Model Checking for Symbolic-Heap Separation Logic with Inductive Predicates

James Brotherston  
University College London, UK  
J.Brotherston@ucl.ac.uk

Nikos Gorogiannis  
Middlesex University, UK  
nikos.gorogiannis@gmail.com

Max Kanovich  
University College London, UK and National Research University Higher School of Economics, Russia  
M.Kanovich@ucl.ac.uk

Reuben Rowe  
University College London, UK  
R.Rowe@ucl.ac.uk

Abstract

We investigate the model checking problem for symbolic-heap separation logic with user-defined inductive predicates, i.e., the problem of checking that a given stack-heap memory state satisfies a given formula in this language, as arises e.g. in software testing or runtime verification.

First, we show that the problem is decidable; specifically, we present a bottom-up fixed point algorithm that decides the problem and runs in exponential time in the size of the problem instance.

Second, we show that, while model checking for the full language is EXPTIME-complete, the problem becomes NP-complete or PTIME-solvable when we impose natural syntactic restrictions on the schemata defining the inductive predicates. We additionally present NP and PTIME algorithms for these restricted fragments.

Finally, we report on the experimental performance of our procedures on a variety of specifications extracted from programs, exercising multiple combinations of syntactic restrictions.

Categories and Subject Descriptors  D.2.4 [Software / Program Verification]: Model checking; F.3.1 [Specifying and Verifying and Reasoning about Programs]: Logics of programs, Assertions

Keywords  Separation logic, model checking, inductive definitions, complexity, runtime verification, program testing.

1. Introduction

In modern computer science, model checking is most commonly considered to be the problem of deciding whether a given Kripke structure or transition system $S$ — typically representing a program or system — satisfies, or is a model of, a given formula $A$ of modal or temporal logic [18]; this property is usually written as $S \models A$. More generally, in mathematical logic, $S$ might be a mathematical structure of virtually any kind and $A$ a formula in some appropriate logic for such structures (see e.g. [20] for the cases of first-order and monadic second-order logic).

In this paper, we investigate the model checking problem as it arises in the setting of separation logic with user-defined inductive predicates. Separation logic is an established formalism for the verification of imperative pointer programs, comprising both an assertion language of formulas based on bunched logic and a Hoare-style system of triples manipulating the pre- and postconditions of programs [23, 29]. Given a program annotated with separation logic assertions, one can try to prove statically that each assertion holds at the appropriate program point; a long line of research in this area has resulted in a number of tools that are capable of doing this automatically at least some of the time for industrial code (see e.g. [7, 8, 14, 16, 19, 24, 28]). Alternatively, one might also try to test dynamically whether properties hold: simply execute the program and check whether each assertion is satisfied by the actual memory state of the program at that point (this is sometimes known as run-time verification). Such an approach obviously necessitates a method for deciding, for any memory state $S$ and separation logic formula $A$, whether or not $S \models A$: a model checking problem. While this is straightforward for simple formulas, it becomes much more complicated when arbitrary user-defined inductive predicates, describing complex shape properties of the memory, are permitted.

Our first contribution is a general model checking procedure (in the sense above) for the most commonly considered symbolic heap fragment of separation logic, extended with a general schema for user-defined inductive predicates. Since our definition schema allows inductive predicates to denote possibly-empty heap memories, and any heap trivially decomposes into itself combined with the empty heap, a naive top-down approach based on backtracking search will generally fail to terminate. Instead, we employ a bottom-up approach based on computing the fixed point of all "sub-models" of the original memory that satisfy one of the defined inductive predicates. The crucial insight is that, for any given model checking query, the witnesses for the existentially quantified variables can be chosen from a fixed set of values given in advance. Our algorithm decides the model checking problem for our logic, in (worst-case) exponential time in the query size. Indeed, we show that this problem is EXPTIME-complete.

In practice, however, it is often the case that the inductive predicate definitions encountered in verification practice fall within much more well-behaved fragments of our general inductive schemata. Our second main contribution is an analysis of the model
checking problem in cases where the syntactic form of inductive definitions is restricted in various ways (e.g., when recursion is forbidden in cases where the heap might be empty). We show that, for different combinations of these restrictions, the model checking problem can become NP-complete or even PTIME-solvable; and, in such cases, we give concrete model checking algorithms that fall within the appropriate complexity bound.

Finally, we provide an implementation of our general model checking algorithm, and of our specialised algorithm for the polynomial-time fragment, within the CYCLOIST theorem proving framework; this implementation is available online [1]. We evaluate their performance on a range of examples gathered from the separation logic community, as well as some hand-crafted examples. Our experimental results seem to bear out that our model checking methods are practical for runtime verification applications when suitable syntactic restrictions are present, and for offline testing (such as in unit test suites) in the general case.

**Related work.** Runtime verification for separation logic was addressed first in [26], and then more recently in the Verifast tool [3]. In both cases, model checking works only for classes of recursive predicates that are restricted in various ways, and comes without any formal correctness claims or complexity bounds. As far as we know, the present paper is the first to specifically address model checking for symbolic heap separation logic with general inductive predicates from a fully formal perspective. However, the logic itself has attracted considerable recent interest amongst the verification community. The aforementioned automated program verification tools based on separation logic [7, 8, 14, 16, 19, 24, 28] are all based on symbolic heaps, and increasingly targeted at verifying specifications involving user-defined rather than hard-coded predicates. Indeed, there are now even tools capable of automatically generating the definitions of inductive predicates needed for analysis [11, 25]. On the theoretical side, the satisfiability problem for our logic was recently shown decidable [10] and its entailment analysis [11, 25]. On the theoretical side, the satisfiability problem is then shown to be EXPTIME-complete in Section 4. We present our restricted fragments in Section 5, and establish their various complexities in Section 6. Section 7 presents details of our implementation and experiments, and Section 8 concludes.

## 2. \(SL_{D}^{SH}\): Symbolic-Heap Separation Logic with Inductively Defined Predicates

In this section we present our fragment \(SL_{D}^{SH}\) of separation logic, which restricts the syntax of formulas to symbolic heaps as introduced in [5, 6], but allows arbitrary user-defined inductive predicates over these, as considered e.g. in [9, 10, 11, 22].

We often write vector notation to abbreviate tuples, e.g. \(x\) for \((x_1, \ldots, x_n)\). We write \(\text{proj}_i\) for the \(i\)th projection function on tuples, and we often abuse notation by treating a tuple \(x\) as the set containing exactly the elements occurring in \(x\). If \(X\) and \(Y\) are sets, we write \(X \neq Y\) as a shorthand for \(X \cap Y = \emptyset\).

### 2.1 Syntax

A term is either a variable in the infinite set \(V\) or the constant nil. We write \(x, y, z\), etc. to range over variables, and \(t, u, \ldots\) to range over terms. We assume a finite set \(P = \{P_1, \ldots, P_n\}\) of predicate symbols, each with associated arity.

**Definition 2.1** (Symbolic heap, Spatial formulas \(F\) and pure formulas \(\pi\)) are given by the following grammar:

\[
F ::= \text{emp} \mid x \mapsto t \mid Pt \mid F \circ F \quad \pi ::= t = t \mid t \neq t
\]

where \(x\) ranges over variables, \(t\) over terms, \(P\) over predicate symbols and \(\pi\) over tuples of terms (matching the arity of \(P\) in \(Pt\)).

A symbolic heap is given by \(\exists x. \Pi : F\), where \(x\) is a tuple of distinct variables, \(F\) is a spatial formula and \(\Pi\) is a finite set of pure formulas. Whenever one of \(\Pi, F\) is empty, we omit the colon. We write \(FV(A)\) for the set of free variables occurring in a symbolic heap \(A\); by convention, the bound variable names in \(A\) are chosen disjoint from the free variables \(FV(A)\).

**Definition 2.2.** An inductive rule set is a finite set of inductive rules, each of the form \(A \Rightarrow Px\), where \(A\) is a symbolic heap (called the body of the rule), \(Px\) a formula (called its head), \(x\) is a tuple of distinct variables and \(FV(A) \subseteq x\).

For convenience, we sometimes drop existential quantifiers from inductive rules \(A \Rightarrow Px\); in that case, any variables occurring in \(A\) but not in \(x\) are implicitly existentially quantified.

As usual, the inductive rules with \(P\) in their head should be read as exhaustive, disjunctive clauses of an inductive definition of \(P\). The formal semantics appears below.

### 2.2 Semantics

We use a RAM model employing heaps of records. We assume we countably infinite set \(V\) of values of which an infinite subset \(Loc \subset V\) are addressable locations; we insist on at least one non-addressable value \(\text{nil} \in V \setminus Loc\).

A **stack** is a function \(s : \text{Var} \rightarrow V\); we extend stacks to terms by setting \(s(\text{nil}) \equiv \text{def} \text{nil}\), and write \(s[z \mapsto a]\) for the stack defined as \(s\) except that \(s[z \mapsto a](\pi) = a\). We extend stacks pointwise to act on tuples of terms.

A **heap** is a partial function \(h : \text{Loc} \rightarrow V\) (Val List) mapping finitely many locations to records, i.e. arbitrary-length tuples of values; we set \(dom(h)\) to be the set of locations on which \(h\) is defined, and \(e\) to be the empty heap that is undefined on all locations. We write \(o\) for composition of domain-disjoint heaps: if \(h_1\) and \(h_2\) are heaps, then \(h_1 \circ h_2\) is the union of \(h_1\) and \(h_2\) when \(dom(h_1) \neq dom(h_2)\), and undefined otherwise. Finally, we define the **cover** of a heap \(h\) as

\[
\text{cover}(h) := \text{def} dom(h) \cup \{b \in V \mid b \in h(a), a \in dom(h)\},
\]

i.e., the set of all values mentioned anywhere in \(h\).

**Definition 2.3.** Let \(\Phi\) be a fixed inductive rule set. Then we say that a stack-heap pair \((s, h)\) is a model of a symbolic heap \(A\) if the relation \(s, h \models_{\Phi} A\) holds, defined by structural induction on \(A\):

\[
s, h \models_{\Phi} t_1 = t_2 \iff (s(t_1) = s(t_2)) \\quad s, h \models_{\Phi} t_1 \neq t_2 \iff s(t_1) \neq s(t_2) \\quad s, h \models_{\Phi} \text{emp} \iff h = e \\quad s, h \models_{\Phi} x \mapsto t \iff dom(h) = \{s(x)\} \text{ and } h(s(x)) = s(t) \\quad s, h \models_{\Phi} Pt \iff (s(t), h) \in [P]^{\Phi} \\quad s, h \models_{\Phi} F_1 \circ F_2 \iff \exists h_1, h_2. h_1 = h_2 \circ h_1 \text{ and } s, h_1 \models_{\Phi} F_1 \text{ and } s, h_2 \models_{\Phi} F_2 \\quad s, h \models_{\Phi} \exists x. \Pi : F \iff \exists a \in V^{\Phi}. s[x \mapsto a], h \models_{\Phi} \pi \text{ for all } \pi \in \Pi \text{ and } s[z \mapsto a], h \models_{\Phi} F
\]

where the semantics \([P]^{\Phi}\) of the inductive predicate \(P\) under \(\Phi\) is defined below.

