Non-Deterministic Functions as Non-Deterministic Processes (Extended Version)

Paulus, Joe; Nantes-Sobrinho, Daniele; Pérez, Jorge A.

Published in:
Logical Methods in Computer Science

DOI:
10.46298/lmcs-19(4:1)2023

Logical Methods in Computer Science
Volume 19, Issue 4, 2023, pp. 1:1–1:120
https://lmcs.episciences.org/

Submitted Dec. 08, 2021
Published Oct. 10, 2023

NON-DETERMINISTIC FUNCTIONS AS NON-DETERMINISTIC PROCESSES

JOSEPH W. N. PAULUS [a], DANIELE NANTES-SOBRINHO [b], AND JORGE A. PÉREZ [a]

[a] University of Groningen, The Netherlands
e-mail address: j.w.n.paulus@rug.nl, j.a.perez@rug.nl

[b] Imperial College London, UK and University of Brasília, Brazil
e-mail address: dnantess@ic.ac.uk

Abstract. We study encodings of the λ-calculus into the π-calculus in the unexplored case of calculi with *non-determinism* and *failures*. On the sequential side, we consider $\lambda^{\lightning}_{\oplus}$, a new non-deterministic calculus in which intersection types control resources (terms); on the concurrent side, we consider $\mathsf{s}\pi$, a π-calculus in which non-determinism and failure rest upon a Curry-Howard correspondence between linear logic and session types. We present a typed encoding of $\lambda^{\lightning}_{\oplus}$ into $\mathsf{s}\pi$ and establish its correctness. Our encoding precisely explains the interplay of non-deterministic and fail-prone evaluation in $\lambda^{\lightning}_{\oplus}$ via typed processes in $\mathsf{s}\pi$. In particular, it shows how failures in sequential evaluation (absence/excess of resources) can be neatly codified as interaction protocols.

Introduction

Milner's seminal work on encodings of the λ-calculus into the π-calculus [Mil92] explains how *interaction* in π subsumes *evaluation* in λ. It opened a research strand on formal connections between sequential and concurrent calculi, covering untyped and typed regimes (see, e.g., [San99, BL00, BHY03, TCP12, HYB14, OY16, TY18]). This paper extends this line of work by tackling a hitherto unexplored angle, namely encodability of calculi in which computation is *non-deterministic* and may be subject to *failures*—two relevant features in sequential and concurrent programming models.

We focus on *typed* calculi and study how non-determinism and failures interact with *resource-aware* computation. In sequential calculi, *non-idempotent intersection types* offer one fruitful perspective at resource-awareness (see, e.g., [Gar94, Kfo00, KW04, NM04, BKV17]). Because non-idempotency amounts to distinguish between types σ and $\sigma \wedge \sigma$, this class of intersection types can "count" different resources and enforce quantitative guarantees. In concurrent calculi, resource-awareness has been much studied using *linear types*. Linearity ensures that process actions occur exactly once, which is key to enforce protocol correctness. In particular, *session types* [Hon93, HVK98] specify the protocols that channels must respect; this typing discipline exploits linearity to ensure absence of communication errors and stuck processes. To our knowledge, connections between calculi adopting these two distinct views of

Key words and phrases: concurrency, lambda-calculus, process calculi, intersection types, session types.

DOI:10.46298/LMCS-19(4:1)2023

resource-awareness via types are still to be established. We aim to develop such connections by relating models of sequential and concurrent computation.

On the sequential side, we introduce $\lambda^{\lightning}_{\oplus}$: a λ-calculus with resources, non-determinism, and failures, which distills key elements from λ-calculi studied in [Bou93, PR10]. Evaluation in $\lambda^{\lightning}_{\oplus}$ considers *bags* of resources, and determines alternative executions governed by non-determinism. Failure results from a lack or excess of resources (terms), and is captured by the term $\mathtt{fail}^{\widetilde{x}}$, where $\widetilde{x}$ denotes a sequence of variables. Non-determinism in $\lambda^{\lightning}_{\oplus}$ is *non-collapsing* (i.e., confluent): intuitively, given M and N with reductions $M \longrightarrow M'$ and $N \longrightarrow N'$, the non-deterministic sum $M + N$ reduces to $M' + N'$. In contrast, under a *collapsing* (i.e., non-confluent) approach, as in, e.g., [DdP93], the non-deterministic sum $M + N$ reduces to either M or N.

On the concurrent side, we consider $\mathsf{s}\pi$: a session-typed π-calculus with (non-collapsing) non-determinism and failure, proposed in [CP17]. $\mathsf{s}\pi$ rests upon a Curry-Howard correspondence between session types and (classical) linear logic, extended with modalities that express *non-deterministic protocols* that may succeed or fail. Non-determinism in $\mathsf{s}\pi$ is non-collapsing, which ensures confluent process reductions.

Contributions. This paper presents the first formal connection between a λ-calculus with non-idempotent intersection types and a π-calculus with session types. Specifically, the paper presents the following contributions:

(1) **The resource calculus** $\lambda^{\lightning}_{\oplus}$, a new calculus that distills the distinctive elements from previous resource calculi [BL00, PR10], while offering an explicit treatment of failures in a setting with non-collapsing non-determinism.

We develop the syntax, semantics, and essential meta-theoretical results for $\lambda^{\lightning}_{\oplus}$. In particular, using intersection types, we define *well-typed* (fail-free) expressions and *well-formed* (fail-prone) expressions in $\lambda^{\lightning}_{\oplus}$ and establish their properties.

(2) **An encoding of** $\lambda^{\lightning}_{\oplus}$ **into** $\mathsf{s}\pi$, proven correct following established criteria in the realm of relative expressiveness for concurrency [Gor10, KPY19]. These criteria attest to an encoding's quality; we consider *type preservation*, *operational correspondence* (including completeness and *soundness*), *success sensitiveness*, and *compositionality*.

Thanks to these correctness properties, our encoding precisely describes how typed interaction protocols (given by session types) can codify sequential evaluation in which absence and excess of resources leads to failures (as governed by intersection types).

These contributions entail different challenges. The first is bridging the different mechanisms for resource-awareness involved (i.e., intersection types in $\lambda^{\lightning}_{\oplus}$, session types in $\mathsf{s}\pi$). A direct encoding of $\lambda^{\lightning}_{\oplus}$ into $\mathsf{s}\pi$ is far from obvious, as multiple occurrences of a variable in $\lambda^{\lightning}_{\oplus}$ must be accommodated into the linear setting of $\mathsf{s}\pi$. To overcome this challenge, we introduce a variant of $\lambda^{\lightning}_{\oplus}$, dubbed $\widehat{\lambda}^{\lightning}_{\oplus}$. The distinctive feature of $\widehat{\lambda}^{\lightning}_{\oplus}$ is a *sharing* construct, which we adopt following the *atomic* λ-calculus presented in [GHP13]. Our encoding of $\lambda^{\lightning}_{\oplus}$ expressions into $\mathsf{s}\pi$ processes is then in two steps. We first define a correct encoding from $\lambda^{\lightning}_{\oplus}$ to $\widehat{\lambda}^{\lightning}_{\oplus}$, which relies on the sharing construct to "atomize" occurrences of the same variable. Then, we define another correct encoding, from $\widehat{\lambda}^{\lightning}_{\oplus}$ to $\mathsf{s}\pi$, which extends Milner's with constructs for non-determinism.

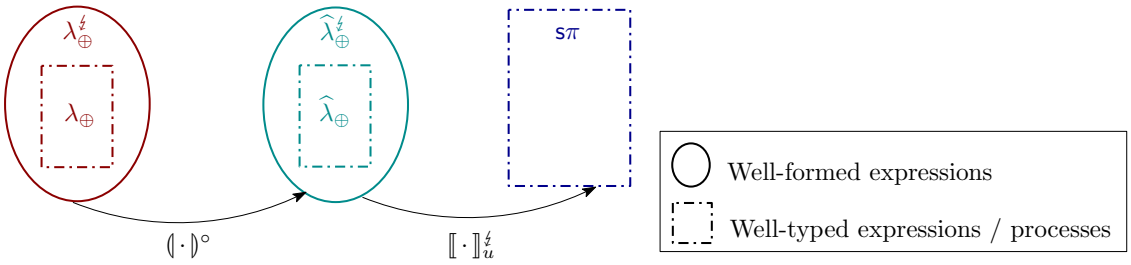


Figure 1: Overview of our approach.

Another challenge is framing failures in $\lambda^{\lightning}_{\oplus}$ (undesirable computations) as well-typed $\mathsf{s}\pi$ processes. Using intersection types, we define *well-formed* $\lambda^{\lightning}_{\oplus}$ expressions, which can fail, in two stages. First, we consider $\lambda_{\oplus}$, the sub-language of $\lambda^{\lightning}_{\oplus}$ without $\mathtt{fail}^{\widetilde{x}}$. We give an intersection type system for $\lambda_{\oplus}$ to regulate fail-free evaluation. Well-formed expressions are then defined on top of well-typed $\lambda_{\oplus}$ expressions. We show that $\mathsf{s}\pi$ can correctly encode the fail-free $\lambda_{\oplus}$ but, more interestingly, also well-formed $\lambda^{\lightning}_{\oplus}$ expressions, which are fail-prone.

Fig. 1 summarizes our approach: the encoding from $\lambda^{\lightning}_{\oplus}$ to $\widehat{\lambda}^{\lightning}_{\oplus}$ is denoted $(\!|\cdot|\!)^{\circ}$, whereas the encoding from $\widehat{\lambda}^{\lightning}_{\oplus}$ to $\mathsf{s}\pi$ is denoted $[\![\cdot]\!]^{\lightning}_{u}$.

Organization. Next, § 1 informally discusses key ideas in our work. § 2 introduces the syntax and semantics of $\lambda^{\lightning}_{\oplus}$, and defines its intersection type system. § 3 introduces $\widehat{\lambda}^{\lightning}_{\oplus}$, the variant of $\lambda^{\lightning}_{\oplus}$ with sharing. It also presents its associated intersection type system, and defines an encoding from $\lambda^{\lightning}_{\oplus}$ to $\widehat{\lambda}^{\lightning}_{\oplus}$. In § 4 we summarize the syntax, semantics, and session type system of $\mathsf{s}\pi$, following [CP17]. § 5 establishes the correctness of the encoding of $\lambda^{\lightning}_{\oplus}$ into $\widehat{\lambda}^{\lightning}_{\oplus}$ and presents and proves correct the encoding of $\widehat{\lambda}_{\oplus}$ into $\mathsf{s}\pi$. § 6 presents comparisons with related works. § 7 closes with a discussion about our approach and results.

This paper is an extended and revised version of the conference paper [PNP21a]. Here we have included full technical details, additional examples, and extended explanations. For the sake of readability, and to make the paper self-contained, we have included proof sketches in the main text; their corresponding full proofs have been collected in the appendices.

1. Overview of Key Ideas

Before embarking into our technical developments, we discuss some key ideas in the definition of $\lambda^{\lightning}_{\oplus}$ and its correct encodability into $\mathsf{s}\pi$.

Non-determinism. Our source language $\lambda^{\lightning}_{\oplus}$ has three syntactic categories: terms (M, M'), bags (B, B') and expressions $(\mathbb{M}, \mathbb{L})$. Terms can be variables, abstractions $\lambda x.M$, applications $(M\ B)$, explicit substitutions $M\langle\!\langle B/x \rangle\!\rangle$, or the explicit failure term $\mathtt{fail}$ (see below). Bags are multisets of terms (the resources); this way, e.g., $B = \{\!|M_1, M_1, M_2|\!\}$ is a bag with three resources (M_1, M_1, and M_2). Expressions are sums of terms, written $M_1 + M_2$; they denote a non-deterministic choice between different ways of *fetching* resources from the bag.

In $\lambda^{\lightning}_{\oplus}$, reduction is lazy: first, a β-reduction evolves to an explicit substitution, which will then fetch the elements in the bag to be substituted for the corresponding variable, when

some conditions are satisfied: we interpret this as "consuming a resource". For instance, given a $\lambda^{\not{!}}_{\oplus}$-term M with head variable x and two occurrences of x, we have the reduction:

$$\begin{aligned} \lambda x.M\wr M_1, M_2\wr &\longrightarrow M\langle\!\langle \wr M_1, M_2\wr / x\rangle\!\rangle \\ &\longrightarrow M\{\!|M_1/x|\!\}\langle\!\langle \wr M_2\wr / x\rangle\!\rangle + M\{\!|M_2/x|\!\}\langle\!\langle \wr M_1\wr / x\rangle\!\rangle = M' \end{aligned} \tag{1.1}$$

The resulting expression M' is a sum that gathers two alternative computations: it may reduce by either (i) first fetching M_1 from the bag and linearly substituting it for x in the head position of M (this is denoted with $M\{\!|M_1/x|\!\}$) and then continue with the rest of the bag (M_2, wrapped in an explicit substitution), or (ii) fetching and linearly substituting M_2 in head position, leaving M_1 in an explicit substitution.

Successful Reductions. We consider a computation as successful only when the number of elements in the bag matches the number of occurrences of the variable to be substituted; otherwise the computation fails. As an example, consider the previous example, now with $M = x\wr x\wr I\wr\wr$ where $I = \lambda z.z$ is the identity. The reduction in (1.1) is then

$$(\lambda x.x\wr x\wr I\wr\wr)\wr M_1, M_2\wr \longrightarrow^* M_1\wr x\wr I\wr\wr\langle\!\langle \wr M_2\wr / x\rangle\!\rangle + M_2\wr x\wr I\wr\wr\langle\!\langle \wr M_1\wr / x\rangle\!\rangle$$

Hence, when $\lambda x.M$ is applied to a bag with two resources, it evolves successfully. However, if $\lambda x.M$ is applied to a bag with less (or more) than two resources, the computation evolves to the *explicit failure* term $\mathtt{fail}^{\widetilde{z}}$, where $\widetilde{z}$ is a multiset of variables, as we explain next.

Explicit Failure. A construct for failure is present in the resource λ-calculus in [PR10]. In this formulation, the failure term '0' is consumed by sums and disappears at the end of the computation; as such, it gives no information about the failed computation and its origins.

Following [PR10], a design decision in $\lambda^{\not{!}}_{\oplus}$ is to have $\mathtt{fail}^{\widetilde{x}}$ in the syntax of terms. The sequence $\widetilde{x}$ denotes the variables captured by failure; this provides useful information on the origins of a failure. As an example, consider a term M with free variables $\widetilde{y}$ and in which the number of occurrences of x is different from 2. Given a bag $B = \wr M_1, M_2\wr$, reduction leads to a failure, as follows:

$$(\lambda x.M)B \longrightarrow M\ \langle\!\langle \wr M_1, M_2\wr / x\rangle\!\rangle \longrightarrow \sum_{\mathsf{PER}(\wr M_1, M_2\wr)} \mathtt{fail}^{\widetilde{y}} = M'$$

In this case, M' is the sum $\mathtt{fail}^{\widetilde{y}} + \mathtt{fail}^{\widetilde{y}}$, which has as many summands as the permutations of the elements of B. Intuitively, it means that it does not matter if one replaces the occurrence(s) of x first with M_1 (or M_2), then the other occurrence (if any), with M_2 (or M_1), the result will be the same, i.e., $\mathtt{fail}^{\widetilde{y}}$. Here again both possibilities are expressed in a sum. The precise semantics of failure will be presented in § 2.2.

Typability and Well-formedness. We define an intersection type system for $\lambda^{\not{!}}_{\oplus}$. This choice follows a well-established tradition of coupling resource λ-calculi with intersection types [Bou93, BL96, PR10]. Intersection types are also adopted in related calculi [ER03]. Intersection types are a natural typing structure for resources: they have similar mathematical properties of non-idempotency and commutativity, and can help to "count" the number of occurrences of a variable in a term, as well as the number of components in a bag.

In our type systems, each element of a bag must have the same type. This way, e.g., a well-typed bag $B = \wr M_1, M_2, M_3\wr$ has type $\sigma \wedge \sigma \wedge \sigma$, where σ is a strict type (cf. Def. 2.15). Then, an application $M\ B$ is well-typed, say, with type τ, only if $M : \sigma \wedge \sigma \wedge \sigma \to \tau$. We

shall write σ^k to denote the intersection type $\sigma \wedge \ldots \wedge \sigma$, with $k \geq 0$ copies of σ. Notice that σ^0 denotes the empty type ω. The typing rule for application is then as expected:

$$[\mathtt{T} : \mathtt{app}]\ \frac{\Gamma \vdash M : \sigma^k \to \tau \qquad \Gamma \vdash B : \sigma^k}{\Gamma \vdash M\ B : \tau}$$

where Γ is a type context assigning types to variables.

We chose to express explicit failing terms and computation. To properly account for these computations, we define a separate type system with so-called *well-formedness* rules, with notation '$\models$'. Unlike rules for typability, rules for well-formedness capture computations that fail due to a mismatch of resources (lack or excess). This entails some increased flexibility in selected rules. This way, e.g, the following is the well-formedness rule for application:

$$[\mathtt{F} : \mathtt{app}]\ \frac{\Gamma \models M : \sigma^j \to \tau \qquad \Gamma \models B : \sigma^k}{\Gamma \models M\ B : \tau}$$

Here the added flexibility is that we do not require $k = j$; hence, the rule can capture successful *and* failing computations, depending on whether $k = j$ or not. As expected, the term $\mathtt{fail}^{\widetilde{z}}$ is not well-typed, but it is well-formed: the judgement $\Gamma \models \mathtt{fail}^{\widetilde{z}} : \tau$ holds for an arbitrary type τ and a Γ consisting of variable assignments for the variables in $\widetilde{z}$.

Therefore, we consider two intersection type systems: one captures exclusively successful computations (see Fig. 3); the other, which we call the well-formedness system (see Fig. 4), subsumes the first one by admitting both successful and failing computations. The weakening rule is admissible in both systems (see below). Both systems enjoy subject reduction, whereas only well-typed terms satisfy subject expansion.

Controlling resources via sharing. In order to better control the use of resources, i.e., substituting variables for terms with a careful form of duplication, we borrow ideas from the *sharing graphs* by Guerrini et al. [Gue99, GMM03] and define the calculus $\widehat{\lambda}^{\mathlarger{\mathlarger{\mathlarger{\mathlarger{\iota}}}}}_{\oplus}$. The key idea is as follows: whenever a bound variable x occurs multiple times within a term, these occurrences, say $x_1, \ldots, x_n$, are temporarily assigned new names (think aliases). This assignment is indicated with the *sharing construct* $[x_1, \ldots, x_n \leftarrow x]$, which we adopt following [GHP13]. This way, for instance, the $\lambda^{\mathlarger{\mathlarger{\mathlarger{\mathlarger{\iota}}}}}_{\oplus}$-term $\lambda x.x\wr x \wr$ would correspond to $\lambda x.x_1\wr x_2 \wr[x_1, x_2 \leftarrow x]$ in $\widehat{\lambda}^{\mathlarger{\mathlarger{\mathlarger{\mathlarger{\iota}}}}}_{\oplus}$.

We also carefully treat the "erasing" of resources: if a term has vacuous abstractions, this is also indicated with the sharing construct, where the bound variable maps to "empty". Hence, the $\lambda^{\mathlarger{\mathlarger{\mathlarger{\mathlarger{\iota}}}}}_{\oplus}$-term $\lambda x.y\wr z \wr$ is expressed as $\lambda x.y\wr z \wr[\leftarrow x]$ in $\widehat{\lambda}^{\mathlarger{\mathlarger{\mathlarger{\mathlarger{\iota}}}}}_{\oplus}$. The tight control of resources in $\widehat{\lambda}^{\mathlarger{\mathlarger{\mathlarger{\mathlarger{\iota}}}}}_{\oplus}$ turns out to be very convenient to encode $\lambda^{\mathlarger{\mathlarger{\mathlarger{\mathlarger{\iota}}}}}_{\oplus}$ into $\mathsf{s}\pi$, as we discuss next.

Encoding $\lambda^{\mathlarger{\mathlarger{\mathlarger{\mathlarger{\iota}}}}}_{\oplus}$ into $\mathsf{s}\pi$. The central result of our work is a correct translation of $\lambda^{\mathlarger{\mathlarger{\mathlarger{\mathlarger{\iota}}}}}_{\oplus}$ into $\mathsf{s}\pi$. In defining our translation we use $\widehat{\lambda}^{\mathlarger{\mathlarger{\mathlarger{\mathlarger{\iota}}}}}_{\oplus}$ as a stepping stone. This is advantageous, because (i) the relation between $\widehat{\lambda}_{\oplus}$ and $\widehat{\lambda}^{\mathlarger{\mathlarger{\mathlarger{\mathlarger{\iota}}}}}_{\oplus}$ is fairly direct and (ii) the sharing construct in $\widehat{\lambda}^{\mathlarger{\mathlarger{\mathlarger{\mathlarger{\iota}}}}}_{\oplus}$ makes it explicit the variable occurrences that should be treated as linear names in $\mathsf{s}\pi$.

The encoding of $\lambda^{\mathlarger{\mathlarger{\mathlarger{\mathlarger{\iota}}}}}_{\oplus}$ into $\widehat{\lambda}^{\mathlarger{\mathlarger{\mathlarger{\mathlarger{\iota}}}}}_{\oplus}$ is denoted $(\!|\cdot|\!)^{\bullet}$ and given in § 3.4. The encoding of $\widehat{\lambda}^{\mathlarger{\mathlarger{\mathlarger{\mathlarger{\iota}}}}}_{\oplus}$ into $\mathsf{s}\pi$, denoted $[\![\cdot]\!]^{\mathlarger{\mathlarger{\mathlarger{\mathlarger{\iota}}}}}_{u}$ and presented in § 5.3.2, is arguably more interesting—we discuss it below.

The definition of $[\![\cdot]\!]^{\mathlarger{\mathlarger{\mathlarger{\mathlarger{\iota}}}}}_{u}$ considers well-formed source terms in $\widehat{\lambda}^{\mathlarger{\mathlarger{\mathlarger{\mathlarger{\iota}}}}}_{\oplus}$ which are translated into well-typed $\mathsf{s}\pi$ processes. As usual, the translation is parametric on a channel name u, which is used to provide the behavior of the source term.

The calculus $\mathsf{s}\pi$ includes a non-deterministic choice operator $P \oplus Q$ and formalizes sessions which are *non-deterministically available*. Intuitively, this means that a given session protocol along a name can either be available and proceed as prescribed by the corresponding session type, or fail to be available. Clearly, such a failure may have repercussions on other sessions that depend on it. To this end, $\mathsf{s}\pi$ includes prefixes $x.\overline{\texttt{some}}$ and $x.\overline{\texttt{none}}$, which are used to confirm the availability of x and to signal its failure, respectively. Process $x.\texttt{some}_{(w_1,\cdots,w_k)}; Q$ declares the dependency of sessions $w_1, \ldots, w_k$ in Q on an external session along x. The corresponding reduction rules are then:

$$\begin{array}{rcl} x.\overline{\texttt{some}} \mid x.\texttt{some}_{(w_1,\cdots,w_k)}; Q & \longrightarrow & Q \\ x.\overline{\texttt{none}} \mid x.\texttt{some}_{(w_1,\cdots,w_k)}; Q & \longrightarrow & w_1.\overline{\texttt{none}} \mid \cdots \mid w_k.\overline{\texttt{none}} \end{array}$$

Following Milner, $[\![\cdot]\!]^{\natural}_u$ maps computation in $\widehat{\lambda}^{\natural}_{\oplus}$ into session communication in $\mathsf{s}\pi$; non-deterministic sessions are used to codify the non-deterministic fetching of resources in $\widehat{\lambda}^{\natural}_{\oplus}$. This way, the translation of $(\lambda x.M[x_1, x_2 \leftarrow x])B$ will enable synchronizations between the translations of $M[x_1, x_2 \leftarrow x]$ and B. More in details, the translation of a bag $B = \wr M_1, M_2 \wr$ is as follows:

$$\begin{array}{rcl} [\![\wr M_1 \wr \cdot \wr M_2 \wr]\!]^{\natural}_x & = & x.\texttt{some}_{\widetilde{z_1},\widetilde{z_2}}; x(y_i).x.\texttt{some}_{y_i,\widetilde{z_1},\widetilde{z_2}}; x.\overline{\texttt{some}}; \\ & & \quad \overline{x}(x_i).(x_i.\texttt{some}_{\widetilde{z_1}}; [\![M_1]\!]^{\natural}_{x_i} \mid [\![\wr M_2 \wr]\!]^{\natural}_x \mid y_i.\overline{\texttt{none}}) \end{array}$$

where $\widetilde{z_1}$ and $\widetilde{z_2}$ denote the free variables of M_1 and M_2, respectively. Process $[\![\wr M_1 \wr \cdot \wr M_2 \wr]\!]^{\natural}_x$ first expects confirmation of session x; then, the translation of each resource M_i is made available in a dedicated name x_i, which will be communicated to other processes. Accordingly, the translation of $[\![M[x_1, x_2 \leftarrow x]]\!]^{\natural}_u$ is expected to synchronize with the translation of the bag B: indeed, it confirms behavior along x, before receiving the names, one for each shared copy of x that should be used throughout the synchronizations:

$$\begin{array}{rcl} [\![M[x_1, x_2 \leftarrow x]]\!]^{\natural}_u = x.\overline{\texttt{some}}.\overline{x}(y_1).\Big(y_1.\texttt{some}_{\emptyset}; y_1.\texttt{close} \mid x.\overline{\texttt{some}}; x.\texttt{some}_{u,(\mathsf{fv}(M)\setminus\{x_1,x_2\})}; x(x_1). \\ \quad .x.\overline{\texttt{some}}.\overline{x}(y_2).\big(y_2.\texttt{some}_{\emptyset}; y_2.\texttt{close} \mid x.\overline{\texttt{some}}; x.\texttt{some}_{u,(\mathsf{fv}(M)\setminus\{x_2\})}; x(x_2) \\ \quad .x.\overline{\texttt{some}}; \overline{x}(y).(y.\texttt{some}_{u,\mathsf{fv}(M)}; y.\texttt{close}; [\![M]\!]^{\natural}_u \mid x.\overline{\texttt{none}})\ \big)\Big) \end{array}$$

Several confirmations take place along the channel names involved in the synchronizations; see § 5.3.2 for details.

Non-determinism plays a key role in the translation of an application $M'B$. In this case, we consider the permutations of the elements of B using non-deterministic choice in $\mathsf{s}\pi$. When $B = \wr M_1, M_2 \wr$, the translation is:

$$\begin{array}{rcl} [\![M'\,B]\!]^{\natural}_u = (\nu v)([\![M']\!]^{\natural}_v \mid v.\texttt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([v \leftrightarrow u] \mid [\![\wr M_1, M_2 \wr]\!]^{\natural}_x)) \\ \quad \oplus \\ \quad (\nu v)([\![M']\!]^{\natural}_v \mid v.\texttt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([v \leftrightarrow u] \mid [\![\wr M_2, M_1 \wr]\!]^{\natural}_x)) \end{array}$$

A synchronization occurs when process $[\![M']\!]^{\natural}_v$ can confirm its behavior along v. For instance, when $M' = \lambda x.M[x_1, x_2 \leftarrow x]$ the translation is as

$$[\![\lambda x.M[x_1, x_2 \leftarrow x]]\!]^{\natural}_v = v.\overline{\texttt{some}}; v(x).[\![M[x_2, x_2 \leftarrow x]]\!]^{\natural}_v$$

and the synchronization may be possible; it depends on the translations of M, M_1, and M_2.

We close this section by observing that our translations $(\!|\cdot|\!)^{\bullet}$ and $[\![\cdot]\!]^{\lightning}_{u}$ satisfy well-known correctness criteria, as formulated by Gorla [Gor10] and Kouzapas et al. [KPY19] (see § 5.1 for details).

2. $\lambda^{\lightning}_{\oplus}$: A λ-calculus with Non-Determinism and Failure

We define the syntax and reduction semantics of $\lambda^{\lightning}_{\oplus}$, our new resource calculus with non-determinism and failure. We then equip it with non-idempotent session types, and establish the subject reduction property for well-typed and well-formed expressions (Theorems 2.20 and 2.28, respectively). We also consider the subject expansion property, which holds for well-typed expressions (Theorem 2.22) but not for well-formed ones (Theorem 2.29).

2.1. Syntax.

The syntax of $\lambda^{\lightning}_{\oplus}$ combines elements from calculi introduced and studied by Boudol and Laneve [BL00] and by Pagani and Ronchi della Rocca [PR10]. We use $x, y, \ldots$ to range over the set of *variables*. We write $\widetilde{x}$ to denote the sequence of pairwise distinct variables $x_1, \ldots, x_k$, for some $k \geq 0$. We write $|\widetilde{x}|$ to denote the length of $\widetilde{x}$.

Definition 2.1 (Syntax of $\lambda^{\lightning}_{\oplus}$)**.** The $\lambda^{\lightning}_{\oplus}$ calculus is defined by the following grammar:

$$\begin{array}{lllll} \text{(Terms)} & M, N, L & ::= & x \mid \lambda x.M \mid (M\ B) \mid M\langle\!\langle B/x \rangle\!\rangle \mid \mathtt{fail}^{\widetilde{x}} \\ \text{(Bags)} & A, B & ::= & \mathtt{1} \mid \wr M \wr \mid A \cdot B \\ \text{(Expressions)} & \mathbb{M}, \mathbb{N}, \mathbb{L} & ::= & M \mid \mathbb{M} + \mathbb{N} \end{array}$$

We have three syntactic categories: *terms* (in functional position); *bags* (in argument position), which denote multisets of resources; and *expressions*, which are finite formal sums that represent possible results of a computation. Terms are unary expressions: they can be variables, abstractions, and applications. Following [Bou93, BL00], the *explicit substitution* of a bag B for a variable x in a term M, written $M\langle\!\langle B/x \rangle\!\rangle$, is also a term. The term $\mathtt{fail}^{\widetilde{x}}$ results from a reduction in which there is a lack or excess of resources to be substituted, where $\widetilde{x}$ denotes a multiset of free variables that are encapsulated within failure.

The empty bag is denoted $\mathtt{1}$. The bag enclosing the term M is $\wr M \wr$. The concatenation of bags B_1 and B_2 is denoted as $B_1 \cdot B_2$; the concatenation operator '$\cdot$' is associative and commutative, with $\mathtt{1}$ as its identity. To ease readability, we rely on a shorthand notation for bags: we often write $\wr N_1, N_2 \wr$ rather than $\wr N_1 \wr \cdot \wr N_2 \wr$.

We treat expressions as *sums*, and use notations such as $\sum_i^n N_i$ for them. Sums are associative and commutative; reordering of the terms in a sum is performed silently.

Example 2.2. We give some examples of terms and expressions in $\lambda^{\lightning}_{\oplus}$:

- $M_1 = (\lambda x.x)\wr y \wr$
- $M_2 = (\lambda x.x)(\wr y, z \wr)$
- $M_3 = (\lambda x.x)\mathtt{1}$
- $M_4 = (\lambda x.y)\mathtt{1}$
- $M_5 = \mathtt{fail}^{\emptyset}$
- $M_6 = (\lambda x.x)\wr y \wr + (\lambda x.x)\wr z \wr$

Terms M_1, M_2, and M_3 illustrate the application of the identity function $I = \lambda x.x$ to bags with different formats: a bag with one component, two components, and the empty bag, respectively. Special attention should be given to the fact that the x has only one occurrence in I, whereas the bags contain zero or more components (resources). This way:

- M_1 represents a term with a *correct* number of resources;
- M_2 denotes a term with an *excess* of resources; and
- M_3 denotes a term with a *lack* of resources

This resource interpretation will become clearer once the reduction semantics is introduced in the next subsection (cf. Example 2.11).

Term M_4 denotes the application of a vacuous abstraction on x to the empty bag $\mathtt{1}$. Term M_5 denotes a failure term with no associated variables. Expression M_6 denotes the non-deterministic sum between two terms, each of which denotes an application of I to a bag containing one element.

Notation 2.3 (Expressions)**.** Notation $N \in \mathbb{M}$ denotes that N is part of the sum denoted by $\mathbb{M}$. Similarly, we write $N_i \in B$ to denote that N_i occurs in the bag B, and $B \setminus\!\setminus N_i$ to denote the bag that is obtained by removing one occurrence of the term N_i from B.

2.2. **Reduction Semantics.**

Reduction in $\lambda^{\lightning}_{\oplus}$ is defined in terms of the relation $\longrightarrow$, defined in Fig. 2; it operates lazily on expressions, and will be described after introducing some auxiliary notions.

Notation 2.4. We write $\mathsf{PER}(B)$ to denote the set of all permutations of bag B. Also, $B_i(n)$ denotes the n-th term in the (permuted) B_i. We define $\mathsf{size}(B)$ to denote the number of terms in bag B. That is, $\mathsf{size}(\mathtt{1}) = 0$ and $\mathsf{size}(\wr M \wr \cdot B) = 1 + \mathsf{size}(B)$.

Definition 2.5 (Set and Multiset of Free Variables)**.** The set of free variables of a term, bag, and expression, is defined as

$$\begin{aligned} \mathsf{fv}(x) &= \{x\} \\ \mathsf{fv}(\lambda x.M) &= \mathsf{fv}(M) \setminus \{x\} \\ \mathsf{fv}(M\ B) &= \mathsf{fv}(M) \cup \mathsf{fv}(B) \\ \mathsf{fv}(M\langle\!\langle B/x \rangle\!\rangle) &= (\mathsf{fv}(M) \setminus \{x\}) \cup \mathsf{fv}(B) \end{aligned} \qquad \begin{aligned} \mathsf{fv}(\mathtt{1}) &= \emptyset \\ \mathsf{fv}(\wr M \wr) &= \mathsf{fv}(M) \\ \mathsf{fv}(B_1 \cdot B_2) &= \mathsf{fv}(B_1) \cup \mathsf{fv}(B_2) \\ \mathsf{fv}(\mathtt{fail}^{x_1,\cdots,x_n}) &= \{x_1, \cdots, x_n\} \\ \mathsf{fv}(\mathbb{M} + \mathbb{N}) &= \mathsf{fv}(\mathbb{M}) \cup \mathsf{fv}(\mathbb{N}) \end{aligned}$$

We use $\mathsf{mfv}(M)$ or $\mathsf{mfv}(B)$ to denote a multiset of free variables, defined similarly. We sometimes treat the sequence $\widetilde{x}$ as a (multi)set. We write $\widetilde{x} \uplus \widetilde{y}$ to denote the multiset union of $\widetilde{x}$ and $\widetilde{y}$ and $\widetilde{x} \setminus y$ to express that every occurrence of y is removed from $\widetilde{x}$. A term M is *closed* if $\mathsf{fv}(M) = \emptyset$ (and similarly for expressions). As usual, we shall consider $\lambda^{\lightning}_{\oplus}$-terms modulo α-equivalence.

Notation 2.6. $\#(x, M)$ denotes the number of (free) occurrences of x in M. Similarly, we write $\#(x, \widetilde{y})$ to denote the number of occurrences of x in the multiset $\widetilde{y}$.

Definition 2.7 (Head)**.** Given a term M, we define $\mathsf{head}(M)$ inductively as:

$$\begin{aligned} \mathsf{head}(x) &= x \\ \mathsf{head}(\lambda x.M) &= \lambda x.M \\ \mathsf{head}(M\ B) &= \mathsf{head}(M) \end{aligned} \qquad \begin{aligned} \mathsf{head}(\mathtt{fail}^{\widetilde{x}}) &= \mathtt{fail}^{\widetilde{x}} \\ \mathsf{head}(M\langle\!\langle B/x \rangle\!\rangle) &= \begin{cases} \mathsf{head}(M) & \text{if } \#(x, M) = \mathsf{size}(B) \\ \mathtt{fail}^{\emptyset} & \text{otherwise} \end{cases} \end{aligned}$$

Definition 2.8 (Linear Head Substitution)**.** Let M be a term such that $\mathsf{head}(M) = x$. The *linear head substitution* of a term N for x in M, denoted $M\{\!|N/x|\!\}$, is defined as:

$$\begin{aligned} x\{\!|N/x|\!\} &= N \\ (M\ B)\{\!|N/x|\!\} &= (M\{\!|N/x|\!\})\ B \\ (M\ \langle\!\langle B/y \rangle\!\rangle)\{\!|N/x|\!\} &= (M\{\!|N/x|\!\})\ \langle\!\langle B/y \rangle\!\rangle \qquad \text{where } x \neq y \end{aligned}$$

$$[\mathtt{R}:\mathtt{Beta}]\ \frac{}{(\lambda x.M)B \longrightarrow M\ \langle\!\langle {}^{B}/_{x} \rangle\!\rangle}$$

$$[\mathtt{R}:\mathtt{Fetch}]\ \frac{\mathsf{head}(M)=x \qquad B=\wr N_1,\ldots,N_k\wr,\ k\geq 1 \qquad \#(x,M)=k}{M\ \langle\!\langle {}^{B}/_{x} \rangle\!\rangle \longrightarrow M\{\!|N_1/x|\!\}\langle\!\langle {}^{(B\setminus\!\setminus N_1)}/_{x} \rangle\!\rangle + \cdots + M\{\!|N_k/x|\!\}\langle\!\langle {}^{(B\setminus\!\setminus N_k)}/_{x} \rangle\!\rangle}$$

$$[\mathtt{R}:\mathtt{Fail}]\ \frac{\#(x,M)\neq \mathsf{size}(B) \qquad \widetilde{y}=(\mathsf{mfv}(M)\setminus x)\uplus \mathsf{mfv}(B)}{M\ \langle\!\langle {}^{B}/_{x} \rangle\!\rangle \longrightarrow \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{y}}}$$

$$[\mathtt{R}:\mathtt{Cons_1}]\ \frac{\widetilde{y}=\mathsf{mfv}(B)}{\mathtt{fail}^{\widetilde{x}}\ B \longrightarrow \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{x}\uplus\widetilde{y}}}$$

$$[\mathtt{R}:\mathtt{Cons_2}]\ \frac{\mathsf{size}(B)=k \qquad \#(z,\widetilde{x})+k\neq 0 \qquad \widetilde{y}=\mathsf{mfv}(B)}{\mathtt{fail}^{\widetilde{x}}\ \langle\!\langle {}^{B}/_{z} \rangle\!\rangle \longrightarrow \sum_{\mathsf{PER}(B)} \mathtt{fail}^{(\widetilde{x}\setminus z)\uplus\widetilde{y}}}$$

$$[\mathtt{R}:\mathtt{TCont}]\ \frac{M \longrightarrow M'_1+\cdots+M'_k}{C[M]\longrightarrow C[M'_1]+\cdots+C[M'_k]} \qquad [\mathtt{R}:\mathtt{ECont}]\ \frac{\mathbb{M}\longrightarrow\mathbb{M}'}{D[\mathbb{M}]\longrightarrow D[\mathbb{M}']}$$

Figure 2: Reduction Rules for $\lambda^{\lightning}_{\oplus}$

Finally, we define contexts for terms and expressions and convenient notations:

Definition 2.9 (Term and Expression Contexts)**.** Contexts for terms (CTerm) and expressions (CExpr) are defined by the following grammar:

$$\text{(CTerm)}\quad C[\cdot], C'[\cdot] ::= ([\cdot])B \mid ([\cdot])\langle\!\langle {}^{B}/_{x} \rangle\!\rangle \qquad \text{(CExpr)}\quad D[\cdot], D'[\cdot] ::= M + [\cdot] \mid [\cdot] + M$$

The reduction relation on $\lambda^{\lightning}_{\oplus}$ is defined by the rules in Fig. 2. Intuitively, reductions in $\lambda^{\lightning}_{\oplus}$ work as follows: A β-reduction induces an explicit substitution of a bag B for a variable x in a term M, denoted $M\langle\!\langle {}^{B}/_{x} \rangle\!\rangle$. In the case the head of the term M is x and the size of the bag B coincides with the number of occurrences of x in M, this explicit substitution is expanded into a sum of terms, each of which features a *linear head substitution* $M\{\!|N_i/x|\!\}$, where N_i is a term in B, which will replace the variable x occurring in the head of M; the rest of the bag $(B \setminus\!\setminus N_i)$ is kept in an explicit substitution. However, if there is a mismatch between the number of occurrences of the variable to be substituted and the number of resources available, then the reduction leads to the failure term. Formally,

- **Rule** $[\mathtt{R}:\mathtt{Beta}]$ is standard and admits a bag (possibly empty) as parameter.
- **Rule** $[\mathtt{R}:\mathtt{Fetch}]$ transforms a term into an expression: it opens up an explicit substitution into a sum of terms with linear head substitutions, each denoting the partial evaluation of an element from the bag, considering all the possible choices for substituting an element N_i of the bag for x. Hence, the size of the bag will determine the number of summands in the resulting expression.

There are three rules reduce to the failure term: their objective is to accumulate all (free) variables involved in failed reductions.

- **Rule** $[\mathtt{R} : \mathtt{Fail}]$ formalizes failure in the evaluation of an explicit substitution $M\ \langle\!\langle {}^{B}\!/_{x} \rangle\!\rangle$, which occurs if there is a mismatch between the resources (terms) present in B and the number of occurrences of x to be substituted. The resulting failure preserves all free variables in M and B within its attached multiset $\widetilde{y}$, and all possible computations that could have failed, via permutation of the bags, are captured in a non-deterministic sum.
- **Rules** $[\mathtt{R} : \mathtt{Cons}_1]$ **and** $[\mathtt{R} : \mathtt{Cons}_2]$ describe reductions that lazily consume the failure term, when a term has $\mathtt{fail}^{\widetilde{x}}$ at its head position. The former rule consumes bags attached to it whilst preserving all its free variables. The latter rule is similar but for the case of explicit substitutions; its second premise ensures that either (i) the bag in the substitution is not empty or (ii) the number of occurrences of z in the current multiset of accumulated variables is not zero.

Notice that our Rule $[\mathtt{R} : \mathtt{Fail}]$ rule evolves to a sum of failure terms, where each summand accounts for a permutation of the elements of the bag. As our reduction strategy fails eagerly this may not be evident at first; however, there is still a non-deterministic choice of elements in B that are waiting to be substituted at the point of failure (see Example 2.12).

Finally, we describe the contextual rules:

- **Rule** $[\mathtt{R} : \mathtt{TCont}]$ describes the reduction of sub-terms within an expression; in this rule, summations are expanded outside of term contexts.
- **Rule** $[\mathtt{R} : \mathtt{ECont}]$ says that reduction of expressions is closed by expression contexts.

Notation 2.10. As standard, $\longrightarrow$ denotes one step reduction; $\longrightarrow^{+}$ and $\longrightarrow^{*}$ denote the transitive and the reflexive-transitive closure of $\longrightarrow$, respectively. We write $\mathbb{N} \longrightarrow_{[\mathtt{R}]} \mathbb{M}$ to denote that $[\mathtt{R}]$ is the last (non-contextual) rule used in inferring the step from $\mathbb{N}$ to $\mathbb{M}$.

Example 2.11 (Cont. Example 2.2)**.** We show how the terms in Example 2.2 can reduce:

- Reduction of the term M_1 with an adequate number of resources:

$$\begin{aligned}(\lambda x.x)\wr y \wr &\longrightarrow_{[\mathtt{R:Beta}]} x\langle\!\langle \wr y \wr /_{x} \rangle\!\rangle \\ &\longrightarrow_{[\mathtt{R:Fetch}]} y\langle\!\langle \mathtt{1}/_{x} \rangle\!\rangle \qquad \text{since } \#(x,x) = \mathsf{size}(\wr y \wr) = 1\end{aligned}$$

- Reduction of term M_2 with excess of resources:

$$\begin{aligned}(\lambda x.x)(\wr y, z \wr) &\longrightarrow_{[\mathtt{R:Beta}]} x\langle\!\langle (\wr y, z \wr)/_{x} \rangle\!\rangle \\ &\longrightarrow_{[\mathtt{R:Fail}]} \mathtt{fail}^{y,z} + \mathtt{fail}^{y,z}, \quad \text{since } \#(x,x) = 1 \neq \mathsf{size}(\wr y, z \wr) = 2\end{aligned}$$

- Reduction of term M_3 with lack of resources:

$$\begin{aligned}(\lambda x.x)\mathtt{1} &\longrightarrow_{[\mathtt{R:Beta}]} x\langle\!\langle \mathtt{1}/_{x} \rangle\!\rangle \\ &\longrightarrow_{[\mathtt{R:Fail}]} \mathtt{fail}^{\emptyset}, \quad \text{since } \#(x,x) = 1 \neq \mathsf{size}(\mathtt{1}) = 0\end{aligned}$$

- Reduction of term M_4 which is a vacuous abstraction applied to an empty bag:

$$(\lambda x.y)\mathtt{1} \longrightarrow_{[\mathtt{R:Beta}]} y\langle\!\langle \mathtt{1}/_{x} \rangle\!\rangle$$

- $M_5 = \mathtt{fail}^{\emptyset}$ is unable to perform any reductions, i.e., it is irreducible.
- Reductions of the expression $M_6 = (\lambda x.x)\wr y \wr + (\lambda x.x)\wr z \wr$:

$$\begin{array}{ccccc} & & x\langle\!\langle \wr y \wr /_{x} \rangle\!\rangle + (\lambda x.x)\wr z \wr & & \\ & \nearrow & & \searrow & \\ (\lambda x.x)\wr y \wr + (\lambda x.x)\wr z \wr & & & & x\langle\!\langle \wr y \wr /_{x} \rangle\!\rangle + x\langle\!\langle \wr z \wr /_{x} \rangle\!\rangle \\ & \searrow & & \nearrow & \\ & & (\lambda x.x)\wr y \wr + x\langle\!\langle \wr z \wr /_{x} \rangle\!\rangle & & \end{array}$$

The following example illustrates the use of $\mathsf{PER}(B)$ in Rule [R : Fail]: independently of the order in which the resources in the bag are used, the computation fails.

Example 2.12. Let $M = (\lambda x.x\wr x\wr y\int\int)\ B$, with $B = \wr z_1, z_2, z_1\int$. We have:

$$M \longrightarrow_{[\mathtt{R:Beta}]} x\wr x\wr y\int\int\langle\!\langle \wr z_1, z_2, z_1\int/x\rangle\!\rangle$$
$$\longrightarrow_{[\mathtt{R:Fail}]} \sum_{\mathsf{PER}(B)} \mathtt{fail}^{y,z_1,z_2,z_1}$$

The number of occurrences of x in the term obtained after β-reduction (2) does not match the size of the bag (3). Therefore, the reduction leads to failure. Notice that $\sum_{\mathsf{PER}(B)} \mathtt{fail}^{y,z_1,z_2,z_1}$ expands to a sum between six instances of $\mathtt{fail}^{y,z_1,z_2,z_1}$, corresponding to permutation of 3 elements of the bag B.

Notice that the left-hand sides of the reduction rules in $\lambda^{\wr}_{\oplus}$ do not interfere with each other. Therefore, reduction in $\lambda^{\wr}_{\oplus}$ satisfies a *diamond property*:

Proposition 2.13 (Diamond Property for $\lambda^{\wr}_{\oplus}$)**.** *For all* $\mathbb{N}$, $\mathbb{N}_1$, $\mathbb{N}_2$ *in* $\lambda^{\wr}_{\oplus}$ *s.t.* $\mathbb{N} \longrightarrow \mathbb{N}_1$, $\mathbb{N} \longrightarrow \mathbb{N}_2$ *with* $\mathbb{N}_1 \neq \mathbb{N}_2$ *then there exists* $\mathbb{M}$ *such that* $\mathbb{N}_1 \longrightarrow \mathbb{M}$, $\mathbb{N}_2 \longrightarrow \mathbb{M}$.

Proof (Sketch). By inspecting the rules of Fig. 2 one can check that the left-hand sides only clash in a non-variable position with Rules [R : Fail] and [R : Cons2]. The clash does not generate a critical pair: in fact, when applied to the $\lambda^{\wr}_{\oplus}$-term $\mathtt{fail}^{z,\widetilde{x}}\langle\!\langle \mathsf{1}/z\rangle\!\rangle$ both rules reduce to $\mathtt{fail}^{\widetilde{x}}$. For all the other rules, whenever they have the same shape, the side conditions of the rules determine which rule can be applied. Therefore, an expression can only perform a choice of reduction steps when it is a sum of terms in which multiple summands can perform independent reductions. Without loss of generality, consider an expression $\mathbb{N} = N + M$ such that $N \longrightarrow N'$ and $M \longrightarrow M'$. Then we let $\mathbb{N}_1 = N' + M$ and $\mathbb{N}_2 = N + M'$ by Rule [R : ECont]. The result follows for $\mathbb{M} = N' + M'$, since $\mathbb{N}_1 \longrightarrow \mathbb{M}$ and $\mathbb{N}_2 \longrightarrow \mathbb{M}$. □

Remark 2.14 (A Sub-calculus without Failure ($\lambda_{\oplus}$))**.** We find it convenient to define $\lambda_{\oplus}$, the sub-calculus of $\lambda^{\wr}_{\oplus}$ without explicit failure. The syntax of $\lambda_{\oplus}$ is obtained from Definition 2.1 by excluding $\mathtt{fail}^{\widetilde{x}}$ from the syntax of terms. Accordingly, the reduction relation for $\lambda_{\oplus}$ is given by Rules [R : Beta], [R : Fetch], [R : ECont], and [R : TCont] in Fig. 2. Finally, Definition 2.7 is kept unchanged with the provision that $\mathsf{head}(M\langle\!\langle B/x\rangle\!\rangle)$ is undefined when $\#(x, M) \neq \mathsf{size}(B)$.

2.3. Well-formed $\lambda^{\wr}_{\oplus}$-Expressions.

As mentioned in § 1, we define a notion of *well-formed expressions* for $\lambda^{\wr}_{\oplus}$ by relying on a non-idempotent intersection type system, similar to the one given by Pagani and Della Rocca in [PR10]. Our system for well-formed expressions will be defined in two stages:

(1) First we define a intersection type system for the sub-language $\lambda_{\oplus}$ (cf. Rem. 2.14), given in Fig. 3. Unlike the system in [PR10], our type system includes a weakening rule and a rule for typing explicit substitutions.
(2) Second, we define well-formed expressions for the full language $\lambda^{\wr}_{\oplus}$, via Def. 2.24.

We say that we check for "well-formedness" (of terms, bags, and expressions) to stress that, unlike standard type systems, our system is able to account for terms that may reduce to the failure term.

$$[\mathtt{T}:\mathtt{var}]\ \frac{}{x:\sigma\vdash x:\sigma} \qquad [\mathtt{T}:\mathtt{1}]\ \frac{}{\vdash \mathtt{1}:\omega} \qquad [\mathtt{T}:\mathtt{weak}]\ \frac{\Gamma\vdash M:\sigma}{\Gamma,x:\omega\vdash M:\sigma}$$

$$[\mathtt{T}:\mathtt{abs}]\ \frac{\Gamma,x:\sigma^k\vdash M:\tau}{\Gamma\vdash \lambda x.M:\sigma^k\to\tau} \qquad [\mathtt{T}:\mathtt{bag}]\ \frac{\Gamma\vdash M:\sigma \qquad \Delta\vdash B:\sigma^k}{\Gamma\wedge\Delta\vdash \{\!|M|\!\}\cdot B:\sigma^{k+1}}$$

$$[\mathtt{T}:\mathtt{app}]\ \frac{\Gamma\vdash M:\pi\to\tau \qquad \Delta\vdash B:\pi}{\Gamma\wedge\Delta\vdash M\ B:\tau} \qquad [\mathtt{T}:\mathtt{ex\text{-}sub}]\ \frac{\Gamma,x:\sigma^k\vdash M:\tau \qquad \Delta\vdash B:\sigma^k}{\Gamma\wedge\Delta\vdash M\langle\!\langle {}^{B}\!/_{x}\rangle\!\rangle:\tau}$$

$$[\mathtt{T}:\mathtt{sum}]\ \frac{\Gamma\vdash \mathbb{M}:\sigma \qquad \Gamma\vdash \mathbb{N}:\sigma}{\Gamma\vdash \mathbb{M}+\mathbb{N}:\sigma}$$

Figure 3: Typing Rules for $\lambda_{\oplus}$

2.3.1. *Intersection Types.*

Intersection types allow us to reason about types of resources in bags but also about every occurrence of a variable. That is, non-idempotent intersection types enable us to distinguish expressions not only by measuring the size of a bag but also by counting the number of times a variable occurs within a term.

Definition 2.15 (Types for $\lambda^{\not\iota}_{\oplus}$)**.** We define *strict* and *multiset types* by the grammar:

$$\text{(Strict)}\quad \sigma,\tau,\delta ::= \mathbf{unit} \mid \pi\to\sigma \qquad\qquad \text{(Multiset)}\quad \pi ::= \sigma^k \mid \omega$$

where σ^k stands for $\sigma\wedge\cdots\wedge\sigma$ (k times, for some $k>0$).

A strict type can be the unit type **unit** or a functional type $\pi\to\sigma$, where π is a multiset type and σ is a strict type. Multiset types can be either an intersection of strict types σ^k (if $k>0$) or the empty type ω, which would correspond to σ^k with $k=0$. Hence, σ^k denotes an intersection; the operator $\wedge$ is commutative, associative, and non-idempotent, that is, $\sigma\wedge\sigma\neq\sigma$. The empty type is the type of the empty bag; it acts as the identity element to $\wedge$.

Definition 2.16. *Type contexts* $\Gamma,\Delta,\ldots$ are sets of type assignments $x:\pi$, as defined by the grammar:

$$\Gamma,\Delta = \text{-} \mid \Gamma, x:\pi$$

The set of variables in Γ is denoted as $\mathtt{dom}(\Gamma)$. In writing $\Gamma,x:\pi$ we assume that $x\notin\mathtt{dom}(\Gamma)$. We generalize the operator $\wedge$ from types to contexts, and define $\Gamma\wedge\Delta$ as follows:

$$(\Gamma_1\wedge\Gamma_2)(x) = \begin{cases} x:\pi_1\wedge\pi_2 & x:\pi_i\in\Gamma_i,\ \pi_i\neq\omega,\ i\in\{1,2\} \\ x:\pi_i & x:\pi_i\in\Gamma_i, x\notin\mathtt{dom}(\Gamma_j),\ i\neq j,\ i,j\in\{1,2\} \\ \text{undefined} & \text{otherwise} \end{cases}$$

Type judgements are of the form $\Gamma\vdash\mathbb{M}:\sigma$, where Γ is a type context. We write $\vdash\mathbb{M}:\sigma$ to denote $\text{-}\vdash\mathbb{M}:\sigma$.

Definition 2.17. (Well-typed Expressions) An expression $\mathbb{M}\in\lambda_{\oplus}$ is *well-typed* (or typable) if there exist Γ and τ such that $\Gamma\vdash\mathbb{M}:\tau$ is entailed via the rules in Fig. 3.

The rules are standard. We only consider intersections of the same strict type, say σ, since the current objective is to count the number of occurrences of a variable in a term, and measure the size of a bag. We now give a brief description of the rules in Fig. 3:

- **Rules** [T:var]**,** [T:1] **and** [T:weak] are as expected: the first assigns a type to a variable, the second assigns the empty bag $\mathtt{1}$ the empty type ω, and the third introduces a useful weakening principle.
- **Rule** $[\mathtt{T}:\mathtt{abs}]$ types an abstraction $\lambda x.M$ with $\sigma^k \to \tau$, as long as the variable assignment $x : \sigma^k$ has an intersection type with σ occurring exactly k times.
- **Rule** $[\mathtt{T}:\mathtt{bag}]$ types a bag B with a type σ^{k+1} as long as every component of B is typed with same type σ, a defined amount of times.
- **Rule** [T:app] types an application $M\ B$ with τ as long as M and B match on the multiset type π, i.e., $M : \pi \to \tau$ and $B : \pi$. Intuitively, this means that M expects a fixed amount of resources, and B has exactly this number of resources.
- **Rule** [T:ex-sub] types an explicit substitution $M\langle\!\langle {}^{B}/_{x} \rangle\!\rangle$ with τ as long as the bag B consists of elements of the same type as x and the size of B matches the number of times x occurs in M, i.e., $B : \sigma^k$ and $x : \sigma^k$ types the assignment of $M : \tau$.
- **Rule** $[\mathtt{T}:\mathtt{sum}]$ types an expression (a sum) with a type σ, if each summand has type σ.

Notice that with the typing rules for $\lambda_{\oplus}$ the failure term `fail` cannot be typed. We could consider this set of rules as a type system for $\lambda^{\lightning}_{\oplus}$, i.e. the extension of $\lambda_{\oplus}$ with failure, in which failure can be expressed but not typed.

Example 2.18 (Cont. Example 2.11)**.** We explore the typability of some of the terms given in previous examples:

(1) Term $M_1 = (\lambda x.x)\wr y \wr$ is typable, as we have:

$$\dfrac{\dfrac{[\mathtt{T}:\mathtt{var}]\ \dfrac{}{x:\sigma \vdash x:\sigma}}{[\mathtt{T}:\mathtt{abs}]\ \vdash \lambda x.x : \sigma \to \sigma} \qquad \dfrac{[\mathtt{T}:\mathtt{var}]\ \dfrac{}{y:\sigma \vdash y:\sigma}}{[\mathtt{T}:\mathtt{bag}]\ y:\sigma \vdash \wr y \wr \cdot \mathtt{1} : \sigma} \qquad [\mathtt{T}:\mathtt{1}]\ \dfrac{}{\vdash \mathtt{1} : \omega}}{[\mathtt{T}:\mathtt{app}]\ y:\sigma \vdash (\lambda x.x)\wr y \wr : \sigma}$$

(2) Term $M_2 = (\lambda x.x)(\wr y, z \wr)$ is not typable.
- The function $\lambda x.x$ has a functional type $\sigma \to \sigma$;
- The bag has an intersection type of size two: $y : \sigma, z : \sigma \vdash (\wr y, z \wr) : \sigma^2$;
- Rule $[\mathtt{T}:\mathtt{app}]$ requires a match between the type of the bag and the left of the arrow: it can only consume a bag of type σ.

(3) Similarly, $M_3 = (\lambda x.x)\mathtt{1}$ is not typable: since $\lambda x.x$ has type $\sigma \to \sigma$, to apply the Rule $[\mathtt{T}:\mathtt{app}]$ the bag must have a type σ, but the empty bag $\mathtt{1}$ can only be typed with ω.

(4) Term $M_4 = (\lambda x.y)\mathtt{1}$ is typable, as follows:

$$\dfrac{\dfrac{[\mathtt{T}:\mathtt{var}]\ \dfrac{}{y:\sigma \vdash y:\sigma}}{[\mathtt{T}:\mathtt{weak}]\ y:\sigma, x:\omega \vdash y:\sigma} \qquad [\mathtt{T}:\mathtt{1}]\ \dfrac{}{\vdash \mathtt{1} : \omega}}{[\mathtt{T}:\mathtt{abs}]\ y:\sigma \vdash \lambda x.y : \omega \to \sigma \qquad [\mathtt{T}:\mathtt{app}]\ y:\sigma \vdash (\lambda x.y)\mathtt{1} : \sigma}$$

Our typing system for $\lambda_{\oplus}$ satisfies standard properties, such as subject reduction, which follows from the *Linear* Substitution Lemma. We stress 'linearity' because the lemma is stated in terms of the head linear substitution $\{\!|\cdot|\!\}$.

