Tractability of Separation Logic with Inductive Definitions: Beyond Lists

Taolue Chen, Fu Song, and Zhilin Wu

1 Department of Computer Science and Information Systems, Birkbeck, University of London, UK
2 School of Information Science and Technology, ShanghaiTech University, China
3 State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, China
4 State Key Laboratory of Novel Software Technology, Nanjing University, China

Abstract

In 2011, Cook et al. showed that the satisfiability and entailment can be checked in polynomial time for a fragment of separation logic that allows for reasoning about programs with pointers and linked lists. In this paper, we investigate whether the tractability results can be extended to more expressive fragments of separation logic that allow defining data structures beyond linked lists. To this end, we introduce separation logic with a simply-nonlinear compositional inductive predicate where source, destination, and static parameters are identified explicitly (SLID\textsubscript{SNC}). We show that if the inductive predicate has more than one source (destination) parameter, the satisfiability problem for SLID\textsubscript{SNC} becomes intractable in general. This is exemplified by an inductive predicate for doubly linked list segments. By contrast, if the inductive predicate has only one source (destination) parameter, the satisfiability and entailment problems for SLID\textsubscript{SNC} are tractable. In particular, the tractability results hold for inductive predicates that define list segments with tail pointers and trees with one hole.

1998 ACM Subject Classification F.4.1 Mathematical Logic

Keywords and phrases Separation logic, Inductive definitions, Satisfiability, Entailment

Digital Object Identifier 10.4230/LIPIcs.CONCUR.2017.33

Introduction

Separation Logic (SL, \cite{23, 25}), an extension of Hoare logic, is a well-established formalism for the verification of heap manipulating programs. SL features a separating conjunction operator and inductive predicates, which allow to express how data structures are laid out in memory in a succinct way. Since its introduction, various verification tools based on separation logic have been developed. A notable one among them is the INF\textsc{er} tool \cite{9}, which was acquired by Facebook in 2013 and has been actively used in its development process \cite{10}. To enable program verification with SL assertions in a Hoare-logic style, it is vital to be able to check satisfiability and entailment of SL formulae. Unfortunately, entailment checking in full SL is undecidable \cite{11}. Thus one has to either resort to heuristics or consider restricted, decidable fragments. We focus on the latter approach in this paper. Earlier efforts, including the theoretical work \cite{2}, which leads to the tool SMALL\textsc{foot} \cite{3}, considered SL with primitives of pointers and the hardwired singly linked list segments. A remarkable result on this fragment was given by Cook et al. \cite{14}, who developed a polynomial-time algorithm for...
the satisfiability and entailment problems based on graph reasoning. This has also led to the tool SeLoger [19].

Hardwired inductive predicates have obvious limitations. More recent research has been focusing on automated reasoning about generic user-defined inductive predicates inside the framework of SL. This class of logic is usually referred to as Separation Logic with Inductive Definitions (SLID). Because of their generality, satisfiability and entailment checking are usually much more difficult. Nevertheless, notable progress has been made in this direction. For instance, Iosif et al. showed decidability of satisfiability and entailment for an expressive fragment of SLID by a reduction to Monadic Second Order Logic on graphs with bounded tree width [20]. Later on, they reduced the entailment problem to the language inclusion problem of tree automata, and implemented the tool SLIDE [21]. Brotherston et al. showed that the satisfiability problem (but not entailment) for a very expressive fragment of SLID is ExpTime-complete [6]. In the same paper, they also proved that the satisfiability problem becomes Np-complete if the arities of all predicates are bounded by a constant.

Contributions. We are mostly interested in tractable (polynomial-time) satisfiability and entailment checking for SLID. Our strategy is to generalise the graph reasoning initiated in [14], which currently is limited to singly linked lists only. To this end, we concentrate on a class of simply-nonlinear compositional inductive predicates, where the source, destination, and static parameters are identified explicitly. This class of inductive predicates enjoys some nice compositional properties introduced in [17], which makes, for example, the entailment problem easier to solve. The main question is whether the satisfiability and entailment checking for the resulting SLID fragment, denoted by SLID_{SNC}, can be done in polynomial time. We obtain both positive and negative results in this regard.

(1) We show that, with an inductive predicate dllseg for doubly linked list segments, the satisfiability problem for SLID_{SNC}[dllseg] is Np-complete. From the perspective of data structures, doubly linked list segments are perhaps the minimal extension of singly linked list segments, and thus one would have expected the tractability result for doubly linked list segments by a straightforward adaptation of the method for singly linked list segments by Cook et al. in [14]. Our result is among the strongest intractability results for the satisfiability problem for SLID so far. Note that the Np-hardness reduction in [6] requires four predicates, while our reduction uses only one predicate dllseg. However, it should be noted that there are at most three parameters for predicates in [6], but dllseg has four parameters (i.e., two source and destination parameters respectively). The result suggests that SLID_{SNC} becomes intractable in general if inductive predicates with more than one source (destination) parameter are allowed.

(2) We show that both the satisfiability and the entailment checking can be done in polynomial time if the inductive predicate has only one source (destination) parameter. Remarkably, the fragment covers linear data structures (e.g., list segments with tail pointers), as well as non-linear data structures (e.g., trees with one hole). To our best knowledge, this is one of the first tractability results of SLID for a class of user-defined inductive predicates. (Independently, [8] studied a different class mostly on the model checking problem; cf. related work for comparison.)

To achieve this, we generalise the graph-theoretic techniques developed in [14], in particular, the concept of graph homomorphisms, to non-linear structures. Compared to [14], the graph representations of the SLID_{SNC} formulae have a considerably more involved structure, e.g., the unique simple path property between a pair of nodes in [14] is lost here. An additional intricacy is that we consider the classical semantics of SLID_{SNC} formulae rather than the (less general) intuitionistic semantics in [14]. The authors of [14] did briefly mention
that, to tackle the classical semantics, extra conditions—although not specified—should be added to ensure that all arcs are covered in the graph homomorphism. They, however, suggested that “the details are messy and deferred to a full version.” We concur with these insights. As singly linked list segments are a (very) special case of our inductive predicates, the decision procedure in this paper provides a complete account for the entailment checking under the classical semantics.

Related work. There is a vast literature on separation logic, and we will have to focus on work which is the most relevant to us. In particular, we only cover the work on SLID, and skip many results on, for instance, first-order separation logic (without inductive definitions) [4, 15]. Antonopoulos et al. established some fundamental decidability and complexity results for the entailment problem of SLID [1]. In particular, they showed that deciding the entailment \( \varphi \models \psi \) for SLID is intractable where \( \psi \) may contain existentially quantified variables, even for a single predicate of list segments. This result is largely incomparable to us, since existential quantified variables are disallowed in our setting. The work [5, 13] took the cyclic-proof approach which is based on induction on the paths of proof trees, but the decision procedures therein are incomplete in general. Brotherston et al. investigated array separation logic and obtained some complexity results [7]: They showed that the satisfiability is \( \text{Np} \)-complete, entailment is decidable with high complexity, and bi-abduction is in \( \text{Np} \). Recently, [8] gave another tractable fragment of SLID, but mostly focused on the model checking problem. The tractable fragment of [8], defined by three constraints MEM (“Memory-consuming”), CV (“Constructively valued”) and DET (“Deterministic”), is incomparable to ours: “trees with one hole” is in our tractable fragment, while it does not belong to MEM+CV+DET, as the DET constraint fails; however, an MEM+CV+DET formula may contain several different inductive predicates, while an SLID\textsubscript{SNC} formula allows at most one inductive predicate. We also mention recent work considering decision procedures for SLID extended with data and size constraints [12, 18, 26, 22, 24, 27].

