Certified Derivation of Small-Step From Big-Step Skeletal Semantics
Guillaume Ambal, Sergueï Lenglet, Alan Schmitt, Camille Noûs

To cite this version:

HAL Id: hal-03768820
https://inria.hal.science/hal-03768820
Submitted on 5 Sep 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Certified Derivation of Small-Step From Big-Step Skeletal Semantics

Guillaume Ambal
Univ Rennes
France
guillaume.ambal@irisa.fr

Sergueï Lenglet
Université de Lorraine
France
serguei.lenglet@univ-lorraine.fr

Alan Schmitt
Inria
France
alan.schmitt@inria.fr

Camille Noûs
Laboratoire Cogitamus
France
camille.nous@cogitamus.fr

ABSTRACT
We present an automatic translation of a skeletal semantics written in big-step style into an equivalent structural operational semantics. This translation is implemented on top of the Necro tool, which lets us automatically generate an OCaml interpreter for the small step semantics and a Coq mechanization of both semantics. We prove the framework correct in two ways: we provide a paper proof of the core of the transformation, and we generate Coq certification scripts alongside the transformation. We illustrate the approach using a simple imperative language and show how it scales to larger languages.

CCS CONCEPTS
• Theory of computation → Operational semantics.

KEYWORDS
Big-Step, Small-Step, Operational Semantics

ACM Reference Format:

1 INTRODUCTION
Any given programming language may come with many semantics. Even focusing on operational semantics, one can use a big-step (or natural) semantics [14], a small-step semantics [22], a context-based reduction semantics [28], or even an abstract machine [10, 15]. They all describe identical behaviors of programs, but each may be better adapted for some purposes, such as proving properties of the language, dealing with non-terminating or interacting programs, or being close to an implementation.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

PPDP 2022, September 20–22, 2022, Tbilisi, Georgia © 2022 Copyright held by the owner/author(s). Publication rights licensed to ACM. ACM ISBN 978-1-4503-9703-2/22/09... $15.00 https://doi.org/10.1145/3551357.3551384

In this skeleton, p stands for the recursive evaluation of a subterm. The constructs isTrue and isFalse are not specified: they may complete or fail, in the latter case making the whole branch fail. One may thus read this skeleton as follows. Recursively evaluate e as b, then branch on two behaviors: either compute isTrue with b then recursively evaluate s1; or compute isFalse with b then recursively evaluate s2. This piece of syntax becomes a semantics when one provides a meaning for “recursively evaluate”, “branch”, or the function isTrue; skeletal semantics enables the specification of multiple semantics for the same definition just by interpreting differently its building blocks.

A skeletal semantics can be written either in a big-step style, evaluating a term to produce a value, or in a small-step style, i.e., as a partial reduction meant to be iterated. A big-step semantics is closer to an interpreter, which explains why many languages are specified using such a style [1, 19]. However, small-step semantics are better suited to reason about intermediate execution states, e.g., in a debugger, or to prove subject reduction. They also allow for non-terminating or stuck computations, while big-step semantics may express the former only in presence of coinduction [18] and the latter only with explicit error states.

Both styles are therefore desirable, and knowing in advance which one to use when defining a language is not easy. In fact, the semantics of the high-level language of CompCert [16] was initially written in big-step, and was later rewritten as small-step. Being able to automatically derive one from the other would render the
issue moot, and proving the equivalence between the source and target semantics would ensure the correctness of the derivation. Equivalence proofs between big-step and small-step semantics are well-known [18, 21, 24] but repetitive for large languages: they can greatly benefit from additional scrutiny and automation, such as the one provided by theorem provers. While the transformation from small-step to big-step has been significantly studied [7, 11, 12, 23], the opposite direction has been less considered [13, 27], and none of these transformations comes with formal guarantees on their correctness.

In this paper, we propose an automatic translation of a big-step skeletal semantics into a small-step one, with no restriction on the input language. A first approach is to replace each recursive evaluation with a new constructor representing what is left to evaluate in the skeleton. For example in the 1f skeleton, we replace the first call with a constructor 1f2 so that if e reduces to e’, 1f(e, s1, s2) reduces to 1f2(e’, s1, s2), and if e’ is a value, 1f2 continues with the branching. We would also create two new constructors for the evaluations of s1 and s2.

Such an approach produces a lot of new constructors, which is not a problem if the resulting semantics is not meant to be manipulated by humans, e.g., if it is only produced for a debugger, where the internal states matter more than the constructors themselves. However, the main challenge of our work is to also generalize a minimal, human-readable small-step semantics — more precisely, a structural operational semantics (SOS) [22] — close to what one would write by hand, and to do so independently of the input language. We achieve such a goal by reusing the constructors of the initial big-step semantics as much as possible: in the previous example, we can reuse If instead of creating 1f2. Reusing constructors is not always possible: for example, (while e do s) does not reduce to (while e’ do s’) if e reduces to e’, as e may be needed in further executions of the loop. We create new constructors in such cases only.

Our contributions are: an automatic way of generating small-step skeletal semantics, with or without constructors reuse, from a big-step skeletal semantics of any language, from which we derive OCaml interpreters using Necro. Without reuse, we prove on paper the transformation independently from the input language, by showing that a finite or infinite sequence of small-step reductions is equivalent to an inductive or coinductive big-step evaluation. For the more complex transformation with reuse, we produce for any input language a certificate checkable in Coq of the equivalence in the finite case. We evaluate the approach on various imperative and functional languages with constructs such as pattern matching or exceptions.

The paper is structured as follows. In Section 2, we give a detailed example of skeletal semantics and of its transformation, using a simple imperative language. We formalize skeletal semantics in Section 3 and the transformation in Section 4. Section 5 presents the correspondence results without or with reuse, and shows how to generate a Coq certificate of the equivalence in the latter case. We experiment on several languages in Section 6, and discuss related work in Section 7. The appendix contains the full example introduced in Section 2, as well as the pen-and-paper proof. An implementation is available online [1] with examples of generated semantics, interpreters, and Coq certificates.

2 OVERVIEW ON AN EXAMPLE

2.1 IMP in Skeletal Semantics

Skeletal semantics is an approach to formalize the operational semantics of programming languages. The fundamental idea is to only specify the structure of evaluation functions (e.g., sequences of operations, non-deterministic choices, recursive calls) while keeping abstract basic operations (e.g., updating an environment or comparing two values). The motivation for this semantics is that the structure can be analyzed, transformed, or certified independently from the implementation choices of the basic operations. A skeletal semantics is composed of types, filters, procedures, and rules. We distinguish between base and program types. Base types are left unspecified and correspond to the base elements of the language, like environments or identifiers for variables. Program types are defined with a list of constructors, each having a precise typing.

Example 1. We write examples using the Necro [9] syntax, and use as a running example a subset of an imperative language called IMP, whose complete definition can be found in Appendix A.1. Types are defined with the keyword type: base types (int, bool, ident, state, and value) are only declared, while program types (exp and stm) are declared alongside the signature of their constructors, like an algebraic datatype definition in OCaml.

```plaintext
| type int | type ident |
| type bool | type state |
| type exp = | type value |
| Iconst of int | type stm = |
| Bconst of bool | Assign of ident * exp |
| Var of ident | Seq of stm = stm |
| Plus of exp * exp | While of exp = stm |
```

Types int and bool represent integers and boolean, collected under the type value. The type ident represents identifiers for the variables of the language and state represents environments mapping variables to values. The two program types define the expressions and statements of the language.

A distinctive feature of skeletal semantics is that we do not need to further specify the implementation of base types. The only way we can manipulate them is through typed unspecified partial functions called filters, which represent the basic operations of the language. For instance, the final representation of state does not matter as long as we define read and write operations as filters. These unspecified functions can be seen as the atomic operations of the language.

Example 2. Filters are declared with the keyword val, and are explicitly typed using the keyword unit in case of a missing input or output. We consider the following filters for IMP.

```plaintext
val add: value * value -> value
val isTrue: value -> unit
val isFalse: value -> unit
val intToVal: int -> value
val boolToVal: bool -> value
val read: ident * state -> value
val write: ident * state * value -> state
```

Procedures, declared with the hook keyword for historical reasons, correspond to the evaluation functions we want to define. Calls to procedures, or proc calls, typically represent the recursive
evaluation of subterms, they are thus the point where we want to interrupt the execution when switching to small step. A procedure operates on a term of program type using pattern matching. The behavior of the procedure on a constructor is defined with a skeleton. A skeleton represents the semantic behavior of a reduction. It is a sequence of skeleton elements, or skelements, linked via a LetIn structure. A skelement is either a function call (filter or procedure), a return of values, or a branching corresponding to a non-deterministic choice over several possible skelements.

Example 3. We define the procedures `hexp` and `hstm` for the evaluation of expressions and statements in Figure 1; the matched term is declared with the keyword matching. A branching is written `branch ... or ... end`, while the other skelements (filter or procedure call, return) are not preceded by keywords, as we can easily tell them apart.

The rule for `While` shows how branching works. We evaluate the first term to get a value `v`; in most programming languages, we would then branch depending on `v`. Here, instead, we encode this behavior with the non-deterministic branching of skeletal semantics by starting each branch with a filter either `isTrue` or `isFalse`, which causes one of the branches to fail.

Evaluating expressions with `hexp` returns a state although it is never modified. This choice prepares for extensions of the language, such as function calls, where the state could be mutated.

We now informally describe the transformation of such a semantics into small step with as much constructor reuse as possible. We first add new term constructors (Section 2.2) for the cases where reuse is impossible, and we then transform the skeletons themselves (Section 2.3). Appendix A contains the results of each transformation phase on the complete version of IMP. We also give the semantics without constructor reuse for comparison in Appendix A.6.

2.2 New Constructors

We first determine which new constructors are required in order to produce a small-step semantics. Most reduction rules use the arguments of the constructor only once. For instance, the evaluation of the term `Plus(e1, e2)` consists of first evaluating `e1`, then evaluating `e2`, then combining the results. If we make progress on one subterm, let us say `e1 ↦ e1'`, then we reconstruct the term as `Plus(e1', e2)`. We can discard the initial value of `e1` because the variables standing for `e1` and `e2` appear only once in the skeleton for `Plus(e1, e2)`. This allows us to reuse the constructor to rebuild a term after a step of computation.

In some cases, however, we cannot reuse the same constructor after a step. The different problematic situations are formally detailed in Section 4.1; here we only describe the main problem, namely that we cannot remember two versions of the same term.

Unlike `Plus`, some constructors make use of their arguments several times in their reduction rules, such as `While`. The reduction of `While(e1, e2)` might evaluate both `e1` and `e2` before cycling back to the original term `While(e1, e2)`. In a small-step setting, to reduce `e1`, we need to remember both a working copy `e1'` of the expression and its initial value to cycle back. We cannot store both `e1` and `e1'` in the `While` constructor, so we create a new one `While1` to do so.

In practice, we analyze each proc call to determine in which case it falls in. If it is a tail-call, i.e., a final procedure call forwarding its return values, there is nothing to do. If the terms it evaluates are only used once, then we reuse the same constructor. In contrast, if some of the evaluated terms are used elsewhere, then we need to create an additional constructor. In that case, the new constructor mirrors the situation at the program point and carries two copies of the terms evaluated several times. We also extend the corresponding procedure with a new reduction rule for the created constructor, which corresponds to the remainder of the initial skeleton rooted at the analyzed proc call.

We illustrate the analysis on several IMP constructors. We can reuse `Plus` after each proc call, as the arguments of the calls—respectively `s1` and `s2`, `e1`, and `e2`—are not needed in the rest of the skeleton (cf. Figure 1). For the same reason, we can reuse `Seq` after its first proc call; its second one is a tail-call, so there is no need to worry about reuse.

```
hook hstm (s: state, t: stm) matching t: state =
| Seq (t1, t2) ->
  let s1 = hstm (s, t1) in (* reuse *)
  hstm (s1, t2) (* tail-call *)

The analysis gets more interesting for `While`:

| While (e1, t2) ->
  let (s1, v) = hexp (s, e1) in (* new constr: While1 *)
  branch
    let () = isTrue (v) in
    let s2 = hstm (s1, t2) in (* new constr: While2 *)
    hstm (s2, While (e1, t2)) (* tail-call *)
  or
    let () = isFalse (v) in
    s1
```

The third proc call is a tail-call, as it is the final instruction of one of the reduction paths. When analyzing the first one, we see that `e1` is needed later, thus we cannot reuse `While` here. Similarly, we
cannot reuse the constructor for the second proc call since t2 is needed in the tail-call.

For each of these two calls, we need to create new constructors corresponding to their respective program point. The new constructors are built with two different kinds of arguments. Firstly, we create an argument for every term being evaluated at the analyzed proc call, namely s, e1 for the first one, and s1, t2 for the other. Secondly, we create arguments for the variables needed in the rest of the skeleton; in our example, it means keeping e1 and t2 in both cases. However, we do not need to duplicate s1 nor add an argument for v as they are no longer necessary. As a result, while most variables appear only once in the arguments of a new constructor, the contentious ones—used in and after the corresponding call—are duplicated. In the end, we extend the stm type with the following constructors:

\[
\begin{align*}
\text{hook } & \text{hstm (s: state, t: stm) matching t: state =} \\
& \text{While1 of state * exp * exp * stm} \\
& \text{While2 of state * stm * exp * stm}
\end{align*}
\]

We also add a new rule for each of them. The new skeleton consists in resuming the computation from the corresponding analyzed proc call and updating the input of the call to make use of the new arguments of the constructor. The resulting rule for While1 is almost the same as the one for While, while the skeleton of While2 covers only its last two skeletons. We do not modify the rules for While nor the other constructors at this stage.

\[
\begin{align*}
\text{hook } & \text{hstm (s: state, t: stm) matching t: state =} \\
& \text{While1 (s0,e0,e1,t2) ->} \\
& \text{let (s1,v) = hexp (s0,e0) in (* reuse *)} \\
& \text{branch} \\
& \text{let () = isTrue (v) in} \\
& \text{let s2 = hstm (s1,t2) in (* new constr: While2 *)} \\
& \text{hstm (s2, While (e1,t2)) (* tail-call *)} \\
& \text{or} \\
& \text{let () = isFalse (v) in} \\
& \text{s1}
\end{align*}
\]

The added rules are used next for the last phase of the transformation. The new rules do not need to be analyzed themselves as they are duplicates of analyzed skeletons.

### 2.3 Make the Skeletons Small-Step

Previous phases set the stage for the main transformation, but the semantics is still big-step, since procedures fully compute their arguments. The last phase of the transformation makes procedures behave in a small-step way.

A small-step reduction transforms a term into another term of the same program type, whereas procedures return values. We thus need to consider these values as terms of the corresponding input type. In our example, we extend the types exp and stm with constructors corresponding to the return types of each procedure, respectively Ret_hexp of type (state, value) -> exp for hexp, and Ret_hstm of type state -> stm for hstm. We also define procedures to unpack coerced values, e.g., for expressions:

\[
\begin{align*}
\text{hook } & \text{getRet_hexp (e: exp) matching e: state * value =} \\
& \text{| Ret_hexp (v1, v2) -> (v1, v2)}
\end{align*}
\]

A similar procedure is defined for statements. These procedures are only defined for the corresponding newly created constructors, as trying to unpack the value of a term not fully reduced should fail.

We also need to change the output types of every user-defined procedure to make them match the input ones. The signature of the procedures become:

\[
\begin{align*}
\text{hook } & \text{hexp (s: state, e: exp) matching e: state * exp = ...} \\
\text{hook } & \text{hstm (s: state, t: stm) matching t: state * stm = ...}
\end{align*}
\]

Doing so makes the types coherent with a small-step reduction process meant to be iterated.

We then update the skeletons themselves. We recall that skeletons are sequences of operations (skellets), which are mostly composed of filter and proc calls. We consider that only proc calls correspond to reduction steps and should be transformed. The reason is that filters represent atomic operations that are not meant to be interrupted, while proc calls often correspond to the evaluation of a subterm. We distinguish four cases; for each of them, we illustrate the resulting skeleton with informal SOS rules to improve readability. Note that, in each example, the variable s is the state coming from the definition of the procedure.

1. If the last element of a skeleton is not a proc call, we need to use coercions to match the new signature. For type checking, we also have to return the other arguments of the procedure, even if they are not of any use. E.g., the rule for IConst returns (s, v) in the initial big-step skeleton (cf. Figure 1). Using a coercion, we turn it into Ret_hexp (s, v); we cannot return this term only, as the output type of hexp is (state * exp), so we also return a useless copy of s.

\[
\begin{align*}
\text{hook } & \text{hexp (s: state, e: exp) matching e: state * exp = ...} \\
\text{hook } & \text{hstm (s: state, t: stm) matching t: state * stm = ...}
\end{align*}
\]

2. The most interesting case is when we can reuse the constructor. It means we are at a program point corresponding to the evaluation of a subterm, and we have two possibilities: either the subterm needs to be evaluated further, in which case we take a reduction step and reconstruct; or the subterm has been fully evaluated, and we extract its value and continue the reduction according to the rest of the skeleton. We distinguish the two behaviors using branches. For instance, transforming the first proc call of the Plus constructor produces a rule structured as follows.

\[
\begin{align*}
\text{hook } & \text{getRet_hexp (e1: exp) in} \\
& \text{Plus (e1, e2) ->} \\
& \text{branch} \\
& \text{let (s',e1') = hexp (s, e1) in} \\
& \text{(s', Plus (e1', e2))} \\
& \text{or} \\
& \text{let (s1,v1) = getRet_hexp (e1) in} \\
& \text{...}
\end{align*}
\]

where the dots stands for the transformation of the second proc call (see Example 6). In the first branch, we reconstruct as (s', Plus (e1', e2)), overwriting s and e1 with the new terms resulting from the step. In the second branch, we extract the value using the procedure dedicated to Ret_hexp. Even though we use
a branching, the reduction is deterministic, as getRet_hexp and hexp are restricted to respectively coerced values and terms that are not values.

3. For a proc call for which we created a constructor, we need to change to the new constructor after a reduction step. To simplify the semantics, we consider the change to be a step by itself; the next small step can then reduce the proc call. For instance, the reduction rule for While becomes:

\[
\text{While} (e_1, t_2) \rightarrow (s, \text{While} (s, e_1, e_1, t_2))
\]

We duplicate \(s\) and \(e_1\) and return the new configuration. Copying \(s\) is not required when writing the semantics by hand but comes from the analysis of Section 2.2. Such useless duplication is not uncommon in systematic derivations of semantics, as discussed in Section 6. Calling the hstm procedure again would then execute the skeleton for \(\text{While}\) where the next reduction step and reconstruction actually take place. Similarly, we call the new constructor \(\text{While}2\) in the rule created for \(\text{While}\).

\[
\begin{align*}
\text{While}1 (s_0, e_0, e_1, t_2) &\rightarrow \text{branch} \\
&\text{let} (s_0', e_0') = \text{hexp} (s_0, e_0) \text{ in} \\
&\text{let} (s_1, v) = \text{getRet_hexp} (e_0) \text{ in} \\
&\text{branch} \\
&\text{let} () = \text{isTrue} (v) \text{ in} \\
&\text{let} () = \text{isFalse} (v) \text{ in} \\
&\text{end} \\
&\text{end}
\end{align*}
\]

This shows that the final transformation phase operates not only on the rules of the initial semantics, but also on the ones created during the analysis, and that the added constructors were sufficient.

4. Finally, we also cut tail-calls to simplify the semantics. This creates administrative steps like \(s, \text{If} (\text{True}, t_1, t_2) \rightarrow s, t_1\) where no subcomputation takes place, which is closer to usual pen-and-paper definitions. For example, the second proc call of the Seq constructor becomes a return—the first one is transformed as previously.

\[
\begin{align*}
\text{Seq} (t_1, t_2) &\rightarrow \\
\text{branch} \\
&\text{let} (s', t_1') = \text{hstm} (s, t_1) \text{ in} \\
&\text{let} (s', t_1') = \text{hstm} (s, t_1) \text{ in} \\
&\text{end} \\
&\text{end}
\end{align*}
\]

This final phase produces a small-step skeletal semantics where each proc call reduces its arguments only once. It is equivalent to the initial big-step one, in the sense that evaluating a term with either semantics produces the same value. The complete result of the transformation on IMP can be found in Appendix A.4, and we prove the equivalence between the two semantics in Sections 5.

3 SKELETAL SEMANTICS

We present the formal definition of skeletal semantics we use to describe the transformation in Section 4 and state the equivalence results in Sections 5. It mostly differs from the original one [5] by the presence of the LetIn structure and the possibility of defining several procedures, which we believe makes writing the skeletal semantics of a given language significantly easier.

3.1 Syntax and Types

We write \(\vec{a}\) for a (possibly empty) tuple \((a_1, \ldots, a_n)\), and \(\|\vec{a}\|\) for its size—here \(n\). We also write \(\vec{a}, b\) or \(\vec{a}, \vec{b}\) for its extension on the right, and \(a_i \in \vec{a}\) to state that \(a_i\) belongs to \(\vec{a}\). Given a function or relation \(f\), we write \(f(a)\) for \((f(a_1), \ldots, f(a_n))\) if \(\|\vec{a}\| = n\), and similarly \(g(a, b)\) for \((g(a_1, b_1), \ldots, g(a_n, b_n))\) if \(\|\vec{a}\| = \|\vec{b}\| = n\).

We let \(c, f, \text{and } p\) range over respectively constructor, filter, and procedure names. Assuming a countable set \(\mathcal{V}\) of variables ranged over by \(v, \omega, x, y, \text{and } z\), the grammar of terms \((t), \text{skeltons} (S), \text{and skeletons} (K)\) is defined as follows.

\[
t ::= v | c(t) \quad S ::= \text{let } \vec{a} = K \text{ in } S | K
\]

\[
K ::= \text{Filter } f (\vec{t}) | \text{Proc } p (\vec{t}, t) | \text{Return } t | \text{Branch } (\vec{S})
\]

The skeletal semantics of a language consists of: a set \(\mathcal{T}\) of types ranged over by \(s\), which includes program types \(T_p\) ranged over by \(g\); a set \(C\) of constructors, with a typing function \(\text{ctype} : C → \mathcal{T}×\mathcal{T}\); a set \(F\) of filters, with \(\text{ftype} : F → \mathcal{T}×\mathcal{T}\); a set \(\mathcal{P}\) of procedures, with \(\text{ptype} : P → (\mathcal{T}×\mathcal{T}) × \mathcal{T}\); a set \(R\) of rules \(p(\vec{g}, c(\vec{x})) : = S\), assuming \(\text{ptype}(p) = (\langle \vec{g}, s_g \rangle, \vec{s}'\rangle, \text{ctype}(c) = (\vec{s}', s_g), \|\vec{y}\| = \|\vec{z}\|, \text{and } \|\vec{x}\| = \|\vec{y}\|\).

The typing of constructors restricts their output to a term of program type, while filters may produce terms of any type. The input of a procedure \(\mathcal{T}×\mathcal{T}\) is composed of auxiliary terms of type \(\mathcal{T}\) and of the term being evaluated of program type \(T_p\), corresponding to the keyword matching in Figure 1. We define projections \(\text{ptype}_g(e)\) and \(\text{ptype}_{out} : \text{if } p(\vec{g}, c(\vec{x})) : = S \text{ then the behavior of } p\text{ on the constructor } c\text{ by the skeleton } S\), which describes the sequence of reductions to perform using the input variables \(\vec{x}\) and \(\vec{y}\). We assume the variables \(\vec{x}, \vec{y}\) to be
pairwise distinct, and to contain the free variables of $S$. We suppose that at most one rule handling $c$ for $p$ exists in $R$. The matching does not have to be exhaustive: a procedure $p$ without a rule for $c$ simply cannot reduce terms with $c$ as head constructor.