Lemma 2.19 (Linear Substitution Lemma for $\lambda_{\oplus}$)**.** *If* $\Gamma, x : \sigma^k \vdash M : \tau$ *(with* $k \geq 1$*),* $\mathsf{head}(M) = x$*, and* $\Delta \vdash N : \sigma$ *then* $\Gamma \wedge \Delta, x : \sigma^{k-1} \vdash M\{\!|N/x|\!\} : \tau$*.*

Proof. Standard, by induction on the rule applied in $\Gamma, x : \sigma \vdash M : \tau$. □

$$[\mathtt{F}:\mathtt{wf\text{-}expr}]\ \frac{\Gamma \vdash \mathbb{M} : \tau}{\Gamma \models \mathbb{M} : \tau} \qquad [\mathtt{F}:\mathtt{wf\text{-}bag}]\ \frac{\Gamma \vdash B : \pi}{\Gamma \models B : \pi} \qquad [\mathtt{F}:\mathtt{weak}]\ \frac{\Delta \models M : \tau}{\Delta, x : \omega \models M : \tau}$$

$$[\mathtt{F}:\mathtt{abs}]\ \frac{\Gamma, x : \sigma^n \models M : \tau \quad x \notin \mathtt{dom}(\Gamma)}{\Gamma \models \lambda x.M : \sigma^n \to \tau} \qquad [\mathtt{F}:\mathtt{bag}]\ \frac{\Gamma \models M : \sigma \qquad \Delta \models B : \sigma^k}{\Gamma \wedge \Delta \models \wr M \wr \cdot B : \sigma^{k+1}}$$

$$[\mathtt{F}:\mathtt{sum}]\ \frac{\Gamma \models \mathbb{M} : \sigma \qquad \Gamma \models \mathbb{N} : \sigma}{\Gamma \models \mathbb{M} + \mathbb{N} : \sigma} \qquad [\mathtt{F}:\mathtt{fail}]\ \frac{\mathtt{dom}(\Gamma^\dagger) = \widetilde{x}}{\Gamma \models \mathtt{fail}^{\widetilde{x}} : \tau}$$

$$[\mathtt{F}:\mathtt{ex\text{-}sub}]\ \frac{\Gamma, x : \sigma^k \models M : \tau \qquad \Delta \models B : \sigma^j \quad k, j \geq 0}{\Gamma \wedge \Delta \models M\langle\!\langle B/x \rangle\!\rangle : \tau}$$

$$[\mathtt{F}:\mathtt{app}]\ \frac{\Gamma \models M : \sigma^j \to \tau \qquad \Delta \models B : \sigma^k \qquad k, j \geq 0}{\Gamma \wedge \Delta \models M\ B : \tau}$$

Figure 4: Well-Formed Rules for $\lambda^{\not\iota}_{\oplus}$

Theorem 2.20 (Subject Reduction for $\lambda_{\oplus}$)**.** *If* $\Gamma \vdash \mathbb{M} : \tau$ *and* $\mathbb{M} \longrightarrow \mathbb{M}'$ *then* $\Gamma \vdash \mathbb{M}' : \tau$.

Proof. By induction on the reduction rule (Fig. 2) applied in $\mathbb{M}$. □

Lemma 2.21 (Linear Anti-substitution Lemma for $\lambda_{\oplus}$)**.** *Let* M *and* N *be* $\lambda_{\oplus}$*-terms such that* $\mathsf{head}(M) = x$*, then we have:*

- $\Gamma, x : \sigma^{k-1} \vdash M\{\!|N/x|\!\} : \tau$*, with* $k > 1$*, then there exist* Γ_1, Γ_2 *such that* $\Gamma_1, x : \sigma^k \vdash M : \tau$*, and* $\Gamma_2 \vdash N : \sigma$*, where* $\Gamma = \Gamma_1 \wedge \Gamma_2$.
- $\Gamma \vdash M\{\!|N/x|\!\} : \tau$*, with* $x \notin \mathtt{dom}(\Gamma)$*, then there exist* Γ_1, Γ_2 *such that* $\Gamma_1, x : \sigma \vdash M : \tau$ *, and* $\Gamma_2 \vdash N : \sigma$*, where* $\Gamma = \Gamma_1 \wedge \Gamma_2$.

Proof. Standard, by structural induction. □

Theorem 2.22 (Subject Expansion for $\lambda_{\oplus}$)**.** *If* $\Gamma \vdash \mathbb{M}' : \tau$ *and* $\mathbb{M} \longrightarrow \mathbb{M}'$ *then* $\Gamma \vdash \mathbb{M} : \tau$.

Proof. Standard, by structural induction. See App. B for details. □

2.3.2. *Well-formed Expressions (in* $\lambda^{\not\iota}_{\oplus}$*).*

Building upon the type system for $\lambda_{\oplus}$, we now define a type system for checking *well-formed* $\lambda^{\not\iota}_{\oplus}$-expressions. This approach enables us to admit expressions with a failing computational behavior, may it be due to the mismatch in the number of resources required and available, or be due to consumption of a failing behavior by another expression. Such definition relies on the *core context* which is the key to the well-formedness of failure terms: free variables that are result of weakening will disregarded in the typing of the failure term.

Definition 2.23 (Core Context)**.** Given a context Γ, the associated *core context* is defined as $\Gamma^\dagger = \{x : \pi \in \Gamma \mid \pi \neq \omega\}$.

Definition 2.24 (Well-formed $\lambda^{\not\iota}_{\oplus}$ expressions)**.** An expression $\mathbb{M}$ is *well-formed* if there exist Γ and τ such that $\Gamma \models \mathbb{M} : \tau$ is entailed via the rules in Fig. 4.

Below we give a brief description of the rules in Fig. 4. Essentially, they differ from the ones in Fig. 3, by allowing mismatches between the number of copies of a variable in a functional position and the number of components in a bag.

- **Rules** [F:wf-expr] **and** [F:wf-bag] derive that well-typed expressions and bags in $\lambda_{\oplus}$ are well-formed.
- **Rules** [F:abs]**,** [F:bag]**, and** [F:sum] are as in the type system for $\lambda_{\oplus}$, but extended to the system of well-formed expressions.
- **Rules** [F:ex-sub] **and** [F:app] differ from the similar typing rules as the size of the bags (as declared in their types) is no longer required to match the number of occurrences of the variable assignment in the typing context ([F : ex-sub]), or the type of the term in the functional position ([F : app]).
- **Rule** [F:fail] has no analogue in the type system: we allow $\mathtt{fail}^{\widetilde{x}}$ to be well-formed with any strict type, provided that the core context contains the types of the variables in $\widetilde{x}$ (i.e., none of the variables in $\widetilde{x}$ is typed with ω).

Clearly, the set of well-typed expressions is strictly included in the set of well-formed expressions. Take, e.g., $M = x\langle\!\langle \wr N_1, N_2 \wr / x \rangle\!\rangle$, where both N_1 and N_2 are well-typed. It is easy to see that M is well-formed. However, M is not well-typed.

Example 2.25 (Cont. Example 2.18)**.** We explore the well-formedness of some of the terms motivated in previous examples:

(1) Term $M_1 = (\lambda x.x)\wr y \wr$ is well-typed and also well-formed, as we have:

$$[\mathtt{F} : \mathtt{wf\text{-}expr}]\ \frac{y : \sigma \vdash (\lambda x.x)\wr y \wr : \sigma}{y : \sigma \models (\lambda x.x)\wr y \wr : \sigma}$$

(2) We saw that term $M_2 = (\lambda x.x)(\wr y, z \wr)$ is not typable; however, it is well-formed:

$$\dfrac{[\mathtt{F} : \mathtt{wf\text{-}expr}]\ \dfrac{\vdash \lambda x.x : \sigma^1 \to \sigma}{\models \lambda x.x : \sigma^1 \to \sigma} \quad [\mathtt{F} : \mathtt{wf\text{-}bag}]\ \dfrac{y : \sigma, z : \sigma \vdash \wr y, z \wr : \sigma^2}{y : \sigma, z : \sigma \models \wr y, z \wr : \sigma^2} \qquad 1, 2 \geq 0}{y : \sigma, z : \sigma \models (\lambda x.x)(\wr y, z \wr) : \sigma}\ [\mathtt{F} : \mathtt{app}]$$

Notice that both $\vdash \lambda x.x : \sigma^1 \to \sigma$ and $\Gamma \vdash \wr y, z \wr : \sigma^2$ are well-typed.

(3) Similarly, the term $M_3 = (\lambda x.x)\mathtt{1}$ is also well-formed. The corresponding derivation is as above, but uses an empty context as well as the well-formedness rule for bags:

$$[\mathtt{F} : \mathtt{wf\text{-}bag}]\ \frac{\vdash \mathtt{1} : \sigma^0}{\models \mathtt{1} : \sigma^0}$$

Notice how $\sigma^0 = \omega$ and that $\models \mathtt{1} : \omega$.

(4) Term $M_4 = (\lambda x.y)\mathtt{1}$ is well-typed and also well-formed.

(5) Interestingly, term $M_5 = \mathtt{fail}^{\emptyset}$ is well-formed as:

$$[\mathtt{F} : \mathtt{fail}]\ \frac{}{\models \mathtt{fail}^{\emptyset} : \tau}$$

Example 2.26. Let us consider an expression that is not well-formed:

$$\lambda x.x\wr \lambda y.y,\ \ \lambda z.z_1\wr z_1\wr z_2 \wr\wr.$$

Notice that $\lambda x.x$ is applied to bags of two different types:

- The first bag containing $\lambda y.y$ is well-typed, thus well-formed. Consider the derivation Π_1:

$$\dfrac{\dfrac{\dfrac{}{y:\sigma \vdash y:\sigma}[\mathtt{T}:\mathtt{var}]}{\vdash \lambda y.y:\sigma\to\sigma}[\mathtt{T}:\mathtt{abs}] \qquad \dfrac{}{\vdash \mathtt{1}:\omega}[\mathtt{T}:\mathtt{1}]}{\vdash \wr \lambda y.y \wr \cdot \mathtt{1}:\sigma\to\sigma}[\mathtt{T}:\mathtt{bag}]}{\models \wr \lambda y.y \wr \cdot \mathtt{1}:\sigma\to\sigma}[\mathtt{F}:\mathtt{wf\text{-}bag}]$$

In the rest of the example we will omit the labels of rule applications, and concatenations with the empty bag $\mathtt{1}$ (i.e., $\wr \lambda y.y \wr \cdot \mathtt{1}$ will be written simply as $\wr \lambda y.y \wr$) and corresponding sub-derivations consisting of applications of Rule $[\mathtt{T}:\mathtt{1}]$.

- The second bag contains $\lambda z.z_1 \wr z_1 \wr z_2 \wr \wr$ contains an abstraction that acts as a weakening as z does not appear within $z_1 \wr z_1 \wr z_2 \wr \wr$. Consider the derivation Π_2:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{z_1:\sigma\to\sigma\vdash z_1:\sigma\to\sigma} \quad \dfrac{\dfrac{\dfrac{}{z_2:\sigma\vdash z_2:\sigma}}{z_2:\sigma\vdash \wr z_2 \wr:\sigma}}{z_1:\sigma\to\sigma, z_2:\sigma\vdash z_1 \wr z_2 \wr:\sigma}}{z_1:\sigma\to\sigma, z_2:\sigma\vdash \wr z_1 \wr z_2 \wr \wr:\sigma}}{z_1:\sigma\to\sigma\wedge\sigma\to\sigma, z_2:\sigma\vdash z_1 \wr z_1 \wr z_2 \wr \wr:\sigma}}{z_1:\sigma\to\sigma\wedge\sigma\to\sigma, z_2:\sigma, z:\omega\vdash z_1 \wr z_1 \wr z_2 \wr \wr:\sigma}}{z_1:\sigma\to\sigma\wedge\sigma\to\sigma, z_2:\sigma\vdash \lambda z.z_1 \wr z_1 \wr z_2 \wr \wr:\omega\to\sigma}}{\underbrace{z_1:\sigma\to\sigma\wedge\sigma\to\sigma, z_2:\sigma}_{\Gamma}\models \wr \lambda z.z_1 \wr z_1 \wr z_2 \wr \wr \wr:\omega\to\sigma}$$

- The concatenation of these two bags is not well-formed since each component has a different type: $\sigma\to\sigma$ and $\omega\to\sigma$. Therefore, $\lambda x.x \wr\ \lambda y.y\ ,\ \lambda z.z_1 \wr z_1 \wr z_2 \wr \wr\ \wr$ is not well-formed.

Notice that if we change $\lambda y.y$ to $\lambda y.y_1$ in the first bag, we would have a derivation Π_1' for $y_1:\sigma\models\lambda y.y_1:\omega\to\sigma$. This would allow us to concatenate the bags with derivation Π_3:

$$\dfrac{\Pi_1' \qquad \dfrac{\Pi_2 \qquad \dfrac{}{\mathtt{1}:\omega}}{\Gamma\models\lambda z.z_1 \wr z_1 \wr z_2 \wr \wr:\omega\to\sigma}}{y_1:\sigma\models\lambda y.y_1:\omega\to\sigma \qquad \Gamma\models \wr \lambda z.z_1 \wr z_1 \wr z_2 \wr \wr \wr\cdot\mathtt{1}:\omega\to\sigma}$$
$$\Gamma, y_1:\sigma\models \wr \lambda y.y_1 \wr \cdot \wr \lambda z.z_1 \wr z_1 \wr z_2 \wr \wr \wr\cdot\mathtt{1}:(\omega\to\sigma)^2$$

Thus, the whole term becomes well-formed:

$$\dfrac{\dfrac{\dfrac{x:\omega\to\sigma\vdash x:\omega\to\sigma}{\vdash\lambda x.x:(\omega\to\sigma)\to\omega\to\sigma}}{\models\lambda x.x:(\omega\to\sigma)\to\omega\to\sigma} \qquad \Gamma, y_1:\sigma\models \wr\ \lambda y.y_1\ ,\ \lambda z.z_1 \wr z_1 \wr z_2 \wr \wr\ \wr:(\omega\to\sigma)^2}{\Gamma, y_1:\sigma\models\lambda x.x \wr\ \lambda y.y_1\ ,\ \lambda z.z_1 \wr z_1 \wr z_2 \wr \wr\ \wr:\omega\to\sigma}$$

Well-formedness rules satisfy subject reduction with respect to the rules in Fig. 2 and relies on the linear substitution lemma for $\lambda^{\wr}_{\oplus}$:

Lemma 2.27 (Substitution Lemma for $\lambda^{\wr}_{\oplus}$)**.** *If* $\Gamma, x:\sigma^k\models M:\tau$ *(with* $k\geq 1$*),* $\mathsf{head}(M)=x$*, and* $\Delta\models N:\sigma$ *then* $\Gamma\wedge\Delta, x:\sigma^{k-1}\models M\{\!\{N/x\}\!\}$.

We now show subject reduction on well formed expressions in $\lambda^{\wr}_{\oplus}$. We use our results of subject reduction for well-typed $\lambda_{\oplus}$ (Theorem 2.20) and extend them to $\lambda^{\wr}_{\oplus}$.

Theorem 2.28 (Subject Reduction in $\lambda^{\wr}_{\oplus}$)**.** *If* $\Gamma\models\mathbb{M}:\tau$ *and* $\mathbb{M}\longrightarrow\mathbb{M}'$ *then* $\Gamma\models\mathbb{M}':\tau$.

Proof (Sketch). By structural induction on the reduction rules. See App. A for details. □

Differently from $\lambda_{\oplus}$, subject expansion fails for $\lambda^{\not{t}}_{\oplus}$. This is due to the possibility of failure in the use of resources. In $\lambda_{\oplus}$, if a resource is substituted within a term it is always done once, hence the term substituted must always be well-typed; however, in reductions that lead to the failure term, resources within a bag may be discarded before ever being substituted and hence, there is no requirement to be well-formed. Formally, we have:

Theorem 2.29 (Failure of Subject Expansion in $\lambda^{\not{t}}_{\oplus}$)**.** *If* $\Gamma \models \mathbb{M}' : \tau$ *and* $\mathbb{M} \longrightarrow \mathbb{M}'$ *then it is not necessarily the case that* $\Gamma \models \mathbb{M} : \tau$.

Proof. A counter-example suffices here. Consider the term $\mathtt{fail}^{\emptyset}$, which is well-formed but not well-typed, and let Ω^l be the term $(\lambda x.x\{\!|x|\!\})\{\!|\lambda x.x\{\!|x|\!\}\!\}$. Notice that $\text{-} \models \mathtt{fail}^{\emptyset} : \tau$ and $\mathtt{fail}^{x}\langle\!\langle \{\!|\Omega^l|\!\}/x \rangle\!\rangle \longrightarrow \mathtt{fail}^{\emptyset}$, but $\mathtt{fail}^{x}\langle\!\langle \{\!|\Omega^l|\!\}/x \rangle\!\rangle$ is not well-formed (nor well-typed) . □

3. $\widehat{\lambda}^{\not{t}}_{\oplus}$: A Resource Calculus With Sharing

We define $\widehat{\lambda}^{\not{t}}_{\oplus}$, a variant of $\lambda^{\not{t}}_{\oplus}$ with a sharing construct, which we adopt following the atomic λ-calculus in [GHP13]. In $\widehat{\lambda}^{\not{t}}_{\oplus}$, a variable is only allowed to appear once in a term: multiple occurrences of the same variable are atomized, i.e., they are given new different variable names. The "atomization" of variable occurrences realized in $\widehat{\lambda}^{\not{t}}_{\oplus}$ via sharing will turn out to be very convenient to define our encoding into $\mathtt{s}\pi$.

Our language $\widehat{\lambda}^{\not{t}}_{\oplus}$, defined in § 3.1, includes also a form of explicit substitution, called *explicit linear substitution*, which enables a refined analysis of the consumption of linear resources. Later, in § 3.2, we introduce the reduction semantics that implements a lazy evaluation. In § 3.3, we present a non-idempotent intersection type system to control the use of resources. Finally, in § 3.4 we give an encoding from $\lambda^{\not{t}}_{\oplus}$ into $\widehat{\lambda}^{\not{t}}_{\oplus}$, denoted $(\!|\cdot|\!)^{\circ}$, whose correctness is established in § 5.

3.1. Syntax.

The syntax of $\widehat{\lambda}^{\not{t}}_{\oplus}$ only modifies the syntax of $\lambda^{\not{t}}_{\oplus}$-terms, which is defined by the grammar below; the syntax of bags B and expressions $\mathbb{M}$ is as in Def. 2.1.

$$\begin{array}{rl} \text{(Terms)} & M, N, L ::= x \mid \lambda x.(M[\widetilde{x} \leftarrow x]) \mid (M\ B) \mid M\langle\!|N/x|\!\rangle \mid \mathtt{fail}^{\widetilde{x}} \\ & \qquad \mid M[\widetilde{x} \leftarrow x] \mid (M[\widetilde{x} \leftarrow x])\langle\!\langle B/x \rangle\!\rangle \end{array}$$

Distinctive aspects are the *sharing construct* $M[\widetilde{x} \leftarrow x]$ and the *explicit linear substitution* $M\langle\!|N/x|\!\rangle$. The term $M[\widetilde{x} \leftarrow x]$ defines the sharing of variables $\widetilde{x}$ occurring in M using x. We shall refer to x as *sharing variable* and to $\widetilde{x}$ as *shared variables*. Notice that $\widetilde{x}$ can be empty: $M[\leftarrow x]$ expresses that x does not share any variables in M. The sharing construct $M[\widetilde{x} \leftarrow x]$ binds the variables in $\widetilde{x}$; the occurrence of x_i can appear within the fail term $\mathtt{fail}^{\widetilde{y}}$, if $x_i \in \widetilde{y}$. In the explicit linear substitution $M\langle\!|N/x|\!\rangle$ binds x in M. As in $\lambda^{\not{t}}_{\oplus}$, the term $\mathtt{fail}^{\widetilde{x}}$ explicitly accounts for failed attempts at substituting the variables $\widetilde{x}$, due to an excess or lack of resources. A variable that is not explicitly sharing/shared is called *independent*.

Example 3.1. The following are examples of $\widehat{\lambda}^{\not{t}}_{\oplus}$-terms.

- (Shared identity) $\hat{\mathbf{I}} = \lambda x.x_1[x_1 \leftarrow x]$

- (Independent variables) An independent variable x applied to a 1-component bag (another independent variable): $x\wr x_1 \wr$
- $\hat{\mathbf{I}}$ applied to a 1-component bag: $\hat{\mathbf{I}}\wr y_1 \wr[y_1 \leftarrow y]$
- $\hat{\mathbf{I}}$ applied to a 2-component bag: $\hat{\mathbf{I}}(\wr y_1, y_2 \wr)[y_1, y_2 \leftarrow y]$
- Shared vacuous abstraction: $(\lambda y.x_1\wr x_2 \wr[\leftarrow y])[x_1, x_2 \leftarrow x]$
- $\hat{\mathbf{I}}$ applied to a bag containing an explicit substitution of a failure term that does not share the variable y: $\hat{\mathbf{I}}\wr \mathtt{fail}^{\emptyset}[\leftarrow y]\langle\!\langle \wr N \wr / y \rangle\!\rangle \wr$
- An abstraction on x of two shared occurrences of x: $\hat{D} = \lambda x.x_1\wr x_2 \wr[x_1, x_2 \leftarrow x]$

The syntax of terms is subject to some natural conditions on variable occurrences and on the structure of the sharing construct and the explicit linear substitution. We formalize these conditions as *consistency*, defined as follows:

Definition 3.2 (Consistent Terms, Bags, and Expressions)**.** We say that the expression $\mathbb{M}$ is *consistent* if each subterm M_0 of $\mathbb{M}$ satisfies the following conditions:

(1) If $M_0 = M[\widetilde{x} \leftarrow x]$ then: (i) $\widetilde{x}$ contains pairwise distinct variables; (ii) every $x_i \in \widetilde{x}$ must occur exactly once in M; (iii) x_i is not a sharing variable; (iv) M is consistent.
(2) If $M_0 = M\langle\!|N/x|\!\rangle$ then: (i) the variable x must occur exactly once in M; (ii) x cannot be a sharing variable; (iii) M and N are consistent; (iv) $\mathsf{fv}(M) \cap \mathsf{fv}(N) = \emptyset$.
(3) Otherwise, for other forms of M_0, variables must occur exactly once, i.e.,:
   - If $M_0 = \lambda x.(M[\widetilde{x} \leftarrow x])$ then: $x \notin \mathsf{fv}(M)$; $\widetilde{x}$ contains pairwise distinct variables; every $x_i \in \widetilde{x}$ must occur exactly once in M and is not a sharing variable; M is consistent.
   - If $M_0 = (M\ B)$ then $\mathsf{fv}(M) \cap \mathsf{fv}(B) = \emptyset$ and M and B are consistent.
   - If $M_0 = \mathtt{fail}^{\widetilde{x}}$ then $\widetilde{x}$ contains pairwise distinct variables.
   - If $M_0 = (M[\widetilde{x} \leftarrow x])\langle\!\langle B/x \rangle\!\rangle$ then: $x \notin \mathsf{fv}(M)$; $\widetilde{x}$ contains pairwise distinct variables; every $x_i \in \widetilde{x}$ must occur exactly once in M and is not a sharing variable; $\mathsf{fv}(M) \cap \mathsf{fv}(B) = \emptyset$; and M and B are consistent.

Consistency extends to bags as follows. The bag $\mathtt{1}$ is always consistent. The bag $\wr M \wr$ is consistent if M is consistent. The bag $A \cdot B$ is consistent if (i) A and B are consistent and (ii) $\mathsf{fv}(A) \cap \mathsf{fv}(B) = \emptyset$.

We now discuss the consistency conditions for the sharing construct $M[\widetilde{x} \leftarrow x]$. Condition 1(ii) enforces that variables cannot have more than one linear occurrence in the subject of a sharing construct: this condition rules out terms such as $x_1\wr x_1\wr y\wr\wr[x_1 \leftarrow x]$. Condition 1(iii), which rules out terms of the form $x_1\wr x_2\wr x_3\wr y\wr\wr\wr[x_1, x_2 \leftarrow x'][x', x_3 \leftarrow x]$, is for convenience: by requiring that sharing occurrences appear at the top level in bindings, we can easily deduce the number of occurrences of a variable by measuring the size of $\widetilde{x}$ in $[\widetilde{x} \leftarrow x]$, rather than inductively having to measure the occurrences of each $x' \in \widetilde{x}$ in multiple sharing constructs.

Conditions on the explicit linear substitution $M\langle\!|N/x|\!\rangle$ formalize our design choice: an explicit linear substitution is defined when the number of variables to be substituted coincides with the number of available resources. In particular, Condition 2(i) rules out terms of the form $y\langle\!|M/x|\!\rangle$, where an explicit linear substitution has no variable to perform a substitution. Condition 2(ii) rules out terms such as $M[x_1, x_2 \leftarrow x]\langle\!|M/x|\!\rangle$, in which a term is to be linearly substituted for a single variable x; however, as the variable is shared twice within M, there are less available terms to be substituted than it is necessary.

Finally, Condition 3 enforces that each variable occurs only once in a consistent term, and also that in $\mathtt{fail}^{\widetilde{x}}$, the $\widetilde{x}$ denotes a set of variables (rather than a multiset), as variables

can appear at most once within consistent terms. Thus, consistent terms also excludes terms such as $\mathtt{fail}^{x,x}$.

In what follows, we shall be working with consistent terms only, which we will call simply terms in our definitions and results. As we will see, consistency will be preserved by reduction (Theorem 3.15) and ensured by typing (Theorem 3.24) and a structural congruence on terms (Theorem 5.26).

3.2. **Reduction Semantics.**

Similarly to $\lambda^{\lightning}_{\oplus}$, the reduction semantics of $\widehat{\lambda}^{\lightning}_{\oplus}$ is given by a relation $\longrightarrow$, defined by the rules in Fig. 5; it consists of an extension of reductions in $\lambda^{\lightning}_{\oplus}$ that deals with the sharing construct $[\cdot \leftarrow \cdot]$ and with the explicit linear substitution $\cdot\langle\!|\, \cdot \,/\, \cdot \,|\!\rangle$. In order to define the reduction rules formally, we require some auxiliary notions: the free variables of an expression/term, the head of a term, linear head substitution, and contexts.

Definition 3.3 (Free Variables)**.** The set of free variables of a term, bag and expressions in $\widehat{\lambda}^{\lightning}_{\oplus}$, is defined inductively as

$$\begin{array}{ll}
\mathsf{fv}(x) = \{x\} & \mathsf{fv}(\mathtt{fail}^{\widetilde{x}}) = \{\widetilde{x}\} \\
\mathsf{fv}(\wr M \wr) = \mathsf{fv}(M) & \mathsf{fv}(B_1 \cdot B_2) = \mathsf{fv}(B_1) \cup \mathsf{fv}(B_2) \\
\mathsf{fv}(M\ B) = \mathsf{fv}(M) \cup \mathsf{fv}(B) & \mathsf{fv}(\mathtt{1}) = \emptyset \\
\mathsf{fv}(M\langle\!|N/x|\!\rangle) = (\mathsf{fv}(M) \setminus \{x\}) \cup \mathsf{fv}(N) & \mathsf{fv}(M[\widetilde{x} \leftarrow x]) = (\mathsf{fv}(M) \setminus \{\widetilde{x}\}) \cup \{x\} \\
\mathsf{fv}(\lambda x.(M[\widetilde{x} \leftarrow x])) = \mathsf{fv}(M[\widetilde{x} \leftarrow x]) \setminus \{x\} & \mathsf{fv}(\mathbb{M} + \mathbb{N}) = \mathsf{fv}(\mathbb{M}) \cup \mathsf{fv}(\mathbb{N}) \\
\multicolumn{2}{l}{\mathsf{fv}((M[\widetilde{x} \leftarrow x])\langle\!\langle B/x \rangle\!\rangle) = (\mathsf{fv}(M[\widetilde{x} \leftarrow x]) \setminus \{x\}) \cup \mathsf{fv}(B)}
\end{array}$$

As usual, a term M is *closed* if $\mathsf{fv}(M) = \emptyset$.

Definition 3.4 (Head)**.** The head of a term M, denoted $\mathsf{head}(M)$, is defined inductively:

$$\begin{array}{ll}
\mathsf{head}(x) = x & \mathsf{head}(\lambda x.(M[\widetilde{x} \leftarrow x])) = \lambda x.(M[\widetilde{x} \leftarrow x]) \\
\mathsf{head}(M\ B) = \mathsf{head}(M) & \mathsf{head}(M\langle\!|N/x|\!\rangle) = \mathsf{head}(M) \\
\mathsf{head}(\mathtt{fail}^{\widetilde{x}}) = \mathtt{fail}^{\widetilde{x}} &
\end{array}$$

$$\mathsf{head}(M[\widetilde{x} \leftarrow x]) = \begin{cases} x & \text{If } \mathsf{head}(M) = y \text{ and } y \in \widetilde{x} \\ \mathsf{head}(M) & \text{Otherwise} \end{cases}$$

$$\mathsf{head}((M[\widetilde{x} \leftarrow x])\langle\!\langle B/x \rangle\!\rangle) = \begin{cases} \mathtt{fail}^{\emptyset} & \text{If } |\widetilde{x}| \neq \mathsf{size}(B) \\ \mathsf{head}(M[\leftarrow x]) & \text{If } \widetilde{x} = \emptyset \text{ and } B = \mathtt{1} \\ (M[\widetilde{x} \leftarrow x])\langle\!\langle B/x \rangle\!\rangle & \text{Otherwise} \end{cases}$$

The most notable difference between $\mathsf{head}(\cdot)$ in $\lambda^{\lightning}_{\oplus}$ (cf. Definition 2.7) and in $\widehat{\lambda}^{\lightning}_{\oplus}$ concerns explicit substitution. Both definitions return $\mathtt{fail}^{\emptyset}$ in a mismatch of resources; in $\widehat{\lambda}^{\lightning}_{\oplus}$, the head term of an explicit substitution is only defined in the case of empty sharing (weakening). As we will see, this allows us to prioritize explicit substitution reductions over fetch reductions, as the head variable will block until an explicit substitution is separated into its linear component.

Definition 3.5 (Linear Head Substitution)**.** Given a term M with $\mathsf{head}(M) = x$, the linear substitution of a term N for x in M, written $M\{\!|N/x|\!\}$ is inductively defined as:

$$\begin{aligned}
x\{\!|N/x|\!\} &= N \\
(M\ B)\{\!|N/x|\!\} &= (M\{\!|N/x|\!\})\ B \\
(M\langle\!|L/y|\!\rangle)\{\!|N/x|\!\} &= (M\{\!|N/x|\!\})\ \langle\!|L/y|\!\rangle && x \neq y \\
((M[\widetilde{y} \leftarrow y])\langle\!\langle {}^{B}/_{y}\rangle\!\rangle)\{\!|N/x|\!\} &= (M[\widetilde{y} \leftarrow y]\{\!|N/x|\!\})\ \langle\!\langle {}^{B}/_{y}\rangle\!\rangle && x \neq y \\
(M[\widetilde{y} \leftarrow y])\{\!|N/x|\!\} &= (M\{\!|N/x|\!\})[\widetilde{y} \leftarrow y] && x \neq y
\end{aligned}$$

We now define contexts for terms and expressions in $\widehat{\lambda}^{\mathsf{lf}}_{\oplus}$. Term contexts involve an explicit linear substitution, rather than an explicit substitution: this is due to the reduction strategy we have chosen to adopt (cf. Rule [RS : Ex-Sub] in Fig. 5), as we always wish to evaluate explicit substitutions first. Expression contexts can be seen as sums with holes.

Definition 3.6 (Term and Expression Contexts in $\widehat{\lambda}^{\mathsf{lf}}_{\oplus}$)**.** Let $[\cdot]$ denote a hole. Contexts for terms and expressions are defined by the following grammar:

$$\begin{array}{lll}
\text{(Term Contexts)} & C[\cdot], C'[\cdot] & ::= ([\cdot])B \mid ([\cdot])\langle\!|N/x|\!\rangle \mid ([\cdot])[\widetilde{x} \leftarrow x] \mid ([\cdot])[\leftarrow x]\langle\!\langle {}^{1}/_{x}\rangle\!\rangle \\
\text{(Expression Contexts)} & D[\cdot], D'[\cdot] & ::= M + [\cdot] \mid [\cdot] + M
\end{array}$$

The substitution of a hole with a term M in a context $C[\cdot]$, denoted $C[M]$, must be a $\widehat{\lambda}^{\mathsf{lf}}_{\oplus}$-term.

We assume that the terms that fill in the holes respect consistency (i.e., variables appear in a term only once, shared variables must occur in the context).

Example 3.7. This example illustrates that certain contexts cannot be filled with certain terms. Consider the hole in context $C[\cdot] = ([\cdot])\langle\!|N/x|\!\rangle$.

- The hole cannot be filled with y, since $C[y] = y\langle\!|N/x|\!\rangle$ is not a consistent term. Indeed, $M\langle\!|N/x|\!\rangle$ requires that x occurs exactly once within M.
- Similarly, the hole cannot be filled with $\mathtt{fail}^{z}$ with $z \neq x$, since $C[\mathtt{fail}^{z}] = (\mathtt{fail}^{z})\langle\!|N/x|\!\rangle$ and x does not occur in the $\mathtt{fail}^{z}$, thus, the result is not a consistent term.

Now we are ready to describe the rules in Fig. 5. Intuitively, the lazy reduction relation $\longrightarrow$ on expressions works as follows: a β-reduction in $\widehat{\lambda}^{\mathsf{lf}}_{\oplus}$ results into an explicit substitution $M[\widetilde{x} \leftarrow x]\langle\!\langle {}^{B}/_{x}\rangle\!\rangle$, which then evolves, as an in intermediate step, to an expression consisting of explicit linear substitutions, which are the ones reducing to a linear head substitution $\{\!|N/x|\!\}$ (with $N \in B$) when the size of B coincides with the number of occurrences of x in M. The term reduces to failure when there is a mismatch between the size of B and the number of shared variables to be substituted. More in details, we have:

- **Rule** [RS:Beta] is standard and reduces to an explicit substitution.
- **Rule** [RS:Ex-Sub] applies when the size k of the bag coincides with the length of the list $\widetilde{x} = x_1, \ldots, x_k$. Intuitively, this rule "distributes" an explicit substitution into a sum of terms involving explicit linear substitutions; it considers all possible permutations of the elements in the bag among all shared variables.
- **Rule** [RS:Lin-Fetch] specifies the evaluation of a term with an explicit linear substitution into a linear head substitution.

We have three rules that reduce to the failure term—their objective is to accumulate all (free) variables involved in failed reductions. Accordingly:

$$[\texttt{RS:Beta}]\ \frac{}{(\lambda x.M[\widetilde{x} \leftarrow x])B \longrightarrow M[\widetilde{x} \leftarrow x]\langle\!\langle {}^{B}/_{x} \rangle\!\rangle}$$

$$[\texttt{RS:Ex-Sub}]\ \frac{B = \wr M_1 \int \cdots \wr M_k \int \qquad k \geq 1 \qquad M \neq \texttt{fail}^{\widetilde{y}}}{M[x_1, \ldots, x_k \leftarrow x]\langle\!\langle {}^{B}/_{x} \rangle\!\rangle \longrightarrow \sum_{B_i \in \mathsf{PER}(B)} M\langle\!| B_i(1)/x_1 |\!\rangle \cdots \langle\!| B_i(k)/x_k |\!\rangle}$$

$$[\texttt{RS:Lin-Fetch}]\ \frac{\mathsf{head}(M) = x}{M\langle\!| N/x |\!\rangle \longrightarrow M\{\!| N/x |\!\}}$$

$$[\texttt{RS:Fail}]\ \frac{k \neq \mathsf{size}(B) \quad \widetilde{y} = (\mathsf{fv}(M) \setminus \{x_1, \ldots, x_k\}) \cup \mathsf{fv}(B)}{M[x_1, \ldots, x_k \leftarrow x]\langle\!\langle {}^{B}/_{x} \rangle\!\rangle \longrightarrow \sum_{\mathsf{PER}(B)} \texttt{fail}^{\widetilde{y}}}$$

$$[\texttt{RS:Cons}_1]\ \frac{\widetilde{y} = \mathsf{fv}(B)}{\texttt{fail}^{\widetilde{x}} B \longrightarrow \sum_{\mathsf{PER}(B)} \texttt{fail}^{\widetilde{x} \cup \widetilde{y}}}\ [\texttt{RS:Cons}_2]\ \frac{\mathsf{size}(B) = k \quad k + |\widetilde{x}| \neq 0 \quad \widetilde{z} = \mathsf{fv}(B)}{(\texttt{fail}^{\widetilde{x} \cup \widetilde{y}}[\widetilde{x} \leftarrow x])\langle\!\langle {}^{B}/_{x} \rangle\!\rangle \longrightarrow \sum_{\mathsf{PER}(B)} \texttt{fail}^{\widetilde{y} \cup \widetilde{z}}}$$

$$[\texttt{RS:Cons}_3]\ \frac{\widetilde{z} = \mathsf{fv}(N)}{\texttt{fail}^{\widetilde{y} \cup x}\langle\!| N/x |\!\rangle \longrightarrow \texttt{fail}^{\widetilde{y} \cup \widetilde{z}}}$$

$$[\texttt{RS:TCont}]\ \frac{M \longrightarrow M'_1 + \cdots + M'_k}{C[M] \longrightarrow C[M'_1] + \cdots + C[M'_k]} \qquad [\texttt{RS:ECont}]\ \frac{\mathbb{M} \longrightarrow \mathbb{M}'}{D[\mathbb{M}] \longrightarrow D[\mathbb{M}']}$$

Figure 5: Reduction Rules for $\widehat{\lambda}^{\lightning}_{\oplus}$.

- **Rule** [RS:Fail] formalizes failure in the evaluation of an explicit substitution $M[\widetilde{x} \leftarrow x]\langle\!\langle {}^{B}/_{x} \rangle\!\rangle$, which occurs if there is a mismatch between the resources (terms) present in B and the number of occurrences of x to be substituted. The resulting failure term preserves all free variables in M and B within its attached set $\widetilde{y}$.
- **Rules** [RS:Cons$_1$] **and** [RS:Cons$_2$] describe reductions that lazily consume the failure term, when a term has $\texttt{fail}^{\widetilde{x}}$ at its head position. The former rule consumes bags attached to it whilst preserving all its free variables.
- **Rule** [RS:Cons$_3$] accumulates into the failure term the free variables involved in an explicit linear substitution.

The contextual Rules [RS:TCont] and [RS:Econt] are standard.

Example 3.8. We show how a term can reduce using Rule [RS:Cons$_2$].

$$\begin{aligned}
(\lambda x.x_1[x_1 \leftarrow x])\wr \texttt{fail}^{\emptyset}[\leftarrow y]\langle\!\langle \wr N \int /_{y} \rangle\!\rangle \int &\longrightarrow_{[\texttt{RS:Beta}]} x_1[x_1 \leftarrow x]\langle\!\langle \wr \texttt{fail}^{\emptyset}[\leftarrow y]\langle\!\langle \wr N \int /_{y} \rangle\!\rangle \int /_{x} \rangle\!\rangle \\
&\longrightarrow_{[\texttt{RS:Ex-Sub}]} x_1\langle\!| \texttt{fail}^{\emptyset}[\leftarrow y]\langle\!\langle \wr N \int /_{y} \rangle\!\rangle /_{x_1} |\!\rangle \\
&\longrightarrow_{[\texttt{RS:Lin-Fetch}]} \texttt{fail}^{\emptyset}[\leftarrow y]\langle\!\langle \wr N \int /_{y} \rangle\!\rangle \\
&\longrightarrow_{[\texttt{RS:Cons}_2]} \texttt{fail}^{\mathsf{fv}(N)}
\end{aligned}$$

Example 3.9. We illustrate how Rule [RS:Fail] can introduce $\mathtt{fail}^{\widetilde{x}}$ into a term. It also shows how Rule [$\mathtt{RS:Cons_3}$] consumes an explicit linear substitution:

$$\begin{aligned} x_1[\leftarrow y]\langle\!\langle (N)/y\rangle\!\rangle[x_1 \leftarrow x]\langle\!\langle (M)/x\rangle\!\rangle &\longrightarrow_{\texttt{[RS:Ex-Sub]}} x_1[\leftarrow y]\langle\!\langle (N)/y\rangle\!\rangle\langle\!|M/x_1|\!\rangle \\ &\longrightarrow_{\texttt{[RS:Fail]}} \mathtt{fail}^{\{x_1\}\cup \mathsf{fv}(N)}\langle\!|M/x_1|\!\rangle \\ &\longrightarrow_{\texttt{[RS:Cons}_3\texttt{]}} \mathtt{fail}^{\mathsf{fv}(M)\cup\mathsf{fv}(N)} \end{aligned}$$

Similarly to $\lambda^{\lightning}_{\oplus}$, reduction in $\widehat{\lambda}^{\lightning}_{\oplus}$ satisfies a *diamond property*. Therefore, we have the analogue of Proposition 2.13:

Proposition 3.10 (Diamond Property for $\widehat{\lambda}^{\lightning}_{\oplus}$)**.** *For all* $\mathbb{N}$, $\mathbb{N}_1$, $\mathbb{N}_2$ *in* $\widehat{\lambda}^{\lightning}_{\oplus}$ *s.t.* $\mathbb{N} \longrightarrow \mathbb{N}_1$, $\mathbb{N} \longrightarrow \mathbb{N}_2$ *with* $\mathbb{N}_1 \neq \mathbb{N}_2$ *then there exists* $\mathbb{M}$ *such that* $\mathbb{N}_1 \longrightarrow \mathbb{M}$ *and* $\mathbb{N}_2 \longrightarrow \mathbb{M}$.

Proof. The thesis follows as in $\lambda^{\lightning}_{\oplus}$ since the left-hand sides of the reduction rules in $\widehat{\lambda}^{\lightning}_{\oplus}$ do not interfere with each other. □

Remark 3.11 (A Calculus with Sharing but Without Failure ($\widehat{\lambda}_{\oplus}$))**.** As we did in Remark 2.14, we define a sub-calculus of $\widehat{\lambda}^{\lightning}_{\oplus}$ in which failure is not explicit. The calculus $\widehat{\lambda}_{\oplus}$ is obtained from the syntax of $\widehat{\lambda}^{\lightning}_{\oplus}$ by disallowing the term $\mathtt{fail}^{\widetilde{x}}$. The relevant reduction rules from Fig. 5 are [$\mathtt{RS:Beta}$], [RS:Ex-Sub], [RS:Lin-Fetch], and the two contextual rules. We keep Def. 3.4 unchanged with the provision that $\mathsf{head}(M\langle\!\langle B/x\rangle\!\rangle)$ is undefined when $|\widetilde{x}| \neq \mathsf{size}(B)$.

3.3. Non-Idempotent Intersection Types.

Similarly to $\lambda^{\lightning}_{\oplus}$, we now define *well-formed* $\widehat{\lambda}^{\lightning}_{\oplus}$ expressions and a system of rules for checking well-formedness by modifying the rules in Fig. 4. The grammar of strict and multiset types, the notions of typing assignments, and judgements are the same as in Section 2.3. We need an extension to the notion of typing context: whereas in $\lambda^{\lightning}_{\oplus}$ variables were only assigned to multiset types, now sharing variables are assigned to multiset types, shared and independent variables are assigned to strict types.

Definition 3.12. We extend the definition of typing contexts (Def. 2.16) as follows:

$$\Gamma, \Delta = \text{-} \mid \Gamma, x : \pi \mid \Gamma, x : \sigma$$

The definition of core contexts is extended accordingly, and also denoted as $\Gamma^{\dagger}$.

The presentation is in two phases:

(1) We consider the intersection type system given in Fig. 6 for which we consider the sub-calculus $\widehat{\lambda}_{\oplus}$, the sharing calculus excluding failure (cf. Rem. 3.11).
(2) We define well-formed expressions for the full language $\widehat{\lambda}^{\lightning}_{\oplus}$, via Def. 3.19 (see below).

To avoid ambiguities, we write $x : \sigma^1$ to make it explicit that the type assignment involves an intersection type (and a sharing variable), rather than a strict type.

3.3.1. *Well-typed Expressions (in $\widehat{\lambda}_{\oplus}$).*

The typing rules in Fig. 6 are essentially the same as the ones in Fig. 3, but now taking into account the sharing construct $M[\widetilde{x} \leftarrow x]$ and the explicit linear substitution. We discuss selected rules:

- **Rules** [TS:var], [TS:1], [TS:bag], [TS:app], **and** [TS:sum] are the same as in Fig. 3, considering sharing within the terms and bags.
- **Rule** [TS:weak] deals with $k = 0$, typing the term $M[\leftarrow x]$, when there are no occurrences of x in M, as long as M is typable.
- **Rule** [TS:abs-sh] is as expected: it requires that the sharing variable is assigned the k-fold intersection type σ^k.
- **Rule** [TS:ex-lin-sub] supports explicit linear substitutions and consumes one occurrence of $x : \sigma$ from the context.
- **Rule** [TS:ex-sub] types explicit substitutions where a bag must consist of both the same type and length of the shared variable it is being substituted for.
- **Rule** [TS:share] requires that the shared variables $x_1, \ldots, x_k$ have the same type as the sharing variable x, for $k \neq 0$. This rule justifies the need for the extension of contexts with assignments of the form $x : \sigma$. This way, e.g., Example 3.14 below gives an application of Rule [TS : share] with $k = 1$).

Definition 3.13 (Well-typed Expressions)**.** An expression $\mathbb{M} \in \widehat{\lambda}^{\wr}_{\oplus}$ is *well-typed* (or typable) if there exist Γ and τ such that $\Gamma \vdash \mathbb{M} : \tau$ is entailed via the rules in Fig. 6.

Again, the failure term `fail` in $\widehat{\lambda}^{\wr}_{\oplus}$ is not typable via this typing system. The following examples illustrate the typing rules.

Example 3.14. The term $((\lambda x.x_1[x_1 \leftarrow x])\wr y_1 \wr)[y_1 \leftarrow y]$ is well-typed, as follows:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{x_1 : \sigma \vdash x_1 : \sigma}\,[\texttt{TS:var}]}{x : \sigma^1 \vdash x_1[x_1 \leftarrow x] : \sigma}\,[\texttt{TS:share}]}{\vdash \lambda x.x_1[x_1 \leftarrow x] : \sigma^1 \to \sigma}\,[\texttt{TS:abs-sh}] \quad \dfrac{\dfrac{}{y_1 : \sigma \vdash y_1 : \sigma}\,[\texttt{TS:var}] \quad \dfrac{}{\vdash 1 : \omega}\,[\texttt{TS:1}]}{y_1 : \sigma \vdash \wr y_1 \wr \cdot 1 : \sigma^1}\,[\texttt{TS:bag}]}{y_1 : \sigma \vdash ((\lambda x.x_1[x_1 \leftarrow x])\wr y_1 \wr) : \sigma}\,[\texttt{TS:app-sh}]}{y : \sigma^1 \vdash ((\lambda x.x_1[x_1 \leftarrow x])\wr y_1 \wr)[y_1 \leftarrow y] : \sigma}\,[\texttt{TS:share}]$$

Theorem 3.15 (Consistency Stability Under $\longrightarrow$)**.** *If $\mathbb{M}$ is a consistent $\widehat{\lambda}^{\wr}_{\oplus}$-expression and $\mathbb{M} \longrightarrow \mathbb{M}'$ then $\mathbb{M}'$ is consistent.*

Proof. By structural induction, and analyzing the reduction rules applied in $\mathbb{M}$. See Appendix B for details. □

As expected, the typing system satisfies the subject reduction property w.r.t. the reduction relation given in Fig. 5, excluding rules for failure.

Theorem 3.16 (Subject Reduction in $\widehat{\lambda}_{\oplus}$)**.** *If $\Gamma \vdash \mathbb{M} : \tau$ and $\mathbb{M} \longrightarrow \mathbb{M}'$ then $\Gamma \vdash \mathbb{M}' : \tau$.*

Proof. Standard by induction on the rule applied in $\mathbb{M}$. □

Lemma 3.17 (Linear Anti-substitution Lemma for $\widehat{\lambda}_{\oplus}$)**.** *Let M and N be $\widehat{\lambda}_{\oplus}$-terms such that $\mathsf{head}(M) = x$. The following hold:*

- *If $\Gamma, x : \sigma^{k-1} \vdash M\{\!|N/x|\!\} : \tau$, with $k > 1$, then there exist Γ_1, Γ_2 such that $\Gamma_1, x : \sigma^k \vdash M : \tau$, and $\Gamma_2 \vdash N : \sigma$, where $\Gamma = \Gamma_1 \wedge \Gamma_2$.*

$$[\texttt{TS:var}]\ \frac{}{x:\sigma \vdash x:\sigma} \qquad [\texttt{TS:1}]\ \frac{}{\vdash \mathtt{1}:\omega} \qquad [\texttt{TS:weak}]\ \frac{\Delta \vdash M:\tau}{\Delta, x:\omega \vdash M[\leftarrow x]:\tau}$$

$$[\texttt{TS:abs-sh}]\ \frac{\Delta, x:\sigma^k \vdash M[\widetilde{x} \leftarrow x]:\tau}{\Delta \vdash \lambda x.(M[\widetilde{x} \leftarrow x]):\sigma^k \to \tau} \qquad [\texttt{TS:app}]\ \frac{\Gamma \vdash M:\pi \to \tau \qquad \Delta \vdash B:\pi}{\Gamma, \Delta \vdash M\ B:\tau}$$

$$[\texttt{TS:bag}]\ \frac{\Gamma \vdash M:\sigma \qquad \Delta \vdash B:\sigma^k}{\Gamma, \Delta \vdash \wr M \wr \cdot B:\sigma^{k+1}} \qquad [\texttt{TS:ex-lin-sub}]\ \frac{\Delta \vdash N:\sigma \qquad \Gamma, x:\sigma \vdash M:\tau}{\Gamma, \Delta \vdash M\langle\!|N/x|\!\rangle:\tau}$$

$$[\texttt{TS: ex-sub}]\ \frac{\Delta \vdash B:\sigma^k \qquad \Gamma, x:\sigma^k \vdash M[\widetilde{x} \leftarrow x]:\tau}{\Gamma, \Delta \vdash M[\widetilde{x} \leftarrow x]\langle\!\langle B/x \rangle\!\rangle:\tau} \qquad [\texttt{TS:sum}]\ \frac{\Gamma \vdash \mathbb{M}:\sigma \qquad \Gamma \vdash \mathbb{N}:\sigma}{\Gamma \vdash \mathbb{M}+\mathbb{N}:\sigma}$$

$$[\texttt{TS:share}]\ \frac{\Delta, x_1:\sigma, \cdots, x_k:\sigma \vdash M:\tau \quad x \notin \mathtt{dom}(\Delta) \quad k \neq 0}{\Delta, x:\sigma^k \vdash M[x_1, \cdots, x_k \leftarrow x]:\tau}$$

Figure 6: Typing Rules for $\widehat{\lambda}_{\oplus}$.

- *If* $\Gamma \vdash M\{\!|N/x|\!\}:\tau$*, with* $x \notin \mathtt{dom}(\Gamma)$*, then there exist* Γ_1, Γ_2 *such that* $\Gamma_1, x:\sigma \vdash M:\tau$ *, and* $\Gamma_2 \vdash N:\sigma$*, where* $\Gamma = \Gamma_1 \wedge \Gamma_2$*.*

Proof. By structural induction on the reduction rule from Fig. 6. See App. B for details. □

Theorem 3.18 (Subject Expansion for $\widehat{\lambda}_{\oplus}$)**.** *If* $\Gamma \vdash \mathbb{M}':\tau$ *and* $\mathbb{M} \longrightarrow \mathbb{M}'$ *then* $\Gamma \vdash \mathbb{M}:\tau$*.*

Proof. Standard, by induction on the reduction rule applied. See App. B for details. □

3.3.2. *Well-formed Expressions (in* $\widehat{\lambda}^{\lightning}_{\oplus}$*).*

On top of the intersection type system for $\widehat{\lambda}_{\oplus}$, we define well-formed expressions: $\widehat{\lambda}^{\lightning}_{\oplus}$-terms whose computation may lead to failure.

Definition 3.19 (Well-formedness in $\widehat{\lambda}^{\lightning}_{\oplus}$)**.** An expression $\mathbb{M}$ is well formed if there exist Γ and τ such that $\Gamma \models \mathbb{M}:\tau$ is entailed via the rules in Fig. 7.

Rules [FS:wf-expr] and [FS:wf-bag] guarantee that every well-typed expression and bag, respectively, is well-formed. Since our language is expressive enough to account for failing computations, we include rules for checking the structure of these ill-behaved terms—terms that can be well-formed, but not typable. For instance,

- **Rules** [FS:ex-sub] **and** [FS:app] differ from similar typing rules in Fig. 6: the size of the bags (as declared in their types) is no longer required to match.
- **Rule** [FS:fail] has no analogue in the type system: we allow the failure term $\mathtt{fail}^{\widetilde{x}}$ to be well-formed with any type, provided that the core context contains types for the variables in $\widetilde{x}$.

The other rules are similar to their corresponding ones in Fig. 4 and Fig. 6.

The following example illustrates a $\widehat{\lambda}^{\lightning}_{\oplus}$ expression that is well-formed but not well-typed.

Example 3.20 (Cont. Example 3.20)**.** The $\widehat{\lambda}^{\lightning}_{\oplus}$ expression consisting of an application of $\hat{I}$ to a bag containing a failure term $\lambda x.x_1[x_1 \leftarrow x])\wr \mathtt{fail}^{\emptyset}[\leftarrow y]\langle\!\langle \mathtt{1}/y \rangle\!\rangle \wr$ is well-formed with type σ. The derivation, with omitted rule labels, is the following:

$$[\texttt{FS:wf-expr}]\ \frac{\Gamma \vdash \mathbb{M} : \tau}{\Gamma \models \mathbb{M} : \tau} \qquad [\texttt{FS:wf-bag}]\ \frac{\Gamma \vdash B : \pi}{\Gamma \models B : \pi} \qquad [\texttt{FS:weak}]\ \frac{\Gamma \models M : \tau}{\Gamma, x : \omega \models M[\leftarrow x] : \tau}$$

$$[\texttt{FS:abs-sh}]\ \frac{\Gamma, x : \sigma^k \models M[\widetilde{x} \leftarrow x] : \tau \quad x \notin \texttt{dom}(\Gamma)}{\Gamma \models \lambda x.(M[\widetilde{x} \leftarrow x]) : \sigma^k \to \tau} \qquad [\texttt{FS:fail}]\ \frac{\texttt{dom}(\Gamma^\dagger) = \widetilde{x}}{\Gamma \models \texttt{fail}^{\widetilde{x}} : \tau}$$

$$[\texttt{FS:app}]\ \frac{\Gamma \models M : \sigma^j \to \tau \quad \Delta \models B : \sigma^k}{\Gamma, \Delta \models M\ B : \tau} \qquad [\texttt{FS:bag}]\ \frac{\Gamma \models M : \sigma \quad \Delta \models B : \sigma^k}{\Gamma, \Delta \models \wr M \wr \cdot B : \sigma^{k+1}}$$

$$[\texttt{FS:ex-lin-sub}]\ \frac{\Gamma, x : \sigma \models M : \tau \quad \Delta \models N : \sigma}{\Gamma, \Delta \models M\langle\!|N/x|\!\rangle : \tau} \qquad [\texttt{FS:sum}]\ \frac{\Gamma \models \mathbb{M} : \sigma \quad \Gamma \models \mathbb{N} : \sigma}{\Gamma \models \mathbb{M} + \mathbb{N} : \sigma}$$

$$[\texttt{FS:ex-sub}]\ \frac{\Gamma, x : \sigma^k \models M[\widetilde{x} \leftarrow x] : \tau \qquad \Delta \models B : \sigma^j}{\Gamma, \Delta \models M[\widetilde{x} \leftarrow x]\langle\!\langle B/x \rangle\!\rangle : \tau}$$

$$[\texttt{FS:share}]\ \frac{\Gamma, x_1 : \sigma, \cdots, x_k : \sigma \models M : \tau \quad x \notin \texttt{dom}(\Gamma) \quad k \neq 0}{\Gamma, x : \sigma^k \models M[x_1, \cdots, x_k \leftarrow x] : \tau}$$

Figure 7: Well-formedness Rules for $\widehat{\lambda}^{\wr}_{\oplus}$.

$$\dfrac{\dfrac{\dfrac{\dfrac{x_1 : \sigma \vdash x_1 : \sigma}{x_1 : \sigma \models x_1 : \sigma}}{x : \sigma^1 \models x_1[x_1 \leftarrow x] : \sigma}}{\models \lambda x.x_1[x_1 \leftarrow x] : \sigma \to \sigma} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\models \texttt{fail}^{\emptyset} : \sigma}}{y : \omega \models \texttt{fail}^{\emptyset}[\leftarrow y] : \sigma} \quad \dfrac{}{\vdash 1 : \omega}}{\models \texttt{fail}^{\emptyset}[\leftarrow y]\langle\!\langle 1/y \rangle\!\rangle : \sigma} \quad \dfrac{}{\vdash 1 : \omega}}{\models \wr \texttt{fail}^{\emptyset}[\leftarrow y]\langle\!\langle 1/y \rangle\!\rangle \wr : \sigma^1}}{\models \lambda x.x_1[x_1 \leftarrow x] \wr \texttt{fail}^{\emptyset}[\leftarrow y]\langle\!\langle 1/y \rangle\!\rangle \wr : \sigma}$$

Besides, we have $\lambda x.x_1[x_1 \leftarrow x])\wr \texttt{fail}^{\emptyset}[\leftarrow y]\langle\!\langle 1/y \rangle\!\rangle \wr \longrightarrow^* \texttt{fail}^{\emptyset}[\leftarrow y]\langle\!\langle 1/y \rangle\!\rangle$.

Well-formed $\widehat{\lambda}^{\wr}_{\oplus}$ expressions satisfy the subject reduction property; as usual, the proof relies on a linear substitution lemma for $\widehat{\lambda}^{\wr}_{\oplus}$.

Lemma 3.21 (Substitution Lemma for $\widehat{\lambda}^{\wr}_{\oplus}$)**.** *If* $\Gamma, x : \sigma \models M : \tau$, $\mathsf{head}(M) = x$, *and* $\Delta \models N : \sigma$ *then* $\Gamma, \Delta \models M\{\!|N/x|\!\} : \tau$.

