Generating next step hints for task oriented programs using symbolic execution

Nico Naus[1] and Tim Steenvoorden[2]

[1] Utrecht University, Utrecht, The Netherlands n.naus@uu.nl
[2] Radboud University, Nijmegen, The Netherlands tim@cs.ru.nl

Abstract. Software that models business workflows is omnipresent in today's society. These systems coordinate collaboration in hospitals, companies, and military institutions. Unfortunately, workflow systems may obfuscate the influence of current user actions on the desired end result. In order to make the right decision, users need to oversee the full process and all information available, both of which are usually buried in the system. We have developed a way to automatically generate next step hints for task oriented programs. Task oriented programming provides programmers with an abstraction over workflow software, while still being expressive enough to describe real world collaboration. By leveraging symbolic execution, we can calculate these hints without modification of the original program. To our knowledge, this is the first time that symbolic execution is used to automatically generate next step hints for end users. We prove the generated hints to be sound and complete, and also demonstrate that the symbolic execution semantics we employ is correct for sequential input. In addition, we have developed a Haskell implementation of our automatic next step hint generation system. By providing next step hints, the chance of human error is reduced, while still allowing end users to intervene if required. The overall performance is raised, since the quality of decisions will improve.

Keywords: Task-oriented programming · Next step hint generation · Symbolic execution.

1 Introduction

Software that supports people working together is used in most workplaces nowadays. Its aim is to automate business workflows, in order to simplify processes, to improve service, or to contain cost. In settings like hospitals, first responders and military operations, these systems could even prevent the loss of lives.

Automation and digitalisation of workflows and business processes comes at a cost. For end users it can be hard to see how an action influences their desired goal. They are unable to oversee the complete flow of the process and there might be an abundance of data that they are not fully aware of. End users might wonder if checking a box may prevent them, or someone else, from reaching their goal, or ask themselves if they have taken all information into consideration before making a decision.

To overcome these difficulties, we propose to integrate a next step hint system into workflow software. By combining previous research on symbolic execution for

Task-Oriented Programming [16] and end-user feedback systems for rule based problems [15], we develop a next step hint end-user feedback system for the Task-Oriented Programming language TopHat ($\widehat{\text{TOP}}$) [20]. Our solution, which we call Assistive $\widehat{\text{TOP}}$, generates next step hints from existing code, and does not require extra work by the programmer. To our knowledge, this is the first work employing symbolic execution to automatically generate next-step hints for end users.

Providing next step hints to end users will provide them with a quick insight in to their situation. It reduces the chance of human error, while still allowing the user to intervene if required. The quality of decisions will improve, raising the overall performance.

In this paper we will introduce Task-Oriented Programming and the $\widehat{\text{TOP}}$ language for readers unfamiliar with either of them, followed by some illustrative examples. Building further on this foundation we show how we use symbolic execution to automatically generate next step hints for end users. It is crucial that these hints are valid, meaning they allow users to reach the desired goal. Therefore we prove correctness of the automatic hint generation system. Our hint generation system relies on symbolic execution as presented in earlier work [16]. There, we proved correctness for the symbolic semantics for single user inputs. Here, we prove the entire symbolic system to be correct, for any sequence of user inputs.

1.1 Contributions

This paper makes the following contributions.

- We describe an automatic end user next step feedback system for $\widehat{\text{TOP}}$, called Assistive $\widehat{\text{TOP}}$, based on a previously presented symbolic semantics.
- We prove the symbolic execution semantics of $\widehat{\text{TOP}}$ to be correct for sequential inputs.
- We change the definition of simulation of $\widehat{\text{TOP}}$ programs to accommodate above proof.
- We prove soundness and completeness of next step hints generated by this system.
- We present an implementation of the end user feedback system in Haskell.

1.2 Structure

Section 2 first introduces the Task-Oriented Programming (TOP) paradigm and the Task-Oriented Programming language $\widehat{\text{TOP}}$. Section 3 lists three example programs to illustrate how $\widehat{\text{TOP}}$ works and to show what we like to achieve with Assistive $\widehat{\text{TOP}}$. In Section 4 we briefly introduce the symbolic execution semantics for $\widehat{\text{TOP}}$, followed by a description of Assistive $\widehat{\text{TOP}}$. In Section 5 soundness and completeness of the assistive system are shown. Section 6 gives an overview of related work, and finally Section 7 concludes.

2 The TopHat language

The Task-Oriented Programming (TOP) paradigm was first introduced by Plasmeijer et al. [19]. It is created to improve the development and quality of software that coor-

dinates collaboration between users. TOP provides programmers with a high level of programming abstraction, while still being expressive enough to describe real world collaborations. It does so by using features from higher-order functional programming languages, combined with the notion of *tasks*. Tasks model units of work, which can be performed by a human or by a computer. From a task specification, a TOP implementation generates a distributive multi-user (web) application.

Tasks have a couple of properties, listed below.

- Tasks model *collaboration*.
  Programmers describe what work needs to be done, by who and in what way.
- Tasks are *interactive*.
  Users can enter or update information into the system by using *editors*. They can progress to the next task, or choose between tasks.
- Tasks can be *observed*.
  Therefore, other users or the system itself can make decisions based on the observed progress of the task.
- Tasks are *modular*.
  They can be combined into bigger tasks by using *combinators*. The basic combinators are chosen in such a way, that they represent basic collaboration patterns. New combinators can be created by making use of basic combinators and the (higher order) facilities of the host language.
- Tasks *share information*.
  Information is passed along control flow, or, in order for tasks to exchange information, across control flow via references. In particular to share data between parallel tasks.
- Tasks are *typed*.
  This is not just to ensure safety at runtime, but also to automatically derive common program elements. TOP systems automatically generate user interfaces and manage persistent storage of information.

Currently, there are three systems implementing the TOP paradigm. The reference implementation is the iTasks framework [19], which is an embedded domain specific language in the non-strict functional programming language Clean [18]. mTasks [13] is a TOP implementation specifically designed for embedded systems. A formalisation of TOP, called $\widehat{\text{TOP}}$ (TopHat), has been created by Steenvoorden, Naus, and Klinik [20]. Assistive $\widehat{\text{TOP}}$ builds on $\widehat{\text{TOP}}$ and its symbolic counterpart Symbolic $\widehat{\text{TOP}}$ [16].

$\widehat{\text{TOP}}$ implements TOP by embedding a task language in the simply typed lambda calculus with references, conditionals, and pairs. Note the omission of any fixed point language constructs, which make $\widehat{\text{TOP}}$ a total language. Symbolic $\widehat{\text{TOP}}$ extends this with built in operators, lists, and most importantly symbols. References are used to model the shared data component of TOP. The complete syntax and semantics can be found in previous work [20]. An overview can be found in the appendix. In the next subsections we describe the basic constructs of the $\widehat{\text{TOP}}$ language. Section 4.1 details Symbolic $\widehat{\text{TOP}}$.

2.1 Editors

Editors form the entry points for interaction and communication with the outside world. They are the most basic tasks and can be seen as an abstraction over widgets in a GUI library or forms on a webpage. Users can change the value held by an editor, in the same way they can manipulate widgets in a GUI.

When a TOP implementation generates an application from a task specification, it derives user interfaces for the editors. The appearance of an editor depends on its type. For example, editors of type string can be represented by simple input fields, dates by calendars, and locations by pins on a map.

There are three different editors in $\widehat{\text{TOP}}$.

$\square\, v$ Valued editor.
: This editor holds a value v of a certain type. The user can replace the value by new values of the same type.

$\boxtimes\, \tau$ Unvalued editor.
: This editor holds no value, and can receive a value of type τ. When that happens, it turns into a valued editor.

$\blacksquare\, l$ Shared editor.
: This editor refers to a store location l. Its observable value is the value stored at that location. When it receives a new value, this value will be stored at location l.

2.2 Combinators

Editors can be combined into larger tasks using combinators. The order in which editors and tasks are executed is specified with combinators. Tasks can be performed in sequence, in parallel or a choice can be made between tasks. These combinators originate from basic collaboration patterns.

The following combinators are available in $\widehat{\text{TOP}}$. Here, t stands for tasks and e for expressions.

$t \blacktriangleright e$ Step.
: Users can work on task t. As soon as t has an observable value, as defined in the next section, that value is passed on to the right hand side e. The expression e is a function, taking the value as an argument, resulting in a new task.

$t \triangleright e$ User Step.
: Users can work on task t. When t has an observable value, the step becomes enabled. Then, users can send a continue event to the combinator. When that happens, the value of t is applied to the right hand side function e, with which it continues in the same way as normal steps do.

$t_1 \bowtie t_2$ Pair.
: Users can work on tasks t_1 and t_2 in at the same time.

$t_1 \blacklozenge t_2$ Choice.
: The system chooses between t_1 or t_2, based on which task first has an observable value. If both tasks have a value, the system chooses the left one. When neither of the two tasks has an observable value, users can continue to work on both tasks until one of them does.

$e_1 \lozenge e_2$ User choice.
A user has to make a choice between either the left or the right hand side. After picking a side, the user can work on that task.

In addition to editors and combinators, $\widehat{\text{TOP}}$ also contains the fail task ($\lightning$). Programmers can use this task to indicate that a task is not reachable or viable. When the right hand side of a step combinator evaluates to $\lightning$, the step will not proceed to that task.

2.3 Observations

Several observations can be made on tasks. These observations are used by the system to determine the progress of combinators, and to draw the user interface. They will also be used by Assistive $\widehat{\text{TOP}}$ to provide next step hints.

Using the value function $\mathcal{V}$, the current value of a task can be determined. The value function is a partial function, since not all tasks have a value. For example empty editors do not have a value. The value of tasks composed of parallel and internal choice combinators, depends on the value of the subtasks. Parallel only has a value if both tasks have an observable value. Internal choice has a value if either of the two tasks has an observable value.

One can also observe whether or not a task is failing, by means of the failing function $\mathcal{F}$. A task is considered to be failing if, after normalisation, a user cannot interact with it. For example, the valued editor is not failing, since the user can update it with a new value. The task $\lightning$ is failing, as is a parallel combination of failing tasks $\lightning \bowtie \lightning$, since both the left and the right task cannot be interacted with. Both observation definitions can be found in Fig. 1

$$
\begin{aligned}
&\mathcal{V} : \text{Tasks} \times \text{States} \rightharpoonup \text{Values}\\
&\mathcal{V}(\square\, v, \sigma) = v\\
&\mathcal{V}(\boxtimes\, \tau, \sigma) = \bot\\
&\mathcal{V}(\blacksquare\, l, \sigma) = \sigma(l)\\
&\mathcal{V}(\lightning, \sigma) = \bot\\
&\mathcal{V}(t_1 \blacktriangleright e_2, \sigma) = \bot\\
&\mathcal{V}(t_1 \triangleright e_2, \sigma) = \bot\\
&\mathcal{V}(t_1 \bowtie t_2, \sigma)\\
&\quad = \begin{cases} \langle v_1, v_2 \rangle & \textbf{when } \mathcal{V}(t_1,\sigma) = v_1 \wedge \mathcal{V}(t_2,\sigma) = v_2\\ \bot & \textbf{otherwise} \end{cases}\\
&\mathcal{V}(t_1 \blacklozenge t_2, \sigma)\\
&\quad = \begin{cases} v_1 & \textbf{when } \mathcal{V}(t_1,\sigma) = v_1\\ v_2 & \textbf{when } \mathcal{V}(t_1,\sigma) = \bot \wedge \mathcal{V}(t_2,\sigma) = v_2\\ \bot & \textbf{otherwise} \end{cases}\\
&\mathcal{V}(t_1 \lozenge t_2, \sigma) = \bot
\end{aligned}
$$

$$
\begin{aligned}
&\mathcal{F} : \text{Tasks} \times \text{States} \to \text{Booleans}\\
&\mathcal{F}(\square\, v, \sigma) = \text{False}\\
&\mathcal{F}(\boxtimes\, \tau, \sigma) = \text{False}\\
&\mathcal{F}(\blacksquare\, l, \sigma) = \text{False}\\
&\mathcal{F}(\lightning, \sigma) = \text{True}\\
&\mathcal{F}(t_1 \blacktriangleright e_2, \sigma) = \mathcal{F}(t_1, \sigma)\\
&\mathcal{F}(t_1 \triangleright e_2, \sigma) = \mathcal{F}(t_1, \sigma)\\
&\mathcal{F}(t_1 \bowtie t_2, \sigma) = \mathcal{F}(t_1, \sigma) \wedge \mathcal{F}(t_2, \sigma)\\
&\mathcal{F}(t_1 \blacklozenge t_2, \sigma) = \mathcal{F}(t_1, \sigma) \wedge \mathcal{F}(t_2, \sigma)\\
&\mathcal{F}(e_1 \lozenge e_2, \sigma) = \mathcal{F}(t_1, \sigma_1') \wedge \mathcal{F}(t_2, \sigma_2')\\
&\qquad \textbf{where } e_1, \sigma \Downarrow t_1, \sigma_1'\\
&\qquad \textbf{and } e_2, \sigma \Downarrow t_2, \sigma_2'
\end{aligned}
$$

Fig. 1: Observations on task t. $\mathcal{V}$ gets the value of t, $\mathcal{F}$ observes if it is unsafe to step to t. Note that $\mathcal{V}$ is a partial function.

The step combinators make use of both functions in order to determine if they can step to the right hand side. First, $\mathcal{V}$ determines if the left hand side produces a value. If that is the case, $\mathcal{F}$ checks if stepping to the right hand side is successful.

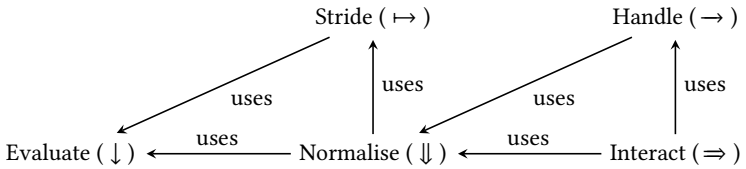

Fig. 2: Semantic functions defined in this report and their relation.

2.4 Input

Input events drive the evaluation of tasks. Because tasks are typed, input is typed as well. Editors only accept input of the correct type. For example, an editor can only be updated with a new value, if it has the same type as the old value. When the system receives a valid event, it applies this event to the current task, which evaluates to a new task. Everything in between two events is evaluated atomically with respect to inputs. This means that tasks are normalised up to the point where they await new user interactions.

Input events are synchronous, which means that the order of execution is completely determined by the order of the events. In particular, the order of input events determine the progression of parallel branches.

2.5 Semantics

The semantics of $\widehat{\text{TOP}}$ are defined in three layers. Figure 2 contains an overview of these semantics and their relations. The first layer consists of the standard big step semantics for the simply typed λ-calculus. We call this semantics evaluation ($\downarrow$). All task specific language constructs, as described previously in Sections 2.1 and 2.2, are normalised using a dedicated big step semantics ($\Downarrow$) in the second layer. Normalisation can be regarded as preparing tasks for user input. It makes use of a helper small step semantics called striding ($\mapsto$).

The above semantics are internal to the system and do not take any user interaction into account. On the third level, the small step interaction semantics ($\Rightarrow$) first handles any user input i using the handle semantics ($\longrightarrow$) and then normalises the resulting task so it is ready to handle the next user input.

The semantic rules can be found in the appendix. For a thorough explanation of all rules, we refer to previous work [20].

3 Examples

This section introduces three example $\widehat{\text{TOP}}$ programs. Each example illustrate different functionality of the $\widehat{\text{TOP}}$ language. Section 3.1 demonstrates the step combinator, Section 3.2 includes the parallel and choice combinators, and finally Section 3.3 demonstrates the use of shares in order for tasks to communicate with each other. The examples will be used in Section 4 to demonstrate how Assistive $\widehat{\text{TOP}}$ works, and are included in the implementation.

3.1 Vending Machine

Using the editors and combinators described in Section 2, we can create a vending machine that dispenses a biscuit for one coin and a chocolate bar for two coins as follows:

```
let vend : Task Snack = □0 ▷ λn.                                    1
  if n ≡ 1 then □Biscuit                                            2
  else if n ≡ 2 then □ChocolateBar                                  3
  else ↯                                                            4
```

Listing 1.1: Vending machine dispensing biscuits or chocolate.

This example demonstrates the usage of a user step guarded by a branching expression (Line 2) using the failure task (Line 4). The editor □ 0 asks the user to enter an amount of money. It simulates a coin slot in a real machine that freely accepts and returns coins. There is a continue button, generated by the user step combinator ▷. Only when the user has inserted exactly 1 or 2 coins will the continue button become enabled. Other cases will result in the failure task ↯, and stepping to it is prohibited by definition. When the user presses the continue button, the machine dispenses either a biscuit or a chocolate bar, depending on the amount of money. Snacks are modelled using a custom type.

3.2 Tax subsidy request

The example program listed in this section is taken from our previous work on symbolic execution for $\widehat{\text{TOP}}$ [20]. It models a simplified tax subsidy application process for citizens who have installed solar panels. This was first described by Stutterheim et al.[21], who worked on modelling a fictional but realistic law about solar panel subsidies.

A subsidy is only given under the following conditions.

- The roofing company has confirmed that they installed solar panels for the citizen.
- The tax officer has approved the request.
- The tax officer can only approve the request if the roofing company has confirmed, and the request is filed within one year of the invoice date.
- The amount of the granted subsidy is at most €600.

```
let today = 13 Feb 2020 in                                                          1
let provideDocuments = ⊠Amount ⋈ ⊠Date in                                           2
let companyConfirm = □True ◊ □False in                                              3
let officerApprove = λinvoiceDate. λtoday. λconfirmed.                              4
  □False ◊ if (today − invoiceDate < 365 days ∧ confirmed) then □True else ↯ in     5
provideDocuments ⋈ companyConfirm ► λ⟨⟨invoiceAmount, invoiceDate⟩ , confirmed⟩ .   6
officerApprove invoiceDate today confirmed ► λapproved.                             7
let subsidyAmount = if approved then min 600 (invoiceAmount / 10) else 0 in         8
□⟨subsidyAmount, approved, confirmed, invoiceDate, today⟩                           9
```

Listing 1.2: Subsidy request and approval workflow at the Dutch tax office.

Listing 1.2 gives the $\widehat{\text{TOP}}$ code for this example. To enhance readability of the example, we omit type annotations and make use of pattern matching on tuples. The program works as follows.

In parallel, the citizen has to provide the invoice documents of the installed solar panels, while the roofing company has to confirm that they have actually installed solar panels at the citizen's address (Line 6). Once the invoice and the confirmation are there, the tax officer has to approve the request (Line 7). The officer can always decline the request, but they can only approve it if the roofing company has confirmed and the application date is within one year of the invoice date (Line 5). The result of the program is the amount of the subsidy, together with all information needed to prove the required properties (Line 9).

In previous work, we have shown that this code indeed adheres to the requirements listed above. There we focussed on assisting the developer by proving the program correct. In this work we focus on supporting the end user that is requesting a subsidy. The end user wants the outcome of this program to be a subsidy amount larger than zero. In Section 4.4 we will show how to generate hints for the end user to reach this goal.

3.3 Dining Computer Scientists Problem

The dining philosophers problem is a classic concurrency problem in computer science. A number of philosophers sit at a round table with a meal in front of them. In between the plates lies a fork. In order to eat their meal, each philosopher has to acquire two forks. Only after eating his or her meal, is a philosopher allowed to place the two forks back on the table. This, of course, means that the philosophers cannot eat at the same time, since there are not enough forks. Deadlock can occur when all philosophers pick up the fork to their right (or left). Then, everybody has one fork. This means that each philosopher cannot start his or her meal. Next to that, is also not allowed to put his fork back on the table.

We look at dining computer scientists instead. Listing 1.3 lists an implementation in $\widehat{\text{TOP}}$ for this problem, with three computer scientists. The forks are represented by references containing Booleans (Lines 1 to 3). Using references allows tasks to communicate with each other across control flow. The value True indicates that the fork is available, False indicates that the fork is being used.

Picking up a fork is only possible when the fork is available, i.e. reading the reference results in True (Line 5). This fork is then marked as being used (Line 6). Reading a reference l is denoted as $!l$, assigning a new value v to a reference l is written as $l := v$.

The use of references ensures that the neighbouring scientist cannot pick up this fork: this choice will be disabled. After that, one can press continue if the second fork is also available (Line 7). For the sake of simplicity, one returns the first fork, rather than setting the second fork to False, and then setting both to True again.

Each computer scientist takes as arguments a name and references to the two forks that he or she can reach (Line 9). They have a choice to take either the left or the right fork. This is represented with an user choice ($\Diamond$, Line 10). The last lines instantiate three computer scientists sitting next to each other (Lines 11 to 13). In TOP terms, this means

```
let fork0 = ref True in                                          1
let fork1 = ref True in                                          2
let fork2 = ref True in                                          3
let pickup = λthis. λthat.                                       4
  if !this                                                       5
    then □(this := False) ▷ λ_.                                  6
      if !that then □(this := True) else ↯                       7
    else ↯ in                                                    8
let scientist = λname. λleft. λright.                            9
  pickup left right ◊ pickup right left in                       10
scientist "Alan Turing" fork0 fork1 ⋈                            11
scientist "Grace Hopper" fork1 fork2 ⋈                           12
scientist "Ada Lovelace" fork2 fork0 ▶ λ_ .                      13
  □"Full bellies"                                                14
```

Listing 1.3: Dining philosophers problem with three computer scientists.

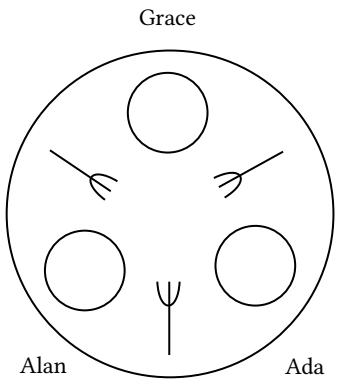

Fig. 3: Rendering with three philosophers.

they collaborate in parallel (⋈) while eating their dinner, sharing some resources, in this case fork0, fork1, and fork2.

By design of $\widehat{\text{TOP}}$, the events of picking up a fork are performed sequentially. That is, when one computer scientist decides to pick up his right fork, we will handle that event first. After that, we will handle the choices from the other scientists. So, the order of the events is explicitly determined by the scientists themselves.

In Section 4.5 we will analyse this example. Our goal is to provide each scientist with a hint on which choice to make, in order to reach the common goal of full bellies. When the scientists follow these hints, no deadlock will occur.

4 Generating next step hints

This section introduces our Assistive $\widehat{\text{TOP}}$ system. The aim of Assistive $\widehat{\text{TOP}}$ is to automatically provide next step hints. When users follow these hints, they can be sure that they will reach the goal they described beforehand. Users can, however, still decide to deviate from the given hints.

During the execution of $\widehat{\text{TOP}}$ programs, users are presented with input fields, choices and continue buttons. The way in which tasks progress and the resulting task value depend on these inputs. At any point during execution, we would like to present users with all possible inputs that leads users to the goal they have selected. These inputs are either concrete actions, like continue, pick the left task, pick the right task; or a restricted set of values to be entered into an editor. This set is restricted, since concrete values potentially influence the flow of the program. To give a concrete example, the user should enter an integer, but this integer must be larger than zero to reach the end goal.

To come to these concrete actions and restricted values, we make use of symbolic execution. In the next two sections, we briefly describe how symbolic execution for $\widehat{\text{TOP}}$ works and recap its symbolic semantics presented in earlier work [16]. Thereafter, we show how to turn symbolic execution results into next step hints. In Sections 4.4

and 4.5, we study what these automatically generated hints look like for the examples from Section 3.

All examples have been tested in our implementation. We added Assistive $\widehat{\text{TOP}}$ to our existing implementation of Symbolic $\widehat{\text{TOP}}$, which is written in Haskell.[3] It uses the z3 SMT solver under the hood. By defining the formal hints function directly on top of the symbolic execution semantics, we can leverage the already existing symbolic execution for Symbolic $\widehat{\text{TOP}}$ in the practical implementation.

4.1 Symbolic execution

A symbolic execution semantics [4, 12] aims to execute a program without knowing its input. Instead, symbols are fed into the program. During evaluation, the influence of values is recorded in the path condition. The resulting symbolic value together with the path conditions can be used to prove properties of the program.

```
⊠INT ⋈ ⊠INT ▶ λ⟨x,y⟩ . if x > y then □⟨y, x⟩ else □⟨x, y⟩
```

Listing 1.4: Ordering of tuple elements.

Consider the tiny example in Listing 1.4. This program asks for two integer values. After the user has entered this information, the function to the right of the step combinator makes sure the result will be an editor containing a pair, where the second element is larger then the first. When we run this program symbolically, we have to create fresh symbols to be entered in either of the two editors, say s_0 and s_1. After entering both symbolic values and then normalising the task, there are two possible outcomes, namely

- $\langle s_1, s_0 \rangle$, provided that the path condition $\varphi_1 = s_0 > s_1$ holds; or
- $\langle s_0, s_1 \rangle$, with path condition $\varphi_2 = \neg(s_0 > s_1)$.

Now, the property that we want to prove for this program is that no matter what the input is, the second element should always be larger than the first. We write this property as $\psi(\langle a, b \rangle) = a \leq b$. Looking at the two symbolic runs, we first need to verify that the symbolic runs are indeed viable. This is done by checking that both φ_1 and φ_2 are satisfiable, written $\mathcal{S}(\varphi_1)$ and $\mathcal{S}(\varphi_2)$. Symbolic runs with a path condition that is not satisfiable are discarded. Finally, we check that both path conditions conform to the goal property ψ, which is the case. Therefore, we can conclude that the property holds. When applying this technique to larger programs, it is a powerful tool to show that a program behaves as expected.

4.2 Symbolic semantics

To support symbolic execution in $\widehat{\text{TOP}}$, we extend our host language with symbols. In addition, we also need to modify the semantics described in Section 2.5, to accommodate symbolic execution. The observation functions from Section 2.3 are extended in a similar way. These new semantic relations operate on expressions which may contain symbols. Instead of stepping to one result, they lead to a set of possible symbolic results, accompanied with a path condition φ.

[3] https://github.com/timjs/symbolic-tophat-haskell

Table 1: Overview of meta variables and semantic relations for concrete and symbolic evaluations.

	Concrete	Symbolic
Expressions	e	$\tilde{e}$
Tasks	t	$\tilde{t}$
States	σ	$\tilde{\sigma}$
Inputs	i	$\tilde{\imath}$
Evaluation	$e, \sigma \downarrow v, \sigma'$	$\tilde{e}, \tilde{\sigma} \wr \overline{\tilde{v}, \tilde{\sigma}', \varphi}$
Normalisation	$e, \sigma \Downarrow t, \sigma'$	$\tilde{e}, \tilde{\sigma} \wr\!\wr \overline{\tilde{t}, \tilde{\sigma}', \varphi}$
Striding	$t, \sigma \mapsto t', \sigma'$	$\tilde{t}, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}', \tilde{\sigma}', \varphi}$
Handling	$t, \sigma \xrightarrow{i} t', \sigma'$	$\tilde{t}, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}', \tilde{\sigma}', \tilde{\imath}, \varphi}$
Interacting	$t, \sigma \overset{i}{\Rightarrow} t', \sigma'$	$\tilde{t}, \tilde{\sigma} \approx\!\!\!\!\rightarrow \overline{\tilde{t}', \tilde{\sigma}', \tilde{\imath}, \varphi}$

We denote entities containing symbols with an additional tilde, and symbolic semantic relations with squiggly arrows instead of straight ones. So $\tilde{t}$, $\tilde{\sigma}$, and $\tilde{\imath}$ are respectively tasks, states, and inputs containing symbols. Table 1 gives an overview of the entities in the concrete world, and their symbolic counterparts. Concrete expressions are a subset of symbolic expressions. Therefore, symbolic semantic relations can be applied on concrete expressions, as well as symbolic expressions.

The symbolic interaction semantics ($\approx\!\!\!\!\rightarrow$) results in a set of symbolic runs, each of them just containing one symbolic input. In other words, the symbolic interaction semantics just looks ahead one symbolic interaction. To be able to reason about an end state after multiple symbolic interactions, we introduce the notion of *simulation*. Informally, simulation performs multiple symbolic interactions after each other, until the rewritten task has an observable value. I.e. if n is the number of interactions needed to be done, $\mathcal{V}(t'_i, \sigma'_i)$ has a result for $i = n$ but is undefined for all $i < n$. Apart from this restriction, we want to permit only viable executions. This is enforced by validating the satisfiability ($\mathcal{S}$) of the conjunction of all sequential path conditions. More formally, simulating a task for multiple user inputs is defined as follows.

