Compositional Non-Termination Proving

AZALEA RAAD, Imperial College London, UK
JULIEN VANEGUE, Bloomberg, USA
PETER O'HEARN, University College London and Lacework, UK

Program termination is a classic non-safety property that cannot in general be witnessed by a finite trace. This makes testing for non-termination challenging, and also makes it a natural target for symbolic proof. To confirm that non-termination is a practical and not theoretical problem, we provide a manual analysis of CVE's due to non-termination, corresponding to security issues such as DOS vulnerabilities, finding 916 since 2000. Discovering non-termination is an under-approximate problem. We thus present UNTer, a *sound and complete* under-approximate logic for proving non-termination. We then extend UNTer with separation logic and develop UNTer$^{\text{SL}}$ for programs that manipulate the heap. UNTer$^{\text{SL}}$ yields a compositional proof method, which is amenable to automation via program analysis tools based on under-approximation and bi-abduction. We briefly describe a prototype tool, Pulse$^{\infty}$, under development, which extends the compositional the Pulse analyser from Facebook.

Additional Key Words and Phrases: Divergence, non-termination, under-approximation, incorrectness logic

1 INTRODUCTION

Why Prove Non-termination? Non-termination is a fundamental problem in computer science, dating back to the halting problem. Assuming an unbounded memory or tape, neither it nor its complement is recursively enumerable, making it difficult to approach using testing. This makes non-termination an attractive target for symbolic proof techniques.

Apart from its fundamental nature, one can also ask: is non-termination a practical problem? To understand this better we carried out a manual evaluation of CVE's, security bugs such as denial of service which are due to non-termination. We found 916 such CVE's between 2000 and 2022. Sometimes, for ongoing computations such as operating systems, potential non-termination is desirable and unavoidable. But, we may conclude that import and do have an effect.

Interestingly, we did not detect any reduction in non-termination CVE's during this period. For example, we found 4 such bugs from 2000 and 28 from 2022. We stress that our manual approach might have missed some non-termination CVE's, there is more code in 2022 than in 2000, and the classification of non-termination CVE's might be non-uniform. This data, however, motivated our work on the science and engineering of tools for detecting non-termination bugs.

Why Compositional? A compositional analysis is one where the analysis result of a composite program is computed from those of its constituent parts [5]. Compositionality enables program analysis to be deployed as part of a code review process, where code snippets in a pull request are analysed without the need to re-analyse the entire program (or even to have an entire program, which might not yet exist). A case study from Facebook [14] describes how deploying a compositional static analysis tool on pull requests achieved a 70% fix rate, while the same analysis had a near 0% fix rate for a batch deployment (where a list of bugs is given outside of code review). This illustrates how a deployment of static analysis that meets programmers in their workflows can have considerable advantages over ones that ask them to leave their flow. (See the Facebook article [14] and a related article from Google [26] for more information.)

It stands to reason that if an accurate non-termination prover is developed which is fast enough to be deployed at pull-request time, then it would have the potential to have more non-termination bugs fixed, early. We will not in this paper go so far as setting up an industrial deployment of

Authors' addresses: Azalea Raad, azalea.raad@imperial.ac.uk, Imperial College London, UK; Julien Vanegue, jvanegue@bloomberg.net, Bloomberg, USA; Peter O'Hearn, p.ohearn@ucl.ac.uk, University College London and Lacework, UK.

non-termination proving in the CICD system of a company, but we take the Facebook/Google experience referenced above as motivation for our scientific goals: to establish a compositional proof method together with an algorithm which allow for automatic compositional program analysis, and initial experiments to probe its feasibility.

Our Approach. Proving non-termination is an *under-approximation* problem as the aim is to establish the *existence* of non-terminating executions. Therefore, for compositional reasoning it is natural to consider a formalism akin to incorrectness logic (IL) [23], which brings the compositional nature of Hoare logic to bug proving. It turns out the form of under-approximation we need is a reversed form of that in IL, based on what is called the 'backwards under-approximate triple' by Möller et al. [22] and the 'total Hoare triple' by de Vries and Koutavas [13].

The *backwards under-approximate* (BUA) triple $\vdash_{\mathsf{B}} [p]\ \mathsf{C}\ [ok\colon q]$ denotes that p is a *subset* of the states from which q can be reached executing C. That is, from any state in p it is possible to reach some state in q by executing C. This triple is forwards in terms of reachability, but backwards in terms of under-approximation (mirroring IL): q under-approximates the weakest *possible* precondition, wpp, of C on q: $p \subseteq \mathsf{wpp}(\mathsf{C}, q)$. Here, wpp is the inverse image of the C (relational) semantics, obtained by running Dijkstra's strongest post-condition on the reversal of C.

To this form of under-approximate (UA) triples we add another, for *divergence*. Specifically, we develop *under-approximate non-termination logic* (UNTER), where we write $\vdash [p]\ \mathsf{C}\ [\infty]$ to denote that every state in p leads to a divergent (infinite) execution via C. Note that this does not state that *every* execution diverges; rather, each pre-state leads to *some* divergent execution. Given these triples we can state a proof rule for divergence as follows:

$$\frac{\vdash_{\mathsf{B}} [p \land B]\ \mathsf{C}\ [ok\colon p \land B]}{[p \land B]\ \mathsf{while}\ (B)\ \mathsf{C}\ [\infty]}$$

The idea behind this rule is very simple. As $p \land B$ holds initially, we know that after one loop iteration we can get to a state where $p \land B$ continues to hold because of the triple in the premise. And in that case we can take one more step, *ad infinitum*.

This proof method is related intuitively to a method of non-termination testing whereby one looks for a concrete state to which a loop returns: this would witness divergence as one can get back to the same state again. As a testing method this approach is incomplete, in the presence of unbounded resources (e.g. a Turing machine tape) which gives rise to infinitely many states: then it is possible to diverge with returning to the same state twice. But the logical proof method uses a logical assertion and not a concrete state, and is in fact complete for proving non-termination as we prove later (take p to be the set of all states that lead to divergence).

The proof method is also related to the idea of 'recurrence sets' in a fundamental paper of Gupta et al. [17]. We say more on the relation to their and other work in §9.

Our aim is to *automate* divergence proof rules such as that above. There are several key observations in our approach. First, and remarkably, if we apply the strategy used commonly in abstract interpretation, namely iterating the abstract semantics of loops until we reach a fixpoint, then will have proven non-termination of a loop when a fixpoint is reached. In abstract interpretation this would not imply divergence, but with our under-approximate UNTER logic it does. However, while we can employ the usual method of fixpoint iteration, since not all loops diverge, we additionally need a way to stop the analysis before a fixpoint is reached. It turns out that we can employ similar techniques to IL and bounded model checking, by simply stopping after some fixed number of iterations even when we do not have a fixpoint. This flexibility is not available in Hoare logic, or in over-approximate abstract interpretation, where stopping early is unsound.

Second, by detailing the relationship to the original IL we reveal additional possibilities for automation. Indeed, the BUA proof system is almost the same as that of IL, with the difference limited to the rule of consequence (see §3, §4). The use of the backwards predicate transformer wpp perhaps suggests to attempt a backwards program analysis, at least for a whole-program analysis: given a post, such an analysis would compute an under-approximation of backwards reachability at each program point; in a sense, the mirror image of Floyd's method of calculating over-approximations for forwards reachability. However, a forwards-running analysis is also possible, as long as we *abduce* preconditions as we go forwards: this semantics calculates a collection of triples at each program point, connecting procedure-entry to the program point. In addition to furnishing a compositional inter-procedural analysis, abduction is necessary here: there is no forwards predicate transformer semantics, evidenced by the fact that for some programs C and pre-conditions p there is no post-condition delivering a valid triple $\vdash_{\mathrm{B}} [p]\ \mathrm{C}\ [ok\colon ??]$.

The third key point for automation is that the close connection between the BUA and original IL proof theories suggests a method of automation that leverages *separation logic* [18], and which is obtained by small changes and a fundamental addition to the existing Pulse program analyser [19] from Facebook. We observe that Pulse uses a restricted version of the rule of consequence, making it compatible both with BUA and IL triples. We thus develop UNTer$^{\text{SL}}$ as an extension of UNTer (with divergent triples) with separation logic We then extend Pulse with divergent triples and develop Pulse$^{\infty}$, a prototype compositional non-termination prover underpinned by UNTer$^{\text{SL}}$.

Contributions and Outline. Our contributions in this paper are as follows.

§2 We provide a manual classification of CVE's related to non-termination, providing data to go with existing anecdata, confirming the real-world prevalence of non-termination bugs important enough to be judged as critical security issues.

§3 We present an intuitive overview of BUA and IL reasoning, and describe how we extend them to reason about non-termination.

§4 We present UNTer as a BUA proof system and extend it to account for non-termination, yielding a compositional proof method.

§5 We present several examples of divergence and show how we can detect them using UNTer.

§6 We present the semantic model of UNTer and show that it is *sound* and *complete*.

§7 We develop UNTer$^{\text{SL}}$ by extending UNTer with separation logic for heap reasoning.

§8 We observe that an existing under-approximate reasoning tool, Pulse, can be simply extended to provide a compositional, incremental prover for non-termination, Pulse$^{\infty}$: we outline our prototype implementation of Pulse$^{\infty}$ which is in progress.

§9 We discuss the related work and future work.

Additional Material. The proofs of all stated theorems in the paper are given in the accompanying technical appendix.

2 DIVERGENCE VULNERABILITIES

Divergence bugs are widespread across a number of programming languages. We present several examples taken from the Common Vulnerabilities and Exposures (CVE) database and categorize them along common cases of vulnerabilities – see Fig. 1 for the prevalence of divergence bugs. We focus on control-flow-related divergent behaviours brought about on certain inputs. In particular, we focus on capturing

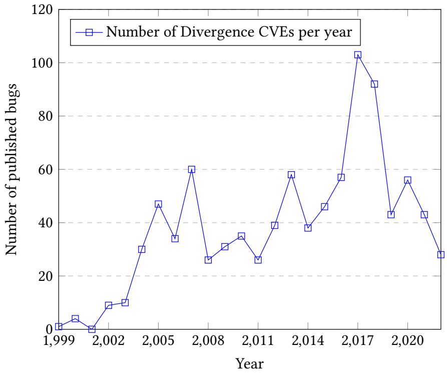

Fig. 1. Vulnerability trend for divergence bugs

behaviours where termination is not intended (unlike interactive programs whose non-termination is expected and induced from an infinite message loop treating streams of incoming input requests), and guarantee that our approach focuses on detecting the most widespread vulnerability classes in publicly available code. We have selected a number of bugs that show a wide cross-section of programming languages and control-flow conditions.

Infinite Loops. Recursive implementations are common in parsers. In some cases, the loop condition is driven by the value of an integer variable (e.g. remaining stream bytes to be read), which can be dynamically set within the parsing loop as the parser reads the input. If the decrement value of such variable in an iteration is set to 0, the loop makes no more progress leading to an unintended divergence. Specifically, when a parsing sub-function f is called to treat a sub-case of input data type, if f returns 0, then the loop makes no progress reading input. Such an example was found in the popular Wireshark network analyser, leading to CVE-2022-3190 (see §G.1).

Infinite Recursion. Infinite recursion bugs are one of the main sources of divergence. Infinite recursion bugs are well-known to parser developers when the recursive parsing function allows input variable expansion or other generative capability, such that when the newly generated input after expanding variables is parsed through a recursive call, the number of subsequently needed recursive calls remains non-null. Such a case was seen in the widely used Log4j logging library for Java programs, leading to CVE 2021-45105 (see §G.2).

Out-of-Order Transition Divergence. Unintended divergence can result from a loop or recursive call to a parsing function where certain input values or record data types are expected to be treated in a certain order, and an out-of-order encoding results in an infinite cycle. In certain cases, special input tag types are intended to be found at certain parsing stages as to disallow spurious transitions. Such a vulnerability was discovered in the GraphQL language interpreter, where the *string* type name can be encoded in the input such that the parsing handler calls itself repeatedly (see §G.3 for an example vulnerability affecting Go programs).

Zero-Sized Input Divergence. Container data structures (e.g. lists or vectors) are typically implemented with access primitives where adding or removing elements can be achieved independently of the current number of elements in the container. This is done by maintaining a meta-data size field. When such data structures are implemented with linear memory access in mind, an additional size field is needed to ascertain the size of an element in the data structure. Whether such element is of a fixed or variable size, an element with zero size can lead to a container iterator that diverges when traversing the structure without making progress. Such a problem was identified in the Linux kernel, leading to CVE-2020-25641 and was fixed in Linux kernel version 3.13 (see §G.4).

Offset-Encoded Divergence. In parser programs it is sometimes possible for the input to describe the actual input offset at which the data object is found. When such input offset indirection occurs, a parsing loop or recursive function can diverge by returning to previously parsed input in a way that will redo previously completed work and diverge. An example of this bug can be found in the popular graphic software Blender, written in C. Additional state would be required to ensure that the current input offset is restored after such out-of-band element is read (see §G.5).

Exception-Induced Divergence. Some parser implementations use exceptions to treat special or error cases where a recovery logic must be encoded in a catch or except block. Exception-induced spurious transitions can then be encoded such that the induction variable is never incremented/decremented, leading to divergence. A particular example of such vulnerability can be found in the *Sklearn* industry-standard library for machine learning and data analysis in Python, where a convergence-based discretisation algorithm can be made to never terminate if the exceptional execution path fails to break from the appropriate number of loop nesting levels (see §G.6).

Algebraic Divergence. Divergence bugs can be found in mathematical software, where specific algebraic conditions are expected on the input to reach a fixpoint in an iterative or recursive function. The OpenSSL cryptographic library contains such code, where a modular square root implementation for an elliptic curve group expects the residue of the recursive operation to reach value 1 eventually, but invalid input parameters fail to meet this condition, leading to CVE-2022-0778. This vulnerability allowed remote SSL/TLS connections to get stuck in an infinite loop (see §G.7). This example illustrates that even security code can be vulnerable to divergence bugs!

3 OVERVIEW

Incorrectness Logic and Under-Approximate Reasoning. As Godefroid [16] argues, the main value of analysis tools lies in the discovery of bugs, not in the proof of program correctness. A bug presented to a developer is often a more convincing utility of a tool than a correctness proof, which is often carried out under certain assumptions that may not hold. This is evidenced by the recent trend in under-approximate reasoning techniques [23–25] and their significant success at finding bugs on an *industrial scale* [19, 4]. Specifically, Incorrectness logic (IL) [23] was recently introduced as an under-approximate formal foundation for bug detection. It was later extended to enable compositional bug detection in heap-manipulating programs [24], and to support concurrency [25]. IL and its later extensions are instances of under-approximate reasoning and are associated with *no-false-positives theorems*, ensuring that all bugs identified by them are true positives.

Intuitively, the under-approximate nature of IL stems from considering a *subset* of program behaviours. More concretely, given a program C whose behaviours (traces) is given by the set S, IL reasoning considers a subset (under-approximated) $S_u \subseteq S$ of the C behaviours. This makes IL ideally suited for bug-detection as it guarantees no-false-positives: if one detects a bug in the smaller set S_u, then the bug is also guaranteed to be in S and thus exhibited by C. This is in contrast to over-approximate reasoning techniques such as Hoare logic, where one considers a superset (over-approximated) set $S_o \supseteq S$ of C behaviours, making them ideal for verification (as they guarantee no false negatives): if one can show that the larger set S_o contains only correct behaviours, then the smaller set S also contains correct behaviours only.

An IL triple, also referred to as a *forward, under-approximate* (FUA) triple, is of the form $\vdash_{\mathsf{F}}$ $[p]$ C $[\epsilon : q]$, where F hints at its *forwards under-approximation*, denoting that q is a subset of program behaviours when C is run (forward) from the states in p. In other words, an FUA triple describes *backward reachability*: *every* post-state in q is *reachable* by running C forward on *some* pre-state in p. The ϵ denotes an *exit condition* and may be either *ok*, to denote a normal execution or *er* to denote an erroneous execution. For instance, executing an explicit error statement (e.g. assert(false)) terminates erroneously and the underlying states are unchanged; this is given by the FUA triple $\vdash_{\mathsf{F}}$ $[p]$ error $[er\colon p]$. The under-approximate nature of FUA triples is best illustrated by their rules for reasoning about branches and loops. To show that a behaviour is possible when executing $\mathsf{C}_1 + \mathsf{C}_2$ (where + denotes non-deterministic choice), it is sufficient to show the behaviour is possible when executing one of the branches, i.e. executing C_i for *some* (rather than all) $i \in \{1, 2\}$, as shown in ChoiceF below (left). Similarly, to show a behaviour is possible when executing $\mathsf{C}^\star$ (where $\mathsf{C}^\star$ denotes a non-deterministic loop, executing C for zero or more iterations), it suffices to show it is possible when executing C for a particular number $n \in \mathbb{N}$ of iterations, as shown in LoopF below (right), where C^n denotes executing C for n times.

$$\textsc{ChoiceF}\ \frac{\vdash_{\mathsf{F}} [p]\ \mathsf{C}_i\ [\epsilon : q] \quad \text{for some } i \in \{1,2\}}{\vdash_{\mathsf{F}} [p]\ \mathsf{C}_1 + \mathsf{C}_2\ [\epsilon : q]} \qquad \textsc{LoopF}\ \frac{\vdash_{\mathsf{F}} [p]\ \mathsf{C}^n\ [\epsilon : q] \quad \text{for some } n \in \mathbb{N}}{\vdash_{\mathsf{F}} [p]\ \mathsf{C}^\star\ [\epsilon : q]}$$

Non-termination and Under-Approximate Reasoning. Existing literature includes a large body of work [12, 15, 21, 2, 10, 3, 9, 6] on *termination* analysis, proving that a program C always terminates by showing that *all* traces of C terminate for *all* given inputs. Showing that a program C terminates is compatible with *over-approximate* reasoning frameworks. Specifically, when the traces of C are given by the set S, showing that all traces in a larger set $S_o \supseteq S$ terminate is sufficient for showing that all traces in S terminate. Showing termination is difficult in the presence of loops. In particular, to show that a loop L terminates typically involves the challenging task of establishing a *loop invariant* as well as a *well-founded measure* (a.k.a. a ranking function) that is decreased after each iteration [12, 15]. Establishing such invariants and measures is far from straightforward and typically involves reasoning about *ordinal* (rather than cardinal) numbers.

Showing that a program C does not terminate is compatible with *under-approximate* reasoning frameworks: when the traces (behaviours) of C are given by the set S, showing that the traces in a smaller (under-approximate), possibly singleton, set $S_u \subseteq S$ do not terminate is sufficient for showing that C does not terminate.

Inspired by the success of under-approximate analysis techniques and their industrial application of detecting bugs at scale, we develop *under-approximate, non-termination logic* (UNTer) as the first *formal, under-approximate foundation* for detecting non-termination bugs. As with existing under-approximate techniques, UNTer is associated with a no-false-positives theorem, ensuring that all non-termination bugs identified are true positives. More concretely, UNTer enables deriving under-approximate, *divergent* triples of the form $[p]\ \mathsf{C}\ [\infty]$, stating that starting from the states in p program C has divergent (non-terminating) traces. Note that $[p]\ \mathsf{C}\ [\infty]$ does not state that C never terminates (i.e. that *all* traces of C are divergent), but rather that it is possible for C not to terminate (i.e. *some* traces of C are divergent). For instance, given the program $\mathsf{C} \triangleq \mathsf{skip} + (\mathsf{while}\ (\mathsf{true})\ \mathsf{skip})$, the triple $[\mathsf{true}]\ \mathsf{C}\ [\infty]$ is valid, since starting from any state (in true) C can always diverge by taking the right branch, even though taking the left branch would immediately lead to termination.

Divergent Triples and FUA Triples. As in the existing formal systems for reasoning about programs (be they over- or under-approximate), we should ideally reason about non-termination in a *compositional* fashion. For instance, given $\mathsf{C}_L \triangleq x := 1; \mathsf{while}\ (x > 0)\ x{+}{+}$ and an arbitrary initial value v, to show that the triple $[x = v]\ \mathsf{C}\ [\infty]$ holds (i.e. C_L does not terminate starting from states satisfying $x = v$), we should ideally show that 1) running $x := 1$ on states in which $x = v$ terminates and modifies the states to those where $x = 1$; and 2) running $\mathsf{while}\ (x > 0)\ x{+}{+}$ on states where $x = 1$ diverges, i.e. $[x = 1]\ \mathsf{while}\ (x > 0)\ x{+}{+}\ [\infty]$. To do (1), we need to reason about *non-divergent* (terminating) program executions in an *under-approximate* fashion. At first glance, this seems an ideal job for FUA triples as they under-approximate reachable program behaviours upon termination; as such, to establish (1), we could simply show $\vdash_{\mathsf{F}} [x = v]\ x := 1\ [ok\colon x = 1]$.

A key feature of our UNTer framework is proof rules for establishing when a loop does not terminate. As a first naive attempt, we can propose the LoopBad rule below (left), stating that if initially the while condition B holds, and executing one iteration of the loop body C starting from p leaves the states (p) and the loop condition (B) unchanged, then while (B) C diverges.

$$\textsc{LoopBad}\ \frac{\vdash_{\mathsf{F}} [p \wedge B]\ \mathsf{C}\ [ok\colon p \wedge B]}{[p \wedge B]\ \mathsf{while}\ (B)\ \mathsf{C}\ [\infty]} \qquad \textsc{LoopFix}\ \frac{\vdash_{\mathsf{B}} [p \wedge B]\ \mathsf{C}\ [ok\colon p \wedge B]}{[p \wedge B]\ \mathsf{while}\ (B)\ \mathsf{C}\ [\infty]}$$

On closer inspection, however, this rule is unsound. Consider the program while $(x > 0)\ x{-}{-}$; this program always terminates regardless of the value of x (for non-positive values the loop is never entered; positive values are eventually decremented to zero). As such, the triple $[x > 0]$ while $(x > 0)\ x{-}{-}\ [\infty]$ is invalid. Nevertheless, we can derive it using LoopBad by showing $\vdash_{\mathsf{F}} [x > 0]\ x{-}{-}\ [ok\colon x > 0]$. Specifically, the $\vdash_{\mathsf{F}} [x > 0]\ x{-}{-}\ [ok\colon x > 0]$ triple stipulates that every post-state in $x > 0$ be reachable from some pre-state in $x > 0$, which is indeed the case. More concretely, consider an arbitrary post-state $s_q \in x > 0$ and let $s_q(x) = v$ (i.e. x holds value v in s_q) for some $v > 0$. State s_q is then reachable by running $x{-}{-}$ on a state $s_p = s_q[x \mapsto v{+}1]$ and $s_p \in x > 0$ (as $v > 0$).

Backward Under-Approximate Triples. Intuitively, the problem lies in the backward reachability of FUA triples: it stipulates that each post-state be reachable from some pre-state, which does not necessarily lead to divergence. In other words, having a backward chain of C executions from $p \wedge B$ to $p \wedge B$ does not yield an infinite execution. Instead, we need a forward chain of C executions from $p \wedge B$ to $p \wedge B$, as we can then repeat this execution forward *ad infinitum*. This is captured in the LoopFix rule above (right), where a *backward, under-approximate* (BUA) triple $\vdash_{\mathsf{B}} [p]\ \mathsf{C}\ [\epsilon : q]$ states that every pre-state in p reaches some post-state in q by executing C. Therefore, if we show that each iteration of the loop body transitions each pre-state in $p \wedge B$ to some post-state also in $p \wedge B$, then we can repeat this transition infinitely, leading to divergence. Note that in the example above, we cannot show $\vdash_{\mathsf{B}} [x > 0]\ x{-}{-}\ [ok\colon x > 0]$ (unlike the $\vdash_{\mathsf{F}}$ variant): given state $s_p \in x > 0$ with $s_p(x) = 1$, running $x{-}{-}$ on s_p yields a state $s_q = s_p[x \mapsto 0]$, which is *not* in $x > 0$. As such, using LoopFix, we cannot derive the invalid triple $[x > 0]$ while $(x > 0)\ x{-}{-}\ [\infty]$. Note that while BUA triples describe *forward reachability*, they denote *backward under-approximation*: $p \subseteq \mathsf{wpp}(\mathsf{C}, q)$, where $\mathsf{wpp}(\mathsf{C}, q)$ denotes running C *backwards* from q. That is, BUA triples mirror FUA ones (which describe *backward reachability* but *forward under-approximation*).

In order to present our divergence proof rules in a compositional fashion, we thus use BUA triples to describe normal, terminating executions. For instance, in order to show that $\mathsf{C}_1; \mathsf{C}_2$ does not terminate starting from p, we can show either C_1 does not terminate starting from p (i.e. $[p]\ \mathsf{C}_1\ [\infty]$), or C_1 terminates normally transforming the states to q, and C_2 does not terminate starting from q (i.e. $\vdash_{\mathsf{B}} [p]\ \mathsf{C}_1\ [ok\colon q]$ and $[q]\ \mathsf{C}_2\ [\infty]$). This is captured by the Div-Seq1 and Div-Seq2 rules in Fig. 3 (§4), where we present our full set of proof rules for detecting divergence.

Forward versus Backward Under-Approximate Triples. As with FUA triples, BUA triples are also inherently under-approximate. Most notably, as we show in §4, the BUA rules for reasoning about branches and loops are identical to their FUA counterparts; i.e. the $\vdash_{\mathsf{F}}$ in ChoiceF and LoopF above can simply be replaced with $\vdash_{\mathsf{B}}$ (see Fig. 2). Indeed, almost all FUA and BUA proof rules coincide, and the only difference between FUA and BUA rules lie in their associated rules of consequence, namely the ConsF (for FUA) and ConsB (for BUA) rules in Fig. 2 (p. 11). However, as we describe shortly, in the practical context of industrially-deployed (under-approximate) bug detection tools such as Pulse [19], it is straightforward to reconcile this difference between FUA and BUA and to develop a unified, under-approximate reasoning framework.

The main application of the FUA rule of consequence, ConsF, is in conjunction with the rule of disjunction, Disj in Fig. 2 (p. 11). More concretely, when a given program contains multiple branches, thanks to the ChoiceF rule, we can analyse each branch (and not necessarily all branches) in isolation and generate a separate triple. Subsequently, we can merge them into a single triple using Disj. However, when there are many branches (and subsequently many disjuncts in the pre- and post-states), we can simply use ConsF to drop some of the disjuncts in the *post-states*. (Note that using ConsB analogously allows us to drop some of the disjuncts in the *pre-states*.)

However, as our conversations with the lead engineer behind Pulse have revealed, in the practical setting of such tools this scenario rarely arises, and it is handled differently when it does. Specifically, different triples of a program are not merged very often, as it is simpler and more efficient to keep them separate. Second, when triples *are* merged, they are done so in a fashion that additionally *tracks* the correspondence between the disjuncts in the pre- and post-states. Specifically, note that the Disj rule is *lossy*: while in its premise we know that the post-states in q_1 (resp. q_2) are reached from the pre-sates in p_1 (resp. p_2), we lose this correspondence in the conclusion and only know that the post-states in $q_1 \vee q_2$ are reached from the pre-sates in $p_1 \vee p_2$. As such, when merging the triples $\vdash_F [p_1]\ C\ [\epsilon : q_1]$ and $\vdash_F [p_2]\ C\ [\epsilon : q_2]$ into $\vdash_F [p_1 \vee p_2]\ C\ [\epsilon : q_1 \vee q_2]$, Pulse additionally tracks the correspondence between p_1 and q_1 (resp. p_2 and q_2). This is beneficial when later dropping branches: when dropping the disjuncts in the post-states (e.g. q_2), we can also drop their associated pre-states (p_2). This allows us to avoid accumulating 'clutter' in the pre-states and is tantamount to dropping a full triple rather than its post-states only.

We thus follow a similar approach here which allows us to unify FUA and BUA reasoning. More concretely, we introduce the notion of *indexed disjunctions*, $P, Q \in \mathbb{N} \xrightarrow{\text{fin}} \mathcal{P}(\text{State})$. Intuitively, an indexed disjunction P can be flattened into a standard disjunction as $\bigvee_{i \in dom(P)} P(i)$. We write $[P]\ C\ [\epsilon : Q]$ as a shorthand for $dom(P) = dom(Q) \wedge \forall i \in dom(P).\ [P(i)]\ C\ [\epsilon : Q(i)]$, denoting a merged set of triples. Note that a triple $[p]\ C\ [\epsilon : q]$ can be simply lifted to $[P]\ C\ [\epsilon : Q]$, where $dom(P) = dom(Q) = \{0\}$ with $P(0) = p$ and $Q(0) = q$. We can then use the DisjTrack rule (Fig. 2 on p. 11) to merge indexed disjuncts – note that the $dom(P_1) \cap dom(P_2) = \emptyset$ premise can be simply satisfied by renaming the domain of P_2. Observe that unlike the Disj rule, DisjTrack is not lossy and preserves the pre-post correspondence. Finally, the unified rule of consequence, Cons (Fig. 2), allows us to drop matching disjuncts from both the pre- and post-states, where $P \downarrow I$ denotes restricting the domain of P to I. The unified Cons rule can be used for both FUA and BUA reasoning.

Unified Triples and Bug Catching Tools. Note that the rules in Fig. 2, excluding ConsB, ConsF and Disj (and instead including Cons and DisjTrack) correspond to the reasoning principles used in the industrially deployed Pulse tool. That is, although Pulse is formally underpinned by IL (with FUA triples), it does not use ConsF and Disj, and instead uses Cons and DisjTrack, meaning that using our unified rules (suitable for both FUA and BUA reasoning) has no practical ramifications, and we can use Pulse as it is! This is indeed great news: in order to reason about divergence, we can extend Pulse without changing its underlying principles, and simply add our divergence rules.

Theoretical Connection between BUA and FUA Triples. As mentioned above, with the exception of their associated rules of consequence (ConsF and ConsB in Fig. 2) all other FUA and BUA reasoning principles and proof rules coincide. In §6 we further bolster this intuition by showing that given any under-approximate triple $[p]\ C\ [\epsilon : q]$, if $[p]\ C\ [\epsilon : q]$ is a valid *FUA* triple *and* its pre-states (p) are *FUA-minimal*, then $[p]\ C\ [\epsilon : q]$ is also a valid *BUA* triple. The pre-states p are FUA-minimal if for all smaller pre-sates $p' \subset p$, the triple $[p']\ C\ [\epsilon : q]$ is not a valid FUA triple. Intuitively, this ensures that pre-states p have not been arbitrarily weakened (grown) using ConsF.

Conversely, we show that given an under-approximate triple $[p]\ C\ [\epsilon : q]$, if $[p]\ C\ [\epsilon : q]$ is a valid *BUA* triple *and* its post-states (q) are *BUA-minimal*, then $[p]\ C\ [\epsilon : q]$ is also a valid *FUA* triple. Analogously, q is BUA-minimal if for all smaller $q' \subset q$, the triple $[p]\ C\ [\epsilon : q']$ is not a valid BUA triple. This ensures that the post-states q have not been arbitrarily weakened using ConsB.

Formal Interpretation of Divergent Triples. As discussed above, we write a divergent triple of the form $[p]\ C\ [\infty]$ to denote that C has *some* divergent trace(s) (i.e. in an under-approximate fashion) starting from p. The next question to answer when interpreting such triples is whether there is some divergent trace starting from *every* state in p or *some* state in p. Observe that both interpretations are under-approximate as they pertain to *some* rather than *all* traces of C. Although the latter interpretation is a weaker statement, it is nevertheless sufficient for an under-approximate divergence detection framework: to establish divergence it suffices to show *some* divergent trace is possible from *some* initial state in p. However, under this weaker interpretation, inspecting a divergent triple $[p]\ \mathsf{C}\ [\infty]$ yields little information on how the divergence arises (which may be needed for debugging and fixing the cause of divergence): as p may contain many states, it is unclear which state(s) in p lead(s) to divergence (unless p describes a single state). On the other hand, the former, stronger interpretation provides more information for debugging and fixing the cause of divergence as it states that starting from any state in p the program has a divergent trace.

Although more useful, at first glance this stronger interpretation may seem too strong and antithetic to the spirit of under-approximation in UNTer. However, this additional strength is not accompanied by a theoretical or practical cost. In theoretical terms, rather than considering an arbitrarily large set of pre-states that contain some states that may lead to divergence, one can always shrink the pre-states to contain exactly those states that lead to divergence. More concretely, when starting from a state s executing C may diverge, one can establish $[p]\ \mathsf{C}\ [\infty]$ by defining p as the singleton set $\{s\}$, rather than an arbitrarily large set that contains s. In practical terms, this stronger interpretation incurs no additional cost when extending existing an under-approximate tool such as Pulse with divergence proof rules. In particular, the divergence rules in Fig. 3 (p. 12) fall into one of two categories: 1) base rules, where the premises contain BUA triples only (e.g. LoopFix above or Div-Loop in Fig. 3); or 2) inductive cases, where the premises contain other divergent triples (e.g. Div-Seq1 in Fig. 3) or a combination of divergent and BUA triples (e.g. Div-Seq2 in Fig. 3). For the base cases such as LoopFix, thanks to the forward reachability of BUA triples, we already establish the desired result for *every* pre-state. Moreover, as discussed above, the BUA and FUA reasoning principles are almost identical and can be easily unified for practical purposes. As such, extending exiting under-approximate tools with a base case under a strong interpretation incurs no additional cost. Similarly, establishing an inductive case requires establishing its premises, and since neither their BUA premises (as argued above) nor their divergent premises (by inductive hypothesis) incur an additional cost, establishing an inductive case under a strong interpretation incurs no additional cost. We therefore opt for the stronger under-approximate interpretation of divergent triples: $[p]\ \mathsf{C}\ [\infty]$ denotes that *every* state in p leads to *some* divergent trace.

4 THE UNTer FRAMEWORK

We present the UNTer framework for detecting non-termination bugs. To present the key ideas underpinning UNTer more clearly, here we develop it as an analogue of Hoare logic/incorrectness logic (IL), in that UNTer enables *global* and not *local* (compositional) reasoning as in separation logic (SL) [18] and incorrectness separation logic (ISL) [24]. Later in §7 we develop an extension of UNTer that marries the compositionality of SL/ISL with the divergence reasoning of UNTer.

Programming Language. To keep our presentation concise, we employ a simple imperative programming language given by the C grammar below. Our language comprises the standard constructs of skip, assignment ($x := e$), assume statements ($\mathsf{assume}(B)$), scoped variable declaration ($\mathsf{local}\ x\ \mathsf{in}\ \mathsf{C}$), sequential composition ($\mathsf{C}_1; \mathsf{C}_2$), non-deterministic choice ($\mathsf{C}_1 + \mathsf{C}_2$) and loops ($\mathsf{C}^\star$), as well as explicit error statements (error, which can be thought of e.g. as $\mathsf{assert}(\mathsf{false})$).

$$\mathsf{C} ::= \mathsf{skip} \mid x := e \mid \mathsf{assume}(B) \mid \mathsf{local}\ x\ \mathsf{in}\ \mathsf{C} \mid \mathsf{error} \mid \mathsf{C}_1 + \mathsf{C}_2 \mid \mathsf{C}_1; \mathsf{C}_2 \mid \mathsf{C}^\star$$

As is standard, deterministic choice and loops can be encoded using their non-deterministic counterparts and assume statements. Specifically, $\mathsf{if}\ (B)\ \mathsf{then}\ \mathsf{C}_1\ \mathsf{else}\ \mathsf{C}_2$ can be encoded as $(\mathsf{assume}(B); \mathsf{C}_1) + (\mathsf{assume}(\neg B); \mathsf{C}_2)$, and $\mathsf{while}\ (B)\ \mathsf{C}$ can be encoded as $(\mathsf{assume}(B); \mathsf{C})^\star; \mathsf{assume}(\neg B)$.

Assertions (Sets of States). The UNTer assertion language is given by the simple grammar below, comprising classical (first-order logic) and Boolean assertions, where $\oplus \in \{=, \neq, <, \leq, \cdots\}$. Other classical connectives can be encoded using existing ones (e.g. $\neg p \triangleq p \Rightarrow \mathsf{false}$). We use p, q, r and their variants (e.g. p') as metavariables for assertions. An assertion describes a set of states, where each state is a (variable) store in $\textsc{Store} \triangleq \textsc{Var} \rightarrow \textsc{Val}$, mapping program variables to values.

$$\textsc{Ast} \ni p, q, r ::= \mathsf{false} \mid p \Rightarrow q \mid \exists x.\ p \mid e \oplus e'$$

An expressions e is interpreted under a variable store, written as $s(e)$; this interpretation is standard and elided here. We interpret assertions as sets of states, and thus write false for $\emptyset$, $p \Rightarrow q$ for $p \subseteq q$, $p \wedge q$ for $p \cap q$, $p \vee q$ for $p \cup q$, and so forth. Similarly, $e \oplus e'$ denotes sets of states (stores) in which $s(e) \oplus s(e')$ holds. As discussed in §3, we introduce the notion of *indexed disjunctions*, $P, Q \in \mathbb{N} \xrightarrow{\text{fin}} \mathcal{P}(\textsc{State})$, as a map from numbers to assertions (disjuncts); i.e. $P \equiv \bigvee_{i \in dom(P)} P(i)$.

UNTer Under-Approximate Proof Rules for Termination. Recall from §3 that to reason about divergence in a piecemeal fashion, we reason about terminating sub-programs via (under-approximate) BUA triples. We present the UNTer under-approximate proof rules for terminating programs in Fig. 2. The rules denoted by $\vdash_\dagger$ are *FUA and BUA* rules in that they are valid when interpreted in either the forward ($\vdash_F$) or backward $\vdash_B$ direction. Note that as discussed in §3, with the exception of ConsF and ConsB rules, all rules in Fig. 2 are valid FUA *and* BUA triples.

The Skip, Error, Seq, SeqEr, Choice, Loop0, Loop and Disj rules are identical to those of existing FUA logics [23–25]. Specifically, executing skip and error leave the state unchanged (Skip and Error), where the former terminates normally while the latter terminates erroneously; Disj allows us to merge two triples into one in a lossy fashion (as discussed in §3); the behaviour of a branching program can be under-approximated as the behaviour of *some* of its branches (Choice); and the behaviour of a loop can be under-approximated through bounded unrolling as zero (Loop0) or more (Loop) iterations. Note that while in correctness frameworks we can over-approximate a loop behaviour via an *invariant*, i.e. an assertion that holds after *any* number of iterations (including zero), in FUA/BUA frameworks we can under-approximate a loop behaviour via a *subvariant* as an indexed assertion p, where $p(n)$ describes the state after n iterations. This is captured by Loop-Subvariant: for an arbitrary k, if executing C terminates normally and transforms $p(n)$ to $p(n{+}1)$ for all $n < k$, then $p(k)$ can be reached by executing $\mathsf{C}^\star$ (i.e. executing C for k iterations) from the initial states $p(0)$. The SeqEr captures the short-circuiting behaviour of erroneous executions: if executing C_1 terminates erroneously, then executing $\mathsf{C}_1; \mathsf{C}_2$ also terminates erroneously. By contrast, Seq captures the case where executing C_1 does not encounter an error: if executing C_1 terminates normally transforming the states in p to those in r, and executing C_2 terminates as ϵ (either ok or er) and transforms r to q, then executing $\mathsf{C}_1; \mathsf{C}_2$ terminates as ϵ, transforming p to q.