If \(A\) contains no inductive predicates, then its satisfaction relation does not depend on the inductive rules \(\Phi\), and we typically write \(s, h \models A\) to mean that \(s, h \models_{\Phi} A\), for any \(\Phi\). Similarly, if \(\Pi\)
is a set of pure formulas, we write $s \models \Pi$ to mean that $s, h \models \Phi$ for any heap $h$ and inductive rule set $\Phi$.

The following definition gives the standard semantics of the inductive predicate symbols $P$ according to a fixed inductive rule set $\Phi$, i.e., as the least fixed point of an $n$-ary monotone operator constructed from $\Phi$.

**Definition 2.4.** First, for each predicate $P_i \in P$ with arity $\alpha_i$, say, we define $\tau_i = \text{Pow}(\text{Val}^{\alpha_i} \times \text{Heap})$ (where $\text{Pow}(\cdot)$ is powerset). We also partition the rule set $\Phi$ into $\Phi_1, \ldots, \Phi_n$, where $\Phi_i$ is the set of all inductive rules in $\Phi$ of the form $A \Rightarrow P_i.x$.

Now let each $\Phi_i$ be indexed by $j$ (i.e., $\Phi_{i,j}$ is the $j$-th rule defining $P_i$), and for each inductive rule $\Phi_{i,j}$ of the form $\exists x. \Pi : F \Rightarrow P_i.x$, we define the operator $\varphi_{i,j} : \tau_1 \times \ldots \times \tau_n \rightarrow \tau_i$ by:

$$\varphi_{i,j}(Y) = \{ (s(x), h) \mid s, h \models \Pi, F \}$$

where $Y \subseteq \tau_1 \times \ldots \times \tau_n$ and $\models_Y$ is the satisfaction relation defined above, except that $[P_i]_Y = \text{proj}(Y)$. We then finally define the tuple $[P]_{\Phi} = (\tau_1 \times \ldots \times \tau_n)$ by:

$$[P]_{\Phi} = \mu Y. ([P_i]_Y \cup \bigcup_j \varphi_{i,j}(Y))$$

where $\mu$ is the least fixed point constructor. We write $[P_i]_{\Phi}$ as an abbreviation for $\text{proj}(P_i, [P]_{\Phi})$.

Note that in computing $\varphi_{i,j}(Y)$ above, we strip the existential quantifiers $\exists x$ from the body of the inductive rule $\Phi_{i,j}$, taking advantage of the convention that the existentially bound variables $x$ are disjoint from the free variables $x$ in $\Phi_{i,j}$.

3. A Model Checking Algorithm for SL$^{SH}_{1D}$

In this section we develop a decision procedure for the model checking problem in our logic SL$^{SH}_{1D}$. Formally, this problem is stated as follows:

**Model checking problem** (MC). Given an inductive rule set $\Phi$, stack $s$, heap $h$ and symbolic heap $A$, decide whether $s, h \models A$.

We observe that whether $s, h \models A$ depends not on the entire (infinite) valuation of $s$ but only on the values of $s$ on $F V(A)$, which is finite; thus an instance of MC can be also viewed as finite. In fact, the problem can be simplified further by noting that, if we can solve the case when $A = P.x$, for $P$ an inductive predicate, then the general case follows almost immediately:

**Restricted model checking problem** (RMC). Given an inductive rule set $\Phi$, tuple of values $a \in \text{Val}$, heap $h$ and predicate symbol $P$, decide whether $(a, h) \in [P]_\Phi$.

**Proposition 3.1.** MC and RMC are (polynomially) equivalent.

**Proof.** Given an instance $(\Phi, a, h, P)$ of RMC, where $m = |a|$ is the arity of $P$, we define the corresponding instance of MC to be $(\Phi, s, h, P.x)$, where $s$ is an $m$-tuple of distinct variables and $s$ is any stack satisfying $s(x) = a$. Then, clearly,

$$s, h \models P.x \iff (s(x), h) \in [P]_\Phi \iff (a, h) \in [P]_\Phi$$

Conversely, let $(\Phi, s, h, A)$ be an instance of MC. Let $F V(A) = x$, let $Q$ be a predicate symbol of arity $|x|$ not occurring in $\Phi$, and define $\Phi' = \Phi \cup \{ A \Rightarrow Qx \}$. We then define the corresponding instance of RMC to be $(\Phi', s(x), h, Q)$. By construction,

$$s, h \models A \iff s, h \models \Phi \land Qx \iff (s(x), h) \in [Q]_\Phi$$

Both reductions are trivially computable in polynomial time. $\square$

Thus it suffices to formulate a decision procedure for the restricted problem RMC. Before diving into the details of our decision procedure, let us motivate its development by making two main observations about this problem.

1. One might be tempted to adopt a top-down approach to the problem by applying inductive rules backwards to $P.x$, obtaining smaller model-checking problems (in the size of the heap $h$) as recursive instances. Unfortunately, our general schema for inductive rules does not guarantee that the models of subformulas of the body of an inductive rule are strictly smaller than the models of the entire body, and so such an approach might fail to terminate. For example, suppose $((a, b), h) \in [P]_\Phi$, and is generated by the inductive rule

$$\exists x. P.xz \land P.yz \Rightarrow P.zx.$$

Then we know that, for some $c \in \text{Val}$, we should have both $((a, c), h_1) \in [P]_\Phi$ and $((c, b), h_2) \in [P]_\Phi$, where $h = h_1 \circ h_2$; but we do not know that $h_1, h_2$ are smaller than $h$; either might be the empty heap $\epsilon$. (Indeed, it is quite possible that all of $h_1, h_2$ are empty.)

Therefore, we adopt a bottom-up approach: we attempt to compute all tuples in $[P]_\Phi$ that are “sub-models” of $(a, h)$, by iteratively applying the inductive rules until we reach a fixed point. (In fact, we have to do this for all inductive predicates $P$ simultaneously, in order to account for possible mutual dependency among them.) This process is guaranteed to terminate provided that there are only finitely many such sub-models.

2. The principal remaining difficulty is one of completeness: i.e., can we guarantee that any $(a, h) \in [P]_\Phi$ can be generated by applying the inductive rules in $\Phi$ to sub-models of $(a, h)$? In fact this point is quite delicate, due to the presence of unrestricted existential quantification in our inductive rules. For example, suppose $(a, e) \in [P]_\Phi$ is generated by the rule

$$\exists z. Pxz \land Pyz \Rightarrow Pz.$$

Then we know that for some $b \in \text{Val}$, we have $((a, b), e) \in [Q]_\Phi$, where $b \neq a$ and $b$ (trivially) does not appear in the empty heap $\epsilon$. Thus we must allow our sub-models to mention fresh, or “spare”, values not mentioned in $a$ or $h$.

Fortunately, as we show (Lemma 3.7), only finitely many such spare values are needed for any given rule set $\Phi$; these can be “recycled” as needed at each fresh application of an inductive rule in our fixed point computation.

We now formally define our fixed point construction computing all tuples $(b, h') \in [P]_\Phi$ that are sub-models of a given $(a, h)$, where “sub-model” means that $h' \subseteq h$ and $b$ consists of values from $a$, $\text{cover}(h)$, the null value nil and a suitably chosen set of “spare” values.

**Definition 3.2.** Let $\Phi$ be an inductive rule set, $a$ a tuple of values (from Val) and $h$ a heap. We define the set $\text{Good}(a, h)$ (of “good sub-model values for $(a, h)$”) by

$$\text{Good}(a, h) = a \cup \{ \text{nil} \} \cup \text{cover}(h).$$

Now let $\beta$ be the maximum number of (free and bound) variable names appearing in any inductive rule in $\Phi$. We define $\text{Spare}_\beta(a, h)$ to be a set of $\beta$ fresh values (from Val) that do not occur in $\text{Good}(a, h)$.

**Definition 3.3.** Let $\Phi$ be an inductive rule set, $a$ a tuple of values and $h$ a heap. For each inductive rule $\Phi_{i,j} \in \Phi$ of the form

$$\exists x. \Pi : F \Rightarrow P_i.x,$$

we define an operator $\psi_{i,j} : \tau_1 \times \ldots \times \tau_n \rightarrow \tau_i$. 
as follows:

\[ \psi_{n,j}(Y) = \text{def} \begin{cases} (s(x), h') & s', h' \models_\Pi F \land h' \subseteq h \land s(x \in s) \subseteq \text{Good}(a, h) \cup \text{Spare}_p(a, h) \end{cases} \]

where \text{Good}(a, h) and \text{Spare}_p(a, h) are the sets of values given by Definition 3.2. It should be clear that each \( \psi_{n,j} \) is a monotone operator. Thus we define the tuple \( MC^p(a, h) \in \tau_1 \times \ldots \times \tau_n \) by

\[ MC^p(a, h) = \text{def} \mu Y. (\bigcup_j \psi_{j,1}(Y), \ldots, \bigcup_j \psi_{n,j}(Y)) \]

We write \( MC^p(a, h) \) as an abbreviation for \( \text{proj}_i(MC^p(a, h)) \).

For the remainder of this section, we shall assume a fixed instance of \( MC^p(a, h) \), given by choosing inductive rule set \( \Phi \), tuple of values \( a \) and heap \( h \).

It should be fairly obvious by comparing the constructions in Definitions 2.4 and 3.3 that \( MC^p(a, h) \) can only contain tuples that are already elements of \( [P]^p \). The following lemma formalises that claim.

**Lemma 3.4 (Soundness).** \( MC^p(a, h) \subseteq [P]^p \).

**Proof.** We proceed by fixed point induction on the tuple of sets \( MC^p(a, h) \). That is, we assume the inclusion \( Y \subseteq [P]^p \) holds for some tuple of sets \( Y = (Y_1, \ldots, Y_n) \in \tau_1 \times \ldots \times \tau_n \), and must show it holds for \( (\bigcup_j \psi_{j,1}(Y), \ldots, \bigcup_j \psi_{n,j}(Y)) \). This means, assuming that \( (b, h') \in \psi_{j,1}(Y) \) for some inductive rule \( \Phi_{i,j} \), we must show that \( (b, h') \in [P]^p \). Without loss of generality, we can consider \( \Phi_{i,j} \) to be written in the form:

\[ \exists z. \Pi : y_1 \rightarrow u_1 \cdots y_k \rightarrow u_k * P_1 x_1 \cdots * P_{\lambda_1} x_{\lambda_1} \Rightarrow P_i x. \]

By construction of \( \psi_{j,1}(Y) \), there is a stack \( s \) with \( s(x) = b \) and \( s, h' \models_\Pi \Pi \). Thus, we have (for some \( y \in Y_j \) and thus, by the induction hypothesis, \( s(x_{k+1}) \in [P]^p_i \)). That is, \( s, h_{k+1} \models_\Pi y_i \rightarrow u_i \) for all \( 1 \leq i \leq k \), and \( s, h_{k+1} \models_\Pi P_j x_i \) for all \( 1 \leq i \leq m \).