In the sequel, we discuss [18] and [16] which are technically more related to this paper. Strictly speaking, [18] considered SLID extended with data constraints, so here we limit the comparison to the data-free part. First of all, [18] tackled linear structures, while here we focus on more general non-linear structures (e.g., trees). More importantly, the decision procedures in [18] are intractable, even when specialised to the data-free setting. Indeed, for both satisfiability and entailment, only \( \text{Np} \) upper-bounds can be obtained. The current work improves [18] by giving polynomial-time algorithms for even non-linear structures. In particular, for satisfiability, we extend the graph-theoretic approach in [14]; for entailment, we give a new definition of graph homomorphism, which is much more involved than that in [18], but yields an efficient checking algorithm.

[16] considered a fragment of SLID where nested lists and skip lists are expressible, and provided an incomplete decision procedure for the entailment problem by generalising the graph homomorphism in [14]. A more technical comparison is deferred to Section 4.2.

2 Preliminaries

For \( n \in \mathbb{N} \), \( [n] := \{1, \ldots, n\} \). We assume a set of variables \( \text{Vars} \) ranged over by \( E, F, X, Y, \cdots \), and a set of locations \( \text{L} \) typically ranged over by \( l, l', \cdots \). We assume a designated variable \( \text{nil} \in \text{Vars} \) (for the “null” value of pointers in programs) and \( \text{L} \) contains a special element \( \text{null} \). Moreover, we assume a set of fields \( \mathcal{F} \) ranged over by \( f, f', \cdots \). We focus on separation logic with a simply-nonlinear compositional inductive predicate (denoted by SLID\textsubscript{SNC}\([P]\)):

\[
\Pi ::\ E = F \mid E \neq F \mid \Pi \land \Pi,
\Sigma ::\ \text{emp} \mid E \leftrightarrow \rho \mid P(E, E'; F, F', B) \mid \Sigma \ast \Sigma,
\]

CONCUR 2017
where $\rho$ is a tuple of elements from $\mathcal{F} \times \text{Vars}$, and $P(E, E'; F, F'; B)$ is a simply-nonlinear compositional predicate whose definition will be specified shortly.

The formulae $\Pi$ and $\Sigma$ are called the pure and spatial formulae respectively. Atomic formulae of the form $E \rightarrow \rho$ and $P(E, E'; F, F'; B)$ are called the points-to and predicate atoms respectively. For an SLID$_\text{SNC}[P]$ formula $\varphi$, we use $\text{Vars}(\varphi)$ to denote the set of variables occurring in $\varphi$, in addition, we use $\text{Atoms}(\varphi)$ to denote the set of points-to or predicate atoms occurring in $\varphi$. We require that the predicate $P$ in SLID$_\text{SNC}[P]$ is simply-nonlinear compositional, that is, of the following form:

1. The parameters of $P$ are divided into three categories: the source parameters $E, E'$, the destination parameters $F, F'$, and the static parameters $B$. (Note that $E', F', B$ denote a vector of variables.) We require that the source and the destination parameters are symmetric, in particular, they must be of the same length. A predicate $P$ is usually denoted by $P(E, E'; F, F'; B)$ to highlight the parameters.

2. $P(E, E'; F, F'; B)$ is defined by a set of rules including:
   - base rule: $P(E, E'; F, F'; B) ::= E = F \land E' = F' \land \text{emp}$,
   - inductive rule:
     \[
     P(E, E'; F, F'; B) ::= \exists X. \ E \rightarrow [(f_1, Y_1), \ldots, (f_k, Y_k)] * \\
     P(X_{010}, X_{11}'; F, F'; B) * P(X_{11}, X_{12}'; \text{null}, \text{null}; B) * \cdots * P(X_{1l}, X_{1l+1}'; \text{null}, \text{null}; B),
     \]
     such that
     - $X_0, \ldots, X_l$ are mutually distinct variables and $X = \{X_0, \ldots, X_l\}$,
     - $Y_1, \ldots, Y_k \in E' \cup B \cup X \cup \text{nil}$ and each variable from $E' \cup B \cup X$ occurs exactly once in $E \rightarrow [(f_1, Y_1), \ldots, (f_k, Y_k)]$,
     - for each $i : 0 \leq i \leq l$, $X_{i+1}' \subseteq \{E\} \cup X$.

Note that above, in $Y_1, \ldots, Y_k \in E' \cup B \cup X \cup \text{nil}$ or $X_{i+1}' \subseteq \{E\} \cup X$, $E'$ should be interpreted as the set of variables occurring in $E'$, similarly for $B, X, X_i'$. We assume that, if there are multiple inductive rules, the same set of fields $\text{Fds}(P)$ is used. In addition, we define the set $\text{PFds}(P)$ of principal fields, as the set of fields $f \in \text{Fds}(P)$ such that there is an inductive rule of $P$ where $(f, Z)$ occurs for some $Z \in X$, and the set $\text{AFds}(P)$ of auxiliary fields, as the set of fields $f \in \text{Fds}(P)$ such that there is an inductive rule of $P$ where $(f, Z')$ occurs for some $Z' \in E' \cup B \cup \{\text{nil}\}$. We assume that $\text{PFds}(P) \cap \text{AFds}(P) = \emptyset$, which implies that $\text{Fds}(P) = \text{PFds}(P) \cup \text{AFds}(P)$.

In the base or inductive rule, the formula on the left (resp. right) of $::=$ is called the head (resp. body) of the rule. For each predicate $P(E, E'; F, F'; B)$, there is exactly one base rule, and in each inductive rule, each destination parameter from $F, F'$ occurs exactly once in the body of the rule, namely, in $P(X_0, X_{01}; F, F'; B)$. We use $\mathcal{P}$ to denote the set of simply-nonlinear compositional inductive predicates. Moreover, we use $\mathcal{P}_1$ to denote the set of inductive predicates $P(E; F; B) \in \mathcal{P}$, i.e., the set of inductive predicates with a single source resp. destination parameter.

**Semantics.** Each SLID$_\text{SNC}[P]$ formula is interpreted on states. Formally, given a finite set of fields $\mathcal{F} \subseteq \mathcal{F}$, a state is a pair $(s, h)$, where
- $s$ is a stack which is a partial function $\text{Vars} \rightarrow \mathbb{L}$ such that $\text{dom}(s)$ is finite, $\text{nil} \in \text{dom}(s)$, and $s(\text{nil}) = \text{null}$,
- $h$ is a heap which is a partial function $\mathbb{L} \times \mathcal{F} \rightarrow \mathbb{L}$ such that $\text{dom}(h)$ is finite, $h(\text{null}, f)$ is undefined for each $f \in \mathcal{F}$, and for each $l \in \mathbb{L}$, if $h(l, f)$ is defined for some $f \in \mathcal{F}$, then $h(l, f')$ is defined for each $f' \in \mathcal{F}$.

We use $\text{States}$ to denote the set of states. For a heap $h$, we use $\text{idom}(h)$ to denote the set of locations $l \in \mathbb{L}$ such that $h(l, f)$ is defined for some $f \in \mathcal{F}$. Note that $\text{null} \notin \text{idom}(h)$. We
write $h_1 \not\equiv h_2$ if $\text{Idom}(h_1) \cap \text{Idom}(h_2) = \emptyset$, in which case we write $h_1 \uplus h_2$ for the union of $h_1$ and $h_2$. A heap $h_1$ is called a subheap of $h_2$ if $\text{Idom}(h_1) \subseteq \text{Idom}(h_2)$ and for each $l \in \text{Idom}(h_1)$ and $f \in F$, $h_1(l, f) = h_2(l, f)$.

