instantiation is actually complete for UCTs. The proof is a slight generalization of the proof that arbitrary term instantiation (not guided by the formula) is sound and complete using Herbrand’s theorem and the compactness theorem [15, 53].

However, in the presence of background theories, we show that this kind of term instantiation is not complete. The central technical contribution of this paper is to identify a safe fragment of FOL over UCTs for which term instantiation is actually a complete procedure.
The safe fragment consists of safe formulas, where a formula is safe if every term with the foreground type occurring in it has all its variables also of the foreground type. This essentially rules out applying functions on terms of the background sorts, that involve universally quantified variables, and that map to the foreground sort. Two simple ways of satisfying the safety requirement are (a) to have no functions that have as part of the domain a background type and map to the foreground type (we call such a UCT as having one-way functions) or (b) that the formula has no quantification over the background sort.

The safe fragment hence admits a much more predictable validity checking procedure, when the background theories are decidable. In particular, for formulas that do not quantify over the background sorts directly, term instantiation is complete, and furthermore results in formulas that are quantifier-free over a combination of the background theories and the theory of uninterpreted functions. When the background theories are individually decidable and stably infinite, these formulas will be decidable using a Nelson-Oppen combination decision procedure, and amenable to solutions provided by current SMT solvers [39].

Beyond FOL: Recursive Definitions and Least Fixpoints

In program verification, not only do we often need quantification to express specifications and invariants, we also require recursively defined properties. For instance, data-structures such as lists, doubly linked lists, trees, binary search trees, AVL trees, etc., are typically defined using recursion. Furthermore, we often need pure recursive functions to aggregate properties of such structures— for example, to define the set of keys stored in a list, to define the height of a tree, to define the sequence defined by a list, and in separation logic, to express the heaplet defined by a data-structure and, more generally, to describe frames that a function modifies in order to support modular reasoning.

Using a simple reduction, we can show that the validity problem for FOL enriched with recursive definitions with least fixpoint semantics is not recursively enumerable, even when there are no background theories present. In fact, there is a fundamental problem in building complete verification engines in the context of program verification when the underlying logic is undecidable. Program configurations are typically enumerable— configurations after all have finitary descriptions, even if they have unbounded datatypes (like integers) or unbounded heaps. Consequently, satisfiability for the logic is recursively enumerable (r.e.) since model-checking formulas for FO enriched with recursive definitions (in fact, for any reasonable logic) over any given finite structure is decidable. Consequently, validity cannot be in r.e. if the validity for the logic is undecidable.

There are several existing program verification systems for reasoning with recursion that use a heuristic roughly known as “unfold-and-match” [9, 24, 29, 33, 40, 46, 49, 56]. These systems involve unfolding recursive definitions a few times, and then finding a simple proof of validity using the unfolded formulas. There is in fact a distinct similarity between unfolding recursive definitions and term instantiation— given an occurrence $r(\bar{t})$ in the formula where $r$ has a recursive definition, unfolding the recursive definition of $r$ at $\bar{t}$ is essentially the same as instantiating the variables $\bar{x}$ in the universally quantified formula $\forall \bar{x}. r(x) \leftrightarrow \phi(r, \bar{x})$ expressing the recursive definition. Furthermore, the instantiated formula will result in new terms that can be instantiated in the next round, corresponding to unfolding the definitions further.

The second contribution of this paper is to show that the completeness result for the safe fragment sheds light on the efficacy of the “unfold-and-match” heuristics used in practice. First, when recursive definitions are just unfolded and used to prove validity, the method essentially ignores the least fixpoint semantics and using only the fact that the definitions define some fixpoint. Moreover, if we are expressing only the fixpoint semantics, then it can be expressed in FOL, and our completeness result says that the method is in fact complete for the safe fragment. We consider one
particular work called *natural proofs* [33, 46, 49, 56] in the literature, and show that the verification conditions obtained for heap verification therein naturally fall into the safe fragment.

In fact, in the work on natural proofs [46, 49], several valid verification conditions are unprovable using “unfold-and-match” techniques, and we show that the reason they are not provable is because they are not valid with respect to *fixpoint* semantics, though they are valid under least fixpoint semantics. In the context of a UCT with Presburger arithmetic as a background theory, this is at first glance puzzling, as recursive definitions can be formulated using fixpoint semantics through induction on natural numbers. However, it turns out that Presburger arithmetic (or any arithmetic) as background theory admits *non-standard* models of arithmetic that prohibit defining such recursive definitions accurately.

In natural proofs [46, 49], the user is required to give additional axioms that provide help in dealing with the incompleteness. The third contribution of this paper is to provide general induction principles that are driven by the property that can be introduced to prove properties involving recursive definitions. These induction principles can be seen as formulae that are valid with respect to least fixpoint semantics of recursive definitions, but not valid with respect to fixpoint semantics. We show an evaluation of these principles in the context of heap verification using natural proofs, showing that the user-given unproven axioms are in fact provable automatically using our automatic insertion of induction principles.

We provide several additional results not mentioned above. One set of results involve logics over arrays. We show that the known decision procedure for the *array property fragment* (APF), which uses finite term instantiation, can be seen as a UCT framework where our term instantiation gives the same decision procedure. Furthermore, we show that non-standard models, being quite non-intuitive, has led to errors in proofs in earlier work. In particular, we point to several errors involving the undecidability of extensions of APF; this leads us to revert one problem, the validity of APF extended with strict inequality between indices, back to being an open problem.

The paper is structured as follows. Section 2 defines many-sorted logic, the UCT framework, and FOL enriched with recursively defined relations with least fixpoint as well as fixpoint semantics. Section 3 considers the simpler setting where there are no background theories, and shows that systematic term instantiation followed by a decision procedure for quantifier-free uninterpreted functions is sound and complete. Section 4 present our main technical results on the safe fragment of FOL with background theories and proves that term instantiation is sound and complete for it. In Section 5 we discuss several ramifications of our main result, in particular in explaining the “unfold-and-match” heuristics in natural proofs, the subtle issues that nonstandard models create when using recursive definitions, and discussions of APF and its extensions. In Section 6, we consider the problem of automatically adding induction principles that bridge the gap created when recursive definitions are treated using fixpoint semantics and show their power in validating the user-provided axioms in the work on natural proofs [46, 49]. Related work is discussed in Section 7 and we conclude with future directions in Section 8.

## 2 DEFINITIONS AND NOTATION

In this section we define some basic notions of many-sorted first-order logic (FOL) with equality, and define the framework of uninterpreted combination of theories (UCT). We also define some formal notions of uninterpreted first-order recursively defined relations.

### 2.1 Many-Sorted Logic

We define a signature as $\Sigma = (S; F; \mathcal{R})$, where $S = \{\sigma_1, \ldots, \sigma_n\}$ is a finite non-empty set of sorts. $F$ is a set of function symbols, where each function $f \in F$ has a type of the form $\tau_1 \times \ldots \times \tau_m \to \tau$. Vol. 1, No. 1, Article 1. Publication date: July 2017.
for some \( m \), with \( \tau_1, \tau \in S \). Function symbols where \( m = 0 \) represent constant symbols of sort \( \tau \) in our signature. Similarly, \( R \) is a set of relation symbols, where each relation \( R \in R \) has a type of the form \( \tau_1 \times \ldots \times \tau_m \). We use = as our infix equality symbol.

For variables, let \( \text{Var}_\tau \) denote the set of variables of sort \( \tau \), where \( \tau \in S \). We abbreviate \( x \in \text{Var}_\tau \) with \( x : \tau \). We sometimes simply use \( x \) if the sort is clear or unimportant. We let \( \overline{x} \) abbreviate \( x_1, \ldots, x_n \). The notation \( \overline{x} : \tau \) abbreviates \( x_1 : \tau, \ldots, x_n : \tau \). If \( n = 0 \), this denotes the empty sequence of variables. We use similar notation for a sequence of terms. A ground term refers to a term \( t \) without any variables.

A \( \Sigma \)-term \( t \) of sort \( \tau \) is formed as

\[
t := x : \tau \mid f(t_1, \ldots, t_m)
\]

where \( f \) has type \( \tau_1 \times \ldots \times \tau_m \rightarrow \tau \), and each \( \Sigma \)-term \( t_i \) is of sort \( \tau_i \).

An atomic \( \Sigma \)-formula \( \psi \) is of the form

\[
\psi := \top | \bot | s = t | R(t_1, \ldots, t_n)
\]

where \( s \) and \( t \) are \( \Sigma \)-terms of the same sort, and \( R \) has type \( \tau_1 \times \ldots \times \tau_n \), and each term \( t_i \) is of sort \( \tau_i \). Finally, a \( \Sigma \)-formula \( \varphi \) takes the form

\[
\varphi := \psi \mid \neg \varphi' \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \rightarrow \varphi_2 \mid \varphi_1 \leftrightarrow \varphi_2 \mid \forall x : \tau. \varphi' \mid \exists x : \tau. \varphi'
\]

where \( \varphi', \varphi_1, \) and \( \varphi_2 \) are \( \Sigma \)-formulas. A quantifier-free \( \Sigma \)-formula is formed using the above grammar, omitting the cases with \( \forall \) and \( \exists \). We often write term instead of \( \Sigma \)-term and formula instead of \( \Sigma \)-formulas when \( \Sigma \) is clear from the context.

An occurrence of a variable \( x \) in a formula is free if it does not occur under the scope of a quantifier for \( x \). By renaming of variables we can assume that each variable only occurs freely in a formula or is quantified by exactly one quantifier in the formula. We write \( \varphi(x_1, \ldots, x_k) \) to indicate that the free variables of \( \varphi \) are among \( x_1, \ldots, x_k \). Substitution of a term \( t \) for all free occurrences of variable \( x \) in a formula \( \varphi \) is denoted \( \varphi[t/x] \). Multiple variables are substituted simultaneously as \( \varphi[t_1/x_1, \ldots, t_n/x_n] \). We abbreviate this by \( \varphi[t/\overline{x}] \).

A model \( M = (U; [\cdot]_M) \) where \( U = \{ U_{\sigma_1}, \ldots, U_{\sigma_n} \} \) contains a set of universes for each sort, and an interpretation function \( [\cdot]_M \). The interpretation function maps each variable \( x \) of sort \( \sigma_1 \) to some concrete element \( u \in U_{\sigma_1} \), each function symbol \( f : \tau_1 \times \ldots \times \tau_m \rightarrow \tau \) to a concrete function \( [f]_M : U_{\tau_1} \times \ldots \times U_{\tau_m} \rightarrow U_{\tau} \), and each relation symbol \( R \) of type \( \tau_1 \times \ldots \times \tau_m \) to a concrete relation \( [R]_M \subseteq U_{\tau_1} \times \ldots \times U_{\tau_m} \). An interpretation function can naturally be extended to terms, such that \( [t]_M \) is the element denoted by the term \( t \) in the model \( M \).

### 2.2 Many-sorted Uninterpreted Combination of Theories (UCT)

We now define the notion of Uninterpreted Combination of Theories (UCT) for many-sorted logic. We use the sort \( \sigma_1 \) as the sort of the “foreground” theory, and \( \sigma_i \) for \( i > 1 \) as the sort for a “background” theory. For each background type, we allow a background theory \( B_{\sigma_i} \) that refers only to function symbols that have type \( \sigma_i^n \rightarrow \sigma_i \) for some \( n \), and relation symbols have type \( \sigma_i^m \) for some \( m \). The background theories be arbitrary (can be just a set of formulas, or presented as an arbitrary axiomatization, even an infinite axiomatization or axiom schema). However, the foreground theory must have no axioms. We refer to this framework as a many-sorted Uninterpreted Combination of Theories (UCT).

We write \( M \models \varphi \) if \( M \) satisfies a formula \( \varphi \) and \( M \models U_{\sigma_i} \models B_{\sigma_i} \) for each sort \( \sigma_i \), under the given interpretation function and standard semantics for the propositional connectives and quantifiers.

We say \( M \models X \) for a set of formulas \( X \) if \( M \models \varphi \) for all \( \varphi \in X \). For a given model \( M \), a formula
\( \varphi(x_1, \ldots, x_k) \) with free variables \( x_1, \ldots, x_k \) of sorts \( \tau_1, \ldots, \tau_k \) defines a relation \( [\varphi]_M \subseteq U_{\tau_1} \times \cdots \times U_{\tau_k} \) that contains the tuples \( (u_1, \ldots, u_k) \) such that \( M \) satisfies \( \varphi \) when each \( x_i \) is interpreted by \( u_i \).

### 2.3 Recursive Definitions

Besides standard first-order logic we use recursive first-order definitions of uninterpreted relations. Before we enter into formal definitions let us give a small example.

**Example 2.1.** Assume that there is an uninterpreted unary function \( f : \sigma_1 \to \sigma_1 \). We can use a recursive definition to define the reflexive and transitive closure of \( f \), which we denote by \( \text{rch}(x, y) \) for reachability:

\[
\varphi_{\text{rch}} := \forall x, y.\varphi(x, y) \iff \varphi_{\text{LFP}}(x, y) = y \lor (x \neq y \land \varphi(\varphi_{\text{rch}}(f(x), y)))
\]

The right-hand side is a formula \( \rho_{\text{rch}} \) with two free variables of same sort as the free variables for the predicate \( \text{rch} \). Furthermore, \( \text{rch} \) occurs only positively in \( \rho \). The formula is satisfied if \( \text{rch} \) is interpreted as the least fixpoint of \( \rho \), which is formalized below.