Proof. By structural induction on M. See App. B for details. □

Theorem 3.22 (Subject Reduction in $\widehat{\lambda}^{\wr}_{\oplus}$)**.** *If* $\Gamma \models \mathbb{M} : \tau$ *and* $\mathbb{M} \longrightarrow \mathbb{M}'$ *then* $\Gamma \models \mathbb{M}' : \tau$.

Proof. By structural induction on the reduction rule from Fig. 5. See App. B for details. □

We close this part by stating the failure of subject expansion for well-formed expressions.

Theorem 3.23 (Failure of Subject Expansion in $\widehat{\lambda}^{\wr}_{\oplus}$)**.** *If* $\Gamma \models \mathbb{M}' : \tau$ *and* $\mathbb{M} \longrightarrow \mathbb{M}'$ *then it is not necessarily the case that* $\Gamma \models \mathbb{M} : \tau$.

Proof. We adapt the counter-example from the proof of Theorem 2.29. Consider the term $\texttt{fail}^{\emptyset}$, which is well-formed but not well-typed, and let Ω^l be the term $(\lambda x.x_1\wr x_2\wr[x_1, x_2 \leftarrow x])\wr \lambda x.x_1\wr x_2\wr[x_1, x_2 \leftarrow x]\wr$. Notice that $\texttt{fail}^{x_1}[x_1 \leftarrow x]\langle\!\langle \wr\Omega^l\wr/x \rangle\!\rangle \longrightarrow \texttt{fail}^{\emptyset}$ and $\text{-} \models \texttt{fail}^{\emptyset} : \tau$, but $\texttt{fail}^{x_1}[x_1 \leftarrow x]\langle\!\langle \wr\Omega^l\wr/x \rangle\!\rangle$ is not well-formed (nor well-typed). □

Theorem 3.24 (Consistency enforced by typing)**.** *Let* $\mathbb{M}$ *be a* $\widehat{\lambda}^{\lightning}_{\oplus}$*-expression. If* $\Gamma \models \mathbb{M}$ *then* $\mathbb{M}$ *is consistent.*

Proof. By induction on the type derivation. See Appendix B for details. □

Taking Stock. Up to here, we have presented our source language $\lambda^{\lightning}_{\oplus}$—a new resource lambda calculus with failure—and its fail-free sub-calculus $\lambda_{\oplus}$. Based on them we defined well-typed and well-formed expressions. Similarly, we defined the intermediate calculus $\widehat{\lambda}^{\lightning}_{\oplus}$ and its sub-calculus $\widehat{\lambda}_{\oplus}$. We now move on to define a translation of $\lambda^{\lightning}_{\oplus}$ into $\widehat{\lambda}^{\lightning}_{\oplus}$.

3.4. **From $\lambda^{\lightning}_{\oplus}$ into $\widehat{\lambda}^{\lightning}_{\oplus}$.** Borrowing inspiration from translations given in [GHP13] for the atomic λ-calculus, we now define a translation $(\!|\cdot|\!)^{\circ}$ from well-formed expressions in $\lambda^{\lightning}_{\oplus}$ into $\widehat{\lambda}^{\lightning}_{\oplus}$. It relies on an auxiliary translation $(\!|\cdot|\!)^{\bullet}$ on $\lambda^{\lightning}_{\oplus}$-terms, which depends on the notion of (simultaneous) linear substitution (Def. 3.25) which, intuitively, forces all bound variables in $\lambda^{\lightning}_{\oplus}$ to become shared variables in $\widehat{\lambda}^{\lightning}_{\oplus}$. The correctness of $(\!|\cdot|\!)^{\circ}$ will be addressed in § 5.2.

Definition 3.25 (Linear substitution)**.** Suppose given a $\lambda^{\lightning}_{\oplus}$-term M, a variable x, and a sequence of variables $\widetilde{w} = y, \widetilde{z}$. When $\#(x, M) = |\widetilde{w}|$ and $\{y\} \cap \widetilde{z} = \emptyset$, the *linear substitution* $M\langle y, \widetilde{z}/x\rangle$ of variable x for variables $\widetilde{w}$ in M is defined inductively as follows:

$$
\begin{aligned}
x\langle y/x\rangle &= y \\
(\lambda z.M)\langle y/x\rangle &= \lambda z.(M\langle y/x\rangle) \quad \text{if } x \in \mathsf{fv}(M) \\
(M\ B)\langle y/x\rangle &= \begin{cases} ((M\langle y/x\rangle)\ B) & \text{if } x \in \mathsf{fv}(M) \\ (M\ (B\langle y/x\rangle)) & \text{if } x \notin \mathsf{fv}(M), x \in \mathsf{fv}(B) \end{cases} \\
\mathtt{fail}^{\widetilde{z}}\langle y/x\rangle &= \mathtt{fail}^{\widetilde{z}',y} \quad \text{if } x \in \widetilde{z} \text{ and } \widetilde{z} = \widetilde{z}', x \\
(M\langle\!\langle {}^{B}/_{z}\rangle\!\rangle)\langle y/x\rangle &= \begin{cases} (M\langle y/x\rangle)\langle\!\langle {}^{B}/_{z}\rangle\!\rangle & \text{if } x \in \mathsf{fv}(M) \\ M\langle\!\langle {}^{B\langle y/x\rangle}/_{z}\rangle\!\rangle & \text{if } x \notin \mathsf{fv}(M), x \in \mathsf{fv}(B) \end{cases} \\
\mathtt{1}\langle y/x\rangle &= \text{undefined} \\
\wr M \int\langle y/x\rangle &= \wr M\langle y/x\rangle \int \quad \text{if } x \in \mathsf{fv}(M) \\
(A \cdot B)\langle y/x\rangle &= \begin{cases} ((A\langle y/x\rangle) \cdot B) & \text{if } x \in \mathsf{fv}(A) \\ (A \cdot (B\langle y/x\rangle)) & \text{if } x \notin \mathsf{fv}(A), x \in \mathsf{fv}(B) \end{cases} \\
M\langle y, \widetilde{z}/x\rangle &= (M\langle y/x\rangle)\langle \widetilde{z}/x\rangle
\end{aligned}
$$

Otherwise, in all other cases, the substitution is undefined. We write $M\langle z_1, z_2, \cdots, z_k/x\rangle$ to stand for $(\cdots((M\langle z_1/x\rangle)\langle z_2/x\rangle)\cdots\langle z_k/x\rangle)$.

Notice that for a $\lambda^{\lightning}_{\oplus}$-term with multiple occurrences of the variable to be substituted for, this linear substitution fixes an ordering of instantiation. For example, $\lambda x.y\wr y, x\int\langle z_1, z_2/y\rangle$ results in $\lambda x.z_1\wr z_2, x\int$, and a permutation of variables as in $\lambda x.z_2\wr z_1, x\int$ is not accounted for. This is not restrictive; actually it is enough for our purposes since this substitution will only be used in Def. 3.26 and the variables being substituted will be bound by sharing, and therefore could be α-renamed.

$$(\!|x|\!)^\bullet = x \qquad (\!|\mathbf{1}|\!)^\bullet = \mathbf{1} \qquad (\!|\mathtt{fail}^{\widetilde{x}}|\!)^\bullet = \mathtt{fail}^{\widetilde{x}}$$
$$(\!|M\ B|\!)^\bullet = (\!|M|\!)^\bullet\ (\!|B|\!)^\bullet \qquad (\!|\wr M \int \cdot B|\!)^\bullet = \wr (\!|M|\!)^\bullet \int \cdot (\!|B|\!)^\bullet$$
$$(\!|\lambda x.M|\!)^\bullet = \lambda x.((\!|M\langle \widetilde{y}/x\rangle|\!)^\bullet[\widetilde{y} \leftarrow x]) \quad \#(x,M) = n, \text{ each } y_i \in \widetilde{y} \text{ is fresh}$$
$$(\!|M\langle\!\langle B/x\rangle\!\rangle|\!)^\bullet = \begin{cases} \sum_{B_i \in \mathsf{PER}((\!|B|\!)^\bullet)} (\!|M\langle \widetilde{y}/x\rangle|\!)^\bullet \langle\!| B_i(1)/x_1 |\!\rangle \cdots \langle\!| B_i(k)/x_k |\!\rangle & \#(x,M) = \mathsf{size}(B) = k \geq 1 \\ (\!|M\langle y_1 . \cdots, y_k/x\rangle|\!)^\bullet[\widetilde{y} \leftarrow x]\langle\!\langle (\!|B|\!)^\bullet/x\rangle\!\rangle & \text{otherwise, } \#(x,M) = k \geq 0 \end{cases}$$

Figure 8: Auxiliary Translation: $\lambda^{\not t}_{\oplus}$ into $\widehat{\lambda}^{\not t}_{\oplus}$.

Definition 3.26 (From $\lambda^{\not t}_{\oplus}$ to $\widehat{\lambda}^{\not t}_{\oplus}$)**.** Let $M \in \lambda^{\not t}_{\oplus}$. Suppose $\Gamma \models M : \tau$, with $\mathtt{dom}(\Gamma) = \mathsf{fv}(M) = \{x_1, \cdots, x_k\}$ and $\#(x_i, M) = j_i$. We define $(\!|M|\!)^\circ$ as

$$(\!|M|\!)^\circ = (\!|M\langle \widetilde{y_1}/x_1\rangle \cdots \langle \widetilde{y_k}/x_k\rangle|\!)^\bullet[\widetilde{y_1} \leftarrow x_1] \cdots [\widetilde{y_k} \leftarrow x_k]$$

where $\widetilde{y_i} = y_{i_1}, \cdots, y_{i_{j_i}}$ and the translation $(\!|\cdot|\!)^\bullet : \lambda^{\not t}_{\oplus} \to \widehat{\lambda}^{\not t}_{\oplus}$ is defined in Fig. 8. The translation $(\!|\cdot|\!)^\circ$ extends homomorphically to expressions.

As already mentioned, the translation $(\!|\cdot|\!)^\circ$ "atomizes" occurrences of variables, in the spirit of [GHP13]: it converts n occurrences of a variable x in a term into n distinct variables $y_1, \ldots, y_n$. The sharing construct coordinates the occurrences of these variables by constraining each to occur exactly once within a term. We proceed in two stages:

(1) First, we use $(\!|\cdot|\!)^\circ$ to ensure that each free variable (say, y) is replaced by a shared variable (say, $y_i \in \widetilde{y}$), which is externally bound by the y in $[\widetilde{y} \leftarrow y]$.
(2) Second, we apply the auxiliary translation $(\!|\cdot|\!)^\bullet$ on the corresponding to the sharing of bound variables.

We now describe the two cases of Fig. 8 that are noteworthy.

- In $(\!|\lambda x.M|\!)^\bullet$, the occurrences of x are replaced with fresh shared variables that only occur once in M.
- The definition of $(\!|M\langle\!\langle B/x\rangle\!\rangle|\!)^\bullet$ considers two possibilities. If the bag being translated is non-empty and the explicit substitution would not lead to failure (the number of occurrences of x and the size of the bag coincide) then we translate the explicit substitution as a sum of explicit linear substitutions. Otherwise, the explicit substitution will lead to a failure, and the translation proceeds inductively. As we will see, doing this will enable a tight operational correspondence result with $\mathsf{s}\pi$.

Example 3.27 (Cont. Example 2.2)**.** We illustrate the translation $(\!|\cdot|\!)^\circ$ on previously discussed examples. In all cases, we start by ensuring that the free variables are shared. This explains the occurrence of $[y_1 \leftarrow y]$ in the translation of M_1 as well as $[y_1 \leftarrow y]$ and $[z_1 \leftarrow z]$ in the translation of M_2. Then, the auxiliary translation $(\!|\cdot|\!)^\bullet$ ensures that bound variables that are guarded by an abstraction are shared. This explains, e.g., the occurrence of $[x_1 \leftarrow x]$ in the translation of M_1.

- The translation of a $\lambda^{\not t}_{\oplus}$-term with one occurrence of a bound variable and one occurrence of a free variable: $M_1 = (\lambda x.x)\wr y \int$.

$$\begin{aligned}(\!|M_1|\!)^\circ &= (\!|(\lambda x.x)\wr y \wr|\!)^\circ \\ &= (\!|(\lambda x.x)\wr y_1 \wr|\!)^\bullet[y_1 \leftarrow y] \\ &= ((\lambda x.x_1[x_1 \leftarrow x])\wr y_1 \wr)[y_1 \leftarrow y]\end{aligned}$$

- The translation of a $\lambda^{\wr}_{\oplus}$-term with one bound and two different free variables: $M_2 = (\lambda x.x)(\wr y, z \wr)$.

$$\begin{aligned}(\!|M_2|\!)^\circ &= (\!|(\lambda x.x)(\wr y, z \wr)|\!)^\circ \\ &= (\!|(\lambda x.x)(\wr y_1, z_1 \wr)|\!)^\bullet[y_1 \leftarrow y][z_1 \leftarrow z] \\ &= ((\lambda x.x_1[x_1 \leftarrow x])(\wr y_1, z_1 \wr))[y_1 \leftarrow y][z_1 \leftarrow z]\end{aligned}$$

- The translation of a $\lambda^{\wr}_{\oplus}$-term with a vacuous abstraction: $M_4 = (\lambda x.y)\mathtt{1}$.

$$\begin{aligned}(\!|M_4|\!)^\circ &= (\!|(\lambda x.y)\mathtt{1}|\!)^\circ \\ &= (\!|(\lambda x.y_1)\mathtt{1}|\!)^\bullet[y_1 \leftarrow y] \\ &= ((\lambda x.y_1[\leftarrow x])\mathtt{1})[y_1 \leftarrow y]\end{aligned}$$

- The translation of a $\lambda^{\wr}_{\oplus}$-expression: $M_6 = (\lambda x.x)\wr y \wr + (\lambda x.x)\wr z \wr$.

$$\begin{aligned}(\!|M_6|\!)^\circ &= (\!|(\lambda x.x)\wr y \wr + (\lambda x.x)\wr z \wr|\!)^\circ \\ &= (\!|(\lambda x.x)\wr y \wr|\!)^\circ + (\!|(\lambda x.x)\wr z \wr|\!)^\circ \\ &= ((\lambda x.x_1[x_1 \leftarrow x])\wr y_1 \wr)[y_1 \leftarrow y] + ((\lambda x.x_1[x_1 \leftarrow x])\wr z_1 \wr)[z_1 \leftarrow y]\end{aligned}$$

Example 3.28. The translation of a $\lambda^{\wr}_{\oplus}$-term with two occurrences of a bound variable and two occurrences of a free variable: $M = (\lambda x.x\wr x \wr)(\wr y, y \wr)$.

$$\begin{aligned}(\!|M|\!)^\circ &= (\!|(\lambda x.x\wr x \wr)(\wr y, y \wr)|\!)^\circ \\ &= (\!|(\lambda x.x\wr x \wr)(\wr y_1, y_2 \wr)|\!)^\bullet[y_1, y_2 \leftarrow y] \\ &= ((\lambda x.x_1\wr x_2 \wr[x_1, x_2 \leftarrow x])(\wr y_1, y_2 \wr))[y_1, y_2 \leftarrow y]\end{aligned}$$

Example 3.29. Now consider the translation of $y\langle\!\langle B/x \rangle\!\rangle$, with $\mathsf{fv}(B) = \emptyset$ and $y \neq x$:

$$\begin{aligned}(\!|y\langle\!\langle B/x \rangle\!\rangle|\!)^\circ &= (\!|y_0\langle\!\langle B/x \rangle\!\rangle|\!)^\bullet[y_0 \leftarrow y] \\ &= y_0[\leftarrow x]\langle\!\langle (\!|B|\!)^\bullet/x \rangle\!\rangle[y_0 \leftarrow y].\end{aligned}$$

Hence, the translation induces (empty) sharing on x, even if x does not occur in the term y.

Proposition 3.30 ($(\!|\cdot|\!)^\circ$ Preserves Consistency)**.** *Let $\mathbb{M}$ be a $\lambda^{\wr}_{\oplus}$-expression. Then $(\!|\mathbb{M}|\!)^\circ$ is a consistent $\widehat{\lambda}^{\wr}_{\oplus}$-expression.*

Proof. By induction on the structure of $\mathbb{M}$. See App. B for details. □

$$
\begin{array}{rcll}
P, Q & ::= & \mathbf{0} & \text{(inaction)} \\
& \mid & \overline{x}(y).P & \text{(output)} \\
& \mid & x(y).P & \text{(input)} \\
& \mid & (P \mid Q) & \text{(parallel)} \\
& \mid & (\nu x)P & \text{(restriction)} \\
& \mid & [x \leftrightarrow y] & \text{(forwarder)} \\
& \mid & x.\overline{\texttt{close}} & \text{(session close)} \\
& \mid & x.\texttt{close}; P & \text{(complementary close)} \\
& \mid & x.\overline{\texttt{some}}; P & \text{(session confirmation)} \\
& \mid & x.\overline{\texttt{none}} & \text{(session failure)} \\
& \mid & x.\texttt{some}_{(w_1,\cdots,w_n)}; P & \text{(session dependency)} \\
& \mid & P \oplus Q & \text{(non-deterministic choice)}
\end{array}
$$

Figure 9: Syntax of $\mathsf{s}\pi$.

4. $\mathsf{s}\pi$: A Session-Typed π-Calculus with Non-Determinism

The π-calculus [MPW92] is a model of concurrency in which *processes* interact via *names* (or *channels*) to exchange values, which can be themselves names. Here we overview $\mathsf{s}\pi$, introduced by Caires and Pérez in [CP17], in which *session types* [Hon93, HVK98] ensure that the two endpoints of a channel perform matching actions: when one endpoint sends, the other receives; when an endpoint closes, the other closes too. Following [CP10, Wad12], $\mathsf{s}\pi$ defines a Curry-Howard correspondence between session types and a linear logic with two dual modalities ($\& A$ and $\oplus A$), which define *non-deterministic* sessions. In $\mathsf{s}\pi$, cut elimination corresponds to process communication, proofs correspond to processes, and propositions correspond to session types.

4.1. Syntax and Semantics.

We use $x, y, z, w \ldots$ to denote names implementing the *(session) endpoints* of protocols specified by session types. We consider the sub-language of [CP17] without labeled choices and replication, which is actually sufficient to encode $\lambda^{\natural}_{\oplus}$.

Definition 4.1 (Processes)**.** The syntax of $\mathsf{s}\pi$ processes is given by the grammar in Fig. 9.

As standard, $\mathbf{0}$ is the inactive process. Session communication is performed using the pair of primitives output and input: the output process $\overline{x}(y).P$ sends a fresh name y along session x and then continues as P; the input process $x(y).P$ receives a name z along x and then continues as $P\{z/y\}$, which denotes the capture-avoiding substitution of z for y in P. Process $P \mid Q$ denotes the parallel execution of P and Q. Process $(\nu x)P$ denotes the process P in which name x has been restricted, i.e., x is kept private to P. The forwarder process $[x \leftrightarrow y]$ denotes a bi-directional link between sessions x and y. Processes $x.\overline{\texttt{close}}$ and $x.\texttt{close}; P$ denote complementary actions for closing session x.

The following constructs introduce non-deterministic sessions which, intuitively, *may* provide a session protocol *or* fail.

- Process $x.\overline{\texttt{some}}; P$ confirms that the session on x will execute and continues as P.
- Process $x.\overline{\texttt{none}}$ signals the failure of implementing the session on x.
- Process $x.\texttt{some}_{(w_1,\cdots,w_n)}; P$ specifies a dependency on a non-deterministic session x. This process can either (i) synchronize with an action $x.\overline{\texttt{some}}$ and continue as P, or (ii) synchronize with an action $x.\overline{\texttt{none}}$, discard P, and propagate the failure on x to $(w_1, \cdots, w_n)$,

$$
\begin{array}{lrcl}
[\texttt{Comm}] & \overline{x}(y).Q \mid x(y).P & \longrightarrow & (\nu y)(Q \mid P) \\
[\texttt{Forw}] & (\nu x)([x \leftrightarrow y] \mid P) & \longrightarrow & P\{y/x\} \quad (x \neq y) \\
[\texttt{Close}] & x.\overline{\texttt{close}} \mid x.\texttt{close}; P & \longrightarrow & P \\
[\texttt{Some}] & x.\overline{\texttt{some}}; P \mid x.\texttt{some}_{(w_1,\cdots,w_n)}; Q & \longrightarrow & P \mid Q \\
[\texttt{None}] & x.\overline{\texttt{none}} \mid x.\texttt{some}_{(w_1,\cdots,w_n)}; Q & \longrightarrow & w_1.\overline{\texttt{none}} \mid \cdots \mid w_n.\overline{\texttt{none}} \\
[\texttt{Cong}] & P \equiv P' \wedge P' \longrightarrow Q' \wedge Q' \equiv Q & \Longrightarrow & P \longrightarrow Q \\
[\texttt{Par}] & Q \longrightarrow Q' & \Longrightarrow & P \mid Q \longrightarrow P \mid Q' \\
[\texttt{Res}] & P \longrightarrow Q & \Longrightarrow & (\nu y)P \longrightarrow (\nu y)Q \\
[\texttt{NChoice}] & Q \longrightarrow Q' & \Longrightarrow & P \oplus Q \longrightarrow P \oplus Q'
\end{array}
$$

Figure 10: Reduction for $\mathsf{s}\pi$.

which are sessions implemented in P. When x is the only session implemented in P, the tuple of dependencies is empty and so we write simply $x.\texttt{some}; P$.

- $P \oplus Q$ denotes a *non-deterministic choice* between P and Q. We shall often write $\bigoplus_{i \in I} P_i$ to stand for $P_1 \oplus \cdots \oplus P_n$.

In $(\nu y)P$ and $x(y).P$ the distinguished occurrence of name y is binding, with scope P. The set of free names of P is denoted by $fn(P)$. We identify process up to consistent renaming of bound names, writing $\equiv_\alpha$ for this congruence. We omit trailing occurrences of $\mathbf{0}$; this way, e.g., we write $x.\texttt{close}$ instead of $x.\texttt{close}; \mathbf{0}$.

Structural congruence, denoted $\equiv$, expresses basic identities on the structure of processes and the non-collapsing nature of non-determinism.

Definition 4.2 (Structural Congruence)**.** Structural congruence is defined as the least congruence relation on processes such that:

$$
\begin{array}{rcl@{\qquad}rcl}
P \mid \mathbf{0} & \equiv & \mathbf{0} & \mathbf{0} \oplus \mathbf{0} & \equiv & \mathbf{0} \\
P \mid Q & \equiv & Q \mid P & P \oplus Q & \equiv & Q \oplus P \\
(P \mid Q) \mid R & \equiv & P \mid (Q \mid R) & (P \oplus Q) \oplus R & \equiv & P \oplus (Q \oplus R) \\
[x \leftrightarrow y] & \equiv & [y \leftrightarrow x] & (\nu x)\mathbf{0} & \equiv & \mathbf{0} \\
((\nu x)P) \mid Q & \equiv & (\nu x)(P \mid Q), x \notin fn(P) & (\nu x)(\nu y)P & \equiv & (\nu y)(\nu x)P \\
(\nu x)(P \mid (Q \oplus R)) & \equiv & (\nu x)(P \mid Q) \oplus (\nu x)(P \mid R) & P \equiv_\alpha Q & \Longrightarrow & P \equiv Q
\end{array}
$$

4.2. **Operational Semantics.**

The operational semantics of $\mathsf{s}\pi$ is given by a reduction relation, denoted $P \longrightarrow Q$, which is the smallest relation on processes generated by the rules in Fig. 10. These rules specify the computations that a process performs on its own. We now explain each rule.

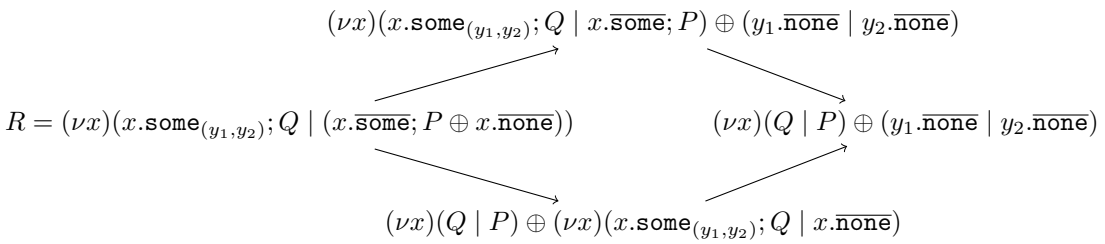
- **Rule** [Comm] formalizes communication, which concerns bound names only (internal mobility): name y is bound in both $\overline{x}(y).Q$ and $x(y).P$.
- **Rule** [Forw] implements the forwarder process that leads to a name substitution.
- **Rule** [Close] formalizes session closure and is self-explanatory.
- **Rule** [Some] describes the synchronization of a process, that is dependent on a non-deterministic session x, with the complementary process $x.\overline{\texttt{some}}$ that confirms the availability of such non-deterministic session.

- **Rule** [None] applies when the non-deterministic session is not available, prefix $x.\overline{\texttt{none}}$ triggers this failure to all dependent sessions $w_1, \ldots, w_n$; this may in turn trigger further failures (i.e., on sessions that depend on $w_1, \ldots, w_n$).
- **Rule** [NChoice] defines the closure of reduction w.r.t. non-collapsing non-deterministic choice.
- **Rules** [Cong], [Par] **and** [Res] are standard and formalize that reduction is closed under structural congruence, and also contextual closure of parallel and restriction constructs.

Example 4.3. We illustrate confluent reductions starting in a non-deterministic process R which will fail during communication due to unavailability of a session:

$$\begin{aligned} R =& (\nu x)(x.\texttt{some}_{(y_1,y_2)}; y_1(z).y_2(w).\mathbf{0} \mid (x.\overline{\texttt{some}}; P \oplus x.\overline{\texttt{none}})) \\ \equiv& (\nu x)(x.\texttt{some}_{(y_1,y_2)}; y_1(z).y_2(w).\mathbf{0} \mid x.\overline{\texttt{some}}; P) \oplus (\nu x)(x.\texttt{some}_{(y_1,y_2)}; y_1(z).y_2(w).\mathbf{0} \mid x.\overline{\texttt{none}}) \end{aligned}$$

Letting $Q = y_1(z).y_2(w).\mathbf{0}$, we have:



Observe that reduction is confluent. The resulting term $(\nu x)(Q \mid P) \oplus (y_1.\overline{\texttt{none}} \mid y_2.\overline{\texttt{none}})$ includes both alternatives for the interaction on x, namely the successful one (i.e., $(\nu x)(Q \mid P)$) but also the failure of x, which is then propagated to y_1 and y_2, i.e., $y_1.\overline{\texttt{none}} \mid y_2.\overline{\texttt{none}}$.

4.3. **Type System.** The type discipline for $\mathtt{s}\pi$ is based on the type system given in [CP17], which contains modalities $\&A$ and $\oplus A$, as dual types for non-deterministic sessions.

Definition 4.4 (Session Types)**.** Session types are given by

$$A, B ::= \bot \mid \mathbf{1} \mid A \otimes B \mid A \parr B \mid \&A \mid \oplus A$$

Types are assigned to names: an *assignment* $x : A$ enforces the use of name x according to the protocol specified by A. The multiplicative units $\bot$ and $\mathbf{1}$ are used to type terminated (closed) endpoints. $A \otimes B$ types a name that first outputs a name of type A before proceeding as specified by B. Similarly, $A \parr B$ types a name that first inputs a name of type A before proceeding as specified by B. Then we have the two modalities introduced in [CP17]. We use $\&A$ as the type of a (non-deterministic) session that *may produce* a behavior of type A. Dually, $\oplus A$ denotes the type of a session that *may consume* a behavior of type A.

The two endpoints of a session must be *dual* to ensure absence of communication errors. The dual of a type A is denoted $\overline{A}$. Duality corresponds to negation $(\cdot)^{\perp}$ in linear logic:

Definition 4.5 (Duality)**.** The duality relation on types is given by:

$$\overline{\mathbf{1}} = \bot \qquad \overline{\bot} = \mathbf{1} \qquad \overline{A \otimes B} = \overline{A} \parr \overline{B} \qquad \overline{A \parr B} = \overline{A} \otimes \overline{B} \qquad \overline{\oplus A} = \&\overline{A} \qquad \overline{\&A} = \oplus\overline{A}$$

Typing judgments are of the form $P \vdash \Delta$, where P is a process and Δ is a context of the form $x_1 : A_1, \ldots, x_n : A_n$, which defines the assignment of type A_i to name x_i (with $1 \leq i \leq n$); all names x_i must be distinct. The context Δ is *linear* in that it is subject

$$[\mathtt{T}\cdot]\ \frac{}{\mathbf{0}\vdash}$$

$$[\mathtt{Tid}]\ \frac{}{[x\leftrightarrow y]\vdash x{:}A, y{:}\overline{A}}$$

$$[\mathtt{T}\otimes]\ \frac{P\vdash\Delta, y:A \quad Q\vdash\Delta', x:B}{\overline{x}(y).(P\mid Q)\vdash\Delta,\Delta', x:A\otimes B}$$

$$[\mathtt{T}\parr]\ \frac{P\vdash\Gamma, y:C, x:D}{x(y).P\vdash\Gamma, x:C\parr D}$$

$$[\mathtt{T}\mathbf{1}]\ \frac{}{x.\overline{\mathtt{close}}\vdash x:\mathbf{1}}$$

$$[\mathtt{T}\bot]\ \frac{P\vdash\Delta}{x.\mathtt{close}; P\vdash x{:}\bot,\Delta}$$

$$[\mathtt{T}\ |]\ \frac{P\vdash\Delta \quad Q\vdash\Delta'}{P\mid Q\vdash\Delta,\Delta'}$$

$$[\mathtt{Tcut}]\ \frac{P\vdash\Delta, x:\overline{A} \quad Q\vdash\Delta', x:A}{(\nu x)(P\mid Q)\vdash\Delta,\Delta'}$$

$$[\mathtt{T}\&^{\mathtt{x}}_{\mathtt{d}}]\ \frac{P\vdash\Delta, x:A}{x.\overline{\mathtt{some}}; P\vdash\Delta, x:\&A}$$

$$[\mathtt{T}\oplus^{\mathtt{x}}_{\widetilde{\mathtt{w}}}]\ \frac{P\vdash\widetilde{w}:\&\Delta, x:A}{x.\mathtt{some}_{\widetilde{w}}; P\vdash\widetilde{w}{:}\&\Delta, x{:}\oplus A}$$

$$[\mathtt{T}\&^{\mathtt{x}}]\ \frac{}{x.\overline{\mathtt{none}}\vdash x:\&A}$$

$$[\mathtt{T}\&]\ \frac{P\vdash\&\Delta \qquad Q\vdash\&\Delta}{P\oplus Q\vdash\&\Delta}$$

Figure 11: Typing rules for $\mathsf{s}\pi$.

to exchange (the ordering of assignments does not matter), but not to weakening and contraction. In writing '$\Delta, x:A$', we assume that x does not occur in Δ; also, in writing 'Δ_1,Δ_2', we assume that the names in Δ_1 are distinct from those in Δ_2. The empty context is denoted '$\cdot$'. We write $\&\Delta$ to denote that all assignments in Δ have a non-deterministic type, i.e., $\&\Delta = w_1:\&A_1,\ldots,w_n:\&A_n$, for some $A_1,\ldots,A_n$. The typing judgment $P\vdash\Delta$ corresponds to the logical sequent $\vdash\Delta$ for classical linear logic, which can be recovered by erasing processes and name assignments.

Typing rules for processes correspond to proof rules in the logic; see Fig. 11. This way, Rule [T$\cdot$] allows us to introduce the inactive process $\mathbf{0}$. Rule [Tid] interprets the identity axiom using the forwarder process. Rules [T$\otimes$] and [T$\parr$] type output and input of a name along a session, respectively. Rules [T$\mathbf{1}$] and [T$\bot$] type the process constructs for session termination. Rules [Tcut] and [T $|$] define cut and mix principles in the logic, which induce typing rules for independent and dependent parallel composition, respectively.

The last four rules in Fig. 11 are used to type process constructs related to non-determinism and failure. Rules [T$\&^{\mathtt{x}}_{\mathtt{d}}$] and [T$\&^{\mathtt{x}}$] introduce a session of type $\&A$, which may produce a behavior of type A: while the former rule covers the case in which $x:A$ is indeed available, the latter rule formalizes the case in which $x:A$ is not available (i.e., a failure). Rule [T$\oplus^{\mathtt{x}}_{\widetilde{\mathtt{w}}}$], accounts for the possibility of not being able to consume the session $x:A$ by considering sessions, the sequence of names $\widetilde{w} = w_1,\ldots,w_n$, different from x as potentially not available. Rule [T$\&$] expresses non-deterministic choice of processes P and Q that implement non-deterministic behaviors only.

The type system enjoys type preservation, a result that follows directly from the cut elimination property in the underlying logic; it ensures that the observable interface of a system is invariant under reduction. The type system also ensures other properties for well-typed processes (e.g. global progress and confluence); see [CP17] for details.

Theorem 4.6 (Type Preservation [CP17])**.** *If $P\vdash\Delta$ and $P\longrightarrow Q$ then $Q\vdash\Delta$.*

Having defined $\mathsf{s}\pi$, we now move on to define a correct translation from $\lambda^{\lightning}_{\oplus}$ to $\mathsf{s}\pi$.

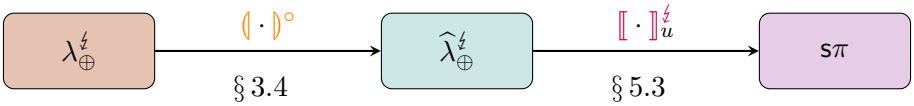


Figure 12: Summary of our approach.

5. A Correct Encoding

Having introduced the typed sequential calculi $\lambda^{\lightning}_{\oplus}$ and $\widehat{\lambda}^{\lightning}_{\oplus}$ (as well as the translation $(\!| \cdot |\!)^{\circ} : \lambda^{\lightning}_{\oplus} \to \widehat{\lambda}^{\lightning}_{\oplus}$) and the typed concurrent calculus $\mathsf{s}\pi$, in this section we show how to correctly translate $\lambda^{\lightning}_{\oplus}$ into $\mathsf{s}\pi$, using $\widehat{\lambda}^{\lightning}_{\oplus}$ as a stepping stone.

Before delving into technical details, we briefly discuss the significance of our encoding. As in Milner's seminal work, our translation explains how interaction in π provides a principled interpretation of evaluation in λ. We tackle the challenging case in which evaluation and interaction are fail-prone and non-deterministic, effectively generalizing previous translations. Because our encoding preserves types, our developments also delineate a new connection between non-idempotent intersection types and logically motivated session types—indeed, our translation of functions as processes goes hand-in-hand with a translation on types (Fig. 17), which reveals a new protocol-oriented interpretation of the non-idempotent intersections that govern functional resources.

As already mentioned, we shall proceed in two steps. We rely on the translation $(\!| \cdot |\!)^{\circ}$ from well-formed expressions in $\lambda^{\lightning}_{\oplus}$ to well-formed expressions in $\widehat{\lambda}^{\lightning}_{\oplus}$ given in § 3.4. As $\lambda^{\lightning}_{\oplus}$ and $\widehat{\lambda}^{\lightning}_{\oplus}$ share the same syntax of types, in this case the translation of types is the identity. Then, the translation $[\![\cdot]\!]^{\lightning}_{u}$ (for some name u) transforms well-formed expressions in $\widehat{\lambda}^{\lightning}_{\oplus}$ to well-typed processes in $\mathsf{s}\pi$ (cf. Fig. 12). We first define *encodability criteria* for translations, which include type preservation; these criteria lead to the notion of *correct encoding* (§ 5.1). Then, in § 5.2 we establish the correctness of the translation $(\!| \cdot |\!)^{\circ}$ (Corollary 5.15); finally, in § 5.3, we present the translation $[\![\cdot]\!]^{\lightning}_{u}$ and establish its correctness (Corollary 5.39).

5.1. Encodability Criteria.

We follow most of the criteria defined by Gorla in [Gor10], a widely studied abstract framework for establishing the *quality* of translations. A *language* $\mathcal{L}$ is defined as a pair containing a set of terms $\mathcal{M}$ and a reduction semantics $\longrightarrow$ on terms (with reflexive, transitive closure denoted $\xrightarrow{*}$). A behavioral equivalence on terms, denoted $\approx$, is also assumed. Then, a *correct encoding*, defined next, concerns a translation of terms of a source language $\mathcal{L}_1$ into terms of a target language $\mathcal{L}_2$ that respects certain criteria. The criteria in [Gor10] concern *untyped* languages; because we consider *typed* languages, we follow Kouzapas et al. [KPY19] in requiring also that translations preserve typability.

Definition 5.1 (Correct Encoding)**.** Let $\mathcal{L}_1 = (\mathcal{M}, \longrightarrow_1)$ and $\mathcal{L}_2 = (\mathcal{P}, \longrightarrow_2)$ be two languages and let $\approx_1$ be a behavioral equivalence on terms in $\mathcal{M}$. We use $M, M', \ldots$ and $P, P', \ldots$ to range over elements in $\mathcal{M}$ and $\mathcal{P}$. We say that a translation $[\![\cdot]\!] : \mathcal{M} \to \mathcal{P}$ is a *correct encoding* if it satisfies the following criteria:

(1) *Type preservation:* For every well-typed M, it holds that $[\![M]\!]$ is well-typed.

(2) *Operational Completeness:* For every M, M', and M'' such that $M \xrightarrow{*}_1 M' \approx_1 M''$, it holds that $[\![M]\!] \xrightarrow{*}_2 [\![M'']\!]$.
(3) *Operational Soundness:* For every M and P such that $[\![M]\!] \xrightarrow{*}_2 P$, there exist M' and M'' such that $M \longrightarrow_1^* M' \approx_1 M''$ and $P \xrightarrow{*}_2 [\![M'']\!]$.
(4) *Success Sensitiveness:* Let $\checkmark_1$ and $\checkmark_2$ denote a success predicate in $\mathcal{M}$ and $\mathcal{P}$, respectively. For every M, it holds that $M\checkmark_1$ if and only if $[\![M]\!]\checkmark_2$.

We briefly describe the criteria. First, type preservation is a natural requirement and a distinguishing aspect of our work, given that we always consider source and target calculi with types. Operational completeness formalizes how reduction steps of a source term are mimicked by its corresponding translation in the target language; $\approx_1$ conveniently abstracts away from source terms useful in the translation but which are not meaningful in comparisons. Operational soundness concerns the opposite direction: it formalizes the correspondence between (i) the reductions of a target term obtained via the translation and (ii) the reductions of the corresponding source term. The role of $\approx_1$ can be explained as in completeness. Our use of the equivalence $\approx_1$ for $\mathcal{M}_1$, rather than of an equivalence on $\mathcal{M}_2$, is a minor difference with respect to [Gor10]. Finally, success sensitiveness complements completeness and soundness, which concern reductions and therefore do not contain information about observable behaviors. The so-called success predicates $\checkmark_1$ and $\checkmark_2$ serve as a minimal notion of *observables*; the criterion then says that observability of success of a source term implies observability of success in the corresponding target term, and vice versa.

Besides these semantic criteria, we also consider *compositionality*, a syntactic criterion that requires that a composite source term is translated as the combination of the translations of its sub-terms.

5.2. Correctness of $(\!|\cdot|\!)^\circ$.

We prove that the translation $(\!|\cdot|\!)^\circ$ from $\lambda^{\lightning}_{\oplus}$ into $\widehat{\lambda}^{\lightning}_{\oplus}$ in § 3.4 is a correct encoding, in the sense of Def. 5.1. Because our translation $(\!|\cdot|\!)^\circ$ is defined in terms of $(\!|\cdot|\!)^\bullet$, it satisfies *weak compositionality*, in the sense of Parrow [Par08].

5.2.1. *Type Preservation.*

We now prove that $(\!|\cdot|\!)^\circ$ translates well-formed $\lambda^{\lightning}_{\oplus}$-expressions into well-formed expressions $\widehat{\lambda}^{\lightning}_{\oplus}$-expressions (Theorem 5.6). Notice that because $\lambda^{\lightning}_{\oplus}$ and $\widehat{\lambda}^{\lightning}_{\oplus}$ share the same type syntax, there is no translation on types/contexts involved (i.e., an identity translation applies).

Next we define well formed preservation in the translation $(\!|\cdot|\!)^\bullet$ from $\lambda^{\lightning}_{\oplus}$ to $\widehat{\lambda}^{\lightning}_{\oplus}$. We rely on the prerequisite proof of type preservation in the translation $(\!|\cdot|\!)^\bullet$ on the sub-calculi from $\lambda_{\oplus}$ to $\widehat{\lambda}_{\oplus}$, and also on syntactic properties of the translation such as: (i) the property below guarantees that the translation $(\!|\cdot|\!)^\bullet$ commutes with the linear head substitution; (ii) preservation of typability/well-formedness w.r.t. linear substitutions in $\widehat{\lambda}^{\lightning}_{\oplus}$.

Proposition 5.2. *Let M, N be $\lambda^{\lightning}_{\oplus}$-terms. We have:*
(1) $(\!|M\{\!|N/x|\!\}|\!)^\bullet = (\!|M|\!)^\bullet\{\!|(\!|N|\!)^\bullet/x|\!\}$.
(2) $(\!|M\langle\widetilde{x}/x\rangle|\!)^\bullet = (\!|M|\!)^\bullet\langle\widetilde{x}/x\rangle$, *where $\widetilde{x} = x_1, \ldots, x_k$ is sequence of pairwise distinct fresh variables.*

Proof. By induction of the structure of M. □

Lemma 5.3 (Preservation under Linear Substitutions in $\widehat{\lambda}^{\natural}_{\oplus}$)**.** *Let* $M \in \widehat{\lambda}^{\natural}_{\oplus}$.
(1) *Typing: If* $\Gamma, x : \sigma^k \vdash M : \tau$ *then* $\Gamma, x_i : \sigma^{k-1} \vdash M\langle x_i/x\rangle : \tau$.
(2) *Well-formedness: If* $\Gamma, x : \sigma^k \models M : \tau$ *then* $\Gamma, x_i : \sigma^{k-1} \models M\langle x_i/x\rangle : \tau$.

Proof. Standard by induction on the rules from Fig. 6 for item (1), and Fig. 7 for item (2). □

The following example illustrates that the translation of a well-formed $\lambda^{\natural}_{\oplus}$-expression is a well-formed $\widehat{\lambda}^{\natural}_{\oplus}$-expression.

Example 5.4 (Cont. Example 2.25)**.** Term $M_2 = (\lambda x.x)(\wr y, z \wr)$ is well-formed with a well-formedness judgment $y : \sigma, z : \sigma \models (\lambda x.x)(\wr y, z \wr) : \sigma$. In Example 3.27 we showed that $(\!|M_2|\!)^{\circ} = ((\lambda x.x_1[x_1 \leftarrow x])(\wr y_1, z_1 \wr))[y_1 \leftarrow y][z_1 \leftarrow z]$ which is well-formed with translated well-formed judgment $y : \sigma^1, z : \sigma^1 \models (\!|M_2|\!)^{\circ} : \sigma$. The derivation is given below (using rules from Fig. 7); we omit the labels of rule applications and concatenations with the empty bag, i.e., we write $\wr y_1 \wr$ instead of $\wr y_1 \wr \cdot \mathtt{1}$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{x_1 : \sigma \vdash x_1 : \sigma}}{x_1 : \sigma \models x_1 : \sigma}}{x : \sigma^1 \models x[x_1 \leftarrow x] : \sigma}}{\models \lambda x.(x[x_1 \leftarrow x]) : \sigma \to \sigma} \quad \dfrac{\dfrac{\dfrac{}{y_1 : \sigma \vdash y_1 : \sigma}}{y_1 : \sigma \models y_1 : \sigma}}{y_1 : \sigma^1 \models \wr y_1 \wr : \sigma^1} \quad \dfrac{\dfrac{\dfrac{}{z_1 : \sigma \vdash z_1 : \sigma}}{z_1 : \sigma \models z_1 : \sigma}}{z_1 : \sigma^1 \models \wr z_1 \wr : \sigma^1}}{\dfrac{y_1 : \sigma^1, z_1 : \sigma^1 \models \wr y_1 \wr \cdot \wr z_1 \wr : \sigma^2}{y_1 : \sigma^1, z_1 : \sigma^1 \models \lambda x.(x_1[x_1 \leftarrow x])\wr y_1, z_1 \wr : \sigma}}{\dfrac{y : \sigma^1, z_1 : \sigma^1 \models \lambda x.(x_1[x_1 \leftarrow x])\wr y_1, z_1 \wr[y_1 \leftarrow y] : \sigma}{y : \sigma^1, z : \sigma^1 \models \lambda x.(x_1[x_1 \leftarrow x])\wr y_1, z_1 \wr[y_1 \leftarrow y][z_1 \leftarrow z] : \sigma}}$$

As the translation $(\!|\cdot|\!)^{\circ}$ for $\lambda^{\natural}_{\oplus}$-terms is defined in terms of $(\!|\cdot|\!)^{\bullet}$, it is natural that preservation of well-formedness under $(\!|\cdot|\!)^{\circ}$ (Theorem 5.6) relies on the preservation of well-formedness under $(\!|\cdot|\!)^{\bullet}$, given next.

To state well-formedness preservation, we use $\Gamma^{\dagger}$, the core context of Γ (Def. 3.12). In the following property, we use an additional condition on $\Gamma^{\dagger}$, which reflects the fact that intersection types get "flattened" by virtue of the translation. The condition, denoted $\widehat{\Gamma}^{\dagger}$, is defined whenever $\Gamma^{\dagger}$ contains only unary multisets as follows: if $x : \sigma^1 \in \Gamma^{\dagger}$ for all $x \in \mathtt{dom}(\Gamma^{\dagger})$, then $x : \sigma \in \widehat{\Gamma}^{\dagger}$.

Lemma 5.5 (Well-formedness preservation for $(\!|\cdot|\!)^{\bullet}$)**.** *Let* B *and* $\mathbb{M}$ *be a bag and an expression in* $\lambda^{\natural}_{\oplus}$*, respectively. Also, let* Γ *be a context such that* $\widehat{\Gamma}^{\dagger}$ *is defined. We have:*
(1) *If* $\Gamma \models B : \pi$ *then* $\widehat{\Gamma}^{\dagger} \models (\!|B|\!)^{\bullet} : \pi$.
(2) *If* $\Gamma \models \mathbb{M} : \sigma$ *then* $\widehat{\Gamma}^{\dagger} \models (\!|\mathbb{M}|\!)^{\bullet} : \sigma$.

Proof (Sketch). By mutual induction on the typing derivations $\Gamma \models B : \sigma$ and $\Gamma \models \mathbb{M} : \sigma$. The proof of item (1) follows mostly by induction hypothesis, by analyzing the rule applied (Fig. 4). The proof of item (2), also follows by analyzing the rule applied, but it is more delicate, especially when treating cases involving Rules [FS : app] or [FS : ex-sub], for which the size of the bag does not match the number of occurrences of variables in the expression. See App. C.1.2 for full details. □

Theorem 5.6 (Well-formedness Preservation for $(\!|\cdot|\!)^{\circ}$)**.** *Let* B *and* $\mathbb{M}$ *be a bag and an expression in* $\lambda^{\natural}_{\oplus}$*, respectively.*

$$
\begin{array}{rcll}
M\langle\!\langle \mathbf{1}/x\rangle\!\rangle & \equiv_\lambda & M & (\text{if } x \notin \mathsf{fv}(M)) \\
MB_1\langle\!\langle B_2/x\rangle\!\rangle & \equiv_\lambda & (M\langle\!\langle B_2/x\rangle\!\rangle)B_1 & (\text{if } x \notin \mathsf{fv}(B_1)) \\
M\langle\!\langle B_1/y\rangle\!\rangle\langle\!\langle B_2/x\rangle\!\rangle & \equiv_\lambda & (M\langle\!\langle B_2/x\rangle\!\rangle)\langle\!\langle B_1/y\rangle\!\rangle & (\text{if } x \neq y, x \notin \mathsf{fv}(B_1) \text{ and } y \notin \mathsf{fv}(B_2)) \\
M \equiv_\lambda M' & \Rightarrow & C[M] \equiv_\lambda C[M'] & \\
\mathbb{M} \equiv_\lambda \mathbb{M}' & \Rightarrow & D[\mathbb{M}] \equiv_\lambda D[\mathbb{M}'] &
\end{array}
$$

Figure 13: Congruence in $\lambda^{\lightning}_{\oplus}$

(1) *If* $\Gamma \models B : \pi$ *then* $\Gamma^\dagger \models (\!|B|\!)^\circ : \pi$.
(2) *If* $\Gamma \models \mathbb{M} : \sigma$ *then* $\Gamma^\dagger \models (\!|\mathbb{M}|\!)^\circ : \sigma$.

Proof (Sketch). By mutual induction on the typing derivations $\Gamma \models B : \sigma$ and $\Gamma \models \mathbb{M} : \sigma$. Note that for a bag B, since the first part of translation consists in sharing the free variables of B, we will work with the translated bag $(\!|B|\!)^\circ = (\!|B\langle\widetilde{x_1}/x_1\rangle \dots \langle\widetilde{x_k}/x_k\rangle|\!)^\bullet[\widetilde{x_1} \leftarrow x_1] \dots [\widetilde{x_k} \leftarrow x_k]$, and the rest of the proof depends on Proposition 5.2 that moves linear substitutions outside $(\!|\cdot|\!)^\bullet$, then Lemma 5.3 that guarantees preservation of typability/well-formedness under linear substitutions, and Lemma 5.5 for treating the closed translation. The dependency extends to the proof of item (2), for expressions. The full proof can be found in App. C.1.2. □

5.2.2. *Operational Correspondence: Completeness and Soundness.*

Def. 5.1 states operational completeness and soundness over the reflexive, transitive closure of the reduction rules. However, in the case of $(\!|\cdot|\!)^\circ$, we prove completeness and soundness for a single reduction step (cf. Fig. 14). This is sufficient: by the diamond property (Proposition 2.13) a result stated for $\longrightarrow$ can be extended easily to $\xrightarrow{*}$, by induction on the length of the reduction sequence. (The result is immediate when the length is zero.)

We rely on a *structural equivalence* over $\lambda^{\lightning}_{\oplus}$-expressions, denoted $\equiv_\lambda$, which is the least congruence satisfying α-conversion and satisfying the identities in Fig. 13. This congruence allows us to move explicit substitutions to the right of the term and to ignore explicit substitutions of a variable x for empty bags in a term that does not contain x.

Example 5.7. Consider the failure term $M = \mathtt{fail}^{y,y,z}\langle\!\langle \mathbf{1}/x\rangle\!\rangle$. Since $\mathsf{size}(\mathbf{1}) = 0$, the term M cannot reduce using Rule $[\mathtt{R} : \mathtt{Cons}_2]$, which requires that the size of the bag is greater than 0. Instead, we use the structural equivalence identity in Fig. 13: $\mathtt{fail}^{y,y,z}\langle\!\langle \mathbf{1}/x\rangle\!\rangle \equiv_\lambda \mathtt{fail}^{y,y,z}$.

Theorem 5.8 (Operational Completeness)**.** *Let* $\mathbb{M}, \mathbb{N}$ *be well-formed* $\lambda^{\lightning}_{\oplus}$ *expressions. Suppose* $\mathbb{N} \longrightarrow_{[\mathtt{R}]} \mathbb{M}$.

(1) *If* $[\mathtt{R}] = [\mathtt{R} : \mathtt{Beta}]$ *then* $(\!|\mathbb{N}|\!)^\circ \longrightarrow^{\leq 2} (\!|\mathbb{M}|\!)^\circ$;
(2) *If* $[\mathtt{R}] = [\mathtt{R} : \mathtt{Fetch}]$ *then* $(\!|\mathbb{N}|\!)^\circ \longrightarrow^{+} (\!|\mathbb{M}'|\!)^\circ$, *for some* $\mathbb{M}'$ *such that* $\mathbb{M} \equiv_\lambda \mathbb{M}'$.
(3) *If* $[\mathtt{R}] \neq [\mathtt{R} : \mathtt{Beta}]$ *and* $[\mathtt{R}] \neq [\mathtt{R} : \mathtt{Fetch}]$ *then* $(\!|\mathbb{N}|\!)^\circ \longrightarrow (\!|\mathbb{M}|\!)^\circ$.

Proof (Sketch). By induction on the rules from Figure 2 applied to infer $\mathbb{N} \longrightarrow_{[\mathtt{R}]} \mathbb{M}$. We analyse the reduction depending on whether $[\mathtt{R}]$ is either $[\mathtt{R} : \mathtt{Beta}]$, or $[\mathtt{R} : \mathtt{Fetch}]$, or neither. In the case the rule applied is $[\mathtt{Beta}]$, then $\mathbb{N} = (\lambda x.M')\wr B \wr$ and $\mathbb{M} = M'\langle\!\langle B/x\rangle\!\rangle$. When applying the translation $(\!|\cdot|\!)^\circ$ to $\mathbb{N}$ and $\mathbb{M}$ we obtain:

- $(\!|\mathbb{N}|\!)^\circ = ((\lambda x.(\!|M''\langle\widetilde{y}/x\rangle|\!)^\bullet[\widetilde{y} \leftarrow x])(\!|B'|\!)^\bullet)[\widetilde{x_1} \leftarrow x_1] \dots [\widetilde{x_k} \leftarrow x_k]$
- $(\!|\mathbb{M}|\!)^\circ = (\!|M''\langle\!\langle B'/x\rangle\!\rangle|\!)^\bullet[\widetilde{x_1} \leftarrow x_1] \dots [\widetilde{x_k} \leftarrow x_k]$

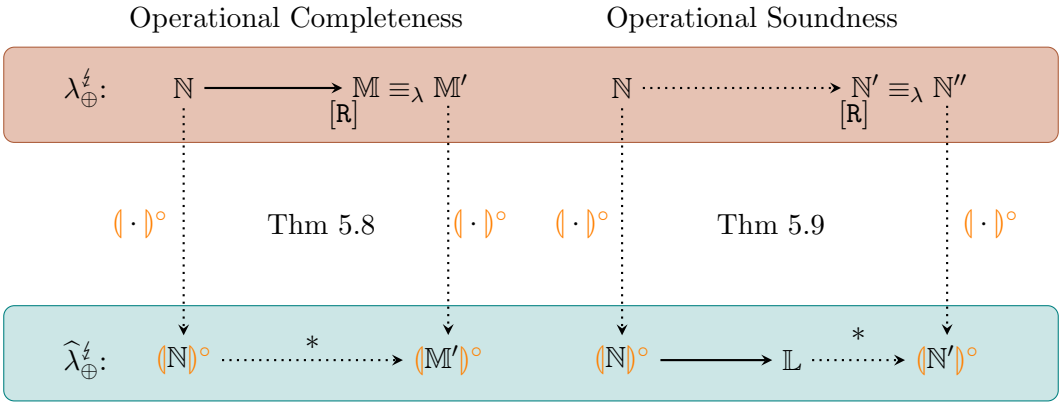


Figure 14: Operational correspondence for $(\!|\cdot|\!)^\circ$

where B' and M'' stand for the renamings of B and M', respectively, after sharing the multiple occurrences of their free/bound variables (Def. 3.26). Note that

$$(\!|\mathbb{N}|\!)^\circ \longrightarrow_{[\texttt{RS:Beta}]} (\!|M''\langle\widetilde{y}/x\rangle|\!)^\bullet[\widetilde{y} \leftarrow x]\langle\!\langle (\!|B'|\!)^\bullet/x\rangle\!\rangle)[\widetilde{x_1} \leftarrow x_1]\ldots[\widetilde{x_k} \leftarrow x_k] := \mathbb{L},$$

and according to rules in Fig. 5, the remaining reduction depends upon the characteristics of the bag $(\!|B'|\!)^\bullet$:

(i) $\mathsf{size}((\!|B'|\!)^\bullet) = \#(x, M'') = k \geq 1$. Then, $(\!|\mathbb{N}|\!)^\circ \longrightarrow_{[\texttt{RS:Beta}]} \mathbb{L} \longrightarrow_{[\texttt{RS:ex-sub}]} (\!|\mathbb{M}|\!)^\circ$.

(ii) Otherwise, $\mathbb{L}$ can be further expanded, the "otherwise case" of the translation of explicit substitutions, such that

$$(\!|\mathbb{N}|\!)^\circ \longrightarrow_{[\texttt{RS:Beta}]} (\!|M''\langle\widetilde{y}/x\rangle|\!)^\bullet[\widetilde{y} \leftarrow x]\langle\!\langle (\!|B'|\!)^\bullet/x\rangle\!\rangle)[\widetilde{x_1} \leftarrow x_1]\ldots[\widetilde{x_k} \leftarrow x_k] = \mathbb{L} = (\!|\mathbb{M}|\!)^\circ.$$

In the case the rule applied is $[\mathtt{R} : \mathtt{Fetch}]$, the proof depends on the size n of the bag. The interesting case is when the bag B has only one component (i.e., $n = 1$): from $\mathbb{N} \longrightarrow_{[\texttt{F:Fetch}]} \mathbb{N}$ we have that $\mathbb{N} = M\langle\!\langle \{\!| N_1 |\!\}/x\rangle\!\rangle$ and $\mathbb{M} = M\{\!|N_1/x|\!\}\langle\!\langle \{\!|1|\!\}/x\rangle\!\rangle$. We need to use the congruence $\equiv_\lambda$ to obtain $\mathbb{M} = M\{\!|N_1/x|\!\}\langle\!\langle \{\!|1|\!\}/x\rangle\!\rangle \equiv_\lambda M\{\!|N_1/x|\!\} := \mathbb{M}'$ and then conclude that $(\!|\mathbb{N}|\!)^\circ \longrightarrow (\!|\mathbb{M}'|\!)^\circ$. The analysis for the other cases is also done by inspecting the structure of expressions and bags. The full proof can be found in App. C.2. □

We establish soundness for a single reduction step. As we discussed for completeness, the property generalizes to multiple steps.

