Reasoning in the Bernays-Schönfinkel-Ramsey Fragment of Separation Logic

Andrew Reynolds¹, Radu Iosif², and Cristina Serban²

¹ The University of Iowa
² Verimag/CNRS/Université de Grenoble Alpes

Abstract. Separation Logic (SL) is a well-known assertion language used in Hoare-style modular proof systems for programs with dynamically allocated data structures. In this paper we investigate the fragment of first-order SL restricted to the Bernays-Schönfinkel-Ramsey quantifier prefix $\exists^*\forall^*$, where the quantified variables range over the set of memory locations. When this set is uninterpreted (has no associated theory) the fragment is PSPACE-complete, which matches the complexity of the quantifier-free fragment [7]. However, SL becomes undecidable when the quantifier prefix belongs to $\exists^*\forall^*\exists^*$ instead, or when the memory locations are interpreted as integers with linear arithmetic constraints, thus setting a sharp boundary for decidability within SL. We have implemented a decision procedure for the decidable fragment of $\exists^*\forall^*\exists^*$SL as a specialized solver inside a DPLL($T$) architecture, within the CVC4 SMT solver. The evaluation of our implementation was carried out using two sets of verification conditions, produced by (i) unfolding inductive predicates, and (ii) a weakest precondition-based verification condition generator. Experimental data shows that automated quantifier instantiation has little overhead, compared to manual model-based instantiation.

1 Introduction

Separation Logic (SL) is a popular logical framework for program verification, used by a large number of methods, ranging from static analysis [10, 28, 6] to Hoare-style proofs [19] and property-guided abstraction refinement [1]. The salient features that make SL particularly attractive for program verification are the ability of defining (i) recursive data structures using small and natural inductive definitions, (ii) weakest pre- and post-condition calculi that capture the semantics of programs with pointers, and (iii) compositional verification methods, based on the principle of local reasoning (analyzing separately pieces of program working on disjoint heaps).

Consider, for instance, the following inductive definitions, describing an acyclic and a possibly cyclic list segment, respectively:

\[
\begin{align*}
\tilde{\text{ls}}(x, y) & \equiv \text{emp} \land x = y \lor x \neq y \land \exists z \cdot x \mapsto z \ast \tilde{\text{ls}}(z, y) \quad \text{acyclic list segment from } x \text{ to } y \\
\text{ls}(x, y) & \equiv \text{emp} \land x = y \lor \exists u \cdot x \mapsto u \ast \text{ls}(u, y) \quad \text{list segment from } x \text{ to } y
\end{align*}
\]

Intuitively, an acyclic list segment is either empty, in which case the head and the tail coincide ($\text{emp} \land x = y$), or it contains at least one element which is disjoint from the rest of the list segment. We denote by $x \mapsto z$ the fact that $x$ is an allocated memory location,
which points to $z$, and by $x \mapsto z \mapsto z$ the fact that $x \mapsto z$ and $\tilde{ls}(z, y)$ hold over disjoint parts of the heap. The constraint $x \neq y$, in the inductive definition of $\tilde{ls}$, captures the fact that the tail of the list segment is distinct from every allocated cell in the list segment, which ensures the acyclicity condition. Since this constraint is omitted from the definition of the second (possibly cyclic) list segment $ls(x, y)$, its tail $y$ is allowed to point inside the set of allocated cells.

Automated reasoning is the key enabler of push-button program verification. Any procedure that checks the validity of a logical entailment between inductive predicates requires checking the satisfiability of formulae from the base (non-inductive) assertion language, as shown by the example below. Consider a fragment of the inductive proof showing that any acyclic list segment is also a list segment, given below:

$$
\begin{align*}
\text{ls}(z, y) + \text{ls}(z, y) \\
x \neq y \land x \mapsto z + \text{ls}(z, y) + \exists u. x \mapsto u + \text{ls}(u, y)
\end{align*}
$$

by instantiation $u \leftarrow z$

The first (bottom) inference in the proof corresponds to one of the two cases produced by unfolding both the antecedent and consequent of the entailment (the second case $\text{emp} \land x = y + \text{emp} \land x = y$ is trivial and omitted for clarity). The second inference is a simplification of the sequent obtained by unfolding, to a sequent matching the initial one (by renaming $z$ to $x$), and allows to conclude this branch of the proof by an inductive argument, based on the principle of infinite descent [5].

The simplification applied by the second inference above relies on the validity of the entailment $x \neq y \land x \mapsto z \models \exists u. x \mapsto u$, which reduces to the (un)satisfiability of the formula $x \neq y \land x \mapsto z \land \forall u. \neg x \mapsto u$. The latter falls into the Bernays-Schönfinkel-Ramsey fragment, defined by the $\exists^* \forall^*$ quantifier prefix, and can be proved unsatisfiable using the instantiation of the universally quantified variable $u$ with the existentially quantified variable $z$ (or a corresponding Skolem constant). In other words, this formula is unsatisfiable because the universal quantified subformula asks that no memory location is pointed to by $x$, which is contradicted by $x \mapsto z$. The instantiation of $u$ that violates the universal condition is $u \leftarrow z$, which is carried over in the rest of the proof.

The goal of this paper is mechanizing satisfiability of the Bernays-Schönfinkel-Ramsey fragment of $\text{SL}$, without inductively defined predicates. This fragment is defined by the quantifier prefix of the formulae in prenex normal form. We consider formulae $\exists x_1 \ldots \exists x_n \forall y_1 \ldots \forall y_n. \phi(x_1, \ldots, x_n, y_1, \ldots, y_n)$, where $\phi$ is any quantifier-free formula of $\text{SL}$, consisting of pure formulae from given base theory $T$, and points-to atomic propositions relating terms of $T$, combined with unrestricted Boolean and separation connectives, and the quantified variables range essentially over the set of memory locations. In a nutshell, the contributions of the paper are two-fold:

1. We draw a sharp boundary between decidability and undecidability, proving essentially that the satisfiability problem for the Bernays-Schönfinkel-Ramsey fragment of $\text{SL}$ is PSPACE-complete, if the domain of memory locations is an uninterpreted

\[\text{Strictly speaking, the Bernays-Schönfinkel-Ramsey class refers to the } \exists^* \forall^* \text{ fragment of first-order logic with equality and predicate symbols, but no function symbols [17].}\]
set, whereas interpreting memory locations as integers with linear arithmetic con-
straints, leads to undecidability. Moreover, undecidability occurs even for uninter-
preted memory locations, if we extend the quantifier prefix to $\exists^* \forall^* \exists^*$.

2. We have implemented an effective decision procedure for quantifier instantiation,
   based on counterexample-driven learning of conflict lemmas, integrated within the
   DPLL($T$) architecture [12] of the CVC4 SMT solver [2]. Experimental evaluation
   of our implementation shows that the overhead of the push-button quantifier in-
   stantiation is negligible, compared to the time required to solve a quantifier-free
   instance of the problem, obtained manually, by model inspection.

Related Work The first theoretical results on the decidability and computational com-
plexity of SL (without inductive definitions) were found by Calcagno, Yang and O’Hearn
[7]. They showed that the satisfiability problem for SL is undecidable, in the presence
of quantifiers, assuming that each memory location can point to two other locations,
i.e. using atomic propositions of the form $x \rightarrow (y, z)$. Decidability can be recovered by
considering the quantifier-free fragment, proved to be PSPACE-complete, by a small
model argument [7]. Refinements of these results consider decidable fragments of SL
with one record field (atomic points-to propositions $x \rightarrow y$), and one or two quantified
variables. In a nutshell, SL with one record field and separating conjunction only is de-
cidable with non-elementary time complexity, whereas adding the magic wand adjoint
leads to undecidability [4]. Decidability, in the presence of the magic wand operator,
is recovered by restricting the number of quantifiers to one, in which case the logic
becomes PSPACE-complete [9]. This bound is sharp, because allowing two quantified
variables leads to undecidability, and decidability with non-elementary time complexity
if the magic wand is removed [8].

SMT techniques were applied to deciding the satisfiability of SL in the work of
Piskac, Wies and Zufferey [21, 22]. They considered quantifier-free fragments of SL
with separating conjunction in positive form (not occurring under negation) and without
magic wand, and allowed for hardcoded inductive predicates (list and tree segments). In
a similar spirit, we previously defined a translation to multi-sorted second-order logic
combined with counterexample-driven instantiation for set quantifiers to define a deci-
sion procedure for the quantifier-free fragment of SL [25]. In a different vein, a tableau-
based semi-decision procedure is given by M´ery and Galmiche [11]. Termination of
this procedure is guaranteed for the (decidable) quantifier-free fragment of SL, yet no
implementation is available for comparison.

