Environmental Bisimulations for Delimited-Control Operators with Dynamic Prompt Generation

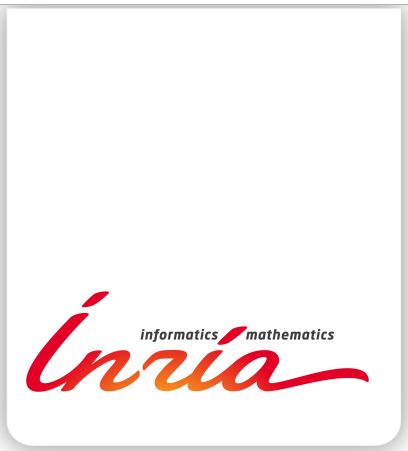
Andrés Aristizábal, Dariusz Biernacki, Sergueï Lenglet, Piotr Polesiuk

Environmental Bisimulations for Delimited-Control Operators with Dynamic Prompt Generation

Andrés Aristizábal, Dariusz Biernacki, Sergueï Lenglet, Piotr Polesiuk

RESEARCH REPORT
N° 8905
April 2016
Project-Team Pareo

ISSN 0249-6399 ISRN INRIA/RR--8905--FR+ENG



Environmental Bisimulations for Delimited-Control Operators with Dynamic Prompt Generation

Andrés Aristizábal*, Dariusz Biernacki†, Sergueï Lenglet‡, Piotr Polesiuk§

Project-Team Pareo

Research Report n° 8905 — April 2016 — 24 pages

Abstract: We present sound and complete environmental bisimilarities for a variant of Dybvig et al.'s calculus of multi-prompted delimited-control operators with dynamic prompt generation. The reasoning principles that we obtain generalize and advance the existing techniques for establishing program equivalence in calculi with single-prompted delimited control.
The basic theory that we develop is presented using Madiot et al.'s framework that allows for smooth integration and composition of up-to techniques facilitating bisimulation proofs. We also generalize the framework in order to express environmental bisimulations that support equivalence proofs of evaluation contexts representing continuations. This change leads to a novel and powerful up-to technique enhancing bisimulation proofs in the presence of control operators.

Key-words: Delimited continuation, dynamic prompt generation, contextual equivalence, environmental bisimulation, up-to technique

* Pontificia Universidad Javeriana Cali, Cali, Columbia
† University of Wrocław, Wrocław, Poland
‡ Université de Lorraine, Nancy, France
§ University of Wrocław, Wrocław, Poland

RESEARCH CENTRE
NANCY – GRAND EST

615 rue du Jardin Botanique
CS20101
54603 Villers-lès-Nancy Cedex

Bismulations environnementales pour les opérateurs de contrôle délimité avec génération dynamique de prompts

Résumé : Nous proposons des bisimilarités environnementales correctes et complètes pour une variante du calcul de Dybvig et al. avec opérateurs de contrôle délimité utilisant des prompts multiples et la génération dynamique de prompts. Nous étendons ainsi les techniques existantes pour prouver l'équivalence de programmes dans les calculs avec opérateurs de contrôle délimité à un seul prompt.

La théorie que nous développons repose sur le canevas de Madiot et al. qui permet l'intégration et la composition facile de techniques modulo, ces dernières simplifiant les preuves d'équivalences par bisimulation. Nous généralisons ce canevas de façon à pouvoir définir des bisimulations environnementales qui prouvent équivalents des contextes d'exécution représentant des continuations. Avec ce changement, nous obtenons une nouvelle technique modulo particulièrement intéressante en présence d'opérateurs de contrôle.

Mots-clés : Continuations délimitées, génération dynamique de prompts, équivalence contextuelle, bisimilarité environmentale, techniques modulo

1 Introduction

Control operators for delimited continuations, introduced independently by Felleisen [11] and by Danvy and Filinski [8], allow the programmer to delimit the current context of computation and to abstract such a delimited context as a first-class value. It has been shown that all computational effects are expressible in terms of delimited continuations [12], and so there exists a large body of work devoted to this canonical control structure, including our work on a theory of program equivalence for the operators shift and reset [4, 5, 6].

In their paper on type-directed partial evaluation for typed λ-calculus with sums, Balat et al. [1] have demonstrated that Gunter et al.'s delimited-control operators set and cupto [14], that support multiple prompts along with dynamic prompt generation, can have a practical advantage over single-prompted operators such as shift and reset. Delimited-control operators with dynamically-generated prompts are now available in several production programming languages such as OCaml [18] and Racket [13], and they have been given formal semantic treatment in the literature. In particular, Dybvig et al. [10] have proposed a calculus that extends the call-by-value λ-calculus with several primitives that allow for: fresh-prompt generation, delimiting computations with a prompt, abstracting control up to the corresponding prompt, and composing captured continuations. Dybvig et al.'s building blocks were shown to be able to naturally express most of other existing control operators and as such they form a general framework for studying delimited continuations. Reasoning about program equivalence in Dybvig et al.'s calculus is considerably more challenging than in single-prompted calculi: one needs to reconcile control effects with the intricacies introduced by fresh-prompt generation and local visibility of prompts.

In this article we investigate the behavioral theory of a slightly modified version of Dybvig et al.'s calculus that we call the $\lambda_{\mathcal{G}\#}$-calculus. One of the most natural notions of program equivalence in languages based on the λ-calculus is *contextual equivalence*: two terms are contextually equivalent if we cannot distinguish them when evaluated within any context. The quantification over contexts makes this relation hard to use in practice, so it is common to characterize it using simpler relations, like coinductively defined *bisimilarities*. As pointed out in [20], among the existing notions of bisimilarities, *environmental bisimilarity* [28] is the most appropriate candidate to characterize contextual equivalence in a calculus with generated resources, such as prompts in $\lambda_{\mathcal{G}\#}$. Indeed, this bisimilarity features an environment which accumulates knowledge about the terms we compare. This is crucial in our case to remember the relationships between the prompts generated by the compared programs. We therefore define environmental bisimilarities for $\lambda_{\mathcal{G}\#}$, as well as *up-to techniques*, which are used to simplify the equivalence proof of two given programs. We do so using the recently developed framework of Madiot et al. [24, 23], where it is simpler to prove that a bisimilarity and its up-to techniques are *sound* (i.e., imply contextual equivalence).

After presenting the syntax, semantics, and contextual equivalence of the calculus in Section 2, in Section 3 we define a sound and complete environmental bisimilarity and its corresponding up-to techniques. In particular, we define a bisimulation *up to context*, which allows to forget about a common context when comparing two terms in a bisimulation proof. The bisimilarity we define is useful enough to prove, e.g., the folklore theorem about delimited control [3] expressing that the static delimited-control operators shift and reset [8] can be simulated by the dynamic control operators control and prompt [11]. The technique, however, in general requires a cumbersome analysis of terms of the form $E[e]$, where E is a captured evaluation context and e is any expression (not necessarily a value). We therefore define in Section 4 a refined bisimilarity, called $\star$-bisimilarity, and a more expressive bisimulation up to context, which allows to factor out a context built with captured continuations. Proving the soundness of these two relations requires us to extend Madiot et al.'s framework. These results non-trivially generalize and considerably improve the existing techniques [6]. Finally, we discuss related work and conclude in Section 5. Appendix A contains the proofs for Section 3, while Appendix B contains the proofs for Section 4.

2 The Calculus $\lambda_{\mathcal{G}\#}$

The calculus we consider, called $\lambda_{\mathcal{G}\#}$, extends the call-by-value λ-calculus with four building blocks for constructing delimited-control operators as first proposed by Dybvig et al. [10]. [1]

Syntax. We assume we have a countably infinite set of term variables, ranged over by x, y, z, and k, as well as a countably infinite set of prompts, ranged over by p, q. Given an entity denoted by a meta-variable m, we write $\overrightarrow{m}$ for a (possibly empty) sequence of such entities. Expressions (e), values (v), and evaluation contexts (E) are defined as follows:

$$\begin{array}{rcll} e & ::= & v \mid e\, e \mid \mathcal{P}x.e \mid \#_v e \mid \mathcal{G}_v x.e \mid v \triangleleft e & \text{(expressions)} \\ v & ::= & x \mid \lambda x.e \mid p \mid \ulcorner E \urcorner & \text{(values)} \\ E & ::= & \Box \mid E\, e \mid v\, E \mid \#_p E & \text{(evaluation contexts)} \end{array}$$

Values include captured evaluation contexts $\ulcorner E \urcorner$, representing delimited continuations, as well as generated prompts p. Expressions include the four building blocks for delimited control: $\mathcal{P}x.e$ is a prompt-generating construct, where x represents a fresh prompt locally visible in e, $\#_v e$ is a control delimiter for e, $\mathcal{G}_v x.e$ is a continuation grabbing or capturing construct, and $v \triangleleft e$ is a throw construct.

Evaluation contexts, in addition to the standard call-by-value contexts, include delimited contexts of the form $\#_p E$, and they are interpreted outside-in. We use the standard notation $E[e]$ ($E[E']$) for plugging a context E with an expression e (with a context E'). Evaluation contexts are a special case of (general) contexts, understood as a term with a hole and ranged over by C.

The expressions $\lambda x.e$, $\mathcal{P}x.e$, and $\mathcal{G}_v x.e$ bind x; we adopt the standard conventions concerning α-equivalence. If x does not occur in e, we write $\lambda\_.e$, $\mathcal{P}\_.e$, and $\mathcal{G}_v\_.e$. The set of free variables of e is written $\mathsf{fv}(e)$; a term e is called closed if $\mathsf{fv}(e) = \emptyset$. We extend these notions to evaluation contexts. We write $\#(e)$ (or $\#(E)$) for the set of all prompts that occur in e (or E respectively). The set $\mathsf{sp}(E)$ of surrounding prompts in E is the set of all prompts guarding the hole in E, defined as $\{p \mid \exists E_1, E_2, E = E_1[\#_p E_2]\}$.

Reduction semantics. The reduction semantics of $\lambda_{\mathcal{G}\#}$ is given by the following rules:

$$\begin{array}{rcll} (\lambda x.e)\, v & \to & e\{v/x\} & \\ \#_p v & \to & v & \\ \#_p E[\mathcal{G}_p x.e] & \to & e\{\ulcorner E \urcorner / x\} & p \notin \mathsf{sp}(E) \\ \ulcorner E \urcorner \triangleleft e & \to & E[e] & \\ \mathcal{P}x.e & \to & e\{p/x\} & p \notin \#(e) \end{array}$$

$$\textsc{Compatibility}\quad \frac{e_1 \to e_2 \qquad \mathsf{fresh}(e_2, e_1, E)}{E[e_1] \to E[e_2]}$$

The first rule is the standard β_v-reduction. The second rule signals that a computation has been completed for a given prompt. The third rule abstracts the evaluation context up to the dynamically nearest control delimiter matching the prompt of the grab operator. In the fourth rule, an expression is thrown (plugged, really) to the captured context. Note that, like in Dybvig et al.'s calculus, the expression e is not evaluated before the throw operation takes place. In the last rule, a prompt p is generated under the condition that it is fresh for e.

The compatibility rule needs a side condition, simply because a prompt that is fresh for e may not be fresh for a surrounding evaluation context. Given three entities m_1, m_2, m_3 for which $\#$ is defined, we write $\mathsf{fresh}(m_1, m_2, m_3)$ for the condition $(\#(m_1) \setminus \#(m_2)) \cap \#(m_3) = \varnothing$, so the side condition states that E must not mention prompts generated in the reduction step $e_1 \to e_2$. This approach differs from the previous work on bisimulations for resource-generating constructs [22, 21, 29, 30, 31, 2, 25], where configurations of the operational semantics contain explicit information about the resources, typically represented by a set. We find our way of proceeding less invasive to the semantics of the calculus.

[1] Dybvig et al.'s control operators slightly differ from their counterparts considered in this work, but they can be straightforwardly macro-expressed in the $\lambda_{\mathcal{G}\#}$-calculus.

When reasoning about reductions in the $\lambda_{\mathcal{G}\#}$-calculus, we rely on the notion of *permutation* (a bijection on prompts), ranged over by σ, which allows to reshuffle the prompts of an expression to avoid potential collisions (e with prompts permuted by σ is written $e\sigma$). E.g., we can use the first item of the following lemma before applying the compatibility rule, to be sure that any prompt generated by $e_1 \to e_2$ is not in $\#(E)$.

Lemma 1. *Let σ be a permutation.*

- *If $e_1 \to e_2$ then $e_1\sigma \to e_2\sigma$.*
- *For any entities m_1, m_2, m_3, we have* $\mathsf{fresh}(m_1, m_2, m_3)$ *iff* $\mathsf{fresh}(m_1\sigma, m_2\sigma, m_3\sigma)$.

A closed term e either uniquely, up to permutation of prompts, reduces to a term e', or it is a normal form (i.e., there is no e'' such that $e \to e''$). In the latter case, we distinguish values, control-stuck terms $E[\mathcal{G}_p k.e]$ where $p \notin \mathsf{sp}(E)$, and the remaining expressions that we call errors (e.g., $E[p\, v]$ or $E[\mathcal{G}_{\lambda x.e} k.e']$). We write $e_1 \to^* e_2$ if e_1 reduces to e_2 in many (possibly 0) steps, and we write $e \not\to$ when a term e diverges (i.e., there exists an infinite sequence of reductions starting with e) or when it reduces (in many steps) to an error.

When writing examples, we use the fixed-point operator fix, let-construct, conditional if along with boolean values true and false, and sequencing ";", all defined as in the call-by-value λ-calculus. We also use the diverging term $\Omega \stackrel{\mathsf{def}}{=} (\lambda x.x\,x)\,(\lambda x.x\,x)$, and we define an operator $\stackrel{?}{=}$ to test the equality between prompts, as follows:

$$e_1 \stackrel{?}{=} e_2 \quad \stackrel{\mathsf{def}}{=} \quad \mathsf{let}\ x = e_1\ \mathsf{in}\ \mathsf{let}\ y = e_2\ \mathsf{in}\ \#_x((\#_y \mathcal{G}_{x\_}.\mathsf{false});\mathsf{true})$$

If e_1 and e_2 evaluate to different prompts, then the grab operator captures the context up to the outermost prompt to throw it away, and false is returned; otherwise, true is returned.

Contextual equivalence. We now define formally what it takes for two terms to be considered equivalent in the $\lambda_{\mathcal{G}\#}$-calculus. First, we characterize when two closed expressions have equivalent observable actions in the calculus, by defining the following relation $\sim$.

Definition 1. We say that e_1 and e_2 have equivalent observable actions, noted $e_1 \sim e_2$, if

1. $e_1 \to^* v_1$ iff $e_2 \to^* v_2$,
2. $e_1 \to^* E_1[\mathcal{G}_{p_1} x.e_1']$ iff $e_2 \to^* E_2[\mathcal{G}_{p_2} x.e_2']$, where $p_1 \notin \mathsf{sp}(E_1)$ and $p_2 \notin \mathsf{sp}(E_2)$,
3. $e_1 \not\to$ iff $e_2 \not\to$.

We can see that errors and divergence are treated as equivalent, which is standard.

Based on $\sim$, we define *contextual equivalence* as follows.

Definition 2 (Contextual equivalence)**.** Two closed expressions e_1 and e_2 are contextually equivalent, written, $e_1 \equiv_E e_2$, if for all E such that $\#(E) = \varnothing$, we have $E[e_1] \sim E[e_2]$.

Contextual equivalence can be extended to open terms in a standard way: if $\mathsf{fv}(e_1) \cup \mathsf{fv}(e_2) \subseteq \overrightarrow{x}$, then $e_1 \equiv_E e_2$ if $\lambda\overrightarrow{x}.e_1 \equiv_E \lambda\overrightarrow{x}.e_2$. We test terms using only promptless contexts, because the testing context should not use prompts that are private for the tested expressions. For example, the expressions $\lambda f.f\,p\,q$ and $\lambda f.f\,q\,p$ should be considered equivalent if nothing is known from the outside about p and q. As common in calculi with resource generation [30, 29, 28], testing with evaluation contexts (as in $\equiv_E$) is not the same as testing with all contexts: we have $\mathcal{P}x.x \equiv_E p$, but these terms can be distinguished by

$$\mathsf{let}\ f = \lambda x.\Box\ \mathsf{in}\ \mathsf{if}\ f\ \lambda x.x \stackrel{?}{=} f\ \lambda x.x\ \mathsf{then}\ \Omega\ \mathsf{else}\ \lambda x.x,$$

In the rest of the article, we show how to characterize $\equiv_E$ with environmental bisimilarities.[2]

[2] If $\equiv_C$ is the contextual equivalence testing with all contexts, then we can prove that $e_1 \equiv_C e_2$ iff $\lambda x.e_1 \equiv_E \lambda x.e_2$, where x is any variable. We therefore obtain a proof method for $\equiv_C$ as well.

$$\frac{e_1 \to e_2 \qquad \mathsf{fresh}(e_2, e_1, \Gamma)}{(\Gamma, e_1) \xrightarrow{\tau} (\Gamma, e_2)} \qquad \frac{\Gamma_i = \lambda x.e}{\Gamma \xrightarrow{\lambda, i, \mathbb{C}_\mathsf{v}} (\Gamma, e\{\mathbb{C}_\mathsf{v}[\Gamma]/x\})} \qquad \frac{}{\Gamma \xrightarrow{\mathsf{v}} \Gamma} \qquad \frac{\Gamma_i = \ulcorner E \urcorner}{\Gamma \xrightarrow{\ulcorner \cdot \urcorner, i, \mathbb{C}} (\Gamma, E[\mathbb{C}[\Gamma]])}$$

$$\frac{\Gamma_i = p \qquad \Gamma_j = p}{\Gamma \xrightarrow{\#, i, j} \Gamma} \qquad \frac{p \notin \#(\Gamma)}{\Gamma \xrightarrow{\#} (\Gamma, p)} \qquad \frac{p \notin \mathsf{sp}(E) \qquad \mathbb{E}[E[\mathcal{G}_p x.e], \Gamma] \xrightarrow{=} e'}{(\Gamma, E[\mathcal{G}_p x.e]) \xrightarrow{\mathbb{E}} (\Gamma, e')}$$

Figure 1: Labeled Transition System for $\lambda_{\mathcal{G}\#}$

3 Environmental Bisimilarity

In this section, we propose a first characterization of $\equiv_E$ using an environmental bisimilarity. We express the bisimilarity in the style of [24], using a so called first-order labeled transition system (LTS), to factorize the soundness proofs of the bisimilarity and its up-to techniques. We start by defining the LTS and its corresponding bisimilarity.

3.1 Labeled Transition System and Bisimilarity

In the original formulation of environmental bisimulation [28], two expressions e_1 and e_2 are compared under some environment $\mathcal{E}$, which represents the knowledge of an external observer about e_1 and e_2. The definition of the bisimulation enforces some conditions on e_1 and e_2 as well as on $\mathcal{E}$. In Madiot et al.'s framework [24, 23], the conditions on e_1, e_2, and $\mathcal{E}$ are expressed using a LTS between *states* of the form (Γ, e_1) (and (Δ, e_2)), where Γ (and Δ) is a finite sequence of values corresponding to the first (and second) projection of the environment $\mathcal{E}$. Note that in (Γ, e_1), e_1 may be a value, and therefore a state can be simply of the form Γ. Transitions from states of the form (Γ, e_1) (where e_1 is not a value) express conditions on e_1, while transitions from states of the form Γ explain how we compare environments. In the rest of the paper we use Γ, Δ to range over finite sequences of values, and we write Γ_i, Δ_i for the i^{th} element of the sequence. We use Σ, Θ to range over states.