Let $(s, h) \in \text{States}$ and $\varphi$ be an $\text{SLDS}_{\text{NC}}[P]$ formula. Then the semantics of $\varphi$ is defined as follows,

- $(s, h) \models E = F$ (resp. $(s, h) \models E \neq F$) if $s(E) = s(F)$ (resp. $s(E) \neq s(F)$),
- $(s, h) \models \Pi_1 \wedge \Pi_2$ if $(s, h) \models \Pi_1$ and $(s, h) \models \Pi_2$,
- $(s, h) \models \text{emp}$ if $\text{Idom}(h) = \emptyset$,
- $(s, h) \models E \Rightarrow [(f_1, X_1), \ldots, (f_k, X_k)]$ if $\text{Idom}(h) = s(E)$, and for each $i : 1 \leq i \leq k$, $h(s(E), f_i) = s(X_i)$,
- $(s, h) \models P(E, E', F, F', B)$ if $(s, h) \in [[P(E, E', F, F', B)]]$,
- $(s, h) \models \Sigma_1 \ast \Sigma_2$ if there are $h_1, h_2$ such that $h = h_1 \uplus h_2$, $(s, h_1) \models \Sigma_1$ and $(s, h_2) \models \Sigma_2$,

where the semantics of predicate $[P(E, E', F, F', B)]$ is given by the least fixpoint of a monotone operator constructed from the body of rules for $P$. More concretely, assume that $P$ contains $m$ inductive rules, each of which is denoted by $R_i$ and is of the form $R_i : P(E, E', F, F', B) := \Theta_i$ (i.e., $\Theta_i$ is the body of $R_i$). For each $R_i$ (where $i \in [m]$), we define a monotone operator $\tau_i : \Sigma^{\text{states}} \rightarrow \Sigma^{\text{states}}$ as follows: $\tau_i(S) := \{(s, h) \mid (s, h) \models P, S \Theta_i\}$, where $\models_{P, S}$ is the satisfaction relation defined above, except that $P$ is interpreted by $S$, that is, $(s, h) \models P(E, E', F, F', B)$ if $(s, h) \in S$. We finally define $[[P]] := \mu S. \bigcup \tau_i(S)$.

- **Example 1.** We use predicates $\text{lseg, dllseg, tlseg}$, and $\text{th}$ to exemplify our definitions, which represent list segments, doubly linked list segments, list segments with tail pointers, and binary trees with one hole, respectively.

\[
\begin{align*}
\text{lseg}(E; F) & ::= E = F \land \text{emp}, \\
\text{lseg}(E; F) & ::= \exists X. E \leftrightarrow (\text{next}(X), E) \ast \text{lseg}(X, F), \\
\text{dllseg}(E, P; F, L) & ::= E = F \land P = L \land \text{emp}, \\
\text{dllseg}(E, P; F, L) & ::= \exists X. E \leftrightarrow ([\text{next}(X), (\text{prev}, P)] \ast \text{dllseg}(X, E; F, L)), \\
\text{tlseg}(E; F; B) & ::= E = F \land \text{emp}, \\
\text{tlseg}(E; F; B) & ::= \exists X. E \leftrightarrow ([\text{next}(X), (\text{tail}, B)] \ast \text{tlseg}(X; F; B)), \\
\text{th}(E; F) & ::= E = F \land \text{emp}, \\
\text{th}(E; F) & ::= \exists X, Y. E \leftrightarrow ([\text{left}, X], [\text{right}, Y]) \ast \text{th}(X; \text{nil}) \ast \text{th}(Y; F), \\
\text{th}(E; F) & ::= \exists X, Y. E \leftrightarrow ([\text{left}, X], [\text{right}, Y]) \ast \text{th}(X; F) \ast \text{th}(Y; \text{nil}).
\end{align*}
\]

For $P \in P$, we investigate the following two decision problems:

- **Satisfiability.** Given an $\text{SLDS}_{\text{NC}}[P]$ formula $\varphi$, decide whether there is a state $(s, h) \models \varphi$.
- **Entailment.** Given two $\text{SLDS}_{\text{NC}}[P]$ formulae $\varphi$ and $\psi$ with $\text{Vars}(\varphi) \subseteq \text{Vars}(\psi)$, decide whether $\varphi \models \psi$, i.e., for every state $(s, h)$, $(s, h) \models \varphi$ implies $(s, h) \models \psi$.

The inductive predicates defined above fall into the category of compositional inductive predicates [17] and admit the composition lemma, i.e., $P(E_1; E'_1; E_2; E'_2; B) \ast P(E_2; E'_2; E_3; E'_3; B) \models P(E_1; E'_1; E_2; E'_2; E_3; E'_3; B)$ holds, which is crucial for the decision procedure of entailment.

In literature, there is usually a distinction of the classical semantics and the intuitionistic semantics. The aforementioned semantics for $\text{SLDS}_{\text{NC}}[P]$ formulae are called the classical semantics. In the intuitionistic semantics, pure and spatial formulae are interpreted in the same way as the classical one. The only difference is, in the intuitionistic semantics, we have, for an $\text{SLDS}_{\text{NC}}[P]$ formula $\varphi = \Pi \land \Sigma$, $(s, h) \models \varphi$ iff there is a subheap $h_1$ of $h$, $(s, h_1) \models \Pi$ and $(s, h_1) \models \Sigma$. Henceforth, when necessary, we write $\models_c$ to denote the satisfiability relation under the classical semantics, and accordingly, $\models_i$ to denote the satisfiability relation under the intuitionistic semantics. The two semantics are equivalent for the satisfiability problem, but differ in the entailment problem. For instance, $\text{lseg}(E_1; E_2) \ast \text{lseg}(E_2; E_3) \models_c \text{lseg}(E_1; E_2)$ does not hold, while $\text{lseg}(E_1; E_2) \ast \text{lseg}(E_2; E_3) \models_i \text{lseg}(E_1; E_2)$ does hold.
Graph-theoretic notions. We shall work extensively upon an arc-labeled directed graph equipped with a symmetry relation. Here we collect some notations on this matter. For simplicity, we ignore the arc-labels and symmetric relations here, since they are irrelevant right now. In general, a directed graph in $G$ is a pair $(N, \mathcal{E})$, where $N$ is a finite set of nodes, $\mathcal{E} \subseteq N \times N$ is a set of directed arcs. For an arc $e = (v, w) \in \mathcal{E}$, $v$ and $w$ are called the source and destination node of $e$ and sometimes $w$ is called a successor of $v$ and $v$ is called a predecessor of $w$.

A path in $G$ is a sequence of consecutive directed arcs in $G$. A node $w$ is reachable from $v$ if there is a path from $v$ to $w$ (note that $v$ is reachable from $v$ itself). In this case, we also say that $v$ is an ancestor of $w$. A cycle is a path where the starting node and the ending node are equal. A path is simple if no nodes occur twice on the path. A cycle is simple if all nodes are distinct, except the ending node. For a node $v$ and a directed arc $e = (v', w')$, $v$ is said to be reachable from $v'$ if there is a path from $v'$ to $v$ and, and is said to be co-reachable from $v'$ if $v$ is reachable from $v'$. We use $R_G(v)$ to denote the set of arcs that are reachable from $v$.

For a graph $G$, let $N(G)$ denote the set of nodes in $G$. For a set of arcs $\mathcal{E}' \subseteq \mathcal{E}$, let $N(\mathcal{E}')$ denote the set of all source or destination nodes of arcs in $\mathcal{E}'$. For $N' \subseteq N$, the subgraph of $G$ induced by $N'$, denoted by $G[N']$, is $(N', \mathcal{E} \cap (N' \times N'))$. On the other hand, for $\mathcal{E}' \subseteq \mathcal{E}$, the subgraph of $G$ induced by $\mathcal{E}'$, denoted by $G[\mathcal{E}']$, is $(N(\mathcal{E}'), \mathcal{E}')$.

A connected component (CC) $C$ (resp. strongly connected component, SCC, $S$) of $G$ is said to be nontrivial if $C$ (resp. $S$) contains at least one arc.