### 3.2 Interpretations

The dynamic of a skeletal semantics is given by an interpretation of the rules defining its procedures [5], which can be inductive or coinductive. It supposes an instantiation of the base types and filters. For each base type, we assume given a set representing its values. The values of program types are inductively built from its constructors. For each filter $f \in F$, we assume a relation $R_f$ between its input and output values, and write $R_f(\bar{a}) \Downarrow \bar{b}$ when the interpretation of $f$ relates the values $\bar{a}$ to $\bar{b}$.

For example, instantiating $\text{bool}$ with Booleans $\{\top, \bot\}$, we could interpret $\text{isTrue}$ to only accept $\top$ so that $R_{\text{isTrue}}(\top) \Downarrow ()$ and similarly for $\text{isFalse}$. We could also allow conditional branching on an integer by extending $\text{isTrue}$ and $\text{isFalse}$ to int, so that $R_{\text{isFalse}}(0) \Downarrow ()$ and $\forall i \neq 0. R_{\text{isTrue}}(i) \Downarrow ()$. The strength of skeletal semantics is that this choice only involves filters: we do not have to change anything in the definitions or interpretations of the procedures.

We write $\Sigma$ for an environment mapping a finite set of variables in $V$ (its domain) to values. We write $\Sigma(v)$ for the value related to $v$ in $\Sigma$, and we write $\Sigma(t)$ so that $\Sigma(c(t)) = c(\Sigma(t))$. The environment $\{v \mapsto b\}$ maps a single variable $v$ to $b$, and we write $\Sigma + \Sigma'$ for the update of $\Sigma$ with $\Sigma'$, so that $(\Sigma + \Sigma')(v) = \Sigma'(v)$ if $v$ is in the domain of $\Sigma'$, and $(\Sigma + \Sigma')(v) = \Sigma(v)$ otherwise.

The inductive interpretation $\Sigma \vdash S \Downarrow \bar{b}$, defined in Figure 2, expresses that $S$ outputs the values $\bar{b}$ under $\Sigma$; it assumes that the free variables of $S$ are in the domain of $\Sigma$. The rules are self-explanatory: e.g., evaluating a proc call consists in evaluating its arguments, which itself consists in finding the skeleton of the appropriate rule and evaluating it. The interpretation is inherently big-step, as a judgment $\Sigma \vdash S \Downarrow \bar{b}$ computes the final value returned by $S$. It is also non-deterministic because of branchings, which return the outcome of one of their successful branches, and filter calls, as $R_f$ may relate several results to the same input. Figure 2 also uses an auxiliary judgment $\bar{a} \Downarrow_p \bar{b}$ saying that the procedure $p$ taking $\bar{a}$ as input can output $\bar{b}$.

### 4 TRANSFORMATION TO SMALL STEP

#### 4.1 New Constructors

Given a big-step semantics, we discriminate its proc calls into three categories: either Tail for a tail-call, Reuse when constructor reuse is possible, or New $c$ when a new constructor $c$ is needed. Formally, we consider an intermediate skeletal semantics where proc calls are annotated: $\text{Proc } a \ p \ (\bar{t}, \bar{i}, \bar{j})$, with $a := \text{New c} | \text{Tail} \ | \text{Reuse}$. We proceed in two steps: we first analyze and annotate the proc calls before creating the new constructors.

A simple way to make the semantics small-step would be to introduce a new constructor for each call. While it is safe to do so, the resulting semantics can be optimized by reusing constructors. We aim to reuse them as much as possible to obtain a semantics close to a usual SOS. We identify three cases where reuse is not possible, or New $c$ when a new constructor $c$ is needed. Formally, we consider an intermediate skeletal semantics where proc calls are annotated: $\text{Proc } a \ p \ (\bar{t}, \bar{i}, \bar{j})$, with $a := \text{New c} | \text{Tail} \ | \text{Reuse}$. We proceed in two steps: we first analyze and annotate the proc calls before creating the new constructors.

First, even if we do not consider computing a filter as a step, we do not want to recompute the same filter several times. A constructor reuse implies that the whole skeleton is evaluated up to the proc call at each reduction step, meaning that a filter placed before the proc call would be called at every reduction step. This could have unintended consequences for filters with side effects. We therefore give up on reuse if the analyzed proc call is after a filter call.

Next, we need to account for branching non-determinism. In $\text{let } \bar{a} = \text{Branch}(\text{Proc } p_1 \bar{t}_1, \text{Proc } p_2 \bar{t}_2)$ in $\text{Proc } p \bar{t}$, two different reduction paths lead to the last call. The premise of constructor reuse is that reevaluating the skeleton from the start should lead to
to h2 has to be modified to make the types match and cannot be a tail-call.

A proc call can only reuse its constructor if it is not after a filter call or a branching $\langle b = \top \rangle$ and every term is a variable not used elsewhere ($\langle w \in V \rangle$). In the case a proc call can be annotated with either Tail or Reuse, we choose to give precedence to the former, because tail-calls are more specific and lead to simpler skeletal semantics at the end of the transformation. Proc calls that cannot be annotated Tail or Reuse are instead associated with a fresh constructor name created on the fly. We apply the analysis to every skeleton in the semantics.

After the analysis, we process every proc call annotated New c to generate the rule of c. The rule contains what is left to compute at the program point of the proc call, i.e., its continuation, that we represent as a context of the form $E := \langle \cdot \rangle \quad \text{let } z := \langle \cdot \rangle \quad \text{in } S$. Given a rule $r = \langle pr \langle y, c(z) \rangle := S \rangle$ we turn each call of $S$, of the form $E\langle \text{Proc } (\text{New } c) \ p \ t \rangle \rightarrow E\langle \text{Proc } \text{Reuse } p \ w \rangle$, where $w$ are fresh variables representing the terms $t$, and $z$ are the variables needed to evaluate $E$. The proc call $p$ is annotated with Reuse in the rule as the variables have been defined so that there is no overlap in their uses. The formal definition of this generation phase is given in Appendix B.3, we illustrate it on the following example.

**Example 4.** We apply the generation process to the second proc call in the rule for While presented in Section 2.2. We reach this proc call $K$ in a context $E$:

$K := \langle \text{Proc } (\text{NewWhile2}) \ hstm \ s2, t2 \rangle$  
$E := \text{let } s2 := \langle \cdot \rangle \quad \text{in } \langle \text{Proc Tail } hstm \ s1, \langle \text{While } \langle e1, t2 \rangle \rangle \rangle \quad \text{in } \langle \text{Proc Tail } hstm \ s1, t2 \rangle$  

The new constructor needs the variables $z = \langle e1, t2 \rangle$ to evaluate $E$. From the arguments of the proc call, we create the fresh variables $w = \langle s0, t0 \rangle$. The rule for While2 is therefore as follows.

$\text{hstm} \langle s, \langle \text{While2 } \langle s0, t0, e1, t2 \rangle \rangle \rangle := \text{let } s2 := \langle \cdot \rangle \quad \text{in } \langle \text{Proc Tail } hstm \ s2, \langle \text{While } \langle e1, t2 \rangle \rangle \rangle \quad \text{in } \langle \text{Proc Tail } hstm \ s2, \langle \text{While } \langle e1, t2 \rangle \rangle \rangle$  

**Example 5 (Without initial constructors reuse).** If we do not aim at reusing initial constructors, the analysis simply creates a new constructor for each proc call, which are processed exactly as above. For Plus (e1, e2), we create Plus1 for the evaluation of e1 and Plus2 for e2.

$\text{hexp} \langle s, \langle \text{Plus1 } \langle s0, e0, e2 \rangle \rangle \rangle := \text{let } (s',v1) := \langle \text{Proc Reuse } \text{hexp } \langle s0, e0 \rangle \rangle \quad \text{in } \langle \cdot \rangle \quad \text{hexp} \langle s, \langle \text{Plus2 } \langle s0, e0, v1 \rangle \rangle \rangle := \text{let } (s'',v2) := \langle \text{Proc Reuse } \text{hexp } \langle s0, e0 \rangle \rangle \quad \text{in } \langle \cdot \rangle$  

The generation phase is applied to every annotated rule. This results in new constructors and rules, that we add to the unmodified initial ones.

### 4.2 Distribute Branchings

This phase is not present in the extended example as the issue it solves does not occur in IMP.
Reusing constructors is problematic for procedures in nested computations. In \( \text{let } x = (\text{let } y = \text{Proc eval } t \text{ in } S_1) \text{ in } S_2 \), a small-step transformation of eval may return a partially evaluated term which ends up stored in \( x \), while \( S_2 \) may expect \( x \) to contain a value; for example \( S_2 \) may start by filtering \( x \) with \( \mathsf{isTrue} \). We avoid the issue by sequencing such nested computations as \( \text{let } y = \text{Proc eval } t \text{ in } \text{let } x = S_1 \text{ in } S_2 \), and the transformation of Section 4.3 ensures that \( x \) may only contain a value.

The grammar of skeletal semantics of Section 2.1 does not allow for nested \text{LetIn}, but the same is present for branches inside \text{LetIn}. We therefore transform a skeleton of the form \( \text{let } \tilde{v} = \text{Branch}(S_1, S_2) \text{ in } S \) into a skeleton \( \text{Branch(} \text{let } \tilde{v} = S_1 \text{ in } S, \text{let } \tilde{v} = S_2 \text{ in } S \) ), so that the reusing proc calls in \( S_1 \) and \( S_2 \) can be transformed in the final phase. To this end, we define a monadic bind on skeletons, noted \( \langle S_1 | \tilde{x} | S_2 > \), which executes \( S_1 \), binds the results to \( \tilde{x} \) then executes \( S_2 \).

\[
\langle \text{let } \tilde{y} = K \text{ in } S_1 | \tilde{x} | S_2 > = \langle \text{let } \tilde{y} = K \text{ in } \langle S_1 | \tilde{x} | S_2 > > \text{ if } K \text{ is } \langle | > \text{, and } \text{let } \tilde{y} = K \text{ in } \langle S_1 | \tilde{x} | S_2 > > \langle \text{let } \tilde{y} = K \text{ in } S_1 \rangle + \langle \text{let } \tilde{y} = \text{Branch}(S_1, S_2) \text{ in } S \rangle \text{ if } B \neq \text{Branch(...)}
\]

The distribution of \text{LetIn} over \text{Branch}, noted \( [S] \) is defined as follows, and is applied to every skeleton at this point of the transformation.

\[
[\text{Branch}(S_1, \ldots, S_n)] = \text{Branch}([S_1], \ldots, [S_n]) \quad [B] = B \quad \text{if } B \neq \text{Branch(...)}
\]

Let \( r = (\pi(y, c_r(\tilde{x}))) := S_r \), and \( R \) be the set of rules

\[\text{Return } \tilde{r} \mid \text{Return } (\tilde{g}, \text{Ret_pr } \tilde{t}) \text{ } \mid \text{Proc Tail } p \tilde{t} \mid \text{Return } \tilde{t} \]

\[\text{let } \tilde{v} = \text{Proc (New c) } p \tilde{t} \text{ in } S \mid \text{Return } (\tilde{g}, c(\tilde{t}, \tilde{z})) \text{ } \mid \text{Proc Tail } \text{pr } \tilde{t} \mid \text{Return } \tilde{t}
\]

\[\text{let } \tilde{v} = \text{Proc Reuse } p \text{ } \tilde{w} \text{ in } S \mid \text{Return } (\tilde{g}, c_r(\tilde{x}))(\sigma :: [\tilde{z} / \tilde{w}]) \]

\[\text{where } \tilde{z} \text{ are fresh and } \tilde{w} = (\tilde{w'}, w)
\]

\[S_1 = \langle \text{let } \tilde{z} = \text{Proc } p \text{ } \tilde{w} \text{ in } S \mid \text{Return } (\tilde{g}, c_r(\tilde{x}))(\sigma :: [\tilde{w} / \tilde{v}]) \text{ where } \tilde{z} \text{ are fresh and } \tilde{w} = (\tilde{w'}, w)
\]

\[S_2 = \langle \text{let } \tilde{v} = \text{Proc } \text{getRet_p } \text{ (w) in } S \mid \text{Return } (\tilde{g}, c_r(\tilde{x}))(\pi(\sigma :: [\text{getRet_p}]))/\tilde{v})
\]

\[\text{Figure 5: Main Cases of the Transformation of a Skeleton}
\]

terms are all variables \( \tilde{w} \). Because we distribute \text{LetIn}s over branchings (Section 4.2), we cannot have a skeleton of the form \( \text{let } \tilde{v} = \text{Branch } \tilde{S}' \text{ in } S \). Finally, if a skeleton ends with \( K \) that is not a tail-call, we transform it into an equivalent one by delaying the return: we replace \( K \) with the skeleton \( \text{let } \tilde{z} = K \text{ in } \text{Return } \tilde{z} \), where \( \tilde{z} \) are fresh variables. As such, it is sufficient to define our procedure on skeletons respecting the simplified grammar.

The transformation relies on a substitution to remember how the initial arguments of the rule are changed through the proc calls, as we show in Example 6. A substitution \( \sigma \) is a total mapping from variables to terms that is the identity except on a finite set of variables called its domain. We write \( x\sigma \) for the application of \( \sigma \) to \( x \), \( e \sigma \) for the identity substitution, and \( [t/x] \) for the substitution whose domain is \( \{x\} \) and such that \( x\sigma = t \). We extend the notion to terms \( t\sigma \) and tuples \( t\sigma \) as expected. Given two substitutions \( \sigma \) and \( \sigma' \), we define their sequence \( \sigma : \sigma' \) so that \( x(\sigma : \sigma') = (x\sigma)\sigma' \) for all \( x \).

Given an annotated skeleton \( S \), a rule \( r = (\pi(y, c_r(\tilde{x}))) := S_r \), and a substitution \( \sigma \) representing the knowledge accumulated so far, the transformation \( [S] r \sigma \) results in a plain skeleton—without annotations (cf. Figure 5).

We coerce the results of a final \text{Return} skeleton with the dedicated constructor \text{Ret_pr}. We remind that we return the environment variables \( \tilde{y} \) of the rule to match the updated typing of the procedure.

A tail-call is simply turned into a return, as the procedure being called is identical to the one where the current rule is defined (see Figure 4).

As explained in Section 2.3, a procedure annotated \( (\text{New c}) \) is turned into a return with a term built with \( c \). One might be surprised the proc call disappears, it is simply delegated to the new rule for \( c \) (see Section 4.1 right before Example 4). By construction of \( c \) and its rule \( (\pi(\tilde{y}, c(\tilde{w}, \tilde{z}))) := S_c \), the variables \( \tilde{w} \) are used as input of the analyzed call and \( \tilde{z} \) to compute the rest of \( S_c \). The result is therefore \( \text{Return } (\tilde{y}, c(\tilde{t}, \tilde{z})) \), where we replace \( \tilde{w} \) with the terms \( \tilde{t} \) being reduced.

We change a proc call which can reuse its constructor into a branching representing its possible behaviors. The first branch begins by making a further step \( \text{let } \tilde{z} = \text{Proc } p \text{ } \tilde{w} \text{ in } \ldots \), storing
the results in some fresh variables ħ. We then reconstruct a configuration starting from the initial input \((\tilde{y}, c_r(\tilde{x}))\), to which we apply \(\sigma\) before changing \(\tilde{w}\) by their new values ħ. The substitution \(\sigma\) is necessary if one of the variables \(\tilde{w}\) is not part of the initial arguments but defined from a previous proc call, as shown in the Plus example below. The second branch covers the case where the last term represented by \(w\) is a coerced set of values: we extract them into ħ and continue transforming \(S\), remembering that \(w\) is equal to \(\text{Ret}_p(\tilde{w})\).

**Example 6.** Consider the rule for Plus:

\[
\begin{align*}
\text{let } (s_1, v_1) &= \text{hexp} (s, e_1) \text{ in } (* \text{ reuse }*) \\
\text{let } (s_2, v_2) &= \text{hexp} (s_1, e_2) \text{ in } (* \text{ reuse }*) \\
\text{let } v &= \text{add} (v_1, v_2) \text{ in } (s_2, v)
\end{align*}
\]

The first call is turned into two branches, the first one stepping once \((s, e_1)\) into some fresh variables \((z_1, z_2)\). The reconstructed configuration is simply the input \((s, \text{Plus} (e_1, e_2))\) where \(s\) and \(e_1\) are replaced by \(z_1\) and \(z_2\). In the second branch, we extract the content of \(e_1\) and then transform the rest of the skeleton, remembering that \(e_1 = \text{Ret}_x(s_1, v_1)\).

Transforming the second proc call shows why we need \(\sigma\). As for the first one, the first branch steps once \((s_1, e_2)\) into some fresh variables \((z_3, z_4)\) and reconstructs a configuration. We see that \(s_1\) does not occur in the initial configuration \((s, \text{Plus} (e_1, e_2))\); we therefore apply the substitution to create \((s, \text{Plus} (\text{Ret}_x(s_1, v_1), e_2))\), and now we can turn \((s_1, e_2)\) into \((z_3, z_4)\), resulting in the configuration \((s, \text{Plus} (\text{Ret}_x(z_3, v_1), z_4))\). The second branch continues transforming the rest of the skeleton, where we no longer need the substitution. In the end, we obtain the following skeleton, which behaves as in the three rules below. The comments indicate the origin of the different parts: the first proc call ("\(|\)"), the second proc call ("\(||\)"), the unmodified filter call ("\(#\)"), and the coerced return ("\(\#\)!").

**hook** \(\text{hexp} (s: \text{state}, e: \text{exp})\) matching e: \(\text{state} * \text{exp} = (s, e_1, e_2) \to (s, e_1 + e_2)\)

**branch**

- \((z_1, z_2) = \text{hexp} (s, e_1)\) in \((* | | *)\)
- \((s, \text{Plus} (z_2, v_2))\) in \((* | | *)\)
- \(\text{or}\)
- \((s_1, v_1) = \text{getRet}_x(e_1)\) in \((* | | *)\)

**branch**

- \((s_3, z_4) = \text{hexp} (s_1, e_2)\) in \((* | | *)\)
- \((s, \text{Plus} (\text{Ret}_x(z_3, v_1), z_4))\) in \((* | | *)\)
- \(\text{or}\)
- \((s_2, v_2) = \text{getRet}_x(e_2)\) in \((* | | *)\)

\(\text{let } v = \text{add} (v_1, v_2) \text{ in } (* \# | | *)\)

**end**

**end**

If we do not reuse the initial constructors, we do not need the substitution \(\sigma\) as we cannot have nested proc calls where we reuse constructors. Instead, we change constructor, e.g., going from Plus1 to Plus2. As a result, the small-step transformation without reuse is written \(\| S \|\) and the skeletons \(S_1\) and \(S_2\) of the last case of Figure 5 become:

\[
S_1 = \text{let } \tilde{z} = \text{Proc } \tilde{h} \text{ in } \text{Return} (\tilde{y}, c_r(\tilde{x})) [\tilde{w}] \\
\tilde{z} \text{ fresh } ; \tilde{w} = (\tilde{w}', \tilde{w})
\]

\[
S_2 = \text{let } \tilde{u} = \text{Proc } \text{getRet}_p (\tilde{w}) \text{ in } \| S \|\]

**Example 7** (Without initial constructors reuse). If we do not reuse Plus, the rules for Plus, Plus1, and Plus2 behave as follows. Unlike Plus1 in Example 6, the new constructors takes three arguments by default (c.f., Example 5 and Appendix A.6).

\[
\begin{align*}
\text{let } (s_1, v_1) &= \text{hexp} (s, e_1) \text{ in } (* \text{ reuse }*) \\
\text{let } (s_2, v_2) &= \text{hexp} (s_1, e_2) \text{ in } (* \text{ reuse }*) \\
\text{let } v &= \text{add} (v_1, v_2) \text{ in } (s_2, v)
\end{align*}
\]

\[
\begin{align*}
\text{let } (s_0, v_0) &= \text{getRet}_p (e_1) \text{ in } \| S_0 \| \\
\text{let } (s_0, v_0) &= \text{getRet}_p (e_2) \text{ in } \| S_0 \|
\end{align*}
\]

This last phase of the transformation is applied to the rules \(R\) defining the procedures \(P \in P_0\). The final rules are:

\[
\begin{align*}
&\{ p(\tilde{y}, c(\tilde{x})) \} = \| S \| \\
&\{ \text{getRet}_p (p) \} = \text{Return} \tilde{u} \mid p \in P_0
\end{align*}
\]

In the end, we obtain a small-step semantics where every initial procedure makes a single step of computation.

The transformation has been implemented in Necro [9], reusing initial constructors by default, but with an option to not reuse them. One of the main features of the framework is the automatic derivation of an OCaml interpreter from a skeletal semantics. The interpreter is parametric in the types and functions representing the base types and filters. Using the transformation, we generate an interpreter providing both big-step and small-step implementations of procedures. The small-step interpreter relies on the same instantiated types and functions for base types and filters as the big-step one, so it provides a small-step semantics at no additional cost. Examples of generated interpreters can be found in the implementation [4].

### 5 EQUIVALENCE PROOF

We prove that the transformation is correct, i.e., that the initial and transformed semantics are equivalent. To deal with the complexity of the approach, we provide two complementary correctness results. The first one is a pen-and-paper proof that the transformation \textit{without constructor reuse} is correct. The proof is available in Appendix C, and we quickly present the results in Section 5.1. To further our trust in the transformation and to deal with constructor reuse, we provide a mechanized approach to correctness, presented in the rest of this section. This second approach does not attempt to formalize the whole transformation nor the reuse analysis, but instead it generates a fully automatic Coq proof of the equivalence...
of the initial and transformed semantics instantiated on a given language.

The pen-and-paper proof gives us confidence that the generation will not fail in the absence of constructor reuse, and the automatic Coq proof shows the correctness of the analysis for constructor reuse for a given language. The generated Coq proof can thus be considered as a certificate for an instance of the transformation.

To state the equivalence theorems between the two semantics, we use the interpretation judgments of Section 3.2 (Figure 2). To simplify notations, we write \( \text{Ret}_{\text{hexp}} \) (resp. \( \text{Ret}_{\text{hs}} \), \( \text{Ret}_{\text{p}} \)) for \( \text{Ret}_{\text{hstm}} \) (resp. \( \text{Ret}_{\text{hexp}} \), \( \text{Ret}_{\text{p}} \)), as well as \( \llbracket_{\text{he}} \) (resp. \( \llbracket_{\text{hs}} \)) for \( \llbracket_{\text{hexp}} \) (resp. \( \llbracket_{\text{p}} \)). We extend the notation to include the semantics, writing \( \bar{a} \uparrow_p \bar{b} \) to state that \( p \) takes the values \( \bar{a} \) as input and output \( \bar{b} \) using the initial big-step semantics. We write \( \bar{a} \uparrow_p^{\text{SS}} \bar{b} \) when we use the generated semantics of Section 4, without reuse in Section 5.1, and with reuse otherwise. We recall that the inductive interpretation is inherently big-step, as a judgment computes the whole skeleton, so we keep the formal notation \( \uparrow_p^{\text{SS}} \) even for the output semantics. However, the resulting set of rules is created such that its interpretation corresponds to a standard small-step reduction.

### 5.1 Pen-and-paper Proof

As said above, we cover the simplified case where we do not reuse constructors, as proving the analysis of Section 4.1 would make the proof substantially more complex. We would need to justify the correctness of the analysis and that the information is used properly, like in the substitution used in Section 4.3. However, the paper proof applies to both finite and diverging computations.

We prove that a big-step evaluation is possible if and only if a sequence of small-step reductions can lead to the same result up to a \( \text{Ret}_{\text{p}} \) coercion. In the finite case, assuming the terms \( \bar{a} \) and \( \bar{b} \) are written using the initial big-step semantics, we show that for all \( p \)

\[
\bar{a} \uparrow_p \bar{b} \iff \exists \bar{a}', \bar{a} \uparrow_p^{\text{SS}} (\bar{a}', \text{Ret}_{\text{p}}(\bar{b})).
\]

The theorem holds even if the input semantics has an unusual shape. However, it only seems useful if the input follows the big-step paradigm. For instance, if the input is already small-step, then the output would be an odd semantics akin to a malformed abstract machine [4].