Figure 1 presents the LTS $\xrightarrow{\alpha}$, where α ranges over all the labels. We define $\#(\Gamma)$ as $\bigcup_i \#(\Gamma_i)$. The transition $\xrightarrow{\mathbb{E}}$ uses a relation $e \xrightarrow{=} e'$, defined as follows: if $e \to e'$, then $e \xrightarrow{=} e'$, and if e is a normal form, then $e \xrightarrow{=} e$.[3] To build expressions out of sequences of values, we use different kinds of *multi-hole contexts* defined as follows.

$$\begin{array}{rcll} \mathbb{C} & ::= & \mathbb{C}_\mathsf{v} \mid \mathbb{C}\,\mathbb{C} \mid \mathcal{P}x.\mathbb{C} \mid \#_{\mathbb{C}_\mathsf{v}}\mathbb{C} \mid \mathcal{G}_{\mathbb{C}_\mathsf{v}}x.\mathbb{C} \mid \mathbb{C}_\mathsf{v} \triangleleft \mathbb{C} & \text{(contexts)} \\ \mathbb{C}_\mathsf{v} & ::= & x \mid \lambda x.\mathbb{C} \mid \ulcorner \mathbb{E} \urcorner \mid \Box_i & \text{(value contexts)} \\ \mathbb{E} & ::= & \Box \mid \mathbb{E}\,\mathbb{C} \mid \mathbb{C}_\mathsf{v}\,\mathbb{E} \mid \#_{\Box_i}\mathbb{E} & \text{(evaluation contexts)} \end{array}$$

The holes of a multi-hole context are indexed, except for the special hole $\Box$ of an evaluation context $\mathbb{E}$, which is in evaluation position (that is, filling the other holes of $\mathbb{E}$ with values gives a regular evaluation context E). We write $\mathbb{C}[\Gamma]$ (respectively $\mathbb{C}_\mathsf{v}[\Gamma]$ and $\mathbb{E}[\Gamma]$) for the application of a context $\mathbb{C}$ (respectively $\mathbb{C}_\mathsf{v}$ and $\mathbb{E}$) to a sequence Γ of values, which consists in replacing $\Box_i$ with Γ_i; we assume that this application produce an expression (or an evaluation context in the case of $\mathbb{E}$), i.e., each hole index in the context is smaller or equal than the size of Γ, and for each $\#_{\Box_i}\mathbb{E}$ construct, Γ_i is a prompt. We write $\mathbb{E}[e, \Gamma]$ for the same operation with evaluation contexts, where we assume that e is put in $\Box$ (note that e may also be a value). Notice that prompts are not part of the syntax of $\mathbb{C}_\mathsf{v}$, therefore a multi-hole context does not contain any prompt: if $\mathbb{C}[\Gamma]$, $\mathbb{C}_\mathsf{v}[\Gamma]$, or $\mathbb{E}[e, \Gamma]$ contains a prompt, then it comes from Γ or e. Our multi-hole contexts are promptless because $\equiv_E$ also tests with promptless contexts.

[3] The relation $\xrightarrow{=}$ is not exactly the reflexive closure of $\to$, since an expression which is not a normal form *has* to reduce.

We now detail the rules of Figure 1, starting with the transitions that one can find in any call-by-value λ-calculus [24]. An internal action $(\Gamma, e_1) \xrightarrow{\tau} \Sigma$ corresponds to a reduction step, except we ensure that any generated prompt is fresh w.r.t. Γ. The transition $\Gamma \xrightarrow{\lambda,i,\mathbb{C}_\mathsf{v}} \Sigma$ signals that Γ_i is a λ-abstraction, which can be tested by passing it an argument built from Γ with the context $\mathbb{C}_\mathsf{v}$. The transition $\xrightarrow{\ulcorner.\urcorner,i,\mathbb{C}}$ for testing continuations is built the same way, except we use a context $\mathbb{C}$, because any expression can be thrown to a captured context. Finally, the transition $\Gamma \xrightarrow{\mathsf{v}} \Gamma$ means that the state Γ is composed only of values; it does not test anything on Γ, but this transition is useful for the soundness proofs of Section 3.2. When we have $\Gamma \mathcal{R} (\Delta, e)$ (where $\mathcal{R}$ is, e.g., a bisimulation), then (Δ, e) has to match with $(\Delta, e) \xrightarrow{\tau}{}^* \xrightarrow{\mathsf{v}} (\Delta, v)$ so that (Δ, v) is related to Γ. We can then continue the proofs with two related sequences of values. Such a transition has been suggested in [23, Remark 5.3.6] to simplify the proofs for a non-deterministic language, like $\lambda_{\mathcal{G}\#}$.

We now explain the rules involving prompts. When comparing two terms generating prompts, one can produce p and the other a different q, so we remember in Γ, Δ that p corresponds to q. But an observer can compare prompts using $\overset{?}{=}$, so p has to be related *only* to q. We check it with $\xrightarrow{\#,i,j}$: if $\Gamma \xrightarrow{\#,i,j} \Gamma$, then Δ has to match, meaning that $\Delta_i = \Delta_j$, and doing so for all j such that $\Gamma_i = \Gamma_j$ ensures that all copies of Γ_i are related only to Δ_i. The transition $\xrightarrow{\#,i,i}$ also signals that Γ_i is a prompt and should be related to a prompt. The other transition involving prompts is $\Gamma \xrightarrow{\#} (\Gamma, p)$, which encodes the possibility for an outside observer to generate fresh prompts to compare terms. If Γ is related to Δ, then Δ has to match by generating a prompt q, and we remember that p is related to q. For this rule to be automatically verified, we define the *prompt checking* rule for a relation $\mathcal{R}$ as follows:

$$\frac{\Gamma \mathcal{R} \Delta \qquad p \notin \#(\Gamma) \qquad q \notin \#(\Delta)}{(\Gamma, p) \mathcal{R} (\Delta, q)} \ (\#\text{-check})$$

Henceforth, when we construct a bisimulation $\mathcal{R}$ by giving a set of rules, we always include the (#-check) rule so that the $\xrightarrow{\#}$ transition is always verified.

Finally, the transition $\xrightarrow{\mathbb{E}}$ deals with stuck terms. An expression $E[\mathcal{G}_p x.e]$ is able to reduce if the surrounding context is able to provide a delimiter $\#_p$. However, it is possible only if p is available for the outside, and therefore is in Γ. If $p \notin \mathsf{sp}(\mathbb{E}[\Gamma])$, then $\mathbb{E}[E[\mathcal{G}_p x.e], \Gamma]$ remains stuck, and we have $\mathbb{E}[E[\mathcal{G}_p x.e], \Gamma] \xrightarrow{=} \mathbb{E}[E[\mathcal{G}_p x.e], \Gamma]$. Otherwise, it can reduce and we have $\mathbb{E}[E[\mathcal{G}_p x.e], \Gamma] \xrightarrow{=} e'$, where e' is the result after the capture. The rule for $\xrightarrow{\mathbb{E}}$ may seem demanding, as it tests stuck terms with all contexts $\mathbb{E}$, but up-to techniques will alleviate this issue (see Example 1).

For weak transitions, we define $\Rightarrow$ as $\xrightarrow{\tau}{}^*$, $\overset{\alpha}{\Rightarrow}$ as $\Rightarrow$ if $\alpha = \tau$ and as $\Rightarrow\xrightarrow{\alpha}\Rightarrow$ otherwise. We define bisimulation and bisimilarity using a more general notion of *progress*. Henceforth, we let $\mathcal{R}$, $\mathcal{S}$ range over relations on states.

Definition 3. A relation $\mathcal{R}$ progresses to $\mathcal{S}$, written $\mathcal{R} \rightarrowtail \mathcal{S}$, if $\mathcal{R} \subseteq \mathcal{S}$ and $\Sigma \mathcal{R} \Theta$ implies

- if $\Sigma \xrightarrow{\alpha} \Sigma'$, then there exists Θ' such that $\Theta \overset{\alpha}{\Rightarrow} \Theta'$ and $\Sigma' \mathcal{S} \Theta'$;
- the converse of the above condition on Θ.

A *bisimulation* is a relation $\mathcal{R}$ such that $\mathcal{R} \rightarrowtail \mathcal{R}$, and *bisimilarity* $\approx$ is the union of all bisimulations.

3.2 Up-to Techniques, Soundness, and Completeness

Before defining the up-to techniques for $\lambda_{\mathcal{G}\#}$, we briefly recall the main definitions and results we use from [27, 24, 23]; see these works for more details and proofs. We use f, g to range over functions on relations on states. An *up-to technique* is a function f such that $\mathcal{R} \rightarrowtail f(\mathcal{R})$ implies $\mathcal{R} \subseteq \approx$. However, this definition can be difficult to use to prove that a given f is an up-to technique, so we rely on *compatibility* instead. A function f is monotone if $\mathcal{R} \subseteq \mathcal{S}$ implies $f(\mathcal{R}) \subseteq f(\mathcal{S})$. Given a set F of functions, we also write

F for the function defined as $\bigcup_{f_i \in F} f_i$ (where $f \cup g$ is defined argument-wise, i.e., $(f \cup g)(R) = f(R) \cup g(R)$). Given a function f, f^ω is defined as $\bigcup_{n \in \mathbb{N}} f^n$.

Definition 4. A function f *evolves* to g, written $f \rightsquigarrow g$, if for all $\mathcal{R} \rightarrowtail \mathcal{S}$, we have $f(\mathcal{R}) \rightarrowtail g(\mathcal{S})$. A set F of monotone functions is compatible if for all $f \in F$, $f \rightsquigarrow F^\omega$.

Lemma 2. *Let F be a compatible set, and $f \in F$; f is an up-to technique, and $f(\approx) \subseteq \approx$.*

Proving that f is in a compatible set F is easier than proving it is an up-to technique, because we just have to prove that it evolves towards a combination of functions in F. Besides, the second property of Lemma 2 can be used to prove that $\approx$ is a congruence just by showing that bisimulation up to context is compatible.

The first technique we define allows to forget about prompt names; in a bisimulation relating (Γ, e_1) and (Δ, e_2), we remember that $\Gamma_i = p$ is related to $\Delta_i = q$ by their position i, not by their names. Consequently, we can apply different permutations to the two states to rename the prompts without harm, and bisimulation *up to permutations*[4] allows us to do so. Given a relation $\mathcal{R}$, we define $\mathsf{perm}(\mathcal{R})$ as $\Sigma\sigma_1\ \mathsf{perm}(\mathcal{R})\ \Theta\sigma_2$, assuming $\Sigma\ \mathcal{R}\ \Theta$ and σ_1, σ_2 are any permutations.

We then allow to remove or add values from the states with, respectively, bisimulation *up to weakening* weak and bisimulation *up to strengthening* str, defined as follows

$$\frac{(\overrightarrow{v}, \Gamma, e_1)\ \mathcal{R}\ (\overrightarrow{w}, \Delta, e_2)}{(\Gamma, e_1)\ \mathsf{weak}(\mathcal{R})\ (\Delta, e_2)} \qquad \frac{(\Gamma, e_1)\ \mathcal{R}\ (\Delta, e_2)}{(\Gamma, \mathbb{C}_\mathsf{v}[\Gamma], e_1)\ \mathsf{str}(\mathcal{R})\ (\Delta, \mathbb{C}_\mathsf{v}[\Delta], e_2)}$$

Bisimulation up to weakening diminishes the testing power of states, since less values means less arguments to build from for the transitions $\xrightarrow{\lambda,i,\mathbb{C}_\mathsf{v}}$, $\xrightarrow{\ulcorner.\urcorner,i,\mathbb{C}}$, and $\xrightarrow{\mathbb{E}}$. This up-to technique is usual for environmental bisimulations, and is called "up to environment" in [28]. In contrast, str adds values to the state, but without affecting the testing power, since the added values are built from the ones already in Γ, Δ.

Finally, we define the well-known bisimulation up to context, which allows to factor out a common context when comparing terms. As usual for environmental bisimulations [28], we define two kinds of bisimulation up to context, depending whether we operate on values or any expressions. For values, we can factor out any common context $\mathbb{C}$, but for expressions that are not values, we can factor out only an evaluation context $\mathbb{E}$, since factoring out any context in that case would lead to an unsound up-to technique [23]. We define up to context for values ctx and for any expression ectx as follows:

$$\frac{\Gamma\ \mathcal{R}\ \Delta}{(\Gamma, \mathbb{C}[\Gamma])\ \mathsf{ctx}(\mathcal{R})\ (\Delta, \mathbb{C}[\Delta])} \qquad \frac{(\Gamma, e_1)\ \mathcal{R}\ (\Delta, e_2)}{(\Gamma, \mathbb{E}[e_1, \Gamma])\ \mathsf{ectx}(\mathcal{R})\ (\Delta, \mathbb{E}[e_2, \Delta])}$$

Lemma 3. *The set $\{\mathsf{perm}, \mathsf{weak}, \mathsf{str}, \mathsf{ctx}, \mathsf{ectx}\}$ is compatible.*

The function ectx is particularly helpful in dealing with stuck terms, as we can see below.

Example 1. Let $\Sigma \stackrel{\mathsf{def}}{=} (\Gamma, \mathcal{G}_p x.e_1)$ and $\Theta \stackrel{\mathsf{def}}{=} (\Delta, \mathcal{G}_q x.e_2)$ (for some e_1, e_2), so that $\Sigma\ \mathcal{R}\ \Theta$. If p and q are not in Γ, Δ, then the two expressions remain stuck, as we have $\Sigma \xrightarrow{\mathbb{E}} (\Gamma, \mathbb{E}[\mathcal{G}_p x.e_1, \Gamma])$ and similarly for Θ. We have directly $(\Gamma, \mathbb{E}[\mathcal{G}_p x.e_1, \Gamma])\ \mathsf{ectx}(\mathcal{R})\ (\Delta, \mathbb{E}[\mathcal{G}_q x.e_2, \Delta])$. Otherwise, the capture can be triggered with a context $\mathbb{E}$ of the form $\mathbb{E}_1[\#_{\square_i}\mathbb{E}_2]$, giving $\Sigma \xrightarrow{\mathbb{E}} (\Gamma, \mathbb{E}_1[e_1\{\ulcorner\mathbb{E}_2[\Gamma]\urcorner/x\}, \Gamma])$ and $\Theta \xrightarrow{\mathbb{E}} (\Delta, \mathbb{E}_1[e_2\{\ulcorner\mathbb{E}_2[\Delta]\urcorner/x\}, \Delta])$. Thanks to ectx, we can forget about $\mathbb{E}_1$ which does not play any role, and continue the bisimulation proof by focusing only on $(\Gamma, e_1\{\ulcorner\mathbb{E}_2[\Gamma]\urcorner/x\})$ and $(\Delta, e_2\{\ulcorner\mathbb{E}_2[\Delta]\urcorner/x\})$.

Because bisimulation up to context is compatible, Lemma 2 ensures that $\approx$ is a congruence w.r.t. all contexts for values, and w.r.t. evaluation contexts for all expressions. As a corollary, we can deduce that $\approx$ is sound w.r.t. $\equiv_E$; we can also prove that it is complete w.r.t. $\equiv_E$, leading to the following full characterization result.

[4] Madiot defines a bisimulation "up to permutation" in [23] which reorders values in a state. Our bisimulation up to permutations operates on prompts.

Theorem 1. $e_1 \equiv_E e_2$ *iff* $(\emptyset, e_1) \approx (\emptyset, e_2)$.

For completeness, we prove that $\{(\Gamma, e_1), (\Delta, e_2) \mid \forall \mathbb{E}, \mathbb{E}[e_1, \Gamma] \sim \mathbb{E}[e_2, \Delta]\}$ is a bisimulation up to permutation; the proof is in Appendix A.2.

3.3 Example

As an example, we show a folklore theorem about delimited control [3], stating that the static operators shift and reset can be simulated by the dynamic operators $\mathsf{control}$ and prompt. In fact, what we prove is a more general and stronger result than the original theorem, since we demonstrate that this simulation still holds when multiple prompts are around.

Example 2 (Folklore theorem)**.** We encode shift, reset, $\mathsf{control}$, and prompt as follows

$$\begin{array}{lcllcl} \mathsf{shift}_p & \stackrel{\mathsf{def}}{=} & \lambda f.\mathcal{G}_p k.\#_p f(\lambda y.\#_p k \triangleleft y) & \mathsf{control}_p & \stackrel{\mathsf{def}}{=} & \lambda f.\mathcal{G}_p k.\#_p f(\lambda y.k \triangleleft y) \\ \mathsf{reset}_p & \stackrel{\mathsf{def}}{=} & \ulcorner \#_p \square \urcorner & \mathsf{prompt}_p & \stackrel{\mathsf{def}}{=} & \ulcorner \#_p \square \urcorner \end{array}$$

Let $\mathsf{shift'}_p \stackrel{\mathsf{def}}{=} \lambda f.\mathsf{control}_p\,(\lambda l.f\,(\lambda z.\mathsf{prompt}_p \triangleleft l\, z))$; we prove that $(\mathsf{shift}_p, \mathsf{reset}_p)$ (encoded as $\lambda f.f\ \mathsf{shift}_p\ \mathsf{reset}_p$) is bisimilar to $(\mathsf{shift'}_p, \mathsf{prompt}_p)$ (encoded as $\lambda f.f\ \mathsf{shift'}_p\ \mathsf{prompt}_p$).

Proof. We iteratively build a relation $\mathcal{R}$ closed under ($\#$-check) such that $\mathcal{R}$ is a bisimulation up to context, starting with $(p, \mathsf{shift}_p)\ \mathcal{R}\ (p, \mathsf{shift'}_p)$. The transition $\xrightarrow{\#,1,1}$ is easy to check. For $\xrightarrow{\lambda,2,\mathbb{C}_\mathsf{v}}$, we obtain states of the form $(p, \mathsf{shift}_p, e_1)$, $(p, \mathsf{shift'}_p, e_2)$ that we add to $\mathcal{R}$, where e_1 and e_2 are the terms below

$$\frac{\Gamma\ \mathcal{R}\ \Delta}{(\Gamma, \mathcal{G}_p k.\#_p \mathbb{C}_\mathsf{v}[\Gamma]\ (\lambda y.\#_p k \triangleleft y))\ \mathcal{R}\ (\Delta, \mathcal{G}_p k.\#_p(\lambda l.\mathbb{C}_\mathsf{v}[\Delta]\ (\lambda z.\mathsf{prompt}_p \triangleleft l\, z))\ (\lambda y.k \triangleleft y))}$$

We use an inductive, more general rule, because we want $\xrightarrow{\lambda,2,\mathbb{C}_\mathsf{v}}$ to be still verified after we extend (p, shift_p) and $(p, \mathsf{shift'}_p)$. The terms e_1 and e_2 are stuck, so we test them with $\xrightarrow{\mathbb{E}}$. If $\mathbb{E}$ does not trigger the capture, we obtain $\mathbb{E}[e_1, \Gamma]$ and $\mathbb{E}[e_2, \Delta]$, and we can use ectx to conclude. Otherwise, $\mathbb{E} = \mathbb{E}'[\#_{\square_1}\mathbb{E}'']$ (where $\#_{\square_1}$ does not surround $\square$ in $\mathbb{E}''$), and we get

$$\mathbb{E}'[\#_p \mathbb{C}_\mathsf{v}[\Gamma]\ (\lambda y.\#_p \ulcorner \mathbb{E}''[\Gamma] \urcorner \triangleleft y), \Gamma] \text{ and } \mathbb{E}'[\#_p \mathbb{C}_\mathsf{v}[\Delta]\ (\lambda z.\mathsf{prompt}_p \triangleleft (\lambda y.\ulcorner \mathbb{E}''[\Delta] \urcorner \triangleleft y)\ z), \Delta]$$

We want to use ctx to remove the common context $\mathbb{E}'[\#_{\square_1}\mathbb{C}_\mathsf{v}\ \square_i]$, which means that we have to add the following states in the definition of $\mathcal{R}$ (again, inductively):

$$\frac{\Gamma\ \mathcal{R}\ \Delta}{(\Gamma, \lambda y.\#_p \ulcorner \mathbb{E}''[\Gamma] \urcorner \triangleleft y)\ \mathcal{R}\ (\Delta, \lambda z.\mathsf{prompt}_p \triangleleft (\lambda y.\ulcorner \mathbb{E}''[\Delta] \urcorner \triangleleft y)\ z)}$$

Testing these functions with $\xrightarrow{\lambda,i,\mathbb{C}_\mathsf{v}}$ gives on both sides states where $\#_{\square_1}\mathbb{E}''[\mathbb{C}_\mathsf{v}]$ can be removed with ctx. Because $(\varnothing, \lambda f.f\ \mathsf{shift}_p\ \mathsf{reset}_p)\ \mathsf{weak}(\mathsf{ctx}(\mathcal{R}))\ (\varnothing, \lambda f.f\ \mathsf{shift'}_p\ \mathsf{prompt}_p)$, it is enough to conclude. Indeed, $\mathcal{R}$ is a bisimulation up to context, so $\mathcal{R} \subseteq \approx$, which implies $\mathsf{weak}(\mathsf{ctx}(\mathcal{R})) \subseteq \mathsf{weak}(\mathsf{ctx}(\approx))$ (because weak and ctx are monotone), and $\mathsf{weak}(\mathsf{ctx}(\approx)) \subseteq \approx$ (by Lemma 2). Note that this reasoning works for any combination of monotone up-to techniques and any bisimulation (up-to). □

What makes the proof of Example 2 quite simple is that we relate (p, shift_p) and $(p, \mathsf{shift'}_p)$, meaning that p can be used by an outside observer. But the control operators $(\mathsf{shift}_p, \mathsf{reset}_p)$ and $(\mathsf{shift'}_p, \mathsf{prompt}_p)$ should be the only terms available for the outside, since p is used only to implement them. If we try to prove equivalent these two pairs directly, i.e., while keeping p private, then testing reset_p and prompt_p with $\xrightarrow{\ulcorner.\urcorner,2,\mathbb{C}}$ requires a cumbersome analysis of the behaviors of $\#_p\mathbb{C}[\Gamma]$ and $\#_p\mathbb{C}[\Delta]$. In the next section, we define a new kind of bisimilarity with a powerful up-to technique to make such proofs more tractable.