The Assign rule is identical to the standard Floyd assignment rule and holds for both FUA and BUA. Observe that as noted by O'Hearn [23], the Hoare assignment rule is not sound for FUA. That is, $\vdash_F \big[p[e/x]\big]\ x := e\ \big[ok\colon p\big]$ is not sound (e.g. let $e = 42$ and p be $x = y$, then the state $s \in p$ such that $s(x) = s(y) = 17$ cannot be reached by executing $x := 42$ on any state in $p[42/x]$. By contrast, the Hoare assignment rule *is* sound for BUA, i.e. $\vdash_B \big[p[e/x]\big]\ x := e\ \big[ok\colon p\big]$ is a sound BUA triple. However, this difference between BUA and FUA does not have a practical ramification as the Floyds assignment rule (in Assign) is sufficient to enable automated reasoning in Pulse.

The Assume, Local and Constancy rules are analogous to the FUA rules of [23]. Concretely, executing $\mathsf{assume}(B)$ terminates normally and leaves the state unchanged, provided that B holds beforehand. When executing the scoped variable declaration local x in C, the information about x is erased by existentially quantifying it in the pre- and post-states. The Constancy rule is used to adapt triples in different contexts and states: if an assertion r holds before executing C, it also holds

$$\textsc{Skip}\quad \vdash_{\dagger}[p]\,\mathsf{skip}\,[ok{:}\,p] \qquad \textsc{Assign}\quad \vdash_{\dagger}[p]\,x := e\,[ok{:}\,\exists y.\,p[y/x] \land x = e[y/x]] \qquad \textsc{Assume}\quad \vdash_{\dagger}[p \land B]\,\mathsf{assume}(B)\,[ok{:}\,p \land B]$$

$$\textsc{Error}\quad \vdash_{\dagger}[p]\,\mathsf{error}\,[er{:}\,p] \qquad \textsc{Seq}\quad \frac{\vdash_{\dagger}[p]\,\mathsf{C}_1\,[ok{:}\,r] \qquad \vdash_{\dagger}[r]\,\mathsf{C}_2\,[\epsilon{:}\,q]}{\vdash_{\dagger}[p]\,\mathsf{C}_1;\mathsf{C}_2\,[\epsilon{:}\,q]} \qquad \textsc{SeqEr}\quad \frac{\vdash_{\dagger}[p]\,\mathsf{C}_1\,[er{:}\,q]}{\vdash_{\dagger}[p]\,\mathsf{C}_1;\mathsf{C}_2\,[er{:}\,q]}$$

$$\textsc{Choice}\quad \frac{\vdash_{\dagger}[p]\,\mathsf{C}_i\,[\epsilon{:}\,q] \qquad \text{for some } i \in \{1,2\}}{\vdash_{\dagger}[p]\,\mathsf{C}_1 + \mathsf{C}_2\,[\epsilon{:}\,q]} \qquad \textsc{Loop0}\quad \vdash_{\dagger}[p]\,\mathsf{C}^{\star}\,[ok{:}\,p] \qquad \textsc{Loop}\quad \frac{\vdash_{\dagger}[p]\,\mathsf{C}^{\star};\mathsf{C}\,[\epsilon{:}\,q]}{\vdash_{\dagger}[p]\,\mathsf{C}^{\star}\,[\epsilon{:}\,q]}$$

$$\textsc{Loop-Subvariant}\quad \frac{\forall n < k.\ \vdash_{\dagger}[p(n)]\,\mathsf{C}\,[ok{:}\,p(n{+}1)]}{\vdash_{\dagger}[p(0)]\,\mathsf{C}^{\star}\,[ok{:}\,p(k)]} \qquad \textsc{Local}\quad \frac{\vdash_{\dagger}[p]\,\mathsf{C}\,[\epsilon{:}\,q]}{\vdash_{\dagger}[\exists x.\,p]\,\mathsf{local}\ x\ \mathsf{in}\ \mathsf{C}\,[\epsilon{:}\,\exists x.\,q]} \qquad \textsc{Subst}\quad \frac{\vdash_{\dagger}[p]\,\mathsf{C}\,[\epsilon{:}\,q] \qquad x \notin \mathrm{fv}(p, \mathsf{C}, q)}{(\vdash_{\dagger}[p]\,\mathsf{C}\,[\epsilon{:}\,q])[y/x]}$$

$$\textsc{Disj}\quad \frac{\vdash_{\dagger}[p_1]\,\mathsf{C}\,[\epsilon{:}\,q_1] \qquad \vdash_{\dagger}[p_2]\,\mathsf{C}\,[\epsilon{:}\,q_2]}{\vdash_{\dagger}[p_1 \lor p_2]\,\mathsf{C}\,[\epsilon{:}\,q_1 \lor q_2]} \qquad \textsc{Constancy}\quad \frac{\vdash_{\dagger}[p]\,\mathsf{C}\,[\epsilon{:}\,q] \qquad \mathrm{fv}(r) \cap \mathrm{mod}(\mathsf{C}) = \emptyset}{\vdash_{\dagger}[p \land r]\,\mathsf{C}\,[\epsilon{:}\,q \land r]}$$

$$\textsc{ConsF}\quad \frac{p' \subseteq p \qquad \vdash_{\mathsf{F}}[p']\,\mathsf{C}\,[\epsilon{:}\,q'] \qquad q \subseteq q'}{\vdash_{\mathsf{F}}[p]\,\mathsf{C}\,[\epsilon{:}\,q]} \qquad \textsc{ConsB}\quad \frac{p \subseteq p' \qquad \vdash_{\mathsf{B}}[p']\,\mathsf{C}\,[\epsilon{:}\,q'] \qquad q' \subseteq q}{\vdash_{\mathsf{B}}[p]\,\mathsf{C}\,[\epsilon{:}\,q]}$$

$$\textsc{DisjTrack}\quad \frac{\vdash_{\dagger}[P_1]\,\mathsf{C}\,[\epsilon{:}\,Q_1] \qquad \vdash_{\dagger}[P_2]\,\mathsf{C}\,[\epsilon{:}\,Q_2]}{\vdash_{\dagger}[P_1 \uplus P_2]\,\mathsf{C}\,[\epsilon{:}\,Q_1 \uplus Q_2]} \qquad \textsc{Cons}\quad \frac{\vdash_{\dagger}[P]\,\mathsf{C}\,[\epsilon{:}\,Q] \qquad I \subseteq dom(P)}{\vdash_{\dagger}[P \downarrow I]\,\mathsf{C}\,[\epsilon{:}\,Q \downarrow I]}$$

$$\textsc{IfTrue}\quad \frac{\vdash_{\dagger}[p \land B]\,\mathsf{C}_1\,[\epsilon{:}\,q]}{\vdash_{\dagger}[p \land B]\,\mathsf{if}\ (B)\ \mathsf{then}\ \mathsf{C}_1\ \mathsf{else}\ \mathsf{C}_2\,[\epsilon{:}\,q]} \qquad \textsc{IfFalse}\quad \frac{\vdash_{\dagger}[p \land \neg B]\,\mathsf{C}_2\,[\epsilon{:}\,q]}{\vdash_{\dagger}[p \land \neg B]\,\mathsf{if}\ (B)\ \mathsf{then}\ \mathsf{C}_1\ \mathsf{else}\ \mathsf{C}_2\,[\epsilon{:}\,q]}$$

$$\textsc{ConsEq}\quad \frac{p \Leftrightarrow p' \qquad \vdash_{\dagger}[p']\,\mathsf{C}\,[\epsilon{:}\,q'] \qquad q' \Leftrightarrow q}{\vdash_{\dagger}[p]\,\mathsf{C}\,[\epsilon{:}\,q]} \qquad \textsc{WhileFalse}\quad \vdash_{\dagger}[p \land \neg B]\,\mathsf{while}\ (B)\ \mathsf{C}\,[ok{:}\,p \land \neg B]$$

$$\textsc{WhileSubvariant}\quad \frac{\forall n < k.\ \vdash_{\dagger}[p(n) \land B]\,\mathsf{C}\,[ok{:}\,p(n{+}1) \land B] \qquad \vdash_{\dagger}[p(k) \land B]\,\mathsf{C}\,[\epsilon{:}\,q \land \neg B]}{\vdash_{\dagger}[p(0) \land B]\,\mathsf{while}\ (B)\ \mathsf{C}\,[\epsilon{:}\,q \land \neg B]}$$

Fig. 2. Under-approximate proof rules where † in each rule can be instantiated as F or B; the highlighted rules can be derived from other rules (see §A).

afterwards provided that it does not refer to free variables that may have been modified by C. This is captured by the $\mathrm{fv}(r) \cap \mathrm{mod}(\mathsf{C}) = \emptyset$, where $\mathrm{fv}(r)$ denotes the free variables of r and $\mathrm{mod}(\mathsf{C})$ denotes the variables modified by C (i.e. those on the left-hand side of assignments).

As discussed in §3, ConsF and ConsB are the FUA and BUA rules of consequence, respectively. We reconcile the two in the unified rule of consequence, Cons, by using indexed disjunctions, where $dom(P \downarrow I) = I$ and $\forall i \in I.\ (P \downarrow I)(i) = P(i)$. Finally, using indexed disjunctions in DisjTrack we can merge triples in a non-lossy fashion, preserving the pre-post correspondence.

The remaining highlighted rules can be derived from existing rules (see §A). The IfTrue (resp. IfFalse) is analogous to its non-deterministic counterpart (Choice) and simply requires that the

$$\textsc{Div-Seq1}\ \frac{\vdash [p]\ \mathsf{C}_1\ [\infty]}{\vdash [p]\ \mathsf{C}_1; \mathsf{C}_2\ [\infty]} \qquad \textsc{Div-Seq2}\ \frac{\vdash_{\mathrm{B}} [p]\ \mathsf{C}_1\ [ok\colon q] \qquad \vdash [q]\ \mathsf{C}_2\ [\infty]}{\vdash [p]\ \mathsf{C}_1; \mathsf{C}_2\ [\infty]} \qquad \textsc{Div-Choice}\ \frac{\vdash [p]\ \mathsf{C}_i\ [\infty] \quad \text{for some } i \in \{1,2\}}{\vdash [p]\ \mathsf{C}_1 + \mathsf{C}_2\ [\infty]}$$

$$\textsc{Div-LoopUnfold}\ \frac{\vdash [p]\ \mathsf{C}; \mathsf{C}^\star\ [\infty]}{\vdash [p]\ \mathsf{C}^\star\ [\infty]} \qquad \textsc{Div-Loop}\ \frac{\vdash_{\mathrm{B}} [p]\ \mathsf{C}\ [ok\colon q] \qquad q \subseteq p}{\vdash [p]\ \mathsf{C}^\star\ [\infty]} \qquad \textsc{Div-Subvariant}\ \frac{\forall n \in \mathbb{N}.\ \vdash_{\mathrm{B}} [p(n)]\ \mathsf{C}\ [ok\colon p(n{+}1)]}{\vdash [p(0)]\ \mathsf{C}^\star\ [\infty]}$$

$$\textsc{Div-Cons}\ \frac{\vdash [p']\ \mathsf{C}\ [\infty] \qquad p \subseteq p'}{\vdash [p]\ \mathsf{C}\ [\infty]} \qquad \textsc{Div-Local}\ \frac{\vdash [p]\ \mathsf{C}\ [\infty]}{\vdash [\exists x.\ p]\ \mathsf{local}\ x\ \mathsf{in}\ \mathsf{C}\ [\infty]} \qquad \textsc{Div-While}\ \frac{\vdash_{\mathrm{B}} [p \wedge B]\ \mathsf{C}\ [ok\colon q \wedge B] \qquad q \subseteq p}{\vdash [p \wedge B]\ \mathsf{while}\ (B)\ \mathsf{C}\ [\infty]}$$

$$\textsc{Div-LoopNest}\ \frac{\vdash [p]\ \mathsf{C}\ [\infty]}{\vdash [p]\ \mathsf{C}^\star\ [\infty]} \qquad \textsc{Div-WhileNest}\ \frac{\vdash [p \wedge B]\ \mathsf{C}\ [\infty]}{\vdash [p \wedge B]\ \mathsf{while}\ (B)\ \mathsf{C}\ [\infty]} \qquad \textsc{Div-WhileSubvariant}\ \frac{\forall n \in \mathbb{N}.\ \vdash_{\mathrm{B}} [p(n) \wedge B]\ \mathsf{C}\ [ok\colon p(n{+}1) \wedge B]}{\vdash [p(0) \wedge B]\ \mathsf{while}\ (B)\ \mathsf{C}\ [\infty]}$$

Fig. 3. The UNTer divergence rules, where the highlighted rules can be derived from other rules

condition B hold (resp. not hold) at the beginning. The ConsEq simply replaces implication (subset inclusion) in the premises of ConsF and ConsB with equivalence. The WhileFalse states that the pre-states are unchanged by the loop if the condition B does not hold to begin with (i.e. the loop is never entered). The WhileSubvariant is analogous to Loop-Subvariant and states that if for all $n < k$ an execution of C transforms $p(n) \wedge B$ to $p(n{+}1) \wedge B$, i.e. loop condition B remains true in the first $k{-}1$ iterations, and the k^{th} iteration results in the states in $q \wedge \neg B$ (i.e. it invalidates the loop condition), then while (B) C terminates, transforming the initial states in $p(0) \wedge B$ to $q \wedge \neg B$.

UNTer Divergent Proof Rules for Non-Termination. We present the (syntactic) proof rules for divergence in Fig. 3. Recall from §3 that we opt for the stronger interpretation of divergent triples, where $[p]$ C $[\infty]$ states that every state in p leads to *some* divergent trace. We provide the formal semantic interpretation of divergent triples later in §6.

In order to show that $\mathsf{C}_1; \mathsf{C}_2$ has a divergent trace starting from p, we can show either C_1 has a divergent trace starting from p (Div-Seq1), or C_1 terminates normally transforming the states to q and C_2 does not terminate starting from q (Div-Seq2). To show that the branching program $\mathsf{C}_1 + \mathsf{C}_2$ has a divergent trace starting from p, it suffices to show that *some* branch C_i has a divergent trace from p, i.e. in an under-approximate fashion. The Div-Cons denotes the rule of consequence for divergence: if C has some divergent trace starting from any state in p' and $p \subseteq p'$, then C also has some divergent trace starting from any state in p.

The remaining rules capture divergence for loops. Specifically, Div-LoopUnfold allows us to establish divergence after unrolling the loop once. This can be used for showing divergence in the case of nested loops, where the inner loop diverges. Specifically, using a combination of Div-Seq1 and Div-LoopUnfold we can derive Div-LoopNest as shown across, stating that if one iteration of the loop body (e.g. a nested loop) has a divergent trace, then the loop itself also has a divergent trace.

$$\cfrac{\cfrac{\cfrac{}{[p]\ \mathsf{C}\ [\infty]}\ \text{(given)}}{[p]\ \mathsf{C}; \mathsf{C}^\star\ [\infty]}\ (\textsc{Div-Seq1})}{[p]\ \mathsf{C}^\star\ [\infty]}\ (\textsc{Div-LoopUnfold})$$

The Div-Loop rule states that if one iteration of a loop body terminates normally and transforms the states in p to ones in q (i.e. $\vdash_{\mathrm{B}} [p]$ C $[ok\colon q]$) and $q \subseteq p$, then $\mathsf{C}^\star$ has a divergent trace starting from p. Intuitively, the forward triple in the premise, $A \triangleq \vdash_{\mathrm{B}} [p]$ C $[ok\colon q]$, allows us to construct an infinite trace of $\mathsf{C}^\star$ from any state in p: given a state in $s_0 \in p$, (from A) executing C on s_0 results in a state $s_1 \in q \subseteq p$, and thus (from A) executing C on s_1 results in a state $s_2 \in q \subseteq p$, *ad infinitum.*

```
while (x = 0)
  skip
```
(a)

```
while (x ≥ 0)
  x := x+1
```
(b)

```
x := 1
y := 2;
while (x+y > 1)
  x := 3 − x
  y := 3 − y
```
(c)

```
while (y < 100)
  if (y ≤ 50)
    x := x+1
  else
    y := y+1
```
(d)

```
while (y < 100)
  x := 0;
  while (x ≤ 100)
    if (x = 100)
      y := 0
    x := x+1
  y := y+1
```
(e)

```
x := 42;   y := 1;
while (y < 100)
  while (x ≤ 100)
    if (x = 100)
      x := 1
      y := 2 × y
    else x := x+1
  y := y+1
```
(f)

Fig. 4. Several examples of programs with non-terminating behaviours where x, y initially hold 0

The Div-Subvariant is the subvariant rule for divergence: if an iteration of the loop body terminates normally and transforms $p(n)$ to $p(n{+}1)$ for an arbitrary n, then $C^\star$ has a divergent trace starting from the initial states $p(0)$. Note that given any loop body C, if C does not contain a conditional (if or while) statement and executing C does not encounter an error, then the non-deterministic loop $C^\star$ always has a divergent trace. However, this is not necessarily the case with conditional if/while statements (encoded via assume statements). This is illustrated in the Div-While rule, requiring that the loop condition B hold at the end of an iteration, which is not always the case. For instance, for while $(x = 0)\ x := 1$ we fail to establish $x = 0$ after an iteration of $x := 1$.

As before, all highlighted rules in Fig. 3 can be derived from other rules (see §A). For instance, Div-WhileNest can be derived from Div-LoopNest, Seq and Assume.

5 EXAMPLES

We present several simple examples of divergent programs (with divergent loops) and demonstrate how we can use our UNTer proof system to detect them. All divergent behaviours presented here, and many more, have also been detected using our Pulse$^\infty$ prototype (see §8).

Example 1 (Fig. 4a). Consider the simple example in Fig. 4a comprising a simple divergent loop. We can detect this using Div-While (with $p = q =$ true) as shown below:

$$\dfrac{\dfrac{}{\vdash_B [x = 0]\ \text{skip}\ [ok\colon x = 0]}\ (\text{Skip})}{[x = 0]\ \text{while}\ (x = 0)\ \text{skip}\ [\infty]}\ (\text{Div-While})$$

Example 2 (Fig. 4b). Consider the simple example in Fig. 4b comprising a simple while loop with a buggy check. We can detect this using Div-While (with $p =$ true and $q = x > 1$) as shown below:

$$\dfrac{\dfrac{\dfrac{}{\vdash_B [x \geq 0]\ x := x{+}1\ [ok\colon \exists v.\ v \geq 0 \land x = v{+}1]}\ (\text{Assign})}{\vdash_B [x \geq 0]\ x := x{+}1\ [ok\colon x \geq 1 \land x \geq 0]}\ (\text{ConsEq}) \qquad x \geq 1 \subseteq x \geq 0}{[x \geq 0]\ \text{while}\ (x \geq 0)\ x := x{+}1\ [\infty]}\ (\text{Div-While})$$

Example 3 (Fig. 4c). Consider the example in Fig. 4c. Prior to the first iteration of the loop $x{+}y = 3$ holds, and although the values of x and y are updated in each iteration, their sum remains unchanged after each iteration (i.e. $x{+}y = 3$) and thus the loop diverges. We present an UNTer proof outline of this divergent behaviour on the left of Fig. 5. For brevity, rather than giving full derivations, we follow the classical Hoare logic proof outline, annotating each line of the code with its pre- and post-states. We further commentate each proof step and write e.g. // Assign to denote an application of Assign. As in Hoare logic proof outlines, we assume that Seq is applied at every step; i.e. later instructions are executed only if the earlier ones execute normally (with ok).

```
1. $[x = 0 \land y = 0]$
2.    $x := 1$;  // Assign, ConsEq
3. $[ok: x = 1 \land y = 0]$
4.    $y := 2$;  // Assign, ConsEq
5. $[ok: x = 1 \land y = 2]$  // Div-Cons
6. $[ok: x+y = 3 \land x+y > 1]$
7.   while $(x+y > 1)$
   Div-While
   |   8. $[x+y = 3 \land x+y > 1]$
   |   9.    $x := 3 - x$ // Assign
   |  10. $[ok: \exists v_x.\ v_x+y = 3 \land v_x+y > 1 \land x = 3 - v_x]$
   |  11.    $y := 3 - y$ // Assign
   |  12. $[ok: \exists v_x, v_y.\ v_x+v_y = 3 \land v_x+v_y > 1 \land x = 3 - v_x \land y = 3 - v_y]$
   |  // ConsEq
   |  13. $[ok: x+y = 3 \land x+y > 1]$
14. $[\infty]$
```

```
1. $[x = 0 \land y = 0]$
// Div-Cons
2. $[y = 0 \land y < 100]$
3.   while $(y < 100)$
   Div-While
   |  4. $[y = 0 \land y < 100]$
   |  // ConsEq
   |  5. $[y = 0 \land y < 100 \land y \leq 50]$
   |  6.   if $(y \leq 50)$
   |     IfTrue
   |     |  7. $[y = 0 \land y < 100 \land y \leq 50]$
   |     |  8.      $x := x+1$ // Assign
   |     |  9. $[ok: \exists v_x.\ y = 0 \land y < 100 \land y \leq 50 \land x = v_x+1]$
   |     |  // ConsEq
   |     |  10. $[ok: y = 0 \land y < 100]$
   |     |  11.    else $\cdots$
   |  12. $[ok: y = 0 \land y < 100]$
13. $[\infty]$
```

Fig. 5. Proof sketches of the divergence bugs in Fig. 4c (left) and Fig. 4d (right)

Let $p \triangleq x+y = 3 \land x+y > 1$; after the initial assignment to x and y and applications of ConsEq and Div-Cons, we establish p (line 6). We then apply Div-While (lines 6–14) to show that the loop body leaves the set of states p unchanged (lines 8–13). The proof of lines 8–13 is then straightforward, and simply involves the applications of Assign and ConsEq.

Example 4 (Fig. 4d). Consider the example in Fig. 4d. At first glance it may seem that the loop terminates since the value of y is incremented in the else branch of each iteration. However, starting from $y = 0$, the then branch is taken in each iteration (since $y \leq 50$) and thus y is never incremented, resulting in divergence. We present an UNTer proof outline of this divergent behaviour on the right of Fig. 5. After applying ConsEq to rewrite p equivalently as $p \land y \leq 50$ (line 5), we apply IfTrue to show we can take the then branch and arrive at p (lines 7–10).

Example 5 (Fig. 4e). Consider the example in Fig. 4e with nested loops. Note that the value of x is incremented at the end of each iteration of the inner loop and thus the inner loop terminates. By contrast, although y is incremented at the end of each iteration of the outer loop and thus it may seem at first glance that the outer loop terminates, on closer inspection the value of y us reset to 0 in the last iteration of the inner loop. As such, at the end of each iteration of the outer loop y is incremented and updated 1, and thus the outer loop diverges.

We present an UNTer proof outline of this at the top of Fig. 6. After applying Div-Cons to obtain $y < 100$, we apply Div-While (lines 2–23) to show that the loop body leaves $y < 100$ unchanged (lines 4–22). After the assignment on line 5, we apply ConsEq to rewrite the states as $p(0) \land x \leq 100$ (line 7), with $p(n)$ defined below the proof at the top of Fig. 6. We then apply WhileSubvariant to show that at the end of the execution of the inner loop we arrive at $y{=}0 \land x{=}101 \land x \not\leq 100$ (lines 7–21). Note that WhileSubvariant has two premises, which we establish in two columns on lines 9–14 and 15–20. On lines 9–14 we show that for $n < 100$, each iteration of the loop transforms $p(n) \land x \leq 100$ to $p(n{+}1) \land x \leq 100$; on lines 15–20 we show that in the final iteration of the loop with $p(100)$ (i.e. when $x = 100$), we reset y to 0 and increment x, arriving at $y{=}0 \land x{=}101 \land x \not\leq 100$ which is included in $y < 100$ (line 22), as per the second premise of Div-While.

```
1. $[x = 0 \wedge y = 0]$ // Div-Cons
2. $[y < 100]$
3.   while ($y < 100$)
  Div-While
    4. $[y < 100]$
    5.    $x := 0$ // Assign
    6. $[ok\colon y < 100 \wedge x = 0]$ // ConsEq
    7. $[ok\colon p(0) \wedge x \le 100]$
    8.    while ($x \le 100$)
      WhileSubvariant
        9. $\forall n < 100.\ [p(n) \wedge n{<}100 \wedge x \le 100]$
        10.        if ($x = 100$) $y := 0$
        11.        else skip // IfFalse, Skip
        12.     $[ok\colon p(n) \wedge n{<}100 \wedge x{\le}100]$
        13.        $x := x{+}1$ // Assign, ConsEq
        14.     $[ok\colon p(n{+}1) \wedge x \le 100]$

        15. $[p(100) \wedge x \le 100]$
        16.    if ($x = 100$) $y := 0$
        17.    else skip // IfTrue, Assign
        18. $[ok\colon p(100) \wedge x \le 100 \wedge y = 0]$
        19.    $x := x{+}1$ // Assign, ConsEq
        20. $[ok\colon y = 0 \wedge x = 101 \wedge x \not\le 100]$
    21. $[ok\colon y = 0 \wedge x = 101 \wedge x \not\le 100]$
    22. $[ok\colon y < 100]$
23. $[\infty]$
where for all $n \in \mathbb{N}:\quad p(n) \triangleq x = n \wedge y < 100$
```

```
1. $[x = 0 \wedge y = 0]$
2.    $x := 42;\ y := 1;$ // Assign, ConsEq
3. $[ok\colon x = 42 \wedge y = 1]$ // Div-Cons
4. $[ok\colon x \le 100 \wedge y < 100]$
5.   while ($y < 100$)
  Div-WhileNest
    6. $[x \le 100 \wedge y < 100]$ // Div-Cons
    7. $[x \le 100]$
    8.   while ($x \le 100$)
      Div-While
        9. $[x \le 100]$ // ConsEq
        10. $[x < 100 \vee x = 100]$
          Disj
            11. $[x < 100]$
            12.    if ($x = 100$) $x := 1;\ y := 2{\times}y$
            13.    else $x := x{+}1$
                   // IfFalse, Assign, ConsEq
            14. $[ok\colon x \le 100]$

            15. $[x = 100]$
            16.    if ($x = 100$) $x := 1;\ y := 2{\times}y$
            17.    else $x := x{+}1$
                   // IfTrue, Assign, ConsB
            18. $[ok\colon x \le 100]$
        19. $[ok\colon x \le 100]$
    20. $[\infty]$
21. $[\infty]$
```

Fig. 6. Proof sketch of divergence in Fig. 4e (above), where the two columns on lines 9–14 and 15–20 denote the proof sketches of the two premises of WhileSubvariant; proof sketch of divergence in Fig. 4f (below), where the two columns on lines 11–14 and 15–18 denote the proof sketches of the two premises of Disj.

Example 6 (Fig. 4f). Consider the nested loops in Fig. 4f. Note that starting with $x = 42$ (after the initial assignment), the else branch of the inner loop increments x in all but the last iteration of the inner loop (since $x = 100$), whereupon the value of x is reset to 1; i.e. the inner loop diverges.

We present an UNTer proof outline of this divergent behaviour at the bottom of Fig. 6. After the initial assignments (line 2) and applying Div-Cons to arrive at $x \le 100 \wedge y < 100$ (line 4), we apply Div-WhileNest (lines 4–21) to show that the loop body diverges (lines 6–20). Once again, we apply

Div-Cons to weaken the states to $x \leq 100$ (line 7) and subsequently apply Div-While (lines 7–20) to show that the body of the inner loop leaves the states $x \leq 100$ unchanged (lines 9–19). To do this, we first rewrite $x \leq 100$ equivalently as $x < 100 \vee x = 100$ (line 10), and then apply Disj to show that either disjunct results in $x \leq 100$ states (the two columns on lines 11–14 and 15–18). The proof of each disjunct is then straightforward and is obtained by reasoning about the associated branch.

6 THE UNTer MODEL AND SEMANTICS

UNTer Operational Semantics. Although in sequential settings the semantics is typically given in the big-step fashion [23, 24], we opt for *small-step* semantics instead. This is because big-step semantics by definition describe *terminating* executions, while our aim is to formalise *divergent* triples. Specifically, we formalise the semantics of a divergent triple as an *infinite*, non-terminating execution trace. The UNTer small-step transitions are straightforward and are of the form $\mathsf{C}, s \rightarrow \mathsf{C}, s', \epsilon$, where C and s respectively denote the current command and store (state), C' and s' denote their continuations (what they reduce to) and ϵ denotes the exit condition, describing whether reducing C to C' took place normally (ok) or erroneously (er). For brevity we present the UNTer small-step transitions in the technical appendix (§B.1).

Semantic BUA and FUA Triples. Recall that intuitively a BUA triple $\vdash_{\mathsf{B}} [p]\ \mathsf{C}\ [\epsilon : q]$ states that every pre-state s_p in p reaches some post-state s_q in q under ϵ by executing C. Analogously, a FUA triple $\vdash_{\mathsf{F}} [p]\ \mathsf{C}\ [\epsilon : q]$ states that every post-state s_q in q can be reached from some pre-state s_p in p under ϵ by executing C. Put formally, in both cases we must have $\mathsf{C}, s_p \xrightarrow{n} -, s_q, \epsilon$, denoting that executing C *terminates* after n steps under ϵ and transforms s_p to s_q (see Def. 1 below).

Definition 1 (Semantic BUA and FUA triples)**.** A BUA triple is *valid*, written $\models_{\mathsf{B}} [p]\ \mathsf{C}\ [\epsilon : q]$, iff for all $s_p \in p$, there exists $s_q \in q$ and n such that $\mathsf{C}, s_p \xrightarrow{n} -, s_q, \epsilon$, where:

$$\begin{aligned}\mathsf{C}, s \xrightarrow{n} \mathsf{C}', s', \epsilon \overset{\text{def}}{\iff} & (n{=}0 \wedge \mathsf{C}{=}\mathsf{C}'{=}\mathsf{skip} \wedge s{=}s' \wedge \epsilon{=}ok) \vee (n{=}1 \wedge \epsilon \in \textsc{ErExit} \wedge \mathsf{C}, s \rightarrow \mathsf{C}', s', \epsilon) \\ & \vee (\exists k, \mathsf{C}'', s''.\ n{=}k{+}1 \wedge \mathsf{C}, s \rightarrow \mathsf{C}'', s'', ok \wedge \mathsf{C}'', s'' \xrightarrow{k} \mathsf{C}', s', \epsilon)\end{aligned}$$

and $\mathsf{C}, s \rightarrow \mathsf{C}', s', \epsilon$ is the UNTer small-step transitions given in §B.1 (Fig. 8). A FUA triple is *valid*, written $\models_{\mathsf{F}} [p]\ \mathsf{C}\ [\epsilon : q]$, iff for all $s_q \in q$, there exists $s_p \in p$ and n such that $\mathsf{C}, s_p \xrightarrow{n} -, s_q, \epsilon$.

The first disjunct in $\mathsf{C}, s \xrightarrow{n} \mathsf{C}', s'$ states that any state can be reached under ok in zero steps without changing the underlying state, provided that C is simply skip. The second disjunct captures the short-circuit semantics of errors: a state s' can be reached in one step under er when C takes an erroneous step. Analogously, the last disjunct captures the inductive cases ($n{=}k{+}1$), where C takes an ok step, and s' is subsequently reached in k steps under ϵ.

We next show that the BUA and FUA proof systems presented in Fig. 2 are *both sound and complete*, with the full proof given in the technical appendix (§B.2 and §C.1).

Theorem 7 (BUA and FUA soundness)**.** *For all p, q, C and ϵ:*

1) *if $\vdash_{\mathsf{B}} [p]\ \mathsf{C}\ [\epsilon : q]$ is derivable using the rules in Fig. 2, then $\models_{\mathsf{B}} [p]\ \mathsf{C}\ [\epsilon : q]$ holds; and*
2) *if $\vdash_{\mathsf{F}} [p]\ \mathsf{C}\ [\epsilon : q]$ is derivable using the rules in Fig. 2, then $\models_{\mathsf{F}} [p]\ \mathsf{C}\ [\epsilon : q]$ holds.*

Theorem 8 (BUA and FUA completeness)**.** *For all p, q, C and ϵ:*

1) *if $\models_{\mathsf{B}} [p]\ \mathsf{C}\ [\epsilon : q]$ holds, then $\vdash_{\mathsf{B}} [p]\ \mathsf{C}\ [\epsilon : q]$ is derivable using the rules in Fig. 2; and*
2) *if $\models_{\mathsf{F}} [p]\ \mathsf{C}\ [\epsilon : q]$ holds, then $\vdash_{\mathsf{F}} [p]\ \mathsf{C}\ [\epsilon : q]$ is derivable using the rules in Fig. 2.*

We next present the formal interpretation of divergent triples.

Definition 2 (Semantic divergent triples)**.** A divergent triple is *valid*, written $\models [p]\ \mathsf{C}\ [\infty]$, iff for all $s \in p$, there exists an infinite series of $\mathsf{C}_1, \mathsf{C}_2, \cdots, s_1, s_2, \cdots$ and $n_1, n_2, \cdots$ such that $\mathsf{C}, s \rightsquigarrow^{n_1} \mathsf{C}_1, s_1, ok \rightsquigarrow^{n_2} \mathsf{C}_2, s_2, ok \rightsquigarrow^{n_3} \cdots$, where the chain $\mathsf{C}, s \rightsquigarrow^{n_1} \mathsf{C}_1, s_1, ok \rightsquigarrow^{n_2} \mathsf{C}_2, s_2, ok \rightsquigarrow^{n_3} \cdots$ is a shorthand for $\mathsf{C}, s \rightsquigarrow^{n_1} \mathsf{C}_1, s_1, ok \land \mathsf{C}_1, s_1 \rightsquigarrow^{n_2} \mathsf{C}_2, s_2, ok \land \cdots$, and $\rightsquigarrow^n$ is defined as follows:

$$\begin{aligned} \mathsf{C}, s \rightsquigarrow^n \mathsf{C}', s', \epsilon \overset{\text{def}}{\iff} \quad & (n = 1 \land \mathsf{C}, s \rightarrow \mathsf{C}', s', \epsilon) \\ & \lor (\exists k, s'', \mathsf{C}''.\ n{=}k{+}1 \land \mathsf{C}, s \rightarrow \mathsf{C}'', s'', ok \land \mathsf{C}'', s'' \rightsquigarrow^k \mathsf{C}', s', \epsilon) \end{aligned}$$

Note that unlike the $\mathsf{C}, s \xrightarrow{n} \mathsf{C}', s'$ transitions in Def. 1 which describe *terminating* traces (either via short-circuiting or by reduction to skip), the $\mathsf{C}, s \rightsquigarrow^n \mathsf{C}', s'$ transitions do not stipulate termination and simply state that executing C from s for n steps reduces to C' and results in s'.

We next formalise the relationship between FUA and BUA triples (see p. 8), with the proof in §D.

Theorem 9. *For all p, C, q, ϵ:*
1) if $\models_{\mathsf{F}} [p]\ \mathsf{C}\ [\epsilon : q]$ and $\mathsf{min}_{\mathsf{pre}}(p, \mathsf{C}, q)$ hold, then $\models_{\mathsf{B}} [p]\ \mathsf{C}\ [\epsilon : q]$ also holds; and
2) if $\models_{\mathsf{B}} [p]\ \mathsf{C}\ [\epsilon : q]$ and $\mathsf{min}_{\mathsf{post}}(p, \mathsf{C}, q)$ hold, then $\models_{\mathsf{F}} [p]\ \mathsf{C}\ [\epsilon : q]$ also holds, where:

$$\mathsf{min}_{\mathsf{pre}}(p, \mathsf{C}, q) \overset{\text{def}}{\iff} \forall p'.\ p' \subset p \Rightarrow \not\models_{\mathsf{F}} [p']\,\mathsf{C}\,[\epsilon : q] \qquad \mathsf{min}_{\mathsf{post}}(p, \mathsf{C}, q) \overset{\text{def}}{\iff} \forall q'.\ q' \subset q \Rightarrow \not\models_{\mathsf{B}} [p]\,\mathsf{C}\,[\epsilon : q']$$

Finally, we show that the divergence proof system presented in Fig. 3 is *both sound and complete*, with the full proof given in the technical appendix (§B.3 and §C.2).

Theorem 10 (Divergence soundness and completeness)**.** *For all p and C, if $\vdash [p]\ \mathsf{C}\ [\infty]$ is derivable using the rules in Fig. 3, then $\models [p]\ \mathsf{C}\ [\infty]$ holds. For all p and C, if $\models [p]\ \mathsf{C}\ [\infty]$ holds, then $\vdash [p]\ \mathsf{C}\ [\infty]$ is derivable using the rules in Fig. 3.*

7 EXTENSION TO SEPARATION LOGIC

We describe how we develop UNTer$^{\text{SL}}$ by extending UNTer with the compositional reasoning principles of separation logic (SL) [18]. Raad et al. [24] have developed incorrectness separation logic (ISL) by extending the FUA-based incorrectness logic (IL) [23] with separation logic. As Raad et al. [24] argue, the original model of SL is unsound for FUA reasoning, and thus they adapt the original model to recover the soundness of ISL (see §E for details). We adopt the model of Raad et al. [24] and show that it is also sound for BUA reasoning.

***UNTer$^{\text{SL}}$* Programming Language and Assertions.** To account for operations that access the heap, in UNTer$^{\text{SL}}$ we extend our programming language from §4 with the following heap-manipulating operations (below, left) for allocation ($x := \mathsf{alloc}()$), deallocation ($\mathsf{free}(x)$), reading from the heap (lookup, $x := [y]$) and writing to the heap (mutation, $[x] := y$). We similarly extend the UNTer assertions as follows (below, right) by adding structural assertions to describe heaps.

$$\begin{aligned} \textsc{Comm} \ni \mathsf{C} ::= \ & \cdots \mid x := \mathsf{alloc}() \mid \mathsf{free}(x) \\ & \mid x := [y] \mid [x] := y \end{aligned} \qquad \begin{aligned} \textsc{Ast} \ni p, q, r ::= \ & \cdots \mid \mathsf{emp} \mid e \mapsto e' \\ & \mid e \not\mapsto \ \mid p * q \end{aligned}$$

The UNTer$^{\text{SL}}$ assertions describe sets of *states*, where a state comprises a (variable) store and a heap. The existing UNTer assertions from §4 then simply describe states in which the heap is empty and the store satisfies the assertion (as in UNTer). The structural assertions above are those of ISL [24] (which themselves are those of SL [18] extended with $e \not\mapsto$), and describe a set of states by constraining the shape of the underlying heap. More concretely, emp describes states in which the heap is empty; $e \mapsto e'$ describes states in which the heap comprises a single location denoted by e containing the value denoted by e'; similarly, $e \not\mapsto$ describes states in which the heap comprises a single location at e containing the designated value $\bot$; and $p * q$ describes states in which the heap can be split into two disjoint sub-heaps, one satisfying p and the other q. Note that whilst $e \mapsto e'$

AssignSL
$\vdash_{\dagger} [x{=}x'] \; x := e \; [ok{:}\, x{=}e[x'/x]]$

Store
$\vdash_{\dagger} [x \mapsto e] \; [x] := y \; [ok{:}\, x \mapsto y]$

StoreEr
$\vdash_{\dagger} [x \not\mapsto] \; [x] := y \; [er{:}\, x \not\mapsto]$

StoreNull
$\vdash_{\dagger} [x{=}\mathsf{null}] \; [x] := y \; [er{:}\, x{=}\mathsf{null}]$

Frame
$$\frac{\vdash_{\dagger} [p] \; \mathrm{C} \; [\epsilon : q] \qquad \mathsf{mod}(\mathrm{C}) \cap \mathsf{fv}(r) {=} \emptyset}{\vdash_{\dagger} [p * r] \; \mathrm{C} \; [\epsilon : q * r]}$$

Div-Frame
$$\frac{\vdash [p] \; \mathrm{C} \; [\infty]}{\vdash [p * r] \; \mathrm{C} \; [\infty]}$$

Fig. 7. UNTer$^{\text{SL}}$ proof rules (excerpt), where x and x' are distinct variables and † in each rule can be instantiated as F or B; see Fig. 9 in §E for the full set of UNTer$^{\text{SL}}$ rules.

states that the location at e is allocated (and contains value e'), $e \not\mapsto$ states that the location at e is *deallocated*. We write $e \mapsto -$ as a shorthand for $\exists v.\ e \mapsto v$.