For diverging derivations, we define infinite small-step reductions coinductively so that \( \bar{a} \uparrow_p^{\text{SS}} \bar{b} \) and \( \bar{b} \rightarrow_p \infty \) implies \( \bar{a} \rightarrow_p \infty \), and we prove that for all \( p \) and initial terms \( \bar{a} \)

\[
\bar{a} \uparrow_p^{\text{SS}} \iff \bar{a} \rightarrow_p \infty.
\]

### 5.2 Coq Certification Proof Sketch

A complete formalization of the transformation in a proof assistant seems out of reach because of its many steps. Instead, we leverage the Coq generation of Necro, that produces a formalization of an inductive big-step semantics given a skeletal semantics, to automatically generate a formalization of the small and big-step semantics and a proof that they coincide.

Unlike the paper proof, our a-posteriori Coq certification includes constructor reuse, as we only check the resulting semantics without having to justify the analysis phase. The Coq script only covers finite evaluations, however, as Necro only generates inductive semantics and some of our proof techniques do not apply in a coinductive setting.

We explain how to generate the scripts using IMP. The implementation [4] contains the script generator and examples of Coq scripts for other languages. For IMP, the correspondence is stated as follows.

**Theorem 1.** For all \( s, s_0 : \text{state} \), \( e : \text{exp} \), \( t : \text{stm} \), and \( v : \text{value} \),

\[
\begin{align*}
(s, e) \llbracket_{\text{he}} (s_0, v) & \iff (|s|, |e|) \llbracket_{\text{he}} \llbracket_{\text{he}} (|s_0|, |v|) \\
(s, t) \llbracket_{\text{hs}} s_0 & \iff (|s|, |t|) \llbracket_{\text{hs}} |s_0|.
\end{align*}
\]

The interesting direction is to show that a sequence of small-step reductions implies a big-step evaluation. We use a concatenation lemma [18, 24], stating that we can merge a small step into a big step:

\[
e \uparrow_p e \uparrow_p^{\text{BS}} v \iff e \uparrow_p^{\text{BS}} v
\]

Such a result can be stated independently from the semantics, so it is easier to formalize. Its downside is that the big-step and small-step semantics need to be defined on the same constructors. The big-step semantics is not defined on the newly created constructors, such as \( \text{While1} \) and \( \text{While2} \). To bridge the gap between the initial big-step (BS) and the small-step (SS) semantics, we consider an extended big-step (EBS) semantics defined on all constructors. It corresponds to the situation before the last phase of the transformation (between Sections 4.2 and 4.3), with additional rules to extract values coerced by the new \( \text{Ret}_{\text{p}} \) constructors: \( p(\overline{y}, \text{Ret}_{\text{p}}(\overline{p})) := \text{Return} \overline{a} \mid p \in P_0 \) — we remind that \( P_0 \) is the initial set of user-defined procedures. These last n4w rules allow for judgments of the form \( (\bar{a}, \text{Ret}_{\text{p}}(\bar{b})) \uparrow_p^{\text{EBS}} \bar{b} \).

Given an input BS semantics, our tool generates the EBS and SS semantics. The EBS and SS semantics are defined on extended terms that we prefix with a letter \( e \), writing for instance e-state for extended states. The EBS generated for IMP can be found in Appendix A.5. The three semantics are transformed into Coq definitions using the export function of Necro. Necro also provides a Coq definition of the inductive interpretation (Figure 2), which itself depends on interpretations for the base types and filters. Our proof script takes as global parameters such interpretations for the initial BS, which are carried to the other two semantics through coercions. This way, the certification is independent from the behavior and implementation of these base elements.

The strategy is to show that BS and EBS are equivalent on initial terms, and then prove that EBS is equivalent to SS on all terms (including the extended ones). In the end, we get that BS is equivalent to SS on initial terms. The first step is easy to verify since EBS is a conservative extension of BS: we simply match every behavior—every applied rule—in big-step with exactly the same one on the other side.

We note \( |t| \) the canonical injection of an initial term \( t \) into the extended semantics, e.g., from type \( \text{stm} \) to \( \text{estm} \).

**Theorem 2 (BS \( \Rightarrow \) EBS).** For all \( (s, s_0 : \text{state}), (e : \text{exp}), (t : \text{stm}), \) and \( (v : \text{value}) \),

\[
\begin{align*}
(s, e) \llbracket_{\text{he}} (s_0, v) & \Rightarrow (|s|, |e|) \llbracket_{\text{he}} \llbracket_{\text{he}} (|s_0|, |v|) \\
(s, t) \llbracket_{\text{hs}} s_0 & \Rightarrow (|s|, |t|) \llbracket_{\text{hs}} |s_0|.
\end{align*}
\]
As hinted above, we rely on a concatenation lemma. (Extended big-step results come for free if the reduction is written using small-step semantics.) Given by the lemmas to apply, but at least the intermediary configurations are given by generating congruence results about the small-step reduction. It would require Coq to guess the intermediate configurations, such as which we want to show.

Theorem 3 (EBS⇒BS). For all (s : state), (e : exp), (t : stm), (s₀' : estate), and (e₀' : evaluate),

\((s₀, e₀') \Downarrow_{\text{BS}} \Rightarrow \exists s₀, v, (s₀', e₀') = ((s₀, |v|) \land (s, e) \Downarrow_{\text{BS}} s₀)\)

\((s, t) \Downarrow_{\text{BS}} s₀' \Rightarrow \exists s₀, s₀' = |s₀| \land (s, t) \Downarrow_{\text{BS}} s₀\)

5.3 Small-Step Implies Extended Big-Step

As hinted above, we rely on a concatenation lemma.

Lemma 4 (Concatenation). For all s, s', s₀, e, e', t, t', and v,

\((s, e) \Downarrow_{\text{SS}} (s', e') \Downarrow_{\text{EBS}} (s₀, v) \Rightarrow (s, e) \Downarrow_{\text{SS}} (s₀, v)\)

\((s, t) \Downarrow_{\text{SS}} (s', t') \Downarrow_{\text{EBS}} (s₀, v) \Rightarrow (s, t) \Downarrow_{\text{SS}} (s₀, v)\)

It is a local result, as it considers small steps one at a time, making it easier to prove automatically. Indeed, the proof is done by induction on the small step; in each case, we also decompose the big-step hypothesis which generates numerous subcases. Fortunately, elementary tactics are sufficient for Coq to automatically reconstruct the extended big step in all cases: it is a simple case analysis to find the big-step hypothesis whose source coincides with the conclusion of the small-step induction hypothesis.

Using the concatenation lemma, a simple induction on the reflexive and transitive closure gives us the desired results:

Theorem 5 (SS⇒EBS). For all s, s', s₀, e, t, and v,

\((s, e) \Downarrow_{\text{SS}} (s', e') \Downarrow_{\text{EBS}} (s₀, v) \Rightarrow (s, e) \Downarrow_{\text{SS}} (s₀, v)\)

\((s, t) \Downarrow_{\text{SS}} (s', t') \Downarrow_{\text{EBS}} (s₀, v) \Rightarrow (s, t) \Downarrow_{\text{SS}} (s₀, v)\)

5.4 Extended Big-Step Implies Small-Step

For the sake of readability, we illustrate this section with a Plus example without states. We also write Ret for Retₜₜₑ and \(\Rightarrow\) for the interpretation of the small-step semantics.

We prove that big-step implies small-step on extended terms by induction on the derivation of the big-step evaluation. In each case, we need to build a complete sequence of small steps from the partial sequences we get from using the induction hypothesis. For instance, decomposing the evaluation \(\text{Plus}(e₁, e₂) \Downarrow_{\text{EBS}} v\) produces the hypotheses \(e₁ \Rightarrow∗ \text{Ret}(v₁), e₂ \Rightarrow∗ \text{Ret}(v₂),\) and \(v = v₁ + v₂,\) from which we want to show \(\text{Plus}(e₁, e₂) \Rightarrow∗ \text{Ret}(v)\).

We could try a brute-force search as in the previous section, but it would require Coq to guess the intermediate configurations, such as \(\text{Plus}(e₁', e₂)\) if \(e₁ \Rightarrow e₁' \Rightarrow∗ \text{Ret}(v₁)\). It works on small languages like IMP, but not for larger ones like miniML. Instead, we help by generating congruence results about the small-step reduction. We still need Coq to automatically find the right combination of lemmas to apply, but at least the intermediary configurations are given by the lemmas. For Plus, we need results of the form:

\(e₁ \Rightarrow e₁' \Rightarrow∗ \text{Plus}(e₁, e₂) \Rightarrow∗ \text{Plus}(e₁', e₂)\)

\(e₂ \Rightarrow e₂' \Rightarrow∗ \text{Plus}(\text{Ret}(v₁), e₂) \Rightarrow∗ \text{Plus}(\text{Ret}(v₁), e₂')\)

\(v = v₁ + v₂ \Rightarrow \text{Plus}(\text{Ret}(v₁), \text{Ret}(v₂)) \Rightarrow∗ \text{Ret}(v)\)

Combining these, we obtain the desired result. Such congruence results come for free if the reduction is written using small-step inference rules. In our case, we have to derive them from the skeletons; it is the only part of the proof script which really depends on the semantics of the language.

Each generated lemma corresponds to a path in a small-step rule: for instance, the three inference rules describing the behavior of the skeleton for Plus in Example 6 corresponds to the three results above (with states). For each path, the LetIns definitions of the skeleton contain the hypothesis of the lemma, while the final result is the configuration to step towards. The generated lemmas are automatically proved either by unfolding the definitions or doing a straightforward induction; each proof is simple since the structure of the lemma matches a path of the skeleton.

With these results, the proof of the main theorem is simply done by induction on the extended big step. In each case, we apply the induction hypothesis on every big-step premise, which gives us several small-step sequences on sub-computations. Then, the congruence lemmas are automatically applied and the results merged together by Coq to create the wanted small-step sequence.

Theorem 6 (EBS⇒SS). For all s, s₀, e, t, and v,

\((s, e) \Downarrow_{\text{BS}} (s₀, v) \Rightarrow ∃ s', (s, e) \Downarrow_{\text{SS}} (s', \text{Retₜₜₑ}(s₀, v))\)

\((s, t) \Downarrow_{\text{BS}} s₀ \Rightarrow ∃ s', (s, t) \Downarrow_{\text{SS}} (s', \text{Retₜₜₑ}(s₀))\)

6 EVALUATION

We compare the size of the generated small-step semantics and equivalence proof scripts for various languages in Table 1. In the constructors columns, BS, SS, and NR contain the number of constructors respectively in the input, output (not counting the constructors coerced values into terms), and in the output without reuse.

The examples include variants of the call-by-value (CBV) and call-by-name (CBN) λ-calculus implemented with closures, evaluated in an environment mapping variables to closures; CBV has also been extended with non-determinism and exceptions. The examples written in an imperative style include a small arithmetic language, extensions of IMP with local (IMP, LetIn) or global (IMP, write) state modification, and with exceptions and handlers (IMP, try/catch). Lastly, miniML is an ML-like language, extending the λ-calculus with arithmetic and boolean operations, and constructs...
to define and handle algebraic datatypes. The generated small-step semantics and proofs for the examples can be found in the implementation [4].

In the certification, about 500 lines of code are completely independent of the input language and contain definitions of skeletons or of the inductive interpretation. About 450 lines of code are templates which are filled with basic information about the syntax of the input semantics (the names of the procedures, constructors, and filters): these are general definitions, results, and tactics to manipulate the inductive interpretation. They are part of the generated proof script, but are not counted in Table 1, where we lists the sizes of the language-dependent parts of the proof. The size of these parts is linear in the size of the small-step semantics. Indeed, it is composed mostly of the generated lemmas of the EBS implies SS part of the proof, which themselves mirror the different paths in the small-step rules (see Section 5.4).

W.r.t. constructors, we see the impact of constructor reuse especially in the IMP case, where we go from two new constructors with reuse to ten new constructors without reuse.

The generated semantics diverge from the ones written by hand when they duplicate the environment variables in the new constructors, like the state for IMP (Section 2.3). Duplication occurs in coercions such as Ret_hexp to make the small steps uniform, with the same input and output types. For new constructors like While1e1, or While1e2, it seems to be the price to pay for a systematic transformation, as it occurs in Vesely and Fisher’s work [27, Section 7], but also when writing pretty-big step semantics [6, Section 5.2]. An extra analysis could detect that the state can be removed from While1e1 or While1e2, but it is not clear that such an optimization is possible in general. Besides, it would prevent other static analyses, such as detecting read-only states.

7 RELATED WORK

Our work uses skeletal semantics to benefit from the simplicity of its foundations. The K framework [25] is noticeably more complex and does not provide a translation into Coq. Other semantic tools, such as Lem [20] and Ott [26], are not equipped for the direct manipulation of semantics—they do not give access to a meta-language. Here, the small meta-language allows for a simple transformation, at the cost of harder definitions of some advanced language features.

While several approaches go from a small-step to a big-step setting by manipulating either inference rules [7, 23] or interpreters [11, 12], the other direction has been less pursued.

Vesely and Fisher [27] propose an automatic transformation from a big-step to a small-step interpreter. The input interpreter contains functions for small operations (e.g., updating a state) and a single evaluation function eval. Roughly, the transformation starts with a partial CPS-transform of eval to turn recursive calls into continuations, considered as newly created terms. After making eval a stepping function, it ends with an inverse CPS-transform recreating a small-step interpreter. As in our work, creating a new constructor for every continuation would be correct but the authors aim for an output closer to a semantics written by hand. For this, they substitute continuations that can be expressed as initial terms in order to simplify the resulting interpreter.

Vesely and Fisher’s approach only considers subcomputations as reduction steps, as they transform only eval calls—similar to proc calls in our case—and ignore other simple functions calls—filter calls—or focus changes. The input interpreter, defined in an ad-hoc language, may not be as expressive as skeletal semantics, in particular because only one evaluation function is possible. It is not clear whether the approach scales to several mutually recursive functions.

An important difference is that their resulting small-step function only recreates a term and not a configuration. This systematically leads to a new constructor C packing a state and a term. It is not necessarily less efficient than our approach, as they do not need new constructors when only state variables are reused. For instance, to reduce a \( \lambda \)-calculus term \( \text{App}(t_1, t_2) \) with a sub-reduction \( s, t_1 \rightarrow s', t'_1 \), we would reconstruct a configuration as \( s, \text{App}(t_1, t_2) \rightarrow s, \text{App}(s', t'_1, t_2) \) while they would reconstruct a term as \( s \triangleright \text{App}(t_1, t_2) \rightarrow \text{App}(C(s'), t_1' \backslash t_2) \). As a result, it is difficult to compare the outputs of the two approaches based on the number of additional constructors or rules, but the output semantics are very close to usual small-step definitions, with a minimal number of created constructors in both cases.

Finally, Vesely and Fisher [27] claim to have informal proofs of several parts of their transformation. We have a language-independent proof of the transformation without initial constructors reuse for terminating and diverging evaluations. With reuse, we generate an equivalence proof script for terminating evaluations for any input semantics.

Huizing et al. [13] present a transformation from a big-step to a small-step semantics, by directly manipulating inference rules. Small-step configurations are extended with a stack to keep track of the big-step premises that have already been computed. For each non-axiom big-step rule, they create several terms to indicate which premise is under evaluation, and a multitude of small-step rules to either initiate/conclude the big-step rule, change the premise under consideration, or reduce it. Rules for focusing on a new premise also guess an input state for the subcomputation; coherence is only checked when concluding the big-step rule. Guessing intermediate states, and delaying the unification until the end of the corresponding big-step rule, make the transformation very generic and interesting for languages with complicated control flow. However, the large number of small-step rules and new terms as well as the stack make the resulting semantics very different from usual SOS definitions.

The functional correspondence [2] is a systematic approach to transform a big-step interpreter into an abstract machine. Compared to a small-step SOS, an abstract machine is closer to an implementation. In particular, it usually does not reconstruct the whole term after reducing a redex. In a recent paper [3], we use the functional correspondence to derive an abstract machine for the skeletal semantics meta-language of Section 3, thus providing an executable interpretation of skeletons. The resulting machine is proven sound w.r.t. concrete interpretation using Coq. Unlike the present work, where we transform directly user-defined languages, our previous work stays at the meta-level: the abstract machine is derived once and for all, and it manipulates skeletons. Even when instantiated with a user-defined language, the resulting machine is very difficult to read and far from an efficient abstract
We present a fully automatic transformation from a big-step to a small-step skeletal semantics with or without reuse of the initial constructors. With reuse, we generate new constructors only for problematic program points. The resulting small-step skeletal semantics can then be given to Necro to generate OCaml interpreters or Coq formalizations. We exploit the latter feature to automatically and a-posteriori certify the correctness of the result of the transformation with reuse on any language for terminating evaluations. The transformation without reuse is proved to be correct independently from the input language in the terminating and diverging cases. The transformations and the proofs make no assumptions about filters, and the filters defined for the big-step input are used by the small-step outputs up to coercions. Our work remains parametric in the implementation of filters, in the spirit of skeletal semantics. Experimenting our method with several languages shows the transformation with reuse produces small-step skeletal semantics close to the SOS ones that one would write by hand.

REFERENCES

APPENDICES

Appendix A contains the successive skeletal semantics of the language IMP at each phase of transformation, including the final semantics with and without constructor reuse. The only modification we made to the generated files is a renaming of the generated names to ease the reading.

Appendix B gives more details on the transformation phases of Section 4. Notably, it contains definitions skipped in the paper, and notations used in the following proof.

Appendix C contains a pen-and-paper proof of the small-step transformation presented in the accompanying paper. We only certify the base transformation, without reuse of constructors or tail-calls. We do not certify the analysis, whose main purpose is to optimize the reuse of constructors, and assume initial proc calls are all annotated with fresh constructor names (New c).

A SUCCESSIVE TRANSFORMATIONS OF IMP

A.1 Initial IMP Skeletal Semantics

type int

| type bool
| type ident
| type state
| type value

type expr =
| Not of expr
| Bconst of bool
| Equal of expr * expr
| Iconst of int
| Plus of expr * expr
| Var of ident

type stmt =
| Assign of ident * expr
| If of expr * stmt * stmt
| Seq of stmt * stmt
| Skip
| While of expr * stmt

val add : value * value -> value
val boolToVal : bool -> value
val eq : value * value -> value
val intToVal : int -> value
val isFalse : value -> unit
val isTrue : value -> unit
val neg : value -> value
val read : ident * state -> value
val write : ident * state * value -> state

hook hexpr (s : state, e : expr) matching e : state * value =
| Iconst (i) ->
  let v = intToVal (i) in
  (s, v)
| Bconst (b) ->
  let v = boolToVal (b) in
  (s, v)
| Var (x) ->
  let v = read (x, s) in
  (s, v)
| Plus (e1, e2) ->
  let (s1, v1) = hexpr (s, e1) in
  let (s2, v2) = hexpr (s1, e2) in
  let v = add (v1, v2) in


\[(s2, v)\]
<table>
<thead>
<tr>
<th>\textbf{Equal} ((e1, e2))</th>
<th>\textbf{Not} ((e1))</th>
</tr>
</thead>
<tbody>
<tr>
<td>\textbf{let} ((s1, v1) = \text{hexpr} (s, e1)) \textbf{in} \textbf{let} ((s2, v2) = \text{hexpr} (s1, e2)) \textbf{in} \textbf{let} (v = \text{eq} (v1, v2)) \textbf{in} (\textbf{(s2, v)})</td>
<td>\textbf{let} ((s1, v) = \text{hexpr} (s, e1)) \textbf{in} \textbf{let} (v1 = \text{neg} (v)) \textbf{in} (\textbf{(s1, v1)})</td>
</tr>
</tbody>
</table>

\[
\text{hook} \ hstmt \ (s : \text{state}, t : \text{stmt}) \text{ matching } t : \text{state} = \\
\text{Skip => } s \\
\text{Assign} \ (x, e) => \\
\text{let} \ (s1, v) = \text{hexpr} (s, e) \textbf{in} \text{write} (x, s1, v) \\
\text{Seq} \ (t1, t2) => \\
\text{let} \ s1 = \text{hstmt} (s, t1) \textbf{in} \text{hstmt} (s1, t2) \\
\text{If} \ (e1, t2, t3) => \\
\text{let} \ (s1, v) = \text{hexpr} (s, e1) \textbf{in} \text{branch} \\
\text{let} () = \text{isTrue} (v) \textbf{in} \text{hstmt} (s1, t2) \\
\text{or} \\
\text{let} () = \text{isFalse} (v) \textbf{in} \text{hstmt} (s1, t3) \textbf{end} \\
\text{While} \ (e1, t2) => \\
\text{let} \ (s1, v) = \text{hexpr} (s, e1) \textbf{in} \text{branch} \\
\text{let} () = \text{isTrue} (v) \textbf{in} \\
\text{let} \ s2 = \text{hstmt} (s1, t2) \textbf{in} \text{hstmt} (s2, \text{While} \ (e1, t2)) \\
\text{or} \\
\text{let} () = \text{isFalse} (v) \textbf{in} \ s1 \textbf{end} \\

\textbf{A.2 After Adding Coercions}\n
In the implementation, the new constructors and procedures for coercions are created first. Since it is independent from the rest of the transformation, it could be done at any point. It is only presented last in Section 4.3 to facilitate the reading.

\[
\text{type} \ \text{int} \\
\text{type} \ \text{bool} \\
\text{type} \ \text{ident} \\
\text{type} \ \text{state} \\
\text{type} \ \text{value} \\
\text{type} \ \text{expr} = \\
\text{Not} \ \text{of} \ \text{expr} \\
\text{Bconst} \ \text{of} \ \text{bool} \\
\text{Equal} \ \text{of} \ \text{expr} \times \ \text{expr} \\
\text{Iconst} \ \text{of} \ \text{int} \\
\text{Plus} \ \text{of} \ \text{expr} \times \ \text{expr} \\
\text{Var} \ \text{of} \ \text{ident} \\
\text{Ret\_hexpr} \ \text{of} \ \text{state} \times \ \text{value}
\]
type stmt =
| Assign of ident * expr
| If of expr * stmt * stmt
| Seq of stmt * stmt
| Skip
| While of expr * stmt
| Ret_hstmt of state

val add : value * value -> value
val boolToVal : bool -> value
val eq : value * value -> value
val intToVal : int -> value
val isFalse : value -> unit
val isTrue : value -> unit
val neg : value -> value
val read : ident * state -> value
val write : ident * state * value -> state

hook getRet_hexpr (e : expr) matching e : state * value =
| Ret_hexpr (v1, v2) ->
  (v1, v2)

hook getRet_hstmt (t : stmt) matching t : state =
| Ret_hstmt v1 ->
  v1

hook hexpr (s : state, e : expr) matching e : state * value =
| Not e1 ->
  let (s1, v) = hexpr (s, e1) in
  let v1 = neg (v) in
  (s1, v1)
| Bconst b ->
  let v = boolToVal (b) in
  (s, v)
| Equal (e1, e2) ->
  let (s1, v1) = hexpr (s, e1) in
  let (s2, v2) = hexpr (s1, e2) in
  let v = eq (v1, v2) in
  (s2, v)
| Iconst i ->
  let v = intToVal (i) in
  (s, v)
| Plus (e1, e2) ->
  let (s1, v1) = hexpr (s, e1) in
  let (s2, v2) = hexpr (s1, e2) in
  let v = add (v1, v2) in
  (s2, v)
| Var x ->
  let v = read (x, s) in
  (s, v)

hook hstmt (s : state, t : stmt) matching t : state =
| Assign (x, e) ->
  let (s1, v) = hexpr (s, e) in
  write (x, s1, v)
| If (e1, t2, t3) ->
  let (s1, v) = hexpr (s, e1) in
branch
  let () = isTrue (v) in
  hstmt (s1, t2)
or
  let () = isFalse (v) in
  hstmt (s1, t3)
end
| Seq (t1, t2) ->
  let s1 = hstmt (s, t1) in
  hstmt (s1, t2)
| Skip ->
  s
| While (e1, t2) ->
  let (s1, v) = hexpr (s, e1) in
  branch
    let () = isTrue (v) in
    let s2 = hstmt (s1, t2) in
    hstmt (s2, (While (e1, t2)))
  or
    let () = isFalse (v) in
    s1
de

