Shape and Content
Incorporating Domain Knowledge into Shape Analysis

D. Calvanese, T. Kotek, M. Šimkus, H. Veith, and F. Zuleger

1 Free University of Bozen-Bolzano
2 Vienna University of Technology

Abstract. The verification community has studied dynamic data structures primarily in a bottom-up way by analyzing pointers and the shapes induced by them. Recent work in fields such as separation logic has made significant progress in extracting shapes from program source code. Many real world programs however manipulate complex data whose structure and content is most naturally described by formalisms from object oriented programming and databases. In this paper, we attempt to bridge the conceptual gap between these two communities. Our approach is based on description logic, a widely used knowledge representation paradigm which gives a logical underpinning for diverse modeling frameworks such as UML and ER. We show how description logic can be used on top of an existing shape analysis to add content descriptions to the shapes. Technically, we assume that we have separation logic shape invariants obtained from a shape analysis tool, and requirements on the program data in terms of description logic. Thus, we obtain a modular description logic based verification methodology which is able to exploit shape information.

1 Introduction

The manipulation and storage of complex information in imperative programming languages is often achieved by dynamic data structures. The verification of programs with dynamic structures however is notoriously difficult, and is a highly active area of current research. This paper aims to put a new perspective on this problem. We discuss how the analysis of the shape can be complemented by an analysis of the content to be stored.

Shape analysis is concerned with the analysis of pointers and of the structures induced by them. Recent years have seen considerable progress in automatic methods for inferring basic shape properties such as lists and trees and variations thereof (cyclic lists, doubly-linked lists, etc.). This success has been enabled by succinct formalisms for representing heap structures, most notably separation logic [25,16]. With a few exceptions e.g. [20,21] the majority of papers on shape analysis has focused on the (graph-theoretic) shape of the data structures rather than their information content. For instance, classical shape analysis does not capture simple concepts such as “a list of students where each student has a list of teachers” but only the more combinatorial concept “list of lists”.
The question of content representation has been studied by other disciplines, in particular databases, modeling and knowledge representation. They typically model reality by classes and binary relationships between these classes. For example, the database community uses entity-relationship (ER) diagrams, UML diagrams have been studied in requirements engineering, and the knowledge representation community uses description logic for various modeling tasks. Importantly, these formalisms address an abstraction layer which is intermediary between the program requirements and the implementation. In particular, they are not intended to specify the shape of the data structures but rather their information content.

Problem Statement. We believe that the verification of complex programs with dynamic data structures needs to combine methods from shape analysis and content representation. Complex software projects typically come with extensive documentation or models which contain a description of data structure content e.g. in UML, ER, diagrams etc. But even in an informal setting, the programmers always have a high-level concept of what they want to achieve with their program, in particular what information has to be represented in the program and how this information is stored in data structures. The goals of verification are often related to the content and its representation, e.g. the verification of complex heap invariants in a file system, the adherence to security policies, etc. Thus, the technical challenge is to find a verification methodology along with a suitable formalism that bridges the gap between shape analysis and content representation.

Our Approach and Methodology. In this paper we explore the use of a description logic as an assertion language for verifying high-level properties of programs on top of a preceding shape analysis. Description Logics (DLs) are a well established and highly popular family of logics for representing knowledge in artificial intelligence [2]. DLs are mature and well understood, they have good algorithmic properties and enjoy efficient reasoners. DLs vary in expressivity and complexity, and are usually selected according to the expressivity needed to formalize the given target domain. Note that DLs can be used as a precise framework for reasoning over UML class diagrams and ER diagrams [6,1]. Moreover, DLs are the logical backbone of the Web Ontology Language (OWL) for the Semantic Web [22]. In this paper we employ a very expressive description logic, based on the so called ALCHOIF, which we specifically tailor to better support reasoning about complex pointer structures.

This paper consists of two parts: In Section 2, we study description logic as a formalism for program invariants, and its relationship to separation logic. In particular, we show that shape invariants in separation logic can be translated into description logic in such a way that the translation is implied by the shape invariant (but possibly weaker than the shape invariant). In Section 3, we describe a program model for sequential imperative programs without procedures, and describe a systematic method for the verification of description logic invariants.

We thus obtain a semi-manual methodology which leverages the results of shape analysis for content analysis. As presented here, our methodology assumes
human guidance, and it is part of future work to automatize the role of the user. The verification method then proceeds in two steps:

1. **Shape Analysis.** We assume that the user has specified a set of program locations $L$ to be annotated in a Hoare-style proof; typically, $L$ is the set of loop headers as well as the beginning and end of the program. The user then annotates the locations $L$ with shape predicates, possibly supported by a shape analysis tool which proves the validity of the shape predicates. We choose a specific separation logic ([8]) for the shape annotations, but our methodology is independent of this choice.

2. **Content Analysis.** The user translates the shape invariants into description logic as discussed above, and annotates the program locations in $L$ with the description logic invariants describing content. The validity of the description logic predicates is then reduced to a DL decision procedure.

Note that our method clearly separates shape analysis from content analysis; throughout this paper, we treat shape analysis as a black box.

1.1 **Running Example: Employees, Projects, Managers**

Our running example will be a simple information system for a company. We start with an informal description of the programmers’ intention. The company has employees working on projects. The employees and projects are stored in two lists, both using the *next* pointer. The heads of the two lists are $\text{projHead}$ and $\text{emplHead}$ respectively. Each employee in the list of employees has a pointer $\text{worksFor}$ to a project on the list of projects, indicating the project that the employee is working on (or to null, in case no project is assigned to that employee). Each project in the list has a pointer $\text{managedBy}$ to the employee list, indicating the manager of the project (or to null, in case the project does not have a manager). Every employee managing a project should also work for that project. Some of the employees are marked as managers via a Boolean field $\text{isManager}$, and only they can manage projects. We will refer to these properties as the *system invariants*.

The programmer has written two program (stated below), which she wants to verify. We will refer to the program on the left by $S_1$ and on the right by $S_2$.

\begin{align*}
    l_b & : \text{proj}.\text{managedBy} := \text{emp}; \\
    & \quad \text{emp}.\text{worksFor} := \text{proj}; \\
    & \quad \text{emp}.\text{isManager} := \text{T}; \\
    l_e & : \text{end}; \\
    l_b & : \text{proj} := \text{new}; \\
    & \quad \text{proj}.\text{next} := \text{projHead}; \\
    & \quad \text{projHead} := \text{proj}; \\
    & \quad \text{e} := \text{emplHead}; \\
    l & : \text{while } \sim (\text{e} = \text{null}) \text{ do} \\
    & \quad \text{if } \{ \text{e}.\text{worksFor} = \text{null} \} \text{ then} \\
    & \quad \quad \text{e}.\text{worksFor} := \text{proj}; \\
    & \quad \quad \text{e} := \text{e}.\text{next}; \\
    & \quad \text{od} \\
    l_e & : \text{end};
\end{align*}
The programmer has the following intuition about her programs: The code $S_1$ assigns the employee $emp$ to manage project $proj$. If $emp$ is not a manager already, $emp$ is promoted. The code $S_2$ adds a new project $proj$ to the project list, and assigns to it all employees in the employee list which are not assigned to any project.

For both pieces of code the programmer wants to verify that the system invariants are true after the execution of the code, if they were true in the beginning (1). Note that during the execution of the code, they might not be true! Additionally the programmer wants to verify that after executing $S_2$ the project list has been extended by $proj$, the employee list still contains the same employees and indeed all employees who did not work for a project before now work for project $proj$ (2). In this paper we will formally prove the correctness of $S_2$ following our verification methodology discussed in the introduction. In Sections 2.4 and Section 2.5 we describe how the description logic $L$ can be used for specifying the verification goals (1) and (2). In Section 3.4 we state verification conditions that allow to conclude the correctness of (1) and (2) for program $S_2$.

2 Description Logic for Invariant Specification

2.1 Structures

We use ordinary first order structures to represent memory in a precise way. A structure (or, interpretation) is a tuple $M = (M, \tau, \cdot)$, where (i) $M$ is an infinite set (the universe), (ii) $\tau$ is a set of constants and relation symbols with an associated non-negative arity, and (iii) $\cdot$ is an interpretation function, which assigns to each constant $c \in \tau$ an element $c^M \in M$, and to each $n$-ary relation symbol $R \in \tau$ an $n$-ary relation $R^M$ over $M$. In this paper, each relation is either unary or binary (i.e. $n \in \{1, 2\}$). Given $A \subseteq M$ and a binary $R^M$, $R^M$ is a (total) function from $A$ if there is exactly one $e'$ with $(e, e') \in R^M$ for every $e \in A$. For such $R^M$, we use $R^M(e)$ to denote $e'$.

2.2 Memory Structures

A Memory structure will describe a snapshot of the heap and the local variables. To this end, we assume a set $\tau_{\text{var}} \subseteq \tau$ of constants and a set $\tau_{\text{fields}} \subseteq \tau$ of binary relation symbols. We will later employ these symbols for variables and fields in programs. A memory structure is a structure $M = (M, \tau, \cdot)$ that satisfies the following conditions:

1. $\tau$ includes the constants $o_{\text{null}}, o_T, o_F$.
2. $\tau$ has the unary relations Addresses, Alloc, MemPool, and Aux.
3. $\text{Aux}^M = \{o_{\text{null}}^M, o_T^M, o_F^M\}$ and $|\text{Aux}^M| = 3$.
4. $\text{Addresses}^M \cap \text{Aux}^M = \emptyset$ and $\text{Addresses}^M \cup \text{Aux}^M = M$.
5. $\text{Alloc}^M \cap \text{MemPool}^M = \emptyset$ and $\text{Alloc}^M \cup \text{MemPool}^M \subseteq \text{Addresses}^M$.
6. $c^M \in M \setminus \text{MemPool}^M$ for every constant $c$ of $\tau$. 

For all $f \in \tau_{\text{fields}}$, $f^M$ is a function from $\text{Addresses}^M$ to $M \setminus \text{MemPool}^M$.