UNTer^{SL} Proof Rules (Syntactic UNTer^{SL} Triples). We present an excerpt of the UNTer$^{\text{SL}}$ proof rules in Fig. 7; please see Fig. 9 in §E for the full set of rules. Note that all UNTer rules (both BUA and FUA) in Fig. 2, except Constancy and Assign, are also UNTer$^{\text{SL}}$ rules and are omitted from Fig. 9. In particular, we replace Constancy with the more powerful Frame rule and give a *local* rule for assignment (see below). As with ISL (and in contrast to UNTer), UNTer$^{\text{SL}}$ triples are *local* in that their pre-states only contain the resources needed by the program. For instance, as assignment requires no heap resources, as shown in AssignSL the pre-state of skip is simply given by the pure (non-heap) assertion $x{=}x'$, recording the old value of x which can be used in the post-state.

As in SL and ISL, the crux of UNTer$^{\text{SL}}$ lies in the Frame rule, allowing one to extend the pre- and post-states with disjoint resources in r, where $\mathsf{fv}(r)$ returns the set of free variables in r, and $\mathsf{mod}(\mathrm{C})$ returns the set of (program) variables modified by C (i.e. those on the left-hand of ':=' in assignment, lookup and allocation). These definitions are standard and elided. Heap manipulation rule are identical to those of ISL. For instance, Store describes a successful heap mutation, while StoreEr and StoreNull state that mutating x causes an error when x is deallocated or null, respectively.

The UNTer$^{\text{SL}}$ divergent proof rules are identical to those of UNTer in Fig. 3, except that the terminating (BUA) UNTer triples in the premises (e.g. the first premise of Div-Seq2) are replaced with their UNTer$^{\text{SL}}$ counterparts. Additionally, we can extend the framing principle to divergent triples as shown in Div-Frame. That is, if C has a divergent trace starting from the states in p, then it also has divergent traces starting from the states in $p * r$.

UNTer^{SL} Model and Semantics. As well as a (variable) store, in UNTer$^{\text{SL}}$ each state additionally includes a *heap* (memory); i.e. an UNTer$^{\text{SL}}$ state, $\sigma \in \textsc{State}^{\text{SL}} \triangleq \textsc{Store} \times \textsc{Heap}$, is a pair of the form (s, h), comprising a store $s \in \textsc{Store} \triangleq \textsc{Var} \rightarrow \textsc{Val}$ (as in UNTer) and a *heap* $h \in \textsc{Heap}$. The set of heaps is $\textsc{Heap} \triangleq \textsc{Loc} \overset{\text{fin}}{\rightharpoonup} \textsc{Val} \uplus \{\bot\}$; that is, each heap is a partial map from locations to either values (for allocated locations) or the designated $\bot$ value (for deallocated locations).

The semantics of UNTer$^{\text{SL}}$ assertions are as those of ISL and elided here (see §E). As with UNTer, we define the UNTer$^{\text{SL}}$ semantics through small-step transitions, where the semantics of constructs imported from UNTer are as in UNTer and are simply lifted to operate on UNTer$^{\text{SL}}$ states. The transitions of to heap-manipulating operations are standard and elided here (see Fig. 10 in §E).

Semantic BUA, FUA and Divergent triples in UNTer^{SL}. The formal interpretations of BUA, FUA and divergent triples in UNTer$^{\text{SL}}$ are identical to their UNTer counterparts, except that the UNTer states (stores) are replaced with corresponding UNTer$^{\text{SL}}$ states (pairs of stores and heaps).

More concretely, a BUA triple in UNTer$^{\text{SL}}$ is *valid*, written $\models_{\mathrm{B}} [p] \; \mathrm{C} \; [\epsilon : q]$, iff for all $\sigma_p \in p$, there exists $\sigma_q \in q$ and n such that $\mathrm{C}, \sigma_p \xrightarrow{n} -, \sigma_q, \epsilon$, where $\mathrm{C}, \sigma \xrightarrow{n} -, \sigma', \epsilon$ is as defined in Def. 1 with the UNTer states s, s', s'' replaced with corresponding UNTer$^{\text{SL}}$ states σ, σ' and σ'', and where

$\mathsf{C}, \sigma \rightarrow \mathsf{C}', \sigma', \epsilon$ corresponds to UNTER$^{\text{SL}}$ transitions described above. A FUA triple in UNTER$^{\text{SL}}$ is *valid*, written $\models_{\mathsf{F}} [p]\ \mathsf{C}\ [\epsilon : q]$, iff for all $\sigma_q \in q$, there exists $\sigma_p \in p$ and n such that $\mathsf{C}, \sigma_p \xrightarrow{n} -, \sigma_q, \epsilon$.

Analogously, a divergent triple in UNTER$^{\text{SL}}$ is *valid*, written $\models \left[p\right]\ \mathsf{C}\ [\infty]$, iff for all $\sigma \in p$, there exists an infinite series of $\mathsf{C}_1, \mathsf{C}_2, \cdots, \sigma_1, \sigma_2, \cdots$ and $n_1, n_2, \cdots$ such that $\mathsf{C}, \sigma \rightsquigarrow^{n_1} \mathsf{C}_1, \sigma_1, ok \rightsquigarrow^{n_2} \mathsf{C}_2, \sigma_2, ok \rightsquigarrow^{n_3} \cdots$, where $\rightsquigarrow^{n}$ is as defined Def. 2 with UNTER states s, s', s'' replaced with corresponding UNTER$^{\text{SL}}$ states σ, σ' and σ'', and where $\mathsf{C}, \sigma \rightarrow \mathsf{C}', \sigma', \epsilon$ denotes UNTER$^{\text{SL}}$ transitions.

Finally, we show that the BUA, FUA and divergent proof system of UNTER$^{\text{SL}}$ presented in Fig. 9 is sound, with the full proof given in the technical appendix (§F).

Theorem 11 (UNTER$^{\text{SL}}$ soundness). *For all p, q, C and ϵ:*

1) *if $\vdash_{\mathsf{B}} [p]\ \mathsf{C}\ [\epsilon : q]$ is derivable using the rules in Fig. 9, then $\models_{\mathsf{B}} [p]\ \mathsf{C}\ [\epsilon : q]$ holds;*
2) *if $\vdash_{\mathsf{F}} [p]\ \mathsf{C}\ [\epsilon : q]$ is derivable using the rules in Fig. 9, then $\models_{\mathsf{F}} [p]\ \mathsf{C}\ [\epsilon : q]$ holds; and*
3) *if $\vdash \left[p\right]\ \mathsf{C}\ [\infty]$ is derivable using the rules in Fig. 9, then $\models \left[p\right]\ \mathsf{C}\ [\infty]$ holds.*

8 PROTOTYPE IMPLEMENTATION

We describe our work-in-progress prototype implementation, Pulse$^\infty$, based on UNTER$^{\text{SL}}$ theory and as an extension of Pulse. Pulse$^\infty$ currently only detects the most obvious kinds of divergence bugs than can be characterised by UNTER$^{\text{SL}}$. As such, we plan on adding more features to Pulse$^\infty$ to support detection of additional divergence bug classes, including function calls, gotos and exception handling, which are all control-flow patterns that are supported by Pulse out of the box.

Pulse$^\infty$ Execution Domain. We generalise the Pulse execution domain in Pulse$^\infty$ by adding a new kind of error state *InfiniteExecution* on top of the existing *ok* and *er* states of Pulse. For every back-edge of the program, Pulse$^\infty$ checks the lasso property between the pre- and the post-states as $\left[p\right]\ \mathsf{C}^\star\ \left[ok\colon p\right]$; i.e. there exists a pre-state before the back-edge that is also a post-state. Each Pulse state contains 1) a disjunctive part that encodes the set of reachable states in a big disjunction, *one disjunct per path*, without merging path conditions; and 2) a non-disjunctive part that encodes other environment conditions that hold for all paths. Pulse$^\infty$ retains this product domain structure and our divergence extension only requires updating the disjunctive part of the Pulse state.

Abstract Interpreter. The Pulse checker implementation is based on an abstract interpretation subsystem of Infer known as Infer.AI, providing generic abstract domain primitives (e.g. top, bottom, and join) as well as generic widening and narrowing extensions for convergence acceleration. Pulse$^\infty$, as with Pulse, only uses widening to encode visiting the analysed program back-edges. Unlike Pulse, however, in Pulse$^\infty$ we also need to define widening for the disjunctive domain part of the state to check that a given state σ_p is reachable from itself *for a given path*. If such condition is found during widening, the new *InfiniteExecution* error state is added to the post-condition, and this error state is eventually reported when it bubbles up in the active Pulse state queue.

Scalability. The abduction and separation logic features of Pulse allow our analysis to be scalable, and running Pulse$^\infty$ on thousands of projects yields no perceptible performance change compared to Pulse, thus validating Pulse as a potential framework for compositional non-termination proving in practice. Further development and evaluation of Pulse$^\infty$ at scale is planned for future work.

9 RELATED WORK

There are of course very many individual reports of personal experience with non-termination bugs which many readers will no doubt have experienced. Our work gathering CVE's related to non-termination was an attempt to collect data on important such bugs occurring in practice. A recent empirical study is also worth noting, which looked at non-termination bugs in OSS projects, finding 445 non-termination bugs from 3,142 GitHub commits [27].

There has been significant work on automated methods for proving termination; see the survey by Cook et al. [11]. When a termination prover fails, the question of whether the failed proof identifies a termination bug or if it is a false positive is more difficult than proving safety: termination bugs cannot be generally witnessed with finite traces (assuming unbounded resources in the computation model, that is). However, as Godefroid argues [16], the main value of analysis tools lies in the discovery of bugs, not in the proof of program correctness. Thus, it is valuable to consider proving non-termination, even without waiting for the wide deployment of termination verifiers.

The fundamental work of Gupta et al. [17] looked at using proof to find non-termination bugs. They work with a transition system consisting of initial and final states and a transition relation, and they identify the concept of a *recurrence set* R as (i) a non-empty intersection with the initial set of states, and (ii) reachability of R from every state satisfying R. Reachability in (ii) corresponds to $\vdash_B \left[R\right]$ C $\left[ok\colon R\right]$. One might argue that the relation between the UNTer proof system for $\vdash_B \left[p\right]$ C $\left[ok\colon q\right]$ and the model of Gupta et al. [17] is analogous to the relation between Hoare's logic and Floyd's proof method [1]: using the under-approximate triples provides a route to compositional reasoning. There are many detailed differences beyond these points. They first run a concolic executor to gather assertions at program points, especially loop entry, but then employ an encoding in arithmetic to determine reachability facts for loop bodies, and they treat the heap concretely (as this encoding is difficult otherwise). By contrast, we reason about reachability both of the loop stems and bodies in the same logical system, and we use separation logic to reason abstractly about heaps (SL-based analyses were not available at the time of Gupta et al. [17]).

Our prototype, Pulse$^\infty$, inherits the strengths and weaknesses of Pulse. In terms of its strengths, it is easy to run Pulse$^\infty$ on program snippets, to scale it to large programs, and to incorporate it in a CI-based deployment on pull requests. In terms of its weaknesses, Pulse has a weak treatment of arithmetic, meaning that tricky examples (as in [17]) may not be provable. The strengths and weaknesses of [17] are the converse. We do not believe the weaknesses of either are inevitable; e.g. by adding a stronger arithmetic solver to Pulse$^\infty$ it would obviously be possible to prove tricky examples; the question is the effect this would have on performance.

After Gupta et al. [17], there have been many further papers on automatic non-termination proving or checking. Cook et al. [8], Chen et al. [7] introduce novel ideas on the use of over-approximation, going beyond the under-approximate logics here. Le et al. [20] introduce a separation logic for proving both termination and non-termination, using temporal predicates in preconditions, and we are not sure of the relation to the under-approximate approach here.

The idea of finding non-termination bugs using proof is appealing, and it is perhaps not intuitively too complicated. Although this paper is but a step on the way, it is not unreasonable to hope that non-termination proof techniques, with further maturation, might be developed to a degree where they could be routinely deployed in engineering practice.

REFERENCES

[1] Krzysztof R. Apt and Ernst-Rüdiger Olderog. 2019. Fifty years of Hoare's logic. *Formal Aspects Comput.* 31, 6 (2019), 751–807. https://doi.org/10.1007/s00165-019-00501-3

[2] Josh Berdine, Aziem Chawdhary, Byron Cook, Dino Distefano, and Peter O'Hearn. 2007. Variance Analyses from Invariance Analyses. *SIGPLAN Not.* 42, 1 (jan 2007), 211–224. https://doi.org/10.1145/1190215.1190249

[3] Josh Berdine, Byron Cook, Dino Distefano, and Peter W. O'Hearn. 2006. Automatic Termination Proofs for Programs with Shape-Shifting Heaps. In *Computer Aided Verification*, Thomas Ball and Robert B. Jones (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 386–400.

[4] Sam Blackshear, Nikos Gorogiannis, Peter W. O'Hearn, and Ilya Sergey. 2018. RacerD: Compositional Static Race Detection. *Proc. ACM Program. Lang.* 2, OOPSLA, Article 144 (Oct. 2018), 28 pages. https://doi.org/10.1145/3276514

[5] Cristiano Calcagno, Dino Distefano, Peter W. O'Hearn, and Hongseok Yang. 2011. Compositional Shape Analysis by Means of Bi-Abduction. *J. ACM* 58, 6, Article 26 (Dec. 2011), 66 pages. http://doi.acm.org/10.1145/2049697.2049700

[6] Aziem Chawdhary, Byron Cook, Sumit Gulwani, Mooly Sagiv, and Hongseok Yang. 2008. Ranking Abstractions. In *Programming Languages and Systems*, Sophia Drossopoulou (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 148–162.

[7] Hong Yi Chen, Byron Cook, Carsten Fuhs, Kaustubh Nimkar, and Peter W. O'Hearn. 2014. Proving Nontermination via Safety. In *Tools and Algorithms for the Construction and Analysis of Systems - 20th International Conference, TACAS 2014, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2014, Grenoble, France, April 5-13, 2014. Proceedings (Lecture Notes in Computer Science)*, Erika Ábrahám and Klaus Havelund (Eds.), Vol. 8413. Springer, 156–171. https://doi.org/10.1007/978-3-642-54862-8_11

[8] Byron Cook, Carsten Fuhs, Kaustubh Nimkar, and Peter W. O'Hearn. 2015. Embracing Overapproximation for Proving Nontermination. *Tiny Trans. Comput. Sci.* 3 (2015). http://tinytocs.org/vol3/papers/TinyToCS_3_cook.pdf

[9] Byron Cook, Andreas Podelski, and Andrey Rybalchenko. 2006. Termination Proofs for Systems Code. *SIGPLAN Not.* 41, 6 (jun 2006), 415–426. https://doi.org/10.1145/1133255.1134029

[10] Byron Cook, Andreas Podelski, and Andrey Rybalchenko. 2006. Terminator: Beyond Safety. In *Computer Aided Verification*, Thomas Ball and Robert B. Jones (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 415–418.

[11] Byron Cook, Andreas Podelski, and Andrey Rybalchenko. 2011. Proving program termination. *Commun. ACM* 54, 5 (2011), 88–98. https://doi.org/10.1145/1941487.1941509

[12] Pedro da Rocha Pinto, Thomas Dinsdale-Young, Philippa Gardner, and Julian Sutherland. 2016. Modular Termination Verification for Non-blocking Concurrency. In *Programming Languages and Systems*, Peter Thiemann (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 176–201.

[13] Edsko de Vries and Vasileios Koutavas. 2011. Reverse Hoare Logic. In *Software Engineering and Formal Methods - 9th International Conference, SEFM 2011, Montevideo, Uruguay, November 14-18, 2011. Proceedings.* 155–171. https://doi.org/10.1007/978-3-642-24690-6_12

[14] Dino Distefano, Manuel Fähndrich, Francesco Logozzo, and Peter W. O'Hearn. 2019. Scaling static analyses at Facebook. *Commun. ACM* 62, 8 (2019), 62–70. https://doi.org/10.1145/3338112

[15] Emanuele D'Osualdo, Julian Sutherland, Azadeh Farzan, and Philippa Gardner. 2021. TaDA Live: Compositional Reasoning for Termination of Fine-Grained Concurrent Programs. *ACM Trans. Program. Lang. Syst.* 43, 4, Article 16 (nov 2021), 134 pages. https://doi.org/10.1145/3477082

[16] Patrice Godefroid. 2005. The soundness of bugs is what matters (position statement). https://www.cs.umd.edu/~pugh/BugWorkshop05/papers/11-godefroid.pdf

[17] Ashutosh Gupta, Thomas A. Henzinger, Rupak Majumdar, Andrey Rybalchenko, and Ru-Gang Xu. 2008. Proving non-termination. In *Proceedings of the 35th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2008, San Francisco, California, USA, January 7-12, 2008*, George C. Necula and Philip Wadler (Eds.). ACM, 147–158. https://doi.org/10.1145/1328438.1328459

[18] Samin S. Ishtiaq and Peter W. O'Hearn. 2001. BI as an Assertion Language for Mutable Data Structures. In *Proceedings of the 28th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages* (London, United Kingdom) *(POPL)*. Association for Computing Machinery, New York, NY, USA, 14–26. https://doi.org/10.1145/360204.375719

[19] Quang Loc Le, Azalea Raad, Jules Villard, Josh Berdine, Derek Dreyer, and Peter W. O'Hearn. 2022. Finding Real Bugs in Big Programs with Incorrectness Logic. *Proc. ACM Program. Lang.* 6, OOPSLA1, Article 81 (apr 2022), 27 pages. https://doi.org/10.1145/3527325

[20] Ton Chanh Le, Shengchao Qin, and Wei-Ngan Chin. 2015. Termination and non-termination specification inference. In *Proceedings of the 36th ACM SIGPLAN Conference on Programming Language Design and Implementation, Portland, OR, USA, June 15-17, 2015*, David Grove and Stephen M. Blackburn (Eds.). ACM, 489–498. https://doi.org/10.1145/2737924.2737993

[21] Hongjin Liang and Xinyu Feng. 2016. A Program Logic for Concurrent Objects under Fair Scheduling. *SIGPLAN Not.* 51, 1 (jan 2016), 385–399. https://doi.org/10.1145/2914770.2837635

[22] Bernhard Möller, Peter W. O'Hearn, and Tony Hoare. 2021. On Algebra of Program Correctness and Incorrectness. In *Relational and Algebraic Methods in Computer Science - 19th International Conference, RAMiCS 2021, Marseille, France, November 2-5, 2021, Proceedings (Lecture Notes in Computer Science)*, Uli Fahrenberg, Mai Gehrke, Luigi Santocanale, and Michael Winter (Eds.), Vol. 13027. Springer, 325–343. https://doi.org/10.1007/978-3-030-88701-8_20

[23] Peter W. O'Hearn. 2019. Incorrectness Logic. *Proc. ACM Program. Lang.* 4, POPL, Article 10 (Dec. 2019), 32 pages. http://doi.acm.org/10.1145/3371078

[24] Azalea Raad, Josh Berdine, Hoang-Hai Dang, Derek Dreyer, Peter O'Hearn, and Jules Villard. 2020. Local Reasoning About the Presence of Bugs: Incorrectness Separation Logic. In *Computer Aided Verification*, Shuvendu K. Lahiri and Chao Wang (Eds.). Springer International Publishing, Cham, 225–252.

[25] Azalea Raad, Josh Berdine, Derek Dreyer, and Peter W. O'Hearn. 2022. Concurrent Incorrectness Separation Logic. *Proc. ACM Program. Lang.* 6, POPL, Article 34 (jan 2022), 29 pages. https://doi.org/10.1145/3498695

[26] Caitlin Sadowski, Edward Aftandilian, Alex Eagle, Liam Miller-Cushon, and Ciera Jaspan. 2018. Lessons from Building Static Analysis Tools at Google. *Commun. ACM* 61, 4 (March 2018), 58–66. https://doi.org/10.1145/3188720

[27] Xiuhan Shi, Xiaofei Xie, Yi Li, Yao Zhang, Sen Chen, and Xiaohong Li. 2022. Large-scale analysis of non-termination bugs in real-world OSS projects. In *Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering, ESEC/FSE 2022, Singapore, Singapore, November 14-18, 2022*, Abhik Roychoudhury, Cristian Cadar, and Miryung Kim (Eds.). ACM, 256–268. https://doi.org/10.1145/3540250.3549129

A DERIVED RULES

IfTrue Derivation

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash_\dagger [p \land B]\ \mathsf{assume}(B)\ [ok\colon p \land B]}\ (\textsc{Assume}) \qquad \dfrac{}{\vdash_\dagger [p \land B]\ \mathsf{C}_1\ [ok\colon q]}\ (\text{given})}{\vdash_\dagger [p \land B]\ \mathsf{assume}(B);\mathsf{C}_1\ [\epsilon : q]}\ (\textsc{Seq})}{\vdash_\dagger [p \land B]\ (\mathsf{assume}(B);\mathsf{C}_1) + (\mathsf{assume}(\neg B);\mathsf{C}_2)\ [\epsilon : q]}\ (\textsc{Choice})}{\vdash_\dagger [p \land B]\ \mathsf{if}\ (B)\ \mathsf{then}\ \mathsf{C}_1\ \mathsf{else}\ \mathsf{C}_2\ [\epsilon : q]}\ (\text{If encoding})$$

IfFalse Derivation

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash_\dagger [p \land \neg B]\ \mathsf{assume}(\neg B)\ [ok\colon p \land \neg B]}\ (\textsc{Assume}) \qquad \dfrac{}{\vdash_\dagger [p \land \neg B]\ \mathsf{C}_2\ [ok\colon q]}\ (\text{given})}{\vdash_\dagger [p \land \neg B]\ \mathsf{assume}(\neg B);\mathsf{C}_2\ [\epsilon : q]}\ (\textsc{Seq})}{\vdash_\dagger [p \land \neg B]\ (\mathsf{assume}(B);\mathsf{C}_1) + (\mathsf{assume}(\neg B);\mathsf{C}_2)\ [\epsilon : q]}\ (\textsc{Choice})}{\vdash_\dagger [p \land \neg B]\ \mathsf{if}\ (B)\ \mathsf{then}\ \mathsf{C}_1\ \mathsf{else}\ \mathsf{C}_2\ [\epsilon : q]}\ (\text{If encoding})$$

ConsEq Derivation (BUA case)

$$\dfrac{\dfrac{\dfrac{}{p \Leftrightarrow p'}\ (\text{given})}{p \subseteq p'} \qquad \dfrac{}{\vdash_{\mathsf{B}}\ [p']\ \mathsf{C}\ [\epsilon : q']}\ (\text{given}) \qquad \dfrac{\dfrac{}{q \Leftrightarrow q'}\ (\text{given})}{q' \subseteq q}}{\vdash_{\mathsf{B}}\ [p]\ \mathsf{C}\ [\epsilon : q]}\ (\textsc{ConsF})$$

ConsEq Derivation (FUA case)

$$\dfrac{\dfrac{\dfrac{}{p \Leftrightarrow p'}\ (\text{given})}{p' \subseteq p} \qquad \dfrac{}{\vdash_{\mathsf{F}}\ [p']\ \mathsf{C}\ [\epsilon : q']}\ (\text{given}) \qquad \dfrac{\dfrac{}{q \Leftrightarrow q'}\ (\text{given})}{q \subseteq q'}}{\vdash_{\mathsf{F}}\ [p]\ \mathsf{C}\ [\epsilon : q]}\ (\textsc{ConsB})$$

WhileFalse Derivation

$$\dfrac{\dfrac{\dfrac{}{\vdash_\dagger [p \land \neg B]\ (\mathsf{assume}(B);\mathsf{C})^\star\ [ok\colon p \land \neg B]}\ (\textsc{Loop0}) \qquad \dfrac{}{\vdash_\dagger [p \land \neg B]\ \mathsf{assume}(\neg B)\ [ok\colon p \land \neg B]}\ (\textsc{Assume})}{\vdash_\dagger [p \land \neg B]\ (\mathsf{assume}(B);\mathsf{C})^\star;\mathsf{assume}(\neg B)\ [ok\colon p \land \neg B]}\ (\textsc{Seq})}{\vdash_\dagger [p \land \neg B]\ \mathsf{while}\ (B)\ \mathsf{C}\ [ok\colon p \land \neg B]}\ (\text{while encoding})$$

WhileSubvariant Derivation

In the following, let $r(n) \triangleq p(n) \land B$ for all $n \in \mathbb{N}$:

$$\dfrac{\dfrac{\dfrac{\dfrac{(1) \quad (2)}{\vdash_\dagger [p(0) \land B]\ (\mathsf{assume}(B);\mathsf{C})^\star;\mathsf{assume}(B);\mathsf{C}\ [ok\colon q \land \neg B]}\ (\textsc{Seq})}{\vdash_\dagger [p(0) \land B]\ (\mathsf{assume}(B);\mathsf{C})^\star\ [ok\colon q \land \neg B]}\ (\textsc{Loop}) \qquad \dfrac{}{\vdash_\dagger [q \land \neg B]\ \mathsf{assume}(\neg B)\ [ok\colon q \land \neg B]}\ (\textsc{Assume})}{\vdash_\dagger [p(0) \land B]\ (\mathsf{assume}(B);\mathsf{C})^\star;\mathsf{assume}(\neg B)\ [ok\colon q \land \neg B]}\ (\textsc{Seq})}{\vdash_\dagger [p(0) \land B]\ \mathsf{while}\ (B)\ \mathsf{C}\ [ok\colon q \land \neg B]}\ (\text{while encoding})$$

with

$$\begin{array}{c}\dfrac{\dfrac{\dfrac{\dfrac{}{\forall n < k.\ \vdash_{\dagger} [r(n)]\ \mathsf{assume}(B)\ [ok\colon r(n)]}\ \text{\textsc{Assume}} \qquad \dfrac{}{\forall n < k.\ \vdash_{\dagger} [r(n)]\ \mathsf{C}\ [ok\colon r(n{+}1)]}\ (\text{given})}{\forall n < k.\ \vdash_{\dagger} [r(n)]\ \mathsf{assume}(B); \mathsf{C}\ [ok\colon r(n{+}1)]}\ (\text{\textsc{Seq}})}{\vdash_{\dagger} [r(0)]\ (\mathsf{assume}(B); \mathsf{C})^{\star}\ [ok\colon r(k)]}\ (\text{\textsc{Loop-Subvariant}})}{\vdash_{\dagger} [p(0) \land B]\ (\mathsf{assume}(B); \mathsf{C})^{\star}\ [ok\colon p(k) \land B]}\ (\text{definition of } r) \\ \hline (1)\end{array}$$

and

$$\begin{array}{c}\dfrac{\dfrac{}{\vdash_{\dagger} [p(k) \land B]\ \mathsf{assume}(B)\ [ok\colon p(k) \land B]}\ (\text{\textsc{Assume}}) \qquad \dfrac{}{\vdash_{\dagger} [p(k) \land B]\ \mathsf{C}\ [ok\colon q \land \neg B]}\ (\text{given})}{\vdash_{\dagger} [p(k) \land B]\ \mathsf{assume}(B); \mathsf{C}\ [ok\colon q \land \neg B]}\ (\text{\textsc{Seq}}) \\ \hline (2)\end{array}$$

\textsc{Div-LoopNest} Derivation

In the following, let $q(n) \triangleq p(n) \land B$ for all $n \in \mathbb{N}$:

$$\dfrac{\dfrac{\dfrac{}{[p]\ \mathsf{C}\ [\infty]}\ (\text{given})}{[p]\ \mathsf{C}; \mathsf{C}^{\star}\ [\infty]}\ (\text{\textsc{Div-Seq1}})}{[p]\ \mathsf{C}^{\star}\ [\infty]}\ (\text{\textsc{Div-LoopUnfold}})$$

\textsc{Div-While} Derivation

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash_{\mathsf{B}}\ [p \land B]\ \mathsf{assume}(B)\ [ok\colon p \land B]}\ (\text{\textsc{Assume}}) \qquad \dfrac{}{\vdash_{\mathsf{B}}\ [p \land B]\ \mathsf{C}\ [ok\colon q \land B]}\ (\text{given})}{\vdash_{\mathsf{B}}\ [p \land B]\ \mathsf{assume}(B); \mathsf{C}\ [ok\colon q \land B]}\ (\text{\textsc{Seq}}) \qquad \dfrac{\dfrac{}{q \subseteq p}\ (\text{given})}{q \land B \subseteq p \land B}}{[p \land B]\ (\mathsf{assume}(B); \mathsf{C})^{\star}\ [\infty]}\ (\text{\textsc{Div-Loop}})}{[p \land B]\ (\mathsf{assume}(B); \mathsf{C})^{\star}; \mathsf{assume}(\neg B)\ [\infty]}\ (\text{\textsc{Div-Seq1}})}{[p \land B]\ \mathsf{while}\ (B)\ \mathsf{C}\ [\infty]}\ (\text{while encoding})$$

\textsc{Div-WhileNest} Derivation

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash_{\mathsf{B}}\ [p \land B]\ \mathsf{assume}(B)\ [ok\colon p \land B]}\ (\text{\textsc{Assume}}) \qquad \dfrac{}{[p \land B]\ \mathsf{C}\ [\infty]}\ (\text{given})}{[p \land B]\ \mathsf{assume}(B); \mathsf{C}\ [\infty]}\ (\text{\textsc{Div-Seq2}})}{[p \land B]\ (\mathsf{assume}(B); \mathsf{C})^{\star}\ [\infty]}\ (\text{\textsc{Div-LoopNest}})}{[p \land B]\ (\mathsf{assume}(B); \mathsf{C})^{\star}; \mathsf{assume}(\neg B)\ [\infty]}\ (\text{\textsc{Div-Seq1}})}{[p \land B]\ \mathsf{while}\ (B)\ \mathsf{C}\ [\infty]}\ (\text{while encoding})$$

\textsc{Div-WhileSubvariant} Derivation

In the following, let $q(n) \triangleq p(n) \land B$ for all $n \in \mathbb{N}$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall n \in \mathbb{N}.\ \vdash_{\mathrm{B}} \big[q(n)\big]\ \mathsf{assume}(B)\ \big[ok\colon q(n)\big]}\ (\textsc{Assume}) \qquad \dfrac{}{\forall n \in \mathbb{N}.\ \vdash_{\mathrm{B}} \big[q(n)\big]\ \mathsf{C}\ \big[ok\colon q(n{+}1)\big]}\ (\text{given})}{\forall n \in \mathbb{N}.\ \vdash_{\mathrm{B}} \big[q(n)\big]\ (\mathsf{assume}(B);\mathsf{C})\ \big[ok\colon q(n{+}1)\big]}\ (\textsc{Seq})}{\big[q(0)\big]\ (\mathsf{assume}(B);\mathsf{C})^{\star}\ [\infty]}\ (\textsc{Div-Subvariant})}{\big[p(0) \land B\big]\ (\mathsf{assume}(B);\mathsf{C})^{\star}\ [\infty]}\ (\text{definition of } q(0))}{\big[p(0) \land B\big]\ (\mathsf{assume}(B);\mathsf{C})^{\star};\mathsf{assume}(\neg B)\ [\infty]}\ (\textsc{Div-Seq1})}{\big[p(0) \land B\big]\ \mathsf{while}\ (B)\ \mathsf{C}\ [\infty]}\ (\text{while encoding})$$

$$\textsc{S-Local}\ \frac{s' = s[x \mapsto v] \quad v \in \textsc{Val}}{\mathsf{local}\ x\ \mathsf{in}\ \mathsf{C}, s \to \mathsf{C}; \mathsf{end}(x, s(x)), s'} \qquad \textsc{S-LocalEnd}\ \frac{s' = s[x \mapsto v]}{\mathsf{end}(x, v), s \to \mathsf{skip}, s'} \qquad \textsc{S-Assign}\ \frac{s' = s[x \mapsto s(e)]}{x := e, s \to \mathsf{skip}, s', ok}$$

$$\textsc{S-Assume}\ \frac{s(B) = \mathsf{true}}{\mathsf{assume}(B), s \to \mathsf{skip}, s, ok} \qquad \textsc{S-Error}\ \mathsf{error}, s \to \mathsf{skip}, s, er \qquad \textsc{S-Choice}\ \frac{i \in \{1, 2\}}{\mathsf{C}_1 + \mathsf{C}_2, s \to \mathsf{C}_i, s, ok} \qquad \textsc{S-Seq1}\ \frac{\mathbb{C}_1, s \to \mathbb{C}_1', s', \epsilon}{\mathbb{C}_1; \mathbb{C}_2, s \to \mathbb{C}_1'; \mathbb{C}_2, s', \epsilon}$$

$$\textsc{S-SeqSkip}\ \mathsf{skip}; \mathbb{C}, s \to \mathbb{C}, s, ok \qquad \textsc{S-Loop0}\ \mathsf{C}^\star, s \to \mathsf{skip}, s, ok \qquad \textsc{S-Loop}\ \mathsf{C}^\star, s \to \mathsf{C}; \mathsf{C}^\star, s, ok$$

Fig. 8. The UNTer small-step operational semantics

B UNTer SEMANTICS AND SOUNDNESS

Instrumented Commands and Operational Semantics. Although in sequential settings the semantics is given in the big-step fashion [23, 24], we opt for *small-step* semantics instead. This is because big-step semantics by definition describe *terminating* executions, while our aim is to formalise the semantics of divergent triples. Specifically, as we describe below, we formalise the semantics of a divergent triple as an *infinite*, non-terminating execution trace.

Note that local x in C declares a variable x whose scope is limited to C. To describe the semantics of local x in C in a small-step fashion, we introduce *instrumented commands*, defined by the grammar below (where C is as defined in §4), which additionally include the $\mathsf{end}(x, v)$ construct, recording the existing (old) value of x when redeclaring x in a new scope.

$$\mathbb{C} ::= \mathsf{C} \mid \mathsf{end}(x, v) \mid \mathbb{C}_1; \mathbb{C}_2$$

We present our small-step semantics in Fig. 8, with transitions of the form $\mathbb{C}, s \to \mathbb{C}', s', \epsilon$, where $\mathbb{C}$ and s respectively denote the current (instrumented) command and store (state), $\mathbb{C}'$ and s' denote their continuations (what they reduce to) and ϵ denotes the exit condition, describing whether reducing $\mathbb{C}$ to $\mathbb{C}'$ took place normally (ok) or erroneously (er). As shown in S-Local, when evaluating local x in C under a state $s \in \textsc{Store}$, we assign an arbitrary value v to x in s, and continue with executing C followed by $\mathsf{end}(x, s(x))$. That is, we record the existing value of x, $s(x)$, so that we can restore it once the execution of C has ended, as reflected in the S-LocalEnd transition.

The remaining transition rules are standard: assigning e to x simply evaluates e in the current state (denoted by $s(e)$) and updates the value of x in the state, terminating normally; $\mathsf{assume}(B)$ reduces to skip normally when B evaluates to true in the current state; error reduces to skip erroneously; and $\mathsf{C}_1 + \mathsf{C}_2$ non-deterministically reduces to one of its branches (C_i with $i \in \{1, 2\}$). When reducing $\mathbb{C}_1; \mathbb{C}_2$, we either reduce the left-hand side until it reduces to skip (S-Seq1), or continue with the right-hand side when the left side is skip (S-SeqSkip). Finally, we either reduce a loop to skip, i.e. unroll it zero times (S-Loop0), or unroll it once and continue with $\mathsf{C}^\star$ (S-Loop).

B.1 UNTer Semantics

Lemma 1. *For all n, s, s', C, C', if $\mathsf{C}, s \xrightarrow{n} \mathsf{C}', s', ok$, then $\mathsf{C}' = \mathsf{skip}$.*

Proof. By induction on n.

Base case n=0

Pick arbitrary s, s', C, C' such that $\mathsf{C}, s \xrightarrow{0} \mathsf{C}', s', ok$. From the definition of $\xrightarrow{0}$ we then have C'=skip, as required.

Inductive case $n{=}k{+}1$

Pick arbitrary s, s', C, C' such that $\mathrm{C}, s \xrightarrow{n} \mathrm{C}', s', \mathit{ok}$. From the definition of $\xrightarrow{n}$ we know there exists C'', s'' such that $\mathrm{C}, s \to \mathrm{C}'', s'', \mathit{ok}$ and $\mathrm{C}'', s'' \xrightarrow{k} \mathrm{C}', s', \mathit{ok}$. As such, from $\mathrm{C}'', s'' \xrightarrow{k} \mathrm{C}', s', \mathit{ok}$ and the inductive hypothesis we have $\mathrm{C}'{=}\mathrm{skip}$, as required. □

B.2 Soundness of BUA and FUA Rules

Proposition 12. *For all* $r, s, \mathrm{C}, n, s', \epsilon$, *if* $s \in r$, $\mathrm{fv}(r) \cap \mathrm{mod}(\mathrm{C}) = \emptyset$ *and* $\mathrm{C}, s \xrightarrow{n} -, s', \epsilon$, *then* $s' \in r$.

Lemma 2. *For all* s, s', s'', C_1, C_2, C', i, j, ϵ, *if* $\mathrm{C}_1, s \xrightarrow{i} -, s'', \mathit{ok}$ *and* $\mathrm{C}_2, s'' \xrightarrow{j} \mathrm{C}', s', \epsilon$, *then there exists* n *such that* $\mathrm{C}_1; \mathrm{C}_2, s \xrightarrow{n} \mathrm{C}', s', \epsilon$.

Proof. Pick arbitrary s, s', s'', C_1, C_2, C', C'', i, j, ϵ, such that $\mathrm{C}_1, s \xrightarrow{i} \mathrm{C}'', s'', \mathit{ok}$ and $\mathrm{C}_2, s'' \xrightarrow{j} \mathrm{C}', s', \epsilon$. We proceed by induction on i.

Case $i = 0$

From $\mathrm{C}_1, s \xrightarrow{0} \mathrm{C}'', s'', \mathit{ok}$ we know $\mathrm{C}_1 = \mathrm{C}'' = \mathrm{skip}$ and $s = s''$. As such, since $\mathrm{C}_1 = \mathrm{skip}$ and $s = s''$, from S-SeqSkip we have $\mathrm{C}_1; \mathrm{C}_2, s \to \mathrm{C}_2, s'', \mathit{ok}$. Consequently, from $\mathrm{C}_2, s'' \xrightarrow{j} \mathrm{C}', s', \epsilon$ and the definition of $\xrightarrow{j+1}$ we have $\mathrm{C}_1; \mathrm{C}_2, s \xrightarrow{j+1} \mathrm{C}', s', \epsilon$, as required.