4 The $\star$-Bisimilarity

4.1 Motivation

Testing continuations. In Section 3, a continuation $\Gamma_i = \ulcorner E \urcorner$ is tested with $\Gamma \xrightarrow{\ulcorner . \urcorner, i, \mathbb{C}} (\Gamma, E[\mathbb{C}[\Gamma]])$. We then have to study the behavior of $E[\mathbb{C}[\Gamma]]$, which depends primarily on how $\mathbb{C}[\Gamma]$ reduces; e.g., if $\mathbb{C}[\Gamma]$ diverges, then E does not play any role. Consequently, the transition $\xrightarrow{\ulcorner . \urcorner, i, \mathbb{C}}$ does not really test the continuation directly, since we have to reduce $\mathbb{C}[\Gamma]$ first. To really exhibit the behavior of the continuation, we change the transition so that it uses a value context instead of a general one. We then have $\Gamma \xrightarrow{\ulcorner . \urcorner, i, \mathbb{C}_\mathsf{v}} (\Gamma, E[\mathbb{C}_\mathsf{v}[\Gamma]])$, and the behavior of the term we obtain depends primarily on E. However, this is not equivalent to testing with $\mathbb{C}$, since $\mathbb{C}[\Gamma]$ may interact in other ways with E if $\mathbb{C}[\Gamma]$ is a stuck term. If E is of the form $E'[\#_p E'']$, and p is in Γ, then $\mathbb{C}$ may capture E'', since p can be used to build an expression of the form $\mathcal{G}_p x.e$. To take into account this possibility, we introduce a new transition $\Gamma \xrightarrow{\ulcorner . \urcorner, i, j} (\Gamma, \ulcorner E' \urcorner, \ulcorner E'' \urcorner)$, which decomposes $\Gamma_i = E'[\#_p E'']$ into $\ulcorner E' \urcorner$ and $\ulcorner E'' \urcorner$, provided $\Gamma_j = p$. The stuck term $\mathbb{C}[\Gamma]$ may also capture E entirely, as part of a bigger context of the form $\mathbb{E}_1[E[\mathbb{E}_2]]$. To take this into account, we introduce a way to build such contexts using captured continuations. This is also useful to make bisimulation up to context more expressive, as we explain in the next paragraph.

A more expressive bisimulation up to context. As we already pointed out in [6], bisimulation up to context is not very helpful in the presence of control operators. For example, suppose we prove the β_Ω axiom of [17], i.e., $(\lambda x.E[x])\ e$ is equivalent to $E[e]$ if $x \notin \mathsf{fv}(E)$ and $\mathsf{sp}(E) = \emptyset$. If e is a stuck term $\mathcal{G}_p y.e_1$, we have to compare $e_1\{\ulcorner E_1[(\lambda x.E[x])\ \Box] \urcorner / y\}$ and $e_1\{\ulcorner E_1[E] \urcorner / y\}$ for some E_1. If e_1 is of the form $y \lhd (y \lhd e_2)$, then we get respectively $E_1[(\lambda x.E[x])\ E_1[(\lambda x.E[x])\ e_2]]$ and $E_1[E[E_1[E[e_2]]]]$. We can see that the two resulting expressions have the same shape, and yet we can only remove the outermost occurrence of E_1 with ectx. The problem is that bisimulation up to context can factor out only a *common* context. We want an up-to technique able to identify *related* contexts, i.e., contexts built out of related continuations. To do so, we modify the multi-hole contexts to include a construct $\star_i[\mathbb{C}]$ with a special hole $\star_i$, which can be filled only with $\ulcorner E \urcorner$ to produce a context $E[\mathbb{C}]$. As a result, if $\Gamma = (\ulcorner (\lambda x.E[x])\ \Box \urcorner)$ and $\Delta = (\ulcorner E \urcorner)$, then $E_1[(\lambda x.E[x])\ E_1[(\lambda x.E[x])\ \Box]]$ and $E_1[E[E_1[E[\Box]]]]$ can be written $\mathbb{E}[\Gamma]$, $\mathbb{E}[\Delta]$ with $\mathbb{E} = E_1[\star_1[E_1[\star_1[\Box]]]]$. We can then focus only on testing Γ and Δ.

However, such a bisimulation up to related context would be unsound if not restricted in some way. Indeed, let $\ulcorner E_1 \urcorner$, $\ulcorner E_2 \urcorner$ be any continuations, and let $\Gamma = (\ulcorner E_1 \urcorner)$, $\Delta = (\ulcorner E_2 \urcorner)$. Then the transitions $\Gamma \xrightarrow{\ulcorner . \urcorner, 1, \mathbb{C}_\mathsf{v}} (\Gamma, E_1[\mathbb{C}_\mathsf{v}[\Gamma]])$ and $\Delta \xrightarrow{\ulcorner . \urcorner, 1, \mathbb{C}_\mathsf{v}} (\Delta, E_2[\mathbb{C}_\mathsf{v}[\Delta]])$ produce states of the form $(\Gamma, \mathbb{C}[\Gamma])$, $(\Delta, \mathbb{C}[\Delta])$ with $\mathbb{C} = \star_1[\mathbb{C}_\mathsf{v}]$. If bisimulation up to related context was sound in that case, it would mean that $\ulcorner E_1 \urcorner$ and $\ulcorner E_2 \urcorner$ would be bisimilar for all E_1 and E_2, which, of course, is wrong.[5] To prevent this, we distinguish *passive* transitions (such as $\xrightarrow{\ulcorner . \urcorner, i, \mathbb{C}_\mathsf{v}}$) from the other ones (called *active*), so that only selected up-to techniques (referred to as *strong*) can be used after a passive transition. In contrast, any up-to technique (including this new bisimulation up to related context) can be used after an active transition. To formalize this idea, we have to extend Madiot et al.'s framework to allow such distinctions between transitions and between up-to techniques.

4.2 Labeled Transition System and Bisimilarity

First, we explain how we alter the LTS of Section 3.1 to implement the changes we sketched in Section 4.1. We extend the grammar of multi-hole contexts $\mathbb{C}$ (resp. $\mathbb{E}$) by adding the production $\star_i[\mathbb{C}]$ (resp. $\star_i[\mathbb{E}]$), where the hole $\star_i$ can be filled only with a continuation (the grammar of value contexts $\mathbb{C}_\mathsf{v}$ is unchanged). When we write $(\star_i[\mathbb{C}])[\Gamma]$, we assume Γ_i is a continuation $\ulcorner E \urcorner$, and the result of the operation is $E[\mathbb{C}[\Gamma]]$ (and similarly for $\mathbb{E}$).

[5] The problem is similar if we test continuations using contexts $\mathbb{C}$ (as in Section 3) instead of $\mathbb{C}_\mathsf{v}$.

We also change the way we deal with captured contexts, by using the following rules:

$$\frac{\Gamma_i = \ulcorner E \urcorner}{\Gamma \xrightarrow{\ulcorner . \urcorner, i, \mathbb{C}_\mathsf{v}} (\Gamma, E[\mathbb{C}_\mathsf{v}[\Gamma]])} \qquad \frac{\Gamma_i = \ulcorner E_1[\#_p E_2] \urcorner \qquad \Gamma_j = p \qquad p \notin \mathsf{sp}(E_2)}{\Gamma \xrightarrow{\ulcorner . \urcorner, i, j} (\Gamma, \ulcorner E_1 \urcorner, \ulcorner E_2 \urcorner)}$$

The transition $\xrightarrow{\ulcorner . \urcorner, i, \mathbb{C}_\mathsf{v}}$ is the same as in Section 3, except that it tests with an argument built with a value context $\mathbb{C}_\mathsf{v}$ instead of a regular context $\mathbb{C}$. We also introduce the transition $\xrightarrow{\ulcorner . \urcorner, i, j}$, which decomposes a captured context $\ulcorner E_1[\#_p E_2] \urcorner$ into sub-contexts $\ulcorner E_1 \urcorner$, $\ulcorner E_2 \urcorner$, provided that p is in Γ. This transition is necessary to take into account the possibility for an external observer to capture a part of a context, scenario which can no longer be tested with $\xrightarrow{\ulcorner . \urcorner, i, \mathbb{C}_\mathsf{v}}$, as explained in Section 4.1, and as illustrated with the next example.

Example 3. Let $\Gamma = (p, \ulcorner \#_p \Box \urcorner)$, $\Delta = (q, \ulcorner \Box \urcorner)$; then $\Gamma \xrightarrow{\ulcorner . \urcorner, 2, \mathbb{C}_\mathsf{v}} (\Gamma, \#_p \mathbb{C}_\mathsf{v}[\Gamma]) \xrightarrow{\tau} (\Gamma, \mathbb{C}_\mathsf{v}[\Gamma])$ and $\Delta \xrightarrow{\ulcorner . \urcorner, 2, \mathbb{C}_\mathsf{v}} (\Delta, \mathbb{C}_\mathsf{v}[\Delta])$. Without the $\xrightarrow{\ulcorner . \urcorner, i, j}$ transition, Γ and Δ would be bisimilar, which would not be sound (they are distinguished by the context $\Box_2 \triangleleft \mathcal{G}_{\Box_1} x.\Omega$).

The other rules are not modified, but their meaning is still affected by the change in the contexts grammars: the transitions $\xrightarrow{\lambda, i, \mathbb{C}_\mathsf{v}}$ and $\xrightarrow{\mathbb{E}}$ can now test with more arguments. This is a consequence of the fact that an observer can build a bigger continuation from a captured context. For instance, if $\Gamma = (p, \ulcorner E \urcorner, \lambda x.x \triangleleft v)$, then with the LTS of Section 3, $\Gamma \xrightarrow{\ulcorner . \urcorner, 2, \mathbb{E}_1[\mathcal{G}_{\Box_1} x.x]} \xrightarrow{\#_{\Box_1} \mathbb{E}_2} \xrightarrow{\lambda, 3, \Box_4} (\Gamma, \ulcorner \mathbb{E}_1[E[\mathbb{E}_2[\Gamma]], \Gamma] \urcorner, \ulcorner \mathbb{E}_1[E[\mathbb{E}_2[\Gamma]], \Gamma] \urcorner \triangleleft v)$. In the new LTS, the first transition is no longer possible, but we can still test the λ-abstraction with the same argument using $\Gamma \xrightarrow{\lambda, 3, \mathbb{E}_1[\star_2[\mathbb{E}_2]]} (\Gamma, \ulcorner \mathbb{E}_1[E[\mathbb{E}_2[\Gamma]], \Gamma] \urcorner \triangleleft v)$.

As explained in Section 4.1, we want to prevent the use of some up-to techniques (like the bisimulation up to related context we introduce in Section 4.3) after some transitions, especially $\xrightarrow{\ulcorner . \urcorner, i, \mathbb{C}_\mathsf{v}}$. To do so, we distinguish the *passive* transitions $\xrightarrow{\ulcorner . \urcorner, i, \mathbb{C}_\mathsf{v}}$, $\xrightarrow{\mathsf{v}}$ from the other ones, called *active*. In a LTS, a visible action $\xrightarrow{\alpha}$ (where $\alpha \neq \tau$) usually corresponds to an interaction with an external observer. The transition $\xrightarrow{\mathsf{v}}$ does not fit that principle; similarly, $\xrightarrow{\ulcorner . \urcorner, i, \mathbb{C}_\mathsf{v}}$ does not correspond exactly to an observer interacting with a continuation, since we throw a value, and not any expression. In contrast, $\xrightarrow{\lambda, i, \mathbb{C}_\mathsf{v}}$ corresponds to function application, $\xrightarrow{\mathbb{E}}$ to context capture, $\xrightarrow{\ulcorner . \urcorner, i, j}$ to continuation decomposition, and $\xrightarrow{\#, i, j}$ to testing prompts equality. This is how we roughly distinguish the former transitions as passive, and the latter ones as active. We then change the definition of progress, to allow a relation $\mathcal{R}$ to progress towards different relations after passive and active transitions.

Definition 5. A relation $\mathcal{R}$ diacritically progresses to $\mathcal{S}$, $\mathcal{T}$ written $\mathcal{R} \rightarrowtail\!\!\!\!\twoheadrightarrow \mathcal{S}, \mathcal{T}$, if $\mathcal{R} \subseteq \mathcal{S}$, $\mathcal{R} \subseteq \mathcal{T}$, and $\Sigma \mathcal{R} \Theta$ implies that

- if $\Sigma \xrightarrow{\alpha} \Sigma'$ and $\xrightarrow{\alpha}$ is passive, then there exists Θ' such that $\Theta \stackrel{\alpha}{\Rightarrow} \Theta'$ and $\Sigma' \mathcal{S} \Theta'$;
- if $\Sigma \xrightarrow{\alpha} \Sigma'$ and $\xrightarrow{\alpha}$ is active, then there exists Θ' such that $\Theta \stackrel{\alpha}{\Rightarrow} \Theta'$ and $\Sigma' \mathcal{T} \Theta'$;
- the converse of the above conditions on Θ.

A $\star$-bisimulation is a relation $\mathcal{R}$ such that $\mathcal{R} \rightarrowtail\!\!\!\!\twoheadrightarrow \mathcal{R}, \mathcal{R}$, and $\star$-bisimilarity $\stackrel{\star}{\approx}$ is the union of all $\star$-bisimulations.

Note that with the same LTS, $\rightarrowtail$ and $\rightarrowtail\!\!\!\!\twoheadrightarrow$ entail the same notions of bisimulation and bisimilarity (but we use a different LTS in this section).

4.3 Up-to Techniques, Soundness, and Completeness

We now discriminate up-to techniques, so that regular up-to techniques cannot be used after passive transitions, while *strong* ones can. An up-to technique (resp. *strong* up-to technique) is a function f such that $\mathcal{R} \rightarrowtail\!\!\!\!\twoheadrightarrow \mathcal{R}, f(\mathcal{R})$ (resp. $\mathcal{R} \rightarrowtail\!\!\!\!\twoheadrightarrow f(\mathcal{R}), f(\mathcal{R})$) implies $\mathcal{R} \subseteq \overset{\star}{\approx}$. We also adapt the notions of evolution and compatibility.

Definition 6. A function f evolves to g, h, written $f \rightsquigarrow g, h$, if for all $\mathcal{R} \rightarrowtail\!\!\!\!\twoheadrightarrow \mathcal{R}, \mathcal{T}$, we have $f(\mathcal{R}) \rightarrowtail\!\!\!\!\twoheadrightarrow g(\mathcal{R}), h(\mathcal{T})$.

A function f *strongly* evolves to g, h, written $f \rightsquigarrow_{\mathsf{s}} g, h$, if for all $\mathcal{R} \rightarrowtail\!\!\!\!\twoheadrightarrow \mathcal{S}, \mathcal{T}$, we have $f(\mathcal{R}) \rightarrowtail\!\!\!\!\twoheadrightarrow g(\mathcal{S}), h(\mathcal{T})$.

Strong evolution is very general, as it uses any relation $\mathcal{R}$, while regular evolution is more restricted, as it relies on relations $\mathcal{R}$ such that $\mathcal{R} \rightarrowtail\!\!\!\!\twoheadrightarrow \mathcal{R}, \mathcal{T}$. But the definition of *diacritical compatibility* below still allows to use any combinations of strong up-to techniques after a passive transition, even for functions which are not themselves strong. In contrast, regular functions can only be used once after a passive transition of an other regular function.

Definition 7. A set F of monotone functions is *diacritically compatible* if there exists $S \subseteq F$ such that

- for all $f \in S$, we have $f \rightsquigarrow_{\mathsf{s}} S^\omega, F^\omega$;
- for all $f \in F$, we have $f \rightsquigarrow S^\omega \circ F \circ S^\omega, F^\omega$.

If S_1 and S_2 are subsets of F which verify the conditions of the definition, then $S_1 \cup S_2$ also does, so there exists the largest subset of F which satisfies the conditions, written $\mathsf{strong}(F)$. This (possibly empty) subset of F corresponds to the strong up-to techniques of F.

Lemma 4. *Let F be a compatible set.*

- *If $\mathcal{R} \rightarrowtail\!\!\!\!\twoheadrightarrow \mathsf{strong}(F)^\omega(\mathcal{R}), F^\omega(\mathcal{R})$, then $F^\omega(\mathcal{R})$ is a bisimulation.*
- *If $f \in F$, then f is an up-to technique. If $f \in \mathsf{strong}(F)$, then f is a strong up-to technique.*
- *For all $f \in F$, we have $f(\approx) \subseteq \approx$.*

We now use this framework to define up-to techniques for the $\star$-bisimulation. The definitions of perm and weak are unchanged. We define bisimulation up to related contexts for values rctx and for any term rectx as follows:

$$\frac{\Gamma\ \mathcal{R}\ \Delta}{(\Gamma, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Gamma], \mathbb{C}[\Gamma])\ \mathsf{rctx}(\mathcal{R})\ (\Delta, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Delta], \mathbb{C}[\Delta])} \qquad \frac{(\Gamma, e_1)\ \mathcal{R}\ (\Delta, e_2)}{(\Gamma, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Gamma], \mathbb{E}[e_1, \Gamma])\ \mathsf{rectx}(\mathcal{R})\ (\Delta, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Delta], \mathbb{E}[e_2, \Delta])}$$

The definitions look similar to the ones of ctx and ectx, but the grammar of multi-hole contexts now include $\star_i$. Besides, we inline strengthening in the definitions of rctx and rectx, allowing Γ, Δ to be extended. This is necessary because, e.g., str and rectx cannot be composed after a passive transition (they are both not strong), so rectx have to include str directly. Note that the behavior of str can be recovered from rectx by taking $\mathbb{E} = \square$.