3 Intractability: Doubly linked list segments

Let $\varphi = \Pi \land \Sigma$ be an $\text{SLID}_{\text{SNC}}[\text{dllseg}]$ formula, where $\text{dllseg}$ is given in Example 1. We shall show the intractability of deciding the satisfiability of $\text{SLID}_{\text{SNC}}[\text{dllseg}]$ formulae. The intractability is proved by a reduction from 3SAT. It turns out that the reduction works even for a restricted class of $\text{SLID}_{\text{SNC}}[\text{dllseg}]$ formulae $\Pi \land \Sigma$ where $\Pi$ only contains inequalities and $\Sigma$ only contains predicate atoms. To ease the presentation of the reduction, we will introduce a graphical representation for this restricted class of $\text{SLID}_{\text{SNC}}[\text{dllseg}]$ formulae. For an $\text{SLID}_{\text{SNC}}[\text{dllseg}]$ formula $\varphi$, recall that $\text{Vars}(\varphi)$ and $\text{Atoms}(\varphi)$ denote the set of variables and atoms in $\varphi$. We construct a graph $G_\varphi = (N, A, \mathcal{L}, R_\varphi)$ as follows.

- $N = \text{Vars}(\varphi)$ and $A = \text{Atoms}(\varphi)$.
- $\mathcal{E} \subseteq N \times A \times N$ is the set of arcs and $\mathcal{L}$ is the arc-labeling function, defined as: for each predicate atom $a = \text{dllseg}(E, F; L)$ in $\text{Atoms}(\varphi)$, there are two arcs $e = (E, a, F) \in \mathcal{E}$ and $e' = (L, a, F)$ with $\mathcal{L}(e) = (a, +)$ and $\mathcal{L}(e') = (a, -)$ respectively.
- $R_\varphi = \{(E, F), (F, E) \mid \Pi \models E \neq F\}$.

For convenience, we usually write $E \xrightarrow{\ell} F$ for an arc $(E, F)$ labeled by $\ell$. Clearly, $\mathcal{E}$ satisfies that, for each predicate atom $a$, there are exactly two arcs in $G_\varphi$ labeled by $(a, +)$ and $(a, -)$ respectively. We usually say that these two arcs are dual and have the opposite poles. All graphs for restricted $\text{SLID}_{\text{SNC}}[\text{dllseg}]$ formulae defined as above form a class of (restricted) $\text{SLID}_{\text{SNC}}[\text{dllseg}]$ graphs. From each restricted $\text{SLID}_{\text{SNC}}[\text{dllseg}]$ graph $G_\varphi = (N, A, \mathcal{L}, R_\varphi)$, we can recover a (restricted) $\text{SLID}_{\text{SNC}}[\text{dllseg}]$ formula $\varphi_G = \Pi_G \land \Sigma_G$, where $\Pi_G = \bigwedge_{(E, F) \in R_\varphi} E \neq F$ and $\Sigma_G = \bigwedge_{a \in A, \ell \in \mathcal{L}(a, F)} \text{dllseg}(E, a, F; L)$. Since $\text{SLID}_{\text{SNC}}[\text{dllseg}]$ formulae and $\text{SLID}_{\text{SNC}}[\text{dllseg}]$ graphs can be easily transformed to each other, we will use them interchangeably.

We are ready to present the reduction from the 3SAT Problem. Let $\Psi$ be a CNF formula with clauses $C_1, \ldots, C_m$ over a set of variables $\{x_1, \ldots, x_n\}$. For each $j \in [m]$, $C_j$ is a disjunction of at most three literals, that is, $C_j = l_{j,1}$, or $C_j = l_{j,1} \lor l_{j,2}$, or
$C_j = l_{j,1} \lor l_{j,2} \lor l_{j,3}$, where for each $k = 1, 2, 3$, $l_{j,k} = x_i$ or $\neg x_i$ for some $i \in [n]$. Without loss of generality, we assume that for each $i \in [n]$ and $j \in [m]$, $x_i$ occurs at most once in $C_j$.

We introduce a set of atoms $A_\varphi = \{x_{i,j} \mid x_i \text{ occurs in } C_j\}$. Furthermore, for each $j \in [m]$, each literal $l_{j,k}$ in $C_j$ ($k \in \{1,2,3\}$) is associated with an atom $x_{i,j}$ defined as follows: if $l_{j,k} = x_i$, then $x_{i,j} = \overline{x}_{i,j}$; otherwise, $x_{i,j} = \overline{x}_{i,j}$.

We then construct $\text{SLID}_{\text{SNC}}[\text{dllseg}]$-graphs for variables and clauses respectively.

- For each variable $x_i$, assume that $x_i$ appears in $C_{j_1}, C_{j_2}, \ldots, C_{j_{n_i}}$ (where $1 \leq j_1 < \cdots < j_{n_i} \leq m$), we have the following arcs: (1) $E_i \xrightarrow{(f_{i,j_1,+})} X_1^i, E_i \xrightarrow{(f_{i,j_1,-})} Y_1^i$, and (2) $X_1^i \xrightarrow{(f_{j_2,j_{n_i},+})} X_{i+1}^i, Y_s \xrightarrow{(f_{j_2,j_{n_i},-})} Y_{s+1}$ for $1 \leq s < k_i$. Moreover, for convenience, we write $F_i$ for $X_1^i$ and $F_i'$ for $Y_1^i$. Then we set $(F_i, F_i') \in \mathcal{R}_\varphi$.

- For each clause $C_j$, if $C_j = l_{j,1} \lor l_{j,2} \lor l_{j,3}$, then we have arcs $G_j \xrightarrow{(l_{j,1},-)} H_j$. In addition, we set $(G_j, H_j), (H_j, G_j) \in \mathcal{R}_\varphi$.

Finally, $\mathcal{G}_\varphi$ comprises the collection of $\text{SLID}_{\text{SNC}}[\text{dllseg}]$-graphs for all variables $x_i$ ($i \in [n]$) and all clauses $C_j$ ($j \in [m]$). Roughly speaking, in $\mathcal{G}_\varphi$, the semantics of separating conjunction $\ast$ and the variable inequalities ensure that each Boolean variable is assigned with exactly one value from \{true, false\}. Moreover, the synchronisation of the two arcs with opposite poles, together with variable inequalities, guarantees that the assignment of Boolean variables satisfies all clauses in $\Psi$.

It is easy to see that in $\mathcal{G}_\varphi$, for each pair of atoms $x_{i,j}$ or $\overline{x}_{i,j}$, one of them appears twice, but the other occurs exactly once. To make $\mathcal{G}_\varphi$ a (restricted) $\text{SLID}_{\text{SNC}}[\text{dllseg}]$-graph defined above, we can simply add some additional isolated arcs. For instance, if $(x_{i,j}, +)$ occurs, but no $(x_{i,j}, -)$ in $\mathcal{G}_\varphi$ (because $\neg x_i$, but not $x_i$, occurs in $C_j$), we add an arc $G_j \xrightarrow{(x_{i,j},-)} H_j^s$, where $G_j^s, H_j^s$ are fresh variables.

**Example 2.** The following example illustrates the intuition of the reduction. Suppose $\Psi = (x_1 \lor x_2) \land (\neg x_1 \lor \neg x_2)$ and the graph $\mathcal{G}_\varphi$ is illustrated in Fig. 1, where dashed lines represent $\mathcal{R}_\varphi$. In a model $(s, h)$ of $\mathcal{G}_\varphi$, since $(G_1, H_1) \in \mathcal{R}_\varphi$, at least one of $F_1, F_2, 1$, say, $F_1$, must be assigned with a nonempty subheap. By the semantics of $\ast$, at least one of the two paths from $E_1$ to $F_1$ and from $E_1$ to $F_1'$ must be empty. Since $(F_1, +)$ appears in the path from $E_1$ to $F_1$ and $F_1$, is nonempty, we deduce that the path from $E_1$ to $F_1'$ has to be assigned with an empty subheap. Accordingly, since $(F_1, +)$ occurs in the path from $E_1$ to $F_1'$, the atom $F_1$ is assigned with an empty subheap. In addition, from $G_2 \xrightarrow{(F_2, -)} G_2' \xrightarrow{(F_2, -)} H_2$ and $(G_2, H_2) \in \mathcal{R}_\varphi$, we have that $F_2$ has to be assigned with a nonempty subheap, which, in turn, implies that the path from $E_2$ to $F_2$ is assigned with an empty subheap. Therefore, $G_2$ and $F_2$ are assigned with a nonempty heap and they induce a satisfiable assignment $\theta$ of $\Psi$ with $\theta(x_1) = \text{true}$ and $\theta(x_2) = \text{false}$.