Case $i = k{+}1$

From the definition of $\mathrm{C}_1, s \xrightarrow{i} \mathrm{C}'', s'', \mathit{ok}$ we then know there exists C_3, s_3 such that $\mathrm{C}_1, s \to \mathrm{C}_3, s_3, \mathit{ok}$ and $\mathrm{C}_3, s_3 \xrightarrow{k} \mathrm{C}'', s'', \mathit{ok}$. As such, from the inductive hypothesis, $\mathrm{C}_3, s_3 \xrightarrow{k} \mathrm{C}'', s'', \mathit{ok}$ and $\mathrm{C}_2, s'' \xrightarrow{j} \mathrm{C}', s', \epsilon$ we know there exists n such that $\mathrm{C}_3; \mathrm{C}_2, s_3 \xrightarrow{n} \mathrm{C}', s', \epsilon$. Moreover, as $\mathrm{C}_1, s \to \mathrm{C}_3, s_3, \mathit{ok}$, from S-Seq1 we have $\mathrm{C}_1; \mathrm{C}_2, s \to \mathrm{C}_3; \mathrm{C}_2, s_3, \mathit{ok}$. Consequently, as $\mathrm{C}_1; \mathrm{C}_2, s \to \mathrm{C}_3; \mathrm{C}_2, s_3, \mathit{ok}$ and $\mathrm{C}_3; \mathrm{C}_2, s_3 \xrightarrow{n} \mathrm{C}', s', \epsilon$, from the definition of $\xrightarrow{n+1}$ we have $\mathrm{C}_1; \mathrm{C}_2, s \xrightarrow{n+1} \mathrm{C}', s', \epsilon$, as required. □

Lemma 3. *For all* s, s', C_1, C_2, C', i, *if* $\mathrm{C}_1, s \xrightarrow{i} \mathrm{C}', s', \mathit{er}$, *then* $\mathrm{C}_1; \mathrm{C}_2, s \xrightarrow{i} \mathrm{C}'; \mathrm{C}_2, s', \mathit{er}$.

Proof. Pick arbitrary s, s', C_1, C_2, C', i such that $\mathrm{C}_1, s \xrightarrow{i} \mathrm{C}', s', \mathit{er}$. We proceed by induction on i.

Case $i = 1$

From $\mathrm{C}_1, s \xrightarrow{1} \mathrm{C}', s', \mathit{er}$ we know $\mathrm{C}_1, s \to \mathrm{C}', s', \mathit{er}$. As such, from S-Seq1 we have $\mathrm{C}_1; \mathrm{C}_2, s \to \mathrm{C}'; \mathrm{C}_2, s', \mathit{er}$. Consequently, from the definition of $\xrightarrow{1}$ we have $\mathrm{C}_1; \mathrm{C}_2, s \xrightarrow{1} \mathrm{C}'; \mathrm{C}_2, s', \mathit{er}$, as required.

Case $i = k{+}1$

From the definition of $\mathrm{C}_1, s \xrightarrow{i} \mathrm{C}', s', \mathit{er}$ we then know there exists C_3, s_3 such that $\mathrm{C}_1, s \to \mathrm{C}_3, s_3, \mathit{ok}$ and $\mathrm{C}_3, s_3 \xrightarrow{k} \mathrm{C}', s', \mathit{er}$. As such, from the inductive hypothesis and $\mathrm{C}_3, s_3 \xrightarrow{k} \mathrm{C}', s', \mathit{er}$ we know $\mathrm{C}_3; \mathrm{C}_2, s_3 \xrightarrow{k} \mathrm{C}'; \mathrm{C}_2, s', \mathit{er}$. Moreover, as $\mathrm{C}_1, s \to \mathrm{C}_3, s_3, \mathit{ok}$, from S-Seq1 we have $\mathrm{C}_1; \mathrm{C}_2, s \to \mathrm{C}_3; \mathrm{C}_2, s_3, \mathit{ok}$. Consequently, as $\mathrm{C}_1; \mathrm{C}_2, s \to \mathrm{C}_3; \mathrm{C}_2, s_3, \mathit{ok}$ and $\mathrm{C}_3; \mathrm{C}_2, s_3 \xrightarrow{k} \mathrm{C}'; \mathrm{C}_2, s', \mathit{er}$, from the definition of $\xrightarrow{k+1}$ we have $\mathrm{C}_1; \mathrm{C}_2, s \xrightarrow{k+1} \mathrm{C}'; \mathrm{C}_2, s', \mathit{er}$, as required. □

Lemma 4. *For all* $n, \mathrm{C}_1, \mathrm{C}_2, s, s', \epsilon$, *if* $\mathrm{C}_1; \mathrm{C}_2, s \xrightarrow{n} -, s', \epsilon$ *then either* $\epsilon = \mathit{er}$ *and* $\mathrm{C}_1, s \xrightarrow{n} -, s', \epsilon$, *or there exists* $i, j \leq n, s''$ *such that* $\mathrm{C}_1, s \xrightarrow{i} -, s'', \mathit{ok}$ *and* $\mathrm{C}_2, s'' \xrightarrow{j} -, s', \epsilon$.

Proof. By induction on n.

Base case n=0
Pick arbitrary $\mathsf{C}_1, \mathsf{C}_2, s, s', \epsilon$ such that $\mathsf{C}_1; \mathsf{C}_2, s \xrightarrow{0} -, s', \epsilon$. This case does not arise as $\mathsf{C}_1; \mathsf{C}_2, s \xrightarrow{0} -, s', \epsilon$ would imply $\mathsf{C}_1; \mathsf{C}_2 = \mathsf{skip}$, leading to a contradiction.

Base case n=1 and ϵ=er
Pick arbitrary $\mathsf{C}_1, \mathsf{C}_2, s, s', \epsilon$ such that $\mathsf{C}_1; \mathsf{C}_2, s \xrightarrow{1} -, s', er$. From the definition of $\mathsf{C}_1; \mathsf{C}_2, s \xrightarrow{1} -, s', er$ we know $\mathsf{C}_1; \mathsf{C}_2, s \rightarrow -, s', er$, and thus by inversion on $\mathsf{C}_1; \mathsf{C}_2, s \rightarrow -, s', er$ we know $\mathsf{C}_1, s \xrightarrow{1} -, s', er$, as required.

Inductive case n=k+1
Pick arbitrary $\mathsf{C}_1, \mathsf{C}_2, s, s', \epsilon$ such that $\mathsf{C}_1; \mathsf{C}_2, s \xrightarrow{n} -, s', \epsilon$. From the definition of $\xrightarrow{n}$ we then know there exist C', s'' such that $\mathsf{C}_1; \mathsf{C}_2, s \rightarrow \mathsf{C}', s'', ok$ and $\mathsf{C}', s'' \xrightarrow{k} -, s', \epsilon$. From inversion on $\mathsf{C}_1; \mathsf{C}_2, s \rightarrow \mathsf{C}', s'', ok$ there are two cases to consider: 1) $\mathsf{C}_1 = \mathsf{skip}$, $\mathsf{C}' = \mathsf{C}_2$, $s'' = s$, i.e. $\mathsf{C}_1; \mathsf{C}_2, s \rightarrow \mathsf{C}_2, s, ok$; or 2) there exists C_1' such that $\mathsf{C}_1, s \rightarrow \mathsf{C}_1', s'', ok$ and $\mathsf{C}' = \mathsf{C}_1'; \mathsf{C}_2$.

In case (1), by definition we have $\mathsf{C}_1, s \xrightarrow{0} \mathsf{skip}, s'', ok$. Moreover, as $\mathsf{C}' = \mathsf{C}_2$, from $\mathsf{C}', s'' \xrightarrow{k} -, s', \epsilon$ we have $\mathsf{C}_2, s'' \xrightarrow{k} -, s', \epsilon$. That is, as $0 \leq n$ and $k \leq n$, we have $\mathsf{C}_1, s \xrightarrow{0} \mathsf{skip}, s'', ok$ and $\mathsf{C}_2, s'' \xrightarrow{k} -, s', \epsilon$, as required.

In case (2), as $\mathsf{C}' = \mathsf{C}_1'; \mathsf{C}_2$ and $\mathsf{C}', s'' \xrightarrow{k} -, s', \epsilon$, from the inductive hypothesis we know either a) ϵ=er and $\mathsf{C}_1', s'' \xrightarrow{k} -, s', \epsilon$; or b) there exist $i, j \leq k, s_2$ such that $\mathsf{C}_1', s'' \xrightarrow{i} -, s_2, ok$ and $\mathsf{C}_2, s_2 \xrightarrow{j} -, s', \epsilon$.

In case (2.a), as ϵ=er, $\mathsf{C}_1, s \rightarrow \mathsf{C}_1', s'', ok$ and $\mathsf{C}_1', s'' \xrightarrow{k} -, s', \epsilon$, from the definition of $\xrightarrow{n}$ we have $\mathsf{C}_1, s \xrightarrow{n} -, s', er$, as required.

In case (2.b), as $i \leq k$, $\mathsf{C}_1, s \rightarrow \mathsf{C}_1', s'', ok$ and $\mathsf{C}_1', s'' \xrightarrow{i} -, s_2, ok$, from the definition of $\xrightarrow{i+1}$ we know there exists m=i+1 $\leq k$+1 $= n$ such that $\mathsf{C}_1, s \xrightarrow{m} -, s_2, ok$. Moreover, we also know there exists $j \leq k < n$ such that $\mathsf{C}_2, s_2 \xrightarrow{j} -, s', \epsilon$. That is, we know there exist $m, j \leq n$ such that $\mathsf{C}_1, s \xrightarrow{m} -, s_2, ok$ and $\mathsf{C}_2, s_2 \xrightarrow{j} -, s', \epsilon$, as required. □

Lemma 5. *For all $n, \mathsf{C}, s, s', \epsilon$, if $\mathsf{C}^\star; \mathsf{C}, s \xrightarrow{n} -, s', \epsilon$ then there exists m such that $\mathsf{C}; \mathsf{C}^\star, s \xrightarrow{m} -, s', \epsilon$.*

Proof. By strong induction on n.

Base case n=0
Pick arbitrary $\mathsf{C}, s, s', \epsilon$ such that $\mathsf{C}^\star; \mathsf{C}, s \xrightarrow{0} -, s', \epsilon$. This case does not arise as $\mathsf{C}^\star; \mathsf{C}, s \xrightarrow{0} -, s', \epsilon$ would imply $\mathsf{C}^\star; \mathsf{C} = \mathsf{skip}$, leading to a contradiction.

Base case n=1
Pick arbitrary $\mathsf{C}, s, s', \epsilon$ such that $\mathsf{C}^\star; \mathsf{C}, s \xrightarrow{1} -, s', \epsilon$. This case also does not arise. Specifically, from $\mathsf{C}^\star; \mathsf{C}, s \xrightarrow{1} -, s', \epsilon$ we know that $\epsilon = er$ and $\mathsf{C}^\star; \mathsf{C}, s \rightarrow -, s', \epsilon$, i.e. $\mathsf{C}^\star; \mathsf{C}, s \rightarrow -, s', er$. By inversion, the only transition that could apply is that of S-Seq1, meaning that there exists C' such that $\mathsf{C}^\star, s \rightarrow -, s', er$. However, by inversion, no transition in Fig. 8 allows us to take an erroneous transition of the form $\mathsf{C}^\star, s \rightarrow -, s', er$.

Inductive case n=k+1
Pick arbitrary $\mathsf{C}, s, s', \epsilon, \mathsf{C}'$ such that $\mathsf{C}^\star; \mathsf{C}, s \xrightarrow{n} \mathsf{C}', s', \epsilon$. From $\mathsf{C}^\star; \mathsf{C}, s \xrightarrow{n} -, s', \epsilon$ we know there exists s'', C' such that $\mathsf{C}^\star; \mathsf{C}, s \rightarrow \mathsf{C}', s'', ok$ and $\mathsf{C}', s'' \xrightarrow{k} -, s', \epsilon$. From $\mathsf{C}^\star; \mathsf{C}, s \rightarrow \mathsf{C}', s'', ok$ and by

inversion through S-Seq1 we know there exists C'_1 such that $\mathrm{C}^\star, s \to \mathrm{C}'_1, s'', \mathit{ok}$ and $\mathrm{C}' = \mathrm{C}'_1; \mathrm{C}$. By inversion on $\mathrm{C}^\star, s \to \mathrm{C}'_1, s'', \mathit{ok}$ there are two cases to consider: 1) Through S-Loop0 we have $\mathrm{C}'_1 = \mathrm{skip}$ and $s'' = s$, i.e. $\mathrm{C}^\star, s \to \mathrm{skip}, s, \mathit{ok}$; or 2) Through S-Loop we have $\mathrm{C}'_1 = \mathrm{C}; \mathrm{C}^\star$ and $s'' = s$, i.e. $\mathrm{C}^\star, s \to \mathrm{C}; \mathrm{C}^\star, s, \mathit{ok}$.

In case (1), from $\mathrm{C}', s'' \xrightarrow{k} -, s', \epsilon$, $\mathrm{C}' = \mathrm{C}'_1; \mathrm{C}$ and the assumption of the case we have $\mathrm{skip}; \mathrm{C}, s \xrightarrow{k} -, s', \epsilon$. As such, from the definition of $\xrightarrow{k}$ and inversion we know the cases where k=0 or k=1 $\land\, \epsilon = \mathit{er}$ do not arise, and that $\mathrm{skip}; \mathrm{C}, s \to \mathrm{C}, s, \mathit{ok}$ and $\mathrm{C}, s \xrightarrow{k-1} -, s', \epsilon$. There are now to subcases to consider: a) ϵ=ok; or b) ϵ=er.

In case (1.a), we have $\mathrm{C}, s \xrightarrow{k-1} -, s', \mathit{ok}$. Moreover, from S-Loop0 we have $\mathrm{C}^\star, s' \to \mathrm{skip}, s', \mathit{ok}$, and thus since by definition we also have $\mathrm{skip}, s' \xrightarrow{0} \mathrm{skip}, s', \mathit{ok}$, by definition we have $\mathrm{C}^\star, s' \xrightarrow{1} \mathrm{skip}, s', \mathit{ok}$. As such, from $\mathrm{C}, s \xrightarrow{k-1} -, s', \mathit{ok}$, $\mathrm{C}^\star, s' \xrightarrow{1} \mathrm{skip}, s', \mathit{ok}$ and Lemma 2 we know there exists m such that $\mathrm{C}; \mathrm{C}^\star, s \xrightarrow{m} -, s', \mathit{ok}$, i.e. $\mathrm{C}; \mathrm{C}^\star, s \xrightarrow{m} -, s', \epsilon$, as required.

In case (1.b), we have $\mathrm{C}, s \xrightarrow{k-1} -, s', \mathit{er}$. As such, from Lemma 3 we have $\mathrm{C}; \mathrm{C}^\star, s \xrightarrow{k-1} -, s', \mathit{er}$, i.e. there exists m such that $\mathrm{C}; \mathrm{C}^\star, s \xrightarrow{m} -, s', \epsilon$, as required.

In case (2), as $\mathrm{C}'_1 = \mathrm{C}; \mathrm{C}^\star$, $s'' = s$, $\mathrm{C}' = \mathrm{C}'_1; \mathrm{C}$ and $\mathrm{C}', s'' \xrightarrow{k} -, s', \epsilon$, we know $\mathrm{C}; \mathrm{C}^\star; \mathrm{C}, s \xrightarrow{k} -, s', \epsilon$. From Lemma 4 we then know there are two cases to consider: a) ϵ=er and $\mathrm{C}, s \xrightarrow{k} -, s', \epsilon$; or b) there exists $i, j \leq n$, s_1 such that $\mathrm{C}, s \xrightarrow{i} -, s_1, \mathit{ok}$ and $\mathrm{C}^\star; \mathrm{C}, s_1 \xrightarrow{j} -, s', \epsilon$.

In case (2.a), as ϵ=er and $\mathrm{C}, s \xrightarrow{k} -, s', \epsilon$, from Lemma 3 we have $\mathrm{C}; \mathrm{C}^\star, s \xrightarrow{k} -, s', \epsilon$, as required.

In case (2.b), as $j \leq k$ and $\mathrm{C}^\star; \mathrm{C}, s_1 \xrightarrow{j} -, s', \epsilon$, from the inductive hypothesis we know there exists a such that $\mathrm{C}; \mathrm{C}^\star, s_1 \xrightarrow{a} -, s', \epsilon$. Moreover, from S-Loop we have $\mathrm{C}^\star, s_1 \to \mathrm{C}; \mathrm{C}^\star, s_1, \mathit{ok}$. As such, from $\mathrm{C}; \mathrm{C}^\star, s_1 \xrightarrow{a} -, s', \epsilon$ and the definition of $\xrightarrow{a+1}$ we have $\mathrm{C}^\star, s_1 \xrightarrow{a+1} -, s', \epsilon$. Consequently, since from the assumption of case (2.b) we also have $\mathrm{C}, s \xrightarrow{i} -, s_1, \mathit{ok}$, from Lemma 2 we know there exists m such that $\mathrm{C}; \mathrm{C}^\star, s \xrightarrow{m} -, s', \epsilon$, as required. □

Lemma 6. *For all* p, C, *if* $\forall n \in \mathbb{N}.\ \models_{\mathrm{B}} \big[p(n)\big]\ \mathrm{C}\ \big[\mathit{ok}\colon p(n{+}1)\big]$, *then* $\forall k, i \in \mathbb{N}.\ \models_{\mathrm{B}} \big[p(i)\big]\ \mathrm{C}^\star\ \big[\mathit{ok}\colon p(i{+}k)\big]$.

Proof. Pick arbitrary p, C such that $\forall n \in \mathbb{N}.\ \models_{\mathrm{B}} \big[p(n)\big]\ \mathrm{C}\ \big[\mathit{ok}\colon p(n{+}1)\big]$. We proceed by induction on k.

Base case k=0

Pick an arbitrary $i \in \mathbb{N}$. We are then required to show $\models_{\mathrm{B}} \big[p(i)\big]\ \mathrm{C}^\star\ \big[\mathit{ok}\colon p(i)\big]$. Pick an arbitrary $s \in p(i)$. From S-Loop0 we have $\mathrm{C}^\star, s \to \mathrm{skip}, s, \mathit{ok}$. As such, as we have $\mathrm{skip}, s \xrightarrow{0} \mathrm{skip}, s, \mathit{ok}$ (from the definition of $\xrightarrow{0}$), by definition we have $\mathrm{C}^\star, s \xrightarrow{1} \mathrm{skip}, s, \mathit{ok}$. Consequently, we have $s \in p(i)$ and $\mathrm{C}^\star, s \xrightarrow{1} \mathrm{skip}, s, \mathit{ok}$, as required.

Inductive case k=j+1

Pick an arbitrary $i \in \mathbb{N}$ and $s \in p(i)$. From $\forall n \in \mathbb{N}.\ \models_{\mathrm{B}} \big[p(n)\big]\ \mathrm{C}\ \big[\mathit{ok}\colon p(n{+}1)\big]$ we know $\models_{\mathrm{B}} \big[p(i)\big]\ \mathrm{C}\ \big[\mathit{ok}\colon p(i{+}1)\big]$ holds, and thus since $s \in p(i)$, from the definition of $\models_{\mathrm{B}}$ we then know there exists $s'' \in p(i{+}1)$, m such that $\mathrm{C}, s \xrightarrow{m} -, s'', \mathit{ok}$.

On the other hand, from the inductive hypothesis we know $\forall a \in \mathbb{N}.\ \models_{\mathrm{B}} [p(a)]\ \mathrm{C}^\star\ [ok\colon p(a{+}j)]$. As such, from the inductive hypothesis we have $\models_{\mathrm{B}} [p(i{+}1)]\ \mathrm{C}^\star\ [ok\colon p(i{+}1{+}j)]$, i.e. $\models_{\mathrm{B}} [p(i{+}1)]\ \mathrm{C}^\star\ [ok\colon p(i{+}k)]$. Consequently, since $s'' \in p(i{+}1)$, from the definition of $\models_{\mathrm{B}}$ we know there exists $s' \in p(i{+}k), b$ such that $\mathrm{C}^\star, s'', \xrightarrow{b} -, s', ok$. Therefore, from Lemma 2, $\mathrm{C}, s \xrightarrow{m} -, s'', ok$ and $\mathrm{C}^\star, s'', \xrightarrow{b} -, s', ok$ we know there exists c such that $\mathrm{C}; \mathrm{C}^\star, s, \xrightarrow{c} -, s', ok$.

Furthermore, from S-Loop we simply have $\mathrm{C}^\star, s, \rightarrow\ \mathrm{C}; \mathrm{C}^\star, s, ok$. As such, since we also have $\mathrm{C}; \mathrm{C}^\star, s, \xrightarrow{c} -, s', ok$, from the definition of $\xrightarrow{c+1}$ we have $\mathrm{C}^\star, s, \xrightarrow{c+1} -, s', ok$. That is, we have $s' \in p(i{+}k)$ such that $\mathrm{C}^\star, s, \xrightarrow{c+1} -, s', ok$, as required. □

Lemma 7 (BUA soundness). *For all p, C, q, ϵ, if $\vdash_{\mathrm{B}} [p]\ \mathrm{C}\ [\epsilon : q]$ can be proven using the proof rules in Fig. 2, then $\models_{\mathrm{B}} [p]\ \mathrm{C}\ [\epsilon : q]$ holds.*

Proof. By induction on the structure of rules in Fig. 2.

Case Skip
Pick arbitrary p such that $\vdash_{\mathrm{B}} [p]\ \mathrm{skip}\ [ok\colon p]$. Pick an arbitrary $s \in p$. From the semantics of skip we then have $\mathrm{skip}, s \xrightarrow{0} \mathrm{skip}, s, ok$ and $s \in p$, as required.

Case Assign
Pick arbitrary p such that $\vdash_{\mathrm{B}} [p]\ x := e\ [ok\colon \exists y.\ p[y/x] \land x = e[y/x]]$. Pick an arbitrary $s \in p$. Let $s(x) = v_x$, $s(e) = v_e$ and $s' = s[x \mapsto v_e]$. From S-Assign we then have $x := e, s \rightarrow \mathrm{skip}, s', ok$. As such, since we also have $\mathrm{skip}, s' \xrightarrow{0} \mathrm{skip}, s', ok$, by definition we have $x := e, s \xrightarrow{1} \mathrm{skip}, s', ok$.

As $s(x) = v_x$ and $s(e) = v_e$, by definition we have $s(e[v_x/x]) = v_e$ and $s'(e[v_x/x]) = v_e$. As $s \in p$ and $s(x) = v_x$, we also have $s \in p[v_x/x]$. Thus, as $s' = s[x \mapsto v_e]$ and $s \in p[v_x/x]$, we also have $s' \in p[v_x/x]$. Similarly, as $s'(e[v_x/x]) = v_e$ and $s' = s[x \mapsto v_e]$ (i.e. $s'(x) = v_e$), we have $s' \in x = e[v_x/x]$. That is, we have $s' \in p[v_x/x] \land x = e[v_x/x]$. Let $s'' = s'[y \mapsto v_x]$. Consequently, as $s' \in p[v_x/x] \land x = e[v_x/x]$, we also have $s'' \in p[y/x] \land x = e[y/x]$. As such, since $s'' \in p[y/x] \land x = e[y/x]$ and $s'' = s'[y \mapsto v_x]$, by definition we have $s' \in \exists y.\ p[y/x] \land x = e[y/x]$. Therefore, we have $x := e, s \xrightarrow{1} \mathrm{skip}, s', ok$ and $s' \in \exists y.\ p[y/x] \land x = e[y/x]$, as required.

Case Assume
Pick arbitrary p, B such that $\vdash_{\mathrm{B}} [p \land B]\ \mathrm{assume}(B)\ [ok\colon p \land B]$. Pick an arbitrary $s \in p \land B$. By definition we then know $s(B) = \mathrm{true}$. From S-Assume we then have $\mathrm{assume}(B), s \rightarrow \mathrm{skip}, s, ok$. As such, since we also have $\mathrm{skip}, s \xrightarrow{0} \mathrm{skip}, s, ok$, by definition we have $\mathrm{assume}(B), s \xrightarrow{1} \mathrm{skip}, s, ok$. Consequently, we have $s \in p \land B$ and $\mathrm{assume}(B), s \xrightarrow{1} \mathrm{skip}, s, ok$, as required.

Case Error
Pick arbitrary p such that $\vdash_{\mathrm{B}} [p]\ \mathrm{error}\ [er\colon p]$. Pick an arbitrary $s \in p$. From S-Error we then have $\mathrm{error}, s \rightarrow \mathrm{skip}, s, er$. As such, by definition we have $\mathrm{error}, s \xrightarrow{1} \mathrm{skip}, s, er$. Consequently, we have $s \in p$ and $\mathrm{error}, s \xrightarrow{1} \mathrm{skip}, s, er$, as required.

Case Seq
Pick arbitrary $p, q, r, \mathrm{C}_1, \mathrm{C}_2, \epsilon$ such that $\vdash_{\mathrm{B}} [p]\ \mathrm{C}_1\ [ok\colon r]$ and $\vdash_{\mathrm{B}} [r]\ \mathrm{C}_2\ [\epsilon : q]$. Pick an arbitrary $s \in p$. From $\vdash_{\mathrm{B}} [p]\ \mathrm{C}_1\ [ok\colon r]$ and the inductive hypothesis we then know there exists $s'' \in r, i$ such that $\mathrm{C}_1, s \xrightarrow{i} -, s'', ok$. Moreover, as $s'' \in r, i$, from $\vdash_{\mathrm{B}} [r]\ \mathrm{C}_2\ [\epsilon : q]$ and the inductive hypothesis

we know there exists $s' \in q, j$ such that $\mathsf{C}_2, s'' \xrightarrow{j} -, s', \epsilon$. As $\mathsf{C}_1, s \xrightarrow{i} -, s'', ok$ and $\mathsf{C}_2, s'' \xrightarrow{j} -, s', \epsilon$, from Lemma 2 we know there exists n such that $\mathsf{C}_1; \mathsf{C}_2, s \xrightarrow{n} -, s', \epsilon$. That is, there exists $s' \in q, n$ such that $\mathsf{C}_1; \mathsf{C}_2, s \xrightarrow{n} -, s', \epsilon$, as required.

Case SeqEr
Pick arbitrary $p, q, \mathsf{C}_1, \mathsf{C}_2$ such that $\vdash_\mathsf{B} [p]\ \mathsf{C}_1; \mathsf{C}_2\ [er\colon q]$. Pick an arbitrary $s \in p$. From the $\vdash_\mathsf{B} [p]$ $\mathsf{C}_1\ [er\colon q]$ premise and the inductive hypothesis we then know there exists $s' \in q, i$ such that $\mathsf{C}_1, s \xrightarrow{i} -, s', er$. As such, from Lemma 3 we know $\mathsf{C}_1; \mathsf{C}_2, s \xrightarrow{i} -, s', er$. That is, there exists $s' \in q$ such that $\mathsf{C}_1; \mathsf{C}_2, s \xrightarrow{i} -, s', er$, as required.

Case Choice
Pick arbitrary $p, q, \mathsf{C}_1, \mathsf{C}_2, \epsilon$ and $i \in \{1, 2\}$ such that $\vdash_\mathsf{B} [p]\ \mathsf{C}_1 + \mathsf{C}_2\ [\epsilon : q]$. Pick an arbitrary $s \in p$. From the $\vdash_\mathsf{B} [p]\ \mathsf{C}_i\ [\epsilon : q]$ premise and the inductive hypothesis we then know there exists $s' \in q, j$ such that $\mathsf{C}_i, s \xrightarrow{j} -, s', \epsilon$. Moreover, from S-Choice we have $\mathsf{C}_1 + \mathsf{C}_2, s \rightarrow \mathsf{C}_i, s, ok$. As such, from the definition of $\xrightarrow{j+1}$ we have $\mathsf{C}_1 + \mathsf{C}_2, s \xrightarrow{j+1} -, s', \epsilon$. That is, there exists $s' \in q$ such that $\mathsf{C}_1 + \mathsf{C}_2, s \xrightarrow{j+1} -, s', \epsilon$, as required.

Case Loop0
Pick arbitrary p, C such that $\vdash_\mathsf{B} \big[p\big]\ \mathsf{C}^\star\ \big[ok\colon p\big]$. Pick an arbitrary $s \in p$. From S-Loop0 we have $\mathsf{C}^\star, s \rightarrow \mathsf{skip}, s, ok$. As such, as we have $\mathsf{skip}, s \xrightarrow{0} \mathsf{skip}, s, ok$ (from the definition of $\xrightarrow{0}$), by definition we have $\mathsf{C}^\star, s \xrightarrow{1} \mathsf{skip}, s, ok$. Consequently, we have $s \in p$ and $\mathsf{C}^\star, s \xrightarrow{1} \mathsf{skip}, s, ok$, as required.

Case Loop
Pick arbitrary p, C, q such that $\vdash_\mathsf{B} [p]\ \mathsf{C}^\star\ [\epsilon : q]$. Pick an arbitrary $s \in p$. From the $\vdash_\mathsf{B} [p]\ \mathsf{C}^\star; \mathsf{C}\ [\epsilon : q]$ premise and the inductive hypothesis we know there exists $s' \in q, j$ such that $\mathsf{C}^\star; \mathsf{C}, s \xrightarrow{j} -, s', \epsilon$. From Lemma 5 we then know there exists i such that $\mathsf{C}; \mathsf{C}^\star, s \xrightarrow{i} -, s', \epsilon$. From S-Loop we have $\mathsf{C}^\star, s \rightarrow \mathsf{C}; \mathsf{C}^\star, s, ok$. As such, from the definition of $\xrightarrow{i+1}$ we have $\mathsf{C}^\star, s \xrightarrow{i+1} -, s', \epsilon$. Consequently, we have $s \in p$ and $\mathsf{C}^\star, s \xrightarrow{i+1} -, s', \epsilon$, as required.

Case Loop-Subvariant
Pick arbitrary p, C, k such that $\vdash_\mathsf{B} \big[p(0)\big]\ \mathsf{C}^\star\ \big[ok\colon p(k)\big]$. From the $\forall n \in \mathbb{N}.\ \vdash_\mathsf{B} \big[p(n)\big]\ \mathsf{C}\ \big[ok\colon p(n{+}1)\big]$ premise and the inductive hypothesis we have $\forall n \in \mathbb{N}.\ \models_\mathsf{B} \big[p(n)\big]\ \mathsf{C}\ \big[ok\colon p(n{+}1)\big]$. Consequently, from Lemma 6 we have $\models_\mathsf{B} \big[p(0)\big]\ \mathsf{C}^\star\ \big[ok\colon p(k)\big]$, as required.

Case Local
Pick arbitrary $p, \mathsf{C}, q, \epsilon$ such that $\vdash_\mathsf{B} [\exists x.\ p]\ \mathsf{local}\ x\ \mathsf{in}\ \mathsf{C}\ [\epsilon : \exists x.\ q]$. Pick an arbitrary $s \in \exists x.\ p$; i.e. there exists v, s_p such that $s_p = s[x \mapsto v]$ and $s_p \in p$. From the $\vdash_\mathsf{B} [p]\ \mathsf{C}\ [\epsilon : q]$ premise and the inductive hypothesis we know there exists $s_q \in q$ and n such that $\mathsf{C}, s_p \xrightarrow{n} -, s_q, \epsilon$. From S-Local we have $\mathsf{local}\ x\ \mathsf{in}\ \mathsf{C}, s \rightarrow \mathsf{C}; \mathsf{end}(x, s(x)), s_p$. There are now two cases to consider: 1) $\epsilon{=}ok$; or 2) $\epsilon{=}er$.

In case (1), let $s'' = s_q[x \mapsto s(x)]$. From S-LocalEnd we then have $\mathsf{end}(x, s(x)), s_q \rightarrow \mathsf{skip}, s''$. From the definition of $\xrightarrow{0}$ we have $\mathsf{skip}, s'' \xrightarrow{0} \mathsf{skip}, s'', ok$, and thus since we have $\mathsf{end}(x, s(x)), s_q \rightarrow \mathsf{skip}, s''$, from the definition of $\xrightarrow{1}$ we have $\mathsf{end}(x, s(x)), s_q \xrightarrow{1} \mathsf{skip}, s''$. Consequently, since we also have $C, s_p \xrightarrow{n} -, s_q, \epsilon$, from Lemma 2 we know there exists m such that $C; \mathsf{end}(x, s(x)), s_p \xrightarrow{m}$ skip, s'', ok. On the other hand, since we have $\mathsf{local}\ x\ \mathsf{in}\ C, s \rightarrow C; \mathsf{end}(x, s(x)), s_p$, by definition of $\xrightarrow{m+1}$ we also have $\mathsf{local}\ x\ \mathsf{in}\ C, s \xrightarrow{m+1} \mathsf{skip}, s'', ok$. Finally, as $s_q \in q$ and $s'' = s_q[x \mapsto s(x)]$, by definition we also have $s'' \in \exists x.\ q$, as required.

In case (2), from $C, s_p \xrightarrow{n} -, s_q, \epsilon$ and Lemma 3 we have $C; \mathsf{end}(x, s(x)), s_p \xrightarrow{n} -, s_q, \epsilon$. On the other hand, since we have $\mathsf{local}\ x\ \mathsf{in}\ C, s \rightarrow C; \mathsf{end}(x, s(x)), s_p$, by definition of $\xrightarrow{n+1}$ we also have $\mathsf{local}\ x\ \mathsf{in}\ C, s \xrightarrow{n+1} -, s_q, \epsilon$. Finally, as $s_q \in q$, by definition we also have $s_q \in \exists x.\ q$, as required.

Case Subst
Pick arbitrary p, C, q, y such that $y \notin \mathsf{fv}(p, C, q)$ and $(\vdash_B [p]\ C\ [\epsilon : q])[y/x]$, i.e. $\vdash_B [p[y/x]]\ C[y/x]$ $[\epsilon : q[y/x]]$. Pick an arbitrary $s \in p[y/x]$ and let $s_p = s[x \mapsto s(y)]$. We then have $s_p \in p$ and thus from the $\vdash_B [p]\ C\ [\epsilon : q]$ premise and the inductive hypothesis we know there exists $s_q \in q, n$ such that $C, s_p \xrightarrow{n} -, s_q \epsilon$. Let $s' = s_q[y \mapsto x]$; as $s_q \in q$, we then have $s' \in q[y/x]$. As such, from the semantics we also have $C[y/x], s \xrightarrow{n} -, s', \epsilon$, as required.

Case Disj
Pick arbitrary p_1, p_2, q_1, q_2, C such that $\vdash_B [p_1 \vee p_2]\ C\ [\epsilon : q_1 \vee q_2]$. Pick an arbitrary $s \in p_1 \vee p_2$. There are then two cases to consider: 1) $s \in p_1$; or 2) $s \in p_2$.

In case (1), from the $\vdash_B [p_1]\ C\ [\epsilon : q_1]$ premise and the inductive hypothesis we know there exists $s' \in q_1, n$ such that $C, s \xrightarrow{n} -, s', \epsilon$. That is, there exists $s' \in q_1 \vee q_2$ and n such that $C, s \xrightarrow{n} -, s', \epsilon$, as required. The proof of case (2) is analogous and omitted.

Case Constancy
Pick arbitrary p, q, r, C such that $\vdash_B [p \wedge r]\ C\ [\epsilon : q \wedge r]$. Pick an arbitrary $s \in p \wedge r$. That is, $s \in p$ and $s \in r$. From the $\vdash_B [p]\ C\ [\epsilon : q]$ premise and the inductive hypothesis we know there exists $s' \in q, n$ such that $C, s \xrightarrow{n} -, s', \epsilon$. As such, from the $\mathsf{fv}(r) \cap \mathsf{mod}(C) = \emptyset$ premise, Prop. 12 and since $s \in r$, we know $s' \in r$. Therefore, we have $s' \in q$ and $s' \in r$ and thus $s' \in q \wedge r$. That is, there exists $s' \in q \wedge r$ and n such that $C, s \xrightarrow{n} -, s', \epsilon$, as required.

Case ConsF
Pick arbitrary p, q, C such that $\vdash_B [p]\ C\ [\epsilon : q]$. Pick an arbitrary $s \in p$. From the $p \subseteq p'$ premise we then have $s \in p'$. Moreover, from the $\vdash_B [p']\ C\ [\epsilon : q']$ and the inductive hypothesis we know there exists $s' \in q'$ and n such that $C, s \xrightarrow{n} -, s', \epsilon$. As $q' \subseteq q$ and $s' \in q'$, we also have $s' \in q$. That is, there exists $s' \in q$ and n such that $C, s \xrightarrow{n} -, s', \epsilon$, as required.

Case DisjTrack
Pick arbitrary P_1, P_2, Q_1, Q_2, C such that $\vdash_B [P_1 \uplus P_2]\ C\ [\epsilon : Q_1 \uplus Q_2]$. Pick an arbitrary $i \in dom(P_1 \uplus P_2)$ and $s \in (P_1 \uplus P_2)(i)$. We then know that either $i \in dom(P_1)$ or $i \in dom(P_2)$. Without loss of generality, let us assume $i \in dom(P_1)$.

As $s \in (P_1 \uplus P_2)(i)$ and $i \in dom(P_1)$, we then have $s \in P_1(i)$. From the $\vdash_B [P_1]\ C\ [\epsilon : Q_1]$ premise, the definition of merged triples premise and the inductive hypothesis we know there exists $s' \in Q_1(i), n$ such that $C, s \xrightarrow{n} -, s', \epsilon$. That is, there exists $s' \in (Q_1 \uplus Q_2)(i)$ and n such that $C, s \xrightarrow{n} -, s', \epsilon$, as required.

Case Cons

Pick arbitrary P, Q, C, I such that $\vdash_{\mathsf{B}} [P \downarrow I]\ \mathsf{C}\ [\epsilon : Q \downarrow I]$. Pick an arbitrary $i \in dom(P \downarrow I)$; that is, from the $I \subseteq dom(P)$ we know $i \in dom(P) \cap I$, i.e. $i \in dom(P)$ and $i \in I$. Pick an arbitrary $s \in P(i)$. From the $\vdash_{\mathsf{B}} [P]\ \mathsf{C}\ [\epsilon : Q]$ premise the definition of merged triples and the inductive hypothesis we know there exists $s' \in Q(i)$ and n such that $\mathsf{C}, s \xrightarrow{n} -, s', \epsilon$. As $i \in I$ and $i \in dom(Q)$, we know $i \in dom(Q \downarrow I)$. That is, there exists $i \in dom(Q \downarrow I)$, $s' \in (Q \downarrow I)(i)$ and n such that $\mathsf{C}, s \xrightarrow{n} -, s', \epsilon$, as required. □

Lemma 8 (FUA soundness). *For all p, C, q, ϵ, if $\vdash_{\mathsf{F}} [p]\ \mathsf{C}\ [\epsilon : q]$ can be proven using the proof rules in Fig. 2, then $\models_{\mathsf{F}} [p]\ \mathsf{C}\ [\epsilon : q]$ holds.*

Proof. By induction on the structure of rules in Fig. 2.

Cases Skip, Assign, Error, Seq, SeqEr, Choice, Loop0, Loop, Loop-Subvariant, Disj, Constancy, ConsB, Subst

The proof of these cases is as given by O'Hearn [23].