The recursive definitions that we use here are based on least fixpoints of monotonic functions. In the following, we briefly introduce the corresponding terminology that is required for our purposes.

For more background on first-order recursive definitions, we refer the reader to [37].

For a domain \( D \), a function \( \mu : 2^D \to 2^D \) that maps subsets of \( D \) to subsets of \( D \) is called monotonic if it preserves set inclusion, that is, \( \mu(V_1) \subseteq \mu(V_2) \) for all \( V_1 \subseteq V_2 \subseteq D \). A fixpoint of \( \mu \) is a subset \( V \subseteq D \) of the domain with \( \mu(V) = V \). A monotonic function \( \mu \) has a unique least fixpoint (w.r.t. set inclusion) by the Knaster-Tarski theorem [21]. For the induction principles that are presented in Section 6, we use the notion of pre-fixpoint of \( \mu \), which is a set \( V \subseteq D \) with \( \mu(V) \subseteq V \). For a monotonic function, the least fixpoint is the intersection of all its pre-fixpoints. In particular, the least fixpoint is contained in all the pre-fixpoints.

We use first-order definable monotonic functions for our recursive definitions, as explained below.

Let \( \tau_1, \ldots, \tau_k \in \{ \sigma_1, \ldots, \sigma_n \} \) be sorts, and \( R \) be a relation symbol of sort \( \overline{\tau} := \tau_1 \times \cdots \times \tau_k \). We say that a formula is of sort \( \overline{\tau} \) if it has \( k \) free variables \( x_1, \ldots, x_k \) with \( x_i \) of type \( \tau_i \).

Let \( \rho(\overline{x}) \) be a formula of sort \( \overline{\tau} \) in which \( R \) occurs only positively (under an even number of negations). We also write \( \rho(\overline{x}, R) \) because we view \( R \) as a free second-order variable that is used for a recursive definition.

Let \( M = (U; [\cdot])_M \) where \( U = \{ U_{\sigma_1}, \ldots, U_{\sigma_n} \} \) be a structure. Then \( \rho \) defines a monotonic function \( \mu_\rho \) over \( D = U_{\tau_1} \times \cdots \times U_{\tau_k} \) by

\[
\mu_\rho(V) = (\rho(\overline{x}))^{\{R \to V\}}_M \text{ for } V \subseteq D
\]

where \( (\rho(\overline{x}))^{\{R \to V\}}_M \) denotes the semantics of the formula under the interpretation function \([\cdot]_M \) with the interpretation of \( R \) changed to \( V \). So \( \mu_\rho(V) \) consists of all tuples \( \overline{u} \in D \) that make \( \rho(\overline{x}) \) true when \( R \) is interpreted as \( V \), and \( \overline{x} \) as \( \overline{u} \). Since \( R \) occurs only positively in \( \rho \), the function \( \mu_\rho \) is indeed monotonic. A recursive definition of \( R \) using \( \rho \) is of the form

\[
\varphi_R = \forall \overline{x} : \overline{\tau}.\text{rch}(\overline{x}) \iff \text{LFP}(\rho(\overline{x}))
\]

with \( M \models \varphi_R \) if \( [R]_M \) is the least fixpoint of \( \mu_\rho \). These recursive definitions can be seen as axioms that the model is supposed to satisfy, and we want to prove some property assuming that these axioms are true. So the type of formula we are interested in, is defined as follows. A first-order formula with recursive definitions is of the form \( \varphi = \varphi_A \to \varphi_P \), where \( \varphi_A \) is a conjunction of first-order formulas and recursive definitions (the “axioms”), and \( \varphi_P \) is a first order formula (the
“property”). We are interested in validity of such formulas, which is equivalent to unsatisfiability of their negation $\varphi_A \land \neg \varphi_B$.

Least fixpoints are not definable in first-order logic. If we want to reason about first-order formulas with recursive definitions within first-order logic, then we can replace the $\leftrightarrow_{\text{LFP}}$ in the recursive definitions $\varphi_R$ by the standard equivalence $\leftrightarrow$, which yields the pure FO formula $\forall \overline{x}. R(\overline{x}) \leftrightarrow \rho(\overline{x})$. One can view this step as an abstraction that admits models in which $R$ is interpreted as any fixpoint of $\mu_R$, not necessarily the least fixpoint. Instead of syntactically changing the formula in order to transform recursive definitions into standard FO formulas, we use two different semantics for FO formulas with recursive definitions. We write $M \models_{\text{LFP}} \varphi$ to denote the fact that the FO part of $\varphi$ is satisfied in $M$ and that recursively defined relations $R$ are interpreted as least fixpoints of their definitions. We write $M \models_{\text{FO}} \varphi$ if $\varphi$ is satisfied in $M$ when $\leftrightarrow_{\text{LFP}}$ is interpreted as $\leftrightarrow$. We refer to these two semantics as LFP-semantics and FO-semantics, respectively. Since in the FO-semantics the least fixpoint definitions are simply interpreted by (arbitrary) fixpoints, we also refer to this as fixpoint semantics or FP-semantics.

The following observations are direct consequences of the definitions.

**Remark 2.2.** Let $\varphi$ be an FO formula with recursive definitions.

1. $M \models_{\text{LFP}} \varphi$ implies that $M \models_{\text{FO}} \varphi$ for any model $M$.
2. If $\varphi$ is valid in the FO-semantics, then $\varphi$ is valid in the LFP-semantics.

In Section 6 we substitute the occurrences of $R$ in $\rho(\overline{x}, R)$ by other first-order formulas $\psi$ of same sort as $R$. We denote this by $\rho(\overline{x}, R \leftarrow \psi)$, which is the formula obtained from $\rho(\overline{x}, R)$ by replacing every occurrence of $R(t_1, \ldots, t_k)$ for terms $t_1, \ldots, t_k$ in $\rho$ by $\psi(t_1, \ldots, t_k)$.

In Section 3 and 4 we use first-order logic without recursive definitions. We come back to recursive definitions in Sections 5 and 6.

### 3 PRESERVATION OF SATISFACTION UNDER TERM INSTANTIATION

In this section, we discuss the completeness of using term instantiation to prove validity of universally quantified formulas in first-order logic. We omit the proof of this result as it is an instance of our main technical contribution in Section 4, but it helps lay the groundwork for the more general case discussed in that section.

Assume one has a signature $\Sigma = (\{\sigma_i\}; F; \mathcal{R})$, with function symbols in $F$ and relation symbols in $\mathcal{R}$ purely uninterpreted. Note a single sort $\sigma_i$ is equivalent to the unsorted first-order case. In general we would like to show the validity of a formula of the form $\varphi = \varphi_1 \land \ldots \land \varphi_{n-1} \rightarrow \neg \varphi_n$, where each $\varphi_i$ is universally quantified. Existential quantifiers can be eliminated through Skolemization: $\exists x. \forall y. \exists z. R(x, y, z)$ can be transformed to the formula $\forall y. R(c, y, f(y))$, where we augment our signature with the uninterpreted constant symbol $c$ and uninterpreted function symbol $f$. Note the validity of $\varphi$ is equivalent to the unsatisfiability of $\psi = \neg \varphi_1 \land \ldots \land \varphi_n$, which is the form we assume our formulas take in the sequel.

The term instantiation technique for which we show completeness proceeds intuitively as follows, assuming $\psi$ is a conjunction of universally quantified formulas: begin with all ground terms present in $\psi$. Then, exhaustively instantiate the universally quantified formulas in $\psi$ with those ground terms. If any resulting formula is unsatisfiable, then $\psi$ is unsatisfiable. Otherwise, repeat the process while also using new ground terms introduced from the previous instantiation. With this, we are able to reduce validity in first-order logic to unsatisfiability of quantifier-free formulas over uninterpreted functions with equality.

We note the similarity to Herbrand’s Theorem [15, 53], which also uses term instantiation to prove completeness of FOL by a reduction to propositional logic. Our instantiation differs from Herbrand’s Theorem in two aspects. First of all, we do not need to instantiate the equality axioms
We sketch the proof here, and lay out the lemmas needed for the full proof. Full proofs for the omitted details can be found in the attached supplemental material. First, we create a set $X^*$ of all fully-instantiated formulas from our instantiation process. Next, given any model $M$ of $X^*$, we create a model $M^*$ such that $M \models X^*$ iff $M^* \models \psi$. For most of this model construction, we can simply restrict the interpretation for function and relation symbols from $M$ to the domain in $M^*$. The only hitch in this procedure is the interpretation for function symbols $f$ on elements in the universe of $M^*$ whose result may not be in the universe of $M$. However, for these, it is sufficient to map $[f]_{M^*}$ to an arbitrary element in the universe of $M^*$. Since the result was not in the universe
of $M$, it will not be used in the instantiation process, so it is sufficient to map it to an arbitrary
element in the model $M^*$.

Next, we prove by induction on the term structure that the interpretation of any term arising
from the instantiation process is the same in both $M$ and $M^*$. We use this lemma to prove that all
subformulas of formulas in $X^*$ are equi-satisfiable, which is used to prove that $\psi$ is satisfiable if
and only if $X^*$ is satisfiable. Thus, we show that if a formula is unsatisfiable, there will be a level
within the instantiation process witnessing the unsatisfiability (and vice versa).

Specifically, the unfolding process proceeds as follows: Let $\psi = \varphi_1 \land \ldots \land \varphi_n$ be a closed $\Sigma$-formula,
where each $\varphi_i$ is of the form $\forall \vec{x}. \varphi_i(\vec{x})$ for quantifier-free $\psi_i$. Define $X^*$ and $T^*$ as follows:

$$T_0 = \{ t \mid t \text{ is a ground term occurring in } \psi \}$$
$$X_0 = \{ \psi_i[\vec{t}/\vec{x}] \mid \text{each term in } \vec{t} \text{ is in } T_0 \}$$
$$T_{n+1} = T_n \cup \{ t \mid t \text{ is a ground term occurring in a formula from } X_n \}$$
$$X_{n+1} = X_n \cup \{ \psi_i[\vec{t}/\vec{x}] \mid \text{each term in } \vec{t} \text{ is in } T_{n+1} \}$$
$$X^* = \bigcup_{i \geq 0} X_i \text{ and } T^* = \bigcup_{i \geq 0} T_i$$

We assume $T^*$ is nonempty. $\psi = \neg \varphi = \varphi_1 \land \ldots \land \varphi_{n-1} \implies \neg \varphi_n$. Our main theorem in this section is below:

**Theorem 3.2 (Completeness of Term Instantiation).** $\psi$ is valid if and only if there is an $m$
such that $X_m$ is unsatisfiable.

As explained above, to prove this we need we need to construct a model $M^*$. First, we observe
that each formula in $X^*$ is quantifier-free, and is implied by some formula $\varphi_i$. $X^*$ is thus weaker
than $\psi$.

Let $M = (U; \llbracket \cdot \rrbracket_M)$ be a model that satisfies $\psi$. As we are in the single-sorted case here, $U$
simply represents a universe for sort $\sigma_1$ rather than a family of universes. Let

$$U^* = \{ u \in U \mid u = \llbracket t \rrbracket_M \text{ for some } t \in T^* \}$$

Now, pick an arbitrary $u^* \in U^*$. Such a $u^*$ exists since $T^*$ is assumed to be nonempty. Define the
model $M^* = (U^*; \llbracket \cdot \rrbracket_{M^*})$, where $\llbracket R \rrbracket_{M^*} = \llbracket R \rrbracket_M \upharpoonright U^*$, and for any $f \in F$ and $u_1, \ldots, u_n \in U^*$,

$$\llbracket f \rrbracket_{M^*}(u_1, \ldots, u_n) = \begin{cases} 
\llbracket f \rrbracket_M(u_1, \ldots, u_n) & \text{if } \llbracket f \rrbracket_M(u_1, \ldots, u_n) \in U^* \\
u^* & \text{otherwise}
\end{cases}$$

With this concrete model construction, we use the following lemmas to prove Theorem 3.2.

**Lemma 3.3.** $\forall t \in T^*, \llbracket t \rrbracket_M = \llbracket t \rrbracket_{M^*}$.

**Lemma 3.4.** Let $\psi$ be a subformula of a formula in $X^*$. Then $M \models \psi \iff M^* \models \psi$.

**Lemma 3.5.** For any model $M$, if $M \models X^*$, then $M^* \models \psi$.

**Lemma 3.6.** $\psi$ is satisfiable if and only if then $X^*$ is satisfiable

Proof of Theorem 3.2. Note that $\psi$ is valid $\iff \neg \psi$ is unsatisfiable $\iff$ (by Lemma 9.4) $X^*$ is
unsatisfiable. By compactness of FOL, $X^*$ is unsatisfiable if and only if there is some finite set
$Y \subseteq X^*$ such that $Y$ is unsatisfiable. But since $Y \subseteq X^*$, we must have that $Y \subseteq X_m$ for some $m$.
Since $Y$ is unsatisfiable, so is $X_m$, and this completes the proof. \(\square\)
### 3.3 Decidability

Though our main contribution regards checking validity, it is important to note in which cases the unfolding yields a decision procedure for the satisfiability problem.

**Lemma 3.7.** Let $m \geq 0$ be some number, and consider a class of formulas such that for all formulas form this class in the instantiation process $X_{m+1} = X_m$. Then the satisfiability for this class of formulas is decidable.