Definition 1 (Simulation ($\approx\!\!\!\!\rightarrow^*$)). *Let t and σ be a concrete task and concrete state. We define the simulation relation*

$$t, \sigma \;\approx\!\!\!\!\rightarrow^*\; \overline{\tilde{v}, \tilde{I}, \Phi}$$

to be the set of results after performing symbolic interaction n times:

$$t, \sigma \;\approx\!\!\!\!\rightarrow\; \tilde{t}_1, \tilde{\sigma}_1, \tilde{\imath}_1, \varphi_1 \;\approx\!\!\!\!\rightarrow\; \cdots \;\approx\!\!\!\!\rightarrow\; \tilde{t}_n, \tilde{\sigma}_n, \tilde{\imath}_n, \varphi_n$$

where:

- *the nth task has a value: $\mathcal{V}(\tilde{t}_n, \tilde{\sigma}_n) = \tilde{v}$;*
- *all tasks before do not have a value: $\mathcal{V}(\tilde{t}_{i<n}, \tilde{\sigma}_{i<n}) = \bot$;*
- *$\tilde{I} = \tilde{\imath}_1 \cdots \tilde{\imath}_n$ is the concatenation of all symbolic inputs generated along the way;*
- *$\Phi = \varphi_1 \wedge \cdots \wedge \varphi_n$, is the conjunction of all path conditions encountered.*

Furthermore we require that:

– *the resulting predicate is satisfiable:* $\mathcal{S}(\Phi)$.

The simulation definition used in this paper differs from the one in previous work [16]. Previously, infinite symbolic executions were filtered out by allowing two steps look-ahead in case of idempotent executions. The definition above only allows finite executions by definition.

4.3 Next step hints observation

As we have seen in Definition 1, a symbolic task $\tilde{t}$ is considered done as soon as it has an observable value $\tilde{v}$. In order to calculate next step hints, one needs to formulate a goal over this resulting value. Only then, we can calculate next step hints for end users.

$$\mathcal{H} : \text{Tasks} \times \text{States} \times (\text{Values} \to \text{Booleans}) \to \mathcal{P}(\text{Inputs} \times \text{Predicates})$$
$$\mathcal{H}(t, \sigma, g) \;=\; \{\langle \tilde{\imath}, \Phi \wedge g(\tilde{v})\rangle \mid \big(t, \sigma \;\overline{\approx\!\!\!\!\!\!\rightarrow}^{*}\; \tilde{v}, \tilde{\imath} \cdot \tilde{I}, \Phi\big),\ \mathcal{S}\big(\Phi \wedge g(\tilde{v})\big)\}$$

Fig. 4: Definition of next step hint function.

Hints are calculated by means of the $\mathcal{H}$ function listed in Fig. 4. As input, it receives a concrete task t and concrete state σ together with a goal predicate g. The hints observation simulates t starting in σ. This results in a set of symbolic values $\tilde{v}$, together with a list of symbolic inputs $\tilde{\imath} \cdot \tilde{I}$ and a condition Φ to reach this path. We only want to use the symbolic executions that satisfy the goal g when applied to $\tilde{v}$. Since $\tilde{v}$ could contain symbols, it might be the case that $g(\tilde{v})$ is symbolic and would clash with the path condition Φ. Therefore, we require that the conjunction of the path condition with the goal is satisfiable ($\mathcal{S}(\Phi \wedge g(\tilde{v}))$). From the executions that fulfill this requirement, we return the first symbolic input $\tilde{\imath}$ from the complete list of inputs $\tilde{\imath} \cdot \tilde{I}$, together with the full condition that must hold ($\Phi \wedge g(\tilde{v})$). The resulting set contains pairs of symbolic inputs guarded by this condition.

To get a better understanding how $\mathcal{H}$ works, we study it more concretely in the next subsections. Section 4.4 demonstrates on the basis of the tax example listed in Section 3.2, how the results of the symbolic execution are used to construct automatic next step hints. Section 4.5 shows how hints can be generated during the execution of the example $\widehat{\text{TOP}}$ program listed in Section 3.3.

4.4 Tax subsidy request

Recall the Tax example program in $\widehat{\text{TOP}}$ from Section 3.2, which models the application for a solar panel tax refund. The user enters the invoice date and invoice amount, the installation company confirms, and finally the tax officer either approves or denies the request.

In this section, we will demonstrate what symbolic execution looks like for this example, and how we generate next step hints from the symbolic execution results. First, we call the simulate function $\overline{\approx\!\!\!\!\!\!\rightarrow}^{*}$ on the program, with an empty state. The

Table 2: The results of simulating the program from Listing 1.2.

Symbolic value ($\tilde{v}$)	Symbolic input ($\tilde{I}$)	Path condition (Φ)
$\langle \min(600, s_a/10)$, True, True, s_i, 13 Feb 2020$\rangle$	F F s_a · F S s_i · S L · S	(13 Feb 2020 − s_i) < 365 days
$\langle \min(600, s_a/10)$, True, True, s_i, 13 Feb 2020$\rangle$	F S s_i · F F s_a · S L · S	(13 Feb 2020 − s_i) < 365 days
$\langle \min(600, s_a/10)$, True, True, s_i, 13 Feb 2020$\rangle$	S L · F F s_a · F S s_i · S	(13 Feb 2020 − s_i) < 365 days
$\langle \min(600, s_a/10)$, True, True, s_i, 13 Feb 2020$\rangle$	S L · F S s_i · F F s_a · S	(13 Feb 2020 − s_i) < 365 days
$\langle \min(600, s_a/10)$, True, True, s_i, 13 Feb 2020$\rangle$	F S s_i · S L · F F s_a · S	(13 Feb 2020 − s_i) < 365 days
$\langle \min(600, s_a/10)$, True, True, s_i, 13 Feb 2020$\rangle$	F F s_a · S L · F S s_i · S	(13 Feb 2020 − s_i) < 365 days
$\langle 0$, False, True, s_i, 13 Feb 2020$\rangle$	F F s_a · F S s_i · S L · F	True
$\langle 0$, False, True, s_i, 13 Feb 2020$\rangle$	F S s_i · F F s_a · S L · F	True
$\langle 0$, False, True, s_i, 13 Feb 2020$\rangle$	S L · F F s_a · F S s_i · F	True
$\langle 0$, False, True, s_i, 13 Feb 2020$\rangle$	S L · F S s_i · F F s_a · F	True
$\langle 0$, False, True, s_i, 13 Feb 2020$\rangle$	F S s_i · S L · F F s_a · F	True
$\langle 0$, False, True, s_i, 13 Feb 2020$\rangle$	F F s_a · S L · F S s_i · F	True
$\langle 0$, False, False, s_i, 13 Feb 2020$\rangle$	F F s_a · F S s_i · S · F	True
$\langle 0$, False, False, s_i, 13 Feb 2020$\rangle$	F S s_i · F F s_a · S · F	True
$\langle 0$, False, False, s_i, 13 Feb 2020$\rangle$	S S · F F s_a · F S s_i · F	True
$\langle 0$, False, False, s_i, 13 Feb 2020$\rangle$	S · F S s_i · F F s_a · F	True
$\langle 0$, False, False, s_i, 13 Feb 2020$\rangle$	F S s_i · S · F F s_a · F	True
$\langle 0$, False, False, s_i, 13 Feb 2020$\rangle$	F F s_a · S · F S s_i · F	True

resulting set of symbolic executions is listed in Table 2. Each line represents one symbolic execution. In the first column, the resulting symbolic value $\tilde{v}$ is listed. The second column lists the symbolic input $\tilde{I}$ that was produced to arrive at that value, followed by the path condition Φ in the third column. The symbolic values that are produced are s_i for the invoice date and s_a for the invoice amount.

The definition of $\mathcal{H}$ describes how these results should be used in order to calculate next step hints. First of all, we need a goal g to select the symbolic runs that we are interested in. The most straight forward goal would be that we want to end up in a situation where we get a subsidy amount larger than zero. This goal can be formulated as $g(\langle v, \_, \_, \_, \_\rangle) = v > 0$.

The first six symbolic runs listed in Table 2 fulfill this goal condition. From those runs, we then take the first symbolic input, together with the path condition conjugated with the goal. After removing duplicates and redundant information, the result of $\mathcal{H}$ is as follows.

$$\begin{aligned}&\langle \mathsf{F\,F}\ s_a\ ,\ \min(600, s_a/10) > 0\rangle\\ &\langle \mathsf{F\,S}\ s_i\ ,\ (13\text{ Feb }2020 - s_i) < 365\text{ days}\rangle\\ &\langle \mathsf{S\,L}\quad ,\ \text{True}\rangle\end{aligned}$$

This means that, at this stage, users have three possible options.[4]

1. The applicant may enter an amount s_a for which $\min(600, s_a/10) > 0$ should hold.
2. The applicant may enter an invoice date s_i for which $(13\text{ Feb }2020 - s_i) < 365$ days should hold.
3. The company should take the left choice (L) to confirm they installed the solar panels.

[4] Note that the first branch, entering an amount, is denoted by F F; the second branch, entering the invoice date, is denoted by F S; and the third branch, making a left/right choice, is denoted by S.

4.5 Dining Computer Scientists

Recall the example program Dining Computer Scientists from Section 3.3. Three computer scientist sit at a table and have to coordinate how to their meals. We want to calculate all possible next steps that lead to the goal. The goal in this example is for all computer scientists to finish their meal. In terms of the resulting task value, this means that we want to reach the value ”Full bellies”. Witten as a predicate, we get $g(v) = v \equiv$ ”Full bellies”.

Let us assume that both Grace Hopper and Ada Lovelace have already picked up the forks to their left (fork1 and fork2 respectively). We then find ourselves in the situation shown in Fig. 5.

Let us assume that both Grace Hopper and Ada Lovelace have already picked up the forks to their left (fork1 and fork2 respectively). We then find ourselves in the following situation.

t = scientist ”Alan Turing” fork0 fork1 ⋈
  $\langle\rangle \triangleright \lambda\langle\rangle$.
    if!fork2 **then** fork1 := True **else** $\lightning$ ⋈
  $\langle\rangle \triangleright \lambda\langle\rangle$.
    if!fork0 **then** fork2 := True **else** $\lightning$ ► $\lambda\_$.
    □ ”Full bellies”

σ = {fork0 ↦ True, fork1 ↦ False, fork2 ↦ False}

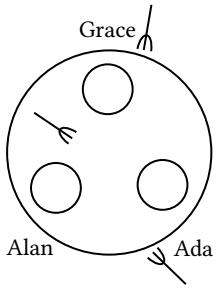

Fig. 5: Task, state and visual representation of dining computer scientists after two moves.

Calling $\mathcal{H}(t, \sigma, g)$ will result in just one hint, namely

$$\langle \mathsf{S\ S\ C}, \mathsf{True} \rangle$$

This means that the only step towards goal g is for the third scientist,[5] which is Ada Lovelace, to pick up the right fork. Although it is also possible for Alan Turing to pick up the fork to his left, this step is not a valid hint and performing this action will result in deadlock.

5 Properties

In this section, we want to validate our approach by proving correctness. For the hints function, which forms the heart of Assistive $\widehat{\text{TOP}}$, we want to prove that its results are both sound and complete. Since the hints function relies on Symbolic $\widehat{\text{TOP}}$, and more specifically, the updated definition of the simulate relation, we first prove correctness of simulate.

[5] The third branch is denoted by S S. The action C means pushing the continue button.

5.1 Correctness of simulate

The symbolic execution semantics is correct when all symbolic runs relate to a concrete run, and the other way around, when all concrete runs are contained in the set of all symbolic executions. These properties are, respectively, soundness and completeness.

The simulation applies symbolic interaction multiple times. In order to prove certain properties with respect to the concrete semantics, we need a concrete analog of simulation. Therefore, we define *execution*, which applies concrete interaction multiple times.

Definition 2 (Execution ($\Rightarrow^*$)). *Let t be a concrete task, σ a concrete state, and $I = i_1 \cdots i_n$ a list of n concrete inputs. We define the execution relation*

$$t, \sigma \overset{I}{\Rightarrow}^* v$$

to be the value of task t after performing concrete interaction for each input i in I:

$$t, \sigma \overset{i_1}{\Rightarrow} t_1, \sigma_1 \overset{i_2}{\Rightarrow} \cdots \overset{i_n}{\Rightarrow} t_n, \sigma_n$$

where

- *v is the value of t_n: $\mathcal{V}(t_n, \sigma_n) = v$; and*
- *all tasks before t_n do not have a value: $\mathcal{V}(t_{i<n}, \sigma_{i<n}) = \bot$.*

Using execution, we can state soundness and completeness for simulation as follows.

Lemma 1 (Soundness of simulate). *For all tasks t and states σ such that $t, \sigma \overset{\sim}{\Rightarrow}^* \tilde{v}, \tilde{I}, \Phi$ where $\tilde{I} = \tilde{\imath}_0 \cdots \tilde{\imath}_n$, for each triple of results $\langle \tilde{v}, \tilde{I}, \Phi \rangle$ there exists a concrete input I with the same length as the symbolic input $\tilde{I}$ such that $t, \sigma \overset{I}{\Rightarrow}^* v$ with $[s_i \mapsto c_i]\tilde{v} = v$ and $[s_i \mapsto c_i]\Phi$ where $SymOf(\tilde{\imath}_i) = s_i$ and $ValOf(i_i) = c_i$.*

Lemma 2 (Completeness of simulate). *For all tasks t, states σ, and lists of input I such that $t, \sigma \overset{I}{\Rightarrow}^* v$, there exists a symbolic value $\tilde{v}$ and a symbolic input $\tilde{I}$ with the same length as I, such that $(\tilde{v}, \tilde{I}, \Phi) \in t, \sigma \overset{\sim}{\Rightarrow}^*$, with $\tilde{\imath}_i \sim i_i$, $[s_i \mapsto c_i]\tilde{v} = v$ and $[s_i \mapsto c_i]\Phi$, where $SymOf(\tilde{\imath}_i) = s_i$ and $ValOf(i_i) = c_i$.*

Where $\tilde{\imath} \sim i$ is defined as follows.

Definition 3 (Input simulation). *A symbolic input $\tilde{\imath}$ simulates a concrete input i denoted as $\tilde{\imath} \sim i$ in the following cases.*
$s \sim a$, where s is a symbol and a a concrete action.
$\tilde{\imath} \sim i \supset \mathsf{F}\,\tilde{\imath} \sim \mathsf{F}\,i$
$\tilde{\imath} \sim i \supset \mathsf{S}\,\tilde{\imath} \sim \mathsf{S}\,i$

And $SymOf(\tilde{\imath}) = s$ and $ValOf(i) = c$ are defined as follows.

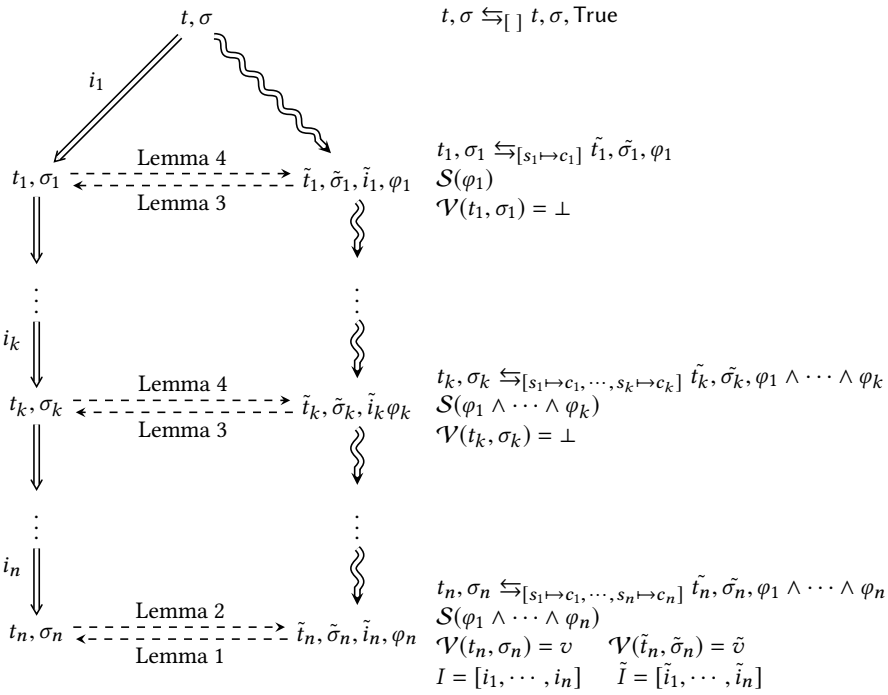

Fig. 6: Proof structure

Definition 4 (Value from input).

$$
\begin{array}{lcl}
\mathit{ValOf} : \text{Inputs} \to \text{Values} & & \\
\mathit{ValOf}(\mathsf{F}\, i) & = & \mathit{ValOf}(i) \\
\mathit{ValOf}(\mathsf{S}\, i) & = & \mathit{ValOf}(i) \\
\mathit{ValOf}(c) & = & c \\
\mathit{ValOf}(\_) & = & \bot
\end{array}
$$

Definition 5 (Symbol from input).

$$
\begin{array}{lcl}
\mathit{SymOf} : \text{Symbolic Inputs} \to \text{Symbolic Values} & & \\
\mathit{SymOf}(\mathsf{F}\, i) & = & \mathit{SymOf}(i) \\
\mathit{SymOf}(\mathsf{S}\, i) & = & \mathit{SymOf}(i) \\
\mathit{SymOf}(s) & = & s \\
\mathit{SymOf}(\_) & = & \bot
\end{array}
$$

Our strategy to prove these two lemma's is outlined in Fig. 6. At the top, we start out with any task t and state σ. The left side of the diagram is an overview of the evaluate function. Inputs i_1 until i_n are sequentially applied, until the task has an observable value.

On the right side, symbolic execution is performed. One step of the symbolic interaction semantics is taken, which results in a symbolic task, state, input and a path condition. Provided that the path condition holds, interaction is executed sequentially until the symbolic task has an observable symbolic value.

Proving soundness and completeness of simulation now comes down to relating the left and right side of the diagram. From symbolic to concrete (right to left) is soundness, as stated in Lemma 1. From concrete to symbolic (left to right) is completeness, as stated in Lemma 1.

Since simulation and execution rely on the (symbolic) handling semantics, we prove soundness and completeness of those semantics first. Looking at Fig. 6, there are two different settings in which the (symbolic) handling semantics are applied. At

the top, both symbolic and concrete execution start out with the same task and state. But further down, the task and state differ for both semantics. The task and state are related to each other however. The symbolic semantics introduces symbols, the concrete semantics handles concrete values. This relation is expressed by the consistence relation listed in Definition 6.

Definition 6 (Consistence relation $\leftrightarrows$). *A concrete task t and concrete state σ are considered to be consistent with a symbolic task $\tilde{t}$, symbolic state $\tilde{\sigma}$ and path condition Φ under a certain mapping $M = [s_1 \mapsto c_1, \cdots, s_n, \mapsto c_n]$, denoted as $t, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ if and only if $M\tilde{t} = t$, $M\tilde{\sigma} = \sigma$ and $M\Phi$*

Now Lemma 3 and Lemma 4 express soundness and completeness of interacting respectively.

Lemma 3 (Soundness of interacting). *For all concrete tasks t, concrete states σ, symbolic tasks $\tilde{t}$, symbolic states $\tilde{\sigma}$ path conditions Φ and mappings M, we have that $t, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ implies that for all pairs $(\tilde{t}', \tilde{\sigma}', \tilde{\imath}, \varphi)$ in $\tilde{t}, \tilde{\sigma} \twoheadrightarrow \overline{\tilde{t}', \tilde{\sigma}', \tilde{\imath}, \varphi}$, $\mathcal{S}(\Phi \wedge \varphi)$ implies that there exists an input i such that $\tilde{\imath} \sim i$, $t, \sigma \overset{i}{\Rightarrow} t', \sigma'$ and $t', \sigma' \leftrightarrows_{M.[s \mapsto c]} \tilde{t}', \tilde{\sigma}', \Phi \wedge \varphi$ where where $SymOf(\tilde{\imath}) = s$ and $ValOf(i) = c$.*

Lemma 4 (Completeness of interacting). *For all concrete tasks t, concrete states σ, symbolic tasks $\tilde{t}$, symbolic states $\tilde{\sigma}$ path conditions Φ and mappings M, we have that $t, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ implies that for all inputs i such that $t, \sigma \overset{i}{\Rightarrow} t', \sigma'$, there exists a symbolic input $\tilde{\imath}, \tilde{\imath} \sim i$ such that $\tilde{t}, \tilde{\sigma} \twoheadrightarrow \overline{\tilde{t}', \tilde{\sigma}', \tilde{\imath}, \varphi}$, $\mathcal{S}(\Phi \wedge \varphi)$ and $t', \sigma' \leftrightarrows_{M.[s \mapsto c]} \tilde{t}', \tilde{\sigma}', \Phi \wedge \varphi$ where where $SymOf(\tilde{\imath}) = s$ and $ValOf(i) = c$.*

In other words, if a symbolic and concrete task and state are related, they will still be related after (symbolic) handling. The top case, where both the symbolic and concrete semantics start out with the same task and state, can be seen as a special case of the consistence relation. Obviously a task and state are consistent with themselves, using the empty mapping and the path condition True.

The full proof of all four lemma's is listed in the appendix.

5.2 Correctness of hints

Now that soundness and completeness of simulate have been proven, we can prove that our hints function produces correct hints. Intuitively, for a next step hint to be correct, it should adhere to the following requirements:

- it leads to concrete input users can actually insert; and
- when users follow the hint, the end goal is still reachable.

Moreover, a set of next step hints is correct when:

- each hint it contains is correct; and
- it covers all possible inputs that lead to the end goal.

We separate these requirements into two lemma's, namely soundness and completeness.

Theorem 1 (Soundness of hints). *For all tasks t, states σ, and goals g, for every next step hint $\langle \tilde{\imath}, \Phi \rangle$ in $\mathcal{H}(t, \sigma, g)$, there exists a sequence of concrete inputs I and a concrete input i such that $\tilde{\imath} \sim i$, $\mathcal{S}([s \mapsto c]\Phi)$, $t, \sigma \overset{i}{\Rightarrow} t', \sigma' \overset{I}{\Rightarrow}^* v$ and $g(v)$.*

Theorem 2 (Completeness of hints). *For all tasks t, states σ, lists of input $i \cdot I$, and goals g, if $t, \sigma, \overset{i \cdot I}{\Rightarrow}^* v$ and $g(v)$, then there exists a symbolic input $\tilde{\imath}$ and path condition Φ such that $\langle \tilde{\imath}, \Phi \rangle \in \mathcal{H}(t, \sigma, g)$ with $\tilde{\imath} \sim i$ and $\mathcal{S}\big([s \mapsto c]\Phi\big)$ with $ValOf(i) = c$ and $SymOf(\tilde{\imath}) = s$.*

The proofs of these two threorems are quite straight forward.

Proof (Theorem 1). Theorem 1 follows from the definition of $\mathcal{H}$ and Lemma 1 as follows.

The definition of $\mathcal{H}$ gives us that for every pair $\langle \tilde{\imath}, \Phi \rangle$ produced by $\mathcal{H}$, there exists a triple $\langle \tilde{v}, \tilde{\imath} : \tilde{is}, \Phi \rangle$ with $\mathcal{S}\big(\Phi \wedge g(\tilde{v})\big)$. Then by Lemma 1 we have that there exists a sequence of concrete inputs I such that $t, \sigma \overset{I}{\Rightarrow}^* v$ and $g(v)$.

Proof (Theorem 2). In order to prove that i is contained in $\mathcal{H}(t, \sigma, g)$, we need to show that $t, \sigma \overset{}{\rightsquigarrow}^* \langle \tilde{v}, \tilde{\imath} \cdot \tilde{I}, \Phi \rangle$, with $\tilde{\imath} \sim i$ and $\mathcal{S}\big([s_0 \mapsto c_0, \cdots, s_n \mapsto c_n] \wedge g(\tilde{v})\big)$, where $ValOf(i_0) = c_0, \cdots, ValOf(i_n) = c_n$ and $[c_0, \cdots, c_n] \in i \cdot I$ and $SymOf(\tilde{\imath}_0) = s_0, \cdots, SymOf(\tilde{\imath}_n) = s_n$.

By Lemma 2, we directly obtain that this indeed exists. Therefore we know that $\tilde{\imath}$ and Φ exist.

6 Related work

In previous work, we have attempted to provide end users with next step hints by viewing workflows as rule based problems [15]. By abstracting over workflows, reasoning about them becomes simpler. A standard search algorithm can be run to find a path to the desired goal state. Two drawbacks of this approach however are that only very general hints can be given, that range over multiple steps, and that a programmer needs to augment existing workflows with extra information in order to convert it to a rule-based problem.

Stutterheim et al. [22] have developed Tonic, a task visualiser for iTasks with limited path prediction capabilities. The main goal is not to provide hints to end users, but the system is able to handle the complete task language, and visualise the effects of user input on the progression of tasks.

In order to overcome the problems of our own previous research and the limited use of Tonic for end user hints, we have combined symbolic execution, together with workflow modelling and next step hint generation. To our knowledge, this is the first work describing the combination of these techniques in this way. The different components coming together in this paper have been studied extensively. The following sections give an overview of the work done in those areas.

6.1 Symbolic execution

Symbolic execution [4, 12] is typically being applied to imperative programming languages, but in recent years it has been used for functional programming languages as well. Ongoing work by Hallahan et al. [8, 9] aims to implement a symbolic execution engine for Haskell. Giantios et al. [7] use symbolic execution for a mix of concrete and symbolic testing of programs written in a subset of Core Erlang. Their goal is to find executions that lead to a runtime error, either due to an assertion violation or an unhandled exception. Chang et al. [5] present a symbolic execution engine for a typed lambda calculus with mutable state where only some language constructs recognise symbolic values. They claim that their approach is easier to implement than full symbolic execution and simplifies the burden on the solver, while still considering all execution paths.

6.2 Workflow modelling

Workflow modelling has been studied extensively from different viewpoints. Since many software exists that automates workflows, it is a research topic that potentially has a huge impact on society.

Workflow patterns are regarded as special design patterns in software engineering. Similar to the combinators in TOP, they describe recurring patterns in workflow systems. Van der Aalst et al. [3] identifies common patterns, and examines their availability in industry workflow frameworks.

Workflow nets allow for the modelling an analysis of business processes [2]. Workflow Nets are a subclass of Petri nets, and are therefore graphical in nature. Research on workflow nets includes verification of models [1] and complexity analysis [14], just to name a few.

iTasks [19] is an implementation of TOP in the programming language Clean. It differs from the above mentioned modelling techniques, since it is not graphical in nature. iTasks supports higher order workflows, and leverages techniques from functional and generic programming.

6.3 Automatic hint generation in intelligent tutoring systems

The intelligent tutoring systems (ITS) research community is very elaborate. Work that is most relevant to our own is the research into automatic hint generation. More traditional ITSs rely heavily on experts to write dedicated hints for every specific case of an exercise. Automatic hint generation attempts to overcome this burden by calculating a hint rather than having every case specified.

Heeren et al. [10] develop a framework for so called domain reasoners that allow for automatic hint generation. Feedback is calculated automatically from a high-level description of an exercise class. Their approach is applicable to domains like logic, mathematics and linear algebra. Paquette et al. [17] present a different automatic next step hint ITS, that is used to provide hints to students in a programming exercise.

Based on the work mentioned above by Heeren et al., an ITS for Haskell exercises has been developed by Gerdes et al. [6]. It tuns out that programming exercises is a

popular area for automatic hint generation. Keuning et al. [11] have written an excellent literature study of this research area.

7 Conclusion

In this paper, we have demonstrated how to apply symbolic execution to automatically generate next step hints for $\widehat{\text{TOP}}$ programs. We have proven the symbolic execution to be sound and complete with regards to sequential inputs. Based on this property, we have also shown that the generated next step hints are correct. Furthermore, we have presented an implementation of the end user feedback system in Haskell.

7.1 Future work

As future work, we are very interested in bringing the theory presented in this paper into practice. We feel that there are three possible angles to pursue this interest.

Presenting hint information The information calculated by the current hints function cannot directly be presented to the end user. The set of calculated hints contains duplicates. This is due to the fact that there might be several different paths to the goal, that start out with the same symbolic input. Another source of redundant information is the path conditions. The path conditions contained in the hint tuple contains information about the complete execution, while the symbolic input is only concerned with the immediate next step. Therefore, the path condition may contain references to future inputs and constraints, which offer no information for the end user. In a future implementation of Assistive $\widehat{\text{TOP}}$, we would like to filter out both sources of redundancy, in order to present the user with more concise information.

Hint generation in iTasks Since iTasks is currently the biggest TOP framework, it would be the next logical step to integrate automatic hint generation into the framework. This would allow a wide range of applications to immediately benefit from automatic next step hint generation. The iTasks framework is shallowly embedded in the purely functional programming language Clean, which means that programmers can leverage the full power of the host language. This makes implementing symbolic execution non-trivial.

Measuring impact of hints Finally, we would like to test the impact of next step hints in workflow systems in an empirical study. TOP research has been applied and studied in the field at the Royal Netherlands Sea Rescue Institution and the Royal Netherlands Navy, which would be ideal testing grounds for Assistive $\widehat{\text{TOP}}$.