Case Local

Pick arbitrary p, C, q, ϵ such that $\vdash_{\mathsf{F}} [\exists x.\ p]\ \mathsf{local}\ x\ \mathsf{in}\ \mathsf{C}\ [\epsilon : \exists x.\ q]$. Pick an arbitrary $s' \in \exists x.\ q$; i.e. there exists v, s_q such that $s_q = s'[x \mapsto v]$ and $s_q \in q$. From the $\vdash_{\mathsf{F}} [p]\ \mathsf{C}\ [\epsilon : q]$ premise and the inductive hypothesis we know there exists $s_p \in p$ and n such that $\mathsf{C}, s_p \xrightarrow{n} -, s_q, \epsilon$. From S-Local we have $\mathsf{local}\ x\ \mathsf{in}\ \mathsf{C}, s_p \to \mathsf{C}; \mathsf{end}(x, s_p(x)), s_p$. There are two cases to consider: 1) ϵ=*ok*; or 2) ϵ=*er*.

In case (1), let $s'' = s_q[x \mapsto s_p(x)]$. From S-LocalEnd we then have $\mathsf{end}(x, s_p(x)), s_q \to \mathsf{skip}, s''$. From the definition of $\xrightarrow{0}$ we have $\mathsf{skip}, s'' \xrightarrow{0} \mathsf{skip}, s'', ok$, and thus since we have $\mathsf{end}(x, s_p(x)), s_q \to \mathsf{skip}, s''$, from the definition of $\xrightarrow{1}$ we have $\mathsf{end}(x, s_p(x)), s_q \xrightarrow{1} \mathsf{skip}, s''$. Consequently, since we also have $\mathsf{C}, s_p \xrightarrow{n} -, s_q, \epsilon$, from Lemma 2 we know there exists m such that $\mathsf{C}; \mathsf{end}(x, s_p(x)), s_p \xrightarrow{m} \mathsf{skip}, s'', ok$. On the other hand, since we have $\mathsf{local}\ x\ \mathsf{in}\ \mathsf{C}, s_p \to \mathsf{C}; \mathsf{end}(x, s_p(x)), s_p$, by definition of $\xrightarrow{m+1}$ we also have $\mathsf{local}\ x\ \mathsf{in}\ \mathsf{C}, s_p \xrightarrow{m+1} \mathsf{skip}, s'', ok$. Finally, as $s_p \in p$, by definition we also have $s_p \in \exists x.\ p$, as required.

In case (2), from $\mathsf{C}, s_p \xrightarrow{n} -, s_q, \epsilon$ and Lemma 3 we have $\mathsf{C}; \mathsf{end}(x, s_p(x)), s_p \xrightarrow{n} -, s_q, \epsilon$. On the other hand, since we have $\mathsf{local}\ x\ \mathsf{in}\ \mathsf{C}, s_p \to \mathsf{C}; \mathsf{end}(x, s_p(x)), s_p$, by definition of $\xrightarrow{n+1}$ we also have $\mathsf{local}\ x\ \mathsf{in}\ \mathsf{C}, s_p \xrightarrow{n+1} -, s_q, \epsilon$. Finally, as $s_p \in p$, by definition we also have $s_p \in \exists x.\ p$, as required.

Case Assume

Pick arbitrary p, B such that $\vdash_{\mathsf{F}} \left[p \land B\right]\ \mathsf{assume}(B)\ \left[ok \colon p \land B\right]$. Pick an arbitrary $s \in p \land B$. By definition we then know $s(B) = \mathsf{true}$. From S-Assume we then have $\mathsf{assume}(B), s \to \mathsf{skip}, s, ok$. As such, since we also have $\mathsf{skip}, s \xrightarrow{0} \mathsf{skip}, s, ok$, by definition we have $\mathsf{assume}(B), s \xrightarrow{1} \mathsf{skip}, s, ok$. Consequently, we have $s \in p \land B$ and $\mathsf{assume}(B), s \xrightarrow{1} \mathsf{skip}, s, ok$, as required.

Case DisjTrack

Pick arbitrary $P_1, P_2, Q_1, Q_2, \mathsf{C}$ such that $\vdash_{\mathsf{F}} [P_1 \uplus P_2]\ \mathsf{C}\ [\epsilon : Q_1 \uplus Q_2]$. Pick an arbitrary $i \in dom(Q_1 \uplus Q_2)$ and $s' \in (Q_1 \uplus Q_2)(i)$. We then know that either $i \in dom(Q_1)$ or $i \in dom(Q_2)$. Without loss of generality, let us assume $i \in dom(Q_1)$.

As $s' \in (Q_1 \uplus Q_2)(i)$ and $i \in dom(Q_1)$, we then have $s' \in Q_1(i)$. From the $\vdash_{\mathsf{F}} [P_1]\ \mathsf{C}\ [\epsilon : Q_1]$ premise, the definition of merged triples and the inductive hypothesis we know there exists

$s \in P_1(i)$, n such that $\mathsf{C}, s \xrightarrow{n} -, s', \epsilon$. That is, there exists $s \in (P_1 \uplus P_2)(i)$ and n such that $\mathsf{C}, s \xrightarrow{n} -, s', \epsilon$, as required.

Case Cons

Pick arbitrary P, Q, C, I such that $\vdash_{\mathsf{B}} [P \downarrow I]\ \mathsf{C}\ [\epsilon : Q \downarrow I]$. Pick an arbitrary $i \in dom(Q \downarrow I)$; that is, from the $I \subseteq dom(P)$ we know $i \in dom(Q) \cap I$, i.e. $i \in dom(Q)$ and $i \in I$. Pick an arbitrary $s' \in Q(i)$. From the $\vdash_{\mathsf{F}} [P]\ \mathsf{C}\ [\epsilon : Q]$ premise the definition of merged triples and the inductive hypothesis we know there exists $s \in P(i)$ and n such that $\mathsf{C}, s \xrightarrow{n} -, s', \epsilon$. As $i \in I$ and $i \in dom(P)$, we know $i \in dom(P \downarrow I)$. That is, there exists $i \in dom(P \downarrow I)$, $s \in (P \downarrow I)(i)$ and n such that $\mathsf{C}, s \xrightarrow{n} -, s', \epsilon$, as required. □

Theorem 13 (Soundness). *For all* $p, \mathsf{C}, q, \epsilon$, *if* $\vdash_{\dagger} [p]\ \mathsf{C}\ [\epsilon : q]$ *can be proven using the proof rules in Fig. 2, then* $\models_{\dagger} [p]\ \mathsf{C}\ [\epsilon : q]$ *holds.*

Proof. Follows immediately from Lemma 7 and Lemma 8. □

B.3 Soundness of Divergence Rules

In what follows, we write $\mathsf{C}, s \rightsquigarrow^{+} \mathsf{C}', s', \epsilon$ for $\exists n.\ \mathsf{C}, s \rightsquigarrow^{n} \mathsf{C}', s', \epsilon$.

Lemma 9. *For all* $\mathsf{C}, s, \mathsf{C}', s', \epsilon, n$, *if* $n > 0$ *and* $\mathsf{C}, s \xrightarrow{n} \mathsf{C}', s', \epsilon$, *then* $\mathsf{C}, s \rightsquigarrow^{n} \mathsf{C}', s', \epsilon$.

Proof. By induction on n.

Base case $n = 1$

Pick arbitrary $\mathsf{C}, \mathsf{C}', s, \mathsf{C}', s', \epsilon$ such that $\mathsf{C}, s \xrightarrow{1} \mathsf{C}', s', \epsilon$. From the definition of $\xrightarrow{1}$ there are then two cases to consider: 1) $\epsilon = er$ and $\mathsf{C}, s \rightarrow \mathsf{C}', s', er$; or 2) $\epsilon = ok$, $\mathsf{C}' = \mathsf{skip}$ and $\mathsf{C}, s \rightarrow \mathsf{C}', s', ok$.

In case (1), from the definition of $\rightsquigarrow^{1}$ we also have $\mathsf{C}, s \rightsquigarrow^{1} \mathsf{C}', s', er$, as required. In case (2), from the definition of $\rightsquigarrow^{1}$ we also have $\mathsf{C}, s \rightsquigarrow^{1} \mathsf{C}', s', ok$, as required.

Inductive case $n = k{+}1$ **with** $k > 0$

Pick arbitrary $\mathsf{C}, \mathsf{C}', s, \mathsf{C}', s', \epsilon$ such that $\mathsf{C}, s \xrightarrow{n} \mathsf{C}', s', \epsilon$. From the definition of $\xrightarrow{n}$, we know there exists C'', s'' such that $\mathsf{C}, s \rightarrow \mathsf{C}'', s'', ok$ and $\mathsf{C}'', s'' \xrightarrow{k} \mathsf{C}', s', \epsilon$. From $\mathsf{C}'', s'' \xrightarrow{k} \mathsf{C}', s', \epsilon$ and the inductive hypothesis we have $\mathsf{C}'', s'' \rightsquigarrow^{k} \mathsf{C}', s', \epsilon$. As such, from $\mathsf{C}, s \rightarrow \mathsf{C}'', s'', ok$ and the definition of $\rightsquigarrow^{n}$ we have $\mathsf{C}, s \rightsquigarrow^{n} \mathsf{C}', s', \epsilon$, as required. □

Lemma 10. *For all* $n, \mathsf{C}_1, \mathsf{C}_2, \mathsf{C}_1', s, \mathsf{C}', s', \epsilon$, *if* $\mathsf{C}_1, s \rightsquigarrow^{n} \mathsf{C}_1', s', \epsilon$, *then* $\mathsf{C}_1; \mathsf{C}_2, s \rightsquigarrow^{n} \mathsf{C}_1'; \mathsf{C}_2, s', \epsilon$.

Proof. By induction on n.

Base case $n = 1$

Pick arbitrary $\mathsf{C}_1, \mathsf{C}_2, \mathsf{C}_1', s, \mathsf{C}', s', \epsilon$ such that $\mathsf{C}_1, s \rightsquigarrow^{1} \mathsf{C}_1', s', \epsilon$. From the definition of $\rightsquigarrow^{1}$ we then know $\mathsf{C}_1, s \rightarrow \mathsf{C}_1', s', \epsilon$. As such, from S-Seq1 we have $\mathsf{C}_1; \mathsf{C}_2, s \rightarrow \mathsf{C}_1'; \mathsf{C}_2, s', \epsilon$, and thus by definition of $\rightsquigarrow^{1}$ we have $\mathsf{C}_1; \mathsf{C}_2, s \rightsquigarrow^{1} \mathsf{C}_1'; \mathsf{C}_2, s', \epsilon$, as required.

Inductive case $n = k{+}1$

Pick arbitrary $\mathsf{C}_1, \mathsf{C}_2, \mathsf{C}_1', s, \mathsf{C}', s', \epsilon$ such that $\mathsf{C}_1, s \rightsquigarrow^{n} \mathsf{C}_1', s', \epsilon$. From the definition of $\rightsquigarrow^{n}$ we then know there exists C'', s'' such that $\mathsf{C}_1, s \rightarrow \mathsf{C}'', s'', ok$ and $\mathsf{C}'', s'' \rightsquigarrow^{k} \mathsf{C}_1', s', \epsilon$. From $\mathsf{C}_1, s \rightarrow \mathsf{C}'', s'', ok$ and S-Seq1 we have $\mathsf{C}_1; \mathsf{C}_2, s \rightarrow \mathsf{C}''; \mathsf{C}_2, s'', ok$. From $\mathsf{C}'', s'' \rightsquigarrow^{k} \mathsf{C}_1', s', \epsilon$ and the inductive hypothesis we have $\mathsf{C}''; \mathsf{C}_2, s'' \rightsquigarrow^{k} \mathsf{C}_1'; \mathsf{C}_2, s', \epsilon$. As such, since we have $\mathsf{C}_1; \mathsf{C}_2, s \rightarrow \mathsf{C}''; \mathsf{C}_2, s'', ok$

and $\mathrm{C}''; \mathrm{C}_2, s'' \rightsquigarrow^k \mathrm{C}'_1; \mathrm{C}_2, s', \epsilon$, from the definition of $\rightsquigarrow^n$ we have $\mathrm{C}_1; \mathrm{C}_2, s \rightsquigarrow^n \mathrm{C}'_1; \mathrm{C}_2, s', \epsilon$, as required. □

Lemma 11. *For all $s, s', s'', \mathrm{C}_1, \mathrm{C}_2, \mathrm{C}', i, j, \epsilon$, if $\mathrm{C}_1, s \xrightarrow{i} -, s'', \mathit{ok}$ and $\mathrm{C}_2, s'' \rightsquigarrow^j \mathrm{C}', s', \epsilon$, then there exists n such that $\mathrm{C}_1; \mathrm{C}_2, s \rightsquigarrow^n \mathrm{C}', s', \epsilon$.*

Proof. Pick arbitrary $s, s', s'', \mathrm{C}_1, \mathrm{C}_2, \mathrm{C}', \mathrm{C}'', i, j, \epsilon$, such that $\mathrm{C}_1, s \xrightarrow{i} \mathrm{C}'', s'', \mathit{ok}$ and $\mathrm{C}_2, s'' \rightsquigarrow^j \mathrm{C}', s', \epsilon$. We proceed by induction on i.

Case $i = 0$
From $\mathrm{C}_1, s \xrightarrow{0} \mathrm{C}'', s'', \mathit{ok}$ we know $\mathrm{C}_1 = \mathrm{C}'' = \mathrm{skip}$ and $s = s''$. As such, since $\mathrm{C}_1 = \mathrm{skip}$ and $s = s''$, from S-SeqSkip we have $\mathrm{C}_1; \mathrm{C}_2, s \rightarrow \mathrm{C}_2, s'', \mathit{ok}$. Consequently, from $\mathrm{C}_2, s'' \rightsquigarrow^j \mathrm{C}', s', \epsilon$ and the definition of $\rightsquigarrow^{j+1}$ we have $\mathrm{C}_1; \mathrm{C}_2, s \rightsquigarrow^{j+1} \mathrm{C}', s', \epsilon$, as required.

Case $i = k{+}1$
From the definition of $\mathrm{C}_1, s \xrightarrow{i} \mathrm{C}'', s'', \mathit{ok}$ we then know there exists C_3, s_3 such that $\mathrm{C}_1, s \rightarrow \mathrm{C}_3, s_3, \mathit{ok}$ and $\mathrm{C}_3, s_3 \xrightarrow{k} \mathrm{C}'', s'', \mathit{ok}$. As such, from the inductive hypothesis, $\mathrm{C}_3, s_3 \xrightarrow{k} \mathrm{C}'', s'', \mathit{ok}$ and $\mathrm{C}_2, s'' \rightsquigarrow^j \mathrm{C}', s', \epsilon$ we know there exists n such that $\mathrm{C}_3; \mathrm{C}_2, s_3 \rightsquigarrow^n \mathrm{C}', s', \epsilon$. Moreover, as $\mathrm{C}_1, s \rightarrow \mathrm{C}_3, s_3, \mathit{ok}$, from S-Seq1 we have $\mathrm{C}_1; \mathrm{C}_2, s \rightarrow \mathrm{C}_3; \mathrm{C}_2, s_3, \mathit{ok}$. Consequently, as $\mathrm{C}_1; \mathrm{C}_2, s \rightarrow \mathrm{C}_3; \mathrm{C}_2, s_3, \mathit{ok}$ and $\mathrm{C}_3; \mathrm{C}_2, s_3 \rightsquigarrow^n \mathrm{C}', s', \epsilon$, from the definition of $\rightsquigarrow^{n+1}$ we have $\mathrm{C}_1; \mathrm{C}_2, s \rightsquigarrow^{n+1} \mathrm{C}', s', \epsilon$, as required. □

Lemma 12. *For all $i, j, \mathrm{C}, \mathrm{C}', \mathrm{C}'', s, s', s'', \epsilon$, if $\mathrm{C}, s \rightsquigarrow^i \mathrm{C}'', s'', \mathit{ok}$ and $\mathrm{C}'', s'' \rightsquigarrow^j \mathrm{C}', s', \epsilon$, then $\mathrm{C}, s \rightsquigarrow^{i+j} \mathrm{C}', s', \epsilon$.*

Proof. By induction on i.

Base case $i{=}1$
Pick arbitrary $j, \mathrm{C}, \mathrm{C}', \mathrm{C}'', s, s', s'', \epsilon$ such that $\mathrm{C}, s \rightsquigarrow^1 \mathrm{C}'', s'', \mathit{ok}$ and $\mathrm{C}'', s'' \rightsquigarrow^j \mathrm{C}', s', \epsilon$. From $\mathrm{C}, s \rightsquigarrow^1 \mathrm{C}'', s'', \mathit{ok}$ we then know $\mathrm{C}, s \rightarrow \mathrm{C}'', s'', \mathit{ok}$, and thus from $\mathrm{C}'', s'' \rightsquigarrow^j \mathrm{C}', s', \epsilon$ and the definition of $\rightsquigarrow^{j+1}$ we have $\mathrm{C}, s \rightsquigarrow^{j+1} \mathrm{C}', s', \epsilon$, as required.

Inductive case $i{=}k{+}1$ and $k > 0$
Pick arbitrary $j, \mathrm{C}, \mathrm{C}', \mathrm{C}'', s, s', s'', \epsilon$ such that $\mathrm{C}, s \rightsquigarrow^i \mathrm{C}'', s'', \mathit{ok}$ and $\mathrm{C}'', s'' \rightsquigarrow^j \mathrm{C}', s', \epsilon$. From $\mathrm{C}, s \rightsquigarrow^i \mathrm{C}'', s'', \mathit{ok}$ and the definition of $\rightsquigarrow^i$ we know there exists C''', s''' such that $\mathrm{C}, s \rightarrow \mathrm{C}''', s''', \mathit{ok}$, and $\mathrm{C}''', s''' \rightsquigarrow^k \mathrm{C}'', s'', \mathit{ok}$. Consequently, from $\mathrm{C}''', s''' \rightsquigarrow^k \mathrm{C}'', s'', \mathit{ok}$, $\mathrm{C}'', s'' \rightsquigarrow^j \mathrm{C}', s', \epsilon$ and the inductive hypothesis we have $\mathrm{C}''', s''' \rightsquigarrow^{k+j} \mathrm{C}', s', \epsilon$. As such, from $\mathrm{C}, s \rightarrow \mathrm{C}''', s''', \mathit{ok}$ and the definition of $\rightsquigarrow^{k+j+1}$ we have $\mathrm{C}, s \rightsquigarrow^{k+j+1} \mathrm{C}', s', \epsilon$. That is, $\mathrm{C}, s \rightsquigarrow^{i+j} \mathrm{C}', s', \epsilon$, as required. □

Theorem 14 (Divergence soundness). *For all p, C, if $\vdash [p]\ \mathrm{C}\ [\infty]$ can be proven using the proof rules in Fig. 3, then $\models [p]\ \mathrm{C}\ [\infty]$ holds.*

Proof. By induction on the structure of rules in Fig. 3.

Case Div-Local
Pick arbitrary p, C such that $\vdash [\exists x.\ p]\ \mathrm{local}\ x\ \mathrm{in}\ \mathrm{C}\ [\infty]$. Pick an arbitrary $s \in \exists x.\ p$; i.e. there exists v, s_p such that $s_p = s[x \mapsto v]$ and $s_p \in p$. From the $[p]\ \mathrm{C}\ [\infty]$ premise and the inductive hypothesis we know there exists an infinite series $\mathrm{C}_1, \mathrm{C}_2, \cdots$ and $s_1, s_2, \cdots$ such that $\mathrm{C}, s_p \rightsquigarrow^+ \mathrm{C}_1, s_1, \mathit{ok} \rightsquigarrow^+ \mathrm{C}_2, s_2, \mathit{ok} \rightsquigarrow^+ \cdots$. As such, from the definition of $\rightsquigarrow^+$ and Lemma 10 we have $\mathrm{C}; \mathrm{end}(x, s(x)), s_p \rightsquigarrow^+ \mathrm{C}_1; \mathrm{end}(x, s(x)), s_1, \mathit{ok} \rightsquigarrow^+ \mathrm{C}_2; \mathrm{end}(x, s(x)), s_2, \mathit{ok} \rightsquigarrow^+ \cdots$ On the other

hand, from S-Local we then have $\mathsf{local}\ x\ \mathsf{in}\ \mathsf{C}, s \to \mathsf{C}; \mathsf{end}(x, s(x)), s_p$. Therefore, since we also have $\mathsf{C}; \mathsf{end}(x, s(x)), s_p \rightsquigarrow^+ \mathsf{C}_1; \mathsf{end}(x, s(x)), s_1, ok \rightsquigarrow^+ \mathsf{C}_2; \mathsf{end}(x, s(x)), s_2, ok \rightsquigarrow^+ \cdots$, from the definition of $\rightsquigarrow^+$ we have $\mathsf{local}\ x\ \mathsf{in}\ \mathsf{C}, s \rightsquigarrow^+ \mathsf{C}_1; \mathsf{end}(x, s(x)), s_1, ok \rightsquigarrow^+ \mathsf{C}_2; \mathsf{end}(x, s(x)), s_2, ok \rightsquigarrow^+ \cdots$, as required.

Case Div-Seq1

Pick arbitrary p, C_1, C_2 such that $[p]\ \mathsf{C}_1; \mathsf{C}_2\ [\infty]$. Pick an arbitrary $s \in p$. From the $[p]\ \mathsf{C}_1\ [\infty]$ premise and the inductive hypothesis we know there exists an infinite series $\mathsf{C}'_2, \mathsf{C}'_3, \cdots$, and $s_2, s_3, \cdots$, such that $\mathsf{C}_1, s \rightsquigarrow^+ \mathsf{C}'_2, s_2, ok \rightsquigarrow^+ \mathsf{C}'_3, s_3, ok \rightsquigarrow^+ \cdots$. As such, from the definition of $\rightsquigarrow^+$ and Lemma 10 we have $\mathsf{C}_1; \mathsf{C}_2, s \rightsquigarrow^+ \mathsf{C}'_2; \mathsf{C}_2, s_2, ok \rightsquigarrow^+ \mathsf{C}'_3; \mathsf{C}_2, s_3, ok \rightsquigarrow^+ \cdots$, as required.

Case Div-Seq2

Pick arbitrary p, q, C_1, C_2 such that $[p]\ \mathsf{C}_1; \mathsf{C}_2\ [\infty]$. Pick an arbitrary $s \in p$. From the $\vdash_{\mathsf{B}}\ [p]\ \mathsf{C}_1\ [ok\colon q]$ premise and Theorem 13 we know there exists $s_q \in q$ and n such that $\mathsf{C}_1, s \xrightarrow{n} -, s_q, ok$. Moreover, from the $[q]\ \mathsf{C}_2\ [\infty]$ premise and the inductive hypothesis we know there exists an infinite series $\mathsf{C}'_3, \mathsf{C}'_4, \cdots$ and $s_3, s_4, \cdots$, such that $\mathsf{C}_2, s_q \rightsquigarrow^+ \mathsf{C}'_3, s_3, ok \rightsquigarrow^+ \mathsf{C}'_4, s_4, ok \rightsquigarrow^+ \cdots$. As $\mathsf{C}_1, s \xrightarrow{n} -, s_q, ok$ and $\mathsf{C}_2, s_q \rightsquigarrow^+ \mathsf{C}'_3, s_3, ok$, from the definition of $\rightsquigarrow^+$ and Lemma 11 we have $\mathsf{C}_1; \mathsf{C}_2, s \rightsquigarrow^+ \mathsf{C}'_3, s_3, ok$. Moreover, as $\mathsf{C}'_3, s_3 \rightsquigarrow^+ \mathsf{C}'_4, s_4, ok \rightsquigarrow^+ \cdots$, we have $\mathsf{C}_1; \mathsf{C}_2, s \rightsquigarrow^+ \mathsf{C}'_3, s_3, ok \rightsquigarrow^+ \mathsf{C}'_4, s_4, ok \rightsquigarrow^+ \cdots$, as required.

Case Div-Choice

Pick arbitrary p, C_1, C_2 such that $[p]\ \mathsf{C}_1 + \mathsf{C}_2\ [\infty]$. Pick an arbitrary $s \in p$ and $i \in \{1, 2\}$. From the $[p]\ \mathsf{C}_i\ [\infty]$ premise and the inductive hypothesis we know there exists an infinite series $\mathsf{C}_3, \mathsf{C}_4, \cdots$ and $s_3, s_4, \cdots$, such that $\mathsf{C}_i, s \rightsquigarrow^+ \mathsf{C}_3, s_3, ok \rightsquigarrow^+ \mathsf{C}_4, s_4, ok \rightsquigarrow^+ \cdots$. Moreover, from S-Choice we have $\mathsf{C}_1 + \mathsf{C}_2, s \to \mathsf{C}_i, s, ok$. And thus we have $\mathsf{C}_1 + \mathsf{C}_2, s \to \mathsf{C}_i, s, ok \rightsquigarrow^+ \mathsf{C}_3, s_3, ok \rightsquigarrow^+ \mathsf{C}_4, s_4, ok \rightsquigarrow^+ \cdots$, as required.

Case Div-LoopUnfold

Pick arbitrary p, C such that $[p]\ \mathsf{C}^\star\ [\infty]$. Pick an arbitrary $s \in p$. From the $[p]\ \mathsf{C}; \mathsf{C}^\star\ [\infty]$ premise and the inductive hypothesis we know there exists an infinite series $\mathsf{C}_1, \mathsf{C}_2, \cdots$ and $s_1, s_2, \cdots$, such that $\mathsf{C}; \mathsf{C}^\star, s \rightsquigarrow^+ \mathsf{C}_1, s_1, ok \rightsquigarrow^+ \mathsf{C}_2, s_2, ok \rightsquigarrow^+ \cdots$. Moreover, from S-Loop we have $\mathsf{C}^\star, s \to \mathsf{C}; \mathsf{C}^\star, s, ok$. And thus we have $\mathsf{C}^\star, s \to \mathsf{C}; \mathsf{C}^\star, s, ok \rightsquigarrow^+ \mathsf{C}_1, s_1, ok \rightsquigarrow^+ \mathsf{C}_2, s_2, ok \rightsquigarrow^+ \cdots$, as required.

Case Div-LoopNest

This rule can be derived as follows:

$$\dfrac{\dfrac{[p]\ \mathsf{C}\ [\infty]}{[p]\ \mathsf{C}; \mathsf{C}^\star\ [\infty]}\ \textsc{Div-Seq1}}{[p]\ \mathsf{C}^\star\ [\infty]}\ \textsc{Div-LoopUnfold}$$

and thus this rule is sound as we established the soundness of Div-Seq1 and Div-LoopUnfold above.

Case Div-Loop

Pick arbitrary p, C, q such that $\vdash\ [p]\ \mathsf{C}^\star\ [\infty]$. From S-Loop we then have:

$$\forall s \in p.\ \mathsf{C}^\star, s \to \mathsf{C}; \mathsf{C}^\star, s, ok \tag{1}$$

From the $\vdash_{\mathrm{B}} \big[p\big]\ \mathrm{C}\ \big[ok\colon q\big]$ premise, Theorem 13, and the $q \subseteq p$ premise we know $\forall s \in p.\ \exists s' \in p, n.\ \mathrm{C}, s \xrightarrow{n} -, s', ok$ and thus from Lemma 1 $\mathrm{C}, s \xrightarrow{n} \mathsf{skip}, s', ok$. That is, from the axiom of choice we know there exist $f : p \to p$ and $g : p \to \mathbb{N}$ such that:

$$\forall s \in p.\ \mathrm{C}, s \xrightarrow{g(s)} \mathsf{skip}, f(s), ok \land f(s) \in p \tag{2}$$

In what follows, we show that $\forall s \in p.\ \mathrm{C}^\star, s \rightsquigarrow^{+} \mathrm{C}^\star, f(s), ok$.

Pick an arbitrary $s \in p$. From (2) we have $\mathrm{C}, s \xrightarrow{g(s)} \mathsf{skip}, f(s), ok$. There are now two cases to consider: i) $g(s) = 0$; or ii) $g(s) > 0$. In case (i), we then have $\mathrm{C} = \mathsf{skip}$ and $s{=}f(s)$. As such, from S-SeqSkip we have $\mathrm{C}; \mathrm{C}^\star, s \to \mathrm{C}^\star, f(s), ok$, and thus by definition of $\rightsquigarrow^{1}$ we have $\mathrm{C}; \mathrm{C}^\star, s \rightsquigarrow^{1} \mathrm{C}^\star, f(s), ok$

In case (ii), from $\mathrm{C}, s \xrightarrow{g(s)} \mathsf{skip}, f(s), ok$ and Lemma 9 we have $\mathrm{C}, s \rightsquigarrow^{g(s)} \mathsf{skip}, f(s), ok$. Consequently, from Lemma 10 we have $\mathrm{C}; \mathrm{C}^\star, s \rightsquigarrow^{g(s)} \mathsf{skip}; \mathrm{C}^\star, f(s), ok$. On the other hand, from S-SeqSkip we have $\mathsf{skip}; \mathrm{C}^\star, f(s) \to \mathrm{C}^\star, f(s), ok$ and thus by definition of $\rightsquigarrow^{1}$ we have $\mathsf{skip}; \mathrm{C}^\star, f(s) \rightsquigarrow^{1} \mathrm{C}^\star, f(s), ok$. From Lemma 12, $\mathrm{C}; \mathrm{C}^\star, s \rightsquigarrow^{g(s)} \mathsf{skip}; \mathrm{C}^\star, f(s), ok$ and $\mathsf{skip}; \mathrm{C}^\star, f(s) \rightsquigarrow^{1} \mathrm{C}^\star, f(s), ok$ we know there exists i such that $\mathrm{C}; \mathrm{C}^\star, s \rightsquigarrow^{i} \mathrm{C}^\star, f(s), ok$.

That is, in both cases we know there exists i such that $\mathrm{C}; \mathrm{C}^\star, s \rightsquigarrow^{i} \mathrm{C}^\star, f(s), ok$. As such, from (1) and the definition of $\rightsquigarrow^{i+1}$ we have $\mathrm{C}^\star, s \rightsquigarrow^{i+1} \mathrm{C}^\star, f(s), ok$, i.e. $\mathrm{C}^\star, s \rightsquigarrow^{+} \mathrm{C}^\star, f(s), ok$. That is, from (2) we have:

$$\forall s \in p.\ \mathrm{C}^\star, s \rightsquigarrow^{+} \mathrm{C}^\star, f(s), ok \land f(s) \in p \tag{3}$$

Pick an arbitrary $s \in p$. From (3) we then know $\mathrm{C}^\star, s \rightsquigarrow^{+} \mathrm{C}^\star, f(s), ok \rightsquigarrow^{+} \mathrm{C}^\star, f^2(s), ok \rightsquigarrow^{+} \cdots$, as required.

Case Div-Subvariant
Pick arbitrary p, C, q such that $\vdash \big[p(0)\big]\ \mathrm{C}^\star\ \big[\infty\big]$. From S-Loop we then have:

$$\forall s \in p.\ \mathrm{C}^\star, s \to \mathrm{C}; \mathrm{C}^\star, s, ok \tag{4}$$

From the $\forall n \in \mathbb{N}.\ \vdash_{\mathrm{B}} \big[p(n)\big]\ \mathrm{C}\ \big[ok\colon p(n{+}1)\big]$ premise and Theorem 13 we know $\forall n \in \mathbb{N}.\ \forall s \in p(n).\ \exists s' \in p(n{+}1), k.\ \mathrm{C}, s \xrightarrow{k} -, s', ok$ and thus from Lemma 1 $\mathrm{C}, s \xrightarrow{k} \mathsf{skip}, s', ok$. That is, from the axiom of choice we know there exists a series of functions, $f_1, g_1, f_2, g_2 \cdots$ such that for each $i \in \mathbb{N}$, we have $f_i : p(i{-}1) \to p(i)$ and $g_i : p(i{-}1) \to \mathbb{N}$ such that:

$$\forall i \in \mathbb{N}^{+}.\ \forall s \in p(i-1).\ \mathrm{C}, s \xrightarrow{g_i(s)} \mathsf{skip}, f_i(s), ok \land f_i(s) \in p(i) \tag{5}$$

In what follows, we show that $\forall i \in \mathbb{N}^{+}.\ \forall s \in p(i{-}1).\ \mathrm{C}^\star, s \rightsquigarrow^{+} \mathrm{C}^\star, f_i(s), ok$.

Pick an arbitrary $i \in \mathbb{N}^{+}$ and $s \in p(i{-}1)$. From (5) we have $\mathrm{C}, s \xrightarrow{g_i(s)} \mathsf{skip}, f_i(s), ok$. There are now two cases to consider: a) $g_i(s) = 0$; or b) $g_i(s) > 0$. In case (a), we then have $\mathrm{C} = \mathsf{skip}$ and $s{=}f_i(s)$. As such, from S-SeqSkip we have $\mathrm{C}; \mathrm{C}^\star, s \to \mathrm{C}^\star, f_i(s), ok$, and thus by definition of $\rightsquigarrow^{1}$ we have $\mathrm{C}; \mathrm{C}^\star, s \rightsquigarrow^{1} \mathrm{C}^\star, f_i(s), ok$

In case (b), from $\mathrm{C}, s \xrightarrow{g_i(s)} \mathsf{skip}, f_i(s), ok$ and Lemma 9 we have $\mathrm{C}, s \rightsquigarrow^{g_i(s)} \mathsf{skip}, f_i(s), ok$. Consequently, from Lemma 10 we have $\mathrm{C}; \mathrm{C}^\star, s \rightsquigarrow^{g_i(s)} \mathsf{skip}; \mathrm{C}^\star, f_i(s), ok$. On the other hand, from S-SeqSkip we have $\mathsf{skip}; \mathrm{C}^\star, f_i(s) \to \mathrm{C}^\star, f_i(s), ok$ and thus by definition of $\rightsquigarrow^{1}$ we have $\mathsf{skip}; \mathrm{C}^\star, f_i(s) \rightsquigarrow^{1} \mathrm{C}^\star, f_i(s), ok$. From Lemma 12, $\mathrm{C}; \mathrm{C}^\star, s \rightsquigarrow^{g_i(s)} \mathsf{skip}; \mathrm{C}^\star, f_i(s), ok$ and $\mathsf{skip}; \mathrm{C}^\star, f_i(s) \rightsquigarrow^{1} \mathrm{C}^\star, f_i(s), ok$ we know there exists j such that $\mathrm{C}; \mathrm{C}^\star, s \rightsquigarrow^{j} \mathrm{C}^\star, f_i(s), ok$.

That is, in both cases we know there exists j such that $\mathrm{C}; \mathrm{C}^\star, s \rightsquigarrow^{j} \mathrm{C}^\star, f_i(s), ok$. As such, from (4) and the definition of $\rightsquigarrow^{j+1}$ we have $\mathrm{C}^\star, s \rightsquigarrow^{j+1} \mathrm{C}^\star, f_i(s), ok$, i.e. $\mathrm{C}^\star, s \rightsquigarrow^{+} \mathrm{C}^\star, f_i(s), ok$. That is, from (5) we have:

$$\forall i \in \mathbb{N}^{+}.\ \forall s \in p(i{-}1).\ \mathrm{C}^{\star}, s \rightsquigarrow^{+} \mathrm{C}^{\star}, f_i(s), ok \wedge f_i(s) \in p(i) \tag{6}$$

Pick an arbitrary $s \in p(0)$. From (6) we then know $\mathrm{C}^{\star}, s \rightsquigarrow^{+} \mathrm{C}^{\star}, f_1(s), ok \rightsquigarrow^{+} \mathrm{C}^{\star}, f_2(s), ok \rightsquigarrow^{+} \cdots$, as required.

Case Div-Cons

Pick arbitrary p, C such that $\vdash [p]\ \mathrm{C}\ [\infty]$. Pick an arbitrary $s \in p$. From the $p \subseteq p'$ premise we know $s \in p'$. As such, from the $[p']\ \mathrm{C}\ [\infty]$ premise we know there exists an infinite series $\mathrm{C}_1, \mathrm{C}_2, \cdots$ and $s_1, s_2, \cdots$, such that $\mathrm{C}, s \rightsquigarrow^{+} \mathrm{C}_1, s_1, ok \rightsquigarrow^{+} \mathrm{C}_2, s_2, ok \rightsquigarrow^{+} \cdots$, as required.

Case Div-Subst

Pick arbitrary p, C, q, y such that $y \notin \mathrm{fv}(p, \mathrm{C})$ and $(\vdash [p]\ \mathrm{C}\ [\infty])[y/x]$, i.e. $\vdash [p[y/x]]\ \mathrm{C}[y/x]\ [\infty]$. Pick an arbitrary $s \in p[y/x]$ and let $s_p = s[x \mapsto s(y)]$. We then have $s_p \in p$ and thus from the $\vdash_{\mathrm{B}} [p]\ \mathrm{C}\ [\epsilon : q]$ premise and the inductive hypothesis we then know there exists an infinite series $\mathrm{C}_1, \mathrm{C}_2, \cdots$ and $s_1, s_2, \cdots$ such that $\mathrm{C}, s_p \rightsquigarrow^{+} \mathrm{C}_1, s_1, ok \rightsquigarrow^{+} \mathrm{C}_2, s_2, ok \rightsquigarrow^{+} \cdots$. Let $\mathrm{C}'_i = \mathrm{C}_i[y/x]$ and $s'_i = s_i[y \mapsto s'_i(y)]$ for all i As such, from the semantics we also have $\mathrm{C}[y/x], s \rightsquigarrow^{+} \mathrm{C}'_1, s'_1, ok \rightsquigarrow^{+} \mathrm{C}'_2, s'_2, ok \rightsquigarrow^{+} \cdots$, as required. □

C UNTER COMPLETENESS

C.1 Completeness of BUA and FUA Rules

Lemma 13 (BUA completeness). *For all p, C, q, ϵ, if $\models_B [p]\ \mathrm{C}\ [\epsilon : q]$ holds, then $\vdash_B [p]\ \mathrm{C}\ [\epsilon : q]$ can be proven using the proof rules in Fig. 2.*

PROOF. We proceed by induction of the structure of C.

Case $\mathrm{C} = \mathrm{skip}$
Pick arbitrary p, q such that $\models_B [p]\ \mathrm{skip}\ [\epsilon : q]$ holds. Given the semantics of skip, we then know $p \subseteq q$. As such, we can derive $\vdash_B [p]\ \mathrm{C}\ [\epsilon : q]$ using SKIP and CONSF.

Cases $\mathrm{C} = \mathrm{assume}(B)$ **and** $\mathrm{C} = \mathrm{error}$
The proofs of these cases are analogous to the $\mathrm{C} = \mathrm{skip}$ case and omitted.

Case $\mathrm{C} = x := e$
Pick arbitrary p such that $\models_B [p]\ x := e\ [ok\colon q]$ holds. As $\exists y.\ p[y/x] \land x = e[y/x]$ is the strongest post of $x := e$ from p (see [23]), we then know $\exists y.\ p[y/x] \land x = e[y/x] \subseteq q$. Moreover, from ASSIGN we have $\vdash_B [p]\ x := e\ [ok\colon \exists y.\ p[y/x] \land x = e[y/x]]$. Consequently, as $\exists y.\ p[y/x] \land x = e[y/x] \subseteq q$, from CONSF we have $\vdash_B [p]\ x := e\ [ok\colon q]$, as required.