**Proof.** Follows immediately from Lemma 9.4, the observation that $X^* = X_m$ and $X_m$ is finite, and that the quantifier-free theory of uninterpreted functions with equality is decidable. □

While this result is not surprising, some decidable classes are subsumed in this fragment. For example, the Bernays-Schönfinkel class [4] is the set of sentences with a prefix of the form $\exists^*\forall^*$ followed by a quantifier-free formula containing no function symbols. Each formula in this class will have a finite unfolding as above, since the quantifier-free formula has no function symbols, and no new function symbols are introduced when eliminating the existential variables, as all existentially quantified variables occur before any universally quantified variables. Thus, we can apply Lemma 3.7 for any formula in this class to give an alternate proof of the decidability of the satisfiability problem for the Bernays-Schönfinkel class.

### 4 TERM INSTANTIATION IN THE PRESENCE OF BACKGROUND THEORIES

We have shown that the method of term instantiation is complete for proving universally quantified statements over uninterpreted functions. We now generalize these ideas to a setting that admits the use of background theories. As explained in Section 2, our logic uses sorts $\sigma_1, \ldots, \sigma_m$, and we assume background theories for the sorts $\sigma_2, \ldots, \sigma_m$. The satisfaction of a formula is considered modulo the background theories, that is, $M \models \varphi$ implicitly also means that $M$ restricted to sort $\sigma_j$ for $j \geq 2$ is a model of the background theory for $\sigma_j$. Validity of $\varphi$ in this context means that all models that satisfy the background theories also satisfy $\varphi$.

As in the previous section, proving validity of a formula is reduced to unsatisfiability of its negation. In the purely uninterpreted case we can deal with arbitrary formulas by eliminating all existential quantifiers using Skolemization. For the instantiation in the presence of background theories, we require that the quantifiers over sort $\sigma_1$ are the outermost ones. Using Skolemization we again reduce those to universal quantifiers only. Hence, the formula that is tested for unsatisfiability is a conjunction $\varphi = \bigwedge_{i=1}^n \varphi_i$ where each $\varphi_i$ is of the form $\forall \bar{x} : \sigma_1. \psi_i(\bar{x})$, where $\psi_i(\bar{x})$ may quantify over sorts $\sigma_j$ (with $j \neq 1$), but does not quantify over sort $\sigma_1$.

The instantiation itself is then defined in the same way as in Section 3, iteratively instantiating the universally quantified variables of sort $\sigma_1$ by ground terms of sort $\sigma_1$:

\[
T_0 := \{ t \mid t \text{ is a ground term of sort } \sigma_1 \text{ occurring in } \varphi \}
\]

\[
X_0 := \{ \psi_i[\bar{t}/\bar{x}] \mid \text{each term in } \bar{t} \text{ is in } T_0 \}
\]

\[
T_{n+1} := T_n \cup \{ t \mid t \text{ is a ground term of sort } \sigma_1 \text{ occurring in a formula from } X_n \}
\]

\[
X_{n+1} = X_n \cup \{ \psi_i[\bar{t}/\bar{x}] \mid \text{each term in } \bar{t} \text{ is in } T_{n+1} \}
\]

\[
X^* = \bigcup_{i \geq 0} X_i \text{ and } T^* = \bigcup_{i \geq 0} T_i
\]

In this definition, we assume that at least one ground term of sort $\sigma_1$ occurs in one of the formulas $\varphi_i$. Otherwise, $T_0$ is defined to contain an arbitrary constant of sort $\sigma_1$. Then $T^*$ and $X^*$ are nonempty.

Our aim is to show that $X^*$ is unsatisfiable if, and only if, $\varphi$ is unsatisfiable. One direction is easy.

**Lemma 4.1.** Each model of $\varphi$ is a model of $X^*$.
For the other direction, we want to modify a model for $X^*$ such that it becomes a model of $\varphi$, such that only the $\sigma_1$ part is modified. This is crucial since in applications we assume that the model for $X^*$ satisfies the background theories for sorts $\sigma_2, \ldots, \sigma_m$. However, such a modification is not possible in general, as illustrated by the following example (the example is artificial to keep it small, one can also come up with natural examples involving, e.g., numbers). In fact, the example shows that term instantiation over the foreground theory is not complete, in general. The set of instantiated formulas is not equisatisfiable with the original formula. One can extend this example to a more complex one showing that even an instantiation including the variables of background sorts does not lead to a complete procedure.

**Example 4.2.** Assume we have sorts $\sigma_1, \sigma_2$ with one constant $d$ of sort $\sigma_1$, and an uninterpreted unary function $g : \sigma_2 \rightarrow \sigma_1$. For sort $\sigma_2$ we have two constants $c_1, c_2$, and the background theory requires $c_1 \neq c_2$.

Let $\varphi = \varphi_1 \land \varphi_2$ with $\varphi_1 := \forall x : \sigma_1, x = d$ and $\varphi_2 := \forall y, z : \sigma_2, y \neq z \rightarrow g(y) \neq g(z)$. These formulas state that $d$ is the only element of sort $\sigma_1$, and that the function $g$ is injective. Note that $\varphi_2$ does not contain variables of sort $\sigma_1$, so $\varphi_2 = \varphi'_2$ with an empty quantifier prefix of universal quantifiers over $\sigma_1$. The only ground term of sort $\sigma_1$ is $d$. Thus, $X^* = \{d = d, \varphi_2\}$ (in $\varphi_1$ is instantiated by $d$, and in $\varphi_2$ there is no variable to be instantiated).

A possible model for $X^*$ is the following one: There are elements $d, d'$ of sort $\sigma_1$, and $c, c'$ of sort $\sigma_2$ with $g(c) = d$ and $g(c') = d'$. However, the original formula is certainly unsatisfiable because it requires $d = g(c_1) \neq g(c_2) = d$.

The problem in this example is comes from the fact that properties of the $\sigma_2$-part of the model imply properties of the $\sigma_1$-part but these properties are not captured by the term instantiation. To avoid this, we assume a restriction on the terms used in $\varphi$, as defined below.

### 4.1 Completeness of Term Instantiation for Safe Formulas

A term $t$ is called $\sigma_1$-guarded if it only contains variables of sort $\sigma_1$. We say that the formula $\varphi$ is $\sigma_1$-safe (or just safe, for short) if all subterms of sort $\sigma_1$ that occur in $\varphi$ are $\sigma_1$-guarded. Note that the formula $\varphi_2$ from Example 4.2 violates the condition because it contains, for example, the term $g(y)$ which is of sort $\sigma_1$ but contains the variable $y$ of sort $\sigma_2$.

We point out that $\varphi$ being safe is a natural restriction that will usually be satisfied in applications. There are at least two natural scenarios that imply that $\varphi$ is safe. Obviously, $\varphi$ is safe if it does not use quantification over sorts $\sigma_2, \ldots, \sigma_m$ because then all variables are of sort $\sigma_1$. In the other scenario, every uninterpreted function $f$ with range $\sigma_1$ has domain $\sigma_1^k$ (so there are no functions producing $\sigma_1$ elements from arguments that are not of sort $\sigma_1$). We refer to such functions as one-way functions. In this case, each term of sort $\sigma_1$ only has subterms of sort $\sigma_1$ (in particular the variables) and is therefore $\sigma_1$-guarded. This is summarized in the following proposition.

**Proposition 4.3.** If $\varphi$ only quantifies over the elements of the foreground theory, or if the signature only contains one-way functions, then $\varphi$ is safe.

We now explain how to modify the $\sigma_1$-part of a model for $X^*$ such that it becomes a model of $\varphi$ under the assumption that $\varphi$ is safe. Its definition does not depend on the fact that $\varphi$ is safe, only its correctness (in the proof of Lemma 4.5 below).

Let $M = (U; \llbracket \cdot \rrbracket_M)$ be a model with $M \models X^*$, where $U = \{U_{\sigma_1}, \ldots, U_{\sigma_m}\}$ is a set of universes for each sort, and $\llbracket \cdot \rrbracket_M$ assigns concrete functions $\llbracket f \rrbracket_M$ and relations $\llbracket R \rrbracket_M$ to the corresponding symbols in the signature.
The construction of $M^*$ is very similar to the construction presented in Section 3. Let

$$U^*_\sigma = \{ u \in U_\sigma \mid u = \llbracket t \rrbracket_M \text{ for some } t \in T^* \}$$

and let $S^* = \{ U^*_\sigma_1, U^*_\sigma_2, \ldots, U^*_\sigma_m \}$. Now, pick an arbitrary $u^* \in U^*_\sigma_1$. Such a $u^*$ exists since $T^*$ is nonempty. Define the model $M^* = (S^*; \llbracket \cdot \rrbracket_{M^*})$ as follows:

1. The relation $[R]_{M^*}$ is the restriction of $[R]_M$ to the new domain $S^*$.
2. Let $f : \sigma_1 \times \cdots \times \sigma_k \rightarrow \sigma_j$ be a function symbol.
   
   (a) If $j \neq 1$, then $[f]_{M^*}$ is the restriction of $[f]_M$ to the new domain (the range did not change).
   
   (b) if $j = 1$, then $[f]_{M^*}(u_1, \ldots, u_n) = \begin{cases} [f]_M(u_1, \ldots, u_n) & \text{if } [f]_M(u_1, \ldots, u_n) \in U^*_{\sigma_1} \\ u^* & \text{otherwise.} \end{cases}$

We first show that the interpretation of the terms in $T^*$ are the same in $M$ and $M^*$.

**Lemma 4.4.** Let $t$ be a subterm of a term in $T^*$. Then $\llbracket t \rrbracket_M = \llbracket t \rrbracket_{M^*}$.

**Proof.** By induction on the structure of $t$. Note that the terms in $T^*$ are all of sort $\sigma_1$ but may contain subterms of different sorts. So we have to consider these cases, too.

If $t = c$ is a constant of sort $\sigma_1$, then $[c]_M \in U^*_{\sigma_1}$ by definition of $U^*_\sigma$ and thus $[c]_{M^*} = [c]_M$ by definition (2b) of the functions in $M^*$. If $t = c$ is a constant of sort different from $\sigma_1$, then its interpretation is the same in $M$ and $M^*$ by definition (2a) of the functions in $M^*$.

If $t = f(t_1, \ldots, t_n)$, then $\llbracket t \rrbracket_M = \llbracket t \rrbracket_{M^*}$ by induction. If $t$ is of sort different from $\sigma_1$, then the claim follows again by definition (2a) of the functions in $M^*$. If $t$ is of sort $\sigma_1$, then $\llbracket t \rrbracket_{M^*} = [f]_{M^*}(\llbracket t_1 \rrbracket_{M^*}, \ldots, \llbracket t_n \rrbracket_{M^*}) = [f]_M(\llbracket t_1 \rrbracket_M, \ldots, \llbracket t_n \rrbracket_M) = \llbracket t \rrbracket_M$ where (†) follows from (2b) of the definition of the functions in $M^*$ and the fact that $\llbracket t \rrbracket_M = [f]_M(\llbracket t_1 \rrbracket_M, \ldots, \llbracket t_n \rrbracket_M)$ is an element of $U^*_\sigma_1$.

We now lift Lemma 4.4 to the formulas in $X^*$.

**Lemma 4.5.** Let $\psi(\overline{y})$ be a subformula of a formula in $X^*$ and let $\overline{u}$ be a sequence of elements from $S^*$ matching the sorts of the variables in $\overline{y}$. If $\varphi$ is safe, then $M \models \psi(\overline{u})$ iff $M^* \models \psi(\overline{u})$.

**Proof.** Note that all variables of sort $\sigma_1$ have been instantiated by ground terms in the formulas of $X^*$, and therefore the variables in $\overline{y}$ are of sorts different from $\sigma_1$.

We prove the claim by induction on the structure of $\psi$. For the base case, $\psi$ is of the form $R(t_1, \ldots, t_n)$ for a predicate $R$, or of the form $t_1 = t_2$. We claim that all subterms of the terms $t_i$ (with variables from $\overline{y}$ substituted by the corresponding elements from $\overline{u}$) evaluate to the same elements in $M$ and $M^*$. Subterms of sort $\sigma_1$ must be ground terms because $\varphi$ is safe and all variables of sort $\sigma_1$ have been instantiated by ground terms. Therefore they are in $T^*$ and the claim follows from Lemma 4.4. For the other subterms it follows from the fact that the models $M$ and $M^*$ are the same for all sorts different from $\sigma_1$. Thus, by definition of the relations in $M^*$, the case of atomic formulas follows.

The Boolean connectives are immediate, and if $\psi$ is of the form $\forall \overline{y}' : \sigma. \psi'(\overline{y}, \overline{y}')$ where $\sigma \neq \sigma_1$, we conclude as follows:

$$M \models \forall \overline{y}' : \sigma. \psi'(\overline{u}, \overline{u}') \iff M \models \psi'(\overline{u}, \overline{u}') \text{ for all } \overline{u}' \in U_\sigma \iff (\dagger) M^* \models \forall \overline{y}' : \sigma. \psi'(\overline{u}, \overline{u}')$$

where (†) holds by induction.

The case of existential quantification can be obtained from the Boolean laws and the case of universal quantification.
Lemma 4.6. Let $\varphi$ be safe. If $M \models X^*$, then $M^* \models \varphi$.