A.3 After Creating New Constructors

type int

type bool

type ident

type state

type value

type expr =
  | Not of expr
  | Bconst of bool
  | Equal of expr * expr
  | Iconst of int
  | Plus of expr * expr
  | Var of ident
  | Ret_hexpr of state * value

type stmt =
  | Assign of ident * expr
  | If of expr * stmt * stmt
  | Seq of stmt * stmt
  | Skip
  | While of expr * stmt
  | While1 of state * expr * expr * stmt
  | While2 of state * stmt * expr * stmt
  | Ret_hstmt of state

val add : value * value -> value
val boolToVal : bool -> value
val eq : value * value -> value
val intToVal : int -> value
val isFalse : value -> unit
val isTrue : value -> unit
val neg : value -> value
val read : ident * state -> value
val write : ident * state * value -> state

hook getRet_expr (e : expr) matching e : state * value =
  | Ret_expr (v1, v2) ->
    (v1, v2)

hook getRet_hstmt (t : stmt) matching t : state =
  | Ret_hstmt v1 ->
    v1

hook hexpr (s : state, e : expr) matching e : state * value =
  | Not e1 ->
    let (s1, v) = hexpr (s, e1) in (* reuse *)
    let v1 = neg (v) in
    (s1, v1)
  | Bconst b ->
    let v = boolToVal (b) in
    (s, v)
  | Equal (e1, e2) ->
    let (s1, v1) = hexpr (s, e1) in (* reuse *)
    let (s2, v2) = hexpr (s1, e2) in (* reuse *)
    let v = eq (v1, v2) in
    (s2, v)
  | Iconst i ->
    let v = intToVal (i) in
    (s, v)
  | Plus (e1, e2) ->
    let (s1, v1) = hexpr (s, e1) in (* reuse *)
    let (s2, v2) = hexpr (s1, e2) in (* reuse *)
    let v = add (v1, v2) in
    (s2, v)
  | Var x ->
    let v = read (x, s) in
    (s, v)

hook hstmt (s : state, t : stmt) matching t : state =
  | Assign (x, e) ->
    let (s1, v) = hexpr (s, e) in (* reuse *)
    write (x, s1, v)
  | If (e1, t2, t3) ->
    let (s1, v) = hexpr (s, e1) in (* reuse *)
    branch
      let () = isTrue (v) in
      hstmt (s1, t2) (* tail-call *)
    or
      let () = isFalse (v) in
      hstmt (s1, t3) (* tail-call *)
  end
  | Seq (t1, t2) ->
    let s1 = hstmt (s, t1) in (* reuse *)
    hstmt (s1, t2) (* tail-call *)
  | Skip ->
    s
  | While (e1, t2) ->
    let (s1, v) = hexpr (s, e1) in (* new constr: While1 *)
    branch
      let () = isTrue (v) in


let s2 = hstmt (s1, t2) in (* new constr: While2 *)
  hstmt (s2, (While (e1, t2))) (* tail-call *)
or let () = isFalse (v) in
  s1
end |
While1 (s0, e0, e1, t2) ->
  let (s1, v) = hexpr (s0, e0) in (* reuse *)
  branch
    let () = isTrue (v) in
    let s2 = hstmt (s1, t2) in (* new constr: While2 *)
      hstmt (s2, (While (e1, t2))) (* tail-call *)
or let () = isFalse (v) in
  s1
end |
While2 (s0, t0, e1, t2) ->
  let s2 = hstmt (s0, t0) in (* reuse *)
  hstmt (s2, (While (e1, t2))) (* tail-call *)

A.4 Final Small-Step Skeletal Semantics

type int

type bool

type ident

type state

type value

type expr =
  | Bconst of bool
  | Equal of expr * expr
  | Iconst of int
  | Not of expr
  | Plus of expr * expr
  | Var of ident
  | Ret_hexpr of state * value

type stmt =
  | Assign of ident * expr
  | If of expr * stmt * stmt
  | Seq of stmt * stmt
  | Skip
  | While of expr * stmt
  | While1 of state * expr * expr * stmt
  | While2 of state * stmt * expr * stmt
  | Ret_hstmt of state

val add : value * value -> value
val boolToVal : bool -> value
val eq : value * value -> value
val intToVal : int -> value
val isFalse : value -> unit
val isTrue : value -> unit
val neg : value -> value
val read : ident * state -> value
val write : ident * state * value -> state
hook getRet_hexpr (e : expr) matching e : state * value =
  | Ret_hexpr (v1, v2) -> (v1, v2)

hook getRet_hstmt (t : stmt) matching t : state =
  | Ret_hstmt v1 -> v1

hook hexpr (s : state, e : expr) matching e : state * expr =
  | Bconst b ->
    let v = boolToVal (b) in
    (s, Ret_hexpr (s, v))
  | Equal (e1, e2) ->
    branch
    let (z1, z2) = hexpr (s, e1) in
    (z1, Equal (z2, e2))
    or
    let (s1, v1) = getRet_hexpr (e1) in
    branch
    let (z3, z4) = hexpr (s1, e2) in
    (s1, Equal (Ret_hexpr (z3, v1), z4))
    or
    let (s2, v2) = getRet_hexpr (e2) in
    let v = eq (v1, v2) in
    (s, Ret_hexpr (s2, v))
  end

end

| Iconst i ->
  let v = intToVal (i) in
  (s, Ret_hexpr (s, v))

| Not e1 ->
  branch
  let (z1, z2) = hexpr (s, e1) in
  (z1, Not z2)
  or
  let (s1, v) = getRet_hexpr (e1) in
  let v1 = neg (v) in
  (s, Ret_hexpr (s1, v1))
end

| Plus (e1, e2) ->
  branch
  let (z1, z2) = hexpr (s, e1) in
  (z1, Plus (z2, e2))
  or
  let (s1, v1) = getRet_hexpr (e1) in
  branch
  let (z3, z4) = hexpr (s1, e2) in
  (s1, Equal (Ret_hexpr (z3, v1), z4))
  or
  let (s2, v2) = getRet_hexpr (e2) in
  let v = add (v1, v2) in
  (s, Ret_hexpr (s2, v))
end

end

| Var x ->
  let v = read (x, s) in
  (s, Ret_hexpr (s, v))
hook hstmt (s : state, t : stmt) matching t : state * stmt = 
  | Assign (x, e) ->
  |   branch
  |     let (z1, z2) = hexpr (s, e) in (z1, Assign (x, z2))
  | or
  |     let (s1, v) = getRet_hexpr (e) in
  |     let z3 = write (x, s1, v) in
  |     (s, Ret_hstmt z3)
  |
  | If (e1, t2, t3) ->
  |   branch
  |     let (z1, z2) = hexpr (s, e1) in (z1, If (z2, t2, t3))
  | or
  |     let (s1, v) = getRet_hexpr (e1) in
  |     branch
  |       let () = isTrue (v) in (s1, t2)
  | or
  |       let () = isFalse (v) in (s1, t3)
  |
  | Seq (t1, t2) ->
  |   branch
  |     let (z1, z2) = hstmt (s, t1) in (z1, Seq (z2, t2))
  | or
  |     let s1 = getRet_hstmt (t1) in
  |     (s1, t2)
  |
  | Skip ->
  | (s, Ret_hstmt s)

| While (e1, t2) ->
| (s, (While1 (s, e1, e1, e1, t2)))
| While1 (s0, e0, e1, e1, t2) ->
| branch
| let (z1, z2) = hexpr (s0, e0) in
| (s, While1 (z1, z2, e1, t2))
| or
| let (s1, v) = getRet_hexpr (e0) in
| branch
| let () = isTrue (v) in
| (s, (While2 (s1, t2, e1, t2)))
| or
| let () = isFalse (v) in
| (s, Ret_hstmt s1)
|
| While2 (s0, t0, e1, t2) ->
| branch
| let (z1, z2) = hstmt (s0, t0) in
| (s, While2 (z1, z2, e1, t2))
| or
| let s2 = getRet_hstmt (t0) in
| (s2, (While (e1, t2)))
|
A.5  Extended Big-Step for Coq Certification

type int

type bool

type ident

type state

type value

type expr =
| Not of expr
| Bconst of bool
| Equal of expr * expr
| Iconst of int
| Plus of expr * expr
| Var of ident
| Ret_hexpr of state * value

type stmt =
| Assign of ident * expr
| If of expr * stmt * stmt
| Seq of stmt * stmt
| Skip
| While of expr * stmt
| While1 of state * expr * expr * stmt
| While2 of state * stmt * expr * stmt
| Ret_hstmt of state

val add : value * value -> value
val boolToVal : bool -> value
val eq : value * value -> value
val intToVal : int -> value
val isFalse : value -> unit
val isTrue : value -> unit
val neg : value -> value
val read : ident * state -> value
val write : ident * state * value -> state

hook hexpr (s : state, e : expr) matching e : state * value =
| Not e1 ->
  let (s1, v) = hexpr (s, e1) in
  let v1 = neg (v) in
  (s1, v1)
| Bconst b ->
  let v = boolToVal (b) in
  (s, v)
| Equal (e1, e2) ->
  let (s1, v1) = hexpr (s, e1) in
  let (s2, v2) = hexpr (s1, e2) in
  let v = eq (v1, v2) in
  (s2, v)
| Iconst i ->
  let v = intToVal (i) in
  (s, v)
| Plus (e1, e2) ->
  let (s1, v1) = hexpr (s, e1) in
  let (s2, v2) = hexpr (s1, e2) in
  let v = add (v1, v2) in
  (s2, v)
A.6 Resulting Small-Step without Reuse

type int
type bool
type ident
type state
type value
type expr =
  | Not of expr
  | Not1 of state * expr
  | Bconst of bool
  | Equal of expr * expr
  | Equal1 of state * expr * expr
  | Equal2 of state * expr * value
  | Iconst of int
  | Plus of expr * expr
  | Plus1 of state * expr * expr
  | Plus2 of state * expr * value
  | Var of ident
  | Ret_hexpr of state * value

type stmt =
  | Assign of ident * expr
  | Assign1 of state * expr * ident
  | If of expr * stmt * stmt
  | If1 of state * expr * stmt * stmt
  | Seq of stmt * stmt
  | Seq1 of state * stmt * stmt
  | Skip
  | While of expr * stmt
  | While1 of state * expr * expr * stmt
  | While2 of state * stmt * expr * stmt
  | Ret_hstmt of state

val add : value * value -> value
val boolToVal : bool -> value
val eq : value * value -> value
val intToVal : int -> value
val isFalse : value -> unit
val isTrue : value -> unit
val neg : value -> value
val read : ident * state -> value
val write : ident * state * value -> state

hook getRet_hexpr (e : expr) matching e : state * value =
  | Ret_hexpr (v1, v2) -> (v1, v2)

hook getRet_hstmt (t : stmt) matching t : state =
  | Ret_hstmt v1 -> v1

hook hexpr (s : state, e : expr) matching e : state * expr =
  | Not e1 ->
    (s, Not1 (s, e1))
  | Not1 (s0, e0) ->
    branch
    let (z1, z2) = hexpr (s0, e0) in
    (s, Not1 (z1, z2))
  | or
    let (s1, v) = getRet_hexpr (e0) in
    let v1 = neg (v) in
    (s, Ret_hexpr (s1, v1))
  | Bconst b ->
    let v = boolToVal (b) in
    (s, Ret_hexpr (s, v))
Certified Derivation of Small-Step From Big-Step Skeletal Semantics

| Equal (e1, e2) -> (s, Equal1 (s, e1, e2)) |
| Equal1 (s0, e0, e2) -> |
| branch |
| let (z1, z2) = hexpr (s0, e0) in (s, Equal1 (z1, z2, e2)) |
| or let (s1, v1) = getRet_hexpr (e0) in (s, Equal2 (s1, e2, v1)) |
| end |
| Equal2 (s0, e0, v1) -> |
| branch |
| let (z1, z2) = hexpr (s0, e0) in (s, Equal2 (z1, z2, v1)) |
| or let (s2, v2) = getRet_hexpr (e0) in let v = eq (v1, v2) in (s, Ret_hexpr (s2, v)) |
| end |
| Iconst i -> let v = intToVal (i) in (s, Ret_hexpr (s, v)) |
| Plus (e1, e2) -> (s, Plus1 (s, e1, e2)) |
| Plus1 (s0, e0, e2) -> |
| branch |
| let (z1, z2) = hexpr (s0, e0) in (s, Plus1 (z1, z2, e2)) |
| or let (s1, v1) = getRet_hexpr (e0) in let v = add (v1, v2) in (s, Ret_hexpr (s2, v)) |
| end |
| Plus2 (s0, e0, v1) -> |
| branch |
| let (z1, z2) = hexpr (s0, e0) in (s, Plus2 (z1, z2, v1)) |
| or let (s2, v2) = getRet_hexpr (e0) in let v = add (v1, v2) in (s, Ret_hexpr (s2, v)) |
| end |
| Var x -> let v = read (x, s) in (s, Ret_hexpr (s, v)) |

hook hstmt (s : state, t : stmt) matching t : state * stmt =
| Assign (x, e) -> (s, Assign1 (s, e, x)) |
| Assign1 (s0, e0, x) -> |
| branch |
| let (z1, z2) = hexpr (s0, e0) in (s, Assign1 (z1, z2, x)) |
| or let (s1, v) = getRet_hexpr (e0) in let z3 = write (x, s1, v) in (s, Ret_hstmt z3) |
| end |
\begin{align*}
\text{If} & (e_1, t_2, t_3) \rightarrow \\
(s, \text{If1} (s, e_1, t_2, t_3)) \\
\text{If1} (s_0, e_0, t_2, t_3) \rightarrow & \\
\text{branch} & \\
\text{let} (z_1, z_2) = \text{hexpr} (s, e_0) \text{ in} & \\
(s, \text{If1} (z_1, z_2, t_2, t_3)) \\
or & \\
\text{let} (s_1, v) = \text{getRet_hexpr} (e_0) \text{ in} & \\
\text{branch} & \\
\text{let } () = \text{isTrue} (v) \text{ in} & \\
(s_1, t_2) \\
or & \\
\text{let } () = \text{isFalse} (v) \text{ in} & \\
(s_1, t_3) \\
\end{align*}

\begin{align*}
\text{Seq} (t_1, t_2) \rightarrow & \\
(s, \text{Seq1} (s, t_1, t_2)) \\
\text{Seq1} (s_0, t_0, t_2) \rightarrow & \\
\text{branch} & \\
\text{let} (z_1, z_2) = \text{hstmt} (s_0, t_0) \text{ in} & \\
(s, \text{Seq1} (z_1, z_2, t_2)) \\
or & \\
\text{let } s_1 = \text{getRet_hstmt} (t_0) \text{ in} & \\
(s_1, t_2) \\
\end{align*}

\begin{align*}
\text{Skip} \rightarrow & \\
(s, \text{Ret_hstmt} s) \\
\text{While} (e_1, t_2) \rightarrow & \\
(s, \text{While1} (s, e_1, e_1, t_2)) \\
\text{While1} (s_0, e_0, e_1, t_2) \rightarrow & \\
\text{branch} & \\
\text{let} (z_1, z_2) = \text{hexpr} (s_0, e_0) \text{ in} & \\
(s, \text{While1} (z_1, z_2, e_1, t_2)) \\
or & \\
\text{let} (s_1, v) = \text{getRet_hexpr} (e_0) \text{ in} & \\
\text{branch} & \\
\text{let } () = \text{isTrue} (v) \text{ in} & \\
(s, \text{While2} (s_1, t_2, e_1, t_2)) \\
or & \\
\text{let } () = \text{isFalse} (v) \text{ in} & \\
(s, \text{Ret_hstmt} s_1) \\
\end{align*}

\begin{align*}
\text{While2} (s_0, t_0, e_1, t_2) \rightarrow & \\
\text{branch} & \\
\text{let} (z_1, z_2) = \text{hstmt} (s_0, t_0) \text{ in} & \\
(s, \text{While2} (z_1, z_2, e_1, t_2)) \\
or & \\
\text{let } s_2 = \text{getRet_hstmt} (t_0) \text{ in} & \\
(s_2, \text{While} (e_1, t_2)) \\
\end{align*}
\[ \text{Branch}(S_1, \ldots, S_n)_L^r \doteq \text{Branch}([S_1]_L^r, \ldots, [S_n]_L^r) \]
\[ \text{Filter } f \overline{t}^r_L \doteq \text{Filter } f \overline{t} \]
\[ \text{Return } \overline{t}^r_L \doteq \text{Return } \overline{t} \]
\[ \text{Proc } \overline{t}^r_L \doteq \text{Proc Tail } p \overline{t} \quad \text{if } L = \top, pr = p \]
\[ \text{Proc } \overline{t}^r_L \doteq \text{Proc } (\text{New } c) \ p \overline{t} \quad \text{otherwise, } c \text{ fresh} \]
\[ \text{let } \overline{v} = \text{K } \text{in } S^r_L \doteq \text{let } \overline{v} = [K]^r_L \text{ in } [S]^r_L \quad \text{if } K \neq \text{Proc } p \overline{t} \]
\[ \text{let } \overline{v} = \text{Proc } p \overline{w} \text{ in } S^r_L \doteq \text{let } \overline{v} = \text{Proc Reuse } p \overline{w} \text{ in } [S]^r_L \quad \text{if } b = \top, \overline{w} \in V \]
\[ \text{let } \overline{v} = \text{Proc } p \overline{t} \text{ in } S^r_L \doteq \text{let } \overline{v} = \text{Proc Reuse } p \overline{w} \text{ in } [S]^r_L \quad \text{otherwise, } c \text{ fresh} \]

\[ \text{Figure 6: Proc Calls Analysis} \]

B TRANSFORMATION DETAILS

B.1 Initial Semantics

The initial big-step skeletal semantics is given as \((T_b, T_g, C_0, F, P_0, R_{\text{BS}}, \text{ctype}, \text{ftype}, \text{ptype})\), where the set \(T\) of types is the union of base types \(T_b\) and program types \(T_g\). The transformation modifies or completes these elements. Note that ctype and ptype are slightly modified, but we keep the same name to simplify the notations.

B.2 Analysis

The first phase is the analysis described in Section 4.1. The full rules are given in Figure 6. This analysis is applied to every skeleton of the semantics.

\[ R_{\text{BS}} = \{ p(\overline{y}, c(\overline{x})) \mid [S]^r_T, (p(\overline{y}, c(\overline{x})) : S) \in R_{\text{BS}} \} \]

Where Sg1Use(S) is the set of variables that are used exactly once in S.

B.3 Generation

After the analysis, we process every proc call annotated with a fresh constructor \(c\) to compute the type and rule of \(c\). For this, we need to decompose skeletons into a proc call and a context representing the continuation.

The operation \([S]^r_L\) inductively goes through \(S\), building the continuation in its parameter \(E\) and returning the set of new rules. Assuming \(r\) of the form \(pr(\overline{y}, c_r(\overline{x_r})) := S_r\), we define it as follows:

\[ \text{Branch } \text{([S_1, \ldots, S_n])}_E^r \doteq [S_1]^r_E \cup \ldots \cup [S_n]^r_E \]
\[ \text{Filter } f \overline{t}_E^r = \text{Return } \overline{t}_E^r = 0 \]
\[ \text{Proc Reuse } p \overline{t}_E^r = \text{Proc Tail } p \overline{t}_E^r = 0 \]
\[ [\text{Proc (New } c) \ p \overline{t}_E^r = [\text{Proc Reuse } p \overline{w}] \]
\[ \text{where } \overline{w} \text{ are fresh and } \overline{z} = (fv(E) \setminus \overline{y}) \]
\[ \text{let } \overline{v} = \text{K } \text{in } S^r_E \doteq [K]^r_{<\overline{v}=[\overline{z}]} \cup [S]^r_E \]

where \(fv(E)\) are the free variables of \(E\), defined as expected (see Definition 1 in Appendix C).

We update the semantics by adding \(c\), its typing, and its rule. As explained in Section 4.1, the variables \(\overline{w}\) can be deduced, and the new skeleton can reuse the fresh constructor so we change the annotation.

The generation phase is applied to every rule in \(R_{\text{BS}}\), resulting in a new set \(C_1 \supseteq C_0\) of constructors and a new set \(R_{\text{gen}} \supseteq R_{\text{BS}}\) of rules. The output of this phase is the extended semantics \((T_b, T_g, C_1, F, P_0, R_{\text{gen}}, \text{ctype}, \text{ftype}, \text{ptype})\).
Assuming \( r = (pr(\tilde{y}, c_r(\tilde{x}))) \) and 
\[
\begin{align*}
&\text{Branch } (S_1, ..., S_n) \models \text{Branch } (S_1' \cup S_n') \\
&\text{let } \tilde{o} = \text{return } \tilde{T} \text{ in } S \models \text{let } \tilde{o} = \text{return } \tilde{T} \text{ in } S' \\
&\text{let } \tilde{o} = \text{filter } f \tilde{T} \text{ in } S \models \text{let } \tilde{o} = \text{filter } f \tilde{T} \text{ in } S' \\
&\text{Return } \tilde{T} \models \text{Return } (\tilde{y}, \text{ret}_\text{pr}(\tilde{T})) \\
&\text{Proc } \text{tail } \text{pr } \tilde{T} \models \text{Return } \tilde{T} \\
&\text{let } \tilde{o} = \text{proc } (\text{new } c) \text{ pr } \tilde{T} \text{ in } S \models \text{let } \tilde{o} = \text{return } (\tilde{y}, c(\tilde{T}(\tilde{z}))) \\
&\text{where } (pr(\tilde{y}, c(\tilde{w}))) \models S_c \
\end{align*}
\]

\[\begin{align*}
S_1 &= \text{let } \tilde{x} = \text{proc } \text{pr } \tilde{w} \text{ in } \text{return } (\tilde{y}, c_r(\tilde{x}))(\sigma; [\tilde{z}/\tilde{w}]) & \tilde{w} \text{ fresh ; } \tilde{w} = (\tilde{w}', \tilde{w}) \\
S_2 &= \text{let } \tilde{o} = \text{proc } \text{getret}_\text{pr } (\tilde{w}) \text{ in } S \models S' \models S_c \models S_c(\tilde{w}/\tilde{w}) \\
&
\end{align*}\]

**Figure 7:** Small-Step Transformation of a Skeleton

### B.4 Distribute Branchings
This phase is described in Section 4.2. The distribution of \( S \) over \( \text{Branch} \), noted \([S] \) is defined as follows.

\[
[S] = \begin{cases}
\text{Branch}(S_1, ..., S_n) & \text{if } K = \text{Branch}(\ldots) \\
\text{Branch}(S_1', ..., S_n') & \text{if } K = \text{Branch}(\ldots)
\end{cases}
\]

As mentioned, this forces proc calls to be at the toplevel of the program. This way, the next phase is able to modify proc calls to immediately return and stop the computation, which is not possible in nested computations.