A number of automated theorem provers have efficient and complete approaches
for the Bernays-Schönfinkel-Ramsey fragment of first-order-logic, also known as ef-
effectively propositional logic (EPR) [3, 16]. A dedicated approach for EPR in the SMT
solver Z3 was developed in [20]. An approach based on finite model finding is imple-
mented in CVC4 [26], which is model-complete for EPR. Our approach is based on
counterexample-guided quantifier instantiation, which has been used in the context of
SMT solving in previous works [13, 23].
2 Preliminaries

We consider formulae in multi-sorted first-order logic. A signature $\Sigma$ consists of a set $\Sigma^s$ of sort symbols and a set $\Sigma^f$ of (sorted) function symbols $f^{\sigma_1,\ldots,\sigma_n}$, where $n \geq 0$ and $\sigma_1,\ldots,\sigma_n, \sigma \in \Sigma^s$. If $n = 0$, we call $f^\sigma$ a constant symbol. In this paper, we consider signatures $\Sigma$ containing the Boolean sort, and write $\top$ and $\bot$ for the Boolean constants true and false. For this reason, we do not consider predicate symbols as part of a signature, as predicates are viewed as Boolean functions. Additionally, we assume for any finite sequence of sorts $\sigma_1,\ldots,\sigma_n \in \Sigma^s$, the tuple sort $\sigma_1 \times \ldots \times \sigma_n$ also belongs to $\Sigma^s$, and that $\Sigma^f$ includes the $i^{th}$ tuple projection function for each $i = 1,\ldots,n$. For each $k > 0$, let $\sigma^k$ denote the $k$-tuple sort $\sigma \times \ldots \times \sigma$.

Let $\text{Vars}$ be a countable set of first-order variables, each $x^\sigma \in \text{Vars}$ having an associated sort $\sigma$. First-order terms and formulae over the signature $\Sigma$ (called $\Sigma$-terms and $\Sigma$-formulae) are defined as usual. For a $\Sigma$-formula $\varphi$, we denote by $\text{Fvc}(\varphi)$ the set of free variables and constant symbols in $\varphi$, and by writing $\varphi(x)$ we mean that $x \in \text{Fvc}(\varphi)$. Whenever $\text{Fvc}(\varphi) \cap \text{Vars} = \emptyset$, we say that $\varphi$ is a sentence, i.e. $\varphi$ has no free variables. A $\Sigma$-interpretation $I$ maps: (1) each sort symbol $\sigma \in \Sigma$ to a non-empty set $\sigma^I$, (2) each function symbol $f^{\sigma_1,\ldots,\sigma_n}$ to a total function $f^I: \sigma_1^I \times \ldots \times \sigma_n^I \to \sigma^I$ where $n > 0$, and (3) each variable $x^\sigma \in \text{Vars}$ to an element of $\sigma^I$ when $n = 0$, and (3) each variable $x^\sigma \in \text{Vars}$ to an element of $\sigma^I$. For an interpretation $I$ a sort symbol $\sigma$ and a variable $x$, we denote by $I[\sigma \leftarrow S]$ and, respectively $I[x \leftarrow v]$, the interpretation associating the set $S$ to $\sigma$, respectively the value $v$ to $x$, and which behaves like $I$ in all other cases. For a $\Sigma$-term $t$, we write $t^I$ to denote the interpretation of $t$ in $I$, defined inductively, as usual. A satisfiability relation between $\Sigma$-interpretations and $\Sigma$-formulae, written $I \models \varphi$, is also defined inductively, as usual. We say that $I$ is a model of $\varphi$ if $I$ satisfies $\varphi$.

A (multi-sorted first-order) theory is a pair $T = (\Sigma, I)$ where $\Sigma$ is a signature and $I$ is a non-empty set of $\Sigma$-interpretations, the models of $T$. We assume that $\Sigma$ always contains the equality predicate, which we denote by $=$, as well as projection functions for each tuple sort. A $\Sigma$-formula $\varphi$ is $T$-satisfiable if it is satisfied by some interpretation in $I$. We write $\text{E}$ to denote the empty theory (with equality), whose signature consists of a sort $U$ with no additional function symbols, and LIA to denote the theory of linear integer arithmetic, whose signature consists of the sort $\text{Int}$, the binary predicate symbol $\geq$, function $+$ denoting addition, and the constants $0,1$ of sort $\text{Int}$, interpreted as usual. In particular, there are no uninterpreted function symbols in LIA. By ELIA we denote the theory obtained by extending the signature of LIA with the sort $U$ of $\text{E}$ and the equality over $U$.

Let $T = (\Sigma, I)$ be a theory and let Loc and Data be two sorts from $\Sigma$, with no restriction other than the fact that Loc is always interpreted as a countable set. Also, we consider that $\Sigma$ has a designated constant symbol nil$^{\text{Loc}}$. The Separation Logic fragment SL(T)$_{\text{Loc, Data}}$ is the set of formulae generated by the following syntax:

$$\varphi ::= \phi \mid \text{emp} \mid t \mapsto u \mid \varphi_1 \ast \varphi_2 \mid \varphi_1 \Rightarrow \varphi_2 \mid \neg \varphi_1 \mid \varphi_1 \land \varphi_2 \mid \exists x^\sigma. \varphi_1(x)$$

---

4 By writing $I[\sigma \leftarrow S]$ we ensure that all variables of sort $\sigma$ are mapped by $I$ to elements of $S$. 
where $\phi$ is a $\Sigma$-formula, and $t, u$ are $\Sigma$-terms of sorts $\text{Loc}$ and $\text{Data}$, respectively. As usual, we write $\forall x^\sigma \cdot \varphi(x)$ for $\neg \exists x^\sigma \cdot \neg \varphi(x)$. We omit specifying the sorts of variables and constants when they are clear from the context.

Given an interpretation $I$, a heap is a finite partial mapping $h : \text{Loc}^f \rightarrow \text{fin} \cdot \text{Data}^f$. For a heap $h$, we denote by $\text{dom}(h)$ its domain. For two heaps $h_1$ and $h_2$, we write $h_1 \# h_2$ for $\text{dom}(h_1) \cap \text{dom}(h_2) = \emptyset$ and $h = h_1 \lor h_2$ for $h_1 \# h_2$ and $h = h_1 \lor h_2$. We define the satisfaction relation $I, h \models_{\text{SL}} \phi$ inductively, as follows:

\[
\begin{align*}
I, h \models_{\text{SL}} \phi & \iff I \models \phi \text{ if } \phi \text{ is a } \Sigma\text{-formula} \\
I, h \models_{\text{SL}} \text{emp} & \iff h = \emptyset \\
I, h \models_{\text{SL}} t \mapsto u & \iff h = \{(t^f, u^f)\} \text{ and } t^f \neq \emptyset \\
I, h \models_{\text{SL}} \phi_1 \star \phi_2 & \iff \text{there exist heaps } h_1, h_2 \text{ s.t. } h = h_1 \lor h_2 \text{ and } I, h_1 \models_{\text{SL}} \phi_1, i = 1, 2 \\
I, h \models_{\text{SL}} \phi_1 \rightarrow \phi_2 & \iff \text{for all heaps } h' \text{ if } h' \# h \text{ and } I, h' \models_{\text{SL}} \phi_1 \text{ then } I, h' \lor h \models_{\text{SL}} \phi_2 \\
I, h \models_{\text{SL}} \exists x^S \cdot \varphi(x) & \iff I[\{x \leftarrow s\}, h] \models_{\text{SL}} \varphi(x) \text{, for some } s \in S^f
\end{align*}
\]

The satisfaction relation for $\Sigma$-formulae, Boolean connectives $\land, \neg$, and linear arithmetic atoms, are the classical ones from first-order logic. Notice that the range of a quantified variable $x^S$ is the interpretation of its associated sort $S^f$.

A formula $\varphi$ is said to be satisfiable if there exists an interpretation $I$ and a heap $h$ such that $I, h \models_{\text{SL}} \varphi$. The $(\text{SL}, T)$-satisfiability problem asks, given an $\text{SL}$ formula $\varphi$, whether there exists an interpretation $I$ of $T$ and a heap $h$ such that $I, h \models_{\text{SL}} \varphi$. We write $\varphi \models_{\text{SL}} \psi$ if for every interpretation $I$ and heap $h$, if $I, h \models_{\text{SL}} \varphi$ then $I, h \models_{\text{SL}} \psi$, and we say that $\varphi$ entails $\psi$ in this case.

The Bernays-Schönfinkel-Ramsey Fragment of SL In this paper we address the satisfiability problem for the class of sentences $\phi \equiv \exists x_1 \ldots \exists x_m \forall y_1 \ldots \forall y_n \cdot \varphi(x_1, \ldots, x_m, y_1, \ldots, y_n)$, where $\varphi$ is a quantifier-free formula of $\text{SL}(T)_{\text{Loc,Data}}$. We shall denote this fragment by $\exists^* \forall^* \text{SL}(T)_{\text{Loc,Data}}$. It is easy to see that any sentence $\phi$, as above, is satisfiable if and only if the sentence $\forall y_1 \ldots \forall y_n \cdot \varphi(c_1/x_1, \ldots, c_m/x_m)$ is satisfiable, where $c_1, \ldots, c_m$ are fresh (Skolem) constant symbols. The latter is called the functional form of $\phi$.