Proof. Since each $\varphi_i$ is of the form $\forall \overline{x} : \sigma_1 \cdot \psi_i(\overline{x})$, we need to show $M^* \models \psi_i(\overline{u})$ for all tuples $\overline{u}$ of elements from $U^*_{\sigma_1}$. Indeed, for each $\overline{u}$, we know there is a tuple $\overline{t}$ of terms from $T^*$ such that $\overline{u} = [\overline{t}]_M$ by definition of $U^*$. The formula $\psi_i(\overline{t})$ is contained in $X^*$, and thus $M \models \psi_i(\overline{t})$ since we assume that $M \models X^*$. Lemma 4.5 yields that $M^* \models \psi_i(\overline{t})$. By Lemma 4.4, $[\overline{t}]_M = [\overline{t}]_{M^*}$, and thus $M^* \models \psi_i(\overline{u})$. \hfill $\square$

We can now formulate the completeness result of term instantiation in the presence of background theories for safe formulas.

Theorem 4.7 (Completeness of Term Instantiation with Background Theories). Let $\varphi$ be a safe formula over a combination of theories. If $\varphi$ is unsatisfiable, then there is a level $X_i$ of the term instantiation such that $X_i$ is unsatisfiable.

Proof. If $\varphi$ is unsatisfiable, then $X^*$ is unsatisfiable by Lemma 4.6. By compactness of FOL, there is a finite subset of $X^*$ that is unsatisfiable, which is included in one of the $X_i$. \hfill $\square$

The term instantiation without background theories described in Section 3 produces a sequence of finite sets $X_i$ of quantifier-free formulas over the theory of uninterpreted functions with equality, for which satisfiability is decidable. If $\varphi$ is a safe formula over a combination of theories, then the formulas in $X_i$ are quantifier free if $\varphi$ does not quantify over the background sorts. If for all the background theories satisfiability of quantifier-free formulas is decidable, then the decision procedures can be combined to a decision procedure for the combined theory using the method of Nelson-Oppen [39]. This combination methods requires the background theories to be stably infinite [43], where a theory is stably infinite if each satisfiable quantifier-free formula of that theory is satisfiable in an infinite model of the theory. Hence, satisfiability is decidable for each set $X_i$ in this setting. By Theorem 4.7, this yields a semi decision procedure for unsatisfiability of safe formulas without quantification over the background structures, as stated in the following corollary.

Corollary 4.8. Consider a combination of stably infinite theories such that satisfiability of quantifier-free formulas is decidable for the background theories. Then term instantiation yields a semi-decision procedure for formulas that do not quantify over the elements of the background structures.

If the signature does not contain uninterpreted function symbols (only relation symbols and constants), then the only ground terms of sort $\sigma_1$ are constants, which means that $X^* = X_0$ is finite. In the setting without background theories, this observation leads to the decidability of satisfiability for formulas of the form $\exists \overline{x} \cdot \forall \overline{y} \cdot \psi(\overline{x}, \overline{y})$ for quantifier-free $\varphi$, known as the Bernays-Schönfinkel class of formulas [4]. Based on Corollary 4.8, we can extend this result to the setting with background theories assuming that there are no function with range $\sigma_1$ in the signature (so there are no terms of sort $\sigma_1$ other than constants).

Proposition 4.9. Consider a combination of stably infinite theories such that satisfiability of quantifier-free formulas is decidable for the background theories, and the signature does not contain functions with range $\sigma_1$. Then satisfiability is decidable for formulas of the form $\exists \overline{x} : \sigma_1 \cdot \forall \overline{y} : \sigma_1 \cdot \psi(\overline{x}, \overline{y})$, where $\psi$ is quantifier-free.
5 RAMIFICATIONS AND APPLICATIONS OF COMPLETE TERM INSTANTIATION FOR THE SAFE FRAGMENT

We now explore some of the ramifications of our main theorem on the soundness and completeness of systematic term instantiation for the safe fragment of FOL (in particular, Theorem 4.7 and Corollary 4.8).

5.1 Explaining the efficacy of natural proofs and the unfold-and-match technique

There are several techniques in current literature where validation engines find proofs using the unfold-and-match technique, wherein the negation of the formula is proved unsatisfiable by “unfolding” recursive definitions followed by a proof of unsatisfiability that uses simple derivations of the resulting formulas. We concentrate in this section on one such paradigm called “natural proofs”, which is a formalization of this tactic. Though the results herein are for natural proofs, they apply also to other unfold-and-match paradigms in the literature.

In the setting of natural proofs for heap verification [46, 49], a dialect of separation logic called Dryad is encoded using first order logic with recursive definitions, and with background theories of numbers (that capture key values in data-structures and recursive functions such as length and height of structures) and background theory of sets (that model heaplets required to capture separation logic semantics and also to capture collections such as the set/multiset of keys stored in a data structure). In this section, we use our main theorem (Theorem 4.7) to give foundational reasons for the efficacy of the heuristics used in natural proofs.

Recall the fundamental problem of finding sound and complete procedures for checking validity for undecidable logics in the realm of program verification. Program configurations are inherently finite in nature (even with unbounded heaps, unbounded stacks, unbounded data-structures, and arbitrarily large integers) and hence are enumerable. Since model-checking logics are (almost) always decidable on finite structures, satisfiability is r.e. (recursively enumerable). Consequently, a sound and complete procedure simply cannot exist for validity, if the underlying logic is undecidable.

We propose that natural proofs, as presented in [46, 49], is best understood in two phases:

Phase 1: Abstracting least fixpoints to fixpoints:
Natural proofs first translate recursive definitions in separation logic that have least fixpoint definitions to recursive equations, which essentially impose only a fixpoint semantics (this corresponds to moving from LFP-semantics to FO-semantics in the terminology of Section 2.3).

Phase 2: Heuristics involving unfolding of recursive definitions:
Natural proofs then unroll recursive definitions (expanding recursive definitions on the footprint of the program segment), and send the resulting quantifier-free formulas to solvers for the combination of background theories and uninterpreted functions.

In the sequel, we assume that natural proofs in Phase 2 unroll recursive definitions systemically, ad infinitum (and call this natural proofs with systematic unbounded unfolding).

Phase 1 of the above procedure is crucial in side-stepping the fundamental block of building sound and complete verification engines for validating verification conditions in program verification. By moving from least fixpoints to fixpoint-based definitions, the logic allows infinite models, that cannot be enumerated, and hence satisfiability is not necessarily r.e. under this semantics, opening the possibility of validity being r.e.

In this section, our main aim is to show that Phase 2, in the context of verification of heap properties, is actually not a heuristic! We show that natural proofs with systematic unbounded unfolding is actually a sound and complete procedure for validity.

, Vol. 1, No. 1, Article 1. Publication date: July 2017.
Before we delve into Phase 2, we describe the subtleties of moving from least fixpoint semantics to fixpoint semantics, and describe the non-standard models that this change brings. We will discuss more sophisticated methods that handle the inaccuracy Phase 1 brings in the next section, Section 6.

Moving from least fixpoint semantics to fixpoint semantics

Let us illustrate the difference in semantics using an example. Consider linked lists with a field pointer n. A formalization of this using heaplets could be:

$$lseg(x, y) \leftrightarrow (x = y \land h_{lseg}(x, y) = \emptyset) \lor (x \neq y \land lseg(n(x), y) \land x \notin h_{lseg}(n(x), y))$$

where \(h_{lseg}\) is defined as follows, using the standard if-then-else connective \(ite\):

$$h_{lseg}(x, y) = ite(x = nil, \emptyset, \{x\} \cup h_{lseg}(n(x), y)).$$

In the least fixpoint semantics, this definition of \(lseg\) does indeed capture the linked lists precisely. It may be tempting to think that the definition without the least fixpoint semantics is correct, too. In fact, it is easy to see that in any model, if \(x\) to \(y\) does form a finite list segment, then \(lseg(x, y)\) would definitely hold, and if \(x\) points to a finite circular list that does not reach \(y\), then the \(lseg(x, y)\) would definitely be false. The reason that the above does not capture precisely linked list segments is that if \(x\) points to an infinitely long list that does not reach \(y\), then one can interpret \(lseg(x, y)\) to be true (as well as \(lseg(z, y)\) to be true for all nodes \(z\) reachable from \(x\)) and still satisfy the constraints. Such a model is depicted in Figure 1, where the solid edges indicate the next pointer, and the additional \(lseg\)-edges (outside the least fixpoint) are indicated by dashed arrows.

One can try to fix this using a theory of finite sets for the heaplets or using induction on the length of lists, where length is modeled using a background theory of natural numbers; however, it turns out that that too will not work, as we discuss later in Section 5.2.

However, if we prove that a verification condition is valid with respect to the above fixpoint semantics, then it will of course be valid with respect to the least fixpoint semantics (see Remark 2.2).

The completeness of natural proofs with fixpoint semantics

We now show that such recursive definitions (interpreted using FO-semantics) are indeed amenable to sound and complete validation using systematic term instantiation. In other words, systematic term instantiation done in Phase 2 is not a heuristic, but a complete method.

Our first goal is to show that heaps can be modeled in our UCT framework consisting of an uninterpreted combination of standard decidable background theories. We will then show that typical verification conditions fall into the safe fragment (as defined in Section 4.1), and in fact satisfy both conditions of having one-way functions as well as not quantifying over background theories, which ensure that the formulas are safe according to Proposition 4.3. This will lead us to conclude that systematic instantiation done in natural proofs is in fact sound and complete.

In the heap verification setting, we can model the heap locations and pointers to heap locations using a foreground theory of uninterpreted functions, along with a background theory of natural numbers, integers, and sets of natural numbers/integers, and other theories that are both stably...
infinite [43] and have a decidable satisfiability problem for quantifier free first-order logics over their respective signatures.

Consider the kind of functions and relations we would need to talk effectively about typical heap properties:

- Pointers to heap locations are naturally modeled as functions from the foreground type to the foreground type.
- Data elements stored in the data-structure, for instance the keys stored in a tree data-structure, can be modeled using a function key that maps heap locations in the foreground type to data-elements in the background type (like integers or natural numbers with addition, or Presburger Arithmetic).
- The set of keys stored in a data-structure can be modeled using maps from tuples of heap locations (that define the boundaries of the data structure) to the keys stored in them. For instance, the keys stored in a list-segment between two locations can be defined as a function from pairs of locations to sets of keys. The background types will offer functions and relations (such as ∈ and ⊆) to compare these sets, and will adhere to standard set-theoretic axioms.
- The heaplet of a data-structure can be also be modeled as a function that maps tuples of locations (that define the boundaries of a structure, typically) to sets modeled as first class elements in the background theory. For instance, the heaplet of a linked list segment from a location $u$ to a location $v$, can be seen as $h_{lseg}(u, v)$, mapping to a set of integers that model the addresses of the heap.
- The definitions of data-structures (such as trees, list segments, binary search trees, etc.) can then be defined using the above functions and relations, and form predicates on tuples in the foreground universe.

The crucial aspect of the above modeling to note is that the modeling only uses functions that are from the foreground universe to the foreground universe (such as function modeling pointer fields) or whose range is the background universe (key, set-of-keys, heaplet, etc.). Hence, the logic naturally falls into the safe fragment of the many-sorted logic, as it satisfies the one-way function restriction (Proposition 4.3). This guarantees that systematic term instantiation is complete, by Theorem 4.7.

Moreover, in the setting of verification, in the negated verification condition that we check for satisfiability, it is naturally the case that the universal quantification is over the foreground theory. The scalar variables (like integer variables, etc.) the program accesses in a basic path are modeled using existential quantification, while it is natural to use universal quantification to express properties of the heap, which is unbounded. There can be implicit unbounded quantification of the background universe by applications of functions on universally quantified variables over the foreground universe (such as saying a linked list is sorted), but this is allowed by the safe fragment. The negated verification conditions hence fall into the logic where universal quantification is restricted to the foreground sort.

Consequently, not only are the formulas generated in the heap verification setting in [46, 49] result in the safe fragment, each level of term instantiation gives a entirely quantifier-free formula over uninterpreted functions and the background theories. The resulting instantiated formulas at each level hence fall into the quantifier-free fragments of the combined background theories, which is decidable by Nelson-Oppen combination of the individual decidable theories [39, 43].

It turns out that the entire class of formulas generated in the work of natural proofs of heap verification reported in [46, 49], where recursive definitions are treated with fixpoint semantics, falls in the above category, leading us to conclude the following:
Result #1: All verification conditions generated in the work on natural proofs for heap verification, as reported in [46, 49], with recursive definitions given fixpoint semantics, fall into the safe fragment of many-sorted logic with background theories, where each background theory has a decidable quantifier-free satisfiability problem and is stably infinite. Consequently, each level of term instantiation results in a formula that is decidable, and furthermore, the procedure that successively performs term instantiation followed by deciding satisfiability of the instantiated formulas is a sound and complete procedure.

We believe that the above explains the efficacy of the instantiation technique used in natural proofs— the procedure, despite seeming to resort to heuristics, is actually sound and complete for fixpoint semantics of the underlying recursive definitions.

Note that the work reported in [46, 49] for natural proofs on heap verification further have a simplification that only does a particular fixed term instantiation. Our result only shows that repeated instantiation is complete; we do not claim to give any rationale for the heuristic that deterministically instantiated terms. Of course, for general FOL (or even safe FOL) over a UCT with even Presburger arithmetic as background, no deterministic instantiation can be complete, for otherwise validity would be decidable, which we know is false.