Putting everything together, we have:

\[ s, h' \models_\Pi \Pi : y_1 \rightarrow u_1 \cdots y_k \rightarrow u_k * P_1 x_1 \cdots * P_{\lambda_1} x_{\lambda_1} \Rightarrow P_i x. \]

Therefore, \( MC^p(a, h) \subseteq [P]^p \) as required. □

Next, we must show that \( MC^p(a, h) \) contains all \( (b, h') \in [P]^p \) that are “sub-models” of \( (a, h) \). To do this, we need to argue that for any element \( (b, h') \in [P]^p \) that is “almost a sub-model” of \( (a, h) \) in that \( h' \subseteq h \) but \( b \) contains “bad” values (not in \text{Good}(a, h) or \text{Spare}_p(a, h)), there are corresponding sub-models in \( MC^p(a, h) \), obtained by substituting “spare” values for “bad” ones. The following definition captures the relevant notion of substitution.

**Definition 3.5.** A finite partial function \( \theta : Val \rightarrow Val \) is called a substitution on \( MC^p(a, h) \) if it is injective, and, for all \( b \in \text{dom}(\theta) \),

\[ \theta(b) = b \text{ if } b \in \text{Good}(a, h) \text{, and} \]

\[ \theta(b) \in \text{Spare}_p(a, h) \text{ if } b \notin \text{Good}(a, h). \]

Next, the following technical lemma, which will be crucial to completeness, captures the fact that we can “recycle” values as needed. Roughly speaking, it says that we can extend a substitution on the values \( b \) instantiating the head of an inductive rule to a substitution on the values \( V \supseteq b \) instantiating the head of the rule and the existentially quantified variables in its body. This relies on the fact that, by construction, there are at least as many spare values in \( \text{Spare}_p(a, h) \) as there are variables in any inductive rule.

**Lemma 3.6.** Let \( \theta \) be a substitution for \( MC^p(a, h) \) such that \( \text{dom}(\theta) \ni \{ b \} \subseteq b \), and \( V \subseteq Val \) a (finite) set of values \( b \subseteq V \) and \( |V| \leq |\text{Spare}_p(a, h)| \). Let \( \text{Spare}_p(a, h) \ni \theta(b) = \{ d_1, \ldots, d_n \} \) and let \( V \setminus \{ b \cup \text{Good}(a, h) \} = \{ e_1, \ldots, e_k \} \). Then the function \( \theta' : V \rightarrow Val \), defined by

\[ \theta'(c) = \text{def} \begin{cases} c & \text{if } c \in \text{Good}(a, h) \\ \theta(c) & \text{if } c \in b \setminus \text{Good}(a, h) \\ d_i & \text{if } c = e_i \text{ for some } 1 \leq i \leq k, \end{cases} \]

is also a substitution for \( MC^p(a, h) \), with \( \theta'(b) = \theta(b) \).

**Proof.** For convenience, we abbreviate \( \text{Good}(a, h) \) by \( G \) and \( \text{Spare}_p(a, h) \) by \( S \) in this proof.

First, since \( V \subseteq Val \) is finite, \( \theta' \) is indeed a finite partial function \( Val \rightarrow Val \). We argue that \( \theta' \) is well-defined. The three cases of its definition above are non-overlapping by construction, the first case is trivially well-defined and the second case is well-defined since \( \text{dom}(\theta) \ni \{ b \} \subseteq b \). Thus we just need to show that the third case is well-defined, which means showing that \( k \leq m \), i.e.,

\[ |V \setminus \{ b \cup G \}| \leq |S| - |\theta(b)|. \]

Since \( \theta \) is injective by assumption, \( |\theta(b)| = |b| \). Thus, as \( |V| \leq |S| \), we have \( |V \setminus \{ b \}| \leq |S| - |\theta(b)| \). Then, using standard set theory, we have as required

\[ |V \setminus \{ b \cup G \}| \leq |V \setminus \{ b \}| \leq |S| - |\theta(b)| \leq |S| - |\theta(b)| \]

Next we argue that \( \theta' \) is indeed a substitution for \( MC^p(a, h) \). It is easy to see that \( \theta'(c) = c \) if \( c \in \text{Good}(a, h) \) and \( \theta'(c) \in \text{Spare}_p(a, h) \) otherwise. We just need to show \( \theta' \) is injective. This follows from the fact that the three definitional cases of \( \theta' \) are given by three injective functions with pairwise disjoint ranges: \( G, \theta'(b) \subseteq S \) and \( S \setminus \theta(b) \), respectively. Hence if \( \theta'(c_1) = \theta'(c_2) \) then both \( c_1 \) and \( c_2 \) fall into the same definitional case of \( \theta' \), and so \( c_1 = c_2 \) by injectivity of the corresponding function. Thus indeed \( \theta' \) is a substitution for \( MC^p(a, h) \) as required. □

**Lemma 3.7 (Completeness).** Let \( (b, h') \in [P]^p \) and \( h' \subseteq h \), and let \( \theta \) be a substitution for \( MC^p(a, h) \) with \( \text{dom}(\theta) \ni \{ b \} \). Then \( \theta(b, h') \in MC^p(a, h) \).

**Proof.** We proceed by fixed point induction on \( [P]^p \). That is, we assume the lemma holds for \( Y = (Y_1, \ldots, Y_n) \in \tau_1 \times \ldots \times \tau_n \), and must show it holds for \( (\bigcup_j \phi_{j,1}(Y), \ldots, \bigcup_j \phi_{n,j}(Y)) \). This means, assuming that \( (b, h') \in \phi_{j,1}(Y) \) for some inductive rule \( \Phi_{j,1} \), \( h' \subseteq h \) and we have a \( \theta \) satisfying the conditions of the lemma, we must show that \( (\theta(b), h') \in MC^p(a, h) \).

Without loss of generality, we may consider \( \Phi_{j,1} \) to be written in the form:

\[ \exists z. \Pi : y_1 \rightarrow u_1 \cdots y_k \rightarrow u_k * P_1 x_1 \cdots * P_{\lambda_1} x_{\lambda_1} \Rightarrow P_i x. \]

By construction of \( \phi_{j,1} \), we have a stack \( s \) such that \( s(x) = b \) and \( s, h' \models_\Pi \Pi : y_1 \rightarrow u_1 \cdots y_k \rightarrow u_k * P_1 x_1 \cdots * P_{\lambda_1} x_{\lambda_1} \Rightarrow P_i x. \)
This means that $s \models \Pi$ and $h' = h_1 \circ \ldots \circ h_{k+m}$, where

$$s, h_i \models y_i \rightarrow u_i \quad \text{for all } 1 \leq i \leq k,$$

and

$$s, h_{k+i} \models P_i(x_i) \quad \text{for all } 1 \leq i \leq m.$$

The latter two statements can be rewritten as follows:

$$\text{dom}(h_i) = \{(s(y_i)) \} \text{ and } h_i(s(y_i)) = s(u_i) \text{ for all } 1 \leq i \leq k,$$

and

$$\text{dom}(h_{k+i}) = \text{proj}_i(MC^\Phi(a, h) \text{ for all } 1 \leq i \leq m).$$

Recall that $x$ and $z$ describe respectively the sets of all free and bound variables appearing in the inductive rule $\Phi_i$. We have that $\{x \cup z\} \subseteq \text{Val}$ is finite, and $b = \{x\} \subseteq \{x \cup z\}$ and $|\{x \cup z\}| \leq |\text{Spare}_\Phi(a, h)|$ by construction. Therefore, by taking $V = \{x \cup z\}$ in Lemma 3.6, and noting $\text{dom}(\theta) \supseteq b$ by assumption, we can obtain a substitution $\theta'$ for $MC^\Phi(a, h)$ with $\text{dom}(\theta') = \{x \cup z\}$ and $\theta'(b) = \theta(b)$.

Now, since $\theta'$ is injective, it is easy to see that $s \circ \theta' \models \Pi$ (where $\circ$ here denotes function composition). Additionally, since $s(y_i), s(u_i) \subseteq \text{cover}(a, h)$, we have by construction, for all $1 \leq i \leq k$,

$$\text{dom}(h_i) = \{(s(y_i))\} \text{ and } h_i(s(y_i)) = s(u_i),$$

i.e. $s \circ \theta', h_i \models y_i \rightarrow u_i$.

Notice that, for any $1 \leq i \leq m$, we have both $h_{k+i} \subseteq h' \subseteq h$ and $\text{dom}(\theta') \supseteq s(x)$. Therefore, by the induction hypothesis,

$$(\theta'(s(x_i)), h_{k+i}) \in MC^\Phi(a, h) \text{ for all } 1 \leq i \leq m.$$ Putting everything together, we obtain

$$s \circ \theta', h' \models MC^\Phi(a, h) \quad \Pi: y_1 \rightarrow u_1 \ast \ldots \ast y_k \rightarrow u_k.$$

As $(s \circ \theta')(x \cup z) \subseteq \text{Good}(a, h) \cup \text{Spare}_\Phi(a, h)$ by construction, we obtain by the definition of $MC^\Phi(a, h)$ (Definition 3.3):

$$(s \circ \theta')(x, h') \in MC^\Phi(a, h).$$

Finally, as $s(x) = b$ and $\theta'$ coincides with $\theta$ on $b$, we have $(s \circ \theta')(x) = \theta'(s(x)) = \theta(b)$. Thus we obtain as required

$$(\theta(b), h') \in MC^\Phi(a, h).$$

**Lemma 3.8.** For each $1 \leq i \leq n$,

$$(a, h) \in [P_i]^\Phi \iff (a, h) \in MC^\Phi(a, h).$$

**Proof.** The $(\Rightarrow)$ direction follows directly from Lemma 3.4. The $(\Leftarrow)$ direction follows from Lemma 3.7 by taking $(b, h')$ there to be $(a, h)$, and $\theta$ to be the identity function on $a$ (noting that $a \subseteq \text{Good}(a, h)$, so this is trivially a substitution in the sense of Definition 3.5).