Lemma 5. $F \overset{\mathsf{def}}{=} \{\mathsf{perm}, \mathsf{weak}, \mathsf{rctx}, \mathsf{rectx}\}$ *is compatible, with* $\mathsf{strong}(F) = \{\mathsf{perm}, \mathsf{weak}\}$.

As a result, these functions are up-to techniques, and weak and perm can be used after a passive transition. Because of the last item of Lemma 4, $\overset{\star}{\approx}$ is also a congruence w.r.t. evaluation contexts, which means that $\overset{\star}{\approx}$ is sound w.r.t. $\equiv_E$. We can also prove it is complete the same way as for Theorem 1, leading again to full characterization.

Theorem 2. $e_1 \equiv_E e_2$ *iff* $(\emptyset, e_1) \overset{\star}{\approx} (\emptyset, e_2)$.

4.4 Examples

We illustrate the use of $\overset{\star}{\approx}$, rctx, and rectx with two examples that would be much harder to prove with the techniques of Section 3.

Example 4 (β_Ω axiom)**.** We prove $(\lambda x.E[x])\, e \overset{\star}{\approx} E[e]$ if $x \notin \mathsf{fv}(E)$ and $\mathsf{sp}(E) = \emptyset$. Define $\mathcal{R}$ starting with $(\ulcorner(\lambda x.E[x])\,\square\urcorner)\ \mathcal{R}\ (\ulcorner E\urcorner)$, and closing it under the ($\#$-check) and the following rule:

$$\frac{\Gamma\ \mathcal{R}\ \Delta}{(\Gamma, (\lambda x.E[x])\ \mathbb{C}_\mathsf{v}[\Gamma])\ \mathcal{R}\ (\Delta, E[\mathbb{C}_\mathsf{v}[\Delta]])}$$

Then $(\emptyset, (\lambda x.E[x])\ e)\ \ \mathsf{weak}(\mathsf{rctx}(\mathcal{R}))\ \ (\emptyset, E[e])$ and $\mathcal{R}$ is a bisimulation up to context, since the sequence $\Gamma \xrightarrow{\ulcorner.\urcorner,1,\mathbb{C}_\mathsf{v}} (\Gamma, (\lambda x.E[x])\ \mathbb{C}_\mathsf{v}[\Gamma]) \xrightarrow{\tau} (\Gamma, E[\mathbb{C}_\mathsf{v}[\Gamma]])$ fits $\Delta \xrightarrow{\ulcorner.\urcorner,1,\mathbb{C}_\mathsf{v}} (\Delta, E[\mathbb{C}_\mathsf{v}[\Delta]]) \overset{\tau}{\Rightarrow} (\Delta, E[\mathbb{C}_\mathsf{v}[\Delta]])$, where the final states are in rctx. Notice we use rctx after $\xrightarrow{\tau}$, and not after the passive $\xrightarrow{\ulcorner.\urcorner,1,\mathbb{C}_\mathsf{v}}$ transition.

Example 5 (Exceptions)**.** A possible way of extending a calculus with exception handling is to add a construct $\mathsf{try}_r\ e\ \mathsf{with}\ v$, which evaluates e with a function raising an exception stored under the variable r. When e calls the function in r with some argument v', even inside another try block, then the computation of e is aborted and replaced by $v\ v'$. We can implement this behavior directly in $\lambda_{\mathcal{G}\#}$; more precisely, we write $\mathsf{try}_r\ e\ \mathsf{with}\ v$ as $\mathsf{handle}\ (\lambda r.e)\ v$, where handle is a function expressed in the calculus. One possible implementation of handle in $\lambda_{\mathcal{G}\#}$ is very natural and heavily relies on fresh-prompt generation:

$$\mathsf{handle} \overset{\mathsf{def}}{=} \lambda f.\lambda h.\mathcal{P}x.\#_x f\ (\lambda z.\mathcal{G}_{x\_}.h\ z)$$

The idea is to raise an exception by aborting the current continuation up to the corresponding prompt. The same function can be implemented using any comparable-resource generation and only one prompt p:

$$\begin{array}{rcl} \mathsf{handle}_p & \overset{\mathsf{def}}{=} & \lambda f.\lambda h.\mathcal{P}x.(\#_p \mathsf{let}\ r = f\ \mathsf{raise}_{p,x}\ \mathsf{in}\ \lambda\_.\lambda\_.r)\ x\ h \\ \mathsf{raise}_{p,x} & \overset{\mathsf{def}}{=} & \mathsf{fix}\ r(z).\mathcal{G}_{p\_}.\lambda y.\lambda h.\mathsf{if}\ x \overset{?}{=} y\ \mathsf{then}\ h\ z\ \mathsf{else}\ r\ z \end{array}$$

Here the idea is to keep a freshly generated name x and a handler function h with the prompt corresponding to each call of handle_p. The exception-raising function $\mathsf{raise}_{p,x}$ iteratively aborts the current delimited continuation up to the nearest call of handle_p and checks the name stored there in order to find the corresponding handler. Note that this implementation also uses prompt generation, since it is the only comparable resource that can be dynamically generated in $\lambda_{\mathcal{G}\#}$, but the implementation can be easily translated to, e.g., a calculus with single-prompted delimited-control operators and first-order store.

Proof. We prove that both versions of handle are bisimilar. As in Example 2 we iteratively build a relation $\mathcal{R}$ closed under the ($\#$-check) rule, so that $\mathcal{R}$ is a bisimulation up to context. We start with $(\mathsf{handle})\ \mathcal{R}\ (\mathsf{handle}_p)$; to match the $\xrightarrow{\lambda,1,\mathbb{C}_\mathsf{v}}$ transition, we extend $\mathcal{R}$ as follows:

$$\frac{\Gamma\ \mathcal{R}\ \Delta}{(\Gamma, \lambda h.\mathcal{P}x.\#_x \mathbb{C}_\mathsf{v}[\Gamma]\ (\lambda z.\mathcal{G}_{x\_}.h\ z))\ \mathcal{R}\ (\Delta, \lambda h.\mathcal{P}x.(\#_p \mathsf{let}\ r = \mathbb{C}_\mathsf{v}[\Delta]\ \mathsf{raise}_{p,x}\ \mathsf{in}\ \lambda\_.\lambda\_.r)\ x\ h)}$$

We obtain two functions which are in turn tested with $\xrightarrow{\lambda,n+1,\mathbb{C}'_\mathsf{v}}$, and we obtain the states

$$(\Gamma, \#_{p_1} \mathbb{C}_\mathsf{v}[\Gamma]\ (\lambda z.\mathcal{G}_{p_1\_}.\mathbb{C}'_\mathsf{v}[\Gamma]\ z)) \text{ and } (\Delta, (\#_p \mathsf{let}\ r = \mathbb{C}_\mathsf{v}[\Delta]\ \mathsf{raise}_{p,p_2}\ \mathsf{in}\ \lambda\_.\lambda\_.r)\ p_2\ \mathbb{C}'_\mathsf{v}[\Delta]).$$

Instead of adding them to $\mathcal{R}$ directly, we decompose them into corresponding parts using up to context (with $\mathbb{C} = \star_{n+1}[\mathbb{C}_\mathsf{v}\ \square_{n+2}]$), and we add these subterms to $\mathcal{R}$:

$$\frac{\Gamma\ \mathcal{R}\ \Delta \qquad p_1 \notin \#(\Gamma) \qquad p_2 \notin \#(\Delta)}{(\Gamma, \ulcorner \#_{p_1} \square \urcorner, \lambda z.\mathcal{G}_{p_1\_}.\mathbb{C}'_\mathsf{v}[\Gamma]\ z)\ \mathcal{R}\ (\Delta, \ulcorner(\#_p \mathsf{let}\ r = \square\ \mathsf{in}\ \lambda\_.\lambda\_.r)\ p_2\ \mathbb{C}'_\mathsf{v}[\Delta]\urcorner, \mathsf{raise}_{p,p_2})} \quad (*)$$

Testing the two captured contexts with $\xrightarrow{\ulcorner.\urcorner,n+1,\mathbb{C}''_{\mathsf{v}}}$ is easy, because they both evaluate to the thrown value. We now consider $\lambda z.\mathcal{G}_{p_1\_}.\mathbb{C}'_{\mathsf{v}}[\Gamma]\ z$ and raise_{p,p_2}; after the transition $\xrightarrow{\lambda,n+2,\mathbb{C}_{\mathsf{v}}}$ we get the two control stuck terms

$$\mathcal{G}_{p_1\_}.\mathbb{C}'_{\mathsf{v}}[\Gamma]\ \mathbb{C}_{\mathsf{v}}[\Gamma] \quad \text{and} \quad \mathcal{G}_{p\_}.\lambda y.\lambda h.\mathsf{if}\ p_2 \stackrel{?}{=} y\ \mathsf{then}\ h\ \mathbb{C}_{\mathsf{v}}[\Delta]\ \mathsf{else}\ \mathsf{raise}_{p,p_2}\ \mathbb{C}_{\mathsf{v}}[\Delta]$$

Adding such terms to the relation will not be enough. The first one can be unstuck only using the corresponding context $\ulcorner \#_{p_1} \square \urcorner$, but the second one can be unstuck using any context added by rule $(*)$, even for a different p_2. In such a case, it will consume a part of the context and evaluate to itself. To be more general we add the following rule:

$$\frac{\Gamma\ \mathcal{R}\ \Delta \qquad \mathbb{E}[\mathcal{G}_{p_1\_}.\mathbb{C}'_{\mathsf{v}}[\Gamma]\ \mathbb{C}_{\mathsf{v}}[\Gamma], \Gamma] \text{ is control-stuck}}{(\Gamma, \mathbb{E}[\mathcal{G}_{p_1\_}.\mathbb{C}'_{\mathsf{v}}[\Gamma]\ \mathbb{C}_{\mathsf{v}}[\Gamma], \Gamma])\ \mathcal{R}\ (\Delta, \mathcal{G}_{p\_}.\lambda y.\lambda h.\mathsf{if}\ p_2 \stackrel{?}{=} y\ \mathsf{then}\ h\ \mathbb{C}_{\mathsf{v}}[\Delta]\ \mathsf{else}\ \mathsf{raise}_{p,p_2}\ \mathbb{C}_{\mathsf{v}}[\Delta])}$$

The newly introduced stuck terms are tested with $\xrightarrow{\mathbb{E}'}$; if $\mathbb{E}'$ does not have $\star_i$ surrounding $\square$, they are still stuck, and we can use up to evaluation context to conclude. Assume $\mathbb{E}' = \mathbb{E}_1[\star_i[\mathbb{E}_2]]$ where $\mathbb{E}_2$ has not $\star_j$ around $\square$. If i points to the evaluation context added by $(*)$ for the same p_2, then they both evaluate to terms of the same shape, so we use up to context with $\mathbb{C} = \mathbb{E}_1[\mathbb{C}'_{\mathsf{v}}\ \mathbb{C}_{\mathsf{v}}]$. Otherwise, we know the second program compares two different prompts, so it evaluates to $\mathbb{E}_1[\mathcal{G}_{p\_}.\lambda y.\lambda h.\mathsf{if}\ p_2 \stackrel{?}{=} y\ \mathsf{then}\ h\,\mathbb{C}_{\mathsf{v}}[\Delta]\ \mathsf{else}\ \mathsf{raise}_{p,p_2}\ \mathbb{C}_{\mathsf{v}}[\Delta], \Delta]$ and we use rectx with the last rule. $\square$

5 Related Work and Conclusion

Related work. In previous works [4, 5, 6], we defined several bisimilarities for a calculus (called $\lambda_{\mathcal{S}}$) with the (less expressive) delimited-control operators shift and reset. The bisimilarity of Section 3 and the corresponding up-to techniques are close to the ones of [6, Section 3], except that in [6], we do not compare stuck terms using *all* evaluation contexts. However, there is no equivalent of bisimulation up to related contexts in [6], which makes the proof of the β_Ω axiom very difficult in that paper. The proof in Example 4 is as easy as the proof of the β_Ω axiom in [5], but the bisimilarity of [5] is not complete, unlike $\stackrel{\star}{\approx}$. As a matter of fact, following the developments of Section 4, we believe it is possible to define environmental bisimulations up to related contexts for the $\lambda_{\mathcal{S}}$-calculus.

Environmental bisimilarity has been defined in several calculi with dynamic resource generation, like stores and references [22, 21, 29], information hiding constructs [30, 31], or name creation [2, 25]. In these works, an expression is paired with its generated resources, and behavioral equivalences are defined on these pairs. Our approach is different since we do not carry sets of generated prompts when manipulating expressions (e.g., in the semantic rules of Section 2); instead, we rely on side-conditions and permutations to avoid collisions between prompts. This is possible because all we need to know is if a prompt is known to an outside observer or not, and the correspondences between the public prompts of two related expressions; this can be done through the environment of the bisimilarity. This approach cannot be adapted to more complex generated resources, which are represented by a mapping (e.g., for stores or existential types), but we believe it can be used for name creation in π-calculus [25].

A line of work on program equivalence for which relating evaluation contexts is crucial, as in our work, are logical relations based on the notion of biorthogonality [26]. In particular, this concept has been successfully used to develop techniques for establishing program equivalence in ML-like languages with $\mathsf{call/cc}$ [9], and for proving the coherence of control-effect subtyping [7]. Hur et al. combine logical relations and behavioral equivalences in the definition of *parametric bisimulation* [15], where terms are reduced to normal forms that are then decomposed into subterms related by logical relations. This framework has been extended to abortive control in [16], where *stuttering* is used to allow terms not to reduce for a finite amount of time when comparing them in a bisimulation proof. This is reminiscent of our distinction between active and passive transitions, as passive transitions can be seen as "not reducing", but there is still some testing involved in

these transitions. Besides, the concern is different, since the active/passive distinction prevents the use of up-to techniques, while stuttering has been proposed to improve plain parametric bisimulations.

Conclusion and future work. We have developed a behavioral theory for Dybvig et al.'s calculus of multi-prompted delimited control, where the enabling technology for proving program equivalence are environmental bisimulations, presented in Madiot's style. The obtained results generalize our previous work in that they account for multiple prompts and local visibility of dynamically generated prompts. Moreover, the results of Section 4 considerably enhance reasoning about captured contexts by treating them as first-class objects at the level of bisimulation proofs (thanks to the construct $\star_i$) and not only at the level of terms. The resulting notion of bisimulation up to related contexts improves on the existing bisimulation up to context in presence of control operators, as we can see when comparing Example 4 to the proof of the same result in [6]. We believe bisimulation up to related contexts could be useful for constructs akin to control operators, like passivation in π-calculus [25]. The soundness of this up-to technique has been proved in an extension of Madiot's framework; we plan to investigate further this extension, to see how useful it could be in defining up-to techniques for other languages. Finally, it may be possible to apply the tools developed in this paper to [19], where a single-prompted calculus is translated into a multi-prompted one, but no operational correspondence is given to guarantee the soundness of the translation.

Acknowledgements We would like to thank Jean-Marie Madiot for the insightful discussions about his work, and Małgorzata Biernacka, Klara Zielińska, and the anonymous reviewers for the helpful comments on the presentation of this work.

This work was partially supported by PHC Polonium and by National Science Centre, Poland, grant no. 2014/15/B/ST6/00619.

References

[1] Vincent Balat, Roberto Di Cosmo, and Marcelo P. Fiore. Extensional normalisation and type-directed partial evaluation for typed lambda calculus with sums. In Xavier Leroy, editor, *Proceedings of the Thirty-First Annual ACM Symposium on Principles of Programming Languages*, pages 64–76, Venice, Italy, January 2004. ACM Press.

[2] Nick Benton and Vasileios Koutavas. A mechanized bisimulation for the nu-calculus. Technical Report MSR-TR-2008-129, Microsoft Research, September 2008.

[3] Dariusz Biernacki and Olivier Danvy. A simple proof of a folklore theorem about delimited control. *Journal of Functional Programming*, 16(3):269–280, 2006.

[4] Dariusz Biernacki and Sergueï Lenglet. Applicative bisimulations for delimited-control operators. In Lars Birkedal, editor, *Foundations of Software Science and Computation Structures, 15th International Conference (FOSSACS'12)*, volume 7213 of *Lecture Notes in Computer Science*, pages 119–134, Tallinn, Estonia, March 2012. Springer.

[5] Dariusz Biernacki and Sergueï Lenglet. Normal form bisimulations for delimited-control operators. In Tom Schrijvers and Peter Thiemann, editors, *Functional and Logic Programming, 13th International Symposium (FLOPS'12)*, volume 7294 of *Lecture Notes in Computer Science*, pages 47–61, Kobe, Japan, May 2012. Springer.

[6] Dariusz Biernacki and Sergueï Lenglet. Environmental bisimulations for delimited-control operators. In Chung-chieh Shan, editor, *Proceedings of the 11th Asian Symposium on Programming Languages and Systems (APLAS'13)*, volume 8301 of *Lecture Notes in Computer Science*, pages 333–348, Melbourne, VIC, Australia, December 2013. Springer.

[7] Dariusz Biernacki and Piotr Polesiuk. Logical relations for coherence of effect subtyping. In Thorsten Altenkirch, editor, *Typed Lambda Calculi and Applications, 13th International Conference, TLCA 2015*, volume 38 of *Leibniz International Proceedings in Informatics*, pages 107–122, Warsaw, Poland, July 2015. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[8] Olivier Danvy and Andrzej Filinski. Abstracting control. In Mitchell Wand, editor, *Proceedings of the 1990 ACM Conference on Lisp and Functional Programming*, pages 151–160, Nice, France, June 1990. ACM Press.

[9] Derek Dreyer, Georg Neis, and Lars Birkedal. The impact of higher-order state and control effects on local relational reasoning. *Journal of Functional Programming*, 22(4-5):477–528, 2012.

[10] R. Kent Dybvig, Simon Peyton-Jones, and Amr Sabry. A monadic framework for delimited continuations. *Journal of Functional Programming*, 17(6):687–730, 2007.

[11] Matthias Felleisen. The theory and practice of first-class prompts. In Jeanne Ferrante and Peter Mager, editors, *Proceedings of the Fifteenth Annual ACM Symposium on Principles of Programming Languages*, pages 180–190, San Diego, California, January 1988. ACM Press.

[12] Andrzej Filinski. Representing monads. In Hans-J. Boehm, editor, *Proceedings of the Twenty-First Annual ACM Symposium on Principles of Programming Languages*, pages 446–457, Portland, Oregon, January 1994. ACM Press.

[13] Matthew Flatt, Gang Yu, Robert Bruce Findler, and Matthias Felleisen. Adding delimited and composable control to a production programming environment. In Norman Ramsey, editor, *Proceedings of the 2007 ACM SIGPLAN International Conference on Functional Programming (ICFP'07)*, pages 165–176, Freiburg, Germany, September 2007. ACM Press.

[14] Carl Gunter, Didier Rémy, and Jon G. Riecke. A generalization of exceptions and control in ML-like languages. In Simon Peyton Jones, editor, *Proceedings of the Seventh ACM Conference on Functional Programming and Computer Architecture*, pages 12–23, La Jolla, California, June 1995. ACM Press.

[15] Chung-Kil Hur, Derek Dreyer, Georg Neis, and Viktor Vafeiadis. The marriage of bisimulations and Kripke logical relations. In John Field and Michael Hicks, editors, *Proceedings of the Thirty-Ninth Annual ACM Symposium on Principles of Programming Languages*, pages 59–72, Philadelphia, PA, USA, January 2012. ACM Press.

[16] Chung-Kil Hur, Georg Neis, Derek Dreyer, and Viktor Vafeiadis. A logical step forward in parametric bisimulations. Technical Report MPI-SWS-2014-003, Max Planck Institute for Software Systems (MPI-SWS), Saarbrücken, Germany, January 2014.