5.2 Nonstandard Models and Inductive Definitions

We now describe a subtle aspect of many-sorted logics with background theories that explains the inability of these logics to capture the least fixpoint. First, given a background theory of natural numbers with their underlying induction axioms, it is tempting to define structures that are inductive on a measure based on natural numbers. As a simple example, consider defining a list as follows. This does not follow the definition obtained from separation logic as it does not use heaplets, but a similar one can be defined using heaplets as well; in fact, work in separation logic suggests such a definition that inducts using natural numbers [42].

\[ n(\text{nil}) = \text{nil} \land \text{list}(\text{nil}) \land \text{len}(	ext{nil})=0 \land \forall y. (\text{list}(y) \land \text{len}(y) = 0) \rightarrow y = \text{nil} \]

\[ \land \forall y, z. (y \neq \text{nil} \land n(y)=z) \rightarrow (\text{list}(z) \leftrightarrow (\text{list}(y) \land \text{len}(z) = \text{len}(y) + 1)) \]

The above says that \text{nil} is a 0-length list and the only one, and whenever \text{n}(y) = z, one is a list iff the other is a list, and the length of the list at y is one more than the list at z. When \text{len} is interpreted to map to natural numbers, we invite the reader to verify that the above precisely defines lists—those nodes that reach \text{nil} in finitely many applications of \text{n}. If \text{list}(x) is true, we can walk to successive nodes \text{n}(x), \text{n}(n(x)), . . . by the last conjunct that point to shorter and shorter lists, and hence must reach \text{nil}.

However, perhaps surprisingly, the above does not capture the intended meaning of lists in the many-sorted logic with the background theory of Presburger arithmetic. The reason is that Presburger arithmetic (in fact, any FO axiomatic scheme for numbers) does not capture precisely the standard model of arithmetic, but always allows non-standard models as well (by Skolem’s Theorem [55]).

Consequently, we can have a model for the foreground type, as below, with one infinite list ending in \text{nil} (labeled by \mathbb{N}), and one list that is infinite in both directions (labeled by \mathbb{Z}). We can interpret \text{list}(x) to be true for all nodes when defining \text{len}(x) to be a nonstandard number.

Despite the fact that Presburger arithmetic comes with (an infinite set of) induction axioms, the signature of these axioms do not refer to the foreground universe, and hence do not capture induction on additional properties that can be expressed using uninterpreted functions. Note that the above formulation also is in the safe fragment, as functions are one-way.

Also, note that in the above model with \text{n} interpreted as shown, we can also interpret \text{list}(x) to be \text{false} (by interpreting \text{list} to be true only on the \mathbb{N} prefix).

---

Foundations for Natural Proofs and Quantifier Instantiation 1:17
It turns out that we may hence be unable to prove certain theorems that we expect to be true of lists. For instance, if we defined list-segments in a similar fashion as above, then the formula

\[(\text{lseg}(x, y) \land \text{list}(y)) \rightarrow \text{list}(x)\]

is not valid as there are models that have a non-standard background model for arithmetic where the negation of the formula holds (for example, there is model that looks like the model above, has \(\text{list}(x)\) to be false, and \(\text{lseg}(x, y)\) maps to true if \(y\) is in the initial \(\mathbb{N}\) prefix).

In fact, in the work of natural proofs reported in [46, 49], the above is not provable using term instantiation, and the authors resort to adding user-provided axioms that capture facts such as the above. Our results show that the reason term instantiation cannot prove the above is that it is not valid in the FO-semantics where recursive definitions are interpreted as fixpoints. In Section 6, we go into this problem in more detail, exploring how we can automatically add induction principles that can prove such properties correct, alleviating the user from having to provide them (these automatic ways of adding induction principles, however, will not be complete; in fact, no automatic complete scheme can exist, as we explain in Section 6).

### 5.3 Applications to the Array Property Fragment

The goal of this section is to (a) show that the known decidable theory of arrays for the logic array property fragment (APF) [8] can be translated into an equisatisfiable formula in the UCT setting such that the term instantiation given in this paper is a decision procedure, and (b) show certain errors in existing proofs for extensions of APF stemming from the fact that they do not handle non-standard models carefully.

The array property fragment is a restricted fragment of the standard theory of arrays; we do not define them here, but refer the reader to the literature [6, 8]. We work with integer-indexed array property fragment, where contents are also integers.

There is a standard rewriting of array-writes, as given in [8], that transforms the formula so that there are no more writes. Subsequently, APF really resembles a logic that combines uninterpreted functions from integers to integers (modeling integer-indexed arrays).

However, we can embed this in a UCT framework using the following representation, where we have a single background theory of integers with addition. Let us have a foreground universe of abstract indices \(AI\), endowed we a linear order \(\leq_a\) and functions that map abstract indices to concrete indices, the latter being integers. Let us denote this map as \(r()\). We further introduce a constant \(a_c\) over the abstract indices for each constant \(c\) that is mentioned in the formula.

Then we have the following requirements:

\[r(a_c) = c, \text{ for every constant } c \text{ mentioned in the formula}\]

\[\forall x, y:\sigma_1. x \leq_a y \leftrightarrow r(x) \leq r(y)\]

and the axioms for \(\leq_a\) being a linear order on the foreground universe.

Now let us transform the APF formula \(\varphi\) (without writes) by replacing all quantification over indices to quantification over the foreground type of abstract indices, and replace every occurrence of such a quantified index \(i\) by \(r(i)\). Since this framework has only one-way functions (as \(r\) maps
foreground to background), this falls into the safe fragment of the UCT, and hence by our results, term instantiation is complete. Furthermore, since the only functions from the foreground theory map to the background theory, term instantiation terminates in the first round as described in Proposition 4.9. Consequently, term instantiation here is a decision procedure.

The formula transformed to UCT framework above is different from the original formula as universal quantification is restricted to the indices corresponding to the abstract indices, which can be always be realized as a finite model, where we have one element at most for each term instantiated to the foreground type. However, as the proof of decidability of APF [8] shows, term instantiation is complete for APF. Consequently, the original formula in APF and the transformed formula in the UCT fragment are equisatisfiable. We emphasize that we are not claiming a new proof of the APF fragment, but just that it can be easily mapped to a UCT framework where our term instantiation is precisely the same done in the APF decision procedure, and hence is a decision procedure for the logic.

**Negative results for extensions of APF.** Several extensions of APF have been proved undecidable in [8]; for instance, having an additional inner existential quantifier, allowing + on universally quantified indices, allowing nested reads, etc. These results and more have been proved again in the thesis [6] of one of the authors of the paper [8].

However, it turns out that the proofs given in this thesis [6] are incorrect. The proofs reduce finding whether Diophantine equations have a solution to satisfiability of the various logics; however, all these proofs assume that the models for the formula will be standard models of arithmetic and fail for non-standard models. In fact, the structure of the proofs themselves seem wrong—checking whether Diophantine equations are satisfiable (which is clearly a problem in r.e.) is reduced to checking satisfiability of the logic, which should be impossible. For if it were possible, it would mean validity is co-r.e. hard, while we know that validity is in r.e. as these are all theories with a recursive axiomatization.

Note, however, that the APF decidability result does indeed work for indices and values satisfying Presburger axioms of arithmetic (not just the standard theory of natural numbers).

One important additional result in the thesis [6] (that is not in [8]) is that APF with < (allowing < and not just ≤ to compare indices) is undecidable, and this proof suffers from the same problem. We are unable to confirm the decidability/undecidability status of this logic, and declare this problem to be open:

**Open Problem:** Does the array property fragment with < allowed in addition to ≤ (or equivalently, with indices allowing disequality of indices) and contents of arrays being axiomatized by Presburger arithmetic, admit a decidable satisfiability problem?

### 6 INDUCTION PRINCIPLES

In Sections 3 and 4 we have presented a sound and complete term instantiation method for proving validity (or unsatisfiability) of safe formulas that only quantify over the foreground theory. Section 5.1 links this method to the proof technique of natural proofs for recursive data structures from [46, 49]. However, since these natural proofs work within the FO-semantics instead of the LFP-semantics (this corresponds to Phase 1 mentioned in Section 5.1), they cannot prove properties that are valid in the LFP-semantics but not in the FO-semantics. Such an example is explained for list segments in Section 5.1. This is compensated by adding user specified axioms for the recursively defined data structures (which are known to hold in the LFP-semantics).

---

1 Note to reviewers: We did contact Aaron Bradley, and while he did not confirm that these proofs are incorrect, he said that the flaws we outlined seem entirely plausible, given that the thesis was not peer-reviewed.
Often, these properties that hold in the LFP-semantics but not the FO-semantics require some form of an inductive proof. Let us illustrate this on an example. We use recursive transitive closure definitions for illustration purposes in this section in order to keep the formulas simple.

Example 6.1. We modify the definition of reachability from Example 2.1 to a definition of sorted reachability. The following formula refers to \( d(x) \) as the data at node \( x \) (a natural number, for example), and compares the data values using \( \leq \).

\[
\varphi_{srch} := \forall x, y. srch(x, y) \iff \text{LFP } x = y \lor (x \neq y \land srch(f(x), y)) \land d(x) \leq d(f(x))
\]

We want to prove validity in LFP-semantics of the following formula:

\[
\varphi_{rch} \land \varphi_{srch} \rightarrow (\forall x, y. srch(x, y) \rightarrow rch(x, y)).
\]

In the pure FO-semantics, the formula is not valid because of infinite models that do not interpret \( srch \) as the least fixpoint of its definition. For example, take a model consisting of two infinite \( f \)-chains with \( d(u) = 0 \) for all elements. Then interpret \( rch \) as the transitive and reflexive closure of \( f \), and \( srch \) as the transitive and reflexive closure of \( f \) plus \( srch(u, v) \) for \( u \) from the first \( f \)-chain and \( v \) from the second \( f \)-chain.

One can prove validity of the formula \( \varphi_{rch} \land \varphi_{srch} \rightarrow \varphi \) from Example 6.1 in LFP-semantics by induction. This induction could proceed by using a function that defines the distance of two nodes that are related by \( srch \). A more direct approach would proceed by induction directly along the recursive definition of \( srch \). The aim of this section is to formalize such inductive proofs along the recursive definitions by first-order definable induction principles.

First-order induction principles are a common way of formalizing inductive proofs. For example, it is well known that Presburger arithmetic (the theory of natural numbers with addition) can be axiomatized by a schema of first-order induction principles for the natural numbers. An axiomatization of the theory of finite trees based on first-order induction schemas is presented in [1]. Induction principles specifically tailored for transitive closure definitions are considered in [30] in the context of first-order theorem proving. We propose in this section a general form of induction principles for recursively defined relations, which subsume all of these induction schemas. Our experiments (presented in Section 6.3) show that properties about recursively defined data structure that require additional axioms in the natural proof context can be proven based on our induction principles.

Note that we cannot hope for a complete set of induction axioms from which we can prove all valid properties because recursive definitions are too powerful for their theories to be recursively axiomatizable. For example, we can define transitive closures with recursive definitions (see Example 2.1) and in [30, Proposition 4.1] it is shown that there is no recursively enumerable axiomatization of first-order logic with transitive closure. One can also easily see that it is possible to define the structure \((\mathbb{N}, +, \cdot, 0, 1)\) of full arithmetic by a recursive predicate \(N(x) \iff \text{LFP } x = 0 \lor \exists y. x = y + 1 \land N(y)\) in combination with a formula \(\forall x. N(x)\) and the standard axioms for addition and multiplication. So a complete set of induction axioms for recursive definitions would provide a recursive axiomatization of \((\mathbb{N}, +, \cdot, 0, 1)\), which cannot exist by Gödel’s incompleteness theorem.

Of course, a lot of research has been done on induction in the context of automated theorem proving. The aim of this section is not to compare to existing methods for automated inductive proofs, but rather to illustrate that there is a simple way of incorporating inductive reasoning in the context of recursive first-order definitions.
6.1 First-Order Induction Principles for Recursive Definitions

We refer to the notation for recursive definitions from Section 2.3. Assume that we want to prove a property of the form

\[ \varphi_P := \forall \overline{x}. R(\overline{x}) \rightarrow \psi(\overline{x}) \]

with recursive definition \( \varphi_R = \forall \overline{x}. R(x) \leftrightarrow_{LFP} \rho(\overline{x}, R). \)

So we are interested in the validity of the formula \( \varphi_R \rightarrow \varphi_P \) (in the LFP-semantics). The following induction principle expresses the fact that if \( \psi(\overline{x}) \) defines a pre-fixpoint of \( \mu_\rho \), then \( [R]_M \) is included in \( [\psi]_M \) for every model \( M \):

\[ IP(R, \psi) := PFP(\rho, \psi) \rightarrow (\forall \overline{x}. R(\overline{x}) \rightarrow \psi(\overline{x})) \quad \text{with} \quad PFP(\rho, \psi) := \forall \overline{x}. \rho(\overline{x}, R \rightarrow \psi) \rightarrow \psi(\overline{x}). \]

The following lemma states that the formula \( PFP(\rho, \psi) \) indeed expresses that \( \psi(\overline{x}) \) defines a pre-fixpoint of \( \mu_\rho \).

**Lemma 6.2.** For each model \( M \) we have that \( M \models_{LFP} PFP(\rho, \psi) \) if, and only if, \([\psi(\overline{x})]_M \) is a pre-fixpoint of \( \mu_\rho \) on \( M \).

