Structuring the Synthesis of Heap-Manipulating Programs

NADIA POLIKARPOVA, University of California, San Diego, USA
ILYA SERGEY, Yale-NUS College, Singapore and University College London, UK

This paper describes a deductive approach to synthesizing imperative programs with pointers from declarative specifications expressed in Separation Logic. Our synthesis algorithm takes as input a pair of assertions—a pre- and a postcondition—which describe two states of the symbolic heap, and derives a program that transforms one state into the other, guided by the shape of the heap. The program synthesis algorithm rests on the novel framework of Synthetic Separation Logic (SSL), which generalises the classical notion of heap entailment \( P \vdash Q \) to incorporate a possibility of transforming a heap satisfying an assertion \( P \) into a heap satisfying an assertion \( Q \). A synthesized program represents a proof term for a transforming entailment statement \( P \leadsto Q \), and the synthesis procedure corresponds to a proof search. The derived programs are, thus, correct by construction, in the sense that they satisfy the ascribed pre/postconditions, and are accompanied by complete proof derivations, which can be checked independently.

We have implemented a proof search engine for SSL in a form the program synthesizer called SuSLik. For efficiency, the engine exploits properties of SSL rules, such as invertibility and commutativity of rule applications on separate heaps, to prune the space of derivations it has to consider. We explain and showcase the use of SSL on characteristic examples, describe the design of SuSLik, and report on our experience of using it to synthesize a series of benchmark programs manipulating heap-based linked data structures.

1 INTRODUCTION

Consider the task of implementing a procedure \( \text{swap}(x, y) \), which swaps the values stored in two distinct heap locations, \( x \) and \( y \). The desired effect of \( \text{swap} \) can be concisely captured via pre/postconditions expressed in Separation Logic (SL)—a Hoare-style program logic for specifying and verifying stateful programs with pointers (O’Hearn et al. 2001; Reynolds 2002):

\[
\{ x \mapsto a \ast y \mapsto b \} \quad \text{void} \quad \text{swap}(\text{loc } x, \text{ loc } y) \quad \{ x \mapsto b \ast y \mapsto a \} \tag{1}
\]

This specification is declarative: it describes what the heap should look like before and after executing \( \text{swap} \) without saying how to get from one to the other. Specifically, it states that the program takes as input two pointers, \( x \) and \( y \), and runs in a heap where \( x \) points to an unspecified value \( a \), and \( y \) points to \( b \). Both \( a \) and \( b \) here are logical (ghost) variables, whose scope captures both pre- and postcondition (Kleymann 1999). Because these variables are ghosts, we cannot use them directly to update the values in \( x \) and \( y \) as prescribed by the postcondition; the program must first “materialize” them by readings them into local variables, \( a_2 \) and \( b_2 \) (cf. lines 2–3 of the code on the right). In our minimalistic C-like language, \text{loc} denotes untyped pointers, and \text{let} introduces a local dynamically-typed variable. Unlike in C, both formals and locals are immutable (the only mutation is allowed on the heap).

As a result of the two reads, the ghost variables in the postcondition can now be substituted with equal program-level variables: \( x \mapsto b_2 \ast y \mapsto a_2 \). This updated postcondition can be realized by the two writes on lines 4–5, which conclude our implementation, so the whole program can now be verified against the specification (1).

Having done this exercise in program derivation, let us now observe that the SL specification has been giving us guidance on what effectful commands (e.g., reads and writes) should be emitted next. In other words, the synthesis of \( \text{swap} \) has been governed by the given specification in the same way...
the proof search is guided by a goal in ordinary logics. In this work, we make this connection explicit and employ it for efficiently synthesizing imperative programs from SL pre- and postconditions.

Motivation. The goal of this work is to advance the state of the art in synthesizing provably correct heap-manipulating programs from declarative functional specifications. Fully-automated program synthesis has been an active area of research in the past years, but recent techniques mostly targeted simple DSLs (Gulwani et al. 2011; Le and Gulwani 2014; Polozov and Gulwani 2015) or purely functional languages (Feser et al. 2015; Kneuss et al. 2013; Osera and Zdancewic 2015; Polikarpova et al. 2016). The primary reason is that those computational models impose strong structural constraints on the space of programs, either by means of restricted syntax or through a strong type system. These structural constraints enable the synthesizer to discard many candidate terms a-priori, before constructing the whole program, leading to efficient synthesis.

Low-level heap-manipulating programs in general-purpose languages like C or Rust lack inherent structural constraints wrt. control- and data-flow, and as a result the research in synthesizing such programs has been limited to cases when such constraints can be imposed by the programmer. From the few existing approaches we are aware of, SIMPL (So and Oh 2017) and IMPSYNTH (Qiu and Solar-Lezama 2017) require the programmer to provide rather substantial sketches of the control-flow structure, which help restrict the search space; Jennisys by Leino and Milicevic (2012) can only handle functions that construct and read from data structures, but do not allow for destructive heap updates, which are necessary for, e.g., deallocating, modifying, or copying a linked data structure.

Key Ideas. Our theoretical insight is that the structural constraints missing from an imperative language itself, can be recovered from the program logic used to reason about programs in that language. We observe that synthesis of heap-manipulating programs can be formulated as a proof search in a generalized proof system that combines entailment with Hoare-style reasoning for unknown programs. In this generalized proof system, a statement $P \vdash Q$ means that there exists a program $c$, such that the Hoare triple $\{P\} \ c \ {Q}$ holds; the witness program $c$ serves as a proof term for the statement. In order to be useful, the system must satisfy a number of practical restrictions. First, it should be expressive enough to (automatically) verify the programs with non-trivial heap manipulation. Second, it should be restrictive enough to make the synthesis problem tractable. Finally, it must ensure the termination of the (possibly recursive) synthesized programs, to avoid vacuous proofs of partial correctness.

In this paper we design such a generalized proof system based on the symbolic heap fragment of malloc/free Separation Logic\(^1\) with inductive predicates, to which we will further refer as just Separation Logic or SL (O’Hearn et al. 2009; Reynolds 2002). Separation Logic has been immensely successful at specifying and verifying many kinds of heap-manipulating programs, both interactively and automatically (Appel et al. 2014; Berdine et al. 2011; Charguéraud 2010; Chen et al. 2015; Chin et al. 2012; Chlipala 2011; Distefano and Parkinson 2008; Nanevski et al. 2010; Piskac et al. 2014a), and is employed in modern symbolic execution tools (Berdine et al. 2005; Rowe and Brotherston 2017). We demonstrate how to harness all this power for program synthesis, devise the corresponding search procedure and apply it to synthesize a number of non-trivial programs that manipulate linked data structures. Finally, we show how to exploit laws of SL and properties of our proof system to prune the search space and make the synthesis machinery efficient for realistic examples.

Contributions. The central theoretical contribution of the paper is Synthetic Separation Logic (SSL): a system of deductive synthesis rules, which prescribe how to decompose specifications for complex programs into specifications for simpler programs, while synthesizing the corresponding computations compositionally. In essence, SSL is a proof system for a new transformation judgment

---

\(^1\)This nomenclature is due to Cao et al. (2017), who provide it as a rigorous alternative to the folklore notion of classical SL.
\( \mathcal{P} \rightarrow \mathcal{Q}\) c (reads as “the assertion \( \mathcal{P} \) transforms into \( \mathcal{Q} \) via a program \( c \)”), which unifies SL entailment \( \mathcal{P} \vdash \mathcal{Q} \) and verification \( \{ \mathcal{P} \} c \{ \mathcal{Q} \} \), with the former expressible as \( \mathcal{P} \rightarrow \mathcal{Q} \) \( \text{skip} \).

The central practical contribution is the design and implementation of SuSLik—a deductive synthesizer for heap-manipulating programs, based on SSL. SuSLik takes as its input a library of inductive predicates, a (typically empty) list of auxiliary function specifications, and an SL specification of the function to be synthesized. It returns a—possibly recursive, but loop-free—program (in a minimalistic C-like language), which provably satisfies the given specification.

Our evaluation shows that SuSLik can synthesize all structurally-recursive benchmarks from previous work on heap-based synthesis (Qiu and Solar-Lezama 2017), without any sketches and in most cases much faster. To the best of our knowledge, it is also the first synthesizer to automatically discover the implementations of copying linked lists and trees, and flattening a tree to a list.

The essence of SuSLik’s synthesis algorithm is a backtracking search in the space of SSL derivations. Even though the structural constraints (i.e., the shape of the heap) embodied in the synthesis rules already prune the search space significantly (as shown by our swap example), a naïve backtracking search is still impractical, especially in the presence of inductive heap predicates. To eliminate redundant backtracking, we develop several principled optimizations. In particular, we draw inspiration from focusing proof search (Pfenning 2010) to identify invertible synthesis rules that do not require backtracking, and exploit the frame rule of SL, observing that the order of rule applications is irrelevant whenever their subderivations have disjoint footprints.

Paper outline. In the remainder of the paper we give an overview of the reasoning principles of SSL, describe its rules and the meta-theory, outline the design and implementation of our synthesis tool, present the optimizations and extensions of the basic search algorithm, and report on the evaluation of the approach on a set of case studies involving various linked structures, concluding with a discussion of limitations and a comparison to the related work.

2 Deductive Synthesis from Separation Logic Specifications

In Separation Logic, assertions capture the program state, represented by a symbolic heap. An SL assertion (ranged over by symbols \( \mathcal{P} \) and \( \mathcal{Q} \) in the remainder of the paper) is customarily represented as a pair \( \{ \phi; \mathcal{P} \} \) of a pure part \( \phi \) and a spatial part \( \mathcal{P} \). The pure part (ranged over by \( \phi \), \( \psi \), \( \xi \), and \( \chi \)) is a quantifier-free boolean formula, which describes the constraints over symbolic values (represented by variables \( x, y, \) etc). The spatial part (denoted \( \mathcal{P}, \mathcal{Q}, \) and \( \mathcal{R} \)) is represented by a collection of primitive heap assertions describing disjoint symbolic heaps (heaplets), conjoined by the separating conjunction \( \ast \), which is commutative and associative (Reynolds 2002). For example, in the assertion \( \{ a \neq b; x \mapsto a * y \mapsto b \} \) the spatial part describes two disjoint memory cells that store symbolic values \( a \) and \( b \), while the pure part states that these values are distinct.

Our development is agnostic to the exact logic of pure formulae, as long as it is decidable and supports standard Boolean connectives and equality.\(^2\) Our implementation uses the quantifier-free logic of arrays, uninterpreted functions, and linear integer arithmetic, which is efficiently decidable by SMT solvers, and sufficient to express all examples in this paper.

To begin with our demonstration, the only kinds of heaplets we are going to consider are the empty heap assertion \( \text{emp} \) and points-to assertions of the form \( \langle x, i \rangle \mapsto e \), where \( x \) is a symbolic variable or pointer constant (e.g., \( 0 \)), \( i \) is a non-negative integer offset (necessary to represent records and arrays) and \( e \) is a symbolic value, stored in a memory cell, addressed via a value of \( \langle x + i \rangle \).\(^3\) In most cases, the offset is \( 0 \), so we will abbreviate heap assertions \( \langle x, 0 \rangle \mapsto e \) as \( x \mapsto e \).

\(^{2}\)We require decidability for making the synthesis problem tractable, but it is not required for soundness of the logic.

\(^{3}\)Further in the paper, we will extend the language of heap assertions to support memory blocks (arrays) with explicit memory management, as well as user-defined inductive predicates.
Our programming component (to be presented formally in Sec. 3) is a simple imperative language, supporting reading from pointer variables to (immutable) local variables (let \( x = *y \)), storing values into pointers (\(*y = x\)), conditionals, recursive calls, and pure expressions. The language has no return statement; instead, a function stores its result into an explicitly passed pointer.

2.1 Specifications for Synthesis

A synthesis goal is a triple \( \Gamma; P \leadsto Q \), where \( \Gamma \) is an environment, i.e., a set of immutable program variables, \( P \) is a precondition (pre), and \( Q \) is a postcondition (post). Solving a synthesis goal means to find a program \( c \) and a derivation of the SSL assertion \( \Gamma; P \leadsto Q \mid c \). To avoid clutter, we employ the following naming conventions:

(a) the symbols \( P, \phi, \) and \( P \) refer to the goal’s precondition, its pure, and spatial part;

(b) similarly, the symbols \( Q, \psi, \) and \( Q \) refer to the goal’s postcondition, its pure and spatial part;

(c) whenever the pure part of a SL assertion is true \( (T) \), it is omitted from the presentation.

In addition to these conventions, we will use the following macros to express the scope and the quantification over variables of a goal \( \Gamma; \{P\} \leadsto \{Q\} \). First, by \( \text{Vars} (A) \) we will denote all variables occurring in \( A \), which might be an assertion, a logical formula, or a program. Ghosts (universally-quantified logical variables), whose scope is both the pre and the post, are defined as \( \text{GV} (\Gamma, P, Q) = \text{Vars} (P) \setminus \Gamma \). Goal existentials are defined as \( \text{EV} (\Gamma, P, Q) = \text{Vars} (Q) \setminus (\Gamma \cup \text{Vars} (P)) \). For instance, taking \( \Gamma = \{x\}, P = \{x \neq y; x \mapsto y\}, Q = \{x \mapsto z\} \), we have the ghosts \( \text{GV} (\Gamma, P, Q) = \{y\} \), the existentials \( \text{EV} (\Gamma, P, Q) = \{z\} \), and the pure part of the post \( Q \) is implicitly true.