**Lemma 3.9.** $MC^\Phi(a, h)$ is finite and computable.

**Proof.** By construction (Definition 3.3), $MC^\Phi(a, h)$ can only contain tuples of the form $(b, h')$, where $h' \subseteq h$ and $b$ is a finite tuple of values, drawn from the finite set $\text{Good}(a, h) \cup \text{Spare}_\Phi(a, h)$. As the heap $h$ is also finite, each such $(b, h')$ is a finite object and there can be only finitely many of them. Hence $MC^\Phi(a, h)$ is finite.

To see that $MC^\Phi(a, h)$ is computable, observe that it is defined as the least fixed point of a monotone operator. It is well known that this least fixed point can be approached iteratively in approximant stages, starting from the $n$-tuple $(\emptyset, \ldots, \emptyset)$. Since $MC^\Phi(a, h)$, there can be only finitely many such approximants. To see that each one is computable, it suffices to show that any $\psi_{s,h}(Y)$ is computable, given that $Y \in \tau_1 \times \ldots \times \tau_n$ is computable and the inductive rule $\Phi_i$, is of the form $\exists x. \Pi: \Phi \Rightarrow \Pi(x,x)$. Say, this is quite clear: First, there are only finitely many membership candidates $(b, h')$ with $h' \subseteq h$ and $b \subseteq \text{Good}(a, h) \cup \text{Spare}_\Phi(a, h)$.
4. Complexity of General Model Checking

In this section we investigate the computational complexity of the general model checking problem MC, as described in the previous section. Specifically, we show that MC is EXPTIME-complete, and is still NP-hard in the size of the heap when the underlying inductive rule set is fixed in advance.

In the following, we write ||·|| to denote the length of (some reasonable) encoding of a finite mathematical object o.

**Lemma 4.1.** MC is EXPTIME-hard.

**Proof.** By Proposition 3.1, it suffices to show that the restricted model checking problem, RMC, is EXPTIME-hard. This is by reduction from the following special case of the satisfiability problem for SL(I), which was shown to be EXPTIME-hard in [10]: given an inductive rule set Φ containing no occurrences of →, and a predicate symbol P from Φ of arity 0, decide whether there exists a model s, h such that s, h |= _P_. Since Φ contains no occurrences of → and P no free variables, this means deciding whether e ∈ [P]_Φ^*(recall e is the empty heap). Thus, given any instance (Φ, P) of the above problem, the corresponding instance of RMC is simply given by (Φ, (.), e, P). □

**Lemma 4.2.** MC ∈ EXPTIME.

**Proof.** By Proposition 3.1, it suffices to show RMC ∈ EXPTIME. By Lemma 3.8, deciding a given instance I = (Φ, a, h, P) of RMC can be done by computing MC^Φ^*(a, h) and checking whether (a, h) ∈ prov_Π(MC^Φ^*(a, h)). Thus it suffices to show that MC^Φ^*(a, h) can be computed in exponential time in m = def ||I||. Recall that MC^Φ^*(a, h) is obtained by a fixed point construction of a monotone operator (Definition 3.3):

\[ MC^Φ^*(a, h) = \text{def } hY. (\bigcup_j \psi_{i,j}(Y), \ldots, \bigcup_j \psi_{n,j}(Y)) \]

This least fixed point can be approached iteratively from below, starting from (∅, . . ., ∅). Writing N = |MC^Φ^*(a, h)|, this process will reach a fixed point in at most N iterations. Let T be the maximum number of polynomial-time steps required to compute any ψ_{i,j}(Y), given the earlier fixed point approximant Y. Since each iteration involves the computation of ψ_{i,j}(Y) for every inductive rule Φ_{i,j} ∈ Φ, it is clear that computing MC^Φ^*(a, h) requires N · ||Φ|| · T polynomial-time steps.

Now, to obtain an upper bound for N, observe that by construction [MC^Φ^*(a, h)] contains only pairs of the form (b, b') such that b' ⊆ h, the length of b is bounded by the maximum arity of any predicate, which is bounded by ||Φ||, and b ⊆ ∈ Good(a, h) ∪ Spare_Φ(a, h), which is bounded by ||a|| + ||h|| + 1 + ||Φ|| = ||I|| + 1 (the extra 1 comes from nil). Therefore, we obtain

\[ N \leq (||I|| + 1)^||Φ|| \cdot 2^{||h||} = O(2^{poly(||I||)}) \]

Next, we obtain an upper bound for T. Given Y and the inductive rule Φ_{i,j} of the form ∃x.R.F : F ⇒ P(x), say, it clearly suffices, for any “candidate” (b, b') of the above form, to decide whether or not (b, b') ∈ ψ_{i,j}(Y). This means checking whether b' ⊆ h and, for every valuation of the variables x \cup z into Good(a, h) ∪ Spare_Φ(a, h), checking whether s(x) = b and s, b' \models_Φ F (where s is any stack obtained by extending the chosen valuation). The heap inclusion check can be done in polynomial time, and the number of possible valuations is (easily) bounded by N. To check s, b' \models_Φ F we might need to consider every possible division of h' into a number of “sub-heap”s bounded by the maximum number of s in any rule, in turn bounded by ||Φ|| (as per the proofs of Lemmas 3.4 and 3.7). There are at most 2^||Φ|| such combinations. Finally, as Y might contain up to N elements, checking whether a chosen division of h' satisfies the conditions \[ T \leq N \cdot N \cdot 2^{|h||} = O \left(2^{poly(||I||)} \right) \]

Therefore, altogether, the computation of MC^Φ^*(a, h) requires at most N · ||Φ|| · T = O(2^{poly(||I||)}) polynomial-time steps. □

**Theorem 4.3.** MC is EXPTIME-complete.

**Proof.** Immediate by Lemmas 4.1 and 4.2. □

Typically, in program verification applications, the definitions of the inductive predicates are fixed in advance. Thus, it is also of interest to know how the complexity of MC varies in the size of the heap h over a fixed inductive rule set Φ.

**Proposition 4.4.** MC is NP-hard in ||h||.

**Proof.** By Proposition 3.1, it suffices to show RMC is NP-hard in ||h||. We exhibit a polynomial-time reduction from the following triangle partition problem, known to be NP-complete [21]: given a graph G = (V, E) with |V| = 3q for some q > 0, decide whether there is a partition of G into triangles.

First, we fix the following inductive rule set Φ_{PT}:

\[ x \mapsto \text{nil} \Rightarrow V(x) \]

\[ e \mapsto (x, y) \ 	ext{if} (\exists x \ 	ext{in } E) \]

\[ V(x) \ast V(y) \ast V(z) \ast E(x, y) \ast E(y, z) \ast E(x, z) \Rightarrow T \]

\[ E(x, y) \ast J \Rightarrow J \ 	ext{emp} \Rightarrow J \ T \ast P \Rightarrow P \ J \ast P \]

Now we give the reduction. For any instance G = (V, E) of the above triangle partition problem, first write \[ V = \{v_1, \ldots, v_n\} \] and \[ E = \{e_1, \ldots, e_m\}. \] We let \(a_1, \ldots, a_m\) and \(b_1, \ldots, b_{2m}\) be distinct addresses in Loc, and define a heap h_G, with dom(h_G) = \{a_1, \ldots, a_m, b_1, \ldots, b_{2m}\}, as follows:

\[ h_G(a_i) = \text{nil} \quad \text{for} \quad 1 \leq i \leq n, \]

\[ h_G(b_{2k}) = (a_i, a_j) \quad \text{for} \quad 1 \leq k \leq 2m \quad \text{and} \quad e_k = \{v_i, v_j\}, \]

\[ h_G(b_{2k+1}) = (a_i, a_j) \quad \text{for} \quad 1 \leq k \leq 2m \quad \text{and} \quad e_k = \{v_i, v_j\}. \]

The required instance of RMC is then given by (Φ_{PT}, (.), h_G, P) (note that Φ_{PT} and P are fixed for any G). Clearly it is polynomial-time computable. For correctness, we need to show that G has a partition into triangles if and only if h_G ∈ [P]^{Φ_{PT}}. This follows from the following easy observations, for any subheap h of h_G and values c, d (the formal details are easily reconstructed):

\( (c, d, h) \in [V]^{Φ_{PT}} \text{ iff } (c, h) \text{ exactly represents a vertex in } G; \)

\( ((c, d), h) \in [E]^{Φ_{PT}} \text{ iff } ((c, d, h) \text{ exactly represents an undirected edge in } G; \)

\( h \in [T]^{Φ_{PT}} \text{ iff } h \text{ exactly represents a triangle in } G; \)

\( h \in [J]^{Φ_{PT}} \text{ iff } h \text{ exactly represents some collection of edges in } G; \)

\( h \in [P]^{Φ_{PT}} \text{ iff } h \text{ exactly represents a collection of non-overlapping triangles in } G \text{ covering all vertices in } G, \text{ plus a collection of \lq\lq leftover\rq\rq} \text{ edges from } G, \text{ i.e. iff } G \text{ has a partition into triangles.} \) □

5. Restricted Fragments

According to Theorem 4.3, the general model checking problem is EXPTIME-complete. In practice, however, one frequently encounters definition schemas that are more restrictive than our general schema. Here and in the next section, we investigate the computational complexity of model checking when various natural syntactic restrictions are imposed on predicate definitions. Informally, the restrictions we consider are the following:

...
MEM: “Memory-consuming” rules, which only permit recursion in the presence of explicit non-empty memory.

CV: “Constructively valued” rules, in which the values of all variables occurring in a rule body are uniquely determined by the values of variables occurring in its head, together with the heap.

DET: “Deterministic” rules, in which the pure (dis)equality conditions in the rules for a predicate are mutually exclusive.

Arity: The maximum arity of any predicate is fixed in advance.

Importantly, each of the above restrictions can be described in a clear syntactical way. The restrictions DET and CV have appeared previously in the literature, in various guises (e.g. [16, 3]). Together, as we will show in Section 6.5, they imply precision, the notion that a formula unambiguously circumscribes the part of the heap on which it is true [27]. The restriction MEM, as far as we know, is novel, but is seemingly crucial in reducing the complexity of model checking from EXPTIME down to NP or PTIME.

In Section 6 we show that the general EXPTIME can be reduced to PSPACE to NP or even PTIME for the fragments defined by different combinations of the above restrictions. The following table summarises our results:

<table>
<thead>
<tr>
<th></th>
<th>CV</th>
<th>DET</th>
<th>CV+DET</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEM</td>
<td>EXPTIME</td>
<td>EXPTIME</td>
<td>EXPTIME</td>
</tr>
<tr>
<td>non-MEM</td>
<td>NP</td>
<td>NP</td>
<td>NP</td>
</tr>
<tr>
<td>MEM</td>
<td>NP</td>
<td>NP</td>
<td>PSPACE</td>
</tr>
<tr>
<td>MEM+CV</td>
<td>EXPTIME</td>
<td>EXPTIME</td>
<td>EXPTIME</td>
</tr>
</tbody>
</table>

Remark 5.1. For each of the combinations MEM, MEM+CV, MEM+DET, their NP-completeness holds even when the arity of the predicates involved is fixed in advance.