**Proof.** From the definition of \( \mu_\rho \), we get that \( \mu_\rho([\psi(\overline{x})]_M) = [\rho(\overline{x}, R \rightarrow \psi)]_M \). From the definition of \( PFP(\rho, \psi) \) we obtain that \( M \models_{LFP} PFP(\rho, \psi) \) if, and only if, \([\rho(\overline{x}, R \rightarrow \psi)]_M \subseteq [\psi(\overline{x})]_M \). Hence, \( M \models_{LFP} PFP(\rho, \psi) \) if, and only if, \([\psi(\overline{x})]_M \) is a pre-fixpoint of \( \mu_\rho \).

We can use Lemma 6.2 to show that our induction principles are satisfied in all models that interpret \( R \) as the least fixpoint of its definition, as stated in the following lemma.

**Lemma 6.3.** For each model \( M \), if \( M \models_{LFP} \varphi_R \) then \( M \models_{FO} IP(R, \psi) \).

**Proof.** Assume that \( M \models_{LFP} \varphi_R \) and \( M \models_{FO} PFP(\rho, \psi) \) (otherwise the statement is trivially true). By Lemma 6.2, this means that \([\psi(\overline{x})]_M \) is a pre-fixpoint of \( \mu_\rho \). Since \([R]_M \) is the least fixpoint of \( \mu_\rho \) on \( M \), we obtain that \([R]_M \subseteq [\psi]_M \) and hence \( M \models_{FO} (\forall \overline{x}. R(\overline{x}) \rightarrow \psi(\overline{x})) \). This means that \( M \models_{FO} IP(R, \psi) \).

The following proposition states that validity of formulas in LFP-semantics can be shown by strengthening the formula by induction principles and showing validity in FO-semantics.

**Proposition 6.4.** Let \( \varphi = \varphi_A \rightarrow \varphi_P \) be some FO formula with recursive definitions, including the recursive definition \( \varphi_R \) of \( R \), and let \( \psi \) be an FO formula. If \( (\varphi_A \land IP(R, \psi)) \rightarrow \varphi_P \) is valid in FO-semantics, then \( \varphi_A \rightarrow \varphi_P \) is valid in LFP-semantics.

**Proof.** Assume that \( \varphi_A \rightarrow \varphi_P \) is not valid in LFP-semantics. Then there is a model \( M \) with \( M \models_{LFP} \varphi_A \land \neg \varphi_P \). Since \( \varphi_A \) includes the recursive definition of \( R \), we obtain \( M \models_{LFP} \varphi_R \). By Lemma 6.3, \( M \models_{FO} IP(R, \psi) \). Combining the formulas and using Remark 2.2, we get \( M \models_{FO} \varphi_A \land \neg \varphi_P \land IP(R, \psi) \), which means that \( (\varphi \land IP(R, \psi)) \rightarrow \varphi' \) is not valid in FO-semantics.

We illustrate the use of Proposition 6.4 by continuing Example 6.1.

**Example 6.5.** Consider the formula that states that \( \text{rch} \) is a pre-fixpoint of the definition of \( \text{srch} \):

\[ PFP(\rho_{srch}, \text{rch}(x, y)) = \forall x, y. (x = y \lor (x \neq y \land \text{rch}(f(x), y)) \land d(x) \leq d(f(x))) \rightarrow \text{rch}(x, y) \]

It is not difficult to verify that \( \varphi_{rch} \land \varphi_{srch} \rightarrow PFP(\rho_{srch}, \text{rch}(x, y)) \) is a valid formula in the FO-semantics. We obtain that

\[ \varphi_{rch} \land \varphi_{srch} \land IP(\text{srch}, \text{rch}) \rightarrow (\forall x, y. \text{srch}(x, y) \rightarrow \text{rch}(x, y)) \]

is valid in the FO-semantics, which can be shown by using term instantiation as in Section 4 (on the negation of the formula). By Proposition 6.4 this also yields a proof that the original formula

\[ \varphi_{rch} \land \varphi_{srch} \rightarrow (\forall x, y. \text{srch}(x, y) \rightarrow \text{rch}(x, y)) \]

is valid in the LFP-semantics.
We use the weak induction principle for this example in order to keep the formulas shorter. The
induction principle is stronger because if $\psi$ is a pre-fixpoint of $\mu_\rho$, then $R \land \psi$ is also a
pre-fixpoint of $\mu_\rho$, as formally stated in the lemma below.

**Lemma 6.6.** For each model $M$, if $M \models_{\text{FO}} \varphi_R \land \text{PFP}(\rho, \psi)$ then $M \models_{\text{FO}} \text{PFP}(\rho, \psi \land R)$.

**Proof.** If $M \models_{\text{FO}} \varphi_R \land \text{PFP}(\rho, \psi)$, then $[R]_M$ is a fixpoint of $\mu_\rho$ and by Lemma 6.2 $[\psi]_M$ is a
pre-fixpoint of $\mu_\rho$. Then the intersection $[\psi]_M \land [R]_M = [R \land \psi]_M$ is also a pre-fixpoint of $\mu_\rho$, and
hence $M \models_{\text{FO}} \text{PFP}(\rho, \psi \land R)$. \hfill $\square$

This lemma implies that we can replace the induction principle $\text{IP}(R, \psi)$ in Proposition 6.4 by the
strong induction principle $\text{IP}_s(R, \psi)$.

**Example 6.7.** The following formula expresses that the set of points reachable from $x$ is linearly
ordered: $\forall x, y, z. (rch(x, y) \land rch(x, z)) \rightarrow (rch(y, z) \lor rch(z, y))$.

This formula is valid in the LFP-semantics of $rch$ but not in the FO-semantics. It turns out that
the weak induction principle is not sufficient for proving the formula valid but validity follows
from the strong induction principle. Details are given in the supplementary material.

### 6.2 Deriving New Induction Principles

We now present an example of a formula for which one induction principle is not sufficient to
prove validity in the FO-semantics. We need a second induction principle that is obtained from the
formula of the first induction principle.

Consider the definition of reachability from Example 2.1 and the following equivalent definition
that recurses on the other end of the path ($rch$ for reachability reversed).

$$
\varphi_{rch} := \forall x, y. \text{rch}(x, y) \iff_{\text{LFP}} x = y \lor (x \neq y \land \exists v. f(v) = y \land \text{rch}(x, v))
$$

In the least fixpoint interpretation, both definitions correspond to the transitive and reflexive
closure of the function $f$. Consider the formula $\varphi := \forall x, y. \text{rch}(x, y) \rightarrow \text{rch}(x, y)$. Then $\varphi_{rch} \land 
\varphi_{rch} \rightarrow \varphi$ is certainly valid in LFP-semantics but not in the FO-semantics (using a model similar to
the one described in Example 6.1). Letting $\psi(x, y) := \text{rch}(x, y) \rightarrow \text{rch}(x, y)$, the induction principle yields

$$
\text{IP}(rch, rchr) = (\forall x, y. (x = y \lor (x \neq y \land \text{rch}(f(x), y)))) \rightarrow \text{rch}(x, y) \rightarrow (\forall x, y. \psi(x, y)).
$$

We use the weak induction principle for this example in order to keep the formulas shorter. The
reasoning would not change for the strong induction principle. It turns out that this induction
principle does not suffice, that is, $\varphi_{rch} \land \varphi_{rch} \land \text{IP}(rch, rchr) \rightarrow \varphi$ is not valid in the FO-semantics
(see supplementary material). However, we can view this first induction principle as providing a
new proof obligation, namely proving $\text{PFP}(rch, rchr)$, which then implies $\varphi$.

We explain how we can derive a second induction principle from the formula $\text{PFP}(rch, rchr)$ that
states that $rch$ is a pre-fixpoint of $\rho_{rch}$:

$$
\text{PFP}(rch, rchr) = \forall x, y. (x = y \lor (x \neq y \land \text{rch}(f(x), y))) \rightarrow \text{rch}(x, y)
$$

This formula can be rewritten as

$$
(\forall x, y. x = y \rightarrow \text{rch}(x, y)) \land (\forall x, y. (x \neq y \land \text{rch}(f(x), y)) \rightarrow \text{rch}(x, y))
$$
The second conjunct is equivalent to
\[ \forall x, y. (rchr(f(x), y) \to (x \neq y \to rchr(x, y))) \]

Introducing a variable \( z \) for the term \( f(x) \), we obtain
\[ \forall z, y. rchr(z, y) \to (\forall x. (z = f(x) \land x \neq y) \to rchr(x, y)) \]
for the term \( \theta(z, y) \)

which is of the form required for the induction principle \( IP(rchr(z, y), \theta(z, y)) \):

\[ \forall z, y. ((z = y \lor (z \neq y \land \exists v. f(v) = y \land \theta(z, v))) \to \theta(z, y)) \to \forall z, y. (rchr(z, y) \to \theta(z, y)) \]

One can check that this second induction principle together with the first one is sufficient to prove
the original formula correct. This is confirmed by our experiments where the property for two

Note that the second induction principle is obtained by rewriting a formula that contains a
recursively defined predicate into an implication with this recursive predicate on the left-hand side.
This illustrates that these induction principles can to some extent be derived automatically in order
to prove formulas valid.

### 6.3 Evaluation

To demonstrate the efficacy of these induction principles, we manually encoded some examples in
Z3 [12] most existing systems cannot prove correct, due to the existence of non-standard models
discussed in Section 6.

We borrowed many of our examples from [9]. Our analysis is not exhaustive, but all lemmas we
considered were verified in the LFP semantics using the induction principles. The examples cover
traditional data structures encountered in program verification, such as list segments, heaplets,
etc. We discuss some of the examples below, please see the supplemental material for the full Z3
programs.

In these lemmas, \textit{list} refers to a linked list, and \textit{list} \textsubscript{1} is a linked list with an explicit parameter
for the length of the list. The data structures \textit{dllist} and \textit{slist} are similar, but refer to doubly linked
lists and sorted lists respectively. The doubly linked lists and sorted lists contain a function \textit{key} on
nodes, while the singly linked list does not. The last lemma refers to \textit{h\_lseg}, the heaplet segment
between two nodes \( x \) and \( y \). If \( y \) is \textit{nil}, this is the heaplet for the list segment from \( x \). This lemma is
proved and then used as an axiom in many of our other lemmas.

\textit{lseg} \textsubscript{v} is a unary definition of a list segment parametrized by a constant \( v \), while \textit{lseg} and \textit{lsegr}
are binary definitions for list segments, defined both with the moving pointer moving forwards and
backwards (similar to the two definitions \textit{rch} and \textit{rchr} of reachability from Section 6). We similarly
define \textit{dlseg} and \textit{slseg} for doubly linked list segments and sorted list segments.

The relation \textit{rev}(x, y) holds if the reverse of a list beginning at node \( x \) is \( y \), and \textit{keys(\cdot \cdot \cdot)} represents all
the keys reachable from a node. Finally, \textit{bst} and \textit{btree} are data structures for binary search trees
and binary trees respectively, and \textit{leftmost}(x, v) asserts that the leftmost non-nil node reachable
from node \( x \) contains the key \( v \).

The lemmas in Table 1 include examples similar to those discussed in the previous subsection.
Specifically, the fourth lemma proved represents an example similar to Example 6.7 where the
stronger induction principle is needed. In most of the other programs, we also use the stronger
induction principle as it is implied by the weaker induction principle (see Lemma 6.6).

The fifth lemma demonstrates the implication of one list segment definition to another, similar
to Example 6.5. Two induction principles are needed for this lemma, in contrast with only one
induction principle for all other examples. The major difference between the examples for the
reachability definitions in Sections 6.1 and 6.2 and the lemmas in Table 1 is that these lemmas also
refer to semantics of separation using an uninterpreted \( h \text{-} \text{Iseg} \) function that is also used in the
unfolding process.

In all examples above, the maximum depth of unfolding required for any lemma was 2. Though
the completeness result requires a potential infinite depth, these examples show that in practice we
are able to witness the unsatisfiability rather quickly.

Besides these lemmas, we can also use our technique for proving functional programs correct.
For example, consider the McCarthy 91 function [34]. Using our induction principles and unfolding
technique, we have no trouble verifying interesting properties of this function. The function
evaluates \( M(n) \) to \( n - 10 \) if \( n > 100 \), and to the recursive \( M(M(n + 1)) \) otherwise. The interesting
claim regarding this function is that \( M(n) = 91 \) for all \( n \leq 100 \). By encoding \( M \) as a relation \( M_R(n, m) \)
such that \( M(n) = m \) iff \( M_R(n, m) \) holds, the claim is in the correct form for using our induction
principle. The induction principle, together with unfolding the recursive definition just twice (each
at depth 1) proves the claim. This example is also included in our supplemental material.