As previously mentioned, SL is used mainly specify properties of a program’s heap. If the program under consideration uses pointer arithmetic, as in C or C++, it is useful to consider $\text{LIA}$ for the theory of memory addresses. Otherwise, if the program only compares the values of the pointers for equality, as in Java, one can use $\text{E}$ for this purpose. This distinction led us to considering the satisfiability problem for $\exists^* \forall^* \text{SL}(T)_{\text{Loc,Data}}$ in the following cases:

1. $\text{Loc}$ is interpreted as the sort $U$ of $\text{E}$ and $\text{Data}$ as $U^k$, for some $k \geq 1$. The satisfiability problem for the fragment $\exists^* \forall^* \text{SL}(\text{E})_{U,U^k}$ is PSPACE-complete, and the proof follows a small model property argument.
2. as above, with the further constraint that $U$ is interpreted as an infinite countable set, i.e. of cardinality $\aleph_0$. In this case, we prove a cut-off property stating that all locations not in the domain of the heap and not used in the interpretation of constants, are equivalent from the point of view of an SL formula. This satisfiability problem is reduced to the unconstrained one above, and also found to be PSPACE-complete.
3. both $\text{Loc}$ and $\text{Data}$ are interpreted as $\text{Int}$, equipped with addition and total order, in which case $\exists^* \forall^* \text{SL}(\text{LIA})_{\text{Int,Int}}$ is undecidable.
4. \( \text{Loc} \) is interpreted as the sort \( U \) of \( E \), and \( \text{Data} \) as \( U \times \text{Int} \). Then \( \exists^* \forall^* \text{SL}(\text{ELIA})_{U \times \text{Int}} \) is undecidable.

Additionally, we prove that the fragment \( \exists^* \forall^* \text{SL}(E)_{U \times \text{Int}} \), with two quantifier alternations, is undecidable, if \( k \geq 2 \). The question whether the fragment \( \exists^* \forall^* \text{SL}(\text{ELIA})_{U \times \text{Int}} \) is decidable is currently open, and considered for future work.

For space reasons, all missing proofs are given in [24].

## 3 Decidability and Complexity Results

This section defines the decidable cases of the Bernays-Schönfinkel-Ramsey fragment of \( \text{SL} \), with matching undecidable extensions. The decidable fragment \( \exists^* \forall^* \text{SL}(E)_{U \times \text{Int}} \) relies on a small model property given in Section 3.1. Undecidability of \( \exists^* \forall^* \text{SL}(\text{LIA})_{\text{Int}, \text{Int}} \) is obtained by a refinement of the undecidability proof for Presburger arithmetic with one monadic predicate [14], in Section 3.4.

### 3.1 Small Model Property

The decidability proof for the quantifier-free fragment of \( \text{SL} \) [7, 30] relies on a small model property. Intuitively, no quantifier-free \( \text{SL} \) formula can distinguish between heaps in which the number of invisible locations, not in the range of the set of free variables, exceeds a certain threshold, linear in the size of the formula. Then a formula is satisfiable iff it has a heap model of size linear in the size of the input formula.

For reasons of self-containment, we recall a number of definitions and results from [30]. Some of them are slightly modified for our purposes, but these changes have no effect on the validity of the original proofs for the Lemmas 1 and 2 below. In the rest of this section, we consider formulae of \( \text{SL}(E)_{U \times \text{Int}} \), meaning that (i) \( \text{Loc} = U \), and (ii) there exists an integer \( k > 0 \) such that \( \text{Data} = U^k \), where \( U \) is the (uninterpreted) sort of \( E \). We fix \( k \) for the rest of this section.

**Definition 1.** [30, Definition 90] Given a set of locations \( S \), the equivalence relation \( \equiv_S \) between \( k \)-tuples of locations is defined as \( (v_1, \ldots, v_k) \equiv_S (v'_1, \ldots, v'_k) \) if and only if

- if \( v_i \in S \) then \( v_i = v'_i \), and
- if \( v_i \notin S \) then \( v'_i \notin S \),

for all \( i = 1, \ldots, k \).

Intuitively, \( \equiv_S \) restricts the equality to the elements in \( S \). Observe that \( \equiv_S \) is an equivalence relation and that \( S \subseteq T \) implies \( \equiv_T \subseteq \equiv_S \). For a set \( S \), we write \( |S| \) for its cardinality, in the following.

**Definition 2.** [30, Definition 91] Given an interpretation \( \mathcal{I} \), an integer \( n > 0 \), a set of variables \( X \subseteq \text{Vars} \) and a set of locations \( S \subseteq U^J \), for any two heaps \( h, h' : U^J \to^\text{fin} (U^J)^k \), we define \( h \sim_{n,X,S}^J h' \) if and only if

1. \( \mathcal{I}(X) \cap \text{dom}(h) = \mathcal{I}(X) \cap \text{dom}(h') \),
2. for all \( \ell \in \mathcal{I}(X) \cap \text{dom}(h) \), we have \( h(\ell) =_{\mathcal{I}(X), S} h'(\ell) \),
3. if \( |\text{dom}(h) \setminus \mathcal{I}(X)| < n \) then \( |\text{dom}(h) \setminus \mathcal{I}(X)| = |\text{dom}(h') \setminus \mathcal{I}(X)| \),
4. if \( |\text{dom}(h) \setminus \mathcal{I}(X)| \geq n \) then \( |\text{dom}(h') \setminus \mathcal{I}(X)| \geq n \).
Observe that, for any $n \leq m$ and $S \subseteq T$ we have $\sim^n_{\text{f}} \subseteq \sim^I_{\text{f}} \subseteq \sim^n_{\text{f}}$. In addition, for any integer $k > 0$, subset $S \subseteq U^I$ and location $\ell \in U^I$, we consider the function $\text{prun}^k_{I,S}(\ell_1, \ldots, \ell_k)$, which replaces each value $\ell_i \notin S$ in its argument list by $\ell$.

**Lemma 1.** [30, Lemma 94] Given an interpretation $I$ and a heap $h : U^I \rightarrow \text{fin} (U^I)^k$, for each integer $n > 0$, each set of variables $X \subseteq \text{Vars}$, each set of locations $L \subseteq U^I$ such that $L \cap I(X) = \emptyset$ and $|L| = n$, and each location $v \in U^I \setminus (I(X) \cup \{\text{nil}^I \} \cup L)$, there exists a heap $h' : U^I \rightarrow \text{fin} (U^I)^k$, with the following properties:

1. $h \sim^I_{\text{f}} h'$,
2. $\text{dom}(h') \setminus I(X) \subseteq L$,
3. for all $\ell \in \text{dom}(h')$, we have $h'(\ell) = \text{prun}^k_{I,I(X) \cup L}(h(\ell))$.

Next, we define the following measure on quantifier-free SL formulae:

$$\|\phi \| = |\phi| + |\phi|, \quad |\phi \rightarrow \psi| = |\phi|, \quad |\phi \land \psi| = \max(|\phi|, |\psi|), \quad |\neg\phi| = |\phi|$$

Intuitively, $|\phi|$ is the maximum number of invisible locations, that are not in $I(Fvc(\phi))$, and which can be distinguished by the quantifier-free SL($\text{E}$)$_{U,U^k}$ formula $\phi$. The crux of the PSPACE-completeness proof for quantifier-free SL($\text{E}$)$_{U,U^k}$ is that two heaps equivalent up to $|\phi|$ invisible locations are also equivalent from the point of view of satisfiability of $\phi$, which provides a small model property for this fragment [30, 7].

**Lemma 2.** [30, Prop. 95] Given a quantifier-free SL($\text{E}$)$_{U,U^k}$ formula $\phi$, an interpretation $I$, and two heaps $h$ and $h'$, if $h \sim^I_{\phi,Fvc(\phi),\emptyset} h'$ and $I, h \models_{\text{SL}} \phi$ then $I, h' \models_{\text{SL}} \phi$.

Our aim is to extend this result to $\exists^* \forall^* \text{SL(E)}_{U,U^k}$, in the first place. This new small model property is given by the next lemma.