Theorem 5.9 (Operational Soundness)**.** *Let $\mathbb{N}$ be a well-formed $\lambda^{\lightning}_{\oplus}$ expression. Suppose $(\!|\mathbb{N}|\!)^\circ \longrightarrow \mathbb{L}$. Then, there exists $\mathbb{N}'$ such that $\mathbb{N} \longrightarrow_{[\mathtt{R}]} \mathbb{N}'$ and*

(1) *If $[\mathtt{R}] = [\mathtt{R} : \mathtt{Beta}]$ then $\mathbb{L} \longrightarrow^{\leq 1} (\!|\mathbb{N}'|\!)^\circ$;*
(2) *If $[\mathtt{R}] \neq [\mathtt{R} : \mathtt{Beta}]$ then $\mathbb{L} \longrightarrow^* (\!|\mathbb{N}''|\!)^\circ$, for $\mathbb{N}''$ such that $\mathbb{N}' \equiv_\lambda \mathbb{N}''$.*

Proof (Sketch). By induction on the structure of $\mathbb{N}$ and inspecting the rules from Fig. 5 that can be applied in $(\!|\mathbb{N}|\!)^\circ$. The interesting cases happen when $\mathbb{N}$ is either an application $\mathbb{N} = (M\ B)$ or an explicit substitution $\mathbb{N} = M\langle\!\langle B/x\rangle\!\rangle$. The former is reducible when $\mathbb{N}$ is an instance of $[\mathtt{R} : \mathtt{Beta}]$ or when $M = \mathtt{fail}^{\widetilde{x}}$ and $\mathbb{N}$ is an instance of $[\mathtt{R} : \mathtt{Cons}_1]$. The latter, for $\mathbb{N} = M\langle\!\langle B/x\rangle\!\rangle$, the proof is split in several subcases depending whether: (i) size of the bag $\mathsf{size}(B) = \#(x, M) \geq 1$, and three possible reductions can take place $[\mathtt{RS} : \mathtt{lin\text{-}fetch}]$, $[\mathtt{RS} : \mathtt{Cons}_3]$ and $[\mathtt{RS} : \mathtt{Cont}]$, depending if M is a failing term or not; (ii) $\mathsf{size}(B) \neq \#(x, M)$

or $\mathsf{size}(B) = 0$, and the proof follows either applying Rule [RS : Fail] or by induction hypothesis. The full proof can be found in App. C.2. □

5.2.3. *Success Sensitiveness.*

We now consider success sensitiveness, a property that complements (and relies on) operational completeness and soundness. For the purposes of the proof, we consider the extension of $\lambda^{\lightning}_{\oplus}$ and $\widehat{\lambda}^{\lightning}_{\oplus}$ with dedicated constructs and predicates that specify success.

Definition 5.10. We extend the syntax of terms for $\lambda^{\lightning}_{\oplus}$ and $\widehat{\lambda}^{\lightning}_{\oplus}$ with the same ✓ construct. In both cases, we assume ✓ is well formed. Also, we define $\mathsf{head}(✓) = ✓$ and $(\!|✓|\!)^{\bullet} = ✓$

An expression $\mathbb{M}$ has success, denoted $\mathbb{M} \Downarrow_{✓}$, when there is a sequence of reductions from $\mathbb{M}$ that leads to an expression that includes a summand that contains an occurrence of ✓ in head position.

Definition 5.11 (Success in $\lambda^{\lightning}_{\oplus}$ and $\widehat{\lambda}^{\lightning}_{\oplus}$)**.** In $\lambda^{\lightning}_{\oplus}$ and $\widehat{\lambda}^{\lightning}_{\oplus}$, we define

$$\mathbb{M} \Downarrow_{✓} \iff \exists M_1, \cdots, M_k.\ \mathbb{M} \longrightarrow^{*} M_1 + \cdots + M_k \text{ and } \mathsf{head}(M_j) = ✓,$$

for some $j \in \{1, \ldots, k\}$.

Definition 5.12 (Head of an expression)**.** We extend Def. 3.4 from terms to expressions as follows:

$$\mathsf{head}_{\sum}(\mathbb{M}) = \begin{cases} \mathsf{head}(M_i) & \text{if } \mathsf{head}(M_i) = \mathsf{head}(M_j) \text{ for all } M_i, M_j \in \mathbb{M} \\ \text{undefined} & \text{otherwise} \end{cases}$$

Proposition 5.13 (Preservation of head term)**.** *The head of a term is preserved when applying the translation* $(\!|\cdot|\!)^{\circ}$*, i.e.,*

$$\forall M \in \lambda^{\lightning}_{\oplus}.\ \mathsf{head}(M) = ✓ \iff \mathsf{head}_{\sum}((\!|M|\!)^{\circ}) = ✓.$$

Proof (Sketch). By induction on the structure of M considering the extension of the language established in Def. 5.10. See App. C.3 for details. □

Theorem 5.14 (Success Sensitivity)**.** *Let* $\mathbb{M}$ *be a well-formed* $\lambda^{\lightning}_{\oplus}$*-expression. Then,*

$$\mathbb{M} \Downarrow_{✓} \iff (\!|\mathbb{M}|\!)^{\circ} \Downarrow_{✓}.$$

Proof (Sketch). By induction on the structure of $\lambda^{\lightning}_{\oplus}$ and $\widehat{\lambda}^{\lightning}_{\oplus}$ expressions. The if-case follows from operational soundness (Thm. 5.9) by analyzing a reductions starting from $(\!|\mathbb{M}|\!)^{\circ}$. Reciprocally, the only-if-case follows by operational completeness (Thm. 5.8), analyzing reductions starting from $\mathbb{M}$. See App. C.3 for details. □

We have the corollary below, which follows from Theorems 5.6, 5.8, 5.9, and 5.14:

Corollary 5.15. *Our translation* $(\!|\cdot|\!)^{\circ}$ *is a correct encoding, in the sense of Def. 5.1.*

$$
\begin{aligned}
[\![x]\!]_u &= x.\overline{\texttt{some}};[x \leftrightarrow u] \\
[\![\lambda x.M[\widetilde{x} \leftarrow x]]\!]_u &= u.\overline{\texttt{some}};u(x).[\![M[\widetilde{x} \leftarrow x]]\!]_u \\
[\![M\ B]\!]_u &= \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)([\![M]\!]_v \mid v.\texttt{some}_{u,\mathsf{fv}(B)};\overline{v}(x).(x.\texttt{some}_{\mathsf{fv}(B_i)};[\![B_i]\!]_x \mid [v \leftrightarrow u])) \\
[\![M[x_1,\ldots,x_k \leftarrow x]]\!]_u &= x.\overline{\texttt{some}};x(x_1).\cdots.x(x_k).x.\texttt{close};[\![M]\!]_u \\
[\![M[\leftarrow x]]\!]_u &= x.\overline{\texttt{some}};x.\texttt{close};[\![M]\!]_u \\
[\![\wr M \wr \cdot B]\!]_x &= \overline{x}(x_1).(x_1.\texttt{some}_{\mathsf{fv}(B)};[\![M]\!]_{x_1} \mid [\![B]\!]_x) \\
[\![\mathtt{1}]\!]_x &= x.\overline{\texttt{close}} \\
[\![M[\widetilde{x} \leftarrow x]\langle\!\langle {}^{B}\!/_{x} \rangle\!\rangle]\!]_u &= \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x)([\![M[\widetilde{x} \leftarrow x]]\!]_u \mid x.\texttt{some}_{\mathsf{fv}(B_i)};[\![B_i]\!]_x) \\
[\![M\langle\!| N/x |\!\rangle]\!]_u &= (\nu x)([\![M]\!]_u \mid x.\texttt{some}_{\mathsf{fv}(N)};[\![N]\!]_x) \\
[\![\mathbb{M} + \mathbb{N}]\!]_u &= [\![\mathbb{M}]\!]_u \oplus [\![\mathbb{N}]\!]_u
\end{aligned}
$$

Figure 15: An auxiliary translation of $\widehat{\lambda}_{\oplus}$ into $\mathsf{s}\pi$, without failures

5.3. From $\widehat{\lambda}^{\lightning}_{\oplus}$ to $\mathsf{s}\pi$.

We now define our translation of $\widehat{\lambda}^{\lightning}_{\oplus}$ into $\mathsf{s}\pi$, denoted $[\![\cdot]\!]^{\lightning}_u$, and establish its correctness. As usual in translations of λ into π, we use a name u to provide the behavior of the translated expression. In our case, u is a non-deterministic session: the translated expression can be available or not; this is signalled by prefixes '$u.\overline{\texttt{some}}$' and '$u.\overline{\texttt{none}}$', respectively. Notice that every (free) variable x in a $\widehat{\lambda}^{\lightning}_{\oplus}$-term M becomes a name x in its corresponding process $[\![M]\!]^{\lightning}_u$ and is assigned an appropriate session type.

5.3.1. *An Auxiliary Translation.* Before introducing $[\![\cdot]\!]^{\lightning}_u$, we first discuss the translation $[\![\cdot]\!]_u : \widehat{\lambda}_{\oplus} \to \mathsf{s}\pi$, i.e., the translation in which the source language does not include failures. This auxiliary translation, shown in Fig. 15, is given for pedagogical purposes: it allows us to gradually discuss several key design decisions in $[\![\cdot]\!]^{\lightning}_u$.

We describe each case of the translation $[\![\cdot]\!]_u$, focusing on the rôle of non-deterministic sessions (expressed using prefixes '$x.\overline{\texttt{some}}$' and '$x.\texttt{some}_{(w_1,\cdots,w_n)}$' in $\mathsf{s}\pi$):

- $[\![x]\!]_u$: Because sessions are non-deterministically available, the translation first confirms that the behavior along x is available; subsequently, the forwarder process induces a substitution $\{{}^{x}\!/_{u}\}$.
- $[\![\lambda x.M[\widetilde{x} \leftarrow x]]\!]_u$: As in the case of variables, the translation first confirms the behavior along u before receiving a name, which will be used in the translation of $M[\widetilde{x} \leftarrow x]$, discussed next.
- $[\![M\ B]\!]_u$: This process models the application of M to bag B as a non-deterministic choice in the order in which the elements of B are substituted into M. Substituting each B_i involves a protocol in which the translation of a term $\lambda x.M'[\widetilde{x} \leftarrow x]$ within M confirms its own availability, before and after the exchange of the name x, on which the translation of B_i is spawned. This protocol uses the fact that $M\ B$ does not reduce to failure, i.e., there is no lack or excess of resources in B.

- $[\![M[x_1,\ldots,x_k \leftarrow x]]\!]_u$: The translation first confirms the availability of the behavior along x. Then, it receives along x a name for each x_i: these received names will be used to synchronize with the translation of bags (see below). Subsequently, the protocol on x safely terminates and the translation of M is executed.
- $[\![M[\leftarrow x]]\!]_u$: When there are no variables to be shared with x, the translation simply confirms the behavior on x, close the protocol immediately after, and executes the translation of M.
- $[\![\wr M \wr \cdot B]\!]_x$: The translation of a non-empty bag essentially makes each element available in its corresponding order. This way, for the first element M a name x_1 is sent over x; the translation of $M[x_1,\cdots,x_n \leftarrow x]$, discussed above, must send a confirmation on x_1 before the translation of M is executed. After these exchanges, the translation of the rest of the bag is spawned.
- $[\![\mathtt{1}]\!]_x$: In line with the previous item, the translation of the empty bag simply closes the name x; this signals that there are no (further) elements in the bag and that all synchronizations are complete.
- $[\![M[\widetilde{x} \leftarrow x]\langle\!\langle {}^{B}/_{x}\rangle\!\rangle]\!]_u$: In this case, the translation is a sum involving the parallel composition of (i) the translation of each element B_i in the bag and (ii) the translation of M. Observe that a fresh name x is created to enable synchronization between these two processes. Also, as in previous cases, notice how the translation of B_i must first confirm its availability along x.
- $[\![M\{\!|N/x|\!\}]\!]_u$: This translation essentially executes the translations of M and N in parallel, with a caveat: the translation of N depends on the availability of a behavior along x, to be produced within the translation of M.
- $[\![\mathbb{M}+\mathbb{N}]\!]_u$: This translation homomorphically preserves the non-determinism between M and N.

Example 5.16. Consider the $\widehat{\lambda}_{\oplus}$-term $M_0 = (\lambda x.M[x_1,x_2 \leftarrow x])\wr N_1, N_2 \wr$. Writing $\mathsf{fv}(B)$ to denote the free variables in N_1 and N_2, the process $[\![M_0]\!]_u$ is as follows:

$$
\begin{aligned}
[\![M_0]\!]_u =& [\![(\lambda x.M[x_1,x_2 \leftarrow x])\wr N_1, N_2 \wr]\!]_u \\
=& (\nu v)([\![\lambda x.M[x_1,x_2 \leftarrow x]]\!]_v \mid \underbrace{v.\mathtt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).(x.\mathtt{some}_{\mathsf{fv}(B)}; [\![\wr N_1, N_2 \wr]\!]_x \mid [v \leftrightarrow u])}_{P_1}) \\
& \oplus \\
& (\nu v)([\![\lambda x.M[x_1,x_2 \leftarrow x]]\!]_v \mid \underbrace{v.\mathtt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).(x.\mathtt{some}_{\mathsf{fv}(B)}; [\![\wr N_2, N_1 \wr]\!]_x \mid [v \leftrightarrow u])}_{P_2}) \\
=& (\nu v)(v.\overline{\mathtt{some}}; v(x).x.\overline{\mathtt{some}}; x(x_1).x(x_2).x.\mathtt{close}; [\![M]\!]v \mid P_1) \\
& \oplus \\
& (\nu v)(v.\overline{\mathtt{some}}; v(x).x.\overline{\mathtt{some}}; x(x_1).x(x_2).x.\mathtt{close}; [\![M]\!]v \mid P_2)
\end{aligned}
$$

The translation immediately opens up a non-deterministic choice with two alternatives, corresponding to the bag of size 2. Because of non-collapsing non-determinism, after some reductions, this amounts to accounting for the two different orders in which N_1 and N_2 can be extracted from the bag.

$$\begin{aligned}\llbracket M_0 \rrbracket_u \longrightarrow^* & (\nu x)(x(x_1).x(x_2).x.\texttt{close}; \llbracket M \rrbracket_u \mid \llbracket (N_1, N_2) \rrbracket_x) \\ & \oplus \\ & (\nu x)(x(x_1).x(x_2).x.\texttt{close}; \llbracket M \rrbracket_u \mid \llbracket (N_2, N_1) \rrbracket_x)\end{aligned}$$

We show further reductions for one of the processes, which we will denote R, for $R = (\nu x)(x(x_1).x(x_2).x.\texttt{close}; \llbracket M \rrbracket_u \mid \llbracket (N_1, N_2) \rrbracket_x)$, in the resulting sum (reductions for the other process are similar):

$$\begin{aligned}R =& (\nu x)(x(x_1).x(x_2).x.\texttt{close}; \llbracket M \rrbracket_u \mid \llbracket (N_1, N_2) \rrbracket_x) \\ =& (\nu x)(x(x_1).x(x_2).x.\texttt{close}; \llbracket M \rrbracket_u \mid \overline{x}(x_1).(x_1.\texttt{some}_{\mathsf{fv}(N_1)}; \llbracket N_1 \rrbracket_{x_1} \mid \\ & \qquad \overline{x}(x_2).(x_2.\texttt{some}_{\mathsf{fv}(N_2)}; \llbracket N_2 \rrbracket_{x_2} \mid x.\overline{\texttt{close}}))) \\ \longrightarrow^* & (\nu x_1, x_2)(\llbracket M \rrbracket_u \mid x_1.\texttt{some}_{\mathsf{fv}(N_1)}; \llbracket N_1 \rrbracket_{x_1} \mid x_2.\texttt{some}_{\mathsf{fv}(N_2)}; \llbracket N_2 \rrbracket_{x_2})\end{aligned}$$

5.3.2. *The Translation.*

The translation $\llbracket \cdot \rrbracket_x$ leverages non-deterministic sessions in $\mathsf{s}\pi$ to give a concurrent interpretation of $\widehat{\lambda}_{\oplus}$, the non-deterministic (but fail-free) sub-calculus of $\widehat{\lambda}^{\lightning}_{\oplus}$. In a nutshell, non-deterministic sessions entail the explicit confirmation of the availability of a name's behavior, via synchronizations of a prefix '$x.\texttt{some}_{(w_1,\cdots,w_n)}$' with a corresponding prefix '$x.\overline{\texttt{some}}$'. Clearly, $\llbracket \cdot \rrbracket_x$ under-utilizes the expressivity of $\mathsf{s}\pi$: in processes resulting from $\llbracket \cdot \rrbracket_x$, no prefix '$x.\texttt{some}_{(w_1,\cdots,w_n)}$' will ever synchronize with a prefix '$x.\overline{\texttt{none}}$'. Indeed, because terms in $\widehat{\lambda}_{\oplus}$ never reduce to failure, $\llbracket \cdot \rrbracket_x$ should not account for such failures.

We may now introduce $\llbracket \cdot \rrbracket^{\lightning}_u$, our translation of the fail-prone calculus $\widehat{\lambda}^{\lightning}_{\oplus}$ into $\mathsf{s}\pi$. It builds upon the structure of $\llbracket \cdot \rrbracket_x$ to account for failures in expressions due to the lack or excess of resources. To this end, as we will see, $\llbracket \cdot \rrbracket^{\lightning}_u$ does exploit prefixes '$x.\overline{\texttt{none}}$' to signal failures.

Translating Expressions. We introduce the translation $\llbracket \cdot \rrbracket^{\lightning}_u$, which will be shown to be a correct encoding, according to the criteria given in § 5.1.

Definition 5.17 (From $\widehat{\lambda}^{\lightning}_{\oplus}$ into $\mathsf{s}\pi$: Expressions)**.** Let u be a name. The translation $\llbracket \cdot \rrbracket^{\lightning}_u : \widehat{\lambda}^{\lightning}_{\oplus} \to \mathsf{s}\pi$ is defined in Fig. 16.

We discuss the most interesting aspects of the translation in Fig. 16, in particular how the possibility of failure (lack or excess of resources in bags) induces differences with respect to the translation in Fig. 15.

Most salient differences can be explained by looking at the translation of the application $M\,B$. Indeed, the sources of failure in $\widehat{\lambda}^{\lightning}_{\oplus}$ concern a mismatch between the number of variable occurrences in M and the number of resources present in B. Both M and B can fail on their own, and our translation into $\mathsf{s}\pi$ must capture this mutual dependency. Let us recall the translation given in Fig. 15:

$$\llbracket M\ B \rrbracket_u = \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)(\llbracket M \rrbracket_v \mid v.\texttt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).(x.\texttt{some}_{\mathsf{fv}(B_i)}; \llbracket B_i \rrbracket_x \mid [v \leftrightarrow u]))$$

The corresponding translation in Fig. 16 is seemingly simpler:

$$\llbracket M\,B \rrbracket^{\lightning}_u = \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)(\llbracket M \rrbracket^{\lightning}_v \mid v.\texttt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([v \leftrightarrow u] \mid \llbracket B_i \rrbracket^{\lightning}_x))$$

$$
\begin{aligned}
[\![x]\!]^{\not\downarrow}_u &= x.\overline{\texttt{some}};[x \leftrightarrow u] \\
[\![\lambda x.M[\widetilde{x} \leftarrow x]]\!]^{\not\downarrow}_u &= u.\overline{\texttt{some}};u(x).[\![M[\widetilde{x} \leftarrow x]]\!]^{\not\downarrow}_u \\
[\![M\ B]\!]^{\not\downarrow}_u &= \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)([\![M]\!]^{\not\downarrow}_v \mid v.\texttt{some}_{u,\mathsf{fv}(B)};\overline{v}(x).([v \leftrightarrow u] \mid [\![B_i]\!]^{\not\downarrow}_x)) \\
[\![M[\widetilde{x} \leftarrow x]\langle\!\langle {}^{B}\!/_{x} \rangle\!\rangle]\!]^{\not\downarrow}_u &= \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x)([\![M[\widetilde{x} \leftarrow x]]\!]^{\not\downarrow}_u \mid [\![B_i]\!]^{\not\downarrow}_x) \\
[\![M[x_1, x_2 \leftarrow x]]\!]^{\not\downarrow}_u &= x.\overline{\texttt{some}}.\overline{x}(y_1).\Big(y_1.\texttt{some}_{\emptyset};y_1.\texttt{close} \,|\, x.\overline{\texttt{some}};x.\texttt{some}_{u,(\mathsf{fv}(M)\setminus\{x_1,x_2\})};x(x_1). \\
&\quad .x.\overline{\texttt{some}}.\overline{x}(y_2).\big(y_2.\texttt{some}_{\emptyset};y_2.\texttt{close} \,|\, x.\overline{\texttt{some}};x.\texttt{some}_{u,(\mathsf{fv}(M)\setminus\{x_2\})};x(x_2) \\
&\quad .x.\overline{\texttt{some}};\overline{x}(y).(y.\texttt{some}_{u,\mathsf{fv}(M)};y.\texttt{close};[\![M]\!]^{\not\downarrow}_u \mid x.\overline{\texttt{none}})\ \big)\Big) \\
[\![M[\leftarrow x]]\!]^{\not\downarrow}_u &= x.\overline{\texttt{some}}.\overline{x}(y).(y.\texttt{some}_{u,\mathsf{fv}(M)};y.\texttt{close};[\![M]\!]^{\not\downarrow}_u \mid x.\overline{\texttt{none}}) \\
[\![\wr M \wr \cdot B]\!]^{\not\downarrow}_x &= x.\texttt{some}_{\mathsf{fv}(\wr M \wr \cdot B)};x(y_i).x.\texttt{some}_{y_i,\mathsf{fv}(\wr M \wr \cdot B)};x.\overline{\texttt{some}};\overline{x}(x_i) \\
&\quad .(x_i.\texttt{some}_{\mathsf{fv}(M)};[\![M]\!]^{\not\downarrow}_{x_i} \mid [\![B]\!]^{\not\downarrow}_x \mid y_i.\overline{\texttt{none}}) \\
[\![\mathtt{1}]\!]^{\not\downarrow}_x &= x.\texttt{some}_{\emptyset};x(y).(y.\overline{\texttt{some}};y.\overline{\texttt{close}} \mid x.\texttt{some}_{\emptyset};x.\overline{\texttt{none}}) \\
[\![\mathtt{fail}^{x_1,\cdots,x_k}]\!]^{\not\downarrow}_u &= u.\overline{\texttt{none}} \mid x_1.\overline{\texttt{none}} \mid \cdots \mid x_k.\overline{\texttt{none}} \\
[\![M\{\!\!\{N/x\}\!\!\}]\!]^{\not\downarrow}_u &= (\nu x)([\![M]\!]^{\not\downarrow}_u \mid x.\texttt{some}_{\mathsf{fv}(N)};[\![N]\!]^{\not\downarrow}_x) \\
[\![\mathbb{M} + \mathbb{N}]\!]^{\not\downarrow}_u &= [\![\mathbb{M}]\!]^{\not\downarrow}_u \oplus [\![\mathbb{N}]\!]^{\not\downarrow}_u
\end{aligned}
$$

Figure 16: Translating $\widehat{\lambda}^{\not\downarrow}_{\oplus}$ expressions into $\mathsf{s}\pi$ processes.

Indeed, the main difference is the prefix '$x.\texttt{some}_{\mathsf{fv}(B_i)}$', which is present in process $[\![M\ B]\!]_u$ but is not explicit in process $[\![M\,B]\!]^{\not\downarrow}_u$. Intuitively, such a prefix denotes the dependency of B on M; because terms in $\widehat{\lambda}_{\oplus}$ do not fail, we can be certain that a corresponding confirming prefix '$x.\overline{\texttt{some}}$' will be available to spawn every $[\![B_i]\!]_x$. When moving to $\widehat{\lambda}^{\not\downarrow}_{\oplus}$, however, this is not the case: $[\![M]\!]^{\not\downarrow}_v$ may fail to provide the expected number of corresponding confirmations. For this reason, the role of prefix '$x.\texttt{some}_{\mathsf{fv}(B_i)}$' in $[\![M\ B]\!]_u$ is implemented within process $[\![B_i]\!]^{\not\downarrow}_x$. As a consequence, the translations for sharing terms ($M[\widetilde{x} \leftarrow x]$ and $M[\leftarrow x]$) and for bags ($\wr M \wr \cdot B$ and $\mathtt{1}$) are more involved in the case of failure.

With this motivation for $[\![M\,B]\!]^{\not\downarrow}_u$ in mind, we discuss the remaining entries in Fig. 16:

- Translations for x and $\lambda x.M[\widetilde{x} \leftarrow x]$ are exactly as in Fig. 15:

$$[\![x]\!]^{\not\downarrow}_u = x.\overline{\texttt{some}};[x \leftrightarrow u] \qquad [\![\lambda x.M[\widetilde{x} \leftarrow x]]\!]^{\not\downarrow}_u = u.\overline{\texttt{some}};u(x).[\![M[\widetilde{x} \leftarrow x]]\!]^{\not\downarrow}_u$$

- Similarly as $[\![M\,B]\!]^{\not\downarrow}_u$, discussed above, the translation of $M[\widetilde{x} \leftarrow x]\langle\!\langle {}^{B}\!/_{x} \rangle\!\rangle$ is more compact than the one in Fig. 15, because confirmations for each of the elements of the bag are

handled within their respective translations:

$$[\![M[\widetilde{x} \leftarrow x]\langle\!\langle B/x \rangle\!\rangle]\!]_u^{\ell} = \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x)([\![M[\widetilde{x} \leftarrow x]]\!]_u^{\ell} \mid [\![B_i]\!]_x^{\ell})$$

- As anticipated, the translation of $M[x_1, \ldots, x_k \leftarrow x]$ is more involved than before. For simplicity, let us discuss the representative case when $k = 2$ (two shared variables):

$$\begin{aligned}[\![M[x_1, x_2 \leftarrow x]]\!]_u^{\ell} = x.\overline{\texttt{some}}.\overline{x}(y_1).\Big(y_1.\texttt{some}_{\emptyset}; y_1.\texttt{close} \,|\, x.\overline{\texttt{some}}; x.\texttt{some}_{u,(\mathsf{fv}(M)\setminus\{x_1,x_2\})}; x(x_1).\\ x.\overline{\texttt{some}}.\overline{x}(y_2).\big(y_2.\texttt{some}_{\emptyset}; y_2.\texttt{close} \,|\, x.\overline{\texttt{some}}; x.\texttt{some}_{u,(\mathsf{fv}(M)\setminus\{x_2\})}; x(x_2).\\ x.\overline{\texttt{some}}; \overline{x}(y).(y.\texttt{some}_{u,\mathsf{fv}(M)}; y.\texttt{close}; [\![M]\!]_u^{\ell} \mid x.\overline{\texttt{none}})\ \big)\Big)\end{aligned}$$

  This process is meant to synchronize with the translation of a bag. After confirming the presence of a behavior on name x, an auxiliary name y_i is sent to signal that there are elements to be substituted. This name implements a short protocol that allows us to check for lack of resources in the bag. These steps on y_i are followed by another confirmation and also a request for confirmation of behavior along x; this represents that the name can fail in one of two ways, capturing the mutual dependency between M and the bag mentioned above. Once these two steps on x have succeeded, it is finally safe for the process to receive a name x_i. This process is repeated for each shared variable to ensure safe communication of the elements of the bag. The last line shows the very final step: a name y is communicated to ensure that there are no further elements in the bag; in such a case, y fails and the failure is propagated to $[\![M]\!]_u^{\ell}$. The prefix '$x.\overline{\texttt{none}}$' signals the end of the shared variables, and is meant to synchronize with the translation of $\texttt{1}$, the last element of the bag. If the bag has elements that still need to be synchronized then the failure along x is propagated to the remaining resources within the translation of the bag.
- The translation of $M[\leftarrow x]$ corresponds to the final step in the translation just discussed:

$$[\![M[\leftarrow x]]\!]_u^{\ell} = x.\overline{\texttt{some}}.\overline{x}(y).(y.\texttt{some}_{u,\mathsf{fv}(M)}; y.\texttt{close}; [\![M]\!]_u^{\ell} \mid x.\overline{\texttt{none}})$$

- The translation of the non-empty bag $\wr M \wr \cdot B$ is as follows:

$$\begin{aligned}[\![\wr M \wr \cdot B]\!]_x^{\ell} = x.\texttt{some}_{\mathsf{fv}(\wr M \wr \cdot B)}; x(y_i).x.\texttt{some}_{y_i,\mathsf{fv}(\wr M \wr \cdot B)}; x.\overline{\texttt{some}}; \overline{x}(x_i)\\ .(x_i.\texttt{some}_{\mathsf{fv}(M)}; [\![M]\!]_{x_i}^{\ell} \mid [\![B]\!]_x^{\ell} \mid y_i.\overline{\texttt{none}})\end{aligned}$$

  Notice how this process operates hand in hand with the translation of $M[x_1, \ldots, x_k \leftarrow x]$. The process first waits for its behavior to be confirmed; then, the auxiliary name y_i is received from the translation of $M[x_1, \ldots, x_k \leftarrow x]$. The name y_i fails immediately to signal that there are more resources in the bag. Name x then confirms its behavior and awaits its behavior to be confirmed. Subsequently, a name x_i is sent: this is the name on which the translation of M will be made available to the application. After that, name x is used in the translation of B, the rest of the bag.
- The translation of $\texttt{1}$ operates aligned with the translations just discussed, exploiting the fact that in fail-free reductions the last element of the bag must be $\texttt{1}$:

$$[\![\texttt{1}]\!]_x^{\ell} = x.\texttt{some}_{\emptyset}; x(y).(y.\overline{\texttt{some}}; y.\overline{\texttt{close}} \mid x.\texttt{some}_{\emptyset}; x.\overline{\texttt{none}})$$

  This process relays the information that the translated empty bag is no longer able to provide resources for further substitutions. It first waits upon a correct behavior followed by the reception of a name y. The process then confirms its behavior along y: this signals

that there are no further resources. Concurrently, name x waits for a confirmation of a behavior and ends with '$x.\overline{\texttt{none}}$', thus signaling the failure of producing further behaviors.
- The explicit failure term $\texttt{fail}^{x_1,\cdots,x_k}$ is not part of $\widehat{\lambda}_{\oplus}$ and so it was not covered in Fig. 15. Its translation is straightforward:

$$[\![\texttt{fail}^{x_1,\cdots,x_k}]\!]^{\ell}_{u} = u.\overline{\texttt{none}} \mid x_1.\overline{\texttt{none}} \mid \cdots \mid x_k.\overline{\texttt{none}}$$

  The failure term is translated as the non-availability of a behavior along name u, composed with the non-availability of sessions along the names/variables $x_1, \ldots, x_n$ encapsulated by the source failure term.
- The translations for $M\{\!|N/x|\!\}$ and $\mathbb{M} + \mathbb{N}$ are exactly as before:

$$[\![M\{\!|N/x|\!\}]\!]^{\ell}_{u} = (\nu x)([\![M]\!]^{\ell}_{u} \mid x.\texttt{some}_{\mathsf{fv}(N)}; [\![N]\!]^{\ell}_{x}) \qquad [\![\mathbb{M} + \mathbb{N}]\!]^{\ell}_{u} = [\![\mathbb{M}]\!]^{\ell}_{u} \oplus [\![\mathbb{N}]\!]^{\ell}_{u}$$

5.3.3. *Examples.* Before presenting the session types associated to our translation $[\![\cdot]\!]^{\ell}_{u}$, we present a series of examples that illustrate different possibilities in a step-by-step fashion:
- No failure: an explicit substitution that is provided an adequate amount of resources;
- Failure due to excess of resources in the bag;
- Failure due to lack of resources in the bag.

We first discuss the translation of a term in which there is no failure. In that follows, we refer to a specific reduction by adding a number as in, e.g., '$\longrightarrow_{[3]}$'.

Example 5.18 (No Failure)**.** Let us consider the well-formed $\widehat{\lambda}^{\ell}_{\oplus}$-term $N[x_1 \leftarrow x]\langle\!\langle (\!| M |\!) / x \rangle\!\rangle$, where, for simplicity, we assume that $\mathsf{fv}(N) \setminus \{x_1\} = \mathsf{fv}(M) = \emptyset$. As we have seen, $N[x_1 \leftarrow x]\langle\!\langle (\!| M |\!) / x \rangle\!\rangle \longrightarrow N\{\!|M/x|\!\}$. We discuss reduction steps for $[\![N[x_1 \leftarrow x]\langle\!\langle (\!| M |\!) / x \rangle\!\rangle]\!]^{\ell}_{u}$, highlighting in blue relevant prefixes. First, we have:

$$\begin{aligned}
[\![N[x_1 \leftarrow x]\langle\!\langle (\!| M |\!) / x \rangle\!\rangle]\!]^{\ell}_{u} &= (\nu x)([\![N[x_1 \leftarrow x]]\!]^{\ell}_{u} \mid [\![(\!| M |\!)]\!]^{\ell}_{x}) \\
&= (\nu x)\big(x.\overline{\texttt{some}}.\overline{x}(y_1).(y_1.\texttt{some}_{\emptyset}; y_1.\texttt{close} \mid x.\overline{\texttt{some}}; x.\texttt{some}_{u}; \\
&\qquad .x(x_1).x.\overline{\texttt{some}}; \overline{x}(y).(y.\texttt{some}_{u,x_1}; y.\texttt{close}; [\![N]\!]^{\ell}_{u} \mid x.\overline{\texttt{none}}) \ ) \\
&\qquad \mid x.\texttt{some}_{\emptyset}; x(y_1).x.\texttt{some}_{y_1}; x.\overline{\texttt{some}}; \overline{x}(x_1) \\
&\qquad .(x_1.\texttt{some}_{\emptyset}; [\![M]\!]^{\ell}_{x_1} \mid y_1.\overline{\texttt{none}} \mid x.\texttt{some}_{\emptyset}; x(y).(y.\overline{\texttt{some}}; y.\overline{\texttt{close}} \\
&\qquad \mid x.\texttt{some}_{\emptyset}; x.\overline{\texttt{none}}))\big)
\end{aligned}$$

A detailed description of the reduction steps follows:
- Reduction $\longrightarrow_{[1]}$ concerns the name x confirming its behavior (see highlighted prefixes above), and reduction $\longrightarrow_{[2]}$ concerns the communication of name y_1:

$$\begin{aligned}
[\![N[x_1 \leftarrow x]\langle\!\langle (\!| M |\!) / x \rangle\!\rangle]\!]^{\ell}_{u} &\longrightarrow_{[1]} (\nu x)(\overline{x}(y_1).\big(y_1.\texttt{some}_{\emptyset}; y_1.\texttt{close} \mid x.\overline{\texttt{some}}; x.\texttt{some}_{u}; x(x_1). \\
&\qquad .x.\overline{\texttt{some}}; \overline{x}(y).(y.\texttt{some}_{u,x_1}; y.\texttt{close}; [\![N]\!]^{\ell}_{u} \mid x.\overline{\texttt{none}}) \ ) \\
&\qquad \mid x(y_1).x.\texttt{some}_{y_1}; x.\overline{\texttt{some}}; \overline{x}(x_1).(x_1.\texttt{some}_{\emptyset}; [\![M]\!]^{\ell}_{x_1} \\
&\qquad \mid y_1.\overline{\texttt{none}} \mid x.\texttt{some}_{\emptyset}; x(y).(y.\overline{\texttt{some}}; y.\overline{\texttt{close}} \mid x.\texttt{some}_{\emptyset}; x.\overline{\texttt{none}}))) \\
&\longrightarrow_{[2]} (\nu x, y_1)(y_1.\texttt{some}_{\emptyset}; y_1.\texttt{close} \mid x.\overline{\texttt{some}}; x.\texttt{some}_{u}; x(x_1). \\
&\qquad .x.\overline{\texttt{some}}; \overline{x}(y).(y.\texttt{some}_{u,x_1}; y.\texttt{close}; [\![N]\!]^{\ell}_{u} \mid x.\overline{\texttt{none}}) \\
&\qquad \mid x.\texttt{some}_{y_1}; x.\overline{\texttt{some}}; \overline{x}(x_1).(x_1.\texttt{some}_{\emptyset}; [\![M]\!]^{\ell}_{x_1} \\
&\qquad \mid y_1.\overline{\texttt{none}} \mid x.\texttt{some}_{\emptyset}; x(y).(y.\overline{\texttt{some}}; y.\overline{\texttt{close}} \mid x.\texttt{some}_{\emptyset}; x.\overline{\texttt{none}}))) \ (:= P)
\end{aligned}$$

- Reduction $\longrightarrow_{[3]}$ concerns x confirming its behavior, which signals that there are variables free for substitution in the translated term. In the opposite direction, reduction $\longrightarrow_{[4]}$ signals that there are elements in the bag which are available for substitution in the translated term.

$$\begin{aligned} P &\longrightarrow_{[3]} (\nu x, y_1)(y_1.\mathtt{some}_\emptyset; y_1.\mathtt{close} \mid x.\mathtt{some}_u; x(x_1). \\ &\quad .x.\overline{\mathtt{some}}; \overline{x}(y).(y.\mathtt{some}_{u,x_1}; y.\mathtt{close}; [\![N]\!]^{\not z}_u \mid x.\overline{\mathtt{none}}) \\ &\quad \mid x.\overline{\mathtt{some}}; \overline{x}(x_1).(x_1.\mathtt{some}_\emptyset; [\![M]\!]^{\not z}_{x_1} \mid y_1.\overline{\mathtt{none}} \mid x.\mathtt{some}_\emptyset; x(y). \\ &\quad (y.\overline{\mathtt{some}}; y.\overline{\mathtt{close}} \mid x.\mathtt{some}_\emptyset; x.\overline{\mathtt{none}}))) \\ &\longrightarrow_{[4]} (\nu x, y_1)(y_1.\mathtt{some}_\emptyset; y_1.\mathtt{close} \mid x(x_1).x.\overline{\mathtt{some}}; \overline{x}(y).(y.\mathtt{some}_{u,x_1}; y.\mathtt{close}; \\ &\quad [\![N]\!]^{\not z}_u \mid x.\overline{\mathtt{none}}) \mid \overline{x}(x_1).(x_1.\mathtt{some}_\emptyset; [\![M]\!]^{\not z}_{x_1} \mid y_1.\overline{\mathtt{none}} \\ &\quad \mid x.\mathtt{some}_\emptyset; x(y).(y.\overline{\mathtt{some}}; y.\overline{\mathtt{close}} \mid x.\mathtt{some}_\emptyset; x.\overline{\mathtt{none}}))) \qquad (:= Q) \end{aligned}$$

- Given the confirmations in the previous two steps, reduction $\longrightarrow_{[5]}$ can now safely communicate a name x_1. This reduction synchronizes the shared variable x_1 with the first element in the bag.

$$\begin{aligned} Q &\longrightarrow_{[5]} (\nu x, y_1, x_1)(y_1.\mathtt{some}_\emptyset; y_1.\mathtt{close} \mid x.\overline{\mathtt{some}}; \overline{x}(y).(y.\mathtt{some}_{u,x_1}; y.\mathtt{close}; [\![N]\!]^{\not z}_u \\ &\quad \mid x.\overline{\mathtt{none}}) \mid x_1.\mathtt{some}_\emptyset; [\![M]\!]^{\not z}_{x_1} \mid y_1.\overline{\mathtt{none}} \mid x.\mathtt{some}_\emptyset; x(y).(y.\overline{\mathtt{some}}; y.\overline{\mathtt{close}} \\ &\quad \mid x.\mathtt{some}_\emptyset; x.\overline{\mathtt{none}})) \qquad (:= R) \end{aligned}$$

- Reduction $\longrightarrow_{[6]}$ concerns x confirming its behavior. At this point, we could have alternatively performed a reduction on name y_1. We chose to discuss all reductions on x first; thanks to confluence this choice has no effect on the overall behavior. Reduction $\longrightarrow_{[7]}$ communicates name y along x.

$$\begin{aligned} R &\longrightarrow_{[6]} (\nu x, y_1, x_1)(y_1.\mathtt{some}_\emptyset; y_1.\mathtt{close} \mid \overline{x}(y).(y.\mathtt{some}_{u,x_1}; y.\mathtt{close}; [\![N]\!]^{\not z}_u \\ &\quad \mid x.\overline{\mathtt{none}}) \mid x_1.\mathtt{some}_\emptyset; [\![M]\!]^{\not z}_{x_1} \mid y_1.\overline{\mathtt{none}} \mid x(y).(y.\overline{\mathtt{some}}; y.\overline{\mathtt{close}} \\ &\quad \mid x.\mathtt{some}_\emptyset; x.\overline{\mathtt{none}})) \\ &\longrightarrow_{[7]} (\nu x, y, y_1, x_1)(y_1.\mathtt{some}_\emptyset; y_1.\mathtt{close} \mid y.\mathtt{some}_{u,x_1}; y.\mathtt{close}; [\![N]\!]^{\not z}_u \mid x.\overline{\mathtt{none}} \\ &\quad \mid x_1.\mathtt{some}_\emptyset; [\![M]\!]^{\not z}_{x_1} \mid y_1.\overline{\mathtt{none}} \mid y.\overline{\mathtt{some}}; y.\overline{\mathtt{close}} \mid x.\mathtt{some}_\emptyset; x.\overline{\mathtt{none}}) \qquad (:= S) \end{aligned}$$

- Reduction $\longrightarrow_{[8]}$ cancels the behavior along x, meaning that there are no more free variables to synchronize with. Subsequently, reduction $\longrightarrow_{[9]}$ cancels the behavior along y_1: at the beginning, when y_1 was received, the encoded bag had the element M left to be synchronized; at this point, the failure on y_1 signals that the bag still has elements to be synchronized with.

$$\begin{aligned} S &\longrightarrow_{[8]} (\nu y, y_1, x_1)(y_1.\mathtt{some}_\emptyset; y_1.\mathtt{close} \mid y.\mathtt{some}_{u,x_1}; y.\mathtt{close}; [\![N]\!]^{\not z}_u \mid x_1.\mathtt{some}_\emptyset; [\![M]\!]^{\not z}_{x_1} \\ &\quad \mid y_1.\overline{\mathtt{none}} \mid y.\overline{\mathtt{some}}; y.\overline{\mathtt{close}}) \\ &\longrightarrow_{[9]} (\nu y, x_1)(y.\mathtt{some}_{u,x_1}; y.\mathtt{close}; [\![N]\!]^{\not z}_u \mid x_1.\mathtt{some}_\emptyset; [\![M]\!]^{\not z}_{x_1} x \mid y.\overline{\mathtt{some}}; y.\overline{\mathtt{close}}) \qquad (:= T) \end{aligned}$$

- Finally, reductions $\longrightarrow_{[10]}$ and $\longrightarrow_{[11]}$ concern name y: the former signals that the bag has no more elements to be synchronized for substitution; the latter closes the session, as it has served its purpose of correctly synchronizing the translated term. The resulting process corresponds to the translation of $N\{\!\{M/x\}\!\}$.

$$\begin{aligned} T &\longrightarrow_{[10]} (\nu y, x_1)(y.\mathtt{close}; [\![N]\!]^{\not z}_u \mid x_1.\mathtt{some}_\emptyset; [\![M]\!]^{\not z}_{x_1} \mid y.\overline{\mathtt{close}}) \\ &\longrightarrow_{[11]} (\nu x_1)([\![N]\!]^{\not z}_u \mid x_1.\mathtt{some}_\emptyset; [\![M]\!]^{\not z}_{x_1}) = [\![N\{\!\{M/x\}\!\}]\!]^{\not z}_u \end{aligned}$$

We now discuss the translation of a term that fails due to an excess of resources.

Example 5.19 (Excess of Resources)**.** Let us consider the well-formed $\widehat{\lambda}^{\lightning}_{\oplus}$-term that does not share occurrences of x, i.e., $N[\leftarrow x]\langle\!\langle (\!| M |\!)/x \rangle\!\rangle$, where M, N are closed (i.e. $\mathsf{fv}(N) = \mathsf{fv}(M) = \emptyset$). This term's translation is:

$$\begin{aligned}[\![N[\leftarrow x]\langle\!\langle (\!| M |\!)/x \rangle\!\rangle]\!]^{\lightning}_u &= (\nu x)([\![N[\leftarrow x]]\!]^{\lightning}_u \mid [\![(\!| M |\!)]\!]^{\lightning}_x) \\ &= (\nu x)(x.\overline{\texttt{some}}.\overline{x}(y_1).(y_1.\texttt{some}_u; y_1.\texttt{close}; [\![N]\!]^{\lightning}_u \mid x.\overline{\texttt{none}}) \mid \\ &\quad x.\texttt{some}_\emptyset; x(y_1).x.\texttt{some}_{y_1}; x.\overline{\texttt{some}}; \overline{x}(x_i).(x_i.\texttt{some}_\emptyset; [\![M]\!]^{\lightning}_{x_i} \mid [\![\mathbf{1}]\!]^{\lightning}_x \mid y_1.\overline{\texttt{none}}))\end{aligned}$$

- Reductions $\longrightarrow_{[1]}$ and $\longrightarrow_{[2]}$ follow as in Example 5.18.

$$\begin{aligned}[\![N[\leftarrow x]\langle\!\langle (\!| M |\!)/x \rangle\!\rangle]\!]^{\lightning}_u &\longrightarrow_{[1]} (\nu x)(\overline{x}(y_1).(y_1.\texttt{some}_u; y_1.\texttt{close}; [\![N]\!]^{\lightning}_u \mid x.\overline{\texttt{none}}) \mid \\ &\quad x(y_1).x.\texttt{some}_{y_1}; x.\overline{\texttt{some}}; \overline{x}(x_i).(x_i.\texttt{some}_\emptyset; [\![M]\!]^{\lightning}_{x_i} \mid [\![\mathbf{1}]\!]^{\lightning}_x \mid y_1.\overline{\texttt{none}})) \\ &\longrightarrow_{[2]} (\nu x, y_1)(y_1.\texttt{some}_u; y_1.\texttt{close}; [\![N]\!]^{\lightning}_u \mid x.\overline{\texttt{none}} \mid \\ &\quad x.\texttt{some}_{y_1}; x.\overline{\texttt{some}}; \overline{x}(x_i).(x_i.\texttt{some}_\emptyset; [\![M]\!]^{\lightning}_{x_i} \mid [\![\mathbf{1}]\!]^{\lightning}_x \mid y_1.\overline{\texttt{none}})) \qquad (:= P)\end{aligned}$$

  Notice how the translation of the term first triggers the failure: prefix $x.\overline{\texttt{none}}$ (highlighted in red) signals that there are no (more) occurrences of x within the process; nevertheless, the translation of the bag is still trying to communicate the translation of M. This failure along x causes the chain reaction of the failure along y_1, which eventually triggers across the translation of N.
- Reduction $\longrightarrow_{[3]}$ differs from $\longrightarrow_{[3]}$ in Example 5.18, as the translation of the shared variable is empty, we abort along the name x; as the translated bag still contains elements to synchronize, the abortion of the bag triggers that failure of the dependant name y_1.

$$\begin{aligned}P &\longrightarrow_{[3]} (\nu y_1)(y_1.\texttt{some}_u; y_1.\texttt{close}; [\![N]\!]^{\lightning}_u \mid \longrightarrow y_1.\overline{\texttt{none}}) \\ &\longrightarrow_{[4]} u.\overline{\texttt{none}} = [\![\texttt{fail}^{\emptyset}]\!]^{\lightning}_u\end{aligned}$$

- Reduction $\longrightarrow_{[4]}$ differs from that of $\longrightarrow_{[9]}$ and $\longrightarrow_{[10]}$ from Example 5.18: the name y_1 fails signaling that there was an element in the bag that was to be sent; as the translation of the term N is guarded by the confirmation along y_1, it aborts.

Finally, we illustrate how $[\![\,\cdot\,]\!]^{\lightning}_u$ acts on a term that fails due to lack of resources in a bag.

Example 5.20 (Lack of Resources)**.** Consider the well-formed $\widehat{\lambda}^{\lightning}_{\oplus}$-term $N[x_1 \leftarrow x]\langle\!\langle \mathbf{1}/x \rangle\!\rangle$, where N is a closed term (i.e. $\mathsf{fv}(N) = \emptyset$). This term's translation is:

$$\begin{aligned}[\![N[x_1 \leftarrow x]\langle\!\langle \mathbf{1}/x \rangle\!\rangle]\!]^{\lightning}_u &= (\nu x)([\![N[x_1 \leftarrow x]]\!]^{\lightning}_u \mid [\![\mathbf{1}]\!]^{\lightning}_x) \\ &= (\nu x)(x.\overline{\texttt{some}}.\overline{x}(y_1).(y_1.\texttt{some}_\emptyset; y_1.\texttt{close} \mid x.\overline{\texttt{some}}; x.\texttt{some}_u; \\ &\quad x(x_1).x.\overline{\texttt{some}}; \overline{x}(y_2).(y_2.\texttt{some}_{u,x_1}; y_2.\texttt{close}; [\![N]\!]^{\lightning}_u \mid x.\overline{\texttt{none}})) \mid \\ &\quad x.\texttt{some}_\emptyset; x(y_1).(y_1.\overline{\texttt{some}}; y_1.\overline{\texttt{close}} \mid x.\texttt{some}_\emptyset; x.\overline{\texttt{none}})) \qquad (:= P)\end{aligned}$$

Notice how the translation of the empty bag $\mathbf{1}$ triggers the failure: prefix '$x.\overline{\texttt{none}}$' signals that there are no (more) elements in the bag; however, the translated term aims to synchronize, as it (still) requires resources.

- Reductions $\longrightarrow_{[1]}$ and $\longrightarrow_{[2]}$ follow from Example 5.18.

$$\begin{aligned} P \longrightarrow_{[1]}\ & (\nu x)(\overline{x}(y_1).(y_1.\mathtt{some}_{\emptyset}; y_1.\mathtt{close} \mid x.\overline{\mathtt{some}}; x.\mathtt{some}_u; x(x_1). \\ & \quad x.\overline{\mathtt{some}}; \overline{x}(y_2).(y_2.\mathtt{some}_{u,x_1}; y_2.\mathtt{close}; [\![N]\!]^{\lightning}_u \mid x.\overline{\mathtt{none}})\ ) \mid \\ & \quad x(y_1).(y_1.\overline{\mathtt{some}}; y_1.\overline{\mathtt{close}} \mid x.\mathtt{some}_{\emptyset}; x.\overline{\mathtt{none}})) \\ \longrightarrow_{[2]}\ & (\nu x, y_1)(y_1.\mathtt{some}_{\emptyset}; y_1.\mathtt{close} \mid x.\overline{\mathtt{some}}; x.\mathtt{some}_u; x(x_1). \\ & \quad x.\overline{\mathtt{some}}; \overline{x}(y_2).(y_2.\mathtt{some}_{u,x_1}; y_2.\mathtt{close}; [\![N]\!]^{\lightning}_u \mid x.\overline{\mathtt{none}}) \mid \\ & \quad y_1.\overline{\mathtt{some}}; y_1.\overline{\mathtt{close}} \mid x.\mathtt{some}_{\emptyset}; x.\overline{\mathtt{none}}) \end{aligned}$$

- Reductions $\longrightarrow_{[3]}$ and $\longrightarrow_{[4]}$ follow from that of $\longrightarrow_{[9]}$ and $\longrightarrow_{[10]}$ in Example 5.18; as the term contains the element x_1 for synchronization, the encoding of N is not guarded by y_1.

$$\begin{aligned} Q \longrightarrow_{[3]}\ & (\nu x, y_1)(y_1.\mathtt{close} \mid x.\overline{\mathtt{some}}; x.\mathtt{some}_u; x(x_1). \\ & \quad x.\overline{\mathtt{some}}; \overline{x}(y_2).(y_2.\mathtt{some}_{u,x_1}; y_2.\mathtt{close}; [\![N]\!]^{\lightning}_u \mid x.\overline{\mathtt{none}}) \mid \\ & \quad y_1.\overline{\mathtt{close}} \mid x.\mathtt{some}_{\emptyset}; x.\overline{\mathtt{none}}) \\ \longrightarrow_{[4]}\ & (\nu x)(x.\overline{\mathtt{some}}; x.\mathtt{some}_u; x(x_1).x.\overline{\mathtt{some}}; \overline{x}(y_2).(y_2.\mathtt{some}_{u,x_1}; y_2.\mathtt{close}; \\ & \quad [\![N]\!]^{\lightning}_u \mid x.\overline{\mathtt{none}}) \mid x.\mathtt{some}_{\emptyset}; x.\overline{\mathtt{none}}) \\ \longrightarrow_{[5]}\ & (\nu x)(x.\mathtt{some}_u; x(x_1).x.\overline{\mathtt{some}}; \overline{x}(y_2).(y_2.\mathtt{some}_{u,x_1}; y_2.\mathtt{close}; [\![N]\!]^{\lightning}_u \mid x.\overline{\mathtt{none}}) \mid x.\overline{\mathtt{none}}) \\ \longrightarrow_{[6]}\ & u.\overline{\mathtt{none}} = [\![\mathtt{fail}^{\emptyset}]\!]^{\lightning}_u \end{aligned}$$

- Reduction $\longrightarrow_{[5]}$ follows from reduction $\longrightarrow_{[3]}$ in Example 5.18.
- Reduction $\longrightarrow_{[6]}$ differs from that of $\longrightarrow_{[4]}$ from Example 5.18: the bag contains no elements, and signals this by aborting along the name x; still, the term expects to receive an element of the bag, and prematurely aborts.

Translating Types. In describing our translation $[\![\cdot]\!]^{\lightning}_{-}$ we have informally referred to (non-deterministic) session protocols in $\mathsf{s}\pi$ that implement (non-deterministic) expressions in $\widehat{\lambda}^{\lightning}_{\oplus}$. We are actually able to make these intuitions precise and give a translation of intersection types (for $\widehat{\lambda}^{\lightning}_{\oplus}$, cf. Def. 2.15) into session types (for $\mathsf{s}\pi$, cf. Def. 4.4). This provides the protocol-oriented interpretation of intersections mentioned earlier. Intuitively speaking, given an intersection type π, we will have a corresponding session type $[\![\pi]\!]^{\lightning}$ that determines a protocol tied to the evaluation of a (fail-prone, non-deterministic) expression with type π.

Definition 5.21 (From $\widehat{\lambda}^{\lightning}_{\oplus}$ into $\mathsf{s}\pi$: Types)**.** The translation $[\![\cdot]\!]^{\lightning}$ on types is defined in Fig. 17. Let $\Gamma = x_1 : \sigma_1, \cdots, x_m : \sigma_k, v_1 : \pi_1, \cdots, v_n : \pi_n$ be as in Def. 3.12.

For some strict types $\tau_1, \cdots, \tau_n$ and $i_1, \cdots, i_n \geq 0$ we define:

$$[\![\Gamma]\!]^{\lightning} = x_1 : \&\overline{[\![\sigma_1]\!]^{\lightning}}, \cdots, x_k : \&\overline{[\![\sigma_k]\!]^{\lightning}}, v_1 : \&\overline{[\![\pi_1]\!]^{\lightning}_{(\tau_1,i_1)}}, \cdots, v_n : \&\overline{[\![\pi_n]\!]^{\lightning}_{(\tau_n,i_n)}}$$

As we will see, given a well-formedness judgement $\Gamma \models \mathbb{M} : \tau$, with the translations on types and assignments defined above, we will have $[\![\mathbb{M}]\!]^{\lightning}_u \vdash [\![\Gamma]\!]^{\lightning}, u : [\![\tau]\!]^{\lightning}$; this is the content of the *type preservation* property (Theorem 5.23).

The translation of types in Fig. 17 leverages non-deterministic session protocols (typed with '&') to represent non-deterministic fetching and fail-prone evaluation in $\widehat{\lambda}^{\lightning}_{\oplus}$. Notice that the translation of the multiset type π depends on two arguments (a strict type τ and a number $i \geq 0$) which are left unspecified above, but are appropriately specified in Proposition 5.22. This is crucial to represent mismatches in $\widehat{\lambda}^{\lightning}_{\oplus}$ (i.e., sources of failures) as

$$
\begin{aligned}
[\![\mathbf{unit}]\!]^{\not\downarrow} &= \&\mathbf{1} \\
[\![\pi \to \tau]\!]^{\not\downarrow} &= \&((\overline{[\![\pi]\!]^{\not\downarrow}_{(\sigma,i)}}) \parr [\![\tau]\!]^{\not\downarrow}) \quad \text{(for some strict type } \sigma\text{, with } i \geq 0) \\
[\![\sigma \wedge \pi]\!]^{\not\downarrow}_{(\tau,i)} &= \overline{\&((\oplus\bot) \otimes (\& \oplus ((\&\overline{[\![\sigma]\!]^{\not\downarrow}}) \parr (\overline{[\![\pi]\!]^{\not\downarrow}_{(\tau,i)}}))))} \\
&= \oplus((\&\mathbf{1}) \parr (\oplus\&((\oplus[\![\sigma]\!]^{\not\downarrow}) \otimes ([\![\pi]\!]^{\not\downarrow}_{(\tau,i)})))) \\
[\![\omega]\!]^{\not\downarrow}_{(\sigma,i)} &= \begin{cases} \overline{\&((\oplus\bot) \otimes (\& \oplus \bot)))} & \text{if } i = 0 \\ \overline{\&((\oplus\bot) \otimes (\& \oplus ((\&\overline{[\![\sigma]\!]^{\not\downarrow}}) \parr (\overline{[\![\omega]\!]^{\not\downarrow}_{(\sigma,i-1)}}))))} & \text{if } i > 0 \end{cases}
\end{aligned}
$$

Figure 17: Translating intersection types as session types.

typable processes in $\mathsf{s}\pi$. For instance, in Fig. 7, Rule [FS:app] admits a mismatch between $\sigma^j \to \tau$ and σ^k, for it allows $j \neq k$. In our proof of type preservation, these two arguments are instantiated appropriately, enabling typability as session-typed processes.

We are now ready to consider correctness for $[\![\cdot]\!]^{\not\downarrow}_u$, in the sense of Def. 5.1. First, the compositionality property follows directly from Fig. 16. In the following sections, we state the remaining properties in Def. 5.1: type preservation, operational correspondence, and success sensitiveness.

5.3.4. *Type Preservation.* We prove that our translation from $\widehat{\lambda}^{\not\downarrow}_{\oplus}$ to $\mathsf{s}\pi$ maps well-formed $\widehat{\lambda}^{\not\downarrow}_{\oplus}$ expressions to session-typed processes in $\mathsf{s}\pi$. First, we show that translated multiset types can be "lengthened" by setting appropriate parameters to the encoding.