7 RELATED WORK

Gilmore [20] proposed one of the first sound and complete procedures for first-order logic, imple-
menting it on the IBM 704 Data Processing Machine in 1960; this was refutation-based and
relied on Herbrand’s theorems [15, 53] on reducing satisfiability of quantified FOL reasoning to
satisfiability of larger and larger classes of propositional formulas. In a sense, our work is in a
similar vein—we reduce FOL reasoning to sequences of formulas that are in decidable logics. Given
the efficient implementation of Boolean reasoning, quantifier-free formulas over a combination
of a variety of theories, and some quantified theories, our goal is to reduce reasoning to these
logics rather than just propositional logic. Davis and Putnam [11], also in 1960, proposed a more
efficient algorithm for FOL validity based on ground instantiations and improved the reasoning of
propositional logic using propositional resolution (later refinements of the latter led to the DPLL
technique used in modern SAT solver algorithms). Robinson [51] lifted resolution from ground

| Lemma | Defs Unfolded | Depth |
|-------|--------------|-------|
| \( \forall x, l \text{ list}_1(x, l) \rightarrow \text{list}(x) \) | 1 | 1 |
| \( \forall x. \text{lseg}_2(x) \land \text{list}(v) \rightarrow \text{list}(x) \) | 4 | 2 |
| \( \forall x, y. \text{lseg}(x, y) \land \text{list}(y) \rightarrow \text{list}(x) \) | 4 | 2 |
| \( \forall x, y. \text{lseg}(x, y) \rightarrow (\exists z. \text{lseg}(x, z) \lor \text{lseg}(y, z)) \lor \text{lseg}(z, y)) \) | 2 | 1 |
| \( \forall x, y. \text{Iseg}(x, y) \rightarrow \text{Iseg}(y, x) \) | 7 | 1 |
| \( \forall x. \text{dist}(x) \rightarrow \text{list}(x) \) | 1 | 1 |
| \( \forall x, l \text{ dist}_1(x, l) \rightarrow \text{dist}(x) \) | 1 | 1 |
| \( \forall x, y. \text{dist}(x, y) \lor \text{dist}(y) \rightarrow \text{dist}(x) \) | 4 | 2 |
| \( \forall x, y. \text{dist}(x) \land \text{dist}(y) \land \text{rev}(x, y) \rightarrow \text{keys}(x) = \text{keys}(y) \) | 0 | 0 |
| \( \forall x. \text{l list}_2(x, l) \rightarrow \text{list}(x) \) | 1 | 1 |
| \( \forall x. \text{list}(x) \rightarrow \text{list}(x) \) | 3 | 2 |
| \( \forall x. \text{list}(x) \rightarrow \text{list}(x) \) | 1 | 1 |
| \( \forall x. \text{list}(x) \rightarrow \text{list}(x) \) | 5 | 2 |
| \( \forall x. \text{bst}(x) \rightarrow \text{btree}(x) \) | 1 | 1 |
| \( \forall x. \text{bst}(x) \land \text{leftmost}(x, v) \rightarrow v \leq \text{key}(x) \) | 0 | 0 |
| \( \forall x, y. \text{H} = h \text{Iseg}(n(n(x), y) \land x \in H \rightarrow n(x) \in H \) | 1 | 1 |

Table 1. Examples of lemmas proved correct in LFP semantics using the induction principles covered in
Section 6. The Defs Unfolded column refers to the number of definitions needed to be unfolded for the proof
to go through. Depth represents the maximum level of unfolding needed to witness the unsatisfiability. None
of the lemmas above are provable without the induction principles.
instances using unification of clauses, and this led to the superposition calculus for equational logic which many FO theorem provers use today (Vampire [27], SPASS [57], E [54]). Apart from these, there is, of course, a vast literature on interactive theorem provers [22, 25, 26, 35, 41, 44, 45].

Quantified logics for certain important theories are known to be decidable as well, in particular Presburger arithmetic (natural numbers/integers with addition), rationals, and reals, using quantifier elimination techniques [7].

The development of quantified reasoning techniques over SMT solvers have typically been based on quantifier instantiation (see [50] for a recent survey of these methods). The Simplify theorem prover [13, 38] introduced the E-matching technique, which chooses instantiations based on matching pattern terms. A number of similar methods have since emerged and these techniques are now implemented in several SMT solvers [2, 3, 12, 13, 52]. Combining term instantiations with background SMT solvers have also been investigated in [17, 18].

One work that is close to ours is that of Ge and de Moura [19], where an instantiation method for combinations of uninterpreted functions and relations with background theories is presented. However, the combinations of theories in [19] is not over many-sorted logic but uses one sort for all of the theories. Term instantiation is shown to be complete for formulas that are called essentially uninterpreted [19] which means that only uninterpreted functions or relations are applied directly to the quantified variables. This class of formulas differs from the class of safe formulas for which we show our instantiation procedure to be complete. In particular, equality is an interpreted relation in [19] and thus variables cannot even be compared for equality. For example, defining injectivity of a function $f$ by $\forall x, y. x \neq y \rightarrow f(x) \neq f(y)$ is not an essentially uninterpreted formula (but falls into our safe fragment). Furthermore, most verification conditions arising from programs do not fall into the essentially uninterpreted fragment as properties of scalar variables that are over background sorts are typically required. Hence, the result from [19] is similar in spirit to ours but the classes of formulas for which the instantiation is complete are different. The model-based quantifier instantiation introduced in [19] has been implemented in Z3 and has also been shown to be complete when, through external arguments, one can ensure that the formula will generate only a finite number of instantiations before a real model is found [23].

Turning to reasoning with recursive definitions, logics with recursive functions have been studied for a long time. The NQTHM prover developed by Boyer and Moore [5], and its successor ACL2 [25, 26] had a Lisp-like language that had support for recursive functions and had several induction heuristics to find inductive proofs. Our treatment of induction is similar in spirit but is in the context of a UCT with background theory solvers.

There are also several decidable logics, especially for separation logic, on recursive data-structures, some of which use SMT solvers [31, 32, 47, 48]; this is an active area of research and we refer the reader to the recent paper [28] and references therein. These logics are naturally restricted in expressive power to obtain a decidable validity problem. In contrast to interactive theorem proving and procedures for decidable logics, there is a third class of techniques and tools that allow expressive logics that have an undecidable validity problem, but allow automated sound and complete verification. In a general software verification context with specifications and complex manipulation of ghost structures, techniques in use commonly unfold recursive definitions (using either unfold/fold techniques or just unfolding followed by abstracted reasoning); see for instance work of this kind in Dafny [29] and Verifast [24], where the latter accepts such fold/unfold tactic suggestions from the user.

The work of Suter et al [56] introduced the notion of verifying abstractions of programs manipulating purely functional data-structures, where the procedure did unfolding followed by abstracting recursive functions as uninterpreted functions in order to reduce them to decidable logics, and conditions under which these procedures are complete was investigated. The work on natural
proofs [33, 46, 49] advocates this as a principle for showing imperative programs manipulating
pointer data-structures to be correct, showing its efficacy for a large class of programs against
separation logic specifications. The focus on this paper has been more particularly on natural proofs
because of its systematic mapping of data-structure properties into first-order logic with recursion.

The work presented here however does indeed give foundations to the unfold-and-match method
in general, followed in the various works above.

The drawback in the natural proof work that the user needs to provide (unproven) axioms in
order to prove properties correct has also been addressed by the work of Nguyen et al [40] and Chu
et al [9]. In the latter, the authors, working in a CLP framework, show how inductive hypotheses
can be generated using proof obligations that arise during verification. Incorporating these ideas in
addition to our induction principles is an interesting future direction.

In recent work [16], quantifier instantiation is used for verifying inductive invariants for programs.
While this technique is related to our work, it does not introduce general formulas expressing the
induction principle, but rather uses term instantiation to generate a sequence of quantifier-free
formulas that in the limit expresses that the property is not an invariant. The advantage of our
induction principles is that they can be used to derive new proof obligations, as explained in
Section 6.2.

Induction principles specifically tailored for transitive closure are considered in [30] in a context
of first-order theorem proving. If we formalize transitive closure using recursive definitions, then
our induction principles imply the ones proposed in [30].

8 CONCLUSIONS AND FUTURE WORK

Reasoning with quantified FOL with recursive definitions has mostly been heuristic in nature. We
have, however, provided results that characterize both the power of these heuristics as well as
their limitations. In particular, when dealing with quantified logics in a many-sorted uninterpreted
combination of background theories, term instantiation heuristics are not in general complete,
but are indeed complete for the safe fragment of FOL. The efficacy of practical tools using such
heuristics can be reconciled by observing that they reason with safe formulas. When the logic is
enriched with recursive definitions with least fixpoint semantics, no technique can be complete,
but heuristics for discovering and adding induction principles during term instantiation can be
significantly helpful. We believe that our results give a more compelling foundation to support the
ideas emerging from practice that recursive definitions be handled using discovery of inductive
principles, while quantified logics be handled using term instantiation.

The most interesting future direction is an implementation of tools for the safe fragment, with
and without recursive definitions (with LFP-semantics). An efficient realization of our algorithm
by incorporating SMT solvers for the safe fragment that works using term instantiation would
provide useful, robust and more predictable quantified reasoning for verification engines than what
is available today. Designing and implementing program logics that are guaranteed to produce safe
formulas would extend this robustness to program verifiers.

On the theoretical front, it would be interesting to see whether the safe fragment can be extended
while providing completeness guarantees. Furthermore, it would be interesting to calibrate the
effectiveness of the induction principles given in this paper (or some expansion of them) by
identifying settings where they can be proved to be complete. The discovery of inductive hypotheses
that facilitate recursive reasoning is very similar to invariant synthesis in current literature (like
interpolation [36] and abduction [14]), and incorporating ideas developed for the latter to facilitate
robust discovery of inductive hypotheses is an interesting direction to pursue.
REFERENCES

[1] Rolf Backofen, James Rogers, and K. Vijay-Shanker. 1995. A First-Order Axiomatization of the Theory of Finite Trees. *Journal of Logic, Language and Information*, 4, 1 (1995), 5–39. https://doi.org/10.1007/BF01048403

[2] Clark Barrett, Christopher L. Conway, Morgan Deters, Liana Hadarean, Dejan Jovanovic, Tim King, Andrew Reynolds, and Cesare Tinelli. 2011. CVCC. In *CAV’11*. 171–177. https://doi.org/10.1007/978-3-642-22110-1_14

[3] Clark Barrett and Cesare Tinelli. 2007. CVCC. In *CAV’07*. 298–302. https://doi.org/10.1007/978-3-540-73368-3_34

[4] Egon Börger, Erich Grädel, and Yuri Gurevich. 1997. *The Classical Decision Problem*. Springer.

[5] Robert S. Boyer and J. Strother Moore. 1980. *A computational logic*. Academic Press.

[6] Aaron Bradley. 2007. *Safety Analysis of Systems*. Ph.D. Dissertation. Stanford University.

[7] Aaron R. Bradley, Zohar Manna. 2007. *The Calculus of Computation: Decision Procedures with Applications to Verification*. Springer-Verlag New York, Inc., Secaucus, NJ, USA.

[8] Aaron R. Bradley, Zohar Manna, and Henny B. Sipma. 2006. What’s Decidable About Arrays?. In *VMCAI’06*. Vol. 3855. Springer, 427–442. https://doi.org/10.1007/11609773

[9] Duc-Hiep Chu, Joxan Jaffar, and Minh-Thai Trinh. 2015. Automatic induction proofs of data-structures in imperative programs. In *PLDI’15*. 457–466.

[10] Martin Davis and Hilary Putnam. 1960. A Computing Procedure for Quantification Theory. *J. ACM* 7, 3 (1960), 201–215. https://doi.org/10.1145/321033.321034

[11] Martin Davis and Hilary Putnam. 1960. A Computing Procedure for Quantification Theory. *J. ACM* 7, 3 (1960), 201–215. https://doi.org/10.1145/321033.321034

[12] Leonardo de Moura and Nikolaj Bjørner. 2008. *Z3: An Efficient SMT Solver*. Springer Berlin Heidelberg, Berlin, Heidelberg, 337–340.

[13] David Detlefs, Greg Nelson, and James B. Saxe. 2005. Simplify: A Theorem Prover for Program Checking. *J. ACM* 52, 3 (May 2005), 365–473. https://doi.org/10.1145/1066100.1066102

[14] Isil Dillig, Thomas Dillig, Boyang Li, and Kenneth L. McMillan. 2013. Inductive invariant generation via abductive inference. In *OOPSLA’13*. 443–456. https://doi.org/10.1145/2509136.2509511

[15] Heinz-Dieter Ebbinghaus, Jörg Flum, and Wolfgang Thomas. 1994. *Mathematical logic (2. ed.)*. Springer.

[16] Yotam M. Y. Feldman, Oded Padon, Neil Immerman, Mooly Sagiv, and Sharon Shoham. 2017. Bounded Quantifier Instantiation for Checking Inductive Invariants. In *TACAS 2017 (Lecture Notes in Computer Science)*, Vol. 10205. 76–95. https://doi.org/10.1007/978-3-662-54577-5_5.

[17] Harald Ganzinger and Konstantin Korovin. 2003. New Directions in Instantiation-Based Theorem Proving. In *LICS’03*. IEEE Computer Society, 55–64.

[18] Harald Ganzinger and Konstantin Korovin. 2006. Theory Instantiation. In *LPAR’06*. 497–511. https://doi.org/10.1007/11916277_34

[19] Yeting Ge and Leonardo Mendonça de Moura. 2009. Complete Instantiation for Quantified Formulas in Satisfiability Modulo Theories. In *CAV’09 (Lecture Notes in Computer Science)*, Vol. 5643. Springer, 306–320. https://doi.org/10.1007/978-3-642-02658-4

[20] Paul C. Gilmore. 1960. A Proof Method for Quantification Theory: Its Justification and Realization. *IBM Journal of Research and Development* 4, 1 (1960), 28–35. https://doi.org/10.1147.rd.41.0028

[21] Andrzej Granas and James Dugundji. 2003. *Fixed Point Theory*. Springer.