If $e \in \text{MemPool}^M$, then $f^M(e) \in \{\text{null}^M, \text{F}^M\}$.

$R^M \subseteq (M \setminus \text{MemPool}^M)^n$ for every $n$-ary $R \in \tau \setminus (\{\text{MemPool}\} \cup \tau_{\text{fields}})$, $n = 1, 2$.

$\text{Alloc}^M$ and $\text{Addresses}^M \setminus \text{MemPool}^M$ are finite. $\text{MemPool}$ is infinite.

The intuition behind memory structures is as follows. Variables in programs will either have a Boolean value or be pointers. Thus, to represent null and the Boolean values $\text{T}$ and $\text{F}$, we employ the auxiliary relation $\text{Aux}^M$ storing 3 elements corresponding to the 3 values. Clearly, $\text{Addresses}^M$ represents the memory cells. The relation $\text{Alloc}^M$ contains the allocated cells. $\text{MemPool}^M$ contains the cells which are not allocated, do not have any field values other than null and $\text{F}$, are not pointed to by any field, do not participate in any other relation and do not interpret any constant (see (6-9)). The memory cells in $\text{MemPool}$ are the candidates for allocation during the run of a program. $\text{Addresses}^M \setminus \{\text{Alloc}^M \cup \text{MemPool}^M\}$ is the set of memory cells which are not allocated, but are pointed to from cells in $\text{Alloc}^M$. Since the allocated memory should by finite at any point of the execution of a program, $\text{Alloc}^M$ and $\text{Addresses} \setminus (\text{Alloc}^M \cup \text{MemPool}^M)$ are finite (see (10)). However, the available memory $\text{Addresses}^M$ and the memory pool $\text{MemPool}^M$ are infinite. Finally, each cell is seen as a record with exactly the fields $\tau_{\text{fields}}$.

2.3 The Description Logic $\mathcal{L}$

Domain information in description logics is expressed by means of atomic concepts, atomic roles, constants (also known as individuals), and complex formulae built from them. The various constructors available to build formulae determine the particular description logic, giving rise to a wide family of logics with varying expressivity and complexity of reasoning. The semantics to formulae is given in terms of structures, where atomic concepts and atomic roles are interpreted as unary and binary relations in a structure, respectively, and constants are interpreted as elements in the structure’s universe.

Complex formulae can be used to create and interrelate complex concept descriptions. For instance, the (complex) concept $\text{Employee} \sqcap \exists \text{worksFor}. \text{Project}$, where $\text{Employee}$ and $\text{Project}$ are atomic concepts and $\text{worksFor}$ is an atomic role, describes persons who work for some project. We can use the formula $\exists \text{worksFor}. \text{Project} \subseteq \text{Employee}$ to express the requirement that every object working for a project must be an employee. In this paper, we will use complex concepts and formulae to express “lower-level” requirements on the content of data structures in a program. E.g. for a program operating on a list of employees and a list of projects, we may use $\text{EmpList} \sqcap \exists \text{worksFor}. \text{ProjList}$ to refer to elements of the employee list whose value of the $\text{worksFor}$ field appears in the project list.
We next make these intuitions more formal by introducing the following expressive description logic $\mathcal{L}^3$.

**Definition 1 (Syntax of $\mathcal{L}$).** The set of roles and concepts of $\mathcal{L}$ is defined inductively as follows:

- every unary relation symbol is a concept (called atomic concept);
- every constant symbol is a concept (called nominal concept);
- every binary relation symbol is a role (called atomic role);
- if $r$ and $s$ are roles, then $r \cup s$, $r \cap s$, $r \setminus s$ and $r^-$ are also roles;
- if $C$ and $D$ are concepts, then so are $C \cap D$, $C \cup D$, and $\neg C$;
- if $r$ is a role and $C$ is a concept, then $\exists r.C$ is also a concept;
- if $C$ and $D$ are concepts, then $C \times D$ is a role (called product role).

The set of formulae of $\mathcal{L}$ is defined inductively as well.

- The following are formulae:
  - $C \subseteq D$ (concept inclusion), where $C, D$ are concepts;
  - $r \sqsubseteq s$ (role inclusion), where $r, s$ are roles;
  - $\text{func}(r)$ (functionality assertion), where $r$ is a role;
  - if $\varphi$ and $\psi$ are formulae, then $\varphi \land \psi$, and $\neg \psi$ are formulae;
  - If $\varphi$ and $\psi$ are formulae, then $\varphi \land \psi$, and $\neg \psi$ are formulae.

**Definition 2 (Semantics of $\mathcal{L}$).** The semantics to an $\mathcal{L}$-formula $\varphi$ is given in terms of structures $\mathcal{M} = (M, \tau, \cdot)$, where $\tau$ contains all atomic concepts, atomic roles and constants occuring in $\varphi$. The function $\cdot^\mathcal{M}$ is extended to the remaining concepts and roles inductively below. The satisfaction relation $\models$ between structures and formulae is also given in below.

\[
\begin{align*}
(C \cap D)^\mathcal{M} &= C^\mathcal{M} \cap D^\mathcal{M} \\
(C \cup D)^\mathcal{M} &= C^\mathcal{M} \cup D^\mathcal{M} \\
(\neg C)^\mathcal{M} &= M \setminus C^\mathcal{M} \\
(r \sqsubseteq s)^\mathcal{M} &= r^\mathcal{M} \sqsubseteq s^\mathcal{M} \\
(r \sqcap s)^\mathcal{M} &= r^\mathcal{M} \sqcap s^\mathcal{M} \\
(r \setminus s)^\mathcal{M} &= r^\mathcal{M} \setminus s^\mathcal{M} \\
(\neg r)^\mathcal{M} &= \{ (e, e') \mid (e', e) \in r^\mathcal{M} \} \\
(C \times D)^\mathcal{M} &= C^\mathcal{M} \times D^\mathcal{M} \\
(\forall r.C)^\mathcal{M} &= \{ e \mid \exists e' : (e, e') \in r^\mathcal{M} \}
\end{align*}
\]

If $\mathcal{M} \models \varphi$, then $\mathcal{M}$ is a model of $\varphi$. We write $\mathcal{M} \models \varphi$ if every model of $\varphi$ is also a model of $\varphi$.

For the remainder of the paper we will use the following abbreviations:

$\top = C \cup \neg C$, where $C$ is an arbitrary atomic concept and $\bot = \neg \top$; $\alpha \equiv \beta$ for the formula $\alpha \sqsubseteq \beta \land \beta \sqsubseteq \alpha$; $\exists r$ for the concept $\exists r.\top$; $(o, o')$ for the role $o \times o'$; and $\varphi \lor \psi$ and $\varphi \rightarrow \psi$ for formulae $\neg(\neg \varphi \land \neg \psi)$ and $\neg \varphi \lor \psi$, respectively. Note that $\top^\mathcal{M} = M$ and $\bot^\mathcal{M} = \emptyset$ for any structure $\mathcal{M} = (M, \tau, \cdot)$.

---

$^3$ In DL terms, $\mathcal{L}$ corresponds to Boolean $\text{ALCHOIF}$ knowledge bases with the additional support for role intersection, role union, role difference and product roles.
Definition 3 (Satisfiability and implication in memory structures). An \( L \)-formula \( \phi \) is satisfiable in a memory structure if there is a memory structure \( M \) such that \( M | \models \phi \). We write \( \psi | \models_\text{m} \phi \) if \( M | \models \psi \) implies \( M | \models \phi \) for every memory structure \( M \).

The following is an easy consequence of the existing results in the description logic literature.

Theorem 1. Checking whether an \( L \)-formula is satisfiable in a memory structure is NExpTime-complete.

Proof (Sketch). The upper bound can be shown by reducing the problem to finite satisfiability in \( C^2 \), the two-variable fragment of the first-order logic with counting quantifiers [24]. The lower bound comes from the NExpTime-hardness of satisfiability in the DL \( ALCQ \) [27].

Clearly, since \( \psi | \models_\text{m} \phi \) iff \( \psi \land \neg \phi \) is not satisfiable in a memory structure, we get that deciding \( \psi | \models_\text{m} \phi \) for a pair \( \psi, \phi \) of \( L \)-formula is coNExpTime-complete.

In the rest of the paper, we will only be interested in satisfiability and implication of formulae in memory structures. Thus, the term satisfiability will always refer to satisfiability in a memory structure, and we will use \( \models \) instead of \( | \models_\text{m} \).

2.4 Expressing Content Invariants in \( L \)

Here we show how content requirements can be expressed in \( L \). We start with the formulae describing the content and only then move to the shape.

Employees, Projects, Managers We can now make the example from Section 1.1 more precise. The concepts \( \text{EmplList} \) and \( \text{ProjList} \) are interpreted as the sets of elements in the employee list resp. the project list. \( \text{managedBy} \), \( \text{isManager} \) and \( \text{worksFor} \) are roles. \( o_{\text{emplHead}} \) and \( o_{\text{projHead}} \) are the constants which correspond to the heads of the two lists. The invariants of the systems are:

1. The project and employee lists are allocated: \( \text{ProjList} \sqcup \text{EmplList} \sqsubseteq \text{Alloc} \)
2. Projects and employees are distinct: \( \text{ProjList} \sqcap \text{EmplList} \sqsubseteq \bot \)
3. \( \text{worksFor} \) is set to null for projects: \( \text{ProjList} \sqsubseteq \exists \text{worksFor}.o_{\text{null}} \)
4. \( \text{managedBy} \) is set to null for employees: \( \text{EmplList} \sqsubseteq \exists \text{managedBy}.o_{\text{null}} \)
5. \( \text{managedBy} \) of projects in the list point to managers:
   \( \exists \text{managedBy}^- \cdot \text{ProjList} \sqsubseteq \exists \text{isManager}.o_\top \sqcup o_{\text{null}} \)
6. \( \exists \text{worksFor}^- \cdot \text{EmplList} \sqsubseteq \text{ProjList} \sqcap o_{\text{null}} \)
7. \( \exists \text{isManager}^- \cdot \text{EmplList} \sqsubseteq \text{Boolean} \)
8. The manager of a project must work for the project:
   \( \text{worksFor}^- \cap \left( \top \times \text{EmplList} \sqcap \text{isManager}.o_\top \right) \sqsubseteq \text{managedBy} \)
Let the conjunction of the invariants be given by $\varphi_{\text{invariants}}$.