**Lemma 3.** Let $\phi(x_1^U, \ldots, x_n^U)$ be a quantifier-free SL($\text{E}$)$_{U,U^k}$-formula, and $\phi' \equiv \forall x_1^U \ldots \forall x_n^U . \phi(x_1^U, \ldots, x_n^U)$ be its universal closure. Then $\phi'$ has a model if and only if only if there exists an interpretation $I$ and a heap $h : U^I \rightarrow \text{fin} (U^I)^k$ such that $I, h \models_{\text{SL}} \phi'$ and:

1. $|U^I| \leq |\phi| + |Fvc(\phi')| + n$,
2. $\text{dom}(h) \subseteq L \cup I(Fvc(\phi'))$,
3. for all $\ell \in \text{dom}(h)$, we have $h(\ell) \in (I(Fvc(\phi')) \cup \{\text{nil}^I \} \cup L \cup \{v\})^k$, where $L \subseteq U^I \setminus I(Fvc(\phi'))$ is a set of locations such that $|L| = |\phi| + n$ and $v \in U^I \setminus (I(Fvc(\phi')) \cup \{\text{nil}^I \} \cup L)$ is an arbitrary location.

We are ready to prove two decidability results, based on the above small model property, concerning the cases where (i) $\text{Loc}$ is interpreted as a countable set with equality, and (ii) $\text{Loc}$ is interpreted as an infinite countable set with no other operators than equality.

### 3.2 Uninterpreted Locations without Cardinality Constraints

In this section, we consider the satisfiability problem for the fragment $\exists^* \forall^* \text{SL(E)}_{U,U^k}$, where the location sort $U$ can be interpreted by any (possibly finite) countable set, with no other operations than the equality, and the data sort consists of $k$-tuples of locations.
Theorem 1. The satisfiability problem for $\exists^* \forall^* \SL(E)_{U,U^k}$ is PSPACE-complete.

Proof. PSPACE-hardness follows from the fact that satisfiability is PSPACE-complete for quantifier-free $\SL(E)_{U,U^k}$ [7]. To prove membership in PSPACE, consider the formula $\phi \equiv \exists x_1 \ldots \exists x_m \forall y_1 \ldots \forall y_n \cdot \varphi(x,y)$, where $\varphi$ is a quantifier-free $\SL(E)_{U,U^k}$ formula. Let $c = (c_1, \ldots, c_m)$ be a tuple of constant symbols, and $\bar{\phi} \equiv \forall y_1 \ldots \forall y_n \cdot \varphi(c,y)$ be the functional form of $\phi$, obtained by replacing $x_i$ with $c_i$, for all $i = 1, \ldots, m$. By Lemma 3, $\bar{\phi}$ has a model if and only if it has a model $I,h$ such that:
- $|U^I| \leq |\varphi| + n + m$,
- $\dom(h) \subseteq L \cup \ell^I$,
- $\forall \ell \in \dom(h). h(\ell) \in (I(c) \cup \{\text{nil}\} \cup L \cup \{v\})^k$.

where $L \subseteq U^I \setminus I(c)$. $|L| = |\varphi| + m$ and $v \in U^I \setminus (I(c) \cup \{\text{nil}\} \cup L)$. We describe below a nondeterministic polynomial space algorithm that decides satisfiability of $\bar{\phi}$. First, nondeterministically chose a model $I,h$ that meets the above requirements. Then we check, for each tuple $(u_1,\ldots,u_n) \in (U^I)^n$ that $I[y_1 \leftarrow u_1,\ldots,y_n \leftarrow u_n].h \models_{SL} \varphi$. In order to enumerate all tuples from $(U^I)^n$ we need $n \cdot \log_2(|\varphi| + n + m)$ extra bits, and the check for each such tuple can be done in PSPACE, according to [7, §5].

This result is somewhat surprising, because the classical Bernays-Schönfinkel fragment of first-order formulae with predicate symbols (but no function symbols) and quantifier prefix $\exists^* \forall^* \exists^*$ is known to be NEXPTIME-complete [17, §7]. The explanation lies in the fact that the interpretation of an arbitrary predicate symbol $P(x_1,\ldots,x_n)$ cannot be captured using only points-to atomic propositions, e.g. $x_1 \rightarrow (x_2,\ldots,x_n)$, between locations and tuples of locations, due to the interpretation of points-to’s as heaps\(^5\) (finite partial functions).

The following lemma sets a first decidability boundary for $\SL(E)_{U,U^k}$, by showing how extending the quantifier prefix to $\exists^* \forall^* \exists^*$ leads to undecidability.

Lemma 4. The satisfiability problem for $\exists^* \forall^* \exists^* \SL(E)_{U,U^k}$ is undecidable, if $k \geq 2$.

Observe that the result of Lemma 4 sets a fairly tight boundary between the decidable and undecidable fragments of $\SL$. On the one hand, simplifying the quantifier prefix to $\exists^* \forall^*$ yields a decidable fragment (Theorem 1), whereas $\SL(E)_{U,U} (k = 1)$ without the magic wand ($\rightarrow$) is decidable with non-elementary time complexity, even when considering an unrestricted quantifier prefix [4].

3.3 Uninterpreted Locations with Cardinality $\mathbb{N}_0$

We consider the stronger version of the satisfiability problem for $\exists^* \forall^* \SL(E)_{U,U^k}$, where $U$ is interpreted as an infinite countable set (of cardinality $\mathbb{N}_0$) with no function symbols, other than equality. Instances of this problem occur when, for instance, the location sort is taken to be Int, but no operations are used on integers, except for testing equality.

Observe that this restriction changes the satisfiability status of certain formulae. For instance, $\exists x \forall y. y \neq \text{nil} \Rightarrow (y \rightarrow \langle x \ast \top \rangle)$ is satisfiable if $U$ is interpreted as a finite set, but becomes unsatisfiable when $U$ is infinite. The reason is that this formula requires

---

\(^5\) If $x_1 \rightarrow (x_2,\ldots,x_n)$ and $x_1 \rightarrow (x'_2,\ldots,x'_n)$ hold, this forces $x_i = x'_i$ for all $i = 2,\ldots,n$. 


every location from $U^T$ apart from nil to be part of the domain of the heap, which is impossible due to the fact that only finite heaps are considered by the semantics of SL.

In the following proof, we use the formula $\text{alloc}(x) \equiv x \mapsto (x, \ldots, x) \in \bot$, expressing the fact that a location variable $x$ is allocated, i.e., its interpretation is part of the heap’s domain [4]. Intuitively, we reduce any instance of the $\exists \forall^\ast \text{SL}(E)_{U,U^T}$ satisfiability problem, with $U$ of cardinality $\aleph_0$, to an instance of the same problem without this restriction, by the following cut-off argument: if a free variable is interpreted as a location which is neither part of the heap’s domain, nor equal to the interpretation of some constant, then it is not important which particular location is chosen for that interpretation.

**Theorem 2.** The satisfiability problem for $\exists \forall^\ast \text{SL}(E)_{U,U^T}$ is PSPACE-complete if $U$ is required to have cardinality $\aleph_0$.

**Proof.** PSPACE-hardness follows from the PSPACE-completeness of the satisfiability problem for quantifier-free SL, with uninterpreted locations [7, §5.2]. Since the reduction from [7, §5.2] involves no universally quantified variables, the $\aleph_0$ cardinality constraint has no impact on this result.

Let $\exists x_1 \ldots \exists x_n \forall y_1 \ldots \forall y_n \cdot \varphi(x, y)$ be a formula, and $\forall y_1 \ldots \forall y_n \cdot \varphi(c, y)$ be its functional form, obtained by replacing each $x_i$ with $c_j$, for $i = 1, \ldots, m$. We consider the following formulae, parameterized by $y_i$, for $i = 1, \ldots, n$:

$$
\begin{align*}
\psi_0(y_i) &\equiv \text{alloc}(y_i) \\
\psi_1(y_i) &\equiv \bigwedge_{j=1}^m y_i = c_j \\
\psi_2(y_i) &\equiv y_i = d_i \\
\text{external} &\equiv \bigwedge_{i=1}^n (\neg \text{alloc}(d_i) \land \bigwedge_{j=1}^m d_i \neq c_j)
\end{align*}
$$

where $\{d_i | i = 1, \ldots, n\}$ is a set of fresh constant symbols. We show the following fact:

**Fact 1** There exists an interpretation $I$ and a heap $h$ such that $|U^T| = \aleph_0$ and $I, h \models_{\text{SL}} \forall y_1 \ldots \forall y_n \cdot \varphi(c, y)$ if there exists an interpretation $I'$, not constraining the cardinality of $U^T$, and a heap $h'$ such that:

$$
I', h' \models_{\text{SL}} \text{external} \land \forall y_1 \ldots \forall y_n \bigwedge_{(t_1, \ldots, t_n) \in \{0,1,2\}^n} \bigwedge_{i=1}^n (\psi_{t_i}(y_i) \Rightarrow \varphi(c, y))
$$

To show membership in PSPACE, consider a nondeterministic algorithm that chooses $I'$ and $h'$ and uses $2n$ extra bits to check that $I', h' \models_{\text{SL}} \text{external} \land \forall y_1 \ldots \forall y_n \cdot \varphi(t_1, \ldots, t_n)$ separately, for each $(t_1, \ldots, t_n) \in \{0,1,2\}^n$. By Lemma 3, the sizes of $I'$ and $h'$ are bounded by a polynomial in the size of $\Psi_{(t_1, \ldots, t_n)}$, which is polynomial in the size of $\varphi$, and by Theorem 1, each of these checks can be done in polynomial space. \hfill $\square$

### 3.4 Integer Locations with Linear Arithmetic

In the rest of this section we show that the Bernays-Schönfinkel-Ramsey fragment of SL becomes undecidable as soon as we use integers to represent the set of locations and
combine SL with linear integer arithmetic (LIA). The proof relies on an undecidability argument for a fragment of Presburger arithmetic with one monadic predicate symbol, interpreted over finite sets. Formally, we denote by \((\exists^* \forall^* \cap \forall^* \exists^*)\) – LIA the set of formulae consisting of a conjunction between two linear arithmetic formulae, one with quantifier prefix in the language \(\exists^* \forall^*\), and another with quantifier prefix \(\forall^* \exists^*\).