Acknowledgements

This research is supported by the Dutch Technology Foundation STW, which is part of the Netherlands Organisation for Scientific Research (NWO), and which is partly funded by the Ministry of Economic Affairs.

Bibliography

[1] van der Aalst, W.M.P.: Verification of workflow nets. In: Application and Theory of Petri Nets 1997, 18th International Conference, ICATPN '97, Toulouse, France, June 23-27, 1997, Proceedings. pp. 407–426 (1997)

[2] van der Aalst, W.M.P.: The application of petri nets to workflow management. Journal of Circuits, Systems, and Computers **8**(1), 21–66 (1998)

[3] van der Aalst, W.M.P., ter Hofstede, A.H.M., Kiepuszewski, B., Barros, A.P.: Workflow patterns. Distributed and Parallel Databases **14**(1), 5–51 (2003)

[4] Boyer, R.S., Elspas, B., Levitt, K.N.: Select - a formal system for testing and debugging programs by symbolic execution. In: Proceedings of the International Conference on Reliable Software. pp. 234–245. ACM, New York, NY, USA (1975)

[5] Chang, S., Knauth, A., Torlak, E.: Symbolic types for lenient symbolic execution. PACMPL **2**(POPL), 40:1–40:29 (2018)

[6] Gerdes, A., Heeren, B., Jeuring, J., van Binsbergen, L.T.: Ask-elle: an adaptable programming tutor for haskell giving automated feedback. I. J. Artificial Intelligence in Education **27**(1), 65–100 (2017)

[7] Giantsios, A., Papaspyrou, N., Sagonas, K.: Concolic testing for functional languages. Science of Computer Programming **147**, 109–134 (2017)

[8] Hallahan, W.T., Xue, A., Bland, M.T., Jhala, R., Piskac, R.: Lazy counterfactual symbolic execution. In: McKinley, K.S., Fisher, K. (eds.) Proceedings of the 40th ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI 2019, Phoenix, AZ, USA, June 22-26, 2019. pp. 411–424. ACM (2019)

[9] Hallahan, W.T., Xue, A., Piskac., R.: Building a symbolic execution engine for haskell. In: Proceedings of TAPAS 17 (2017)

[10] Heeren, B., Jeuring, J.: Feedback services for stepwise exercises. Sci. Comput. Program. **88**, 110–129 (2014)

[11] Keuning, H., Jeuring, J., Heeren, B.: A systematic literature review of automated feedback generation for programming exercises. TOCE **19**(1), 3:1–3:43 (2019)

[12] King, J.C.: A new approach to program testing. SIGPLAN Notices **10**(6), 228–233 (Apr 1975)

[13] Koopman, P., Lubbers, M., Plasmeijer, R.: A task-based DSL for microcomputers. In: Proceedings of the Real World Domain Specific Languages Workshop, RWDSL@CGO 2018, Vienna, Austria, February 24-24, 2018. pp. 4:1–4:11. ACM (2018)

[14] Lassen, K.B., van der Aalst, W.M.P.: Complexity metrics for workflow nets. Information & Software Technology **51**(3), 610–626 (2009)

[15] Naus, N., Jeuring, J.: Building a generic feedback system for rule-based problems. In: Trends in Functional Programming - 17th International Conference, TFP 2016, College Park, MD, USA, June 8-10, 2016, Revised Selected Papers. pp. 172–191 (2016)

[16] Naus, N., Steenvoorden, T., Klinik, M.: A symbolic execution semantics for tophat. In: IFL'19 (accepted for publication) (2019)

[17] Paquette, L., Lebeau, J., Beaulieu, G., Mayers, A.: Automating next-step hints generation using ASTUS. In: Cerri, S.A., Clancey, W.J., Papadourakis, G., Panourgia, K. (eds.) Intelligent Tutoring Systems - 11th International Conference, ITS 2012, Chania, Crete, Greece, June 14-18, 2012. Proceedings. Lecture Notes in Computer Science, vol. 7315, pp. 201–211. Springer (2012)
[18] Plasmeijer, R., van Eekelen, M., van Groningen, J.: Clean language report version 2.1 (2002)
[19] Plasmeijer, R., Lijnse, B., Michels, S., Achten, P., Koopman, P.W.M.: Task-oriented programming in a pure functional language. In: Principles and Practice of Declarative Programming, PPDP'12, Leuven, Belgium - September 19 - 21, 2012. pp. 195–206 (2012)
[20] Steenvoorden, T., Naus, N., Klinik, M.: Tophat: A formal foundation for task-oriented programming. In: Proceedings of the 21st International Symposium on Principles and Practice of Programming Languages, PPDP 2019, Porto, Portugal, October 7-9, 2019. pp. 17:1–17:13 (2019)
[21] Stutterheim, J., Achten, P., Plasmeijer, R.: Maintaining separation of concerns through task oriented software development. In: Trends in Functional Programming - 18th International Symposium, TFP 2017, Canterbury, UK (2017)
[22] Stutterheim, J., Plasmeijer, R., Achten, P.: Tonic: An infrastructure to graphically represent the definition and behaviour of tasks. In: Trends in Functional Programming - 15th International Symposium, TFP 2014, Soesterberg, The Netherlands, May 26-28, 2014. Revised Selected Papers. pp. 122–141 (2014)

A Complete syntax

Expressions

$$
\begin{array}{lll}
e ::= \lambda x : \tau.\ e \mid e_1\ e_2 \mid x \mid c \mid \langle\rangle & & \text{– abstraction, application, variable, constant, unit} \\
\quad \mid u\ e_1 \mid e_1\ o\ e_2 \mid \textbf{if}\ e_1\ \textbf{then}\ e_2\ \textbf{else}\ e_3 & & \text{– unary, binary operation, conditional} \\
\quad \mid \langle e_1, e_2\rangle \mid \mathsf{fst}\ e \mid \mathsf{snd}\ e \mid [\,]_\beta \mid e_1 :: e_2 & & \text{– pair, projections, nil, cons} \\
\quad \mid \mathsf{head}\ e \mid \mathsf{tail}\ e, p & & \text{– first element, list tail, pretask} \\
\quad \mid \textbf{ref}\ e \mid !e \mid e_1 := e_2 \mid l & & \text{– reference, dereference, assignment, location}
\end{array}
$$

$$
\begin{array}{rll}
\text{Constants } c ::= & B \mid I \mid S & \text{– boolean, integer, string} \\
\text{Unary Operations } u ::= & \neg \mid - \mid \mathsf{len} \mid \mathsf{uniq} & \text{– not, negate, length, unique} \\
\text{Binary Operations } o ::= & < \mid \leq \mid \equiv \mid \not\equiv \mid \geq \mid > & \text{– equational} \\
& \mid + \mid - \mid \times \mid / & \text{– numerical} \\
& \mid +\!\!+ \mid \in & \text{– append, elementhood}
\end{array}
$$

Fig. 7: Language grammar

Pretasks

$$
\begin{array}{lll}
p ::= \square\, e \mid \boxtimes \tau \mid \blacksquare\, e \mid e_1 \blacktriangleright e_2 \mid e_1 \triangleright e_2 & & \text{– editors: valued, empty, shared, steps: internal, external} \\
\quad \mid e_1 \blacklozenge e_2 \mid e_1 \lozenge e_2 \mid e_1 \bowtie e_2 \mid \lightning & & \text{– choice: internal, external, composition, fail}
\end{array}
$$

Fig. 8: Task grammar

$$
\begin{array}{rll}
\text{Types } \tau ::= & \tau_1 \to \tau_2 \mid \beta \mid \textsc{Ref}\ \tau \mid \textsc{Task}\ \tau & \text{– function, basic, reference, task} \\
\text{Basic types } \beta ::= & \tau_1 \times \tau_2 \mid \textsc{List}\ \beta \mid \textsc{Unit} & \text{– product, list, unit} \\
& \mid \textsc{Bool} \mid \textsc{Int} \mid \textsc{String} & \text{– boolean, integer, string}
\end{array}
$$

Fig. 9: Type grammar

★

Be consistent with headings of grammars.

Values

$$
\begin{array}{lll}
v ::= \lambda x : \tau.\ e \mid \langle v_1, v_2\rangle \mid \langle\rangle \mid [\,]_\beta \mid v_1 :: v_2 & & \text{– abstraction, pair, unit, nil, cons} \\
\quad \mid c \mid l \mid t \mid u\ v \mid v_1\ o\ v_2 & & \text{– constant, location, task,unary/binary operation}
\end{array}
$$

Tasks

$$
\begin{array}{lll}
t ::= \square\, v \mid \boxtimes \tau \mid \blacksquare\, l \mid t_1 \blacktriangleright e_2 \mid t_1 \triangleright e_2 & & \text{– editors: valued, empty, shared, steps: internal, external} \\
\quad \mid t_1 \blacklozenge t_2 \mid e_1 \lozenge e_2 \mid t_1 \bowtie t_2 \mid \lightning & & \text{– choice: internal, external, composition, fail}
\end{array}
$$

Fig. 10: Value grammar

B $\widehat{\text{TOP}}$ semantics

B.1 Typing rules

$$\boxed{\Gamma, \Sigma \vdash e : \tau}$$

$$\text{T-ConstBool}\ \frac{c \in B}{\Gamma, \Sigma \vdash c : \textsc{Bool}} \qquad \text{T-ConstInt}\ \frac{c \in I}{\Gamma, \Sigma \vdash c : \textsc{Int}} \qquad \text{T-ConstString}\ \frac{c \in S}{\Gamma, \Sigma \vdash c : \textsc{String}} \qquad \text{T-Unit}\ \frac{}{\Gamma, \Sigma \vdash \langle\rangle : \textsc{Unit}}$$

$$\text{T-Var}\ \frac{x : \tau \in \Gamma}{\Gamma, \Sigma \vdash x : \tau} \qquad \text{T-Loc}\ \frac{\Sigma(l) = \beta}{\Gamma, \Sigma \vdash l : \textsc{Ref}\ \beta} \qquad \text{T-Pair}\ \frac{\Gamma, \Sigma \vdash e_1 : \tau_1 \qquad \Gamma, \Sigma \vdash e_2 : \tau_2}{\Gamma, \Sigma \vdash \langle e_1, e_2 \rangle : \tau_1 \times \tau_2}$$

$$\text{T-First}\ \frac{\Gamma, \Sigma \vdash e_1 : \tau}{\Gamma, \Sigma \vdash \mathsf{fst}\langle e_1, e_2 \rangle : \tau} \qquad \text{T-Second}\ \frac{\Gamma, \Sigma \vdash e_2 : \tau}{\Gamma, \Sigma \vdash \mathsf{snd}\langle e_1, e_2 \rangle : \tau} \qquad \text{T-ListEmpty}\ \frac{}{\Gamma, \Sigma \vdash [\,]_\beta : \textsc{List}\ \beta}$$

$$\text{T-ListCons}\ \frac{\Gamma, \Sigma \vdash e_1 : \beta \qquad \Gamma, \Sigma \vdash e_2 : \textsc{List}\ \beta}{\Gamma, \Sigma \vdash e_1 :: e_2 : \textsc{List}\ \beta} \qquad \text{T-ListHead}\ \frac{\Gamma, \Sigma \vdash e : \textsc{List}\ \beta}{\Gamma, \Sigma \vdash \mathsf{head}\ e : \beta} \qquad \text{T-ListTail}\ \frac{\Gamma, \Sigma \vdash e : \textsc{List}\ \beta}{\Gamma, \Sigma \vdash \mathsf{tail}\ e : \textsc{List}\ \beta}$$

$$\text{T-Abs}\ \frac{\Gamma[x : \tau_1], \Sigma \vdash e : \tau_2}{\Gamma, \Sigma \vdash \lambda x : \tau_1 . e : \tau_1 \to \tau_2} \qquad \text{T-App}\ \frac{\Gamma, \Sigma \vdash e_1 : \tau_1 \to \tau_2 \qquad \Gamma, \Sigma \vdash e_2 : \tau_1}{\Gamma, \Sigma \vdash e_1 e_2 : \tau_2}$$

$$\text{T-If}\ \frac{\Gamma, \Sigma \vdash e_1 : \textsc{Bool} \qquad \Gamma, \Sigma \vdash e_2 : \tau \qquad \Gamma, \Sigma \vdash e_3 : \tau}{\Gamma, \Sigma \vdash \textbf{if}\ e_1\ \textbf{then}\ e_2\ \textbf{else}\ e_3 : \tau} \qquad \text{T-Ref}\ \frac{\Gamma, \Sigma \vdash e : \beta}{\Gamma, \Sigma \vdash \textbf{ref}\ e : \textsc{Ref}\ \beta}$$

$$\text{T-Deref}\ \frac{\Gamma, \Sigma \vdash e : \textsc{Ref}\ \beta}{\Gamma, \Sigma \vdash !e : \beta} \qquad \text{T-Assign}\ \frac{\Gamma, \Sigma \vdash e_1 : \textsc{Ref}\ \beta \qquad \Gamma, \Sigma \vdash e_2 : \beta}{\Gamma, \Sigma \vdash e_1 := e_2 : \textsc{Unit}}$$

$$\text{T-Edit}\ \frac{\Gamma, \Sigma \vdash e : \tau}{\Gamma, \Sigma \vdash \Box\, e : \textsc{Task}\ \tau} \qquad \text{T-Enter}\ \frac{}{\Gamma, \Sigma \vdash \boxtimes\, \tau : \textsc{Task}\ \tau} \qquad \text{T-Update}\ \frac{\Gamma, \Sigma \vdash e : \textsc{Ref}\ \beta}{\Gamma, \Sigma \vdash \blacksquare\, e : \textsc{Task}\ \beta}$$

$$\text{T-Fail}\ \frac{}{\Gamma, \Sigma \vdash \lightning : \textsc{Task}\ \tau} \qquad \text{T-Then}\ \frac{\Gamma, \Sigma \vdash e_1 : \textsc{Task}\ \tau_1 \qquad \Gamma, \Sigma \vdash e_2 : \tau_1 \to \textsc{Task}\ \tau_2}{\Gamma, \Sigma \vdash e_1 \blacktriangleright e_2 : \textsc{Task}\ \tau_2} \qquad \text{T-Next}\ \frac{\Gamma, \Sigma \vdash e_1 : \textsc{Task}\ \tau_1 \qquad \Gamma, \Sigma \vdash e_2 : \tau_1 \to \textsc{Task}\ \tau_2}{\Gamma, \Sigma \vdash e_1 \triangleright e_2 : \textsc{Task}\ \tau_2}$$

$$\text{T-And}\ \frac{\Gamma, \Sigma \vdash e_1 : \textsc{Task}\ \tau_1 \qquad \Gamma, \Sigma \vdash e_2 : \textsc{Task}\ \tau_2}{\Gamma, \Sigma \vdash e_1 \bowtie e_2 : \textsc{Task}\ (\tau_1 \times \tau_2)} \qquad \text{T-Or}\ \frac{\Gamma, \Sigma \vdash e_1 : \textsc{Task}\ \tau \qquad \Gamma, \Sigma \vdash e_2 : \textsc{Task}\ \tau}{\Gamma, \Sigma \vdash e_1 \blacklozenge e_2 : \textsc{Task}\ \tau} \qquad \text{T-Xor}\ \frac{\Gamma, \Sigma \vdash e_1 : \textsc{Task}\ \tau \qquad \Gamma, \Sigma \vdash e_2 : \textsc{Task}\ \tau}{\Gamma, \Sigma \vdash e_1 \lozenge e_2 : \textsc{Task}\ \tau}$$

B.2 Evaluation rules

$$\boxed{e, \sigma \ \downarrow \ v, \sigma'}$$

E-App
$$\frac{e_1, \sigma \ \downarrow \ \lambda x : \tau . e_1', \sigma' \qquad e_2, \sigma' \ \downarrow \ v_2, \sigma'' \qquad e_1'[x \mapsto v_2], \sigma'' \ \downarrow \ v_1, \sigma'''}{e_1 e_2, \sigma \ \downarrow \ v_1, \sigma'''}$$

E-IfTrue
$$\frac{e_1, \sigma \downarrow \mathsf{True}, \sigma' \qquad e_2, \sigma' \downarrow v_2, \sigma''}{\textbf{if } e_1 \textbf{ then } e_2 \textbf{ else } e_3, \sigma \downarrow v_2, \sigma''}$$

E-Ref
$$\frac{e, \sigma \downarrow v, \sigma' \qquad l \notin Dom(\sigma')}{\textbf{ref } e, \sigma \downarrow l, \sigma'[l \mapsto v]}$$

E-IfFalse
$$\frac{e_1, \sigma \downarrow v_1, \sigma' \qquad e_3, \sigma' \downarrow v_3, \sigma''}{\textbf{if } e_1 \textbf{ then } e_2 \textbf{ else } e_3, \sigma \downarrow v_3, \sigma''}$$

E-Deref
$$\frac{e, \sigma \downarrow l, \sigma'}{!e, \sigma \downarrow \sigma'(l), \sigma'}$$

E-Value
$$\frac{}{v, \sigma \downarrow v, \sigma}$$

E-Assign
$$\frac{e_1, \sigma \downarrow l, \sigma' \qquad e_2, \sigma' \downarrow v_2, \sigma''}{e_1 := e_2, \sigma \downarrow \langle\rangle, \sigma''[l \mapsto v_2]}$$

E-Pair
$$\frac{e_1, \sigma \downarrow v_1, \sigma' \qquad e_2, \sigma' \downarrow v_2, \sigma''}{\langle e_1, e_2 \rangle, \sigma \downarrow \langle v_1, v_2 \rangle, \sigma''}$$

E-First
$$\frac{e_1, \sigma \downarrow v_1, \sigma'}{\mathsf{fst}\langle e_1, e_2 \rangle, \sigma \downarrow v_1, \sigma'}$$

E-Second
$$\frac{e_2, \sigma \downarrow v_2, \sigma'}{\mathsf{snd}\langle e_1, e_2 \rangle, \sigma \downarrow v_2, \sigma'}$$

E-Cons
$$\frac{e_1, \sigma \downarrow v_1, \sigma' \qquad e_2, \sigma' \downarrow v_2, \sigma''}{e_1 :: e_2, \sigma \downarrow v_1 :: v_2, \sigma''}$$

E-Head
$$\frac{e, \sigma \downarrow v_1 :: v_2, \sigma'}{\mathsf{head}\, e, \sigma \downarrow v_1, \sigma'}$$

E-Tail
$$\frac{e, \sigma \downarrow v_1 :: v_2, \sigma'}{\mathsf{tail}\, e, \sigma \downarrow v_2, \sigma'}$$

E-Edit
$$\frac{e, \sigma \downarrow v, \sigma'}{\square\, e, \sigma \downarrow \square\, v, \sigma'}$$

E-Update
$$\frac{e, \sigma \downarrow l, \sigma'}{\blacksquare\, e, \sigma \downarrow \blacksquare\, l, \sigma'}$$

E-Then
$$\frac{e_1, \sigma \downarrow t_1, \sigma'}{e_1 \blacktriangleright e_2, \sigma \downarrow t_1 \blacktriangleright e_2, \sigma'}$$

E-Next
$$\frac{e_1, \sigma \downarrow t_1, \sigma'}{e_1 \triangleright e_2, \sigma \downarrow t_1 \triangleright e_2, \sigma'}$$

E-And
$$\frac{e_1, \sigma \downarrow t_1, \sigma' \qquad e_2, \sigma' \downarrow t_2, \sigma''}{e_1 \bowtie e_2, \sigma \downarrow t_1 \bowtie t_2, \sigma''}$$

E-Or
$$\frac{e_1, \sigma \downarrow t_1, \sigma' \qquad e_2, \sigma' \downarrow t_2, \sigma''}{e_1 \blacklozenge e_2, \sigma \downarrow t_1 \blacklozenge t_2, \sigma''}$$

B.3 Striding rules

$$\boxed{t, \sigma \;\mapsto\; t', \sigma'}$$

S-ThenStay
$$\frac{t_1, \sigma \mapsto t_1', \sigma'}{t_1 \blacktriangleright e_2, \sigma \mapsto t_1' \blacktriangleright e_2, \sigma'}\ \mathcal{V}(t_1', \sigma') = \bot$$

S-ThenFail
$$\frac{t_1, \sigma \mapsto t_1', \sigma' \qquad e_2\ v_1, \sigma' \downarrow t_2, \sigma''}{t_1 \blacktriangleright e_2, \sigma \mapsto t_1' \blacktriangleright e_2, \sigma'}\ \mathcal{V}(t_1', \sigma') = v_1 \wedge \mathcal{F}(t_2, \sigma'')$$

S-ThenCont
$$\frac{t_1, \sigma \mapsto t_1', \sigma' \qquad e_2\ v_1, \sigma' \downarrow t_2, \sigma''}{t_1 \blacktriangleright e_2, \sigma \mapsto t_2, \sigma''}\ \mathcal{V}(t_1', \sigma') = v_1 \wedge \neg\mathcal{F}(t_2, \sigma'')$$

S-OrLeft
$$\frac{t_1, \sigma \mapsto t_1', \sigma'}{t_1 \blacklozenge t_2, \sigma \mapsto t_1', \sigma'}\ \mathcal{V}(t_1', \sigma') = v_1$$

S-OrRight
$$\frac{t_1, \sigma \mapsto t_1', \sigma' \qquad t_2, \sigma' \mapsto t_2', \sigma''}{t_1 \blacklozenge t_2, \sigma \mapsto t_2', \sigma''}\ \mathcal{V}(t_1', \sigma') = \bot \wedge \mathcal{V}(t_2', \sigma'') = v_2$$

S-OrNone
$$\frac{t_1, \sigma \mapsto t_1', \sigma' \qquad t_2, \sigma' \mapsto t_2', \sigma''}{t_1 \blacklozenge t_2, \sigma \mapsto t_1' \blacklozenge t_2', \sigma''}\ \mathcal{V}(t_1', \sigma') = \bot \wedge \mathcal{V}(t_2', \sigma'') = \bot$$

S-Edit
$$\frac{}{\square\, v, \sigma \mapsto\; \square\, v, \sigma}$$

S-Fill
$$\frac{}{\boxtimes\, \tau, \sigma \mapsto\; \boxtimes\, \tau, \sigma}$$

S-Update
$$\frac{}{\blacksquare\, l, \sigma \mapsto\; \blacksquare\, l, \sigma}$$

S-Fail
$$\frac{}{\lightning, \sigma \mapsto\; \lightning, \sigma}$$

S-Xor
$$\frac{}{e_1 \lozenge e_2, \sigma \mapsto e_1 \lozenge e_2, \sigma}$$

S-Next
$$\frac{t_1, \sigma \mapsto t_1', \sigma'}{t_1 \triangleright e_2, \sigma \mapsto t_1' \triangleright e_2, \sigma'}$$

S-And
$$\frac{t_1, \sigma \mapsto t_1', \sigma' \qquad t_2, \sigma' \mapsto t_2', \sigma''}{t_1 \bowtie t_2, \sigma \mapsto t_1' \bowtie t_2', \sigma''}$$

B.4 Normalisation rules

$$\boxed{e, \sigma \;\Downarrow\; t, \sigma'}$$

N-Done
$$\frac{e, \sigma \downarrow t, \sigma' \qquad t, \sigma' \mapsto t', \sigma''}{e, \sigma \Downarrow t, \sigma'}\ \sigma' = \sigma'' \wedge t = t'$$

N-Repeat
$$\frac{e, \sigma \downarrow t, \sigma' \qquad t, \sigma' \mapsto t', \sigma'' \qquad t', \sigma'' \Downarrow t'', \sigma'''}{e, \sigma \Downarrow t'', \sigma'''}\ \sigma' \neq \sigma'' \vee t \neq t'$$

B.5 Handling rules

$$\boxed{t, \sigma \xrightarrow{i} t', \sigma'}$$

H-Change
$$\frac{}{\square\, v, \sigma \xrightarrow{v'} \square\, v', \sigma}\; v, v' : \tau$$

H-Fill
$$\frac{}{\boxtimes\, \tau, \sigma \xrightarrow{v} \square\, v, \sigma}\; v : \tau$$

H-Update
$$\frac{}{\blacksquare\, l, \sigma \xrightarrow{v} \blacksquare\, l, \sigma[l \mapsto v]}\; \sigma(l), v : \tau$$

H-Next
$$\frac{e_2\ v_1, \sigma \Downarrow t_2, \sigma'}{t_1 \triangleright e_2, \sigma \xrightarrow{\mathsf{C}} t_2, \sigma'}\; \mathcal{V}(t_1, \sigma) = v_1 \wedge \neg\mathcal{F}(t_2, \sigma')$$

H-PickLeft
$$\frac{e_1, \sigma \Downarrow t_1, \sigma'}{e_1 \lozenge e_2, \sigma \xrightarrow{\mathsf{L}} t_1, \sigma'}\; \neg\mathcal{F}(t_1, \sigma')$$

H-PickRight
$$\frac{e_2, \sigma \Downarrow t_2, \sigma'}{e_1 \lozenge e_2, \sigma \xrightarrow{\mathsf{R}} t_2, \sigma'}\; \neg\mathcal{F}(t_2, \sigma')$$

H-PassThen
$$\frac{t_1, \sigma \xrightarrow{i} t_1', \sigma'}{t_1 \blacktriangleright e_2, \sigma \xrightarrow{i} t_1' \blacktriangleright e_2, \sigma'}$$

H-PassNext
$$\frac{t_1, \sigma \xrightarrow{i} t_1', \sigma'}{t_1 \triangleright e_2, \sigma \xrightarrow{i} t_1' \triangleright e_2, \sigma'}$$

H-FirstAnd
$$\frac{t_1, \sigma \xrightarrow{i} t_1', \sigma'}{t_1 \bowtie t_2, \sigma \xrightarrow{\mathsf{F}\,i} t_1' \bowtie t_2, \sigma'}$$

H-SecondAnd
$$\frac{t_2, \sigma \xrightarrow{i} t_2', \sigma'}{t_1 \bowtie t_2, \sigma \xrightarrow{\mathsf{S}\,i} t_1 \bowtie t_2', \sigma'}$$

H-FirstOr
$$\frac{t_1, \sigma \xrightarrow{i} t_1', \sigma'}{t_1 \blacklozenge t_2, \sigma \xrightarrow{\mathsf{F}\,i} t_1' \blacklozenge t_2, \sigma'}$$

H-SecondOr
$$\frac{t_2, \sigma \xrightarrow{i} t_2', \sigma'}{t_1 \blacklozenge t_2, \sigma \xrightarrow{\mathsf{S}\,i} t_1 \blacklozenge t_2', \sigma'}$$

B.6 Interacting rules

$$\boxed{t, \sigma \overset{i}{\Rightarrow} t', \sigma'}$$

I-Handle
$$\frac{t, \sigma \xrightarrow{i} t', \sigma' \qquad t', \sigma' \Downarrow t'', \sigma''}{t, \sigma \overset{i}{\Rightarrow} t'', \sigma''}$$

C Complete symbolic semantics

C.1 Symbolic evaluation rules

$$\boxed{\tilde{e}, \tilde{\sigma} \;\wr\; \overline{\tilde{v}, \tilde{\sigma}', \varphi}}$$

SE-Value
$$\frac{}{\tilde{v}, \tilde{\sigma} \;\wr\; \tilde{v}, \tilde{\sigma}, \mathsf{True}}$$

SE-Pair
$$\frac{\tilde{e}_1, \tilde{\sigma} \;\wr\; \overline{\tilde{v}_1, \tilde{\sigma}', \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma}' \;\wr\; \overline{\tilde{v}_2, \tilde{\sigma}'', \varphi_2}}{\langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma} \;\wr\; \overline{\langle \tilde{v}_1, \tilde{v}_2 \rangle, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2}}$$

SE-First
$$\frac{\tilde{e}_1, \tilde{\sigma} \;\wr\; \overline{\tilde{v}_1, \tilde{\sigma}', \varphi}}{\mathsf{fst}\langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma} \;\wr\; \overline{\tilde{v}_1, \tilde{\sigma}', \varphi}}$$

SE-Second
$$\frac{\tilde{e}_2, \tilde{\sigma} \;\wr\; \overline{\tilde{v}_2, \tilde{\sigma}', \varphi}}{\mathsf{snd}\langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma} \;\wr\; \overline{\tilde{v}_2, \tilde{\sigma}', \varphi}}$$

SE-Cons
$$\frac{\tilde{e}_1, \tilde{\sigma} \;\wr\; \tilde{v}_1, \tilde{\sigma}', \varphi_1 \qquad \tilde{e}_2, \tilde{\sigma}' \;\wr\; \tilde{v}_2, \tilde{\sigma}'', \varphi_2}{\tilde{e}_1 :: \tilde{e}_2, \tilde{\sigma} \;\wr\; \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2}$$

SE-Head
$$\frac{\tilde{e}, \tilde{\sigma} \;\wr\; \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}', \varphi}{\mathsf{head}\, \tilde{e}, \tilde{\sigma} \;\wr\; \tilde{v}_1, \tilde{\sigma}', \varphi}$$