Now consider the code $S_2$ from the introduction. The states of the heap before and after the execution of $S_2$ can be related by the following $\mathcal{L}$ formulae. $\varphi_{\text{lists-updt}}$ and $\varphi_{\text{p-assgn}}$. $\varphi_{\text{lists-updt}}$ states that the employee list at the end of the program ($\text{EmplList}$) is equal to the employee list at the beginning of the program ($\text{EmplList}_\text{gho}$), and that the project list at the end of the program ($\text{ProjList}$) is the same as the project list at the beginning of the program ($\text{ProjList}_\text{gho}$), except that $\text{ProjList}$ also contains the new project $o_{\text{proj}}$. $\text{EmplList}_\text{gho}$ and $\text{worksFor}_\text{gho}$ are ghost relation symbols, whose interpretations hold the corresponding values at the beginning of $S_2$.

$$\varphi_{\text{lists-updt}} = \text{EmplList}_\text{gho} \equiv \text{EmplList} \land \text{ProjList}_\text{gho} \sqcup o_{\text{proj}} \equiv \text{ProjList}$$

$$\varphi_{\text{p-assgn}} = \text{EmplList}_\text{gho} \sqcap \exists \text{worksFor}_\text{gho}. o_{\text{null}} \equiv \text{EmplList} \sqcap \exists \text{worksFor}. o_{\text{proj}}$$

**The Virtual File System** The Virtual File System (VFS)\textsuperscript{4} is comprised of various types of objects, arranged in a large number of lists. A directory entry (dentry) corresponds to a path in the file system. Both files and directories have dentries and the dentries are arranged in a tree which is implemented by lists. Each dentry points to a file. The files are partitioned between lists depending on whether they are used or not. A file may have more than one dentry pointing to it, corresponding to different names of the same file. Other elements of the VFS which we do not discuss further here include file system types and files pointers, which are interrelated with the above mentioned elements and stored in various lists and other data structures.

The concepts containing the elements of the lists and tree are respectively $\text{UsedList}$, $\text{UnusedList}$, and $\text{DTree}$. dentryFile (dentryF for short) is a role corresponding to the field pointing from dentries to files. $\text{FileId}$ is a role corresponding to a field which is considered to be the Id of the file. The tree $\text{DTree}$ is implemented as a binary tree with three roles for the fields $\text{firstChild}$, $\text{nextSibling}$ and $\text{parent}$. Fig. 1 illustrates the VFS. $\text{DTree}$ is represented in the memory as a binary tree with fields $fC = \text{firstChild}$ and $nS = \text{nextSibling}$ (above). We think of it as a tree with unbounded degree (below). $n$ is short for next. Additionally every file in the two lists has a $\text{FileId}$ field. The invariants of system:

1. The allocated memory contains three disjoint sets of elements: $\text{UsedList}$, $\text{UnusedList}$ and $\text{DTree}$:

   - $\text{UsedList} \sqcup \text{UnusedList} \sqcup \text{DTree} \sqsubseteq \text{Alloc}$
   - $\text{UsedList} \cap \text{DTree} \equiv \bot$
   - $\text{UsedList} \cap \text{UnusedList} \equiv \bot$

\textsuperscript{4} We present here a simplified description. The terminology used here is different from the one used in the linux kernel. E.g., files are called inodes and file systems are called superblocks in the terminology of VFS.
2. Null fields: UsedList \sqcup UnusedList \sqsubseteq \exists \text{dentryF}.o_{null} \land DT\text{ree} \sqsubseteq \exists \text{FileId}.o_{null}

3. The root of DT\text{ree} is a directory:
   \begin{align*}
   & DT\text{ree} \sqcap \neg \exists \text{firstChild}.DT\text{ree} \sqcap \neg \text{nextSibling}.DT\text{ree} \sqsubseteq \exists \text{dentryF}.o_{null} \\
   \end{align*}

4. A file belongs to the UsedList if and only if a dentry in DT\text{ree} points to it:
   \exists \text{dentryF}.DT\text{ree} \equiv \text{UsedList}

5. If a dentry in DT\text{ree} points to a file with the pointer dentryFile, then it has no children in DT\text{ree} (otherwise it would necessarily be a directory):
   \begin{align*}
   & DT\text{ree} \sqcap \exists \text{dentryF}.\neg o_{null} \sqsubseteq \exists \neg \text{firstChild} \\
   \end{align*}

6. The FileId is unique with respect to the lists UsedList and UnusedFiles:
   \begin{align*}
   & \text{func(FileId}^- \cap \top \times (\text{UsedList} \sqcup \text{UnusedList})) \\
   \end{align*}

2.5 Translating Shape Invariants into L

Here we discuss how to translate shape invariants from a preceding shape analysis into L. First, we discuss how lists and trees can be dealt with in L. Next, we apply this to a popular separation logic fragment.

Lists and Trees A concept L is a singly linked list from o_{var_1} to o_{var_2} with respect to the field next if it satisfies the following five conditions. Except for (5), the conditions are expressed fully in L to the right:

1. o_{var_1} belongs to L:
   \alpha^1_{ls} = o_{var_1} \subseteq L

2. o_{var_2} is pointed to by an L element:
   \alpha^2_{ls} = o_{var_2} \subseteq \exists \text{next}.L

3. The next of every element in L points to an L or to var_2:
   \begin{align*}
   & \alpha^3_{ls} = L \subseteq \exists \text{next}.\left( L \sqcup o_{var_2} \right) \\
   & \alpha^4_{ls} = L \subseteq \exists \text{next}.L \sqcup o_{var_1} \\
   \end{align*}

4. Every L element is pointed to from an L element, except possibly for var_1:
   \begin{align*}
   & \forall \text{var}_1 \exists \text{next}.\left( L \subseteq \exists o_{var_2} \right) \\
   \end{align*}

5. All of the elements of L are reachable from o_{var_1} via next.

In structures M satisfying \alpha^1_{ls} \land \ldots \land \alpha^4_{ls}, L^M contains a list segment from o_{var_1}^M to o_{var_2}^M, but additionally L^M may contain disjoint cycles with respect to next. Due to the lack of means to express transitive closure, we only express (5) for lists of length at most m, where m is a parameter. Let

\begin{align*}
\alpha^5_{ls,m} = D \equiv & \exists \left( o_{var_1} \sqcup o_{var_2} \right) \sqcup \exists \text{next} \sqcup \ldots \sqcup \exists \left( o_{var_1} \sqcup o_{var_1} \right) \sqcup \exists \text{next}. \sqcup o_{var_1} \\
& \land ( o_{var_2} \subseteq D \rightarrow L \subseteq D )
\end{align*}

where \alpha^5_{ls,m} contains m repetitions of \exists \left( o_{var_1} \sqcup o_{var_2} \right) \sqcup \exists \text{next} \sqcup \ldots \sqcup \exists \left( o_{var_1} \sqcup o_{var_1} \right) \sqcup \exists \text{next}. \sqcup o_{var_1}. D is a new atomic concept, which contains the elements at distance at most m from o_{var_1}. If o_{var_1}^M belongs to D^M, then all the elements of L should belong to D.

We denote by \alpha_{ls,m}(var_1, var_2, next, L) the conjunction of \alpha^1_{ls}, \ldots, \alpha^4_{ls} and \alpha^5_{ls,m}. We write e.g., \alpha_{ls,m}(var_3, var_4, next_2, L_2) to use other start and end points, pointer or concept. We may write null instead of the second variable.

Note that due to the flexibility of L, it is easy to express variations of singly-linked lists, such as doubly-linked lists, or lists in which every element points to a special head element via a pointer head.

The case of trees is similar. We can write L-formulae which express all the conditions needed to express that T is a tree, except for a connectivity condition. We can define a (linearly sized) formula which expresses that if T^M is small, then all the elements are reachable from the root.
A Separation Logic Fragment

Here we discuss how a fragment of separation logic can be translated into $L$. The material in this subsection is not required to understand the remainder of the paper. Our separation logic is $\text{SL}_\text{lis}$, which is the logic from [8] with lists and multiple pointer fields, but without trees.

The memory model used in [8] is very similar to our memory structures. The allocated cells of the memory all have the same finite collection of fields (denoted $\text{Fields}$). Let $\text{Add}$ and $\text{Val}$ be disjoint sets. $\text{Add}$ is the set of addresses (locations in the terminology of [8], not to be confused with our use of “locations in a program”). $\text{Val}$ is a set of values which include nil. The description of the memory consists of two parts, a heap and a stack. A heap is a partial function $h : \text{Add} \rightarrow \text{Val} \cup \text{Add}$ which is only defined on a finite subset of $\text{Add}$. A stack is a function from a finite set $\text{Var}$ of local variables $s : \text{Var} \rightarrow \text{Val} \cup \text{Add}$.

First we define the logic $\text{SL}$. The syntax of $\text{SL}$ is as follows:

- Variables: $\Pi ::= T | E = E | E \neq E | \Pi \land \Pi$
- Fields: $\Sigma ::= \text{emp} | \text{var} \rightarrow [f_1 : E_1, \ldots, f_k : E_k] | S \ast \Sigma$
- $E ::= \text{null} | \text{var}_1$

$\text{SL}$-formula $::= \Pi \ast \Sigma$

The semantics of $\text{SL}$ is given by a relation $s, h \models \phi$ where $s \in \text{Stacks}, h \in \text{Heaps}$.