2.2 Basic Inference Rules

To get an intuition on how to represent program synthesis as a proof derivation in SSL, consider Fig. 1, which shows four basic rules of the logic, targeted to synthesize programs with constant memory footprint (remember that we use \( P \) and \( Q \) for the entire pre/post in a rule’s conclusion!).

The Emp rule is applicable when both pre and post’s spatial parts are empty. It requires that no existentials remains in the goal, and the pure pre implies the pure post (per our assumptions on the logic, the validity of this implication is decidable, so we can check it algorithmically). Emp has no synthesis subgoals among the premises (making it a terminal rule), and no computational effect: its witness program is simply skip.
The Read rule turns a ghost variable $a$ into a program variable $y$ (fresh in the original goal). That is, the newly assigned immutable program variable $y$ is added to the environment of the sub-goal, and all occurrences of $a$ are substituted by $y$ in both the pre and post. As a side-effect, the rule prepends the read statement $let y = \ast(x + i)$ to the remainder of the program to be synthesized.

The rule Write allows for writing a symbolic expression $e$ into a memory cell, provided all $e$’s variables are program-level. It is customary for this rule to be followed by an application of Frame, which is SSL’s version of Separation Logic’s frame rule. Here, we show a version of the rule, which is a bit weaker than what’s in the full version of SSL, and will be generalized later. This rule enables “framing out” a shared sub-heap $R$ from the pre and post, as long as this does not create new existential variables. Notice, that unlike the classical SL’s Frame rule by O’Hearn et al. (2001), our version does not require a side condition saying that $R$ must not contain program variables that are modified by the program [to be synthesized]: by removing $R$ from the subgoal, we ensure that the residual program will not be able to access any pointers from $R$, because it will be synthesized in a symbolic footprint disjoint from $R$, and all local variables in SSL language are immutable.

Synthesizing swap. Armed with the basic SSL inference rules from Fig. 1, let us revisit our initial example: the swap function (1). Fig. 2 shows the derivation of the program using the rules, and should be read bottom-up. For convenience, we name each subgoal’s witness program, starting from $c_1$ (which corresponds to swap’s body). Furthermore, each intermediate sub-goal highlights via gray boxes a part of the pre and/or the post, which “triggers” the corresponding SSL rule. Intuitively, the goal of the synthesis process is to “empty” the spatial parts of the pre and the post, so that the derivation can eventually be closed via Emp; to this end, Read and Write work together to create matching heaplets between the two assertions, which are then eliminated by Frame.

### 2.3 Spatial Unification and Backtracking

Now, consider the synthesis goal induced by the following SL specification:

$$\{x \mapsto 239 \ast y \mapsto 30\} \ void \ \text{pick}(\text{loc} \ x, \ \text{loc} \ y) \ \{x \mapsto z \ast y \mapsto z\} \quad (2)$$

Since $z$ does not appear among the formals or in the precondition, it is treated as an existential. The postcondition thus allows $x$ and $y$ to point to any value, as long as it is the same value.

To deal with existentials in the heap, we introduce the rule UnifyHeaps, which attempts to find a unifying substitution $\sigma$ for some sub-heaps of the pre and the post. The domain of $\sigma$ must only contain existentials. For example, applying UnifyHeaps to the spec (2) with $R \models x \mapsto 239$ and $R' \models x \mapsto z$ results in the substitution $\sigma = [z \mapsto 239]$, and the residual synthesis goal $\{x, y\} \ \{x \mapsto 239 \ast y \mapsto 30\} \ \Rightarrow \ \{x \mapsto 239 \ast y \mapsto 239\}$, which can be now synthesized by using the Frame, Write, and Emp rules.

Due to their freedom to choose a sub-heap (and a unifying substitution), Frame and UnifyHeaps introduce non-determinism into the synthesis procedure and might require backtracking—a fact also widely observed in interactive verification community (Gonthier et al. 2011; McCreight 2009) wrt. SL assertions. For instance, consider the spec below:

$$\{x \mapsto a \ast y \mapsto b\} \ void \ \text{notSure}(\text{loc} \ x, \ \text{loc} \ y) \ \{x \mapsto c \ast c \mapsto 0\} \quad (3)$$

One way to approach the spec (3) is to first read from $x$, making $a$ a program-level variable $a2$ (via Read), then use UnifyHeaps and Frame on the $x \mapsto \bullet$ heaplets in the

```plaintext
void \ notSure(\text{loc} \ x, \ \text{loc} \ y) 
{
  \ast x = y;
  \ast y = 0;
}
```
pre/post, substituting the existential c by a2. That, however, leaves us with an unsolvable goal \{x, y, a2\} \{y \mapsto b\} \sim \{a2 \mapsto 0\}. Hence we have to backtrack, and instead unify c with y, eventually deriving the correct program notSure.

### 2.4 Reasoning with Pure Constraints

So far we have only looked at SL specifications whose *pure* parts were trivially true. Let us now turn our attention to the goals that make use of non-trivial pure boolean assertions.

#### 2.4.1 Preconditions

To leverage pure *preconditions*, we adopt a number of the traditional SMALL-foot-style rules, whose SSL counterparts are shown in the top part of Fig. 4. In the nomenclature of Berdine et al. (2005), all those rules are *non-operational*, i.e., correspond to constructing the proofs of symbolic heap entailment and involve no programming component. Note that the original rules in Berdine et al. (2005) assume a restricted pure logic with only equalities; we adapt these rules to our logic-agnostic style, relying on the oracle for pure validity instead of original syntactic premises.

For instance, the rule **SubstLeft** makes use of a precondition that implies equality between two universal variables, \(x = y\), substituting all occurrences of \(x\) in the subgoal by \(y\). The rule **StarPartial** makes explicit the fundamental assumption of SL: disjointness of symbolic heaps connected by the * operator. Most commonly, this rule’s effect is observable in combination with another rule, **Inconsistency**, which identifies an inconsistent pre, and emits an always-failing program error.

These three SSL rules can be observed in practice via the following example:

\[
\{a = x \land y = a; x \mapsto y \ast y \mapsto z\} \text{void urk(} loc x, \ loc y\) \{true; y \mapsto a \ast x \mapsto y\}
\]  

(4)

After applying **SubstLeft**, the goal transforms to \(\{x, y\} \{x \mapsto x \ast x \mapsto z\} \sim \{x \mapsto x \ast x \mapsto x\}\), which is clearly unsatisfiable, as the precondition requires two disjoint points-to heaplets with the same source—a fact, which converted into a pure sub-formula \(x \neq x\) by **StarPartial**, resulting in the error body via **Inconsistency**.

#### 2.4.2 Postconditions

In the presence of non-trivial pure *postconditions*, we face the problem to find suitable instantiations for their existentials. This is a challenging, yet well-studied problem, tackled by *pure program synthesis* (Alur et al. 2013). We consider this problem orthogonal to our agenda of deriving pointer-manipulating programs, and represent pure synthesis with a simplification rule **SubstRight** (Berdine et al. 2005), exploiting an equality in a goal’s postcondition, and an oracle rule **Pick**, which picks an instantiation for an existential non-deterministically.

In practice, the non-determinism can be curbed, for example, by delegating to an existing pure synthesizer (Kuncak et al. 2010; Reynolds et al. 2015). In our implementation, however, we found a
combination of first-order unification (rule UnifyPure) and restricted enumerative search (rule Pck restricted to variables) to be very effective at discharging such synthesis goals.

As an example, consider the following goal (where \(S\) and \(S_1\) are finite sets and \(\cup\) is disjoint union):

\[
\{S = \{v\} \cup S_1; x \mapsto a\} \text{ void elem(loc } x, \text{ int } v\} \{S = \{v_1\} \cup S_1; x \mapsto v_1 + 1\}
\]  

(5)

Following the rule UnifyPure, one can unify the two facts about sets in the pre and the post, obtaining the substitution \([v_1 \mapsto v]\). The rest is accomplished by the rule Write, which emits the only necessary statement for elem’s body: \(x = v + 1\).

2.5 Synthesis with Inductive Predicates

The real power of Separation Logic stems from its ability to compositionally reason about linked heap-based data structures, such as lists and trees, whose shape is defined recursively via inductive heap predicates. The most traditional example of a data structure defined this way is a linked list segment \(lseg(x, y, S)\) (Reynolds 2002), whose definition is given by the two-clause predicate below:

\[
lseg(x, y, S) \triangleq x = y \land \{S = \emptyset; \text{emp}\} \quad \text{and} \quad x \neq y \land \{S = \{v\} \cup S_1; [x, 2] \ast x \mapsto \langle x, 1 \rangle \mapsto \text{nxt} \ast lseg(\text{nxt}, y, S_1)\} \quad (6)
\]

The predicate definition, which we will abstractly denote as \(D \triangleq p(x)\{(\xi_j, \{\chi_j, R_j\})\}_{j \in 1 \ldots N}\) starts from the name \(p\) and a vector or formal parameters \(x\); for lseg those are the symbolic pointer variables, \(x\) and \(y\) for the first and the last pointer in the list, as well as for the logical set \(S\) of its elements. What follows is a sequence of \(N\) inductive clauses, with a \(j\)th clause starting from a guard \(\xi_j\)—a boolean formula defining a condition on the predicate’s formals,\(^4\) followed by the clause body—a SL assertion with a spatial part \(R_j\) and pure part \(\chi_j\), describing the shape of the heap and pure constraints, correspondingly. Clauses’ free variables, i.e., non-formals, (e.g., \(v\), \(\text{nxt}\)) are treated as ghosts or existentials, depending on whether the predicate instance is in a pre or post of a goal. From now on, we extend the definition of the goal, with a context \(\Sigma\), which will store the definitions of inductive predicates and specified functions, which are accessible in the derivation.

That is, the first clause of lseg states that in the case of \(x\) and \(y\) being equal, the linked list’s set of element is empty and its implementation is an empty heap emp. The complementary second clause postulates the existence of the allocated memory block (or just block) of two consecutive pointers rooted at \(x\) (denoted \([x, 2] \ast x \mapsto \langle x, 1 \rangle \mapsto \text{nxt}\)), that the first pointer stores the payload \(v\), while the second one points to the tail of the list, whose shape is defined recursively via the same predicate, although with different actuals, as captured by the predicate instance \(lseg(\text{nxt}, y, S_1)\).

2.5.1 Dynamic Memory. In order to support dynamically allocated linked structures, as demonstrated by definition (6), we extend the language of symbolic heaps with two new kinds of assertions: blocks and predicate instances. Symbolic blocks are a well-established way to add to SL support for consecutive memory chunks (Brotherston et al. 2017; Jacobs et al. 2011), which can be allocated and disposed all together.\(^5\) Two SSL rules, Alloc and Free (presented in Sec. 3), make use of blocks, as those appear in the post- and the pre-conditions of their corresponding goals. Conceptually, Alloc looks for a block in the postcondition rooted at an existential and allocates a block of the same size (by emitting the command \(\text{let } x = \text{malloc}(n)\)), adding it to the subgoal’s precondition. Free is triggered by an un-matched block in the goal’s pre, rooted at some program variable \(x\), which it then disposes by emitting the call to free\((x)\), removing it from the subgoal’s precondition.

\(^4\)In the case of logical overlap, the conditions for different clauses are checked in the order the clauses are defined.

\(^5\)An alternative would be to adopt an object model with fields, which is more verbose (Berdine et al. 2005).
2.5.2 Induction. Let us now synthesize our first recursive heap-manipulating function, a linked list’s destructor \texttt{listfree}(x), which expects a linked list starting from its argument \( x \) and ending with the null-pointer, and leaves an empty heap as its result:

\[
\{ \text{seg}(x, 0, S) \} \textbf{ void listfree}(\textbf{loc} \ x) \{ \text{emp} \}
\]  (7)

The first synthesis step is carried out by the SSL rule \textsc{Induction}. We postpone its formal description until the next section, conveying the basic intuition here. \textsc{Induction} only applies to the initial synthesis goal whose precondition contains an inductive predicate instance, and its effect is to add a new \emph{function symbol} to the goal’s context, such that an invocation of this function would correspond to a recursive call. In our example (7) \textsc{Induction} extends the context \( \Sigma \) with a “recursive hypothesis” as follows (we explain the meaning of the tag 1 in \( \text{seg}^1(x', 0, S') \) later):

\[
\Sigma_1 \triangleq \Sigma, \text{listfree}(x') : \{ \text{seg}^1(x', 0, S') \} \{ \text{emp} \}
\]  (8)

2.5.3 Unfolding Predicates. The top-level rule \textsc{Induction} is complemented by the rule \textsc{Open} (defined in Sec. 3), which \emph{unfolds} a predicate instance in the goal’s precondition according to its definition, and creates a subgoal for each inductive clause. For instance, invoked immediately on our goal (7), it has the following effect on the derivation:

(a) Two sub-goals, one for each of the clauses of \texttt{seg}, are generated to solve:

\begin{enumerate}
\item \( \Sigma_1; \{ x \}; \{ x = 0 \land S = \emptyset; \text{emp} \} \leadsto \{ \text{emp} \} \)
\item \( \Sigma_1; \{ x \}; \{ x \neq 0 \land S = \{ v \} \cup S_1; \{ x, 2 \} \text{ * } x \leftrightarrow v \ast (x, 1) \text{ * } \text{nxt} \ast \text{seg}^1(\text{nxt}, y, S_1) \} \leadsto \{ \text{emp} \} \)
\end{enumerate}

(b) Assuming \( c_1 \) and \( c_2 \) are the programs solving the sub-goals (i) and (ii), the final program is obtained by combining them as if \( (x = 0) \) \( c_1 \) else \( c_2 \).