We apply this operation to every skeleton of our semantics:

\[ R_{\text{dist}} = \{p(\tilde{y}, c(\tilde{x})): [S] \mid (p(\tilde{y}, c(\tilde{x}))) \models S) \in R_{\text{gen}}\} \]

### B.5 Small-Step
Finally, the last phase of the transformation produces the coercions and the small-step rules.

\[ \forall p \in P_0 \text{ with ptype}(p) = ((\tilde{x}, s_g), \tilde{u}), \text{ we redefine: } \text{ptype}(p) = ((\tilde{x}, s_g)) \]

\[ C_2 = C_1 \cup \{\text{ret}_p \mid p \in P_0\} \]

\[ P_{\text{getret}} = \{\text{getret}_p \mid p \in P_0\} \]

\[ R_{\text{getret}} = \{\text{getret}_p(\text{ret}_p \tilde{o}) : = \text{return } \tilde{o} \mid p \in P_0 \land \text{ptype}_\text{out}(p) = (\tilde{o})\} \]

The full set of cases for the final phase is given in Figure 7. It is applied to the rules defining the procedures of \( P_0 \).

\[ R_{\text{SS}} = \{p(\tilde{y}, c(\tilde{x})): [S] \mid (p(\tilde{y}, c(\tilde{x}))) \models S) \in R_{\text{dist}} \cup R_{\text{getret}}\} \]

In the end, we obtain the semantics \( (T_b, T_g, C_2, F, P_0 \cup P_{\text{getret}}, R_{\text{SS}}, \text{ctype}, \text{ftype}, \text{ptype}) \) where every \( p \in P_0 \) makes a single step of computation.
We present a pen-and-paper proof that the transformation of Section 4 is correct, in the simplified case where we systematically create new constructors. We note that the following definitions are not explicited in the paper.

The skeletal semantics as well as the different phases of the transformation are presented in the accompanying paper, and completed in Appendix B. We only redefine the last phase of the transformation (Figure 10), as it can be simplified to not use substitutions.

C EQUIVALENCE PROOF

C.1 Definitions and Proof Structure

We present a pen-and-paper proof that the transformation of Section 4 is correct, in the simplified case where we systematically create new constructors.

We recall the rules for the inductive (Figure 8) and coinductive (Figure 9) interpretations of skeletal semantics.

The skeletal semantics as well as the different phases of the transformation are presented in the accompanying paper, and completed in Appendix B. We only redefine the last phase of the transformation (Figure 10), as it can be simplified to not use substitutions.

The following definitions are not explicited in the paper.

Definition 1. We note \( \text{fv}(S) \) the free variables of a tuple/term/skelement/skeleton/context.

\[
\begin{align*}
\text{fv}((a_1, \ldots, a_n)) & \triangleq \text{fv}(a_1) \cup \ldots \cup \text{fv}(a_n) \\
\text{fv}(c(\bar{t})) & \triangleq \text{fv}(\bar{t}) \\
\text{fv}(\text{Proc } p(\bar{t}, i)) & \triangleq \text{fv}(\bar{t}) \cup \text{fv}(t) \\
\text{fv}(\text{Branch } S) & \triangleq \text{fv}(S) \\
\text{fv}([\cdot]) & \triangleq \emptyset \\
\text{fv}(v) & \triangleq \{v\} \\
\text{fv}(\text{Filter } f(\bar{t})) & \triangleq \text{fv}(\bar{t}) \\
\text{fv}(\text{Return } \bar{t}) & \triangleq \text{fv}(\bar{t}) \\
\text{fv}(<[\cdot]|\bar{t}|S> ) & \triangleq \text{fv}(S \setminus \{\bar{t}\}) \\
\end{align*}
\]
Definition 2. We note bv(S) the variables defined in a skeleton.

\[ \begin{align*}
    \text{bv(Filter } f (\vec{i})) & \triangleq \emptyset \\
    \text{bv(Proc } p (\vec{t}, \vec{t})) & \triangleq \emptyset \\
    \text{bv(Return } \vec{i}) & \triangleq \emptyset \\
    \text{bv(Branch } (S_1, \ldots, S_n)) & \triangleq \text{bv}(S_1) \cup \ldots \cup \text{bv}(S_n) \\
    \text{bv(let } \vec{v} = K \text{ in } S) & \triangleq (\vec{v}) \cup \text{bv}(S)
\end{align*} \]

Definition 3. We note SSA(S) the statement that a skeleton S does not reuse variables names. This can be seen as a Static Single Assignment form.

\[ \text{SSA}(S) \triangleq \text{NoRedef}(S) \land \text{fv}(S) \cap \text{bv}(S) = \emptyset \]

\[ \begin{align*}
    \text{NoRedef(Filter } f (\vec{i})) & \triangleq \top \\
    \text{NoRedef(Proc } p (\vec{t}, \vec{t})) & \triangleq \top \\
    \text{NoRedef(Return } \vec{i}) & \triangleq \top \\
    \text{NoRedef(Branch } (S_1, \ldots, S_n)) & \triangleq \forall i, \text{NoRedef}(S_i)
\end{align*} \]

\[ \begin{align*}
    \text{NoRedef(let } \vec{v} = K \text{ in } S) & \triangleq \begin{cases}
        \text{bv}(K) \cap (\vec{v}) = \emptyset & \text{bv}(S) \cap (\vec{v}) = \emptyset \\
        \text{bv}(K) \cap \text{bv}(S) = \emptyset \\
        \text{NoRedef}(K) \\
        \text{NoRedef}(S)
    \end{cases}
\end{align*} \]

Our transformation is meant to apply to such skeletons. If need be, a first transformation putting skeletons in SSA form can be necessary.

Note that the naming “SSA” is an abuse, as parallel branchings are allowed to define the same variables. However, every execution of the skeleton follows a single branch and never overwrites the content of a variable.

Definition 4. We note \( S_1 \in S_2 \) when \( S_1 \) is a subskeleton of \( S_2 \). This property is the reflexive transitive closure of the following rules.

\[ \begin{align*}
    K \in \text{let } \vec{v} = K \text{ in } S \\
    S \in \text{let } \vec{v} = K \text{ in } S \\
    S_1 \in \text{Branch } (S_1, \ldots, S_n)
\end{align*} \]

Definition 5. We note \( S_1 \prec S_2 \) when \( S_1 \) is a tail subskeleton of \( S_2 \). This property is the reflexive transitive closure of the following two rules.

\[ \begin{align*}
    S \in \text{let } \vec{v} = K \text{ in } S \\
    S_1 \in \text{Branch } (S_1, \ldots, S_n)
\end{align*} \]

This definition does not consider subskeletons inside subevaluations.

For instance, \( S_t \neq \text{let } \vec{v} = \text{Branch } (S_1, \ldots, S_n) \text{ in } S' \).

The proof uses the sets of rules at the different phases of the transformation to state and certify results. As explained in Section 5, we additionally introduce a set \( R_{EBS} \), corresponding to an extended big-step semantics, to simplify the proof strategy. We recall the notations for the different sets and the semantics they represent.

- \( RBS \): initial rules, input of the transformation;
- \( Rgen \): rules after generation of new constructors and rules;
- \( Rdist \): rules after distributing branchings;
- \( R_{EBS} \): similar to \( R_{dist} \) (after delaying returns), with rules for \( \text{Ret}_p \) constructors;

\[ R_{EBS} \triangleq R_{dist} \cup \{ p(\vec{g}, \text{Ret}_p(\vec{v})) := \text{Return } \vec{v} \mid p \in P_0 \} \]

- \( RSS \): result of the transformation after going small-step, with \( \text{getRet}_p \) procedures.

We use these sets to specify the notations for derivation judgments. We write for instance \( \Sigma \vdash S \parallel^{RBS} \vec{b} \) and \( \vec{a} \parallel_p^{RBS} \vec{b} \) for the concrete evaluation, and \( \Sigma \vdash S \parallel^{RBS} \vec{a} \) and \( \vec{a} \parallel_p^{RBS} \) for the divergence of the initial big-step semantics.

Definition 6. We note \( \vec{a} \rightarrow_p^\infty \vec{b} \) the divergence in the small-step skeletal semantics. It is defined coinductively with the following rule.

\[ \frac{\vec{a} \parallel_p^{RBS} \vec{b} \quad \vec{b} \rightarrow_p \vec{c}}{\vec{a} \rightarrow_p^\infty \vec{c}} \]

Other equivalent definitions include:
The simple proofs of the first few trivial lemmas are omitted.

Let \( F(X) = \{ (\bar{a}, p) \mid \exists \bar{b}, \bar{a} \Rightarrow_R \bar{b} \wedge (\bar{b}, p) \in X \} \), we have:

\[
\overset{\Rightarrow}{\rightarrow} = \{ (\bar{a}, p) \mid \bar{a} \overset{\Rightarrow}{\rightarrow} p \} \equiv vX.F(X)
\]

We also recall notations from the transformation phases (Appendix B). We use the following:

- \( < S_1 \mid \bar{x} \mid S_2 > \) for the monadic bind of two skeletons;
- \([S]\) for the generation of new constructors, skeletons, and big-step rules (after adding a “New c” annotation to every proc call);
- \([S]\) for the distribution of branchings;
- \( \| S \| \) for the final small-step transformation, redefined with simpler rules in Figure 10.

A first section (C.2) covers simple lemmas about our different definitions, unconnected to the different rule sets. Afterwards, we check that our SSA property is preserved throughout the transformation (C.3). Then we certify important properties of the different phases of the transformation, to make sure they behave as intended (C.4). Using these results, we finally prove the equivalences between the different semantics. Section C.5 covers the equivalence between Big-Step and Extended Big-Step. Section C.6 certifies that an EBS evaluation/divergence implies a small-step (in)finite sequence. Finally, Section C.7 proves the reverse direction: a small-step (in)finite reduction sequence implies an EBS evaluation/divergence.

### C.2 Basic Lemmas

The simple proofs of the first few trivial lemmas are omitted.

**Lemma 7.** For all \( S_1, \bar{S}, S_2, \bar{S}, \) and \( S_3, \)

\[
<< S_1 \mid \bar{S} \mid S_2 >> \quad \text{and} \quad \bar{S} \quad = \quad < S_1 \mid \bar{S} \mid S_2 > \]

**Lemma 8.** For all \( \Sigma_1, \Sigma_2, \) and \( \Sigma_3, \)

\[
(\Sigma_1 + \Sigma_2) + \Sigma_3 = \Sigma_1 + (\Sigma_2 + \Sigma_3)
\]

**Lemma 9.** For all \( \Sigma_1, \Sigma_2, \) and \( \Sigma_3, \)

- \( \forall x, \quad x \notin (\text{dom}(\Sigma_2) \setminus \text{dom}(\Sigma_3)) \implies (\Sigma_1 + \Sigma_3)(x) = (\Sigma_1 + \Sigma_2 + \Sigma_3)(x) \)
- \( \forall t, \quad (\text{dom}(\Sigma_2) \setminus \text{dom}(\Sigma_3)) \cap \text{fv}(t) = \emptyset \implies (\Sigma_1 + \Sigma_3)(t) = (\Sigma_1 + \Sigma_2 + \Sigma_3)(t) \)
- \( \forall t, \quad (\text{dom}(\Sigma_2) \setminus \text{dom}(\Sigma_3)) \cap \text{fv}(t) = \emptyset \implies (\Sigma_1 + \Sigma_3)(t) = (\Sigma_1 + \Sigma_2 + \Sigma_3)(t) \)

**Lemma 10.** For all \( S, \Sigma_1, \Sigma_2, \) and \( \bar{a}, \) if \( (\text{dom}(\Sigma_2) \setminus \text{dom}(\Sigma_3)) \cap \text{fv}(S) = \emptyset, \) then

\[
\Sigma_1 + \Sigma_3 + S \downarrow \bar{a} \iff \Sigma_1 + \Sigma_2 + \Sigma_3 + S \downarrow \bar{a}
\]

**Proof.** By structural induction on \( S. \)

- If \( S = \text{Return}(\bar{t}) \)
  \[
  \Sigma_1 + \Sigma_3 + \text{Return}(\bar{t}) \downarrow \bar{a} \]
  \[
  \quad \iff (\Sigma_1 + \Sigma_3)(t) = \bar{a} \]
  \[
  \quad \iff (\Sigma_1 + \Sigma_2 + \Sigma_3)(t) = \bar{a} \quad \text{using Lemma 9 (because } \text{fv}(\bar{t}) = \text{fv}(S)) \]
  \[
  \quad \iff \Sigma_1 + \Sigma_2 + \Sigma_3 + \text{Return}(\bar{t}) \downarrow \bar{a}
  \]
- If \( S = \text{Branch}(\bar{S}) \)
  \[
  \Sigma_1 + \Sigma_3 + \text{Branch}(\bar{S}) \downarrow \bar{a} \]
  \[
  \quad \iff \exists \bar{S}_1 \in \bar{S}, \Sigma_1 + \Sigma_3 + \bar{S}_1 \downarrow \bar{a} \]
  \[
  \quad \iff \exists \bar{S}_1 \in \bar{S}, \Sigma_1 + \Sigma_2 + \Sigma_3 + \bar{S}_1 \downarrow \bar{a} \quad \text{using induction hypothesis} \]
  \[
  \quad \iff \Sigma_1 + \Sigma_2 + \Sigma_3 + \text{Branch}(\bar{S}) \downarrow \bar{a}
  \]
- If \( S = (\text{let } \bar{b} = K \text{ in } S') \)
  \[
  \Sigma_1 + \Sigma_3 + \text{let } \bar{b} = K \text{ in } S' \downarrow \bar{a} \]
  \[
  \quad \iff \exists \bar{b}, \Sigma_1 + \Sigma_3 + \{v \mapsto \bar{b}\} + S' \downarrow \bar{a}
  \]
  \[
  \quad \iff \exists \bar{b}, \Sigma_1 + \Sigma_2 + \Sigma_3 + \{v \mapsto \bar{b}\} + S' \downarrow \bar{a} \quad \text{using IH twice and Lemma 8.} \]

\[
\text{fv}(S') \subset \text{fv}(S) \cup \{\bar{b}\}, \text{ so } (\text{dom}(\Sigma_2) \setminus (\text{dom}(\Sigma_3) \cup \{\bar{b}\}) \cap \text{fv}(S') = \emptyset \]
\[
\iff \Sigma_1 + \Sigma_2 + \Sigma_3 + \text{let } \bar{b} = K \text{ in } S' \downarrow \bar{a}
\]
**Lemma 11.** For all $S$, $\Sigma_1$, $\Sigma_2$, and $\Sigma_3$, if $(\text{dom}(\Sigma_2) \setminus \text{dom}(\Sigma_3)) \cap \text{fv}(S) = \emptyset$, then

$$\Sigma_1 + \Sigma_3 \vdash S \uparrow \iff \Sigma_1 + \Sigma_2 + \Sigma_3 \vdash S \uparrow$$

**Proof.** This lemma is similar to Lemma 10, but for divergence. See Figure 9 for the coinductive definition of $\Sigma \vdash S \uparrow$. The proof is done by a straightforward induction on $S$, and case analysis on the rule used. The only two places where the environment $\Sigma$ is used are:

- in rules Div-Pc, where both environments agree on the mapping of the variables $\tilde{\tau}$ by hypothesis.
- in the first leaf of rule Div-LetR, where we can use Lemma 10 to go from one environment to the other.

$\square$

**Lemma 12.** For all $S$, $x$, $S_2$, and $\Sigma$, if $(\text{bv}(S_1) \setminus \{\tilde{x}\}) \cap \text{fv}(S_2) = \emptyset$, then

$$\begin{align*}
\Sigma \vdash S_1 \uparrow & \iff \exists \overline{b}. \{ \Sigma + \{v \mapsto c\} \vdash S'_1 \uparrow \} \cup \\
& \quad \cup \{ \Sigma + \{v \mapsto c\} + \{x \mapsto b\} \vdash S_2 \uparrow \}
\end{align*}$$

I.e., $< S_1 | \tilde{x} | S_2 >$ diverges if either $S_1$ or $S_2$ diverges.

**Proof.** This lemma is similar to Lemma 13, but for divergence. It is also done by structural induction on $S_1$.

If $S_1$ is a skeleton $K$, then $< K | \tilde{x} | S_2 >$ is defined as $1 \text{et } \tilde{\tau} = K$ in $S_2$ and the result comes directly from the definition (see rules Div-LetR and Div-LetL of Figure 9).

If $S_1 = (1 \text{et } \tilde{\tau} = K$ in $S')$, then $< S_1 | \tilde{x} | S_2 >$ is defined as $1 \text{et } \tilde{\tau} = K$ in $< S' | \tilde{x} | S_2 >$.

Then:

$$\begin{align*}
\Sigma \vdash S_1 | \tilde{x} | S_2 > \uparrow & \iff \Sigma + \{v \mapsto c\} \vdash S'_1 \uparrow \\
& \quad \lor \Sigma + \{v \mapsto c\} + \{x \mapsto b\} \vdash S_2 \uparrow
\end{align*}$$

I.e., $< S_1 | \tilde{x} | S_2 >$ diverges if either $S_1$ or $S_2$ diverges.

$\square$

**Lemma 13.** For all $S$, $x$, $S_2$, $\Sigma$, and $\tilde{\tau}$, if $(\text{bv}(S_1) \setminus \{\tilde{x}\}) \cap \text{fv}(S_2) = \emptyset$, then

$$\begin{align*}
\Sigma \vdash S_1 | \tilde{x} | S_2 > \uparrow \tilde{\tau} & \iff \exists \overline{b}. \{ \Sigma + \{v \mapsto c\} \vdash S'_1 \uparrow \} \cup \\
& \quad \cup \{ \Sigma + \{v \mapsto c\} + \{x \mapsto b\} \vdash S_2 \uparrow \}
\end{align*}$$

**Proof.** By structural induction on $S_1$.

If $S_1$ is a skeleton $K$, then $< K | \tilde{x} | S_2 >$ is defined as $1 \text{et } \tilde{\tau} = K$ in $S_2$ and the result comes directly from the definition (see Figure 8).

If $S_1$ is of the form $1 \text{et } \tilde{\tau} = K$ in $S'$, then $< S_1 | \tilde{x} | S_2 >$ is defined as $1 \text{et } \tilde{\tau} = K$ in $< S' | \tilde{x} | S_2 >$, and we have the following.

$$\begin{align*}
\Sigma \vdash S_1 | \tilde{x} | S_2 > \uparrow \tilde{\tau} & \iff \Sigma + \{v \mapsto c\} \vdash S'_1 \uparrow \\
& \quad \lor \Sigma + \{v \mapsto c\} + \{x \mapsto b\} \vdash S_2 \uparrow
\end{align*}$$

I.e., $< S_1 | \tilde{x} | S_2 >$ diverges if either $S_1$ or $S_2$ diverges.

$\square$
Lemma 17. For all \( S_1, \overline{v}, S_2 \), if \( \text{SSA}(1 \text{et } \overline{v} = \text{Branch}(S_1) \text{ in } S_2) \), then:

- \( \text{SSA}(S_1) \)
- \( \text{bv}(1 \text{et } \overline{v} = \text{Branch}(S_1) \text{ in } S_2) = \text{bv}(S_1) \)
- \( \text{fv}(1 \text{et } \overline{v} = \text{Branch}(S_1) \text{ in } S_2) = \text{fv}(S_1) \)

Remark 17.1. Note that the reverse of the first point is not true. See for instance \( S_1 = (1 \text{et } y = K \text{ in } S) \) and \( S_2 = \text{Return } y \).

Proof. First, by unfolding definitions, note that we always have:

- \( \text{NoRedef}({\text{Branch}}(S_1)) \iff \text{NoRedef}(S_1) \)
- \( \text{bv}({\text{Branch}}(S_1)) = \text{bv}(S_1) \)
- \( \text{fv}({\text{Branch}}(S_1)) = \text{fv}(S_1) \)

We proceed by structural induction on \( S_1 \). If \( S_1 = K \) is a skeleton, then \( < S_1 | \overline{v} | S_2 > = (1 \text{et } \overline{v} = K \text{ in } S_2) \). We can easily unfold the definitions and check the desired results hold, using the three points above.

Else \( S_1 \) is of the form \( (1 \text{et } \overline{w} = K \text{ in } S) \),

\[
\text{fv}(\ldots) \cap \text{bv}(\ldots) = \emptyset \\
\text{bv}(S_1) \cap \overline{v} = \emptyset \\
\text{bv}(S_2) \cap \overline{v} = \emptyset \\
\text{bv}(S_1) \cap \text{bv}(S_2) = \emptyset \\
\text{NoRedef}(S_1) \\
\text{NoRedef}(S_2)
\]

Cutting our hypothesis gives us:
Lemma 19. The distribution of branchings preserves SSA form.

Second half is proved separately (Lemma 17). □

Once again, the third case is trivial, and the second can be solved using Lemma 16. The remaining (first) point can be cut in two halves, by proving the intermediate result SSA(let \( w = K \) in \( S \)) by checking the definition. Using our induction hypothesis, we have:

- SSA(<S | \( \overline{w} | S_2 >) \)
- bv(<S | \( \overline{w} | S_2 >) = \overline{w} \cup bv(S) \cup bv(S_2)
- fv(<S | \( \overline{w} | S_2 >) = fv(S) \cup (fv(S_2) \setminus \overline{v}) = fv(S) \cup fv(S_2)

Then, we have enough pieces to prove our desired result, once again directly by checking the definition:

- SSA(let \( w = K \) in \( <S | \overline{w} | S_2 >) \)
- bv(let \( w = K \) in \( <S | \overline{w} | S_2 >) = \overline{w} \cup \overline{w} \cup bv(K) \cup bv(S) \cup bv(S_2)
- fv(let \( w = K \) in \( <S | \overline{w} | S_2 >) = bv(K) \cup fv(S) \cup fv(S_2)

□

Lemma 18. SSA form is preserved during the generation phase creating new skeletons. I.e.:

- If SSA(E[Branch \( (S_1, \ldots, S_n) \)]) then SSA(E[S_1]).
- If SSA(E[let \( \overline{v} = K \) in \( S \)]) then SSA(E[S]).
- If SSA(E[let \( \overline{v} = K \) in \( S \)]) then SSA(<[.] | \( \overline{v} | E[S] > [K] \)).

Proof. If \( E = [.] \), the three points simplify to:

- If SSA(Branch \( (S_1, \ldots, S_n) \)) then SSA(S_1).
- If SSA(let \( \overline{v} = K \) in \( S \)) then SSA(S).
- If SSA(let \( \overline{v} = K \) in \( S \)) then SSA(let \( \overline{v} = K \) in \( S \))

The third case is trivial, the other two are solved using Lemma 16.

Else \( E = [.] \) \( | \overline{w} | S_E > \) for some \( \overline{w} \) and \( S_E \). The three points simplify to:

- If SSA(let \( \overline{w} = \text{Branch} \( (S_1, \ldots, S_n) \) in \( S_E \)) then SSA(<\( S_1 \) | \( \overline{w} | S_E >).\)
- If SSA(let \( \overline{v} = K \) in \( <S | \overline{w} | S_E > \)) then SSA(<\( S \) | \( \overline{w} | S_E > \))
- If SSA(let \( \overline{v} = K \) in \( <S | \overline{w} | S_E > \)) then SSA(let \( \overline{v} = K \) in \( <S | \overline{w} | S_E > \)).

Once again, the third case is trivial, and the second can be solved using Lemma 16. The remaining (first) point can be cut in two halves, by proving the intermediate result SSA(let \( w = \text{Branch} \( (S_i) \) in \( S_E \)). The first half can be checked directly by following Definition 3. The second half is proved separately (Lemma 17).

□

Lemma 19. The distribution of branchings preserves SSA form.

I.e., for all skeleton \( S \), if SSA(S), then SSA([S]).

Proof. For this, we prove the following by structural induction on \( S \).

\[
\forall S, SSA(S) \implies \begin{cases} 
SSA([S]) \\
\text{bv}(S) = \text{bv}([S]) \\
\text{fv}(S) = \text{fv}([S])
\end{cases}
\]

Most cases are straightforward. The only interesting case is when \( S \) is of the form let \( \overline{v} = \text{Branch} \( (S_1, \ldots, S_n) \) in \( S' \). Then by definition

\[ [S] \triangleq \text{Branch} \( ([S_1 | \overline{v} | S'] >, \ldots, [S_n | \overline{v} | S'] >) \).