We define $[\text{var}_1]s :: s(x)$ and $[\text{nil}]s :: \text{nil}$, and:

- $s, h \models E_1 = E_2$ if $[E_1]s = [E_2]s$
- $s, h \models E_1 \neq E_2$ if $[E_1]s \neq [E_2]s$
- $s, h \models \Pi_0 \land \Pi_1$ if $s, h \models \Pi_0$ and $s, h \models \Pi_1$
- $s, h \models \text{var}_1 \rightarrow [f_1 : E_1]$ if $h = [\text{var}_1]s \rightarrow r$ where $r(f_1) = [E_1]s$
- $s, h \models \text{emp}$ if $h = \emptyset$
- $s, h \models \Sigma_1 \ast \Sigma_2$ if $\exists h_0 h_1. h = h_0 \ast h_1$ and $s, h_0 \models \Sigma_0$ and $s, h_1 \models \Sigma_1$
- $s, h \models \Pi \ast \Sigma$ if $s, h \models \Pi$ and $s, h \models \Sigma$

where $h_0 \ast h_1$ enforces there is no address in $\text{Add}$ on which both $h_0$ and $h_1$ are defined, and $h = h_0 \ast h_1$ denotes that $h$ is the union of $h_0$ and $h_1$. Additionally, not all fields in $\text{Fields}$ need to occur in $\text{var}_1 \rightarrow [f_1 : E_1]$, and those that do not are assigned nil implicitly.

$\text{SL}_\text{lis}$ extends $\text{SL}$ by adding list segments: the syntax is extended by $\Sigma ::= \cdots | \text{ls}(E_1, E_2)$ and the semantics of $\text{ls}(E_1, E_2)$ is the least fixed point of the predicate given by $(E_1 = E_2 \land \text{emp}) \lor (E_1 \neq E_2 \land \exists y. E_1 \rightarrow [n : y] \ast \text{ls}(y, E_2))$.

Heaps and Stacks vs. Memory Structures. The memory model of separation logic and our memory model are easily translatable. The distinction between values in $\text{Val}$ and addresses in $\text{Add}$ does not play a major role in [8], so we simplify by setting $\text{Val} = \{\text{nil}, \text{true}, \text{false}\}$.

Given $M$ we define $s_M$ and $h_M$ as follows. $\text{Fields}$ is equal to $\tau_{\text{fields}}$, and $\text{Add} = \text{Addresses}$ and we have $M = \text{Val} \cup \text{Add}$ with $\text{nil} = s^M_{\text{null}}$, $\text{true} = s^M_T$ and $\text{false} = s^M_F$. For every variable $\text{var}_i$, $s(\text{var}_i) = s^M_{\text{var}_i}$. For every $\text{add} \in \text{Add}$ we define $h(\text{add}) = h_{\text{add}}$ as follows: for every $f \in \text{Fields}$, $h_{\text{add}}(f) = f^M(\text{add})$.

Given $s$ and $h$, we define $M_{s,h} = M$ as follows. The universe $M_{s,h}$ is $\text{Add} \cup \{s^M_{\text{null}}, s^M_T, s^M_F\}$, with $s^M_{\text{null}} = \text{nil}$, $s^M_T = \text{true}$ and $s^M_F = \text{false}$ and $\text{Addresses}^M = \text{Add}$. The set of addresses on which $h$ is defined is $\text{Alloc}^M$. For
every field \( f \in \text{Fields} \), \( f^M = h_f \), where \( h_f(\text{add}) = h(\text{add})(f) \) is the value the field \( f \) of address \( \text{add} \) receives under \( h \). For every variable \( \text{var}_i \), \( o^M_{\text{var}_i,h} = s(\text{var}_i) \).

The above shows how to transform the memory models into each other in a natural way. More precisely:

**Lemma 1.** If \( s \) and \( h \) are a stack and a heap, and if \( s^M_{s,h} \) and \( h^M_{s,h} \) are the stack and heap obtained by applying the two transformations above on \( s \) and \( h \) in order, then \( s^M_{s,h} = s \) and \( h^M_{s,h} = h \).

**Reduction from SL** \( N \) to \( L \). For every SL formula \( \varphi \) and \( m \in \mathbb{N} \) we define an \( L \)-formula \( \alpha^m_{\varphi} \) such that the following Lemma holds:

**Lemma 2.** For every heap \( h \), stack \( s \), and \( m \in \mathbb{N} \), if \( \varphi \in \text{SL} \) and \( s, h \models \varphi \), then \( M_{s,h} \models \alpha^m_{\varphi} \).

It is convenient to define the following notation: if \( \varphi = \Pi \Sigma \), then there exist \( \beta_1, \ldots, \beta_r \) such that \( \Sigma = \beta_1 \cdots \beta_r \) and the \( \beta_i \) are of one of the forms \( \text{var}_1 \rightarrow [f_i : E_i] \) or \( l_{s}(E_1, E_2) \). We use the concepts \( P_1, \ldots, P_r \) which partition the allocated memory cells according to \( \Sigma \).

First we define the formula \( \alpha_{\varphi} \) for \( \varphi \in \text{SL} \)

\[
\begin{align*}
\alpha_{E_1=E_2} & = (o_{E_1} \equiv o_{E_2}) \\
\alpha_{E_1 \neq E_2} & = \neg (o_{E_1} \equiv o_{E_2}) \\
\alpha_{\Pi} & = \alpha_{\Pi_1} \wedge \alpha_{\Pi_2} \\
\alpha_{\text{true}} & = (\top \subseteq \top) \\
\alpha_{\text{emp}} & = (\text{Alloc} \equiv \bot) \\
\alpha_{E_1 \Sigma} & = (\Pi \Sigma) \\
\alpha_{E_1 \neq E_2} & = (\Pi \neq \Sigma)
\end{align*}
\]

For every \( \varphi \in \text{SL} \), \( s, h \models \varphi \) iff \( M_{s,h} \models \alpha_{\varphi} \).

For \( \beta_i = l_{s}(\text{var}_1, \text{var}_2) \), we define \( \alpha^m_{\beta_i} = \alpha_{\text{is},m}(\text{var}_1, \text{var}_2, \text{next}, P_1) \). From the discussion above we get that, if the interpretation of \( P_i \) in \( M \) is a list, then \( M \models \alpha_{\beta_i} \), implying Lemma 2.

**Running Example: Shape Invariants** At the loop header of the program \( S_2 \) from the introduction, the memory contains two distinct lists, namely the employee list and the project list. The employee list is partitioned into two parts, the employees who have been visited in the loop so far, and those that have not. This can be expressed in SL by the formula:

\[
\varphi_{l} = l_{s}(\text{emplHead}, e) \land l_{s}(e, \text{nil}) \land l_{s}(\text{projHead}, \text{nil}) \land \text{true}
\]

The translation into \( L \) is

\[
\begin{align*}
\alpha^m_{\varphi_{l}} &= P_1 \cup P_2 \cup P_3 \cup P_4 \equiv \text{Alloc} \land \alpha_{\text{is},m}(\text{emplHead}, e, \text{next}, P_1) \\
&\land \alpha_{\text{is},m}(e, \text{null}, \text{next}, P_2) \land \alpha_{\text{is},m}(\text{projHead}, \text{null}, \text{next}, P_3) \\
&\land P_1 \cap P_2 \equiv \bot \land P_1 \cap P_3 \equiv \bot \ldots \land P_3 \cap P_4 \equiv \bot \land \top \subseteq \top
\end{align*}
\]

The translation from separation logic assigns the lists and contents concepts \( P_i \) which do not reflect their content. In order to clarify the meaning of \( \alpha^m_{\varphi_{l}} \), we replace the \( P_i \) with the concepts from Section 2.4 and simplify the formula.
somewhat. The union of \( P_1 \) and \( P_2 \) is \( \text{EmplList} \), \( P_3 \) is \( \text{ProjList} \). \( VList = P_3 \) contains the elements of \( \text{EmplList} \) visited in the loop so far. \( \alpha^{\text{ll}}_m \) can be rewritten:

\[
\varphi_{\text{shp} - \ell}^m = \text{EmplList} \cup \text{ProjList} \subseteq \text{Alloc} \land VList \subseteq \text{EmplList} \land \\
\neg \text{ProjList} \equiv \perp \land \alpha_{\text{ls}, m}(\text{emplHead}, e, \text{next}, VList) \land \text{EmplList} \land \\
\alpha_{\text{ls}, m}(e, \text{null, next, EmplList} \setminus VList) \land \\
\alpha_{\text{ls}, m}(\text{projHead}, \text{null, next, ProjList})
\] (1)

3 Content Analysis

In this section we present our general methodology. To do so we first introduce our programming language precisely. The general methodology uses a backward propagation of formulae over loopless code.

3.1 Syntax and Semantics of the Programming Language

Loopless Programs The syntax of our loopless programming language is:

\[
e :: \text{var} \cdot f \mid \text{var} \mid \text{null} \quad (f \in \tau_{\text{fields}}, \alpha_{\text{var}} \in \tau_{\text{var}}) \\
b :: (e_1 = e_2) \mid \sim b \mid (b_1 \land b_2) \mid \neg (b_1 \lor b_2) \mid \text{T} \mid \text{F} \\
S :: \text{var}_1 := e_2 \mid \text{var}_1 := e_2 \mid \text{skip} \mid S_1; S_2 \mid \text{var} := \text{new} \mid \text{dispose(var)} \\
\mid \text{if } b \text{ then } S_1 \text{ else } S_2 \text{ fi} \mid \text{if } b \text{ then } S_1 \text{ fi} \mid \text{assume(b)}
\]

Let \( \text{Exp} \) denote the set of expressions \( e \) and \( \text{Bool} \) denote the set of Boolean expressions \( b \). We denote by \( \text{LLPrograms} \) the set of loopless programs generated by the above syntax.