Thus, \textsc{Open} performs case-analysis according to the predicate definition. Note how the precondition of each generated sub-goal is refined by the corresponding clause’s guard and body. The resulting sub-programs, once synthesized, are then combined with the conditional statement (this is why we require decidability of the guard statements), which branches on the predicate’s guard. It is easy to see that the first sub-goal (i) can be immediately solved via \textsc{Emp} rule, producing the program skip.

2.5.4 Level Tags. Synthesizing recursive programs requires extra care in order to avoid infinite derivations, as well as vacuously correct (in the sense of partial program correctness) non-terminating programs that simply call themselves. To avoid this pitfall, we adopt the ideas from the Cyclic Termination Proofs in SL (Brotherston et al. 2012), under the assumption that employed user-defined inductive predicates are well-founded, i.e., have their recursive applications only on strictly smaller sub-heaps (Brotherston et al. 2008). We ensure that this is the case by checking that there is at least one points-to predicate in clauses that also contain predicate instances.

Specifically, to avoid infinite unfolding of predicate instances we introduce \emph{level tags} (natural numbers, ranged over by \( \ell \)), which now annotate some predicate instances in the pre and post of the goal and the context functions. For an instance in a goal’s pre, a tag determines whether a set of functions in \( \Sigma \) that can be “applied” to it. As a result of a function application, tags are modified (as we explain later), thus preventing functions from being “re-applied” to their own symbolic post-heaps. Since tags only serve to control function calls, the rules \textsc{Frame} (Fig. 1) and \textsc{UnifyHeaps} (Fig. 3) ignore them when comparing sub-heaps for equality. All predicates in the pre/post of the initial goal have their level tag set as \( \ell = 0 \), and the rule \textsc{Open} only applies to 0-tagged predicates, incrementing their tag (i.e., one cannot “unfold again” an already opened instance).

\footnote{In SSL, a context \( \Sigma \) can also store user-provided specifications of auxiliary functions synthesized earlier. We will elaborate on case studies relying on user-provided auxiliary functions in Sec. 6.2.}
To see how tags control what functions from $\Sigma$ can be applied, consider the rule CALL in Fig. 5. It fires when the goal contains in its precondition a symbolic sub-heap $R$, which can be unified with the precondition $P_f$ of a function symbol $f$ from the goal’s context $\Sigma$. This unification is similar to the effect of UNIFYHEAPS, with the difference that CALL takes level tags into the account (i.e., instances with different tags cannot be unified), reflected in the tag-aware equality predicate $=^\ell$.

Our example’s second goal $(ii)$

$$\{x\} : \{x \neq 0 \land S = \{v\} \cup S_1; [x, 2] * x \mapsto v * (x, 1) \mapsto \text{nxt} \mapsto \text{lseg}^1(\text{nxt}, y, S_1)\} \leadsto \{\text{emp}\} \quad (9)$$

can be now transformed, via READ (focused on $(x, 1) \mapsto \text{nxt}$), into

$$\{x, \text{nxt}2\} : \{x \neq 0 \land S = \{v\} \cup S_1; [x, 2] * x \mapsto v * (x, 1) \mapsto \text{nxt}2 \mapsto \text{lseg}^1(\text{nxt}2, y, S_1)\} \leadsto \{\text{emp}\} \quad (10)$$

The grayed fragment in (10) can now be unified with the precondition of listfree (8) following CALL’s premise. As the tags match (both indicate the first unfolding of the predicate), unification succeeds with the substitution $\sigma = [x' \mapsto \text{nxt}2, S' \mapsto S_1]$ from $f$’s parameters and ghosts to the goal variables. The same rule produces, from the $f$’s postcondition, a new symbolic heap $R'$, which replaces the targeted fragment in the pre, recording the effect of the call. All tagged predicate instances in $R'$ get their tags erased ([[\sigma]Q_f])], thus, preventing any future recursive applications (via CALL) on the produced symbolic heap (more on that design decision in Sec. 7). However, in this example, the function’s post is merely $\{\text{emp}\}$, so the goal becomes:

$$\{x, \text{nxt}2\} : \{x \neq 0 \land S = \{v\} \cup S_1; [x, 2] * x \mapsto v * (x, 1) \mapsto \text{nxt}2 \mapsto \text{emp}\} \leadsto \{\text{emp}\} \quad (11)$$

The remaining steps are carried out by the rule FREE, followed by EMP, with the former disposing the remaining block, thus, completing the derivation with program listfree shown in Fig. 6.

2.5.5 Unfolding in the postcondition. Whereas OPEN unfolds predicate instances in a goal’s precondition, a complementary rule CLOSE (Fig. 5) performs a similar operation on the goal’s postcondition. The main difference is that instead of performing a case-split and emitting several subgoals, CLOSE non-deterministically picks a single clause $k$ from the predicate’s definition (the intuition being that the required case split has already been performed by OPEN). Upon unfolding, the clause’s adapted guard ($[[\sigma]\xi_k]$) and pure part ($[[\sigma]\chi_k]$) are
added to the subgoal’s postcondition, while its spatial part also gets its level tags increased by one
([\sigma]R_k)^{(r+1)}, in order to account for the depth of unfoldings.\footnote{We will elaborate on the control of unfolding depth in Sec. 3.1.}

To showcase the use of \textsc{Close}, let us define a new predicate for a linked null-terminating structure \textbf{lseg}2, which stores in each node the payload \(v\) and \(v+1\):

\[
\text{lseg}2(x,S) \triangleq x = 0 \land \{S = \emptyset; \text{emp}\}
\]

\[
x \neq 0 \land \begin{cases} \{S = \{v\} \cup S_1; \\{x,3\} * x \leftrightarrow v * \langle x,1 \rangle \leftrightarrow v + 1 * \langle x,2 \rangle \leftrightarrow \text{nxt} * \text{lseg}2(\text{nxt},S_1)\} \end{cases}
\]  

(12)

We now synthesize an implementation for the following specification, requiring to morph a regular list \text{lseg}(x,0,S) to \text{lseg}2(y,S), both parameterized by the same set \(S\):

\[
\{r \mapsto 0 * \text{lseg}(x,0,S)\} \textbf{ void listmorph}(\text{loc} x, \text{loc} r) \{r \mapsto y * \text{lseg}2(y,S)\}
\]  

(13)

The derivation starts \textsc{Induction}, then \textsc{Open} \text{lseg}(x,0,S), producing two sub-goals. The first one:

\[
\{x, r\}; \{S = \emptyset \land x = 0; r \mapsto 0 \mapsto [x,2] * x \leftrightarrow v * \langle x,1 \rangle \leftrightarrow \text{nxt}2 * \text{lseg}2(\text{nxt}2,0,S_1)\} \sim
\]  

(14)

is easy to solve via \textsc{Close}, which should pick the first clause from \text{lseg}2’s definition (12) (corresponding to \text{emp}), followed by \textsc{Frame} to \(r \mapsto y\) in the postcondition. The second subgoal, after having read the value of \((x+1)\), thus into a program variable \text{nxt}2 looks as follows:

\[
\{x, r, \text{nxt}2\}; \begin{cases} \{S = \{v\} \cup S_1 \land x \neq 0; r \mapsto 0 \mapsto [x,2] * x \leftrightarrow v * \langle x,1 \rangle \leftrightarrow \text{nxt}2 * \text{lseg}2(\text{nxt}2,0,S_1)\} \sim \{r \mapsto y * \text{lseg}2(y,S)\} \end{cases}
\]  

(15)

Now, \textsc{Close} comes to the rescue, by allowing us to unfold the grayed instance in (15)’s post:

\[
\{x, r, \text{nxt}2\}; \begin{cases} \{S = \{v\} \cup S_1 \land x \neq 0; r \mapsto 0 \mapsto [x,2] * x \leftrightarrow v * \langle x,1 \rangle \leftrightarrow \text{nxt}2 * \text{lseg}2(\text{nxt}2,0,S_1)\} \sim \{r \mapsto y * \text{lseg}2(y,S)\} \end{cases}
\]

(16)

In principle, nothing in the postcondition prevents us from applying \textsc{Close} again, unfolding the instance \text{lseg}2(\text{nxt}1, S_2) even further. Intuitively, a postcondition with a symbolic heap that elaborated is less likely to be satisfied, hence we limit the number of “telescopic” unfoldings by enforcing the boundary \textsc{MaxUnfold} for the level tag. We can now use the \textsc{Call} rule, unifying the precondition of the induction hypothesis (13) with the grayed parts in the goal (16), obtaining the following subgoal (notice the new instance \text{lseg}2(y_1, S_1) in the pre with its tag erased):

\[
\{x, r, \text{nxt}2\}; \begin{cases} \{S = \{v\} \cup S_1 \land x \neq 0; [x,2] * x \leftrightarrow v * \langle x,1 \rangle \leftrightarrow \text{nxt}2 * \text{lseg}2(\text{nxt}2,0,S_1)\} \sim \{y \mapsto \text{nxt}_1 * \text{lseg}2(y_1,S_1)\} \end{cases}
\]

(17)

The instances of \text{lseg}2 in the pre and the post, can now be unified via \textsc{UnifyHeaps} instantiating \text{nxt}1 with \(y_1\), followed by \textsc{UnifyPure} on pure parts, instantiating \text{S}2 with \(S_1\), and then framed via \textsc{Frame}. The remaining derivation is done by \textsc{Reading} from \(r\) and \(x\), subsequent disposing of a two-cell block (grayed in the pre) and allocation of a three-cell block in order to match the grayed block in the post. Finally, the exact payload for cells of the newly-allocated 3-pointer block is determined by unifying the set assertions in the pure parts of the pre and post (via \textsc{UnifyPure}), and then \textsc{Write} records the right values to satisfy the constraints imposed for the head of \text{lseg}2-like list by Definition (12). The resulted synthesized implementation of \text{listmorph} is shown in Fig. 7.

2.6 Enabling Procedure Calls by Means of Call Abduction

We conclude this overview with one last example—a recursive procedure for copying a linked list:

\[
\{ r \mapsto x^* \text{lseg}(x, 0, S) \} \text{void listcopy(loc) } \{ r \mapsto y^* \text{lseg}(x, 0, S) \} \text{lseg}(y, 0, S) \}
\]

(17)

To make things more fun, we pass the pointer to the head of the list via another pointer \( r' \), which is also used to record the result of the function—an address \( y \) of a freshly allocated list copy. The synthesis begins by using induction, producing the function symbol

\[
\text{void listcopy(loc r') : } \{ r' \mapsto x'^* \text{lseg}^1(x', 0, S') \} \{ r' \mapsto y'^* \text{lseg}^1(x', 0, S') \} \text{lseg}^1(y', 0, S')
\]

(18)

It follows by \text{Read} (from \( r \) into \( x2 \)) and \text{Open}, resulting in two subgoals, the first of which (an empty list) is trivial. The synthesis proceeds, reading from \( x2 \) into \( v2 \) and from \( x2 + 1 \) into \( \text{nxt}2 \), so after using \text{Close} (on \( \text{lseg}^0(x, 0, S) \)) in the post, \text{UnifyHeaps} and \text{Frame}, we reach the following subgoal:

\[
\{ x, r, x2, v2, \text{nxt}2 \}; \begin{cases} S = \{ v2 \} \cup S_1 \land x2 \neq 0; & r \mapsto x2 \mapsto \text{lseg}^1(\text{nxt}2, 0, S_1) \} \rightarrow \{ r \mapsto y \mapsto \text{lseg}^1(\text{nxt}2, 0, S_2) \} \rightarrow \text{lseg}^0(y, 0, S) \}
\]

(19)

At this point of our derivation, we run into an issue. Ideally, we would like to use the grayed fragment of the goal \((19)\)'s precondition, to fire the rule \text{Call} with the spec \((18)\), i.e. to make a recursive call on the tail list. However, the \((18)\)'s precondition requires \( r \) to point to the start of that list \( \text{nxt}2 \), whereas in our case it still points to the start of the original list \( x2 \).