First, we check by following Definition 3 that we have SSA(let \( \overline{v} = \text{Branch} \( S_i \) in \( S' \)) for each \( i \). Then, using Lemma 17, we get:

- SSA(<\( S_i \) | \( \overline{v} | S' > \))
We have that
\[ \llbracket S \rrbracket = \bigcup_j \llbracket S_j \rrbracket = \bigcup_j (\llbracket S_j \rrbracket \cup \llbracket S_j' \rrbracket) = (\bigcup_j \llbracket S_j \rrbracket) \cup (\llbracket S \rrbracket \cup \llbracket S' \rrbracket) = \llbracket S \rrbracket \]

And we can conclude:
\[ \llbracket S \rrbracket = \bigcup_j \llbracket S_j \rrbracket = \bigcup_j (\llbracket S_j \rrbracket \cup \llbracket S_j' \rrbracket) = (\bigcup_j \llbracket S_j \rrbracket) \cup (\llbracket S_j \rrbracket \cup \llbracket S' \rrbracket) = \llbracket S \rrbracket \]

Lemma 20. If all initial skeletons are in SSA form, then the new skeletons created during the generation phase respect the SSA conditions. I.e., if for all rule \( (p \langle \bar{y}, c(\bar{z}) \rangle := S) \in R_{BS} \) we initially have \( SSA(S) \), then for all rule \( (p \langle \bar{y}, c(\bar{z}) \rangle := S) \in R_{gen} \) we also have \( SSA(S) \).

Proof. Initial rules are left untouched, so we only need to check SSA(S) for new skeletons, constructed from a generation operation \( \llbracket Proc (New \; c) \; t \rrbracket_{BS} \). The important part of the proof is to check SSA(\( E[Proc \; p \; \bar{t}] \)), as the new skeleton is then \( E[Proc \; p \; \bar{w}] \) where \( \bar{w} \) are fresh variables, and the property trivially ensues.

For this, we check we have \( SSA(\llbracket S \rrbracket) \) at every step \( \llbracket S \rrbracket_{BS} \). Initially, we start with a given skeleton \( S \) (from a rule of \( R_{BS} \), for which we now SSA(\( S \))) and an environment \( E = [\;] \), so it holds. Then, the preservation of the property comes from Lemma 18.

C.4 Properties of the Transformation Phases

Lemma 21. For all environment \( \Sigma \), terms \( a \), and skeleton \( S \) such that \( SSA(S) \),
\[ \Sigma \vdash S \upharpoonright a \iff \Sigma \vdash [S] \upharpoonright a \]
I.e., the distribution of branchings preserves the concrete interpretation.

Proof. The proof is done by induction on the size of \( S \), and dealing with the different forms \( S \) can take. Three of the four cases are trivial (see Section B.4 for the definition). The only interesting case is when \( S \) is of the form \( \llbracket S \rrbracket = \text{Branch}(\llbracket S_1 \rrbracket, \ldots, \llbracket S_n \rrbracket) \)  in \( S' \). Then, by definition,
\[ \llbracket S \rrbracket = \text{Branch}(\llbracket S_1 \rrbracket | \bar{b} | S') \]
\[ \llbracket S \rrbracket = \text{Branch}(\llbracket S_1 \rrbracket | \bar{b} | S') \]
\[ \llbracket S \rrbracket = \text{Branch}(\llbracket S_1 \rrbracket | \bar{b} | S') \]
\[ \llbracket S \rrbracket = \text{Branch}(\llbracket S_1 \rrbracket | \bar{b} | S') \]
\[ \llbracket S \rrbracket = \text{Branch}(\llbracket S_1 \rrbracket | \bar{b} | S') \]

We have \( (\llbracket S \rrbracket \cup \llbracket S \rrbracket) \) and \( \llbracket S \rrbracket \) from \( SSA(S) \)
\[ \llbracket S \rrbracket \cup \llbracket S \rrbracket = \llbracket S \rrbracket \]
\[ \llbracket S \rrbracket \cup \llbracket S \rrbracket = \llbracket S \rrbracket \]
\[ \llbracket S \rrbracket \cup \llbracket S \rrbracket = \llbracket S \rrbracket \]
\[ \llbracket S \rrbracket \cup \llbracket S \rrbracket = \llbracket S \rrbracket \]
\[ \llbracket S \rrbracket \cup \llbracket S \rrbracket = \llbracket S \rrbracket \]

Lemma 22. For all environment \( \Sigma \) and skeleton \( S \) such that \( SSA(S) \),
\[ \Sigma \vdash S \uparrow \iff \Sigma \vdash [S] \uparrow \]
I.e., the distribution of branchings also preserves the coinductive semantics.

Proof. This lemma is similar to Lemma 21, and so is the proof. This is done by a straightforward induction on \( S \). Instead of using Lemma 13, we use the similar Lemma 12 for divergence. Also, we directly use Lemma 21 instead of the induction hypothesis for finite subvaluations.

Lemma 23. Delaying returns does not impact the inductive interpretation. Thus, the rules common to \( R_{dist} \) and \( R_{EBS} \) behave the same way.

Proof. This is done by induction on skeletons. The induction case is trivial, and the base case is to check that \( \Sigma \vdash Filter \; f \; \bar{t} \uparrow \bar{a} \iff \Sigma \vdash \text{let } \bar{w} = \text{Filter } f \; \bar{t} \text{ in Return } \bar{w} \uparrow \bar{a} \)
(and similarly for procedures, with the same reasoning). This comes from the two following derivation trees having the same leaf \( R_f(\Sigma(i)) \uparrow \bar{a} \).
\[ R_f(\Sigma(i)) \uparrow \bar{a} \]
\[ R_f(\Sigma(i)) \uparrow \bar{a} \]
\[ (\Sigma + \{ w \mapsto a \})(\bar{w}) = \bar{a} \]
\[ (\Sigma + \{ w \mapsto a \})(\bar{w}) = \bar{a} \]
\[ \Sigma \vdash \text{let } \bar{w} = \text{Filter } f \; \bar{t} \text{ in Return } \bar{w} \uparrow \bar{a} \]
\[ \Sigma \vdash \text{let } \bar{w} = \text{Filter } f \; \bar{t} \text{ in Return } \bar{w} \uparrow \bar{a} \]
The following two lemmas show that the rules added to create $R_{EBS}$ (from $R_{dsym}$) behave as intended.

Lemma 24. For all procedure $p$ and terms $\bar{a}, \bar{b},$ and $\bar{d}$,
\[
\bar{b} = \bar{d} \iff (\bar{a}, \text{Ret}_p(\bar{b})) \Downarrow_{R_{EBS}}^p \bar{d}
\]

**Proof.** This comes from the following derivation tree, either by creating it or because there is only one possible inversion of the rules of Figure 8.

\[
\begin{align*}
(p(y \mapsto a), (x \mapsto b)) \in R_{EBS} & \quad \Downarrow_{R_{EBS}}^p \bar{b} \\
\left(\begin{array}{l}
\{y \mapsto a\} + \{x \mapsto b\} + \text{Return } \bar{x} \Downarrow_{R_{EBS}}^p b \\
\{y \mapsto a\} + \{x \mapsto b\}
\end{array}\right) & \quad \Downarrow_{R_{EBS}}^p \bar{b}
\end{align*}
\]

\[\Box\]

Lemma 25. For all procedure $p$ and terms $\bar{b}$ and $\bar{d}$,
\[
\bar{b} = \bar{d} \iff \text{Ret}_p(\bar{b}) \Downarrow_{R_{getRet}_p}^p \bar{d}
\]

**Proof.** This comes from the following derivation tree, either by creating it or because there is only one possible inversion of the rules of Figure 8.

\[
\begin{align*}
(p(\text{Ret}_p(\bar{x})), ) := \text{Return } \bar{x} & \in R_{SS} \\
\left(\begin{array}{l}
\{x \mapsto b\} + \text{Return } \bar{x} \Downarrow_{R_{SS}}^p \bar{b} \\
\{x \mapsto b\}
\end{array}\right) & \quad \Downarrow_{R_{SS}}^p \bar{b}
\end{align*}
\]

\[\Box\]

The following two lemmas show the small-step semantics exhibits the usual congruence rules for proc calls labeled Reuse.

Lemma 26. If $(p(y, c(\bar{w}, \bar{z}))) := 1$ let $\bar{b} = \text{Proc } p_1 \bar{w}$ in $S \in R_{EBS}$, then
\[
(\bar{c}, e_0) \Downarrow_{R_{P1}}^{p_1} (\bar{c}, e_0') \implies (\bar{a}, c((\bar{c}, e_0), \bar{a}')) \Downarrow_{R_{EBS}}^p (\bar{a}, c((\bar{c}, e_0'), \bar{a}'))
\]

**Proof.** Let $r$ be the rule in the formulation of the lemma.

\[
\begin{align*}
\Sigma'(\bar{g}, c(\bar{u}, \bar{z})) & = (\bar{a}, c((\bar{c}, e_0'), \bar{a}')) \\
\Sigma + \text{let } \bar{a} = \text{Proc } p_1 \bar{w} \text{ in } S \Downarrow_r \bar{a} & \Downarrow_{R_{EBS}}^p (\bar{a}, c((\bar{c}, e_0'), \bar{a}'))
\end{align*}
\]

\[
\begin{align*}
\left(\begin{array}{l}
\{y \mapsto a\} \quad \{\bar{w} \mapsto (\bar{c}, e_0)\} \quad \{z \mapsto a'\} \quad \Sigma' = \Sigma + \{\bar{u} \mapsto (\bar{c}, e_0')\}
\end{array}\right)
\end{align*}
\]

\[\Box\]

Lemma 27. If $(p(y, c(\bar{w}, \bar{z}))) := 1$ let $\bar{b} = \text{Proc } p_1 \bar{w}$ in $S \in R_{EBS}$, and $e_0$ is not of the form $\text{Ret}_p(\bar{a})$, then
\[
(\bar{a}, c((\bar{c}, e_0), \bar{a}')) \Downarrow_{R_{EBS}}^p \bar{a} \iff \exists e_0'. \left(\begin{array}{l}
\bar{d} = (\bar{a}, c((\bar{c}, e_0'), \bar{a}')) \\
\bar{c}, e_0, e_0' \Downarrow_{R_{P1}}^{p_1} (\bar{c}, e_0')
\end{array}\right)
\]

This Lemma is the converse of Lemma 26 above.

**Proof.** The property holds because the only possible evaluation tree is the one presented in the proof of Lemma 26 above. Indeed $\Sigma + \text{let } \bar{a} = \text{Proc } p_1 \bar{w} \text{ in } S \Downarrow_r \bar{a} \Downarrow_{R_{EBS}}^p \ldots$, with $\Sigma(w) = e_0$, is not possible since $\text{getRet}_p1$ only has a rule for the constructor $\text{Ret}_p1$.

\[\Box\]

The following two lemmas show the small-step semantics can also extract coerced values and continue a computation, for proc calls labeled Reuse when the first computation is finished.

Lemma 28. If $(p(y, c((\bar{w}, \bar{z}))) := 1$ let $\bar{b} = \text{Proc } p_1 (\bar{w}, \bar{w})$ in $S \in R_{EBS}$, then
\[
\{y \mapsto a\} + \{z \mapsto a'\} + \| S \| \Downarrow_r \bar{a} \Downarrow_{R_{EBS}}^p (\bar{a}, c((\bar{c}, \text{Ret}_p1(\bar{b})), \bar{a}'))
\]
Lemma 29. If \((p(y, c), (\tilde{w}, w), \tilde{z})) \models \text{let } \tilde{v} = \text{Proc Reuse } p_1 (\tilde{w}, w) \text{ in } S \in R_{SS}, \) then
\[
(ac((\tilde{v}, \text{Proc Reuse } p_1(\tilde{b})), a')))^{R_{SS}} d \implies (y \mapsto a) + (z \mapsto a') + (v \mapsto b) + \| S' \|^{R_{SS}} d
\]
This Lemma is the converse of Lemma 28 above.

Proof. The property holds because the only possible evaluation tree is the one presented in the proof of Lemma 28 above. Indeed \(\Sigma + \text{let } \tilde{v} = \text{Proc } p_1 (\tilde{w}, w) \text{ in } S \in R_{SS}, \) with \(\Sigma(w) = \text{Proc Reuse } p_1(\tilde{b}), \) is not possible since, in \(R_{SS}, \) the procedure \(p_1\) does not have a rule for the constructor \(\text{Proc Reuse}. \) We also use Lemma 10 to simplify the environment.

Lemma 30. For every rule \(r = (p(y, c), (\tilde{w}, w), \tilde{z})) \models \text{let } \tilde{v} = \text{Proc Reuse } p_1 (\tilde{w}, w) \text{ in } S \in R_{SS}, \) during the generation phase with the skeleton \(S,\) every time we apply the generation operation on a subskeleton, i.e. \([S]_{E}^{r}, \) we have \([E[S]] \triangleright [S].\)

Proof. The property trivially holds at the start \((\lfloor S \rfloor_E^{r})\) of the generation, since \([S] \triangleright [S]\) by reflexivity. Now we check that we preserve this property during the generation, assuming we are at the point \([S]_{E}^r,\) with \([E[S]] \triangleright [S].\)

\(\triangleright \) If \(S_0\) is a skeleton.
- If \(S_0\) is not a branching, there is no recursive call to the generation operation and we are done.
- If \(S_0 = \text{Branch } (S_1, \ldots, S_n),\) for each \(i\) we generate \([S_i]_E^r,\) and so we want to show \([E[S_i]] \triangleright [S].\) Note that we necessarily have \([E[S_0]] = \text{Branch } ([E[S_1]], \ldots, [E[S_n]]).\) If \(E = [\cdot]\), this is trivial. If \(E\) is of the form \(< \cdot | \tilde{v} | S' >\), we have:
  \[
  [E[S_0]] = \langle < \text{Branch } (S_1, \ldots, S_n) | \tilde{v} | S' > \rangle
  = \langle \text{let } \tilde{v} = \text{Branch } (S_1, \ldots, S_n) \text{ in } S' \rangle
  = \text{Branch } ([< S_1 | \tilde{v} | S' >], \ldots, [< S_n | \tilde{v} | S' >])
  = \text{Branch } ([E[S_1]], \ldots, [E[S_n]])
  \]
So by transitivity we have \([E[S_i]] \triangleright [E[S]] \triangleright [S].\)

\(\triangleright \) If \(S_0\) is of the form \(\text{let } \tilde{v} = K \text{ in } S_1.\) Now we need to check to the property for the two recursive calls \([K]_{E}^{r, [\cdot | \tilde{v} | S_i]} \triangleright [S_i]_E^r\) and \([S_i]_E^r.\)

We notice that \([E[S_0]] = \langle \text{let } \tilde{v} = K \text{ in } E[S_1] \rangle = \langle < \cdot | \tilde{v} | E[S_1] > \rangle[K],\) so the property holds for the first one from our assumption \([E[S_i]] \triangleright [S].\)

We are left with checking the property for \([S_i]_E^r, i.e., we want to show that \([E[S_i]] \triangleright [S].\)
- If we have \(K = \text{Branch } (S'_1, \ldots, S'_n),\) then \([E[S_0]] = \text{Branch } ([< S'_1 | \tilde{v} | E[S_1] >], \ldots).\) Using Lemma 14, we conclude \([E[S_1]] \triangleright [< S'_1 | \tilde{v} | E[S_1] >] \triangleright [S].\)
- Lastly, if \(K\) is not a branching, we simply have \([E[S_0]] = \langle \text{let } \tilde{v} = K \text{ in } E[S_1] \rangle,\) so we also have \([E[S_1]] \triangleright [E[S_0]] \triangleright [S]\) by definition.

The next two lemmas explain where the rules for new constructors come from. If after distribution, we have an initial skeleton with \(E[K_P]\) (where \(K_P = \text{Proc } (\text{New } c_0) p_1 \tilde{t}\) as its tail, then it comes from the distribution of a skeleton of the form \(E' [K_P].\) The new rule for \(c_0\) is the distribution of \(E'[K_P],\) which results in \(E[K_P]\) as well.

E.g., if the skeleton of While ends with \(\text{let } \tilde{v} = \text{Proc } (\text{NewWhile2}) p \tilde{t} \text{ in } S\) then the skeleton of While2 is necessarily of the form \(\text{let } \tilde{v} = \text{Proc Reuse } p \tilde{w} \text{ in } S.\)

Lemma 31. For all \(S_0, E, E_0, r, c_0, p_1, \tilde{t},\) let \(K_P \triangleq \text{Proc } (\text{New } c_0) p_1 \tilde{t}.\)

If we generate \([S_0]_{E}^r,\) and know that \(K_P \in S_0, K_P \notin E_0,\) and that \([E[K_P]] \triangleright [E_0[S_0]],\) then there exists \(E'\) such that we also generate \([K_P]_{E'}^r,\) and have \([E'[K_P]] = E[K_P].\)

Proof. Note that \(K_P\) appears exactly once in \(S_0,\) since \(K_P\) is annotated with a fresh constructor name \(c_0.\) We prove this lemma by induction on \(S_0.\)
Lemma 32. For all rule $(p(\vec{y}, c(\vec{x})) : = [S]) \in R_{\text{dist}}$, if $E[\text{Proc} (\text{New } c_0) p_1 \bar{t}] \vdash [S]$, then $R_{\text{dist}}$ contains a rule of the form:

$$p(\vec{y}, c_0(\vec{w}, \vec{z})) := E[\text{Proc Reuse } p_1 \vec{w}]$$

where $\vec{w}$ does not appear in $\text{fv}(E)$.

Proof. Firstly, if $c$ is not an initial constructor, we can recover the same kind of hypotheses with an initial constructor. In this case, our rule is of the form:

$$p(\vec{y}, c(\vec{x}_1, \vec{x}_2)) := E_S[\text{Proc Reuse } p_2 \vec{x}_1] \in R_{\text{gen}}$$

with $\vec{x} = \vec{x}_1, \vec{x}_2$. So it has been created from a generation operation $\text{Proc} (\text{New } c) p_2 \bar{t}' \in E_S$, with $r = (p(\vec{y}, c'(\vec{d})) : = S_0) \in R_{\text{gen}}$ where $c'$ is an initial constructor. Using Lemma 30, we have $[S] = [E_S[\text{Proc Reuse } p_2 \vec{x}_1]] \subseteq [S_0]$. So by transitivity we recover the following hypothesis:

$$(p(\vec{y}, c'(\vec{d})) : = [S_0]) \in R_{\text{dist}}$$

where $c'$ is an initial constructor and $E[\text{Proc } (\text{New } c_0) p_1 \bar{t}] \vdash [S_0]$.

Now, we can assume without loss of generality that $c$ is an initial constructor, and so that we have $r = (p(\vec{y}, c(\vec{x})) : = S) \in R_{\text{gen}}$. We use Lemma 31 with $[S_0]$ to get $E'$ such that we generate $[\text{Proc } (\text{New } c_0) p_1 \bar{t}]_{E'}$ and have $[E'[\text{Proc } (\text{New } c_0) p_1 \bar{t}]] = E[\text{Proc } (\text{New } c_0) p_1 \bar{t}]$. Thus the creation of new skeletons produces a rule $(p(\vec{y}, c_0(\vec{w}, \vec{z})) := E'[\text{Proc Reuse } p_1 \vec{w}]) \in R_{\text{gen}}$ with fresh variables $\vec{w}$. And after distributing branchings we have

$$(p(\vec{y}, c_0(\vec{w}, \vec{z})) := E[\text{Proc Reuse } p_1 \vec{w}]) \in R_{\text{dist}}$$

Lemma 33. $\forall (p(\vec{y}, c(\vec{x})) : = [S]) \in R_{\text{EBS}}$, if $(1 \text{et } \vec{d} = \text{Proc } (\text{New } c_0) p_1 \bar{t} \text{ in } S_0) \vdash [S]$, then $R_{\text{EBS}}$ contains a rule of the form:

$$p(\vec{y}, c_0(\vec{w}, \vec{z})) := 1 \text{et } \vec{d} = \text{Proc Reuse } p_1 \vec{w} \text{ in } S_0$$

where $\vec{w}$ does not appear in $\text{fv}(S_0)$.

Proof. Directly from Lemma 32, as we go from $R_{\text{dist}}$ to $R_{\text{EBS}}$ by only delaying returns at the end of skeletons. This operation does the same modifications on both rules (we assume it selects the same fresh variables for simplicity), and does not create new free variables.

C.5  Big-Step and Extended Big-Step

The following three theorems state the equivalence between the initial and extended big-step semantics. For this, we note $|t|$ the canonical injection of a term $t$ into the extended semantics. We show that the behavior is preserved when we limit ourselves to initial terms, i.e., to terms using only constructors in $c_0$ (see Appendix B), and not newly created constructors (e.g., while $e_1$ or $\text{Ret } h$).

Theorem 34 ($\text{BS} \Rightarrow \text{EBS}$). For all $p$ and initial terms $\vec{a}$, and $\vec{b}$,

$$\vec{a} \ x_p^{\text{EBS}} \vec{b} \iff [a] \ x_p^{\text{BS}} [b]$$

Proof. Our hypothesis comes from a rule of the form $p(\vec{y}, c(\vec{x})) : = S \in R_{\text{BS}} \subseteq R_{\text{gen}}$ with $\vec{a} = \vec{d}, c(\vec{d'})$ and a derivation $(y \rightarrow d) + (x \rightarrow d') + S \parallel \vec{b}$. By definition, $p(\vec{y}, c(\vec{x})) : = [S]$ is a rule of $R_{\text{dist}}$. And from Lemma 21, we have $(y \rightarrow d) + (x \rightarrow d') + [S] \parallel \vec{b}$ and $[a] \ x_p^{\text{BS}} [b]$. Since delaying returns does not change the behavior (Lemma 23), we also have $[a] \ x_p^{\text{BS}} [b]$. $

\square$
Theorem 35 (EBS⇒BS). For all \( p \), initial terms \( \overline{a} \) and extended terms \( \overline{b}' \),

\[
\overset{\text{EBS}}{\overline{a}} \downarrow_p \overline{b}' \implies \exists \overline{b} \land \overline{a} \overset{\text{RS}}{\downarrow}_p \overline{b}
\]

Proof. Since \( \overline{a} \) are initial terms and do not use coercion constructors of the form Ret\(_{\text{t}}\_h\), we also have \( \overset{\text{EBS}}{\overline{a}} \downarrow_p \overline{b}' \) from Lemma 23.

This comes from a rule of the form \( p(y, c(\overline{x})) : := [S] \in R_{\text{dist}} \) with \( \overline{a} = \overline{d}, c(d') \) and a derivation \( \{y \mapsto d\} + \{x \mapsto d'\} \vdash [S] \downarrow \overline{b} \). By definition, \( p(y, c(\overline{x})) := S \) is a rule of \( R_{\text{gen}} \), and from Lemma 21, we have \( \overset{\text{EBS}}{\overline{a}} \downarrow_p \overline{b}' \).

Since \( \overline{a} \) are initial terms and do not use newly generated constructors (e.g., While\(_1\)e\(_1\)), then \( c \) is an initial constructor, \( p(y, c(\overline{x})) := S \) is also a rule of \( R_{\text{RS}} \), and we have \( \overline{a} \overset{\text{RS}}{\downarrow}_p \overline{b}' \). This shows that \( \overline{b}' \) is necessarily restricted to initial constructors, which can be stated as

\[
\exists \overline{b}, \overline{b}' = [b] \land \overline{a} \overset{\text{RS}}{\downarrow}_p \overline{b}
\]

\( \square \)

Theorem 36 (Div: BS⇒EBS). For all \( p \) and initial terms \( \overline{a} \),

\[
\overline{a} \overset{\text{RS}}{\downarrow}_p \implies [\overline{a}] \overset{\text{EBS}}{\downarrow}_p
\]

Proof. Similarly to the two previous theorems. Since we only focus on initial terms (no new generated constructors), \( \overline{a} \overset{\text{RS}}{\downarrow}_p \iff [\overline{a}] \overset{\text{EBS}}{\downarrow}_p \). From the definition of \( R_{\text{dist}} \) and Lemma 22, \( [\overline{a}] \overset{\text{EBS}}{\downarrow}_p \iff [\overline{a}] \overset{\text{RS}}{\downarrow}_p \). Since we only focus on initial terms (no coerced returns and delaying returns is also equivalent for coinduction, \( [\overline{a}] \overset{\text{dist}}{\downarrow}_p \iff [\overline{a}] \overset{\text{EBS}}{\downarrow}_p \). \( \square \)

C.6 Extended Big-Step Implies Small-Step

We first certify the finite case with the following theorem.