**Theorem 3.** The satisfiability problem is undecidable for the fragment \((\exists^* \forall^* \cap \forall^* \exists^*)\) – LIA, with one monadic predicate symbol, interpreted over finite sets of integers.

**Proof.** We reduce from the following variant of *Hilbert's 10th Problem*: given a multivariate Diophantine polynomial \(R(x_1, \ldots, x_n)\), the problem “does \(R(x_1, \ldots, x_n) = 0\) have a solution in \(\mathbb{N}^n\)” is undecidable [18].

By introducing sufficiently many free variables, we encode \(R(x_1, \ldots, x_n) = 0\) as an equisatisfiable Diophantine system of degree at most two, containing only equations of the form \(x = yz\) (resp. \(x = y^2\)) and linear equations \(\sum_{i=1}^{d} a_i x_i = b\), where \(a_1, \ldots, a_d, b \in \mathbb{Z}\). Next, we replace each equation of the form \(x = yz\), with \(y\) and \(z\) distinct variables, with the quadratic system \(2x + t_x + t_z = t_{yz} \land t_z = y^2 \land t_z = z^2 \land t_{yz} = (y + z)^2\), where \(t_x, t_z\) and \(t_{yz}\) are fresh (free) variables. In this way, we replace all multiplications between distinct variables by occurrences of the squaring function. Let \(\Psi^R(x_1, \ldots, x_n) = 0\) be the conjunction of the above equations. It is manifest that \(R(x_1, \ldots, x_n) = 0\) has a solution in \(\mathbb{N}^n\) iff \(\Psi^R(x_1, \ldots, x_n) = 0\) is satisfiable, with all free variables ranging over \(\mathbb{N}\).

Now we introduce a monadic predicate symbol \(P\), which is intended to denote a (possibly infinite) set of consecutive perfect squares, starting with 0. To capture this definition, we require the following:

\[
P(0) \land P(1) \land \forall x \forall y \forall z . P(x) \land P(y) \land P(z) \land x < y < z \land 
(\forall u . x < u < y \lor y < u < z \Rightarrow \neg P(u)) \Rightarrow z - y = y - x + 2
\]  

(sqr)

Observe that this formula is a weakening of the definition of the infinite set of perfect squares given by Halpern [14], from which the conjunct \(\forall x \exists y . y > x \land P(y)\), requiring that \(P\) is an infinite set of natural numbers, has been dropped. Moreover, notice that \(\text{sqr}\) has quantifier prefix \(\forall^3 \exists\), due to the fact that \(\forall u\) occurs implicitly under negation, on the left-hand side of an implication. If \(P\) is interpreted as a finite set \(P^d = \{p_0, p_1, \ldots, p_N\}\) such that (w.l.o.g.) \(p_0 < p_1 < \ldots < p_N\), it is easy to show, by induction on \(N > 0\), that \(p_i = i^2\), for all \(i = 0, 1, \ldots, N\).

The next step is encoding the squaring function using the monadic predicate \(P\). This is done by replacing each atomic proposition \(x = y^2\) in \(\Psi^R(x_1, \ldots, x_n) = 0\) by the formula \(\theta_{x = y^2} \equiv P(x) \land P(x + 2y + 1) \land \forall z . x < z < x + 2y + 1 \Rightarrow \neg P(z)\).

**Fact 2** For any interpretation \(\mathcal{I}\) mapping \(x\) and \(y\) into \(\mathbb{N}\), \(\mathcal{I} \models x = y^2\) iff \(\mathcal{I}\) can be extended to an interpretation of \(P\) as a finite set of consecutive perfect squares such that \(\mathcal{I} \models \theta_{x = y^2}\).

Let \(\Phi^R(x_1, \ldots, x_n) = 0\) be the conjunction of \(\text{sqr}\) with the formula obtained by replacing each atomic proposition \(x = y^2\) with \(\theta_{x = y^2}\) in \(\Psi^R(x_1, \ldots, x_n) = 0\). Observe that each universally quantified variable in \(\Phi^R(x_1, \ldots, x_n) = 0\) occurs either in \(\text{sqr}\) or in some \(\theta_{x = y^2}\), and moreover, each \(\theta_{x = y^2}\) belongs to the \(\exists^* \forall^*\) fragment of LIA. \(\Phi^R(x_1, \ldots, x_n) = 0\) belongs thus to the \(\exists^* \forall^* \cap \forall^* \exists^*\).
∀ \exists \forall \θ fragment of LIA, with P being the only monadic predicate symbol. Finally, we prove that \( R(x_1, \ldots, x_n) = 0 \) has a solution in \( \mathbb{N}^n \) iff \( \Phi_{R(x_1, \ldots, x_n)} = 0 \) is satisfiable.

⇒ Let \( \mathcal{I} \) be a valuation mapping \( x_1, \ldots, x_n \) into \( \mathbb{N} \), such that \( \mathcal{I} \models R(x_1, \ldots, x_n) = 0 \). Obviously, \( \mathcal{I} \) can be extended to a model of \( \forall \exists \forall \θ \) by assigning \( t^I_x = (x^2)^2 \) for all auxiliary variables \( t_x \) occurring in \( \forall \exists \forall \theta(R(x_1, \ldots, x_n)) = 0 \). We extend \( \mathcal{I} \) to a model of \( \forall \exists \forall \theta(R(x_1, \ldots, x_n)) = 0 \) by assigning \( P^I = \{ n^2 \mid 0 \leq n \leq \sqrt{m} \} \), where \( m = \max\{ x^2 + 1 \mid x \in \text{Fvc}(\forall \exists \forall \theta(R(x_1, \ldots, x_n)) = 0) \} \). Clearly, \( P^I \) meets the requirements of \( \text{sqr} \). By Fact 2, we obtain that \( \mathcal{I} \models \exists \forall \theta \) for each subformula \( \theta_{x=y} \) of \( \Phi_{R(x_1, \ldots, x_n)} = 0 \), thus \( \mathcal{I} \models \Phi_{R(x_1, \ldots, x_n)} = 0 \).

⇐ If \( \mathcal{I} \models \forall \exists \forall \theta(R(x_1, \ldots, x_n)) = 0 \), then, by \( \text{sqr} \), \( P^I \) is a set of consecutive perfect squares, and, by Fact 2, \( \mathcal{I} \models x = y^2 \) for each subformula \( \theta_{x=y} \) of \( \Phi_{R(x_1, \ldots, x_n)} = 0 \). Then \( \mathcal{I} \models \forall \exists \forall \theta(R(x_1, \ldots, x_n)) = 0 \) and consequently \( \mathcal{I} \models R(x_1, \ldots, x_n) = 0 \).

We consider now the satisfiability problem for the fragment \( \exists \forall \exists \forall \text{SL} \text{(LIA)}_{\text{Int}, \text{Int}} \) where both \( \text{Loc} \) and \( \text{Data} \) are taken to be the \( \text{Int} \) sort, equipped with addition and total order. Observe that, in this case, the heap consists of a set of lists, possibly with aliases and circularities. Without losing generality, we consider that \( \text{Int} \) is interpreted as the set of positive integers.