Any programmer would know a solution to this conundrum: we have to write \( \text{nxt}2 \) into \( r \), in order to provide a suitable symbolic heap to make a recursive call. Emitting such a write command is a synthesis sub-goal in itself. To generate such sub-goals, we introduce a novel rule, \text{AbduceCall}, which is shown in Fig. 8 and attempts to \text{prepare} the symbolic pre-heap for the recursive call by adjusting constant-size symbolic footprint to become unifiable with the recursive calls' precondition.

First, the rule inspects the preconditions of the goal and of the candidate callee \( F \) from \( \Sigma \), it tries to split the former into two symbolic sub-heaps, \( P_f \) and \( F_f \), such that all predicate instances are contained within \( P_f \), while the rest of the heaplets (i.e., blocks and points-to-assertions) are in \( F_f \). Next, it tries to unify \( P_f \) from the function spec with some sub-heap \( P \) from the goal’s precondition, finding a suitable substitution \( \sigma \), such that \( P = [\sigma]P_f \). While doing so, it does not account for the “remainder” \([\sigma]F_f\), which might not be immediately matched by anything in the goal's precondition. In order to make it match, the goal emits, as one of its premises, a sub-goal \( \Sigma; F; \{ \phi; F \} \rightarrow \{ \text{true}, F' \} \} c_1 \), whose purpose is to synthesize a program \( c_1 \), which will serve as an impedance matcher between some symbolic subheap \( F \) from the original goal’s pre and \( F' = [\sigma]F_f \).\(^8\)

\(^8\)Our implementation is smarter than that: it ensures that \( F \) and \( F' \) have the same shape and differ only in pointers' values.

It follows by \text{Read} (from \( r \) into \( x2 \)) and \text{Open}, resulting in two subgoals, the first of which (an empty list) is trivial. The synthesis proceeds, reading from \( x2 \) into \( v2 \) and from \( x2 + 1 \) into \( \text{nxt}2 \), so after using \text{Close} (on \( \text{lseg}^0(x, 0, S) \)) in the post, \text{UnifyHeaps} and \text{Frame}, we reach the following subgoal:

\[
\{ x, r, x2, v2, \text{nxt}2 \}; \begin{cases} S = \{ v2 \} \cup S_1 \land x2 \neq 0; & r \mapsto x2 \mapsto \text{lseg}^1(\text{nxt}2, 0, S_1) \} \rightarrow \{ r \mapsto y \mapsto \text{lseg}^1(\text{nxt}2, 0, S_2) \} \rightarrow \text{lseg}^0(y, 0, S) \}
\]

(19)

At this point of our derivation, we run into an issue. Ideally, we would like to use the grayed fragment of the goal \((19)\)'s precondition, to fire the rule \text{Call} with the spec \((18)\), i.e. to make a recursive call on the tail list. However, the \((18)\)'s precondition requires \( r \) to point to the start of that list \( \text{nxt}2 \), whereas in our case it still points to the start of the original list \( x2 \).

Any programmer would know a solution to this conundrum: we have to write \( \text{nxt}2 \) into \( r \), in order to provide a suitable symbolic heap to make a recursive call. Emitting such a write command is a synthesis sub-goal in itself. To generate such sub-goals, we introduce a novel rule, \text{AbduceCall}, which is shown in Fig. 8 and attempts to \text{prepare} the symbolic pre-heap for the recursive call by adjusting constant-size symbolic footprint to become unifiable with the recursive calls' precondition.

First, the rule inspects the preconditions of the goal and of the candidate callee \( F \) from \( \Sigma \), it tries to split the former into two symbolic sub-heaps, \( P_f \) and \( F_f \), such that all predicate instances are contained within \( P_f \), while the rest of the heaplets (i.e., blocks and points-to-assertions) are in \( F_f \). Next, it tries to unify \( P_f \) from the function spec with some sub-heap \( P \) from the goal's precondition, finding a suitable substitution \( \sigma \), such that \( P = [\sigma]P_f \). While doing so, it does not account for the “remainder” \([\sigma]F_f\), which might not be immediately matched by anything in the goal’s precondition. In order to make it match, the goal emits, as one of its premises, a sub-goal \( \Sigma; F; \{ \phi; F \} \rightarrow \{ \text{true}, F' \} \} c_1 \), whose purpose is to synthesize a program \( c_1 \), which will serve as an impedance matcher between some symbolic subheap \( F \) from the original goal’s pre and \( F' = [\sigma]F_f \).\(^8\)

\(^8\)Our implementation is smarter than that: it ensures that \( F \) and \( F' \) have the same shape and differ only in pointers’ values.
The language of commands does not include loops, which are modelled via recursive procedure
variables, values, boolean equality checks and additional theory-specific expressions (e.g.,

3 SYNTHETIC SEPARATION LOGIC IN A NUTSHELL

Having shown SSL in action, we now proceed with giving a complete set of its inference rules,
along with statements of the formal guarantees SSL provides wrt. synthesized imperative programs.

The syntax for the imperative language supported by SSL is given in Fig. 10. The set of values
includes at least integers and pointers (isomorphic to non-negative integers). Expressions include
variables, values, boolean equality checks and additional theory-specific expressions (e.g., integer or
boolean operations). The command magic does not appear in runnable code and is included in the
language for the purpose of a deductive synthesis optimization, which we will explain in Sec. 5.4.
The language of commands does not include loops, which are modelled via recursive procedure
calls (f(τi)). Notice that for simplicity we do not provide a mechanism to return a variable from a
procedure (so the language is missing the return command) and therefore all procedures’ return
type is void. However, the result-returning discipline for a procedure can be encoded via passing a
result-storing additional pointer, as, e.g., in Example (17). A function dictionary Δ is simply a list of
function definitions of the form f(τi, xi) { c }.

The complete syntax of SSL assertions is shown in Fig. 11, and their meaning was explained in
detail throughout Sec. 2. We only notice here that, syntactically, pure assertions φ, ψ, etc coincide
with the language’s expressions e. The lack of the distinction between the two kinds is for the sake
of uniformity and to enable the use of third-party SMT solvers without committing to a specific
first-order logic as an inherent part of SSL. We use a simple type system to make sure that the
expressions serving as pure formulae are of type bool, while also making sure that set-theoretical
operations, such as ∪, do not leak to the program level.

3.1 The Zoo of SSL Rules

Fig. 12 presents all rules of SSL. Since most of them have already made an appearance in Sec. 2,
here, we only elaborate on the new ones, and highlight some important aspects of their interaction.
It is convenient to split the set of rules into the following six categories:

C1 Top-level rules are represented by just one rule: INDUCTION (Fig. 12, bottom right). This rule is
only applicable at the very first stage of the derivation, and it produced a specified symbol f, with
the specification identical to the top-level goal (modulo renaming of variables to avoid
capturing conflicts). In the case of several predicate instances pθ(τi) in the goal’s pre, the
Fig. 12. All rules of SSL. Grayed parts are parameters; instantiating them differently yields different rules.
rule non-deterministically picks one recursion scheme, whereas other predicate instances in $f$’s precondition get “sealed” via tag erasure [P]).

C2 **Terminals** include **EMP** and **INCONSISTENCY**. These rules conclude a successful derivation by emitting **skip** or **error**, respectively.

C3 **Normalization rules** include **NULLNOTLVAL**, **SUBSTLEFT**, **STARPARTIAL**, and **READ**. The role of these rules is to normalize the precondition: eliminate ghosts and equal variables, and make explicit the assumptions encoded in the spatial part. As we discuss in Sec. 5.1, a characteristic feature of those rules is that they cannot cause their subderivation fail.

C4 **Unfolding rules** are the rules targeted specifically to predicate instances. The four basic unfolding rules are **OPEN**, **CLOSE**, **ABDUCCECALL**, and **CALL**. As hinted before, the rule **OPEN** picks an instance $p^f(\tau_i)$ in the goal’s pre, and produces a number of subgoals, emitting a conditional that accounts for all of $p$’s clauses. **CLOSE** acts symmetrically on the post. Both rules increment the tag for the instances in the substituted clause bodies, and are not applicable for $\ell$, which is equal or greater than the set boundary on the depth of unfoldings, defined by the global synthesis parameter $\text{MaxUnfold}$.\(^9\) In our practical experience $\text{MaxUnfold}$ taken to be equal 1 suffices for most of realistic case studies. The rule **ABDUCCECALL** prepares the heap for a call application (via **CALL**), as described in Sec. 2.6. Note that the rules **UNIFYHEAP** and **FRAME** have been slightly generalized wrt. to what was shown in Fig. 1 and Fig. 3, and now include a parametric premise frameable. If we define frameable to return true only for predicate instances, we obtain unfolding versions of these rules, which deal specifically with predicate instances.

C5 **Flat** rules deal with with the flat part of the heap (which consists of block heaplets and heaplets of the form $x \mapsto e$). They include **ALLOC**, **FREE**, **WRITE**, as well as the flat versions of **UNIFYHEAP** and **FRAME**, with frameable defined to return true for flat heaplets.

C6 **Pure synthesis** rules are responsible for instantiating existentials. In Fig. 12 this category is represented by three rules. The first one is nondeterministic **Pick**, which is difficult to implement efficiently. In order to make the presentation complete, we include two remaining, somewhat redundant but more algorithmic, pure synthesis rules introduced in Sec. 2.4.2 for the sake of efficient search, namely **UNIFYPURE** and **SUBSTRIGHT**.

Let us refer to rules that emit a sub-program as operational and to the rest (i.e., to the rules that only change the assertions) as non-operational. The rules from Fig. 12 form the basis of SSL as a proof system, allowing for possible extensions for the sake of optimization or handling pure constraints. We make them intentionally declarative rather than algorithmic, which is essential for establishing the logic’s soundness, leaving a lot of freedom for possible implementations. Such decisions have to be made, for instance, when engineering an implementation of **ABDUCCECALL** or **PICK**. The algorithmic aspects of SSL, e.g., non-deterministic choice of a frame or a unifying substitution, are handled by the procedures from Sec. 4.

### 3.2 Formal Guarantees for the Synthesized Programs

The definition of the operational semantics of the SSL language (Fig. 10) follows the standard RAM model. **Heaps** (ranged over by $h$) are represented as partial finite maps from pointers to values, with support for pointer arithmetic (via offsets). A function call is executed within its own stack frame $(c, s)$, where $c$ is the next command to reduce and $s$ is a store recording the values of the function’s local variables and parameters. A stack $S$ is a sequence of stack frames, and a configuration is a pair of a heap and a stack. The small-step operational semantics relates a function dictionary $\Delta$, and a pair of configurations: $\Delta; \langle h, S \rangle \rightsquigarrow \langle h’, S’ \rangle$,\(^{10}\) with $\rightsquigarrow^*$ meaning its reflexive-transitive closure.

\(^9\)Having the derivation/search depth bound by $\text{MaxUnfold}$ affects the completeness but not soundness of SSL.

\(^{10}\)We elide the transition rules for brevity; similar rules can be found, e.g., in the work by Rowe and Brotherston (2017).
Let us denote the valuation of an expression $e$ under a store $s$ as $\llbracket e \rrbracket_s$. Let $I$ range over interpretations—mappings from user-provided predicates $\mathcal{D}$ to the relations on heaps and vectors of values. To formally define the validity of Hoare-style specs in SSL, we use the standard definition of the satisfaction relation $\models I$ as a relation between pairs of heaps and stores, contexts, interpretations, and SSL assertions without ghosts. For instance, the following SSL definitions are traditional for Separation Logics with interpreted predicates (Berdine et al. 2005; Nguyen et al. 2007):

- $\langle h, s \rangle \models I \{\phi; \text{emp}\}$ iff $\llbracket \phi \rrbracket_s$ is true and $\text{dom}(h) = \emptyset$.
- $\langle h, s \rangle \models I \{\phi; [x, n]\}$ iff $\llbracket \phi \rrbracket_s$ is true and $\text{dom}(h) = \emptyset$.
- $\langle h, s \rangle \models I \{\phi; (e_1, i) \mapsto e_2\}$ iff $\llbracket \phi \rrbracket_s$ is true and $\text{dom}(h) = [e_1]_s + i$ and $\text{dom}(h) = [e_2]_s$.
- $\langle h, s \rangle \models I \{\phi; P_1 \ast P_2\}$ iff $\exists h_1, h_2, h = h_1 \cup h_2$ and $\langle h_1, s \rangle \models I \{\phi; P_1\}$ and $\langle h_2, s \rangle \models I \{\phi; P_2\}$.
- $\langle h, s \rangle \models I \{\phi; \rho(x_i)\}$ iff $\llbracket \phi \rrbracket_s$ is true and $\mathcal{D} \triangleq \rho(x_i)\langle \xi_j, \{\chi_j, R_j\}\rangle \in \Sigma$ and $\langle h, [x_i]_s \rangle \in I(D)$.

Therefore, blocks have no spatial meaning, except for serving as an indicator on the memory fragments that we allocated and can be disposed.