Proposition 5.22. *Suppose σ^j and σ^k are arbitrary strict types (Def. 2.15), for some $j, k \geq 0$. Following Fig. 17, consider their encoding into session types $[\![\sigma^j]\!]^{\not\downarrow}_{(\tau_1,m)}$ and $[\![\sigma^k]\!]^{\not\downarrow}_{(\tau_2,n)}$, respectively, where τ_1, τ_2 are strict types and $n, m \geq 0$.*
We have $[\![\sigma^j]\!]^{\not\downarrow}_{(\tau_1,m)} = [\![\sigma^k]\!]^{\not\downarrow}_{(\tau_2,n)}$ under the following conditions:

(1) *If $j > k$ then we take τ_1 to be an arbitrary strict type and $m = 0$; also, we take τ_2 to be σ and $n = j - k$.*
(2) *If $j < k$ then we take τ_1 to be σ and $m = k - j$; also, we take τ_2 to be an arbitrary strict type and $n = 0$.*
(3) *Otherwise, if $j = k$ then we take $m = n = 0$. Also, τ_1, τ_2 are arbitrary strict types.*

Proof. Immediate by unfolding the translation. The full analysis can be found in App. D.1. □

Given Proposition 5.22 we now show that the translation preserves types:

Theorem 5.23 (Type Preservation for $[\![\cdot]\!]^{\not\downarrow}_u$)**.** *Let B and $\mathbb{M}$ be a bag and an expression in $\widehat{\lambda}^{\not\downarrow}_{\oplus}$, respectively.*

(1) *If $\Gamma^\dagger \models B : \pi$ then $[\![B]\!]^{\not\downarrow}_u \vdash [\![\Gamma^\dagger]\!]^{\not\downarrow}, u : [\![\pi]\!]^{\not\downarrow}_{(\sigma,i)}$, for some strict type σ and index $i \geq 0$.*
(2) *If $\Gamma^\dagger \models \mathbb{M} : \tau$ then $[\![\mathbb{M}]\!]^{\not\downarrow}_u \vdash [\![\Gamma^\dagger]\!]^{\not\downarrow}, u : [\![\tau]\!]^{\not\downarrow}$.*

Proof. By mutual induction on the typing derivation of B and $\mathbb{M}$, with an analysis of the last rule applied in $\Gamma \models B : \pi$ and in $\Gamma \models \mathbb{M} : \tau$. One key aspect of this proof is the application of Proposition 5.22 to ensure duality of types. Intuitively, the conditions given by Proposition 5.22 are used to instantiate the parameters in the encoding of intersection types, so as to ensure that when intersection types have different types the smaller type can be correctly "padded" to match the size of the larger type—Example 5.24, given below, illustrates this padding. The full proof can be found in App. D.1. □

Example 5.24 (Parameters in the encoding of types)**.** We give the dual types when encoding intersection types, namely the case of $[\![\sigma \wedge \pi]\!]^{\lightning}_{(\sigma,i)}$, to express the encoding of intersection typed behavior into session typed behavior. The application of dual types is most evident in the application of a bag into an abstraction: the bag providing the intersection type and the abstraction consuming it. In session types the interaction between these is expressed by dual session types where one channel provides a behavior and and the dual channel provides the dual session type behavior via the cut rule. Let us consider the term $(\lambda x.M[x_1, x_2 \leftarrow x])B$ typed with the well-formedness rules by:

$$[\texttt{FS:app}]\ \frac{\Gamma \models \lambda x.M[x_1, x_2 \leftarrow x] : (\sigma \wedge \sigma) \to \tau \quad \Delta \models B : \sigma^k}{\Gamma, \Delta \models (\lambda x.M[x_1, x_2 \leftarrow x])B : \tau}$$

When applying the translation of Fig. 16 to the term we obtain:

$$\bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)([\![\lambda x.M[x_1, x_2 \leftarrow x]]\!]^{\lightning}_{v} \mid v.\texttt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([v \leftrightarrow u] \mid [\![B_i]\!]^{\lightning}_{x}))$$

By appealing to Type Preservation (Theorem 5.23) we obtain both $[\![\lambda x.M[x_1, x_2 \leftarrow x]]\!]^{\lightning}_{v} \vdash [\![\Gamma]\!]^{\lightning}, v : [\![(\sigma \wedge \sigma) \to \tau]\!]^{\lightning}$ and $[\![B]\!]^{\lightning}_{x} \vdash [\![\Delta]\!]^{\lightning}, x : [\![\sigma^k]\!]^{\lightning}_{(\delta_2,i_2)}$. We give the typing for one non-deterministic branch where we take an arbitrary permutation of B is as follows by applying the rules of Fig. 11 and that Π_1 is derived to be:

$$[\texttt{T}\oplus^{\texttt{x}}_{\texttt{w}}]\ \frac{[\texttt{T}\otimes]\ \dfrac{[\texttt{Tid}]\ \dfrac{}{[v \leftrightarrow u] \vdash v : \overline{[\![\tau]\!]^{\lightning}}, u : [\![\tau]\!]^{\lightning}} \qquad [\![B]\!]^{\lightning}_{x} \vdash [\![\Delta]\!]^{\lightning}, x : [\![\sigma^k]\!]^{\lightning}_{(\delta_2,i_2)}}{\overline{v}(x).([v \leftrightarrow u] \mid [\![B]\!]^{\lightning}_{x}) \vdash [\![\Delta]\!]^{\lightning}, v : [\![\sigma^k]\!]^{\lightning}_{(\delta_2,i_2)} \parr \overline{[\![\tau]\!]^{\lightning}}, u : [\![\tau]\!]^{\lightning}}}{v.\texttt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([v \leftrightarrow u] \mid [\![B]\!]^{\lightning}_{x}) \vdash [\![\Delta]\!]^{\lightning}, v : \overline{[\![(\sigma^k) \to \tau]\!]^{\lightning}}, u : [\![\tau]\!]^{\lightning}}$$

Hence we obtain the derivation:

$$[\texttt{Tcut}]\ \frac{[\![\lambda x.M[x_1, x_2 \leftarrow x]]\!]^{\lightning}_{v} \vdash [\![\Gamma]\!]^{\lightning}, v : [\![(\sigma \wedge \sigma) \to \tau]\!]^{\lightning} \qquad \Pi_1}{(\nu v)([\![\lambda x.M[x_1, x_2 \leftarrow x]]\!]^{\lightning}_{v} \mid v.\texttt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([v \leftrightarrow u] \mid [\![B]\!]^{\lightning}_{x}) \vdash [\![\Gamma]\!]^{\lightning}, [\![\Delta]\!]^{\lightning}, u : [\![\tau]\!]^{\lightning}}$$

Now we shall focus on the typing of the channel v and x in this process as these channel describes the behavior of the encoded intersection type which we are trying to match via duality. By the translation on types from Fig. 17 we have that

$$[\![(\sigma \wedge \sigma) \to \tau]\!]^{\lightning} = \&((\overline{[\![(\sigma \wedge \sigma)]\!]^{\lightning}_{(\delta_1,i_1)}}) \parr [\![\tau]\!]^{\lightning})$$

- When $B = \texttt{1}$ we have derivation:

$$[\![\texttt{1}]\!]^{\lightning}_{x} \models [\![\Delta]\!]^{\lightning}, x : [\![\omega]\!]^{\lightning}_{(\delta_2,i_2)}$$

$$
\begin{array}{rll}
M[\leftarrow x]\langle\!\langle \mathbf{1}/x\rangle\!\rangle & \equiv_\lambda M & \\
MB\{\!|N/x|\!\} & \equiv_\lambda (M\{\!|N/x|\!\})B & \text{with } x \notin \mathsf{fv}(B) \\
M\{\!|N_2/y|\!\}\{\!|N_1/x|\!\} & \equiv_\lambda M\{\!|N_1/x|\!\}\{\!|N_2/y|\!\} & \text{with } x \notin \mathsf{fv}(N_2), y \notin \mathsf{fv}(N_1) \\
MA[\widetilde{x} \leftarrow x]\langle\!\langle B/x\rangle\!\rangle & \equiv_\lambda (M[\widetilde{x} \leftarrow x]\langle\!\langle B/x\rangle\!\rangle)A & \text{with } x_i \in \widetilde{x} \Rightarrow x_i \notin \mathsf{fv}(A) \\
M[\widetilde{y} \leftarrow y]\langle\!\langle A/y\rangle\!\rangle[\widetilde{x} \leftarrow x]\langle\!\langle B/x\rangle\!\rangle & \equiv_\lambda (M[\widetilde{x} \leftarrow x]\langle\!\langle B/x\rangle\!\rangle)[\widetilde{y} \leftarrow y]\langle\!\langle A/y\rangle\!\rangle & \text{with } x_i \in \widetilde{x} \Rightarrow x_i \notin \mathsf{fv}(A) \\
C[M] & \equiv_\lambda C[M'] & \text{with } M \equiv_\lambda M' \\
D[\mathbb{M}] & \equiv_\lambda D[\mathbb{M}'] & \text{with } \mathbb{M} \equiv_\lambda \mathbb{M}'
\end{array}
$$

Figure 18: Congruence in $\widehat{\lambda}^{\lightning}_{\oplus}$.

To obtain duality from Rule [Tcut] we must have that $[\![\sigma^2]\!]^{\lightning}_{(\delta_1,i_1)} = [\![\omega]\!]^{\lightning}_{(\delta_2,i_2)}$. By Proposition 5.22 we can take δ_1 to be an arbitrary strict type, $i_1 = 0$, $i_2 = 2$, $\delta_2 = \sigma$. We have:

$$
\begin{aligned}
[\![\omega]\!]^{\lightning}_{(\sigma,2)} &= \overline{\&((\oplus\bot) \otimes (\& \oplus ((\&\overline{[\![\sigma]\!]^{\lightning}}) \parr (\overline{[\![\omega]\!]^{\lightning}_{(\sigma,1)}})))} \\
&= \overline{\&((\oplus\bot) \otimes (\& \oplus ((\&\overline{[\![\sigma]\!]^{\lightning}}) \parr (\&((\oplus\bot) \otimes (\& \oplus ((\&\overline{[\![\sigma]\!]^{\lightning}}) \parr (\overline{[\![\omega]\!]^{\lightning}_{(\sigma,0)}}))))))))} \\
&= [\![\sigma^2]\!]^{\lightning}_{(\delta_1,i_1)}
\end{aligned}
$$

- When $B = \wr N_1, N_2 \wr$ we have derivation:

$$[\![\wr N_1, N_2 \wr]\!]^{\lightning}_x \models [\![\Delta]\!]^{\lightning}, x : [\![\sigma^2]\!]^{\lightning}_{(\delta_2,i_2)}$$

To obtain duality from Rule [Tcut] we must have that $[\![\sigma^2]\!]^{\lightning}_{(\delta_1,i_1)} = [\![\sigma^2]\!]^{\lightning}_{(\delta_2,i_2)}$. By Proposition 5.22 we can take δ_1 and δ_2 to be an arbitrary strict type and $i_1 = i_2 = 0$. We then obtain $[\![\sigma^2]\!]^{\lightning}_{(\delta_1,0)} = [\![\sigma^2]\!]^{\lightning}_{(\delta_2,0)}$, as $[\![\omega]\!]^{\lightning}_{(\delta_1,0)} = [\![\omega]\!]^{\lightning}_{(\delta_2,0)}$ for any two strict types δ_1, δ_2.

- When $B = \wr N_1, N_2, N_3 \wr$ we have derivation:

$$[\![\wr N_1, N_2, N_3 \wr]\!]^{\lightning}_x \models [\![\Delta]\!]^{\lightning}, x : [\![\sigma^3]\!]^{\lightning}_{(\delta_2,i_2)}$$

To obtain duality from Rule [Tcut] we must have that $[\![\sigma^2]\!]^{\lightning}_{(\delta_1,i_1)} = [\![\sigma^3]\!]^{\lightning}_{(\delta_2,i_2)}$. By Proposition 5.22 we can take δ_2 to be an arbitrary strict type, $i_2 = 0$, $i_1 = 2$, $\delta_1 = \sigma$. Then the case proceeds similarly to when $B = \mathtt{1}$.

5.3.5. *Operational Correspondence: Completeness and Soundness.* We now state our operational correspondence results (completeness and soundness, cf. Fig. 19).

A Congruence. We will identify some $\widehat{\lambda}^{\lightning}_{\oplus}$-terms such as $M[\leftarrow x]\langle\!\langle \mathbf{1}/x\rangle\!\rangle$ and M. The identification is natural, as the former is a term M with no occurrences of x in which x is going to be replaced with $\mathtt{1}$, which clearly describes a substitution that "does nothing", and would result in M itself. With this intuition, other terms are identified via a *congruence* (denoted $\equiv_\lambda$) on terms and expressions that is formally defined in Fig. 18.

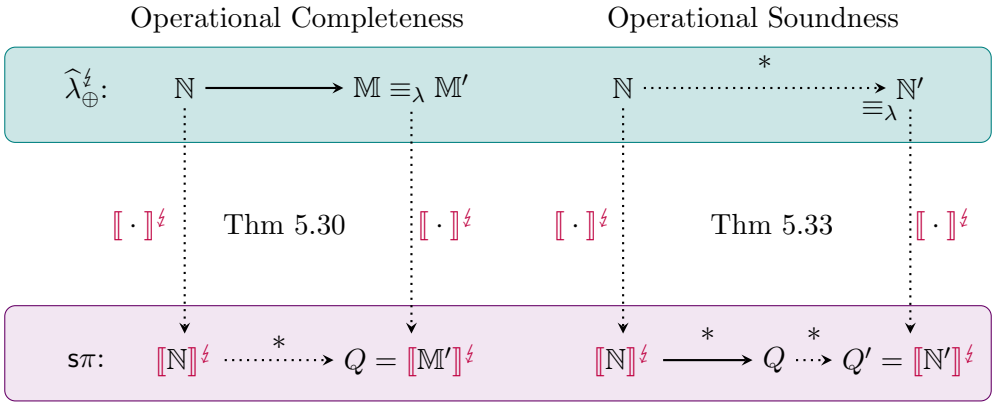


Figure 19: Operational Correspondence for $[\![\cdot]\!]^{\lightning}$

Example 5.25 (Cont. Example 3.20)**.** We illustrate the congruence in case of failure:

$$\begin{aligned}(\lambda x.x_1[x_1 \leftarrow x])\{\!\{\mathtt{fail}^{\emptyset}[\leftarrow y]\langle\!\langle 1/y\rangle\!\rangle\}\!\} &\longrightarrow_{[\mathtt{RS:Beta}]} x_1[x_1 \leftarrow x]\langle\!\langle \{\!\{\mathtt{fail}^{\emptyset}[\leftarrow y]\langle\!\langle 1/y\rangle\!\rangle\}\!\}/x\rangle\!\rangle \\ &\longrightarrow_{[\mathtt{RS:Ex\text{-}Sub}]} x_1\langle\!|\mathtt{fail}^{\emptyset}[\leftarrow y]\langle\!\langle 1/y\rangle\!\rangle/x_1|\!\rangle \\ &\longrightarrow_{[\mathtt{RS:Lin\text{-}Fetch}]} \mathtt{fail}^{\emptyset}[\leftarrow y]\langle\!\langle 1/y\rangle\!\rangle \\ &\equiv_{\lambda} \mathtt{fail}^{\emptyset}\end{aligned}$$

In the last step, Rule $[\mathtt{RS:Cons}_2]$ cannot be applied: y is sharing with no shared variables and the explicit substitution involves the bag 1.

Theorem 5.26 (Consistency Stability Under $\equiv$)**.** *Let $\mathbb{M}$ be a consistent $\widehat{\lambda}^{\lightning}_{\oplus}$-expression. If $\mathbb{M} \equiv \mathbb{M}'$ then $\mathbb{M}'$ is consistent.*

Proof. By induction on the structure of $\mathbb{M}$; see Appendix D.2 for details. □

Definition 5.27 (Partially Open Terms)**.** We say that a $\widehat{\lambda}^{\lightning}_{\oplus}$-term M is *partially open* if $\forall x \in \mathsf{fv}(M)$ (cf. Def. 3.3) implies that x is not a sharing variable.

Notice that the class of open terms (no conditions on free variables) subsumes the class of partially open terms, which in turn subsumes the class of closed terms. Consider the following example.

Example 5.28 (Partially Open Terms)**.** We give three examples of well-formed $\widehat{\lambda}^{\lightning}_{\oplus}$-terms:

$$M_1 = \lambda x.x_1[x_1 \leftarrow x] \qquad M_2 = \lambda x.(x_1\{\!\{y\}\!\})[x_1 \leftarrow x] \qquad M_3 = (x_1\{\!\{y\}\!\})[x_1 \leftarrow x]$$

Here the only closed term is M_1 as M_2 has one free variable (i.e., y) and M_3 has two free variables (y and x). While M_2 is partially open, M_3 is not because x is a sharing variable.

The following proposition will be used in the proof of operational completeness (Theorem 5.30) and operational soundness (Theorem 5.33). The proposition relies on well-formed partially open terms; however, in the proof of operational correspondence we only consider closed terms rather then partially open terms.

Proposition 5.29. *Suppose N is a well-formed, partially open $\widehat{\lambda}^{\natural}_{\oplus}$-term with $\mathsf{head}(N) = x$. Then, there exist an index set I, names $\widetilde{y}$ and n, and processes P_i such that the following four conditions hold:*

(1)
$$[\![N]\!]^{\natural}_{u} \longrightarrow^{*} \bigoplus_{i\in I}(\nu\widetilde{y})([\![x]\!]^{\natural}_{n} \mid P_i)$$

(2) *There exists a $\widehat{\lambda}^{\natural}_{\oplus}$-term N' such that $N \equiv_{\lambda} N'$ and:*
$$[\![N']\!]^{\natural}_{u} = \bigoplus_{i\in I}(\nu\widetilde{y})([\![x]\!]^{\natural}_{n} \mid P_i)$$

(3) *For any well-formed and partially open $\widehat{\lambda}^{\natural}_{\oplus}$-term M:*
$$[\![N\{\!|M/x|\!\}]\!]^{\natural}_{u} \longrightarrow^{*} \bigoplus_{i\in I}(\nu\widetilde{y})([\![M]\!]^{\natural}_{n} \mid P_i)$$

(4) *There exists a $\widehat{\lambda}^{\natural}_{\oplus}$-term M' such that $M' \equiv_{\lambda} N\{\!|M/x|\!\}$ and:*
$$[\![M']\!]^{\natural}_{u} = \bigoplus_{i\in I}(\nu\widetilde{y})([\![M]\!]^{\natural}_{n} \mid P_i)$$

Proof. By induction on the structure of N. We briefly sketch the strategy for proving it case below, but the complete proof can be found in App. D.2.

(1) The interesting cases are for $N = M\langle\!|N'/x|\!\rangle$ and $N = M[\widetilde{y} \leftarrow y]\langle\!\langle B/y\rangle\!\rangle$, when $\mathsf{size}(B) = \mathsf{size}(\widetilde{y}) = 0$ and $\mathsf{head}(M) = x$. Notice that $N = M[\widetilde{y} \leftarrow y]$ is not a case, because of the definition of partially open term: y is a sharing variable in N and $y \in \mathsf{fv}(N)$. The other cases follow easily by the induction hypothesis.
(2) Reductions are only introduced by explicit weakening, which can be eliminated via the precongruence.
(3) Follows from (1) and the fact that linear head substitution can be placed deeper within the term until it reaches the head variable.
(4) Follows from (2) and (3). □

Because of the diamond property (Proposition 3.10), it suffices to consider a completeness result based on a single reduction step in $\widehat{\lambda}^{\natural}_{\oplus}$:

Theorem 5.30 (Operational Completeness)**.** *Let $\mathbb{N}$ and $\mathbb{M}$ be well-formed, partially open $\widehat{\lambda}^{\natural}_{\oplus}$ expressions. If $\mathbb{N} \longrightarrow \mathbb{M}$ then there exist Q and $\mathbb{M}'$ such that $\mathbb{M}' \equiv_{\lambda} \mathbb{M}$, $[\![\mathbb{N}]\!]^{\natural}_{u} \longrightarrow^{*} Q = [\![\mathbb{M}']\!]^{\natural}_{u}$.*

Proof. By induction on the reduction rule applied to infer $\mathbb{N} \longrightarrow \mathbb{M}$. The case in which $\mathbb{N} \longrightarrow_{\texttt{[RS:Lin- Fetch]}} \mathbb{M}$ happens for $\mathbb{N} = M\langle\!|N'/x|\!\rangle$ with $\mathsf{head}(M) = x$, and $\mathbb{M} = M\{\!|N'/x|\!\}$. The translation of $\mathbb{N}$ is of the form (omitting details):

$$\begin{aligned}
[\![\mathbb{N}]\!]^{\natural}_{u} &= (\nu x)([\![M]\!]^{\natural}_{u} \mid x.\mathtt{some}_{\mathsf{fv}(N')}; [\![N']\!]^{\natural}_{x}) \\
&\longrightarrow^{*} (\nu x)(\bigoplus_{i\in I}(\nu\widetilde{y})([\![x]\!]^{\natural}_{n} \mid P_i) \mid x.\mathtt{some}_{\mathsf{fv}(N')}; [\![N']\!]^{\natural}_{x}), \text{ by Proposition 5.29} \\
&\longrightarrow^{*} \bigoplus_{i\in I}(\nu\widetilde{y})(P_i \mid [\![N']\!]^{\natural}_{n}) = [\![\mathbb{M}]\!]^{\natural}_{u}
\end{aligned}$$

The other cases follow by analyzing reductions from the translation of $\mathbb{N}$. The full proof can be found in App. D.2. □

Notice how Proposition 5.29 requires a term to be partially open; however, we prove operational correspondence for closed terms. The reason for this is that we start from a source closed term in $\lambda^{\lightning}_{\oplus}$, which is translated by $(\!|\cdot|\!)^{\circ}$ into a closed $\widehat{\lambda}^{\lightning}_{\oplus}$-term.

Example 5.31 (Cont. Example 5.19)**.** Recall that M and N are well-formed with $\mathsf{fv}(N) = \mathsf{fv}(M) = \emptyset$, we can verify that $N[\leftarrow x]\langle\!\langle \wr M \int / x \rangle\!\rangle$ and $\mathtt{fail}^{\mathsf{fv}(N)\cup\mathsf{fv}(M)}$ are also well-formed. We have

$$N[\leftarrow x]\langle\!\langle \wr M \int / x \rangle\!\rangle \longrightarrow_{[\mathtt{RS:Fail}]} \mathtt{fail}^{\mathsf{fv}(N)\cup\mathsf{fv}(M)}$$

In $\mathsf{s}\pi$, this reduction is mimicked as

$$[\![N[\leftarrow x]\langle\!\langle \wr M \int / x \rangle\!\rangle]\!]^{\lightning}_{u} \longrightarrow^{*} [\![\mathtt{fail}^{\mathsf{fv}(N)\cup\mathsf{fv}(M)}]\!]^{\lightning}_{u}.$$

In fact,

$$\begin{aligned}
[\![N[\leftarrow x]\langle\!\langle \wr M \int / x \rangle\!\rangle]\!]^{\lightning}_{u} &= (\nu x)([\![N[\leftarrow x]]\!]^{\lightning}_{u} \mid [\![\wr M \int]\!]^{\lightning}_{x}) \\
&= (\nu x)(x.\overline{\mathtt{some}}.\overline{x}(y_i).(y_i.\mathtt{some}_u; y_i.\mathtt{close}; [\![N]\!]^{\lightning}_{u} \mid x.\overline{\mathtt{none}}) \mid \\
&= x.\mathtt{some}_{\emptyset}; x(y_i).x.\mathtt{some}_{y_i}; x.\overline{\mathtt{some}}; \overline{x}(x_i).(x_i.\mathtt{some}_{\emptyset}; [\![M]\!]^{\lightning}_{x_i} \mid [\![\mathtt{1}]\!]^{\lightning}_{x} \mid y_i.\overline{\mathtt{none}})) \\
&\longrightarrow (\nu x)(\overline{x}(y_i).(y_i.\mathtt{some}_u; y_i.\mathtt{close}; [\![N]\!]^{\lightning}_{u} \mid x.\overline{\mathtt{none}}) \mid \\
&\qquad x(y_i).x.\mathtt{some}_{y_i}; x.\overline{\mathtt{some}}; \overline{x}(x_i).(x_i.\mathtt{some}_{\emptyset}; [\![M]\!]^{\lightning}_{x_i} \mid [\![\mathtt{1}]\!]^{\lightning}_{x} \mid y_i.\overline{\mathtt{none}})) \\
&\longrightarrow (\nu x)(y_i.\mathtt{some}_u; y_i.\mathtt{close}; [\![N]\!]^{\lightning}_{u} \mid x.\overline{\mathtt{none}} \mid \\
&\qquad x.\mathtt{some}_{y_i}; x.\overline{\mathtt{some}}; \overline{x}(x_i).(x_i.\mathtt{some}_{\emptyset}; [\![M]\!]^{\lightning}_{x_i} \mid [\![\mathtt{1}]\!]^{\lightning}_{x} \mid y_i.\overline{\mathtt{none}})) \\
&\longrightarrow (\nu x)(y_i.\mathtt{some}_u; y_i.\mathtt{close}; [\![N]\!]^{\lightning}_{u} \mid y_i.\overline{\mathtt{none}}) \\
&\longrightarrow u.\overline{\mathtt{none}} \\
&= [\![\mathtt{fail}^{\mathsf{fv}(N)\cup\mathsf{fv}(M)}]\!]^{\lightning}_{u}
\end{aligned}$$

To state soundness we rely on the congruence relation $\equiv_{\lambda}$, given in Fig. 18.

Notation 5.32. Recall the congruence $\equiv_{\lambda}$ for $\widehat{\lambda}^{\lightning}_{\oplus}$, given in Figure 18. We write $N \longrightarrow_{\equiv_{\lambda}} N'$ iff $N \equiv_{\lambda} N_1 \longrightarrow N_2 \equiv_{\lambda} N'$, for some N_1, N_2. Then, $\longrightarrow^{*}_{\equiv_{\lambda}}$ is the reflexive, transitive closure of $\longrightarrow_{\equiv_{\lambda}}$. We use the notation $M \longrightarrow^{i}_{\equiv_{\lambda}} N$ to state that M performs i steps of $\longrightarrow_{\equiv_{\lambda}}$ to N in $i \geq 0$ steps. When $i = 0$ it refers to no reduction taking place.

Theorem 5.33 (Operational Soundness)**.** *Let $\mathbb{N}$ be a well-formed, partially open $\widehat{\lambda}^{\lightning}_{\oplus}$ expression. If $[\![\mathbb{N}]\!]^{\lightning}_{u} \longrightarrow^{*} Q$ then there exist Q' and $\mathbb{N}'$ such that $Q \longrightarrow^{*} Q'$, $\mathbb{N} \longrightarrow^{*}_{\equiv_{\lambda}} \mathbb{N}'$ and $[\![\mathbb{N}']\!]^{\lightning}_{u} = Q'$.*

Proof (Sketch). By induction on the structure of $\mathbb{N}$ with sub-induction on the number of reduction steps in $[\![\mathbb{N}]\!]^{\lightning}_{u} \longrightarrow^{*} Q$. The cases in which $\mathbb{N} = x$, or $\mathbb{N} = \mathtt{fail}^{\widetilde{x}}$, or $\mathbb{N} = \lambda x.M[\widetilde{x} \leftarrow x]$, are easy since there are no reductions starting from $[\![\mathbb{N}]\!]^{\lightning}_{u}$, i.e., $[\![\mathbb{N}]\!]^{\lightning}_{u} \longrightarrow^{0} Q$ which implies $[\![\mathbb{N}]\!]^{\lightning}_{u} = [\![\mathbb{N}']\!]^{\lightning}_{u} = Q = Q'$ and the result follows trivially. The analysis for some cases are exhaustive, for instance, when $\mathbb{N} = (M\ B)$ or $\mathbb{N} = M[\widetilde{x} \leftarrow x]\langle\!\langle B/x \rangle\!\rangle$, there are several sub-cases to be considered: (i) B being equal to $\mathtt{1}$ or not; (ii) $\mathsf{size}(B)$ matching the number of occurrences of the variable in M or not; (iii) M being a failure term or not.

We now discuss one of these cases to illustrate the recurring idea used in the proof: let $\mathbb{N} = (M\ B)$ and suppose that we are able to perform $k > 1$ steps to a process Q, i.e.,

$$[\![\mathbb{N}]\!]^{\not z}_u = [\![(M\ B)]\!]^{\not z}_u = \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)([\![M]\!]^{\not z}_v \mid v.\mathtt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([v \leftrightarrow u] \mid [\![B_i]\!]^{\not z}_x)) \longrightarrow^k Q \tag{5.1}$$

Then there exist an $\mathsf{s}\pi$ process R and integers n, m such that $k = m + n$ and

$$[\![\mathbb{N}]\!]^{\not z}_u \longrightarrow^m \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)(R \mid v.\mathtt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([\![B_i]\!]^{\not z}_x \mid [v \leftrightarrow u])) \longrightarrow^n Q$$

where the first $m \geq 0$ reduction steps are internal to $[\![M]\!]^{\not z}_v$; type preservation in $\mathsf{s}\pi$ ensures that, if they occur, these reductions do not discard the possibility of synchronizing with $v.\mathtt{some}$. Then, the first of the $n \geq 0$ reduction steps towards Q is a synchronization between R and $v.\mathtt{some}_{u,\mathsf{fv}(B)}$.

We will consider the case when $m = 0$ and $n \geq 1$. Then $R = [\![\mathbb{M}]\!]^{\not z}_u \longrightarrow^0 [\![\mathbb{M}]\!]^{\not z}_u$ and there are two possibilities of having an unguarded $v.\overline{\mathtt{some}}$ or $v.\overline{\mathtt{none}}$ without internal reductions:

(i) $M = (\lambda x.M'[\widetilde{x} \leftarrow x])\langle\!|N_1/y_1|\!\rangle \cdots \langle\!|N_p/y_p|\!\rangle \qquad (p \geq 0)$
(ii) $M = \mathtt{fail}^{\widetilde{z}}$

Firstly we use case (i) to express the need for the reduction $\mathbb{N} \longrightarrow^*_{\equiv_\lambda} \mathbb{N}'$. In this case $\mathbb{N} = ((\lambda x.M'[\widetilde{x} \leftarrow x])\langle\!|N_1/y_1|\!\rangle \cdots \langle\!|N_p/y_p|\!\rangle\ B)$ and $[\![\mathbb{N}]\!]_u$ may perform synchronizations where both $[\![\lambda x.M']\!]_v$ and $[\![B]\!]_x$ synchronize across their shared channel. Here we use the congruence relation as follows:

$$\begin{aligned}\mathbb{N} &= ((\lambda x.M'[\widetilde{x} \leftarrow x])\langle\!|N_1/y_1|\!\rangle \cdots \langle\!|N_p/y_p|\!\rangle\ B) \\ &\equiv_\lambda ((\lambda x.M'[\widetilde{x} \leftarrow x])\ B)\langle\!|N_1/y_1|\!\rangle \cdots \langle\!|N_p/y_p|\!\rangle\end{aligned}$$

This enables the abstraction $\lambda x.M'$ to synchronize with the bag B.

Now we will develop case (ii):

$$[\![M]\!]^{\not z}_v = [\![\mathtt{fail}^{\widetilde{z}}]\!]^{\not z}_v = [\![\mathtt{fail}^{\widetilde{z}}]\!]^{\not z}_v = v.\overline{\mathtt{none}} \mid \widetilde{z}.\overline{\mathtt{none}}$$

With this shape for M, the translation and reductions from (5.1) become

$$\begin{aligned}[\![\mathbb{N}]\!]^{\not z}_u &= \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)([\![M]\!]^{\not z}_v \mid v.\mathtt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([\![B_i]\!]^{\not z}_x \mid [v \leftrightarrow u])) \\ &= \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)(v.\overline{\mathtt{none}} \mid \widetilde{z}.\overline{\mathtt{none}} \mid v.\mathtt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([\![B_i]\!]^{\not z}_x \mid [v \leftrightarrow u])) \\ &\longrightarrow \bigoplus_{B_i \in \mathsf{PER}(B)} u.\overline{\mathtt{none}} \mid \widetilde{z}.\overline{\mathtt{none}} \mid \mathsf{fv}(B).\overline{\mathtt{none}}\end{aligned} \tag{5.2}$$

We also have that $\mathbb{N} = \mathtt{fail}^{\widetilde{z}}\ B \longrightarrow \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{z} \cup \mathsf{fv}(B)} = \mathbb{M}$. Furthermore, we have:

$$\begin{aligned}[\![\mathbb{M}]\!]^{\not z}_u &= [\![\sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{z} \cup \mathsf{fv}(B)}]\!]^{\not z}_u \\ &= \bigoplus_{\mathsf{PER}(B)} [\![\mathtt{fail}^{\widetilde{z} \cup \mathsf{fv}(B)}]\!]^{\not z}_u \\ &= \bigoplus_{\mathsf{PER}(B)} u.\overline{\mathtt{none}} \mid \widetilde{z}.\overline{\mathtt{none}} \mid \mathsf{fv}(B).\overline{\mathtt{none}}\end{aligned} \tag{5.3}$$

From reductions in (5.2) and (5.3) one has $[\![\mathbb{N}]\!]^{\lightning}_u \longrightarrow [\![\mathbb{M}]\!]^{\lightning}_u$, and the result follows with $n = 1$ and $[\![\mathbb{M}]\!]^{\lightning}_u = Q = Q'$. The full proof can be found in App. D.2. □

5.3.6. *Success Sensitiveness.* Finally, we consider success sensitiveness. This requires extending $\widehat{\lambda}^{\lightning}_{\oplus}$ and $\mathsf{s}\pi$ with success predicates.

Definition 5.34. We extend the syntax of $\mathsf{s}\pi$ processes (Definition 4.1) with the ✓ construct, which we assume well typed. Also, we extend Definition 5.17 by defining $[\![\checkmark]\!]^{\lightning}_u = \checkmark$

Definition 5.35. We say that a process occurs *guarded* when it occurs behind a prefix (input, output, closing of channels and non-deterministic session behavior). That is, P is guarded if $\alpha.P$ or $\alpha; P$, where $\alpha = \overline{x}(y), x(y), x.\overline{\texttt{close}}, x.\texttt{close}$, $x.\overline{\texttt{some}}, x.\texttt{some}_{(w_1,\cdots,w_n)}$. We say it occurs *unguarded* if it is not guarded for any prefix.

Definition 5.36 (Success in $\mathsf{s}\pi$)**.** We extend the syntax of $\mathsf{s}\pi$ processes with the ✓ construct, which we assume well-typed. We define $P \Downarrow_{\checkmark}$ to hold whenever there exists a P' such that $P \longrightarrow^* P'$ and P' contains an unguarded occurrence of ✓.

Proposition 5.37 (Preservation of Success)**.** *The ✓ at the head of a partially open term is preserved to an unguarded occurrence of ✓ when applying the translation $[\![\cdot]\!]^{\lightning}_u$ up to reductions and vice-versa. That is to say:*

(1) $\forall M \in \widehat{\lambda}^{\lightning}_{\oplus}: \quad \mathsf{head}(M) = \checkmark \implies [\![M]\!]^{\lightning}_u \longrightarrow^* (P \mid \checkmark) \oplus Q$

(2) $\forall M \in \widehat{\lambda}^{\lightning}_{\oplus}: \quad [\![M]\!]^{\lightning}_u = (P \mid \checkmark) \oplus Q \implies \mathsf{head}(M) = \checkmark$

Proof (Sketch). By induction on the structure of M. For item (1), consider the case $M = (N\ B)$ and $\mathsf{head}(N\ B) = \mathsf{head}(N) = \checkmark$. This term's translation is

$$[\![N\ B]\!]^{\lightning}_u = \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)([\![N]\!]^{\lightning}_v \mid v.\texttt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([v \leftrightarrow u] \mid [\![B_i]\!]^{\lightning}_x)).$$

By the induction hypothesis, ✓ is unguarded in $[\![N]\!]^{\lightning}_u$ after a sequence of reductions, i.e., $[\![N]\!]^{\lightning}_u \longrightarrow^* (\checkmark \mid P') \oplus Q'$, for some $\mathsf{s}\pi$ processes P' and Q'. Thus,

$$\begin{aligned}
[\![N\ B]\!]^{\lightning}_u &\longrightarrow^* \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)((\checkmark \mid P') \oplus Q' \mid v.\texttt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([v \leftrightarrow u] \mid [\![B_i]\!]^{\lightning}_x)) \\
&\equiv \checkmark \mid (\nu v)(P' \oplus Q' \mid v.\texttt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([v \leftrightarrow u] \mid [\![B_j]\!]^{\lightning}_x)) \\
&\quad \oplus \Big(\bigoplus_{B_i \in (\mathsf{PER}(B) \setminus\!\setminus B_j)} \checkmark \mid (\nu v)(P' \oplus Q' \mid v.\texttt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([v \leftrightarrow u] \mid [\![B_i]\!]^{\lightning}_x)) \Big) \\
&\equiv (\checkmark \mid P) \oplus Q
\end{aligned}$$

and the result follows by taking $P = (\nu v)(P' \oplus Q' \mid v.\texttt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([v \leftrightarrow u] \mid [\![B_j]\!]^{\lightning}_x))$ and $Q = \bigoplus_{B_i \in (\mathsf{PER}(B) \setminus\!\setminus B_j)} \checkmark \mid (\nu v)(P' \oplus Q' \mid v.\texttt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([v \leftrightarrow u] \mid [\![B_i]\!]^{\lightning}_x))$. The analysis for the other cases are similar; see App. D.3 for details. □

The translation $[\![\cdot]\!]^{\lightning}_u : \widehat{\lambda}^{\lightning}_{\oplus} \to \mathsf{s}\pi$ is success sensitive on well-formed closed expressions.

Theorem 5.38 (Success Sensitivity)**.** *Let $\mathbb{M}$ be a closed well-formed $\widehat{\lambda}^{\lightning}_{\oplus}$-expression. Then,*

$$\mathbb{M} \Downarrow_{\checkmark} \iff [\![\mathbb{M}]\!]^{\lightning}_u \Downarrow_{\checkmark} .$$

Proof (Sketch). Suppose $\mathbb{M} \Downarrow_{\checkmark}$. By Definition 5.11 there exists $\mathbb{M}' = M_1 + \cdots + M_k$ such that $\mathbb{M} \longrightarrow^* \mathbb{M}'$ and $\mathsf{head}(M_j) = \checkmark$, for some $j \in \{1, \ldots, k\}$ and M_j. By operational completeness (Theorem 5.30), there exists Q such that $[\![\mathbb{M}]\!]^{\lightning}_u \longrightarrow^* Q = [\![\mathbb{M}']\!]^{\lightning}_u$. Due to compositionality of $[\![\cdot]\!]^{\lightning}$ and the homomorphic preservation of non-determinism, we have:

- $Q = [\![M_1]\!]^{\lightning}_u \oplus \cdots \oplus [\![M_k]\!]^{\lightning}_u$
- $[\![M_j]\!]^{\lightning}_u = C[[\![\checkmark]\!]^{\lightning}_v] = C[\checkmark]$

By Proposition 5.37, item (1), since $\mathsf{head}(M_j) = \checkmark$ it follows that $[\![M_j]\!]^{\lightning}_u \longrightarrow^* P \mid \checkmark \oplus Q'$. Hence Q reduces to a process that has an unguarded occurrence of $\checkmark$. The proof of the converse is similar and can be found in App. D.3. □

As main result of this sub-section, we have the corollary below, which follows from the previously stated Theorems 5.23, 5.30, 5.33, and 5.38:

Corollary 5.39. *Our translation $[\![\cdot]\!]^{\lightning}$ is a correct encoding, in the sense of Def. 5.1.*

Together, Corollary 5.15 and Corollary 5.39 ensure that $\lambda^{\lightning}_{\oplus}$ can be correctly translated into $\mathsf{s}\pi$, using $\widehat{\lambda}^{\lightning}_{\oplus}$ as a stepping stone.

6. Related Work

Closely related works have been already discussed in the introduction and throughout the paper; here we mention other related literature.

Intersection Types. The first works on intersection types date back to the late 70s (see, e.g., [CD78, Pot80]) and consider intersections with the *idempotence* property (i.e., $\sigma \wedge \sigma = \sigma$). This formulation enables the analysis of *qualitative* properties of λ-calculi, such as (strong) normalization and solvability. By dropping idempotence, intersection types can characterize *quantitative* properties, such as, e.g., bounds on the number of steps needed to reach a normal form. Early works on non-idempotent intersection types include [Gar94, Kfo00, KW04]. The paper [BD20] overviews the origins, development, and applications of intersection types.

Our work formally connects non-idempotent intersection types and classical linear logic extended with the modalities $\&$ and $\oplus$, interpreted in [CP17] as session types for non-deterministically available protocols. To the best of our knowledge, this is an unexplored angle. Prior connections between (non-idempotent) intersection types and linear logic arise in very different settings (see [MPV18] and references therein). They include [NM04], which presents a connection based on a correspondence between normalization and type inference; the work [dC09, dC18], which shows a correspondence between the *relational model* of linear logic and an non-idempotent intersection type system; and [Ehr20], which concerns *indexed* linear logic (cf. [BE00, BE01]).

The work [LdVMY19] develops a type system for the π-calculus based on non-idempotent intersections. The type system ensures that processes are "well-behaved"—they never produce run-time errors, and can always reduce to an idle process. Remarkably, they show that their type system is *complete*: every well-behaved process is typable. Although their type system does not consider session types, it is related to our work for it builds upon Mazza et al.'s correspondence between linear logic and intersection types, given in terms of *polyadic approximations* [MPV18].

Other Resource λ-calculi. A fine-grained treatment of duplication and erasing—similar to our design for $\widehat{\lambda}^{\wr}_{\oplus}$—is present in Kesner and Lengrand's $\lambda\mathtt{lxr}$-calculus [KL07], a simply-typed, deterministic λ-calculus that is in correspondence with proof nets. The $\lambda\mathtt{lxr}$-calculus includes operators called weakening $\mathcal{W}_{\_}(\_)$ and contraction $\mathcal{C}^{\_|\_}_{\_}(\_)$ to deal with empty and non-empty sharing, respectively. In this approach, our terms $\lambda x.x\wr x\wr$ and $\lambda x.y\wr z\wr$ would be expressed as $\mathcal{C}^{x_1|x_2}_x(\lambda x.x_1\wr x_2\wr)$ and $\mathcal{W}_x(\lambda x.y\wr z\wr)$, respectively.

Our approach is convenient when expressing the sharing of more than two occurrences of a variable in a term; as in, e.g., the $\lambda^{\wr}_{\oplus}$-term $\lambda x.(x\wr x, x\wr)$ which would correspond to $\lambda x.(x_1\wr x_2, x_3\wr)[x_1, x_2, x_3 \leftarrow x]$ in $\widehat{\lambda}^{\wr}_{\oplus}$. In the $\lambda\mathtt{lxr}$-calculus, contractions are binary, and so representing $\lambda x.(x\wr x, x\wr)$ requires the composition of two binary contractions.

More substantial differences appear at the level of types. As we have seen, in $\widehat{\lambda}^{\wr}_{\oplus}$ we use intersection types to define well-typed and well-formed expressions (see Fig. 6 and Fig. 7, respectively). In particular, recall the well-formedness rule for the sharing construct:

$$[\mathtt{FS} : \mathtt{share}]\ \frac{\Gamma, x_1 : \sigma, \ldots, x_k : \sigma \models M : \tau \quad x \notin \mathtt{dom}(\Gamma) \quad k \neq 0}{\Gamma, x : \sigma^k \models M[x_1, \ldots, x_k \leftarrow x] : \tau}$$

where, as mentioned above, σ^k denotes the intersection type $\sigma \wedge \ldots \wedge \sigma$. Differently, the typing rule for contraction in the $\lambda\mathtt{lxr}$-calculus involves an arbitrary (simple) type A:

$$(\text{Cont})\ \frac{\Gamma, y : A, z : A \vdash M : B}{\Gamma, x : A \vdash \mathcal{C}^{y|z}_x(M) : B}$$

Our weakening rule $[\mathtt{FS} : \mathtt{weak}]$ types the empty sharing term $M[\leftarrow x]$ as follows:

$$[\mathtt{FS} : \mathtt{weak}]\ \frac{\Gamma \models M : \tau}{\Gamma, x : \omega \models M[\leftarrow x] : \tau}$$

Hence, the context Γ is weakened with a variable assignment $x : \omega$, where ω denotes the empty type. In contrast, weakening in the $\lambda\mathtt{lxr}$-calculus involves a (simple) type A:

$$(\text{Weak})\ \frac{\Gamma \vdash M : A}{\Gamma, x : B \vdash \mathcal{W}_x(M) : A}$$

Hence, the context can be weakened with an assignment $x : B$, where B is a simple type.

Inspired by the multiplicative exponential fragment of linear logic, Kesner and Renaud [KR11] define the so-called *prismoid of resources*, a parametric framework of simply-typed λ-calculi in which each language incorporates different choices for contraction, weakening, and substitution operations. The prismoid defines a uniform and general setting for establishing key properties of typed terms, including simulation of β-reduction, confluence, and strong normalization. One of the languages included in the prismoid is a minor variant of the $\lambda\mathtt{lxr}$-calculus, which we have just mentioned.

There are some similarities between $\lambda^{\wr}_{\oplus}$ and the differential λ-calculus, introduced in [ER03]. Both express non-deterministic choice via sums and use linear head reduction for evaluation. In particular, our fetch rule, which consumes non-deterministically elements from a bag, is related to the derivation (which has similarities with substitution) of a differential term. However, the focus of [ER03] is not on typability nor encodings to process calculi; instead they relate the Taylor series of analysis to the linear head reduction of λ-calculus.

Functions as Processes. A source of inspiration for our developments is the work by Boudol and Laneve [BL00]. As far as we know, this is the only prior study that connects λ and π from a resource-oriented perspective, via an encoding of a λ-calculus with multiplicities into a π-calculus without sums. The goal of [BL00] is different from ours, as they study the discriminating power of semantics for λ as induced by encodings into π. In contrast, we study how typability delineates the encodability of resource-awareness across sequential and concurrent realms. The source and target calculi in [BL00] are untyped, whereas we consider typed calculi and our encodings preserve typability. As a result, the encoding in [BL00] is conceptually different from ours; remarkably, our encoding respects linearity and homomorphically translates sums.

Prior works have studied encodings of typed λ-calculi into typed π-calculi; see, e.g., [San99, BL00, SW01, BHY03, TCP12, HYB14, TY18]. None of these works consider non-determinism and failures; the one exception is the encoding in [CP17], which involves a λ-calculus with exceptions and failures (but without non-determinism due to bags, as in $\lambda^{\lightning}_{\oplus}$) for which no reduction semantics is given. As a result, the encoding in [CP17] is different from ours, and is only shown to preserve typability: properties such as operational completeness, operational soundness, and success sensitivity—important in our developments—are not considered.

7. Concluding Remarks

Summary. We developed a correct encoding of $\lambda^{\lightning}_{\oplus}$, a new resource λ-calculus in which expressions feature non-determinism and explicit failure, into $\mathsf{s}\pi$, a session-typed π-calculus in which behavior is non-deterministically available: session protocols may perform as stipulated but also fail. Our encodability result is obtained by appealing to $\widehat{\lambda}^{\lightning}_{\oplus}$, an intermediate language with a *sharing construct* that simplifies the treatment of variables in expressions. To our knowledge, we are the first to relate typed λ-calculi and typed π-calculi encompassing non-determinism and failures, while connecting intersection types and session types, two different mechanisms for resource-awareness in sequential and concurrent settings, respectively.

Design of $\lambda^{\lightning}_{\oplus}$ (and $\widehat{\lambda}^{\lightning}_{\oplus}$). The design of $\lambda^{\lightning}_{\oplus}$ has been influenced by the logically justified treatment of non-determinism and explicit failure in $\mathsf{s}\pi$. Our correct encoding of $\lambda^{\lightning}_{\oplus}$ into $\mathsf{s}\pi$ makes this influence precise by connecting terms and processes but also their associated intersection types and linear logic propositions. We have also adopted features from previous resource λ-calculi, in particular those in [Bou93, BL00, PR10]. Major similarities between $\lambda^{\lightning}_{\oplus}$ and these calculi include: as in [BL00], our semantics performs lazy evaluation and linear substitution on the head variable; as in [PR10], our reductions lead to non-deterministic sums. A distinctive feature of $\lambda^{\lightning}_{\oplus}$ is its lazy treatment of failures via the term $\mathtt{fail}^{\widetilde{x}}$. In contrast, in [Bou93, BL00] there is no dedicated term to represent failure. The non-collapsing semantics for non-determinism is another distinctive feature of $\lambda^{\lightning}_{\oplus}$.

Our design for $\widehat{\lambda}^{\lightning}_{\oplus}$ has been informed by the atomic λ-calculus introduced in [GHP13]. Also, our translation from $\lambda^{\lightning}_{\oplus}$ into $\widehat{\lambda}^{\lightning}_{\oplus}$ (Def. 3.26) borrows insights from translations given in [GHP13]. The calculus $\widehat{\lambda}^{\lightning}_{\oplus}$ is also loosely related to the λ-calculus with sharing in [GILL11], which considers (idempotent) intersection types. Notice that the calculi in [GHP13, GILL11] do not consider explicit failure nor non-determinism. We distinguish between *well-typed* and *well-formed* expressions: this allows us to make fail-prone evaluation in $\lambda^{\lightning}_{\oplus}$ explicit. It is

interesting that explicit failures can be elegantly encoded as protocols in $\mathsf{s}\pi$—this way, we make the most out of $\mathsf{s}\pi$'s expressivity.

Bags in $\lambda^{\lightning}_{\oplus}$ have *linear* resources, which are used exactly once. In recent work, we have defined an extension of $\lambda^{\lightning}_{\oplus}$ in which bags contain both linear and *unrestricted* resources, as in [PR10], and established that our approach to encodability into $\mathsf{s}\pi$ extends to such an enriched language [PNP21b]. This development requires the full typed process framework in [CP17], with replicated processes and labeled choices (not needed to encode $\lambda^{\lightning}_{\oplus}$).

Future Work. The approach and results developed here enable us to tackle open questions that go beyond the scope of this work. We comment on some of them:

- It would be useful to investigate the *relative expressiveness* of $\lambda^{\lightning}_{\oplus}$ with respect to other resource calculi, such as those in [BL00, PR10]. Derived encodability (and non-encodability) results could potentially unlock transfer of reasoning techniques between different calculi.
- Besides transfer of techniques, one application of encodings between sequential and concurrent calculi is in the design of functional concurrent languages with advanced features. In this respect, it should be feasible to develop a variant of Wadler's GV [Wad12] with non-determinism, resources, explicit failure, and session communication by exploiting our correct encodings from $\lambda^{\lightning}_{\oplus}$ to $\mathsf{s}\pi$.
- It would be relevant to investigate *decidability properties* of the intersection type systems for $\lambda^{\lightning}_{\oplus}$ and $\widehat{\lambda}^{\lightning}_{\oplus}$. Our translation is proven correct under the assumption that we consider only well-formed $\lambda^{\lightning}_{\oplus}$-terms. The type assignment problem for intersection type systems is, in general, undecidable [Lei83]; it would be interesting to consider decidable fragments of intersection type systems via, for instance, ranking restrictions [vB95].
- It would be insightful to establish *full abstraction* for our translation of $\lambda^{\lightning}_{\oplus}$ into $\mathsf{s}\pi$. We choose not to consider it because, as argued in [GN16], full abstraction is not an informative criterion when it comes to an encoding's quality. Establishing full abstraction requires developing the behavioral theory of $\lambda^{\lightning}_{\oplus}$ and $\mathsf{s}\pi$, which is relevant and challenging in itself.

Acknowledgements. We are grateful to the anonymous reviewers for their detailed and helpful comments. We gratefully acknowledge the support of the Dutch Research Council (NWO) under project No. 016.Vidi.189.046 (Unifying Correctness for Communicating Software). Daniele Nantes-Sobrinho has been partially funded by the EPSRC Fellowship 'VeTSpec: Verified Trustworthy Software Specification' (EP/R034567/1) and Edital DPI/DPG n. 03/2020.

References

[BD20] Viviana Bono and Mariangiola Dezani-Ciancaglini. A tale of intersection types. In Holger Hermanns, Lijun Zhang, Naoki Kobayashi, and Dale Miller, editors, *LICS '20: 35th Annual ACM/IEEE Symposium on Logic in Computer Science, Saarbrücken, Germany, July 8-11, 2020*, pages 7–20. ACM, 2020. doi:10.1145/3373718.3394733.

[BE00] Antonio Bucciarelli and Thomas Ehrhard. On phase semantics and denotational semantics in multiplicative-additive linear logic. *Ann. Pure Appl. Log.*, 102(3):247–282, 2000. doi:10.1016/S0168-0072(99)00040-8.

[BE01] Antonio Bucciarelli and Thomas Ehrhard. On phase semantics and denotational semantics: the exponentials. *Ann. Pure Appl. Log.*, 109(3):205–241, 2001. doi:10.1016/S0168-0072(00)00056-7.

[BHY03] Martin Berger, Kohei Honda, and Nobuko Yoshida. Genericity and the pi-calculus. In Andrew D. Gordon, editor, *Foundations of Software Science and Computational Structures, 6th International Conference, FOSSACS 2003 Held as Part of the Joint European Conference on Theory and Practice of Software, ETAPS 2003, Warsaw, Poland, April 7-11, 2003, Proceedings*, volume 2620 of *Lecture Notes in Computer Science*, pages 103–119. Springer, 2003. doi:10.1007/3-540-36576-1_7.

[BKV17] Antonio Bucciarelli, Delia Kesner, and Daniel Ventura. Non-idempotent intersection types for the lambda-calculus. *Logic Journal of the IGPL*, 25(4):431–464, 2017.

[BL96] Gérard Boudol and Cosimo Laneve. The discriminating power of multiplicities in the lambda-calculus. *Inf. Comput.*, 126(1):83–102, 1996. doi:10.1006/inco.1996.0037.

[BL00] Gérard Boudol and Cosimo Laneve. lambda-calculus, multiplicities, and the pi-calculus. In *Proof, Language, and Interaction, Essays in Honour of Robin Milner*, pages 659–690, 2000.

[Bou93] Gérard Boudol. The lambda-calculus with multiplicities (abstract). In Eike Best, editor, *CONCUR '93, Hildesheim, Germany, August 23-26, 1993, Proceedings*, volume 715 of *Lecture Notes in Computer Science*, pages 1–6. Springer, 1993. doi:10.1007/3-540-57208-2_1.

[CD78] Mario Coppo and Mariangiola Dezani-Ciancaglini. A new type assignment for λ-terms. *Arch. Math. Log.*, 19(1):139–156, 1978. doi:10.1007/BF02011875.

[CP10] Luís Caires and Frank Pfenning. Session types as intuitionistic linear propositions. In *CONCUR 2010 - Concurrency Theory, 21th International Conference, CONCUR 2010, Paris, France, August 31-September 3, 2010. Proceedings*, pages 222–236, 2010. doi:10.1007/978-3-642-15375-4_16.

[CP17] Luís Caires and Jorge A. Pérez. Linearity, control effects, and behavioral types. In Hongseok Yang, editor, *Programming Languages and Systems - 26th European Symposium on Programming, ESOP 2017, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2017, Uppsala, Sweden, April 22-29, 2017, Proceedings*, volume 10201 of *Lecture Notes in Computer Science*, pages 229–259. Springer, 2017. doi:10.1007/978-3-662-54434-1_9.

[dC09] Daniel de Carvalho. Execution time of lambda-terms via denotational semantics and intersection types. *CoRR*, abs/0905.4251, 2009. URL: http://arxiv.org/abs/0905.4251, arXiv:0905.4251.

[dC18] Daniel de Carvalho. Execution time of λ-terms via denotational semantics and intersection types. *Math. Struct. Comput. Sci.*, 28(7):1169–1203, 2018. doi:10.1017/S0960129516000396.

[DdP93] Mariangiola Dezani-Ciancaglini, Ugo de'Liguoro, and Adolfo Piperno. Filter models for a parallel and non deterministic lambda-calculus. In Andrzej M. Borzyszkowski and Stefan Sokolowski, editors, *Mathematical Foundations of Computer Science 1993, 18th International Symposium, MFCS'93, Gdansk, Poland, August 30 - September 3, 1993, Proceedings*, volume 711 of *Lecture Notes in Computer Science*, pages 403–412. Springer, 1993. doi:10.1007/3-540-57182-5_32.

[Ehr20] Thomas Ehrhard. Non-idempotent intersection types in logical form. In Jean Goubault-Larrecq and Barbara König, editors, *Foundations of Software Science and Computation Structures - 23rd International Conference, FOSSACS 2020, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2020, Dublin, Ireland, April 25-30, 2020, Proceedings*, volume 12077 of *Lecture Notes in Computer Science*, pages 198–216. Springer, 2020. doi:10.1007/978-3-030-45231-5_11.

[ER03] Thomas Ehrhard and Laurent Regnier. The differential lambda-calculus. *Theor. Comput. Sci.*, 309(1-3):1–41, 2003. doi:10.1016/S0304-3975(03)00392-X.

[Gar94] Philippa Gardner. Discovering needed reductions using type theory. In Masami Hagiya and John C. Mitchell, editors, *Theoretical Aspects of Computer Software, International Conference TACS '94, Sendai, Japan, April 19-22, 1994, Proceedings*, volume 789 of *Lecture Notes in Computer Science*, pages 555–574. Springer, 1994. doi:10.1007/3-540-57887-0_115.

[GHP13] Tom Gundersen, Willem Heijltjes, and Michel Parigot. Atomic lambda calculus: A typed lambda-calculus with explicit sharing. In *28th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2013, New Orleans, LA, USA, June 25-28, 2013*, pages 311–320, 2013. doi:10.1109/LICS.2013.37.

[GILL11] Silvia Ghilezan, Jelena Ivetic, Pierre Lescanne, and Silvia Likavec. Intersection types for the resource control lambda calculi. In *Theoretical Aspects of Computing - ICTAC 2011 -*

8th International Colloquium, Johannesburg, South Africa, August 31 - September 2, 2011. Proceedings, pages 116–134, 2011. doi:10.1007/978-3-642-23283-1_10.

[GMM03] Stefano Guerrini, Simone Martini, and Andrea Masini. Coherence for sharing proof-nets. *Theoretical Computer Science*, 294(3):379–409, 2003. Linear Logic. doi:10.1016/S0304-3975(01)00162-1.

[GN16] Daniele Gorla and Uwe Nestmann. Full abstraction for expressiveness: history, myths and facts. *Math. Struct. Comput. Sci.*, 26(4):639–654, 2016. doi:10.1017/S0960129514000279.

[Gor10] Daniele Gorla. Towards a unified approach to encodability and separation results for process calculi. *Inf. Comput.*, 208(9):1031–1053, 2010. doi:10.1016/j.ic.2010.05.002.

[Gue99] Stefano Guerrini. A general theory of sharing graphs. *Theoretical Computer Science*, 227(1):99–151, 1999. doi:10.1016/S0304-3975(99)00050-X.

[Hon93] Kohei Honda. Types for dyadic interaction. In Eike Best, editor, *CONCUR '93, Hildesheim, Germany, August 23-26, 1993, Proceedings*, volume 715 of *Lecture Notes in Computer Science*, pages 509–523. Springer, 1993. doi:10.1007/3-540-57208-2_35.

[HVK98] Kohei Honda, Vasco Thudichum Vasconcelos, and Makoto Kubo. Language primitives and type discipline for structured communication-based programming. In Chris Hankin, editor, *Programming Languages and Systems - ESOP'98, 7th European Symposium on Programming, Held as Part of the European Joint Conferences on the Theory and Practice of Software, ETAPS'98, Lisbon, Portugal, March 28 - April 4, 1998, Proceedings*, volume 1381 of *Lecture Notes in Computer Science*, pages 122–138. Springer, 1998. doi:10.1007/BFb0053567.