[17] Yukiyoshi Kameyama and Masahito Hasegawa. A sound and complete axiomatization of delimited continuations. In Olin Shivers, editor, *Proceedings of the 2003 ACM SIGPLAN International Conference on Functional Programming (ICFP'03)*, pages 177–188, Uppsala, Sweden, August 2003. ACM Press.

[18] Oleg Kiselyov. Delimited control in OCaml, abstractly and concretely: System description. In Matthias Blume and German Vidal, editors, *Functional and Logic Programming, 10th International Symposium, FLOPS 2010*, volume 6009 of *Lecture Notes in Computer Science*, pages 304–320, Sendai, Japan, April 2010. Springer.

[19] Ikuo Kobori, Yukiyoshi Kameyama, and Oleg Kiselyov. ATM without tears: prompt-passing style transformation for typed delimited-control operators. In Olivier Danvy, editor, *2015 Workshop on Continuations: Pre-proceedings*, London, UK, April 2015.

[20] Vasileios Koutavas, Paul Blain Levy, and Eijiro Sumii. From applicative to environmental bisimulation. In Michael Mislove and Joël Ouaknine, editors, *Proceedings of the 27th Annual Conference on Mathematical Foundations of Programming Semantics (MFPS XXVII)*, volume 276 of *Electronic Notes in Theoretical Computer Science*, pages 215–235, Pittsburgh, PA, USA, May 2011.

[21] Vasileios Koutavas and Mitchell Wand. Bisimulations for untyped imperative objects. In Peter Sestoft, editor, *15th European Symposium on Programming, ESOP 2006*, volume 3924 of *Lecture Notes in Computer Science*, pages 146–161, Vienna, Austria, March 2006. Springer.

[22] Vasileios Koutavas and Mitchell Wand. Small bisimulations for reasoning about higher-order imperative programs. In J. Gregory Morrisett and Simon L. Peyton Jones, editors, *Proceedings of the 33rd Annual ACM Symposium on Principles of Programming Languages*, pages 141–152, Charleston, SC, USA, January 2006. ACM Press.

[23] Jean-Marie Madiot. *Higher-Order Languages: Dualities and Bisimulation Enhancements*. PhD thesis, Université de Lyon and Università di Bologna, 2015.

[24] Jean-Marie Madiot, Damien Pous, and Davide Sangiorgi. Bisimulations up-to: Beyond first-order transition systems. In Paolo Baldan and Daniele Gorla, editors, *25th International Conference on Concurrency Theory*, volume 8704 of *Lecture Notes in Computer Science*, pages 93–108, Rome, Italy, September 2014. Springer.

[25] Adrien Piérard and Eijiro Sumii. A higher-order distributed calculus with name creation. In *Proceedings of the 27th IEEE Symposium on Logic in Computer Science (LICS 2012)*, pages 531–540, Dubrovnik, Croatia, June 2012. IEEE Computer Society Press.

[26] Andrew Pitts and Ian Stark. Operational reasoning for functions with local state. In Andrew Gordon and Andrew Pitts, editors, *Higher Order Operational Techniques in Semantics*, pages 227–273. Publications of the Newton Institute, Cambridge University Press, 1998.

[27] Damien Pous and Davide Sangiorgi. Enhancements of the bisimulation proof method. In Davide Sangiorgi and Jan Rutten, editors, *Advanced Topics in Bisimulation and Coinduction*, chapter 6, pages 233–289. Cambridge University Press, 2011.

[28] Davide Sangiorgi, Naoki Kobayashi, and Eijiro Sumii. Environmental bisimulations for higher-order languages. *ACM Transactions on Programming Languages and Systems*, 33(1):1–69, January 2011.

[29] Eijiro Sumii. A complete characterization of observational equivalence in polymorphic lambda-calculus with general references. In Erich Grädel and Reinhard Kahle, editors, *Computer Science Logic, CSL'09*, volume 5771 of *Lecture Notes in Computer Science*, pages 455–469, Coimbra, Portugal, September 2009. Springer.

[30] Eijiro Sumii and Benjamin C. Pierce. A bisimulation for dynamic sealing. *Theoretical Computer Science*, 375(1-3):169–192, 2007.

[31] Eijiro Sumii and Benjamin C. Pierce. A bisimulation for type abstraction and recursion. *Journal of the ACM*, 54(5), 2007.

A Proofs for Section 3

A.1 Compatibility proofs

Lemma 6. $\mathsf{perm} \rightsquigarrow \mathsf{perm}$.

Proof. Let $(\Gamma\sigma_1, e_1\sigma_1)$ $\mathsf{perm}(\mathcal{R})$ $(\Delta\sigma_2, e_2\sigma_2)$ with (Γ, e_1) $\mathcal{R}$ (Δ, e_2). The only interesting case is for $\xrightarrow{\tau}$ transitions. Suppose we have $e_1\sigma_1 \to e_1'$ with $\mathsf{fresh}(e_1', e_1\sigma_1, \Gamma\sigma_1)$. There exists e_1'' such that $e_1' = e_1''\sigma_1$, and we have $e_1 \to e_1''$ by Lemma 1. From $\mathsf{fresh}(e_1''\sigma_1, e_1\sigma_1, \Gamma\sigma_1)$ and Lemma 1, we deduce $\mathsf{fresh}(e_1'', e_1, \Gamma)$, and therefore we have $(\Gamma, e_1) \xrightarrow{\tau} (\Gamma, e_1'')$. Consequently, there exists e_2'' such that $(\Delta, e_2) \stackrel{\tau}{\Rightarrow} (\Delta, e_2'')$ and $e_1'' \mathcal{S} e_2''$, which in turn implies $(\Delta\sigma_2, e_2\sigma_2) \stackrel{\tau}{\Rightarrow} (\Delta\sigma_2, e_2''\sigma_2)$ by Lemmas 1 and 1. We have $(\Gamma\sigma_1, e_1''\sigma_1)$ $\mathsf{perm}(\mathcal{S})$ $(\Delta\sigma_2, e_2''\sigma_2)$, as wished.

□

Lemma 7. $\mathsf{weak} \rightsquigarrow (\mathsf{perm} \cup \mathsf{id}) \circ \mathsf{weak}$.

Proof. Let (Γ, e_1) $\mathsf{weak}(\mathcal{R})$ (Δ, e_2) with $(v_1 \dots v_n, \Gamma, e_1)$ $\mathcal{R}$ $(w_1 \dots w_n, \Delta, e_2)$. Suppose $e_1 \to e_1'$ with $\mathsf{fresh}(e_1', e_1, \Gamma)$. Some generated prompts could be in $\bigcup_{1 \le i \le n} \#(v_i)$, so let σ be a permutation that maps $\#(e_1') \setminus \#(e_1)$ to fresh prompts (not in e_1, e_1', Γ, nor v_i for all $1 \le i \le n$). By Lemma 1, we have $e_1 \to e_1'\sigma$, and we also have $\mathsf{fresh}(e_1'\sigma, e_1, v_1 \dots v_n, \Gamma)$ by construction. Consequently, we have $(v_1 \dots v_n, \Gamma, e_1) \xrightarrow{\tau} (v_1 \dots v_n, \Gamma, e_1'\sigma)$, which means $\exists e_2'$ such that $(w_1 \dots w_n, \Delta, e_2) \stackrel{\tau}{\Rightarrow} (w_1 \dots w_n, \Delta, e_2')$ and $(v_1 \dots v_n, \Gamma, e_1'\sigma)$ $\mathcal{S}$ $(w_1 \dots w_n, \Delta, e_2')$. Therefore we have $(\Gamma, e_1'\sigma)$ $\mathsf{weak}(\mathcal{S})$ (Δ, e_2') and by composing with σ^{-1} on the left and the identity on the right, we get (Γ, e_1') $\mathsf{perm}(\mathsf{weak}(\mathcal{S}))$ (Δ, e_2'), hence we have the required result.

Suppose $(\Gamma, e_1) \xrightarrow{\mathbb{E}} (\Gamma, e_1')$. Then $(v_1 \dots v_n, \Gamma, e_1) \xrightarrow{\mathbb{E}_{+n}} (v_1 \dots v_n, \Gamma, e_1')$, where each hole $\Box_j$ in $\mathbb{E}$ is shifted to $\Box_{j+n}$ in $\mathbb{E}_{+n}$. So there exists e_2' such that $(w_1 \dots w_n, \Delta, e_2) \stackrel{\mathbb{E}_{+n}}{\Longrightarrow} (w_1 \dots w_n, \Delta, e_2')$ and $(v_1 \dots v_n, \Gamma, e_1')$ $\mathcal{S}$ $(w_1 \dots w_n, \Delta, e_2')$, which in turn implies $(\Delta, e_2) \stackrel{\mathbb{E}}{\Rightarrow} (\Delta, e_2')$ and (Γ, e_1') $\mathsf{weak}(\mathcal{S})$ (Δ, e_2'), as wished.

Suppose e_1 is a value v. For $\xrightarrow{\lambda, i, \mathbb{C}_\mathsf{v}}$ and $\xrightarrow{\ulcorner \cdot \urcorner, i, \mathbb{C}}$ transitions, the proof is the same as for $\xrightarrow{\mathbb{E}}$ transitions. The case $(\Gamma, v) \xrightarrow{\mathsf{v}} (\Gamma, v)$ follows from the fact that $(v_1 \dots v_n, \Gamma, v) \xrightarrow{\mathsf{v}} (v_1 \dots v_n, \Gamma, v)$ has to be matched by $(w_1 \dots w_n, \Gamma, e_2)$. If $(\Gamma, v) \xrightarrow{\#, i, j} (\Gamma, v)$, then we have $(v_1 \dots v_n, \Gamma, v) \xrightarrow{\#, i+n, j+n} (v_1 \dots v_n, \Gamma, v)$, which implies $(w_1 \dots w_n, \Delta, e_2) \stackrel{\#, i+n, j+n}{\Longrightarrow} (w_1 \dots w_n, \Delta, w)$ for some w, with $(v_1 \dots v_n, \Gamma)$ $\mathcal{S}$ $(w_1 \dots w_n, \Delta, w)$. In turn, we have $(\Delta, e_2) \stackrel{\#, i, j}{\Longrightarrow} (\Delta, w)$ with (Γ, v) $\mathsf{weak}(\mathcal{S})$ (Δ, w), hence the result holds. Finally, if $(\Gamma, v) \xrightarrow{\#} (\Gamma, v, p)$, then the generated prompt might be in $v_1 \dots v_n$, so let σ be a permutation which rename p into a fresh prompt. Then we have $(v_1 \dots v_n, \Gamma, v) \xrightarrow{\#} (v_1 \dots v_n, \Gamma, v, p\sigma)$, which implies $(w_1 \dots w_n, \Delta, e_2) \stackrel{\#}{\Rightarrow} (w_1 \dots w_n, \Delta, w, q)$ for some q and w, with also $(v_1 \dots v_n, \Gamma, v, p\sigma)$ $\mathcal{S}$ $(w_1 \dots w_n, \Delta, w, q)$. As a result, we have $(\Delta, e_2) \stackrel{\#}{\Rightarrow} (\Delta, w, q)$ with (Γ, v, p) $\mathsf{perm}(\mathsf{weak}(\mathcal{S}))$ (Δ, w, q) (using σ^{-1} on the left and the identity permutation on the right), as wished.

□

Lemma 8. $\mathsf{str} \rightsquigarrow \mathsf{str} \circ (\mathsf{id} \cup \mathsf{ctx})$

Proof. Let $(\Gamma, \mathbb{C}_\mathsf{v}[\Gamma], e_1)$ $\mathsf{str}(\mathcal{R})$ $(\Delta, \mathbb{C}_\mathsf{v}[\Delta], e_2)$ so that (Γ, e_1) $\mathcal{R}$ (Δ, e_2). We write n the size of Γ.

Suppose $e_1 \to e_1'$ with $\mathsf{fresh}(e_1', e_1, (\Gamma, \mathbb{C}_\mathsf{v}[\Gamma]))$. We also have $\mathsf{fresh}(e_1', e_1, \Gamma)$, so there exists e_2' such that $(\Delta, e_2) \stackrel{\tau}{\Rightarrow} (\Delta, e_2')$ and (Γ, e_1') $\mathcal{S}$ (Δ, e_2'). We have $\mathsf{fresh}(e_2', e_2, \Delta)$, which implies $\mathsf{fresh}(e_2', e_2, (\Delta, \mathbb{C}_\mathsf{v}[\Delta]))$ because $\#(\mathbb{C}_\mathsf{v}) = \emptyset$. Hence, we have $(\Delta, \mathbb{C}_\mathsf{v}[\Delta], e_2) \stackrel{\tau}{\Rightarrow} (\Delta, \mathbb{C}_\mathsf{v}[\Delta], e_2')$, with $(\Gamma, \mathbb{C}_\mathsf{v}[\Gamma], e_1')$ $\mathsf{str}(\mathcal{S})$ $(\Delta, \mathbb{C}_\mathsf{v}[\Delta], e_2')$, as wished.

Suppose $(\Gamma, \mathbb{C}_\mathsf{v}[\Gamma], e_1) \xrightarrow{\mathbb{E}} (\Gamma, \mathbb{C}_\mathsf{v}[\Gamma], e_1')$. Then we also have the transition $(\Gamma, e_1) \xrightarrow{\mathbb{E}[\mathbb{C}_\mathsf{v}/\Box_{n+1}]} (\Gamma, e_1')$, where $\mathbb{E}[\mathbb{C}_\mathsf{v}/\Box_{n+1}]$ is the context obtained from $\mathbb{E}$ by replacing its $n+1$-th hole with $\mathbb{C}_\mathsf{v}$. Consequently, there exists e_2' such that $(\Delta, e_2) \stackrel{\mathbb{E}[\mathbb{C}_\mathsf{v}/\Box_{n+1}]}{\Longrightarrow} (\Delta, e_2')$ and (Γ, e_1') $\mathcal{S}$ (Δ, e_2'), which implies $(\Delta, \mathbb{C}_\mathsf{v}[\Delta], e_2) \stackrel{\mathbb{E}}{\Rightarrow} (\Delta, \mathbb{C}_\mathsf{v}[\Delta], e_2')$. The resulting terms are in $\mathsf{str}(\mathcal{S})$.

Suppose e_1 is a value v_1. We write $\Gamma' \stackrel{\mathsf{def}}{=} (\Gamma, v_1)$, and $\Gamma'' \stackrel{\mathsf{def}}{=} (\Gamma, \mathbb{C}_\mathsf{v}[\Gamma], v_1)$. We look at the possible transitions of Γ''. First, we have $\Gamma' \xrightarrow{\mathsf{v}} \Gamma'$, therefore there exists v_2 such that $(\Delta, e_2) \stackrel{\mathsf{v}}{\Rightarrow} (\Delta, v_2)$ and $\Gamma'\ \mathcal{S}\ (\Delta, v_2)$. We also have $\Gamma'' \xrightarrow{\mathsf{v}} \Gamma''$, $(\Delta, \mathbb{C}_\mathsf{v}[\Gamma_2], e_2) \stackrel{\mathsf{v}}{\Rightarrow} (\Delta, \mathbb{C}_\mathsf{v}[\Gamma_2], v_2)$ with $\Gamma''\ \mathsf{str}(\mathcal{S})\ (\Delta, \mathbb{C}_\mathsf{v}[\Gamma_2], v_2)$, as wished.

If $\Gamma'' \xrightarrow{\#} (\Gamma'', p)$, then because $p \notin \#(\Gamma'')$, we also have $p \notin \#(\Gamma')$. Therefore, we have $\Gamma' \xrightarrow{\#} (\Gamma', p)$, so there exist v_2, q such that $(\Delta, e_2) \stackrel{\#}{\Rightarrow} (\Delta, v_2, q)$ and $(\Gamma', p)\ \mathcal{S}\ (\Delta, v_2, q)$. We have $q \notin \#(\Delta, v_2)$, and because $\#(\mathbb{C}_\mathsf{v}) = \emptyset$, we also have $q \notin \#(\Delta, \mathbb{C}_\mathsf{v}[\Delta], v_2)$. As a result, we have $(\Delta, \mathbb{C}_\mathsf{v}[\Delta], e_2) \stackrel{\#}{\Rightarrow} (\Delta, \mathbb{C}_\mathsf{v}[\Delta], v_2, q)$, with $(\Gamma'', p)\ \mathsf{str}(\mathcal{S})\ (\Delta, \mathbb{C}_\mathsf{v}[\Delta], v_2, q)$, as wished.

The remaining transitions test Γ''_i depending on the kind of value it is. We distinguish cases based on i.

If $i \leq n$ or $i = n+2$, then we test a value from Γ'. Suppose, e.g., that $\Gamma'' \xrightarrow{\lambda, i, \mathbb{C}'_\mathsf{v}} (\Gamma'', e'_1)$. Then we have $\Gamma' \xrightarrow{\lambda, i, \mathbb{C}'_\mathsf{v}[\mathbb{C}_\mathsf{v}/\Box_{n+1}]} (\Gamma', e'_1)$ for $i \leq n$, or $\Gamma' \xrightarrow{\lambda, n+1, \mathbb{C}'_\mathsf{v}[\mathbb{C}_\mathsf{v}/\Box_{n+1}]} (\Gamma', e'_1)$ if $i = n+2$, where $\mathbb{C}'_\mathsf{v}[\mathbb{C}_\mathsf{v}/\Box_{n+1}]$ is obtained by replacing the $n+1$-th hole of $\mathbb{C}'_\mathsf{v}$ with $\mathbb{C}_\mathsf{v}$. We suppose $i \leq n$, the case $i = n+2$ is similar. There exists v_2, e'_2 such that $(\Delta, e_2) \stackrel{\lambda, i, \mathbb{C}'_\mathsf{v}[\mathbb{C}_\mathsf{v}/\Box_{n+1}]}{\Longrightarrow} (\Delta, v_2, e'_2)$ and $(\Gamma', e'_1)\ \mathcal{S}\ (\Delta, v_2, e'_2)$. Consequently, we have $(\Delta, \mathbb{C}_\mathsf{v}[\Delta], e_2) \stackrel{\lambda, i, \mathbb{C}'_\mathsf{v}}{\Longrightarrow} (\Delta, \mathbb{C}_\mathsf{v}[\Delta], v_2, e'_2)$ with $(\Gamma'', e'_1)\ \mathsf{str}(\mathcal{S})\ (\Delta, \mathbb{C}_\mathsf{v}[\Delta], v_2, e'_2)$, as wished. The case $\Gamma'' \xrightarrow{\ulcorner . \urcorner, i, \mathbb{C}} (\Gamma'', e'_1)$ is similar, and the case $\Gamma'' \xrightarrow{\#, i, j} \Gamma''$ is simpler.

If $i = n+1$, then we test $\mathbb{C}_\mathsf{v}[\Gamma]$. Suppose, e.g., that $\Gamma'' \xrightarrow{\lambda, n+1, \mathbb{C}'_\mathsf{v}} (\Gamma'', e'_1)$. Then e'_1 can be written $\mathbb{C}[\Gamma']$ for some $\mathbb{C}$ (combining $\mathbb{C}'_\mathsf{v}$ and $\mathbb{C}_\mathsf{v}$). Because $\Gamma' \xrightarrow{\mathsf{v}} \Gamma'$, there exists v_2 such that $(\Delta, e_2) \stackrel{\mathsf{v}}{\Rightarrow} (\Delta, v_2) \stackrel{\mathsf{def}}{=} \Delta'$ and $\Gamma'\ \mathcal{S}\ \Delta'$. Let $\Delta'' \stackrel{\mathsf{def}}{=} (\Delta, \mathbb{C}_\mathsf{v}[\Delta], v_2)$. Then we have $(\Delta, \mathbb{C}_\mathsf{v}[\Delta], e_2) \stackrel{\tau}{\Rightarrow} \Delta'' \xrightarrow{\lambda, n+1, \mathbb{C}'_\mathsf{v}} (\Delta'', \mathbb{C}[\Delta'])$ with $(\Gamma'', \mathbb{C}[\Gamma'])\ \mathsf{str}(\mathsf{ctx}(\mathcal{S}))\ (\Delta'', \mathbb{C}[\Delta'])$. The case $\Gamma'' \xrightarrow{\ulcorner . \urcorner, n+1, \mathbb{C}} (\Gamma'', e'_1)$ is similar, and the case $\Gamma'' \xrightarrow{\#, n+1, j} \Gamma''$ is simpler.