Case $\mathrm{C} = \mathrm{local}\ x\ \mathrm{in}\ \mathrm{C}$
Pick arbitrary p, q such that $\models_B [p]\ \mathrm{local}\ x\ \mathrm{in}\ \mathrm{C}\ [\epsilon : q]$ holds. Pick an arbitrary y such that $y \notin \mathrm{fv}(\mathrm{C})$, $y \notin \mathrm{fv}(p)$ and $y \notin \mathrm{fv}(q)$. Then we know that $\mathrm{local}\ y\ \mathrm{in}\ \mathrm{C}$ is semantically equivalent to $\mathrm{local}\ x\ \mathrm{in}\ \mathrm{C}$ and thus $\models_B [p]\ \mathrm{local}\ y\ \mathrm{in}\ \mathrm{C}\ [\epsilon : q]$ holds. From the semantics of $\mathrm{local}\ y\ \mathrm{in}\ \mathrm{C}$ we know there exist v_1, v_2 such that $\models_B [p \land y = v_1]\ \mathrm{C}\ [\epsilon : q \land y = v_2]$ holds. From the inductive hypothesis we then have$\vdash_B [p \land y = v_1]\ \mathrm{C}\ [\epsilon : q \land y = v_2]$, and thus from LOCAL we have $\vdash_B [\exists y.\ p \land y = v_1]\ \mathrm{local}\ y\ \mathrm{in}\ \mathrm{C}\ [\epsilon : \exists y.\ q \land y = v_2]$. As $y \notin \mathrm{fv}(p)$ and $y \notin \mathrm{fv}(q)$, using CONSEQ we have $\vdash_B [p \land \exists y.\ y = v_1]\ \mathrm{local}\ y\ \mathrm{in}\ \mathrm{C}\ [\epsilon : q \land \exists y.\ y = v_2]$. Once again, using CONSEQ we have $\vdash_B [p]\ \mathrm{local}\ y\ \mathrm{in}\ \mathrm{C}\ [\epsilon : q]$. Finally, using SUBST and since $y \notin \mathrm{fv}(\mathrm{C})$, $y \notin \mathrm{fv}(p)$ and $y \notin \mathrm{fv}(q)$, we have $\vdash_B [p]\ \mathrm{local}\ x\ \mathrm{in}\ \mathrm{C}\ [\epsilon : q]$, as required.

Case $\mathrm{C} = \mathrm{C}_1; \mathrm{C}_2$
Pick arbitrary p, q such that $\models_B [p]\ \mathrm{C}_1; \mathrm{C}_2\ [\epsilon : q]$ holds. From the semantics of $\mathrm{C}_1; \mathrm{C}_2$ we then know either 1) $\epsilon = er$ and $\models_B [p]\ \mathrm{C}_1\ [er\colon q]$; or 2) $\epsilon = ok$ and there exists r such that $\models_B [p]\ \mathrm{C}_1\ [ok\colon r]$ and $\models_B [r]\ \mathrm{C}_2\ [\epsilon : q]$. In case (1) from $\models_B [p]\ \mathrm{C}_1\ [er\colon q]$ and the inductive hypothesis we know we can prove $\vdash_B [p]\ \mathrm{C}_1\ [er\colon q]$, and thus using SEQER we can prove $\vdash_B [p]\ \mathrm{C}_1; \mathrm{C}_2\ [\epsilon : q]$, as required. In case (2) from $\models_B [p]\ \mathrm{C}_1\ [ok\colon r]$ and $\models_B [r]\ \mathrm{C}_2\ [\epsilon : q]$ and the inductive hypotheses we know we can prove $\vdash_B [p]\ \mathrm{C}_1\ [ok\colon r]$ and $\vdash_B [r]\ \mathrm{C}_2\ [\epsilon : q]$. Consequently, using SEQ we can prove $\vdash_B [p]\ \mathrm{C}_1; \mathrm{C}_2\ [\epsilon : q]$, as required.

Case $\mathrm{C} = \mathrm{C}_1 + \mathrm{C}_2$
Pick arbitrary p, q such that $\models_B [p]\ \mathrm{C}_1 + \mathrm{C}_2\ [\epsilon : q]$ holds. From the semantics of $\mathrm{C}_1 + \mathrm{C}_2$ we know there exists $i \in \{1, 2\}$ such that $\models_B [p]\ \mathrm{C}_i\ [\epsilon : q]$. From $\models_B [p]\ \mathrm{C}_i\ [\epsilon : q]$ and the inductive hypothesis we know we can prove $\vdash_B [p]\ \mathrm{C}_i\ [\epsilon : q]$, and thus using CHOICE we can prove $\vdash_B [p]\ \mathrm{C}_1 + \mathrm{C}_2\ [\epsilon : q]$, as required.

Case $\mathrm{C} = \mathrm{C}^\star$
Pick arbitrary p, q such that $\models_B [p]\ \mathrm{C}^\star\ [\epsilon : q]$ holds. There are two cases to consider: 1) $\epsilon = ok$; or

$\epsilon = er$. In case (1), let $p(0) = p$ and $p(n)$ be the state reachable after executing C n times starting from $p(0)$ for $n > 0$. By definition we then know there exists $k \geq 0$ such that $q = p(k)$. Moreover, by definition we then have $\models_{\mathsf{B}} \left[p(n)\right]\ \mathsf{C}\ \left[ok\colon p(n{+}1)\right]$ for all $0 \leq nk$. As such, by the inductive hypothesis we have $\vdash_{\mathsf{B}} \left[p(n)\right]\ \mathsf{C}\ \left[ok\colon p(n{+}1)\right]$ for all $n < k$. Using Loop-Subvariant we then have $\vdash_{\mathsf{B}} \left[p(0)\right]\ \mathsf{C}\ \left[ok\colon p(k)\right]$, i.e. $\vdash_{\mathsf{B}} [p]\ \mathsf{C}\ [ok\colon q]$, as required.

In case (2), from the semantics of loops we know that C executed normally for a number of (possibly zero) iterations, and in the subsequent iteration the loop encountered an error. That is, there exist r such that $\models_{\mathsf{B}} [p]\ \mathsf{C}^{\star}\ [ok\colon r]$ and $\models_{\mathsf{B}} [r]\ \mathsf{C}\ [er\colon q]$. From the proof of case (1) we then have $\vdash_{\mathsf{B}} [p]\ \mathsf{C}^{\star}\ [ok\colon r]$. From $\models_{\mathsf{B}} [r]\ \mathsf{C}\ [er\colon q]$ and the inductive hypothesis we have $\vdash_{\mathsf{B}} [r]\ \mathsf{C}\ [er\colon q]$. Consequently, from $\vdash_{\mathsf{B}} [p]\ \mathsf{C}^{\star}\ [ok\colon r]$, $\vdash_{\mathsf{B}} [r]\ \mathsf{C}\ [er\colon q]$ and Seq we have $\vdash_{\mathsf{B}} [p]\ \mathsf{C}^{\star}; \mathsf{C}\ [er\colon q]$, i.e. $\vdash_{\mathsf{B}} [p]\ \mathsf{C}^{\star}; \mathsf{C}\ [\epsilon : q]$. As such, from Loop we have $\vdash_{\mathsf{B}} [p]\ \mathsf{C}^{\star}\ [er\colon q]$, as required. □

Lemma 14 (FUA completeness). *For all p, C, q, ϵ, if $\models_{\mathsf{F}} [p]\ \mathsf{C}\ [\epsilon : q]$ holds, then $\vdash_{\mathsf{F}} [p]\ \mathsf{C}\ [\epsilon : q]$ can be proven using the proof rules in Fig. 2.*

Proof. The proof of this lemma is as given by O'Hearn [23]. □

Theorem 15 (Completeness). *For all p, C, q, ϵ, if $\models_{\dagger} [p]\ \mathsf{C}\ [\epsilon : q]$ holds, then $\vdash_{\dagger} [p]\ \mathsf{C}\ [\epsilon : q]$ can be proven using the proof rules in Fig. 2.*

Proof. Follows immediately from Lemma 13 and Lemma 14. □

C.2 Completeness of Divergence Rules

In what follows, we write $\mathsf{C}, s \rightsquigarrow^{+} \mathsf{C}', s', \epsilon$ for $\exists n.\ \mathsf{C}, s \rightsquigarrow^{n} \mathsf{C}', s', \epsilon$.

Div-Subst

$$\frac{\vdash [p]\ \mathsf{C}\ [\infty] \qquad y \notin \mathsf{fv}(p, \mathsf{C})}{\vdash ([p]\ \mathsf{C}\ [\infty])[y/x]}$$

Theorem 16 (Divergence completeness). *For all p, C, if $\models [p]\ \mathsf{C}\ [\infty]$ holds, then $\vdash [p]\ \mathsf{C}\ [\infty]$ can be proven using the proof rules in Fig. 3,.*

Proof. We proceed by induction of the structure of C.

Cases $\mathsf{C} = \mathsf{skip}$, $\mathsf{C} = x := e$, $\mathsf{C} = \mathsf{error}$, $\mathsf{C} = \mathsf{assume}(B)$
These cases do not arise as they have no divergent steps and reduce to skip in either 0 or 1 steps.

Case $\mathsf{C} = \mathsf{local}\ x\ \mathsf{in}\ \mathsf{C}$
Pick arbitrary p such that $\models [p]\ \mathsf{local}\ x\ \mathsf{in}\ \mathsf{C}\ [\infty]$ holds. Pick an arbitrary y such that $y \notin \mathsf{fv}(\mathsf{C})$ and $y \notin \mathsf{fv}(p)$. Then we know that $\mathsf{local}\ y\ \mathsf{in}\ \mathsf{C}$ is semantically equivalent to $\mathsf{local}\ x\ \mathsf{in}\ \mathsf{C}$ and thus $\models [p]\ \mathsf{local}\ y\ \mathsf{in}\ \mathsf{C}\ [\infty]$ holds. From the semantics of $\mathsf{local}\ y\ \mathsf{in}\ \mathsf{C}$ we know there exist v_1 such that $\models [p \land y = v_1]\ \mathsf{C}\ [\infty]$ holds. From the inductive hypothesis we then have$\vdash [p \land y = v_1]\ \mathsf{C}\ [\infty]$, and thus from Div-Local we have $\vdash [\exists y.\ p \land y = v_1]\ \mathsf{local}\ y\ \mathsf{in}\ \mathsf{C}\ [\infty]$. As $y \notin \mathsf{fv}(p)$, using Div-Cons we have $\vdash [p \land \exists y.\ y = v_1]\ \mathsf{local}\ y\ \mathsf{in}\ \mathsf{C}\ [\infty]$. Once again, using Div-Cons we have $\vdash [p]\ \mathsf{local}\ y\ \mathsf{in}\ \mathsf{C}\ [\infty]$. Finally, using Div-Subst and since $y \notin \mathsf{fv}(\mathsf{C})$ and $y \notin \mathsf{fv}(p)$, we have $\vdash [p]\ \mathsf{local}\ x\ \mathsf{in}\ \mathsf{C}\ [\infty]$, as required.

Case $\mathsf{C} = \mathsf{C}_1; \mathsf{C}_2$
Pick arbitrary p such that $\models [p]\ \mathsf{C}_1; \mathsf{C}_2\ [\infty]$ holds. From the semantics of $\mathsf{C}_1; \mathsf{C}_2$ we then know either 1) $\models [p]\ \mathsf{C}_1\ [\infty]$; or 2) there exists q such that $\models_{\mathsf{B}} [p]\ \mathsf{C}_1\ [ok\colon q]$ and $\models [q]\ \mathsf{C}_2\ [\infty]$. In case (1) from $\models [p]\ \mathsf{C}_1\ [\infty]$ and the inductive hypothesis we know we can prove $\vdash [p]\ \mathsf{C}_1\ [\infty]$, and thus

using Div-Seq1 we can prove $\vdash [p]\ C_1; C_2\ [\infty]$, as required. In case (2) from $\models_B [p]\ C_1\ [ok\colon q]$ and Theorem 15 we have $\vdash_B [p]\ C_1\ [ok\colon q]$. Moreover, from $\models [q]\ C_2\ [\infty]$ and the inductive hypotheses we can prove $\vdash [q]\ C_2\ [\infty]$. Consequently, using Div-Seq2 we can prove $\vdash [p]\ C_1; C_2\ [\infty]$, as required.

Case $C = C_1 + C_2$

Pick arbitrary p such that $\models [p]\ C_1 + C_2\ [\infty]$ holds. From the semantics of $C_1 + C_2$ we know there exists $i \in \{1, 2\}$ such that $\models [p]\ C_i\ [\infty]$ holds. From $\models [p]\ C_i\ [\infty]$ and the inductive hypothesis we know we can prove $\vdash [p]\ C_i\ [\infty]$, and thus using Div-Choice we can prove $\models [p]\ C_1 + C_2\ [\infty]$, as required.

Case $C = C^\star$

Pick arbitrary p such that $\models [p]\ C^\star\ [\infty]$ holds. Let $p(0) = p$ and $p(n)$ be the state reachable after executing C for n times starting from $p(0)$ for $n > 0$. Let $C^0 = \text{skip}$ and let C^n denote iterating C for n times, for all $n > 0$. Given the semantics of loops, there are two cases to consider: There are two cases to consider:

1) $\models_B [p(n)]\ C\ [ok\colon p(n{+}1)]$ for all $n \in \mathbb{N}$; or

2) there exists n and q such that $\models_B [p]\ C^n\ [ok\colon q]$ and $\models [q]\ C\ [\infty]$.

In case (1), from Theorem 15 we have $\vdash_B [p(n)]\ C\ [ok\colon p(n{+}1)]$ for all $n \in \mathbb{N}$. As such, using Div-Subvariant we have $\vdash [p(0)]\ C\ [\infty]$, i.e. $\vdash [p]\ C\ [\infty]$, as required.

In case (2), we proceed by induction on n.

Subcase $n = 0$

As we have $\models_B [p]\ C^n\ [\epsilon : q]$, $\models [q]\ C\ [\infty]$ and $C^0 = \text{skip}$, we know $p \subseteq q$. Moreover, from $\models [q]\ C\ [\infty]$ and the inductive hypothesis we have $\vdash [q]\ C\ [\infty]$, and as such from Div-LoopNest we have $\vdash [q]\ C^\star\ [\infty]$. Consequently, as $p \subseteq q$, from Div-Cons we have $\vdash [p]\ C^\star\ [\infty]$, as required.

Subcase $n = k{+}1$

From $\models_B [p]\ C^n\ [ok\colon q]$ and Theorem 15 we have

$$\vdash_B [p]\ C^n\ [ok\colon q] \tag{7}$$

Moreover, from $\models [q]\ C\ [\infty]$ and the inductive hypothesis we have

$$\vdash [q]\ C\ [\infty] \tag{8}$$

As $C^n = \underbrace{C; \cdots; C}_{n \text{ times}}$, we can then prove $\vdash [p]\ C^\star\ [\infty]$ as follows:

$$\dfrac{\dfrac{\dfrac{(7)}{\vdash_B [p]\ C^n\ [ok\colon q]} \qquad \dfrac{\dfrac{(8)}{\vdash [q]\ C\ [\infty]}\ \text{Div-LoopNest}}{\vdash [q]\ C^\star\ [\infty]}}{\vdash [p]\ C^n; C^\star\ [\infty]}\ \text{Div-Seq2}}{\vdash [p]\ C^\star\ [\infty]}\ \text{Div-LoopUnfold} \times n$$

□

D THE RELATION BETWEEN FUA AND BUA TRIPLES

Theorem 17. *For all p, C, q, ϵ, if* $\models_{\mathsf{F}}$ $[p]$ C $[\epsilon : q]$ *holds and* $\mathsf{min}_{\mathsf{pre}}(p, \mathsf{C}, q)$, *then* $\models_{\mathsf{B}}$ $[p]$ C $[\epsilon : q]$ *also holds, where*

$$\mathsf{min}_{\mathsf{pre}}(p, \mathsf{C}, q) \overset{def}{\iff} \forall p'.\ p' \subset p \Rightarrow \not\models_{\mathsf{F}} [p']\ \mathsf{C}\ [\epsilon : q]$$

Proof. Pick arbitrary p, C, q, ϵ such that $\models_{\mathsf{F}}$ $[p]$ C $[\epsilon : q]$ holds and $\mathsf{min}_{\mathsf{pre}}(p, \mathsf{C}, q)$. Let us proceed by contradiction and assume that $\models_{\mathsf{B}}$ $[p]$ C $[\epsilon : q]$ does not hold. That is, there exists $s_p \in p$ such that:

$$\neg\exists s_q \in q, n.\ \mathsf{C}, s_p \xrightarrow{n} -, s_q, \epsilon \tag{9}$$

Let $p' \triangleq p \setminus \{s_p\}$. We next show that $\models_{\mathsf{F}}$ $[p']$ C $[\epsilon : q]$ holds.
Pick an arbitrary $s_2 \in q$. Since $\models_{\mathsf{F}}$ $[p]$ C $[\epsilon : q]$ holds, from its definition we know there exists $s_1 \in p$, k such that $\mathsf{C}, s_1 \xrightarrow{k} -, s_2, \epsilon$. However, from (??) we know $s_1 \neq s_p$. Consequently, since $p' \triangleq p \setminus \{s_p\}$ and $s_1 \in p$, we know $s_1 \in p'$. That is, there exists $s_1 \in p'$, k such that $\mathsf{C}, s_1 \xrightarrow{k} -, s_2, \epsilon$, and thus by definition we have:

$$\models_{\mathsf{F}} [p']\ \mathsf{C}\ [\epsilon : q] \tag{10}$$

Finally, from $\mathsf{min}_{\mathsf{pre}}(p, \mathsf{C}, q)$, (10) and the definition of $\mathsf{min}_{\mathsf{pre}}$ we have $p' \not\subset p$. This, however, leads to a contradiction as $p' \triangleq p \setminus \{s_p\}$ and thus $p' \subset p$. □

Theorem 18. *For all p, C, q, ϵ, if* $\models_{\mathsf{B}}$ $[p]$ C $[\epsilon : q]$ *holds and* $\mathsf{min}_{\mathsf{post}}(p, \mathsf{C}, q)$, *then* $\models_{\mathsf{F}}$ $[p]$ C $[\epsilon : q]$ *also holds, where*

$$\mathsf{min}_{\mathsf{post}}(p, \mathsf{C}, q) \overset{def}{\iff} \forall q'.\ q' \subset q \Rightarrow \not\models_{\mathsf{B}} [p]\ \mathsf{C}\ [\epsilon : q']$$

Proof. Pick arbitrary p, C, q, ϵ such that $\models_{\mathsf{B}}$ $[p]$ C $[\epsilon : q]$ holds and $\mathsf{min}_{\mathsf{post}}(p, \mathsf{C}, q)$. Let us proceed by contradiction and assume that $\models_{\mathsf{F}}$ $[p]$ C $[\epsilon : q]$ does not hold. That is, there exists $s_q \in q$ such that:

$$\neg\exists s_p \in p, n.\ \mathsf{C}, s_p \xrightarrow{n} -, s_q, \epsilon \tag{11}$$

Let $q' \triangleq q \setminus \{s_q\}$. We next show that $\models_{\mathsf{B}}$ $[p]$ C $[\epsilon : q']$ holds.
Pick an arbitrary $s_1 \in p$. Since $\models_{\mathsf{B}}$ $[p]$ C $[\epsilon : q]$ holds, from its definition we know there exists $s_2 \in q$, k such that $\mathsf{C}, s_1 \xrightarrow{k} -, s_2, \epsilon$. However, from (11) we know $s_2 \neq s_q$. Consequently, since $q' \triangleq q \setminus \{s_q\}$ and $s_2 \in q$, we know $s_q \in q'$. That is, there exists $s_2 \in q'$, k such that $\mathsf{C}, s_1 \xrightarrow{k} -, s_2, \epsilon$, and thus by definition we have:

$$\models_{\mathsf{B}} [p]\ \mathsf{C}\ [\epsilon : q'] \tag{12}$$

Finally, from $\mathsf{min}_{\mathsf{post}}(p, \mathsf{C}, q)$, (12) and the definition of $\mathsf{min}_{\mathsf{post}}$ we have $q' \not\subset q$. This, however, leads to a contradiction as $q' \triangleq q \setminus \{s_q\}$ and thus $q' \subset q$. □

E UNTER$^{\text{SL}}$ MODEL AND SEMANTICS

Separation Logic at a Glance. The essence of SL and its compositional reasoning power is embodied in its *frame rule*, adapted to our notation below (left), which enables one to extend the underlying heap (memory) arbitrarily with additional resources (described by r), allowing the same specification (triple) to be reused in different contexts with different heaps. Intuitively, the heaps described by the frame r lie outside the footprint of C (parts of the heap accessed and modified by C), as stipulated by $\mathrm{mod}(\mathrm{C}) \cap \mathrm{fv}(r) = \emptyset$, and thus this frame remains unchanged when executing C. The $*$ connective denotes the separating conjunction (read as 'and separately'), and is used to combine the underlying heaps (by taking their union provided that they contain distinct locations).

$$\textsc{SL-Frame}\quad \frac{\vdash_{\dagger} [p]\, \mathrm{C}\, [\epsilon : q] \qquad \mathrm{mod}(\mathrm{C}) \cap \mathrm{fv}(r) = \emptyset}{\vdash_{\dagger} [p * r]\ \mathrm{C}\ [\epsilon : q * r]} \qquad \textsc{SL-Free}\quad \vdash_{\mathsf{F}} [x \mapsto v]\, \mathsf{free}(x)\, [ok : \mathsf{emp}] \qquad \textsc{ISL-Free}\quad \vdash_{\mathsf{F}} [x \mapsto v]\, \mathsf{free}(x)\, [ok : x \not\mapsto]$$

The compositionality afforded by SL-Frame allows us to devise *local* axioms describing the behaviour of heap-manipulating operations, in that we can only mention those parts of the heap manipulated by the operation and later extend this behaviour to larger (global) settings by using SL-Frame. For instance, we can describe the behaviour of freeing memory as in the SL-Free axiom above (middle), adapted from the corresponding SL axiom. Specifically, the $x \mapsto v$ assertion describes a state in which the heap comprises a single location at x holding value v. Moreover, $x \mapsto v$ describes a (linear) resource that grants exclusive permission to access location x and thus cannot be duplicated; i.e. for all x, v and v': $x \mapsto v * x \mapsto v' \iff$ false. On the other hand, the emp assertion describes states in which the heap is empty, and thus represents the identity of $*$-composition; i.e. for all p: $p * \mathsf{emp} \iff p$.

FUA Triples and Separation Logic. To achieve compositional reasoning, an SL extension of a FUA reasoning system must preserve the soundness of SL-Frame. However, as Raad et al. [24] show, the original model of SL is unsound for FUA reasoning. in Particular, we can apply SL-Frame with $r \triangleq x \mapsto v$ as shown below, resulting in an invalid FUA triple:

$$\cfrac{\cfrac{\cfrac{}{\vdash_{\mathsf{F}} [x \mapsto v]\ \mathsf{free}(x)\ [ok : \mathsf{emp}]}\ \textsc{SL-Free}}{\not\vdash_{\mathsf{F}} [x \mapsto v * x \mapsto v]\ \mathsf{free}(x)\ [ok : \mathsf{emp} * x \mapsto v]}\ \textsc{SL-Frame}}{\not\vdash_{\mathsf{F}} [\mathsf{false}]\ \mathsf{free}(x)\ [ok : x \mapsto v]}\ (\text{semantics of } *)$$

Note that $[\mathsf{false}]\ \mathsf{free}(x)\ [ok : x \mapsto v]$ in the conclusion is unsound: it states that every state in $x \mapsto v$ can be reached from *some* state in false, while false denotes an empty set of states.

To remedy this, Raad et al. [24] propose an adapted model in which they track the knowledge that a location was previously freed via *negative heap assertions*. Specifically, a negative heap assertion, $x \not\mapsto$, conveys: 1) the *knowledge* that x is an addressable location; 2) the knowledge that x is not allocated; and 3) the *ownership* of location x. That is, $x \not\mapsto$ is analogous to the points-to assertion $x \mapsto -$ and is thus manipulated similarly using $*$-conjunction. More concretely, one cannot consistently $*$-conjoin $x \not\mapsto$ either with $x \mapsto -$ or with itself: $x \mapsto - * x \not\mapsto \iff$ false and $x \not\mapsto * x \not\mapsto \iff$ false. Using negative assertions, one can specify the $\mathsf{free}(x)$ axiom as in ISL-Free above (right), recovering the frame rule: this time, when we frame $x \mapsto v$ on both sides, we obtain the inconsistent assertion $x \mapsto - * x \not\mapsto$ on the right-hand side (i.e. we have false as both pre- and post-states), which always renders a FUA triple vacuously valid.

Assertion Semantics. We present the semantics of UNTER$^{\text{SL}}$ assertions at the top of Fig. 10, where an assertion is interpreted as a set of UNTER$^{\text{SL}}$ states. The semantics of classical assertions

SkipSL
$$\vdash_\dagger [\mathsf{emp}]\ \mathsf{skip}\ [ok\colon \mathsf{emp}]$$

AssumeSL
$$\vdash_\dagger [B]\ \mathsf{assume}(B)\ [ok\colon B]$$

AssignSL
$$\vdash_\dagger [x{=}x']\ x:=e\ [ok\colon x{=}e[x'/x]]$$

Alloc
$$\vdash_\dagger [\mathsf{emp}]\ x:=\mathsf{alloc}()\ [ok\colon \exists l.\ l \mapsto v * x{=}l]$$

AllocFree
$$\vdash_\dagger [y \not\mapsto]\ x:=\mathsf{alloc}()\ [ok\colon y \mapsto v * x{=}y]$$

Free
$$\vdash_\dagger [x \mapsto e]\ \mathsf{free}(x)\ [ok\colon x \not\mapsto]$$

FreeEr
$$\vdash_\dagger [x \not\mapsto]\ \mathsf{free}(x)\ [er\colon x \not\mapsto]$$

FreeNull
$$\vdash_\dagger [x{=}\mathsf{null}]\ \mathsf{free}(x)\ [er\colon x{=}\mathsf{null}]$$

Store
$$\vdash_\dagger [x \mapsto e]\ [x] := y\ [ok\colon x \mapsto y]$$

StoreEr
$$\vdash_\dagger [x \not\mapsto]\ [x] := y\ [er\colon x \not\mapsto]$$

StoreNull
$$\vdash_\dagger [x{=}\mathsf{null}]\ [x] := y\ [er\colon x{=}\mathsf{null}]$$

Load
$$\vdash_\dagger [x{=}x' * y \mapsto e]\ x := [y]\ [ok\colon x{=}e[x'/x] * y \mapsto e[x'/x]]$$

LoadEr
$$\vdash_\dagger [y \not\mapsto]\ x := [y]\ [er\colon y \not\mapsto]$$

LoadNull
$$\vdash_\dagger [y{=}\mathsf{null}]\ x := [y]\ [er\colon y{=}\mathsf{null}]$$

Frame
$$\frac{\vdash_\dagger [p]\ \mathsf{C}\ [\epsilon : q] \qquad \mathsf{mod}(\mathsf{C}) \cap \mathsf{fv}(r){=}\emptyset}{\vdash_\dagger [p * r]\ \mathsf{C}\ [\epsilon : q * r]}$$

Div-Frame
$$\frac{\vdash [p]\ \mathsf{C}\ [\infty]}{\vdash [p * r]\ \mathsf{C}\ [\infty]}$$

Fig. 9. UNTer$^{\text{SL}}$ proof rules where x and x' are distinct variables and $\dagger$ in each rule can be instantiated as F or B; all UNTer rules in Fig. 2 (except Assign, Constancy) and Fig. 3 are also valid in UNTer$^{\text{SL}}$ and are omitted.

(imported from UNTer) are standard and omitted; e.g. the semantics of $e \oplus e'$ is given as the set of pairs of the form $(s, \emptyset)$ such that $s(e) \oplus s(e')$ holds, where $\emptyset$ is the empty heap (with empty domain).

Small-Step Operational Semantics. We present the UNTer$^{\text{SL}}$ operational semantic in Fig. 8 (below). As seen in SL-Local–SL-Loop, the UNTer$^{\text{SL}}$ semantics of constructs imported from UNTer are analogous to their UNTer counterparts and are simply lifted to operate on UNTer$^{\text{SL}}$ states.

The remaining transitions pertain to heap-manipulating operations. Specifically, SL-Alloc describes executing $x := \mathsf{alloc}()$, where a previously unallocated location l is picked, the underlying heap is extended with l, and x is updated in the store to record l. Similarly, SL-AllocFree describes re-allocating a location l that was previously deallocated (i.e. $h(l) = \bot$). The SL-Free transition describes successfully deallocating the memory at x: when x holds location l ($s(x) = l$) and l is allocated in the memory ($h(l) \in \text{Val}$), then l is deallocated by updating its value to $\bot$ in the heap. Conversely, SL-Free describes when deallocating the memory at x fails, namely when either x holds null or x holds a location that has already been deallocated, in which case the underlying state is unchanged. Analogously, SL-Load and SL-LoadEr respectively describe reading from memory via $x := [y]$ successfully (when y holds an allocated location) and erroneously (when y holds either null or a deallocated location). Finally, SL-Store and SL-StoreEr respectively describe writing to memory successfully and erroneously.

$$
\begin{array}{rcl}
(\!|.|\!) & : & \textsc{Ast} \to \mathcal{P}(\textsc{State}^{\text{SL}}) \\
(\!|\mathsf{emp}|\!) & \triangleq & \left\{ (s,h) \;\middle|\; dom(h) = \emptyset \right\} \\
(\!|e \mapsto e'|\!) & \triangleq & \left\{ (s,h) \;\middle|\; dom(h) = \{s(e)\} \land h(s(e)) = s(e') \neq \bot \right\} \\
(\!|e \not\mapsto\ |\!) & \triangleq & \left\{ (s,h) \;\middle|\; dom(h) = \{s(e)\} \land h(s(e)) = \bot \right\} \\
(\!|p * q|\!) & \triangleq & \left\{ \sigma_p \circ \sigma_q \;\middle|\; \sigma_p \in (\!|p|\!) \land \sigma_q \in (\!|q|\!) \right\}
\end{array}
$$

$$
\text{where} \qquad (s,h) \circ (s',h') \triangleq \begin{cases} (s, h \uplus h') & \text{if } s = s' \land dom(h_1) \cap dom(h_2) = \emptyset \land \mathsf{wf}(h \uplus h') \\ \text{undefined} & \text{otherwise} \end{cases}
$$

$$
\textsc{SL-Local}\ \frac{s' = s[x \mapsto v] \qquad v \in \textsc{Val}}{\mathsf{local}\ x\ \mathsf{in}\ \mathsf{C}, (s,h) \to \mathsf{C}; \mathsf{end}(x, s(x)), (s', h)}
\qquad
\textsc{SL-LocalEnd}\ \frac{s' = s[x \mapsto v]}{\mathsf{end}(x, v), (s,h) \to \mathsf{skip}, (s', h)}
\qquad
\textsc{SL-Assign}\ \frac{s' = s[x \mapsto s(e)]}{x := e, (s,h) \to \mathsf{skip}, (s', h), \mathit{ok}}
$$

$$
\textsc{SL-Assume}\ \frac{\sigma = (s, -) \qquad s(B) = \mathsf{true}}{\mathsf{assume}(B), \sigma \to \mathsf{skip}, \sigma, \mathit{ok}}
\qquad
\textsc{SL-Error}\ \ \mathsf{error}, \sigma \to \mathsf{skip}, \sigma, \mathit{er}
\qquad
\textsc{SL-Choice}\ \frac{i \in \{1, 2\}}{\mathsf{C}_1 + \mathsf{C}_2, \sigma \to \mathsf{C}_i, \sigma, \mathit{ok}}
$$

$$
\textsc{SL-Seq1}\ \frac{\mathbb{C}_1, \sigma \to \mathbb{C}_1', \sigma', \epsilon}{\mathbb{C}_1; \mathbb{C}_2, \sigma \to \mathbb{C}_1'; \mathbb{C}_2, \sigma', \epsilon}
\qquad
\textsc{SL-SeqSkip}\ \ \mathsf{skip}; \mathbb{C}, \sigma \to \mathbb{C}, \sigma, \mathit{ok}
\qquad
\textsc{SL-Loop0}\ \ \mathsf{C}^\star, \sigma \to \mathsf{skip}, \sigma, \mathit{ok}
\qquad
\textsc{SL-Loop}\ \ \mathsf{C}^\star, \sigma \to \mathsf{C}; \mathsf{C}^\star, \sigma, \mathit{ok}
$$

$$
\textsc{SL-Alloc}\ \frac{l \notin dom(h) \qquad h' = h \uplus [l \mapsto v] \qquad s' = s[x \mapsto l]}{x := \mathsf{alloc}(), (s,h) \to \mathsf{skip}, (s', h'), \mathit{ok}}
\qquad
\textsc{SL-AllocFree}\ \frac{h(l) = \bot \quad h' = h[l \mapsto v] \quad s' = s[x \mapsto l]}{x := \mathsf{alloc}(), (s,h) \to \mathsf{skip}, (s', h'), \mathit{ok}}
$$

$$
\textsc{SL-Free}\ \frac{s(x) = l \quad h(l) \in \textsc{Val} \quad h' = h[l \mapsto \bot]}{\mathsf{free}(x), (s,h) \to \mathsf{skip}, (s, h'), \mathit{ok}}
\qquad
\textsc{SL-FreeEr}\ \frac{s(x) = \mathsf{null} \lor h(s(x)) = \bot}{\mathsf{free}(x), (s,h) \to \mathsf{skip}, (s, h), \mathit{er}}
\qquad
\textsc{SL-Load}\ \frac{h(s(y)) = v \in \textsc{Val} \quad s' = s[x \mapsto v]}{x := [y], (s,h) \to \mathsf{skip}, (s', h), \mathit{ok}}
$$

$$
\textsc{SL-LoadEr}\ \frac{s(y) = \mathsf{null} \lor h(s(y)) = \bot}{x := [y], (s,h) \to \mathsf{skip}, (s, h), \mathit{er}}
\qquad
\textsc{SL-Store}\ \frac{s(y) = l \quad h(l) \in \textsc{Val} \quad h' = h[l \mapsto s(y)]}{[x] := y, (s,h) \to \mathsf{skip}, (s, h'), \mathit{ok}}
\qquad
\textsc{SL-StoreEr}\ \frac{s(x) = \mathsf{null} \lor h(s(x)) = \bot}{[x] := y, (s,h) \to \mathsf{skip}, (s, h), \mathit{er}}
$$

Fig. 10. The semantics of UNTer$^{\text{SL}}$ assertions (above); the UNTer$^{\text{SL}}$ small-step operational semantics (below)

F UNTER$^{\text{SL}}$ SOUNDNESS

Definition 3.

$$s_1 \sim_A s_2 \overset{\text{def}}{\iff} \forall x \in A.\ s_1(x){=}s_2(x)$$

Definition 4.

$$\begin{aligned} h_p \ \#\ h &\overset{\text{def}}{\iff} dom(h_p) \cap dom(h){=}\emptyset \\ \sigma_p \ \#\ \sigma &\overset{\text{def}}{\iff} \exists \sigma'.\ \sigma_p \circ \sigma = \sigma' \end{aligned}$$

Intuitively, $h_p \ \#\ h$ (resp. $\sigma_p \ \#\ \sigma$) denotes that h_p and h (resp. σ_p and σ) are *compatible* in that their composition is defined.

Proposition 19. *For all assertions p and all s, s', h, if $(s, h) \in p$ and $s \sim_{\mathsf{fv}(p)} s'$, then $(s', h) \in p$. For all ϵ, C, x, v, n, (s_1, h_1) and (s_2, h_2), if $\mathsf{C}, (s_1, h_1) \xrightarrow{n} -, (s_2, h_2), \epsilon$ and $x \notin \mathsf{fv}(\mathsf{C})$, then $\mathsf{C}, ((s_1[x \mapsto v], h_1) \xrightarrow{n} -, (s_2[x \mapsto v], h_2)), \epsilon$.*

F.1 BUA Soundness in UNTER$^{\text{SL}}$

Lemma 15. *For all $n, \sigma, \sigma', \mathsf{C}, \mathsf{C}'$, if $\mathsf{C}, \sigma \xrightarrow{n} \mathsf{C}', \sigma', ok$, then $\mathsf{C}' = \mathsf{skip}$.*

Proof. The proof of this lemma is analogous to that of Lemma 1 and is omitted here. □

Lemma 16. *For all p, C:*
if $\forall n \in \mathbb{N}, (s, h_p) \in p(n), h.\ \ h_p \ \#\ h \Rightarrow \exists (s', h_q) \in p(n{+}1), j.\ s \sim_{\overline{\mathsf{mod}(\mathsf{C})}} s' \land \mathsf{C}, (s, h_p \uplus h) \xrightarrow{j} -, (s', h_q \uplus h), ok$,
then $\forall k, i \in \mathbb{N}, (s, h_p) \in p(i), h.\ h_p \ \#\ h \Rightarrow \exists (s', h_q) \in p(i{+}k), j.\ s \sim_{\overline{\mathsf{mod}(\mathsf{C}^\star)}} s' \land \mathsf{C}^\star, (s, h_p \uplus h) \xrightarrow{j} -, (s', h_q \uplus h), ok$.

Proof. Pick arbitrary p, C such that:

$$\forall n{\in}\mathbb{N}, (s, h_p){\in}p(n), h.\ h_p \# h \Rightarrow \exists (s', h_q){\in}p(n{+}1), j.\ s \sim_{\overline{\mathsf{mod}(\mathsf{C})}} s' {\land} \mathsf{C}, (s, h_p {\uplus} h) \xrightarrow{j} -, (s', h_q {\uplus} h), ok \tag{13}$$

We proceed by induction on k.

Base case $k{=}0$
Pick an arbitrary $i \in \mathbb{N}$, $(s, h_p) \in p(i)$ and h such that $h_p \ \#\ h$. We then simply have $s \sim_{\overline{\mathsf{mod}(\mathsf{C}^\star)}} s$. From S-Loop0 we have $\mathsf{C}^\star, (s, h_p \uplus h) \to \mathsf{skip}, (s, h_p \uplus h), ok$. As such, as we have $\mathsf{skip}, (s, h_p \uplus h) \xrightarrow{0} \mathsf{skip}, (s, h_p \uplus h), ok$ (from the definition of $\xrightarrow{0}$), by definition we have $\mathsf{C}^\star, (s, h_p \uplus h) \xrightarrow{1} \mathsf{skip}, (s, h_p \uplus h), ok$. Consequently, we have $(s, h_p) \in p(i)$ and $\mathsf{C}^\star, (s, h_p \uplus h) \xrightarrow{1} \mathsf{skip}, (s, h_p \uplus h), ok$, as required.

Inductive case $k{=}j{+}1$

$$\forall i{\in}\mathbb{N}, (s, h_p){\in}p(i), h.\ h_p \# h \Rightarrow \exists (s', h_q){\in}p(i{+}j), m.\ s \sim_{\overline{\mathsf{mod}(\mathsf{C}^\star)}} s' \land \mathsf{C}^\star, (s, h_p \uplus h) \xrightarrow{m} -, (s', h_q \uplus h), ok \tag{I.H}$$

Pick an arbitrary $i \in \mathbb{N}$, $(s, h_p) \in p(i)$ and h such that $h_p \ \#\ h$. From (13) and since $(s, h_p) \in p(i)$ we know there exists $(s_i, h_i) \in p(i{+}1)$ and m such that $s \sim_{\overline{\mathsf{mod}(\mathsf{C})}} s_i$ and $\mathsf{C}, (s, h_p {\uplus} h) \xrightarrow{m} -, (s_i, h_i {\uplus} h), ok$. That is, $h_i \ \#\ h$. As $s \sim_{\overline{\mathsf{mod}(\mathsf{C})}} s_i$ and $\mathsf{mod}(\mathsf{C}) = \mathsf{mod}(\mathsf{C}^\star)$, we also have $s \sim_{\overline{\mathsf{mod}(\mathsf{C}^\star)}} s_i$.