In contrast, notwithstanding EXPTIME-hardness, for the fragment defined only by non-memory-consuming rules, model checking can be resolved in PTIME, but the degree of the polynomial is proportional to the maximal arity of the predicates involved.

We now formally introduce the restrictions MEM, CV and DET.

Definition 5.2 (MEM). An inductive rule set is said to be memory-consuming (a.k.a. “in MEM”) if every rule in it is of the form

\[ \Pi : \text{emp} \Rightarrow P \cdot x, \quad \text{or} \quad \exists z. \Pi : F \cdot x \Rightarrow P \cdot x. \]

Remark 5.3. The following definitions of binary predicates \( \text{ls} \) and \( \text{rls} \), defining possibly-cyclic list segments by head recursion, and \( \text{rls} \), defining possibly-cyclic list segments by tail recursion, are both in MEM. Both definitions “consume” a pointer when recursing.

Example 5.3. The following definitions of binary predicates \( \text{ls} \), defining possibly-cyclic list segments by head recursion, and \( \text{rls} \), defining possibly-cyclic list segments by tail recursion, are both in MEM. Both definitions “consume” a pointer when recursing.

\[ x = y : \text{emp} \Rightarrow \text{ls}(x, y) \]

(1)

\[ \exists z. x \Rightarrow z \cdot \text{ls}(z, y) \Rightarrow \text{ls}(x, y) \]

and

\[ x = y : \text{emp} \Rightarrow \text{rls}(x, y) \]

(2)

\[ \exists z. x \neq y : \text{rls}(x, z) 

Definition 5.4 (CV). A variable \( z \) occurring in an inductive rule \( \exists y. \Pi : F \Rightarrow P \cdot x \) is said to be constructively valued in that rule if:

(a) \( z \in x \), or
(b) there is a variable \( w \) also occurring in the rule such that \( w \) is constructively valued, and either

- \( \Pi \models z = w \), or
- \( w \mapsto u \) is a subformula of \( F \) and \( z \in u \).

An inductive rule is constructively valued if all its variables are, and an inductive rule set is constructively valued (a.k.a. “in CV”) if all its rules are.

Example 5.5. The existentially quantified variable \( z \) is constructively valued in the definition of \( \text{ls} \) in Example 5.3 (1), but not in the definition of \( \text{rls} \) (2).

Definition 5.6 (DET). A predicate \( P \) is said to be deterministic (in an inductive rule set \( \Phi \)) if for any two distinct rules of the form

\[ \exists z. \Pi : F \Rightarrow P \cdot x \quad \text{and} \quad \exists z'. \Pi' : F' \Rightarrow P \cdot x, \]

there exists no stack \( s \) such that \( s, e \models \exists z. (\Pi : \text{emp}) \) and \( s, e \models \exists z'. (\Pi' : \text{emp}) \). An inductive rule set \( \Phi \) is deterministic (a.k.a. “in DET”) if all predicates defined in \( \Phi \) are deterministic.

We note that whether \( \Phi \) is deterministic is decidable in polynomial time via a simple procedure that eliminates pure sub-formulas employing quantified variables [10].

Example 5.7. In Example 5.3, the definition of \( \text{rls} \) (2) is deterministic, but the definition of \( \text{ls} \) (1) is not.

6. Complexity of Restricted Fragments

In this section, we investigate the computational complexity of model checking for different combinations of the restrictions MEM, CV and DET introduced in the previous section.

The main technical tool underpinning the following complexity results is the notion of an unfolded inductive tree. The idea is simple: in order to show that \( (a, h) \in [P]^\rho \), we repeatedly unfold the rules from \( \Phi \) backwards (from head to body), instantiating variables with values and matching assertions with pointers in \( h \) as we go according to the rule constraints.

Definition 6.1. For the sake of brevity, given an elementary formula \( Q(x_1, \ldots, x_n) \), we write \( \tilde{Q} \) to denote a statement \( Q(a_1, \ldots, a_n) \) obtained by instantiating the variables in \( Q \) with values and heap pointers in the obvious way. For example, \( \tilde{x} \Rightarrow \tilde{y} \) represents the one-cell heap that contains \( \tilde{y} \) at location \( \tilde{x} \). Then we specify the unfolded inductive tree by induction (see Figure 1):

(a) Let \( \tilde{Q}_m \) be generated by an instantiated rule \( \rho_m \) of the form

\[ \tilde{Q}_m : h_m \Rightarrow \tilde{Q}_m \]

Then we make a tree, \( T_{\tilde{Q}_m} \), consisting of one edge labelled by \( \rho_m \); the root is labelled by \( \tilde{Q}_m \), the leaf by \( h_m \).

(b) Suppose that an instantiated rule \( \rho \) of the form

\[ \tilde{Q}_m \Rightarrow h_m \]

generates \( \tilde{R} \), and \( T_{\tilde{Q}_0}, T_{\tilde{Q}_1}, \ldots, T_{\tilde{Q}_m} \) are inductive trees having been already constructed for \( Q_0, Q_1, \ldots, Q_m \), resp. Then we make a tree, \( T_R \), by taking a new root with \( m+1 \) outgoing edges all labelled by \( \rho \), labelling the root by \( \tilde{R} \), and connecting our root with the roots of \( T_{\tilde{Q}_0}, T_{\tilde{Q}_1}, \ldots, T_{\tilde{Q}_m} \), resp.

![Figure 1. An unfolded inductive tree for \( \tilde{R} \).](image-url)
Proposition 6.2. The restricted model checking problem RMC can be solved by an exhaustive search for an unfolded inductive tree for the query \((a, h) \in \langle P \rangle^h\), where the values for instantiated existential variables are drawn from the set \(\text{Good}(a, h) \cup \text{Spare}_a(a, h)\), as per Definition 3.2.

Proof. (Sketch) The soundness of the approach is obvious. Termination follows from the fact that the range of permissible values is finite, and completeness from the results in Section 3 which show that it suffices to confine our attention to values drawn from the polynomial-size set \(\text{Good}(a, h) \cup \text{Spare}_a(a, h)\).

However, the above procedure might still generate an exponential number of leaves labelled by the empty heap \(e\):

Example 6.3. Let \(\Phi_\rho\) be the set of inductive rules (for \(1 \leq j \leq n\)):
\[
P_1 \ast P_2 \Rightarrow P_0, \quad P_{2j+1} \ast P_{2j+2} \Rightarrow P_{2j-1}, \quad P_{2j+1} \ast P_{2j+2} \Rightarrow P_{2j},
\]
\(\text{emp} \Rightarrow P_{2n+1}, \quad \text{emp} \Rightarrow P_{2n+2}.
\]
Then any unfolded inductive tree for the query \(s, e \models \Phi_\rho\) has \(2^{n+1}\) leaves labelled by \(e\).

Nevertheless, in the case of MEM, we are able to reduce EXPTIME to NP by proving that the number of leaves labelled by \(e\) can be bounded by \(|\text{dom}(h)|\).

6.1 An Upper NP-Bound for MEM
Here, we show that, when we restrict to memory-consuming rules (MEM), model checking becomes an NP problem.

Theorem 6.4. We can design an NP procedure to determine, given a set of memory-consuming inductive rules \(\Phi\), a tuple of values \(a, h\), and predicate symbol \(P\), whether \((a, h) \in \langle P \rangle^h\).

Proof. (Sketch) Taking into account the bounds provided by Section 3, we look for an unfolded inductive tree such that within each rule instance \(\rho\) from \(\Phi\) used in the tree all values are taken only from a set of polynomial size, which is fixed in advance.

To provide an NP procedure, it suffices to prove Lemma 6.5 and Lemma 6.6 below. The crucial issue is that, in contrast to Example 6.3, the number of leaves labelled by \(e\) can be bounded by the size of \(|\text{dom}(h)|\) when all rules are memory-consuming.

Lemma 6.5. According to Section 3, \((a, h) \in \langle P \rangle^h\) iff there is an unfolded tree for the appropriately instantiated \(P\) such that \(h\) is the \(s\)-composition of all heaps labelling the leaves of the tree.

Lemma 6.6. The number of nodes in the above inductive trees for \(P\) is bounded by \(2^{(m + 1)} \cdot |\text{dom}(h)|\), where \(m\) is the maximal number of predicate symbols in the body of the rules.

Proof. It is clear that the number of leaves labelled by non-empty heaplets is bounded by \(|\text{dom}(h)|\). Let \(v\) be a leaf labelled by \(e\). Then either its parent \(w\) is the root of the tree, or the edge of the form \((v_0, w)\) incoming to \(w\) is labelled by some \(\rho\), providing thereby a leaf \(v'\) with its incoming edge \((v_0, v')\) labelled by the same \(\rho\), such that \(v'\) is labelled by a non-empty \(\bar{x} \Rightarrow t\) (Figure 2 shows such a \(\rho\) in MEM). Since no more than \(m\) leaves labelled by \(e\) can be associated with one and the same \(v'\) specified in such a way, the total number of leaves is bounded by \((m + 1) \cdot |\text{dom}(h)|\).

It remains to apply an induction to conclude the proof.

6.2 NP-Hardness for MEM + CV
Here we show NP-hardness for the restricted fragment MEM+ CV. The proof is by reduction from the 3-partition problem [21].

**Figure 2.** \(\rho = \Pi: \bar{x} \Rightarrow t \ast \bar{Q}_1 \ast \bar{Q}_2 \ast \cdots \ast \bar{Q}_m \Rightarrow R\)

Definition 6.7. By means of the length of circular lists, we resolve a key issue: representing integers as logic formulas.

By a ring-formula of length \(\ell\), with leading variable \(x\), we mean a formula of the form \((x_1, x_2, \ldots, x_\ell)\) are fresh):
\[
x \Rightarrow x_1' \ast x_1 \Rightarrow x_2' \ast x_2 \Rightarrow x_3' \ast \cdots \ast x_{\ell-1}' \Rightarrow x_\ell' \ast x_\ell \Rightarrow x_1'
\]

Given a 3-partition problem instance, i.e., a bound \(B\) and a multiset \(S = \{s_1, s_2, \ldots, s_{3m}\}\), we introduce a linear-ordered list \(X\) of distinct variables: \(X = x_1, x_2, \ldots, x_i, \ldots, x_{3m}\).

Then we encode each of the numbers \(s_i\) by a ring-formula, \(S_i(x_i)\), of length \(s_i\), with the leading variable \(x_i\).