To define the semantics of pointer and Boolean expressions, we extend \( f^\mathcal{M} \) by \( f^\mathcal{M}(\text{err}) = \text{err} \) for every \( f \in \tau_{\text{fields}} \). The functions \( \mathcal{E}[e](\mathcal{M}) : \text{Exp} \rightarrow \text{Addresses}^\mathcal{M} \cup \{\text{null, err}\} \) and \( \mathcal{B}[b](\mathcal{M}) : \text{Bool} \rightarrow \{\text{T, F, err}\} \) (with \( \text{err} \notin \mathcal{M} \)) are defined as follows:

\[
\mathcal{E}[\text{var}](\mathcal{M}) = \alpha^\mathcal{M}_{\text{var}}, \text{ if } \alpha^\mathcal{M}_{\text{var}} \in \text{Alloc}^\mathcal{M} \\
\mathcal{E}[\text{var} \cdot f](\mathcal{M}) = \text{err}, \text{ if } \alpha^\mathcal{M}_{\text{var}} \notin \text{Alloc}^\mathcal{M} \\
\mathcal{E}[\text{var}.f](\mathcal{M}) = f^\mathcal{M}(\mathcal{E}[\text{var}](\mathcal{M})) \\
\mathcal{B}[e_1 = e_2](\mathcal{M}) = \text{err} \text{ if } \mathcal{E}[e_i](\mathcal{M}) = \text{err}, i \in \{1, 2\} \\
\mathcal{B}[e_1 = e_2](\mathcal{M}) = \text{T}, \text{ if } \mathcal{E}[e_1](\mathcal{M}) = \mathcal{E}[e_2](\mathcal{M}) \\
\mathcal{B}[e_1 = e_2](\mathcal{M}) = \text{F}, \text{ if } \mathcal{E}[e_1](\mathcal{M}) \neq \mathcal{E}[e_2](\mathcal{M})
\]

\( \mathcal{B} \) extends naturally w.r.t. the Boolean connectives.

The operational semantics of the programming language is: For any command \( S \), if \( \mathcal{E} \) or \( \mathcal{B} \) give the value err, then \( \langle S, \mathcal{M} \rangle \sim \text{abort} \). Otherwise, the semantics is as listed above. If \( \mathcal{M} \) is a memory structure and \( \langle S, \mathcal{M} \rangle \sim \mathcal{M}', \) then \( \mathcal{M}' \) is a memory structure.

1. \( \langle \text{skip}, \mathcal{M} \rangle \sim \mathcal{M} \).
2. \( \langle \text{var}_1 := e_2, \mathcal{M} \rangle \sim [\mathcal{M} \mid \alpha^\mathcal{M}_{\text{var}_1} \text{ is set to } \mathcal{E}[e_2](\mathcal{M})] \).
3. \( \{ \text{var} := \text{new}, \mathcal{M} \} \leadsto \}
\[ \mathcal{M} | \text{For some } t \in \text{MemPool}^\mathcal{M}, t \text{ is added to } \text{Alloc}^\mathcal{M} \text{ and } o_{\text{var}}^\mathcal{M} \text{ is set to } t \],
4. If \( o_{\text{var}}^\mathcal{M} \notin \text{Alloc}^\mathcal{M} \), \( (\text{dispose(}\text{var}), \mathcal{M}) \leadsto \text{abort} \);
\quad otherwise \((\text{dispose(}\text{var}), \mathcal{M}) \leadsto \mathcal{M} | o_{\text{var}}^\mathcal{M} \text{ is removed from } \text{Alloc}^\mathcal{M} \).
5. \( \langle S_1; S_2, \mathcal{M} \rangle \leadsto \langle S_2, \langle S_1, \mathcal{M} \rangle \rangle \)
6. \( (\text{if } b \text{ then } S_T \text{ else } S_F, \mathcal{M}) \leadsto \langle S_{iV}, \mathcal{M} \rangle \) where \( tu = B[b](\mathcal{M}) \).
7. \( (\text{if } b \text{ then } S \text{ else } \text{skip } fi, \mathcal{M}) \leadsto \langle \text{if } b \text{ then } S \text{ else } \text{skip } fi, \mathcal{M} \rangle \). 
\quad otherwise \((\text{assume}(b), \mathcal{M}) \leadsto \mathcal{M} \);
\quad otherwise \((\text{assume}(b), \mathcal{M}) \leadsto \text{abort} \).

**Programs with Loops** Our programs are represented as hybrids of the programming language for loopless code and control flow graphs.

**Definition 4 (Program).** A program is \( G = (V, E, \ell_{\text{init}}, \text{shp}, \text{cnt}, \lambda) \) such that \( G = (V, E) \) is a directed graph with no multiple edge but possibly containing self-loops, \( \ell_{\text{init}} \in V \) has in-degree 0, shp and cnt are functions \( \text{shp}, \text{cnt} : V \rightarrow \mathcal{L}(\tau) \) and \( \lambda : E \rightarrow \text{LP programs} \).

Here is the code \( S_2 \) from the introduction:
\[
\begin{align*}
V &= \{ \ell_b, \ell, \ell_e \} \\
E &= \{ (\ell_b, \ell), (\ell, \ell), (\ell, \ell_e) \} \\
\ell_{\text{init}} &= \ell_b \\
\lambda(\ell_b, \ell) &= \text{null} ; S_b \\
\lambda(\ell, \ell_e) &= \text{null} ; S_e
\end{align*}
\]

\( S_b, S_t \) and \( S_e \) denote the three loopless code blocks which are respectively the code block before the loop, inside the loop and after the loop. The annotations \( \text{shp} \) and \( \text{cnt} \) are described in Section 3.4.

The semantics of programs derive from the semantics of loopless programs and is given in terms of program paths. Given a program \( G \), a path in \( G \) is a finite sequence of directed edges \( e_1, \ldots, e_t \) such for all \( 1 \leq i \leq t-1 \), the tail of \( e_i \) is the head of \( e_{i+1} \). A path may contain cycles.

We extend the \( \leadsto \) relation to paths in programs:

**Definition 5 (\( \leadsto^* \) for paths).** Given a program \( G \), a path \( P \) in \( G \), and memory structures \( M_1 \) and \( M_2 \) we define whether \( \langle P, M_1 \rangle \leadsto^* M_2 \) holds inductively.

- If \( P \) is empty, then \( \langle P, M_1 \rangle \leadsto^* M_2 \) iff \( M_1 = M_2 \).
- If \( e_i \) is the last edge of \( P \), then \( \langle P, M_1 \rangle \leadsto^* M_2 \) iff there exists \( M_3 \) such that \( \langle P \setminus \{ e_i \}, M_1 \rangle \leadsto^* M_3 \) and \( \langle \lambda(e_i), M_1 \rangle \leadsto^* M_3 \). \( P \setminus \{ e_i \} \) denotes the path obtained from \( P \) by removing the last edge \( e_i \).

### 3.2 Methodology Revisited

Now, we have all definitions available to revisit the methodology formulated in the introduction. Our methodology assumes a program \( P \) as stated in Definition 4 as input (ignoring the shp and cnt functions for the moment).

**I. Shape Analysis.** The user annotates the program locations with shape predicates. The validity of the shape predicates is then proved by some suitable technique. For concreteness, we have stated the separation logic \( \text{SLTs} \) as a possible
language for shape annotations in Section 2.4. The validity of \( \text{SL}_{\text{ls}} \) annotations can, for example, be proven by techniques from [8].

II. Content Analysis. The user translates the shape invariants into \( \mathcal{L} \)-formulae (stored in the \( \text{shp} \) function of \( P \)). For concreteness, we have defined an automatic translation from \( \text{SL}_{\text{ls}} \) annotations to \( \mathcal{L} \)-formulae in Section 2.5. However, we want to point out that our methodology is independent of the concrete choice of the shape predicates. We only require a translation of shape invariants to \( \mathcal{L} \)-formulae, as discussed in Section 2.5. Now, the user annotates the program locations with \( \mathcal{L} \)-formulae that she wants to verify (stored in the \( \text{cnt} \) function of \( P \)). We note that the \( \text{cnt} \) annotations can use the concepts obtained from the translated shape invariants.

In the rest of the paper we describe how to verify the \( \text{cnt} \) annotations. In Section 3.3 we state verification conditions and prove that the validity of the verification conditions implies the correctness of the \( \text{cnt} \) annotations. The key point of our methodology is that the verification conditions can be discharged automatically by a satisfiability solver for \( \mathcal{L} \)-formulae. The verification conditions rely on the backwards propagation function \( \Theta \) for \( \mathcal{L} \)-formulae which we introduce in Section 3.5.

3.3 Content Verification

We want to prove that, for every initial memory structure \( \mathcal{M}_1 \) from which the computation satisfies \( \text{shp} \) and which satisfies the content pre-condition \( \text{cnt}(\ell_{\text{init}}) \), the computation satisfies \( \text{cnt} \). Here are the corresponding verification conditions, which annotate the vertices of \( G \):

**Definition 6 (Verification conditions).** Given a program \( G \), \( VC \) is the function from \( E \) to \( \mathcal{L} \) given for \( e = (\ell_0, \ell) \) by

\[
VC(e) = \neg (\text{shp}(\ell_0) \land \text{cnt}(\ell_0) \land \Theta_{\lambda(e)}(\text{shp}(\ell) \land \neg \text{cnt}(\ell)))
\]

\( VC(e) \) holds if \( \top \models VC(e) \), i.e. if \( VC(e) \) is a tautology over memory structures.

We make the notion of a computation satisfying the verification conditions precise using the following definition:

**Definition 7 (Reach(\ell)).** Given a program \( G \), a node \( \ell \in V \), and a set \( \text{Init} \) of memory structures, Reach(\ell) is the set of memory structures \( \mathcal{M} \) for which there exist \( \mathcal{M}_{\text{init}} \in \text{Init} \) and a path \( P \) in \( G \) starting at \( \ell_{\text{init}} \) such that \( (P, \mathcal{M}_{\text{init}}) \sim^* \mathcal{M} \).

In particular, Reach(\ell_{\text{init}}) = \text{Init}. Let \( J \) be a set of memory structures. We write \( J \models \varphi \) if, for every \( \mathcal{M} \in J \), \( \mathcal{M} \models \varphi \).

**Theorem 2 (Soundness of the methodology).** Let \( G \) be a program such that, for all \( \ell \in V \), Reach(\ell) \models \text{shp}(\ell). If Reach(\ell_{\text{init}}) \models \text{cnt}(\ell_{\text{init}}) \) and for all \( e \in E \), \( VC(e) \) holds, then Reach(\ell) \models \text{cnt}(\ell), \) for all \( \ell \in V \).
The proof of Theorem 2 is given in the appendix.