To equip ourselves for the forthcoming proof of SSL soundness, we provide a definition of (sized) specification validity, which relies on the notion of a heap size $|h| \triangleq |\text{dom}(h)|$.

**Definition 3.1 (Sized validity).** We say a specification $\Sigma; I; \{P\} c \{Q\}$ is $n$-valid wrt. the function dictionary $\Delta$ whenever for any $h, h', s, s'$ such that

- $|h| \leq n$,
- $\Delta; \langle h, (c, s), \cdot, e \rangle \leadsto^* \langle h', (\text{skip}, s'), \cdot, e \rangle$, and
- $\text{dom}(s) = \Gamma$ and $\exists \sigma_{\text{ev}} = [x_i \mapsto d_i]_{x_i \in \text{GV}(\Gamma, P, Q)}$ such that $\langle h, s \rangle \models I \{\sigma_{\text{ev}}\}P$,

it is the case that $\exists \sigma_{\text{ev}} = [y_j \mapsto d_j]_{y_j \in \text{EV}(\Gamma, P, Q)}$, such that $\langle h', s' \rangle \models I \{\sigma_{\text{ev}} \cup \sigma_{\text{ev}}\}Q$.

Definition 3.1 is rather peculiar in that it defines a standard Hoare-style soundness wrt. pre/post, while doing that only for heaps of size smaller than $n$. This is an important requirement to stage a well-founded inductive argument for our soundness proof of SSL-based synthesis in the presence of recursive calls. By introducing the explicit sizes to the definition of validity, we can make sure that we only deal with calls on strictly decreasing subheaps wrt. the heap size when invoking functions (auxiliary ones or recursive self). To make full use of this idea, we add one more auxiliary definition, stratifying the shape of function dictionaries wrt. their specifications.

**Definition 3.2 (Coherence).** A dictionary $\Delta$ is $n$-coherent wrt. a context $\Sigma$ (coh $(\Delta, \Sigma, n)$) iff

- $\Delta = \epsilon$ and $\text{functions}(\Sigma) = \epsilon$, or
- $\Delta = \Delta', f \{t_i x_i\} \{c\}$, and $\Sigma = \Sigma', f \{(\overline{x})\} \{\mathcal{P}\} \{Q\}$, and coh $(\Delta', \Sigma', n)$, and $\Sigma'; \{\overline{x}\} \{\mathcal{P}\} c \{Q\}$ is $n$-valid wrt. $\Delta'$, or
- $\Delta = \Delta', f \{t_i x_i\} \{c\}$, and $\Sigma = \Sigma'$, $f \{(\overline{x})\} : \{\phi; [P] \ast P^1(\overline{e})\} \{[Q]\}$, and coh $(\Delta', \Sigma', n)$, and $\Sigma; \{\overline{x}\} : \{[P] \ast P^1(\overline{e})\} \{[Q]\}$ is $n'$-valid wrt. $\Delta$ for all $n' < n$.

That is, coherence is defined inductively on the dictionary/context shape (regarding specified functions and ignoring predicate definitions). A possibility of a (single) recursive definition $f$ is taken into the account in its last option. In that last clause, recursive calls to the function $f$ from $\Delta$ may only take place on heaps of size strictly smaller than $n$, whereas there is no such restriction for the calls to user-provided auxiliary functions, that can be invoked on heaps of sizes up to $n$.

Soundness of Synthetic Separation Logic is stated by Theorem 3.3, which defines validity of the synthesized program for any size of the input heap $n$, assuming that the validity of all recursive calls of the synthesized programs is only established for $n' < n$, where the case $n = 0$ means no calls take place and forms the base of the inductive reasoning.
Theorem 3.3 (Soundness of SSL). For any \( n, \Delta' \), if

(i) \( \Sigma'; \Gamma; \{P\} \rightarrow \{Q\} | c \) for a goal named \( f \) with formal parameters \( \Gamma \triangleq \bar{x}_i \), and

(ii) \( \Sigma' \) is such that \( \text{coh} (\Delta', \Sigma', n) \), and

(iii) for all \( p^0(\bar{e}_i), \phi; P \), such that \( \{P\} = \{\phi; p^0(\bar{e}_i) \ast P\} \), taking \( \mathcal{F} \triangleq f(\bar{x}_i); \{\phi; p^1(\bar{e}_i) \ast [P]\}\{\{Q\}\} \),

\( \Sigma', \mathcal{F}; \Gamma; \{P\} \rightarrow \{Q\} \) is \( n' \)-valid for all \( n' < n \) wrt. \( \Delta \triangleq \Delta' \), \( f(\bar{t}_i, \bar{x}_i) \) \{ c \},

then \( \Sigma'; \Gamma; \{P\} \rightarrow \{Q\} \) is \( n \)-valid wrt. \( \Delta \).

Proof. By the top-level induction on \( n \) and by inner induction on the structure of derivation \( \Sigma'; \Gamma; \{P\} \rightarrow \{Q\} \) | c. We refer the reader to Appendix A for the details. \( \square \)

Theorem 3.3 states that a program derived via SSL constitutes a valid spec with its goal (i.e., all writes, reads and deallocations in it are safe wrt. accessing heap pointers), assuming that recursive calls, if present, are made on reduced sub-heaps. The technique we used—allowing for safe calls done only on smaller sub-heaps—is reminiscent to the one employed in size-change termination-based analyses (Lee et al. 2001), which ensure that every infinite sequence of calls would cause infinite descent of some values, leading to the following result.

Theorem 3.4 (Termination of SSL-synthesized programs). A program, which is derived via SSL rules from a spec that uses only well-founded predicates, terminates.

Proof. The only source of non-termination is calls. Auxiliary function calls cannot be chained infinitely as they erase tags on their post-heaps. Every recursive self-call is applicable after opening a well-founded instance, and hence is done on a smaller sub-heap, erasing tags on its post-heap. \( \square \)

4 BASIC SSL-POWERED SYNTHESIS ALGORITHM

In this section we show how to turn SSL from a declaratively defined system (Fig. 12) into a search algorithm with backtracking for deriving provably correct imperative programs.

Encoding Rules and Derivations. The display on the right shows an algorithmic representation of SSL derivations and rules. To account for the top-level goal (which mandates the program synthesizer to generate a runnable function), we include the function name \( f \) into the goal \( \mathcal{G} \), whose other components are the context \( \Sigma \), environment \( \Gamma \) (initialized with \( f \)’s formals), pre \( \{P\} \) and post \( \{Q\} \). A successful application or a rule \( \mathcal{R} \) results in one or more alternative sub-derivations \( \mathcal{S}_k \). Several alternatives arise when the rule exhibits non-determinism (e.g., due to choosing a sub-heap to a unifying substitution), and are explored by a search engine one by one, until it finds one that succeeds. This is customary for a conversion of a declarative inference system to an algorithmic one (Pierce 2002, Chapter 16).

In its turn, each sub-derivation is a pair. Its first component contains zero (if \( \mathcal{R} \) is a terminal) or more sub-goals, which all need to be solved (think of a conjunction of a rule’s premises). The second component of the sub-derivation is a continuation \( \mathcal{K} \), which combines the list of commands, produced as a result of solving subgoals, into a final program. The arity of a continuation (length of a list it accepts) is the same as a number of sub-goals the corresponding rule emits (typically one or more). Zero-arity means that the continuation has been produced by a terminal, and simply emits a constant program. For non-operational rules (e.g., FRAME), \( \mathcal{K} \triangleq \lambda[c].c \). For operational rules \( \mathcal{K} \) typically prepends a command to the result (e.g., WRITE), or generates a conditional statement (OPEN). Therefore, the synthesizer procedure constructs the program by applying the continuations of rules that have succeeded earlier, to the resulting programs by their subgoals, on the “backwards” walk of the recursive search, in the style of logic programming (Mellish and Hardy 1984).
Algorithm 4.1: synthesize \((G : Goal, rules : Rule^*)\)

<table>
<thead>
<tr>
<th>Line</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Input: Goal (G = (f, \Sigma, \Gamma, {P}, {Q}))</td>
</tr>
<tr>
<td>2</td>
<td>Input: List rules of available rules to try</td>
</tr>
<tr>
<td>3</td>
<td>Result: Program (c), such that (\Sigma, \Gamma, {P} \in {Q}) is valid</td>
</tr>
<tr>
<td>4</td>
<td>function synthesize ((G, rules) =)</td>
</tr>
<tr>
<td>5</td>
<td>function withRules ((rs, G) =)</td>
</tr>
<tr>
<td>6</td>
<td>match (rs)</td>
</tr>
<tr>
<td>7</td>
<td>case [] (\Rightarrow) Fail</td>
</tr>
<tr>
<td>8</td>
<td>case (R :: rs' \Rightarrow)</td>
</tr>
<tr>
<td>9</td>
<td>if isEmpty(subderivs) (\Rightarrow)</td>
</tr>
<tr>
<td>10</td>
<td>withRules(rs')</td>
</tr>
<tr>
<td>11</td>
<td>else</td>
</tr>
<tr>
<td>12</td>
<td>tryAlts(subderivs, (R, rs', G))</td>
</tr>
<tr>
<td>13</td>
<td>function tryAlts ((derivs, R, rs, G) =)</td>
</tr>
<tr>
<td>14</td>
<td>match derivs</td>
</tr>
<tr>
<td>15</td>
<td>case [] (\Rightarrow) if isInvert(R) then Fail else withRules(rs, G)</td>
</tr>
<tr>
<td>16</td>
<td>case (\langle goals, K \rangle :: derivs' \Rightarrow)</td>
</tr>
<tr>
<td>17</td>
<td>match solveSubgoals(goals, K)</td>
</tr>
<tr>
<td>18</td>
<td>case Fail (\Rightarrow) tryAlts(derivs', R, rs, G)</td>
</tr>
<tr>
<td>19</td>
<td>function solveSubgoals ((goals, K) =)</td>
</tr>
<tr>
<td>20</td>
<td>cs := []</td>
</tr>
<tr>
<td>21</td>
<td>pickRules = (\lambda G. phasesEnabled ? nextRules(G) : AllRules)</td>
</tr>
<tr>
<td>22</td>
<td>for (G \leftarrow goals; c = synthesize(G, pickRules(G)); c \neq \text{Fail} ) do</td>
</tr>
<tr>
<td>23</td>
<td>cs := cs ++ [c]</td>
</tr>
<tr>
<td>24</td>
<td>if</td>
</tr>
</tbody>
</table>

The algorithm. The pseudocode of our synthesis procedure is depicted by Algorithm 4.1. Let us ignore the grayed fragments in the pseudocode for now and agree to interpret the code as if they were not present. Those fragments corresponds to optimizations, which we describe in detail in Sec. 5. The algorithm is represented by four mutually-recursive functions:

- synthesize \((G, rules)\) is invoked initially on a top-level goal, with rules instantiated with AllRules—all rules from Fig. 12. It immediately passes control to the first auxiliary function, withRules.
- withRules \((rs, G)\) iterates through the list \(rs\) of remaining rules, applying each one to the goal \(G\). Once an application of some rule \(R\) succeeds (i.e., it emits a non-empty set of alternative sub-derivations \(subderivs\)), those are passed for solving to tryAlts. The case when a rule application emits no sub-derivations, is considered a search failure, so the next rule is tried from the list, until no more rules remains (line 5), at which point the search fails.
- tryAlts \((derivs, R, rs, G)\) recursively processes the list of alternative sub-derivations \(derivs\), generated by the rule \(R\). If the list is exhausted (line 14), withRules is invoked to try the rest of the rules \(rs\). Otherwise, solveSubgoals is invoked for an alternative to solve all its sub-goals \(goals\) and apply the continuation \(K\). In the case of success (line 18), the resulting program \(c\) is returned.
- solveSubgoals \((goals, K)\) tries to solve all subgoals given to it, by invoking synthesize recursively with a suitable (full) list of rules, essentially, restarting the search problem “one level deeper” into the derivation. Unless some of the goals failed, their results are combined via \(K\). \(^{11}\)

The algorithm implements a naïve backtracking search that explores the space of all valid SSL derivations rooted at the initial synthesis goal. The search proceeds in a depth-first manner: it starts from the root (the initial goal) and always extends the current incomplete derivation by applying a rule to its leftmost open leaf (i.e., a leaf that is not a terminal application). The algorithm terminates when the derivation is complete, i.e., it has no open leaves.

In our experience, the algorithm implementation terminated on all inputs we provided. It seems probable that this can be established by considering the following tuples, ordered lexicographically, as a termination measure for a given goal \(G\): \(#0- or 1-tagged predicate instances; \#heaplets in pre and post, for which there is no matching one in the post/pre; \# existentials; \# "flat" heaplets; \# conjuncts in the pre; \# of points-to heaplets, whose disjointness or non-null-ness is not captured\)

\(^{11}\)The actual implementation is more efficient than that and uses a breakable loop.
in the pre⟩. Notice that each rule from Fig. 12, except for Open and Close reduces this value for the emitted sub-goals. Applicability of those two rules is handled via MaxUnfold parameter. That said, we have not proven termination of synthesize and leave it a conjecture.