The whole \(S\) is encoded as a concrete heap \(h_S\), which is a collection of \(3m\) disjoint “circular” lists of the form \(S_i(x_i)\).

With an appropriate stack \(s_s\), \(s_S, h_S = \Pi(X): \varphi_S(X)\), where \(\varphi_S(X) = S_1(x_1) \ast S_2(x_2) \ast \cdots \ast S_{3m}(x_{3m})\) and \(\Pi(X)\) says \((x \neq y)\) for all distinct variable names \(x\) and \(y\) mentioned, explicitly or implicitly, in \(\varphi_S(X)\).

Define a set of inductive rules \(\Phi_\rho\) as follows. To keep the predicate arities fixed and, at the same time, maintain \(i\)-th position inside the tuple \(X\), we define predicates \(Q_i(x)\) by the rules:\n
\[
x \neq \text{nil} : \text{emp} \Rightarrow Q_i(x)
\]

For \(i < j < k\), we use “goal” predicates \(R_{ijk}(x, y, z)\) with the rules:\n
\[
x \neq y, y \neq z, z \neq x : \text{emp} \Rightarrow R_{ijk}(x, y, z)
\]

In the case of \(i < j < k\) and \(s_i + s_j + s_k = B\), we add the rule:\n
\[
S_i(x) \ast S_j(y) \ast S_k(z) \ast R_{ijk}(x, y, z) \Rightarrow R_{ijk}(x, y, z)
\]

Lemma 6.8. Let \(h_S\) and \(s_S\) be defined above. Then \(s_s, h_S = \Pi(X): \bigast_{i=1}^{3m} Q_i(x) \ast \bigast_{i<j<k} R_{ijk}(x, y, z)\) iff there is a complete 3-partition on \(S\) i.e., \(S\) can be partitioned in groups of three, say \(s_i, s_j, s_k\), so that \(s_i + s_j + s_k = B\).

Proof. Each \(R_{ijk}(a_1, a_2, a_3)\) at the top is generated either by (4), with \(\text{emp}\), or by (5), with \((S_i(a_i), S_j(a_j), S_k(a_k))\) being ‘consumed’. The latter provides the corresponding group of \(s_i, s_j, s_k\).

Corollary 6.9. (a) In the case of the memory-consuming rules, the model checking problem is NP-complete (even if the arity of the predicates involved is at most 3).

(a) For the memory-consuming rules with constructively valued variables, model checking is still NP-complete (even if the arity of the predicates involved is at most 3).

Proof. This follows from Sections 6.1 and 6.2.

6.3 NP-Hardness for MEM + DET
The challenge - to simulate intrinsically non-deterministic 3-SAT by deterministic memory-consuming rules, with, moreover, keeping the arity of predicates fixed - is solved using generalised versions of the linked list segments inductively defined in Example 5.3.

Namely, within a list fragment leading from \(x\) to \(y\), by means of \(RLS(x, u, y)\), defined below, we will keep the information about the exact predecessor of the final list in the y.

---

[21]: Number of references and citations are not visible in the text. They are likely included in the context of the full document or in the references section of the original article.
Here we abbreviate $X = x_0, x_1, \ldots, x_n$, $Q = q_0, q_1, \ldots, q_t$, $\Xi = \xi_0, \xi_1, \ldots, \xi_m$. $\Pi_i = \{ x_j \neq q | j \neq i, q \in Q \} \cup \{ z \neq z' | z, z' \in Q \cup \Xi \}$

The final "empty configuration" is generated by the "backward" rule (recall that $\xi_0$ is the blank symbol, $\xi_1$ and $\xi_2$ are end markers)

$$\Pi_0, x_0 = q_0, x_1 = \xi_1, x_2 = x_3 = \cdots = x_{n-1} = \xi_0, x_n = \xi_2; \text{ emp } \Rightarrow T(X, Q, \Xi)$$

An instruction "if in state $q_i$, looking at $\xi_j$, replace it by $\xi_k$, move to the right, and go into state $r_i$" is simulated by $n$ rules (here $0 \leq i < n$):

$$\Pi_i, x_i = q_i, x_{i+1} = \xi_j, y_i = \xi_k, y_{i+1} = q_r; \; T(x_0, x_1, \ldots, x_{i-1}, y_i, y_1, x_{i+2}, \ldots, x_n, Q, \Xi) \Rightarrow T(X, Q, \Xi)$$

An instruction "if in state $q_i$, looking at $\xi_j$, replace it by $\xi_k$, move to the left, and go into state $r_i$" is simulated in a similar "backward" way.

An alternating instruction "if in state $q_i$, run two copies of the configuration in parallel but with states $q_i$ and $q_r$, resp.," is simulated by $0 \leq i < n$:

$$\Pi_i, x_i = q_i, y_i = q_r, z_i = \xi_k; \; T(x_0, x_1, \ldots, y_i, y_{i+1}, \ldots, x_n, Q, \Xi) \Rightarrow T(x_0, x_1, \ldots, z_i, x_{i+1}, \ldots, x_n, Q, \Xi)$$

**Figure 3.** Simulating a Turing machine $M$ running in space $n$, in a backward manner - "from outputs to inputs"

A linked list $RLS(x, u, y)$ is formed by attaching a new tail:

$$x \cdot y : \text{ emp } \Rightarrow RLS(x, y, x)$$

$$\exists n. x \neq z : RLS(x, u, y \cdot y) \Rightarrow RLS(y, y, z)$$

Notice that the rules for $RLS(x, u, y)$ are both memory-consuming and deterministic. The fact that $u$ is not constructively valued is a key ingredient in our reduction, which allows us to cope with the non-deterministic problem 3-SAT.

**Definition 6.10.** By means of the following heaplets $h_{ab}^{(0)}$ and $h_{ab}^{(1)}$ (here $a \neq b$) we represent the truth values, "false" and "true", resp.:

$$h_{ab}^{(0)} = \begin{cases} 
\text{a} \rightarrow \text{b} & \text{a} \rightarrow \text{b} & \text{for } \delta = 0, \\
\text{a} \rightarrow \text{b} & \text{b} \rightarrow \text{b} & \text{for } \delta = 1. 
\end{cases}$$

**Lemma 6.11.** Assuming $a \neq b$, let $h_{ab}^{(d)} \models_{RLS} RLS(a, c, b)$ for some $c$. Then: $(\delta = 0) \land (a \neq c = b)$.

**Proof.** $h_{ab}^{(d)} \models_{RLS} RLS(a, b, b)$ and $h_{ab}^{(d)} \models_{RLS} RLS(a, b, b)$.

Let $\varphi \equiv (C_1 \land \cdots \land C_m)$ be a formula of $m$ clauses over linear ordered $n$ propositional variables $p_1, p_2, \ldots, p_n$, and each $C_j$ is of the form (here, for any $q$, we denote $\overline{q} = q \land \neg q$):

$$C_j(q_1, q_2, q_3) \equiv (q_1^{(j,1)} \lor q_2^{(j,2)} \lor q_3^{(j,3)}$$

Each $C_j$ is encoded by a predicate $C_j(a_1, a_1, a_2, a_2, a_3, a_3)$ with the following rule $q_j$ (for the sake of readability, we squeeze three deterministic rules into one but without conjunction):

$$(a_1 \neq a_1) \lor (a_2 \neq a_2) \lor (a_3 \neq a_3) \lor \land_{k \neq j} (a_k \neq a_k)$$

**Example 6.12.** Here we represent $p_i$ as $x_i \neq u_i$. So satisfiability of $C(p_1, p_2, p_3)$ of the form $(p_1 \lor \neg p_2 \lor p_3)$ is reformulated as

$$(x_1 \neq u_1) \lor (x_2 = u_2) \lor (x_3 = u_3)$$

We take the following linear-ordered variables: $W = w_0, W = x_1, x_2, \ldots, x_n, U = u_1, u_2, \ldots, u_2, Y = y_1, y_2, \ldots, y_2$

The challenge - to maintain the arity fixed and, at the same time, to "keep i-th position" inside the long $X, U, Y$ is solved by taking predicates $Q_i(x, u, y)$ with the rules $\kappa_i$:

$$x \neq y \land \text{ emp } \Rightarrow Q_i(x, u, y) \land x \neq y \land \text{ emp } \Rightarrow Q_i(x, u, y)$$

The key points of reduction are encapsulated in the rule $\omega_{ab}$:

**Lemma 6.14.** With the empty input tuple of values,

$$((\cdot), h_{ab} \circ H_\alpha) \models_{RLS} \omega_{ab} \cup \mathcal{RLS} \cup \{ \xi_0 \uplus U_i, \kappa_1 \uplus U_i, \kappa_2 \uplus U_i \}$$

If and only if $(C_1 \land \cdots \land C_m)$ is satisfiable.

**Proof.** (Sketch) The $(\Rightarrow)$ direction is the hardest. Suppose that $(\cdot)$ is valid. Then $\omega_{ab}$ is generated by $\omega_{ab}$ with an unfolded inductive tree for $\omega$: We can show that, for some values $a_1, a_2, \ldots, a_2, c_1, c_2, \ldots, c_2, d_1, d_2, \ldots, d_2$, the heap $H_{ab}$ can be partitioned into $2n$ disjoint heaplets of the form $h_{ab}^{(d)}$, so that we get the following:

$$h_{ab}^{(d)} \models_{RLS} RLS(a_1, c_1, b_1).$$

Now, using the rules $\xi_1$ and $\kappa_1$, and Lemma 6.11, we can prove the desired satisfiability (see also Example 6.12): $\varphi(\delta_1, \delta_2, \ldots, \delta_n, 1) = 1$

The $(\Leftarrow)$ direction follows essentially by reading the above line of reasoning "bottom-up".

**Corollary 6.15.** For deterministic and memory-consuming rules, model checking is still NP-complete (even if the arity of the predicates involved is at most 6).

6.4 PSPACE- and EXPSPACE-Hardness for Non-MEM Rules

Unexpectedly, with non-memory-consuming rules, such as

$$\exists i. \; Q_i u_1, u_2, \ldots, Q_m u_m \Rightarrow F$$

model checking becomes more complex. Namely:

**Theorem 6.16.** (a) For inductive rule sets in $CV$, model checking is EXPSPACE-complete.

(b) For inductive rule sets in $CV + DET$, model checking is PSPACE-hard.

(c) For inductive rule sets in $CV + DET$, model checking is EXPSPACE-complete.

**Proof.** (Sketch) We prove all three lower bounds by simulating Turing machines in a backward manner - "from outputs to inputs".