Theorem 37 (EBS ⇝ SS). For all \( \overline{a}, c, \overline{a}', \overline{b}, \) and \( p \),

\[
(\overline{a}, c(\overline{a}')) \overset{\text{EBS}}{\downarrow}_p \overline{b} \implies (\overline{a}, c(\overline{a}')) \overset{\text{SS}}{\downarrow}_p (\overline{a}, \text{ret}_t\_p(\overline{b}))
\]

Proof. Since \( (\overline{a}, c(\overline{a}')) \overset{\text{EBS}}{\downarrow}_p \overline{b} \) is defined mutually with the evaluation of skeletons \( (\Sigma \vdash S \overset{\text{REBS}}{\downarrow} \overline{b}) \), we will prove two results at the same time: For all \( \overline{a}, c, \overline{a}', \overline{b}, \overline{y}, \overline{x}, S_0, \Sigma, S \), we have:

\[
\begin{align*}
& (\overline{a}, c(\overline{a}')) \overset{\text{REBS}}{\downarrow}_p \overline{b} \implies (\overline{a}, c(\overline{a}')) \overset{\text{SS}}{\downarrow}_p (\overline{a}, \text{ret}_t\_p(\overline{b})) \\
& (\Sigma \vdash S \overset{\text{REBS}}{\downarrow} \overline{b}) \implies \exists \overline{d}, (\Sigma \vdash S \overset{\text{SS}}{\downarrow} \overline{b}) \\
& S \text{ has no Reuse label}
\end{align*}
\]

The second result says that if \( S \) evaluates to \( \overline{b} \) as part of a big-step evaluation, then \( \Sigma \vdash S \overset{\text{SS}}{\downarrow} \overline{b} \) can be (small-step) reduced to an intermediate configuration \( (\overline{a}, d) \) that can reduce further to \( (\overline{a}, \text{ret}_t(p(\overline{b}))) \).

We reason by mutual induction on the derivations of \( (\overline{a}, c(\overline{a}')) \overset{\text{REBS}}{\downarrow}_p \overline{b} \) and \( \Sigma \vdash S \overset{\text{REBS}}{\downarrow} \overline{b} \).

\begin{itemize}
\item For the first result, our hypothesis is \( (\overline{a}, c(\overline{a}')) \overset{\text{REBS}}{\downarrow}_p \overline{b} \).
\item If \( c = \text{ret}_t\_p \), using Lemma 25 we have \( \overline{a}' = \overline{b} \) and this is trivial as we take zero small-steps.
\item If \( c \) is a new constructor, the bottom of the derivation is of the form
\[
\begin{align*}
& \overline{a} = (a_0', a_1', a_2'), \Sigma_0 = \{a \mapsto a\} + \{\overline{w} \mapsto (a_0', a_1')\} + \{z \mapsto a_2'\}, \text{ and we use the rule } p(\overline{y}, c(\overline{w}, \overline{z})) := 1 \text{ at } \overline{w} = \text{Proc Reuse } p_1 \overline{w} \text{ in } S. \\
& \text{Using our induction hypothesis on the first leaf we get } (a_0', a_1') \overset{\text{RS}}{\downarrow}_p (\overline{a}, \overline{d}) \overset{\text{SS}}{\downarrow}_p (\overline{a}, \text{ret}_t(p(\overline{b}))). \text{ By Lemma 26, we then have } (\overline{a}, c((a_0', a_1'), a_2')) \overset{\text{RS}}{\downarrow}_p (\overline{a}, \text{ret}_t(p(\overline{b}))).
\end{align*}
\end{itemize}
Finally, using Lemma 28 (and Lemma 10 to rewrite the environment), we have \((\tilde{a}, c((\tilde{a}', \text{Ret}_\text{p}1(\tilde{b}')), \tilde{a}')) \parallel^{\text{RSS}}_p (\tilde{a}, d)\), and we just have to assemble the three pieces by transitivity.

- Otherwise, if \(c\) is an initial constructor, the bottom of the tree derivation is of the form:

\[
\frac{p(\tilde{y}, c(x)) := S \in \text{REBS} \quad \Sigma_0 \triangleright S \parallel^{\text{RSS}} b}{(\tilde{a}, c(\tilde{a}')) \parallel^{\text{RSS}}_p (\tilde{a}, d) \quad \Sigma_0 \triangleright S \parallel^{\text{RSS}} (\tilde{a}, d)}
\]

Where \(\Sigma_0 = \{ y \mapsto a \} + \{ x \mapsto a' \}\) and \(S\) does not start with a label \text{Reuse}.

We use our induction hypothesis with \(\Sigma_0 \triangleright S \parallel^{\text{RSS}} b\) to obtain \(d\) such that \(\Sigma_0 \triangleright S \parallel^{\text{RSS}} (\tilde{a}, d)\) and \((\tilde{a}, d) (\parallel^{\text{RSS}}_p)\) (\(\tilde{a}, \text{Ret}_\text{p}(\tilde{b})\)).

Now we can complete our goal as such:

\[
\frac{p(\tilde{y}, c(x)) := S \parallel^{\text{RSS}} \in \text{REBS} \quad \Sigma_0 \triangleright S \parallel^{\text{RSS}} (\tilde{a}, d) \quad \Sigma_0 \triangleright S \parallel^{\text{RSS}} (\tilde{a}, d) \quad \Sigma_0 \triangleright S \parallel^{\text{RSS}} (\tilde{a}, d) \quad \Sigma_0 \triangleright S \parallel^{\text{RSS}} (\tilde{a}, d)}{(\tilde{a}, c(\tilde{a}')) \parallel^{\text{RSS}}_p (\tilde{a}, d) \quad (\tilde{a}, d) (\parallel^{\text{RSS}}_p)\) (\(\tilde{a}, \text{Ret}_\text{p}(\tilde{b})\)}
\]

\[r = (p(\tilde{y}, c(x)) := S_0) \in \text{REBS}\]

\[S \triangleright S_0\]

\[\Sigma_0 \triangleright S \parallel^{\text{RSS}} b\]

\[S\) has no \text{Reuse} label\]

Note that we have \(\text{SSA}(S_0)\), either from assumption for the initial skeletons, or by using Lemmas 20 and 19 for new skeletons. Thus we know extending the environment \(\Sigma\) will not change the mapping of variables \(\tilde{y}\).

As said previously, we proceed by induction on the derivation of \(\Sigma \triangleright S \parallel^{\text{RSS}} b\).

- If \(S\) is of the form \(\text{Return } \tilde{t}\), then we choose \(d = \text{Ret}_\text{p}(\tilde{b})\):

\[
\frac{\Sigma(\tilde{t}) = \tilde{b}}{\Sigma \triangleright \text{Return } \tilde{t} \parallel^{\text{RSS}} b} \quad \frac{\Sigma \triangleright S \parallel^{\text{RSS}} (\tilde{a}, d)}{\Sigma \triangleright (\parallel^{\text{RSS}}_p)\) (\(\tilde{a}, \text{Ret}_\text{p}(\tilde{b})\})}(\text{with zero steps})
\]

- If \(S\) is of the form \(\text{Branch } (S_1, \ldots, S_n)\), using the induction hypothesis with \(S_1\):

\[
\frac{\Sigma \triangleright S_1 \parallel^{\text{RSS}} b}{\Sigma \triangleright \text{Branch } (S_1, \ldots, S_n) \parallel^{\text{RSS}} b} \quad \frac{\Sigma \triangleright S \parallel^{\text{RSS}} (\tilde{a}, d)}{\Sigma \triangleright (\parallel^{\text{RSS}}_p)\) (\(\tilde{a}, \text{Ret}_\text{p}(\tilde{b})\})}
\]

- If \(S\) is of the form \(\text{let } \tilde{v} = \text{Filter } f \tilde{t}\) in \(S_0\), using the induction hypothesis with \(S_0\):

\[
\frac{\mathcal{R}_f(\Sigma(\tilde{t})) \parallel^\beta \tilde{b}'}{\Sigma \triangleright \text{Filter } f \tilde{t} \parallel^\beta \tilde{b}'} \quad \frac{\Sigma \triangleright \text{let } \tilde{v} = \text{Filter } f \tilde{t}\) in \(S_0 \parallel^{\text{RSS}} b\}}{\Sigma \triangleright (\parallel^{\text{RSS}}_p)\) (\(\tilde{a}, \text{Ret}_\text{p}(\tilde{b})\})}
\]

(similarly for \(S := \text{let } \tilde{v} = \text{Return } \tilde{t}\) in \(S_0\))
Lemma 38. For all \( p, \tilde{c}, \tilde{x}, S_0, \Sigma, \tilde{a}, \) and \( \tilde{a} \),

\[
\begin{align*}
\text{r} &= (p(\tilde{y}, c(\tilde{x}))) : S_0 \\
S &\vdash_{R_{\text{EBS}}} S \Delta S_0 \\
\Sigma(\tilde{y}) &= \tilde{a} \\
\Sigma &\vdash S \Delta R_{\text{EBS}} \\
\exists d, \{ \Sigma \vdash S \parallel^r R_{\text{EBS}} (\tilde{a}, d) \} \\
&\text{S has no Reuse label}
\end{align*}
\]

In other words, if evaluating \( S \) diverges during a (big-step) evaluation, then \( S \parallel^r \) can be (small-step) reduced into an intermediate configuration \((\tilde{a}, d)\) whose (big-step) evaluation also diverges.

**Proof.** We prove this by induction on \( S \).

- If \( S \) is of the form \( \text{let } \tilde{a} = \text{Proc( New c_0) } p_1 \overline{t} \) in \( S_0 \), we have:

  \[
  \begin{align*}
  \Sigma(\overline{t}) &\Delta p_1 \tilde{b}' \\
  \Sigma &\vdash \text{Proc( New c_0) } p_1 \overline{t} \Delta \tilde{b}' \\
  \Sigma &\vdash \text{let } \tilde{a} = \text{Proc( New c_0) } p_1 \overline{t} \text{ in } S_0 \Delta R_{\text{EBS}} \tilde{b}' \\
  \end{align*}
  \]

  Let us name \( \Sigma(\overline{t}) = (\tilde{a}, \varepsilon) \). We use our induction hypothesis on the first leaf and get

  \( (\tilde{a}, \varepsilon) (\Delta p_1 \tilde{b}') \). Also, we use our induction hypothesis on the second leaf and we have \( d_0 \) such that \( \Sigma + \{ v \mapsto b' \} \vdash S_0 \parallel^r R_{\text{EBS}} (\tilde{a}, d_0) \) and \( (\tilde{a}, d_0) (\Delta p_1 \tilde{b}') \).

  From Lemma 33, \( R_{\text{EBS}} \) contains a rule of the form

  \[
  p(\tilde{y}, c_0(\tilde{w}, z)) := \text{let } \tilde{a} = \text{Proc( New c_0) } p_1 \tilde{w} \text{ in } S_0.
  \]

  With \( d = c_0(\Sigma(t), \Sigma(z)) = c_0(\tilde{c}, \varepsilon, \Sigma(z)) \), we have \( S \parallel^r = \text{Return } (\tilde{y}, c_0(\tilde{t}, \tilde{z})) \) and thus:

  \[
  \Sigma(\tilde{y}, c_0(\tilde{t}, \tilde{z})) = (\tilde{a}, d) \\
  \Sigma \vdash \text{Return } (\tilde{y}, c_0(\tilde{t}, \tilde{z})) \Delta R_{\text{EBS}} (\tilde{a}, d)
  \]

  To conclude, we are missing \((\tilde{a}, d) (\Delta p_1 \tilde{b}') (\tilde{a}, d_0)\) which can be cut into two pieces:

  \[
  (\tilde{a}, d) (\Delta p_1 \tilde{b}') (\tilde{a}, d_0)
  \]

  The first part comes from iterating Lemma 26. Also, Lemma 28 gives us:

  \[
  \begin{align*}
  \{ y \mapsto a \} + \{ z \mapsto \Sigma(z) \} + \{ v \mapsto b' \} \vdash || S_0 ||^r R_{\text{EBS}} (\tilde{a}, d_0)
  \end{align*}
  \]

Which is enough for the second part, using \( \Sigma + \{ v \mapsto b' \} \vdash || S_0 ||^r R_{\text{EBS}} (\tilde{a}, d_0) \) and Lemma 10.

We know tackle the infinite case. The proof can be separated in two successive lemmas.
From Lemma 33, $R_{EBS}$ contains a rule of the form

$$p(y, c_0(\bar{w}, \bar{z})) \Rightarrow \text{let } \bar{v} = \text{Proc Reuse } p_1 \bar{w} \text{ in } S_0$$

We choose $d = c_0(\Sigma(\bar{t}), \Sigma(\bar{z}))$, we have $\| S \|' = \text{Return } (y, c_0(\bar{t}, \bar{z}))$ and thus:

$$\Sigma(\bar{y}, c_0(\bar{t}, \bar{z})) = (\bar{a}, \bar{d})$$

$$\Sigma \vdash \text{Return } (y, c_0(\bar{t}, \bar{z})) \|_{R_{EBS}} (\bar{a}, \bar{d})$$

We also need to check $(\bar{a}, \bar{d}) \|_{R_{EBS}}^p$. For this we have the following tree:

$$p(y, c_0(\bar{w}, \bar{z})) \Rightarrow \ldots \in R_{EBS}$$

$$\Sigma' \vdash \text{let } \bar{v} = \text{Proc Reuse } p_1 \bar{w} \text{ in } S_0 \|_{R_{EBS}}^{p}$$

$$\langle \bar{a}, \bar{d} \rangle \|_{R_{EBS}}^{p}$$

where $\Sigma' = \{ y \mapsto a \} + \{ w \mapsto \Sigma(\bar{t}) \} + \{ z \mapsto \Sigma(\bar{z}) \}$. The leaf comes from our hypothesis $\Sigma \vdash S \|_{R_{EBS}}^{p}$. If the proc call $(\text{Proc } (\text{New } c_0) p_1 \bar{t})$ diverges, this is straightforward as $\Sigma(\bar{t}) = \Sigma'(\bar{w})$. If evaluating $S_0$ diverges, we go from $\Sigma$ to $\Sigma'$ using Lemma 11.

□

Lemma 39. For all $\bar{a}, c, \bar{a'}$, and $p$,

$$(\bar{a}, c(\bar{a'})) \|_{R_{EBS}}^{p} \Rightarrow \exists \bar{b}, (\bar{a}, c(\bar{a'})) \|_{R_{EBS}}^{p} \bar{b} \land \bar{b} \|_{R_{EBS}}^{p}$$

Proof. We prove this result by induction on $(\bar{a}, c(\bar{a'}))$, keeping $p$ universally quantified. We distinguish the different cases of $(\bar{a}, c(\bar{a'})) \|_{R_{EBS}}^{p}$.

- If it comes from a tree

  $$p(y, c(\bar{w}, \bar{z})) \Rightarrow \ldots \in R_{EBS}$$

  $$\Sigma \vdash \text{Proc Reuse } p_1 \bar{w} \text{ in } S \|_{R_{EBS}}^{p}$$

  $$\langle \bar{a}, c(\bar{a'}, \bar{a}) \rangle \|_{R_{EBS}}^{p}$$

  with $\Sigma = \{ y \mapsto a \} + \{ \bar{w} \mapsto \bar{a}_1 \} + \{ z \mapsto \bar{a}_1 \}$ and $\bar{a'} = (\bar{a}_1, \bar{a}_2)$, then we can use our induction hypothesis since $\bar{a}_1$ is a subterm of $(\bar{a}, c(\bar{a'}))$.

  So there is $\bar{b'}$ such that $\bar{a}_1 \|_{R_{EBS}}^{p} \bar{b'}$ and $\bar{b'} \|_{R_{EBS}}^{p}$. We choose $\bar{b} = (\bar{a}, c(\bar{b'}, \bar{a}_3))$ and we have $(\bar{a}, c(\bar{a}, \bar{a}_3)) \|_{R_{EBS}}^{p} \bar{b}$ from Lemma 26 and $\bar{b} \|_{R_{EBS}}^{p}$ from a tree similar to the one above (replacing $\bar{a}_1$ by $\bar{b'}$).

- If it comes from a tree

  $$p(y, c(\bar{w}, \bar{z})) \Rightarrow \ldots \in R_{EBS}$$

  $$\Sigma \vdash \text{Proc Reuse } p_1 \bar{w} \text{ in } S \|_{R_{EBS}}^{p}$$

  $$\langle \bar{a}, c(\bar{a}, \bar{a}_3) \rangle \|_{R_{EBS}}^{p}$$

  with $\Sigma = \{ y \mapsto a \} + \{ \bar{w} \mapsto (\bar{a}_1, \bar{a}_2) \} + \{ z \mapsto \bar{a}_3 \}$, $\Sigma' = \Sigma + \{ x \mapsto d \}$ and $\bar{a'} = (\bar{a}_1, \bar{a}_2, \bar{a}_3)$, there is two subcases.

  If $\bar{a}_2$ is not the form of $\text{Ret}_{p1}$, then Theorem 37 gives us $\bar{a}_1, a_2 \|_{R_{EBS}}^{p} \bar{a}_1, \text{Ret}_{p1}(\bar{d})$ which implies there is $\bar{a'}_1$ such that $\bar{a}_1, a_2 \|_{R_{EBS}}^{p} \bar{a}_1, a_2' \|_{R_{EBS}}^{p} \bar{a}_1, \text{Ret}_{p1}(\bar{d})$. We take $\bar{b}_1 = (\bar{a}, c(\bar{a}, \bar{a}_2, \bar{a}_3))$ and $\bar{b}_2 = (\bar{a}, a_2, \bar{a}_3)$.

  Otherwise we have $\bar{a}_2 = \text{Ret}_{p1}(\bar{d})$ from Lemma 24. Using Lemma 38 above, there is $d_0$ such that $\Sigma' \vdash \| S \|' \|_{R_{EBS}}^{p} (\bar{a}, d_0)$ and $(\bar{a}, d_0) \|_{R_{EBS}}^{p}$, where $r$ is the rule on the tree above. We choose $\bar{b}_2 = (\bar{a}, d_0)$ and can conclude $(\bar{a}, c(\bar{a'})) \|_{R_{EBS}}^{p} \bar{b}_2$ using Lemma 28.

- Lastly, if it comes from a tree

  $$p(y, c(\bar{x})) \Rightarrow S \in R_{EBS}$$

  $$\Sigma_0 \vdash S \|_{R_{EBS}}^{p}$$

  $$\langle \bar{a}, c(\bar{a'}) \rangle \|_{R_{EBS}}^{p}$$

  where $S$ does not start with a Reuse label, with $\Sigma_0 = \{ y \mapsto a \} + \{ x \mapsto a' \}$. 
Once again we use Lemma 38 and there is d such that $\Sigma_0 \vdash S \parallel \hat{\Sigma}_p \Sigma_0 \vdash \parallel \hat{\Sigma}_p \Sigma_0 \vdash (\hat{a}, d) R^{\text{REBS}}_{p/t} (\hat{a}, d) \iff (\hat{a}, c(\hat{a}')) R^{\text{REBS}}_{p/t} (\hat{a}, d)$.

\[ p(y, c(x)) := \parallel S \parallel \hat{\Sigma}_p \Sigma_0 \vdash \parallel \hat{\Sigma}_p \Sigma_0 \vdash (\hat{a}, c(\hat{a}')) R^{\text{REBS}}_{p/t} (\hat{a}, d) \]

\[ \square \]

**Theorem 40 (Div: EBS $\Rightarrow$ SS).** For all proc $p$ and terms $\hat{a}$,

$$\hat{a} R^{\text{REBS}}_{p/t} \implies \hat{a} \parallel^{\infty}_{p/t}$$

**Proof.** Given Definition 6 of $\hat{a} \parallel^{\infty}_{p/t}$, by coinduction, we want to show that $\hat{a} R^{\text{REBS}}_{p/t}$ satisfies the stated property. Thus it is sufficient to prove:

$$\forall \hat{a}, p, \exists \hat{b}, \hat{a} R^{\text{REBS}}_{p/t} \hat{b}$$

We prove this separately in Lemma 39 above. \[ \square \]

### C.7 Small-Step implies Extended Big-Step

We first certify the finite case. This is done by iterating the following concatenation lemma.

**Lemma 41 (Concatenation).** For all $\hat{a}$, $c$, $\hat{a}'$, $d$, $\hat{b}$, and $p$,

\[
\begin{align*}
& (\hat{a}, c(\hat{a}')) R^{\text{REBS}}_{p/t} (\hat{a}, d) \\
& (\hat{a}, d) R^{\text{REBS}}_{p/t} \hat{b} \\
\implies & (\hat{a}, c(\hat{a}')) R^{\text{REBS}}_{p/t} \hat{b}
\end{align*}
\]

**Proof.** Once again $(\hat{a}, c(\hat{a}')) R^{\text{REBS}}_{p/t} (\hat{a}, d)$ is defined mutually with the evaluation of skeletons $(\Sigma_0 \vdash S \parallel \hat{\Sigma}_p \Sigma_0 \vdash (\hat{a}, d))$, so we will prove two results at the same time:

- Forall $\hat{a}$, $c$, $\hat{a}'$, $d$, $\hat{b}$, $p$, $\hat{y}$, $\hat{x}$, $S$, $\Sigma$, $\hat{a} R^{\text{REBS}}_{p/t} (\hat{a}, d)$ in $\Sigma$ is defined mutually with the evaluation of skeletons $(\Sigma_0 \vdash S \parallel \hat{\Sigma}_p \Sigma_0 \vdash (\hat{a}, d))$, so we will prove two results at the same time:

\[
\begin{align*}
& (\hat{a}, c(\hat{a}')) R^{\text{REBS}}_{p/t} (\hat{a}, d) \\
& (\hat{a}, d) R^{\text{REBS}}_{p/t} \hat{b} \\
\implies & (\hat{a}, c(\hat{a}')) R^{\text{REBS}}_{p/t} \hat{b}
\end{align*}
\]

- The second result says that, if $\parallel S \parallel^{r}$ (small-step) reduces to a configuration $(\hat{a}, d)$ that (big-step) evaluates to $\hat{b}$, then we can create a big-step evaluation of $\hat{b}$ to $\hat{b}$.

We reason by mutual induction on $(\hat{a}, c(\hat{a}')) R^{\text{REBS}}_{p/t} (\hat{a}, d)$ and on $S$.

- First result, by induction on $(\hat{a}, c(\hat{a}')) R^{\text{REBS}}_{p/t} (\hat{a}, d)$.