[HYB14] Kohei Honda, Nobuko Yoshida, and Martin Berger. Process types as a descriptive tool for interaction - control and the pi-calculus. In Gilles Dowek, editor, *Rewriting and Typed Lambda Calculi - Joint International Conference, RTA-TLCA 2014, Held as Part of the Vienna Summer of Logic, VSL 2014, Vienna, Austria, July 14-17, 2014. Proceedings*, volume 8560 of *Lecture Notes in Computer Science*, pages 1–20. Springer, 2014. doi:10.1007/978-3-319-08918-8_1.

[Kfo00] A. J. Kfoury. A linearization of the lambda-calculus and consequences. *J. Log. Comput.*, 10(3):411–436, 2000. doi:10.1093/logcom/10.3.411.

[KL07] Delia Kesner and Stéphane Lengrand. Resource operators for lambda-calculus. *Inf. Comput.*, 205(4):419–473, 2007. doi:10.1016/j.ic.2006.08.008.

[KPY19] Dimitrios Kouzapas, Jorge A. Pérez, and Nobuko Yoshida. On the relative expressiveness of higher-order session processes. *Inf. Comput.*, 268, 2019. doi:10.1016/j.ic.2019.06.002.

[KR11] Delia Kesner and Fabien Renaud. A prismoid framework for languages with resources. *Theor. Comput. Sci.*, 412(37):4867–4892, 2011. doi:10.1016/j.tcs.2011.01.026.

[KW04] A. J. Kfoury and J. B. Wells. Principality and type inference for intersection types using expansion variables. *Theor. Comput. Sci.*, 311(1-3):1–70, 2004. doi:10.1016/j.tcs.2003.10.032.

[LdVMY19] Ugo Dal Lago, Marc de Visme, Damiano Mazza, and Akira Yoshimizu. Intersection types and runtime errors in the pi-calculus. *Proc. ACM Program. Lang.*, 3(POPL):7:1–7:29, 2019. doi:10.1145/3290320.

[Lei83] Daniel Leivant. Polymorphic type inference. In John R. Wright, Larry Landweber, Alan J. Demers, and Tim Teitelbaum, editors, *Conference Record of the Tenth Annual ACM Symposium on Principles of Programming Languages, Austin, Texas, USA, January 1983*, pages 88–98. ACM Press, 1983. doi:10.1145/567067.567077.

[Mil92] Robin Milner. Functions as processes. *Mathematical Structures in Computer Science*, 2(2):119–141, 1992. doi:10.1017/S0960129500001407.

[MPV18] Damiano Mazza, Luc Pellissier, and Pierre Vial. Polyadic approximations, fibrations and intersection types. *Proc. ACM Program. Lang.*, 2(POPL):6:1–6:28, 2018. doi:10.1145/3158094.

[MPW92] Robin Milner, Joachim Parrow, and David Walker. A calculus of mobile processes, I. *Inf. Comput.*, 100(1):1–40, 1992. doi:10.1016/0890-5401(92)90008-4.

[NM04] Peter Møller Neergaard and Harry G. Mairson. Types, potency, and idempotency: why nonlinearity and amnesia make a type system work. In Chris Okasaki and Kathleen Fisher, editors, *Proceedings of the Ninth ACM SIGPLAN International Conference on Functional Programming, ICFP 2004, Snow Bird, UT, USA, September 19-21, 2004*, pages 138–149. ACM, 2004. doi:10.1145/1016850.1016871.

[OY16] Dominic A. Orchard and Nobuko Yoshida. Effects as sessions, sessions as effects. In *Proceedings of the 43rd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages,*

POPL 2016, St. Petersburg, FL, USA, January 20 - 22, 2016, pages 568–581. ACM, 2016. doi:10.1145/2837614.2837634.

[Par08] Joachim Parrow. Expressiveness of process algebras. *Electron. Notes Theor. Comput. Sci.*, 209:173–186, 2008. doi:10.1016/j.entcs.2008.04.011.

[PNP21a] Joseph W. N. Paulus, Daniele Nantes-Sobrinho, and Jorge A. Pérez. Non-deterministic functions as non-deterministic processes. In Naoki Kobayashi, editor, *6th International Conference on Formal Structures for Computation and Deduction, FSCD 2021, July 17-24, 2021, Buenos Aires, Argentina (Virtual Conference)*, volume 195 of *LIPIcs*, pages 21:1–21:22. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. doi:10.4230/LIPIcs.FSCD.2021.21.

[PNP21b] Joseph W. N. Paulus, Daniele Nantes-Sobrinho, and Jorge A. Pérez. Types and terms translated: Unrestricted resources in encoding functions as processes. In Henning Basold, Jesper Cockx, and Silvia Ghilezan, editors, *27th International Conference on Types for Proofs and Programs, TYPES 2021, June 14-18, 2021, Leiden, The Netherlands (Virtual Conference)*, volume 239 of *LIPIcs*, pages 11:1–11:24. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. doi:10.4230/LIPIcs.TYPES.2021.11.

[Pot80] Garrell Pottinger. A type assignment for the strongly normalizable λ-terms. In *To H. B. Curry: Essays on Combinatory Logic, Lambda Calculus, and Formalism*, pages 561–577. Academic Press, New York, 1980.

[PR10] Michele Pagani and Simona Ronchi Della Rocca. Solvability in resource lambda-calculus. In C.-H. Luke Ong, editor, *Foundations of Software Science and Computational Structures, 13th International Conference, FOSSACS 2010, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2010, Paphos, Cyprus, March 20-28, 2010. Proceedings*, volume 6014 of *Lecture Notes in Computer Science*, pages 358–373. Springer, 2010. doi:10.1007/978-3-642-12032-9_25.

[San99] Davide Sangiorgi. From lambda to pi; or, rediscovering continuations. *Math. Struct. Comput. Sci.*, 9(4):367–401, 1999. URL: http://journals.cambridge.org/action/displayAbstract?aid=44843.

[SW01] Davide Sangiorgi and David Walker. *The Pi-Calculus - a theory of mobile processes*. Cambridge University Press, 2001.

[TCP12] Bernardo Toninho, Luís Caires, and Frank Pfenning. Functions as session-typed processes. In Lars Birkedal, editor, *Foundations of Software Science and Computational Structures - 15th International Conference, FOSSACS 2012, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2012, Tallinn, Estonia, March 24 - April 1, 2012. Proceedings*, volume 7213 of *Lecture Notes in Computer Science*, pages 346–360. Springer, 2012. doi:10.1007/978-3-642-28729-9_23.

[TY18] Bernardo Toninho and Nobuko Yoshida. On polymorphic sessions and functions - A tale of two (fully abstract) encodings. In Amal Ahmed, editor, *27th European Symposium on Programming, ESOP 2018, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2018, Thessaloniki, Greece, April 14-20, 2018, Proceedings*, volume 10801 of *Lecture Notes in Computer Science*, pages 827–855. Springer, 2018. doi:10.1007/978-3-319-89884-1_29.

[vB95] Steffen van Bakel. Intersection type assignment systems. *Theor. Comput. Sci.*, 151(2):385–435, 1995. doi:10.1016/0304-3975(95)00073-6.

[Wad12] Philip Wadler. Propositions as sessions. In Peter Thiemann and Robby Bruce Findler, editors, *ACM SIGPLAN International Conference on Functional Programming, ICFP'12, Copenhagen, Denmark, September 9-15, 2012*, pages 273–286. ACM, 2012. doi:10.1145/2364527.2364568.

Contents

Appendix A. Appendix to § 2.3

Lemma 2.21 (Linear Anti-substitution Lemma for $\lambda_{\oplus}$)**.** *Let M and N be $\lambda_{\oplus}$-terms such that $\mathsf{head}(M) = x$, then we have:*

- $\Gamma, x : \sigma^{k-1} \vdash M\{\!|N/x|\!\} : \tau$, *with $k > 1$, then there exist Γ_1, Γ_2 such that $\Gamma_1, x : \sigma^k \vdash M : \tau$, and $\Gamma_2 \vdash N : \sigma$, where $\Gamma = \Gamma_1 \wedge \Gamma_2$.*
- $\Gamma \vdash M\{\!|N/x|\!\} : \tau$, *with $x \notin \mathtt{dom}(\Gamma)$, then there exist Γ_1, Γ_2 such that $\Gamma_1, x : \sigma \vdash M : \tau$, and $\Gamma_2 \vdash N : \sigma$, where $\Gamma = \Gamma_1 \wedge \Gamma_2$.*

Proof. By induction on the structure of M:

(1) When $M = x$ then we have $x\{\!|N/x|\!\} = N$ and may derive the derivation of $\Gamma \vdash N : \tau$ with $x \notin \mathtt{dom}(\Gamma)$. By taking $\Gamma_1 = \emptyset$ and $\Gamma_2 = \Gamma$ as $\Gamma = \emptyset \wedge \Gamma$ the case follows as $\Gamma \vdash N : \tau$ and

$$[\mathtt{T} : \mathtt{var}]\ \frac{}{x : \sigma \vdash x : \sigma}$$

(2) When $M = (M\ B)$ then we have that $(M\ B)\{\!|N/x|\!\} = (M\{\!|N/x|\!\})\ B$. Let us consider two cases:

(I) When $x \in \mathsf{fv}(M\{\!|N/x|\!\})$

$$[\mathtt{T} : \mathtt{app}]\ \frac{\Gamma', x : \sigma^{k-1} \vdash M\{\!|N/x|\!\} : \pi \to \tau' \qquad \Delta \vdash B : \pi}{(\Gamma', x : \sigma^{k-1}) \wedge \Delta \vdash (M\{\!|N/x|\!\})\ B : \tau'}$$

By the IH we have that $\Gamma', x : \sigma^{k-1} \vdash M\{\!|N/x|\!\} : \pi \to \tau'$ implies that $\exists\ \Gamma'_1, \Gamma_2$ such that $\Gamma'_1, x : \sigma^k \vdash M : \tau$, and $\Gamma_2 \vdash N : \sigma$ with $\Gamma' = \Gamma'_1 \wedge \Gamma_2$.

$$[\mathtt{T} : \mathtt{app}]\ \frac{\Gamma'_1, x : \sigma^k \vdash M : \pi \to \tau' \qquad \Delta \vdash B : \pi}{(\Gamma'_1, x : \sigma^k) \wedge \Delta \vdash M\ B : \tau'}$$

(II) When $x \notin \mathsf{fv}(M\{\!|N/x|\!\})$

$$[\mathtt{T} : \mathtt{app}]\ \frac{\Gamma' \vdash M\{\!|N/x|\!\} : \pi \to \tau' \qquad \Delta \vdash B : \pi}{\Gamma' \wedge \Delta \vdash (M\{\!|N/x|\!\})\ B : \tau'}$$

By the IH we have that $\Gamma' \vdash M\{\!|N/x|\!\} : \pi \to \tau'$ implies that $\exists\ \Gamma'_1, \Gamma_2$ such that $\Gamma'_1, x : \sigma \vdash M : \tau$, and $\Gamma_2 \vdash N : \sigma$ with $\Gamma' = \Gamma'_1 \wedge \Gamma_2$.

$$[\mathtt{T} : \mathtt{app}]\ \frac{\Gamma'_1, x : \sigma \vdash M\{\!|N/x|\!\} : \pi \to \tau' \qquad \Delta \vdash B : \pi}{(\Gamma'_1, x : \sigma) \wedge \Delta \vdash M\ B : \tau'}$$

(3) When $M = M\langle\!\langle B/y \rangle\!\rangle$ then we have that $(M\ \langle\!\langle B/y \rangle\!\rangle)\{\!|N/x|\!\} = (M\{\!|N/x|\!\})\ \langle\!\langle B/y \rangle\!\rangle$ where $x \neq y$

(I) When $x \in \mathsf{fv}(M\{\!|N/x|\!\})$

$$[\mathtt{T} : \mathtt{ex\text{-}sub}]\ \frac{\Gamma', x : \sigma^{k-1}, y : \delta^j \vdash (M\{\!|N/x|\!\}) : \tau \qquad \Delta \vdash B : \delta^j}{\Gamma', y : \delta^j \wedge \Delta \vdash (M\{\!|N/x|\!\})\langle\!\langle B/y \rangle\!\rangle : \tau}$$

By the IH we have that $\Gamma', x : \sigma^{k-1}, y : \delta^j \vdash (M\{\!|N/x|\!\}) : \tau$ implies that $\exists\ \Gamma'_1, \Gamma_2$ such that $\Gamma'_1, x : \sigma^k, y : \delta^j \vdash M : \tau$, and $\Gamma_2 \vdash N : \sigma$ with $\Gamma', y : \delta^j = (\Gamma'_1, y : \delta^j) \wedge \Gamma_2$.

$$[\mathtt{T} : \mathtt{ex\text{-}sub}]\ \frac{\Gamma'_1, x : \sigma^k, y : \delta^j \vdash M : \tau \qquad \Delta \vdash B : \delta^j}{\Gamma'_1 \wedge \Delta \vdash M\langle\!\langle B/y \rangle\!\rangle : \tau}$$

(II) When $x \notin \mathsf{fv}(M\{\!|N/x|\!\})$

$$[\mathtt{T} : \mathtt{ex\text{-}sub}]\ \frac{\Gamma', y : \delta^k \vdash (M\{\!|N/x|\!\}) : \tau \qquad \Delta \vdash B : \delta^k}{\Gamma' \wedge \Delta \vdash (M\{\!|N/x|\!\})\langle\!\langle {}^{B}/_{y}\rangle\!\rangle : \tau}$$

By the IH we have that $\Gamma', y : \delta^k \vdash (M\{\!|N/x|\!\}) : \tau$ implies that $\exists\ \Gamma'_1, \Gamma_2$ such that $\Gamma'_1, x : \sigma \vdash M : \tau$, and $\Gamma_2 \vdash N : \sigma$ with $\Gamma', y : \delta^k = (\Gamma'_1, y : \delta^k) \wedge \Gamma_2$.

$$[\mathtt{T} : \mathtt{ex\text{-}sub}]\ \frac{\Gamma'_1, x : \sigma, y : \delta^k \vdash M : \tau \qquad \Delta \vdash B : \delta^k}{\Gamma'_1 \wedge \Delta \vdash M\langle\!\langle {}^{B}/_{y}\rangle\!\rangle : \tau}$$

(4) When $M = \lambda y.M$ then linear head substitution is undefined on this term as $\mathsf{head}(M) \neq x$.

(5) When $M = \mathtt{fail}^{\widetilde{x}}$ then M is not well typed. □

Theorem 2.22 (Subject Expansion for $\lambda_{\oplus}$)**.** *If* $\Gamma \vdash \mathbb{M}' : \tau$ *and* $\mathbb{M} \longrightarrow \mathbb{M}'$ *then* $\Gamma \vdash \mathbb{M} : \tau$.

Proof. By induction on the reduction rule applied. There are four possible cases.

(1) When $\mathbb{M}'$ is reduced to via the Rule $[\mathtt{R} : \mathtt{Beta}]$

$$[\mathtt{R} : \mathtt{Beta}]\ \frac{}{(\lambda x.M)B \longrightarrow M\ \langle\!\langle {}^{B}/_{x}\rangle\!\rangle}$$

Then $\mathbb{M}' = M\ \langle\!\langle {}^{B}/_{x}\rangle\!\rangle$ can be type as follows:

$$[\mathtt{T} : \mathtt{ex\text{-}sub}]\ \frac{\Gamma, x : \sigma^k \vdash M : \tau \qquad \Delta \vdash B : \sigma^k}{\Gamma \wedge \Delta \vdash M\langle\!\langle {}^{B}/_{x}\rangle\!\rangle : \tau}$$

From the typing of $\mathbb{M}'$ we can deduce that $\mathbb{M} = (\lambda x.M)B$ may be typed by:

$$\begin{array}{l}[\mathtt{T} : \mathtt{abs}]\ \dfrac{\Gamma, x : \sigma^k \vdash M : \tau}{\Gamma \vdash \lambda x.M : \sigma^k \to \tau} \qquad \Delta \vdash B : \pi \\ [\mathtt{T} : \mathtt{app}]\end{array}\ \frac{}{\Gamma \wedge \Delta \vdash (\lambda x.M)B : \tau}$$

(2) When $\mathbb{M}'$ is reduced to via the Rule $[\mathtt{R} : \mathtt{Fetch}]$

$$[\mathtt{R} : \mathtt{Fetch}]\ \frac{\mathsf{head}(M) = x \qquad B = \wr N_1, \ldots, N_k \wr\ ,\ k \geq 1 \qquad \#(x, M) = k}{M\ \langle\!\langle {}^{B}/_{x}\rangle\!\rangle \longrightarrow M\{\!|N_1/x|\!\}\langle\!\langle {}^{(B\ \setminus\!\setminus N_1)}/_{x}\rangle\!\rangle + \cdots + M\{\!|N_k/x|\!\}\langle\!\langle {}^{(B\ \setminus\!\setminus N_k)}/_{x}\rangle\!\rangle}$$

Let us consider two cases:

(I) The bag B has k elements where $k > 1$, then we type $M\{\!|N_i/x|\!\}\langle\!\langle {}^{(B\ \setminus\!\setminus N_i)}/_{x}\rangle\!\rangle$ with the derivation Π_i to be:

$$[\mathtt{T} : \mathtt{ex\text{-}sub}]\ \frac{\Gamma, x : \sigma^{k-1} \vdash M\{\!|N_1/x|\!\} : \tau \qquad \Delta \vdash (B\ \setminus\!\setminus N_1) : \sigma^{k-1}}{\Gamma \wedge \Delta \vdash M\{\!|N_1/x|\!\}\langle\!\langle {}^{(B\ \setminus\!\setminus N_1)}/_{x}\rangle\!\rangle : \tau}$$

We can type the sum with each derivation Π_i to be

$$\frac{\dfrac{\Pi_1}{\Gamma \wedge \Delta \vdash M\{\!|N_1/x|\!\}\langle\!\langle {}^{(B\ \setminus\!\setminus N_1)}/_{x}\rangle\!\rangle : \tau} \qquad \begin{array}{c}\dfrac{\Pi_k}{\Gamma \wedge \Delta \vdash M\{\!|N_k/x|\!\}\langle\!\langle {}^{(B\ \setminus\!\setminus N_k)}/_{x}\rangle\!\rangle : \tau} \\ \vdots\end{array}}{\Gamma \wedge \Delta \vdash M\{\!|N_1/x|\!\}\langle\!\langle {}^{(B\ \setminus\!\setminus N_1)}/_{x}\rangle\!\rangle + \cdots + M\{\!|N_k/x|\!\}\langle\!\langle {}^{(B\ \setminus\!\setminus N_k)}/_{x}\rangle\!\rangle : \tau}$$

By the anti-substitution lemma (Lemma 2.21) we have that $\exists\ \Gamma_1, \Gamma_2$ such that $\Gamma_1, x : \sigma^k \vdash M : \tau$, and $\Gamma_2 \vdash N_i : \sigma$ with $\Gamma = \Gamma_1 \wedge \Gamma_2$ and finally we have:

$$[\mathtt{T} : \mathtt{ex\text{-}sub}]\ \frac{\Gamma_1, x : \sigma^k \vdash M : \tau \qquad \Delta \wedge \Gamma_2 \vdash B : \sigma^k}{\Gamma \wedge \Delta \vdash M\langle\!\langle {}^{B}/_{x}\rangle\!\rangle : \tau}$$

notice that we make use that $\Gamma_2 \vdash N_i : \sigma$ to ensure that the bag B is well typed.

(II) The bag B has one element, then we type $M\{\!|N_i/x|\!\}\langle\!\langle 1/x\rangle\!\rangle$ with the derivation Π to be:

$$[\mathtt{T} : \mathtt{ex\text{-}sub}]\ \frac{\Gamma \vdash M\{\!|N_1/x|\!\} : \tau \qquad \Delta \vdash \mathtt{1} : \omega}{\Gamma \wedge \Delta \vdash M\{\!|N_1/x|\!\}\langle\!\langle 1/x\rangle\!\rangle : \tau}$$

By the anti-substitution lemma (Lemma 2.21) we have that $\exists\ \Gamma_1, \Gamma_2$ such that $\Gamma_1, x : \sigma \vdash M : \tau$, and $\Gamma_2 \vdash N_1 : \sigma$ with $\Gamma = \Gamma_1 \wedge \Gamma_2$ and finally we have:

$$[\mathtt{T} : \mathtt{ex\text{-}sub}]\ \frac{\Gamma_1, x : \sigma \vdash M : \tau \qquad \Delta \wedge \Gamma_2 \vdash \wr N_1 \wr : \sigma}{\Gamma \wedge \Delta \vdash M\{\!|N_1/x|\!\}\langle\!\langle N/x\rangle\!\rangle : \tau}$$

(3) When $\mathbb{M}'$ is reduced to via the Rule $[\mathtt{R} : \mathtt{TCont}]$

$$[\mathtt{R} : \mathtt{TCont}]\ \frac{M \longrightarrow M'_1 + \cdots + M'_k}{C[M] \longrightarrow C[M'_1] + \cdots + C[M'_k]}$$

Hence the proof follows by the IH on M.

(4) When $\mathbb{M}'$ is reduced to via the Rule $[\mathtt{R} : \mathtt{ECont}]$

$$[\mathtt{R} : \mathtt{ECont}]\ \frac{\mathbb{M} \longrightarrow \mathbb{M}'}{D[\mathbb{M}] \longrightarrow D[\mathbb{M}']}$$

Hence the proof follows by the IH on M. □

Lemma 2.27 (Substitution Lemma for $\lambda^{i}_{\oplus}$)**.** *If* $\Gamma, x : \sigma^k \models M : \tau$ *(with* $k \geq 1$*),* $\mathsf{head}(M) = x$*, and* $\Delta \models N : \sigma$ *then* $\Gamma \wedge \Delta, x : \sigma^{k-1} \models M\{\!|N/x|\!\}$.

Proof. By structural induction on M with $\mathsf{head}(M) = x$. There are three cases to be analyzed:

(1) $M = x$.

This case follows trivially. First, $x : \sigma \models x : \sigma$ and $\Gamma = \emptyset$. Second, $x\{\!|N/x|\!\} = N$, by definition. Since $\Delta \models N : \sigma$, by hypothesis, the result follows.

(2) $M = M'\ B$.

In this case, $\mathsf{head}(M'\ B) = \mathsf{head}(M') = x$, and by inversion of the typing derivation one has the following derivation:

$$[\mathtt{F{:}app}]\ \frac{\Gamma_1, x : \sigma^m \models M' : \delta^j \to \tau \qquad \Gamma_2 \models B : \delta^l}{(\Gamma_1, x : \sigma^m) \wedge \Gamma_2 \models M'B : \tau}$$

where $\Gamma, x : \sigma^k = (\Gamma_1, x : \sigma^m) \wedge \Gamma_2$, δ is a strict type, and j, l, m are non-negative integers, possibly different with $m \geq 1$.

By IH, we get $\Gamma_1 \wedge \Delta, x : \sigma^{m-1} \models M'\{\!|N/x|\!\} : \delta^j \to \tau$, which gives the following derivation:

$$[\mathtt{F{:}app}]\ \frac{\Gamma_1 \wedge \Delta, x : \sigma^{m-1} \models M'\{\!|N/x|\!\} : \delta^j \to \tau \qquad \Gamma_2 \models B : \delta^l}{(\Gamma_1 \wedge \Delta, x : \sigma^{m-1}) \wedge \Gamma_2 \models (M'\{\!|N/x|\!\})B : \tau}$$

Therefore, from Def. 2.8, one has $\Gamma \wedge \Delta, x : \sigma^{k-1} \models (M'B)\{\!|N/x|\!\} : \tau$, and the result follows.

(3) $M = M'\langle\!\langle B/y\rangle\!\rangle$.

In this case, $\mathsf{head}(M'\langle\!\langle B/y\rangle\!\rangle) = \mathsf{head}(M') = x$, with $x \neq y$, and by inversion of the typing derivation one has the following derivation:

$$[\mathtt{F{:}ex\text{-}sub}]\ \frac{\Gamma_1, y : \delta^l, x : \sigma^m \models M' : \tau \qquad \Gamma_2 \models B : \delta^j}{(\Gamma_1, x : \sigma^m) \wedge \Gamma_2 \models M'\langle\!\langle B/y\rangle\!\rangle : \tau}$$

where $\Gamma, x:\sigma^k = (\Gamma_1, x:\sigma^m) \wedge \Gamma_2$, δ is a strict type and j, l, m are positive integers with $m \geq 1$. By IH, we get $(\Gamma_1, y:\delta^l, x:\sigma^{m-1}) \wedge \Delta \models M'\{\!|N/x|\!\} : \tau$ and

$$[\texttt{F:ex-sub}]\ \frac{(\Gamma_1, y:\delta^l, x:\sigma^{m-1}) \wedge \Delta \models M'\{\!|N/x|\!\} : \tau \qquad \Gamma_2 \models B : \delta^j}{(\Gamma_1, y:\delta^l, x:\sigma^{m-1}) \wedge \Delta \wedge \Gamma_2 \models M'\{\!|N/x|\!\}\langle\!\langle B/y\rangle\!\rangle : \tau}$$

From Def. 2.8, $M'\langle\!\langle B/y\rangle\!\rangle\{\!|N/x|\!\} = M'\{\!|N/x|\!\}\langle\!\langle B/y\rangle\!\rangle$, therefore, $\Gamma \wedge \Delta, x : \sigma^{k-1} \models (M'\langle\!\langle B/y\rangle\!\rangle)\{\!|N/x|\!\} : \tau$ and the result follows. □

Theorem 2.28 (Subject Reduction in $\lambda^{\natural}_{\oplus}$)**.** *If* $\Gamma \models \mathbb{M} : \tau$ *and* $\mathbb{M} \longrightarrow \mathbb{M}'$ *then* $\Gamma \models \mathbb{M}' : \tau$.

Proof. By structural induction on the reduction rules. We proceed by analysing the rule applied in $\mathbb{M}$. There are seven cases:

(1) Rule [R : Beta].
Then $\mathbb{M} = (\lambda x.M)B \longrightarrow M\ \langle\!\langle B/x\rangle\!\rangle = \mathbb{M}'$.
Since $\Gamma \models \mathbb{M} : \tau$, by inversion of the typing derivation one has the following derivation:

$$\begin{array}{l}[\texttt{F:abs}]\\ [\texttt{F:app}]\end{array}\ \frac{\dfrac{\Gamma', x:\sigma^j \models M : \tau}{\Gamma' \models \lambda x.M : \sigma^j \to \tau} \qquad \Delta \models B : \sigma^k}{\Gamma' \wedge \Delta \models (\lambda x.M)B : \tau}$$

for $\Gamma = \Gamma' \wedge \Delta$. Notice that

$$[\texttt{F:ex-sub}]\ \frac{\Gamma', x:\sigma^j \models M : \tau \qquad \Delta \models B : \sigma^k}{\Gamma' \wedge \Delta \models M\langle\!\langle B/x\rangle\!\rangle : \tau}$$

Therefore, $\Gamma \models \mathbb{M}' : \tau$ and the result follows.

(2) Rule [R : Fetch].
Then $\mathbb{M} = M\ \langle\!\langle B/x\rangle\!\rangle$, where $B = \wr N_1, \ldots, N_k \int$, $k \geq 1$, $\#(x, M) = k$, and $\mathsf{head}(M) = x$. The reduction is as follows:

$$[\texttt{R} : \texttt{Fetch}]\ \frac{\mathsf{head}(M) = x \qquad B = \wr N_1, \ldots, N_k \int,\ k \geq 1 \qquad \#(x, M) = k}{M\ \langle\!\langle B/x\rangle\!\rangle \to M\{\!|N_1/x|\!\}\langle\!\langle (B \setminus\!\setminus N_1)/x\rangle\!\rangle + \cdots + M\{\!|N_k/x|\!\}\langle\!\langle (B \setminus\!\setminus N_k)/x\rangle\!\rangle}$$

To simplify the proof we take $k = 2$, as the case $k > 2$ is similar. Therefore, by inversion of the typing derivation and $B = \wr N_1, N_2 \int$:

$$[\texttt{F:ex-sub}]\ \frac{\Gamma', x:\sigma \wedge \sigma \models M : \tau \qquad [\texttt{F:bag}]\ \dfrac{\Delta_1 \models N_1 : \sigma \qquad [\texttt{F:bag}]\ \dfrac{\Delta_2 \models N_2 : \sigma \qquad [\texttt{F:1}]\ \dfrac{}{\models 1 : \omega}}{\Delta_2 \models \wr N_2 \int : \sigma}}{\Delta \models B : \sigma \wedge \sigma}}{\Gamma' \wedge \Delta \models M\langle\!\langle B/x\rangle\!\rangle : \tau}$$

where $\Delta = \Delta_1 \wedge \Delta_2$ and $\Gamma = \Gamma' \wedge \Delta$. By the Substitution Lemma (Lemma 2.27), there exists a derivation Π_1 of $(\Gamma', x:\sigma) \wedge \Delta_1 \models M\{\!|N_1/x|\!\} : \tau$ and a derivation Π_2 of $(\Gamma', x:\sigma) \wedge \Delta_2 \models M\{\!|N_2/x|\!\} : \tau$. Therefore, one has the following derivation:

$$\begin{array}{l}[\texttt{F:ex-sub}]\\ [\texttt{F:sum}]\end{array}\ \frac{\dfrac{\Pi_1 \qquad \Delta_2 \models \wr N_2 \int : \sigma}{\Gamma' \wedge \Delta \models M\{\!|N_1/x|\!\}\langle\!\langle \wr N_2 \int / x\rangle\!\rangle : \tau} \qquad [\texttt{F:ex-sub}]\ \dfrac{\Pi_2 \qquad \Delta_1 \models \wr N_1 \int : \sigma}{\Gamma' \wedge \Delta \models M\{\!|N_2/x|\!\}\langle\!\langle \wr N_1 \int / x\rangle\!\rangle : \tau}}{\Gamma' \wedge \Delta \models M\{\!|N_1/x|\!\}\langle\!\langle \wr N_2 \int / x\rangle\!\rangle + M\{\!|N_2/x|\!\}\langle\!\langle \wr N_1 \int / x\rangle\!\rangle : \tau}$$

Assuming $\mathbb{M}' = \{\!|N_1/x|\!\}\langle\!\langle \wr N_2 \int / x\rangle\!\rangle + M\{\!|N_2/x|\!\}\langle\!\langle \wr N_1 \int / x\rangle\!\rangle$, the result follows.

(3) Rule [R : Fail].
Then $\mathbb{M} = M\ \langle\!\langle B/x\rangle\!\rangle$ where $B = \wr N_1, \cdots, N_k \int$, $k \geq 0$, $\#(x, M) \neq k$ and we can perform the following reduction:

$$[\mathtt{R} : \mathtt{Fail}]\ \frac{\#(x, M) \neq \mathsf{size}(B) \qquad \widetilde{y} = (\mathsf{mfv}(M) \setminus x) \uplus \mathsf{mfv}(B)}{M\ \langle\!\langle B/x \rangle\!\rangle \longrightarrow \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{y}}}$$

with $\mathbb{M}' = \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{y}}$. By hypothesis, one has the derivation:

$$[\mathtt{F{:}ex\text{-}sub}]\ \frac{\Delta \models B : \sigma^j \qquad \Gamma', x : \sigma^k \models M : \tau}{\Gamma' \wedge \Delta \models M\langle\!\langle B/x \rangle\!\rangle : \tau}$$

Notice that we also have from $\#(x, M) \neq \mathsf{size}(B)$ that $j \neq k$.Hence $\Gamma = \Gamma' \wedge \Delta$ and we may type the following:

$$\begin{array}{r} [\mathtt{F{:}fail}]\ \dfrac{}{\Gamma \models \mathtt{fail}^{\widetilde{y}} : \tau} \qquad \cdots \qquad [\mathtt{F{:}fail}]\ \dfrac{}{\Gamma \models \mathtt{fail}^{\widetilde{y}} : \tau} \\ [\mathtt{F{:}sum}]\ \dfrac{}{\Gamma \models \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{y}} : \tau} \end{array}$$

(4) Rule $[\mathtt{R} : \mathtt{Cons}_1]$.

Then $\mathbb{M} = \mathtt{fail}^{\widetilde{x}}\ B$ where $B = \wr N_1, \ldots, N_k \wr$, $k \geq 0$ and we can perform the following reduction:

$$[\mathtt{R} : \mathtt{Cons}_1]\ \frac{\mathsf{size}(B) = k \qquad \widetilde{y} = \mathsf{mfv}(B)}{\mathtt{fail}^{\widetilde{x}}\ B \longrightarrow \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{x} \uplus \widetilde{y}}}$$

where $\mathbb{M}' = \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{x} \uplus \widetilde{y}}$. By hypothesis and inversion of the typing derivation, there exists the following derivation:

$$\begin{array}{r} [\mathtt{F{:}fail}]\ \dfrac{}{\Gamma' \models \mathtt{fail}^{\widetilde{x}} : \pi' \to \tau} \qquad \Delta \models B : \pi \\ [\mathtt{F{:}app}]\ \dfrac{}{\Gamma' \wedge \Delta \models \mathtt{fail}^{\widetilde{x}}\ B : \tau} \end{array}$$

Hence $\Gamma = \Gamma' \wedge \Delta$ and we may type the following:

$$\begin{array}{r} [\mathtt{F{:}fail}]\ \dfrac{}{\Gamma \models \mathtt{fail}^{\widetilde{x} \uplus \widetilde{y}} : \tau} \qquad \cdots \qquad [\mathtt{F{:}fail}]\ \dfrac{}{\Gamma \models \mathtt{fail}^{\widetilde{x} \uplus \widetilde{y}} : \tau} \\ [\mathtt{F{:}sum}]\ \dfrac{}{\Gamma \models \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{x} \uplus \widetilde{y}} : \tau} \end{array}$$

(5) Rule $[\mathtt{R} : \mathtt{Cons}_2]$.

Then $\mathbb{M} = \mathtt{fail}^{\widetilde{z}}\ \langle\!\langle B/x \rangle\!\rangle$ where $B = \wr N_1, \ldots, N_k \wr$, $k \geq 1$ and we can perform the following reduction:

$$[\mathtt{R} : \mathtt{Cons}_2]\ \frac{\mathsf{size}(B) = k \qquad \#(x, \widetilde{z}) + k \neq 0 \qquad \widetilde{y} = \mathsf{mfv}(B)}{\mathtt{fail}^{\widetilde{z}}\ \langle\!\langle B/x \rangle\!\rangle \longrightarrow \sum_{\mathsf{PER}(B)} \mathtt{fail}^{(\widetilde{z} \setminus x) \uplus \widetilde{y}}}$$

where $\mathbb{M}' = \sum_{\mathsf{PER}(B)} \mathtt{fail}^{(\widetilde{z} \setminus x) \uplus \widetilde{y}}$. By hypothesis and inversion of the typing derivation, there exists a derivation:

$$\begin{array}{r} [\mathtt{F{:}fail}]\ \dfrac{\mathtt{dom}((\Gamma', x : \sigma^k)^\dagger) = \widetilde{z}}{\Gamma', x : \sigma^k \models \mathtt{fail}^{\widetilde{z}} : \tau} \qquad \Delta \models B : \sigma^j \\ [\mathtt{F{:}ex\text{-}sub}]\ \dfrac{}{\Gamma' \wedge \Delta \models \mathtt{fail}^{\widetilde{z}}\langle\!\langle B/x \rangle\!\rangle : \tau} \end{array}$$

Hence $\Gamma = \Gamma' \wedge \Delta$ and we may type the following:

$$\begin{array}{r} [\mathtt{F{:}fail}]\ \dfrac{}{\Gamma \models \mathtt{fail}^{(\widetilde{z} \setminus x) \uplus \widetilde{y}} : \tau} \qquad \cdots \qquad [\mathtt{F{:}fail}]\ \dfrac{}{\Gamma \models \mathtt{fail}^{(\widetilde{z} \setminus x) \uplus \widetilde{y}} : \tau} \\ [\mathtt{F{:}sum}]\ \dfrac{}{\Gamma \models \sum_{\mathsf{PER}(B)} \mathtt{fail}^{(\widetilde{z} \setminus x) \uplus \widetilde{y}} : \tau} \end{array}$$

(6) Rule $[\mathtt{R} : \mathtt{TCont}]$.

Then $\mathbb{M} = C[M]$ and the reduction is as follows:

$$[\mathtt{R}:\mathtt{TCont}]\ \frac{M \longrightarrow M_1' + \cdots + M_l'}{C[M] \longrightarrow C[M_1'] + \cdots + C[M_l']}$$

where $\mathbb{M}' = C[M_1'] + \cdots + C[M_l']$. The proof proceeds by analysing the context C:

(1) $C = [\cdot]\ B$.
In this case $\mathbb{M} = M\ B$, for some B, and the following derivation holds:

$$[\mathtt{F{:}app}]\ \frac{\Gamma' \models M : \sigma^j \to \tau \qquad \Delta \models B : \sigma^k}{\Gamma' \wedge \Delta \models M\ B : \tau}$$

where $\Gamma = \Gamma' \wedge \Delta$.
Since $\Gamma' \models M : \sigma^j \to \tau$ and $M \longrightarrow M_1' + \ldots + M_l'$, it follows by IH that $\Gamma' \models M_1' + \ldots + M_l' : \sigma^j \to \tau$. By applying [F:sum], one has $\Gamma' \models M_i' : \sigma^j \to \tau$, for $i = 1, \ldots, l$. Therefore, we may type the following:

$$[\mathtt{F{:}sum}]\ \frac{\forall i \in 1, \cdots, l \qquad [\mathtt{F{:}app}]\ \dfrac{\Gamma' \models M_i' : \sigma^j \to \tau \qquad \Delta \models B : \sigma^k}{\Gamma' \wedge \Delta \models (M_i'\ B) : \tau}}{\Gamma' \wedge \Delta \models (M_1'\ B) + \cdots + (M_l'\ B) : \tau}$$

Thus, $\Gamma \models \mathbb{M}' : \tau$, and the result follows.

(2) $C = ([\cdot])\langle\!\langle {}^{B}/_{x} \rangle\!\rangle$.
This case is similar to the previous one.

(7) Rule [R : ECont].
Then $\mathbb{M} = D[\mathbb{M}'']$ where $\mathbb{M}'' \to \mathbb{M}'''$ then we can perform the following reduction:

$$[\mathtt{R}:\mathtt{ECont}]\ \frac{\mathbb{M}'' \longrightarrow \mathbb{M}'''}{D[\mathbb{M}''] \longrightarrow D[\mathbb{M}''']}$$

Hence $\mathbb{M}' = D[\mathbb{M}''']$. The proof proceeds by analysing the context D:

(1) $D = [\cdot] + \mathbb{N}$. In this case $\mathbb{M} = \mathbb{M}'' + \mathbb{N}$ by inversion of the typing derivation:

$$[\mathtt{F{:}sum}]\ \frac{\Gamma \models \mathbb{M}'' : \tau \qquad \Gamma \models \mathbb{N} : \tau}{\Gamma \models \mathbb{M}'' + \mathbb{N} : \tau}$$

Since $\Gamma \vdash \mathbb{M}^{''} : \tau$ and $\mathbb{M}^{''} \longrightarrow \mathbb{M}^{'''}$, by IH, it follows that $\Gamma \vdash \mathbb{M}^{'''} : \tau$ and we may type the following:

$$[\mathtt{F{:}sum}]\ \frac{\Gamma \models \mathbb{M}''' : \tau \qquad \Gamma \models \mathbb{N} : \tau}{\Gamma \models \mathbb{M}''' + \mathbb{N} : \tau}$$

Therefore, $\Gamma \vdash \mathbb{M}' : \tau$ and the result follows.

(2) $D = \mathbb{N} + [\cdot]$. This case is similar to the previous one. □

Appendix B. Appendix to § 3.3

Theorem 3.15 (Consistency Stability Under $\longrightarrow$)**.** *If $\mathbb{M}$ is a consistent $\widehat{\lambda}^{\natural}_{\oplus}$-expression and $\mathbb{M} \longrightarrow \mathbb{M}'$ then $\mathbb{M}'$ is consistent.*

Proof. By structural induction on the reduction rules. We will consider two key reduction rules, the other cases follow analogously via application of the IH.

(1) Rule [RS:Ex-Sub]. In this case, we have

$$[\mathtt{RS{:}Ex{-}Sub}]\ \frac{B = \wr M_1 \int \cdots \wr M_k \int \qquad k \geq 1 \qquad M \neq \mathtt{fail}^{\widetilde{y}}}{M[x_1, \ldots, x_k \leftarrow x]\langle\!\langle {}^{B}/_{x} \rangle\!\rangle \longrightarrow \sum_{B_i \in \mathsf{PER}(B)} M\{\!|B_i(1)/x_1|\!\} \cdots \{\!|B_i(k)/x_k|\!\}}$$

Notice that if a bag is consistent then each element in the bag is consistent, that is, for any permutation B_i of the bag B then each $B_i(n)$ is consistent. Then, the assumption of consistency for $(M[\widetilde{x} \leftarrow x])\langle\!\langle B/x \rangle\!\rangle$, along with each element of the bag being consistent implies consistency of $\sum_{B_i \in \mathsf{PER}(B)} M\langle\!|B_i(1)/x_1|\!\rangle \cdots \langle\!|B_i(k)/x_k|\!\rangle$ for each permutation of B.

(2) Rule [RS:Lin-Fetch]. In this case, we have

$$[\texttt{RS:Lin-Fetch}]\ \frac{\mathsf{head}(M) = x}{M\langle\!|N/x|\!\rangle \longrightarrow M\{\!|N/x|\!\}}$$

This case follows from the fact that $M\{\!|N/x|\!\}$ preserves consistency. The argument is by structural induction, with base case of $M = x$ together with the fact that N is consistent trivially implies that $x\{\!|N/x|\!\}$ must also be consistent. As for the inductive step, notice that 'adding' N to the structure of M does not break any of the consistency requirements: the consistency of $M\langle\!|N/x|\!\rangle$ implies that the free variables of M and N are disjoint.

□

Lemma 3.17 (Linear Anti-substitution Lemma for $\widehat{\lambda}_{\oplus}$)**.** *Let M and N be $\widehat{\lambda}_{\oplus}$-terms such that $\mathsf{head}(M) = x$. The following hold:*

- *If $\Gamma, x : \sigma^{k-1} \vdash M\{\!|N/x|\!\} : \tau$, with $k > 1$, then there exist Γ_1, Γ_2 such that $\Gamma_1, x : \sigma^k \vdash M : \tau$, and $\Gamma_2 \vdash N : \sigma$, where $\Gamma = \Gamma_1 \wedge \Gamma_2$.*
- *If $\Gamma \vdash M\{\!|N/x|\!\} : \tau$, with $x \notin \mathtt{dom}(\Gamma)$, then there exist Γ_1, Γ_2 such that $\Gamma_1, x : \sigma \vdash M : \tau$, and $\Gamma_2 \vdash N : \sigma$, where $\Gamma = \Gamma_1 \wedge \Gamma_2$.*

Proof. By induction on the structure of M:

(1) When $M = x$ then we have $x\{\!|N/x|\!\} = N$ and may derive the derivation of $\Gamma \vdash N : \tau$ with $x \notin \mathtt{dom}(\Gamma)$. By taking $\Gamma_1 = \emptyset$ and $\Gamma_2 = \Gamma$ as $\Gamma = \emptyset \wedge \Gamma$ the case follows as $\Gamma \vdash N : \tau$ and

$$[\mathtt{TS} : \mathtt{var}]\ \frac{}{x : \sigma \vdash x : \sigma}$$

(2) When $M = (M\ B)$ then we have that $(M\ B)\{\!|N/x|\!\} = (M\{\!|N/x|\!\})\ B$. Let us consider two cases:

(I) When $x \in \mathsf{fv}(M\{\!|N/x|\!\})$

$$[\mathtt{TS} : \mathtt{app}]\ \frac{\Gamma', x : \sigma^{k-1} \vdash M\{\!|N/x|\!\} : \pi \to \tau' \qquad \Delta \vdash B : \pi}{(\Gamma', x : \sigma^{k-1}) \wedge \Delta \vdash (M\{\!|N/x|\!\})\ B : \tau'}$$

By the IH we have that $\Gamma', x : \sigma^{k-1} \vdash M\{\!|N/x|\!\} : \pi \to \tau'$ implies that $\exists\ \Gamma'_1, \Gamma_2$ such that $\Gamma'_1, x : \sigma^k \vdash M : \tau$, and $\Gamma_2 \vdash N : \sigma$ with $\Gamma' = \Gamma'_1 \wedge \Gamma_2$.

$$[\mathtt{TS} : \mathtt{app}]\ \frac{\Gamma'_1, x : \sigma^k \vdash M\{\!|N/x|\!\} : \pi \to \tau' \qquad \Delta \vdash B : \pi}{(\Gamma'_1, x : \sigma^k) \wedge \Delta \vdash M\ B : \tau'}$$

(II) When $x \notin \mathsf{fv}(M\{\!|N/x|\!\})$

$$[\mathtt{TS} : \mathtt{app}]\ \frac{\Gamma' \vdash M\{\!|N/x|\!\} : \pi \to \tau' \qquad \Delta \vdash B : \pi}{\Gamma' \wedge \Delta \vdash (M\{\!|N/x|\!\})\ B : \tau'}$$

By the IH we have that $\Gamma' \vdash M\{\!|N/x|\!\}[\widetilde{y} \leftarrow y] : \pi \to \tau'$ implies that $\exists\ \Gamma'_1, \Gamma_2$ such that $\Gamma'_1, x : \sigma \vdash M[\widetilde{y} \leftarrow y] : \tau$, and $\Gamma_2 \vdash N : \sigma$ with $\Gamma' = \Gamma'_1 \wedge \Gamma_2$.

$$[\texttt{TS} : \texttt{app}]\ \frac{\Gamma_1', x : \sigma \vdash M : \pi \to \tau' \qquad \Delta \vdash B : \pi}{(\Gamma_1', x : \sigma) \wedge \Delta \vdash M\ B : \tau'}$$

(3) When $M = M[\widetilde{y} \leftarrow y]\langle\!\langle B/y \rangle\!\rangle$ then we have that $(M[\widetilde{y} \leftarrow y]\langle\!\langle B/y \rangle\!\rangle)\{\!|N/x|\!\} = (M\{\!|N/x|\!\})\ [\widetilde{y} \leftarrow y]\langle\!\langle B/y \rangle\!\rangle$ where $x \neq y$.

(I) When $x \in \mathsf{fv}(M\{\!|N/x|\!\})$:

$$\begin{array}{r} [\texttt{TS:share}]\ \dfrac{\Gamma', x : \sigma^{k-1}, \widetilde{y} : \delta^j \vdash (M\{\!|N/x|\!\}) : \tau}{\Gamma', x : \sigma^{k-1}, y : \delta^j \vdash (M\{\!|N/x|\!\})[\widetilde{y} \leftarrow y] : \tau} \\ [\texttt{TS} : \texttt{ex-sub}]\ \dfrac{}{\Gamma' \wedge \Delta \vdash (M\{\!|N/x|\!\})[\widetilde{y} \leftarrow y]\langle\!\langle B/y \rangle\!\rangle : \tau} \end{array} \qquad \Delta \vdash B : \delta^j$$

By the IH we have that $\Gamma', x : \sigma^{k-1}, \widetilde{y} : \delta^j \vdash (M\{\!|N/x|\!\}) : \tau$ implies that $\exists\ \Gamma_1', \Gamma_2$ such that $\Gamma_1', x : \sigma^k, \widetilde{y} : \delta^j \vdash M : \tau$, and $\Gamma_2 \vdash N : \sigma$ with $\Gamma', y : \delta^j = (\Gamma_1', y : \delta^j) \wedge \Gamma_2$.

$$\begin{array}{r} [\texttt{TS:share}]\ \dfrac{\Gamma_1', x : \sigma^k, \widetilde{y} : \delta^j \vdash M : \tau}{\Gamma_1', x : \sigma^k, y : \delta^j \vdash M[\widetilde{y} \leftarrow y] : \tau} \\ [\texttt{TS} : \texttt{ex-sub}]\ \dfrac{}{\Gamma_1' \wedge \Delta \vdash (M)[\widetilde{y} \leftarrow y]\langle\!\langle B/y \rangle\!\rangle : \tau} \end{array} \qquad \Delta \vdash B : \delta^j$$

(II) When $x \notin \mathsf{fv}(M\{\!|N/x|\!\})$:

$$\begin{array}{r} [\texttt{TS:share}]\ \dfrac{\Gamma', \widetilde{y} : \delta^k \vdash (M\{\!|N/x|\!\}) : \tau}{\Gamma', y : \delta^k \vdash (M\{\!|N/x|\!\})[\widetilde{y} \leftarrow y] : \tau} \\ [\texttt{TS} : \texttt{ex-sub}]\ \dfrac{}{\Gamma' \wedge \Delta \vdash (M\{\!|N/x|\!\})[\widetilde{y} \leftarrow y]\langle\!\langle B/y \rangle\!\rangle : \tau} \end{array} \qquad \Delta \vdash B : \delta^k$$

By the IH we have that $\Gamma', y : \delta^k \vdash (M\{\!|N/x|\!\}) : \tau$ implies that $\exists\ \Gamma_1', \Gamma_2$ such that $\Gamma_1', x : \sigma, \widetilde{y} : \delta^k \vdash M : \tau$, and $\Gamma_2 \vdash N : \sigma$ with $\Gamma', y : \delta^k = (\Gamma_1', y : \delta^k) \wedge \Gamma_2$.

$$\begin{array}{r} [\texttt{TS:share}]\ \dfrac{\Gamma', x : \sigma, \widetilde{y} : \delta^k \vdash M : \tau}{\Gamma', x : \sigma, y : \delta^k \vdash M[\widetilde{y} \leftarrow y] : \tau} \\ [\texttt{TS} : \texttt{ex-sub}]\ \dfrac{}{\Gamma' \wedge \Delta \vdash (M[\widetilde{y} \leftarrow y]\{\!|N/x|\!\})\langle\!\langle B/y \rangle\!\rangle : \tau} \end{array} \qquad \Delta \vdash B : \delta^k$$

(4) When $M = M[\widetilde{y} \leftarrow y]$ then we have that $(M[\widetilde{y} \leftarrow y])\{\!|N/x|\!\} = (M\{\!|N/x|\!\})\ [\widetilde{y} \leftarrow y]$ where $x \neq y$.

(I) When $x \in \mathsf{fv}(M\{\!|N/x|\!\})$:

$$[\texttt{TS:share}]\ \frac{\Gamma', x : \sigma^{k-1}, \widetilde{y} : \delta^j \vdash (M\{\!|N/x|\!\}) : \tau}{\Gamma', x : \sigma^{k-1}, y : \delta^j \vdash (M\{\!|N/x|\!\})[\widetilde{y} \leftarrow y] : \tau}$$

By the IH we have that $\Gamma', x : \sigma^{k-1}, \widetilde{y} : \delta^j \vdash (M\{\!|N/x|\!\}) : \tau$ implies that $\exists\ \Gamma_1', \Gamma_2$ such that $\Gamma_1', x : \sigma^k, \widetilde{y} : \delta^j \vdash M : \tau$, and $\Gamma_2 \vdash N : \sigma$ with $\Gamma', y : \delta^j = (\Gamma_1', y : \delta^j) \wedge \Gamma_2$.

$$[\texttt{TS:share}]\ \frac{\Gamma_1', x : \sigma^k, \widetilde{y} : \delta^j \vdash M : \tau}{\Gamma_1', x : \sigma^k, y : \delta^j \vdash M[\widetilde{y} \leftarrow y] : \tau}$$

(II) When $x \notin \mathsf{fv}(M\{\!|N/x|\!\})$:

$$[\texttt{TS:share}]\ \frac{\Gamma', \widetilde{y} : \delta^k \vdash (M\{\!|N/x|\!\}) : \tau}{\Gamma', y : \delta^k \vdash (M\{\!|N/x|\!\})[\widetilde{y} \leftarrow y] : \tau}$$

By the IH we have that $\Gamma', y : \delta^k \vdash (M\{\!|N/x|\!\}) : \tau$ implies that $\exists\ \Gamma'_1, \Gamma_2$ such that $\Gamma'_1, x : \sigma, \widetilde{y} : \delta^k \vdash M : \tau$, and $\Gamma_2 \vdash N : \sigma$ with $\Gamma', y : \delta^k = (\Gamma'_1, y : \delta^k) \wedge \Gamma_2$.

$$[\texttt{TS:share}]\ \frac{\Gamma', x : \sigma, \widetilde{y} : \delta^k \vdash M : \tau}{\Gamma', x : \sigma, y : \delta^k \vdash M[\widetilde{y} \leftarrow y] : \tau}$$

(5) When $M = M\langle\!|N/y|\!\rangle$ then we have that $(M\langle\!|N/y|\!\rangle)\{\!|N/x|\!\} = (M\{\!|N/x|\!\})\ \langle\!|N/y|\!\rangle$ where $x \neq y$.

(I) When $x \in \mathsf{fv}(M\{\!|N/x|\!\})$:

$$[\texttt{TS:ex-lin-sub}]\ \frac{\Delta \vdash N : \delta \qquad \Gamma', x : \sigma^{k-1}, y : \delta \vdash (M\{\!|N/x|\!\}) : \tau}{\Gamma', x : \sigma^{k-1}, y : \delta, \Delta \vdash (M\{\!|N/x|\!\})\langle\!|N/y|\!\rangle : \tau}$$

By the IH we have that $\Gamma', x : \sigma^{k-1}, \widetilde{y} : \delta^j \vdash (M\{\!|N/x|\!\}) : \tau$ implies that $\exists\ \Gamma'_1, \Gamma_2$ such that $\Gamma'_1, x : \sigma^k, \widetilde{y} : \delta^j \vdash M : \tau$, and $\Gamma_2 \vdash N : \sigma$ with $\Gamma', y : \delta^j = (\Gamma'_1, y : \delta^j) \wedge \Gamma_2$.

$$[\texttt{TS:ex-lin-sub}]\ \frac{\Delta \vdash N : \delta \qquad \Gamma'_1, x : \sigma^k, y : \delta \vdash M : \tau}{\Gamma'_1, x : \sigma^k, y : \delta, \Delta \vdash M\langle\!|N/y|\!\rangle : \tau}$$

(II) When $x \notin \mathsf{fv}(M\{\!|N/x|\!\})$:

$$[\texttt{TS:ex-lin-sub}]\ \frac{\Delta \vdash N : \delta \qquad \Gamma', y : \delta \vdash (M\{\!|N/x|\!\}) : \tau}{\Gamma', y : \delta, \Delta \vdash (M\{\!|N/x|\!\})\langle\!|N/y|\!\rangle : \tau}$$

By the IH we have that $\Gamma', y : \delta^k \vdash (M\{\!|N/x|\!\}) : \tau$ implies that $\exists\ \Gamma'_1, \Gamma_2$ such that $\Gamma'_1, x : \sigma, \widetilde{y} : \delta^k \vdash M : \tau$, and $\Gamma_2 \vdash N : \sigma$ with $\Gamma', y : \delta^k = (\Gamma'_1, y : \delta^k) \wedge \Gamma_2$.

$$[\texttt{TS:ex-lin-sub}]\ \frac{\Delta \vdash N : \delta \qquad \Gamma'_1, x : \sigma, y : \delta \vdash M : \tau}{\Gamma'_1, x : \sigma, y : \delta, \Delta \vdash M\langle\!|N/y|\!\rangle : \tau}$$

(6) When $M = \lambda y.M[\widetilde{y} \leftarrow y]$ then linear head substitution is undefined on this term as $\mathsf{head}(M) \neq x$.

(7) When $M = \mathtt{fail}^{\widetilde{x}}$ then M is not well typed. □

Theorem 3.18 (Subject Expansion for $\widehat{\lambda}_{\oplus}$)**.** *If* $\Gamma \vdash \mathbb{M}' : \tau$ *and* $\mathbb{M} \longrightarrow \mathbb{M}'$ *then* $\Gamma \vdash \mathbb{M} : \tau$.

Proof. By induction on the reduction rule applied. There are five possible cases.

(1) When $\mathbb{M}'$ is reduced to via the Rule $[\texttt{RS} : \texttt{Beta}]$:

$$[\texttt{RS} : \texttt{Beta}]\ \frac{}{(\lambda x.M[\widetilde{x} \leftarrow x])B \longrightarrow M[\widetilde{x} \leftarrow x]\ \langle\!\langle B/x \rangle\!\rangle}$$

Then $\mathbb{M}' = M[\widetilde{x} \leftarrow x]\ \langle\!\langle B/x \rangle\!\rangle$ can be type as followed:

$$[\texttt{TS} : \texttt{ex-sub}]\ \frac{\Gamma, x : \sigma^k \vdash M[\widetilde{x} \leftarrow x] : \tau \qquad \Delta \vdash B : \sigma^k}{\Gamma \wedge \Delta \vdash M[\widetilde{x} \leftarrow x]\langle\!\langle B/x \rangle\!\rangle : \tau}$$

From the typing of $\mathbb{M}'$ we can deduce that $\mathbb{M} = (\lambda x.M[\widetilde{x} \leftarrow x])B$ may be typed by:

$$\begin{array}{l}[\texttt{TS} : \texttt{abs}]\ \dfrac{\Gamma, x : \sigma^k \vdash M[\widetilde{x} \leftarrow x] : \tau}{\Gamma \vdash \lambda x.M[\widetilde{x} \leftarrow x] : \sigma^k \to \tau} \qquad \Delta \vdash B : \sigma^k \\ [\texttt{TS} : \texttt{app}]\ \dfrac{}{\Gamma \wedge \Delta \vdash (\lambda x.M[\widetilde{x} \leftarrow x])B : \tau}\end{array}$$

(2) When $\mathbb{M}'$ is reduced to via the Rule [RS:Ex-Sub]:

$$[\texttt{RS:Ex-Sub}]\ \frac{B = \wr M_1 \wr \cdots \wr M_k \wr \qquad k \geq 1 \qquad M \neq \mathtt{fail}^{\widetilde{y}}}{M[x_1, \ldots, x_k \leftarrow x]\langle\!\langle {}^{B}/_{x} \rangle\!\rangle \longrightarrow \sum_{B_i \in \mathsf{PER}(B)} M\langle\!|B_i(1)/x_1|\!\rangle \cdots \langle\!|B_i(k)/x_k|\!\rangle}$$

Then $\mathbb{M}' = M[x_1, \ldots, x_k \leftarrow x]\langle\!\langle {}^{B}/_{x} \rangle\!\rangle$ can be type as followed:

$$\dfrac{\dfrac{\Gamma, x_1 : \sigma, \cdots, x_k : \sigma \vdash M : \tau \qquad \Delta_1 \vdash B_i(1) : \sigma}{\vdots \qquad\qquad \Delta_k \vdash B_i(k) : \sigma}\ [\texttt{TS:ex-lin-sub}]}{\dfrac{\Gamma, \Delta_1, \cdots, \Delta_k \vdash M\langle\!|B_i(1)/x_1|\!\rangle \cdots \langle\!|B_i(k)/x_k|\!\rangle : \tau \qquad \forall B_i \in \mathsf{PER}(B)}{\Gamma, \Delta_1, \cdots, \Delta_k \vdash \sum_{B_i \in \mathsf{PER}(B)} M\langle\!|B_i(1)/x_1|\!\rangle \cdots \langle\!|B_i(k)/x_k|\!\rangle : \tau}\ [\texttt{TS:sum}]}$$

From the typing of $\mathbb{M}'$ we can deduce that $\mathbb{M} = (\lambda x.M[\widetilde{x} \leftarrow x])B$ may be typed by:

$$\dfrac{\dfrac{\dfrac{\Delta_k \vdash M_k : \sigma}{\Delta_1 \vdash M_1 : \sigma \qquad \vdots}\ [\texttt{TS:bag}]}{\Delta_1, \cdots, \Delta_k \vdash B : \sigma^k} \qquad \dfrac{\Gamma, x_1 : \sigma, \cdots, x_k : \sigma \vdash M : \tau}{\Gamma, x : \sigma^k \vdash M[\widetilde{x} \leftarrow x] : \tau}}{\Gamma, \Delta_1, \cdots, \Delta_k \vdash M[\widetilde{x} \leftarrow x]\langle\!\langle {}^{B}/_{x} \rangle\!\rangle : \tau}\ [\texttt{TS: ex-sub}]$$

(3) When $\mathbb{M}'$ is reduced to via the Rule [RS:Lin-Fetch]:

$$[\texttt{RS:Lin-Fetch}]\ \frac{\mathsf{head}(M) = x}{M\langle\!|N/x|\!\rangle \longrightarrow M\{\!|N/x|\!\}}$$

The result follow from Lemma 3.17.