In the definition of a program, we defined the range of \( shp \) and \( cnt \) as \( \mathcal{L}(\tau) \). However, in order to allow invariants of the form

\[
\phi_{\text{lists-updt}} = \text{EmpList}_{\text{gho}} \equiv \text{EmpList} \land \text{ProjList}_{\text{gho}} \uplus o_{\text{proj}} \equiv \text{ProjList}
\]

we add ghost concepts, roles and constants. We extended the vocabulary from \( \tau \) to \( \tau_{\text{ext}} \) by adding, for every symbol e.g. \( R \in \tau \), the symbol \( R_{\text{gho}} \). We think of \( \tau_{\text{ext}} \) structures as containing two snapshots of the memory: one is the current snapshot, and the other is a ghost snapshot, which is a snapshot of the memory at the beginning of the program. We denote the two underlying memory structures of \( M \) by \( M_{\text{cur}} \) and \( M_{\text{gho}} \). By \( \langle P, M_1 \rangle \sim^* M_2 \) we mean \( \langle P, (M_1)_{\text{cur}} \rangle \sim^* (M_2)_{\text{cur}} \).

In the sequel we refer to ghost elements of structures explicitly only when the treatment of them is different then other elements.

### 3.4 Running Example: General Methodology

The shape annotations of \( \ell_b \), \( \ell \) and \( \ell_e \) in the program \( S_2 \) all describe the two lists \( \text{ProjList} \) and \( \text{EmpList} \) using \( \alpha_{\text{ls}},m \) from Section 2.5.

The loop invariant also states that from \( \text{emplHead} \) to \( e \) we have a sub-list \( V \text{List} \) of \( \text{EmpList} \), where \( V \text{List} \) is a new concept. We think of \( V \text{List} \) as the subset of \( \text{EmpList} \) which has been visited so far in the loop. (\( V \text{List} \) was \( P_1 \) in Eq. (1)). At the start of every iteration, \( V \text{List} \) is a list starting at \( \text{emplHead} \) and ending at \( e \) (not inclusive). The variable \( \text{proj} \) points at the start of \( S_2 \) to an isolated cell not belonging to any of the lists. At the loop invariant and at the end of \( S_2 \), \( \text{proj} \) belongs to \( \text{ProjList} \).

\[
\phi_{\text{two-lists}} = \alpha_{\text{n},1}(\text{EmpList}, \text{null}, \text{next}, P_2) \land \alpha_{\text{n},1}(\text{ProjList}, \text{null}, \text{next}, \text{EmpList})
\]

\[
\text{shp}(\ell_b) = \phi_{\text{two-lists}} \land \text{proj} \sqsubseteq \text{Alloc} \land \neg(\text{EmpList} \uplus \text{ProjList})
\]

\[
\text{shp}(\ell_e) = \phi_{\text{two-lists}} \land \text{proj} \sqsubseteq \text{ProjList}
\]

\[
\text{shp}(\ell) = \alpha_{\text{shp-}l}^m
\]

where \( \phi_{\text{shp-}l} \) is from Section 2.5.

The three content annotations require that the invariants of the system \( \phi_{\text{invariants}} \) from Section 2.4 hold. The post-condition additionally requires that \( \phi_{\text{p-assgn}} \) and \( \phi_{\text{lists-updt}} \) hold. Recall \( \phi_{\text{p-assgn}} \) states that every employee which was not assigned a project, is assigned to \( o_{\text{proj}} \). \( \phi_{\text{lists-updt}} \) states that the content of the two lists remain unchanged, except that the project \( o_{\text{proj}} \) is inserted to the project list.

\[
\text{cnt}(\ell_b) = \phi_{\text{invariants}}
\]

\[
\text{cnt}(\ell_e) = \phi_{\text{invariants}} \land \phi_{\text{lists-updt}} \land \phi_{\text{p-assgn}}
\]

\[
\text{cnt}(\ell) = \phi_{\text{invariants}} \land \phi_{\text{lists-updt}} \land \phi_{\text{p-assgn-}l}
\]

\[
\phi_{\text{p-assgn-}l} = V \text{List} \sqcap \exists \text{worksFor}_{\text{gho}-o_{\text{null}}} \equiv V \text{List} \sqcap \exists \text{worksFor}.o_{\text{proj}}
\]
\( \varphi_{p\text{-assign} \cdot \ell} \) states that, in the list \( VList \) containing the employees visited so far in the loop, any employee which was not assigned to a project at the start of the program (i.e., in the ghost version of worksFor) is assigned to the project \( \text{proj} \). \( \varphi_{VList} \) makes no demands on elements of \( \text{EmplList} \) which have not been reach in the loop so far.

The verification conditions of \( G \) are

\[
\begin{align*}
VC(\ell_0, \ell) &= \neg (\text{shp}(\ell_0) \land \text{cnt}(\ell_0) \land \Theta_{\lambda(\ell_0, \ell)}(\text{shp}(\ell) \land \neg \text{cnt}(\ell))) \\
VC(\ell, \ell) &= \neg (\text{shp}(\ell) \land \text{cnt}(\ell) \land \Theta_{\lambda(\ell, \ell)}(\text{shp}(\ell) \land \neg \text{cnt}(\ell))) \\
VC(\ell, \ell_e) &= \neg (\text{shp}(\ell) \land \text{cnt}(\ell) \land \Theta_{\lambda(\ell, \ell_e)}(\text{shp}(\ell_e) \land \neg \text{cnt}(\ell_e)))
\end{align*}
\]

To apply Theorem 2 to \( G \), we only need to prove that the verification conditions \( VC(e) \) hold. Using Lemma 3, \( VC(\ell_0, \ell) \) is holds iff for every memory structures \( M, M' \) which satisfies the shape and content invariants \( \text{shp}(\ell_0) \) and \( \text{cnt}(\ell_0) \) such that the computation of \( S_b \) on \( M \) does not abort, \( \langle S_b, M \rangle \prec M' \) at \( M' \) satisfies \( \text{shp}(\ell) \), then \( M' \) satisfies \( \text{cnt}(\ell) \). The case is similar for the two other verification conditions. Since in this case the verification conditions hold, the program satisfies the annotation \( \text{cnt} \).

**Conclusion 1** \( \text{Reach}(\ell) \models \text{cnt}(\ell), \text{ for all } \ell \in V \).

### 3.5 Backwards Propagation

In this section we present the backwards propagation of a formula along a loopless program \( S \). Let \( \langle S, M_1 \rangle \prec M_2 \). Fields and variables (and other nominals) in \( M_2 \) are translated into expressions involving elements of \( M_1 \). For the remaining relations (e.g. \( \text{ProjList} \) and \( \text{EmplList} \) in our example) the treatment is different, in order to permit them to be deduced from a shape analysis in Section 3.3. These relations are copied as they are from \( M_2 \) and added to \( M_1 \). For every such relation symbol \( R \), we add a relation symbol \( R^{\text{end}} \) for the copied relation.

We denote by \( \langle M_1, R^{\text{end}} \rangle \) the structure obtained from \( M \) by adding the relations \( \langle R^{\text{end}} \rangle M_1 = R^M, R \in \tau \setminus \text{fields} \). The vocabulary \( \tau^{\text{end}} \) of \( \langle M, R^M \rangle \) extends \( \tau^{\text{end}} \) by relation symbols \( R^{\text{end}} \) for every relation \( R \in \tau \setminus \text{fields} \). For every formula \( \varphi \) of \( \tau \), we first substitute in \( \varphi \) the relations \( R \) which are not fields with \( R^{\text{end}} \). Then we perform the backwards propagation, which updates the fields and variables according to the loopless code.

We need a further extension of our structures. Given a finite set \( Y \) of labels, memory structures \( M_1 \) and \( M_2 \) with universe \( M \), and a tuple \( \vec{d}_Y = (d_y : y \in Y) \) of elements of \( M \), we denote by \( \langle M_1, R^{\text{end}}, \vec{d}_Y \rangle \) the structure obtained from \( \langle M, R^{\text{end}} \rangle \) by adding the constants \( d_y, y \in Y \). The vocabulary \( \tau^{\text{end}}_Y \) of \( \langle M, R^{\text{end}}, \vec{d}_Y \rangle \) extends \( \tau^{\text{end}} \) by constant symbols \( \{a_y : y \in Y\} \).

Given a loopless program \( S \), we assign unique labels \( y \) to the commands of \( S \). We denote by \( Y_S \) the set of labels of commands in \( S \).

**Lemma 3.** Let \( S \) be a loopless program, \( Y_S \) be the set of labels of commands in \( S \), \( M_1 \) and \( M_2 \) be memory structures, and \( \varphi \) be an \( L \)-formula over \( \tau \). There exists a program \( \overline{S} \) and a new label \( \text{abo} \notin Y_S \) such that:
1. Let \( \langle S, M_1 \rangle \sim M_2 \). Then: \( M_2 \models \varphi \) if there exists a tuple \( d_{Y_{1: \cup \{ablo\}}} \) of \( M \) elements such that \( \langle M_1, R^{end}, d_{Y_{1: \cup \{ablo\}}} \rangle \models \Theta_{S}(\varphi \land (o_{abo} \equiv o_{\varphi})) \).

2. If \( \langle S, M_1 \rangle \sim \text{abort} \), then for every tuple \( d_{Y_{1: \cup \{ablo\}}} \) of \( M \) elements, \( \langle M_1, R^{end}, d_{Y_{1: \cup \{ablo\}}} \rangle \not\models \Theta_{S}(\varphi \land (o_{abo} \equiv o_{\varphi})) \).

The definition of \( \Theta_{S} \) is:

**Definition 8** (\( \Theta_{S}(\varphi) \)). \( \Theta_{S}(\varphi) \) is obtained from \( \Psi \) by substituting every relation symbol \( R \in \tau^{\backslash \text{fields}} \) in \( \varphi \) by \( R^{end} \).