SE-Tail
$$\frac{\tilde{e}, \tilde{\sigma} \;\wr\; \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}', \varphi}{\mathsf{tail}\, \tilde{e}, \tilde{\sigma} \;\wr\; \tilde{v}_2, \tilde{\sigma}', \varphi}$$

SE-App
$$\frac{\tilde{e}_1, \tilde{\sigma} \;\wr\; \overline{\lambda x : \tau . \tilde{e}_1', \tilde{\sigma}', \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma}' \;\wr\; \overline{\tilde{v}_2, \tilde{\sigma}'', \varphi_2} \qquad \tilde{e}_1'[x \mapsto \tilde{v}_2], \tilde{\sigma}'' \;\wr\; \overline{\tilde{v}_1, \tilde{\sigma}''', \varphi_3}}{\tilde{e}_1 \tilde{e}_2, \tilde{\sigma} \;\wr\; \overline{\tilde{v}_1, \tilde{\sigma}''', \varphi_1 \wedge \varphi_2 \wedge \varphi_3}}$$

SE-If
$$\frac{\tilde{e}_1, \tilde{\sigma} \;\wr\; \overline{\tilde{v}_1, \tilde{\sigma}', \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma}' \;\wr\; \overline{\tilde{v}_2, \tilde{\sigma}'', \varphi_2} \qquad \tilde{e}_3, \tilde{\sigma}' \;\wr\; \overline{\tilde{v}_3, \tilde{\sigma}''', \varphi_3}}{\textbf{if}\ \tilde{e}_1\ \textbf{then}\ \tilde{e}_2\ \textbf{else}\ \tilde{e}_3, \tilde{\sigma} \;\wr\; \overline{\tilde{v}_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2 \wedge \tilde{v}_1} \cup \overline{\tilde{v}_3, \tilde{\sigma}''', \varphi_1 \wedge \varphi_3 \wedge \neg \tilde{v}_1}}$$

SE-Ref
$$\frac{\tilde{e}, \tilde{\sigma} \;\wr\; \overline{\tilde{v}, \tilde{\sigma}', \varphi} \qquad l \notin \mathit{Dom}(\sigma')}{\textbf{ref}\, \tilde{e}, \tilde{\sigma} \;\wr\; \overline{l, \tilde{\sigma}'[l \mapsto \tilde{v}], \varphi}}$$

SE-Deref
$$\frac{\tilde{e}, \tilde{\sigma} \;\wr\; \overline{l, \tilde{\sigma}', \varphi}}{!\tilde{e}, \tilde{\sigma} \;\wr\; \overline{\tilde{\sigma}'(l), \tilde{\sigma}', \varphi}}$$

SE-Assign
$$\frac{\tilde{e}_1, \tilde{\sigma} \;\wr\; \overline{l, \tilde{\sigma}', \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma}' \;\wr\; \overline{\tilde{v}_2, \tilde{\sigma}'', \varphi_2}}{\tilde{e}_1 := \tilde{e}_2, \tilde{\sigma} \;\wr\; \overline{\langle\rangle, \tilde{\sigma}''[l \mapsto \tilde{v}_2], \varphi_1 \wedge \varphi_2}}$$

SE-Edit
$$\frac{\tilde{e}, \tilde{\sigma} \;\wr\; \overline{\tilde{v}, \tilde{\sigma}', \varphi}}{\Box\, \tilde{e}, \tilde{\sigma} \;\wr\; \overline{\Box\, \tilde{v}, \tilde{\sigma}', \varphi}}$$

SE-Enter
$$\frac{}{\boxtimes \tau, \tilde{\sigma} \;\wr\; \boxtimes \tau, \tilde{\sigma}, \mathsf{True}}$$

SE-Update
$$\frac{\tilde{e}, \tilde{\sigma} \;\wr\; \overline{l, \tilde{\sigma}', \varphi}}{\blacksquare\, \tilde{e}, \tilde{\sigma} \;\wr\; \overline{\blacksquare\, l, \tilde{\sigma}', \varphi}}$$

SE-Then
$$\frac{\tilde{e}_1, \tilde{\sigma} \;\wr\; \overline{\tilde{t}_1, \tilde{\sigma}', \varphi}}{\tilde{e}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \;\wr\; \overline{\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \varphi}}$$

SE-Next
$$\frac{\tilde{e}_1, \tilde{\sigma} \;\wr\; \overline{\tilde{t}_1, \tilde{\sigma}', \varphi}}{\tilde{e}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \;\wr\; \overline{\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma}', \varphi}}$$

SE-And
$$\frac{\tilde{e}_1, \tilde{\sigma} \;\wr\; \overline{\tilde{t}_1, \tilde{\sigma}', \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma}' \;\wr\; \overline{\tilde{t}_2, \tilde{\sigma}'', \varphi_2}}{\tilde{e}_1 \bowtie \tilde{e}_2, \tilde{\sigma} \;\wr\; \overline{\tilde{t}_1 \bowtie \tilde{t}_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2}}$$

SE-Or
$$\frac{\tilde{e}_1, \tilde{\sigma} \;\wr\; \overline{\tilde{t}_1, \tilde{\sigma}', \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma}' \;\wr\; \overline{\tilde{t}_2, \tilde{\sigma}'', \varphi_2}}{\tilde{e}_1 \blacklozenge \tilde{e}_2, \tilde{\sigma} \;\wr\; \overline{\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2}}$$

SE-Xor
$$\frac{}{\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \;\wr\; \tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma}, \mathsf{True}}$$

SE-Fail
$$\frac{}{\lightning, \tilde{\sigma} \;\wr\; \lightning, \tilde{\sigma}, \mathsf{True}}$$

C.2 Symbolic striding rules

$$\boxed{\tilde{t}, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}', \tilde{\sigma}', \varphi}}$$

SS-ThenStay

$$\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \varphi}}{\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \varphi}} \mathcal{V}(\tilde{t}_1', \tilde{\sigma}') = \bot$$

SS-ThenFail

$$\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \varphi} \quad \tilde{e}_2\ \tilde{v}_1, \tilde{\sigma}' \lightning \overline{\tilde{t}_2, \tilde{\sigma}'', \_}}{\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \varphi}} \mathcal{V}(\tilde{t}_1', \tilde{\sigma}') = \tilde{v}_1 \wedge \mathcal{F}(\tilde{t}_2, \tilde{\sigma}'')$$

SS-ThenCont

$$\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \varphi_1} \quad \tilde{e}_2\ \tilde{v}_1, \tilde{\sigma}' \lightning \overline{\tilde{t}_2, \tilde{\sigma}'', \varphi_2}}{\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{t_2, \sigma'', \varphi_1 \wedge \varphi_2}} \mathcal{V}(\tilde{t}_1', \tilde{\sigma}') = \tilde{v}_1 \wedge \neg\mathcal{F}(\tilde{t}_2, \tilde{\sigma}'')$$

SS-OrLeft

$$\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \varphi}}{\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \varphi}} \mathcal{V}(\tilde{t}_1', \tilde{\sigma}') = \tilde{v}_1$$

SS-OrRight

$$\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \varphi_1} \quad \tilde{t}_2, \tilde{\sigma}' \rightsquigarrow \overline{\tilde{t}_2', \tilde{\sigma}'', \varphi_2}}{\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_2', \tilde{\sigma}'', \varphi_1 \wedge \varphi_2}} \mathcal{V}(\tilde{t}_1', \tilde{\sigma}') = \bot \wedge \mathcal{V}(\tilde{t}_2', \tilde{\sigma}'') = \tilde{v}_2$$

SS-OrNone

$$\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \varphi_1} \quad \tilde{t}_2, \tilde{\sigma}' \rightsquigarrow \overline{\tilde{t}_2', \tilde{\sigma}'', \varphi_2}}{\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \blacklozenge \tilde{t}_2', \tilde{\sigma}'', \varphi_1 \wedge \varphi_2}} \mathcal{V}(\tilde{t}_1', \tilde{\sigma}') = \bot \wedge \mathcal{V}(\tilde{t}_2', \tilde{\sigma}'') = \bot$$

SS-Edit

$$\frac{}{\square\, \tilde{v}, \tilde{\sigma} \rightsquigarrow \square\, \tilde{v}, \tilde{\sigma}, \mathsf{True}}$$

SS-Fill

$$\frac{}{\boxtimes\, \tau, \tilde{\sigma} \rightsquigarrow \boxtimes\, \tau, \tilde{\sigma}, \mathsf{True}}$$

SS-Update

$$\frac{}{\blacksquare\, l, \tilde{\sigma} \rightsquigarrow \blacksquare\, l, \tilde{\sigma}, \mathsf{True}}$$

SS-Fail

$$\frac{}{\lightning, \tilde{\sigma} \rightsquigarrow \lightning, \tilde{\sigma}, \mathsf{True}}$$

SS-Xor

$$\frac{}{\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma}, \mathsf{True}}$$

SS-Next

$$\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \varphi}}{\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \triangleright \tilde{e}_2, \tilde{\sigma}', \varphi}}$$

SS-And

$$\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \varphi_1} \quad \tilde{t}_2, \tilde{\sigma}' \rightsquigarrow \overline{\tilde{t}_2', \tilde{\sigma}'', \varphi_2}}{\tilde{t}_1 \bowtie \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \bowtie \tilde{t}_2', \tilde{\sigma}'', \varphi_1 \wedge \varphi_2}}$$

C.3 Symbolic normalisation rules

$$\boxed{\tilde{e}, \tilde{\sigma} \;\; \lll \;\; \overline{\tilde{t}, \tilde{\sigma}', \varphi}}$$

SN-Done

$$\frac{\tilde{e}, \tilde{\sigma} \;\; \swarrow \;\; \overline{\tilde{t}, \tilde{\sigma}', \varphi_1} \qquad \tilde{t}, \tilde{\sigma}' \;\; \rightsquigarrow \;\; \overline{\tilde{t}', \tilde{\sigma}'', \varphi_2}}{\tilde{e}, \tilde{\sigma} \;\; \lll \;\; \overline{\tilde{t}, \tilde{\sigma}', \varphi_1}} \; \tilde{\sigma}' = \tilde{\sigma}'' \wedge \tilde{t} = \tilde{t}'$$

SN-Repeat

$$\frac{\tilde{e}, \tilde{\sigma} \;\; \swarrow \;\; \overline{\tilde{t}, \tilde{\sigma}', \varphi_1} \qquad \tilde{t}, \tilde{\sigma}' \;\; \rightsquigarrow \;\; \overline{\tilde{t}', \tilde{\sigma}'', \varphi_2} \qquad \tilde{t}', \tilde{\sigma}'' \;\; \lll \;\; \overline{\tilde{t}'', \tilde{\sigma}''', \varphi_3}}{\tilde{e}, \tilde{\sigma} \;\; \lll \;\; \overline{\tilde{t}'', \tilde{\sigma}''', \varphi_1 \wedge \varphi_2 \wedge \varphi_3}} \; \tilde{\sigma}' \neq \tilde{\sigma}'' \vee \tilde{t} \neq \tilde{t}'$$

C.4 Symbolic driving rules

$$\boxed{\tilde{t}, \tilde{\sigma} \;\; \twoheadrightarrow \;\; \overline{\tilde{t}', \tilde{\sigma}', \tilde{\imath}, \varphi}}$$

SI-Handle

$$\frac{\tilde{t}, \tilde{\sigma} \;\; \rightsquigarrow \;\; \overline{\tilde{t}', \tilde{\sigma}', \tilde{\imath}, \varphi_1} \qquad \tilde{t}', \tilde{\sigma}' \;\; \lll \;\; \overline{\tilde{t}'', \tilde{\sigma}'', \varphi_2}}{\tilde{t}, \tilde{\sigma} \;\; \twoheadrightarrow \;\; \overline{\tilde{t}'', \tilde{\sigma}'', \tilde{\imath}, \varphi_1 \wedge \varphi_2}}$$

C.5 Symbolic handling rules

$$\boxed{\tilde{t}, \tilde{\sigma} \;\rightsquigarrow\; \overline{\tilde{t}', \tilde{\sigma}', \tilde{\imath}, \varphi}}$$

SH-Change
$$\frac{\text{fresh } s}{\square\, \tilde{v}, \tilde{\sigma} \;\rightsquigarrow\; \square\, s, \tilde{\sigma}, s, \mathsf{True}}\; \tilde{v}, s : \tau$$

SH-Fill
$$\frac{\text{fresh } \tilde{s}}{\boxtimes\, \tau, \tilde{\sigma} \;\rightsquigarrow\; \square\, s, \tilde{\sigma}, s, \mathsf{True}}\; s : \tau$$

SH-Update
$$\frac{\text{fresh } s}{\blacksquare\, l, \tilde{\sigma} \;\rightsquigarrow\; \blacksquare\, l, \tilde{\sigma}[l \mapsto s], s, \mathsf{True}}\; \sigma(l), s : \tau$$

SH-PassNext
$$\frac{\tilde{t}_1, \tilde{\sigma} \;\rightsquigarrow\; \overline{\tilde{t}_1', \tilde{\sigma}', \tilde{\imath}, \varphi}}{\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \;\rightsquigarrow\; \overline{\tilde{t}_1' \triangleright \tilde{e}_2, \tilde{\sigma}', \tilde{\imath}, \varphi}}\; \mathcal{V}(\tilde{t}_1, \tilde{\sigma}) = \bot$$

SH-PassNextFail
$$\frac{\tilde{t}_1, \tilde{\sigma} \;\rightsquigarrow\; \overline{\tilde{t}_1', \tilde{\sigma}_1', \tilde{\imath}, \varphi} \qquad \tilde{e}_2\; \tilde{v}_1, \tilde{\sigma} \;\lll\; \overline{\tilde{t}_2, \tilde{\sigma}_2', \_}}{\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \;\rightsquigarrow\; \overline{\tilde{t}_1' \triangleright \tilde{e}_2, \tilde{\sigma}_1', \tilde{\imath}, \varphi}}\; \mathcal{V}(\tilde{t}_1, \tilde{\sigma}) = \tilde{v}_1 \wedge \mathcal{F}(\tilde{t}_2, \tilde{\sigma}_2')$$

SH-Next
$$\frac{\tilde{t}_1, \tilde{\sigma} \;\rightsquigarrow\; \overline{\tilde{t}_1', \tilde{\sigma}_1', \tilde{\imath}, \varphi_1} \qquad \tilde{e}_2\; \tilde{v}_1, \tilde{\sigma} \;\lll\; \overline{\tilde{t}_2, \tilde{\sigma}_2', \varphi_2}}{\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \;\rightsquigarrow\; \overline{\tilde{t}_1' \triangleright \tilde{e}_2, \tilde{\sigma}_1', \tilde{\imath}, \varphi_1} \cup \overline{\tilde{t}_2, \tilde{\sigma}_2', \mathsf{C}, \varphi_2}}\; \mathcal{V}(\tilde{t}_1, \tilde{\sigma}) = \tilde{v}_1 \wedge \neg\mathcal{F}(\tilde{t}_2, \tilde{\sigma}')$$

SH-PassThen
$$\frac{\tilde{t}_1, \tilde{\sigma} \;\rightsquigarrow\; \overline{\tilde{t}_1', \tilde{\sigma}', \tilde{\imath}, \varphi}}{\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \;\rightsquigarrow\; \overline{\tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \tilde{\imath}, \varphi}}$$

SH-Pick
$$\frac{\tilde{e}_1, \tilde{\sigma} \;\Downarrow\; \overline{\tilde{t}_1, \tilde{\sigma}_1, \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma} \;\Downarrow\; \overline{\tilde{t}_2, \tilde{\sigma}_2, \varphi_2}}{\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \;\rightsquigarrow\; \overline{\tilde{t}_1, \tilde{\sigma}_1, \mathsf{L}, \varphi_1} \cup \overline{\tilde{t}_2, \tilde{\sigma}_2, \mathsf{R}, \varphi_2}}\; \neg\mathcal{F}(\tilde{t}_1, \tilde{\sigma}_1) \wedge \neg\mathcal{F}(\tilde{t}_2, \tilde{\sigma}_2)$$

SH-PickLeft
$$\frac{\tilde{e}_1, \tilde{\sigma} \;\lll\; \overline{\tilde{t}_1, \tilde{\sigma}_1, \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma} \;\lll\; \overline{\tilde{t}_2, \tilde{\sigma}_2, \varphi_2}}{\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \;\rightsquigarrow\; \tilde{t}_1, \tilde{\sigma}_1, \mathsf{L}, \varphi_1}\; \neg\mathcal{F}(\tilde{t}_1, \tilde{\sigma}_1) \wedge \mathcal{F}(\tilde{t}_2, \tilde{\sigma}_2)$$

SH-PickRight
$$\frac{\tilde{e}_1, \tilde{\sigma} \;\lll\; \overline{\tilde{t}_1, \tilde{\sigma}_1, \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma} \;\lll\; \overline{\tilde{t}_2, \tilde{\sigma}_2, \varphi_2}}{\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \;\rightsquigarrow\; \tilde{t}_2, \tilde{\sigma}_2, \mathsf{R}, \varphi_2}\; \mathcal{F}(\tilde{t}_1, \tilde{\sigma}_1) \wedge \neg\mathcal{F}(\tilde{t}_2, \tilde{\sigma}_2)$$

SH-And
$$\frac{\tilde{t}_1, \tilde{\sigma} \;\rightsquigarrow\; \overline{\tilde{t}_1', \tilde{\sigma}_1', \tilde{\imath}_1, \varphi_1} \qquad \tilde{t}_2, \tilde{\sigma} \;\rightsquigarrow\; \overline{\tilde{t}_2', \tilde{\sigma}_2', \tilde{\imath}_2, \varphi_2}}{\tilde{t}_1 \bowtie \tilde{t}_2, \tilde{\sigma} \;\rightsquigarrow\; \overline{\tilde{t}_1' \bowtie \tilde{t}_2, \tilde{\sigma}_1', \mathsf{F}\, \tilde{\imath}_1, \varphi_1} \cup \overline{\tilde{t}_1 \bowtie \tilde{t}_2', \tilde{\sigma}_2'', \mathsf{S}\, \tilde{\imath}_2, \varphi_2}}$$

SH-Or
$$\frac{\tilde{t}_1, \tilde{\sigma} \;\rightsquigarrow\; \overline{\tilde{t}_1', \tilde{\sigma}_1', \tilde{\imath}_1, \varphi_1} \qquad \tilde{t}_2, \tilde{\sigma} \;\rightsquigarrow\; \overline{\tilde{t}_2', \tilde{\sigma}_2', \tilde{\imath}_2, \varphi_2}}{\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma} \;\rightsquigarrow\; \overline{\tilde{t}_1' \blacklozenge \tilde{t}_2, \tilde{\sigma}_1', \mathsf{F}\, \tilde{\imath}_1, \varphi_1} \cup \overline{\tilde{t}_1 \blacklozenge \tilde{t}_2', \tilde{\sigma}_2', \mathsf{S}\, \tilde{\imath}_2, \varphi_2}}$$

D Soundness proofs

Proof (Soundness of simulate). The structure of this proof is outlined in Fig. 6.

We have t and σ such that $t, \sigma \;\tilde{\approx}^*\; \overline{\tilde{v}, \tilde{I}, \Phi}$. By definition of simulation ($\tilde{\approx}^*$), we know that for each tuple $(\tilde{v}, \tilde{I}, \Phi)$, the following sequence of symbolic drive steps has occurred.

$$
\begin{array}{llll}
t, \sigma \;\tilde{\approx}\; \tilde{t}_1, \tilde{\sigma}_1, \tilde{\imath}_1, \varphi_1 & & & \\
\quad \tilde{t}_1, \tilde{\sigma}_1 \;\tilde{\approx}\; & \tilde{t}_2, \tilde{\sigma}_2, \tilde{\imath}_2, \varphi_2 & & \\
& \quad \tilde{t}_2, \tilde{\sigma}_2 \;\tilde{\approx}\; \cdots & & \\
& & \cdots & \tilde{\approx}\; \tilde{t}_n, \tilde{\sigma}_n, \tilde{\imath}_n, \varphi_n
\end{array}
$$

with $\mathcal{V}(\tilde{t}_n, \tilde{\sigma}_n) = \tilde{v}$ and $\mathcal{S}(\varphi_1 \wedge \cdots \wedge \varphi_n)$.

We need to show that there exits an I such that $t, \sigma \overset{I}{\Rightarrow}^* v$, which is defined similarly as follows.

$t, \sigma \overset{i_1}{\Rightarrow} t_1, \sigma_1 \overset{i_2}{\Rightarrow} t_2, \sigma_2 \overset{i_3}{\Rightarrow} \cdots \overset{i_n}{\Rightarrow} t_n, \sigma_n$ with $\mathcal{V}(t_n, \sigma_n)$.

By Lemma 3, we know that $t, \sigma \overset{i_1}{\Rightarrow} t_1, \sigma_1$ exists, since $t, \sigma \leftrightarrows_{\emptyset} t, \sigma, \mathsf{True}$. This also gives us that $\tilde{\imath}_1 \sim i_1$, and $t_1, \sigma_1 \leftrightarrows_{[s_1 \mapsto c_1]} \tilde{t}_1, \tilde{\sigma}_1, \varphi_1$ with $\mathit{SymOf}(\sim_1) = s_1$ and $\mathit{ValOf}(i_1) = c_1$.

By repeatedly applying Lemma 3, until we arrive at $\tilde{t}_n, \sigma t_n$, we can show that there indeed exists an I such that $t, \sigma \overset{I}{\Rightarrow}^* v$ with $[s_1 \mapsto c_1, \cdots, s_n \mapsto c_n]\tilde{v} = v$ and $[s_1 \mapsto c_1, \cdots, s_n \mapsto c_n]\Phi$, namely $I = [i_1, \cdots, i_n]$.

Proof (Soundness of driving). The symbolic driving semantics consists of only one rule, SI-Handle. Given that $t, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\tilde{t}, \tilde{\sigma} \;\tilde{\approx}\; \overline{\tilde{t}', \tilde{\sigma}', \tilde{\imath}, \varphi_1}$, Lemma 5 gives us that for each pair $(\tilde{t}', \tilde{\sigma}', \tilde{\imath}, \varphi_1)$ there exists an input i such that $\tilde{\imath} \sim i$, $t, \sigma \xrightarrow{i} t', \sigma'$ and $t', \sigma' \leftrightarrows_{M.[s \mapsto c]} \tilde{t}', \tilde{\sigma}', \Phi \wedge \varphi_1$.

Then, by Lemma 6, given that $\tilde{t}', \tilde{\sigma}' \Downarrow \overline{\tilde{t''}, \tilde{\sigma''}', \varphi_2}$, we obtain that for each pair $(\tilde{t''}, \tilde{\sigma''}', \varphi_2)$, we have that $\mathcal{S}(\Phi \wedge \varphi_1 \wedge \varphi_2)$ implies that $t', \sigma' \lessapprox t'', \sigma''$ with $t'', \sigma'' \leftrightarrows_{M.[s \mapsto c]} \tilde{t''}, \tilde{\sigma''}, \Phi \wedge \varphi_1 \wedge \varphi_2$.

Lemma 5 (Soundness of handling).
For all concrete tasks t, concrete states σ, symbolic tasks $\tilde{t}$, symbolic states $\tilde{\sigma}$ path conditions Φ and mappings M, we have that $t, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ implies that for all symbolic inputs $\tilde{\imath}$ such that $\tilde{t}, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}', \tilde{\sigma}', \tilde{\imath}, \varphi}$ and for all pairs $(\tilde{t}', \tilde{\sigma}', \tilde{\imath}, \varphi)$, $\mathcal{S}(\Phi \wedge \varphi)$ implies that there exists an input i such that $\tilde{\imath} \sim i$, $t, \sigma \xrightarrow{i} t', \sigma'$ and $t', \sigma' \leftrightarrows_{M.[s \mapsto c]} \tilde{t}', \tilde{\sigma}', \Phi \wedge \varphi$ where where $\mathit{SymOf}(\tilde{\imath}) = s$ and $\mathit{ValOf}(i) = c$.

Lemma 6 (Soundness of normalisation). *For all concrete expressions e, concrete states σ, symbolic expressions $\tilde{e}$, symbolic states $\tilde{\sigma}$ path conditions Φ and mappings M, we have that $e, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ implies that if $\tilde{e}, \tilde{\sigma} \lessapprox \overline{\tilde{t}, \tilde{\sigma}', \varphi}$, then for all pairs $(\tilde{t}, \tilde{\sigma}', \varphi)$ it holds that $\mathcal{S}(\Phi \wedge \varphi)$ implies that $e, \sigma \Downarrow t, \sigma'$ with $t, \sigma' \leftrightarrows_M \tilde{t}, \tilde{\sigma}', \Phi \wedge \varphi$.*

Lemma 7 (Soundness of striding). *for all concrete tasks t, concrete states σ, symbolic tasks $\tilde{t}$, symbolic states $\tilde{\sigma}$ path conditions Φ and mappings M, we have that $t, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ implies that if $\tilde{t}, \tilde{\sigma} \rightarrowtail \overline{\tilde{t}', \tilde{\sigma}', \varphi}$, then for all pairs $(\tilde{t}', \tilde{\sigma}', \varphi)$ it holds that $\mathcal{S}(\Phi \wedge \varphi)$ implies that $t, \sigma \rightarrowtail t', \sigma'$ with $t', \sigma' \leftrightarrows_M \tilde{t}', \tilde{\sigma}', \Phi \wedge \varphi$.*

Lemma 8 (Soundness of evaluation). *For all concrete expressions e, concrete states σ, symbolic expressions $\tilde{e}$, symbolic states $\tilde{\sigma}$ path conditions Φ and mappings M, we have that $e, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ implies that if $\tilde{e}, \tilde{\sigma} \rightsquigarrow \overline{\tilde{v}, \tilde{\sigma}', \varphi}$, then for all pairs $(\tilde{v}, \tilde{\sigma}', \varphi)$ it holds that $\mathcal{S}(\Phi \wedge \varphi)$ implies that $e, \sigma \rightsquigarrow v, \sigma'$ with $v, \sigma' \leftrightarrows_M \tilde{v}, \tilde{\sigma'}, \Phi \wedge \varphi$.*

Proof (Soundness of handle).

We prove Lemma 5 by induction over $\tilde{t}$.

Case $\tilde{t} = \boxtimes\, \tau$

Since we have $t, \sigma \leftrightarrows_M \boxtimes\, \tau, \tilde{\sigma}, \Phi$, we know that t must be $\boxtimes\, \tau$ too, $\tilde{t}$ contains no symbols. There exists only one symbolic execution, namely $\dfrac{\text{SH-Fill}\quad \text{fresh } \tilde{s}}{\boxtimes\, \tau, \tilde{\sigma} \rightsquigarrow \square\, s, \tilde{\sigma}, s, \text{True}}\ s : \tau$.

We need to show that there exists an i such that $s \sim i$ and $\square\, v, \sigma \xrightarrow{i} t', \sigma'$.

Any concrete value c of type τ will do. Now we have to show that we end up with $\square\, c, \sigma \leftrightarrows_{M.[s \mapsto c]} \square\, s, \tilde{\sigma}, \Phi \wedge \text{True}$, which holds trivially.

Case $\tilde{t} = \square\, \tilde{v}$

Since we have $t, \sigma \leftrightarrows_M \square\, \tilde{v}, \tilde{\sigma}, \Phi$, we know that either $\tilde{v}$ is a concrete value, or M contains a mapping such that $M\tilde{v}$ becomes a concrete value c. We know therefore that t must be $\square\, c$.

There exists only one symbolic execution, namely $\dfrac{\text{SH-Change}\quad \text{fresh } s}{\square\, \tilde{v}, \tilde{\sigma} \rightsquigarrow \square\, s, \tilde{\sigma}, s, \text{True}}\ \tilde{v}, s : \tau$.

We need to show that there exists an i such that $s \sim i$ and $\square\, c, \sigma \xrightarrow{i} t', \sigma'$.

Any concrete value c' of the same type as c will do. Now we have to show that we end up with $\square\, c', \sigma \leftrightarrows_{M.[s \mapsto c']} \square\, s, \tilde{\sigma}, \Phi \wedge \text{True}$, which holds trivially.

Case $\tilde{t} = \blacksquare\, l$

Since we have $t, \sigma \leftrightarrows_M \blacksquare\, l, \tilde{\sigma}, \Phi$, we know that t must be $\blacksquare\, l$ too, $\tilde{t}$ contains no symbols. There exists only one symbolic execution, namely $\dfrac{\text{SH-Update}\quad \text{fresh } s}{\blacksquare\, l, \tilde{\sigma} \rightsquigarrow \blacksquare\, l, \tilde{\sigma}[l \mapsto s], s, \text{True}}\ \sigma(l), s : \tau$.

We need to show that there exists an i such that $s \sim i$ and $\blacksquare\, l, \sigma \xrightarrow{i} t', \sigma'$.