(4) When $\mathbb{M}'$ is reduced to via the Rule [RS : TCont]:

$$[\texttt{RS : TCont}]\ \frac{M \longrightarrow M'_1 + \cdots + M'_k}{C[M] \longrightarrow C[M'_1] + \cdots + C[M'_k]}$$

Hence the proof follows by the IH on M.

(5) When $\mathbb{M}'$ is reduced to via the Rule [RS : ECont]:

$$[\texttt{RS : ECont}]\ \frac{\mathbb{M} \longrightarrow \mathbb{M}'}{D[\mathbb{M}] \longrightarrow D[\mathbb{M}']}$$

Hence the proof follows by the IH on M. □

Lemma 3.21 (Substitution Lemma for $\widehat{\lambda}^{\iota}_{\oplus}$)**.** *If* $\Gamma, x : \sigma \models M : \tau$, $\mathsf{head}(M) = x$, *and* $\Delta \models N : \sigma$ *then* $\Gamma, \Delta \models M\{\!|N/x|\!\} : \tau$.

Proof. By structural induction on M with $\mathsf{head}(M) = x$. There are six cases to be analyzed:

(1) $M = x$.

In this case, $x : \sigma \models x : \sigma$ and $\Gamma = \emptyset$. Observe that $x\{\!|N/x|\!\} = N$, since $\Delta \models N : \sigma$, by hypothesis, the result follows.

(2) $M = M'\ B$.

Then $\mathsf{head}(M'\ B) = \mathsf{head}(M') = x$, and the derivation is the following by inversion of the typing derivation:

$$[\texttt{FS:app}]\ \frac{\Gamma_1, x : \sigma \models M' : \delta^j \to \tau \qquad \Gamma_2 \models B : \delta^k}{\Gamma_1, \Gamma_2, x : \sigma \models M'B : \tau}$$

where $\Gamma = \Gamma_1, \Gamma_2$, and j, k are non-negative integers, possibly different. Since $\Delta \vdash N : \sigma$, by IH, the result holds for M', that is,

$$\Gamma_1, \Delta \models M'\{\!|N/x|\!\} : \delta^j \to \tau$$

which gives the derivation:

$$[\texttt{FS:app}]\ \frac{\Gamma_1, \Delta \models M'\{\!|N/x|\!\} : \delta^j \to \tau \qquad \Gamma_2 \models B : \delta^k}{\Gamma_1, \Gamma_2, \Delta \models (M'\{\!|N/x|\!\})B : \tau}$$

From Def. 3.5, $(M'B)\{\!|N/x|\!\} = (M'\{\!|N/x|\!\})B$, therefore, $\Gamma, \Delta \models (M'B)\{\!|N/x|\!\} : \tau$ and the result follows.

(3) $M = M'[\widetilde{y} \leftarrow y]$.

Then $\mathsf{head}(M'[\widetilde{y} \leftarrow y]) = \mathsf{head}(M') = x$, for $y \neq x$. Therefore by inversion of the typing derivation,

$$[\texttt{FS:share}]\ \frac{\Gamma_1, y_1 : \delta, \cdots, y_k : \delta, x : \sigma \models M' : \tau \quad y \notin \Gamma_1 \quad k \neq 0}{\Gamma_1, y : \delta^k, x : \sigma \models M'[y_1, \cdots, y_k \leftarrow y] : \tau}$$

where $\Gamma = \Gamma_1, y : \delta^k$. By IH, the result follows for M', that is,

$$\Gamma_1, y_1 : \delta, \cdots, y_k : \delta, \Delta \models M'\{\!|N/x|\!\} : \tau$$

and we have the derivation:

$$[\texttt{FS:share}]\ \frac{\Gamma_1, y_1 : \delta, \cdots, y_k : \delta, \Delta \models M'\{\!|N/x|\!\} : \tau \quad y \notin \Gamma_1 \quad k \neq 0}{\Gamma_1, y : \delta^k, \Delta \models M'\{\!|N/x|\!\}[\widetilde{y} \leftarrow y] : \tau}$$

From Def. 3.5 one has $M'[\widetilde{y} \leftarrow y]\{\!|N/x|\!\} = M'\{\!|N/x|\!\}[\widetilde{y} \leftarrow y]$. Therefore, $\Gamma, \Delta \models M'[\widetilde{y} \leftarrow y]\{\!|N/x|\!\} : \tau$ and the result follows.

(4) $M = M'[\leftarrow y]$.

Then $\mathsf{head}(M'[\leftarrow y]) = \mathsf{head}(M') = x$ with $x \neq y$,

$$[\texttt{FS:weak}]\ \frac{\Gamma, x : \sigma \models M : \tau}{\Gamma, y : \omega, x : \sigma \models M[\leftarrow y] : \tau}$$

and $M'[\leftarrow y]\{\!|N/x|\!\} = M'\{\!|N/x|\!\}[\leftarrow y]$. Then by the IH:

$$[\texttt{FS:weak}]\ \frac{\Gamma, \Delta \models M\{\!|N/x|\!\} : \tau}{\Gamma, y : \omega, \Delta \models M\{\!|N/x|\!\}[\leftarrow y] : \tau}$$

(5) $M = M'[\widetilde{y} \leftarrow y]\langle\!\langle B/y \rangle\!\rangle$.

Then $\mathsf{head}(M'[\widetilde{y} \leftarrow y]\langle\!\langle B/y \rangle\!\rangle) = \mathsf{head}(M'[\widetilde{y} \leftarrow y]) = x \neq y$ by inversion of the typing derivation we have:

$$[\texttt{FS:ex-sub}]\ \frac{\Gamma_1, \hat{y} : \delta^k, x : \sigma \models M'[\widetilde{y} \leftarrow y] : \tau \qquad \Gamma_2 \models B : \delta^j}{\Gamma_1, \Gamma_2, x : \sigma \models M'[\widetilde{y} \leftarrow y]\langle\!\langle B/y \rangle\!\rangle : \tau}$$

and $M'[\widetilde{y} \leftarrow y]\langle\!\langle B/y \rangle\!\rangle\{\!|N/x|\!\} = M'[\widetilde{y} \leftarrow y]\{\!|N/x|\!\}\langle\!\langle B/y \rangle\!\rangle$. By IH:

$$[\texttt{FS:ex-sub}]\ \frac{\Gamma_1, \hat{y} : \delta^k, \Delta \models M'[\widetilde{y} \leftarrow y]\{\!|N/x|\!\} : \tau \qquad \Gamma_2 \models B : \delta^j}{\Gamma_1, \Gamma_2, \Delta \models M'[\widetilde{y} \leftarrow y]\{\!|N/x|\!\}\langle\!\langle B/y \rangle\!\rangle : \tau}$$

(6) $M = M'\langle\!|M''/y|\!\rangle$.

Then $\mathsf{head}(M'\langle\!|M''/y|\!\rangle) = \mathsf{head}(M') = x \neq y$, by inversion of the typing derivation we have:

$$[\texttt{FS:ex-lin-sub}]\ \frac{\Delta \models M'' : \delta \qquad \Gamma, y : \delta, x : \sigma \models M : \tau}{\Gamma_1, \Gamma_2, x : \sigma \models M'\langle\!|M''/y|\!\rangle : \tau}$$

and $M'\langle\!\langle M''/y\rangle\!\rangle\{\!|N/x|\!\} = M'\{\!|N/x|\!\}\langle\!\langle M''/y\rangle\!\rangle$. Then by the IH:

$$[\texttt{FS:ex-lin-sub}]\ \frac{\Delta \models M'' : \delta \qquad \Gamma, y : \delta, \Delta \models M'\{\!|N/x|\!\} : \tau}{\Gamma_1, \Gamma_2, \Delta \models M'\{\!|N/x|\!\}\langle\!\langle M''/y\rangle\!\rangle : \tau}$$

□

Theorem 3.22 (Subject Reduction in $\widehat{\lambda}^{\mathcal{L}}_{\oplus}$)**.** *If* $\Gamma \models \mathbb{M} : \tau$ *and* $\mathbb{M} \longrightarrow \mathbb{M}'$ *then* $\Gamma \models \mathbb{M}' : \tau$.

Proof. By structural induction on the reduction rule from Fig. 5 applied in $\mathbb{M} \longrightarrow \mathbb{N}$. There are nine cases to be analyzed:

(1) Rule [RS:Beta].
Then $\mathbb{M} = (\lambda x.M[\widetilde{x} \leftarrow x])B$ and the reduction is:

$$[\texttt{RS:Beta}]\ \frac{}{(\lambda x.M[\widetilde{x} \leftarrow x])B \longrightarrow M[\widetilde{x} \leftarrow x]\ \langle\!\langle B/x\rangle\!\rangle}$$

where $\mathbb{M}' = M[\widetilde{x} \leftarrow x]\ \langle\!\langle B/x\rangle\!\rangle$. Since $\Gamma \models \mathbb{M} : \tau$ we get the following derivation by inversion of the typing derivation:

$$\begin{array}{rl} [\texttt{FS:share}] & \dfrac{\Gamma', x_1 : \sigma, \cdots, x_j : \sigma \models M : \tau}{\Gamma', x : \sigma^j \models M[\widetilde{x} \leftarrow x] : \tau} \\ [\texttt{FS:abs-sh}] & \dfrac{}{\Gamma' \models \lambda x.M[\widetilde{x} \leftarrow x] : \sigma^j \to \tau} \qquad \Delta \models B : \sigma^k \\ [\texttt{FS:app}] & \dfrac{}{\Gamma', \Delta \models (\lambda x.M[\widetilde{x} \leftarrow x])B : \tau} \end{array}$$

for $\Gamma = \Gamma', \Delta$ and $x \notin \texttt{dom}(\Gamma')$. Notice that:

$$\begin{array}{rl} [\texttt{FS:share}] & \dfrac{\Gamma', x_1 : \sigma, \cdots, x_j : \sigma \models M : \tau}{\Gamma', x : \sigma^j \models M[\widetilde{x} \leftarrow x] : \tau} \\ [\texttt{FS:ex-sub}] & \dfrac{}{\Gamma', \Delta \models M[\widetilde{x} \leftarrow x]\ \langle\!\langle B/x\rangle\!\rangle : \tau} \qquad \Delta \models B : \sigma^k \end{array}$$

Therefore $\Gamma', \Delta \models \mathbb{M}' : \tau$ and the result follows.

(2) Rule [RS:Ex-Sub].
Then $\mathbb{M} = M[x_1, \cdots, x_k \leftarrow x]\ \langle\!\langle B/x\rangle\!\rangle$ where $B = \wr N_1, \ldots, N_k \int$. By inversion of the typing derivation the reduction is:

$$[\texttt{RS:Ex-Sub}]\ \frac{B = \wr N_1, \cdots, N_k \int \quad k \geq 1 \qquad M \neq \texttt{fail}^{\widetilde{y}}}{M[x_1, \cdots, x_k \leftarrow x]\ \langle\!\langle B/x\rangle\!\rangle \longrightarrow \sum_{B_i \in \mathsf{PER}(B)} M\ \langle\!\langle B_i(1)/x_1\rangle\!\rangle \cdots \langle\!\langle B_i(k)/x_k\rangle\!\rangle}$$

and $\mathbb{M}' = \sum_{B_i \in \mathsf{PER}(B)} M\ \langle\!\langle B_i(1)/x_1\rangle\!\rangle \cdots \langle\!\langle B_i(k)/x_k\rangle\!\rangle$. To simplify the proof we take $k = 2$, as the case $k > 2$ is similar. Therefore,

- $B = \wr N_1, N_2 \int$; and
- $\mathsf{PER}(B) = \{\wr N_1, N_2 \int, \wr N_2, N_1 \int\}$

Since $\Gamma \models \mathbb{M} : \tau$ we get a derivation where we first type the bag B with the derivation Π, given next:

$$[\texttt{FS:bag}]\ \frac{\Delta_1 \models N_1 : \sigma \qquad [\texttt{FS:bag}]\ \dfrac{\Delta_2 \models N_2 : \sigma \qquad [\texttt{FS:1}]\ \dfrac{}{\models \mathtt{1} : \omega}}{\Delta_2 \models \wr N_2 \int : \sigma}}{\Delta \models B : \sigma \wedge \sigma}$$

The full derivation is as follows:

$$\begin{array}{rl} [\texttt{FS:share}] & \dfrac{\Gamma', x_1 : \sigma, x_2 : \sigma \models M : \tau}{\Gamma', x : \sigma \wedge \sigma \models M[\widetilde{x} \leftarrow x] : \tau} \\ [\texttt{FS:ex-sub}] & \dfrac{}{\Gamma', \Delta \models M[\widetilde{x} \leftarrow x]\ \langle\!\langle B/x\rangle\!\rangle : \tau} \qquad \Pi \end{array}$$

where $\Delta = \Delta_1, \Delta_2$ and $\Gamma = \Gamma', \Delta$. We can build a derivation $\Pi_{1,2}$ of $\Gamma', \Delta \models M\langle\!|N_1/x_1|\!\rangle\langle\!|N_2/x_2|\!\rangle : \tau$ as :

$$[\texttt{FS:ex-lin-sub}]\ \frac{\Gamma', x_1 : \sigma, x_2 : \sigma \models M : \tau \qquad \Delta_1 \models N_1 : \sigma}{[\texttt{FS:ex-lin-sub}]\ \dfrac{\Gamma, \Delta_1, x_2 : \sigma \models M\langle\!|N_1/x_1|\!\rangle : \tau \qquad \Delta_2 \models N_2 : \sigma}{\Gamma', \Delta \models M\langle\!|N_1/x_1|\!\rangle\langle\!|N_2/x_2|\!\rangle : \tau}}$$

Similarly, we can obtain a derivation $\Pi_{2,1}$ of $\Gamma', \Delta \models M\langle\!|N_2/x_1|\!\rangle\langle\!|N_1/x_2|\!\rangle : \tau$. Finally, applying Rule [FS:sum]:

$$[\texttt{FS:sum}]\ \frac{\Pi_{1,2} \qquad \Pi_{2,1}}{\Gamma', \Delta \models M\langle\!|N_1/x_1|\!\rangle\langle\!|N_2/x_k|\!\rangle + M\langle\!|N_2/x_1|\!\rangle\langle\!|N_1/x_k|\!\rangle : \tau}$$

and the result follows.

(3) Rule [RS:Lin-Fetch].

Then $\mathbb{M} = M\ \langle\!|N/x|\!\rangle$ where $\mathsf{head}(M) = x$. The reduction is:

$$[\texttt{RS:Lin-Fetch}]\ \frac{\mathsf{head}(M) = x}{M\ \langle\!|N/x|\!\rangle \longrightarrow M\{\!|N/x|\!\}}$$

and $\mathbb{M}' = M\{\!|N/x|\!\}$. Since $\Gamma \models \mathbb{M} : \tau$ we get the following derivation by inversion of the typing derivation:

$$[\texttt{FS:ex-lin-sub}]\ \frac{\Delta \models N : \sigma \qquad \Gamma', x : \sigma \models M : \tau}{\Gamma', \Delta \models M\langle\!|N/x|\!\rangle : \tau}$$

where $\Gamma = \Gamma', \Delta$. By the Substitution Lemma (Lemma 3.21), we obtain a derivation $\Gamma', \Delta \models M\{\!|N/x|\!\} : \tau$, and the result follows.

(4) Rule [RS:TCont].

Then $\mathbb{M} = C[M]$ and the reduction is as follows:

$$[\texttt{RS:TCont}]\ \frac{M \longrightarrow M'_1 + \cdots + M'_k}{C[M] \longrightarrow C[M'_1] + \cdots + C[M'_k]}$$

with $\mathbb{M}' = C[M'_1] + \cdots + C[M'_k]$. The proof proceeds by analysing the context C. There are four cases:

(1) $C = [\cdot]\ B$.

In this case $\mathbb{M} = M\ B$, for some B. Since $\Gamma \vdash \mathbb{M} : \tau$ by inversion of the typing derivation, one has the derivation:

$$[\texttt{FS:app}]\ \frac{\Gamma' \models M : \sigma^j \to \tau \qquad \Delta \models B : \sigma^k}{\Gamma', \Delta \models M\ B : \tau}$$

where $\Gamma = \Gamma', \Delta$. From $\Gamma' \models M : \sigma^j \to \tau$ and the reduction $M \longrightarrow M'_1 + \cdots + M'_k$, one has by IH that $\Gamma' \models M'_1 + \ldots, M'_k : \sigma^j \to \tau$, which entails $\Gamma' \models M'_i : \sigma^j \to \tau$, for $i = 1, \ldots, k$, via Rule [FS:sum]. Finally, we may type the following:

$$[\texttt{FS:sum}]\ \frac{\forall i \in 1, \cdots, l \qquad [\texttt{FS:app}]\ \dfrac{\Gamma' \models M'_i : \sigma^j \to \tau \qquad \Delta \models B : \sigma^k}{\Gamma', \Delta \models (M'_i\ B) : \tau}}{\Gamma', \Delta \models (M'_1\ B) + \cdots + (M'_l\ B) : \tau}$$

Since $\mathbb{M}' = (C[M'_1]) + \cdots + (C[M'_l]) = M'_1 B + \ldots + M'_k B$, the result follows.

(2) Cases $C = [\cdot]\langle\!|N/x|\!\rangle$ and $C = [\cdot][\widetilde{x} \leftarrow x]$ are similar to the previous one.

(3) $C = [\cdot][\leftarrow x]\langle\!\langle \mathtt{1}/x \rangle\!\rangle$
In this case $\mathbb{M} = C[M] = M[\leftarrow x]\langle\!\langle \mathtt{1}/x \rangle\!\rangle$. Since $\Gamma \models \mathbb{M} : \tau$ by inversion of the typing derivation, one has a derivation

$$\dfrac{[\mathtt{FS\text{-}weak}]\ \dfrac{\Gamma \models M : \tau}{\Gamma, x : \omega \models M[\leftarrow x] : \tau} \qquad [\mathtt{FS{:}wf\text{-}bag}]\ \dfrac{[\mathtt{TS{:}1}]\ \dfrac{}{\vdash \mathtt{1} : \omega}}{\models \mathtt{1} : \omega}}{[\mathtt{FS{:}ex\text{-}sub}]\ \Gamma \models M[\leftarrow x]\langle\!\langle \mathtt{1}/x \rangle\!\rangle : \tau}$$

From $M \longrightarrow M_1 + \ldots + M_k$ and $\Gamma \models M : \tau$, by the IH, it follows that $\Gamma \models M_1 + \ldots + M_k : \tau$, and consequently, $\Gamma \models M_i$, via application of [FS:sum]. Therefore, there exists a derivation

$$\dfrac{\dfrac{\Gamma \models M_i : \tau}{\Gamma, x : \omega \models M_i[\leftarrow x] : \tau} \qquad \models \mathtt{1} : \omega}{\Gamma \models M_i[\leftarrow x]\langle\!\langle \mathtt{1}/x \rangle\!\rangle : \tau}$$

for each $i = 1, \ldots, k$. By applying [FS:sum], we obtain $\Gamma \models M_1[\leftarrow x]\langle\!\langle \mathtt{1}/x \rangle\!\rangle + \ldots + M_k[\leftarrow x]\langle\!\langle \mathtt{1}/x \rangle\!\rangle : \tau$, and the result follows.

(5) Rule [RS:ECont].
Then $\mathbb{M} = D[\mathbb{M}_1]$ where $\mathbb{M}_1 \longrightarrow \mathbb{M}_2$ then we can perform the following reduction:

$$[\mathtt{RS{:}ECont}]\ \dfrac{\mathbb{M}_1 \longrightarrow \mathbb{M}_2}{D[\mathbb{M}_1] \longrightarrow D[\mathbb{M}_2]}$$

and $\mathbb{M}' = D[\mathbb{M}_2]$.
The proof proceeds by analysing the context D. There are two cases: $D = [\cdot] + \mathbb{N}$ and $D = \mathbb{N} + [\cdot]$. We analyze only the first one:
$D = [\cdot] + \mathbb{N}$. In this case $\mathbb{M} = \mathbb{M}_1 + \mathbb{N}$ and by inversion of the typing derivation:

$$[\mathtt{FS{:}sum}]\ \dfrac{\Gamma \models \mathbb{M}_1 : \tau \qquad \Gamma \models \mathbb{N} : \tau}{\Gamma \models \mathbb{M}_1 + \mathbb{N} : \tau}$$

From $\Gamma \models \mathbb{M}_1 : \tau$ and $\mathbb{M}_1 \longrightarrow \mathbb{M}_2$, by IH, one has that $\Gamma \models \mathbb{M}_2 : \tau$. Hence we may type the following:

$$[\mathtt{FS{:}sum}]\ \dfrac{\Gamma \models \mathbb{M}_2 : \tau \qquad \Gamma \models \mathbb{N} : \tau}{\Gamma \models \mathbb{M}_2 + \mathbb{N} : \tau}$$

Since $\mathbb{M}' = D[\mathbb{M}_2] = \mathbb{M}_2 + \mathbb{N}$, the result follows.

(6) Rule [RS:Fail].
Then $\mathbb{M} = M[x_1, \cdots, x_k \leftarrow x]\ \langle\!\langle B/x \rangle\!\rangle$ where $B = \wr N_1, \ldots, N_l \wr$ and the reduction is:

$$[\mathtt{RS{:}Fail}]\ \dfrac{k \neq \mathsf{size}(B) \qquad \widetilde{y} = (\mathsf{fv}(M) \setminus \{x_1, \cdots, x_k\}) \cup \mathsf{fv}(B)}{M[x_1, \cdots, x_k \leftarrow x]\ \langle\!\langle B/x \rangle\!\rangle \longrightarrow \sum_{B_i \in \mathsf{PER}(B)} \mathtt{fail}^{\widetilde{y}}}$$

where $\mathbb{M}' = \sum_{B_i \in \mathsf{PER}(B)} \mathtt{fail}^{\widetilde{y}}$. Since $\Gamma \models \mathbb{M}$ and by inversion of the typing derivation, one has a derivation:

$$\dfrac{[\mathtt{FS{:}ex\text{-}sub}]\ \dfrac{\Gamma', x_1 : \sigma, \ldots, x_k : \sigma \models M : \tau}{[\mathtt{FS{:}ex\text{-}sub}]\ \dfrac{\Gamma', x : \sigma^k \models M[x_1, \cdots, x_k \leftarrow x] : \tau}{\Gamma', \Delta \models M[x_1, \cdots, x_k \leftarrow x]\ \langle\!\langle B/x \rangle\!\rangle : \tau}} \qquad \Delta \models B : \sigma^j}$$

where $\Gamma = \Gamma', \Delta$. We may type the following:

$$[\mathtt{FS{:}fail}]\ \dfrac{}{\Gamma', \Delta \models \mathtt{fail}^{\widetilde{y}} : \tau}$$

since Γ', Δ contain assignments on the free variables in M and B. Therefore, $\Gamma \models \mathtt{fail}^{\widetilde{y}} : \tau$, by applying [FS:sum], it follows that $\Gamma \models \sum_{B_i \in \mathsf{PER}(B)} \mathtt{fail}^{\widetilde{y}} : \tau$, as required.

(7) Rule [RS:Cons$_1$].

Then $\mathbb{M} = \mathtt{fail}^{\widetilde{x}}\ B$ where $B = \wr N_1, \ldots, N_k \wr$ and the reduction is:

$$[\text{RS:Cons}_1]\ \frac{B = \wr N_1, \ldots, N_k \wr \qquad \widetilde{y} = \mathsf{fv}(B)}{\mathtt{fail}^{\widetilde{x}}\ B \longrightarrow \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{x} \cup \widetilde{y}}}$$

and $\mathbb{M}' = \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{x} \cup \widetilde{y}}$. Since $\Gamma \models \mathbb{M} : \tau$ and by inversion of the typing derivation, one has the derivation:

$$\begin{array}{c} [\text{FS:fail}]\ \dfrac{}{\Gamma' \models \mathtt{fail}^{\widetilde{x}} : \omega \to \tau} \qquad \Delta \models B : \pi \\ [\text{FS:app}]\ \dfrac{}{\Gamma', \Delta \models \mathtt{fail}^{\widetilde{x}}\ B : \tau} \end{array}$$

where $\Gamma = \Gamma', \Delta$. After $\mathsf{PER}(B)$ applications of [FS:sum], we obtain $\Gamma \models \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{x} \cup \widetilde{y}} : \tau$, and the result follows.

(8) Rule [RS:Cons$_2$].

Then $\mathbb{M} = (\mathtt{fail}^{\widetilde{x} \cup \widetilde{y}}[\widetilde{x} \leftarrow x])\langle\!\langle B/x \rangle\!\rangle$for $B = \wr N_1, \ldots, N_k \wr$ and the reduction is:

$$[\text{RS:Cons}_2]\ \frac{B = \wr N_1, \ldots, N_k \wr \quad k + |\widetilde{x}| \neq 0 \qquad \widetilde{y} = \mathsf{fv}(B)}{(\mathtt{fail}^{\widetilde{x} \cup \widetilde{y}}[\widetilde{x} \leftarrow x])\langle\!\langle B/x \rangle\!\rangle \longrightarrow \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{y} \cup \widetilde{z}}}$$

with $\mathbb{M}' = \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{y} \cup \widetilde{z}}$. Since $\Gamma \models \mathbb{M} : \tau$ and by inversion of the typing derivation, one has the derivation:

$$\begin{array}{c} [\text{FS:fail}]\ \dfrac{}{\Delta, x_1 : \sigma, \cdots, x_j : \sigma \models \mathtt{fail}^{\widetilde{x} \cup \widetilde{y}} : \tau \quad x \notin \Delta \quad k \neq 0} \\ [\text{FS:share}]\ \dfrac{}{\Delta, x : \sigma^j \models \mathtt{fail}^{\widetilde{x} \cup \widetilde{y}}[x_1, \cdots, x_j \leftarrow x] : \tau} \qquad \Delta \models B : \sigma^k \\ [\text{FS:ex-sub}]\ \dfrac{}{\Gamma, \Delta \models \mathtt{fail}^{\widetilde{x} \cup \widetilde{y}}[\widetilde{x} \leftarrow x]\langle\!\langle B/x \rangle\!\rangle : \tau} \end{array}$$

Hence $\Gamma = \Gamma', \Delta$ and $\mathbb{M}' = \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{y} \cup \widetilde{z}}$ and we may type the following:

$$\begin{array}{c} [\text{FS:fail}]\ \dfrac{}{\Gamma \models \mathtt{fail}^{\widetilde{y} \cup \widetilde{z}} : \tau} \qquad \cdots \\ [\text{FS:sum}]\ \dfrac{}{\Gamma \models \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{y} \cup \widetilde{z}} : \tau} \end{array}$$

(9) Rule [RS:Cons$_3$].

Then $\mathbb{M} = \mathtt{fail}^{\widetilde{y} \cup x}$ and the reduction is

$$[\text{RS:Cons}_3]\ \frac{\widetilde{z} = \mathsf{fv}(N)}{\mathtt{fail}^{\widetilde{y} \cup x}\langle\!|N/x|\!\rangle \longrightarrow \mathtt{fail}^{\widetilde{y} \cup \widetilde{z}}}$$

with $\mathbb{M}' = \mathtt{fail}^{\widetilde{y} \cup \widetilde{z}}$. Since $\Gamma \models \mathbb{M}$ and by inversion of the typing derivation, one has the derivation

$$\begin{array}{c} [\text{FS:fail}]\ \dfrac{}{\Gamma', x : \sigma \models \mathtt{fail}^{\widetilde{y} \cup x} : \tau} \qquad \Delta \models N : \sigma \\ [\text{FS:ex-lin-sub}]\ \dfrac{}{\Gamma', \Delta \models \mathtt{fail}^{\widetilde{y} \cup x}\langle\!|N/x|\!\rangle : \tau} \end{array}$$

where $x \notin \mathtt{dom}(\Gamma')$, $\mathtt{dom}(\Gamma') = \widetilde{y}$ and $\mathtt{dom}(\Delta) = \widetilde{z} = \mathsf{fv}(N)$.

We can type the following:

$$[\text{FS:fail}]\ \frac{}{\Gamma', \Delta \models \mathtt{fail}^{\widetilde{y} \cup \widetilde{z}} : \tau}$$

and the result follows. □

Theorem 3.24 (Consistency enforced by typing)**.** *Let* $\mathbb{M}$ *be a* $\widehat{\lambda}^{\mathsf{lf}}_{\oplus}$*-expression. If* $\Gamma \models \mathbb{M}$ *then* $\mathbb{M}$ *is consistent.*

Proof. By induction on the typing derivation, with a case analysis on the last applied rule (Figure 7). We only consider the cases for the typing rules that relate to the sharing construct and the explicit substitution. First, consider conditions 1(i) to 1(iv), which are related to $M[\widetilde{x} \leftarrow x]$. The conditions are as follows (i) $\widetilde{x}$ contains pairwise distinct variables; (ii) every $x_i \in \widetilde{x}$ must occur exactly once in M; (iii) x_i is not a sharing variable; (iv) M is consistent. By considering rule [FS:share], we have:

$$[\texttt{FS:share}]\ \frac{\Gamma, x_1 : \sigma, \cdots, x_k : \sigma \models M : \tau \quad x \notin \mathtt{dom}(\Gamma) \quad k \neq 0}{\Gamma, x : \sigma^k \models M[x_1, \cdots, x_k \leftarrow x] : \tau}$$

Condition 1(i) follows from uniquness of variables within the context. Condition 1(ii) follows from the premise, which ensures that M is well-formed with a context including each x_i; linearity conditions imply that each x_i must be consumed so it must occur in M. Condition 1(iii) also follows directly from the well-formedness of M: each x_i is typed with a strict type, and the rule ensures that the sharing variable x is typed with the multiset type σ^k. Finally condition 1(iv) is ensured by the IH.

For conditions 2(i) to 2(iv) which are (i) the variable x must occur exactly once in M; (ii) x cannot be a sharing variable; (iii) M and N are consistent; (iv) $\mathsf{fv}(M) \cap \mathsf{fv}(N) = \emptyset$. Consider the case of rule [FS:ex-lin-sub]:

$$[\texttt{FS:ex-lin-sub}]\ \frac{\Gamma, x : \sigma \models M : \tau \quad \Delta \models N : \sigma}{\Gamma, \Delta \models M\langle\!\langle N/x \rangle\!\rangle : \tau}$$

First, because Γ and Δ are disjoint, x cannot appear within Δ and M must consume the type of $x : \sigma$; hence x must occur in M, satisfying condition 2(i) and 2(iv). Second, $\Gamma, x : \sigma$ ensures a strict type for x; if x were a sharing variable in M then x would have a multiset type π. Therefore, condition 2(ii) is satisfied. Finally, condition (iii) is satisfied by induction on M and N. □

Proposition 3.30 ($(\!|\cdot|\!)^\circ$ Preserves Consistency)**.** *Let* $\mathbb{M}$ *be a* $\lambda^{\mathsf{lf}}_{\oplus}$*-expression. Then* $(\!|\mathbb{M}|\!)^\circ$ *is a consistent* $\widehat{\lambda}^{\mathsf{lf}}_{\oplus}$*-expression.*

Proof. By induction on the structure of $\mathbb{M}$. Notice that $(\!|\cdot|\!)^\bullet$ ensures consistency for bound variables: it replaces all occurrences of a bound variable (say y) with fresh bound variables (say, $y_1, \ldots, y_k$). Thus, the following hold for bound variables: (i) they occur once within a term and (ii) they are not shared themselves, as the sharing of variables only occurs when handling binders associated to explicit substitutions and abstractions. As for free variables, the translation $(\!|\cdot|\!)^\circ$ replaces each occurrence with a fresh variable, and does so before applying $(\!|\cdot|\!)^\bullet$; this ensures that free variables that are already shared are not shared again. Because of this design, the translations preserve consistency. □

Appendix C. Appendix to § 5.2

C.1. Encoding $(\!|\cdot|\!)^\bullet$.

C.1.1. *Auxiliary Encoding: From $\lambda_{\oplus}$ into $\widehat{\lambda}_{\oplus}$.*

Proposition C.1. *The encoding commutes with linear substitution:* $(\!|M\{\!|N/x|\!\}|\!)^{\bullet} = (\!|M|\!)^{\bullet}\{\!|(\!|N|\!)^{\bullet}/x|\!\}$

Proof. By induction of the structure of M in $M\{\!|(\!|N|\!)^{\bullet}/x|\!\}$. □

Proposition C.2 (Well-typedness preservation for $(\!|-|\!)^{\bullet}$)**.** *Let B and $\mathbb{M}$ be a bag and an expression in $\lambda^{\natural}_{\oplus}$, respectively.*

(1) *If $\Gamma \vdash B : \sigma$ then $\widehat{\Gamma}^{\dagger} \vdash (\!|B|\!)^{\bullet} : \sigma$.*
(2) *If $\Gamma \vdash \mathbb{M} : \sigma$ then $\widehat{\Gamma}^{\dagger} \vdash (\!|\mathbb{M}|\!)^{\bullet} : \sigma$.*

Proof. By mutual induction on the typing derivations for B and $\mathbb{M}$, with an analysis of the last rule applied.
Part (1) includes two cases:

i) Rule $[\mathtt{T} : \mathtt{1}]$: Then $B = \mathtt{1}$ and the thesis follows trivially, because the encoding of terms/bags (cf. Figure 8) ensures that $(\!|\mathtt{1}|\!)^{\bullet} = \mathtt{1}$.
ii) Rule $[\mathtt{T} : \mathtt{bag}]$. Then $B = \wr M \int \cdot A$, where M is a term and A is a bag, and

$$[\mathtt{T} : \mathtt{bag}]\ \frac{\Gamma \vdash M : \sigma \qquad \Delta \vdash A : \pi}{\Gamma \wedge \Delta \vdash \wr M \int \cdot A : \sigma \wedge \pi}$$

By the IHs, we have both $\widehat{\Gamma}^{\dagger} \vdash (\!|M|\!)^{\bullet} : \sigma$ and $\widehat{\Delta}^{\dagger} \vdash (\!|A|\!)^{\bullet} : \pi$. The thesis then follows by applying Rule $[\mathtt{TS} : \mathtt{bag}]$ in $\widehat{\lambda}^{\natural}_{\oplus}$:

$$[\mathtt{TS} : \mathtt{bag}]\ \frac{\widehat{\Gamma}^{\dagger} \vdash (\!|M|\!)^{\bullet} : \sigma \qquad \widehat{\Delta}^{\dagger} \vdash (\!|A|\!)^{\bullet} : \pi}{\widehat{\Gamma}^{\dagger}, \widehat{\Delta}^{\dagger} \vdash \wr (\!|M|\!)^{\bullet} \int \cdot (\!|A|\!)^{\bullet} : \sigma \wedge \pi}$$

Part (2) considers six cases:

i) Rule $[\mathtt{T} : \mathtt{var}]$: Then $\mathbb{M} = x$ and

$$[\mathtt{T} : \mathtt{var}]\ \frac{}{x : \sigma \vdash x : \sigma}$$

By the encoding of terms (cf. Fig. 8), we infer $x : \sigma \vdash x : \sigma$ and so the thesis holds immediately.
ii) Rule $[\mathtt{T} : \mathtt{abs}]$: Then $\mathbb{M} = \lambda x.M$ and

$$[\mathtt{T} : \mathtt{abs}]\ \frac{\Gamma, x : \sigma^n \vdash M : \tau}{\Gamma \vdash \lambda x.M : \sigma^n \to \tau}$$

By the encoding of terms (cf. Fig. 8), we have $(\!|\mathbb{M}|\!)^{\bullet} = \lambda x.(\!|M\langle x_1, \cdots, x_n/x\rangle|\!)^{\bullet}[\widetilde{x} \leftarrow x]$, where $\#(x, M) = n$ and each x_i is fresh.

We work on the premise $\Gamma, x : \sigma^n \vdash M : \tau$ before appealing to the IH.

Then, by n applications of Lemma 5.3 to this judgment, we obtain

$$\Gamma, x_1 : \sigma, \cdots, x_n : \sigma \vdash M\langle x_1, \cdots, x_n/x\rangle : \tau \tag{C.1}$$

By IH on (C.1) we have

$$\widehat{\Gamma}^{\dagger}, x_1 : \sigma, \cdots, x_n : \sigma \vdash (\!|M\langle x_1, \cdots, x_n/x\rangle|\!)^{\bullet} : \tau \tag{C.2}$$

Starting from (C.2), we then have the following type derivation for $(\!|\mathbb{M}|\!)^{\bullet}$, which concludes the proof for this case:

$$[\mathtt{TS}:\mathtt{share}]\ \frac{\widehat{\Gamma}^{\dagger}, x_1:\sigma,\cdots,x_n:\sigma \vdash (\!|M\langle x_1,\cdots,x_n/x\rangle|\!)^{\bullet}:\tau}{\widehat{\Gamma}^{\dagger}, x:\sigma^n \vdash (\!|M\langle x_1,\cdots,x_n/x\rangle|\!)^{\bullet}[x_1,\cdots,x_n \leftarrow x]:\tau}$$
$$[\mathtt{TS}:\mathtt{abs\text{-}sh}]\ \frac{\widehat{\Gamma}^{\dagger}, x:\sigma^n \vdash (\!|M\langle x_1,\cdots,x_n/x\rangle|\!)^{\bullet}[x_1,\cdots,x_n \leftarrow x]:\tau}{\widehat{\Gamma}^{\dagger} \vdash \lambda x.((\!|M\langle x_1,\cdots,x_n/x\rangle|\!)^{\bullet}[x_1,\cdots,x_n \leftarrow x]):\sigma^n \to \tau}$$

iii) Rule $[\mathtt{T}:\mathtt{app}]$: Then $\mathbb{M} = M\ B$ and

$$[\mathtt{T}:\mathtt{app}]\ \frac{\Gamma \vdash M:\pi\to\tau \qquad \Delta \vdash B:\pi}{\Gamma\wedge\Delta \vdash M\ B:\tau}$$

By IH we have both $\widehat{\Gamma}^{\dagger} \vdash (\!|M|\!)^{\bullet}:\pi\to\tau$ and $\widehat{\Delta}^{\dagger} \vdash (\!|B|\!)^{\bullet}:\pi$, and the thesis follows easily by Rule $[\mathtt{TS}:\mathtt{app}]$ in $\widehat{\lambda}^{\natural}_{\oplus}$:

$$[\mathtt{TS}:\mathtt{app}]\ \frac{\widehat{\Gamma}^{\dagger} \vdash (\!|M|\!)^{\bullet}:\pi\to\tau \qquad \widehat{\Delta}^{\dagger} \vdash (\!|B|\!)^{\bullet}:\pi}{\widehat{\Gamma}^{\dagger},\widehat{\Delta}^{\dagger} \vdash (\!|M|\!)^{\bullet}\ (\!|B|\!)^{\bullet}:\tau}$$

iv) Rule $[\mathtt{T}:\mathtt{ex\text{-}sub}]$: Then $\mathbb{M} = M\langle\!\langle B/x\rangle\!\rangle$ and the proof is split in two cases, depending on the shape of B:

(a) $B = \mathtt{1}$. In this case, $\mathbb{M} = M\langle\!\langle \mathtt{1}/x\rangle\!\rangle$ and we obtain the following type derivation:

$$[\mathtt{T}:\mathtt{ex\text{-}sub}]\ \frac{\vdash \mathtt{1}:\omega \qquad [\mathtt{T}:\mathtt{weak}]\ \dfrac{\Gamma \vdash M:\tau}{\Gamma, x:\omega \vdash M:\tau}}{\Gamma \vdash M\langle\!\langle \mathtt{1}/x\rangle\!\rangle:\tau}$$

By IH we have both $\vdash \mathtt{1}:\omega$ and $\widehat{\Gamma}^{\dagger} \vdash (\!|M|\!)^{\bullet}:\tau$. By the encoding of terms (Figure 8), $(\!|M\langle\!\langle \mathtt{1}/x\rangle\!\rangle|\!)^{\bullet} = (\!|M|\!)^{\bullet}[\leftarrow x]\langle\!\langle \mathtt{1}/x\rangle\!\rangle$, and the result holds by the following type derivation:

$$[\mathtt{TS}:\mathtt{ex\text{-}sub}]\ \frac{\vdash \mathtt{1}:\omega \qquad [\mathtt{TS}:\mathtt{weak}]\ \dfrac{\widehat{\Gamma}^{\dagger} \vdash (\!|M|\!)^{\bullet}:\tau}{\widehat{\Gamma}^{\dagger}, x:\omega \vdash (\!|M|\!)^{\bullet}[\leftarrow x]:\tau}}{\widehat{\Gamma}^{\dagger} \vdash (\!|M|\!)^{\bullet}[\leftarrow x]\langle\!\langle \mathtt{1}/x\rangle\!\rangle:\tau}$$

(b) $B = \wr N_1,\ldots,N_n\wr$, $n \geq 1$. Suppose w.l.o.g. that $n = 2$, then $B = \wr N_1, N_2\wr$ and

$$[\mathtt{T}:\mathtt{bag}]\ \frac{\Delta_1 \vdash N_1:\sigma \qquad \Delta_2 \vdash N_2:\sigma}{\Delta_1\wedge\Delta_2 \vdash \wr N_1\wr\cdot\wr N_2\wr:\sigma^2}$$
$$[\mathtt{T}:\mathtt{ex\text{-}sub}]\ \frac{\qquad\qquad \Gamma, x:\sigma^2 \vdash M:\tau}{\Gamma\wedge\Delta_1\wedge\Delta_2 \vdash M\langle\!\langle B/x\rangle\!\rangle:\tau}$$

By IH we have $\widehat{\Delta_1}^{\dagger} \vdash (\!|N_1|\!)^{\bullet}:\sigma$ and $\widehat{\Delta_2}^{\dagger} \vdash (\!|N_2|\!)^{\bullet}:\sigma$. We can expand $\Gamma, x:\sigma^2 \vdash M:\tau$ into $\Gamma, x:\sigma\wedge\sigma \vdash M:\tau$. By Lemma 5.3 and the IH on this last sequent we obtain

$$\widehat{\Gamma}^{\dagger}, y_1:\sigma, y_2:\sigma \vdash (\!|M\langle y_1, y_2/x\rangle|\!)^{\bullet}:\tau$$

where $\#(x, M) = 2$ and y_1, y_2 are fresh variables with the same type as x.
Now, by the encoding of terms (Figure 8), we have

$$\begin{aligned}(\!|M\langle\!\langle \wr N_1, N_2\wr/x\rangle\!\rangle|\!)^{\bullet} &= (\!|M\langle y_1, y_2/x\rangle|\!)^{\bullet}\langle\!|(\!|N_1|\!)^{\bullet}/y_1|\!\rangle\langle\!|(\!|N_2|\!)^{\bullet}/y_2|\!\rangle + \\ &\quad (\!|M\langle y_1, y_2/x\rangle|\!)^{\bullet}\langle\!|(\!|N_1|\!)^{\bullet}/y_2|\!\rangle\langle\!|(\!|N_2|\!)^{\bullet}/y_1|\!\rangle \\ &= \mathbb{M}'\end{aligned}$$

We give typing derivations in $\widehat{\lambda}^{\natural}_{\oplus}$ for each summand. First, let Π_1 be the following derivation:

$$\dfrac{\dfrac{\widehat{\Delta_2}^{\dagger} \vdash (\!|N_2|\!)^{\bullet} : \sigma \qquad \widehat{\Gamma}^{\dagger}, y_2 : \sigma, \widehat{\Delta_1}^{\dagger} \vdash (\!|M\langle y_1, y_2/x\rangle|\!)^{\bullet}\{\!|(\!|N_1|\!)^{\bullet}/y_1|\!\} : \tau}{\widehat{\Gamma}^{\dagger}, \widehat{\Delta_1}^{\dagger}, \widehat{\Delta_2}^{\dagger} \vdash (\!|M\langle y_1, y_2/x\rangle|\!)^{\bullet}\{\!|(\!|N_1|\!)^{\bullet}/y_1|\!\}\{\!|(\!|N_2|\!)^{\bullet}/y_2|\!\} : \tau} \qquad \widehat{\Delta_1}^{\dagger} \vdash (\!|N_1|\!)^{\bullet} : \sigma \qquad \widehat{\Gamma}^{\dagger}, y_1 : \sigma, y_2 : \sigma \vdash (\!|M\langle y_1, y_2/x\rangle|\!)^{\bullet} : \tau}{\widehat{\Gamma}^{\dagger}, \widehat{\Delta_1}^{\dagger}, \widehat{\Delta_2}^{\dagger} \vdash (\!|M\langle y_1, y_2/x\rangle|\!)^{\bullet}\{\!|(\!|N_1|\!)^{\bullet}/y_1|\!\}\{\!|(\!|N_2|\!)^{\bullet}/y_2|\!\} : \tau}$$

Similarly, we can obtain a derivation Π_2 for:

$$\widehat{\Gamma}^{\dagger}, \widehat{\Delta_1}^{\dagger}, \widehat{\Delta_2}^{\dagger} \vdash (\!|M\langle y_1, y_2/x\rangle|\!)^{\bullet}\{\!|(\!|N_1|\!)^{\bullet}/y_2|\!\}\{\!|(\!|N_2|\!)^{\bullet}/y_1|\!\} : \tau$$

From Π_1, Π_2, and Rule $[\mathtt{TS} : \mathtt{sum}]$, the thesis follows:

$$[\mathtt{TS} : \mathtt{sum}]\ \frac{\Pi_1 \qquad \Pi_2}{\widehat{\Gamma}^{\dagger}, \widehat{\Delta_1}^{\dagger}, \widehat{\Delta_2}^{\dagger} \vdash \mathbb{M}' : \tau}$$

v) Rule $[\mathtt{T} : \mathtt{weak}]$: Then $\mathbb{M} = M$ and

$$[\mathtt{T} : \mathtt{weak}]\ \frac{\Gamma \vdash M : \sigma \qquad x \notin \mathtt{dom}(\Gamma)}{\Gamma, x : \omega \vdash M : \sigma}$$

Because $[\mathtt{TS} : \mathtt{weak}]$ is a silent typing rule in $\lambda^{\lightning}_{\oplus}$, we have that $x \notin \mathsf{fv}(M)$ and so this case does not apply.

vi) Rule $[\mathtt{T} : \mathtt{sum}]$:
This case follows easily by IH. □

C.1.2. *Properties.* We divide the proof of well-formedness preservation: we first prove it for $(\!|-|\!)^{\bullet}$, then we extend it to $(\!|-|\!)^{\circ}$.

Lemma 5.5 (Well-formedness preservation for $(\!|\cdot|\!)^{\bullet}$)**.** *Let B and $\mathbb{M}$ be a bag and an expression in $\lambda^{\lightning}_{\oplus}$, respectively. Also, let Γ be a context such that $\widehat{\Gamma}^{\dagger}$ is defined. We have:*

(1) *If $\Gamma \models B : \pi$ then $\widehat{\Gamma}^{\dagger} \models (\!|B|\!)^{\bullet} : \pi$.*
(2) *If $\Gamma \models \mathbb{M} : \sigma$ then $\widehat{\Gamma}^{\dagger} \models (\!|\mathbb{M}|\!)^{\bullet} : \sigma$.*

Proof. By mutual induction on the typing derivations for B and $\mathbb{M}$, with an analysis of the last rule (from Fig. 4) applied. We proceed with the following nine cases:

(1) This case includes two subcases:
   (a) Rule $[\mathtt{F} : \mathtt{wf\text{-}bag}]$.
   Then by inversion of the typing derivation,

$$[\mathtt{F{:}wf} - \mathtt{bag}]\ \frac{\Gamma \vdash B : \sigma}{\Gamma \models B : \sigma}$$

   By Propostion C.2 we have $\Gamma \vdash B : \sigma$ implies $\widehat{\Gamma}^{\dagger} \vdash (\!|B|\!)^{\bullet} : \sigma$. Notice that the encoding $(\!|\cdot|\!)^{\bullet}$ given in Fig. 8, is a restriction of $(\!|\cdot|\!)^{\bullet}$ to $\lambda_{\oplus}$. Therefore, $\widehat{\Gamma}^{\dagger} \vdash (\!|B|\!)^{\bullet} : \sigma$, and the result follows after an application of $[\mathtt{FS{:}wf} - \mathtt{bag}]$.
   (b) Rule $[\mathtt{F} : \mathtt{bag}]$.
   In this case $B = \{\!|M|\!\} \cdot A$, where M is a term and A is a bag, and we have the following derivation by inversion of the typing derivation:

$$[\mathtt{F} : \mathtt{bag}]\ \frac{\Gamma \models M : \sigma \qquad \Delta \models A : \sigma^k}{\Gamma \wedge \Delta \models \{\!|M|\!\} \cdot A : \sigma^{k+1}}$$

   with $\mathtt{dom}(\Gamma) = \mathsf{fv}(M)$ and $\mathtt{dom}(\Delta) = \mathsf{fv}(A)$. By the IHs, we have both
   • $\widehat{\Gamma}^{\dagger} \vdash (\!|M|\!)^{\bullet} : \sigma$; and

- $\widehat{\Delta}^{\dagger} \vdash (\!|A|\!)^{\bullet} : \sigma^{k}$.

By applying Rule [FS:bag] from Fig. 7, for $\widehat{\lambda}^{\natural}_{\oplus}$, we obtain the following derivation:

$$[\texttt{FS:bag}]\ \frac{\widehat{\Gamma}^{\dagger} \models (\!|M|\!)^{\bullet} : \sigma \qquad \widehat{\Delta}^{\dagger} \models (\!|A|\!)^{\bullet} : \sigma^{k}}{\widehat{\Gamma}^{\dagger}, \widehat{\Delta}^{\dagger} \models \wr (\!|M|\!)^{\bullet} \int \cdot (\!|A|\!)^{\bullet} : \sigma^{k+1}}$$

Since $(\!|\wr M \int \cdot A|\!)^{\bullet} = \wr (\!|M|\!)^{\bullet} \int \cdot (\!|A|\!)^{\bullet}$, one has $\widehat{\Gamma}^{\dagger}, \widehat{\Delta}^{\dagger} \vdash (\!|\wr M \int \cdot A|\!)^{\bullet} : \sigma^{k+1}$, and the result follows.

(2) This case is divided in seven subcases:

(a) Rule [F : wf-expr].
Then the thesis follows trivially from type preservation in $(\!|-|\!)^{\circ}$ of Proposition C.2.

(b) Rule [F : weak].
In this case, $\mathbb{M} = M$ and by inversion of the typing derivation we have the derivation

$$[\texttt{F : weak}]\ \frac{\Gamma_1 \models M : \tau}{\Gamma_1, x : \omega \models M : \tau}$$

Because [weak] is a silent well-formed rule in $\lambda^{\natural}_{\oplus}$, we have that $x \notin \mathsf{fv}(M)$ and so this case does not apply.

(c) Rule [F : abs].
In this case $\mathbb{M} = \lambda x.M$ by inversion of the typing derivation and we have the derivation:

$$[\texttt{F : abs}]\ \frac{\Gamma, x : \sigma^{n} \models M : \tau}{\Gamma \models \lambda x.M : \sigma^{n} \to \tau}$$

By the encoding given in Fig. 8, we have $(\!|\mathbb{M}|\!)^{\bullet} = \lambda x.(\!|M\langle x_1, \cdots, x_n/x\rangle|\!)^{\bullet}[x_1, \cdots, x_n \leftarrow x]$, where $\#(x, M) = n$ and each x_i is fresh and has the same type as x. From $\Gamma, x : \sigma^{n} \models M : \tau$, we obtain after n applications of Proposition 5.2 and Lemma 5.3:

$$\Gamma, x_1 : \sigma, \cdots, x_n : \sigma \models M\langle x_1, \cdots, x_n/x\rangle : \tau$$

By IH we have:

$$\widehat{\Gamma}^{\dagger}, x_1 : \sigma, \cdots, x_n : \sigma \models (\!|M\langle x_1, \cdots, x_n/x\rangle|\!)^{\bullet} : \tau$$

which gives us the following derivation:

$$[\texttt{FS:share}]\ \frac{\widehat{\Gamma}^{\dagger}, x_1 : \sigma, \cdots, x_n : \sigma \models (\!|M\langle x_1, \cdots, x_n/x\rangle|\!)^{\bullet} : \tau}{[\texttt{FS:abs-sh}]\ \dfrac{\widehat{\Gamma}^{\dagger}, x : \sigma^{n} \models (\!|M\langle x_1, \cdots, x_n/x\rangle|\!)^{\bullet}[x_1, \cdots, x_n \leftarrow x] : \tau}{\widehat{\Gamma}^{\dagger} \models \lambda x.((\!|M\langle x_1, \cdots, x_n/x\rangle|\!)^{\bullet}[x_1, \cdots, x_n \leftarrow x]) : \sigma^{n} \to \tau}}$$

and the result follows.

(d) Rule [F : app].
In this case $\mathbb{M} = M\ B$, and by inversion of the typing derivation we have the derivation:

$$[\texttt{F : app}]\ \frac{\Gamma \models M : \sigma^{j} \to \tau \qquad \Delta \models B : \sigma^{k}}{\Gamma \wedge \Delta \models M\ B : \tau}$$

By IH we have both $\widehat{\Gamma}^{\dagger} \models (\!|M|\!)^{\bullet} : \sigma^{j} \to \tau$ and $\widehat{\Delta}^{\dagger} \models (\!|B|\!)^{\bullet} : \sigma^{k}$, and the result follows easily by Rule [FS:app] in $\widehat{\lambda}^{\natural}_{\oplus}$:

$$[\texttt{FS:app}]\ \frac{\widehat{\Gamma}^{\dagger} \models (\!|M|\!)^{\bullet} : \sigma^{j} \to \tau \qquad \widehat{\Delta}^{\dagger} \models (\!|B|\!)^{\bullet} : \sigma^{k}}{\widehat{\Gamma}^{\dagger}, \widehat{\Delta}^{\dagger} \models (\!|M|\!)^{\bullet}\ (\!|B|\!)^{\bullet} : \tau}$$

(e) Rule [F : ex-sub].
Then $\mathbb{M} = M\langle\!\langle {}^{B}/_{x} \rangle\!\rangle$ and the proof is split in two cases, depending on the shape of B:

(i) When $\#(x, M) = \mathsf{size}(B) = k \geq 1$.
Then we have $B = \wr N_1, \ldots, N_n \wr$, $n \geq 1$. Suppose w.l.o.g. that $n = 2$, then $B = \wr N_1, N_2 \wr$ and by inversion of the typing derivation we have the following derivation:

$$[\mathtt{F : bag}]\ \dfrac{[\mathtt{F : ex\text{-}sub}]\ \dfrac{\Delta_1 \models N_1 : \sigma \qquad \Delta_2 \models N_2 : \sigma}{\Delta_1 \wedge \Delta_2 \models \wr N_1 \wr \cdot \wr N_2 \wr : \sigma^2} \qquad \Gamma_1, x : \sigma^2 \models M : \tau}{\Gamma_1 \wedge \Delta_1 \wedge \Delta_2 \models M\langle\!\langle {}^{B}/_{x} \rangle\!\rangle : \tau}$$

where $\Gamma = \Gamma_1, \Delta_1, \Delta_2$. By IH we have both

- $\widehat{\Delta_1}^{\dagger} \vdash (\!| N_1 |\!)^{\bullet} : \sigma$; and
- $\widehat{\Delta_2}^{\dagger} \vdash (\!| N_2 |\!)^{\bullet} : \sigma$; and
- $\widehat{\Gamma_1}^{\dagger}, x : \sigma^2 \models (\!| M |\!)^{\bullet} : \tau$

We can expand $\widehat{\Gamma_1}^{\dagger}, x : \sigma^2 \models (\!| M |\!)^{\bullet} : \tau$ into $\widehat{\Gamma_1}^{\dagger}, x : \sigma \wedge \sigma \models (\!| M |\!)^{\bullet} : \tau$, which gives $\widehat{\Gamma_1}^{\dagger}, y_1 : \sigma, y_2 : \sigma \models (\!| M |\!)^{\bullet}\langle y_1, y_2 / x \rangle : \tau$, after two applications of Proposition 5.2 along with the application of Lemma 5.3, with y_1, y_2 fresh variables of the same type as x. Since the encoding $(\!| \cdot |\!)^{\bullet}$ commutes with the linear substitution $\langle / \cdot \rangle$ (Proposition 5.2), if follows that, $\widehat{\Gamma_1}^{\dagger}, y_1 : \sigma, y_2 : \sigma \models (\!| M\langle y_1, y_2 / x \rangle |\!)^{\bullet} : \tau$.
Let Π_1 be the derivation obtained after two consecutive applications of Rule [FS:ex-lin-sub]:

$$\dfrac{\dfrac{\widehat{\Gamma_1}^{\dagger}, y_1 : \sigma, y_2 : \sigma \models (\!| M\langle y_1, y_2 / x \rangle |\!)^{\bullet} : \tau \qquad \widehat{\Delta_1}^{\dagger} \models (\!| N_1 |\!)^{\bullet} : \sigma}{\widehat{\Gamma_1}^{\dagger}, y_2 : \sigma, \widehat{\Delta_1}^{\dagger} \models (\!| M\langle y_1, y_2 / x \rangle |\!)^{\bullet} \{\!| (\!| N_1 |\!)^{\bullet} / y_1 |\!\} : \tau} \qquad \widehat{\Delta_2}^{\dagger} \models (\!| N_2 |\!)^{\bullet} : \sigma}{\widehat{\Gamma_1}^{\dagger}, \widehat{\Delta_1}^{\dagger}, \widehat{\Delta_2}^{\dagger} \models (\!| M\langle y_1, y_2 / x \rangle |\!)^{\bullet} \{\!| (\!| N_1 |\!)^{\bullet} / y_1 |\!\} \{\!| (\!| N_2 |\!)^{\bullet} / y_2 |\!\} : \tau}$$

Similarly, we can obtain a derivation Π_2 for:

$$\widehat{\Gamma_1}^{\dagger}, \widehat{\Delta_1}^{\dagger}, \widehat{\Delta_2}^{\dagger} \models (\!| M\langle y_1, y_2 / x \rangle |\!)^{\bullet} \{\!| (\!| N_1 |\!)^{\bullet} / y_2 |\!\} \{\!| (\!| N_2 |\!)^{\bullet} / y_1 |\!\} : \tau$$

By the encoding given in Figure 8, we have

$$\begin{aligned}(\!| M\langle\!\langle \wr N_1, N_2 \wr / x \rangle\!\rangle |\!)^{\bullet} = &(\!| M\langle y_1, y_2 / x \rangle |\!)^{\bullet} \{\!| (\!| N_1 |\!)^{\bullet} / y_1 |\!\} \{\!| (\!| N_2 |\!)^{\bullet} / y_2 |\!\} + \\ &(\!| M\langle y_1, y_2 / x \rangle |\!)^{\bullet} \{\!| (\!| N_1 |\!)^{\bullet} / y_2 |\!\} \{\!| (\!| N_2 |\!)^{\bullet} / y_1 |\!\}\end{aligned}$$

Therefore,

$$[\mathtt{FS:sum}]\ \dfrac{\Pi_1 \qquad \Pi_2}{\widehat{\Gamma_1}^{\dagger}, \widehat{\Delta_1}^{\dagger}, \widehat{\Delta_2}^{\dagger} \models (\!| M\langle\!\langle \wr N_1, N_2 \wr / x \rangle\!\rangle |\!)^{\bullet} : \tau}$$

and the result follows.