The above theorem cannot be directly used for the undecidability of \( \exists \forall \exists \forall \text{SL} \text{(LIA)}_{\text{Int}, \text{Int}} \), by interpreting the (unique) monadic predicate as the (finite) domain of the heap. The problem is with the \( \text{sqr} \) formula, that defines the interpretation of the monadic predicate as a set of consecutive perfect squares \( 0, 1, \ldots, n^2 \), and whose quantifier prefix lies in the \( \forall \exists \forall \) fragment. We overcome this problem by replacing the \( \text{sqr} \) formula above with a definition of such sets in \( \exists \forall \exists \forall \text{SL} \text{(LIA)}_{\text{Int}, \text{Int}} \). Let us first consider the following properties expressed in \( \text{SL} \) [4]:

\[
\begin{align*}
\#x \geq 1 &\equiv \exists u. u \mapsto x * T \\
\#x \leq 1 &\equiv \forall u \forall t. \neg(u \mapsto x * T \mapsto x * T)
\end{align*}
\]

Intuitively, \( \#x \geq 1 \) states that \( x \) has at least one predecessor in the heap, whereas \( \#x \leq 1 \) states that \( x \) has at most one predecessor. We use \( \#x = 0 \) and \( \#x = 1 \) as shorthands for \( \neg(\#x \geq 1) \) and \( \#x \geq 1 \land \#x \leq 1 \), respectively. The formula below states that the heap can be decomposed into a list segment starting with \( x \) and ending in \( y \), and several disjoint cyclic lists:

\[
x \mapsto y \equiv \#x = 0 \land \text{alloc}(x) \land \#y = 1 \land \neg \text{alloc}(y) \land \\
\forall z. z \neq y \Rightarrow (\#z = 1 \Rightarrow \text{alloc}(z)) \land \forall z. \#z \leq 1
\]

We forbid the existence of circular lists by adding the following arithmetic constraint:

\[
\forall u \forall t. u \mapsto t * T \Rightarrow u < t \tag{nocyc}
\]

We ask, moreover, that the elements of the list segment starting in \( x \) are consecutive perfect squares:

\[
\text{consqr}(x) \equiv x = 0 \land x \mapsto 1 * T \land \forall z. \forall u \forall t. z \mapsto u * u \mapsto t * T \Rightarrow t - u = u - z + 2 \tag{consqr}
\]

Observe that the formula \( \exists x \exists y. x \mapsto y \land \text{nocyc} \land \text{consqr}(x) \) belongs to \( \exists \forall \exists \forall \text{SL} \text{(LIA)}_{\text{Int}, \text{Int}} \).
The satisfiability problem for $\exists \forall^* SL(LIA)_{\text{int, int}}$ is undecidable.

**Proof.** We use the same reduction as in the proof of Theorem 3, with two differences:

- we replace $\text{sqr}$ by $\exists x \exists y . x \rightarrow y \wedge \text{nocyc} \wedge \text{consqr}(x)$, and
- define $\theta_{\text{easy}} \equiv \text{alloc}(x) \wedge \text{alloc}(x+2y+1) \wedge \forall z . x < z < x+2y+1 \Rightarrow \neg \text{alloc}(z)$. \qed

It is tempting, at this point to ask whether interpreting locations as integers and considering subsets of $LIA$ instead may help recover the decidability. For instance, it has been found that the Bernays-Schönfinkel-Ramsey class is decidable in presence of integers with difference bounds arithmetic [29], and the same type of question can be asked about the fragment of $\exists \forall^* SL(LIA)_{\text{int, int}}$ with difference bounds constraints only.

Finally, we consider a variant of the previous undecidability result, in which locations are the (uninterpreted) sort $U$ of $E$ and the data consists of tuples of sort $U \times \text{Int}$. This fragment of SL can be used to reason about lists with integer data. The undecidability of this fragment can be proved along the same lines as Theorem 4.

**Theorem 5.** The satisfiability problem for $\exists \forall^* SL(ELIA)_{U, U \times \text{Int}}$ is undecidable.

## 4 A Procedure for $\exists \forall^*$ Separation Logic in an SMT Solver

This section presents a procedure for the satisfiability of $\exists \forall^* SL(E)_{U, U}$ inputs \footnote{The procedure is incorporated into the master branch of the SMT solver CVC4 (https://github.com/CVC4), and can be enabled by command line parameter --quant-epr}. Our procedure builds upon our previous work [25], which gave a decision procedure for quantifier-free $SL(T)_{\text{Loc, Data}}$ inputs for theories $T$ where the satisfiability problem for quantifier-free $T$-constraints is decidable. Like existing approaches for quantified formulas in SMT [13, 23], our approach is based on incremental quantifier instantiation based on a stream of candidate models returned by a solver for quantifier-free inputs. Our approach for this fragment exploits the small model property given in Lemma 3 to restrict the set of quantifier instantiations it considers to a finite set.

Figure 1 gives a counterexample-guided approach for establishing the satisfiability of input $\exists x \forall y \varphi(x, y)$. We first introduce tuples of fresh constants $k$ and $e$ of the same type as $x$ and $y$ respectively. Our procedure will be based on finding a set of instantiations of $\forall y \varphi(k, y)$ that are either collectively unsatisfiable or are satisfiable and entail our input. Then, we construct a set $L$ which is the union of constants $k$ and a set $L'$ of fresh constants whose cardinality is equal to $|\varphi(x, y)|$ (see Section 3.1) plus the number of universal variables $n$ in our input. Conceptually, $L$ is a finite set of terms from which the instantiations of $y$ in $\forall y \varphi(k, y)$ can be built.

After constructing $L$, we call the recursive subprocedure $\text{solve-rec}$ on $\Gamma$ (initially empty) and $L$. This procedure incrementally adds instances of $\forall y \varphi(k, y)$ to $\Gamma$. In step 1, we first check if $\Gamma$ is $(SL, T)$-unsatisfiable using the procedure from [25]. If so, our input is $(SL, T)$-unsatisfiable. Otherwise, in step 2 we consider the miniscoped form of our input $\exists x \forall y \varphi_1(x, y) \wedge \ldots \wedge \forall y \varphi_p(x, y)$, that is, where quantification over $x$ is distributed over conjunctions. In the following, we may omit quantification on conjunctions $\varphi_j$ that do not contain variables from $y$. Given this formula, for each $j = 1, \ldots, p$, we check the $(SL, T)$-satisfiability of set $\Gamma'_j$ containing $\Gamma$, the negation of $\forall y \varphi_j(k, y)$ where $y$ is...
solve(∃x∀yφ(x,y)) where x = (x₁, ..., xₘ) and y = (y₁, ..., yₙ):

Let k = (k₁, ..., kₙ) and e = (e₁, ..., eₙ) be fresh constants of the same type as x and y.
Let L = L' ∪ {k₁, ..., kₙ}, where L' is a set of fresh constants s.t. |L'| = |φ(x,y)| + n.
Return solve_rec(∃x∀yφ(x,y), L).

solve_rec(∃x∀yφ(x,y), Γ, L):
1. If Γ is (SL,E)-unsat, return “unsat”.
2. Assume ∃x∀yφ(x,y) is equivalent to ∃x∀yφ₁(x,y) ∧ ... ∧ ∀yφₚ(x,y).

If Γ' = Γ ∪ {¬φ_j(k, e) ∧ \bigwedge_{i=1}ⁿ eᵢ = tᵢ} is (SL,E)-unsat for all j = 1, ..., p, return “sat”.
3. Otherwise, let I, h ⊨ₕ Γ'ᵢ for some j ∈ {1, ..., p}.
   Let t = (t₁, ..., tₙ) be such that eᵢ' = uᵢ and tᵢ ∈ L for each i = 1, ..., n.
   Return solve_rec(∃x∀yφ(x,y), Γ ∪ {φⱼ(k,t)}, L).

Fig. 1. A counterexample-guided procedure for ∃x∀ySL(E)₁∪ₚ formulas ∃x∀yφ(x,y), where U is an uninterpreted sort in the signature of E.

replaced by fresh constants e, and a conjunction of constraints that says each eᵢ must be equal to at least one term in L for i = 1, ..., n. If Γ'ᵢ is (SL,T)-unsatisfiable for each j = 1, ..., p, our input is (SL,T)-satisfiable. Otherwise in step 3, given an interpretation I and heap h satisfying Γ'ᵢ, we construct a tuple of terms t = (t₁, ..., tₙ) used for instantiating ∀yφⱼ(k, t). For each i = 1, ..., n, we choose tᵢ to be a term from L whose interpretation is the same as eᵢ. The existence of such a tᵢ is guaranteed by the fact that I satisfies the constraint from Γ'ᵢ that tells us eᵢ is equal to at least one such term. This selection ensures that instantiations on each iteration are chosen from a finite set of possibilities and are unique. In practice, the procedure terminates, both for unsatisfiable and satisfiable inputs, before considering all t from L' for each ∀yφⱼ(k, t).

Theorem 6. Let U be an uninterpreted sort belonging to the signature of E. For all ∃x∀ySL(E)₁∪ₚ formulae ψ of the form ∃x∀yφ(x,y), solve(ψ):
1. Answers “unsat” only if ψ is (SL,E)-unsatisfiable.
2. Answers “sat” only if ψ is (SL,E)-satisfiable.
3. Terminates.

We discuss a few important details regarding our implementation of the procedure.