Any concrete value c of the same type as l will do. Now we have to show that we end up with $\blacksquare\, l, \sigma[l \mapsto c] \leftrightarrows_{M.[s \mapsto c]} \blacksquare\, l, \tilde{\sigma}[l \mapsto s], \Phi \wedge \text{True}$, which holds trivially.

Case $\tilde{t} = \tilde{t}_1 \triangleright \tilde{e}_2$

Since we have $t, \sigma \leftrightarrows_M \tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma}, \Phi$, we know that $M\tilde{t}_1 \triangleright \tilde{e}_2 = t$, which comes down to $t_1 \triangleright e_2$ for some concrete t_1 and e_2.

In this case, three rules apply.

Case $\dfrac{\text{SH-Next}\quad \tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}_1', \tilde{\imath}, \varphi_1} \qquad \tilde{e}_2\ \tilde{v}_1, \tilde{\sigma} \lessdot\!\!\lessdot \overline{\tilde{t}_2, \tilde{\sigma}_2', \varphi_2}}{\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \triangleright \tilde{e}_2, \tilde{\sigma}_1', \tilde{\imath}, \varphi_1} \cup \overline{\tilde{t}_2, \tilde{\sigma}_2', \mathsf{C}, \varphi_2}}\ \mathcal{V}(\tilde{t}_1, \tilde{\sigma}) = \tilde{v}_1 \wedge \neg \mathcal{F}(\tilde{t}_2, \tilde{\sigma}')$

In this case, we have two sets of symbolic executions.

For all tuples $(\tilde{t}_1' \triangleright \tilde{e}_2, \tilde{\sigma}_1', \tilde{\imath}, \varphi_1)$, we know by application of the induction hypothesis that there exits an i such that $\tilde{\imath} \sim i$, $t_1, \sigma \xrightarrow{i} t_1', \sigma'$ and $t_1', \sigma' \leftrightarrows_{M.[s \mapsto c]} \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$ where $\mathit{ValOf}(i) = c$ and $\mathit{ValOf}(\tilde{\imath}) = s$. Therefore we also have $t_1' \triangleright e_2, \sigma_1' \leftrightarrows_{M.[s \mapsto c]} \tilde{t}_1' \triangleright \tilde{e}_2, \tilde{\sigma}_1', \Phi \wedge \varphi_1$.

For all tuples $(\tilde{t}_2, \tilde{\sigma}_2', \mathsf{C}, \varphi_2)$, we first have by Lemma 9 that $v_1, \sigma \leftrightarrows_M \tilde{v}_1, \tilde{\sigma}, \Phi$. Now, before we can apply Lemma 6, we need to establish that $e_2\ v_1, \sigma \leftrightarrows_M \tilde{e}_2\ \tilde{v}_1, \tilde{\sigma}, \Phi$ holds. This means that we have to show that $M\tilde{e}_2\ \tilde{v}_1 = e_2\ v_1$. Since application of the mapping is distributive, it suffices to show that $M\tilde{v}_1 = v_1$, which is given, and $M\tilde{e}_2 = e_2$, which follows from the premise as well.

At this point, by application of Lemma 6, we obtain that $e_2\ v_1, \sigma \Downarrow t_2, \sigma_2'$ and $t_1, \sigma_2' \leftrightarrows_M \tilde{t}_2, \tilde{\sigma}_2', \Phi \wedge \varphi_2$

Case $\dfrac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \tilde{\imath}, \varphi}}{\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \triangleright \tilde{e}_2, \tilde{\sigma}', \tilde{\imath}, \varphi}}\ \text{SH-PassNext}\ \mathcal{V}(\tilde{t}_1, \tilde{\sigma}) = \bot$

For all tuples $(\tilde{t}_1' \triangleright \tilde{e}_2, \tilde{\sigma}_1', \tilde{\imath}, \varphi_1)$, we know by application of the induction hypothesis that there exits an i such that $\tilde{\imath} \sim i, t_1, \sigma \xrightarrow{i} t_1', \sigma'$ and $t_1', \sigma' \leftrightarrows_{M.[s \mapsto c]} \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$ where $\mathit{ValOf}(i) = c$ and $\mathit{ValOf}(\tilde{\imath}) = s$. Therefore we also have $t_1' \triangleright e_2, \sigma_1' \leftrightarrows_{M.[s \mapsto c]} \tilde{t}_1' \triangleright \tilde{e}_2, \tilde{\sigma}_1', \Phi \wedge \varphi_1$.

Case $\dfrac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}_1', \tilde{\imath}, \varphi} \qquad \tilde{e}_2\ \tilde{v}_1, \tilde{\sigma} \lightning \overline{\tilde{t}_2, \tilde{\sigma}_2', \_}}{\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \triangleright \tilde{e}_2, \tilde{\sigma}_1', \tilde{\imath}, \varphi}}\ \text{SH-PassNextFail}\ \mathcal{V}(\tilde{t}_1, \tilde{\sigma}) = \tilde{v}_1 \wedge \mathcal{F}(\tilde{t}_2, \tilde{\sigma}_2')$

For all tuples $(\tilde{t}_1' \triangleright \tilde{e}_2, \tilde{\sigma}_1', \tilde{\imath}, \varphi_1)$, we know by application of the induction hypothesis that there exits an i such that $\tilde{\imath} \sim i, t_1, \sigma \xrightarrow{i} t_1', \sigma'$ and $t_1', \sigma' \leftrightarrows_{M.[s \mapsto c]} \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$ where $\mathit{ValOf}(i) = c$ and $\mathit{ValOf}(\tilde{\imath}) = s$. Therefore we also have $t_1' \triangleright e_2, \sigma_1' \leftrightarrows_{M.[s \mapsto c]} \tilde{t}_1' \triangleright \tilde{e}_2, \tilde{\sigma}_1', \Phi \wedge \varphi_1$.

Case $\tilde{t} = \tilde{t}_1 \blacktriangleright \tilde{e}_2$

One rule applies, namely $\dfrac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \tilde{\imath}, \varphi}}{\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \tilde{\imath}, \varphi}}\ \text{SH-PassThen}$

For all tuples $(\tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \tilde{\imath}, \varphi)$, we know by application of the induction hypothesis that there exists an i such that $\tilde{\imath} \sim i, t_1, \sigma \xrightarrow{1} t_1', \sigma'$ and $t_1', \sigma' \leftrightarrows_{M.[s \mapsto c]} \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$ where $\mathit{ValOf}(i) = c$ and $\mathit{SymOf}(\tilde{\imath}) = s$. Therefore we also have $t_1' \blacktriangleright e_2, \sigma_1' \leftrightarrows_{M.[s \mapsto c]} \tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}_1', \Phi \wedge \varphi_1, M.[s \mapsto c]$).

Case $\tilde{t} = \tilde{e}_1 \lozenge \tilde{e}_2$

In this case, three rules apply.

Case $\dfrac{\tilde{e}_1, \tilde{\sigma} \Downarrow \overline{\tilde{t}_1, \tilde{\sigma}_1, \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma} \Downarrow \overline{\tilde{t}_2, \tilde{\sigma}_2, \varphi_2}}{\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1, \tilde{\sigma}_1, \mathsf{L}, \varphi_1} \cup \overline{\tilde{t}_2, \tilde{\sigma}_2, \mathsf{R}, \varphi_2}}\ \text{SH-Pick}\ \neg\mathcal{F}(\tilde{t}_1, \tilde{\sigma}_1) \wedge \neg\mathcal{F}(\tilde{t}_2, \tilde{\sigma}_2)$

In this case, we have two sets of symbolic executions.

For all tuples $(\tilde{t}_1, \tilde{\sigma}_1, \mathsf{L}, \varphi_1)$, we obtain from Lemma 6 that $e_1, \sigma \Downarrow t_1, \sigma_1$ with $t_1, \sigma_1 \leftrightarrows_M \tilde{t}_1, \tilde{\sigma}_1, \Phi \wedge \varphi_1$.

For all tuples $(\tilde{t}_2, \tilde{\sigma}_2, \mathsf{R}, \varphi_2)$, we obtain from Lemma 6 that $e_2, \sigma \Downarrow t_2, \sigma_2$ with $t_2, \sigma_2 \leftrightarrows_M \tilde{t}_2, \tilde{\sigma}_2, \Phi \wedge \varphi_2$.

Case $\dfrac{\tilde{e}_1, \tilde{\sigma} \lll \overline{\tilde{t}_1, \tilde{\sigma}_1, \varphi_1} \quad \tilde{e}_2, \tilde{\sigma} \lll \overline{\tilde{t}_2, \tilde{\sigma}_2, \varphi_2}}{\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \tilde{t}_1, \tilde{\sigma}_1, \mathsf{L}, \varphi_1}\ \text{SH-PickLeft}\ \neg\mathcal{F}(\tilde{t}_1, \tilde{\sigma}_1) \wedge \mathcal{F}(\tilde{t}_2, \tilde{\sigma}_2)$

For all tuples $(\tilde{t}_1, \tilde{\sigma}_1, \mathsf{L}, \varphi_1)$, we obtain from Lemma 6 that $e_1, \sigma \Downarrow t_1, \sigma_1$ with $t_1, \sigma_1 \leftrightarrows_M \tilde{t}_1, \tilde{\sigma}_1, \Phi \wedge \varphi_1$.

Case $\dfrac{\tilde{e}_1, \tilde{\sigma} \lll \overline{\tilde{t}_1, \tilde{\sigma}_1, \varphi_1} \quad \tilde{e}_2, \tilde{\sigma} \lll \overline{\tilde{t}_2, \tilde{\sigma}_2, \varphi_2}}{\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \tilde{t}_2, \tilde{\sigma}_2, \mathsf{R}, \varphi_2}\ \text{SH-PickRight}\ \mathcal{F}(\tilde{t}_1, \tilde{\sigma}_1) \wedge \neg\mathcal{F}(\tilde{t}_2, \tilde{\sigma}_2)$

For all tuples $(\tilde{t}_2, \tilde{\sigma}_2, \mathsf{R}, \varphi_2)$, we obtain from Lemma 6 that $e_2, \sigma \Downarrow t_2, \sigma_2$ with $t_2, \sigma_2 \leftrightarrows_M \tilde{t}_2, \tilde{\sigma}_2, \Phi \wedge \varphi_2$.

Case $\tilde{t} = \tilde{t}_1 \bowtie \tilde{t}_2$

In this case, one rule applies. $\dfrac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}'_1, \tilde{\sigma}'_1, \tilde{\imath}_1, \varphi_1} \quad \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}'_2, \tilde{\sigma}'_2, \tilde{\imath}_2, \varphi_2}}{\tilde{t}_1 \bowtie \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}'_1 \bowtie \tilde{t}_2, \tilde{\sigma}'_1, \mathsf{F}\,\tilde{\imath}_1, \varphi_1} \cup \overline{\tilde{t}_1 \bowtie \tilde{t}'_2, \tilde{\sigma}''_2, \mathsf{S}\,\tilde{\imath}_2, \varphi_2}}\ \text{SH-And}$

In this case, we have two sets of symbolic executions.

For all tuples $(\tilde{t}'_1 \bowtie \tilde{t}_2, \tilde{\sigma}'_1, \mathsf{F}\,\tilde{\imath}_1, \varphi_1)$, we know by application of the induction hypothesis that there exists an i such that $\tilde{\imath}_1 \sim i, t_1, \sigma \xrightarrow{i} t'_1, \sigma'_1$ and $t'_1, \sigma'_1 \leftrightarrows_{M.[s \mapsto c]} \tilde{t}'_1, \tilde{\sigma}'_1, \Phi \wedge \varphi_1$. Then by H-FirstAnd, we know that also $t_1 \bowtie t_2, \sigma \xrightarrow{\mathsf{F}\,i} t'_1 \bowtie t_2, \sigma'_1$. It follows trivially that $t'_1 \bowtie t_2, \sigma'_1 \leftrightarrows_{M.[s \mapsto c]} \tilde{t}'_1 \bowtie \tilde{t}_2, \tilde{\sigma}'_1, \Phi \wedge \varphi_1$.

For all tuples $(\tilde{t}_1 \bowtie \tilde{t}'_2, \tilde{\sigma}'_2, \mathsf{S}\,\tilde{\imath}_2, \varphi_2)$, we know by application of the induction hypothesis that there exists an i such that $\tilde{\imath}_2 \sim i, t_2, \sigma \xrightarrow{i} t'_2, \sigma'_2$ and $t'_2, \sigma'_2 \leftrightarrows_{M.[s \mapsto c]} \tilde{t}'_2, \tilde{\sigma}'_2, \Phi \wedge \varphi_2$. Then by H-SecondAnd, we know that also $t_1 \bowtie t_2, \sigma \xrightarrow{\mathsf{S}\,i} t_1 \bowtie t'_2, \sigma'_2$. It follows trivially that $t_1 \bowtie t'_2, \sigma'_2 \leftrightarrows_{M.[s \mapsto c]} \tilde{t}_1 \bowtie \tilde{t}'_2, \tilde{\sigma}'_2, \Phi \wedge \varphi_2$.

Case $\tilde{t} = \tilde{e}_1 \blacklozenge \tilde{e}_2$

One rule applies, namely $\dfrac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}'_1, \tilde{\sigma}'_1, \tilde{\imath}_1, \varphi_1} \quad \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}'_2, \tilde{\sigma}'_2, \tilde{\imath}_2, \varphi_2}}{\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}'_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}'_1, \mathsf{F}\,\tilde{\imath}_1, \varphi_1} \cup \overline{\tilde{t}_1 \blacklozenge \tilde{t}'_2, \tilde{\sigma}'_2, \mathsf{S}\,\tilde{\imath}_2, \varphi_2}}\ \text{SH-Or}$

In this case, we have two sets of symbolic executions.

For all tuples $(\tilde{t}'_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}'_1, \mathsf{F}\,\tilde{\imath}_1, \varphi_1)$, we know by application of the induction hypothesis that there exists an i such that $\tilde{\imath}_1 \sim i, t_1, \sigma \xrightarrow{i} t'_1, \sigma'_1$ and $t'_1, \sigma'_1 \leftrightarrows_{M.[s \mapsto c]} \tilde{t}'_1, \tilde{\sigma}'_1, \Phi \wedge \varphi_1$. Then by H-FirstOr, we know that also $t_1 \blacklozenge t_2, \sigma \xrightarrow{\mathsf{F}\,i} t'_1 \blacklozenge t_2, \sigma'_1$. It follows trivially that $t'_1 \blacklozenge t_2, \sigma'_1 \leftrightarrows_{M.[s \mapsto c]} \tilde{t}'_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}'_1, \Phi \wedge \varphi_1$.

For all tuples $(\tilde{t}_1 \blacklozenge \tilde{t}_2', \tilde{\sigma}_2', \mathrm{S}\,\tilde{\imath}_2, \varphi_2)$, we know by application of the induction hypothesis that there exists an i such that $\tilde{\imath}_2 \sim i$, $t_2, \sigma \xrightarrow{i} t_2', \sigma_2'$ and $t_2', \sigma_2' \leftrightarrows_{M.[s \mapsto c]} \tilde{t}_2', \tilde{\sigma}_2', \Phi \wedge \varphi_2$. Then by H-SecondOr, we know that also $t_1 \blacklozenge t_2, \sigma \xrightarrow{\mathrm{S}\,i} t_1 \blacklozenge t_2', \sigma_2'$. It follows trivially that $t_1 \blacklozenge t_2', \sigma_2' \leftrightarrows_{M.[s \mapsto c]} \tilde{t}_1 \blacklozenge \tilde{t}_2', \tilde{\sigma}_2', \Phi \wedge \varphi_2$.

Lemma 9 ($\mathcal{V}$ preserves consistence). *For all concrete tasks t, concrete states σ, symbolic tasks $\tilde{t}$, symbolic states $\tilde{\sigma}$, path conditions Φ and mappings $M = [s_1 \mapsto c_1 \cdots s_n \mapsto c_n]$, if $t, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\mathcal{V}(t, \sigma) = v$ and $\mathcal{V}(\tilde{t}, \tilde{\sigma})$, then also $v, \sigma \leftrightarrows_M \tilde{v}, \tilde{\sigma}, \Phi$*

Proof ($\mathcal{V}$ preserves consistence).

Case $\tilde{t} = \square\, s$

If we have $t, \sigma \leftrightarrows_M \square\, s, \tilde{\sigma}, \Phi$, then we know that t must be $\square\, c$ for some concrete value of the same type as s.

Then by definition of $\mathcal{V}$, we have $\mathcal{V}(\square\, c, \sigma) = c$ and $\mathcal{V}(\square\, s, \tilde{\sigma}) = s$. Since we have $M(\square\, s) = \square\, c$ from the premise, we know that $Ms = c$, since mapping propagates. Therefore $c, \sigma \leftrightarrows_M s, \tilde{\sigma}, \Phi$.

Case $\tilde{t} = \boxtimes\, \tau$

If we have $t, \sigma \leftrightarrows_M \boxtimes\, \tau, \tilde{\sigma}, \Phi$, then we know that t is also $\boxtimes\, \tau$.

By definition of $\mathcal{V}$, $\mathcal{V}(\boxtimes\, \tau, \sigma) = \bot$ and $\mathcal{V}(\boxtimes\, \tau, \tilde{\sigma}) = \bot$, so this case holds trivially.

Case $\tilde{t} = \blacksquare\, l$

If we have $t, \sigma \leftrightarrows_M \blacksquare\, l, \tilde{\sigma}, \Phi$, then we know that t is also $\blacksquare\, l$.

By definition of $\mathcal{V}$, $\mathcal{V}(\blacksquare\, l, \sigma) = \sigma(l)$ and $\mathcal{V}(\blacksquare\, l, \tilde{\sigma}) = \tilde{\sigma}(l)$.

We now need to show that $M(\tilde{\sigma}(l)) = \sigma(l)$. From the premise we know that $M\tilde{\sigma} = \sigma$, from which this immediately follows.

Case $\tilde{t} = \lightning$

If we have $t, \sigma \leftrightarrows_M \lightning, \tilde{\sigma}, \Phi$, then we know that t is also $\lightning$.

By definition of $\mathcal{V}$, $\mathcal{V}(\lightning, \sigma) = \bot$ and $\mathcal{V}(\lightning, \tilde{\sigma}) = \bot$, so we know that this case holds trivially.

Case $\tilde{t} = \tilde{t}_1 \blacktriangleright \tilde{e}_2$

If we have $t, \sigma \leftrightarrows_M \tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}, \Phi$, then we know that t is $t_1 \blacktriangleright e_2$.

By definition of $\mathcal{V}$, $\mathcal{V}(t_1 \blacktriangleright e_2, \sigma) = \bot$ and $\mathcal{V}(\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}) = \bot$, so we know that this case holds trivially.

Case $\tilde{t} = \tilde{t}_1 \triangleright \tilde{e}_2$

If we have $t, \sigma \leftrightarrows_M \tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma}, \Phi$, then we know that t is $t_1 \triangleright e_2$.

By definition of $\mathcal{V}$, $\mathcal{V}(t_1 \triangleright e_2, \sigma) = \sigma(l)$ and $\mathcal{V}(\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma}) = \bot$, so we know that this case holds trivially.

Case $\tilde{t} = \tilde{t}_1 \bowtie \tilde{t}_2$

If we have $t, \sigma \leftrightarrows_M \tilde{t}_1 \bowtie \tilde{t}_2, \tilde{\sigma}, \Phi$, then we know that t is also $t_1 \bowtie t_2$.

By definition of $\mathcal{V}$, we can find ourselves in one of two cases.

If $\mathcal{V}(\tilde{t}_1, \sigma) = \tilde{v}_1$ and $\mathcal{V}(\tilde{t}_2, \sigma) = \tilde{v}_2$, then $\mathcal{V}(t_1 \bowtie t_2, \sigma) = \langle v_1, v_2 \rangle$ and $\mathcal{V}(\tilde{t}_1 \bowtie \tilde{t}_2, \tilde{\sigma}) = \langle \tilde{v}_1, \tilde{v}_2 \rangle$. This case follows from the induction hypothesis.

Otherwise, if either one of the two branches returns $\bot$, we have that $\mathcal{V}(t_1 \bowtie t_2, \sigma) = \bot$ and $\mathcal{V}(\tilde{t}_1 \bowtie \tilde{t}_2, \tilde{\sigma}) = \bot$, so we know that this case holds trivially

Case $\tilde{t} = \tilde{t}_1 \blacklozenge \tilde{t}_2$

If we have $t, \sigma \leftrightarrows_M \tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}, \Phi$, then we know that t is also $t_1 \blacklozenge t_2$.

By definition of $\mathcal{V}$, we find ourselves in one of three cases.

If $\mathcal{V}(\tilde{t}_1, \tilde{\sigma}) = \tilde{v}_1$, then $\mathcal{V}(\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}) = \tilde{v}_1$ and $\mathcal{V}(t_1 \blacklozenge t_2, \sigma) = v_1$. This case follows from the induction hypothesis.

Otherwise, if $\mathcal{V}(\tilde{t}_2, \tilde{\sigma}) = \tilde{v}_2$, then $\mathcal{V}(\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}) = \tilde{v}_2$ and $\mathcal{V}(t_1 \blacklozenge t_2, \sigma) = v_2$. This case follows from the induction hypothesis.

Otherwise, if either one of the two branches returns $\bot$, we have that $\mathcal{V}(t_1 \blacklozenge t_2, \sigma) = \bot$ and $\mathcal{V}(\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}) = \bot$, so we know that this case holds trivially.

Case $\tilde{t} = \tilde{t}_1 \lozenge \tilde{t}_2$

If we have $t, \sigma \leftrightarrows_M \tilde{t}_1 \lozenge \tilde{t}_2, \tilde{\sigma}, \Phi$, then we know that t is $t_1 \lozenge t_2$.

By definition of $\mathcal{V}$, $\mathcal{V}(t_1 \lozenge t_2, \sigma) = \bot$ and $\mathcal{V}(\tilde{t}_1 \lozenge \tilde{t}_2, \tilde{\sigma}) = \bot$, so we know that this case holds trivially.

Proof (Soundness of normalise). We prove Lemma 6 by induction over $\tilde{e}$.

From the premise, we can assume that $e, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$. Now, given that $\tilde{e}, \sigma e \twoheadrightarrow \overline{\tilde{t}, \tilde{\sigma}', \varphi}$, we need to demonstrate that for all pairs $(\tilde{t}, \tilde{\sigma}', \varphi)$, $\mathcal{S}(\Phi \wedge \varphi)$ implies that $e, \sigma \Downarrow t, \sigma'$ with $t, \sigma' \leftrightarrows_M \tilde{t}, \tilde{\sigma}', \Phi \wedge \varphi$.

The base case is when the SN-Done rule applies.

SN-Done

$$\frac{\tilde{e}, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}, \tilde{\sigma}', \varphi_1} \qquad \tilde{t}, \tilde{\sigma}' \mapsto \overline{\tilde{t}', \tilde{\sigma}'', \varphi_2}}{\tilde{e}, \tilde{\sigma} \twoheadrightarrow \overline{\tilde{t}, \tilde{\sigma}', \varphi_1}} \; \tilde{\sigma}' = \tilde{\sigma}'' \wedge \tilde{t} = \tilde{t}'$$

In this case, we obtain from Lemma 8 that $e, \sigma \Downarrow t, \sigma'$ with $t, \sigma' \leftrightarrows_M \tilde{t}, \tilde{\sigma}', \Phi \wedge \varphi$, which is exactly what we needed to show.

The only induction step is when

SN-Repeat

$$\frac{\tilde{e}, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}, \tilde{\sigma}', \varphi_1} \qquad \tilde{t}, \tilde{\sigma}' \mapsto \overline{\tilde{t}', \tilde{\sigma}'', \varphi_2} \qquad \tilde{t}', \tilde{\sigma}'' \twoheadrightarrow \overline{\tilde{t}'', \tilde{\sigma}''', \varphi_3}}{\tilde{e}, \tilde{\sigma} \twoheadrightarrow \overline{\tilde{t}'', \tilde{\sigma}''', \varphi_1 \wedge \varphi_2 \wedge \varphi_3}} \; \tilde{\sigma}' \neq \tilde{\sigma}'' \vee \tilde{t} \neq \tilde{t}'$$

applies.

In this case, we obtain from Lemma 8 that $e, \sigma \Downarrow t, \sigma'$ with $t, \sigma' \leftrightarrows_M \tilde{t}, \tilde{\sigma}', \Phi \wedge \varphi_1$, which is exactly what we needed to show. Furthermore, by Lemma 7 we obtain that $t, \sigma' \mapsto t', \sigma''$ with $t', \sigma'' \leftrightarrows_M \tilde{t}', \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. Then finally, by application of the induction hypothesis, we obtain what we needed to prove. $t', \sigma'' \Downarrow t'', \sigma'''$ with $t'', \sigma''' \leftrightarrows_M \tilde{t}'', \tilde{\sigma}''', \Phi \wedge \varphi_1 \wedge \varphi_2 \wedge \varphi_3$.

Proof (Soundness of stride).

Provided that $t, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\tilde{t}, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}', \tilde{\sigma}', \varphi}$, we want to show that for all pairs $(\tilde{t}', \tilde{\sigma}', \varphi)$, we have $\mathcal{S}(\Phi \wedge \varphi)$ implies that $t, \sigma \mapsto t', \sigma'$ We prove Lemma 7 by induction over t.

Case $\tilde{t} = \square\, \tilde{v}$

SS-Edit

$$\overline{\square\, \tilde{v}, \tilde{\sigma} \rightsquigarrow \square\, \tilde{v}, \tilde{\sigma}, \mathsf{True}}$$

One rule applies, namely
Given that $t, \sigma \leftrightarrows_M \square\, \tilde{v}, \tilde{\sigma}, \Phi$ and $\square\, \tilde{v}, \tilde{\sigma} \rightsquigarrow \square\, \tilde{v}, \tilde{\sigma}, \mathsf{True}$, we know that $t = \square\, M\tilde{v}$, and we have $\square\, M\tilde{v}, \sigma \mapsto \square\, M\tilde{v}, \sigma$ by S-Edit and $\square\, M\tilde{v}, \sigma \leftrightarrows_M \square\, \tilde{v}, \tilde{\sigma}, \Phi$, since none of the tasks and states were altered.

Case $t = \boxtimes\, \tau$

SS-Fill

$$\overline{\boxtimes\, \tau, \tilde{\sigma} \rightsquigarrow \boxtimes\, \tau, \tilde{\sigma}, \mathsf{True}}$$

One rule applies, namely
Given that $t, \sigma \leftrightarrows_M \boxtimes\, \tau, \tilde{\sigma}, \Phi$ and $\boxtimes\, \tau, \tilde{\sigma} \rightsquigarrow \boxtimes\, \tau, \tilde{\sigma}, \mathsf{True}$, we know that $t = \boxtimes\, \tau$, and we have $\boxtimes\, \tau, \sigma \mapsto \boxtimes\, \tau, \sigma$ by S-Fill and $\boxtimes\, \tau, \sigma \leftrightarrows_M \square\, \tilde{v}, \tilde{\sigma}, \Phi$, since none of the tasks and states were altered.

Case $t = \blacksquare\, l$

SS-Update

$$\overline{\blacksquare\, l, \tilde{\sigma} \rightsquigarrow \blacksquare\, l, \tilde{\sigma}, \mathsf{True}}$$

One rule applies, namely
Given that $t, \sigma \leftrightarrows_M \blacksquare\, l, \tilde{\sigma}, \Phi$ and $\blacksquare\, l, \tilde{\sigma} \rightsquigarrow \blacksquare\, l, \tilde{\sigma}, \mathsf{True}$, we know that $t = \blacksquare\, l$, and we have $\blacksquare\, l, \sigma \mapsto \blacksquare\, l, \sigma$ by S-Update and $\blacksquare\, l, \sigma \leftrightarrows_M \blacksquare\, l, \tilde{\sigma}, \Phi$, since none of the tasks and states were altered.

Case $t = \lightning$

SS-Fail

$$\overline{\lightning, \tilde{\sigma} \rightsquigarrow \lightning, \tilde{\sigma}, \mathsf{True}}$$

One rule applies, namely
Given that $t, \sigma \leftrightarrows_M \lightning, \tilde{\sigma}, \Phi$ and $\lightning, \tilde{\sigma} \rightsquigarrow \lightning, \tilde{\sigma}, \mathsf{True}$, we know that $t = \lightning$, and we have $\lightning, \sigma \mapsto \lightning, \sigma$ by S-Fail and $\lightning, \sigma \leftrightarrows_M \lightning, \tilde{\sigma}, \Phi$, since none of the tasks and states were altered.

Case $t = \tilde{e}_1 \lozenge \tilde{e}_2$

SS-Xor

$$\overline{\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma}, \mathsf{True}}$$

One rule applies, namely
Given that $t, \sigma \leftrightarrows_M \tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma}, \Phi$ and $\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma}, \mathsf{True}$, we know that $t = M\tilde{e}_1 \lozenge M\tilde{e}_2$, and we have $M\tilde{e}_1 \lozenge M\tilde{e}_2, \sigma \mapsto M\tilde{e}_1 \lozenge M\tilde{e}_2, \sigma$ by S-Xor and $M\tilde{e}_1 \lozenge M\tilde{e}_2, \sigma \leftrightarrows_M \tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma}, \Phi$, since none of the tasks and states were altered.