On the other hand, since $(s_i, h_i) \in p(i{+}1)$ and $h_i \ \#\ h$, from (I.H) we know there exists $(s', h_q) \in p(i{+}1{+}j)$ and b such that $s_i \sim_{\overline{\mathsf{mod}(\mathsf{C}^\star)}} s' {\land} \mathsf{C}^\star, (s_i, h_i {\uplus} h) \xrightarrow{b} -, (s', h_q {\uplus} h), ok$. That is, $(s', h_q) \in p(i{+}k)$.

Therefore, from Lemma 2, $\mathsf{C}, (s, h_p \uplus h) \xrightarrow{m} -, (s_i, h_i \uplus h), ok$ and $\mathsf{C}^\star, (s_i, h_i \uplus h), \xrightarrow{b} -, (s', h_q \uplus h), ok$ we know there exists c such that $\mathsf{C}; \mathsf{C}^\star, (s, h_p \uplus h), \xrightarrow{c} -, (s', h_q \uplus h), ok$.

Furthermore, from S-Loop we simply have $\mathsf{C}^\star, (s, h_p \uplus h), \rightarrow \mathsf{C}; \mathsf{C}^\star, (s, h_p \uplus h), ok$. As such, since we also have $\mathsf{C}; \mathsf{C}^\star, (s, h_p \uplus h), \xrightarrow{c} -, (s', h_q \uplus h), ok$, from the definition of $\xrightarrow{c+1}$ we have $\mathsf{C}^\star, (s, h_p \uplus h), \xrightarrow{c+1} -, (s', h_q \uplus h), ok$. Finally, since $s \sim_{\overline{\mathsf{mod}(\mathsf{C}^\star)}} s_i$ and $s_i \sim_{\overline{\mathsf{mod}(\mathsf{C}^\star)}} s'$, we also have $s \sim_{\overline{\mathsf{mod}(\mathsf{C}^\star)}} s'$. That is, we have $(s', h_q) \in p(i+k)$, $s \sim_{\overline{\mathsf{mod}(\mathsf{C}^\star)}} s'$ and $\mathsf{C}^\star, (s, h_p \uplus h), \xrightarrow{c+1} -, (s', h_q \uplus h), ok$, as required. □

Lemma 17. *For all $p, \mathsf{C}, q, \epsilon$, if $\vdash_{\mathsf{B}} [p]\ \mathsf{C}\ [\epsilon : q]$ can be derived using the proof rules in Fig. 9, then:*

$$\begin{aligned}&\forall (s_p, h_p) \in p.\ \forall h.\ h_p \ \#\ h \implies \\ &\qquad \exists (s_q, h_q) \in q, n.\ s_p \sim_{\overline{\mathsf{mod}(\mathsf{C})}} s_q \land \mathsf{C}, (s_p, h_p \uplus h) \xrightarrow{n} -, (s_q, h_q \uplus h), \epsilon\end{aligned}$$

Proof. By induction on the structure of rules in Fig. 9.

Case Skip
Pick an arbitrary $\sigma_p = (s, h_p) \in p$ and an arbitrary h such that $h_p \ \#\ h$. It then suffices to show that $\mathsf{skip}, (s, h_p \uplus h) \xrightarrow{0} \mathsf{skip}, (s, h_p \uplus h), ok$, which follows from the definition of $\xrightarrow{0}$ immediately.

Case AssignSL
Pick an arbitrary $\sigma_p \in x = x'$ and an arbitrary h such that $h_p \ \#\ h$. That is, there exists s such that $\sigma_p = (s, \emptyset)$. Let $s(x) = v_x$, $s(e) = v_e$ and $s' = s[x \mapsto v_e]$. As $\sigma_p = (s, \emptyset) \in x = x'$ we also have $s(x') = v_x$. As $\mathsf{mod}(x := e) = \{x\}$, by definition of s' we have $s \sim_{\overline{\mathsf{mod}(x := e)}} s'$. From SL-Assign we then have $x := e, (s, h) \rightarrow \mathsf{skip}, (s', h), ok$. As such, since we also have $\mathsf{skip}, (s', h) \xrightarrow{0} \mathsf{skip}, (s', h), ok$, by definition we have $x := e, (s, h) \xrightarrow{1} \mathsf{skip}, (s', h), ok$, i.e. $x := e, (s, \emptyset \uplus h) \xrightarrow{1} \mathsf{skip}, (s', \emptyset \uplus h), ok$

As $s(x) = s(x') = v_x$ and $s(e) = v_e$, by definition we have $s(e[x'/x]) = v_e$ and $s'(e[x'/x]) = v_e$. As $s'(e[x'/x]) = v_e$ and $s' = s[x \mapsto v_e]$ (i.e. $s'(x) = v_e$), we have $(s', \emptyset) \in x = e[x'/x]$. Therefore, we have $(s', \emptyset) \in x = e[x'/x]$, $s \sim_{\overline{\mathsf{mod}(x := e)}} s'$ and $x := e, (s, \emptyset \uplus h) \xrightarrow{1} \mathsf{skip}, (s', \emptyset \uplus h), ok$, as required.

Case Assume
Pick arbitrary p, B such that $\vdash_{\mathsf{B}} \big[p \land B\big]\ \mathsf{assume}(B)\ \big[ok\!: p \land B\big]$. Pick an arbitrary $(s, h_p) \in p \land B$ and an arbitrary h such that $h_p \ \#\ h$. By definition we then know $s(B) = \mathsf{true}$. As $\mathsf{mod}(\mathsf{assume}(B)) = \emptyset$, by definition we have $s \sim_{\overline{\mathsf{mod}(\mathsf{assume}(B))}} s$. From S-Assume we then have $\mathsf{assume}(B), (s, h_p \uplus h) \rightarrow \mathsf{skip}, (s, h_p \uplus h), ok$. As such, since we also have $\mathsf{skip}, (s, h_p \uplus h) \xrightarrow{0} \mathsf{skip}, (s, h_p \uplus h), ok$, by definition we have $\mathsf{assume}(B), (s, h_p \uplus h) \xrightarrow{1} \mathsf{skip}, (s, h_p \uplus h), ok$. Consequently, we have $(s, h_p) \in p \land B$, $s \sim_{\overline{\mathsf{mod}(\mathsf{assume}(B))}} s$ and $\mathsf{assume}(B), (s, h_p \uplus h) \xrightarrow{1} \mathsf{skip}, (s, h_p \uplus h), ok$, as required.

Case AssumeSL
This rule can be immediately derived from Assume (proved above) by picking $p \triangleq \mathsf{true}$.

Case Error
Pick arbitrary p such that $\vdash_{\mathsf{B}} [p]\ \mathsf{error}\ [er\!: p]$. Pick an arbitrary $(s, h_p) \in p$ and an arbitrary h such that $h_p \ \#\ h$. Let $\sigma = (s, h_p \uplus h)$. From S-Error we then have $\mathsf{error}, \sigma \rightarrow \mathsf{skip}, \sigma, er$. As such, since $(s, h_p) \in p$, by definition we have $\mathsf{error}, \sigma \xrightarrow{1} \mathsf{skip}, \sigma, er$, as required. Moreover, as $\mathsf{mod}(\mathsf{error}) = \emptyset$ we also have $s \sim_{\overline{\mathsf{mod}(\mathsf{error})}} s$, as required.

Case Seq
Pick arbitrary $p, q, r, \mathsf{C}_1, \mathsf{C}_2, \epsilon$ such that $\vdash_B [p]\ \mathsf{C}_1\ [ok\colon r]$ and $\vdash_B [r]\ \mathsf{C}_2\ [\epsilon : q]$. Pick an arbitrary $(s, h_p) \in p$ and an arbitrary h such that $h_p \# h$. From $\vdash_B [p]\ \mathsf{C}_1\ [ok\colon r]$ and the inductive hypothesis we then know there exists $(s_r, h_r) \in r, i$ such that $s \sim_{\overline{\mathsf{mod}(\mathsf{C}_1)}} s_r$ and $\mathsf{C}_1, (s, h_p \uplus h) \xrightarrow{i} -, (s_r, h_r \uplus h), ok$. Moreover, as $(s_r, h_r) \in r, i$, from $\vdash_B [r]\ \mathsf{C}_2\ [\epsilon : q]$ and the inductive hypothesis we know there exists $(s', h_q) \in q, j$ such that $s_r \sim_{\overline{\mathsf{mod}(\mathsf{C}_2)}} s'$ and $\mathsf{C}_2, (s_r, h_r \uplus h) \xrightarrow{j} -, (s', h_q \uplus h), \epsilon$. As $s \sim_{\overline{\mathsf{mod}(\mathsf{C}_1)}} s_r$ and $s_r \sim_{\overline{\mathsf{mod}(\mathsf{C}_2)}} s'$, by definition we also have $s \sim_{\overline{\mathsf{mod}(\mathsf{C}_1;\mathsf{C}_2)}} s_r$ and $s_r \sim_{\overline{\mathsf{mod}(\mathsf{C}_1;\mathsf{C}_2)}} s'$, and thus we also have $s \sim_{\overline{\mathsf{mod}(\mathsf{C}_1;\mathsf{C}_2)}} s'$. On the other hand, as $\mathsf{C}_1, (s, h_p \uplus h) \xrightarrow{i} -, (s_r, h_r \uplus h), ok$ and $\mathsf{C}_2, (s_r, h_r \uplus h) \xrightarrow{j} -, (s', h_q \uplus h), \epsilon$, from Lemma 2 we know there exists n such that $\mathsf{C}_1; \mathsf{C}_2, (s, h_p \uplus h) \xrightarrow{n} -, (s', h_q \uplus h), \epsilon$. That is, there exists $(s', h_q) \in q, n$ such that $s \sim_{\overline{\mathsf{mod}(\mathsf{C}_1;\mathsf{C}_2)}} s'$, $\mathsf{C}_1; \mathsf{C}_2, (s, h_p \uplus h) \xrightarrow{n} -, (s', h_q \uplus h), \epsilon$, as required.

Case SeqEr
Pick arbitrary $p, q, \mathsf{C}_1, \mathsf{C}_2$ such that $\vdash_B [p]\ \mathsf{C}_1; \mathsf{C}_2\ [er\colon q]$. Pick an arbitrary $(s, h_p) \in p$ and an arbitrary h such that $h_p \# h$. From the $\vdash_B [p]\ \mathsf{C}_1\ [er\colon q]$ premise and the inductive hypothesis we then know there exists $(s', h_q) \in q, i$ such that $s \sim_{\overline{\mathsf{mod}(\mathsf{C}_1)}} s'$ and $\mathsf{C}_1, (s, h_p \uplus h) \xrightarrow{i} -, (s', h_q \uplus h), er$. As such, from Lemma 3 we know $\mathsf{C}_1; \mathsf{C}_2, (s, h_p \uplus h) \xrightarrow{i} -, (s', h_q \uplus h), er$, as required.

Case Choice
Pick arbitrary $p, q, \mathsf{C}_1, \mathsf{C}_2, \epsilon$ and $i \in \{1, 2\}$ such that $\vdash_B [p]\ \mathsf{C}_1 + \mathsf{C}_2\ [\epsilon : q]$. Pick an arbitrary $(s, h_p) \in p$ and an arbitrary h such that $h_p \# h$. From the $\vdash_B [p]\ \mathsf{C}_i\ [\epsilon : q]$ premise and the inductive hypothesis we then know there exists $(s', h_q) \in q, i$ such that $s \sim_{\overline{\mathsf{mod}(\mathsf{C}_i)}} s'$ and $\mathsf{C}_i, (s, h_p \uplus h) \xrightarrow{i} -, (s', h_q \uplus h), \epsilon$. As $s \sim_{\overline{\mathsf{mod}(\mathsf{C}_i)}} s'$, by definition we also have $s \sim_{\overline{\mathsf{mod}(\mathsf{C}_1+\mathsf{C}_2)}} s'$ Moreover, from S-Choice we have $\mathsf{C}_1 + \mathsf{C}_2, (s, h_p \uplus h) \to \mathsf{C}_i, (s, h_p \uplus h), ok$. As such, from the definition of $\xrightarrow{i+1}$ we have $\mathsf{C}_1 + \mathsf{C}_2, (s, h_p \uplus h) \xrightarrow{i+1} -, (s', h_q \uplus h)', \epsilon$, as required.

Case Loop0
Pick arbitrary p, C such that $\vdash_B [p]\ \mathsf{C}^\star\ [ok\colon p]$. Pick an arbitrary $(s, h_p) \in p$ and an arbitrary h such that $h_p \# h$. From S-Loop0 we have $\mathsf{C}^\star, (s, h_p \uplus h) \to \mathsf{skip}, (s, h_p \uplus h), ok$. As such, as we have $\mathsf{skip}, (s, h_p \uplus h) \xrightarrow{0} \mathsf{skip}, (s, h_p \uplus h), ok$ (from the definition of $\xrightarrow{0}$), by definition we have $\mathsf{C}^\star, (s, h_p \uplus h) \xrightarrow{1} \mathsf{skip}, (s, h_p \uplus h), ok$. Moreover, by definition we have $s \sim_{\overline{\mathsf{mod}(\mathsf{C}^\star)}} s$, as required.

Case Loop
Pick arbitrary p, C, q such that $\vdash_B [p]\ \mathsf{C}^\star\ [\epsilon : q]$. Pick an arbitrary $(s, h_p) \in p$ and an arbitrary h such that $h_p \# h$. From the $\vdash_B [p]\ \mathsf{C}^\star; \mathsf{C}\ [\epsilon : q]$ premise and the inductive hypothesis we know there exists $(s', h_q) \in q, j$ such that $s \sim_{\overline{\mathsf{mod}(\mathsf{C}^\star;\mathsf{C})}} s'$ and $\mathsf{C}^\star; \mathsf{C}, (s, h_p \uplus h) \xrightarrow{j} -, (s', h_q \uplus h), \epsilon$. As $s \sim_{\overline{\mathsf{mod}(\mathsf{C}^\star;\mathsf{C})}} s'$, by definition we also have $s \sim_{\overline{\mathsf{mod}(\mathsf{C}^\star)}} s'$. On the other hand, from Lemma 5 we then know there exists i such that $\mathsf{C}; \mathsf{C}^\star, (s, h_p \uplus h) \xrightarrow{i} -, (s', h_q \uplus h), \epsilon$. From S-Loop we have $\mathsf{C}^\star, (s, h_p \uplus h) \to \mathsf{C}; \mathsf{C}^\star, (s', h_q \uplus h), ok$. As such, from the definition of $\xrightarrow{i+1}$ we have $\mathsf{C}^\star, (s, h_p \uplus h) \xrightarrow{i+1} -, (s', h_q \uplus h), \epsilon$, as required.

Case Loop-Subvariant
Pick p, C, k such that $\vdash_{\mathrm{B}} \big[p(0)\big]\ \mathsf{C}^\star\ \big[ok\colon p(k)\big]$. Pick arbitrary $(s, h_p) \in p(0)$ and h such that $h_p \# h$. From the $\forall n \in \mathbb{N}.\ \vdash_{\mathrm{B}} \big[p(n)\big]\ \mathsf{C}\ \big[ok\colon p(n{+}1)\big]$ premise and the inductive hypothesis we know:

$$\forall n \in \mathbb{N}, (s, h_p) \in p(n), h.\ h_p \# h \Rightarrow \exists (s', h_q) \in p(n{+}1), j.\ s \sim_{\overline{\mathsf{mod}(\mathsf{C})}} s' \land \mathsf{C}, (s, h_p \uplus h) \xrightarrow{j} -, (s', h_q \uplus h), ok$$

Consequently, from Lemma 16 we know there exists $(s', h_q) \in p(k)$ and j such that $s \sim_{\overline{\mathsf{mod}(\mathsf{C}^\star)}} s'$ and $\mathsf{C}^\star, (s, h_p \uplus h) \xrightarrow{j} -, (s', h_q \uplus h), ok$, as required.

Case Local
Pick arbitrary $p, \mathsf{C}, q, \epsilon$ such that $\vdash_{\mathrm{B}} [\exists x.\ p]\ \mathsf{local}\ x\ \mathsf{in}\ \mathsf{C}\ [\epsilon : \exists x.\ q]$. Pick an arbitrary $(s, h_p) \in \exists x.\ p$ and an arbitrary h such that $h_p \# h$; i.e. there exists v, s_p such that $s_p = s[x \mapsto v]$ and $(s_p, h_p) \in p$. From the $\vdash_{\mathrm{B}} [p]\ \mathsf{C}\ [\epsilon : q]$ premise and the inductive hypothesis we know there exists $(s_q, h_q) \in q$ and n such that $s_p \sim_{\overline{\mathsf{mod}(\mathsf{C})}} s_q$ and $\mathsf{C}, (s_p, h_p \uplus h) \xrightarrow{n} -, (s_q, h_q \uplus h), \epsilon$. From S-Local we have $\mathsf{local}\ x\ \mathsf{in}\ \mathsf{C}, (s, h_p \uplus h) \to \mathsf{C}; \mathsf{end}(x, s(x)), (s_p, h_p \uplus h)$. There are now two cases to consider: 1) $\epsilon{=}ok$; or 2) $\epsilon{=}er$.

In case (1), let $s'' = s_q[x \mapsto s(x)]$. Consequently, as $s_p \sim_{\overline{\mathsf{mod}(\mathsf{C})}} s_q$ and $s''(x) = s(x)$, from the definitions of s_p and s'' we also have $s \sim_{\overline{\mathsf{mod}(\mathsf{local}\ x\ \mathsf{in}\ \mathsf{C})}} s''$. From S-LocalEnd we then have $\mathsf{end}(x, s(x)), (s_q, h_q \uplus h) \to \mathsf{skip}, (s'', h_q \uplus h)$. From the definition of $\xrightarrow{0}$ we have $\mathsf{skip}, (s'', h_q \uplus h) \xrightarrow{0} \mathsf{skip}, (s'', h_q \uplus h), ok$, and thus since we have $\mathsf{end}(x, s(x)), (s_q, h_q \uplus h) \to \mathsf{skip}, (s'', h_q \uplus h)$, from the definition of $\xrightarrow{1}$ we have $\mathsf{end}(x, s(x)), (s_q, h_q \uplus h) \xrightarrow{1} \mathsf{skip}, (s'', h_q \uplus h)$. Consequently, since we also have $\mathsf{C}, (s_p, h_p \uplus h) \xrightarrow{n} -, (s_q, h_q \uplus h), \epsilon$, from Lemma 2 we know there exists m such that $\mathsf{C}; \mathsf{end}(x, s(x)), (s_p, h_p \uplus h) \xrightarrow{m} \mathsf{skip}, (s'', h_q \uplus h), ok$. On the other hand, since we have $\mathsf{local}\ x\ \mathsf{in}\ \mathsf{C}, (s, h_p \uplus h) \to \mathsf{C}; \mathsf{end}(x, s(x)), (s_p, h_p \uplus h)$, by definition of $\xrightarrow{m+1}$ we also have $\mathsf{local}\ x\ \mathsf{in}\ \mathsf{C}, (s, h_p \uplus h) \xrightarrow{m+1} \mathsf{skip}, (s'', h_q \uplus h), ok$. Finally, as $(s_q, h_q) \in q$ and $s'' = s_q[x \mapsto s(x)]$, by definition we also have $(s'', h_q) \in \exists x.\ q$, as required.

In case (2), from $\mathsf{C}, (s_p, h_p \uplus h) \xrightarrow{n} -, (s_q, h_q \uplus h), \epsilon$ and Lemma 3 we have $\mathsf{C}; \mathsf{end}(x, s(x)), (s_p, h_p \uplus h) \xrightarrow{n} -, (s_q, h_q \uplus h), \epsilon$. On the other hand, since we have $\mathsf{local}\ x\ \mathsf{in}\ \mathsf{C}, (s, h_p \uplus h) \to \mathsf{C}; \mathsf{end}(x, s(x)), (s_p, h_p \uplus h)$, by definition of $\xrightarrow{n+1}$ we also have $\mathsf{local}\ x\ \mathsf{in}\ \mathsf{C}, (s, h_p \uplus h) \xrightarrow{n+1} -, (s_q, h_q \uplus h), \epsilon$. Moreover, as $s_p = s[x \mapsto v]$, $\mathsf{mod}(\mathsf{local}\ x\ \mathsf{in}\ \mathsf{C}) = \mathsf{mod}(\mathsf{C}) \cup \{x\}$ and $s_p \sim_{\overline{\mathsf{mod}(\mathsf{C})}} s_q$, by definition we also have $s \sim_{\overline{\mathsf{mod}(\mathsf{local}\ x\ \mathsf{in}\ \mathsf{C})}} s_q$. Finally, as $(s_q, h_q) \in q$, by definition we also have $(s_q, h_q) \in \exists x.\ q$, as required.

Case Disj
Pick arbitrary $p_1, p_2, q_1, q_2, \mathsf{C}$ such that $\vdash_{\mathrm{B}} [p_1 \lor p_2]\ \mathsf{C}\ [\epsilon : q_1 \lor q_2]$. Pick an arbitrary $(s, h_p) \in p_1 \lor p_2$ and an arbitrary h such that $h_p \# h$. There are then two cases to consider: 1) $(s, h_p) \in p_1$; or 2) $(s, h_p) \in p_2$.

In case (1), from the $\vdash_{\mathrm{B}} [p_1]\ \mathsf{C}\ [\epsilon : q_1]$ premise and the inductive hypothesis we know there exists $(s', h_q) \in q_1, n$ such that $s \sim_{\overline{\mathsf{mod}(\mathsf{C})}} s'$, $\mathsf{C}, (s, h_p \uplus h) \xrightarrow{n} -, (s', h_q \uplus h), \epsilon$. That is, there exists $(s', h_q) \in q_1 \lor q_2$ and n such that $s \sim_{\overline{\mathsf{mod}(\mathsf{C})}} s'$, $\mathsf{C}, (s, h_p \uplus h) \xrightarrow{n} -, (s', h_q \uplus h), \epsilon$, as required. The proof of case (2) is analogous and omitted.

Case DisjTrack
Pick arbitrary $P_1, P_2, Q_1, Q_2, \mathsf{C}$ such that $\vdash_{\mathrm{B}} [P_1 \uplus P_2]\ \mathsf{C}\ [\epsilon : Q_1 \uplus Q_2]$. Pick an arbitrary $i \in dom(P_1 \uplus$

P_2), $(s, h_p) \in (P_1 \uplus P_2)(i)$ and an arbitrary h such that $h_p \ \# \ h$. We then know that either $i \in dom(P_1)$ or $i \in dom(P_2)$. Without loss of generality, let us assume $i \in dom(P_1)$.

As $(s, h_p) \in (P_1 \uplus P_2)(i)$ and $i \in dom(P_1)$, we then have $(s, h_p) \in P_1(i)$. From the $\vdash_{\mathrm{B}}$ $[P_1]$ C $[\epsilon : Q_1]$ premise, the definition of merged triples premise and the inductive hypothesis we know there exists $(s', h_q) \in Q_1(i), n$ such that $s \sim_{\overline{\mathsf{mod}(\mathsf{C})}} s'$ and C, $(s, h_p \uplus h) \xrightarrow{n} -, (s', h_q \uplus h), \epsilon$. That is, there exists $(s', h_q) \in (Q_1 \uplus Q_2)(i)$ and n such that $s \sim_{\overline{\mathsf{mod}(\mathsf{C})}} s'$ and C, $(s, h_p \uplus h) \xrightarrow{n} -, (s', h_q \uplus h), \epsilon$, as required.

Case Cons

Pick arbitrary P, Q, C, I such that $\vdash_{\mathrm{B}}$ $[P \downarrow I]$ C $[\epsilon : Q \downarrow I]$. Pick an arbitrary $i \in dom(P \downarrow I)$; that is, from the $I \subseteq dom(P)$ we know $i \in dom(P) \cap I$, i.e. $i \in dom(P)$ and $i \in I$. Pick an arbitrary $(s, h_p) \in P(i)$ and an arbitrary h such that $h_p \ \# \ h$. From the $\vdash_{\mathrm{B}}$ $[P]$ C $[\epsilon : Q]$ premise, the definition of merged triples and the inductive hypothesis we know there exists $(s', h_q) \in Q(i)$ and n such that $s \sim_{\overline{\mathsf{mod}(\mathsf{C})}} s'$ and C, $(s, h_p \uplus h) \xrightarrow{n} -, (s', h_q \uplus h), \epsilon$. As $i \in I$ and $i \in dom(Q)$, we know $i \in dom(Q \downarrow I)$. That is, there exists $i \in dom(Q \downarrow I)$, $(s', h_q) \in (Q \downarrow I)(i)$ and n such that $s \sim_{\overline{\mathsf{mod}(\mathsf{C})}} s'$ and C, $(s, h_p \uplus h) \xrightarrow{n} -, (s', h_q \uplus h), \epsilon$, as required.

Case Alloc

Pick arbitrary x, v and $(s, h_p) \in p$ and h such that $h_p \ \# \ h$. We then know $h_p \triangleq \emptyset$. Pick l such that $l \notin dom(h)$ and let $h_q{=}[l \mapsto v]$ and $s' = s[x \mapsto l]$; as such, we also have $(s', h_q) \in l \mapsto v * x = l$ and $s \sim_{\overline{\mathsf{mod}(x := \mathsf{alloc}())}} s'$. Since $l \notin dom(h)$ and $h_q{=}[l \mapsto v]$, by definition of # we also know $h_q \ \# \ h$. From SL-Alloc we then have $x :=$ alloc(), $(s, h_p \uplus h) \longrightarrow$ skip, $(s', h_q \uplus h)$, *ok*, and since we also have skip, $(s', h_q \uplus h) \xrightarrow{0}$ skip, $(s', h_q \uplus h)$, *ok*, by definition of $\xrightarrow{1}$ we have $x :=$ alloc(), $(s, h_p \uplus h) \xrightarrow{1}$ skip, $(s', h_q \uplus h)$, *ok*, as required.

Case AllocFree

Pick arbitrary x, y and $(s, h_p) \in p$ and h such that $h_p \ \# \ h$. We then know there exists l such that $s(y){=}l$ and $h_p \triangleq [l \mapsto \perp]$. Let $h_q{=}[l \mapsto v]$ and $s' = s[x \mapsto l]$; as such, we also have $(s', h_q) \in y \mapsto v * x = y$ and $s \sim_{\overline{\mathsf{mod}(x := \mathsf{alloc}())}} s'$. Since $h_p \ \# \ h$ and $dom(h_p){=}dom(h_q)$, by definition of # we also know $h_q \ \# \ h$. From SL-AllocFree we then have $x :=$ alloc(), $(s, h_p \uplus h) \longrightarrow$ skip, $(s', h_q \uplus h)$, *ok*, and since we also have skip, $(s', h_q \uplus h) \xrightarrow{0}$ skip, $(s', h_q \uplus h)$, *ok*, by definition of $\xrightarrow{1}$ we have $x :=$ alloc(), $(s, h_p \uplus h) \xrightarrow{1}$ skip, $(s', h_q \uplus h)$, *ok*, as required.

Case Free

Pick an arbitrary x and $(s, h_p) \in p$ and h such that $h_p \ \# \ h$. We then know there exists l, v such that $s(x){=}l$, $s(e) = v$ and $h_p \triangleq [l \mapsto v]$. Let $h_q{=}[l \mapsto \perp]$; we then have $(s, h_q) \in x \not\mapsto$ and $s \sim_{\overline{\mathsf{mod}(\mathsf{free}(x))}} s$. Since $h_p \ \# \ h$ and $dom(h_p){=}dom(h_q)$, from the definition of $\uplus$ we also know that $h_q \ \# \ h$. From SL-Free we then have free(x), $(s, h_p \uplus h) \longrightarrow$ skip, $(s, h_q \uplus h)$, *ok*, and since we also have skip, $(s, h_q \uplus h) \xrightarrow{0}$ skip, $(s, h_q \uplus h)$, *ok*, by definition of $\xrightarrow{1}$ we have free(x), $(s, h_p \uplus h) \xrightarrow{1}$ skip, $(s, h_q \uplus h)$, *ok*, as required.

Case FreeEr

Pick an arbitrary x and $(s, h_p) \in p$ and h such that $h_p \ \# \ h$. We then know there exists l such that $s(x){=}l$ and $h_p \triangleq [l \mapsto \perp]$. Let $h_q{=}h_p$; we then have $(s, h_q) \in x \not\mapsto$ and $s \sim_{\overline{\mathsf{mod}(\mathsf{free}(x))}} s$. From

SL-FreeEr we then have $\texttt{free}(x), (s, h_p \uplus h) \longrightarrow \texttt{skip}, (s, h_q \uplus h), er$, and thus by definition of $\xrightarrow{1}$ we have $\texttt{free}(x), (s, h_p \uplus h) \xrightarrow{1} \texttt{skip}, (s, h_q \uplus h), er$, as required.

Case FreeNull
Pick an arbitrary x and $(s, h_p) \in p$ and h such that $h_p \# h$. We then know $s(x)$=null and $h_p \triangleq \emptyset$. Let h_q=h_p; we then have $(s, h_q) \in x = \text{null}$ and $s \sim_{\overline{\text{mod}(\texttt{free}(x))}} s$. From SL-FreeEr we then have $\texttt{free}(x), (s, h_p \uplus h) \longrightarrow \texttt{skip}, (s, h_q \uplus h), er$, and thus by definition of $\xrightarrow{1}$ we have $\texttt{free}(x), (s, h_p \uplus h) \xrightarrow{1} \texttt{skip}, (s, h_q \uplus h), er$, as required

Case Store
Pick an arbitrary x and $(s, h_p) \in p$ and h such that $h_p \# h$. We then know there exists l, v, v_y such that $s(x)$=l, $s(y) = v_y$, $s(e) = v$ and $h_p \triangleq [l \mapsto v]$. Let h_q=$[l \mapsto v_y]$; we then have $(s, h_q) \in x \mapsto y$ and $s \sim_{\overline{\text{mod}([x] := y)}} s$. Since $h_p \# h$ and $dom(h_p)$=$dom(h_q)$, from the definition of $\uplus$ we also know that $h_q \# h$. From SL-Store we then have $[x] := y, (s, h_p \uplus h) \longrightarrow \texttt{skip}, (s, h_q \uplus h), ok$, and since we also have $\texttt{skip}, (s, h_q \uplus h) \xrightarrow{0} \texttt{skip}, (s, h_q \uplus h), ok$, by definition of $\xrightarrow{1}$ we have $[x] := y, (s, h_p \uplus h) \xrightarrow{1} \texttt{skip}, (s, h_q \uplus h), ok$, as required.

Case StoreEr
Pick an arbitrary x and $(s, h_p) \in p$ and h such that $h_p \# h$. We then know there exists l such that $s(x)$=l and $h_p \triangleq [l \mapsto \bot]$. Let h_q=h_p; we then have $(s, h_q) \in x \not\mapsto$ and $s \sim_{\overline{\text{mod}([x] := y)}} s$. From SL-StoreEr we then have $[x] := y, (s, h_p \uplus h) \longrightarrow \texttt{skip}, (s, h_q \uplus h), er$ and thus by definition of $\xrightarrow{1}$ we have $[x] := y, (s, h_p \uplus h) \xrightarrow{1} \texttt{skip}, (s, h_q \uplus h), er$, as required.

Case StoreNull
Pick an arbitrary x and $(s, h_p) \in p$ and h such that $h_p \# h$. We then know $s(x)$=null and $h_p \triangleq \emptyset$. Let h_q=h_p; we then have $(s, h_q) \in x = \text{null}$ and $s \sim_{\overline{\text{mod}([x] := y)}} s$. From SL-StoreEr we then have $[x] := y, (s, h_p \uplus h) \longrightarrow \texttt{skip}, (s, h_q \uplus h), er$, and thus by definition of $\xrightarrow{1}$ we have $[x] := y, (s, h_p \uplus h) \xrightarrow{1} \texttt{skip}, (s, h_q \uplus h), er$, as required.

Case Load
Pick arbitrary x and $(s, h_p) \in p$ and h such that $h_p \# h$. We then know there exists l, v, v_x such that $s(x) = s(x') = v_x, s(y)$=l, $s(e) = v$ and $h_p \triangleq [l \mapsto v]$. Let h_q=h_p and $s' = s[x \mapsto v]$; as such, we also have $(s', h_q) \in x = e[x'/x] * y \mapsto e[x'/x]$ and $s \sim_{\overline{\text{mod}(x := [y])}} s'$. Since $h_p \# h$ and h_p=h_q, we also know $h_q \# h$. From SL-Load we then have $x := [y], (s, h_p \uplus h) \longrightarrow \texttt{skip}, (s', h_q \uplus h), ok$, and since we also have $\texttt{skip}, (s', h_q \uplus h) \xrightarrow{0} \texttt{skip}, (s', h_q \uplus h), ok$, by definition of $\xrightarrow{1}$ we have $x := [y], (s, h_p \uplus h) \xrightarrow{1} \texttt{skip}, (s', h_q \uplus h), ok$, as required.

Case LoadEr
Pick an arbitrary y and $(s, h_p) \in p$ and h such that $h_p \# h$. We then know there exists l such that $s(y)$=l and $h_p \triangleq [l \mapsto \bot]$. Let h_q=h_p; we then have $(s, h_q) \in y \not\mapsto$ and $s \sim_{\overline{\text{mod}(x := [y])}} s$. From SL-LoadEr we then have $x := [y], (s, h_p \uplus h) \longrightarrow \texttt{skip}, (s, h_q \uplus h), er$ and thus by definition of $\xrightarrow{1}$ we

have $x := [y], (s, h_p \uplus h) \xrightarrow{1} \text{skip}, (s, h_q \uplus h), er$, as required.

Case LoadNull
Pick an arbitrary y and $(s, h_p) \in p$ and h such that $h_p \ \# \ h$. We then know $s(y)$=null and $h_p \triangleq \emptyset$. Let h_q=h_p; we then have $(s, h_q) \in y = \text{null}$ and $s \sim_{\overline{\text{mod}(x := [y])}} s$. From SL-LoadEr we then have $x := [y], (s, h_p \uplus h) \rightarrow \text{skip}, (s, h_q \uplus h), er$, and thus by definition of $\xrightarrow{1}$ we have $x := [y], (s, h_p \uplus h) \xrightarrow{1} \text{skip}, (s, h_q \uplus h), er$, as required.

Case Frame
Pick arbitrary $(s_1, h_1) \in p * r$ and h such that $h_1 \ \# \ h$. From the definition of $*$ we then know there exists h_p, h_r such that $(s_1, h_p) \in p$, $(s_1, h_r) \in r$ and $h_1 \triangleq h_p \uplus h_r$. From the definition of # and $\uplus$ we then also have $h_p \ \# \ h_r \uplus h$. On the other hand, from the premise of Frame we have $\vdash_B [p] \ \mathsf{C} \ [\epsilon : q]$ and thus from the inductive hypothesis we know there exists s_2, h_q, n such that $s_1 \sim_{\overline{\text{mod}(\mathsf{C})}} s_2$, $(s_2, h_q) \in q$ and $\mathsf{C}, (s_1, h_p \uplus h_r \uplus h) \xrightarrow{n} -, (s_2, h_q \uplus h_r \uplus h), \epsilon$. Moreover, since $s_1 \sim_{\overline{\text{mod}(\mathsf{C})}} s_2$ and as from the premise of Frame we have $\text{mod}(\mathsf{C}) \cap \text{fv}(r)$=$\emptyset$, we also have $s_1 \sim_{\text{fv}(r)} s_2$. Consequently, since $(s_1, h_r) \in r$, from Prop. 19 we have $(s_2, h_r) \in r$. As such from the definition of $*$ we have $(s_2, h_q \uplus h_r) \in q * r$. That is, we know there exists s_2 and h_2=$h_q \uplus h_r$ such that $s_1 \sim_{\overline{\text{mod}(\mathsf{C})}} s_2$, $(s_2, h_2) \in q * r$ and $\mathsf{C}, (s_1, h_1 \uplus h) \xrightarrow{n} -, (s_2, h_2 \uplus h), \epsilon$, as required. □

Lemma 18 (BUA soundness in UNTer$^{\text{SL}}$). *For all $p, \mathsf{C}, q, \epsilon$, if $\vdash_B [p] \ \mathsf{C} \ [\epsilon : q]$ is derivable using the rules in Fig. 9, then $\models_B [p] \ \mathsf{C} \ [\epsilon : q]$ holds.*

Proof. Pick arbitrary $p, \mathsf{C}, q, \epsilon$ such that $\vdash_B [p] \ \mathsf{C} \ [\epsilon : q]$ is derivable using the rules in Fig. 9. Pick an arbitrary $(s_p, h_p) \in p$. It then suffices to show there exists $(s_q, h_q) \in q$ and n such that $\mathsf{C}, (s_p, h_p) \xrightarrow{n} -, (s_q, h_q), \epsilon$.

Let $h_0 = \emptyset$ denote the empty heap (with an empty domain). From the definition of $\uplus$ and # we then know that $h_p \ \# \ h_0$. As such, from Lemma 17 we know there exists $(s_q, h_q) \in q$ and n such that $\mathsf{C}, (s_p, h_p \uplus h_0) \xrightarrow{n} -, (s_q, h_q \uplus h_0), \epsilon$. That is, there exists $(s_q, h_q) \in q$ and n such that $\mathsf{C}, (s_p, h_p) \xrightarrow{n} -, (s_q, h_q), \epsilon$, as required. □

F.2 FUA Soundness in UNTer$^{\text{SL}}$

Lemma 19. *For all $p, \mathsf{C}, q, \epsilon$, if $\vdash_B [p] \ \mathsf{C} \ [\epsilon : q]$ can be derived using the proof rules in Fig. 9, then:*

$$\forall (s_q, h_q) \in q. \ \forall h. \ h_q \ \# \ h \implies \exists (s_p, h_p) \in p, n. \ s_p \sim_{\overline{\text{mod}(\mathsf{C})}} s_q \wedge \mathsf{C}, (s_p, h_p \uplus h) \xrightarrow{n} -, (s_q, h_q \uplus h), \epsilon$$

Proof. The proof of this lemma is analogous to that of Lemma 17 and is omitted. □

Lemma 20 (FUA soundness in UNTer$^{\text{SL}}$). *For all $p, \mathsf{C}, q, \epsilon$, if $\vdash_F [p] \ \mathsf{C} \ [\epsilon : q]$ is derivable using the rules in Fig. 9, then $\models_F [p] \ \mathsf{C} \ [\epsilon : q]$ holds.*

Proof. Pick arbitrary $p, \mathsf{C}, q, \epsilon$ such that $\vdash_B [p] \ \mathsf{C} \ [\epsilon : q]$ is derivable using the rules in Fig. 9. Pick an arbitrary $(s_q, h_q) \in q$. It then suffices to show there exists $(s_p, h_p) \in p$ and n such that $\mathsf{C}, (s_p, h_p) \xrightarrow{n} -, (s_q, h_q), \epsilon$.