□

Lemma 9. $\mathsf{ctx} \rightsquigarrow \mathsf{str} \cup \mathsf{str} \circ \mathsf{ctx} \cup \mathsf{ctx} \cup \mathsf{ectx}$.

Proof. Let $(\Gamma, \mathbb{C}[\Gamma])\ \mathsf{ctx}(\mathcal{R})\ (\Delta, \mathbb{C}[\Delta])$ so that $\Gamma\ \mathcal{R}\ \Delta$. We write n the size of Γ. If $\mathbb{C} = \Box_i$ for some i, then we progress to str, so we assume now that $\mathbb{C} \neq \Box_i$.

First, we assume $\mathbb{C}$ is a value context $\mathbb{C}_\mathsf{v}$. The transition $\xrightarrow{\mathsf{v}}$ is easily matched (we stay in ctx). Suppose $(\Gamma, \mathbb{C}_\mathsf{v}[\Gamma]) \xrightarrow{\#} (\Gamma, \mathbb{C}_\mathsf{v}[\Gamma], p)$. We also have $\Gamma \xrightarrow{\#} (\Gamma, p)$, therefore there exists q such that $\Delta \stackrel{\#}{\Rightarrow} (\Delta, q)$ and $(\Gamma, p)\ \mathcal{S}\ (\Gamma, q)$. Because $\#(\mathbb{C}_\mathsf{v}) = \emptyset$, we also have $(\Delta, \mathbb{C}_\mathsf{v}[\Delta]) \stackrel{\#}{\Rightarrow} (\Delta, \mathbb{C}_\mathsf{v}[\Delta], q)$, with $(\Gamma, \mathbb{C}_\mathsf{v}[\Gamma], p)\ \mathsf{ctx}(\mathcal{S})\ (\Delta, \mathbb{C}_\mathsf{v}[\Delta], q)$, as wished.

Suppose $(\Gamma, \mathbb{C}_\mathsf{v}[\Gamma]) \xrightarrow{\lambda, i, \mathbb{C}'_\mathsf{v}} (\Gamma, \mathbb{C}_\mathsf{v}[\Gamma], e'_1)$. If $i = n+1$, then we have $(\Gamma, \mathbb{C}_\mathsf{v}[\Gamma]) \xrightarrow{\lambda, n+1, \mathbb{C}'_\mathsf{v}} (\Gamma, \mathbb{C}_\mathsf{v}[\Gamma], \mathbb{C}'_\mathsf{v}[\Gamma])$ for some $\mathbb{C}'_\mathsf{v}$, and similarly for $(\Delta, \mathbb{C}_\mathsf{v}[\Delta])$; we obtain terms in $\mathsf{str}(\mathsf{ctx}(\mathcal{R}))$. Suppose $i < n+1$. Then $(\Gamma, \mathbb{C}_\mathsf{v}[\Gamma]) \xrightarrow{\lambda, i, \mathbb{C}'_\mathsf{v}} (\Gamma, \mathbb{C}_\mathsf{v}[\Gamma], e'_1)$ implies $\Gamma \xrightarrow{\lambda, i, \mathbb{C}'_\mathsf{v}[\mathbb{C}_\mathsf{v}/\Box_{n+1}]} (\Gamma, e'_1)$, where $\mathbb{C}'_\mathsf{v}[\mathbb{C}_\mathsf{v}/\Box_{n+1}]$ is the context obtained by replacing the $n+1$-th hole of $\mathbb{C}'_\mathsf{v}$ with $\mathbb{C}_\mathsf{v}$. Consequently, there exists e'_2 such that $\Delta \stackrel{\lambda, i, \mathbb{C}'_\mathsf{v}[\mathbb{C}_\mathsf{v}/\Box_{n+1}]}{\Longrightarrow} (\Delta, e'_2)$ and $(\Gamma, e'_1)\ \mathcal{S}\ (\Delta, e'_2)$. This implies $(\Delta, \mathbb{C}_\mathsf{v}[\Delta]) \stackrel{\lambda, i, \mathbb{C}'_\mathsf{v}}{\Longrightarrow} (\Delta, \mathbb{C}_\mathsf{v}[\Delta], e'_2)$, and we have $(\Gamma, \mathbb{C}_\mathsf{v}[\Gamma], e'_1)\ \mathsf{str}(\mathcal{S})\ (\Delta, \mathbb{C}_\mathsf{v}[\Delta], e'_2)$, as wished. The proof for $\xrightarrow{\ulcorner . \urcorner, i, \mathbb{C}'}$ is similar.

Suppose $(\Gamma, \mathbb{C}_\mathsf{v}[\Gamma]) \xrightarrow{\#, i, j} (\Gamma, \mathbb{C}_\mathsf{v}[\Gamma])$. If $i, j \leq n$, then the transition comes from Γ, and we progress to str. If i and/or $j = n+1$, then $\mathbb{C}_\mathsf{v} = \Box_k$ for some k, and we have either $\Gamma \xrightarrow{\#, k, j} \Gamma$ (if $i = n+1$ and $j \neq n+1$), $\Gamma \xrightarrow{\#, k, i} \Gamma$ (if $i \neq n+1$ and $j = n+1$), or $\Gamma \xrightarrow{\#, k, k} \Gamma$ (if $i = j = n+1$). In the three cases, Δ matches the transition, and so does $(\Delta, \mathbb{C}_\mathsf{v}[\Delta])$, and we progress to str.

Now, we assume $\mathbb{C}[\Gamma]$ is not a value. If $(\Gamma, \mathbb{C}[\Gamma]) \xrightarrow{\mathbb{E}} (\Gamma, e'_1)$, then $e'_1 = \mathbb{C}'[\Gamma]$ for some $\mathbb{C}'$, and we also have $(\Delta, \mathbb{C}[\Delta]) \xrightarrow{\mathbb{E}} (\Delta, \mathbb{C}'[\Delta])$. The two terms are in $\mathsf{ctx}(\mathcal{R})$.

Suppose $(\Gamma, \mathbb{C}[\Gamma]) \xrightarrow{\tau} (\Gamma, e'_1)$. If the transition comes from $\mathbb{C}$ and does not generate a new prompt, i.e., $(\Gamma, \mathbb{C}[\Gamma]) \xrightarrow{\tau} (\Gamma, \mathbb{C}'[\Gamma])$, for some $\mathbb{C}'$, then we also have $(\Delta, \mathbb{C}[\Delta]) \xrightarrow{\tau} (\Delta, \mathbb{C}'[\Delta])$, and we progress to $\mathsf{ctx}(\mathcal{R})$.

If a prompt p is generated, then we have $(\Gamma, \mathbb{C}[\Gamma]) \xrightarrow{\tau} (\Gamma, \mathbb{C}'[\Gamma, p])$, for some $\mathbb{C}'$. Because $\Gamma \xrightarrow{\#} (\Gamma, p)$, there exists q such that $\Delta \stackrel{\#}{\Rightarrow} (\Delta, q)$ and $(\Gamma, p)\ \mathcal{S}\ (\Delta, q)$. We also have $(\Delta, \mathbb{C}[\Delta]) \xrightarrow{\tau} (\Delta, \mathbb{C}'[\Delta, q])$, with $(\Gamma, \mathbb{C}'[\Gamma, p])\ \mathsf{ctx}(\mathcal{S})\ (\Delta, \mathbb{C}'[\Delta, q])$, as wished.

Otherwise, a Γ_i is involved, and we have several possibilities. First, suppose $\mathbb{C}[\Gamma] = \mathbb{E}[\Gamma_i \mathbb{C}_{\mathsf{v}}[\Gamma], \Gamma]$ for some $\mathbb{E}$, $\mathbb{C}_{\mathsf{v}}$, and Γ_i is a λ-abstraction. We have $\Gamma \xrightarrow{\lambda, i, \mathbb{C}_{\mathsf{v}}} (\Gamma, e_1'')$, which means $(\Gamma, \mathbb{C}[\Gamma]) \xrightarrow{\tau} (\Gamma, \mathbb{E}[e_1'', \Gamma])$. Because $\Gamma\ \mathcal{R}\ \Delta$, there exists e_2'' such that $\Delta \xRightarrow{\lambda, i, \mathbb{C}_{\mathsf{v}}} (\Delta, e_2'')$ and $(\Gamma, e_1'')\ \mathcal{S}\ (\Delta, e_2'')$. Consequently, we have $(\Delta, \mathbb{C}[\Delta]) \stackrel{\tau}{\Rightarrow} (\Delta, \mathbb{E}[e_2'', \Delta])$, with $(\Gamma, \mathbb{E}[e_1'', \Gamma])\ \mathsf{ectx}(\mathcal{S})\ (\Delta, \mathbb{E}[e_2'', \Delta])$, as wished. The case where $\mathbb{C}[\Gamma] = \mathbb{E}[\Gamma_i \triangleleft \mathbb{C}'[\Gamma], \Gamma]$ for some $\mathbb{E}$, $\mathbb{C}'$, and Γ_i is a continuation, is treated similarly. Finally, if $\mathbb{C}[\Gamma] = \mathbb{E}[\#_p \Gamma_i, \Gamma]$ for some $\mathbb{E}$, then $(\Gamma, \mathbb{C}[\Gamma]) \stackrel{\tau}{\Rightarrow} (\Gamma, \mathbb{E}[\Gamma_i, \Gamma]$, but we also have $(\Delta, \mathbb{C}[\Delta]) \stackrel{\tau}{\Rightarrow} (\Delta, \mathbb{E}[\Delta_i, \Delta]$, with $(\Gamma, \mathbb{E}[\Gamma_i, \Gamma])\ \mathsf{ectx}(\mathcal{R})\ (\Delta, \mathbb{E}[\Delta_i, \Delta])$, as wished.

□

Lemma 10. $\mathsf{ectx} \rightsquigarrow \mathsf{ectx} \cup \mathsf{id} \cup \mathsf{weak} \circ (\mathsf{ctx} \cup \mathsf{ectx})$.

Proof. Let $(\Gamma, \mathbb{E}[e_1, \Gamma])\ \mathsf{ectx}(\mathcal{R})\ (\Delta, \mathbb{E}[e_2, \Delta])$ so that $(\Gamma, e_1)\ \mathcal{R}\ (\Delta, e_2)$. We write n the size of Γ.

Suppose e_1 is not a value nor a stuck term, and $(\Gamma, \mathbb{E}[e_1, \Gamma]) \xrightarrow{\tau} (\Gamma, \mathbb{E}[e_1', \Gamma])$ with $\mathsf{fresh}(\mathbb{E}[e_1', \Gamma], \mathbb{E}[e_1, \Gamma], \Gamma)$. Because $\#(\mathbb{E}) = \emptyset$, we also have $\mathsf{fresh}(e_1', e_1, \Gamma)$, and therefore $(\Gamma, e_1) \xrightarrow{\tau} (\Gamma, e_1')$ holds. As a result, there exists e_2' such that $(\Delta, e_2) \stackrel{\tau}{\Rightarrow} (\Delta, e_2')$ and $(\Gamma, e_1')\ \mathcal{S}\ (\Delta, e_2')$. Because $\#(\mathbb{E}) = \emptyset$, we have $(\Delta, \mathbb{E}[e_2, \Delta]) \stackrel{\tau}{\Rightarrow} (\Delta, \mathbb{E}[e_2', \Delta])$ with $(\Gamma, \mathbb{E}[e_1', \Delta])\ \mathsf{ectx}(\mathcal{S})\ (\Delta, \mathbb{E}[e_2', \Delta])$, as wished.

Suppose e_1 is a stuck term, and $(\Gamma, \mathbb{E}[e_1, \Gamma]) \xrightarrow{\mathbb{E}'} (\Gamma, e_1')$. Then we also have $(\Gamma, e_1) \xrightarrow{\mathbb{E}'[\mathbb{E}/\Box]} (\Gamma, e_1')$, where $\mathbb{E}'[\mathbb{E}/\Box_1]$ is the context obtained by replacing $\Box$ by $\mathbb{E}$. Consequently, there exists e_2' such that $(\Delta, e_2) \xRightarrow{\mathbb{E}'[\mathbb{E}/\Box]} (\Delta, e_2')$ and $(\Delta, e_1')\ \mathcal{S}\ (\Delta, e_2')$. This implies $(\Delta, \mathbb{E}[e_2, \Delta]) \stackrel{\mathbb{E}'}{\Rightarrow} (\Delta, e_2')$, and we have the required result.

Suppose e_1 is a stuck term, and $(\Gamma, \mathbb{E}[e_1, \Gamma]) \xrightarrow{\tau} (\Gamma, e_1')$. Then $\mathbb{E} = \mathbb{E}_1 \#_{\Box_i} \mathbb{E}_2$, and we have $(\Gamma, e_1) \xrightarrow{\#_{\Box_i} \mathbb{E}_2} (\Gamma, e_1'')$, such that $e_1' = \mathbb{E}_1[e_1'', \Gamma]$. There exists e_2'' such that $(\Delta, e_2) \xRightarrow{\#_{\Box_i} \mathbb{E}_2} (\Delta, e_2'')$ and $(\Gamma, e_1'')\ \mathcal{S}\ (\Delta, e_2'')$. Consequently, we have $(\Delta, \mathbb{E}[e_2, \Delta]) \stackrel{\tau}{\Rightarrow} (\Delta, \mathbb{E}_1[e_2'', \Delta])$ with $(\Gamma, \mathbb{E}_1[e_1'', \Delta])\ \mathsf{ectx}(\mathcal{S})\ (\Delta, \mathbb{E}_1[e_2'', \Delta])$, as wished.

Suppose e_1 is a value v_1. If $\mathbb{E} = \Box$, then we progress to $\mathcal{S}$. Otherwise, $\mathbb{E}[v_1, \Gamma]$ is not a value. Because $(\Gamma, v_1)\ \mathcal{R}\ (\Delta, e_2)$ and $(\Gamma, v_1) \xrightarrow{\mathsf{v}} (\Gamma, v_1)$, there exists v_2 such that $(\Delta, e_2) \stackrel{\mathsf{v}}{\Rightarrow} (\Delta, v_2)$ and $(\Gamma, v_1)\ \mathcal{S}\ (\Delta, v_2)$. Let $\Gamma' = (\Gamma, v_1)$ and $\Delta' = (\Delta, v_2)$.

If $(\Gamma, \mathbb{E}[\Gamma']) \xrightarrow{\mathbb{E}'} (\Gamma, e_1')$, then $e_1' = \mathbb{C}'[\Gamma']$ for some $\mathbb{C}'$, and we also have $(\Delta, \mathbb{E}[\Delta']) \xrightarrow{\mathbb{E}'} (\Delta, \mathbb{C}'[\Delta'])$. We progress to $\mathsf{weak}(\mathsf{ctx}(\mathcal{S}))$.

Suppose $(\Gamma, \mathbb{E}[\Gamma']) \xrightarrow{\tau} (\Gamma, e_1')$. If the transition comes from $\mathbb{E}$, i.e., $(\Gamma, \mathbb{E}[\Gamma']) \xrightarrow{\tau} (\Gamma, \mathbb{C}'[\Gamma'])$, for some $\mathbb{C}'$, then we also have $(\Delta, \mathbb{E}[\Delta']) \xrightarrow{\tau} (\Delta, \mathbb{C}'[\Delta'])$, and we progress to $\mathsf{weak}(\mathsf{ctx}(\mathcal{S}))$. Otherwise, a Γ_i' is involved, and we have several possibilities. Suppose $\mathbb{E}[\Gamma'] = \mathbb{E}'[\Gamma_i' \mathbb{C}_{\mathsf{v}}[\Gamma'], \Gamma']$ for some $\mathbb{E}'$, $\mathbb{C}_{\mathsf{v}}$, and Γ_i' is a λ-abstraction. We have $\Gamma' \xrightarrow{\lambda, i, \mathbb{C}_{\mathsf{v}}} (\Gamma', e_1'')$, which means $(\Gamma, \mathbb{E}[\Gamma']) \xrightarrow{\tau} (\Gamma, \mathbb{E}'[e_1'', \Gamma'])$. Because $\Gamma'\ \mathcal{R}\ (\Delta, e_2)$, there exist v_2', e_2'' such that $\Delta \xRightarrow{\lambda, i, \mathbb{C}_{\mathsf{v}}} (\Delta, v_2', e_2'')$ and $(\Gamma', e_1'')\ \mathcal{S}\ (\Delta, v_2', e_2'')$. Consequently, we have $(\Delta, \mathbb{E}[e_2, \Delta]) \stackrel{\tau}{\Rightarrow} (\Delta, \mathbb{E}'[e_2'', \Delta, v_2'])$, with $(\Gamma, \mathbb{E}'[e_1'', \Gamma'])\ \mathsf{weak}(\mathsf{ectx}(\mathcal{S}))\ (\Delta, \mathbb{E}'[e_2'', \Delta, v_2'])$, as wished. The case where $\mathbb{E}[\Gamma'] = \mathbb{E}'[\Gamma_i' \triangleleft \mathbb{C}'[\Gamma'], \Gamma']$ for some $\mathbb{E}'$, $\mathbb{C}'$, and Γ_i' is a continuation, is treated similarly. Finally, if $\mathbb{E}[\Gamma'] = \mathbb{E}'[\#_p \Gamma_i', \Gamma']$ for some $\mathbb{E}'$, then $(\Gamma', \mathbb{E}[\Gamma']) \xrightarrow{\tau} (\Gamma', \mathbb{E}'[\Gamma_i', \Gamma']$. Because $\Gamma'\ \mathcal{R}\ (\Delta, e_2)$ and $\Gamma' \xrightarrow{\mathsf{v}} \Gamma'$, there exists v_2 such that $(\Delta, e_2) \stackrel{\mathsf{v}}{\Rightarrow} (\Delta, v_2)$ and $\Gamma'\ \mathcal{S}\ (\Delta, v_2)$. Let $\Delta' = (\Delta, v_2)$, we have $(\Delta, \mathbb{E}[e_2, \Delta]) \stackrel{\tau}{\Rightarrow} (\Delta, \mathbb{E}'[\Delta_i', \Delta'])$, with $(\Gamma, \mathbb{E}'[\Gamma_i', \Gamma'])\ \mathsf{ectx}(\mathcal{R})\ (\Delta, \mathbb{E}'[\Delta_i', \Delta'])$, as wished.

□

A.2 Completeness proof

Proof. We prove that

$$\mathcal{R} \stackrel{\mathsf{def}}{=} \{(\Gamma, e_1), (\Delta, e_2) \mid \forall \mathbb{E}, \mathbb{E}[e_1, \Gamma] \sim \mathbb{E}[e_2, \Delta]\}$$

is a bisimulation up to permutation.

Suppose $(\Gamma, e_1) \xrightarrow{\tau} (\Gamma, e_1')$. The expression $\mathbb{E}[e_1, \Gamma]$ has the same observable actions as $\mathbb{E}[e_1', \Gamma]$, therefore we still have $\mathbb{E}[e_1', \Gamma] \sim \mathbb{E}[e_2, \Delta]$ for all $\mathbb{E}$, which implies $(\Gamma, e_1') \mathcal{R} (\Gamma, e_2)$, as wished.