Case $\tilde{t} = \tilde{t}_1 \blacktriangleright \tilde{e}_2$

Three rules apply.

Case
SS-ThenStay
$$\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \varphi}}{\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \varphi}}\ \mathcal{V}(\tilde{t}_1', \tilde{\sigma}') = \bot$$

Provided that $t, \sigma \leftrightarrows_M \tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}, \Phi$ and $\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \varphi_1$, we obtain from the induction hypothesis that $t_1, \sigma \mapsto t_1', \sigma'$ and $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi$. From this, we can directly conclude that $t_1 \blacktriangleright e_2, \sigma \mapsto t_1' \blacktriangleright e_2, \sigma'$ and $t_1' \blacktriangleright e_2, \sigma' \leftrightarrows_M \tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \Phi$.

Case SS-ThenFail

$$\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \varphi} \qquad \tilde{e}_2\ \tilde{v}_1, \tilde{\sigma}' \not\downarrow \overline{\tilde{t}_2, \tilde{\sigma}'', \_}}{\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \varphi}} \mathcal{V}(\tilde{t}_1', \tilde{\sigma}') = \tilde{v}_1 \wedge \mathcal{F}(\tilde{t}_2, \tilde{\sigma}'')$$

Provided that $t, \sigma \leftrightarrows_M \tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}, \Phi$ and $\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \varphi_1$, we obtain from the induction hypothesis that $t_1, \sigma \mapsto t_1', \sigma'$ and $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi$. From this, we can directly conclude that $t_1 \blacktriangleright e_2, \sigma \mapsto t_1' \blacktriangleright e_2, \sigma'$ and $t_1' \blacktriangleright e_2, \sigma' \leftrightarrows_M \tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \Phi$.

Case SS-ThenCont

$$\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \varphi_1} \qquad \tilde{e}_2\ \tilde{v}_1, \tilde{\sigma}' \not\downarrow \overline{\tilde{t}_2, \tilde{\sigma}'', \varphi_2}}{\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{t_2, \sigma'', \varphi_1 \wedge \varphi_2}} \mathcal{V}(\tilde{t}_1', \tilde{\sigma}') = \tilde{v}_1 \wedge \neg\mathcal{F}(\tilde{t}_2, \tilde{\sigma}'')$$

Provided that $t, \sigma \leftrightarrows_M \tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}, \Phi$ and $\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \tilde{t}_2, \tilde{\sigma}', \varphi_1 \wedge \varphi_2$ with $\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \tilde{t}_1', \tilde{\sigma}', \varphi_1$ and $\mathcal{V}(\tilde{t}_1', \tilde{\sigma}') = \tilde{v}_1$, we obtain from the induction hypothesis that $t_1, \sigma \mapsto t_1', \sigma'$ and $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi$. Then from the consistence relation, we can conclude that $\mathcal{V}(t_1', \sigma') = \mathcal{V}(Mt_1', M\sigma') = M\tilde{v}_1$.

At this point, we have $e_2 M\tilde{v}_1, \sigma' \leftrightarrows_M \tilde{e}_2\tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi_1$ and $\tilde{e}_2\tilde{v}_1, \tilde{\sigma}' \not\downarrow \tilde{t}_2, \tilde{sigma}'', \varphi_2$. This allows us to apply Lemma 8 to obtain $e_2(M\tilde{v}_1), \sigma' \downarrow t_2, \sigma''$ and $t_2, \sigma'' \leftrightarrows_M \tilde{t}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

From this, we can directly conclude that $t_1 \blacktriangleright e_2, \sigma \mapsto t_2, \sigma''$ and $t_2, \sigma'' \leftrightarrows_M \tilde{t}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

Case $\tilde{t} = \tilde{t}_1 \blacklozenge \tilde{t}_2$

One of three rules applies.

Case SS-OrLeft

$$\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \varphi}}{\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \varphi}} \mathcal{V}(\tilde{t}_1', \tilde{\sigma}') = \tilde{v}_1$$

Provided that $t, \sigma \leftrightarrows_M \tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}, \Phi$ and $\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \tilde{t}_1', \tilde{\sigma}', \varphi$, we obtain from the induction hypothesis that $t_1, \sigma \mapsto t_1', \sigma'$ and $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi$. From this, we can directly conclude that $t_1 \blacklozenge t_2, \sigma \mapsto t_1', \sigma'$.

Case SS-OrRight

$$\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \varphi_1} \qquad \tilde{t}_2, \tilde{\sigma}' \rightsquigarrow \overline{\tilde{t}_2', \tilde{\sigma}'', \varphi_2}}{\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_2', \tilde{\sigma}'', \varphi_1 \wedge \varphi_2}} \mathcal{V}(\tilde{t}_1', \tilde{\sigma}') = \bot \wedge \mathcal{V}(\tilde{t}_2', \tilde{\sigma}'') = \tilde{v}_2$$

Provided that $t, \sigma \leftrightarrows_M \tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}, \Phi$ and $\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \tilde{t}_2', \tilde{\sigma}'', \varphi_1 \wedge \varphi_2$, we obtain from the induction hypothesis that $t_1, \sigma \mapsto t_1', \sigma'$ and $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$. Then by a second application of the induction hypothesis, we obtain that $t_2, \sigma' \mapsto t_2', \sigma''$ and $t_2', \sigma'' \leftrightarrows_M \tilde{t}_2', \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. This leads us to conclude $t_1 \blacklozenge t_2, \sigma \mapsto t_2', \sigma''$.

SS-OrNone

$$\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \varphi_1} \qquad \tilde{t}_2, \tilde{\sigma}' \rightsquigarrow \overline{\tilde{t}_2', \tilde{\sigma}'', \varphi_2}}{\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \blacklozenge \tilde{t}_2', \tilde{\sigma}'', \varphi_1 \wedge \varphi_2}} \mathcal{V}(\tilde{t}_1', \tilde{\sigma}') = \bot \wedge \mathcal{V}(\tilde{t}_2', \tilde{\sigma}'') = \bot$$

Case

Provided that $t, \sigma \leftrightarrows_M \tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}, \Phi$ and $\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \tilde{t}_2', \tilde{\sigma}'', \varphi_1 \wedge \varphi_2$, we obtain from the induction hypothesis that $t_1, \sigma \mapsto t_1', \sigma'$ and $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$. Then by a second application of the induction hypothesis, we obtain that $t_2, \sigma' \mapsto t_2', \sigma''$ and $t_2', \sigma'' \leftrightarrows_M \tilde{t}_2', \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. This leads us to conclude $t_1 \blacklozenge t_2, \sigma \mapsto t_1' \blacklozenge t_2', \sigma''$ and $t_1' \blacklozenge t_2', \sigma'' \leftrightarrows_M \tilde{t}_1' \blacklozenge \tilde{t}_2', \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

Case $\tilde{t} = \tilde{t}_1 \triangleright \tilde{e}_2$

SS-Next

$$\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \varphi}}{\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \triangleright \tilde{e}_2, \tilde{\sigma}', \varphi}}$$

One rule applies, namely

Provided that $t, \sigma \leftrightarrows_M \tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma}, \Phi$ and $\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \varphi$, we obtain from the induction hypothesis that $t_1, \sigma \mapsto t_1', \sigma'$ and $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi$. From this, we can directly conclude that $t_1 \triangleright e_2, \sigma \mapsto t_1' \triangleright e_2, \sigma'$ and $t_1' \triangleright e_2, \sigma' \leftrightarrows_M \tilde{t}_1' \triangleright \tilde{e}_2, \tilde{\sigma}', \Phi \wedge \varphi$.

Case $\tilde{t} = \tilde{t}_1 \bowtie \tilde{t}_2$

SS-And

$$\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \varphi_1} \qquad \tilde{t}_2, \tilde{\sigma}' \rightsquigarrow \overline{\tilde{t}_2', \tilde{\sigma}'', \varphi_2}}{\tilde{t}_1 \bowtie \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \bowtie \tilde{t}_2', \tilde{\sigma}'', \varphi_1 \wedge \varphi_2}}$$

One rule applies, namely

Provided that $t, \sigma \leftrightarrows_M \tilde{t}_1 \bowtie \tilde{t}_2, \tilde{\sigma}, \Phi$ and $\tilde{t}_1 \bowtie \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \tilde{t}_1' \bowtie \tilde{t}_2', \tilde{\sigma}'', \varphi_1 \wedge \varphi_2$, we obtain from the induction hypothesis that $t_1, \sigma \mapsto t_1', \sigma'$ and $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$. Then by a second application of the induction hypothesis, we obtain that $t_2, \sigma' \mapsto t_2', \sigma''$ and $t_2', \sigma'' \leftrightarrows_M \tilde{t}_2', \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. This leads us to conclude $t_1 \bowtie t_2, \sigma \mapsto t_1' \bowtie t_2', \sigma''$ and $t_1' \bowtie t_2', \sigma'' \leftrightarrows_M \tilde{t}_1' \bowtie \tilde{t}_2', \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

Proof (Soundness of evaluate).

We prove Lemma 8 by induction over $\tilde{e}$.

Case $\tilde{e} = \tilde{v}$

SE-Value

$$\overline{\tilde{v}, \tilde{\sigma} \lightning \tilde{v}, \tilde{\sigma}, \mathsf{True}}$$

One rule applies, namely

We assume $e, \sigma \leftrightarrows_M \tilde{v}, \tilde{\sigma}, \Phi$ and $\tilde{v}, \tilde{\sigma} \lightning \tilde{v}, \tilde{\sigma}, \mathsf{True}$. By E-Value we have $v, \sigma \downarrow v, \sigma$, so this case holds trivially.

Case $\tilde{e} = \langle \tilde{e}_1, \tilde{e}_2 \rangle$

SE-Pair

$$\frac{\tilde{e}_1, \tilde{\sigma} \lightning \overline{\tilde{v}_1, \tilde{\sigma}', \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma}' \lightning \overline{\tilde{v}_2, \tilde{\sigma}'', \varphi_2}}{\langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma} \lightning \overline{\langle \tilde{v}_1, \tilde{v}_2 \rangle, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2}}$$

One rule applies, namely

Provided that $e, \sigma \leftrightarrows_m \langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma}, \Phi$ and $\langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma} \lightning \langle \tilde{v}_1, \tilde{v}_2 \rangle, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2$, we obtain from the induction hypothesis that $e_1, \sigma \downarrow v_1, \sigma'$ with $v_1, \sigma' \leftrightarrows_m \tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi_1$.

Then by a second application of the induction hypothesis, we obtain that $e_2, \sigma' \downarrow v_2, \sigma''$ with $v_2, \sigma'' \leftrightarrows_m \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. From this, we can conclude that $\langle e_1, e_2 \rangle, \sigma \downarrow \langle v_1, v_2 \rangle, \sigma''$ with $\langle v_1, v_2 \rangle, \sigma'' \leftrightarrows_m \langle \tilde{v}_1, \tilde{v}_2 \rangle, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

Case $\tilde{e} = \mathsf{fst}\langle \tilde{e}_1, \tilde{e}_2 \rangle$

$$\text{SE-First}\ \frac{\tilde{e}_1, \tilde{\sigma} \swarrow \overline{\tilde{v}_1, \tilde{\sigma}', \varphi}}{\mathsf{fst}\langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma} \swarrow \overline{\tilde{v}_1, \tilde{\sigma}', \varphi}}$$

One rule applies, namely
Provided that $e, \sigma \leftrightarrows_m \mathsf{fst}\langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma}, \Phi$ and $\mathsf{fst}\langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma} \swarrow \tilde{v}_1, \tilde{\sigma}'', \varphi$, we obtain from the induction hypothesis that $e_1, \sigma \downarrow v_1, \sigma'$ with $v_1, \sigma' \leftrightarrows_m \tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi$. From this, we can conclude that $\mathsf{fst}\langle e_1, e_2 \rangle, \sigma \downarrow v_1, \sigma'$.

Case $e = \mathsf{snd}\langle \tilde{e}_1, \tilde{e}_2 \rangle$

$$\text{SE-Second}\ \frac{\tilde{e}_2, \tilde{\sigma} \swarrow \overline{\tilde{v}_2, \tilde{\sigma}', \varphi}}{\mathsf{snd}\langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma} \swarrow \overline{\tilde{v}_2, \tilde{\sigma}', \varphi}}$$

One rule applies, namely
Provided that $e, \sigma \leftrightarrows_m \mathsf{snd}\langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma}, \Phi$ and $\mathsf{snd}\langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma} \swarrow \tilde{v}_2, \tilde{\sigma}'', \varphi$, we obtain from the induction hypothesis that $e_1, \sigma \downarrow v_2, \sigma'$ with $v_2, \sigma' \leftrightarrows_m \tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi$. From this, we can conclude that $\mathsf{snd}\langle e_1, e_2 \rangle, \sigma \downarrow v_2, \sigma'$.

Case $\tilde{e} = \tilde{e}_1 :: \tilde{e}_2$

$$\text{SE-Cons}\ \frac{\tilde{e}_1, \tilde{\sigma} \swarrow \tilde{v}_1, \tilde{\sigma}', \varphi_1 \qquad \tilde{e}_2, \tilde{\sigma}' \swarrow \tilde{v}_2, \tilde{\sigma}'', \varphi_2}{\tilde{e}_1 :: \tilde{e}_2, \tilde{\sigma} \swarrow \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2}$$

One rule applies, namely
Provided that $e, \sigma \leftrightarrows_m \tilde{e}_1 :: \tilde{e}_2, \tilde{\sigma}, \Phi$ and $\tilde{e}_1 :: \tilde{e}_2, \tilde{\sigma} \swarrow \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2$, we obtain from the induction hypothesis that $e_1, \sigma \downarrow v_1, \sigma'$ with $v_1, \sigma' \leftrightarrows_m \tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi_1$. Then by a second application of the induction hypothesis, we obtain that $e_2, \sigma' \downarrow v_2, \sigma''$ with $v_2, \sigma'' \leftrightarrows_m \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. From this, we can conclude that $e_1 :: e_2, \sigma \downarrow v_1 :: v_2, \sigma''$ with $v_1 :: v_2, \sigma'' \leftrightarrows_m \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

Case $\tilde{e} = \mathsf{head}\, \tilde{e}$

$$\text{SE-Head}\ \frac{\tilde{e}, \tilde{\sigma} \swarrow \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}', \varphi}{\mathsf{head}\, \tilde{e}, \tilde{\sigma} \swarrow \tilde{v}_1, \tilde{\sigma}', \varphi}$$

One rule applies, namely
Provided that $e, \sigma \leftrightarrows_m \mathsf{head}\, \tilde{e}, \tilde{\sigma}, \Phi$ and $\mathsf{head}\, \tilde{e}, \tilde{\sigma} \swarrow \tilde{v}_1, \tilde{\sigma}', \varphi$, we obtain from the induction hypothesis that $e, \sigma \downarrow v_1 :: v_2, \sigma'$ with $v_1 :: v_2, \sigma' \leftrightarrows_m \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}', \Phi \wedge \varphi$. From this, we can conclude that $\mathsf{head}\, e, \sigma \downarrow v_1, \sigma'$.

Case $\tilde{e} = \mathsf{tail}\, \tilde{e}$

$$\text{SE-Tail}\ \frac{\tilde{e}, \tilde{\sigma} \swarrow \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}', \varphi}{\mathsf{tail}\, \tilde{e}, \tilde{\sigma} \swarrow \tilde{v}_2, \tilde{\sigma}', \varphi}$$

One rule applies, namely
Provided that $e, \sigma \leftrightarrows_m \mathsf{tail}\, \tilde{e}, \tilde{\sigma}, \Phi$ and $\mathsf{tail}\, \tilde{e}, \tilde{\sigma} \swarrow \tilde{v}_2, \tilde{\sigma}', \varphi$, we obtain from the induction hypothesis that $e, \sigma \downarrow v_1 :: v_2, \sigma'$ with $v_1 :: v_2, \sigma' \leftrightarrows_m \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}', \Phi \wedge \varphi$. From this, we can conclude that $\mathsf{tail}\, e, \sigma \downarrow v_2, \sigma'$.

Case $\tilde{e} = \tilde{e}_1\tilde{e}_2$

One rule applies, namely

SE-App

$$\frac{\tilde{e}_1, \tilde{\sigma} \lesssim \overline{\lambda x : \tau.\tilde{e}_1', \tilde{\sigma}', \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma}' \lesssim \overline{\tilde{v}_2, \tilde{\sigma}'', \varphi_2} \qquad \tilde{e}_1'[x \mapsto \tilde{v}_2], \tilde{\sigma}'' \lesssim \overline{\tilde{v}_1, \tilde{\sigma}''', \varphi_3}}{\tilde{e}_1\tilde{e}_2, \tilde{\sigma} \lesssim \overline{\tilde{v}_1, \tilde{\sigma}''', \varphi_1 \wedge \varphi_2 \wedge \varphi_3}}$$

Provided that $e, \sigma \leftrightarrows_m \tilde{e}_1\tilde{e}_2, \tilde{\sigma}, \Phi$ and $\tilde{e}_1\tilde{e}_2, \tilde{\sigma} \lesssim \tilde{v}_1, \tilde{\sigma}''', \varphi_1 \wedge \varphi_2 \wedge \varphi_3$, we obtain from the induction hypothesis that $e_1, \sigma \downarrow \lambda x : \tau.e_1', \sigma'$ with $\lambda x : \tau.e_1', \sigma' \leftrightarrows_m \lambda x : \tau.\tilde{e}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$. Then by a second application of the induction hypothesis, we obtain that $e_2, \sigma' \downarrow v_2, \sigma''$ with $v_2, \sigma'' \leftrightarrows_m \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. A third and final application of the induction hypothesis gives us that $e_1'[x \mapsto v_2], \sigma'' \downarrow v_1, \sigma'''$ with $v_1, \sigma''' \leftrightarrows_m \tilde{v}_1, \tilde{\sigma}''', \Phi \wedge \varphi_1 \wedge \varphi_2 \wedge \varphi_3$. From this, we can conclude that $e_1e_2, \sigma \downarrow v_1, \sigma'''$.

Case $\tilde{e} =$ **if** $\tilde{e}_1$ **then** $\tilde{e}_2$ **else** $\tilde{e}_3$

One rule applies, namely

SE-If

$$\frac{\tilde{e}_1, \tilde{\sigma} \lesssim \overline{\tilde{v}_1, \tilde{\sigma}', \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma}' \lesssim \overline{\tilde{v}_2, \tilde{\sigma}'', \varphi_2} \qquad \tilde{e}_3, \tilde{\sigma}' \lesssim \overline{\tilde{v}_3, \tilde{\sigma}''', \varphi_3}}{\textbf{if } \tilde{e}_1 \textbf{ then } \tilde{e}_2 \textbf{ else } \tilde{e}_3, \tilde{\sigma} \lesssim \overline{\tilde{v}_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2 \wedge \tilde{v}_1} \cup \overline{\tilde{v}_3, \tilde{\sigma}''', \varphi_1 \wedge \varphi_3 \wedge \neg\tilde{v}_1}}$$

Provided that $e, \sigma \leftrightarrows_m$ **if** $\tilde{e}_1$ **then** $\tilde{e}_2$ **else** $\tilde{e}_3, \tilde{\sigma}, \Phi$ and , we obtain from the induction hypothesis that $e_1, \sigma \downarrow v_1, \sigma'$ with $v_1, \sigma' \leftrightarrows_m \tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi_1$. At this point, we have two potential branches. Applying the induction hypothesis to either of them, we obtain that $e_2, \sigma' \downarrow v_2, \sigma''$ with $v_2, \sigma'' \leftrightarrows_m \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$ and $e_3, \sigma' \downarrow v_3, \sigma''$ with $v_3, \sigma'' \leftrightarrows_m \tilde{v}_3, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_3$. From this, we can conclude that **if** e_1 **then** e_2 **else** $e_3, \sigma \downarrow v_2, \sigma''$ with $v_2, \sigma'' \leftrightarrows_M \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$ or **if** e_1 **then** e_2 **else** $e_3, \sigma \downarrow v_3, \sigma''$ with $v_3, \sigma'' \leftrightarrows_M \tilde{v}_3, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_3$.

Case $\tilde{e} =$ **ref** $\tilde{e}$

SE-Ref

$$\frac{\tilde{e}, \tilde{\sigma} \lesssim \overline{\tilde{v}, \tilde{\sigma}', \varphi} \qquad l \notin Dom(\sigma')}{\textbf{ref } \tilde{e}, \tilde{\sigma} \lesssim \overline{l, \tilde{\sigma}'[l \mapsto \tilde{v}], \varphi}}$$

One rule applies, namely

Provided that $e, \sigma \leftrightarrows_m$ **ref** $\tilde{e}, \tilde{\sigma}, \Phi$ and **ref** $\tilde{e}, \tilde{\sigma} \lesssim l, \tilde{\sigma}'[l \mapsto \tilde{v}], \varphi$, we obtain from the induction hypothesis that $e, \sigma \downarrow v_1, \sigma'$ with $v_1, \sigma' \leftrightarrows_m \tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi$. From this, we can conclude that **ref** $e, \sigma \downarrow l, \sigma'[l \mapsto v]$ with $l, \sigma'[l \mapsto v] \leftrightarrows_m l, \tilde{\sigma}'[l \mapsto \tilde{v}], \Phi \wedge \varphi$.

Case $\tilde{e} = !\tilde{e}$

SE-Deref

$$\frac{\tilde{e}, \tilde{\sigma} \lesssim \overline{l, \tilde{\sigma}', \varphi}}{!\tilde{e}, \tilde{\sigma} \lesssim \overline{\tilde{\sigma}'(l), \tilde{\sigma}', \varphi}}$$

One rule applies, namely

Provided that $e, \sigma \leftrightarrows_m !\tilde{e}, \tilde{\sigma}, \Phi$ and $!\tilde{e}, \tilde{\sigma} \lesssim \tilde{\sigma}'(l), \tilde{\sigma}', \varphi$, we obtain from the induction hypothesis that $e, \sigma \downarrow l, \sigma'$ with $l, \sigma' \leftrightarrows_m l, \tilde{\sigma}', \Phi \wedge \varphi$. From this, we can conclude that $!e, \sigma \downarrow \sigma'(l), \sigma'$ with $\sigma'(l), \sigma' \leftrightarrows_m \tilde{\sigma}'(l), \tilde{\sigma}', \Phi \wedge \varphi$.

Case $\tilde{e} = \tilde{e}_1 := \tilde{e}_2$

$$\text{SE-Assign}\quad \frac{\tilde{e}_1, \tilde{\sigma} \;\wr\; \overline{l, \tilde{\sigma}', \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma}' \;\wr\; \overline{\tilde{v}_2, \tilde{\sigma}'', \varphi_2}}{\tilde{e}_1 := \tilde{e}_2, \tilde{\sigma} \;\wr\; \overline{\langle\rangle, \tilde{\sigma}''[l \mapsto \tilde{v}_2], \varphi_1 \wedge \varphi_2}}$$

One rule applies, namely
Provided that $e, \sigma \leftrightarrows_m \tilde{e}_1 := \tilde{e}_2, \tilde{\sigma}, \Phi$ and $\tilde{e}_1 := \tilde{e}_2, \tilde{\sigma} \;\wr\; \langle\rangle, \tilde{\sigma}''[l \mapsto \tilde{v}_2], \varphi_1 \wedge \varphi_2$, we obtain from the induction hypothesis that $e_1, \sigma \downarrow l, \sigma'$ with $l, \sigma' \leftrightarrows_m l, \tilde{\sigma}', \Phi \wedge \varphi_1$. Then by a second application of the induction hypothesis, we obtain that $e_2, \sigma' \downarrow v_2, \sigma''$ with $v_2, \sigma'' \leftrightarrows_m \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. From this, we can conclude that $e_1 := e_2, \sigma \downarrow \langle\rangle, \sigma''[l \mapsto v_2]$ with $\langle\rangle, \sigma''[l \mapsto v_2] \leftrightarrows_m \langle\rangle, \tilde{\sigma}''[l \mapsto \tilde{v}_2], \Phi \wedge \varphi_1 \wedge \varphi_2$.

Case $\tilde{e} = \square\, \tilde{e}$

$$\text{SE-Edit}\quad \frac{\tilde{e}, \tilde{\sigma} \;\wr\; \overline{\tilde{v}, \tilde{\sigma}', \varphi}}{\square\, \tilde{e}, \tilde{\sigma} \;\wr\; \overline{\square\, \tilde{v}, \tilde{\sigma}', \varphi}}$$

One rule applies, namely
Provided that $e, \sigma \leftrightarrows_m \square\, \tilde{e}, \tilde{\sigma}, \Phi$ and $\square\, \tilde{e}, \tilde{\sigma} \;\wr\; \square\, \tilde{v}, \tilde{\sigma}', \varphi$, we obtain from the induction hypothesis that $e, \sigma \downarrow v, \sigma'$ with $v, \sigma' \leftrightarrows_m \tilde{v}, \tilde{\sigma}', \Phi \wedge \varphi$. From this, we can conclude that $\square\, e, \sigma \downarrow \square\, v, \sigma'$ with $\square\, v, \sigma' \leftrightarrows_m \square\, \tilde{v}, \tilde{\sigma}', \Phi \wedge \varphi$.

Case $\tilde{e} = \boxtimes\, \tau$

$$\text{SE-Enter}\quad \frac{}{\boxtimes\, \tau, \tilde{\sigma} \;\wr\; \boxtimes\, \tau, \tilde{\sigma}, \mathsf{True}}$$

One rule applies, namely
We assume $e, \sigma \leftrightarrows_M \boxtimes\, \tau, \tilde{\sigma}, \Phi$ and $\boxtimes\, \tau, \tilde{\sigma} \;\wr\; \boxtimes\, \tau, \tilde{\sigma}, \mathsf{True}$. By E-Enter we have $\boxtimes\, \tau, \sigma \downarrow \boxtimes\, \tau, \sigma$, so this case holds trivially.

Case $\tilde{e} = \blacksquare\, \tilde{e}$

$$\text{SE-Update}\quad \frac{\tilde{e}, \tilde{\sigma} \;\wr\; \overline{l, \tilde{\sigma}', \varphi}}{\blacksquare\, \tilde{e}, \tilde{\sigma} \;\wr\; \overline{\blacksquare\, l, \tilde{\sigma}', \varphi}}$$

One rule applies, namely
Provided that $e, \sigma \leftrightarrows_m \blacksquare\, \tilde{e}, \tilde{\sigma}, \Phi$ and $\blacksquare\, \tilde{e}, \tilde{\sigma} \;\wr\; \blacksquare\, l, \tilde{\sigma}', \varphi$, we obtain from the induction hypothesis that $e, \sigma \downarrow l, \sigma'$ with $l, \sigma' \leftrightarrows_m l, \tilde{\sigma}', \Phi \wedge \varphi$. From this, we can conclude that $\blacksquare\, e, \sigma \downarrow \blacksquare\, l, \sigma'$ with $\blacksquare\, l, \sigma' \leftrightarrows_m \blacksquare\, l, \tilde{\sigma}', \Phi \wedge \varphi$.

Case $\tilde{e} = \tilde{e}_1 \blacktriangleright \tilde{e}_2$

$$\text{SE-Then}\quad \frac{\tilde{e}_1, \tilde{\sigma} \;\wr\; \overline{\tilde{t}_1, \tilde{\sigma}', \varphi}}{\tilde{e}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \;\wr\; \overline{\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \varphi}}$$

One rule applies, namely
Provided that $e, \sigma \leftrightarrows_m \tilde{e}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}, \Phi$ and $\tilde{e}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \;\wr\; \tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \varphi$, we obtain from the induction hypothesis that $e_1, \sigma \downarrow t_1, \sigma'$ with $t_1, \sigma' \leftrightarrows_m \tilde{t}_1, \tilde{\sigma}', \Phi \wedge \varphi$. From this, we can conclude that $e_1 \blacktriangleright e_2, \sigma \downarrow t_1 \blacktriangleright e_2, \sigma'$ with $t_1 \blacktriangleright e_2, \sigma' \leftrightarrows_m \tilde{t}_1 \blacktriangleright e_2, \tilde{\sigma}', \Phi \wedge \varphi$.