Matching Heuristics When constructing the terms t for instantiation, it may be the case that eᵢ' = uᵢ for multiple u ∈ L for some i ∈ {1, ..., n}. In such cases, the procedure will choose one such u for instantiation. To increase the likelihood of the instantiation being relevant to the satisfiability of our input, we use heuristics for selecting the best possible u among those whose interpretation is equal to eᵢ in I. In particular, if eᵢ' = uᵢ' = uᵢ", and Γ" contains predicates of the form eᵢ → v and u₁ → v₁ for some v, v₁ where v" = v'₁ but no predicate of the form u₂ → v₂ for some v₂ where v" = v'₂, then we strictly prefer term u₁ over term u₂ when choosing term tᵢ for eᵢ.
Finding Minimal Models} Previous work [26] developed efficient techniques for finding small models for uninterpreted sorts in CVC4. We have found these techniques to be beneficial to the performance of the procedure in Figure 1. In particular, we use these techniques to find $\Sigma$-interpretations $I$ in $\text{solve}_{\text{rec}}$ that interpret $U$ as a finite set of minimal size. When combined with the aforementioned matching heuristics, these techniques lead to finding useful instantiations more quickly, since more terms are constrained to be equal to $e_i$ for $i = 1, \ldots, n$ in interpretations $I$.

**Symmetry Breaking** The procedure in Figure 1 introduces a set of fresh constants $L$, which in turn introduce the possibility of discovering $\Sigma$-interpretations $I$ that are isomorphic, that is, identical up to renaming of constants in $L'$. Our procedure adds additional constraints to $\Gamma$ that do not affect its satisfiability, but reduce the number of isomorphic models. In particular, we consider an ordering $\prec$ on the constants from $L'$, and add constraints that ensure that all models $(I, h)$ of $\Gamma$ are such that if $\ell_2 \not\in \text{dom}(h)$, then $\ell_2 \not\in \text{dom}(h)$ for all $\ell_2$ such that $\ell_1 < \ell_2$.

**Example 1.** Say we wish to show the validity of the entailment $x \neq y \land x \rightarrow z \models_{\text{SL}} e, x \mapsto u$, from the introductory example (Section 1), where $x, y, z, u$ are of sort $U$ of $E$. This entailment is valid iff the $\exists^* \forall^* \text{SL}(E)_{U,L,U}$ formula $\exists x \exists y \exists z \forall u . x \neq y \land x \rightarrow z \land \neg x \rightarrow u$ is $(\text{SL}, E)$-unsatisfiable. A run of the procedure in Figure 1 on this input constructs tuples $k = (k_x, k_y, k_z)$ and $e = (e_u)$, and set $L = \{k_x, k_y, k_z, \ell_1, \ell_2\}$, noting that $x \neq y \land x \rightarrow z \land \neg x \rightarrow u$ is $\{k_x, k_y, k_z, \ell_1, \ell_2\}$. We then call $\text{solve}_{\text{rec}}$ where $\Gamma$ is initially empty. By miniscoping, our input is equivalent to $\exists x \exists y \exists z . x \neq y \land x \rightarrow z \land \neg x \rightarrow u$. On the first two recursive calls to $\text{solve}_{\text{rec}}$, we may add $k_x \neq k_y$ and $k_x \mapsto k_z$ to $\Gamma'$ by trivial instantiation of the first two conjuncts. On the third recursive call to $\text{solve}_{\text{rec}}$, we may add $k_x \neq k_y$ and $k_x \mapsto k_z$ to $\Gamma'$ by trivial instantiation of the first two conjuncts. On the third recursive call to $\text{solve}_{\text{rec}}$, we may add $k_x \neq k_y$ and $k_x \mapsto k_z$ to $\Gamma'$ by trivial instantiation of the first two conjuncts. On the third recursive call to $\text{solve}_{\text{rec}}$, we may add $k_x \neq k_y$ and $k_x \mapsto k_z$ to $\Gamma'$ by trivial instantiation of the first two conjuncts.

A modified version of the procedure in Figure 1 can be used for $\exists^* \forall^* \text{SL}(T)_{\text{Loc, Data}}$-satisfiability for theories $T$ beyond equality, and where $\text{Loc}$ and $\text{Data}$ are not restricted to uninterpreted sorts. Notice that in such cases, we cannot restrict $\Sigma$-interpretations $I$ in $\text{solve}_{\text{rec}}$ to interpret each $e_i$ as a member of finite set $L$, and hence we modify $\text{solve}_{\text{rec}}$ to omit the constraint restricting variables in $e$ to be equal to a term from $L$ in the check in Step 2. This modification results in a procedure that is sound both for “unsat” and “sat”, but is no longer terminating in general. Nevertheless, it may be used as a heuristic for determining $\exists^* \forall^* \text{SL}(T)_{\text{Loc, Data}}$-(un)satisfiability.

5 Experimental Evaluation

We implemented the $\text{solve}$ procedure from Figure 1 within the CVC4 SMT solver\(^8\) (version 1.5 prerelease). This implementation was tested on two kinds of benchmarks:

\(^8\) Available at http://cvc4.cs.nyu.edu/web/.
(i) finite unfoldings of inductive predicates, mostly inspired by benchmarks used in the SL-COMP'14 solver competition [27], and (ii) verification conditions automatically generated by applying the weakest precondition calculus of [15] to the program loops in Figure 2. All experiments were run on a 2.80GHz Intel(R) Core(TM) i7 CPU machine with 8MB of cache 9.

We compared our implementation with the results of applying the CVC4 decision procedure for the quantifier-free fragment of SL [25] to a variant of the benchmarks, obtained by manual quantifier instantiation, as follows. Consider checking the validity of the entailment $\exists x . \phi(x) \models_{SL} \exists y . \psi(y)$, which is equivalent to the unsatisfiability of the formula $\exists x \forall y . \phi(x) \land \neg \psi(y)$. We first check the satisfiability of $\phi$. If $\phi$ is not satisfiable, the entailment holds trivially, so let us assume that $\phi$ has a model. Second, we check the satisfiability of $\phi \land \psi$. Again, if this is unsatisfiable, the entailment cannot hold, because there exists a model of $\phi$ which is not a model of $\psi$. Else, if $\phi \land \psi$ has a model, we add an equality $x = y$ for each pair of variables $(x, y) \in \mathbf{x} \times \mathbf{y}$ that are mapped to the same term in this model, the result being a conjunction $E(\mathbf{x}, \mathbf{y})$ of equalities. Finally, we check the satisfiability of the formula $\phi \land \neg \psi \land E$. If this formula is unsatisfiable, the entailment is valid, otherwise, the check is inconclusive. The times in Table 1 correspond to checking satisfiability of $\exists x \forall y . \phi(x) \land \neg \psi(y)$ using the $\text{solve}$ procedure (Figure 1), compared to checking satisfiability of $\phi \land \neg \psi \land E$, where $E$ is manually generated.

In the first set of experiments (Table 1) we have considered inductive predicates commonly used as verification benchmarks [27]. Here we check the validity of the entailment between lhs and rhs, where both predicates are unfolded $n = 1, 2, 3, 4, 8$ times. The entailment between $\text{pos}_1$ and $\text{neg}_1$ is skipped because it is not valid (since the negated formula is satisfiable, we cannot generate the manual instantiation).

The second set of experiments considers the verification conditions of the forms $\varphi \Rightarrow \text{wp}(l, \phi)$ and $\varphi \Rightarrow \text{wp}^n(l, \phi)$, where $\text{wp}(l, \phi)$ denotes the weakest precondition of the SL formula $\phi$ with respect to the sequence of statements $l$, and $\text{wp}^n(l, \phi) = \text{wp}(l, \ldots \text{wp}(l, \text{wp}(l, \phi)) \ldots)$ denotes the iterative application of the weakest precondition $n$ times in a row. We consider the loops depicted in Figure 2, where, for each loop $l$, we consider the variant $z\mathbf{l}$ as well, which tests that the data values contained within the memory cells

9 The CVC4 binary and examples used in these experiments are available at http://cs.uiowa.edu/~ajreynol/VMCAI2017-seplog-epr.
are equal to a constant $c_0$ of sort Loc, by the assertions on line 2. The postconditions are specified by finite unfoldings of the inductive predicates list and zlist.

We observed that, compared to checking the manual instantiation, the fully automated solver was less than 0.5 seconds slower on 72% of the test cases, and less than 1 second slower on 79% of the test cases. The automated solver experienced 3 timeouts, where the manual instantiation succeeds (for tree vs tree with $n = 8$, fs vs ts with $n = 3$, and list$^n(u) \land \text{list}^0(v)$ vs wp$^n(\text{rev}, u = \text{nil} \land \text{list}^0(v))$ with $n = 8$). These timeouts are caused by the first call to the quantifier-free SL decision procedure, which fails to produce a model in less than 300 seconds (time not accounted for in the manually produced instance of the problem).