Suppose $(\Gamma, e_1) \xrightarrow{\mathbb{E}'} (\Gamma, e_1')$; then e_1 is a stuck term, and because $e_1 \sim e_2$ (by taking $\mathbb{E} = \Box$), then e_2 evaluates to a stuck term as well. Therefore, we also have $(\Delta, e_2) \stackrel{\mathbb{E}'}{\Rightarrow} (\Delta, e_2')$ for some e_2'. But $(\Gamma, e_1) \xrightarrow{\mathbb{E}'} (\Gamma, e_1')$ and $(\Delta, e_2) \stackrel{\mathbb{E}'}{\Rightarrow} (\Delta, e_2')$ implies respectively $\mathbb{E}'[e_1, \Gamma] \to^* e_1'$ and $\mathbb{E}'[e_2, \Delta] \to^* e_2'$, which in turn implies $\mathbb{E}[\mathbb{E}'[e_1, \Gamma], \Gamma] \to^* \mathbb{E}[e_1', \Gamma]$ and $\mathbb{E}[\mathbb{E}'[e_2, \Delta], \Delta] \to^* \mathbb{E}[e_2', \Delta]$ for all $\mathbb{E}$. Because $\mathbb{E}[\mathbb{E}'[e_1, \Gamma], \Gamma] \sim \mathbb{E}[\mathbb{E}'[e_2, \Gamma], \Gamma]$, we have also $\mathbb{E}[e_1', \Gamma] \sim \mathbb{E}[e_2', \Delta]$, which implies $(\Gamma, e_1') \mathcal{R} (\Delta, e_2')$, as wished.

Suppose e_1 is a value v_1. Because $e_1 \sim e_2$, there exists v_2 such that $e_2 \to^* v_2$. Let $\Gamma' = (\Gamma, v_1)$, and $\Delta' = (\Delta, v_2)$. We now consider the possible transitions of Γ'. First, we have $\Gamma' \xrightarrow{\mathsf{v}} \Gamma'$. Because $\mathbb{E}[v_1, \Gamma] \sim \mathbb{E}[e_2, \Delta]$, we also have $\mathbb{E}[v_1, \Gamma] \sim \mathbb{E}[v_2, \Delta]$, therefore we have $(\Delta, e_2) \stackrel{\mathsf{v}}{\Rightarrow} \Delta'$ with $\Gamma' \mathcal{R} \Delta'$, as wished.

In all the cases below, we write n for the size of Γ, and we define $\mathbb{C}_{\mathsf{v}}^k \stackrel{\mathsf{def}}{=} \Box_k$ if $k \leq n$ and $\mathbb{C}_{\mathsf{v}}^{n+1} \stackrel{\mathsf{def}}{=} x$. Also, when (Δ, e_2) reduces in some context $\mathbb{E}$, we obtain v_2' such that $v_2' = v_2\sigma$ for some permutation σ. We therefore work implicitly up to permutation.

Suppose $\Gamma' \xrightarrow{\#,i,j} \Gamma'$. Let $\mathbb{E} \stackrel{\mathsf{def}}{=} \mathsf{let}\ x = \Box\ \mathsf{in}\ \mathsf{if}\ \mathbb{C}_{\mathsf{v}}^i \stackrel{?}{=} \mathbb{C}_{\mathsf{v}}^j\ \mathsf{then}\ \lambda x.x\ \mathsf{else}\ \mathcal{G}_{\mathbb{C}_{\mathsf{v}}^i} y.\lambda x.x$. Then we have $\mathbb{E}[v_1, \Gamma] \sim \mathbb{E}[e_2, \Delta]$, meaning that Δ_i' and Δ_j' are equal prompts, which implies $(\Delta, e_2) \stackrel{\#,i,j}{\Longrightarrow} \Delta'$. We already proved before that $\Gamma'\ \mathsf{perm}(\mathcal{R})\ \Delta'$.

Consider $\Gamma' \xrightarrow{\#} (\Gamma', p)$, where p is a fresh prompt. We also have $(\Delta, e_2) \stackrel{\#}{\Rightarrow} (\Delta', q)$ for a fresh prompt q. We now prove that $\mathbb{E}[p, \Gamma'] \sim \mathbb{E}[q, \Delta']$ holds up to permutation. We define $\mathbb{E}' \stackrel{\mathsf{def}}{=} \mathsf{let}\ x = \Box\ \mathsf{in}\ \mathcal{P}y.\mathbb{E}[y/\Box, x/\Box_{n+1}]$. Then we have $\mathbb{E}'[v_1, \Gamma] \sim \mathbb{E}'[e_2, \Delta]$, but $\mathbb{E}'[v_1, \Gamma] \to^* \mathbb{E}[p', \Gamma']$ and $\mathbb{E}'[e_2, \Delta] \to^* \mathbb{E}[q', \Delta']$ for some fresh p', q', so we also have $\mathbb{E}[p', \Gamma'] \sim \mathbb{E}[q', \Delta']$. We therefore have $(\Gamma', p)\ \mathsf{perm}(\mathcal{R})\ (\Delta', q)$, as wished.

Suppose $\Gamma' \xrightarrow{\lambda,i,\mathbb{C}_{\mathsf{v}}} (\Gamma', e_1')$ for some e_1'. Because $\Gamma_i' \sim \Delta_i'$ (by taking $\mathbb{E} = \mathsf{let}\ x = \Box\ \mathsf{in}\ \mathbb{C}_{\mathsf{v}}^i$), we know that Δ_i' is also a λ-abstraction, so we have $(\Delta, e_2) \stackrel{\lambda,i,\mathbb{C}_{\mathsf{v}}}{\Longrightarrow} (\Delta', e_2')$ for some e_2'. We now prove that $\mathbb{E}[e_1', \Gamma'] \sim \mathbb{E}[e_2', \Delta']$ holds. We define $\mathbb{E}' \stackrel{\mathsf{def}}{=} \mathsf{let}\ x = \Box\ \mathsf{in}\ \mathbb{E}[\mathbb{C}_{\mathsf{v}}^i\ \mathbb{C}_{\mathsf{v}}/\Box, x/\Box_{n+1}]$. Then we have $\mathbb{E}'[v_1, \Gamma] \sim \mathbb{E}'[e_2, \Delta]$, but $\mathbb{E}'[v_1, \Gamma] \to^* \mathbb{E}[e_1', \Gamma']$ and $\mathbb{E}'[e_2, \Delta] \to^* \mathbb{E}[e_2', \Delta']$, hence $\mathbb{E}[e_1', \Gamma'] \sim \mathbb{E}[e_2', \Delta']$ holds. We therefore have $(\Gamma', e_1')\ \mathsf{perm}(\mathcal{R})\ (\Delta', e_2')$, as wished.

Suppose $\Gamma' \xrightarrow{\ulcorner \cdot \urcorner,i,\mathbb{C}} (\Gamma', e_1')$ for some e_1. Because $\Gamma_i' \sim \Delta_i'$ (by taking $\mathbb{E} = \mathsf{let}\ x = \Box\ \mathsf{in}\ \mathbb{C}_{\mathsf{v}}^i$), we know that Δ_i' is also a continuation, so we have $(\Delta, e_2) \stackrel{\ulcorner \cdot \urcorner,i,\mathbb{C}}{\Longrightarrow} (\Delta', e_2')$ for some e_2'. We now prove that $\mathbb{E}[e_1', \Gamma'] \sim \mathbb{E}[e_2', \Delta']$ holds. We define $\mathbb{E}' \stackrel{\mathsf{def}}{=} \mathsf{let}\ x = \Box\ \mathsf{in}\ \mathbb{E}[\mathbb{C}_{\mathsf{v}}^i \triangleleft \mathbb{C}/\Box, x/\Box_{n+1}]$. Then we have $\mathbb{E}'[v_1, \Gamma] \sim \mathbb{E}'[e_2, \Delta]$, but $\mathbb{E}'[v_1, \Gamma] \to^* \mathbb{E}[e_1', \Gamma']$ and $\mathbb{E}'[e_2, \Delta] \to^* \mathbb{E}[e_2', \Delta']$, hence $\mathbb{E}[e_1', \Gamma'] \sim \mathbb{E}[e_2', \Delta']$ holds. We therefore have $(\Gamma', e_1')\ \mathsf{perm}(\mathcal{R})\ (\Delta', e_2')$, as wished. □

B Proofs for Section 4

B.1 Properties of diacritical compatibility

Lemma 11. *Let F be a compatible set. If $\mathcal{R} \rightarrowtail\!\!\!\!\twoheadrightarrow \mathsf{strong}(F)^\omega, F^\omega$, then $F^\omega(\mathcal{R})$ is a bisimulation.*

Proof. Let $S \stackrel{\mathsf{def}}{=} \mathsf{strong}(F)$. We prove $(S^\omega \circ F \circ S^\omega)^n(\mathcal{R}) \rightarrowtail\!\!\!\!\twoheadrightarrow (S^\omega \circ F \circ S^\omega)^n(S^\omega(\mathcal{R})), F^\omega(\mathcal{R})$ by induction on n. There is nothing to prove for $n = 0$. Suppose $n > 0$. We know that

$$(S^\omega \circ F \circ S^\omega)^{n-1}(\mathcal{R}) \rightarrowtail\!\!\!\!\twoheadrightarrow (S^\omega \circ F \circ S^\omega)^{n-1}(S^\omega(\mathcal{R})), F^\omega(\mathcal{R}).$$

For all $f \in S$, we have

$$f((S^\omega \circ F \circ S^\omega)^{n-1}(\mathcal{R})) \rightarrowtail\!\!\!\!\twoheadrightarrow S^\omega(S^\omega \circ F \circ S^\omega)^{n-1}(S^\omega(\mathcal{R})), F^\omega(F^\omega(\mathcal{R})),$$

therefore we have

$$S^\omega(((S^\omega \circ F \circ S^\omega)^{n-1}(\mathcal{R}))) \rightarrowtail\!\!\!\!\twoheadrightarrow S^\omega(S^\omega \circ F \circ S^\omega)^{n-1}(S^\omega(\mathcal{R})), F^\omega(\mathcal{R}).$$

Because $S^\omega \circ (S^\omega \circ F \circ S^\omega)^{n-1} = S^\omega \circ (S^\omega \circ F \circ S^\omega)^{n-1} \circ S^\omega$, for all $f \in F$, we have

$$f(S^\omega(((S^\omega \circ F \circ S^\omega)^{n-1}(\mathcal{R}))) \rightarrowtail\!\!\!\!\twoheadrightarrow (S^\omega \circ F \circ S^\omega)(S^\omega(S^\omega \circ F \circ S^\omega)^{n-1}(S^\omega(\mathcal{R}))), E^\omega(E^\omega(\mathcal{R})),$$

which implies $F(S^\omega(((S^\omega \circ F \circ S^\omega)^{n-1}(\mathcal{R}))) \rightarrowtail\!\!\!\!\twoheadrightarrow (S^\omega(S^\omega \circ F \circ S^\omega)^n(S^\omega(\mathcal{R}))), E^\omega(\mathcal{R})$. Finally, composing again with S^ω, we obtain

$$S^\omega(((S^\omega \circ F \circ S^\omega)^n(\mathcal{R})) \rightarrowtail\!\!\!\!\twoheadrightarrow S^\omega \circ (S^\omega \circ F \circ S^\omega)^n(S^\omega(\mathcal{R})), F^\omega(\mathcal{R}),$$

as wished.

Because F^ω can be written as $(S^\omega \circ F \circ S^\omega)^\omega$, we get that $F^\omega(\mathcal{R}) \rightarrowtail\!\!\!\!\twoheadrightarrow F^\omega(\mathcal{R}), F^\omega(\mathcal{R})$, i.e., $F^\omega(\mathcal{R})$ is a bisimulation. □

Lemma 12. *Let F be a compatible set and $S = \mathsf{strong}(F)$.*

- *If $f \in F$ (resp. $f \in S$), then f is an up-to technique (resp. strong up-to technique).*
- *For all $f \in F$, we have $f(\approx) \subseteq \approx$.*

Proof. Let $f \in S$ and suppose $\mathcal{R} \rightarrowtail\!\!\!\!\twoheadrightarrow f(\mathcal{R}), f(\mathcal{R})$. Then

$$\begin{aligned} \mathcal{R} &\subseteq f(\mathcal{R}) && \text{by definition of } \rightarrowtail\!\!\!\!\twoheadrightarrow \\ &\subseteq F^\omega(\mathcal{R}) \\ &\subseteq \overset{\star}{\approx} && \text{by Lemma 11} \end{aligned}$$

The proof is similar for $f \in F$.

Let $f \in F$. Because $\overset{\star}{\approx} \rightarrowtail\!\!\!\!\twoheadrightarrow \overset{\star}{\approx}, \overset{\star}{\approx}$, we have $f(\overset{\star}{\approx}) \subseteq E^\omega(\overset{\star}{\approx}) \subseteq \overset{\star}{\approx}$ by Lemma 11. □

B.2 Compatibility proofs

Lemma 13.

- $\mathsf{perm} \rightsquigarrow_{\mathsf{s}} \mathsf{perm}, \mathsf{perm}$.
- $\mathsf{weak} \rightsquigarrow_{\mathsf{s}} \mathsf{weak}, (\mathsf{perm} \cup \mathsf{id}) \circ \mathsf{weak}$.

Proof. Same as for Lemmas 6 and 7. □

Lemma 14.

- $\mathsf{rctx} \rightsquigarrow \mathsf{weak}^\omega \circ \mathsf{perm} \circ (\mathsf{rctx} \cup \mathsf{rectx}), \mathsf{weak}^\omega \circ \mathsf{perm} \circ (\mathsf{rctx} \cup \mathsf{rectx})$
- $\mathsf{rectx} \rightsquigarrow \mathsf{weak}^\omega \circ \mathsf{perm} \circ (\mathsf{rctx} \cup \mathsf{rectx}), \mathsf{weak}^\omega \circ \mathsf{perm} \circ (\mathsf{rctx} \cup \mathsf{rectx})$

Proof. Both cases are proved by mutual induction on the size of the context $\mathbb{C}$ or $\mathbb{E}$. For rctx, the size of the context is decreasing, while the proof for rectx uses the induction hypothesis for rctx with a context of same size. We therefore start with rctx. Let $(\Gamma, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Gamma], \mathbb{C}[\Gamma])\ \mathsf{rctx}(\mathcal{R})\ (\Delta, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Delta], \mathbb{C}[\Delta])$ so that $\Gamma\ \mathcal{R}\ \Delta$.

First, we assume $\mathbb{C}$ is a value context. We write n for the size of Γ and we write $\mathbb{C}_{\mathsf{v}}\{\overrightarrow{\mathbb{C}_{\mathsf{v}}}\}$ for $\mathbb{C}_{\mathsf{v}}$ where for every $i \geq 1$ we substitute $(\overrightarrow{\mathbb{C}_{\mathsf{v}}})_i$ for all holes $\Box_{n+i}$. The transition $\xrightarrow{\mathsf{v}}$ is easy to check.

Suppose $(\Gamma, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Gamma]) \xrightarrow{\lambda, i, \mathbb{C}_{\mathsf{v}}} (\Gamma, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Gamma], e_1)$. If $i = n + k$ where $(\overrightarrow{\mathbb{C}_{\mathsf{v}}})_k = \Box_j$ or $i = j \leq n$ then we have $\Gamma \xrightarrow{\lambda, j, \mathbb{C}_{\mathsf{v}}\{\overrightarrow{\mathbb{C}_{\mathsf{v}}}\}} (\Gamma, e_1)$ and therefore $\Delta \xRightarrow{\lambda, j, \mathbb{C}_{\mathsf{v}}\{\overrightarrow{\mathbb{C}_{\mathsf{v}}}\}} (\Delta, e_2)$ and $(\Gamma, e_1)\ \mathcal{S}\ (\Delta, e_2)$. Then we know that $(\Delta, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Delta]) \xRightarrow{\lambda, i, \mathbb{C}_{\mathsf{v}}} (\Delta, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Delta], e_2)$, and taking $\mathbb{E} = \Box$ we have $(\Gamma, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Gamma], e_1)\ \mathsf{rectx}(S)\ (\Delta, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Delta], e_2)$, as wished.

If $i = n + k$ and $(\overrightarrow{\mathbb{C}_\mathsf{v}})_k \neq \Box_j$, then $(\overrightarrow{\mathbb{C}_\mathsf{v}})_i$ is of the form $\lambda x.\mathbb{C}$. Therefore $e_1 = (\mathbb{C}\{\mathbb{C}_\mathsf{v}\{\overrightarrow{\mathbb{C}_\mathsf{v}}/x\}\})[\Gamma]$ and $(\Delta, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Delta]) \xRightarrow{\lambda,i,\mathbb{C}_\mathsf{v}} (\Delta, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Delta], e_2)$ where $e_2 = (\mathbb{C}\{\mathbb{C}_\mathsf{v}\{\overrightarrow{\mathbb{C}_\mathsf{v}}/x\}\})[\Delta]$. Consequently we have $(\Gamma, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Gamma], e_1)\ \mathsf{rctx}(\mathcal{R})\ (\Delta, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Delta], e_2)$ which implies $(\Gamma, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Gamma], e_1)\ \mathsf{rctx}(\mathcal{S})\ (\Delta, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Delta], e_2)$ since $\mathcal{R} \subseteq \mathcal{S}$ and rctx is monotone.

Suppose $(\Gamma, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Gamma]) \xrightarrow{\ulcorner.\urcorner,i,\mathbb{C}_\mathsf{v}} (\Gamma, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Gamma], e_1)$. If $i = n + k$ where $(\overrightarrow{\mathbb{C}_\mathsf{v}})_k = \Box_j$ or $i = j \leq n$ then we proceed as with $\xrightarrow{\lambda,i,\mathbb{C}_\mathsf{v}}$. If $i = n + k$ and $(\overrightarrow{\mathbb{C}_\mathsf{v}})_k \neq \Box_j$, then $(\overrightarrow{\mathbb{C}_\mathsf{v}})_i$ has the form $\ulcorner\mathbb{E}\urcorner$. Therefore $e_1 = \mathbb{E}[\mathbb{C}_\mathsf{v}\{\overrightarrow{\mathbb{C}_\mathsf{v}}\}][\Gamma]$ and $(\Delta, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Delta]) \xRightarrow{\ulcorner.\urcorner,i,\mathbb{C}_\mathsf{v}} (\Delta, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Delta], e_2)$ where $e_2 = \mathbb{E}[\mathbb{C}_\mathsf{v}\{\overrightarrow{\mathbb{C}_\mathsf{v}}\}][\Delta]$. As a result, we have $(\Gamma, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Gamma], e_1)\ \mathsf{rctx}(\mathcal{R})\ (\Delta, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Delta], e_2)$, as wished.

Suppose $(\Gamma, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Gamma]) \xrightarrow{\#,i,j} (\Gamma, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Gamma])$. Let $i_0 = i$ when $i \leq n$ or $i_0 = i'$ where $i = n + k$ and $(\overrightarrow{\mathbb{C}_\mathsf{v}})_k = \Box_{i'}$ (there are no other cases). Define j_0 analogously. Then we know that the transition $\Gamma \xrightarrow{\#,i_0,j_0} \Gamma$ is matched by Δ and therefore i and j point to the same prompt in $(\Delta, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Delta])$.

Suppose $(\Gamma, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Gamma]) \xrightarrow{\ulcorner.\urcorner,i,j} (\Gamma, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Gamma], \ulcorner E_1\urcorner, \ulcorner E_2\urcorner)$. If i points to Γ (even indirectly, when $i = n + k$ and $(\overrightarrow{\mathbb{C}_\mathsf{v}})_k = \Box_{i'}$), then the transition comes from Γ and we end up in $\mathsf{rctx}(\mathcal{S})$ (with a similar proof as in the previous case). We only have to check the case where $i = n + k$, $(\overrightarrow{\mathbb{C}_\mathsf{v}})_k = \ulcorner\mathbb{E}_1 \#_{\Box'_j} \mathbb{E}_2\urcorner$, j' and j points to the same prompt p in Γ, and $p \notin \mathsf{sp}(\mathbb{E}_2[\Gamma])$. With the transition for testing prompt equality, we can ensure that j and j' points to the same prompt q in Δ and $q \notin \mathsf{sp}(\mathbb{E}_2[\Delta])$, therefore we have $(\Delta, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Delta]) \xRightarrow{\ulcorner.\urcorner,i,j} (\Delta, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Delta], \ulcorner\mathbb{E}_1[\Delta]\urcorner, \ulcorner\mathbb{E}_2[\Delta]\urcorner)$ and $(\Gamma, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Gamma], \ulcorner\mathbb{E}_1[\Gamma]\urcorner, \ulcorner\mathbb{E}_2[\Gamma]\urcorner)\ \mathsf{rctx}(\mathcal{R})\ (\Delta, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Delta], \ulcorner\mathbb{E}_1[\Delta]\urcorner, \ulcorner\mathbb{E}_2[\Delta]\urcorner)$ as wished.