  - If $c$ is a new constructor, the main rule $r \in R^{\text{REBS}}_{p/t}$ is of the form $p(y, c(\hat{w}, \hat{z})) := 1 \hat{u} = \text{Proc Reuse } p_1 \hat{w} \in S_0$, and we have

\[
\begin{align*}
\Sigma' & := \Sigma_0 \parallel S \parallel^{r} \\
(\hat{a}, d) & R^{\text{REBS}}_{p/t} \hat{b} \\
\end{align*}
\]

where $d = c((\hat{a}_0', \hat{a}_1', \hat{a}_2'))$, and $\Sigma_0 = \{ y \mapsto a \} \cup \{ \hat{t} \mapsto (\hat{a}_0', \hat{a}_1') \} \cup \{ \hat{z} \mapsto \hat{a}' \}$, and $\Sigma' = \Sigma_0 + \{ \hat{a} \mapsto (\hat{a}_0', \hat{a}_1') \}$.
We perform an induction on $\Sigma$. We use our induction hypothesis on the leaf, and we complete our goal as such:

$$(\ldots \vdash \ldots) \in \Rebs \quad \Sigma_1 + \text{let } \dd = \text{Proc Reuse } p_1 \ w \ \text{in } S_0 \ \parallel \Rebs \ b$$

with $\Sigma_1 = \{y \mapsto a\} + \{w \mapsto (a'_0, a'_1)\} + \{z \mapsto a'_2\}$. We can use our first induction hypothesis to combine $(a'_0, a'_1) \parallel_{p_1} (a'_0, a'_1)$ and $(\dd, a') \parallel_{\overline{b'}}$ and produce our goal, i.e., $(\dd, c((a'_0, a'_1), a'_2)) \parallel_{\overline{b'}}$

$$(\ldots \vdash \ldots) \in \Rebs \quad \Sigma_0 + \text{let } \dd = \text{Proc Reuse } p_1 \ w \ \text{in } S_0 \ \parallel \Rebs \ b$$

where we go from $\Sigma_1$ to $\Sigma_0$ with Lemma 10, since $\dd$ does not appear in $S_0$.

1. If $a'_j = \text{Ret}_p(b')$, then the small-step reduction uses the second branch. We can single out the last variable of the proc call to simplify notations:

$p(\dd, c((\dd, w), \dd)) := \text{let } \dd = \text{Proc Reuse } p_1 \ (\dd, w) \ \text{in } S_0$, with a state

$\Sigma_0 = \{y \mapsto a\} + \{w \mapsto a'_0\} + \{w \mapsto \text{Ret}_p(b')\} + \{z \mapsto a'_2\}$. Our first hypothesis then corresponds to the following tree.

2. We can now use our second induction hypothesis (with $\Sigma_0$ and the second leaf) to get $\Sigma_0 + \{v \mapsto b'\} \parallel \Rebs \ b$, which allows us to create our goal derivation:

$$(\dd, c((a'_0, \text{Ret}_p(b'))), a'_2)) \parallel_{\overline{b'}}$$

where the other leaf comes from Lemma 24.

3. If $c$ is an initial constructor, the bottom of the tree derivation is of the form:

$$p(\dd, c(\dd)) := \ldots \quad \Sigma_0 + \{v \mapsto b'\} \parallel \Rebs \ b$$

Where $r = (p(\dd, c(\dd)) := S) \in \Rebs$, $S$ does not start with a Reuse label, and $\Sigma_0 = \{y \mapsto a\} + \{x \mapsto a'\}$. We use our induction hypothesis on the leaf, and we complete our goal as such:

$$(\dd, c((a'_0, \text{Ret}_p(b')))) \parallel_{\overline{b'}}$$

Where $r = (p(\dd, c(\dd)) := S) \in \Rebs$, $S$ does not start with a Reuse label, and $\Sigma_0 = \{y \mapsto a\} + \{x \mapsto a'\}$. We use our induction hypothesis on the leaf, and we complete our goal as such:

$$(\dd, c((a'_0, \text{Ret}_p(b')))) \parallel_{\overline{b'}}$$

Where $r = (p(\dd, c(\dd)) := S) \in \Rebs$, $S$ does not start with a Reuse label, and $\Sigma_0 = \{y \mapsto a\} + \{x \mapsto a'\}$. We use our induction hypothesis on the leaf, and we complete our goal as such:
• If $S$ is of the form $\text{Return } \widetilde{t}$:

\[
\Sigma(\overline{\gamma}, \text{Ret}_p(\overline{t})) = (\overline{a}, d) \\
\Sigma \vdash \text{Return } (\overline{y}, \text{Ret}_p(\overline{t})) \inp^{\text{Res}} (\overline{a}, d) \\
(\overline{a}, d) \inp^{\text{Res}} \overline{b}
\]

implies, from Lemma 24, that we have $d = \text{Ret}_p(\overline{b})$ and so $\overline{b} = \Sigma(\overline{t})$. So we have our goal:

\[
\Sigma(\overline{t}) = \overline{b} \\
\Sigma \vdash \text{Return } \overline{t} \inp^{\text{Res}} \overline{b}
\]

• If $S$ is of the form $\text{Branch } (S_1, \ldots, S_n)$, using the induction hypothesis with $S_i$:

\[
\Sigma \vdash S_i \inp^{\text{Res}} \overline{b} \\
\Sigma \vdash \text{Branch } (\parallel S_1 \parallel', \ldots, \parallel S_n \parallel') \inp^{\text{Res}} (\overline{a}, d) \\
(\overline{a}, d) \inp^{\text{Res}} \overline{b}
\]

• If $S$ is of the form $\text{let } \overline{a} = K \text{ in } S_0$, where $K$ is a filter or a return, using the induction hypothesis with $S_0$:

\[
\Sigma \vdash \parallel \overline{b} \parallel' \\
\Sigma \vdash \text{let } \overline{a} = K \text{ in } S_0 \parallel' \inp^{\text{Res}} (\overline{a}, d) \\
(\overline{a}, d) \inp^{\text{Res}} \overline{b}
\]

• If $S$ is of the form $\text{let } \overline{a} = \text{Proc } (\text{New } c_0) \ p_1 \overline{t} \text{ in } S_0$, then from Lemma 33, $\text{Res}$ contains a rule of the form $p(\overline{y}, c_0(\overline{w}, \overline{z})) \models \text{let } \overline{a} = \text{Proc } p_1 \overline{w} \text{ in } S_0$. We have:

\[
\Sigma(\overline{y}, c_0(\overline{t}, \overline{z})) = (\overline{a}, d) \\
\Sigma \vdash \text{Return } (\overline{y}, c_0(\overline{t}, \overline{z})) \inp^{\text{Res}} (\overline{a}, d) \\
(\overline{a}, d) \inp^{\text{Res}} \overline{b}
\]

From which we can deduce $d = c_0(\Sigma(\overline{t}), \Sigma(\overline{z}))$, and our second hypothesis corresponds, with $\Sigma' = \{ y \mapsto a \} + \{ w \mapsto \Sigma(\overline{t}) \} + \{ z \mapsto \Sigma(\overline{b}) \}$, to a tree of the form:

\[
p(\overline{y}, c_0(\overline{w}, \overline{z})) = \ldots \in \text{Res} \\
\Sigma' \vdash \text{Proc } p_1 \overline{w} \inp^{\text{Res}} \overline{b} \\
\Sigma' \vdash \text{let } \overline{a} = \text{Proc } p_1 \overline{w} \in S_0 \inp^{\text{Res}} \overline{b}
\]

Note that $\Sigma'(\overline{w}) = \Sigma(\overline{t})$. Also, using Lemma 10, we can deduce $\Sigma + \{ v \mapsto b' \} \vdash S_0 \inp^{\text{Res}} \overline{b}$ and create our goal derivation:

\[
\Sigma \vdash \text{Proc } (\text{New } c_0) \ p_1 \overline{t} \inp^{\text{Res}} \overline{b'} \\
\Sigma \vdash \text{let } \overline{a} = \text{Proc } p_1 \overline{t} \text{ in } S_0 \inp^{\text{Res}} \overline{b}
\]

\[\square\]

Theorem 42 (SS ⇒ EBS).
\[\forall \overline{a}, c, \overline{a}', \overline{b}, p, \ (\overline{a}, c(\overline{a}')) \inp^{\text{Res}} (\overline{a}, \text{Ret}_p(\overline{b})) \Rightarrow (\overline{a}, c(\overline{a}')) \inp^{\text{Res}} \overline{b}
\]

Proof. We prove it by induction on the number of small-step reductions. If $c(\overline{a}) = \text{Ret}_p(\overline{b})$, i.e. there is zero small steps, the result holds from Lemma 24. Otherwise, the induction case comes directly from Lemma 41 above. \[\square\]

We now certify the infinite case. This time, we cannot use a concatenation result. Instead, we check the infinite sequence satisfies the properties of the coinductive interpretation. Before this, we need the following small lemma to split the infinite sequence when needed.
Lemma 43. Assuming \((p(\bar{y}, c((\bar{w}, w), \bar{z})) := 1 \text{let } \bar{v} = \text{Proc Reuse } p_1(\bar{w}, w) \text{ in } S) \in R_{\text{EBS}}\), if we have a small-step divergence 
\[ (b, c((\bar{a}, a_0), b')) \xrightarrow{\infty} p \]
then either the first proc call diverges
\[ (\bar{a}, a_0) \xrightarrow{\infty} p \]
or the first proc call finishes and the rest of the computation diverges
\[ 2a', \begin{cases} (\bar{a}, a_0) \{(\|_{R_p}^{\text{Reus}})^* (\bar{a}, \text{Ret}_p 1(\bar{a}'))\} \\ (\bar{b}, c((\bar{a}, \text{Ret}_p 1(\bar{a}')), b')) \xrightarrow{\infty} p \end{cases} \]

**Proof.** We use the excluded middle axiom, and perform a case disjunction on whether there is a tuple of the form \((\bar{b}, c((\bar{a}, \text{Ret}_p 1(\bar{a}')), b'))\) in the infinite sequence of reduction.

- If there is, we take the first such tuple and we have:
  \[ (\bar{b}, c((\bar{a}, a_0), b')) \{(\|_{R_p}^{\text{Reus}})^* (\bar{b}, c((\bar{a}, \text{Ret}_p 1(\bar{a}')), b'))\} \xrightarrow{\infty} p \]

Now we show by induction on \((\bar{b}, c((\bar{a}, a_0), b')) \{(\|_{R_p}^{\text{Reus}})^*(\bar{b}, c((\bar{a}, \text{Ret}_p 1(\bar{a}')), b'))\}) that we have \((\bar{a}, a_0) \{(\|_{R_p}^{\text{Reus}})^*(\bar{a}, \text{Ret}_p 1(\bar{a}')))\). The base case (zero steps) is trivial. For the induction case, note that \(a_0\) cannot be of the form \(\text{Ret}_p 1(\ldots)\) as we chose \((\bar{b}, c((\bar{a}, \text{Ret}_p 1(\bar{a}')), b'))\) to be the first of this form. We then use Lemma 27 to transform the first step, and the induction hypothesis to transform the rest.

- If there is no such tuple, we show \((\bar{a}, a_0) \xrightarrow{\infty} p\) by coinduction. We cut our hypothesis and there is \(\bar{T}\) such that \((\bar{b}, c((\bar{a}, a_0), b')) \{(\|_{R_p}^{\text{Reus}})^{\infty} \bar{T}\} \xrightarrow{\infty} p\).

From Lemma 27, we have \(\bar{T} = (\bar{b}, c((\bar{a}, a_0), b'))\) with \((\bar{a}, a_0) \{(\|_{R_p}^{\text{Reus}})^{\infty} \bar{T}\}\). Also, \((\bar{b}, c((\bar{a}, a_0'), b')) \xrightarrow{\infty} p\) still has the property of not having any intermediate tuple of the form \((\bar{b}, c((\bar{a}, \text{Ret}_p 1(\bar{a}')), b'))\), so we can use our induction hypothesis with it to conclude.

\[ \Box \]

**Theorem 44 (Div: SS \Rightarrow EBS).** For all proc \(p\) and terms \(\bar{a}\),
\[ \bar{a} \xrightarrow{\infty} p \quad \Rightarrow \quad \bar{a} \|_{R_p}^{\text{EBS}} \]

**Proof.** Since \(\bar{a} \|_{R_p}^{\text{EBS}}\) is defined mutually with \(\Sigma \vdash S \|_{R_p}^{\text{EBS}}\), we show two properties at the same time:

- \(\forall \bar{a}, p, (\bar{a} \xrightarrow{\infty} p) \quad \Rightarrow \quad \bar{a} \|_{R_p}^{\text{EBS}}\)

- \(\forall p, \bar{y}, c, \bar{x}, S, \Sigma, \bar{b}, \bar{T}, \begin{cases} r = (p(\bar{y}, c(\bar{x}))) := S_0) \in R_{\text{EBS}} \\ S \vdash S_0 \quad \Rightarrow \quad \Sigma \vdash S \|_{R_p}^{\text{RSS}} b \quad \xrightarrow{\infty} p \quad \bar{b} \|_{R_p}^{\text{R}} \quad S \text{ has no Reuse label} \end{cases} \]

We note the predicates
\[ Q = \{(\bar{a}, p) \mid \bar{a} \xrightarrow{\infty} p\} \]
\[ Q' = \{(\Sigma, S) \mid \exists p, \bar{b}, (p(\ldots)) := S_0) \in R_{\text{EBS}}, \text{ such that} \quad \Sigma \vdash S \|_{R_p}^{\infty} b \quad \bar{b} \xrightarrow{\infty} p \quad S \text{ has no Reuse label} \} \]

To prove both these results by coinduction, we show that the two predicates satisfy the properties corresponding to the rules of Figure 9. I.e., for every element of \(Q\) and \(Q'\), we can create a derivation of the goal statement using at least one rule of Figure 9 and using elements of \(Q\) and \(Q'\) as leaves.

- For elements of \(Q\). We assume \((\bar{a}, c(\bar{a}')) \xrightarrow{\infty} p\).
  - If \(c\) is an initial constructor, then \(R_{\text{EBS}}\) contains a rule \(r\) of the form \(p(\bar{y}, c(\bar{x})) := S_0)\) where \(S_0\) has no label \(\text{Reuse}\). We note \(\Sigma = \{y \mapsto a\} + \{x \mapsto a'\}\). Splitting the first small-step of the infinite reduction, we have \(\bar{b}\) such that \(\Sigma \vdash S \|_{R_p}^{\text{RSS}} b\) and \(\bar{b} \xrightarrow{\infty} p\). We immediately have \((\Sigma, S_0) \in Q'\) using \(r\) and \(S_0 \vdash S_0\), so we can start constructing a derivation as follows.
    \[ (p(\bar{y}, c(\bar{x})) := S_0) \in R_{\text{EBS}}, \quad (\Sigma, S_0) \in Q' \quad \xrightarrow{\text{DIV-TUPLE}} (\bar{a}, c(\bar{a}')) \|_{R_p}^{\text{EBS}} \]

- If \(c\) is a new constructor, then \(R_{\text{EBS}}\) contains a rule \(r\) of the form
  \[ p(\bar{y}, c(\bar{w}, \bar{z})) := 1 \text{let } \bar{v} = \text{Proc Reuse } p_1(\bar{w}, w) \text{ in } S_0 \]
  where \(S_0\) has no label \(\text{Reuse}\). We have \(\bar{a}' = (\bar{a}_1, \bar{a}_2)\), we note \(\Sigma = \{y \mapsto a\} + \{w \mapsto a_1\} + \{z \mapsto a_2\}\). We use Lemma 43 to perform a case disjunction on the behavior of \(\bar{a}, c(\bar{a}_1, \bar{a}_2) \xrightarrow{\infty} p\).
If $\tilde{a}_1 \rightarrow^p \tilde{p}_1$, then we can start constructing our goal as such:

$$
\begin{align*}
& (\tilde{a}_1, p_1) \in Q \\
& \Sigma \vdash \text{Proc } p_1 \ 	ilde{w}^{\mathsf{RS}} \text{ Div-Pc} \\
& \rho(\tilde{y}, c(\tilde{w}, \tilde{z})) := \ldots \in \mathcal{R}_{\mathsf{EBS}} \\
& \Sigma \vdash \text{let } \tilde{v} = \text{Proc } p_1 \ 	ilde{w} \text{ in } S_0 \ 	ilde{w}^{\mathsf{RS}} \text{ Div-LETL} \\
& \tilde{a}, c(\tilde{a}_1, \tilde{a}_2) \ 	ilde{w}^{\mathsf{RS}}_p \\
\end{align*}
$$

Else there is $\tilde{a}_1'$ such that $\tilde{a}_1 \overset{\mathsf{RS}}{\rightarrow} (\ldots \text{Ret } p_1(\tilde{a}_1'))$ and $(\tilde{a}, c(\ldots \text{Ret } p_1(\tilde{a}_1'), \tilde{a}_2)) \rightarrow^p_\Sigma$. Using Theorem 42 on the first point, we get $\tilde{a}_1 \overset{\mathsf{RS}}{\rightarrow} \tilde{a}_1'$. Using Lemma 29 on the second point (after splitting a step), we get there is $\tilde{b}$ such that $\Sigma' \vdash || S_0 ||' \overset{\mathsf{RS}}{\rightarrow} \tilde{b}$ and $\tilde{b} \rightarrow^p_\Sigma$, where $\Sigma' = \{ y \mapsto a_1 \} \cup \{ z \mapsto a_2 \} \cup \{ v \mapsto a_1' \}$. We can add the mapping of the unused variables $\tilde{w}$ with Lemma 10, and so $(\Sigma + \{ v \mapsto a_1' \}, S_0) \in Q'$ using rule $r$, and we can construct our goal as such:

$$
\begin{align*}
& \Sigma \vdash \text{Proc } p_1 \ 	ilde{w}^{\mathsf{RS}}_p \tilde{a}_1' \\
& (\Sigma + \{ v \mapsto a_1' \}, S_0) \in Q' \text{ Div-LETL} \\
& \rho(\tilde{y}, c(\tilde{w}, \tilde{z})) := \ldots \in \mathcal{R}_{\mathsf{EBS}} \\
& \Sigma \vdash \text{let } \tilde{v} = \text{Proc } p_1 \ 	ilde{w} \text{ in } S_0 \ 	ilde{w}^{\mathsf{RS}}_p \text{ Div-TUPLE} \\
& \tilde{a}, c(\tilde{a}_1, \tilde{a}_2) \ 	ilde{w}^{\mathsf{RS}}_p \\
\end{align*}
$$

- For elements of $Q'$. We assume:

$$
\begin{align*}
& S \in S_0 \\
& \Sigma \vdash || S ||' \overset{\mathsf{RS}}{\rightarrow} \tilde{b} \\
& \tilde{b} \rightarrow^p_\Sigma \\
& S \text{ has no Reuse label}
\end{align*}
$$

First, we can see certain cases for $S$ are not possible. $S$ cannot be a procedure or filter, because we delay returns to create the set $\mathcal{R}_{\mathsf{EBS}}$. Also, $S$ cannot be a return, because $\tilde{b}$ would be of the form $(\ldots \text{Ret } p(\ldots))$ and $\tilde{b} \rightarrow^p_\Sigma$ contradicts this.

- If $S = \text{Branch } (S_1, \ldots, S_n)$, then $\Sigma \vdash \text{Branch } (|| S_1 ||', \ldots, || S_n ||') \overset{\mathsf{RS}}{\rightarrow} \tilde{b}$ implies there is $S_i$ such that $\Sigma \vdash || S_i ||' \overset{\mathsf{RS}}{\rightarrow} \tilde{b}$. We have $(\Sigma, S_i) \in Q'$ using the same rule and terms, since $S_i \in S \in S_0$. We can then start the derivation of the goal as follows.

$$
\begin{align*}
& S_i \in (S_1, \ldots, S_n) \\
& (\Sigma, S_i) \in Q' \text{ Div-BR} \\
& \Sigma \vdash \text{Branch } (S_1, \ldots, S_n) \tilde{w}^{\mathsf{RS}}_p \text{ Div-LETL}
\end{align*}
$$

Note that we have $\Sigma \vdash K \overset{\mathsf{RS}}{\rightarrow} \tilde{b}' \iff \Sigma \vdash K \overset{\mathsf{RS}}{\rightarrow} \tilde{b}'$ for filters and returns, as evaluating these skeletom does not look up any rule.

- If $S = (\text{let } \tilde{v} = \text{Proc } (\text{New } c_0) \ p_1 \ i \text{ in } S')$ then, from Lemma 33, $\mathcal{R}_{\mathsf{EBS}}$ contains a rule $r'$ of the form

$$
\begin{align*}
& \rho(\tilde{y}, c_0(\tilde{w}, \tilde{z})) := \text{let } \tilde{v} = \text{Proc } p_1 \ 	ilde{w} \text{ in } S' \\
\end{align*}
$$

Let $\tilde{a}_0 = \Sigma(\tilde{y})$, $\tilde{a}_1 = \Sigma(\tilde{i})$, and $\tilde{a}_2 = \Sigma(\tilde{z})$. We have $|| S ||' = \text{Return } (\tilde{y}, c_0(\tilde{t}, \tilde{z}))$ and so $\tilde{b} = (\tilde{a}_0, c_0(\tilde{a}_1, \tilde{a}_2))$. We use Lemma 43 to perform a case disjunction on the behavior of $\tilde{a}_0, c_0(\tilde{a}_1, \tilde{a}_2)$.

- If $\tilde{a}_1 \rightarrow^p_\Sigma$, then we can start constructing our goal as such:

$$
\begin{align*}
& (\tilde{a}_1, p_1) \in Q \\
& \Sigma \vdash \text{Proc } p_1 \ i \tilde{t}^{\mathsf{RS}} \text{ Div-Pc} \\
& \Sigma \vdash \text{let } \tilde{v} = \text{Proc } (\text{New } c_0) \ p_1 \ i \text{ in } S' \tilde{w}^{\mathsf{RS}}_p \text{ Div-LETL}
\end{align*}
$$

- Else there is $\tilde{a}'_1$ such that $\tilde{a}_1 \overset{\mathsf{RS}}{\rightarrow} (\ldots \text{Ret } p_1(\tilde{a}_1'))$ and $(\tilde{a}_0, c_0(\ldots \text{Ret } p_1(\tilde{a}_1'), \tilde{a}_2)) \rightarrow^p_\Sigma$. Using Theorem 42 on the first point, we get $\tilde{a}_1 \overset{\mathsf{RS}}{\rightarrow} \tilde{a}_1'$. Using Lemma 29 on the second point (after splitting a step), we get there is $\tilde{b}'$ such that $\Sigma' \vdash || S' ||' \overset{\mathsf{RS}}{\rightarrow} \tilde{b}'$ and $\tilde{b}' \rightarrow^p_\Sigma$, where $\Sigma' = \{ y \mapsto a_0 \} \cup \{ z \mapsto a_2 \} \cup \{ v \mapsto a_1' \}$. We can add the mapping of the unused variables $\tilde{w}$ with Lemma 10, and so $(\Sigma + \{ v \mapsto a_1' \}, S') \in Q'$ using rule $r$, and we can construct our goal as such:

$$
\begin{align*}
& \Sigma \vdash \text{Proc } p_1 \ 	ilde{w}^{\mathsf{RS}}_p \tilde{a}_1' \\
& (\Sigma + \{ v \mapsto a_1' \}, S') \in Q' \text{ Div-LETL} \\
& \rho(\tilde{y}, c(\tilde{w}, \tilde{z})) := \ldots \in \mathcal{R}_{\mathsf{EBS}} \\
& \Sigma \vdash \text{let } \tilde{v} = \text{Proc } p_1 \ 	ilde{w} \text{ in } S_0 \ 	ilde{w}^{\mathsf{RS}}_p \text{ Div-TUPLE} \\
& \tilde{a}, c(\tilde{a}_1, \tilde{a}_2) \ 	ilde{w}^{\mathsf{RS}}_p \\
\end{align*}
$$
using rule $r'$, and we can construct our goal as such:

$$
\frac{
\begin{array}{c}
\Sigma \vdash \text{Proc} \ p_1 \ i \ \parallel_{\text{RES}} \ a'_1 \\
\Sigma \vdash \text{let } \sigma = \text{Proc} (\text{New} c_0) \ p_1 \ i \ \text{in} \ S' \ \parallel_{\text{RES}}
\end{array}
}{
\Sigma \vdash \text{let } \sigma = \text{Proc} (\text{New} c_0) \ p_1 \ i \ \text{in} \ S' \ \parallel_{\text{RES}}
} \quad \text{Div-LetR}
$$