<table>
<thead>
<tr>
<th>lhs</th>
<th>rhs</th>
<th>$n = 1$</th>
<th>$n = 2$</th>
<th>$n = 3$</th>
<th>$n = 4$</th>
<th>$n = 8$</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unfoldings of inductive predicates</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\text{ls}(x,y) \equiv \text{emp} \land x=y \land y \neq y$</td>
<td>$\text{ls}(x,y) \equiv \text{emp} \land x=y \land y \neq y$</td>
<td>solve</td>
<td>&lt; 0.01s</td>
<td>0.02s</td>
<td>0.03s</td>
<td>0.05s</td>
</tr>
<tr>
<td>$\exists r. x = r \land x \neq x \lor \text{emp}(y)$</td>
<td>$\exists r. x = r \land x \neq x \lor \text{emp}(y)$</td>
<td>manual</td>
<td>&lt; 0.01s</td>
<td>&lt; 0.01s</td>
<td>&lt; 0.01s</td>
<td>&lt; 0.01s</td>
</tr>
<tr>
<td>$\text{tree}(x) \equiv \text{emp} \land x = x \lor \text{tree}(y)$</td>
<td>$\text{tree}(x) \equiv \text{emp} \land x = x \lor \text{tree}(y)$</td>
<td>solve</td>
<td>&lt; 0.01s</td>
<td>0.04s</td>
<td>1.43s</td>
<td>23.42s</td>
</tr>
<tr>
<td>$\exists r. x = r \lor x \neq (x+y) \lor \text{tree}(y)$</td>
<td>$\exists r. x = r \lor x \neq (x+y) \lor \text{tree}(y)$</td>
<td>manual</td>
<td>&lt; 0.01s</td>
<td>&lt; 0.01s</td>
<td>&lt; 0.01s</td>
<td>&lt; 0.01s</td>
</tr>
<tr>
<td>$\text{ts}(x,a) \equiv \text{emp} \land x = x \lor \text{ts}(y)$</td>
<td>$\text{ts}(x,a) \equiv \text{emp} \land x = x \lor \text{ts}(y)$</td>
<td>solve</td>
<td>&lt; 0.01s</td>
<td>0.81s</td>
<td>&gt; 300s</td>
<td>&gt; 300s</td>
</tr>
<tr>
<td>$\exists r. x = r \lor x \neq (x+y) \lor \text{ts}(y)$</td>
<td>$\exists r. x = r \lor x \neq (x+y) \lor \text{ts}(y)$</td>
<td>manual</td>
<td>&lt; 0.01s</td>
<td>0.03s</td>
<td>103.89s</td>
<td>&gt; 300s</td>
</tr>
<tr>
<td>pos$^1(x,a) \equiv a \neq a \lor \text{ts}(3, y)$</td>
<td>neg$^1(x,a) \equiv a \neq a \lor \text{ts}(3, y)$</td>
<td>solve</td>
<td>0.34s</td>
<td>0.01s</td>
<td>0.31s</td>
<td>0.76s</td>
</tr>
<tr>
<td>$x = x \land \text{pos}(y,b)$</td>
<td>$x = x \land \text{pos}(y,b)$</td>
<td>manual</td>
<td>0.04s</td>
<td>0.05s</td>
<td>0.08s</td>
<td>0.12s</td>
</tr>
<tr>
<td>pos$^1(x,a) \equiv a \neq a \lor \text{ts}(3, y)$</td>
<td>neg$^1(x,a) \equiv a \neq a \lor \text{ts}(3, y)$</td>
<td>solve</td>
<td>0.03s</td>
<td>0.12s</td>
<td>0.23s</td>
<td>0.46s</td>
</tr>
<tr>
<td>$x = x \land \text{pos}(y,b)$</td>
<td>$x = x \land \text{pos}(y,b)$</td>
<td>manual</td>
<td>0.05s</td>
<td>0.08s</td>
<td>0.08s</td>
<td>0.12s</td>
</tr>
<tr>
<td>pos$^2(x,a) \equiv \text{ts}(3, y)$</td>
<td>neg$^2(x,a) \equiv \text{ts}(3, y)$</td>
<td>solve</td>
<td>0.04s</td>
<td>0.13s</td>
<td>0.28s</td>
<td>0.48s</td>
</tr>
<tr>
<td>$x = x \land \text{pos}(y,a)$</td>
<td>$x = x \land \text{pos}(y,a)$</td>
<td>manual</td>
<td>0.02s</td>
<td>0.03s</td>
<td>0.05s</td>
<td>0.09s</td>
</tr>
<tr>
<td>pos$^2(x, a) \equiv a \neq a \lor \text{ts}(3, y)$</td>
<td>neg$^2(x, a) \equiv a \neq a \lor \text{ts}(3, y)$</td>
<td>solve</td>
<td>—</td>
<td>0.08s</td>
<td>0.15s</td>
<td>0.26s</td>
</tr>
<tr>
<td>$x = x \land \neg \text{neg}(y,a)$</td>
<td>$x = x \land \neg \text{neg}(y,a)$</td>
<td>manual</td>
<td>—</td>
<td>0.03s</td>
<td>0.06s</td>
<td>0.09s</td>
</tr>
</tbody>
</table>

| Verification conditions | | | | | | |
| lists$^w$ | wp$^n(\text{disp}, \text{list}^n(w))$ | solve | 0.01s | 0.03s | 0.08s | 0.19s | 1.47s |
| $\exists r. x = r \land x \neq x \lor \text{emp}(y)$ | manual | < 0.01s | 0.01s | 0.02s | 0.05s | 0.26s |
| lists$^w$ | wp$^n(\text{disp}, \text{emp})$ | solve | 0.01s | 0.06s | 0.17s | 0.53s | 7.08s |
| $\exists r. x = r \land x \neq x \lor \text{emp}(y)$ | manual | < 0.01s | 0.02s | 0.08s | 0.14s | 2.26s |
| zlist$^w$ | wp$^n(\text{disp}, \text{zlist}^n(w))$ | solve | 0.04s | 0.05s | 0.09s | 0.19s | 1.25s |
| $\exists r. x = r \land x \neq x \lor \text{emp}(y)$ | manual | < 0.01s | 0.01s | 0.02s | 0.04s | 0.29s |
| zlist$^w$ | wp$^n(\text{disp}, \text{zlist})$ | solve | 0.01s | 0.10s | 0.32s | 0.87s | 11.88s |
| $\exists r. x = r \land x \neq x \lor \text{emp}(y)$ | manual | 0.01s | 0.02s | 0.07s | 0.15s | 2.20s |
| lists$^u \land \text{list}^0(v)$ | wp$^n(\text{rev}, u = \text{nil} \land \text{list}^0(v))$ | solve | 0.38s | 0.06s | 0.11s | 0.16s | 0.56s |
| lists$^u \land \text{list}^0(v)$ | manual | 0.07s | 0.03s | 0.07s | 0.11s | 0.43s |
| lists$^u \land \text{list}^0(v)$ | wp$^n(\text{rev}, u = \text{nil} \land \text{list}^0(v))$ | solve | 0.38s | 0.07s | 0.30s | 68.68s | > 300s |
| lists$^u \land \text{list}^0(v)$ | manual | 0.08s | 0.06s | 0.11s | 0.23s | 1.79s |
| lists$^u \land \text{list}^0(v)$ | wp$^n(\text{rev}, u = \text{nil} \land \text{list}^0(v))$ | solve | 0.22s | 0.07s | 0.15s | 0.21s | 0.75s |
| lists$^u \land \text{list}^0(v)$ | manual | 0.04s | 0.02s | 0.04s | 0.06s | 0.31s |
| lists$^u \land \text{list}^0(v)$ | wp$^n(\text{rev}, u = \text{nil} \land \text{list}^0(v))$ | solve | 0.23s | 0.09s | 0.17s | 0.30s | 2.06s |
| lists$^u \land \text{list}^0(v)$ | manual | 0.04s | 0.02s | 0.05s | 0.09s | 0.48s |

Table 1. Experimental results
6 Conclusions and Future Work

We present theoretical and practical results for the existence of effective decision procedures for the fragment of Separation Logic obtained by restriction of formulae to quantifier prefixes in the set $\exists^*\forall^*$. The theoretical results range from undecidability, when the set of memory locations is taken to be the set of integers and linear arithmetic constraints are allowed, to PSPACE-completeness, when locations and data in the cells belong to an uninterpreted sort, equipped with equality only. We have implemented a decision procedure for the latter case in the CVC4 SMT solver, using an effective counterexample-driven instantiation of the universal quantifiers. The procedure is shown to be sound, complete and termination is guaranteed when the input belongs to a decidable fragment of SL.

As future work, we aim at refining the decidability chart for $\exists^*\forall^*SL(T)_{\text{Loc,Data}}$ by considering the case where the locations are interpreted as integers, with weaker arithmetics, such as sets of difference bounds, or octagonal constraints. These results are likely to extend the application range of our tool, to e.g. solvers working on SL with inductive definitions and data constraints. The current implementation should also benefit from improvements of the underlying quantifier-free SL and set theory solvers.

References