Let $h_0 = \emptyset$ denote the empty heap (with an empty domain). From the definition of $\uplus$ and # we then know that $h_q \ \# \ h_0$. As such, from Lemma 19 we know there exists $(s_p, h_p) \in p$ and n such that $\mathsf{C}, (s_p, h_p \uplus h_0) \xrightarrow{n} -, (s_q, h_q \uplus h_0), \epsilon$. That is, there exists $(s_p, h_p) \in p$ and n such that $\mathsf{C}, (s_p, h_p) \xrightarrow{n} -, (s_q, h_q), \epsilon$, as required. □

F.3 Divergent Soundness in UNTER$^{\text{SL}}$

Lemma 21. *For all* $\mathsf{C}, \sigma, \mathsf{C}', \sigma', \epsilon, n$, *if* $n > 0$ *and* $\mathsf{C}, \sigma \xrightarrow{n} \mathsf{C}', \sigma', \epsilon$, *then* $\mathsf{C}, \sigma \rightsquigarrow^{n} \mathsf{C}', \sigma', \epsilon$.

Proof. The proof of this lemma is analogous to that of Lemma 9 and is omitted. □

Lemma 22. *For all* $n, \mathsf{C}_1, \mathsf{C}_2, \mathsf{C}_1', \sigma, \mathsf{C}', \sigma', \epsilon$, *if* $\mathsf{C}_1, \sigma \rightsquigarrow^{n} \mathsf{C}_1', \sigma', \epsilon$, *then* $\mathsf{C}_1; \mathsf{C}_2, \sigma \rightsquigarrow^{n} \mathsf{C}_1'; \mathsf{C}_2, \sigma', \epsilon$.

Proof. The proof of this lemma is analogous to that of Lemma 10 and is omitted. □

Lemma 23. *For all* $\sigma, \sigma', \sigma'', \mathsf{C}_1, \mathsf{C}_2, \mathsf{C}', i, j, \epsilon$, *if* $\mathsf{C}_1, \sigma \xrightarrow{i} -, \sigma'', ok$ *and* $\mathsf{C}_2, \sigma'' \rightsquigarrow^{j} \mathsf{C}', \sigma', \epsilon$, *then there exists* n *such that* $\mathsf{C}_1; \mathsf{C}_2, \sigma \rightsquigarrow^{n} \mathsf{C}', \sigma', \epsilon$.

Proof. The proof of this lemma is analogous to that of Lemma 11 and is omitted. □

Lemma 24. *For all* $i, j, \mathsf{C}, \mathsf{C}', \mathsf{C}'', s, s', s'', \epsilon$, *if* $\mathsf{C}, s \rightsquigarrow^{i} \mathsf{C}'', s'', ok$ *and* $\mathsf{C}'', s'' \rightsquigarrow^{j} \mathsf{C}', s', \epsilon$, *then* $\mathsf{C}, s \rightsquigarrow^{i+j} \mathsf{C}', s', \epsilon$.

Proof. The proof of this lemma is analogous to that of Lemma 12 and is omitted. □

Lemma 25. *For all* p, C, *if* $\vdash [p]\ \mathsf{C}\ [\infty]$ *can be derived using the proof rules in Fig. 9, then:*

$$\begin{aligned} &\forall \sigma_p \in p.\ \forall \sigma.\ \sigma_p \# \sigma \implies \\ &\qquad \exists \mathsf{C}_1, \sigma_1, \mathsf{C}_2, \sigma_2, \cdots .\ \mathsf{C}, \sigma_p \circ \sigma \rightsquigarrow^{+} \mathsf{C}_1, \sigma_1, ok \rightsquigarrow^{+} \mathsf{C}_2, \sigma_2, ok \rightsquigarrow^{+} \cdots \end{aligned}$$

Proof. By induction on the structure of the divergence rules in Fig. 3 and Fig. 9.

Case Div-Seq1

Pick arbitrary p, C_1, C_2 such that $[p]\ \mathsf{C}_1; \mathsf{C}_2\ [\infty]$. Pick an arbitrary $\sigma_p \in p$ and σ such that $\sigma_p \# \sigma$. From the $[p]\ \mathsf{C}_1\ [\infty]$ premise and the inductive hypothesis we know there exists an infinite series $\mathsf{C}_2', \mathsf{C}_3', \cdots$, and $\sigma_2, \sigma_3, \cdots$, such that $\mathsf{C}_1, \sigma_p \circ \sigma \rightsquigarrow^{+} \mathsf{C}_2', \sigma_2, ok \rightsquigarrow^{+} \mathsf{C}_3', \sigma_3, ok \rightsquigarrow^{+} \cdots$. As such, from the definition of $\rightsquigarrow^{+}$ and Lemma 22 we have $\mathsf{C}_1; \mathsf{C}_2, \sigma_p \circ \sigma \rightsquigarrow^{+} \mathsf{C}_2'; \mathsf{C}_2, \sigma_2, ok \rightsquigarrow^{+} \mathsf{C}_3'; \mathsf{C}_2, \sigma_3, ok \rightsquigarrow^{+} \cdots$, as required.

Case Div-Seq2

Pick arbitrary p, q, C_1, C_2 such that $[p]\ \mathsf{C}_1; \mathsf{C}_2\ [\infty]$. Pick an arbitrary $\sigma_p \in p$ and σ such that $\sigma_p \# \sigma$. From the $\vdash_{\mathsf{B}}$ $[p]\ \mathsf{C}_1\ [ok\colon q]$ premise and Lemma 17 we know there exists $\sigma_q \in q$ and n such that $\mathsf{C}_1, \sigma_p \circ \sigma \xrightarrow{n} -, \sigma_q \circ \sigma, ok$. Moreover, since $\sigma_q \in q$, from the $[q]\ \mathsf{C}_2\ [\infty]$ premise and the inductive hypothesis we know there exists an infinite series $\mathsf{C}_3', \mathsf{C}_4', \cdots$ and $\sigma_3, \sigma_4, \cdots$, such that $\mathsf{C}_2, \sigma_q \circ \sigma \rightsquigarrow^{+} \mathsf{C}_3', \sigma_3, ok \rightsquigarrow^{+} \mathsf{C}_4', \sigma_4, ok \rightsquigarrow^{+} \cdots$. As $\mathsf{C}_1, \sigma_p \circ \sigma \xrightarrow{n} -, \sigma_q \circ \sigma, ok$ and $\mathsf{C}_2, \sigma_q \circ \sigma \rightsquigarrow^{+} \mathsf{C}_3', \sigma_3, ok$, from the definition of $\rightsquigarrow^{+}$ and Lemma 11 we have $\mathsf{C}_1; \mathsf{C}_2, \sigma_p \circ \sigma \rightsquigarrow^{+} \mathsf{C}_3', \sigma_3, ok$. Moreover, as $\mathsf{C}_3', \sigma_3 \rightsquigarrow^{+} \mathsf{C}_4', s_4, ok \rightsquigarrow^{+} \cdots$, we have $\mathsf{C}_1; \mathsf{C}_2, \sigma_p \circ \sigma \rightsquigarrow^{+} \mathsf{C}_3', \sigma_3, ok \rightsquigarrow^{+} \mathsf{C}_4', \sigma_4, ok \rightsquigarrow^{+} \cdots$, as required.

Case Div-Choice

Pick arbitrary p, C_1, C_2 such that $[p]\ \mathsf{C}_1 + \mathsf{C}_2\ [\infty]$. Pick an arbitrary $i \in \{1, 2\}$, $\sigma_p \in p$ and σ such that $\sigma_p \# \sigma$. From the $[p]\ \mathsf{C}_i\ [\infty]$ premise and the inductive hypothesis we know there exists an infinite series $\mathsf{C}_3, \mathsf{C}_4, \cdots$ and $\sigma_3, \sigma_4, \cdots$, such that $\mathsf{C}_i, \sigma_p \circ \sigma \rightsquigarrow^{+} \mathsf{C}_3, \sigma_3, ok \rightsquigarrow^{+} \mathsf{C}_4, \sigma_4, ok \rightsquigarrow^{+} \cdots$. Moreover, from SL-Choice we have $\mathsf{C}_1 + \mathsf{C}_2, \sigma_p \circ \sigma \rightarrow \mathsf{C}_i, \sigma_p \circ \sigma, ok$. And thus we have $\mathsf{C}_1 + \mathsf{C}_2, \sigma_p \circ \sigma \rightarrow \mathsf{C}_i, \sigma_p \circ \sigma, ok \rightsquigarrow^{+} \mathsf{C}_3, \sigma_3, ok \rightsquigarrow^{+} \mathsf{C}_4, \sigma_4, ok \rightsquigarrow^{+} \cdots$. That is, by definition of $\rightsquigarrow^{+}$ we have $\mathsf{C}_1 + \mathsf{C}_2, \sigma_p \circ \sigma \rightsquigarrow^{+} \mathsf{C}_3, \sigma_3, ok \rightsquigarrow^{+} \mathsf{C}_4, \sigma_4, ok \rightsquigarrow^{+} \cdots$, as required.

Case $\textsc{Div-LoopUnfold}$

Pick arbitrary p, C such that $[p]\ \mathsf{C}^\star\ [\infty]$. Pick an arbitrary $\sigma_p \in p$ and σ such that $\sigma_p \# \sigma$. From the $[p]\ \mathsf{C};\mathsf{C}^\star\ [\infty]$ premise and the inductive hypothesis we know there exists an infinite series $\mathsf{C}_1, \mathsf{C}_2, \cdots$ and $\sigma_1, \sigma_2, \cdots$, such that $\mathsf{C};\mathsf{C}^\star, \sigma_p \circ \sigma \rightsquigarrow^+ \mathsf{C}_1, \sigma_1, ok \rightsquigarrow^+ \mathsf{C}_2, \sigma_2, ok \rightsquigarrow^+ \cdots$. Moreover, from $\textsc{SL-Loop}$ we have $\mathsf{C}^\star, \sigma_p \circ \sigma \rightarrow \mathsf{C};\mathsf{C}^\star, \sigma_p \circ \sigma, ok$. And thus we have $\mathsf{C}^\star, \sigma_p \circ \sigma \rightarrow \mathsf{C};\mathsf{C}^\star, \sigma_p \circ \sigma, ok \rightsquigarrow^+ \mathsf{C}_1, \sigma_1, ok \rightsquigarrow^+ \mathsf{C}_2, \sigma_2, ok \rightsquigarrow^+ \cdots$. That is, by definition of $\rightsquigarrow^+$ we have $\mathsf{C}^\star, \sigma_p \circ \sigma \rightsquigarrow^+ \mathsf{C}_1, \sigma_1, ok \rightsquigarrow^+ \mathsf{C}_2, \sigma_2, ok \rightsquigarrow^+ \cdots$, as required.

Case $\textsc{Div-LoopNest}$

This rule can be derived as follows:

$$\dfrac{\dfrac{[p]\ \mathsf{C}\ [\infty]}{[p]\ \mathsf{C};\mathsf{C}^\star\ [\infty]}\ \textsc{Div-Seq1}}{[p]\ \mathsf{C}^\star\ [\infty]}\ \textsc{Div-LoopUnfold}$$

and thus this rule is sound as we established the soundness of $\textsc{Div-Seq1}$ and $\textsc{Div-LoopUnfold}$ above.

Case $\textsc{Div-Loop}$

Pick arbitrary p, C, q such that $\vdash [p]\ \mathsf{C}^\star\ [\infty]$. From $\textsc{SL-Loop}$ we then have:

$$\forall \sigma_p \in p, \sigma.\ \sigma_p \# \sigma \Rightarrow \mathsf{C}^\star, \sigma_p \circ \sigma \rightarrow \mathsf{C};\mathsf{C}^\star, \sigma_p \circ \sigma, ok \tag{14}$$

From the $\vdash_{\mathrm{B}} [p]\ \mathsf{C}\ [ok\colon q]$ premise, Lemma 17, and the $q \subseteq p$ premise we know $\forall \sigma_p \in p, \sigma.\ \sigma_p \# \sigma \Rightarrow \exists \sigma'_p \in p, n.\ \mathsf{C}, \sigma_p \circ \sigma \xrightarrow{n} -, \sigma'_p \circ \sigma, ok$ and thus from Lemma 15 $\mathsf{C}, \sigma_p \circ \sigma \xrightarrow{n} \mathsf{skip}, \sigma'_p \circ \sigma, ok$. That is, from the axiom of choice we know there exist $f : p \rightarrow p$ and $g : p \rightarrow \mathbb{N}$ such that:

$$\forall \sigma_p \in p, \sigma.\ \sigma_p \# \sigma \Rightarrow \mathsf{C}, \sigma_p \circ \sigma \xrightarrow{g(\sigma_p)} \mathsf{skip}, f(\sigma_p) \circ \sigma, ok \land f(\sigma_p) \in p \tag{15}$$

In what follows, we show that $\forall \sigma_p \in p, \sigma.\ \sigma_p \# \sigma \Rightarrow \mathsf{C}^\star, \sigma_p \circ \sigma \rightsquigarrow^+ \mathsf{C}^\star, f(\sigma_p) \circ \sigma, ok$.

Pick an arbitrary $\sigma_p \in p$ and σ such that $\sigma_p \# \sigma$. From (2) we have $\mathsf{C}, \sigma_p \circ \sigma \xrightarrow{g(\sigma_p)} \mathsf{skip}, f(\sigma_p) \circ \sigma, ok$. There are now two cases to consider: i) $g(\sigma_p) = 0$; or ii) $g(\sigma_p) > 0$. In case (i), we then have $\mathsf{C} = \mathsf{skip}$ and $\sigma_p{=}f(\sigma_p)$. As such, from $\textsc{SL-SeqSkip}$ we have $\mathsf{C};\mathsf{C}^\star, \sigma_p \circ \sigma \rightarrow \mathsf{C}^\star, f(\sigma_p) \circ \sigma, ok$, and thus by definition of $\rightsquigarrow^1$ we have $\mathsf{C};\mathsf{C}^\star, \sigma_p \circ \sigma \rightsquigarrow^1 \mathsf{C}^\star, f(\sigma_p) \circ \sigma, ok$

In case (ii), from $\mathsf{C}, \sigma_p \circ \sigma \xrightarrow{g(\sigma_p)} \mathsf{skip}, f(\sigma_p) \circ \sigma, ok$ and Lemma 21 we have $\mathsf{C}, \sigma_p \circ \sigma \rightsquigarrow^{g(\sigma_p)} \mathsf{skip}, f(\sigma_p) \circ \sigma, ok$. Consequently, from Lemma 22 we have $\mathsf{C};\mathsf{C}^\star, \sigma_p \circ \sigma \rightsquigarrow^{g(s)} \mathsf{skip};\mathsf{C}^\star, f(\sigma_p) \circ \sigma, ok$. On the other hand, from $\textsc{SL-SeqSkip}$ we have $\mathsf{skip};\mathsf{C}^\star, f(\sigma_p) \circ \sigma \rightarrow \mathsf{C}^\star, f(\sigma_p) \circ \sigma, ok$ and thus by definition of $\rightsquigarrow^1$ we have $\mathsf{skip};\mathsf{C}^\star, f(\sigma_p) \circ \sigma \rightsquigarrow^1 \mathsf{C}^\star, f(\sigma_p) \circ \sigma, ok$. From Lemma 24, $\mathsf{C};\mathsf{C}^\star, \sigma_p \circ \sigma \rightsquigarrow^{g(s)} \mathsf{skip};\mathsf{C}^\star, f(\sigma_p) \circ \sigma, ok$ and $\mathsf{skip};\mathsf{C}^\star, f(\sigma_p) \circ \sigma \rightsquigarrow^1 \mathsf{C}^\star, f(\sigma_p) \circ \sigma, ok$ we know there exists i such that $\mathsf{C};\mathsf{C}^\star, \sigma_p \circ \sigma \rightsquigarrow^i \mathsf{C}^\star, f(\sigma_p) \circ \sigma, ok$.

That is, in both cases we know there exists i such that $\mathsf{C};\mathsf{C}^\star, \sigma_p \circ \sigma \rightsquigarrow^i \mathsf{C}^\star, f(\sigma_p) \circ \sigma, ok$. As such, from (14) and the definition of $\rightsquigarrow^{i+1}$ we have $\mathsf{C}^\star, \sigma_p \circ \sigma \rightsquigarrow^{i+1} \mathsf{C}^\star, f(\sigma_p) \circ \sigma, ok$, i.e. $\mathsf{C}^\star, \sigma_p \circ \sigma \rightsquigarrow^+ \mathsf{C}^\star, f(\sigma_p) \circ \sigma, ok$. That is, from (15) we have:

$$\forall \sigma_p \in p, \sigma.\ \sigma_p \# \sigma \Rightarrow \mathsf{C}^\star, \sigma_p \circ \sigma \rightsquigarrow^+ \mathsf{C}^\star, f(\sigma_p) \circ \sigma, ok \land f(\sigma_p) \in p \tag{16}$$

Pick an arbitrary $\sigma_p \in p$ and σ such that $\sigma_p \# \sigma$. From (16) we then know $\mathsf{C}^\star, \sigma_p \circ \sigma \rightsquigarrow^+ \mathsf{C}^\star, f(\sigma_p) \circ \sigma, ok \rightsquigarrow^+ \mathsf{C}^\star, f^2(\sigma_p) \circ \sigma, ok \rightsquigarrow^+ \cdots$, as required.

Case Div-Subvariant

Pick arbitrary p, C, q such that $\vdash [p(0)]\ \mathsf{C}^\star\ [\infty]$. From SL-Loop we then have:

$$\forall \sigma_p \in p, \sigma.\ \sigma_p \# \sigma \Rightarrow \mathsf{C}^\star, \sigma_p \circ \sigma \rightarrow \mathsf{C}; \mathsf{C}^\star, \sigma_p \circ \sigma, ok \tag{17}$$

From the $\forall n \in \mathbb{N}.\ \vdash_{\mathrm{B}} [p(n)]\ \mathsf{C}\ [ok\colon p(n{+}1)]$ premise, Lemma 17, and the $q \subseteq p$ premise we know $\forall n \in \mathbb{N}, \sigma_p \in p(n), \sigma.\ \sigma_p \# \sigma \Rightarrow \exists \sigma'_p \in p(n{+}1), k.\ \mathsf{C}, \sigma_p \circ \sigma \xrightarrow{k} -, \sigma'_p \circ \sigma, ok$. That is, from the axiom of choice we know there exists a series of functions, $f_1, g_1, f_2, g_2 \cdots$ such that for each $i \in \mathbb{N}$, we have $f_i : p(i{-}1) \rightarrow p(i)$ and $g_i : p(i{-}1) \rightarrow \mathbb{N}$ such that:

$$\forall i \in \mathbb{N}^+.\ \forall \sigma_p \in p(i-1), \sigma.\ \sigma_p \# \sigma \Rightarrow \mathsf{C}, \sigma_p \circ \sigma \xrightarrow{g_i(\sigma_p)} \mathsf{skip}, f_i(\sigma_p) \circ \sigma, ok \wedge f_i(\sigma_p) \in p(i) \tag{18}$$

In what follows, we show that $\forall i \in \mathbb{N}^+.\ \forall \sigma_p \in p(i{-}1), \sigma.\ \sigma_p \# \sigma \Rightarrow \mathsf{C}^\star, \sigma_p \circ \sigma \rightsquigarrow^+ \mathsf{C}^\star, f_i(\sigma_p) \circ \sigma, ok$.

Pick an arbitrary $i \in \mathbb{N}^+$, $\sigma_p \in p(i{-}1)$ and σ such that $\sigma_p \# \sigma$. From (18) we have $\mathsf{C}, \sigma_p \circ \sigma \xrightarrow{g_i(\sigma_p)} \mathsf{skip}, f_i(\sigma_p) \circ \sigma, ok$. There are now two cases to consider: a) $g_i(\sigma_p) = 0$; or b) $g_i(\sigma_p) > 0$. In case (a), we then have $\mathsf{C} = \mathsf{skip}$ and $\sigma_p{=}f_i(\sigma_p)$. As such, from SL-SeqSkip we have $\mathsf{C}; \mathsf{C}^\star, \sigma_p \circ \sigma \rightarrow \mathsf{C}^\star, f_i(\sigma_p) \circ \sigma, ok$, and thus by definition of $\rightsquigarrow^1$ we have $\mathsf{C}; \mathsf{C}^\star, \sigma_p \circ \sigma \rightsquigarrow^1 \mathsf{C}^\star, f_i(\sigma_p) \circ \sigma, ok$.

In case (b), from $\mathsf{C}, \sigma_p \circ \sigma \xrightarrow{g_i(\sigma_p)} \mathsf{skip}, f_i(\sigma_p) \circ \sigma, ok$ and Lemma 21 we have $\mathsf{C}, \sigma_p \circ \sigma \rightsquigarrow^{g_i(\sigma_p)} \mathsf{skip}, f_i(\sigma_p) \circ \sigma, ok$. Consequently, from Lemma 22 we have $\mathsf{C}; \mathsf{C}^\star, \sigma_p \circ \sigma \rightsquigarrow^{g_i(\sigma_p)} \mathsf{skip}; \mathsf{C}^\star, f_i(\sigma_p) \circ \sigma, ok$. On the other hand, from SL-SeqSkip we have $\mathsf{skip}; \mathsf{C}^\star, f_i(\sigma_p) \circ \sigma \rightarrow \mathsf{C}^\star, f_i(\sigma_p) \circ \sigma, ok$ and thus by definition of $\rightsquigarrow^1$ we have $\mathsf{skip}; \mathsf{C}^\star, f_i(\sigma_p) \circ \sigma \rightsquigarrow^1 \mathsf{C}^\star, f_i(\sigma_p) \circ \sigma, ok$. From Lemma 24, $\mathsf{C}; \mathsf{C}^\star, \sigma_p \circ \sigma \rightsquigarrow^{g_i(\sigma_p)} \mathsf{skip}; \mathsf{C}^\star, f_i(\sigma_p) \circ \sigma, ok$ and $\mathsf{skip}; \mathsf{C}^\star, f_i(\sigma_p) \circ \sigma \rightsquigarrow^1 \mathsf{C}^\star, f_i(\sigma_p) \circ \sigma, ok$ we know there exists j such that $\mathsf{C}; \mathsf{C}^\star, \sigma_p \circ \sigma \rightsquigarrow^j \mathsf{C}^\star, f_i(\sigma_p) \circ \sigma, ok$.

That is, in both cases we know there exists j such that $\mathsf{C}; \mathsf{C}^\star, \sigma_p \circ \sigma \rightsquigarrow^j \mathsf{C}^\star, f_i(\sigma_p) \circ \sigma, ok$. As such, from (17) and the definition of $\rightsquigarrow^{j+1}$ we have $\mathsf{C}^\star, \sigma_p \circ \sigma \rightsquigarrow^{j+1} \mathsf{C}^\star, f_i(\sigma_p) \circ \sigma, ok$, i.e. $\mathsf{C}^\star, \sigma_p \circ \sigma \rightsquigarrow^+ \mathsf{C}^\star, f_i(\sigma_p) \circ \sigma, ok$. That is, from (18) we have:

$$\forall i \in \mathbb{N}^+.\ \forall \sigma_p \in p(i{-}1), \sigma.\ \sigma_p \# \sigma \Rightarrow \mathsf{C}^\star, \sigma_p \circ \sigma \rightsquigarrow^+ \mathsf{C}^\star, f_i(\sigma_p) \circ \sigma, ok \wedge f_i(\sigma_p) \in p(i) \tag{19}$$

Pick an arbitrary $\sigma_p \in p(0)$ and σ such that $\sigma_p \# \sigma$. From (19) we then know $\mathsf{C}^\star, \sigma_p \circ \sigma \rightsquigarrow^+ \mathsf{C}^\star, f_1(\sigma_p) \circ \sigma, ok \rightsquigarrow^+ \mathsf{C}^\star, f_2(\sigma_p) \circ \sigma, ok \rightsquigarrow^+ \cdots$, as required.

Case Div-Cons

Pick arbitrary p, C such that $[p]\ \mathsf{C}\ [\infty]$. Pick an arbitrary $\sigma_p \in p$ and σ such that $\sigma_p \# \sigma$. From the $p \subseteq p'$ premise we know $\sigma_p \in p'$. As such, from the $[p']\ \mathsf{C}\ [\infty]$ premise we know there exists an infinite series $\mathsf{C}_1, \mathsf{C}_2, \cdots$ and $\sigma_1, \sigma_2, \cdots$, such that $\mathsf{C}, \sigma_p \circ \sigma \rightsquigarrow^+ \mathsf{C}_1, \sigma_1, ok \rightsquigarrow^+ \mathsf{C}_2, \sigma_2, ok \rightsquigarrow^+ \cdots$, as required.

Case Div-Frame

Pick arbitrary p, r, C such that $[p * r]\ \mathsf{C}\ [\infty]$. Pick an arbitrary $\sigma_{pr} \in p * r$ and σ such that $\sigma_{pr} \# \sigma$. As $\sigma_{pr} \in p * r$, we know there exist $\sigma_p \in p$ and $\sigma_r \in r$ such that $\sigma_{pr} = \sigma_p \circ \sigma_r$. From the definitions of $\circ$ and σ_{pr} and since $\sigma_{pr} \# \sigma$ we know $\sigma_r \# \sigma$ and $\sigma_p \# \sigma_r \circ \sigma$.

On the other hand, from the premise of Div-Frame we have $[p]\ \mathsf{C}\ [\infty]$ and thus from the inductive hypothesis we know there exists an infinite series $\mathsf{C}_1, \mathsf{C}_2, \cdots$ and $\sigma_1, \sigma_2, \cdots$, such that $\mathsf{C}, \sigma_p \circ (\sigma_r \circ \sigma) \rightsquigarrow^+ \mathsf{C}_1, \sigma_1, ok \rightsquigarrow^+ \mathsf{C}_2, \sigma_2, ok \rightsquigarrow^+ \cdots$. That is, by associativity of $\circ$ we have $\mathsf{C}, (\sigma_p \circ \sigma_r) \circ \sigma \rightsquigarrow^+ \mathsf{C}_1, \sigma_1, ok \rightsquigarrow^+ \mathsf{C}_2, \sigma_2, ok \rightsquigarrow^+ \cdots$, i.e. $\mathsf{C}, \sigma_{pr} \circ \sigma \rightsquigarrow^+ \mathsf{C}_1, \sigma_1, ok \rightsquigarrow^+ \mathsf{C}_2, \sigma_2, ok \rightsquigarrow^+ \cdots$, as required. □

Lemma 26. *For all p, C, if $\vdash [p]\ \mathsf{C}\ [\infty]$ is derivable using the rules in Fig. 3 and Fig. 9, then $\models [p]\ \mathsf{C}\ [\infty]$ holds.*

Proof. Pick arbitrary p, C such that $[p]\ \mathsf{C}\ [\infty]$ is derivable using the rules in Fig. 3 and Fig. 9. Pick an arbitrary $\sigma_p = (s_p, h_p) \in p$. It then suffices to show there exists an infinite series $\mathsf{C}_1, \mathsf{C}_2, \cdots$ and $\sigma_1, \sigma_2, \cdots$, such that $\mathsf{C}, \sigma_p \rightsquigarrow^+ \mathsf{C}_1, \sigma_1, ok \rightsquigarrow^+ \mathsf{C}_2, \sigma_2, ok \rightsquigarrow^+ \cdots$.

Let $\sigma_0 = (s_p, h_0)$, where h_0 denotes the empty heap (with an empty domain). From the definition of $\circ$ and # we then know that $\sigma_p \# \sigma_0$. As such, from Lemma 25 we know there exists an infinite series $\mathsf{C}_1, \mathsf{C}_2, \cdots$ and $\sigma_1, \sigma_2, \cdots$, such that $\mathsf{C}, \sigma_p \circ \sigma_0 \rightsquigarrow^+ \mathsf{C}_1, \sigma_1, ok \rightsquigarrow^+ \mathsf{C}_2, \sigma_2, ok \rightsquigarrow^+ \cdots$. That is, as $\sigma_p \circ \sigma_0 = \sigma_p$, we know there exists an infinite series $\mathsf{C}_1, \mathsf{C}_2, \cdots$ and $\sigma_1, \sigma_2, \cdots$, such that $\mathsf{C}, \sigma_p \rightsquigarrow^+ \mathsf{C}_1, \sigma_1, ok \rightsquigarrow^+ \mathsf{C}_2, \sigma_2, ok \rightsquigarrow^+ \cdots$, as required. □

Theorem 20 (UNTER$^{\text{SL}}$ soundness). *For all p, q, C and ϵ:*

1) if $\vdash_{\mathsf{B}} [p]\ \mathsf{C}\ [\epsilon : q]$ is derivable using the rules in Fig. 9, then $\models_{\mathsf{B}} [p]\ \mathsf{C}\ [\epsilon : q]$ holds;
2) if $\vdash_{\mathsf{F}} [p]\ \mathsf{C}\ [\epsilon : q]$ is derivable using the rules in Fig. 9, then $\models_{\mathsf{F}} [p]\ \mathsf{C}\ [\epsilon : q]$ holds; and
3) if $\vdash [p]\ \mathsf{C}\ [\infty]$ is derivable using the rules in Fig. 9, then $\models [p]\ \mathsf{C}\ [\infty]$ holds.

Proof. The proof of part (1) follows immediately from Lemma 18. The proof of part (2) follows immediately from Lemma 20. The proof of part (3) follows immediately from Lemma 26. □

G NON-TERMINATION CVES

G.1 Network software: Wireshark (C, CVE-2022-3190)

Table 1. Wireshark F5 Ethernet trailer vulnerability (CVE-2022-3190, August 2022). Fix available at https://gitlab.com/wireshark/wireshark/-/merge_requests/7981/diffs. Failure to show parsing progress leads to parsing loop stuck reading the same broken trailer over and over.

```
static gint
dissect_old_trailer(tvbuff_t *tvb, packet_info *pinfo,
                    proto_tree *tree, void *data)
{
    proto_tree *ttree   = NULL;
    proto_item *ti = NULL;
    guint off = 0;
    guint read = 0;
    f5eth_tap_data_t *tdata = (f5eth_tap_data_t *)data;
    guint8 type, len, ver;
    while (tvb_reported_length_remaining(tvb, off)) {
        type = tvb_get_guint8(tvb, offset);
        len = tvb_get_guint8(tvb, off + F5_OFF_LENGTH) + F5_OFF_VERSION;
        ver = tvb_get_guint8(tvb, off + F5_OFF_VERSION);
        if (len <= tvb_reported_length_remaining(tvb, offset)
            && type >= F5TYPE_LOW && type <= F5TYPE_HIGH
            && len >= F5_MIN_SANE && len <= F5_MAX_SANE
            && ver <= F5TRAILER_VER_MAX) {
            /* Parse out the specified trailer. */
            switch (type) {
            case F5TYPE_LOW:
                ti = proto_tree_add_item(tree, hf_low_id, tvb,
                                         off, len, ENC_NA);
                ttree = proto_item_add_subtree(ti);
                read = dissect_low(tvb, pinfo, ttree,
                                off, len, ver, tdata);
                tdata->trailer_len += read ;
                // Bug: next 3 lines should execute after switch
                if (read == 0) {
                    proto_item_set_len(ti, 1);
                    return off;
                }
                break;
            case F5TYPE_MED:
                ti = proto_tree_add_item(tree, hf_med_id, tvb,
                                         off, len, ENC_NA);
                ttree = proto_item_add_subtree(ti);
                read = dissect_med(tvb, pinfo, ttree,
                                off, len, ver, tdata);
                tdata->trailer_len += read;
                break;
            }
        }
    }
```

G.2 Web software: log4j (Java, CVE 2021-45105)

Table 2. A String substitution function is called recursively with a string reference pointing to the string being replaced, leading to an infinite loop. (Java code, CVE 2021-45105). Root cause analysis available at https://www.zerodayinitiative.com/blog/2021/12/17/cve-2021-45105-denial-of-service-via-uncontrolled-recursion-in-log4j-strsubstitutor

```
// Recursive function that may not terminate
private int substitute(final LogEvent event,
                       final StringBuilder buf,
                       final int offset, final
                       int length,
                       List<String> priorVariables) {
if (priorVariables == null) {
    priorVariables = new ArrayList<>();
    priorVariables.add(new String(chars, offset, length + lengthChange));
}
// Handle cyclic substitution
if (!priorVariables.contains(varName)) {
        return;
}
priorVariables.add(varName);
String varValue = resolveVariable(event, varName, buf, startPos, endPos);
// Recursive replace
final int varLen = varValue.length();
buf.replace(startPos, endPos, varValue);
int change = substitute(event, buf, startPos, varLen, priorVariables);
change = change + (varLen - (endPos - startPos));
pos += change;
bufEnd += change;
lengthChange += change;
chars = getChars(buf); // in case buffer was altered
String varNameExpr = new String(chars, startPos + startMatchLen,
                                pos - startPos - startMatchLen);
// Substitute in variable
final StringBuilder bufName = new StringBuilder(varNameExpr);
// Bug: Missing priorVariables param leads to infinite execution
substitute(event, bufName, 0, bufName.length());
(...)
}
```

G.3 Data mining Software: GraphQL (Golang, Sept 2022)

Table 3. Infinite recursion bug in Data Query Language interpreter GraphQL. A parsing lookup table containing function pointers is populated with handlers that can be called recursively while parsing the graph data structure. Bug was fixed in September 2022 to avoid node type confusion when node value string representation is equal to a node type string representation (e.g. String String = "String"). Fix available at https://github.com/solidwall/graphql-go/blob/master/language/parser/parser.go#L843)

```
func init() {
        tokenDefinitionFn = make(map[string]parseDefinitionFn)
        {
            // FIXME: comment below 4 lines
                tokenDefinitionFn[lexer.BRACE_L.String()] = parseOperationDef
                tokenDefinitionFn[lexer.STRING.String()] = parseTypeSystemDef
                tokenDefinitionFn[lexer.BLOCK_STRING.String()] = parseTypeSystemDef
                tokenDefinitionFn[lexer.NAME.String()] = parseTypeSystemDef
                switch kind := parser.Token.Kind; kind {
                case lexer.BRACE_L, lexer.NAME, lexer.STRING, lexer.BLOCK_STRING:
                        item = tokenDefinitionFn[kind.String()]
                // FIX: replace above 2 lines with:
                //case lexer.BRACE_L:
                //      item = parseOperationDefinition
                //case lexer.NAME, lexer.STRING, lexer.BLOCK_STRING:
                //      item = parseTypeSystemDefinition
                default:
                        return nil, unexpected(parser, lexer.Token{})
            }
                if node, err = item(parser); err != nil {
                        return nil, err
                }
}
func parseTypeSystemDef(parser *Parser) (ast.Node, error) {
        keywordToken := parser.Token
        var ok bool
        if item, ok = tokenDefinitionFn[keywordToken.Value]; !ok {
                return nil, unexpected(parser, keywordToken)
        }
        // Bug: infinite recursion on parseTypeSystemDef
        return item(parser)
}
```

G.4 System Software: Linux Kernel (C, CVE-2020-25641)

Table 4. Termination bug in the Linux kernel (August 2020). Macro for_each_bvec contains an infinite loop due to zero sized bvec which fails to increment the loop index. Bug discussed at https://www.mail-archive.com/linux-kernel@vger.kernel.org/msg2262077.html. Details available at https://nvd.nist.gov/vuln/detail/CVE-2020-25641. Table shows minimized vulnerable code.

```
+static inline void bvec_iter_skip_zero_bvec(struct bvec_iter *iter)
+{
+       iter->bi_bvec_done = 0;
+       iter->bi_idx++;
+}
+
 #define for_each_bvec(bvl, bio_vec, iter, start)
        for (iter = (start); (iter).bi_size &&
                ((bvl = bvec_iter_bvec((bio_vec), (iter))), 1);
-           bvec_iter_advance((bio_vec), &(iter), (bvl).bv_len))
+           (bvl).bv_len ? bvec_iter_advance((bio_vec), &(iter),
+               (bvl).bv_len) : bvec_iter_skip_zero_bvec(&(iter)))
```

G.5 Graphical Software : Blender (C language)

Table 5. Termination bug in graphical software (Blender v3.2). Function blendthumb_extract_from_file_impl contains an infinite loop due to a user-supplied negative stream offset. Fix available at https://developer.blender.org/rB24a2b5cb1292f769dd86e314471443976d5e9512. Table shows minimized vulnerable code.

```
eThumbStatus blendthumb_extract_from_file_impl(FileReader *file,
                                               Thumbnail *thumb,
                                               const size_t bhead_size,
                                               const bool endian)
{
uint8_t *bhead_data = BLI_array_alloca(bhead_data, bhead_size);
while (file_read(file, bhead_data, bhead_size)) {
   int32_t block_size = bytes_to_native_i32(&bhead_data[4], endian);
   switch (*bhead_data) {
      case V: {
        if (!file_seek(file, block_size))
          return BT_INVALID_THUMB;
        }
    }
}
```

G.6 Machine Learning Software : Sklearn (Python)

Table 6. Termination bug in Machine Learning software (python sklearn version of November 2021). A failing try block prevents the induction variable from being incremented properly. Break in catch block only breaks the inner loop and not the outter one. Fix available at https://github.com/scikit-learn/scikit-learn/pull/21271/commits/325d32fedb48b42faa32b0873a9eeee9ff35a125. Table shows minimized vulnerable code.

```
def discretize(vectors, max_svd_restarts=30, n_iter_max=20):
  svd_restarts = 0
  has_converged = False
  n_samples, n_components = vectors.shape
  while (svd_restarts < max_svd_restarts) and not has_converged:
        n_iter = 0
        while not has_converged:
            n_iter += 1
            vectors_discrete = csc_matrix(np.arange(0, n_samples))
            t_svd = vectors_discrete.T * vectors
            try:
                U, S, Vh = np.linalg.svd(t_svd)
                svd_restarts += 1
            except LinAlgError:
                print("SVD did not converge, try again.")
                break
            if (n_iter > n_iter_max):
                has_converged = True
```

G.7 Cryptographic Software: OpenSSL (C lang, CVE-2022-0778)

Table 7. Fix for termination bug in OpenSSL. Function BN_mod_sqrt has a non termination condition when computing modular square root arithmetic on a non-prime moduli with invalid curve parameters. Advisory available at https://www.openssl.org/news/secadv/20220315.txt (March 2022).

```
-        /* find smallest  i  such that  b^(2^i) = 1 */
-        i = 1;
-        if (!BN_mod_sqr(t, b, p, ctx))
-            goto end;
-        while (!BN_is_one(t)) {
-            i++;
-            if (i == e) {
-                BNerr(BN_F_BN_MOD_SQRT, BN_R_NOT_A_SQUARE);
-                goto end;
+        /* Find the smallest i, 0 < i < e, such that b^(2^i) = 1. */
+        for (i = 1; i < e; i++) {
+            if (i == 1) {
+                if (!BN_mod_sqr(t, b, p, ctx))
+                    goto end;
+
+            } else {
+                if (!BN_mod_mul(t, t, t, p, ctx))
+                    goto end;
             }
-            if (!BN_mod_mul(t, t, t, p, ctx))
-                goto end;
+            if (BN_is_one(t))
+                break;
+        }
+        /* If not found, a is not a square or p is not prime. */
+        if (i >= e) {
+            BNerr(BN_F_BN_MOD_SQRT, BN_R_NOT_A_SQUARE);
+            goto end;
         }
```