5 OPTIMIZATIONS AND EXTENSIONS

The basic synthesis algorithm presented in Sec. 4 is a naïve backtracking in the space of all valid SSL derivations. Note that this is already an improvement over a blind search in the space of all programs: some incorrect programs are excluded from consideration a-priori, such as, e.g., programs that read from unallocated heap locations. In this section we show how to further prune the search space by identifying unsolvable goals and avoiding their exploration.

5.1 Invertible Rules

Our first optimization relies on a well-known fact from proof theory (Liang and Miller 2009) that certain proof rules are invertible: applying such a rule to any derivable goal produces a goal that is still derivable. In other words, applying invertible rules eagerly without backtracking does not affect completeness. Algorithm 4.1 leverages this fact in line 14: when all sub-derivations of an invertible rule \( R \) fail, the algorithm need not backtrack and try other rules, since the failure cannot be due to \( R \) and must have been caused by a choice made earlier in the search.

In SSL, the normalization rules—\texttt{Read}, \texttt{StarPartial}, \texttt{NullNotLVal}, and \texttt{SubstLeft}—are invertible. The effect of these rules on the goal is either to change a ghost into a program-level variable or to strengthen the precondition; no rule that is applicable to the original goal can become inapplicable as a result of this modification, which is confirmed by inspection of all rules in Fig. 12.

5.2 Multi-Phased Search

Among the rules of SSL described in Sec. 3, the unfolding rules are focused on transforming (and eventually eliminating) instances of inductive predicates, while flat rules are focused on other types of heaplets (i.e., points-to and blocks). We observe that if the unfolding rules failed to eliminate a predicate instance from the goal, there is no point to apply flat rules to that goal. It is easy to show that the flat rules can neither eliminate predicates from the goal, nor enable previously disabled unfolding rules: the only unfolding rule that matches on flat heaplets is \texttt{Call}, but those heaplets need not be “prepared” by the flat rules, since that’s what \texttt{AbduceCall} is for.

Following this observation, without loss of completeness, we can split the synthesis process into two phases: the unfolding phase, where flat rules are disabled, and the flat phase, which only starts when the goal contains no more predicate instances, and hence unfolding rules are inapplicable. This optimization is implemented in line 21 of Algorithm 4.1. As a result, some unsolvable goals will be identified early, in the unfolding phase. For example, the following goal:

\[
\{y, a, b\}; \{y \mapsto b \ast a \mapsto 0;\} \sim \{y \mapsto u \ast u \mapsto 0 \ast \text{lsseg}^1(u, 0, S)\}
\]

will fail immediately without exploring fruitless transformations on its flat heap, since no unfolding rules are applicable (assuming MaxUnfold = 1).

5.3 Symmetry reduction

Backtracking search often explores all reorderings of a sequence of rule applications, even if they commute, i.e., the order of applications does not change the end sub-goal. As an examples, consider the following goal:

\[
\{x, y, a, b\}; \{x \mapsto a \ast y \mapsto b \ast a \mapsto 0\} \sim \{x \mapsto a \ast y \mapsto b \ast b \mapsto 0\}
\]
Framing out $x \mapsto a$ and then $y \mapsto b$, reveals the unsolvable goal $\{a \mapsto 0\} \leadsto \{b \mapsto 0\}$; upon backtracking, the naïve search would try the two applications of Frame in the opposite order, leading to the same result.

We implemented a symmetry reduction optimization to eliminate redundant backtracking of this kind. To this end, we keep track of the footprint of each rule application, i.e., the sub-heaps of its goal’s pre and post that the application modifies. This enables us to identify whether two sequential rule applications commute. Next, we impose a total order on rule applications; line 7 of Algorithm 4.1 rejects a new rule application $\mathcal{R}$ if it commutes with an earlier application $\mathcal{R}'$ in the current derivation, but comes before $\mathcal{R}'$ in the total order.

### 5.4 Early Failure Rules

Sometimes one can identify an unsolvable goal by analyzing its pre and post. For example, the goal

$$\{x, y\}; \{a = 0; x \mapsto a\}; \leadsto \{a = u \land u \neq 0; x \mapsto u\}$$

is unsolvable because its pure postcondition is logically inconsistent with the precondition. To leverage this observation and eliminate redundant backtracking, we extend SSL with failure rules, which fire when they identify such unsolvable goals. Each failure rule is a terminal one, so it prevents further exploration of the (unsolvable) goal. Unlike other terminals, which conclude a successful derivation with skip or error, a failure rule emits a special spurious program magic. Algorithm 4.1 intercepts any appearance of magic in line 18, and treats the derivation as a unsuccessful. All failure rules are also invertible, hence the effect is to backtrack an application of an earlier rule.

Our set of failure rules is shown in Fig. 13. The rule $\text{PostInconsistent}$ identifies a goal where the the pure postcondition is logically inconsistent with the precondition. This is safe because during the derivation both assertions can only become stronger (as a result of unfolding rules); also, even if the postcondition still contains existentials, no instantiation of those existentials can produce a formula that is consistent with (let alone implied by) the precondition.

$$\Sigma; \Gamma; \{\phi; P\} \leadsto \{\psi; Q\} \mid \text{magic}$$

The rule $\text{PostInvalid}$ fires on a goal where the pure postcondition (which is free of existentials) is not implied by the precondition; this rule only applies when the precondition is free of predicate applications, and hence its pure part cannot be strengthened any further. The rule $\text{UnreachHeap}$ fires when the spatial pre and post contain only points-to heaplets, but the left-hand sides of these heaplets cannot be unified; in this case neither UnifyHeaps nor Write can make the heaplets match. Note that it is important for completeness that failure rules are checked after Inconsistency: if the pure precondition is inconsistent, the derivation should not fail, but should instead emit error.

### 5.5 Extensions

We wrap up this section with a description of two SSL extensions used by our implementation in order to expand the class of programs it can synthesize.

#### 5.5.1 Auxiliary Functions and Call Rule

The presented in Fig. 12 version of Call, which erases the tags from the callee’s post, hurts the framework’s completeness. While it is not unsafe to employ the predicates from the procedure call’s postcondition in further procedure calls, one cannot ensure that they denote “smaller heaplets” and thus that the program terminates.\(^{12}\) To

---

\(^{12}\)A similar issue is reported in the work by Rowe and Brotherston (2017) on verifying termination of procedural programs.
circumvent this limitation for particularly common scenarios, we had to introduce one divergence between SuSLik and SSL as shown in Fig. 12. Specifically, in the tool, we implemented support for stratified chained auxiliary function calls, i.e., calls on a heap resulted from another, preceding, call (e.g., in flatten w/append and insertion sort). To allow for them, we had to implement slightly different versions of induction/call rules, with an additional alternative in their premises, which instead of erasing tags of the corresponding part of the post ([Q_f]) would increment them: [Q_f]^{*+1}. This would prevent a call of the same function on the resulting heap fragment, but would enable calls of auxiliary functions, whose specs’ pre feature predicates with matching higher-level tags. Eventually, due to incrementation, no applicable functions would have left in the context Σ. While this extension is unlikely to break the SSL soundness and termination results (due to the limit of chained applications, enabled by growing tags), it would require us to generalize the well-foundedness argument in Sec. 3.2, and in the interest of time we did not carry out this exercise.

5.5.2 Branch Abduction. As described, SSL rules only emit conditional statements when unfolding an inductive predicate instance in the goal’s precondition via open. This prevents our framework from synthesizing some useful functions, in particular, those that branch on the content on a data structure rather than its shape. This source of incompleteness can easily be mitigated by adding a rule branch (Fig. 14), which is always applicable and generates a conditional statement with a non-deterministically chosen guard. Of course, in practice picking the guard blindly is not feasible. Our implementation employs a variation of a popular technique in program synthesis, known as condition (or branch) abduction (Alur et al. 2017; Kneuss et al. 2013; Leino and Milicevic 2012; Polikarpova et al. 2016). Instead of emitting conditionals eagerly, branch abduction tries to detect when the current program under consideration is a promising candidate for becoming a branch of a conditional, and then abduces a guard that would make this branch satisfy the specification.

The SSL variation of branch abduction piggy-backs on the failure rule postinvalid (Sec. 5.4), which detect a goal whose pure postcondition ψ has no existentials and does not follow from the precondition ϕ. Instead of rejecting this goal as unsolvable, branch abduction searches a small set of pure formulas (all atomic formulas over program variables in Γ); if it can find a formula ϕ’ such that ϕ ∧ ϕ’ ⇒ ψ, it abduces ϕ’ as the branch guard for the current goal.

For a simple example, consider the following synthesis goal that corresponds to computing a lower bound of two integers x and y:

\{x, y : r \rightarrow 0 \} \leadsto \{m \leq x \land m \leq y; r \rightarrow m\}

We first apply Pick with [m \rightarrow x], arriving at the goal \{r \rightarrow 0 \} \leadsto \{x \leq x \land x \leq y; r \rightarrow x\}. At this point, the postcondition is invalid, so branch abduction fires and infers a guard x ≤ y for the current derivation. It also emits a new goal for synthesizing the else branch, where the negation of the abduced condition is added to the precondition: \{¬(x \leq y); r \rightarrow 0 \} \leadsto \{m \leq x \land m \leq y; r \rightarrow m\}. If the synthesis of the else branch succeeds, the two branches are joined by a conditional; otherwise branch abduction fails.

6 IMPLEMENTATION AND EVALUATION

We implemented SSL-based synthesis as a tool, called SuSLik, in Scala, using Z3 (de Moura and Bjørner 2008) as the back-end SMT solver via the SCALASMT library (Cassez and Sloane 2017).13 We evaluated our implementation with the goal of answering the following research questions:

13The tool sources can be found at https://github.com/TyGuS/suslik.
Table 1. Benchmarks and SuSLik results. For each benchmark, we report the size of the synthesized Code (in AST nodes) and the ratio Code/Spec of code to specification; as well as synthesis times (in seconds): with all optimizations enabled (Time), without phase distinction (T-phase), without invertible rules (T-inv), without early failure rules (T-fail), without the commutativity optimization (T-com), and without any optimizations (T-all). T-IS reports the ratio of synthesis time in ImpSynt to Time. “-” denotes timeout of 120 seconds.