The satisfiability of $\text{SLID}_{\text{SNC}}[\text{dllseg}]$ can be checked easily in NP. Hence, we have:

**Theorem 3.** The satisfiability problem for $\text{SLID}_{\text{SNC}}[\text{dllseg}]$ is NP-complete.
4 Tractability: Beyond list segments

In this section, we show that if \( P \in \mathcal{P}_1 \), then SLID\(_{SNC}\)[\( P \)] is tractable for both satisfiability and entailment. We fix a predicate \( P(E; F; B) \in \mathcal{P}_1 \).

4.1 Satisfiability

For an SLID\(_{SNC}\)[\( P \)] formula \( \varphi \), we construct a graph \( \mathcal{G}_\varphi \) to represent \( \varphi \). Specifically, \( \mathcal{G}_\varphi \) is a tuple \((\text{Vars}(\varphi), \text{Atoms}(\varphi), \mathcal{N}_\varphi, \mathcal{E}_\varphi, \mathcal{L}_\varphi, R_\varphi)\) defined as follows.

\[
\mathcal{N}_\varphi = \{ [E] \mid E \in \text{Vars}(\varphi) \}
\]

\( \mathcal{E}_\varphi \) is the set of arcs, and \( \mathcal{L}_\varphi \) is the arc-labeling function, defined as follows:

- for each points-to atom \( a = E \mapsto [(f_1, F_1), \ldots, (f_k, F_k)] \) in \( \text{Atoms}(\varphi) \) and each \( i \in [k] \) with \( f_i \in \text{PFids}(P) \), \( \mathcal{E}_\varphi \) contains a field-labeled arc \( e = ([E], [F_i]) \) with \( \mathcal{L}_\varphi(e) = (f_i, a) \);
- for each predicate atom \( a = P(E; F; B) \) in \( \text{Atoms}(\varphi) \), \( \mathcal{E}_\varphi \) contains a predicate-labeled arc \( e = ([E], [F]) \) with \( \mathcal{L}_\varphi(e) = (P, a) \);

In both cases, \( a \) is the atom associated with \( e \), denoted by \( \text{atom}(e) \). In some places later on, in order to emphasise that \( e \) is from \( \mathcal{G}_\varphi \), we also use \( \text{atom}_\varphi(e) \) instead of \( \text{atom}(e) \).

\[
\mathcal{E}_\varphi = \{ ([E], [F]), ([F], [E]) \mid \Pi \models E \neq F \}.
\]

As a convention, \( \perp \) represents the graph for an unsatisfiable SLID\(_{SNC}\)[\( P \)] formula.

All graphs for SLID\(_{SNC}\)[\( P \)] formulae defined as above form a class of SLID\(_{SNC}\)[\( P \)] graphs, whose formal definition is omitted here due to the page limit. It is easy to verify that SLID\(_{SNC}\)[\( P \)] formulae and SLID\(_{SNC}\)[\( P \)] graphs are equivalent, namely, they can be transformed into each other. Hence we will use them interchangeably.

Example 4. An SLID\(_{SNC}\)[th]-graph \( \mathcal{G} \) is given in Fig. 2, where each node is just one variable. Labels of the arcs are abbreviated, e.g., the label \( (\text{left}, E_1 \mapsto [(\text{left}, E_2), (\text{right}, E_3)]) \) of the arc \( (E_1, E_2) \) is abbreviated as \( \text{left} \).

Figure 2 An example of SLID\(_{SNC}\)[th] graphs

Our decision procedure for satisfiability follows [14] closely. The underpinning idea is, on a high level, to reduce the SLID\(_{SNC}\)[\( P \)] graph by exploiting that the subheaps represented by different spatial atoms must be domain disjoint. The main difference to [14] will be discussed when they appear. We start with some notion of persistent set of arcs, largely from [14]. Intuitively, a set of arcs is persistent if in every model, a nonempty subheap has to be assigned to it.

Definition 5 (Persistent set of arcs [14]). Suppose \( \mathcal{G} = (\mathcal{V}, \mathcal{A}, \mathcal{N}, \mathcal{E}, \mathcal{L}, R_\varphi) \) is an SLID\(_{SNC}\)[\( P \)]-graph and \( \mathcal{E}' \subseteq \mathcal{E} \). Then \( \mathcal{E}' \) is said to be persistent in \( \mathcal{G} \) if either \( \mathcal{E}' \) contains a field-labeled
For each pair of distinct nodes $s, h$, we consider the entailment problem, i.e., to decide whether $\phi, \psi$ are satisfiable,

$$\phi \models \psi \quad \text{(Reduced graphs)}$$

We would like to remark that the arcs $e$ in (C2) and (C3) may be field-labeled arcs. Moreover, we would like to mention the connection of the aforementioned conditions with those in [14, Table 2]: (C2) is adapted from conditions (i)—(iii) therein to deal with nonlinear structures, and (C4) is adapted from condition (iv) therein. On the other hand, (C3) is new to deal with the special variable nil ([14] did not consider nil).

Example 7. The graph $G$ in Fig. 2 is not reduced, because it violates (C2). For the arc $e_1 = (E_2, F_3)$, $R_{g-atom(e_1)}(E_2)$ is persistent; (C3): For the arc $e_2 = (F_{11}, F_{12})$, nil is reachable from $F_{11}$ in $R_{g-atom(e_2)}(F_{11})$; and (C4): There are two arc-disjoint predicate-labeled simple paths from $F_3$ to $F_8$. $G$ can be transformed into a reduced graph, given as $G_r$ in Fig. 3.

As in [14], deciding whether a non-$\perp$ SLID$_{SNC}[P]$ graph $G$ is reduced can be done in polynomial time in the size of $G$. To transform an arbitrary non-$\perp$ SLID$_{SNC}[P]$ graph in to a reduced one, we provide a procedure which checks, for a given input non-$\perp$ SLID$_{SNC}[P]$ graph $G$ if any condition in Def. 6 is violated. If this is the case, the algorithm performs certain operations (e.g., contract arcs, or merge nodes, or mark the graph to be $\perp$ directly) depending on which condition is violated, until $G$ is reduced. Most of these are similar to [14]. However, regarding the new condition (C3), if there is an arc $e$ out of $[E]$ and [nil] is reachable from $[E]$ in $R_{g-atom(e)}([E])$, then we contract the arc $e$ in $G$ if $e$ is predicate-labeled, and mark $G$ to be $\perp$ directly otherwise. The details of the procedure is omitted due to the page limit.

By Def. 6, when the graph $G$ is reduced, there are only two possibilities: either $G = \bot$ implying that the corresponding formula SLID$_{SNC}[P]$ is unsatisfiable, or $G \neq \bot$ in which case one can construct a model out of $G$. The similar result for linked lists is rather straightforward [14]. However, it is a bit more involved in our setting, since we need to construct a nonlinear structure to witness the satisfiability of $G$.

Theorem 9. Suppose $P \in \mathcal{P}_l$. Then the satisfiability for SLID$_{SNC}[P]$ is in polynomial time.

4.2 Entailment

In this section, we consider the entailment problem, i.e., to decide whether $\varphi \models \psi$ for two satisfiable SLID$_{SNC}[P]$ formulae $\varphi, \psi$ such that $\text{Vars}(\psi) \subseteq \text{Vars}(\varphi)$. Our goal is to provide a polynomial time decision procedure for the entailment problem.