[22] John Harrison, Josef Urban, and Freek Wiedijk. 2014. History of Interactive Theorem Proving. In *Computer-Aided Reasoning: An Approach*. 1–35. https:

[23] Carsten Ihlemann, Swen Jacobs, and Viorica Sofronie-Stokkermans. 2008. On Local Reasoning in Verification. In *TACAS’08/ETAPS’08*. 265–281. https://doi.org/10.1007/978-3-540-78800-3_19

[24] Bart Jacobs and Frank Piessens. 2008. The VeriFast Program Verifier. (2008).

[25] Matt Kaufmann and J. Strother Moore. 1997. An Industrial Strength Theorem Prover for a Logic Based on Common Lisp. *IEEE Trans. Software Eng.*, 23, 4 (1997), 203–213. https://doi.org/10.1109/32.588534

[26] Matt Kaufmann, J. Strother Moore, and Panagiotis Manolios. 2000. *Computer-Aided Reasoning: An Approach*. Kluwer Academic Publishers, Norwell, MA, USA.

[27] Laura Kovács and Andrei Voronkov. 2013. First-Order Theorem Proving and Vampire. In *CAV’13*. 1–35. https://doi.org/10.1007/978-3-642-39799-8_1

[28] Q. L. (Quang Loc) Le, M. Tatsuta, J. (Jun) Sun, and W. N. (Wei-Ngan) Chin. 2017. A Decidable Fragment in Separation Logic with Inductive Predicates and Arithmetic. In *CAV’17*. http://hdl.handle.net/10149/621090

[29] K. Rustom M. Leino. 2012. Automating Induction with an SMT Solver. In *VMCAI’12*. 315–331. https://doi.org/10.1007/978-3-642-27940-9_21

[30] Tal Lev-Ami, Neil Immerman, Thomas W. Reps, Mooly Sagiv, Siddharth Srivastava, and Greta Yorsh. 2009. Simulating reachability using first-order logic with applications to verification of linked data structures. *Logical Methods in Computer Science*, 5, 2 (2009). https://doi.org/10.1007/978-3-642-39799-8_53
9 APPENDIX

Proofs of Omitted Lemmas from Section 3

In this section we give formal proofs of omitted lemmas from Section 3. We first recall our unfolding process and model construction:

\[\text{Proofs of Omitted Lemmas from Section 3}\]

\[\text{process and model construction:}\]
Let $\psi = \varphi_1 \land \ldots \land \varphi_n$ be a closed $\Sigma$-formula, where each $\varphi_i$ is of the form $\forall \overline{x} \cdot \psi_i(\overline{x})$ for quantifier-free $\psi_i$. Define $X^*$ and $T^*$ as follows:

$$T_0 = \{ t \mid t \text{ is a ground term occurring in } \psi \}$$

$$X_0 = \{ \psi_i(\overline{t}/\overline{x}) \mid \text{each term in } \overline{t} \text{ is in } T_0 \}$$

$$T_{n+1} = T_n \cup \{ t \mid t \text{ is a ground term occurring in a formula from } X_n \}$$

$$X_{n+1} = X_n \cup \{ \psi_i(\overline{t}/\overline{x}) \mid \text{each term in } \overline{t} \text{ is in } T_{n+1} \}$$

$$X^* = \bigcup_{i \geq 0} X_i \text{ and } T^* = \bigcup_{i \geq 0} T_i$$

We assume $T^*$ is nonempty. $\psi = \neg \varphi = \varphi_1 \land \ldots \land \varphi_{n-1} \rightarrow \neg \varphi_n$.

Let $M = (U; [\cdot ]_M)$ be a model that satisfies $\psi$. As we are in the single-sorted case here, $U$ simply represents a universe for sort $\sigma_1$ rather than a family of universes. Let

$U^* = \{ u \in U \mid u = [t]_M \text{ for some } t \in T^* \}$

Now, pick an arbitrary $u^* \in U^*$. Such a $u^*$ exists since $T^*$ is assumed to be nonempty. Define the model $M^* = (U^*; [\cdot ]_{M^*})$, where $[R]_{M^*} = [R]_M \upharpoonright U^*$, and for any $f \in F$ and $u_1, \ldots, u_n \in U^*$,

$$[f]_{M^*}(u_1, \ldots, u_n) = \begin{cases} [f]_M(u_1, \ldots, u_n) & \text{if } [f]_M(u_1, \ldots, u_n) \in U^* \\ u^* & \text{otherwise} \end{cases}$$

**Lemma 9.1.** $\forall t \in T^*, [t]_M = [t]_{M^*}$.

**Proof.** We will prove this by induction on the structure of a term $t$. If $t$ is a variable the interpretations are the same. If $t = f(t_1, \ldots, t_n)$, then all the $t_i$ are in $T^*$ by definition of $T^*$. Thus, by induction we know that $[t]_M = [t]_{M^*}$. Further, since $t \in T^*$, then $[f]_M(t_1)_M, \ldots, [t_n]_M) \in U^*$. So by definition this is equal to $[f]_{M^*}(t_1, \ldots, [t_n]_{M^*}) \in U^*$ as needed. □

**Lemma 9.2.** Let $\psi$ be a subformula of a formula in $X^*$. Then $M \models \psi \iff M^* \models \psi$.

**Proof.** The proof is by induction on the structure of the formula $\psi$. First, if $\psi$ is atomic, then it is either $\top$, $\bot$, or $R(t_1, \ldots, t_n)$ for terms $t_1, \ldots, t_n \in T^*$ and $R \in R$. The $\top$ and $\bot$ cases are trivial. The last case follows by Lemma 9.1, as well as recognizing that by definition the interpretations of $R$ are the same.

For the induction step, note $M \models \psi_1 \land \psi_2 \iff M \models \psi_1$ and $M \models \psi_2 \iff M^* \models \psi_1$ and $M^* \models \psi_2 \iff M^* \models \psi_1 \land \psi_2$. Similarly for logical connectives $\lor$ and $\neg$. □

**Lemma 9.3.** For any model $M$, if $M \models X^*$, then $M^* \models \psi$.

**Proof.** Since each $\varphi_i$ is of the form $\forall \overline{x} \cdot \psi_i(\overline{x})$, we need to show $M^* \models \psi_i(\overline{u}/\overline{x})$ for all $\overline{u} \in U^*$. Indeed, for each $\overline{u}$, we know there are terms $\overline{t}$ such that $\overline{u} = [\overline{t}]_M$ by definition of $U^*$. By Lemma 9.1, $\overline{t} = [\overline{u}]_{M^*}$, and $\psi_i(\overline{t}/\overline{x})$ is a formula in $X^*$. So since $M \models X^*$, $M \models \psi_i(\overline{t})$, so by Lemma 9.2, $M^* \models \psi_i(\overline{t}/\overline{x})$ and therefore $M^* \models \varphi_i$ for each $i$. □

**Lemma 9.4.** $\psi$ is satisfiable if and only if then $X^*$ is satisfiable

**Proof.** "$\Rightarrow$" follows from the observation that $X^*$ is weaker than $\varphi$, and "$\Leftarrow$" is immediate from Lemma 9.3. □
Additional Explanations for Example 6.7
We give a detailed explanation why the formula from Example 6.7 does not follow from the weak induction principle but from the strong one. For the description of the example, we use the simplified version of the formula stating that $\psi \land R$ is a pre-fixpoint of $\mu \rho$:

$$\text{PFP}(\rho, \psi \land R) := \forall \overline{x}. \rho(\overline{x}, R \leftarrow (\psi \land R)) \rightarrow \psi(\overline{x}).$$

In this formula the conjunction with $R$ is missing on the right-hand side of the implication. It can be omitted because $R$ is a fixpoint of its recursive definition, and therefore is always implied by $\rho(\overline{x}, R \leftarrow (\psi \land R))$.

We consider the formula expressing that the set of points reachable from $x$ is linearly ordered:

$$\forall x, y, z. (rch(x, y) \land rch(x, z)) \rightarrow (rch(y, z) \lor rch(z, y))$$

This formula is valid in the LFP-semantics of $rch$. For the FO-semantics, consider a model consisting of three infinite disjoint $f$-chains. In the FO-semantics we can interpret $rch$ as the set of all pairs $u, v$ of nodes that are either connected by a finite $f$-path, or where $u$ is in the first chain, and $v$ is in the second or third chain. Let $u_1, u_2, u_3$ be from the first, second, and third chain, respectively. Then $rch(u_1, u_2)$ and $rch(u_1, u_3)$ but $u_2$ and $u_3$ are not related by $rch$. So the property does not hold if $rch$ is not interpreted by the least fixpoint.

We can rewrite the formula into the form required for the induction principle as follows:

$$\forall x, y. rch(x, y) \rightarrow (\forall z. rch(x, z) \rightarrow (rch(y, z) \lor rch(z, y)))$$

The (weak) induction principle $IP(rch, \psi_{linear})$ states that this formula is valid if $\psi_{linear}(x, y)$ is a pre-fixpoint of $\rho_{rch}$. The latter property is expressed by

$$\text{PFP}(\rho_{rch}, \psi_{linear}) = \forall x, y. (x = y \lor (x \neq y \land \psi_{linear}(f(x, y))) \rightarrow \psi_{linear}(x, y)).$$

However, one can construct a model $M$ such that $M \models_{FO} \varphi_{rch} \land \neg\text{PFP}(\rho_{rch}, \psi_{linear}(x, y))$ as follows. The universe has 3 elements $U = \{u, v, w\}$, with $f(x) = w$ for all $x \in U$. The interpretation of $rch$ we take the reflexive and transitive closure of $f$. The formula $\psi_{linear}(x, y)$ is not satisfied by the pair $x = u$ and $y = v$ because then for $z = u$, we have that $rch(x, z)$ but not $rch(y, z)$ and not $rch(z, y)$.

However, $\psi_{linear}(f(x, y))$ is satisfied for the pair $x = u$ and $y = v$ because $f(u) = w$ and all elements that are reachable from $w$ are also reachable from $v$.

Hence, there are elements for $x$ and $y$ that make the left-hand side of the implication in $\text{PFP}(\rho_{rch}, \psi_{linear}(x, y))$ true but falsify the right-hand side of the implication.

Now consider the strong induction principle $IP(rch, rch \land \psi_{linear})$. The corresponding formula for the pre-fixpoint is obtained from the above one by adding a conjunct $rch(f(x, y))$ as follows:

$$\text{PFP}(\rho_{rch}, rch \land \psi_{linear}) = \forall x, y. (x = y \lor (x \neq y \land rch(f(x, y)) \land \psi_{linear}(f(x, y)))) \rightarrow \psi_{linear}(x, y)).$$

It turns out that this formula is valid, more precisely, for each model $M$, if $M \models_{FO} \varphi_{rch}$ then $M \models_{FO} \text{PFP}(\rho_{rch}, rch \land \psi_{linear})$. To see that, consider a model $M$ with $M \models_{FO} \varphi_{rch}$, and pick any two elements $x = u$ and $y = v$. The case $u = v$ is easy. So we assume that $u \neq v$ and $rch(f(u), v)$ and $\psi_{linear}(f(u), v)$. We need to show that this implies $\psi_{linear}(u, v)$. So let $z = w$ be such that $rch(u, w)$. We want to show that $rch(v, w)$ or $rch(w, v)$). Since $M \models_{FO} \varphi_{rch}$, we obtain that $rch(u, w)$ implies $rch(f(u), w)$ or $u = w$. In the first case, $\psi_{linear}(f(u), v))$ and thus $rch(v, w)$ or $rch(w, v)$. In the second case, $u = w$, clearly $rch(f(u), v)$ implies $rch(w, v)$). Note that this step uses the fact that $rch(f(u), v)$, which is introduced by the strong induction principle.
Fig. 2. A model showing that one induction principle is not sufficient for proving that $rch(x, y)$ implies $rchr(x, y)$.

**Details for Section 6.2**

For showing that $\varphi_{rch} \land \varphi_{rchr} \land IP(rch, rchr) \rightarrow \varphi$ is not valid in the FO-semantics, we construct a model of its negation $\varphi_{rch} \land \varphi_{rchr} \land IP(rch, rchr) \land \neg \varphi$. Such a model is depicted in Figure 2. It consists of two infinite $f$-chains (indicated by the solid arrows) of elements $a_i$ and $b_i$, respectively, with $i \in \mathbb{Z}$. The interpretation of $rch$ and $rchr$ both include the reflexive and transitive closure of $f$ (not shown in the picture). Additionally, $rch$ contains the dotted edges from all the $a_i$ to $b_0$, and $rchr$ contains the dashed edges from $a_0$ to all the $b_i$. One can check that these relations are fixpoints of the defining formulas of $rch$ and $rchr$. Obviously, the model also satisfies $\neg \varphi$ because $rch$ is not included in $rchr$. It remains to show that $IP(rch, rchr)$ is satisfied. This follows from the fact that $rchr$ is not a pre-fixpoint of $\rho_{rch}$. To see this, choose $x = a_{-1}$ and $y = b_0$. Then we have $\neg rchr(x, y)$ but $(x \neq y \land rchr(f(x), y))$. This witnesses that $rchr$ is not a pre-fixpoint of $\rho_{rch}$ in this model. So the induction principle is satisfied.