Let $M$ be a Turing machine that accepts in space $n$, with states $q_0, q_1, \ldots, q_t$, and tape symbols $\xi_0, \xi_1, \ldots, \xi_n$. Here $\xi_1$ is the initial state, $\xi_0$ is an accept state, $\xi_n$ is the blank symbol, and $M$ acts in the space $n$ between two unused markers, say $\xi_1$ and $\xi_2$. Let $M$ always jump, and no $M$’s instruction starts with $q_0$. By $(\eta_1, \eta_2, \ldots, \eta_n, \eta_0, \eta_0, \eta_0, \eta_0)$ we formalize that "in state $\xi_0$, $M$ scans i-th square, when $\eta_1, \eta_2, \ldots, \eta_n, \eta_0$ is printed on its tape". We encode $M$ by means of the rules $\Phi_M$ given in Figure 3, where the "tape" predicate $T$ depicts $M$’s configurations:

$$T(x_0, x_1, \ldots, x_n, q_0, q_1, \ldots, q_t, \xi_0, \xi_1, \xi_2)$$

**Lemma 6.17.** Let $M$ be a deterministic TM or an alternating TM [15]. Then $s, e \models \Phi_M T(q_0, \xi_1, \xi_0, \xi_0, \xi_0, \xi_2, Q, \Xi)$ if and only if $M$ can go from the initial "empty configuration" to the final "empty configuration".


All variables in $\Phi_{M}$ occur in $Q \cup \mathbf{Q} \cup \mathbf{E}$, hence, they are constructively valued, which provides item (a) in Theorem 6.16.

Whenever $M$ is deterministic, $\Phi_{M}$ is deterministic, which provides item (b) in Theorem 6.16.

To answer the challenging (c), $M$'s non-deterministic instruction “if in state $\bar{q}_{i}$ looking at $\xi_{o}$, go either into $\bar{q}_{i+1}$ or into $\bar{q}_{i+2}$” is simulated by the deterministic rules (here $0 \leq i < n$, $\ell = 1, 2$):

$$\exists y. \Pi_{1}, x_{i} = x_{i+1} = \xi_{o}, y \notin \Xi, y_{i+1} = \xi_{o}(x_{i+1}), T(x_{0}, \ldots, x_{i+1}, y, y_{i+1}, x_{i+2}, \ldots, x_{n}, Q, \Xi) \Rightarrow T(X, Q, \Xi), \Pi_{2}, x_{i} = x_{i+2} = \xi_{o}(x_{i+1}), y_{i+1} = \xi_{o}, T(x_{0}, \ldots, x_{i+1}, y_{i+1}, x_{i+2}, \ldots, x_{n}, Q, \Xi) \Rightarrow T(X, Q, \Xi)$$

where, however, $y$ is not constructively valued. The idea behind the encoding is as follows. First, $M$ goes non-deterministically into any state $y$, with encrypting the theory by a special ‘double’ $\xi_{o}(x_{i+1})$. To continue a computation, the lucky guess should be one of our specially introduced states $\bar{q}_{i+1}$ and $\bar{q}_{i+2}$. As a result, $M$ finishes either in $\bar{q}_{i+1}$ or in $\bar{q}_{i+2}$.

Remark 6.18. The above EXPTIME-hardness necessarily employs predicates of unbounded arity (cf. Remark 5.1).

6.5 Polynomial Time for MEM+CV+DET

We next show that the model checking problem is in PTIME whenever $\Phi$ is in MEM+CV+DET. Essentially, predicates in CV+DET make a top-down procedure fully deterministic; and, the size of any possible proof is linear in the size of the heap, if $\Phi$ is in MEM.

Where $h$ is a heap and $v$ is a value such that $v \in \text{dom}(h)$, we write $h \downarrow v$ to denote the heap $h'$ that has domain $\text{dom}(h) \setminus v$ and agrees with $h$ on its domain. This operation is lifted in the obvious way to sets of values, i.e., $h \downarrow V$ where $V \subseteq \text{dom}(h)$.

Definition 6.19. The construct $s, h \vdash_{\Phi} A \leadsto h'$ is called a reduction, where $s$ is a stack, $h, h'$ are heaps and $A$ is a symbolic heap with inductive predicate occurrences defined in $\Phi$. We say that the above reduction is valid if $h' \subseteq h$ and $s, h \vdash_{\Phi} \text{dom}(h') \vdash_{\Phi} A$.

Figure 4 presents a proof system for reductions. A proof is, as usual, a tree whose leaves are labelled by axioms and internal nodes are labelled by inference rules accordingly. We say that a reduction $R$ is provable if there exists a proof whose root is labelled by $R$.

Lemma 6.20. (Soundness) For any set of rules $\Phi$, formula $A$, stack $s$ and heap $h$, if $s, h \vdash_{\Phi} A \leadsto h'$ is provable then it is valid.

Proof. Follows by induction over the structure of the proof.

We recall the notion of precision: a formula $A$ is precise iff for every stack $s$ and heap $h$, there is at most one $h'' \subseteq h$ such that $s, h \vdash_{\Phi} A \leadsto h''$.

Lemma 6.21. (Completeness) For any set of rules $\Phi$ and formula $A$ that are in $\mathbf{C}$, and any stack $s$ and heap $h$, if $s, h \vdash_{\Phi} A \leadsto h'$ is valid then it is provable.

Proof. We proceed by well-founded induction over $(R, \prec)$, i.e., we show that if all $R' \in R$ such that $R' \prec R$ are provable, then so is $R \in R$.

Let $R \in R$ be the reduction $s, h \vdash_{\Phi} \exists \mathbf{V} : A \leadsto h'$. As $R$ is constructively valued, there must be some variable $x \in v$ such that (i) there is a free variable $y$ such that $x = y$ is a subformula of $A$, or (ii) $x$ appears in the right-hand side of a subformula $y \mapsto t$ of $A$. Let $z \equiv_{	ext{def}} v \setminus \{x\}$. As $R$ is valid we have $h' \subseteq h$ and $s, h \vdash_{\Phi} \text{dom}(h') \vdash_{\Phi} \exists \mathbf{V} : A$, thus there is a stack $s'$ such that $s'(\text{FV}(\exists \mathbf{V} : A)) = s(\text{FV}(\exists \mathbf{V} : A))$ and $s', h \vdash_{\Phi} \text{dom}(h') \vdash_{\Phi} \exists \mathbf{V} : A$. If clause (i) is true then clearly $s'(x) = s(y)$ by the semantics of $\equiv$, and $s'(y) = s(y)$ as $y$ is free. Thus without loss of generality we can set $s' = s[x \mapsto s(y)]$. Therefore the reduction $R' \equiv s[x \mapsto s(y)], h \vdash_{\Phi} \exists \mathbf{V} : A \leadsto h'$ is valid and constructively valued. It is easy to see that $R'$ must be $\alpha$-supported (otherwise we can derive a contradiction with the assumption that $\alpha$ is the least such ordinal), thus $R' \prec R$ by clause (2c) of the definition of $\prec$. By the inductive hypothesis, $R'$ is provable and the rule $(\exists \mathbf{V})$ can be applied, thus proving $R$. Clause (ii) is similar and uses $(\exists \mathbf{V})$.

Next, let $R \in R$ be of the form $s, h \vdash_{\Phi} x = y$, $\Pi : F \leadsto h'$, thus, $h' \subseteq h$ and $s, h \vdash_{\Phi} \text{dom}(h') \vdash_{\Phi} x = y, \Pi : F$. It is easy to see that the reduction $R' \equiv s, h \vdash_{\Phi} F : F \leadsto h'$ is valid, constructively valued and $\alpha$-supported. By clause (2a) of the definition of $\prec$ it follows that $R' \prec R$. Thus by the inductive hypothesis, $R'$ is provable and the rule $(=)$ applies, therefore $R$ is also provable. Disequalities are treated similarly via the rule $(\neq)$.

Now, let $R \in R$ be of the form $s, h \vdash_{\Phi} x \neq F \leadsto h'$. Thus, $h' \subseteq h$ and $s, h \vdash_{\Phi} \text{dom}(h') \vdash_{\Phi} \exists \mathbf{V} : F$. Therefore there are two disjoint heaps $h_{a}, h_{F}$ such that $h' \equiv_{\Phi} h_{a} \circ h_{F}$ and $s, h_{a} \vdash_{\Phi} \exists \mathbf{V} : F$ and $s, h_{F} \vdash_{\Phi} \exists \mathbf{V} : F$, where $\alpha = \max\{\alpha_{a}, \alpha_{F}\}$. Thus $h = h_{a} \circ h_{F}$ or $h_{a} \circ h_{F}$ and $s, h \vdash_{\Phi} \text{dom}(h') \vdash_{\Phi} \exists \mathbf{V} : F$ and $s, h \vdash_{\Phi} \exists \mathbf{V} : F$ for $F' \subseteq h'$ are both valid and constructively valued. In addition, $R_{s} : h_{F} \preceq_{\Phi} F \leadsto s(t) (\text{equality of tuples}), \alpha' < \alpha$. Trivially, $s', h \vdash_{\Phi} \text{dom}(h') \vdash_{\Phi} \exists \mathbf{V} : F$. Thus the query $R' \equiv s', h \vdash_{\Phi} \exists \mathbf{V} : F \leadsto h'$ is valid, constructively valued and $\alpha'$-supported. By the inductive hypothesis, $R'$ is provable and therefore so is $R$ by applying $(P_{t})$.

The cases for $\rightarrow$, emp easily treated with rules $(\rightarrow\rightarrow), (\ell)$. 

We recall the notion of precision: a formula $A$ is precise iff for every stack $s$ and heap $h$, there is at most one $h'' \subseteq h$ such that $s, h \vdash_{\Phi} A \leadsto h''$. Precision entails that if $s, h \vdash_{\Phi} A \leadsto h'$ is valid then there is no other $h'' \not= h'$ such that $s, h \vdash_{\Phi} A \leadsto h''$ is valid. Thus precision allows the deterministic application of $(\ast)$.

Lemma 6.22. Let $\Phi$ be a set of rules in $\mathbf{C}+\mathbf{V}+\mathbf{D}$. Then any formula in $\mathbf{C}$ using predicates defined in $\Phi$ is precise.

Proof. Observe the following points: if $\Sigma$ and $\Sigma'$ are precise then so is $\Sigma \ast \Sigma'$; if $\Sigma$ is precise then so is $\Pi : \Sigma$; for any $\Pi$; if $\Pi : \Sigma$ is precise then so is $A \equiv_{\mathbf{V}} \Pi$ ($\Pi : \Sigma$), provided all variables in $\mathbf{V}$ are constructively valued in $\mathbf{A}$. Finally, note that the problem reduces to guaranteeing that every formula of the form $P_{t}$ is precise.