By Prop. 8, we assume that $G_\varphi = (\text{Vars}(\varphi), \text{Atoms}(\varphi), N_\varphi, E_\varphi, L_\varphi, R_{\varphi, \varphi})$ and $G_\psi = (\text{Vars}(\psi), \text{Atoms}(\psi), N_\psi, E_\psi, L_\psi, R_{\psi, \psi})$ are reduced. For $E \in \text{Vars}(\varphi)$ (resp. $E \in \text{Vars}(\psi)$),
we use \([E]_\varphi\) (resp. \([E]_\psi\)) to denote the node in \(G_\varphi\) (resp. \(G_\psi\)) that contains \(E\). Moreover, we assume that for each \([E]_\varphi, [F]_\varphi \in N_\varphi\) (resp. \([E]_\psi, [F]_\psi \in N_\psi\), if \(E = F \land \varphi\) (resp. \(E = F \land \psi\)) is unsatisfiable, then \(([E], [F]), ([F], [E]) \in R_{\varphi, \psi}\) (resp. \(([E], [F]), ([F], [E]) \in R_{\psi, \varphi}\)). According to Prop. 8, these (possibly implicit) inequalities can be added to \(G_\varphi\) and \(G_\psi\) in polynomial time. Fig. 3 depicts two graphs \(G_\varphi\) and \(G_\psi\), which will be used as the running example. \((G_\varphi\) is obtained from the graph \(G\) in Example 4.)

\[ \begin{array}{c}
\text{Figure 3} \quad G_\varphi \text{ and } G_\psi: \text{Running example for the entailment problem}
\end{array} \]

The main idea of our decision procedure is to utilise graph representations \(G_\varphi\) and \(G_\psi\), and to extend the concept of graph homomorphisms used in [14] to nonlinear structures and the classical semantics. Let us first briefly recall the decision procedure for the entailment problem in [14]: As mentioned in the introduction, [14] focused on singly linked list segments and the intuitionistic semantics. In [14], the entailment \(\varphi \models_i \psi\) is reduced to the existence of a graph homomorphism from \(G_\psi\) to some subgraph of \(G_\varphi\), that is, a mapping that assigns to each arc \(e\) from \([E]_\psi\) to \([F]_\psi\) of \(G_\psi\) a simple path from \([E]_\varphi\) to \([F]_\varphi\) of \(G_\varphi\). In addition, these simple paths are mutually arc-disjoint. The arcs that belong to these simple paths are called covered, and those that do not are called uncovered. As a result of the intuitionistic semantics, the uncovered arcs of \(G_\varphi\) can be ignored. The fact that the existence of a graph homomorphism from \(G_\psi\) to some subgraph of \(G_\varphi\) can be decided in polynomial time is attributed to the unique simple path property enjoyed by \(G_\varphi\), that is, for each pair of distinct nodes, say \([E]_\varphi\) and \([F]_\varphi\), there is at most one simple path from \([E]_\varphi\) to \([F]_\varphi\). The unique simple path property of \(G_\varphi\) implies that the graph homomorphism from \(G_\psi\) to some subgraph of \(G_\varphi\) is unique if it exists.

To deal with the entailment problem \(\varphi \models_i \psi\) for SLID\(_{\text{SNC}}\)[P] formulae \(\varphi\) and \(\psi\) in this paper, we need to generalise the concept of graph homomorphisms in [14] to nonlinear structures and deal with the classical semantics as follows:

1. Since the structures defined by the predicate atoms in SLID\(_{\text{SNC}}\)[P] are nonlinear in general, a graph homomorphism should map each predicate-labeled arc \(e\) of \(G_\psi\) to a potentially nonlinear subgraph Subgraph\(_e\)(\(G_\varphi\)) of \(G_\varphi\), instead of just a simple path. In addition, for each predicate-labeled arc \(e\) of \(G_\psi\), Subgraph\(_e\)(\(G_\varphi\)) should match atom\(_\psi\)(\(e\)), that is, Subgraph\(_e\)(\(G_\varphi\)) \models_i \text{atom}_\psi(e).\) (Recall that we assume that an SLID\(_{\text{SNC}}\)[P] formula and its graph representation are interchangeable.) Actually, we will choose Subgraph\(_e\)(\(G_\varphi\)) to be the minimum subgraph of \(G_\varphi\) that matches atom\(_\psi\)(\(e\)), in order to guarantee the uniqueness of the graph homomorphism.

2. Because we are considering the classical semantics in this paper, those uncovered arcs of \(G_\varphi\) cannot be simply ignored. We need to guarantee that there is a way to dispatch the
uncovered arcs of $\mathcal{G}_\varphi$ to the predicate-labeled arcs of $\mathcal{G}_\varphi$ so that for each predicate-labeled arc $e$ of $\mathcal{G}_\varphi$, $\text{atom}_\varphi(e)$ is matched by the graph consisting of $\text{Subgraph}_e(\mathcal{G}_\varphi)$ and these uncovered arcs of $\mathcal{G}_\varphi$ which are dispatched to $e$.

Finally, we need to show that checking whether a subgraph of $\mathcal{G}_\varphi$ matches $\text{atom}_\varphi(e)$ for a predicate-labeled arc $e$ of $\mathcal{G}_\varphi$ can be done in polynomial time.

We shall use examples to illustrate the main ideas of our decision procedure and delegate the technical details to the appendix. Let us first demonstrate, for each predicate-labeled arc $e$ of $\mathcal{G}_\varphi$, how we choose the graph $\text{Subgraph}_e(\mathcal{G}_\varphi)$ to be the minimum subgraph of $\mathcal{G}_\varphi$ that matches $\text{atom}_\varphi(e)$. The following example shows that $\mathcal{G}_\varphi$ for an SLID$_\text{SNC}[P]$ formula $\varphi$ does not enjoy the unique simple path property in general.

- **Example 10.** Let us consider the SLID$_\text{SNC}[P]$ formulae $\varphi, \psi$ whose graph representations are illustrated in Fig. 3. The graph $\mathcal{G}_\varphi$ does not satisfy the unique simple path property: there are two arc-disjoint simple paths from $E_0$ to $E_7$ in $\mathcal{G}_\varphi$. Note that the subgraph of $\mathcal{G}_\varphi$ comprising the arcs reachable from $E_0$ does match $\text{th}(E_0; E_7)$. This follows from the fact $E_0 \leadsto ([\text{left}, F_{13}]; ([\text{right}, F_{14}]) \ast \text{th}(F_{13}; E_7) \ast \text{th}(F_{14}; \text{nil}) = \text{th}(E_0; E_7)$ and $F_{14} \leadsto ([\text{left}, E_7]; ([\text{right}, \text{nil}])) \ast E_7 \leadsto ([\text{left}, \text{nil}], ([\text{right}, \text{nil}])) = \text{th}(F_{14}; \text{nil})$.

Although the graph representations of SLID$_\text{SNC}[P]$ formulae do not satisfy the unique simple path property in general, we can still find a way to define $\text{Subgraph}_e(\mathcal{G}_\varphi)$ as the minimum subgraph of $\mathcal{G}_\varphi$ that matches $\text{atom}_\varphi(e)$.

- **Definition 11** (Subgraph$_e(\mathcal{G}_\varphi)$). Given a predicate-labeled arc $e = ([E]_\varphi, [F]_\psi)$ in $\mathcal{G}_\varphi$, Subgraph$_e(\mathcal{G}_\varphi)$ is defined as follows:

  - If $[E]_\varphi = [F]_\psi$, then Subgraph$_e(\mathcal{G}_\varphi)$ is the empty graph.
  