Case $\tilde{e} = \tilde{e}_1 \rhd \tilde{e}_2$

$$\text{SE-Next}\quad \frac{\tilde{e}_1, \tilde{\sigma} \;\wr\; \overline{\tilde{t}_1, \tilde{\sigma}', \varphi}}{\tilde{e}_1 \rhd \tilde{e}_2, \tilde{\sigma} \;\wr\; \overline{\tilde{t}_1 \rhd \tilde{e}_2, \tilde{\sigma}', \varphi}}$$

One rule applies, namely
Provided that $e, \sigma \leftrightarrows_m \tilde{e}_1 \rhd \tilde{e}_2, \tilde{\sigma}, \Phi$ and $\tilde{e}_1 \rhd \tilde{e}_2, \tilde{\sigma} \;\wr\; \tilde{t}_1 \rhd \tilde{e}_2, \tilde{\sigma}', \varphi$, we obtain from the induction hypothesis that $e_1, \sigma \;\downarrow\; t_1, \sigma'$ with $t_1, \sigma' \leftrightarrows_m \tilde{t}_1, \tilde{\sigma}', \Phi \wedge \varphi$. From this, we can conclude that $e_1 \rhd e_2, \sigma \;\downarrow\; t_1 \rhd e_2, \sigma'$ with $t_1 \rhd e_2, \sigma' \leftrightarrows_m \tilde{t}_1 \rhd e_2, \tilde{\sigma}', \Phi \wedge \varphi$.

Case $\tilde{e} = \tilde{e}_1 \blacklozenge \tilde{e}_2$

$$\text{SE-Or}\quad \frac{\tilde{e}_1, \tilde{\sigma} \;\wr\; \overline{\tilde{t}_1, \tilde{\sigma}', \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma}' \;\wr\; \overline{\tilde{t}_2, \tilde{\sigma}'', \varphi_2}}{\tilde{e}_1 \blacklozenge \tilde{e}_2, \tilde{\sigma} \;\wr\; \overline{\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2}}$$

One rule applies, namely
Provided that $e, \sigma \leftrightarrows_m \tilde{e}_1 \blacklozenge \tilde{e}_2, \tilde{\sigma}, \Phi$ and $\tilde{e}_1 \blacklozenge \tilde{e}_2, \tilde{\sigma} \;\wr\; \tilde{v}_1 \blacklozenge \tilde{v}_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2$, we obtain from the induction hypothesis that $e_1, \sigma \;\downarrow\; v_1, \sigma'$ with $v_1, \sigma' \leftrightarrows_m \tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi_1$. Then by a second application of the induction hypothesis, we obtain that $e_2, \sigma' \;\downarrow\; v_2, \sigma''$ with $v_2, \sigma'' \leftrightarrows_m \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. From this, we can conclude that $e_1 \blacklozenge e_2, \sigma \;\downarrow\; v_1 \blacklozenge v_2, \sigma''$ with $v_1 \blacklozenge v_2, \sigma'' \leftrightarrows_m \tilde{v}_1 \blacklozenge \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

Case $\tilde{e} = \tilde{e}_1 \lozenge \tilde{e}_2$

$$\text{SE-Xor}\quad \frac{}{\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \;\wr\; \tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma}, \mathsf{True}}$$

One rule applies, namely
We assume $e, \sigma \leftrightarrows_M \tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma}, \Phi$ and $\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \;\wr\; \tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma}, \mathsf{True}$. By E-Xor we have $e_1 \lozenge e_2, \sigma \;\downarrow\; e_1 \lozenge e_2, \sigma$, so this case holds trivially.

Case $\tilde{e} = \lightning$

$$\text{SE-Fail}\quad \frac{}{\lightning, \tilde{\sigma} \;\wr\; \lightning, \tilde{\sigma}, \mathsf{True}}$$

One rule applies, namely
We assume $e, \sigma \leftrightarrows_M \lightning, \tilde{\sigma}, \Phi$ and $\lightning, \tilde{\sigma} \;\wr\; \lightning, \tilde{\sigma}, \mathsf{True}$. By E-Fail we have $\lightning, \sigma \;\downarrow\; \lightning, \sigma$, so this case holds trivially.

E Completeness proofs

Proof (Completeness of simulate). The structure of this proof is outlined in Fig. 6.

We have t and σ such that $t, \sigma \overset{I}{\Rightarrow}^{*} v$. By definition of $\overset{I}{\Rightarrow}^{*}$, we have the following.
$t, \sigma \overset{i_1}{\Rightarrow} t_1, \sigma_1 \overset{i_2}{\Rightarrow} \cdots \overset{i_n}{\Rightarrow} t_n, \sigma_n$ with $\mathcal{V}(t_n, \sigma_n)$ and $I = [i_1, \cdots, i_n]$.
We need to show that we have $(\tilde{v}, \tilde{I}, \Phi) \in t, \sigma \Rightarrow^{*})$, which is defined as follows.

$$\begin{array}{lllll} t, \sigma \Rightarrow \tilde{t}_1, \tilde{\sigma}_1, \tilde{\imath}_1, \varphi_1 & & & & \\ \quad \tilde{t}_1, \tilde{\sigma}_1 \Rightarrow & & \tilde{t}_2, \tilde{\sigma}_2, \tilde{\imath}_2, \varphi_2 & & \\ & & \quad \tilde{t}_2, \tilde{\sigma}_2 \Rightarrow \cdots & & \\ & & & \cdots & \Rightarrow \tilde{t}_n, \tilde{\sigma}_n, \tilde{\imath}_n, \varphi_n \end{array}$$

with $\mathcal{V}(\tilde{t}_n, \tilde{\sigma}_n) = \tilde{v}$ and $\mathcal{S}(\varphi_1 \wedge \cdots \wedge \varphi_n)$.

By Lemma 4, we know that $t, \sigma \Rightarrow \tilde{t}_1, \tilde{\sigma}_1, \tilde{\imath}_1, \varphi_1$ exists, since $t, \sigma, t \leftrightarrows_{\emptyset} \sigma, \mathsf{True}$. This also gives us that $\tilde{\imath}_1 \sim i_1$ and $t_1, \sigma_1 \leftrightarrows_{[s_1 \mapsto c_1]} \tilde{t}_1, \tilde{\sigma}_1, \varphi_1$ with $\mathit{SymOf}(\tilde{\imath}_1) = s_1$ and $\mathit{ValOf}(i_1) = c_1$.

By repeated application of Lemma 4, untill we arrive at t_n, σ_n, we can show that there exists a $\tilde{I}$ such that $t, \sigma \Rightarrow^* \tilde{t}_n, \tilde{\sigma}_n, \tilde{I}, \Phi$, namely $[\tilde{\imath}_1, \cdots, \tilde{\imath}_n]$.

Lemma 10 (Completeness of handling). *For all concrete tasks t, concrete states σ, concrete inputs i, symbolic tasks $\tilde{t}$, symbolic states $\tilde{\sigma}$ path conditions Φ and mappings M, we have that $t, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $t, \sigma \xrightarrow{i} t', \sigma'$ together with $\tilde{t}, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}', \tilde{\sigma}', \tilde{\imath}, \varphi}$, and for all pairs $(\tilde{t}', \tilde{\sigma}', \tilde{\imath}, \varphi)$ we have that $\mathcal{S}(\Phi \wedge \varphi)$ and $\imath \sim i$ implies $t', \sigma' \leftrightarrows_{M.[s \mapsto c]} \tilde{t}', \tilde{\sigma}', \Phi \wedge \varphi$ where where $\mathit{SymOf}(\tilde{\imath}) = s$ and $\mathit{ValOf}(i) = c$.*

Lemma 11 (Completeness of normalisation). *For all concrete expressions e, concrete states σ, symbolic expressions $\tilde{e}$, symbolic states $\tilde{\sigma}$ path conditions Φ and mappings M, we have that $e, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and $e, \sigma \Downarrow t, \sigma'$, then $\tilde{e}, \tilde{\sigma} \lll \overline{\tilde{t}, \tilde{\sigma}', \varphi}$, and for all pairs $(\tilde{t}, \tilde{\sigma}', \varphi)$ we have that $\mathcal{S}(\Phi \wedge \varphi)$ implies $t, \sigma' \leftrightarrows_M \tilde{t}, \tilde{\sigma}', \Phi \wedge \varphi$.*

Lemma 12 (Completeness of striding). *For all concrete tasks t, concrete states σ, symbolic tasks $\tilde{t}$, symbolic states $\tilde{\sigma}$ path conditions Φ and mappings M, we have that $t, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $t, \sigma \mapsto t', \sigma'$, then $\tilde{t}, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}', \tilde{\sigma}', \varphi}$, and for all pairs $(\tilde{t}', \tilde{\sigma}', \varphi)$ we have that $\mathcal{S}(\Phi \wedge \varphi)$ implies $t', \sigma' \leftrightarrows_M \tilde{t}', \tilde{\sigma}', \Phi \wedge \varphi$.*

Lemma 13 (Completeness of evaluate). *For all concrete expressions e, concrete states σ, symbolic expressions $\tilde{e}$, symbolic states $\tilde{\sigma}$ path conditions Φ and mappings M, we have that $e, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and $e, \sigma \downarrow v, \sigma'$, then $\tilde{e}, \tilde{\sigma} \wr \overline{\tilde{v}, \tilde{\sigma}', \varphi}$, and for all pairs $(\tilde{v}, \tilde{\sigma}', \varphi)$ we have that $\mathcal{S}(\Phi \wedge \varphi)$ implies $v, \sigma' \leftrightarrows_M \tilde{v}, \tilde{\sigma}', \Phi \wedge \varphi$.*

Proof (Completeness of handle). We prove Lemma 10 by induction over t.

Case $t = \square\, v$

$$\text{H-Change}\ \frac{}{\square\, v, \sigma \xrightarrow{v'} \square\, v', \sigma}\ v, v' : \tau$$

Provided that $\square\, v, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and , then $\square\, \tilde{v}, \tilde{\sigma} \rightarrow \square\, s, \tilde{\sigma}, s, \mathsf{True}$. $\mathcal{S}(\Phi \wedge \mathsf{True}) = \mathcal{S}(\Phi)$, which follows from the premise. Furthermore we have $s \sim v'$ by definition. Then finally $\square\, v', \sigma \leftrightarrows M[s \mapsto v']\, \square\, s, \tilde{\sigma}, \Phi$ since $M[s \mapsto v']s = v'$.

Case $t = \boxtimes\, \tau$

$$\text{H-Fill}\ \frac{}{\boxtimes\, \tau, \sigma \xrightarrow{v} \square\, v, \sigma}\ v : \tau$$

Provided that $\boxtimes\, \tau, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and then $\boxtimes\, \tau, \tilde{\sigma} \rightarrow \square\, s, \tilde{\sigma}, s, \mathsf{True}$. $\mathcal{S}(\Phi \wedge \mathsf{True}) = \mathcal{S}(\Phi)$, which follows from the premise. Furthermore we have $s \sim v$ by definition. Then finally $\square\, v, \sigma \leftrightarrows M[s \mapsto v]\, \square\, s, \tilde{\sigma}, \Phi$ since $M[s \mapsto v]s = v$.

Case $t = \blacksquare\, l$

$$\text{H-Update}\ \frac{}{\sigma(l), v : \tau}$$

Provided that $\blacksquare\, l, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\blacksquare\, l, \sigma \xrightarrow{v} \blacksquare\, l, \sigma[l \mapsto v]$, then $\blacksquare\, l, \tilde{\sigma} \rightarrow \blacksquare\, l, \tilde{\sigma}[l \mapsto s], s, \mathsf{True}$. $\mathcal{S}(\Phi \wedge \mathsf{True}) = \mathcal{S}(\Phi)$, which follows from the premise. Furthermore we have $s \sim v$ by definition. Then finally $\blacksquare\, l, \sigma[l \mapsto v] \leftrightarrows M[s \mapsto v] \blacksquare\, l, \tilde{\sigma}[l \mapsto s], \Phi$ since $M[s \mapsto v]s = v$.

Case $t = t_1 \triangleright e_2$

Case $i = \mathsf{C}$

$$\text{H-Next}\ \frac{e_2\ v_1, \sigma \Downarrow t_2, \sigma'}{t_1 \triangleright e_2, \sigma \xrightarrow{\mathsf{C}} t_2, \sigma'}\ \mathcal{V}(t_1, \sigma) = v_1 \wedge \neg\mathcal{F}(t_2, \sigma')$$

Provided that $t_1 \triangleright e_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and , then $\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}_1', \tilde{\imath}, \varphi_1}$ $\tilde{e}_2\ \tilde{v}_1, \tilde{\sigma} \lessapprox \overline{\tilde{t}_2, \tilde{\sigma}_2', \varphi_2}$

$$\text{SH-Next}\ \frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}_1', \tilde{\imath}, \varphi_1} \quad \tilde{e}_2\ \tilde{v}_1, \tilde{\sigma} \lessapprox \overline{\tilde{t}_2, \tilde{\sigma}_2', \varphi_2}}{\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \triangleright \tilde{e}_2, \tilde{\sigma}_1', \tilde{\imath}, \varphi_1} \cup \overline{\tilde{t}_2, \tilde{\sigma}_2', \mathsf{C}, \varphi_2}}\ \mathcal{V}(\tilde{t}_1, \tilde{\sigma}) = \tilde{v}_1 \wedge \neg\mathcal{F}(\tilde{t}_2, \tilde{\sigma}')$$

then . The simulation step results in two sets, from which only the second adheres to the requirement that the symbolic input should simulate the concrete input. For this set, $\overline{\tilde{t}_2, \tilde{\sigma}_2', \mathsf{C}, \varphi_2}$, we have $\mathcal{S}(\Phi \wedge \varphi_2)$ implies $t_2, \sigma_2' \leftrightarrows_M \tilde{t}_2, \tilde{\sigma}_2', \Phi \wedge \varphi_2$, Which follows directly from Lemma 11.

Case $i \neq \mathsf{C}$

$$\text{H-PassNext}\ \frac{t_1, \sigma \xrightarrow{i} t_1', \sigma'}{t_1 \triangleright e_2, \sigma \xrightarrow{i} t_1' \triangleright e_2, \sigma'}$$

Provided that $t_1 \triangleright e_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and . There are three symbolic rules that apply, namely

$$\text{SH-PassNext}\ \frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \tilde{\imath}, \varphi}}{\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \triangleright \tilde{e}_2, \tilde{\sigma}', \tilde{\imath}, \varphi}}\ \mathcal{V}(\tilde{t}_1, \tilde{\sigma}) = \bot$$

,

$$\text{SH-PassNextFail}\ \frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}_1', \tilde{\imath}, \varphi} \quad \tilde{e}_2\ \tilde{v}_1, \tilde{\sigma} \lessapprox \overline{\tilde{t}_2, \tilde{\sigma}_2', \_}}{\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \triangleright \tilde{e}_2, \tilde{\sigma}_1', \tilde{\imath}, \varphi}}\ \mathcal{V}(\tilde{t}_1, \tilde{\sigma}) = \tilde{v}_1 \wedge \mathcal{F}(\tilde{t}_2, \tilde{\sigma}_2')$$

and

$$\text{SH-Next}\ \frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}_1', \tilde{\imath}, \varphi_1} \quad \tilde{e}_2\ \tilde{v}_1, \tilde{\sigma} \lessapprox \overline{\tilde{t}_2, \tilde{\sigma}_2', \varphi_2}}{\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \triangleright \tilde{e}_2, \tilde{\sigma}_1', \tilde{\imath}, \varphi_1} \cup \overline{\tilde{t}_2, \tilde{\sigma}_2', \mathsf{C}, \varphi_2}}\ \mathcal{V}(\tilde{t}_1, \tilde{\sigma}) = \tilde{v}_1 \wedge \neg\mathcal{F}(\tilde{t}_2, \tilde{\sigma}')$$

.

We are only interested in the runs that produce a symbolic input that simulates the concrete input i. Whichever rule applies, we deal with the same premise because of this restriction. This allows us to apply the induction hypothesis and obtain that $\mathcal{S}(\Phi \wedge \varphi_1) \supset t_1', \sigma' \leftrightarrows_{M.[s \mapsto c]} \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$. From this, we can directly conclude that $t_1' \triangleright e_2, \sigma' \leftrightarrows_{M.[s \mapsto c]} \tilde{t}_1' \triangleright \tilde{e}_2, \tilde{\sigma}', \Phi \wedge \varphi_1$.

Case $t = t_1 \blacktriangleright e_2$

$$\text{H-PassThen}\ \frac{t_1, \sigma \xrightarrow{i} t_1', \sigma'}{t_1 \blacktriangleright e_2, \sigma \xrightarrow{i} t_1' \blacktriangleright e_2, \sigma'}$$

Provided that $t_1 \blacktriangleright e_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\text{SH-PassThen}\ \frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \tilde{\imath}, \varphi}}{\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \tilde{\imath}, \varphi}}$ then .

By application of the induction hypothesis, we obtain $\mathcal{S}(\Phi \wedge \varphi)$ implies $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi$ from which we can conclude that $t_1' \blacktriangleright e_2, \sigma' \leftrightarrows_M \tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \Phi \wedge \varphi$.

Case $t = e_1 \lozenge e_2$

Case $i = \mathsf{L}$

$$\text{H-PickLeft}\ \frac{e_1, \sigma \Downarrow t_1, \sigma'}{e_1 \lozenge e_2, \sigma \xrightarrow{\mathsf{L}} t_1, \sigma'}\ \neg\mathcal{F}(t_1, \sigma')$$

Provided that $e_1 \lozenge e_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\text{SH-Pick}\ \frac{\tilde{e}_1, \tilde{\sigma} \Downarrow \overline{\tilde{t}_1, \tilde{\sigma}_1, \varphi_1} \quad \tilde{e}_2, \tilde{\sigma} \Downarrow \overline{\tilde{t}_2, \tilde{\sigma}_2, \varphi_2}}{\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1, \tilde{\sigma}_1, \mathsf{L}, \varphi_1} \cup \overline{\tilde{t}_2, \tilde{\sigma}_2, \mathsf{R}, \varphi_2}}\ \neg\mathcal{F}(\tilde{t}_1, \tilde{\sigma}_1) \wedge \neg\mathcal{F}(\tilde{t}_2, \tilde{\sigma}_2)$ then .

By Lemma 11 we obtain $\mathcal{S}(\Phi \wedge \varphi_1)$ implies $t_1, \sigma' \leftrightarrows_M \tilde{t}_1, \tilde{\sigma}', \Phi \wedge \varphi_1$ from which we can conclude that $t_1, \sigma' \leftrightarrows_M \tilde{t}_1, \tilde{\sigma}', \Phi \wedge \varphi_1$.

Case $i = \mathsf{R}$

$$\text{H-PickLeft}\ \frac{e_1, \sigma \Downarrow t_1, \sigma'}{e_1 \lozenge e_2, \sigma \xrightarrow{\mathsf{L}} t_1, \sigma'}\ \neg\mathcal{F}(t_1, \sigma')$$

Provided that $e_1 \lozenge e_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\text{SH-Pick}\ \frac{\tilde{e}_1, \tilde{\sigma} \Downarrow \overline{\tilde{t}_1, \tilde{\sigma}_1, \varphi_1} \quad \tilde{e}_2, \tilde{\sigma} \Downarrow \overline{\tilde{t}_2, \tilde{\sigma}_2, \varphi_2}}{\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1, \tilde{\sigma}_1, \mathsf{L}, \varphi_1} \cup \overline{\tilde{t}_2, \tilde{\sigma}_2, \mathsf{R}, \varphi_2}}\ \neg\mathcal{F}(\tilde{t}_1, \tilde{\sigma}_1) \wedge \neg\mathcal{F}(\tilde{t}_2, \tilde{\sigma}_2)$ then .

By Lemma 11 we obtain $\mathcal{S}(\Phi \wedge \varphi_2)$ implies $t_2, \sigma' \leftrightarrows_M \tilde{t}_2, \tilde{\sigma}', \Phi \wedge \varphi_2$ from which we can conclude that $t_2, \sigma' \leftrightarrows_M \tilde{t}_2, \tilde{\sigma}', \Phi \wedge \varphi_2$.

Case $t = t_1 \blacklozenge t_2$

Two rules applies in this case.

Case $i = \mathsf{F}\, i$

$$\text{H-FirstOr}\ \frac{t_1, \sigma \xrightarrow{i} t_1', \sigma'}{t_1 \blacklozenge t_2, \sigma \xrightarrow{\mathsf{F}\, i} t_1' \blacklozenge t_2, \sigma'}$$

Provided that $t_1 \blacklozenge t_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\text{SH-Or}\ \frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}_1', \tilde{\imath}_1, \varphi_1} \quad \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_2', \tilde{\sigma}_2', \tilde{\imath}_2, \varphi_2}}{\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \blacklozenge \tilde{t}_2, \tilde{\sigma}_1', \mathsf{F}\, \tilde{\imath}_1, \varphi_1} \cup \overline{\tilde{t}_1 \blacklozenge \tilde{t}_2', \tilde{\sigma}_2', \mathsf{S}\, \tilde{\imath}_2, \varphi_2}}$ then .

By application of the induction hypothesis we obtain $\mathcal{S}(\Phi \wedge \varphi_1)$ implies $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$ from which we can conclude that $t_1' \blacklozenge t_2, \sigma' \leftrightarrows_M \tilde{t}_1' \blacklozenge \tilde{t}_2, \tilde{\sigma}', \Phi \wedge \varphi_1$.

Case $i = \mathsf{S}\, i$

$$\text{H-SecondOr}\ \frac{t_2, \sigma \xrightarrow{i} t_2', \sigma'}{t_1 \blacklozenge t_2, \sigma \xrightarrow{\mathsf{S}\, i} t_1 \blacklozenge t_2', \sigma'}$$

Provided that $t_1 \blacklozenge t_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and ,

$$\text{SH-Or}\ \frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}_1', \tilde{\imath}_1, \varphi_1} \qquad \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_2', \tilde{\sigma}_2', \tilde{\imath}_2, \varphi_2}}{\text{then}\ \ \tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \blacklozenge \tilde{t}_2, \tilde{\sigma}_1', \mathsf{F}\, \tilde{\imath}_1, \varphi_1} \cup \overline{\tilde{t}_1 \blacklozenge \tilde{t}_2', \tilde{\sigma}_2', \mathsf{S}\, \tilde{\imath}_2, \varphi_2}}$$

By application of the induction hypothesis we obtain $\mathcal{S}(\Phi \wedge \varphi_2)$ implies $t_2', \sigma' \leftrightarrows_M \tilde{t}_2', \tilde{\sigma}', \Phi \wedge \varphi_2$ from which we can conclude that $t_1 \blacklozenge t_2', \sigma' \leftrightarrows_M \tilde{t}_1 \blacklozenge \tilde{t}_2', \tilde{\sigma}', \Phi \wedge \varphi_2$.

Case $t = t_1 \bowtie t_2$

Two rules applies in this case.

Case $i = \mathsf{F}\, i$

$$\text{H-FirstAnd}\ \frac{t_1, \sigma \xrightarrow{i} t_1', \sigma'}{t_1 \bowtie t_2, \sigma \xrightarrow{\mathsf{F}\, i} t_1' \bowtie t_2, \sigma'}$$

Provided that $t_1 \bowtie t_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and ,

$$\text{SH-And}\ \frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}_1', \tilde{\imath}_1, \varphi_1} \qquad \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_2', \tilde{\sigma}_2', \tilde{\imath}_2, \varphi_2}}{\text{then}\ \ \tilde{t}_1 \bowtie \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \bowtie \tilde{t}_2, \tilde{\sigma}_1', \mathsf{F}\, \tilde{\imath}_1, \varphi_1} \cup \overline{\tilde{t}_1 \bowtie \tilde{t}_2', \tilde{\sigma}_2'', \mathsf{S}\, \tilde{\imath}_2, \varphi_2}}$$

By application of the induction hypothesis we obtain $\mathcal{S}(\Phi \wedge \varphi_1)$ implies $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$ from which we can conclude that $t_1' \bowtie t_2, \sigma' \leftrightarrows_M \tilde{t}_1' \bowtie \tilde{t}_2, \tilde{\sigma}', \Phi \wedge \varphi_1$.

Case $i = \mathsf{S}\, i$

$$\text{H-SecondAnd}\ \frac{t_2, \sigma \xrightarrow{i} t_2', \sigma'}{t_1 \bowtie t_2, \sigma \xrightarrow{\mathsf{S}\, i} t_1 \bowtie t_2', \sigma'}$$

Provided that $t_1 \bowtie t_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and ,

$$\text{SH-And}\ \frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}_1', \tilde{\imath}_1, \varphi_1} \qquad \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_2', \tilde{\sigma}_2', \tilde{\imath}_2, \varphi_2}}{\text{then}\ \ \tilde{t}_1 \bowtie \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \bowtie \tilde{t}_2, \tilde{\sigma}_1', \mathsf{F}\, \tilde{\imath}_1, \varphi_1} \cup \overline{\tilde{t}_1 \bowtie \tilde{t}_2', \tilde{\sigma}_2'', \mathsf{S}\, \tilde{\imath}_2, \varphi_2}}$$

By application of the induction hypothesis we obtain $\mathcal{S}(\Phi \wedge \varphi_2)$ implies $t_2', \sigma' \leftrightarrows_M \tilde{t}_2', \tilde{\sigma}', \Phi \wedge \varphi_2$ from which we can conclude that $t_1 \bowtie t_2', \sigma' \leftrightarrows_M \tilde{t}_1 \bowtie \tilde{t}_2', \tilde{\sigma}', \Phi \wedge \varphi_2$.

Proof (Completeness of normalise). We prove Lemma 11 by induction over e.

From the premise, we can assume that $e, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$. Now, given that $e, \sigma \Downarrow t, \sigma'$, we need to demonstrate that $\tilde{e}, \tilde{\sigma} \Downarrow \tilde{t}, \tilde{\sigma}'$ with $t, \sigma' \leftrightarrows_M \tilde{t}, \tilde{\sigma}', \Phi \wedge \varphi$.

The base case is when the N-Done rule applies.

$$\text{N-Done}\ \frac{e, \sigma \downarrow t, \sigma' \qquad t, \sigma' \mapsto t', \sigma''}{e, \sigma \Downarrow t, \sigma'}\ \sigma' = \sigma'' \wedge t = t'$$

In this case, we obtain from Lemma 13 that $\tilde{e}, \tilde{\sigma} \lll \tilde{t}, \tilde{\sigma}'$ with $t, \sigma' \leftrightarrows_M \tilde{t}, \tilde{\sigma}', \Phi \wedge \varphi$, which is exactly what we needed to show.

The only induction step is when

$$\text{N-Repeat}\ \frac{e, \sigma \downarrow t, \sigma' \qquad t, \sigma' \mapsto t', \sigma'' \qquad t', \sigma'' \Downarrow t'', \sigma'''}{e, \sigma \Downarrow t'', \sigma'''}\ \sigma' \neq \sigma'' \vee t \neq t'$$

applies.

In this case, we obtain from Lemma 13 that $\tilde{e}, \tilde{\sigma} \lll \tilde{t}, \tilde{\sigma}'$ with $t, \sigma' \leftrightarrows_M \tilde{t}, \tilde{\sigma}', \Phi \wedge \varphi$. Furthermore, by Lemma 12 we obtain that $\tilde{t}, \tilde{\sigma}' \rightsquigarrow \tilde{t}', \tilde{\sigma}''$ with $t', \sigma'' \leftrightarrows_M \tilde{t}', \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. Then finally, by application of the induction hypothesis, we obtain what we needed to prove. $\tilde{t}', \tilde{\sigma}'' \lll \tilde{t}'', \tilde{\sigma}'''$ with $t'', \sigma''' \leftrightarrows_M \tilde{t}'', \tilde{\sigma}''', \Phi \wedge \varphi_1 \wedge \varphi_2 \wedge \varphi_3$.

Proof (Completeness of stride).

Case $t = \square\, v$

S-Edit

$$\frac{}{\square\, v, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi \quad \text{and} \quad \square\, v, \sigma \mapsto \square\, v, \sigma}$$

Provided that $\square\, v, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\square\, v, \sigma \mapsto \square\, v, \sigma$, we can conclude that $\tilde{t} = \square\, \tilde{v}$ and then by SS-Edit, $\square\, \tilde{v}, \tilde{\sigma} \rightsquigarrow \square\, \tilde{v}, \tilde{\sigma}$. Since the expressions do not change in this case, consistency holds trivially.

Case $t = \boxtimes\, \tau$

S-Fill

$$\frac{}{\boxtimes\, \tau, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi \quad \text{and} \quad \boxtimes\, \tau, \sigma \mapsto \boxtimes\, \tau, \sigma}$$

Provided that $\boxtimes\, \tau, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\boxtimes\, \tau, \sigma \mapsto \boxtimes\, \tau, \sigma$, we can conclude that $\tilde{t} = \boxtimes\, \tau$ and then by SS-Fill, $\boxtimes\, \tau, \tilde{\sigma} \rightsquigarrow \boxtimes\, \tau, \tilde{\sigma}$. Since the expressions do not change in this case, consistency holds trivially.