Thus we need to show that for every tuple of values $a$ and heap $h$ there is at most one $h' \subseteq h$ such that $h_{1} \neq h_{2}$ and $(a, h_{1}), (a, h_{1}) \in$ $[P_{t}]^{\mathbf{A}}$.
\[ s(x) = s(y) \quad s, h \vdash \Phi \colon F \rightsquigarrow h' \]  
\[ s(x) \neq s(y) \quad s, h \vdash \Phi \colon F \rightsquigarrow h' \]  
\[ s(x) \in \text{dom}(h) \quad h(s(x)) = s(t) \]  
\[ s, h \vdash \Phi \colon x = y, \Pi \colon F \rightsquigarrow h' \]  
\[ s, h \vdash \Phi \colon x \neq y, \Pi \colon F \rightsquigarrow h' \]  
\[ s, h \vdash \sigma \rightsquigarrow h' \quad s, h' \vdash \Phi \rightsquigarrow h'' \]  
\[ x \in \mathbf{v} \quad y \notin \mathbf{v} \quad s(y) \in \text{dom}(h) \quad \exists i, t \quad \exists x \quad s(x \mapsto h(s(y)), x), h \vdash \exists (v \setminus \{x\}), (x = y, \Pi : F) \rightsquigarrow h' \]  
\[ s, h \vdash \exists v. (\Pi : F \mapsto t) \rightsquigarrow h' \]

Figure 4. Proof rules for reductions. The formula \( \sigma \) in the rule (\( \ast \)) is atomic.

\[ \bigcup_{i,j} \varphi_{i,j}(Y). \] As the rules are precise there must be \( k \neq l \) such that \((a, h_1) \in \varphi_{i,k}(Y)\) and \((a, h_2) \in \varphi_{i,l}(Y)\). This, however, directly contradicts determinism.

Finally, we establish that proof search is a deterministic, terminating decision procedure when all predicates are in \( \text{CV}+\text{DET} \); and, its runtime is naturally bounded by a polynomial in the input size, if in addition, all rules are in \( \text{MEM} \).

**Theorem 6.23.** Let \( A \) be a formula in \( \text{CV} \) and \( \Phi \) a set of rules in \( \text{MEM}+\text{CV}+\text{DET} \). Then, for any stack \( s \) and heap \( h \), checking whether \( s, h \models \Phi \) can be performed in polynomial time.

**Proof.** First, note that \( s, h \models \Phi \) iff \( s, h \vdash \Phi \) \( \Rightarrow \) \( s, e \vdash \Phi \) is provable. Observe that the structure of a given reduction dictates that there is at most one applicable rule from Fig. 4. Rules about quantifiers, (\( \exists _{\omega} \)) and (\( \exists _{\omega} \)), form an exception but the order of their applications, as well as the choice of quantified variable to eliminate next, is immaterial to the provability of a CV reduction, thus a fixed order can be used.

As \( \Phi \) is in \( \text{DET} \), (\( P_i \)) can be used with at most one rule and this rule can be found in polynomial by evaluating the side condition of (\( P_i \)) for all rules. This means no back-tracking is required over \( \Phi \).

The rule (\( \ast \)) resembles a cut in that the intermediate heap \( h' \) does not appear in the conclusion. This can be seen as a source of non-determinism as many choices for \( h' \) may have to be checked (due to the fact that \( h' \subseteq h \)). However, as all formulas involved are precise (Lemma 6.22) if there is such a heap \( h' \) it is unique. In addition, observe that only axioms impose constraints on the RHS heap. Thus, we avoid back-tracking by using meta-variables for the heap \( h' \) and order the proof search to first prove the left-hand subgoal of (\( \ast \)). If the left subgoal of (\( \ast \)) is proven, then \( h' \) is instantiated by axioms and the search continues in the right subgoal of (\( \ast \)). Otherwise, the goal reduction is clearly invalid.

These observations together guarantee that the proof search is fully deterministic.

Now, for \( \text{MEM} \) rules each application of (\( P_i \)) leads to at least one subgoal that requires (\( \rightarrow \)), and there cannot be more instances of (\( \rightarrow \)) in a proof than the size of the heap \( h \) in the root reduction. Thus the size of the proof is \( O(|h|) \), and as the search is deterministic, runtime is linear as well.

**Remark 6.24.** Deciding intuitionistic queries (cf. Remark 3.12) in \( \text{MEM}+\text{CV}+\text{DET} \) can be done in \( \text{PTIME} \). This follows easily by noting that the proof search described in Theorem 6.23 actually computes a heap for the RHS of any reduction. Given the precision of the formulas involved (Lemma 6.22), this means that we can answer correctly intuitionistic queries using the same algorithm.

7. Implementation and Evaluation

We implemented the general model checking algorithm described in Section 3 as well as the \( \text{CV}+\text{DET} \) algorithm described in Section 6.5, in about 1400 lines of OCaml code. Our implementation is part of the CYCLIST theorem proving framework [13] which provides support for inductive definitions, and in particular for our logic \( \text{SL}\text{\textsuperscript{\text{DET}}} \). Both model checking algorithms are parameterised over the datatypes for heap locations and ground values (e.g. integers, booleans, strings, etc.) and thus may be instantiated to handle models where heap locations have arbitrary representations (e.g. hex strings) and heap cells contain arbitrary data. We employed a number of techniques to improve the efficiency of the implementation, including pre-computing the models for points-to subformulas, using hashsets to store submodels, and using bit vectors to represent heaps. We also implemented the intuitionistic version of our algorithms as per Remark 3.12 and Remark 6.24. The code and test suite for our tool are available online [1].

We tested the performance of our implementation across a range of ‘typical’ predicate definitions gathered from the verification community, and a number of hand-crafted definitions designed to elicit the worst-case, exponential performance. We extracted models from a number of example programs at runtime using an extension of GDB which supports scripting using Python [2]. All tests were carried out on a 2.93GHz Intel Core i7-870 processor with 8GB RAM.

We note that all tests carried out were on positive instances. This was decided for two reasons. First, the worst-case performance can be exhibited with positive instances as shown below. Second, when using runtime checks, for instance in code contracts or offline test suites, negative instances usually lead to program termination because they indicate that some pre- or postcondition, or invariant is no longer satisfied. Thus the runtime on positive instances is a much more important measure of performance.

‘Typical’ Performance. Testing our implementation against typical, real-world data requires sourcing programs annotated with separation logic assertions. We identified 6 programs from the suite of examples in the Verifast distribution [24] containing non-trivial inductive predicates which translate into our assertion language: (i) **stack.c**: a stack data-structure implemented using linked lists. (ii) **queue.c**: a lock-free concurrent queue based on list segments. (iii) **set.c**: a concurrent set data-structure based on linked lists. (iv) **schorr-waite.c**: an implementation of the Schorr-Waite graph marking algorithm over binary trees. (v) **iter.c**: a list data-structure with an iterator pointing into the list. (vi) **composite.c**: an example of the composite design pattern, where each node of a tree must maintain local data consistent with a global property.
The assertions we collected cover most combinations of the syntactic restrictions defined in Section 5. The first four programs use standard list segment and tree predicates, all of which are $\text{MEM+CV+DET}$ from $\text{iter.c}$ which uses a non-DET predicate (describing a possibly cyclic list). The predicate describing the set data-structure in $\text{set.c}$ is in $\text{MEM+DET}$, but is not in $\text{CV}$. The models we tested for the Schorr-Waite algorithm were taken from the entry and exit points and the start of each loop iteration. The precondition is $\text{MEM+CV+DET}$, although the postcondition is not $\text{CV}$. The loop condition given in the Verifast code is $\text{CV}$ but not $\text{MEM}$ or $\text{DET}$, and we also checked against a natural ‘simplified’ version, obtained by a predicate fold, which falls outside all the restrictions. For the iterator example one of the three formulas we model checked against is $\text{MEM+CV+DET}$, while the others are only $\text{MEM}$. The $\text{composite.c}$ example uses ‘non-standard’ predicates, making essential use of non-DFT and non-CV rules: we checked against one formula $\text{MEM+CV}$, and the other in the general EXPTIME fragment.

From each program we extracted models with heaps containing 0–100 cells, with each cell containing 1–4 data values. We extracted over 2150 models in total, covering 15 different assertions across various program points. The results of our model checking tests of the general algorithm can be seen in Figures 5(a) and 5(b). Where we were able to collect a number of non-isomorphic models per heap size, we show both the minimum and maximum times observed for model checking. In Figure 5(a), where we give a result for a range of heap sizes, this represents the maximum time observed over that range. All times are given in milliseconds, and averaged over 3 test runs. Where runtimes are not given, this indicates that we elected not to check models of the corresponding size due to the length of time required to obtain an answer; in these cases we felt that the data we collected was sufficient to analyse the performance of the algorithm.

The results, e.g. for $\text{set.c}$ and the $\text{schorr-waite.c}$ postcondition, clearly show the exponential nature of the general algorithm. The maximum times observed for the $\text{schorr-waite.c}$ loop invariants display a similar profile, although the large variation between minimum and maximum times shows that the particular shape of the model being checked also has a large influence.

(a) Tests using single model per heap size
(b) Tests using multiple models per heap size
(c) Spatial True Encoding

Figure 5. Test results of fixed point model checking algorithm (all times in milliseconds)
the 4-bit counter in just over 6 minutes; the 5-bit counter had not returned a value after 20 hours.

8. Conclusions

Our main contribution in this paper is a general fixed point algorithm that decides model checking in symbolic-heap separation logic with user-defined inductive predicates. Furthermore, we show that while model checking for this logic is EXPTIME-complete in the general case, it can be made NP-complete and even polynomial by restricting the admissible definitions of inductive predicates in various natural (syntactic) ways. Finally, we implement two algorithms, the general one described in Section 3 and the algorithm for the CV+DET fragment, described in Section 6.5.

The performance of the CV+DET algorithm is good enough for runtime verification, when additionally the rules employed are memory-consuming. This, however, significantly restricts the kinds of properties that can be checked during program execution. As evidenced by the complex properties found in the Verifast examples, the general model checking algorithm can usefully extend the expressiveness available to the programmer; its performance may not be appropriate for verification during execution, but it can still be used productively in offline testing such as in unit tests.

The ability to model-check formulas also opens up the possibility of disproving entailments in our logic via the direct generation and testing of possible countermodels, in contrast e.g. to the approach based on overapproximation in [12]. We are uncertain as to the scalability of such an approach, but nevertheless consider it an interesting avenue for potential future work. Another possibility includes employing SAT solvers for deciding model-checking of rule sets that fall within the MEM+DET or MEM+CV fragments.

Acknowledgements. We wish to thank the anonymous referees for their comments, which have enabled us to improve the presentation of the paper. Thanks also to Matt Parkinson for pointing us towards the Verifast benchmarks.

Brotherston is supported by an EPSRC Career Acceleration Fellowship, and Kanovich and Rowe by EPSRC grant EP/K040049/1.

References