- \( \Psi_{\text{skip}}(\varphi) = \varphi \)
- \( \Psi_{\var_{1:=e}}(\varphi) = \varphi[o_{\var_{1}}/o_{e}], e = \var_{2} \) or \( e = \text{null} \)
- \( \Psi_{\text{var}_{1:=\text{var}_{2},f}}(\varphi) = \varphi[o_{\var_{1}}/o_{f}] \land (\exists f - o_{\text{var}_{2}} \equiv o_{f}) \)
- \( \Psi_{\text{disp}_{1:=2}}(\varphi) = \varphi[f / f \setminus (o_{\text{var}_{1}} \times T) \cup (o_{\text{var}_{1}}, o_{e})], e = \var_{2} \) or \( e = \text{null} \)
- \( \Psi_{\text{new}_{1:=2}}(\varphi) = \varphi[o_{\text{var}}/o_{2}][\text{Alloc} / \text{Alloc} \sqcup o_{g}] \)
- \( \Psi_{\text{disp}_{1:=2}}(\varphi) = \varphi[\text{var}_{f_{1}}:=\text{null}; \ldots ; \text{var}_{f_{u}}:=\text{null}][\text{Alloc} / \text{Alloc} \sqcup \neg o_{\text{var}}] \)
- \( \Psi_{S_{1};S_{2}}(\varphi) = \Psi_{S_{1}}(\Psi_{S_{2}}(\varphi)) \)

The notation \( \varphi[A/B] \) should be interpreted as the syntactic replacement of any occurrence of \( A \) with \( B \). We write e.g. \( y : \text{var} := \text{new} \) to indicate that the command \( \text{var} := \text{new} \) is new is labeled with \( y \). \( e_{b} \) is defined inductively: for \( e_{1} = e_{2} \) we set \( e_{b} = (A \epsilon_{1} = A \epsilon_{2}) \), with \( A \epsilon_{var} = o_{\epsilon_{var}} \) and \( A \epsilon_{var,f} = \exists f - o_{\epsilon_{var}} \), \( \epsilon \) extends naturally to the Boolean connectives. In the definition of \( \Psi_{\text{disp}_{1:=2}}(\varphi) \), \( f_{1}, \ldots , f_{u} \) are the members of \( \tau^{\text{fields}} \) which occur in \( \varphi \).

W.l.o.g. we assume that \( S \) does not contain commands of the form \( i f \) \( b \) then \( S_{1} \) \( f i \) or \( \text{var}_{1},f_{1} := \text{var}_{2},f_{2} \), since they can be expressed using the other commands.

We obtained \( \overline{S} \) from \( S \) as follows. Let \( abo \) be a new variable, whose corresponding constant symbol is \( o_{abo} \). We will use \( abo \) to indicate whether the run of \( M_{1} \) on \( S \) has aborted. The program \( \overline{S} \) does not abort. The command \( abo := \text{F} \) is added at the beginning of the code. Every command \( C \) of the form \( \text{var}_{1} := \text{var}_{2},f, \text{var}_{1},f := \text{var}_{2} \) or \( \text{dispose}(\text{var}_{2}) \) is replaced with \( \overline{C} = \text{if} \ \text{var}_{2} = \text{null} \) then \( abo := \text{T} \) else \( C \) \( fi \). For \( \text{if} \) and \( \text{assume} \) commands and for general assignment \( \text{var}_{1},f_{1} := \text{var}_{2},f_{2} \) commands the case is similar, except that there may be two evaluations of the form \( \text{var}_{1},f_{j} \), which need to be reflected in the condition in \( \overline{C} \).

By the construction of \( \overline{S} \), the run of \( M_{1} \) on \( \overline{S} \) does not abort. Moreover, \( abo \) has the value \( \text{T} \) at the end of the run of \( \overline{S} \) on \( M_{1} \) if and only if \( S \) aborts on \( M_{1} \).

Lemma 3 has to undergo a small correction in order to deal with ghost concepts, roles and constants, due to the fact \( \langle M_{1} \rangle_{gho} = \langle M_{2} \rangle_{gho} \). \( \Theta \) is augmented so that every occurrence of \( s_{gho}^{end} \) in \( \Theta_{S}(\varphi) \) is substituted with \( s_{gho} \), for every symbol \( s \).
3.6 Running Example: Backwards Propagation

As an example of the backwards propagation process, we consider a formula from Section 3.4, which is part of the content annotation of $\ell$:

$$\varphi_{passign} = VList \sqcap \exists worksFor_{gho} \cdot o_{null} \equiv VList \sqcap \exists worksFor \cdot o_{proj}$$

The result of the backwards propagation on $\varphi_{passign}$ is:

$$\Psi_{S_t}(\varphi_{passign}) = \exists worksFor^{-} \cdot o_{null} \land \Psi_{e.worksFor:=proj}(\varphi_{passign}) \lor 
\neg(\exists worksFor^{-} \cdot o_{null} \land \varphi_{passign})$$

$$\Psi_{e.worksFor:=proj}(\varphi_{passign}) = VList \sqcap \exists worksFor_{gho} \cdot o_{null} \equiv 
VList \sqcap \exists((worksFor \setminus (o_e \times T)) \cup (o_e, o_{proj})).o_{proj}$$

$\Psi_{e.worksFor:=proj}(\varphi_{passign})$ is obtained from $\varphi_{passign}$ by substituting the worksFor role with the correction $((worksFor \setminus (o_e \times T)) \cup (o_e, o_{proj}))$ which updates the value of $o_e$ in worksFor to proj. Note $\Psi_{e:=e.next}(\varphi_{passign}) = \varphi_{passign}$, because next does not occur in $\varphi_{passign}$. $\Psi_{e:=e.next}$ would alter formulae such as $\varphi_{ls_i}(empHead, e, next.VList)$, stating that $VList$ is a list with pointer next.

$\Theta_{S_t}(\varphi_{passign})$ is obtained from $\Psi_{S_t}(\varphi_{passign})$ by substituting $VList$ with $VList_{end}$. $VList$ and $VList_{end}$ stand for the list at the start respectively end of the iteration. While $\Theta_{S_t}(\varphi_{passign})$ does not contain $VList$, it is intended to be a part of a larger formula, which does refer to $VList$.

4 Related Work

Shape Analysis. Shape analysis has attracted considerable attention in the literature. The classical introductory paper to separation logic [25] presents an expressive separation logic which has turned out to be undecidable. We have restricted our attention to the restricted and better behaved fragment in [8], see also [7]. The work on separation logic focuses mostly on shape rather than content in our sense. Separation logic has been extended to object oriented languages, cf. e.g. [23] and [11], where shape properties similar to those studied in the non objected oriented case are the focus, and the main goal is to overcome difficulties introduced by the additional features of OO languages.

Other shape analyses could be potential candidates for integration in our methodology. [26] and [28] use 3-valued logic to perform shape analysis. Regional logic is used to check correctness of program with shared dynamically allocated memory areas [5]. [15] uses nested tree automata to represent the heap. [19] combines monadic second order logic with SMT solvers.

Description Logic. DLs have not been considerd for verification of programs with dynamically allocated memory, with the exception of [12] whose use (mostly undecidable) DLs to express shape-type invariants, ignoring content information. In [10] the authors consider verification of loopless code (transactions) in graph databases with integrity constraints expressed in DLs. Verification of temporal properties of dynamic systems in the presence of DL knowledge bases...
has received significant attention (see [4,3,13] and the references therein). Temporal Description Logics, which combine classic DLs with classic temporal logics, have also received significant attention in the last decade (see [18] for a survey).

**Related Ideas.** Several recent research projects have concentrated on verification strategies which use information beyond the semantics of the source code. For instance, [17] is using diagrams from design documentation to support verification. Another recent paper [29] is inferring the intended use of program variables to guide a program analysis. Instead of starting from code and verifying its correctness, [14] explores how to declaratively specify data structures with sharing and how to automatically generate code from this specification.

Due to the interdisciplinary nature of this work and space limitations, it is difficult to cover all the relevant literature. We welcome all suggestions.

## 5 Conclusion

In this paper we have demonstrated that description logic can be used as the basis of a novel program analysis methodology. Our method analyzes the data content of dynamic data structures on top of existing shape analysis methods. A central feature of our approach is the systematic translation of shape invariants into description logic. Our future work will focus on the identification of new description logics which are particularly well-suited for this application, enable us to obtain more precise translations of shapes, and have good algorithmic properties. While the current approach is semi-manual, our long term goal is to increase the automatization of the method.

## References

Many fresh elements with M.

Note that any finite model M of a formula \( \phi \) is obtained by adding to MemPool infinitely many fresh elements e and setting \( f^M(e) = o^M_{null} \) for all \( f \in \tau_{fields} \).

A Satisfiability in Memory Structures

Proof (Theorem 1). For the upper bound, we employ the fact that finite satisfiability of \( \mathcal{L} \)-formulae, i.e. truth in a structure with a finite domain, is in NExpTime. This can be shown by a fairly standard reduction (see e.g. [9]) to finite satisfiability of formulae in \( \mathcal{C}^2 \), the two-variable fragment of the first-order logic with counting quantifiers. The latter problem is in NExpTime due to [24]. We give a finite satisfiability preserving translation from \( \mathcal{L} \) to \( \mathcal{C}^2 \) in Table 1.

To show that satisfiability of a formula \( \psi \) in a memory structure can be decided in nondeterministic exponential time, it suffices to construct in linear time a formula \( \psi_m \) such that \( \psi \) is satisfiable in a memory structure iff \( \psi_m \wedge \psi \) is finitely satisfiable. The formula \( \psi_m \) is the conjunction of the following formulae corresponding to requirements (3)-(9) we placed on memory structures:

- \( Aux \equiv o_{null} \sqcup o_T \sqcup o_F \).
- \( Addresses \sqsubseteq \neg Aux \) and \( Addresses \sqcup Aux \equiv T \).
- \( Alloc \sqsubseteq \neg MemPool \) and \( Alloc \sqcup MemPool \sqsubseteq Addresses \).
- \( o \sqsubseteq \neg MemPool \) for every nominal concept o of \( \psi \).
- \( func(f) \) and \( Addresses \sqsubseteq \exists f. \neg MemPool \) for every f of \( \psi \) with f \( \in \tau_{fields} \).
- \( MemPool \sqsubseteq \forall f. o_{null} \sqcup o_F \) for every f \( \in \tau_{fields} \), and
- \( C \sqsubseteq \neg MemPool \) for every atomic concept C \( \in \tau \) with \( C \neq MemPool \).