  - Otherwise,

    - if $[F]_\psi = [\text{nil}]_\varphi$, then $\text{Subgraph}_e(\mathcal{G}_\varphi) = \mathcal{G}_\varphi[\mathcal{R}_\varphi([E]_\varphi)]$, that is, the subgraph of $\mathcal{G}_\varphi$ comprising all the arcs reachable from $[E]_\varphi$,

    - if $[F]_\psi \neq [\text{nil}]_\varphi$,

      - if there is a unique simple path from $[E]_\varphi$ to $[F]_\psi$, denoted by $\pi_e$, then $\text{Subgraph}_e(\mathcal{G}_\varphi)$ is the subgraph of $\mathcal{G}_\varphi$ comprising: (1) all the arcs in $\pi_e$, (2) all field-labeled arcs $e' = ([E']_\varphi, [F']_\psi)$ such that $[E']_\varphi \in \mathcal{N}(\pi_e)$ and $[F']_\psi \neq \mathcal{N}(\pi_e)$, and (3) all arcs of $\mathcal{G}_\varphi$ that are reachable from $[F']_\psi$,

      - otherwise, $\text{Subgraph}_e(\mathcal{G}_\varphi) = \mathcal{G}_\varphi[\mathcal{R}_\varphi([E]_\varphi)\ast \mathcal{R}_\varphi([F]_\psi)]$.

- **Example 12.** Let us consider the formulae $\varphi, \psi$ illustrated in Fig. 3. Let $e_1, e_2, e_3$ be the predicate-labeled arcs in $\mathcal{G}_\varphi$, from $E_2$ to $E_4$, $E_3$ to $E_5$, and $E_0$ to $E_7$ respectively. Since $[E_2]_\varphi \neq [E_4]_\varphi$, $[E_3]_\varphi \neq [\text{nil}]_\varphi$, and there is a unique path from $[E_2]_\varphi$ to $[E_4]_\varphi$ according to Definition 11, Subgraph$_{e_1}(\mathcal{G}_\varphi)$ comprises the unique simple path from $[E_2]_\varphi$ to $[E_4]_\varphi$, the arc from $[E_2]_\varphi$ to $[F_2]_\varphi$, and all the arcs reachable from $[F_2]_\varphi$. Similarly, Subgraph$_{e_2}(\mathcal{G}_\varphi)$ comprises the unique simple path from $[E_3]_\varphi$ to $[E_5]_\varphi$ in $\mathcal{G}_\varphi$, which is just the predicate-labeled arc from $[E_3]_\varphi$ to $[E_5]_\varphi$. Since $[E_0]_\varphi \neq [E_2]_\varphi$, $[E_1]_\varphi \neq [\text{nil}]_\varphi$, and there are two distinct simple paths from $[E_0]_\varphi$ to $[E_7]_\varphi$, we have that Subgraph$_{e_3}(\mathcal{G}_\varphi) = \mathcal{G}_\varphi[\mathcal{R}_\varphi([E_0]_\varphi)\ast \mathcal{R}_\varphi([E_7]_\varphi)]$, that is, the subgraph of $\mathcal{G}_\varphi$ comprising all the arcs reachable from $[E_0]_\varphi$.

Example 13 illustrates the difference between the intuitionistic and classical semantics.

- **Example 13.** Let $\varphi = \text{lseg}(E_1; E_2) \ast \text{lseg}(E_2; E_3) \ast \text{lseg}(E_3; E_4) \ast \text{lseg}(E_4; E_5)$, $\psi = \text{lseg}(E_1; E_4)$, and $\mathcal{G}_\varphi$ and $\mathcal{G}_\psi$ are depicted in Fig. 4. (For simplicity, arc label (lseg, lseg(E1; E2)) is abbreviated as lseg, sic passim.) We claim $\varphi \models \psi$. To see this, let $(s, h)$ be the state such that $s(E_1) = 1$, $s(E_2) = 2$, $s(E_3) = s(E_4) = 3$, $h(1, \text{next}) = 2$, $h(2, \text{next}) = 3$, $h(3, \text{next}) = 2$. 

CONCUR 2017
Then \((s, h) \models \varphi\), but \((s, h) \not\models \psi\) under the classical semantics, although the subheap \(h'\) of \(h\) with \(\text{ldom}(h') = \{1, 2\}\) satisfies \(\psi\). This is in contrast to the intuitionistic semantics, under which \(h \models \psi\) follows from \(h' \models \psi\).

Regarding the homomorphism [14], although the unique simple path from \(E_1\) to \(E_4\) in \(G_{\varphi}\) matches \(\text{lseg}(E_1; E_4)\), the arc \((E_3, E_2)\) in \(G_{\psi}\) is uncovered. This is the issue of using graph homomorphism to entailment under the classical semantics, as also pointed out in [14]. On the other hand, let us assume another pair of graphs in Fig. 5. It is not hard to see that the entailment \(\varphi \models \psi\) holds. Interestingly, in this case, all the arcs in the cycle \(E_2 \rightarrow E_3\) in \(G_{\varphi}\) are uncovered.

As suggested in Example 13, to deal with the classical semantics, it is necessary to put some proper constraints on the uncovered arcs of nontrivial SCCs in \(G_{\varphi}\). Let us introduce some additional notations for \(G_{\varphi}\). An arc \(e'\) in \(G_{\varphi}\) is covered if

- either \(e'\) is an arc labeled by \((f, \cdot)\) from \([E]_\varphi\) to \([F]_\varphi\) and there is an arc \(e\) labeled by \((f, \cdot)\) from \([E]_\psi\) to \([F]_\psi\) in \(G_{\psi}\), where \(E, F \in \text{Vars}(\psi)\),
- or \(e'\) belongs to \(\text{Subgraph}_x(G_{\varphi})\) for some predicate-labeled arc \(e\) in \(G_{\psi}\).

A simple cycle \(C\) of \(G_{\varphi}\) is covered if all arcs in \(C\) are covered; \(C\) is uncovered if none of the arcs in \(C\) are covered. A nontrivial SCC \(S\) is said to be final w.r.t. covered arcs if there are no covered arcs that are reachable from the nodes in \(S\), moreover, one of the following holds:

1) there is a covered arc whose destination node belongs to \(S\),
2) there is a predicate-labeled arc \(e\) from \([E]_\psi\) to \([F]_\psi\) in \(G_{\psi}\) such that \([E]_\varphi = [F]_\varphi\) is in \(S\). A collection of simple cycles \(S = \{C_1, \ldots, C_n\}\) is said to be unentangled if \(C_i\) and \(C_j\) \((i \neq j)\) do not share any arc, and share at most one node.

In the sequel, we first analyse the structure of nontrivial SCCs in \(G_{\varphi}\).

> **Proposition 14.** Suppose \(\varphi, \psi\) are two \(\text{SLID}_{\text{SNC}}[P]\) formulae such that \(\varphi \models_{<\varphi} \psi\). Then the nontrivial SCCs of \(G_{\varphi}\) satisfy the following structural constraints.

- If a nontrivial SCC \(S\) of \(G_{\varphi}\) contains only predicate-labeled arcs, then \(S\) comprises a collection of unentangled simple cycles \(\{C_1, \ldots, C_n\}\).

- If a nontrivial SCC \(S\) of \(G_{\varphi}\) contains both an uncovered arc and a field-labeled arc, then \(S\) is final w.r.t. covered arcs and is exactly a simple cycle.

A graph homomorphism from \(G_{\varphi}\) to \(G_{\psi}\) is required to satisfy that each simple cycle \(C\) of \(G_{\varphi}\) is either covered or uncovered. In addition, the uncovered simple cycles of \(G_{\psi}\) should satisfy some additional constraint given below.

> **Definition 15.** Let \(S = \{C_1, \ldots, C_n\}\) be a nontrivial SCC of \(G_{\varphi}\) with unentangled simple cycles, where all \(C_i\)'s are either covered or uncovered, with at least one uncovered \(C_i\).

- An uncovered connected component (UCC) \(C\) of \(S\) is a connected component of the graph obtained from \(S\) by removing all covered simple cycles.