Case $t = \blacksquare\, l$

S-Update

$$\frac{}{\blacksquare\, l, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi \quad \text{and} \quad \blacksquare\, l, \sigma \mapsto \blacksquare\, l, \sigma}$$

Provided that $\blacksquare\, l, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\blacksquare\, l, \sigma \mapsto \blacksquare\, l, \sigma$, we can conclude that $\tilde{t} = \blacksquare\, l$ and then by SS-Update, $\blacksquare\, l, \tilde{\sigma} \rightsquigarrow \blacksquare\, l, \tilde{\sigma}$. Since the expressions do not change in this case, consistency holds trivially.

Case $t = \lightning$

S-Fail

$$\frac{}{\lightning, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi \quad \text{and} \quad \lightning, \sigma \mapsto \lightning, \sigma}$$

Provided that $\lightning, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\lightning, \sigma \mapsto \lightning, \sigma$, we can conclude that $\tilde{t} = \lightning$ and then by SS-Fail, $\lightning, \tilde{\sigma} \rightsquigarrow \lightning, \tilde{\sigma}$. Since the expressions do not change in this case, consistency holds trivially.

Case $t = e_1 \Diamond e_2$

S-Xor

$$\frac{}{e_1 \Diamond e_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi \quad \text{and} \quad e_1 \Diamond e_2, \sigma \mapsto e_1 \Diamond e_2, \sigma}$$

Provided that $e_1 \Diamond e_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $e_1 \Diamond e_2, \sigma \mapsto e_1 \Diamond e_2, \sigma$, we can conclude that $\tilde{t} = \tilde{e}_1 \Diamond \tilde{e}_2$ and then by SS-Xor, $\tilde{e}_1 \Diamond \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \tilde{e}_1 \Diamond \tilde{e}_2, \tilde{\sigma}$. Since the expressions do not change in this case, consistency holds trivially.

Case $t = t_1 \blacktriangleright e_2$

Three rules apply.

Case S-ThenStay

Provided that $t_1 \blacktriangleright e_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\dfrac{t_1, \sigma \mapsto {t_1}', \sigma'}{t_1 \blacktriangleright e_2, \sigma \mapsto {t_1}' \blacktriangleright e_2, \sigma'}\ \text{S-ThenStay}\ \mathcal{V}({t_1}', \sigma') = \bot$, then by the induction hypothesis, we have $\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \tilde{t}_1', \tilde{\sigma}', \varphi$ and $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi$. Then by SS-ThenStay, we have $\tilde{t}_1 \blacktriangleright \tilde{e}_2, \sigma \rightsquigarrow \tilde{t}_1' \blacktriangleright \tilde{e}_2, \sigma', \varphi$ and $t_1' \blacktriangleright e_2, \sigma' \leftrightarrows_M \tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \Phi \wedge \varphi$.

Case S-ThenFail

Provided that $t_1 \blacktriangleright e_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and

$\dfrac{t_1, \sigma \mapsto {t_1}', \sigma' \qquad e_2\ v_1, \sigma' \downarrow t_2, \sigma''}{t_1 \blacktriangleright e_2, \sigma \mapsto {t_1}' \blacktriangleright e_2, \sigma'}\ \text{S-ThenFail}\ \mathcal{V}({t_1}', \sigma') = v_1 \wedge \mathcal{F}(t_2, \sigma'')$, then by the induction hypothesis, we have $\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \tilde{t}_1', \tilde{\sigma}', \varphi$ and $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi$. Then by SS-ThenFail, we have $\tilde{t}_1 \blacktriangleright \tilde{e}_2, \sigma \rightsquigarrow \tilde{t}_1' \blacktriangleright \tilde{e}_2, \sigma', \varphi$ and $t_1' \blacktriangleright e_2, \sigma' \leftrightarrows_M \tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \Phi \wedge \varphi$.

Case S-ThenCont

Provided that $t_1 \blacktriangleright e_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and

$\dfrac{t_1, \sigma \mapsto {t_1}', \sigma' \qquad e_2\ v_1, \sigma' \downarrow t_2, \sigma''}{t_1 \blacktriangleright e_2, \sigma \mapsto t_2, \sigma''}\ \text{S-ThenCont}\ \mathcal{V}({t_1}', \sigma') = v_1 \wedge \neg\mathcal{F}(t_2, \sigma'')$, then by the induction hypothesis, we have $\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \tilde{t}_1', \tilde{\sigma}', \varphi$ and $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$. Lemma 13 gives us that $\tilde{e}_2 \tilde{v}_1, \tilde{\sigma}' \wr \tilde{t}_2, \tilde{\sigma}'', \varphi_2$ and $t_2, \sigma'' \leftrightarrows_M \tilde{t}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. Then by SS-ThenCont, we have $\tilde{t}_1 \blacktriangleright \tilde{e}_2, \sigma \rightsquigarrow \tilde{t}_2, \sigma'', \varphi_1 \wedge \varphi_2$ and $t_2, \sigma'' \leftrightarrows_M \tilde{t}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

Case $t = t_1 \blacklozenge t_2$

One of three rules applies.

Case S-OrLeft

Provided that $t_1 \blacklozenge t_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\dfrac{t_1, \sigma \mapsto {t_1}', \sigma'}{t_1 \blacklozenge t_2, \sigma \mapsto {t_1}', \sigma'}\ \text{S-OrLeft}\ \mathcal{V}({t_1}', \sigma') = v_1$, then by the induction hypothesis, we have $\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \tilde{t}_1', \tilde{\sigma}', \varphi$ and $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi$. Then by SS-OrLeft, we have $\tilde{t}_1 \blacklozenge \tilde{t}_2, \sigma \rightsquigarrow \tilde{t}_1', \sigma', \varphi$ and $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi$.

Case S-OrRight

Provided that $t_1 \blacklozenge t_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and

$\dfrac{t_1, \sigma \mapsto {t_1}', \sigma' \qquad t_2, \sigma' \mapsto {t_2}', \sigma''}{t_1 \blacklozenge t_2, \sigma \mapsto {t_2}', \sigma''}\ \text{S-OrRight}\ \mathcal{V}({t_1}', \sigma') = \bot \wedge \mathcal{V}({t_2}', \sigma'') = v_2$, then by the induction hypothesis, we have $\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \tilde{t}_1', \tilde{\sigma}', \varphi$ and $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$. A second application of the induction hypothesis gives us that $\tilde{t}_2, \tilde{\sigma}' \wr \tilde{t}_2', \tilde{\sigma}'', \varphi_2$ and $t_2', \sigma'' \leftrightarrows_M \tilde{t}_2', \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. Then by SS-OrRight, we have $\tilde{t}_1 \blacklozenge \tilde{t}_2, \sigma \rightsquigarrow \tilde{t}_2', \sigma'', \varphi_1 \wedge \varphi_2$ and $t_2', \sigma'' \leftrightarrows_M \tilde{t}_2', \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

Case S-OrNone

Provided that $t_1 \blacklozenge t_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and

S-OrRight
$$\frac{t_1, \sigma \mapsto t_1', \sigma' \qquad t_2, \sigma' \mapsto t_2', \sigma''}{t_1 \blacklozenge t_2, \sigma \mapsto t_2', \sigma''} \mathcal{V}(t_1', \sigma') = \bot \wedge \mathcal{V}(t_2', \sigma'') = v_2$$
, then by the induction hypothesis, we have $\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \tilde{t}_1', \tilde{\sigma}', \varphi$ and $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$. A second application of the induction hypothesis gives us that $\tilde{t}_2, \tilde{\sigma}' \rightsquigarrow \tilde{t}_2', \tilde{\sigma}'', \varphi_2$ and $t_2', \sigma'' \leftrightarrows_M \tilde{t}_2', \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. Then by SS-OrNone, we have $\tilde{t}_1 \blacklozenge \tilde{t}_2, \sigma \rightsquigarrow \tilde{t}_1' \blacklozenge \tilde{t}_2', \sigma'', \varphi_1 \wedge \varphi_2$ and $t_1' \blacklozenge t_2', \sigma'' \leftrightarrows_M \tilde{t}_1' \blacklozenge \tilde{t}_2', \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

Case $t = t_1 \triangleright e_2$

S-Next
$$\frac{t_1, \sigma \mapsto t_1', \sigma'}{t_1 \triangleright e_2, \sigma \mapsto t_1' \triangleright e_2, \sigma'}$$
Provided that $t_1 \triangleright e_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and , then by the induction hypothesis, we have $\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \tilde{t}_1', \tilde{\sigma}', \varphi$ and $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi$. Then by SS-Next, we have $\tilde{t}_1 \triangleright \tilde{e}_2, \sigma \rightsquigarrow \tilde{t}_1', \sigma', \varphi$ and $t_1' \triangleright e_2, \sigma' \leftrightarrows_M \tilde{t}_1' \triangleright \tilde{e}_2, \tilde{\sigma}', \Phi \wedge \varphi$.

Case $t = t_1 \bowtie t_2$

S-And
$$\frac{t_1, \sigma \mapsto t_1', \sigma' \qquad t_2, \sigma' \mapsto t_2', \sigma''}{t_1 \bowtie t_2, \sigma \mapsto t_1' \bowtie t_2', \sigma''}$$
Provided that $t_1 \bowtie t_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and , then by the induction hypothesis, we have $\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \tilde{t}_1', \tilde{\sigma}', \varphi$ and $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$. A second application of the induction hypothesis gives us that $\tilde{t}_2, \tilde{\sigma}' \rightsquigarrow \tilde{t}_2', \tilde{\sigma}'', \varphi_2$ and $t_2', \sigma'' \leftrightarrows_M \tilde{t}_2', \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. Then by SS-And, we have $\tilde{t}_1 \bowtie \tilde{t}_2, \sigma \rightsquigarrow \tilde{t}_1' \bowtie \tilde{t}_2', \sigma'', \varphi_1 \wedge \varphi_2$ and $t_1' \bowtie t_2', \sigma'' \leftrightarrows_M \tilde{t}_1' \bowtie \tilde{t}_2', \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

Proof (Completeness of evaluate). We prove Lemma 13 by induction over e.

Case $e = v$

E-Value
$$\frac{}{v, \sigma \downarrow v, \sigma}$$
One rule applies, namely
Since $v, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$, we know that $\tilde{e} = \tilde{v}$. By SE-Value, we have $\tilde{v}, \tilde{\sigma} \tilde{\downarrow} \tilde{v}, \tilde{\sigma}$, True. Since the expressions did not change, this case holds trivially.

Case $e = \langle e_1, e_2 \rangle$

E-Pair
$$\frac{e_1, \sigma \downarrow v_1, \sigma' \qquad e_2, \sigma' \downarrow v_2, \sigma''}{\langle e_1, e_2 \rangle, \sigma \downarrow \langle v_1, v_2 \rangle, \sigma''}$$
Provided that $\langle e_1, e_2 \rangle, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and , then by application of the induction hypothesis we obtain $\tilde{e}_1, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_1, \tilde{\sigma}', \varphi_1$ and $v_1, \sigma' \leftrightarrows_M \tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi_1$. A second application of the induction hypothesis gives us $\tilde{e}_2, \tilde{\sigma}' \tilde{\downarrow} \tilde{v}_2, \tilde{\sigma}'', \varphi_2$ and $v_2, \sigma'' \leftrightarrows_M \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_2$. By SE-Pair, we have $\langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma} \tilde{\downarrow} \langle \tilde{v}_1, \tilde{v}_2 \rangle, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2$ and $\langle v_1, v_2 \rangle, \sigma'' \leftrightarrows_M \langle \tilde{v}_1, \tilde{v}_2 \rangle, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

Case $e = \mathrm{fst}\langle e_1, e_2 \rangle$

E-First
$$\frac{e_1, \sigma \downarrow v_1, \sigma'}{\mathrm{fst}\langle e_1, e_2 \rangle, \sigma \downarrow v_1, \sigma'}$$
Provided that $\mathrm{fst}\langle e_1, e_2 \rangle, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and , then by application of the induction hypothesis we obtain $\tilde{e}_1, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_1, \tilde{\sigma}', \varphi$ and $v_1, \sigma' \leftrightarrows_M \tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi$. By SE-First, we have $\mathrm{fst}\langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_1, \tilde{\sigma}', \varphi$.

Case $e = \mathsf{snd}\langle e_1, e_2\rangle$

$$\text{E-Second}\ \frac{e_2, \sigma \downarrow v_2, \sigma'}{\mathsf{snd}\langle e_1, e_2\rangle, \sigma \downarrow v_2, \sigma'}$$

Provided that $\mathsf{snd}\langle e_1, e_2\rangle, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and , then by application of the induction hypothesis we obtain $\tilde{e}_2, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_2, \tilde{\sigma}', \varphi$ and $v_2, \sigma' \leftrightarrows_M \tilde{v}_2, \tilde{\sigma}', \Phi \wedge \varphi$. By SE-Second, we have $\mathsf{snd}\langle \tilde{e}_1, \tilde{e}_2\rangle, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_2, \tilde{\sigma}', \varphi$.

Case $e = e_1 :: e_2$

$$\text{E-Cons}\ \frac{e_1, \sigma \downarrow v_1, \sigma' \qquad e_2, \sigma' \downarrow v_2, \sigma''}{e_1 :: e_2, \sigma \downarrow v_1 :: v_2, \sigma''}$$

Provided that $e_1 :: e_2, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and , then by application of the induction hypothesis we obtain $\tilde{e}_1, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_1, \tilde{\sigma}', \varphi_1$ and $v_1, \sigma' \leftrightarrows_M \tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi_1$. A second application of the induction hypothesis gives us $\tilde{e}_2, \tilde{\sigma}' \tilde{\downarrow} \tilde{v}_2, \tilde{\sigma}'', \varphi_2$ and $v_2, \sigma'' \leftrightarrows_M \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_2$. By SE-Cons, we have $\tilde{e}_1 :: \tilde{e}_2, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2$ and $v_1 :: v_2, \sigma'' \leftrightarrows_M \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

Case $e = \mathsf{head}\, e$

$$\text{E-Head}\ \frac{e, \sigma \downarrow v_1 :: v_2, \sigma'}{\mathsf{head}\, e, \sigma \downarrow v_1, \sigma'}$$

Provided that $\mathsf{head}\, e, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and , then by application of the induction hypothesis we obtain $\tilde{e}, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}', \varphi$ and $v_1 :: v_2, \sigma' \leftrightarrows_M \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}', \Phi \wedge \varphi$. By SE-Head, we have $\tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_1, \tilde{\sigma}', \varphi$.

Case $e = \mathsf{tail}\, e$

$$\text{E-Tail}\ \frac{e, \sigma \downarrow v_1 :: v_2, \sigma'}{\mathsf{tail}\, e, \sigma \downarrow v_2, \sigma'}$$

Provided that $\mathsf{tail}\, e, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and , then by application of the induction hypothesis we obtain $\tilde{e}, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}', \varphi$ and $v_1 :: v_2, \sigma' \leftrightarrows_M \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}', \Phi \wedge \varphi$. By SE-Tail, we have $\tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_2, \tilde{\sigma}', \varphi$.

Case $e = e_1 e_2$

Provided that $e_1 e_2, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and

$$\text{E-App}\ \frac{e_1, \sigma \downarrow \lambda x : \tau . e_1', \sigma' \qquad e_2, \sigma' \downarrow v_2, \sigma'' \qquad e_1'[x \mapsto v_2], \sigma'' \downarrow v_1, \sigma'''}{e_1 e_2, \sigma \downarrow v_1, \sigma'''}$$

, then by application of the induction hypothesis we obtain $\tilde{e}_1, \tilde{\sigma} \tilde{\downarrow} \lambda x : \tau . \tilde{e}_1', \tilde{\sigma}', \varphi_1$ and $\lambda x : \tau . e_1', \sigma' \leftrightarrows_M \lambda x : \tau . \tilde{e}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$. A second application of the induction hypothesis gives us $\tilde{e}_2, \tilde{\sigma}' \tilde{\downarrow} \tilde{v}_2, \tilde{\sigma}'', \varphi_2$ and $v_2, \sigma'' \leftrightarrows_M \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. Then finally by a third application of the induction hypothesis, we get $\tilde{e}_1'[x \mapsto \tilde{v}_2], \tilde{\sigma}'' \tilde{\downarrow} \tilde{v}_1, \tilde{\sigma}''', \varphi_3$ and $v_1, \sigma''' \leftrightarrows_M \tilde{v}_1, \tilde{\sigma}''', \Phi \wedge \varphi_1 \wedge \varphi_2 \wedge \varphi_3$. By SE-App, we have $\tilde{e}_1 \tilde{e}_2, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_1, \tilde{\sigma}''', \varphi_1 \wedge \varphi_2 \wedge \varphi_2$.

Case $e = \mathbf{if}\, e_1\, \mathbf{then}\, e_2\, \mathbf{else}\, e_3$

Case 1

Provided that $\textbf{if}\ e_1\ \textbf{then}\ e_2\ \textbf{else}\ e_3, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and
E-IfTrue
$$\frac{e_1, \sigma \downarrow \mathsf{True}, \sigma' \qquad e_2, \sigma' \downarrow v_2, \sigma''}{\textbf{if}\ e_1\ \textbf{then}\ e_2\ \textbf{else}\ e_3, \sigma \downarrow v_2, \sigma''}$$
, then by application of the induction hypothesis we obtain $\tilde{e}_1, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_1, \tilde{\sigma}', \varphi_1$ and $\mathsf{True}, \sigma' \leftrightarrows_M \tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi_1$. A second application of the induction hypothesis gives us $\tilde{e}_2, \tilde{\sigma}' \tilde{\downarrow} \tilde{v}_2, \tilde{\sigma}'', \varphi_2$ and $v_2, \sigma'' \leftrightarrows_M \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. By SE-If, we have $\textbf{if}\ \tilde{e}_1\ \textbf{then}\ \tilde{e}_2\ \textbf{else}\ \tilde{e}_3, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2 \wedge \tilde{v}_1$.

Case 2

Provided that $\textbf{if}\ e_1\ \textbf{then}\ e_2\ \textbf{else}\ e_3, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and
E-IfFalse
$$\frac{e_1, \sigma \downarrow v_1, \sigma' \qquad e_3, \sigma' \downarrow v_3, \sigma''}{\textbf{if}\ e_1\ \textbf{then}\ e_2\ \textbf{else}\ e_3, \sigma \downarrow v_3, \sigma''}$$
, then by application of the induction hypothesis we obtain $\tilde{e}_1, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_1, \tilde{\sigma}', \varphi_1$ and $\mathsf{False}, \sigma' \leftrightarrows_M \tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi_1$. A second application of the induction hypothesis gives us $\tilde{e}_3, \tilde{\sigma}' \tilde{\downarrow} \tilde{v}_3, \tilde{\sigma}'', \varphi_2$ and $v_3, \sigma'' \leftrightarrows_M \tilde{v}_3, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. By SE-If, we have $\textbf{if}\ \tilde{e}_1\ \textbf{then}\ \tilde{e}_2\ \textbf{else}\ \tilde{e}_3, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_3, \tilde{\sigma}'', \varphi_1 \wedge \varphi_3 \wedge \neg \tilde{v}_1$.

Case $e = \textbf{ref}\ e$

E-Ref
$$\frac{e, \sigma \downarrow v, \sigma' \qquad l \notin Dom(\sigma')}{\textbf{ref}\ e, \sigma \downarrow l, \sigma'[l \mapsto v]}$$
Provided that $\textbf{ref}\ e, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and , then by application of the induction hypothesis we obtain $\tilde{e}, \tilde{\sigma} \tilde{\downarrow} \tilde{v}, \tilde{\sigma}', \varphi$ and $v, \sigma' \leftrightarrows_M \tilde{v}, \tilde{\sigma}', \Phi \wedge \varphi$. By SE-Ref, we have $\textbf{ref}\ \tilde{e}, \tilde{\sigma} \tilde{\downarrow} l, \tilde{\sigma}'[l \mapsto \tilde{v}], \varphi$ and $l, \sigma'[l \mapsto v] \leftrightarrows_M l, \tilde{\sigma}'[f \mapsto \tilde{v}], \Phi \wedge \varphi$.

Case $e = !e$

E-Deref
$$\frac{e, \sigma \downarrow l, \sigma'}{!e, \sigma \downarrow \sigma'(l), \sigma'}$$
Provided that $!e, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and , then by application of the induction hypothesis we obtain $\tilde{e}, \tilde{\sigma} \tilde{\downarrow} l, \tilde{\sigma}', \varphi$ and $l, \sigma' \leftrightarrows_M l, \tilde{\sigma}', \Phi \wedge \varphi$. By SE-Deref, we have $!\tilde{e}, \tilde{\sigma} \tilde{\downarrow} \tilde{\sigma}'(l), \tilde{\sigma}', \varphi$ and $\sigma'(l), \sigma' \leftrightarrows_M \tilde{\sigma}'(l), \tilde{\sigma}', \Phi \wedge \varphi$.

Case $e = e_1 := e_2$

E-Assign
$$\frac{e_1, \sigma \downarrow l, \sigma' \qquad e_2, \sigma' \downarrow v_2, \sigma''}{e_1 := e_2, \sigma \downarrow \langle\rangle, \sigma''[l \mapsto v_2]}$$
Provided that $e_1 := e_2, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and , then by application of the induction hypothesis we obtain $\tilde{e}_1, \tilde{\sigma} \tilde{\downarrow} l, \tilde{\sigma}', \varphi_1$ and $l, \sigma' \leftrightarrows_M l, \tilde{\sigma}', \Phi \wedge \varphi_1$. A second application of the induction hypothesis gives us $\tilde{e}_2, \tilde{\sigma}' \tilde{\downarrow} \tilde{v}_2, \tilde{\sigma}'', \varphi_2$ and $v_2, \sigma'' \leftrightarrows_M \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_2$. By SE-Assign, we have $\tilde{e}_1 := \tilde{e}_2, \tilde{\sigma} \tilde{\downarrow} \langle\rangle, \tilde{\sigma}''[l \mapsto \tilde{v}_2], \varphi_1 \wedge \varphi_2$ and $\mathsf{Unit}, \sigma''[l \mapsto v_2] \leftrightarrows_M \mathsf{Unit}, \tilde{\sigma}''[l \mapsto \tilde{v}_2], \Phi \wedge \varphi_1 \wedge \varphi_2$.

Case $e = \square\, e$

E-Edit
$$\frac{e, \sigma \downarrow v, \sigma'}{\square\, e, \sigma \downarrow \square\, v, \sigma'}$$
Provided that $\square\, e, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and , then by application of the induction hypothesis we obtain $\tilde{e}, \tilde{\sigma} \tilde{\downarrow} \tilde{v}, \tilde{\sigma}', \varphi$ and $v, \sigma' \leftrightarrows_M \tilde{v}, \tilde{\sigma}', \Phi \wedge \varphi$. By SE-Edit, we have $\square\, \tilde{e}, \tilde{\sigma} \tilde{\downarrow} \square\, \tilde{v}, \tilde{\sigma}', \varphi$ and $\square\, v, \sigma' \leftrightarrows_M \square\, \tilde{v}, \tilde{\sigma}', \Phi \wedge \varphi$.

Case $e = \boxtimes\, \tau$

$$\text{E-Enter}\quad \frac{}{\boxtimes\, \tau, \sigma \downarrow \boxtimes\, \tau, \sigma}$$

One rule applies, namely $\frac{}{\boxtimes\, \tau, \sigma \downarrow \boxtimes\, \tau, \sigma}$. Since $\boxtimes\, \tau, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$, we know that $\tilde{e} = \boxtimes\, \tau$. By SE-Enter, we have $\boxtimes\, \tau, \tilde{\sigma} \tilde{\downarrow} \boxtimes\, \tau, \tilde{\sigma}$, True. Since the expressions did not change, this case holds trivially.

Case $e = \blacksquare\, e$

$$\text{E-Update}\quad \frac{e, \sigma \downarrow l, \sigma'}{\blacksquare\, e, \sigma \downarrow \blacksquare\, l, \sigma'}$$

Provided that $\blacksquare\, e, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and $\frac{e, \sigma \downarrow l, \sigma'}{\blacksquare\, e, \sigma \downarrow \blacksquare\, l, \sigma'}$, then by application of the induction hypothesis we obtain $\tilde{e}, \tilde{\sigma} \tilde{\downarrow} l, \tilde{\sigma}', \varphi$ and $l, \sigma' \leftrightarrows_M l, \tilde{\sigma}', \Phi \wedge \varphi$. By SE-Update, we have $\blacksquare\, \tilde{e}, \tilde{\sigma} \tilde{\downarrow} \blacksquare\, l, \tilde{\sigma}', \varphi$ and $\blacksquare\, l, \sigma' \leftrightarrows_M \blacksquare\, l, \tilde{\sigma}', \Phi \wedge \varphi$.

Case $e = e_1 \blacktriangleright e_2$

$$\text{E-Then}\quad \frac{e_1, \sigma \downarrow t_1, \sigma'}{e_1 \blacktriangleright e_2, \sigma \downarrow t_1 \blacktriangleright e_2, \sigma'}$$

Provided that $e_1 \blacktriangleright e_2, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and $\frac{e_1, \sigma \downarrow t_1, \sigma'}{e_1 \blacktriangleright e_2, \sigma \downarrow t_1 \blacktriangleright e_2, \sigma'}$, then by application of the induction hypothesis we obtain $\tilde{e}_1, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_1, \tilde{\sigma}', \varphi$ and $v_1, \sigma' \leftrightarrows_M \tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi$. By SE-Then, we have $\tilde{e}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \varphi$ and $v_1 \blacktriangleright e_2, \sigma' \leftrightarrows_M \tilde{v}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \Phi \wedge \varphi$.

Case $e = e_1 \triangleright e_2$

$$\text{E-Next}\quad \frac{e_1, \sigma \downarrow t_1, \sigma'}{e_1 \triangleright e_2, \sigma \downarrow t_1 \triangleright e_2, \sigma'}$$

Provided that $e_1 \triangleright e_2, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and $\frac{e_1, \sigma \downarrow t_1, \sigma'}{e_1 \triangleright e_2, \sigma \downarrow t_1 \triangleright e_2, \sigma'}$, then by application of the induction hypothesis we obtain $\tilde{e}_1, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_1, \tilde{\sigma}', \varphi$ and $v_1, \sigma' \leftrightarrows_M \tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi$. By SE-Next, we have $\tilde{e}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_1 \triangleright \tilde{e}_2, \tilde{\sigma}', \varphi$ and $v_1 \blacktriangleright e_2, \sigma' \leftrightarrows_M \tilde{v}_1 \triangleright \tilde{e}_2, \tilde{\sigma}', \Phi \wedge \varphi$.

Case $e = e_1 \blacklozenge e_2$

$$\text{E-Or}\quad \frac{e_1, \sigma \downarrow t_1, \sigma' \qquad e_2, \sigma' \downarrow t_2, \sigma''}{e_1 \blacklozenge e_2, \sigma \downarrow t_1 \blacklozenge t_2, \sigma''}$$

Provided that $e_1 \blacklozenge e_2, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and $\frac{e_1, \sigma \downarrow t_1, \sigma' \qquad e_2, \sigma' \downarrow t_2, \sigma''}{e_1 \blacklozenge e_2, \sigma \downarrow t_1 \blacklozenge t_2, \sigma''}$, then by application of the induction hypothesis we obtain $\tilde{e}_1, \tilde{\sigma} \tilde{\downarrow} \tilde{t}_1, \tilde{\sigma}', \varphi_1$ and $t_1, \sigma' \leftrightarrows_M \tilde{t}_1, \tilde{\sigma}', \Phi \wedge \varphi_1$.

A second application of the induction hypothesis gives us $\tilde{e}_2, \tilde{\sigma}' \tilde{\downarrow} \tilde{t}_2, \tilde{\sigma}'', \varphi_2$ and $t_2, \sigma'' \leftrightarrows_M \tilde{t}_2, \tilde{\sigma}'', \Phi \wedge \varphi_2$. By SE-Or, we have $\tilde{e}_1 \blacklozenge \tilde{e}_2, \tilde{\sigma} \tilde{\downarrow} \tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2$ and $t_1 \blacklozenge t_2, \sigma'' \leftrightarrows_M \tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

Case $e = e_1 \lozenge e_2$

$$\text{E-Xor}\quad \frac{}{e_1 \lozenge e_2, \sigma \downarrow e_1 \lozenge e_2, \sigma}$$

One rule applies, namely $\frac{}{e_1 \lozenge e_2, \sigma \downarrow e_1 \lozenge e_2, \sigma}$. Since $e_1 \lozenge e_2, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$, we know that $\tilde{e} = \tilde{e}_1 \lozenge \tilde{e}_2$. By SE-Xor, we have $\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \tilde{\downarrow} \tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma}$, True. Since the expressions did not change, this case holds trivially.

Case $e = \lightning$

$$\textsc{E-Fail}\quad \frac{}{\lightning, \sigma \downarrow \lightning, \sigma}$$

One rule applies, namely $\frac{}{\lightning, \sigma \downarrow \lightning, \sigma}$. Since $\lightning, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$, we know that $\tilde{e} = \lightning$. By SE-Fail, we have $\lightning, \tilde{\sigma} \tilde{\downarrow} \lightning, \tilde{\sigma}$, True. Since the expressions did not change, this case holds trivially.