Note that any finite model \( M \) of \( \psi_m \wedge \psi \) is almost the desired memory structure with \( M \models \psi \). The desired \( M \) is obtained by adding to \( MemPool^M \) infinitely many fresh elements e and setting \( f^M(e) = o^M_{null} \) for all f \( \in \tau_{fields} \).

Table 1. Translation of \( \mathcal{L} \) into \( \mathcal{C}^2 \) by employing only two variables x and y. In each translation rule, z \( \in \{x,y\} \). Moreover, z = y if z = x, and \( \bar{z} = x \) if z = y.
The lower bound comes from the $\mathsf{NExpTime}$-hardness of satisfiability in the DL $\mathcal{ACCHOTIQ}$ [27]. We note that the proof in [27] concerns satisfiability in arbitrary structures, including structures that are not memory structures. However, the reduction from the $2^n \times 2^n$ tiling problem given in [27] can be easily recast in terms of memory structures.

### B Backwards propagation: Proof of Lemma 3

To prove Lemma 3 we need the following lemma:

**Lemma 4.** Let $S$ be a loopless program without assume commands, $Y_S$ be the set of labels of commands in $S$, $Y$ be a set of labels disjoint from $Y_S$, $M_1$ and $M_2$ be memory structures with universe $M$ such that $(S, M_1) \sim M_2$. $d_Y$ be a tuple of $M$ elements and $\varphi$ be an $\mathcal{L}$-formula over $\tau \cup \{o_y : y \in Y\}$. $(M_2, d_Y) \models \varphi$ iff there exists a tuple $d_{Y_S}$ of $M$ elements such that $(M_1, R^{\text{end}}, d_Y, d_{Y_S}) \models \Theta_S(\varphi)$.

**Proof.** We prove the lemma by induction.

- $S = \text{skip}$: $Y_S = \emptyset$, and we have $(M_2, d_Y) \models \varphi$ iff $(M_1, R^{\text{end}}, d_Y) \models \Theta_S(\varphi)$, as required. ($d_{Y_S}$ is the empty tuple.)
- $S = \text{if then } S_1 \text{ else } S_2 \text{ fi}$: depending on whether $\varepsilon_b$ is true or false, $\Theta_{S_1}(\varphi)$ or $\Theta_{S_2}(\varphi)$ should be used.
- $var_1 := e$, where $e$ is a variable $var_2$ or null: every reference to $var_1$ in $\varphi$ is replaced by a reference to $var_2$ or null, respectively.
- $var_1 := var_2, f$: every reference to $var_1$ in $\varphi$ is replaced with a reference to $d_Y$, the interpretation of $o_y$, and $d_y$ is required to be the result of applying $f$ on $var_2$.
- $var_1 := : e$, where $e$ is a variable $var_2$ or null: the function symbol $f$ is updated by removing the current value of $f$ on $var_1$ by subtracting $(o_{var_1} \times \top)^{M_1}$ from $f^{M_1}$ and setting the new value explicitly by adding the pair $(o_{var_1}, o_{e}^{M_1})$ to $f^{M_1}$.
- $S = \text{var} := \text{new}$ with label $y$: $Y_S = \{y\}$, and we set $d_{Y_S} = (d_y)$ such that $(d_y) = \text{Alloc}^{M_2} \setminus \text{Alloc}^{M_1}$. Such $d_y$ exists by the semantics of the allocation command. $\Theta_S(\varphi)$ adds $d_y$ to $\text{Alloc}^{M_1}$ and replaces every reference to $var$ by a reference to $d_y$.
- $S = \text{dispose}(\text{var})$: $\Theta_S(\varphi)$ removes $\text{var}$ from $\text{Alloc}$, and using an application of $\Theta$ to the program $\text{var} \cdot f_1 := \text{null} ; \ldots ; \text{var} \cdot f_k := \text{null}$, sets all of the fields in $\varphi$ to null.
- $S = S_1; S_2$: $\Theta_S(\varphi) = \Theta_{S_1}(\Theta_{S_2}(\varphi))$. Let $M_3$ be an memory structure such that $(S_1, M_1) \sim M_3$ and $(S_2, M_3) \sim M_2$.

Consider first $\Theta_{S_1}(\varphi)$. By the induction hypothesis, there exist $d_{Y_{S_2}}$ such that $(M_2, d_Y) \models \varphi$ iff there exists a tuple $d_{Y_{S_2}}$ of $M$ elements such that $(M_3, R^{\text{end}}, d_Y, d_{Y_{S_2}}) \models \Theta_{S_2}(\varphi)$.

Let $M_4$ be obtained from $M_3$ by replacing every relation $R^{M_3}$ with $R^{M_2}$ for $R \in \tau \setminus \text{fields}$. In other words, $R^{\text{end}} = R^{\text{end}}$. Let $\psi = \Psi_{S_1}(\varphi), \Theta_{S_2}(\varphi)$ does not use any relation $R \in \tau \setminus \text{fields}$ (but rather the $R^{\text{end}}$), and therefore the
vocabulary of $\psi$ is that of $\langle M_4, \bar{d}_Y, \bar{d}_{\bar{y}_S} \rangle$. Moreover, $\psi \models \langle M_4, \bar{d}_Y, \bar{d}_{\bar{y}_S} \rangle$ iff $\Theta_{S_2}(\varphi) \models \langle M_3, \bar{d}_{\text{end}}, d_Y, \bar{d}_{\bar{y}_S} \rangle$.

Applying the induction hypothesis once again, there exists $\bar{d}_{\bar{y}_S_1}$ such that $\langle M_4, \bar{d}_Y, \bar{d}_{\bar{y}_S_1} \rangle \models \varphi$ if there exists a tuple $\bar{d}_{\bar{y}_S_1}$ of $M$ elements such that $\langle M_1, \bar{d}_Y, \bar{d}_{\bar{y}_S_1}, \bar{d}_{\bar{y}_S_2} \rangle \models \Theta_{S_1}(\Theta_{S_2}(\varphi))$. Denoting the concatenation of $\bar{d}_{\bar{y}_S_1}$ and $\bar{d}_{\bar{y}_S_2}$ by $\bar{d}_{\bar{y}_S}$, we get $\langle M_2, \bar{d}_Y \rangle \models \varphi$ iff $\langle M_1, \bar{d}_{\text{end}}, \bar{d}_Y, \bar{d}_{\bar{y}_S} \rangle \models \Theta_{S_1}(\Theta_{S_2}(\varphi))$.

Lemma 4 applies to memory structures with ghost concepts, roles and constants by the same correction of $\Theta$ as discussed in Section 3.

Proof (Lemma 3).

Using Lemma 4 with $Y = \emptyset$, if $S$ aborts on $M_1$, then for every $\bar{d}_{\bar{y}_S}$ and $d_{\text{abo}}$ and $\bar{U}$ we have $\langle M_1, \bar{U}, \bar{d}_{\bar{y}_S}, d_{\text{abo}} \rangle \not\models \Psi_S(\varphi \land (o_{\text{abo}} \equiv o_F))$; if $\langle S, M_1 \rangle \sim M_2$, $M_2 \models \varphi$ iff $\langle M_1, \bar{d}_{\bar{y}_S}, d_{\text{abo}} \rangle \models \Psi_S(\varphi \land (o_{\text{abo}} \equiv o_F))$. Note that $d_{\text{abo}}$ is the value of $\text{abo}$ at the beginning of the run of $S$. Since the first command of $S$ assigns $\text{abo}$ a new value, $d_{\text{abo}}$ plays no role (it appears because, technically, $\text{abo}$ still needs a value at the beginning of the run).

C Proof of Theorem 2

Let $M \in \text{Reach}(\ell)$, and let $P$ be a path and $M_{\text{init}} \in \text{Init}$ as guaranteed for members of $\text{Reach}(\ell)$. We prove the claim by induction on the length of $P$.

If $P$ is empty, the claim holds.

If $P$ is not empty, let $e = (\ell_0, \ell)$ be the last edge of $P$, and let $P_0$ be the path obtained from $P$ by removing $e$. Let $M_0$ be an memory structure such that $\langle P_0, M_{\text{init}} \rangle \sim^* M_0$, and $\langle e, M_0 \rangle \sim^* M$. We have $M_0 \models \text{shp}(\ell_0)$ and $M \models \text{shp}(\ell)$. By the induction hypothesis, $M_0 \models \text{cnt}(\ell_0)$.

Since $\text{VC}(e)$ holds, in particular we have for every $\bar{U}$ and $\bar{d}$, $\langle M_0, \bar{U}, \bar{d} \rangle \models \text{VC}(e)$, Let $\bar{U} = \bar{d}_{\text{end}}$. For every $\bar{d}$, $\langle M_0, \bar{U}, \bar{d} \rangle \models \text{shp}(\ell_0) \land \text{cnt}(\ell_0)$. Therefore, for every $\bar{d}$, $\langle M_0, \bar{U}, \bar{d} \rangle \not\models \Theta_{\lambda(e)}(\text{shp}(\ell) \land \neg \text{cnt}(\ell))$. By Lemma 3, $M \not\models \text{shp}(\ell) \land \neg \text{cnt}(\ell)$. Since $M \models \text{shp}(\ell)$, we get $M \models \text{cnt}(\ell)$.

Remark 1. In the proof of Theorem 2 only case 1. of Lemma 3 is used. The purpose of case 2. of Lemma 3 is to make the verification conditions less strict, in the sense that they require nothing of aborted executions.