- Suppose \(S\) is not final w.r.t. covered arcs. Then \(S\) is indirectly covered if for each UCC \(C\) of \(S\) and each simple cycle \(C\) in \(C\), and there is an arc \(e = ([E]_\psi, [F]_\psi)\) in \(G_{\psi}\) with \(\text{atom}_\psi(e) = P(E; F; B)\), satisfying one of the following constraints:
Definition 16 (Criteria of coverage of arcs). A graph homomorphism from $G_{\psi}$ to $G_{\varphi}$ is fully covered, if

(I) for each nontrivial SCC $S$ that is not final w.r.t. covered arcs and contains an uncovered arc which implies that $S$ contains predicate-labeled arcs only by Prop. 14), each simple cycle $C$ in $S$ is either covered or uncovered, and each UCC of $S$ is indirectly covered,

(II) for each nontrivial SCC $S$ that is final w.r.t. covered arcs, $S$ is indirectly covered,

(III) each uncovered arc of $G_{\varphi}$ either belongs to some nontrivial SCC or is reachable from a node in some nontrivial SCC that is final w.r.t. covered arcs.

We now collate all the ingredients together and specify the formal definition of the graph homomorphism from $G_{\psi}$ to $G_{\varphi}$.

Definition 17 (Graph homomorphism from $G_{\psi}$ to $G_{\varphi}$). A homomorphism from $G_{\psi}$ to $G_{\varphi}$ is a function $\theta : N_{\psi} \rightarrow N_{\varphi}$ satisfying the following constraints.

- Variable subsumption: For each $E \in \text{Vars}(\psi)$, $[E]_{\psi} \subseteq \theta([E]_{\varphi})$. In particular, we have $E \in \theta([E]_{\psi})$. This implies that $\theta([E]_{\psi})$ has to be $[E]_{\varphi}$, and thus, for convenience, we sometime use $[E]_{\psi}$ to denote $\theta([E]_{\psi})$.

- Field-labeled arc: For each field-labeled arc $e = ([E]_{\psi},[F]_{\psi})$ in $G_{\psi}$ with $L_{\psi}(e) = (f,E \mapsto \rho)$, there is a field-labeled arc $e' = ([E]_{\varphi},[F]_{\varphi})$ in $G_{\varphi}$ with $L_{\varphi}(e') = (f,E' \mapsto \rho')$, and for each $(f',F_1)$ in $\rho$ and $(f',F'_1)$ in $\rho'$, if $\theta([F_1]_{\psi}) = [F'_1]_{\varphi}$.

- Predicate-labeled arc: For each predicate-labeled arc $e = ([E]_{\psi},[F]_{\psi})$ in $G_{\psi}$ with $\text{atom}_{\psi}(e) = P(E;F;B)$ and $[E]_{\psi} \neq [F]_{\psi}$. $\text{Subgraph}_{e}(G_{\psi})$ matches $P(E;F;B)$.

- Inequality: For each $(([E]_{\psi},[F]_{\psi}) \in R_{\neq,\psi}$, $([E]_{\varphi},[F]_{\varphi}) \in R_{\neq,\varphi}$.

- Coverage: $\theta$ is fully covered (cf. Definition 16).

- Separation constraint:
  - For each pair of distinct arcs $e_1,e_2$ in $G_{\psi}$, the two subgraphs $\text{Subgraph}_{e_1}(G_{\psi})$ and $\text{Subgraph}_{e_2}(G_{\psi})$ are arc-disjoint.
  - For every two distinct nontrivial SCCs $S_1,S_2$ of $G_{\varphi}$ that are final w.r.t. covered arcs, the sets of arcs that are reachable from (nodes in) $S_1$ and $S_2$ respectively are disjoint.

Proposition 18. $\varphi \models e$ iff there is a graph homomorphism from $G_{\psi}$ to $G_{\varphi}$.

Example 19. Consider the graphs $G_{\psi},G_{\varphi}$ in Fig. 3. The function $\theta : N_{\psi} \rightarrow N_{\varphi}$ can be defined obviously, for instance $\theta(E_2) = \{E_2,F_4\}$. For the predicate-labeled arc $e = (E_2,E_4)$ in $G_{\psi}$, it is a routine to check that $\text{Subgraph}_{e}(G_{\psi})$ matches $e$. Similarly for the other predicate-labeled arcs in $G_{\varphi}$. In addition, the homomorphism $\theta$ is fully covered. Let $S_1,S_2$ be the uncovered nontrivial SCCs in $G_{\varphi}$, which contain the node $\{F_5,F_7,F_8\}$ and $E_5$ respectively.
Tractability of separation logic with inductive definitions: Beyond lists

$S_1$ is not final w.r.t. covered arcs and contains only one uncovered connected component (i.e., itself). Since $th$ contains no static parameters and the arc from $F_1$ to $\{F_5, F_7, F_8\}$ is covered, according to Definition 15, we know that $S_1$ is indirectly covered. Moreover, $S_2$ is final w.r.t. covered arcs. Because the arc from $E_3$ to $E_5$ is covered and $G_\varphi (R_{G_\varphi} (E_5))$, which comprises all the arcs reachable from $E_5$ in $G_\varphi$, matches $tb(E_5; E_5)$, we deduce that $S_2$ is indirectly covered as well. Finally, it is easy to see that the separation constraint is satisfied. Therefore, $\theta$ is a graph homomorphism, and we conclude that $\varphi \models \psi$.

Finally, in order to show that the existence of a graph homomorphism from $G_\varphi$ to $G_\psi$ can be decided in polynomial time, it remains to show that checking that a subgraph of $G_\varphi$ matches a predicate atom $P(E; F; B)$ can be decided in polynomial time.

**Proposition 20.** Given a subgraph $G$ of $G_\varphi$ and a predicate atom $P(E; F; B)$, one can decide whether $G$ matches $P(E; F; B)$ in polynomial time.

The proof of Prop. 20 relies on the fact that the problem of whether $G$ matches $P(E; F; B)$ can be reduced to checking some structural properties of $G$, which can be done in polynomial time.

Combining Prop. 18 and Prop. 20, we conclude:

**Theorem 21.** Let $P \in \mathcal{P}_1$. The entailment problem for SLID$_{SNC}$[$P$] is in polynomial time.

A detailed comparison with [16].

Our polynomial-time decision procedure for SLID$_{SNC}$[$P$] formulae with $P \in \mathcal{P}_1$ is related to that in [16], since the parameters of an inductive predicate in [16] are also divided as source, destination, and static parameters. Nevertheless, our decision procedure differs from that in [16] in the following three aspects. (1) SLID$_{SNC}$[$P$] formulae with $P \in \mathcal{P}_1$ and the fragment of SL in [16] are incomparable: The latter allows nesting inductive predicates so that nested lists and skip lists can be defined, while our fragment disallows this. On the other hand, SLID$_{SNC}$[$P$] formulae with $P \in \mathcal{P}_1$ allows defining tree structures, which are not supported in [16]. (2) The inequality $E \neq F$ may appear in the inductive rules of predicates in [16], but is excluded here. As a result, the fragment in [16] is precise in the sense that when checking $\varphi \models \psi$, for each arc $e$ in $G_\varphi$, there is a unique subgraph of $G_\varphi$ that matches $atom_\varphi(e)$. On the other hand, SLID$_{SNC}$[$P$] is not precise because of the uncovered simple cycles of $G_\varphi$. Some proper constraints on these uncovered simple cycles are necessary in the graph homomorphism to achieve a complete decision procedure for the entailment problem. (3) In [16], checking whether a subgraph of $G_\varphi$ matches a predicate atom $P(E; F; B)$ is reduced to the membership problem of a tree automaton constructed from the inductive definitions of $P$, which is of exponential size in the worst case, due to the nested inductive predicates. However, in our decision procedure, we simply check whether the subgraph satisfies some structural properties in polynomial time.

5 Conclusion

We have provided polynomial-time satisfiability and entailment checking algorithms for SLID$_{SNC}$ with one source (destination) parameter. We have also shown that the satisfiability problem is generally NP-complete if more than one source (destination) parameter is allowed, particularly for an inductive predicate of doubly linked list segments.

For the future work, we strongly believe that our polynomial-time decision procedures can be further generalised to handle inductive predicates with multiple source (destination) parameters in a constrained form. Moreover, adding data constraints certainly is one of the promising extensions of the current work.
References