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
<th>Code</th>
<th>Code/Spec</th>
<th>Time</th>
<th>T-phase</th>
<th>T-inv</th>
<th>T-fail</th>
<th>T-com</th>
<th>T-all</th>
<th>T-IS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integers</td>
<td>swap two</td>
<td>12</td>
<td>0.9x</td>
<td>&lt; 0.1</td>
<td>&lt; 0.1</td>
<td>&lt; 0.1</td>
<td>&lt; 0.1</td>
<td>&lt; 0.1</td>
<td>&lt; 0.1</td>
<td>1.4</td>
</tr>
<tr>
<td></td>
<td>min of two²</td>
<td>10</td>
<td>0.7x</td>
<td>0.1</td>
<td>0.1</td>
<td>0.1</td>
<td>&lt; 0.1</td>
<td>0.1</td>
<td>0.2</td>
<td>1.4</td>
</tr>
<tr>
<td>Linked List</td>
<td>length²</td>
<td>21</td>
<td>1.2x</td>
<td>0.4</td>
<td>0.9</td>
<td>0.5</td>
<td>0.4</td>
<td>0.6</td>
<td>1.4</td>
<td>29x</td>
</tr>
<tr>
<td></td>
<td>max¹</td>
<td>27</td>
<td>1.7x</td>
<td>0.6</td>
<td>0.8</td>
<td>0.5</td>
<td>0.4</td>
<td>0.4</td>
<td>0.8</td>
<td>20x</td>
</tr>
<tr>
<td></td>
<td>min¹</td>
<td>27</td>
<td>1.7x</td>
<td>0.5</td>
<td>0.9</td>
<td>0.5</td>
<td>0.4</td>
<td>0.5</td>
<td>1.2</td>
<td>49x</td>
</tr>
<tr>
<td></td>
<td>singleton²</td>
<td>11</td>
<td>0.8x</td>
<td>&lt; 0.1</td>
<td>&lt; 0.1</td>
<td>&lt; 0.1</td>
<td>&lt; 0.1</td>
<td>&lt; 0.1</td>
<td>&lt; 0.1</td>
<td>&lt; 1.1</td>
</tr>
<tr>
<td></td>
<td>dispose</td>
<td>11</td>
<td>2.8x</td>
<td>&lt; 0.1</td>
<td>&lt; 0.1</td>
<td>&lt; 0.1</td>
<td>&lt; 0.1</td>
<td>&lt; 0.1</td>
<td>&lt; 0.1</td>
<td>&lt; 1.1</td>
</tr>
<tr>
<td></td>
<td>initialize</td>
<td>13</td>
<td>1.4x</td>
<td>&lt; 0.1</td>
<td>0.1</td>
<td>0.1</td>
<td>&lt; 0.1</td>
<td>&lt; 0.1</td>
<td>&lt; 0.1</td>
<td>&lt; 1.1</td>
</tr>
<tr>
<td></td>
<td>copy³</td>
<td>35</td>
<td>2.5x</td>
<td>0.2</td>
<td>0.3</td>
<td>0.3</td>
<td>0.1</td>
<td>0.2</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>append³</td>
<td>19</td>
<td>1.1x</td>
<td>0.2</td>
<td>0.3</td>
<td>0.3</td>
<td>0.2</td>
<td>0.3</td>
<td>0.7</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>delete³</td>
<td>44</td>
<td>2.6x</td>
<td>0.7</td>
<td>0.5</td>
<td>0.3</td>
<td>0.2</td>
<td>0.3</td>
<td>0.7</td>
<td>-</td>
</tr>
<tr>
<td>Sorted List</td>
<td>prepend¹</td>
<td>11</td>
<td>0.3x</td>
<td>0.2</td>
<td>1.4</td>
<td>8.35</td>
<td>0.1</td>
<td>0.1</td>
<td>-</td>
<td>48x</td>
</tr>
<tr>
<td></td>
<td>insert¹</td>
<td>58</td>
<td>1.2x</td>
<td>4.8</td>
<td>-</td>
<td>-</td>
<td>5.0</td>
<td>-</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>insertion sort¹</td>
<td>28</td>
<td>1.3x</td>
<td>1.1</td>
<td>1.8</td>
<td>1.3</td>
<td>1.2</td>
<td>1.2</td>
<td>74.2</td>
<td>82x</td>
</tr>
<tr>
<td>Tree</td>
<td>size</td>
<td>38</td>
<td>2.7x</td>
<td>0.2</td>
<td>0.3</td>
<td>0.2</td>
<td>0.2</td>
<td>0.3</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>dispose</td>
<td>16</td>
<td>4.0x</td>
<td>&lt; 0.1</td>
<td>&lt; 0.1</td>
<td>&lt; 0.1</td>
<td>&lt; 0.1</td>
<td>&lt; 0.1</td>
<td>&lt; 0.1</td>
<td>&lt; 1.1</td>
</tr>
<tr>
<td></td>
<td>copy</td>
<td>55</td>
<td>3.9x</td>
<td>0.4</td>
<td>49.8</td>
<td>-</td>
<td>0.8</td>
<td>1.4</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>flatten w/append</td>
<td>48</td>
<td>4.0x</td>
<td>0.4</td>
<td>0.6</td>
<td>0.5</td>
<td>0.4</td>
<td>0.4</td>
<td>0.6</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>flatten w/acc</td>
<td>35</td>
<td>1.9x</td>
<td>0.6</td>
<td>1.7</td>
<td>0.7</td>
<td>0.5</td>
<td>0.6</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>BST</td>
<td>insert²</td>
<td>58</td>
<td>1.2x</td>
<td>31.9</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>11x</td>
</tr>
<tr>
<td></td>
<td>rotate left¹</td>
<td>15</td>
<td>0.1x</td>
<td>37.7</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0.5x</td>
</tr>
<tr>
<td></td>
<td>rotate right¹</td>
<td>15</td>
<td>0.1x</td>
<td>17.2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0.8x</td>
</tr>
</tbody>
</table>

1 From (Qiu and Solar-Lezama 2017) ² From (Leino and Milicevic 2012) ³ From (Qiu et al. 2013)

(1) **Generality:** Is SuSLik general enough to synthesize a range of nontrivial programs with pointers?
(2) **Utility:** How does the size of the inputs required by SuSLik compare to the size of the generated programs? Does SuSLik require any additional hints apart from pre- and post-conditions? What is the quality of the generated programs?
(3) **Efficiency:** Is it efficient? What is the effect of optimizations from Sec. 5 on synthesis times? What is the quality of the generated programs?
(4) **Comparison with existing tools:** How does SuSLik fare in comparison with existing tools for synthesizing heap-manipulating programs, specifically, ImpSynt (Qiu and Solar-Lezama 2017)?

### 6.1 Benchmarks

In order to answer these questions, we assembled a suite of 22 programs listed in Tab. 1. The benchmarks are grouped by the main data structure they manipulate: integer pointers, singly linked lists, sorted singly linked lists, binary trees, and binary search trees.

To facilitate comparison with existing work, most of the programs are taken from the literature on synthesis and verification of heap-manipulating programs: the ImpSynt synthesis benchmarks (Qiu and Solar-Lezama 2017), the Jennisys synthesis benchmarks (Leino and Milicevic 2012), and the Dryad verification benchmarks (Qiu et al. 2013). We manually translated these benchmarks into the input language of SuSLik, taking care to preserve their semantics. Dryad and ImpSynt use the Dryad dialect of separation logic as their specification language, hence the translation in this case was relatively straightforward. As an example, consider an ImpSynt specification and its SuSLik equivalent in Fig. 15. The “??” are part of the ImpSynt spec language, denoting unknown holes to be filled by the synthesizer. The main difference between the two pre-/post-condition
 Nadia Polikarpova and Ilya Sergey

\begin{verbatim}
loc srtl_insert(loc x, int k)
requires srtl(x)
ensures srtl(ret) ∧
  len(ret) = old(len(x)) + 1 ∧
  min(ret) = \{ 0 ≤ n ∧ 0 ≤ k ∧ k ≤ 7 ;
                ret ↦ k + srtl(x, n, lo, hi) \} ∧
  max(ret) = \{ 0 ≤ n ∧ 0 ≤ k ∧ k ≤ 7 ;
                ret ↦ k + srtl(x, n, lo, hi) \} ∧

{ if (cond(1)) {
  loc ?? := new;
  return ??;
} else {
  statement(1);
  loc ?? := srtl_insert(??, ??);
  statement(1);
  return ??;
}
\end{verbatim}

Fig. 15. (left) The \textsc{ImpSynt} input for the sorted list insertion; (right) The \textsc{SuSLik} input for the same benchmark.

pairs is that the \textsc{Dryad} logic supports recursive functions such as \texttt{len}, \texttt{min}, and \texttt{max}; in \textsc{SuSLik} this information is encoded in more traditional SL style: by passing additional ghost parameters to the inductive predicate \texttt{srtl}. The extra precondition $0 ≤ n ∧ 0 ≤ k ∧ k ≤ 7$ in \textsc{SuSLik} corresponds to implicit axioms in \textsc{ImpSynt} (in particular, the condition on $k$ is due to its encoding of list elements as unsigned 3-bit integers—there is no such restriction in \textsc{SuSLik}). In addition to benchmarks from the literature, we also added several new programs that show-case interesting features of \textsc{SuSLik}.

6.2 Results

Evaluation results are summarized in Tab. 1. All experiments were conducted on a commodity laptop (2.7 GHz Intel Core i7 Lenovo Thinkpad with 16GB RAM).

6.2.1 Generality and Utility. Our experiment confirms that \textsc{SuSLik} is capable of synthesizing programs that manipulate a range of heap data structures, including nontrivial manipulations that require reasoning about both the shape and the content of the data structure, such as insertion into a binary search tree. We manually inspected all generated solutions, as well as their accompanying SSL derivations, and confirmed that they are indeed correct.\footnote{In the future, we plan to output SSL derivations as SL proofs, checkable by a third-party system such as VST (Appel 2011).} Perhaps unsurprisingly, some of the solutions were not entirely intuitive: as one example, the synthesized version of list copy, in a bizarre yet valid move, \textit{swaps the tails} of the original list and the copy at each recursive call!

Two of the programs in Tab. 1 make use of auxiliary functions: “insertion sort” calls “insert”, and “tree flatten w/append” calls the “append” function on linked lists. The specifications of auxiliary functions have to be supplied by the user (while their implementations can, of course, be synthesized independently). Alternatively, tree flattening can be synthesized without using an auxiliary function, if the user supplies an additional list argument that plays the role of an accumulator (see “tree flatten w/acc”). As such, \textsc{SuSLik} shares the limitation of all existing synthesizers for recursive functions: they require the initial synthesis goal to be inductive, and do not try to discover recursive auxiliary functions (which is a hard problem, akin to lemma discovery in theorem proving).

For simple programs specification sizes are mostly comparable with the size of the synthesized code, whereas more complex benchmarks is where declarative specifications really shine: for example, for all Tree programs, the specification is at most half the size of the generated code. Three
notable outliers are “prepend”, “rotate left”, and “rotate right”, whose implementations are relatively short, while the specification we inherited from ImpSynt describes the effects of the functions on the minimum and maximum of the list/tree. Note that the specification sizes we report exclude the definitions of inductive predicates, which are reusable, and are shared between the benchmarks.

6.2.2 Efficiency. SuSLik has proven to be efficient in synthesizing a variety of programs: all 22 benchmarks are synthesized within 40 seconds, and all but four of them take less than a second.

In order to assess the impact on performance of various optimizations described in Sec. 5, Tab. 1 also reports synthesis times with each optimization disabled: the column T-phase corresponds to eliminating the distinction between phases; T-inv corresponds to ignoring rule invertibility; T-fail corresponds to dropping all failure rules; T-com corresponds to disabling the symmetry reduction; finally, T-all corresponds to a variant of SuSLik with all the above optimizations disabled. The results demonstrate the importance of optimizations for nontrivial programs: 8 out of 22 benchmarks time out when all optimizations are disabled. The simpler benchmarks (e.g., swap) do not benefit from the optimizations at all, since they do not exhibit a lot of backtracking. At the same time, all three BST benchmarks time-out as a result of disabling even a single optimization.

6.2.3 Comparison with Existing Synthesis Tools. We compare SuSLik with the most closely related prior work on ImpSynt (Qiu and Solar-Lezama 2017). Out of the 14 benchmarks from (Qiu and Solar-Lezama 2017) successfully synthesized by ImpSynt, we excluded 5 that are not structurally recursive (4 of them use loops, and bst_del_root uses non-structural recursion); the other 9 were successfully synthesized by SuSLik. The qualitative difference in terms of the required user input is immediately obvious from the representative example in Fig. 15: in addition to the declarative specification, ImpSynt requires the user to provide an implementation sketch, which fixes the control structure of the program, the positions of function calls, and the number of other statements. These additional structural constraints are vital for reducing the size of the search space in ImpSynt. Instead, SuSLik prunes the search space by leveraging the structure inherent in separation logic proofs, allowing for more concise, purely declarative specifications.

Despite the additional hints from the user, ImpSynt is also less efficient: as shown in the column T-IS of Tab. 1, on 6 out of 9 common benchmarks, ImpSynt takes at least an order of magnitude longer than SuSLik, even though the ImpSynt experiments were conducted on a 10-core server with 96GB of RAM.

On the other hand, ImpSynt is more general than SuSLik in that it can synthesize both recursive and looping programs. We discuss this and other limitations of SuSLik in more detail in Sec. 7.

7 LIMITATIONS AND DISCUSSION

There are several known limitations of Synthetic Separation Logic and SuSLik design.

SSL does not support synthesis of programs with while-loops, as this would require discovering loop invariants, which significantly increases the search space; instead, the initial goal is considered as inductive and handled via Induction rule. As of now, SSL does not allow for mutually-recursive inductive predicates. While not impossible in principle, this would require us to explore advanced techniques for inductive proofs (Ta et al. 2016) and also generalize the use of tags; we plan to look into this in the future. By limiting the number of unfoldings, via Open and Close rules, via MaxUnfold, we circumvent a commonly known decidability problem of solving entailments in the presence of general inductive predicates (Antonopoulos et al. 2014), but this also prevents some non-unreasonable and perfectly specifiable in SSL programs from being synthesized, e.g., allocating a large constant-size list.

Currently, SSL and SuSLik cannot automatically synthesize programs that are not structurally recursive with some inductive predicate, such as, for instance, merging sorted lists or Merge-Sort.
One approach to mitigate this limitation is to prove termination by showing that each recursive call decreases the value of a custom termination metric; this technique is used in several automated verifiers and synthesizers (Leino 2013; Polikarpova et al. 2016). A termination metric maps the tuple of function’s arguments into an element of a set with a pre-defined well-founded order (usually a tuple of natural numbers), and can be either provided by the user or inferred by the synthesizer.

Some of SSL limitations are inherent for Separation Logics in general: SLs are known to work well with disjoint tree-like linked structures, and programs, whose recursion scheme matches the data definition, but not so well with ramified data structures, e.g., graphs. To address those, one could integrate a more powerful, ramified version of FRAME rule (Hobor and Villard 2013) into SSL, but this would likely require more hints from the user, thus, reducing the utility of the approach.

8 RELATED WORK

There are two main directions in the area of program synthesis: synthesis from informal descriptions (such as examples, natural language, or hints) (Albarghouthi et al. 2013; Feng et al. 2017; Feser et al. 2015; Murali et al. 2018; Osera and zdancewic 2015; Polozov and Gulwani 2015; Smith and Albarghouthi 2016; Yaghmazadeh et al. 2017) and synthesis from formal specifications. We will only discuss the more relevant latter direction. The goal of this type of program synthesis is to obtain a provably correct program.