Finally, suppose $(\Gamma, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Gamma]) \xrightarrow{\#} (\Gamma, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Gamma], p)$. We have also $\Gamma \xrightarrow{\#} (\Gamma, p)$, therefore there exists q such that $\Delta \overset{\#}{\Rightarrow} (\Delta, q)$ and $(\Gamma, p)\ \mathcal{S}\ (\Delta, q)$. Because $\#(\overrightarrow{\mathbb{C}_\mathsf{v}}[\Delta]) \subseteq \#(\Delta)$ we also have $(\Delta, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Gamma]) \overset{\#}{\Rightarrow} (\Delta, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Delta], q)$, with $(\Gamma, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Gamma], p)\ \mathsf{rctx}(\mathcal{S})\ (\Delta, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Delta], q)$, as wished.

Now we suppose $\mathbb{C}$ is not a value context, and we proceed by case analysis on the form of $\mathbb{C}$.

Suppose $\mathbb{C} = \mathbb{E}[\star_i[\mathbb{C}_\mathsf{v}]]$. We have $\Gamma \xrightarrow{\ulcorner.\urcorner,i,\mathbb{C}_\mathsf{v}} (\Gamma, (\star_i[\mathbb{C}_\mathsf{v}])[\Gamma])$, therefore there exists e'_2 such that $\Delta \xRightarrow{\ulcorner.\urcorner,i,\mathbb{C}_\mathsf{v}} (\Delta, e'_2)$ and $(\Gamma, (\star_i[\mathbb{C}_\mathsf{v}])[\Gamma])\ \mathcal{R}\ (\Delta, e'_2)$, implying that $(\Gamma, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Gamma], (\mathbb{E}[\star_i[\mathbb{C}_\mathsf{v}]])[\Gamma])\ \mathsf{rectx}(\mathcal{R})\ (\Delta, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Delta], \mathbb{E}[e'_2, \Delta])$ holds. But the size of $\mathbb{E}$ is strictly smaller then the size of $\mathbb{C}$, so we conclude using the induction hypothesis.

Suppose $\mathbb{C} = \mathbb{E}[(\lambda x.\mathbb{C}')\ \mathbb{C}_\mathsf{v}]$. Then

$$(\Gamma, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Gamma], (\mathbb{E}[(\lambda x.\mathbb{C}')\ \mathbb{C}_\mathsf{v}])[\Gamma]) \xrightarrow{\tau} (\Gamma, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Gamma], (\mathbb{E}[\mathbb{C}'\{\mathbb{C}_\mathsf{v}/x\}])[\Gamma])$$
$$(\Delta, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Delta], (\mathbb{E}[(\lambda x.\mathbb{C}')\ \mathbb{C}_\mathsf{v}])[\Delta]) \xrightarrow{\tau} (\Delta, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Delta], (\mathbb{E}[\mathbb{C}'\{\mathbb{C}_\mathsf{v}/x\}])[\Delta])$$

The two resulting terms are in $\mathsf{rctx}(\mathcal{R})$, and therefore also in $\mathsf{rctx}(\mathcal{S})$ because $\mathcal{R} \subseteq \mathcal{S}$ and rctx is monotone. For $\mathbb{C} = \mathbb{E}[\ulcorner\mathbb{E}'\urcorner \triangleleft \mathbb{C}']$ and $\mathbb{C} = \mathbb{E}[\#_{\Box_i}\mathbb{C}_\mathsf{v}]$, the proof is similar.

Suppose $\mathbb{C} = \mathbb{E}[\mathcal{P}x.\mathbb{C}']$. Then $(\Gamma, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Gamma], (\mathbb{E}[\mathcal{P}x.\mathbb{C}'])[\Gamma]) \xrightarrow{\tau} (\Gamma, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Gamma], \mathbb{E}[\mathbb{C}'[\Gamma]\{p/x\}, \Gamma])$ for $p \notin \#(\Gamma)$. Therefore we have $\Gamma \xrightarrow{\#} (\Gamma, p)$, which implies that there exists $q \notin \#(\Delta)$ such that $(\Gamma, p)\ \mathcal{S}\ (\Delta, q)$. Because $(\Delta, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Delta], (\mathbb{E}[\mathcal{P}x.\mathbb{C}'])[\Delta]) \xrightarrow{\tau} (\Delta, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Delta], \mathbb{E}[\mathbb{C}'[\Delta]\{q'/x\}, \Delta])$ for $q' \notin \#(\Delta)$, by considering $\mathbb{C}'' = \mathbb{E}[\mathbb{C}'\{\Box_{n+1}/x\}]$, we get $(\Gamma, p, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Gamma], \mathbb{C}''[\Gamma, p])\ \mathsf{perm}(\mathsf{rctx}(\mathcal{S}))\ (\Gamma, q, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Delta], \mathbb{C}''[\Delta, q])$, which in turn implies that $(\Gamma, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Gamma], \mathbb{C}''[\Gamma, p])\ \mathsf{weak}(\mathsf{perm}(\mathsf{rctx}(\mathcal{S})))\ (\Gamma, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Delta], \mathbb{C}''[\Delta, q])$ holds, as wished.

Suppose $\mathbb{C} = \mathbb{E}[\Box_i\ \mathbb{C}_\mathsf{v}]$. The only possible transition is $(\Gamma, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Gamma], (\mathbb{E}[\Box_i\ \mathbb{C}_\mathsf{v}])[\Gamma]) \xrightarrow{\tau} (\Gamma, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Gamma], \mathbb{E}[e_1, \Gamma])$ with $\Gamma \xrightarrow{\lambda,i,\mathbb{C}_\mathsf{v}} (\Gamma, e_1)$. Therefore there exists e_2 such that $\Delta \xRightarrow{\lambda,i,\mathbb{C}_\mathsf{v}} (\Delta, e_2)$ and $(\Gamma, e_1)\ \mathcal{S}\ (\Delta, e_2)$, so we have $(\Delta, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Delta], (\mathbb{E}[\Box_i\ \mathbb{C}_\mathsf{v}])[\Delta]) \Rightarrow (\Delta, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Delta], \mathbb{E}[e_2, \Delta])$ and $(\Gamma, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Gamma], \mathbb{E}[e_1, \Gamma])\ \mathsf{rectx}(\mathcal{S})\ (\Delta, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Delta], \mathbb{E}[e_2, \Delta])$, as wished.

Suppose $\mathbb{C} = \mathbb{E}[\Box_i \triangleleft \mathbb{C}']$. Then

$$(\Gamma, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Gamma], (\mathbb{E}[\Box_i \triangleleft \mathbb{C}'])[\Gamma]) \xrightarrow{\tau} (\Gamma, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Gamma], (\mathbb{E}[\star_i[\mathbb{C}']])[\Gamma])$$
$$(\Delta, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Delta], (\mathbb{E}[\Box_i \triangleleft \mathbb{C}'])[\Delta]) \xrightarrow{\tau} (\Delta, \overrightarrow{\mathbb{C}_\mathsf{v}}[\Delta], (\mathbb{E}[\star_i[\mathbb{C}']])[\Delta])$$

The two resulting terms are in $\mathsf{rctx}(\mathcal{R})$, and therefore also in $\mathsf{rctx}(\mathcal{S})$ because $\mathcal{R} \subseteq \mathcal{S}$ and rctx is monotone.

Suppose $\mathbb{C} = \mathbb{E}[\mathcal{G}_{\Box_i} k.\mathbb{C}']$, $\Gamma_i = p$ and $(\Gamma, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Gamma], (\mathbb{E}[\mathcal{G}_{\Box_i} k.\mathbb{C}'])[\Gamma]) \xrightarrow{\tau} (\Gamma, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Gamma], e_1)$. If $\mathbb{E}$ has the form $\mathbb{E}_1 \#_{\Box_j} \mathbb{E}_2$ where $\Gamma_j = p$ we end up in $\mathsf{rctx}(\mathcal{S})$ (the proof is the same as for $\mathbb{C} = \mathbb{E}[(\lambda x.\mathbb{C}')\, \mathbb{C}_{\mathsf{v}}]$, except we use the $\xrightarrow{\#,i,j}$ transition to ensure that the prompts Δ_i and Δ_j are the same). Suppose $\mathbb{E} = \mathbb{E}_1[\star_j[\mathbb{E}_2]]$ and $\Gamma_j = \ulcorner F_1 \#_p E_1 \urcorner$ where $p \notin \mathsf{sp}(E_1) \cup \mathsf{sp}(\mathbb{E}_2[\Gamma])$. Now we have $e_1 = \mathbb{E}_1[F_1[\mathbb{C}'[\Gamma]\{\ulcorner E_1[\mathbb{E}_2[\Gamma]] \urcorner / k\}], \Gamma]$. Using prompt equality transition, we can ensure that $\Delta_i = q$ and $q \notin \mathsf{sp}(\mathbb{E}_2[\Delta])$ for some prompt q. We also have $\Gamma \xrightarrow{\ulcorner . \urcorner, j, i} (\Gamma, \ulcorner F_1 \urcorner, \ulcorner E_1 \urcorner)$, so we have $\Delta_j = \ulcorner F_2 \#_q E_2 \urcorner$ and $(\Gamma, \ulcorner F_1 \urcorner, \ulcorner E_1 \urcorner)\ \mathcal{S}\ (\Delta, \ulcorner F_2 \urcorner, \ulcorner E_2 \urcorner)$. Therefore we have $(\Delta, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Delta], (\mathbb{E}[\mathcal{G}_{\Box_i} k.\mathbb{C}'])[\Delta]) \Rightarrow (\Delta, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Delta], e_2)$ for $e_2 = \mathbb{E}_1[F_2[\mathbb{C}'[\Delta]\{\ulcorner E_2[\mathbb{E}_2[\Delta]] \urcorner / k\}], \Delta]$. By considering $\mathbb{E}_1[\star_{n+1}[\mathbb{C}'\{\ulcorner \star_{n+2}[\mathbb{E}_2] \urcorner / k\}]]$, we finally have $(\Gamma, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Gamma], e_1)\ \mathsf{weak}(\mathsf{weak}(\mathsf{rctx}(\mathcal{S})))\ (\Delta, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Delta], e_2)$ as wished.

Suppose $\mathbb{C} = \mathbb{E}[\mathcal{G}_{\Box_i} k.\mathbb{C}']$ and $(\Gamma, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Gamma], \mathbb{C}[\Gamma]) \xrightarrow{\mathbb{E}'} (\Gamma, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Gamma], e_1)$. If $\mathbb{E}'[\mathbb{C}[\Gamma], \Gamma]$ remains stuck, we simply end up in $\mathsf{rctx}(\mathcal{S})$. Otherwise, we proceed as in the previous case.

Now we do the proof for rectx. Let $(\Gamma, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Gamma], \mathbb{E}[e_1, \Gamma])\ \mathsf{rctx}(\mathcal{R})\ (\Delta, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Delta], \mathbb{E}[e_2, \Delta])$ so that $(\Gamma, e_1)\ \mathcal{R}\ (\Delta, e_2)$.

Suppose e_1 is not a normal form. Then $(\Gamma, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Gamma], \mathbb{E}[e_1, \Gamma]) \xrightarrow{\tau} (\Gamma, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Gamma], \mathbb{E}[e_1', \Gamma])$ where $(\Gamma, e_1) \xrightarrow{\tau} (\Gamma, e_1')$. Hence, there exists e_2' such that $(\Delta, e_2) \Rightarrow (\Delta, e_2')$ and $(\Gamma, e_1')\ \mathcal{S}\ (\Delta, e_2')$. So we get $(\Delta, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Delta], \mathbb{E}[e_2, \Delta]) \overset{\tau}{\Rightarrow} (\Delta, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Delta], \mathbb{E}[e_2', \Delta])$, with also $(\Gamma, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Gamma], \mathbb{E}[e_1', \Gamma])\ \mathsf{rectx}(\mathcal{S})\ (\Delta, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Delta], \mathbb{E}[e_2', \Delta])$, as wished.

Suppose $e_1 = v_1$ and $(\Gamma, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Gamma], \mathbb{E}[v_1, \Gamma]) \xrightarrow{\alpha} \gamma$. Because $(\Gamma, v_1) \xrightarrow{\mathsf{v}} (\Gamma, v_1)$, there exists v_2 such that $(\Delta, e_2) \overset{\mathsf{v}}{\Rightarrow} (\Delta, v_2)$ and $(\Gamma, v_1)\ \mathcal{R}\ (\Delta, v_2)$. But $\mathbb{E}[v_1, \Gamma] = (\mathbb{E}[\Box_{n+1}])[(\Gamma, v_1)]$ and $\mathbb{E}[v_2, \Delta] = (\mathbb{E}[\Box_{n+1}])[(\Delta, v_2)]$, which means that we also have $(\Gamma, v_1, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Gamma], \mathbb{E}[v_1, \Gamma])\ \mathsf{rctx}(\mathcal{R})\ (\Delta, v_2, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Delta], \mathbb{E}[v_2, \Delta])$, and we can use induction hypothesis on rctx since $(\mathbb{E}[\Box_{n+1}])$ has the same size as $\mathbb{E}$. Let α' be the label α where all indices $i > n$ are shifted by one, and let γ' be γ with we add v_1 at position n. We have $(\Gamma, v_1, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Gamma], \mathbb{E}[v_1, \Gamma]) \xrightarrow{\alpha'} \gamma'$ and by the induction hypothesis there exists δ' such that $(\Delta, v_2, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Delta], \mathbb{E}[v_2, \Delta]) \overset{\alpha'}{\Rightarrow} \delta'$ and $\gamma'\ (\mathsf{weak}^\omega \circ \mathsf{perm} \circ (\mathsf{rctx} \cup \mathsf{rectx}))(\mathcal{T})\ \delta'$ where $\mathcal{T}$ is $\mathcal{R}$ or $\mathcal{S}$ depending if α is passive or active. It is easy to see that δ' has v_2 on the n-th position, so let δ be a δ' where the n-th element of the state is removed. We have $(\Delta, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Delta], \mathbb{E}[e_2, \Delta]) \Rightarrow (\Delta, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Delta], \mathbb{E}[v_2, \Delta]) \overset{\alpha}{\Rightarrow} \delta$ and $\gamma\ (\mathsf{weak} \circ \mathsf{weak}^\omega \circ \mathsf{perm} \circ (\mathsf{rctx} \cup \mathsf{rectx}))(\mathcal{T})\ \delta$ as wished.

Suppose e_1 and $\mathbb{E}[e_1, \Gamma]$ are control stuck terms; then we have $(\Gamma, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Gamma], \mathbb{E}[e_1, \Gamma]) \xrightarrow{\mathbb{E}'} (\Gamma, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Gamma], e_1')$ for some e_1'. But $(\Gamma, e_1) \xrightarrow{\mathbb{E}'\mathbb{E}} (\Gamma, e_1')$, so there exists e_2' such that $(\Delta, e_2) \overset{\mathbb{E}'\mathbb{E}}{\Longrightarrow} (\Delta, e_2')$ and $(\Gamma, e_1')\ \mathcal{S}\ (\Delta, e_2')$. Therefore we have $(\Delta, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Delta], \mathbb{E}[e_2, \Delta]) \overset{\mathbb{E}'}{\Rightarrow} (\Delta, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Delta], e_2')$ and (by taking the empty evaluation context) we have $(\Gamma, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Gamma], e_1')\ \mathsf{rectx}(\mathcal{S})\ (\Delta, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Delta], e_2')$ as wished.

Finally, suppose e_1 is a control stuck term and $(\Gamma, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Gamma], \mathbb{E}[e_1, \Gamma]) \xrightarrow{\tau} (\Gamma, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Gamma], e_1')$. Then we have $(\Gamma, e_1) \xrightarrow{\mathbb{E}} (\Gamma, e_1')$, so there exists e_2' such that $(\Delta, e_2) \xrightarrow{\mathbb{E}} (\Delta, e_2')$ and $(\Gamma, e_1')\ \mathcal{S}\ (\Delta, e_2')$. By the definition of $\xrightarrow{\mathbb{E}}$ we have $\mathbb{E}[e_2, \Delta] \xrightarrow{=} e_2'$. Therefore we have $(\Delta, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Delta], \mathbb{E}[e_2, \Delta]) \Rightarrow (\Delta, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Delta], e_2')$, and (by taking the empty evaluation context) we have $(\Gamma, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Gamma], e_1')\ \mathsf{rectx}(\mathcal{S})\ (\Delta, \overrightarrow{\mathbb{C}_{\mathsf{v}}}[\Delta], e_2')$ as wished. □

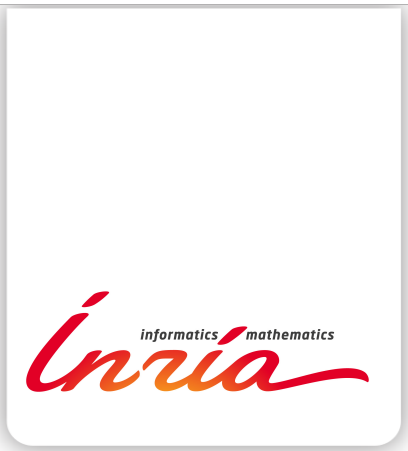
B.3 Completeness proof

Proof. We prove that

$$\mathcal{R} \overset{\mathsf{def}}{=} \{(\Gamma, e_1), (\Delta, e_2) \mid \forall \mathbb{E}, \mathbb{E}[e_1, \Gamma] \sim \mathbb{E}[e_2, \Delta]\}$$

is a bisimulation up to permutation. The proof is the same as in Appendix A.2, except we use value arguments in the $\xrightarrow{\ulcorner . \urcorner, i, \mathbb{C}_{\mathsf{v}}}$ case, and we have an extra transition $(\Gamma, v_1) \xrightarrow{\ulcorner . \urcorner, i, j} (\Gamma, v_1, \ulcorner E_1 \urcorner, \ulcorner E_2 \urcorner)$. In that case, the discriminating context is $\mathbb{E}' \overset{\mathsf{def}}{=} \mathsf{let}\ x = \Box\ \mathsf{in}\ \mathsf{let}\ y = \mathbb{C}_{\mathsf{v}}^i \triangleleft \mathcal{G}_{\mathbb{C}_{\mathsf{v}}^j} x.x\ \mathsf{in}\ \mathsf{let}\ z = \mathcal{P} x_0 . \#_{x_0} \mathbb{C}_{\mathsf{v}}^i \triangleleft \mathcal{G}_{\mathbb{C}_{\mathsf{v}}^j} x_1 . \mathcal{G}_{x_0} x_2 . x_2\ \mathsf{in}\ \mathbb{E}[z/\Box, x/\Box_{n+1}, y/\Box_{n+2}]$. The reasoning is otherwise the same as in the other cases involving values.

□



RESEARCH CENTRE
NANCY – GRAND EST

615 rue du Jardin Botanique
CS20101
54603 Villers-lès-Nancy Cedex

Publisher
Inria
Domaine de Voluceau - Rocquencourt
BP 105 - 78153 Le Chesnay Cedex
inria.fr

ISSN 0249-6399