In this area, there is a well-known trade-off between three dimensions: how complex the synthesized programs are, how strong the correctness guarantees are, and how much input is required from the user. On one end of the spectrum there are interactive synthesizers (Delaware et al. 2015; Itzhaky et al. 2016), which can be very expressive and provide strong guarantees, but the user is expected to guide the synthesis process (although, usually, with aid of dedicated proof tactics). On the other end, there is fully automated synthesis for loop- and recursion-free programs over simple domains, like arithmetic and bit-vectors (Alur et al. 2017; Gulwani et al. 2011). Our work lies in the middle of this spectrum, where synthesis is automated but programs are more expressive.

In the presence of loops or recursion, verifying candidates becomes nontrivial. Synthesizers like Sketch (Solar-Lezama 2013) and Rosette (Torlak and Bodík 2014) circumvent this problem by resorting to bounded verification, which only provides restricted guarantees and has scalability issues due to path explosion. In contrast, our work relies on unbounded deductive verification.

Among synthesis approaches that use unbounded verification, synthesizers like Leon (Kneuss et al. 2013) and Synquid (Polikarpova et al. 2016) focus on pure functional (recursive) programs, which are an easier target for unbounded verification. Proof-theoretic synthesis (Srivastava et al. 2010) is capable of synthesizing imperative programs with loops and arrays, but no linked structures; they pioneered the idea of synthesizing provably-correct programs by performing symbolic (SMT-based) search over programs and their verification conditions simultaneously.

Finally, the two pieces of prior work that are most closely related to ours in terms of scope are Jennisys (Leino and Milicevic 2012) and Natural Synthesis (Qiu and Solar-Lezama 2017), both of which generate provably-correct heap-manipulating programs. Both of them are essentially instances of proof-theoretic synthesis with a program logic for reasoning about the heap. To that end, Jennisys uses the Dafny verifier (Leino 2013), which supports expressive yet undecidable specifications, and often requires hints from the user, so in practice the tool doesn’t scale to complex examples (for example, none of their benchmarks performs mutation). Natural Synthesis uses Dryad (Madhusudan et al. 2012; Qiu et al. 2013), a decidable program logic for reasoning about heap-manipulating programs. The downside of this approach is that whole-program symbolic search doesn’t scale to larger programs; to mitigate this, they require the user to provide sketches with substantial restrictions on the structure of the program. Our approach does not require sketches (but on the other hand, we do not support loops).

The recent tool FootPatch by van Tonder and Le Goues (2018) is very close in its methods and goals to SuSLik. FootPatch builds on Infer (Calcagno and Distefano 2011), an open-source SL-based static analyzer by Facebook, using it for automated program repair. It takes the intermediate assertions, provided by Infer for programs with bugs, such as resource and memory leaks, and null dereferences, and constructs additive patches based on the observed discrepancy. In this, it acts similarly to our AbduceCALL rule. FootPatch does not synthesize patches that would involve recursion or complex control flow.

Instead of whole-program symbolic search, like in proof-theoretic synthesis, our work follows the tradition of deductive synthesis, i.e., backtracking search in the space of program derivation composed of synthesis rules, which gradually transform a specification into a program. This tradition originates from the work by Manna and Waldinger (1980), and similar ideas have been used in more recent synthesis work (Delaware et al. 2015; Kneuss et al. 2013; Polikarpova et al. 2016). In particular, the overall structure of our synthesis algorithm (backtracking and-or search) is similar to Leon (Kneuss et al. 2013), but our rules focus on heap manipulation, whereas their rules focus on synthesizing pure terms (so in fact Leon can be used as a component by our algorithm).

Recent work on Optitian (Miltner et al. 2018) is very different in scope—they synthesize bijective string lenses from regular expression specifications and examples—but has interesting similarities in the technique. Their pre- and post-condition are regexes, and their technique tries to “align” them by e.g., unfolding the Kleene star; this is similar to how SuSLik tries to align the spatial pre- and post-condition by unfolding predicates.

Deductive synthesis is closely related to proof search, and there has been recent resurgence in applying proof-theoretic techniques, like focusing, to program synthesis (Frankle et al. 2016; Scherer 2017). But none of them do it for a complex logic that can reason about stateful programs.

Despite the vast space of available tools for symbolic verification based on Separation Logic: Smallfoot (Berdine et al. 2006), HTT (Nanevski et al. 2010), Bedrock (Chipala 2011), SLAYER (Berdine et al. 2011), HIP/SLEEK (Chin et al. 2011), VeriFast (Jacobs et al. 2011), SLAD (Bouajjani et al. 2012), GRASShopper (Piskac et al. 2014b), Viper (Müller et al. 2016), Cyclist (Rowe and Brotherston 2017), to name just a few, to the best of our knowledge none of them have been employed for deriving programs from specifications. It is certainly our hope that this work will bring new synergies between the research done in verification, theorem proving, and program synthesis communities.

For instance, in our approach to establish termination of SSL-synthesized programs, we used techniques close in spirit to the methods for proving total correctness in type/SL-based frameworks. E.g., SSL’s tags might be seen as a variant of resource capacities used in HIP/SLEEK (Le et al. 2014). Our use of Definition 3.1 of sized validity is similar to the induction on the finiteness of the heap used by Le and Hobor (2018) in their work on a logic for fractional shares. Tagged predicates we use are reminiscent to the ▷-modality in type theories for state and recursion (Appel et al. 2007).

9 CONCLUSION

In their seminal paper, Manna and Waldinger (1980) set forth an agenda for deductive synthesis of functional programs: “theorem provers have been exhibiting a steady increase in their effectiveness, and program synthesis is one of the most natural application of those systems”.

In this work, we moved this endeavour to an uncharted territory of stateful computations. For this, we employed a proof system which, instead of a pure type theory (Martin-Löf 1984), is based on Separation Logic—a Type Theory of State (Nanevski 2016). Taking this vision as a guiding principle, we designed Synthetic Separation Logic—a modest extension of Separation Logic, tailored for program synthesis, and implemented a proof search algorithm for it. In doing so, we took full advantage of the power of local reasoning about state (O’Hearn et al. 2001), which resulted in a principled and fast approach for synthesizing provably correct heap-manipulating programs.
ACKNOWLEDGMENTS

We wish to thank Aquinas Hobor and Reuben Rowe for their insightful and extremely detailed comments on presentation, formalism, and examples. Their technical feedback has helped immensely to bring out the best of this paper. We also wish to thank Shachar Itzhaky and Ranjit Jhala for their comments on the draft. We are very grateful to Franck Cassez for his help with configuring and using ScalaSMT. Sergey’s research was supported by a generous gift from Google.

REFERENCES


Theorem A.1 (Theorem 3.3, Soundness of SSL). For any \( n, \Lambda', \) if
\[
\begin{align*}
\text{(i)} & \quad \Sigma'; \Gamma; \{P\} \leadsto \{Q\} \mid c \text{ for a goal named } f \text{ with formal parameters } \Gamma \triangleright \overline{x}, \\
\text{(ii)} & \quad \Sigma' \text{ is such that } \text{coh}(\Lambda', \Sigma', n), \text{ and} \\
\text{(iii)} & \quad \text{for all } p^0(\overline{e}), \phi, P, \text{ such that } \{P\} = \{\phi; p^0(\overline{e}) \ast P\}, \text{ taking } \mathcal{F} \triangleright f(\overline{x}) \defeq \{\phi; p^1(\overline{e}) \ast [P]\}\{\{Q\}\}, \\
\Sigma', \mathcal{F}; \Gamma; \{P\} c \{Q\} \text{ is } n'-\text{valid for all } n' < n \text{ wrt. } \Delta \triangleright \Delta', f(\overline{t_i} \overline{x_i}) \{\{c\}\},
\end{align*}
\]
then \( \Sigma'; \Gamma; \{P\} \mid c \{Q\} \) is \( n\)-valid wrt. \( \Delta \).

Proof. Since \( c \) has been produced by an SSL derivation, it is (\( ; \))-associated to the right.

The proof is by the outer-level (well-founded) induction on the “footprint size” \( n \). For each fixed \( n \), the proof is by an inner-level induction on the structure of derivation \( \Sigma'; \Gamma; \{P\} \leadsto \{Q\} \mid c \), with symbolic one-step execution (via \( \leadsto \)). In that induction step we rely on the fact that the residual “suffix” program is already valid, so we only need to show that applying a single rule preserves the validity, while “appending” a command \( c \) in front of an already synthesized program.

The inner proof routine is straightforward for or (sub-)goals, where the spatial part of \( P \) contains no predicate instances.
All non-operational rules (FRAME, PICK, SUBSTLEFT, EMP, NULLNOTLVAL, etc) either instantiate existentials in the post, weaken the pure obligations, or reduce the footprint, which is sound due to locality of reading and writing (O’Hearn et al. 2001) and immutability of local variables; the soundness of operational (READ, WRITE, etc) rules is due to the soundness of SL. Specifically:

- **Case: EMP.** The result follows immediately from Definition 3.1 of validity for any n.
- **Case: SUBSTLEFT.** The result follows immediately from Definition 3.1 of validity for any n.
- **Case: NULLNOTLVAL.** The non-nullness is encoded by the spatial precondition part (Reynolds 2002), so the transformation is sound. The result follows immediately from Definition 3.1 of validity for any heap size n.
- **Case: STARPARTIAL.** The inequality of the two locations is encoded by the spatial part of the precondition, so the transformation is sound. The result follows immediately from Definition 3.1 of validity for any heap size n.
- **Case: INCORRECTNESS.** The result follows immediately from Definition 3.1 of validity for any n, as no physical pre-heap does satisfy $\phi$, so it is safe to emit error.
- **Case: FRAME.** The FRAME rule in SSL is different from its counterpart in vanilla SL in that it does not require a side condition saying that $R$ must not contain program variables that are modified by the program to be synthesized. Due to locality of read/write/malloc/free operations, they could not depend on $R$, as already synthesized in the residual program, hence adding $R$ to post will not break validity, given that $R$ is also added to the precondition.
- **Case: READ.** The synthesized read is safe, as the corresponding pointer is present in the precondition. Furthermore, it creates a program-level variable, which substantiates the environment variable $y$, used for the synthesis in the subgoal, hence the new program is valid according to Definition 3.1.
- **Case: ALLOC.** The subgoal has been synthesized in the larger footprint, afforded by allocation. The soundness of the rule follows from the axiomatization of malloc (O’Hearn et al. 2001).
- **Case: FREE.** Since the subgoal’s result is valid in a smaller pre-heap footprint and does not access any variables from $R$, it is safe to deallocate it, hence the resulting program is valid.
- **Case: ABduceCALL.** The validity is by the properties of the sequential composition $c_1; c_2$ and the soundness of the frame rule of SL, applied as follows to the first sub-goal:

$$\Sigma; \Gamma; \{\phi; F \} \leadsto \{\phi; F'\} \mid c_1$$

- **Case: UNIFYHEAPS.** Since the unification only instantiates existentials, making the goal more specific, and unified variables will not appear in the program freely, the validity is by soundness of the SL’s Auxiliary Variable Elimination rule (O’Hearn et al. 2001).
- **Case: PICK.** By the soundness of substitution and auxiliary variable elimination.
- **Case: UNIFYPURE.** By the soundness of substitution and auxiliary variable elimination.
- **Case: SUBSTRIGHT.** By the soundness of substitution and auxiliary variable elimination.
- **Case: CLOSE.** Validity follows from the fact that the sub-goal is valid in the presence of the elaborated postcondition $\{\psi \wedge [\sigma]_{k} \wedge [\sigma]_{k}; Q * R'\}$ By the definition of $\models_{\Sigma}^{\chi}$, this heap satisfies the corresponding predicate definition in the initial goal’s postcondition.

In the case of predicate instances in the precondition, we take advantage of the tag machinery and the assumptions (ii)–(iii) of the Theorem’s statement.

- **Case: INDUCTION.** The assumption (ii) of the inductive hypothesis is satisfied via the initial assumption (iii) and 1-tagging of the recursive hypothesis’s precondition, so it will only be applicable to heaps of a size strictly smaller than n (follows from OPEN and CALL).
• **Case:** Open. The validity is due to the fact that the emitted if-else will combine the sub-programs, that are already valid wrt. their pres/posts. The access to those elaborated pres/posts, ensuring the satisfiability of the elaborated precondition in each branch is due to the conditionals \( \xi_j \), which are the same as the corresponding guard of the predicate instance being opened.

• **Case:** Call. This is the most interesting case. Validity of a function body’s substitution is via (ii). Notice that Call cannot be the first rule applied in the derivation, as then all predicate instances are 0-tagged, hence it should follow Open, which unfolds the instances, exposing smaller sub-heaps captured by their clauses (due to well-foundedness of the predicates), which are now amenable for using Call on them.

The remaining reasoning differs depending on whether the function \( f \) being called is a user-provided auxiliary one, or a recursive call to the top-level goal. If a function being applied is a user-provided specification (i.e., not a recursive self), then its validity is asserted by the second clause of Definition 3.2, otherwise the call is recursive, and will only take place on a smaller heap, satisfying the third option of Definition 3.2.