(ii) $\#(x, M) = k \neq \mathsf{size}(B)$.
In this case, $\mathsf{size}(B) = j$ for some $j \neq k$, and by inversion of the typing derivation we have the following derivation:

$$[\mathtt{F : ex\text{-}sub}]\ \dfrac{\Delta \models B : \sigma^j \qquad \Gamma_1, x : \sigma^k \models M : \tau}{\Gamma_1 \wedge \Delta \models M\langle\!\langle {}^{B}/_{x} \rangle\!\rangle : \tau}$$

where $\Gamma = \Gamma_1 \wedge \Delta$. By IH we have both

- $\widehat{\Delta}^{\dagger} \models (\!|B|\!)^{\bullet} : \sigma^{j}$; and
- $\widehat{\Gamma_1}^{\dagger}, \hat{x} : \sigma^{k} \models (\!|M|\!)^{\bullet} : \tau$.

We analyse two cases, depending on the number k of occurrences of x in M:

(A) $k = 0$.
From $\Gamma_1, x : \omega \models M : \tau$, which we get $\Gamma_1 \models M : \tau$, via Rule [F : weak].
The IH gives $\widehat{\Gamma_1}^{\dagger} \models (\!|M|\!)^{\bullet} : \tau$, which entails:

$$[\texttt{FS:weak}]\ \frac{\widehat{\Gamma_1}^{\dagger} \models (\!|M|\!)^{\bullet} : \tau}{[\texttt{FS:ex-sub}]\ \dfrac{\widehat{\Gamma_1}^{\dagger}, x : \omega \models (\!|M|\!)^{\bullet}[\leftarrow x] : \tau \qquad \widehat{\Delta}^{\dagger} \models (\!|B|\!)^{\bullet} : \sigma^{j}}{\widehat{\Gamma_1}^{\dagger}, \widehat{\Delta}^{\dagger} \models (\!|M|\!)^{\bullet}[\leftarrow x]\langle\!\langle {}^{B}/_{x} \rangle\!\rangle : \tau}}$$

By the encoding given in Figure 8, $(\!|M\langle\!\langle {}^{B}/_{x} \rangle\!\rangle|\!)^{\bullet} = (\!|M|\!)^{\bullet}[\leftarrow x]\langle\!\langle {}^{(\!|B|\!)^{\bullet}}/_{x} \rangle\!\rangle$, and the result follows.

(B) $k > 0$.
By applying Proposition 5.2 in $\widehat{\Gamma_1}^{\dagger}, x : \sigma^{k} \models (\!|M|\!)^{\bullet} : \tau$, we obtain

$$\widehat{\Gamma_1}^{\dagger}, x_1 : \sigma, \ldots, x_k : \sigma \models (\!|M|\!)^{\bullet}\langle x_1, \ldots, x_k / x \rangle : \tau$$

From Proposition 5.2 and Lemma 5.3, it follows that $\widehat{\Gamma_1}^{\dagger}, x_1 : \sigma, \ldots, x_k : \sigma \models (\!|M\langle x_1, \ldots, x_k/x\rangle|\!)^{\bullet} : \tau$, which entails $x \notin \mathtt{dom}(\Gamma_1)$ since $k \neq 0$. First we give Π:

$$[\texttt{FS:share}]\ \frac{\widehat{\Gamma_1}^{\dagger}, x_1 : \sigma, \ldots, x_k : \sigma \models (\!|M\langle x_1, \ldots, x_k/x\rangle|\!)^{\bullet} : \tau}{\widehat{\Gamma_1}^{\dagger}, x : \sigma^{k} \models (\!|M\langle x_1 . \cdots, x_k/x\rangle|\!)^{\bullet}[x_1 . \cdots, x_k \leftarrow x] : \tau}$$

finally we give the full derivation:

$$[\texttt{FS:ex-sub}]\ \frac{\widehat{\Delta}^{\dagger} \models (\!|B|\!)^{\bullet} : \sigma^{j} \qquad \Pi}{\widehat{\Gamma}^{\dagger}, \widehat{\Delta}^{\dagger} \models (\!|M\langle x_1 . \cdots, x_k/x\rangle|\!)^{\bullet}[x_1 . \cdots, x_k \leftarrow x]\langle\!\langle {}^{(\!|B|\!)^{\bullet}}/_{x} \rangle\!\rangle : \tau}$$

(f) Rule [F : fail].
The result follows trivially, because the encoding of failure in Fig. 8 is such that $(\!|\mathtt{fail}^{\widetilde{x}}|\!)^{\bullet} = \mathtt{fail}^{\widetilde{x}}$.

(g) Rule [F : sum].
This case follows easily by IH. □

Theorem 5.6 (Well-formedness Preservation for $(\!|\cdot|\!)^{\circ}$)**.** *Let B and $\mathbb{M}$ be a bag and an expression in $\lambda^{\lightning}_{\oplus}$, respectively.*

(1) *If $\Gamma \models B : \pi$ then $\Gamma^{\dagger} \models (\!|B|\!)^{\circ} : \pi$.*
(2) *If $\Gamma \models \mathbb{M} : \sigma$ then $\Gamma^{\dagger} \models (\!|\mathbb{M}|\!)^{\circ} : \sigma$.*

Proof. By mutual induction on the typing derivations $\Gamma \models B : \sigma$ and $\Gamma \models \mathbb{M} : \sigma$, exploiting both Proposition 5.2 and Lemma 5.3. The analysis for bags (Part 1) follows directly from the IHs and will be omitted.

As for Part 2, there are two main cases to consider:

i) $\mathbb{M} = M$.
Without loss of generality, assume $\mathsf{fv}(M) = \{x, y\}$. Then,

$$x : \sigma_1^{j}, y : \sigma_2^{k} \models M : \tau \tag{C.3}$$

where $\#(x, M) = j$ and $\#(y, M) = k$, for some positive integers j and k.

After $j + k$ applications of Lemma 5.3 we obtain:

$$x_1 : \sigma_1, \cdots, x_j : \sigma_1, y_1 : \sigma_2, \cdots, y_k : \sigma_2 \models M\langle\widetilde{x}/x\rangle\langle\widetilde{y}/y\rangle : \tau$$

where $\widetilde{x} = x_1, \ldots, x_j$ and $\widetilde{y} = y_1, \ldots, y_k$. From Proposition 5.2 and Lemma 5.3 one has

$$x_1 : \sigma_1, \ldots, x_j : \sigma_1, y_1 : \sigma_2, \ldots, y_k : \sigma_2 \models (\!|M\langle\widetilde{x}/x\rangle\langle\widetilde{y}/y\rangle|\!)^\bullet : \tau$$

Since $x_1 : \sigma_1, \ldots, x_j : \sigma_1, y_1 : \sigma_2, \ldots, y_k : \sigma_2 = x_1 : \sigma_1, \ldots, x_j : \sigma_1, y_1 : \sigma_2, \ldots, y_k : \sigma_2$, we have the following derivation:

$$\dfrac{\dfrac{x_1 : \sigma_1, \cdots, x_j : \sigma_1, y_1 : \sigma_2, \cdots, y_k : \sigma_2 \models (\!|M\langle\widetilde{x}/x\rangle\langle\widetilde{y}/y\rangle|\!)^\bullet : \tau}{x : \sigma_1^j, y_1 : \sigma_2, \cdots, y_k : \sigma_2 \models (\!|M\langle\widetilde{x}/x\rangle\langle\widetilde{y}/y\rangle|\!)^\bullet[\widetilde{x} \leftarrow x] : \tau}\,[\texttt{FS:share}]}{x : \sigma_1^j, y : \sigma_2^k \models (\!|M\langle\widetilde{x}/x\rangle\langle\widetilde{y}/y\rangle|\!)^\bullet[\widetilde{x} \leftarrow x][\widetilde{y} \leftarrow y] : \tau}\,[\texttt{FS:share}]$$

By expanding Def. 3.26, we have

$$(\!|M|\!)^\circ = (\!|M\langle\widetilde{x}/x\rangle\langle\widetilde{y}/y\rangle|\!)^\bullet[\widetilde{x} \leftarrow x][\widetilde{y} \leftarrow y],$$

which completes the proof for this case.

ii) $\mathbb{M} = M_1 + \cdots + M_n$.

This case proceeds easily by IH, using Rule [FS:sum]. □

C.2. **Completeness and Soundness.**

Theorem 5.8 (Operational Completeness)**.** *Let* $\mathbb{M}, \mathbb{N}$ *be well-formed* $\lambda^{\lightning}_{\oplus}$ *expressions. Suppose* $\mathbb{N} \longrightarrow_{[\mathtt{R}]} \mathbb{M}$.

(1) *If* $[\mathtt{R}] = [\mathtt{R} : \mathtt{Beta}]$ *then* $(\!|\mathbb{N}|\!)^\circ \longrightarrow^{\leq 2} (\!|\mathbb{M}|\!)^\circ$;
(2) *If* $[\mathtt{R}] = [\mathtt{R} : \mathtt{Fetch}]$ *then* $(\!|\mathbb{N}|\!)^\circ \longrightarrow^{+} (\!|\mathbb{M}'|\!)^\circ$, *for some* $\mathbb{M}'$ *such that* $\mathbb{M} \equiv_\lambda \mathbb{M}'$.
(3) *If* $[\mathtt{R}] \neq [\mathtt{R} : \mathtt{Beta}]$ *and* $[\mathtt{R}] \neq [\mathtt{R} : \mathtt{Fetch}]$ *then* $(\!|\mathbb{N}|\!)^\circ \longrightarrow (\!|\mathbb{M}|\!)^\circ$.

Proof. By induction on the rule from Fig. 2 applied to infer $\mathbb{N} \longrightarrow \mathbb{M}$, distinguishing three cases. Below $[\widetilde{x_{1k} \leftarrow x_{1k}}]$ abbreviates $[\widetilde{x_1} \leftarrow x_1] \ldots [\widetilde{x_k} \leftarrow x_k]$:

(1) The rule applied is $[\mathtt{R}] = [\mathtt{R} : \mathtt{Beta}]$.

In this case, $\mathbb{N} = (\lambda x.M)B$, the reduction is

$$[\mathtt{R} : \mathtt{Beta}]\ \dfrac{}{(\lambda x.M)B \longrightarrow M\ \langle\!\langle B/x\rangle\!\rangle}$$

and $\mathbb{M} = M\langle\!\langle B/x\rangle\!\rangle$. Below we assume $\mathsf{fv}(\mathbb{N}) = \{x_1, \ldots, x_k\}$ and $\widetilde{x_i} = x_{i_1}, \ldots, x_{i_{j_i}}$, where $j_i = \#(x_i, N)$, for $1 \leq i \leq k$. On the one hand, we have:

$$\begin{aligned}
(\!|\mathbb{N}|\!)^\circ &= (\!|(\lambda x.M)B|\!)^\circ \\
&= (\!|((\lambda x.M)B)\langle\widetilde{x_1}/x_1\rangle \cdots \langle\widetilde{x_k}/x_k\rangle|\!)^\bullet[\widetilde{x_{1k} \leftarrow x_{1k}}] \\
&= (\!|(\lambda x.M')B'|\!)^\bullet[\widetilde{x_{1k} \leftarrow x_{1k}}] \\
&= ((\!|\lambda x.M'|\!)^\bullet(\!|B'|\!)^\bullet)[\widetilde{x_{1k} \leftarrow x_{1k}}] \\
&= ((\lambda x.(\!|M'\langle\widetilde{y}/x\rangle|\!)^\bullet[\widetilde{y} \leftarrow x])(\!|B'|\!)^\bullet)[\widetilde{x_{1k} \leftarrow x_{1k}}] \\
&\longrightarrow_{[\mathtt{RS:Beta}]} ((\!|M'\langle\widetilde{y}/x\rangle|\!)^\bullet[\widetilde{y} \leftarrow x]\langle\!\langle(\!|B'|\!)^\bullet/x\rangle\!\rangle)[\widetilde{x_{1k} \leftarrow x_{1k}}] = \mathbb{L}
\end{aligned} \tag{C.4}$$

where we define M' and B' to be M and B after the substitutions of $\langle\widetilde{x_1}/x_1\rangle\cdots\langle\widetilde{x_k}/x_k\rangle$. On the other hand, we have:

$$\begin{aligned}(\!|\mathbb{M}|\!)^\circ &= (\!|M\langle\!\langle B/x\rangle\!\rangle|\!)^\circ\\ &= (\!|M\langle\!\langle B/x\rangle\!\rangle\langle\widetilde{x_1}/x_1\rangle\cdots\langle\widetilde{x_k}/x_k\rangle|\!)^\bullet[\widetilde{x_{1k}\leftarrow x_{1k}}] \qquad (C.5)\\ &= (\!|M'\langle\!\langle B'/x\rangle\!\rangle|\!)^\bullet[\widetilde{x_{1k}\leftarrow x_{1k}}]\end{aligned}$$

We need to analyse two sub-cases: either $\#(x,M') = \mathsf{size}(B) = k \geq 1$ or $\#(x,M') = k$ and our first sub-case is not met.

i) If $\#(x,M') = \mathsf{size}(B) = k \geq 1$ then we can reduce $\mathbb{L}$ using Rule $[\mathtt{RS}:\mathtt{Ex}-\mathtt{sub}]$:

$$\mathbb{L} \longrightarrow \sum_{B_i\in\mathsf{PER}((\!|B|\!)^\bullet)} (\!|M'\langle\widetilde{y}/x\rangle|\!)^\bullet\{\!|B_i(1)/y_1|\!\}\cdots\{\!|B_i(n)/y_n|\!\}[\widetilde{x_{1k}\leftarrow x_{1k}}] = (\!|\mathbb{M}|\!)^\circ$$

From (C.4) and (C.5) and $\widetilde{y} = y_1\ldots y_n$, one has the desired result.

ii) Otherwise, $\#(x,M) = k$ (either $k=0$ or $k\neq\mathsf{size}(B)$).
Expanding the encoding in (C.5) :

$$\begin{aligned}(\!|M|\!)^\circ &= (\!|M'\langle\!\langle B'/x\rangle\!\rangle|\!)^\bullet[\widetilde{x_{1k}\leftarrow x_{1k}}]\\ &= ((\!|M'\langle\widetilde{y}/x\rangle|\!)^\bullet[\widetilde{y}\leftarrow x]\langle\!\langle(\!|B'|\!)^\bullet/x\rangle\!\rangle)[\widetilde{x_{1k}\leftarrow x_{1k}}]\end{aligned}$$

Therefore $(\!|M|\!)^\circ = \mathbb{L}$ and $(\!|\mathbb{N}|\!)^\circ \longrightarrow (\!|\mathbb{M}|\!)^\circ$.

(2) The rule applied is $[\mathtt{R}] = [\mathtt{R}:\mathtt{Fetch}]$.
Then $\mathbb{N} = M\langle\!\langle B/x\rangle\!\rangle$ and the reduction is

$$[\mathtt{R}:\mathtt{Fetch}]\ \frac{\mathsf{head}(M)=x \quad B=\wr N_1,\ldots,N_n\wr,\ n\geq 1 \quad \#(x,M)=n}{M\langle\!\langle B/x\rangle\!\rangle \longrightarrow \sum_{i=1}^n M\{\!|N_i/x|\!\}\langle\!\langle B\setminus\!\setminus N_i/x\rangle\!\rangle}$$

with $\mathbb{M} = \sum_{i=1}^n M\{\!|N_i/x|\!\}\langle\!\langle B\setminus\!\setminus N_i/x\rangle\!\rangle$.
Below we assume $\mathsf{fv}(\mathbb{N}) = \mathsf{fv}(M\langle\!\langle\wr N1\wr/x\rangle\!\rangle) = \{x_1,\ldots,x_k\}$. We distinguish two cases:

(1) $n=1$.
Then $B = \wr N_1\wr$ and $\mathbb{N} = M\langle\!\langle\wr N_1\wr/x\rangle\!\rangle \longrightarrow M\{\!|N_1/x|\!\}\langle\!\langle 1/x\rangle\!\rangle = \mathbb{M}$.
On the one hand, we have:

$$\begin{aligned}(\!|\mathbb{N}|\!)^\circ &= (\!|M\langle\!\langle\wr N_1\wr/x\rangle\!\rangle|\!)^\circ\\ &= (\!|(M\langle\!\langle\wr N_1\wr/x\rangle\!\rangle)\langle\widetilde{x_1}/x_1\rangle\cdots\langle\widetilde{x_k}/x_k\rangle|\!)^\bullet[\widetilde{x_{1k}\leftarrow x_{1k}}]\\ &= (\!|M'\langle\!\langle\wr N_1'\wr/x\rangle\!\rangle|\!)^\bullet[\widetilde{x_{1k}\leftarrow x_{1k}}]\\ &= (\!|M'\langle y_1/x\rangle|\!)^\bullet\{\!|(\!|N_1'|\!)^\bullet/y_1|\!\}[\widetilde{x_{1k}\leftarrow x_{1k}}],\ \text{notice that } \mathsf{head}(M') = y_1\\ &= (\!|M''|\!)^\bullet\{\!|(\!|N_1'|\!)^\bullet/y_1|\!\}[\widetilde{x_{1k}\leftarrow x_{1k}}]\\ &\longrightarrow_{[\mathtt{RS}:\mathtt{Lin}-\mathtt{Fetch}]} (\!|M''|\!)^\bullet\{\!|(\!|N_1'|\!)^\bullet/y_1|\!\}[\widetilde{x_{1k}\leftarrow x_{1k}}]\end{aligned}$$

where we define M' and N_1' to be M and N_1 after the substitutions of $\langle\widetilde{x_1}/x_1\rangle\cdots\langle\widetilde{x_k}/x_k\rangle$; similarly, we define M'' to be M'after the substitution of y_1 for x. On

the other hand,

$$\begin{aligned}(\!|\mathbb{M}|\!)^\circ &= (\!|M\{\!|N_1/x|\!\}\langle\!\langle \mathbf{1}/x\rangle\!\rangle|\!)^\circ \\ &= (\!|M\{\!|N_1/x|\!\}\langle\!\langle \mathbf{1}/x\rangle\!\rangle\langle\widetilde{x_1}/x_1\rangle\cdots\langle\widetilde{x_k}/x_k\rangle|\!)^\bullet[x_{1k}\widetilde{\leftarrow x_{1k}}] \\ &= (\!|M'\{\!|N_1'/x|\!\}\langle\!\langle \mathbf{1}/x\rangle\!\rangle|\!)^\bullet[x_{1k}\widetilde{\leftarrow x_{1k}}] \\ &= (\!|M'\{\!|N_1'/x|\!\}|\!)^\bullet[\leftarrow x]\langle\!\langle \mathbf{1}/x\rangle\!\rangle[x_{1k}\widetilde{\leftarrow x_{1k}}]\end{aligned}$$

By the congruence defined in Fig. 13 for $\lambda^{\lightning}_{\oplus}$, one has $M\langle\!\langle \mathbf{1}/x\rangle\!\rangle \equiv_\lambda M$. Therefore, $\mathbb{M} = M\{\!|N_1/x|\!\}\langle\!\langle \mathbf{1}/x\rangle\!\rangle \equiv_\lambda M\{\!|N_1/x|\!\} = \mathbb{M}'$. Expanding $(\!|\mathbb{M}'|\!)^\circ$ we have:

$$\begin{aligned}(\!|\mathbb{M}'|\!)^\circ &= (\!|M\{\!|N_1/x|\!\}|\!)^\circ \\ &= (\!|M\{\!|N_1/x|\!\}\langle\widetilde{x_1}/x_1\rangle\cdots\langle\widetilde{x_j}/x_j\rangle|\!)^\bullet[x_{1k}\widetilde{\leftarrow x_{1k}}] \\ &= (\!|M'\{\!|N_1'/x|\!\}|\!)^\bullet[x_{1k}\widetilde{\leftarrow x_{1k}}] \\ &= (\!|M'|\!)^\bullet\{\!|(\!|N_1'|\!)^\bullet/x|\!\}[x_{1k}\widetilde{\leftarrow x_{1k}}]\end{aligned}$$

Hence, $(\!|\mathbb{N}|\!)^\circ \longrightarrow (\!|\mathbb{M}'|\!)^\circ$ and the result follows.

(2) $n > 1$

To simplify the proof, we take $n = 2$ (the analysis when $n > 2$ is similar). Then $B = \wr N_1, N_2 \wr$ and the reduction is

$$\mathbb{N} = M\langle\!\langle B/x\rangle\!\rangle \longrightarrow M\{\!|N_1/x|\!\}\langle\!\langle \wr N_2 \wr/x\rangle\!\rangle + M\{\!|N_2/x|\!\}\langle\!\langle \wr N_1 \wr/x\rangle\!\rangle = \mathbb{M}$$

Notice that $\#(x, M) = 2$, we take y_1, y_2 fresh variables. On the one hand, we have:

$$\begin{aligned}(\!|\mathbb{N}|\!)^\circ &= (\!|M\langle\!\langle B/x\rangle\!\rangle|\!)^\circ = (\!|M\langle\!\langle B/x\rangle\!\rangle\langle\widetilde{x_1}/x_1\rangle\cdots\langle\widetilde{x_k}/x_k\rangle|\!)^\bullet[x_{1k}\widetilde{\leftarrow x_{1k}}] \\ &= (\!|M'\langle\!\langle B'/x\rangle\!\rangle|\!)^\bullet[x_{1k}\widetilde{\leftarrow x_{1k}}] \\ &= ((\!|M'\langle y_1, y_2/x\rangle|\!)^\bullet\langle\!|(\!|N_1'|\!)^\bullet/y_1|\!\rangle\langle\!|(\!|N_2'|\!)^\bullet/y_2|\!\rangle \\ &\quad + (\!|M'\langle y_1, y_2/x\rangle|\!)^\bullet\langle\!|(\!|N_2'|\!)^\bullet/y_1|\!\rangle\langle\!|(\!|N_1'|\!)^\bullet/y_2|\!\rangle)[x_{1k}\widetilde{\leftarrow x_{1k}}] \\ &= ((\!|M''|\!)^\bullet\langle\!|(\!|N_1'|\!)^\bullet/y_1|\!\rangle\langle\!|(\!|N_2'|\!)^\bullet/y_2|\!\rangle \\ &\quad + (\!|M''|\!)^\bullet\langle\!|(\!|N_2'|\!)^\bullet/y_1|\!\rangle\langle\!|(\!|N_1'|\!)^\bullet/y_2|\!\rangle)[x_{1k}\widetilde{\leftarrow x_{1k}}] \\ &\longrightarrow^2_{[\texttt{RS:Lin-Fetch}]} ((\!|M''|\!)^\bullet\{\!|(\!|N_1'|\!)^\bullet/y_1|\!\}\langle\!|(\!|N_2'|\!)^\bullet/y_2|\!\rangle \\ &\quad + (\!|M''|\!)^\bullet\{\!|(\!|N_2'|\!)^\bullet/y_1|\!\}\langle\!|(\!|N_1'|\!)^\bullet/y_2|\!\rangle)[x_{1k}\widetilde{\leftarrow x_{1k}}] \\ &= \mathbb{L}.\end{aligned} \tag{C.6}$$

where we define M' and B' to be M and B after the substitutions of $\langle\widetilde{x_1}/x_1\rangle\cdots\langle\widetilde{x_k}/x_k\rangle$ and N_1', N_2' are the the elements of the bag B'. Similarly, we define M''

to be M' after the substitution $\langle y_1, y_2/x\rangle$. On the other hand, we have:

$$\begin{aligned}
(\!|\mathbb{M}|\!)^\circ &= (\!|M\{\!|N_1/x|\!\}\langle\!\langle \wr N_2 \wr/x\rangle\!\rangle + M\{\!|N_2/x|\!\}\langle\!\langle \wr N_1 \wr/x\rangle\!\rangle|\!)^\circ \\
&= (\!|M\{\!|N_1/x|\!\}\langle\!\langle \wr N_2 \wr/x\rangle\!\rangle|\!)^\circ + (\!|M\{\!|N_2/x|\!\}\langle\!\langle \wr N_1 \wr/x\rangle\!\rangle|\!)^\circ \\
&= (\!|M\{\!|N_1/x|\!\}\langle\!\langle N_2/x\rangle\!\rangle|\!)^\bullet\langle\widetilde{x_1}/x_1\rangle\cdots\langle\widetilde{x_k}/x_k\rangle[\widetilde{x_{1k} \leftarrow x_{1k}}] \\
&\qquad + (\!|M\{\!|N_2/x|\!\}\langle\!\langle N_1/x\rangle\!\rangle\langle\widetilde{x_1}/x_1\rangle\cdots\langle\widetilde{x_k}/x_k\rangle|\!)^\bullet[\widetilde{x_{1k} \leftarrow x_{1k}}] \\
&= (\!|M'\{\!|N_1'/x|\!\}\langle\!\langle N_2'/x\rangle\!\rangle|\!)^\bullet[\widetilde{x_{1k} \leftarrow x_{1k}}] \\
&\qquad + (\!|M'\{\!|N_2'/x|\!\}\langle\!\langle N_1'/x\rangle\!\rangle|\!)^\bullet[\widetilde{x_{1k} \leftarrow x_{1k}}] \\
&= (\!|M'\{\!|N_1'/x|\!\}|\!)^\bullet\langle\!|(\!|N_2'|\!)^\bullet/y_2|\!\rangle[\widetilde{x_{1k} \leftarrow x_{1k}}] \\
&\qquad + (\!|M'\{\!|N_2'/x|\!\}|\!)^\bullet\langle\!|(\!|N_1'|\!)^\bullet/y_2|\!\rangle[\widetilde{x_{1k} \leftarrow x_{1k}}]
\end{aligned} \tag{C.7}$$

The reductions in (C.6) and (C.7) lead to identical expressions, up to renaming of shared variables, which are taken to be fresh by definition. In both cases, we have taken the same fresh variables.

(3) The rule applied is $[\mathtt{R}] \neq [\mathtt{R} : \mathtt{Beta}]$ and $[\mathtt{R}] \neq [\mathtt{R} : \mathtt{Fetch}]$. There are two possible cases. Below $[\widetilde{x_{1n} \leftarrow x_{1n}}]$ abbreviates $[\widetilde{x_1} \leftarrow x_1]\cdots[\widetilde{x_n} \leftarrow x_n]$:

(I) $[\mathtt{R}] = [\mathtt{R} : \mathtt{Fail}]$

Then $\mathbb{N} = M\langle\!\langle B/x\rangle\!\rangle$ and the reduction is

$$[\mathtt{R} : \mathtt{Fail}]\ \frac{\#(x, M) \neq \mathsf{size}(B) \qquad \widetilde{y} = (\mathsf{mfv}(M) \setminus x) \uplus \mathsf{mfv}(B)}{M\ \langle\!\langle B/x\rangle\!\rangle \longrightarrow \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{y}}}$$

where $\mathbb{M} = \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{y}}$. Below assume $\mathsf{fv}(\mathbb{N}) = \{x_1, \ldots, x_n\}$.
On the one hand, we have:

$$\begin{aligned}
(\!|\mathbb{N}|\!)^\circ &= (\!|M\langle\!\langle B/x\rangle\!\rangle|\!)^\circ = (\!|M\langle\!\langle B/x\rangle\!\rangle\langle\widetilde{x_1}/x_1\rangle\cdots\langle\widetilde{x_n}/x_n\rangle|\!)^\bullet[\widetilde{x_{1n} \leftarrow x_{1n}}] \\
&= (\!|M'\langle\!\langle B'/x\rangle\!\rangle|\!)^\bullet[\widetilde{x_{1n} \leftarrow x_{1n}}] \\
&= (\!|M'\langle y_1, \cdots, y_k/x\rangle|\!)^\bullet[y_1, \cdots, y_k \leftarrow x]\langle\!\langle (\!|B'|\!)^\bullet/x\rangle\!\rangle[\widetilde{x_{1n} \leftarrow x_{1n}}] \\
&\longrightarrow_{[\mathtt{RS:Fail}]} \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{y}}\ [\widetilde{x_{1n} \leftarrow x_{1n}}] = \mathbb{L}
\end{aligned}$$

where we define M' and B' to be M and B after the substitutions of $\langle\widetilde{x_1}/x_1\rangle\cdots\langle\widetilde{x_k}/x_k\rangle$. On the other hand, we have:

$$\begin{aligned}
(\!|\mathbb{M}|\!)^\circ &= (\!|\sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{y}}|\!)^\circ = \sum_{\mathsf{PER}(B)} (\!|\mathtt{fail}^{\widetilde{y}}|\!)^\circ \\
&= \sum_{\mathsf{PER}(B)} (\!|\mathtt{fail}^{\widetilde{y}}|\!)^\bullet[\widetilde{x_{1n} \leftarrow x_{1n}}] = \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{y}}[\widetilde{x_{1n} \leftarrow x_{1n}}] = \mathbb{L}
\end{aligned}$$

Therefore, $(\!|\mathbb{N}|\!)^\circ \longrightarrow (\!|\mathbb{M}|\!)^\circ$ and the result follows.

(II) $[\mathtt{R}] = [\mathtt{R} : \mathtt{Cons}_1]$.

Then $\mathbb{N} = \mathtt{fail}^{\widetilde{y}}\ B$ and the reduction is

$$[\mathtt{R} : \mathtt{Cons}_1]\ \frac{\mathsf{size}(B) = k \qquad \widetilde{z} = \mathsf{mfv}(B)}{\mathtt{fail}^{\widetilde{y}}\ B \longrightarrow \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{y} \uplus \widetilde{z}}}$$

and $\mathbb{M}' = \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{y} \uplus \widetilde{z}}$. Below we assume $\mathsf{fv}(\mathbb{N}) = \{x_1, \ldots, x_n\}$. On the one hand, we have:

$$
\begin{aligned}
(\!|N|\!)^\circ &= (\!|\mathtt{fail}^{\widetilde{y}}\ B|\!)^\circ = (\!|\mathtt{fail}^{\widetilde{y}}\ B\langle\widetilde{x_1}/x_1\rangle \cdots \langle\widetilde{x_n}/x_n\rangle|\!)^\bullet[x_{1n} \widetilde{\leftarrow} x_{1n}] \\
&= (\!|\mathtt{fail}^{\widetilde{y'}}\ B'|\!)^\bullet[x_{1n} \widetilde{\leftarrow} x_{1n}] = (\!|\mathtt{fail}^{\widetilde{y'}}|\!)^\bullet\ (\!|B'|\!)^\bullet[x_{1n} \widetilde{\leftarrow} x_{1n}] \\
&= \mathtt{fail}^{\widetilde{y'}}\ (\!|B'|\!)^\bullet[x_{1n} \widetilde{\leftarrow} x_{1n}] \\
&\longrightarrow_{[\mathtt{RS:Cons}_1]} \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{y'} \cup \widetilde{z'}}[x_{1n} \widetilde{\leftarrow} x_{1n}] = \mathbb{L}
\end{aligned}
$$

where we define B' to be B after the substitutions of $\langle\widetilde{x_1}/x_1\rangle \cdots \langle\widetilde{x_k}/x_k\rangle$. Similarly, $\widetilde{y'}$ and $\widetilde{z'}$ are $\widetilde{y}$ and $\widetilde{z}$ after the substitution $\langle\widetilde{x_1}/x_1\rangle \cdots \langle\widetilde{x_k}/x_k\rangle$. On the other hand, we have:

$$
\begin{aligned}
(\!|M|\!)^\circ &= (\!|\sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{y} \uplus \widetilde{z}}|\!)^\circ = \sum_{\mathsf{PER}(B)} (\!|\mathtt{fail}^{\widetilde{y} \uplus \widetilde{z}}|\!)^\circ \\
&= \sum_{\mathsf{PER}(B)} (\!|\mathtt{fail}^{\widetilde{y'} \uplus \widetilde{z'}}|\!)^\bullet[x_{1n} \widetilde{\leftarrow} x_{1n}] = \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{y'} \cup \widetilde{z'}}[x_{1n} \widetilde{\leftarrow} x_{1n}] = \mathbb{L}
\end{aligned}
$$

Therefore, $(\!|\mathbb{N}|\!)^\circ \longrightarrow \mathbb{L} = (\!|\mathbb{M}|\!)^\circ$, and the result follows.

(III) $[\mathtt{R}] = [\mathtt{R} : \mathtt{Cons}_2]$

Then $\mathbb{N} = \mathtt{fail}^{\widetilde{y}}\ \langle\!\langle B/x \rangle\!\rangle$ and the reduction is

$$
[\mathtt{R} : \mathtt{Cons}_2]\ \frac{\mathsf{size}(B) = k \qquad \#(x, \widetilde{y}) + k \neq 0 \qquad \widetilde{z} = \mathsf{mfv}(B)}{\mathtt{fail}^{\widetilde{y}}\ \langle\!\langle B/x \rangle\!\rangle \longrightarrow \sum_{\mathsf{PER}(B)} \mathtt{fail}^{(\widetilde{y} \setminus x) \uplus \widetilde{z}}}
$$

and $\mathbb{M} = \sum_{\mathsf{PER}(B)} \mathtt{fail}^{(\widetilde{y} \setminus x) \uplus \widetilde{z}}$. Below we assume $\mathsf{fv}(\mathbb{N}) = \{x_1, \ldots, x_n\}$. On the one hand, we have: (below $\widetilde{y} = y_1, \ldots, y_m$)

$$
\begin{aligned}
(\!|\mathbb{N}|\!)^\circ &= (\!|\mathtt{fail}^{\widetilde{y}}\ \langle\!\langle B/x \rangle\!\rangle|\!)^\circ \\
&= (\!|\mathtt{fail}^{\widetilde{y}}\ \langle\!\langle B/x \rangle\!\rangle\langle\widetilde{x_1}/x_1\rangle \cdots \langle\widetilde{x_n}/x_n\rangle|\!)^\bullet[x_{1n} \widetilde{\leftarrow} x_{1n}] \\
&= (\!|\mathtt{fail}^{\widetilde{y'}}\langle y_1/x\rangle \cdots \langle y_m/x\rangle|\!)^\bullet[\widetilde{y} \leftarrow x]\ \langle\!\langle (\!|B'|\!)^\bullet/x \rangle\!\rangle[x_{1n} \widetilde{\leftarrow} x_{1n}] \qquad \text{(C.8)} \\
&= \mathtt{fail}^{\widetilde{y''}}[\widetilde{y} \leftarrow x]\ \langle\!\langle (\!|B'|\!)^\bullet/x \rangle\!\rangle[x_{1n} \widetilde{\leftarrow} x_{1n}] \\
&\longrightarrow_{[\mathtt{RS:Cons}_2]} \mathtt{fail}^{(\widetilde{y'} \setminus x) \cup \widetilde{z'}}[x_{1n} \widetilde{\leftarrow} x_{1n}]
\end{aligned}
$$

As $\widetilde{y}$ consists of free variables, in $\mathtt{fail}^{\widetilde{y}}\ \langle\!\langle B/x \rangle\!\rangle\langle\widetilde{x_1}/x_1\rangle \cdots \langle\widetilde{x_n}/x_n\rangle$ the substitutions also occur on $\widetilde{y}$ resulting in a new $\widetilde{y'}$ where all x_i's are replaced with their fresh components in $\widetilde{x_i}$. Similarly for z' and B' as well as $\widetilde{y''}$ being $\widetilde{y'}$ with each x replaced with a fresh y_i. On the other hand, we have:

$$
\begin{aligned}
(\!|M|\!)^\circ &= (\!|\sum_{\mathsf{PER}(B)} \mathtt{fail}^{(\widetilde{y} \setminus x) \uplus \widetilde{z}}|\!)^\circ = \sum_{\mathsf{PER}(B)} (\!|\mathtt{fail}^{(\widetilde{y} \setminus x) \uplus \widetilde{z}}|\!)^\circ \\
&= \sum_{\mathsf{PER}(B)} (\!|\mathtt{fail}^{(\widetilde{y'} \setminus x) \uplus \widetilde{z}}|\!)^\bullet[x_{1n} \widetilde{\leftarrow} x_{1n}] = \mathtt{fail}^{(\widetilde{y'} \setminus x) \cup \widetilde{z'}}[x_{1n} \widetilde{\leftarrow} x_{1n}]
\end{aligned}
\qquad \text{(C.9)}
$$

The reductions in (C.8) and (C.9) lead to identical expressions.

As before, the reduction via Rule [R] could occur inside a context (cf. Rules [R : TCont] and [R : ECont]). We consider only the case when the contextual rule used is [R : TCont]. We have $\mathbb{N} = C[N]$. When we have $C[N] \longrightarrow_{[R]} C[M]$ such that $N \longrightarrow_{[R]} M$ we need to show that $(\!|C[N]|\!)^\circ \longrightarrow^j (\!|C[M]|\!)^\circ$for some j dependent on [R]. Firstly, let us assume $[R] = [R : \mathtt{Cons}_2]$ then we take $j = 1$. Let us take $C[\cdot]$ to be $[\cdot]B$ and $\mathsf{fv}(NB) = \{x_1, \cdots, x_k\}$ then

$$\begin{aligned}(\!|NB|\!)^\circ &= (\!|NB\langle\widetilde{x_1}/x_1\rangle \cdots \langle\widetilde{x_k}/x_k\rangle|\!)^\bullet[\widetilde{x_{1k} \leftarrow x_{1k}}] \\ &= (\!|N'B'|\!)^\bullet[\widetilde{x_{1k} \leftarrow x_{1k}}] = (\!|N'|\!)^\bullet(\!|B'|\!)^\bullet[\widetilde{x_{1k} \leftarrow x_{1k}}]\end{aligned}$$

We take $N'B' = NB\langle\widetilde{x_1}/x_1\rangle \cdots \langle\widetilde{x_k}/x_k\rangle$, and by the IH that $(\!|N|\!)^\bullet \longrightarrow (\!|M|\!)^\bullet$ and hence we can deduce that $(\!|N'|\!)^\bullet \longrightarrow (\!|M'|\!)^\bullet$ where $M'B' = MB\langle\widetilde{x_1}/x_1\rangle \cdots \langle\widetilde{x_k}/x_k\rangle$. Finally,

$$(\!|N'|\!)^\bullet(\!|B'|\!)^\bullet[\widetilde{x_{1k} \leftarrow x_{1k}}] \longrightarrow (\!|M'|\!)^\bullet(\!|B'|\!)^\bullet[\widetilde{x_{1k} \leftarrow x_{1k}}]$$

and hence $(\!|C[N]|\!)^\circ \longrightarrow (\!|C[M]|\!)^\circ$. □

Theorem 5.9 (Operational Soundness)**.** *Let $\mathbb{N}$ be a well-formed $\lambda^{\not\downarrow}_{\oplus}$ expression. Suppose $(\!|\mathbb{N}|\!)^\circ \longrightarrow \mathbb{L}$. Then, there exists $\mathbb{N}'$ such that $\mathbb{N} \longrightarrow_{[R]} \mathbb{N}'$ and*

(1) *If $[R] = [R : \mathtt{Beta}]$ then $\mathbb{L} \longrightarrow^{\leq 1} (\!|\mathbb{N}'|\!)^\circ$;*
(2) *If $[R] \neq [R : \mathtt{Beta}]$ then $\mathbb{L} \longrightarrow^* (\!|\mathbb{N}''|\!)^\circ$, for $\mathbb{N}''$ such that $\mathbb{N}' \equiv_\lambda \mathbb{N}''$.*

Proof. By induction on the structure of $\mathbb{N}$ with the following six cases given below, where $\widetilde{[x_{1k} \leftarrow x_{1k}]}$ abbreviates $[\widetilde{x_1 \leftarrow x_1}] \ldots [\widetilde{x_k \leftarrow x_k}]$:

i) $\mathbb{N} = x$:
Then $(\!|x|\!)^\circ = x_1[x_1 \leftarrow x]$, and no reductions can be performed.

ii) $\mathbb{N} = \lambda x.N$:
Suppose $\mathsf{fv}(N) = \{x_1, \cdots, x_k\}$. Then,

$$\begin{aligned}(\!|\lambda x.N|\!)^\circ &= (\!|\lambda x.N\langle\widetilde{x_1}/x_1\rangle \cdots \langle\widetilde{x_k}/x_k\rangle|\!)^\bullet[\widetilde{x_{1k} \leftarrow x_{1k}}] \\ &= (\!|\lambda x.N'|\!)^\bullet[\widetilde{x_{1k} \leftarrow x_{1k}}] = \lambda x.(\!|N'\langle\widetilde{y}/x\rangle|\!)^\bullet[\widetilde{y} \leftarrow x][\widetilde{x_{1k} \leftarrow x_{1k}}],\end{aligned}$$

where N' is N after the substitutions $\langle\widetilde{x_1}/x_1\rangle \cdots \langle\widetilde{x_k}/x_k\rangle$ and no reductions can be performed.

iii) $\mathbb{N} = NB$:
Suppose $\mathsf{fv}(NB) = \{x_1, \cdots, x_n\}$. Then

$$\begin{aligned}(\!|\mathbb{N}|\!)^\circ &= (\!|NB|\!)^\circ = (\!|NB\langle\widetilde{x_1}/x_1\rangle \cdots \langle\widetilde{x_n}/x_n\rangle|\!)^\bullet[\widetilde{x_{1n} \leftarrow x_{1n}}] \\ &= (\!|N'B'|\!)^\bullet[\widetilde{x_{1n} \leftarrow x_{1n}}] = (\!|N'|\!)^\bullet(\!|B'|\!)^\bullet[\widetilde{x_{1n} \leftarrow x_{1n}}]\end{aligned} \tag{C.10}$$

where $\widetilde{x_i} = x_{i1}, \ldots, x_{ij_i}$, for $1 \leq i \leq n$ and N', B' are N and B after performing the substitutions $\langle\widetilde{x_1}/x_1\rangle \cdots \langle\widetilde{x_k}/x_k\rangle$. By the reduction rules in Fig. 5 there are three possible reductions starting in $\mathbb{N}$:

(a) $(\!|N'|\!)^\bullet(\!|B'|\!)^\bullet[\widetilde{x_{1n} \leftarrow x_{1n}}]$ reduces via rule [RS:Beta].
In this case $N = \lambda x.N_1$, and the encoding in (C.10) gives $N' = N\langle\widetilde{x_1}/x_1\rangle \cdots \langle\widetilde{x_n}/x_n\rangle$, which implies $N' = \lambda x.N_1^{'}$ and the following holds:

$$(\!|N'|\!)^\bullet = (\!|(\lambda x.N_1')|\!)^\bullet = (\lambda x.(\!|N_1'\langle\widetilde{y}/x\rangle|\!)^\bullet[\widetilde{y} \leftarrow x]) = (\lambda x.(\!|N^{''}|\!)^\bullet[\widetilde{y} \leftarrow x])$$

Thus, we have the following [RS:Beta] reduction from (C.10):

$$\begin{aligned}(\!|\mathbb{N}|\!)^\circ &= (\!|N'|\!)^\bullet(\!|B'|\!)^\bullet[\widetilde{x_{1n} \leftarrow x_{1n}}] = (\lambda x.(\!|N''|\!)^\bullet[\widetilde{y} \leftarrow x](\!|B'|\!)^\bullet)[\widetilde{x_{1n} \leftarrow x_{1n}}] \\ &\longrightarrow_{[\texttt{RS:Beta}]} (\!|N^{''}|\!)^\bullet[\widetilde{y} \leftarrow x]\langle\!\langle(\!|B'|\!)^\bullet/x\rangle\!\rangle[\widetilde{x_{1n} \leftarrow x_{1n}}] = \mathbb{L}\end{aligned} \tag{C.11}$$

where N'' is N' after the substitutions $\langle\widetilde{y}/x\rangle$. Notice that the expression $\mathbb{N}$ can perform the following [R : Beta]-reduction:

$$\mathbb{N} = (\lambda x.N_1)B \longrightarrow_{[\texttt{R:Beta}]} N_1\langle\!\langle B/x\rangle\!\rangle$$

Assuming $\mathbb{N}' = N_1\langle\!\langle B/x\rangle\!\rangle$, there are two cases:

(i) $\#(x, M) = \mathsf{size}(B) = k \geq 1$.
On the one hand:

$$\begin{aligned}(\!|\mathbb{N}'|\!)^\circ &= (\!|N_1\langle\!\langle B/x\rangle\!\rangle|\!)^\circ \\ &= (\!|N_1\langle\!\langle B/x\rangle\!\rangle\langle\widetilde{x_1}/x_1\rangle\cdots\langle\widetilde{x_n}/x_n\rangle|\!)^\bullet[\widetilde{x_{1n} \leftarrow x_{1n}}] \\ &= (\!|N_1'\langle\!\langle B'/x\rangle\!\rangle|\!)^\bullet[\widetilde{x_{1n} \leftarrow x_{1n}}] \\ &= \sum_{B_i \in \mathsf{PER}((\!|B|\!)^\bullet)} (\!|N_1'\langle y_1, \cdots, y_k/x\rangle|\!)^\bullet(\!|B_i(1)/y_1|\!)\cdots(\!|B_i(k)/y_k|\!)[\widetilde{x_{1n} \leftarrow x_{1n}}] \\ &= \sum_{B_i \in \mathsf{PER}((\!|B|\!)^\bullet)} (\!|N_1''|\!)^\bullet(\!|B_i(1)/y_1|\!)\cdots(\!|B_i(k)/y_k|\!)[\widetilde{x_{1n} \leftarrow x_{1n}}]\end{aligned}$$

where N_1'' is N_1' after the substitution $\langle\widetilde{y}/x\rangle$.
On the other hand, after an application of Rule [RS : Ex − Sub]:

$$\begin{aligned}\mathbb{L} &= (\!|N''|\!)^\bullet[\widetilde{y} \leftarrow x]\langle\!\langle(\!|B'|\!)^\bullet/x\rangle\!\rangle[\widetilde{x_{1n} \leftarrow x_{1n}}] \\ &\longrightarrow \sum_{B_i \in \mathsf{PER}((\!|B|\!)^\bullet)} (\!|N_1''|\!)^\bullet(\!|B_i(1)/y_1|\!)\cdots(\!|B_i(k)/y_k|\!)[\widetilde{x_{1n} \leftarrow x_{1n}}] \\ &= (\!|\mathbb{N}'|\!)^\circ\end{aligned}$$

and the result follows.

(ii) Otherwise, either $\#(x, N_1) = k = 0$ or $\#(x, N_1) \neq \mathsf{size}(B)$. In this case:

$$\begin{aligned}(\!|\mathbb{N}'|\!)^\circ &= (\!|N_1\langle\!\langle B/x\rangle\!\rangle|\!)^\circ \\ &= (\!|N_1\langle\!\langle B/x\rangle\!\rangle\langle\widetilde{x_1}/x_1\rangle\cdots\langle\widetilde{x_n}/x_n\rangle|\!)^\bullet[\widetilde{x_{1n} \leftarrow x_{1n}}] \\ &= (\!|N_1'\langle\!\langle B'/x\rangle\!\rangle|\!)^\bullet[\widetilde{x_{1n} \leftarrow x_{1n}}] \\ &= (\!|N^{''}|\!)^\bullet[\widetilde{y} \leftarrow x]\langle\!\langle(\!|B'|\!)^\bullet/x\rangle\!\rangle[\widetilde{x_{1n} \leftarrow x_{1n}}] = \mathbb{L}\end{aligned}$$

From (C.11): $(\!|\mathbb{N}|\!)^\circ \longrightarrow \mathbb{L} = (\!|\mathbb{N}'|\!)^\circ$ and the result follows.

(b) $(\!|N'|\!)^\bullet(\!|B'|\!)^\bullet[\widetilde{x_{1n} \leftarrow x_{1n}}]$ reduces via rule [$\texttt{RS:Cons}_1$].
In this case we would have $N = \texttt{fail}^{\widetilde{y}}$, and the encoding in (C.10) gives $N' = N\langle\widetilde{x_1}/x_1\rangle\ldots\langle\widetilde{x_n}/x_n\rangle$, which implies $N' = \texttt{fail}^{\widetilde{y'}}$, we let $\mathsf{size}(B) = k$ and the following:

$$\begin{aligned}(\!|\mathbb{N}|\!)^\circ &= (\!|N'|\!)^\bullet(\!|B'|\!)^\bullet[\widetilde{x_{1n} \leftarrow x_{1n}}] = (\!|\mathtt{fail}^{\widetilde{y'}}|\!)^\bullet(\!|B'|\!)^\bullet[\widetilde{x_{1n} \leftarrow x_{1n}}] \\ &= \mathtt{fail}^{\widetilde{y'}}(\!|B'|\!)^\bullet[\widetilde{x_{1n} \leftarrow x_{1n}}] \\ &\longrightarrow \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{y'\uplus\widetilde{z}}}[\widetilde{x_{1n} \leftarrow x_{1n}}], \text{ where } \widetilde{z} = \mathsf{fv}(B')\end{aligned} \tag{C.12}$$

The expression $\mathbb{N}$ can perform the following $[\mathtt{R}] = [\mathtt{R} : \mathtt{Cons}_1]$-reduction:

$$\mathbb{N} = \mathtt{fail}^{\widetilde{y}}\ B \longrightarrow_{[\mathtt{R}]} \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{y\uplus z}} \text{ where } \widetilde{z} = \mathsf{mfv}(B) \tag{C.13}$$

From (C.12) and (C.13), we infer that $\mathbb{L} = (\!|\mathbb{N}'|\!)^\circ$ and so the result follows.

(c) Suppose that $(\!|N'|\!)^\bullet \longrightarrow (\!|N''|\!)^\bullet$.
This case follows from the IH.

iv) $\mathbb{N} = N\langle\!\langle B/x \rangle\!\rangle$:
Suppose $\mathsf{fv}(N\langle\!\langle B/x \rangle\!\rangle) = \{x_1, \cdots, x_k\}$. Then,

$$\begin{aligned}(\!|\mathbb{N}|\!)^\circ = (\!|N\langle\!\langle B/x \rangle\!\rangle|\!)^\circ &= (\!|N\langle\!\langle B/x \rangle\!\rangle\langle\widetilde{x_1}/x_1\rangle \cdots \langle\widetilde{x_k}/x_k\rangle|\!)^\bullet[\widetilde{x_{1k} \leftarrow x_{1k}}] \\ &= (\!|N'\langle\!\langle B'/x \rangle\!\rangle|\!)^\bullet[\widetilde{x_{1k} \leftarrow x_{1k}}]\end{aligned} \tag{C.14}$$

where N', B' are N and B after performing the substitutions $\langle\widetilde{x_1}/x_1\rangle \cdots \langle\widetilde{x_k}/x_k\rangle$.
Let us consider the two possibilities of the encoding:

(1) $\#(x, M) = \mathsf{size}(B) = k \geq 1$.
Then we continue equation (C.14) as follows:

$$\begin{aligned}(\!|\mathbb{N}|\!)^\circ &= (\!|N'\langle\!\langle B'/x \rangle\!\rangle|\!)^\bullet[\widetilde{x_{1k} \leftarrow x_{1k}}] \\ &= \sum_{B_i \in \mathsf{PER}((\!|B'|\!)^\bullet)} (\!|N'\langle y_1, \cdots, y_n/x\rangle|\!)^\bullet(\!|B_i(1)/y_1|\!) \cdots (\!|B_i(n)/y_n|\!)[\widetilde{x_{1k} \leftarrow x_{1k}}] \\ &= \sum_{B_i \in \mathsf{PER}((\!|B'|\!)^\bullet)} (\!|N''|\!)^\bullet(\!|B_i(1)/y_1|\!) \cdots (\!|B_i(n)/y_n|\!)[\widetilde{x_{1k} \leftarrow x_{1k}}]\end{aligned} \tag{C.15}$$

where N'' is N' after performing the substitutions $\langle y_1, \cdots, y_n/x\rangle$. There are three possible reductions, these being from rules [RS:Lin-Fetch], [RS:Cons$_3$], and [RS:Cont].

(I) Suppose that $\mathsf{head}(N'') = y_1$.
Then one has to consider the shape of the bag B':

(A) When B' has only one element N_1 then from (C.15) and by letting $B = \wr N_1 \int$ and $B' = \wr N_1' \int$ we have

$$\begin{aligned}(\!|\mathbb{N}|\!)^\circ &= (\!|N''|\!)^\bullet(\!|(\!|N_1'|\!)^\bullet/y_1|\!)[\widetilde{x_{1k} \leftarrow x_{1k}}], \text{since } \mathsf{head}(M') = y_1 \\ &\longrightarrow (\!|N''|\!)^\bullet\{\!|(\!|N_1'|\!)^\bullet/y_1|\!\}[\widetilde{x_{1k} \leftarrow x_{1k}}] = \mathbb{L}\end{aligned} \tag{C.16}$$

We also have:

$$\begin{aligned}&\mathbb{N} = N\langle\!\langle \wr N_1 \int / x \rangle\!\rangle \\ &\quad\longrightarrow N\{\!|N_1/x|\!\}\langle\!\langle 1/x \rangle\!\rangle = \mathbb{N}' \equiv_\lambda N\{\!|N_1/x|\!\} = \mathbb{N}''\end{aligned} \tag{C.17}$$

From (C.16) and (C.17), we infer that $\mathbb{L}' = (\!|\mathbb{N}'|\!)^\circ$ and so the result follows.

(B) When B' has more then one element. Let us say that $B = \wr N_1, N_2 \wr$ and $B' = \wr N_1', N_2' \wr$ and cases for larger bags proceed similarly then from (C.15). (Below we use the fact that $\mathsf{head}(M') = y_1$)

$$\begin{aligned}(\!|\mathbb{N}|\!)^\circ &= (\!|N''|\!)^\bullet \langle\!\langle (\!|N_1'|\!)^\bullet / y_1 \rangle\!\rangle \langle\!\langle (\!|N_2'|\!)^\bullet / y_2 \rangle\!\rangle [x_{1k} \xleftarrow{\sim} x_{1k}] \\ &\quad + (\!|N''|\!)^\bullet \langle\!\langle (\!|N_2'|\!)^\bullet / y_1 \rangle\!\rangle \langle\!\langle (\!|N_1'|\!)^\bullet / y_2 \rangle\!\rangle [x_{1k} \xleftarrow{\sim} x_{1k}], \\ &\longrightarrow (\!|N''|\!)^\bullet \{\!| (\!|N_1'|\!)^\bullet / y_1 |\!\} \langle\!\langle (\!|N_2'|\!)^\bullet / y_2 \rangle\!\rangle [[x_{1k} \xleftarrow{\sim} x_{1k}] \\ &\quad + (\!|N''|\!)^\bullet \{\!| (\!|N_2'|\!)^\bullet / y_1 |\!\} \langle\!\langle (\!|N_1'|\!)^\bullet / y_2 \rangle\!\rangle [x_{1k} \xleftarrow{\sim} x_{1k}] = \mathbb{L}\end{aligned} \tag{C.18}$$

We also have:

$$\begin{aligned}\mathbb{N} &= N \langle\!\langle \wr N_1, N_2 \wr / x \rangle\!\rangle \\ &\longrightarrow N\{\!|N_1/x|\!\}\langle\!\langle \wr N_2 \wr / x \rangle\!\rangle + N\{\!|N_2/x|\!\}\langle\!\langle \wr N_1 \wr / x \rangle\!\rangle = \mathbb{N}'\end{aligned} \tag{C.19}$$

From (C.18) and (C.19), we infer that $\mathbb{L}' = (\!|\mathbb{N}'|\!)^\circ$ and so the result follows.

(II) Suppose that $N'' = \mathtt{fail}^{\widetilde{z'}}$. Then we proceed similarly as from (C.15):

$$\begin{aligned}(\!|\mathbb{N}|\!)^\circ &= \sum_{B_i \in \mathsf{PER}((\!|B'|\!)^\bullet)} \mathtt{fail}^{\widetilde{z'}} \langle\!| B_i(1)/y_1 |\!\rangle \cdots \langle\!| B_i(n)/y_n |\!\rangle \\ &\longrightarrow^* \sum_{B_i \in \mathsf{PER}((\!|B'|\!)^\bullet)} \mathtt{fail}^{(\widetilde{z'} \setminus y_1, \cdots, y_n) \uplus \widetilde{y}}, \text{ since } \mathsf{head}(M') = y_1 \\ &= \mathbb{L}'\end{aligned} \tag{C.20}$$

where $\widetilde{y} = \mathsf{fv}(B_i(1)) \uplus \cdots \uplus \mathsf{fv}(B_i(n))$. We also have that

$$\mathbb{N} = \mathtt{fail}^{\widetilde{z}} \langle\!\langle B/x \rangle\!\rangle \longrightarrow \mathtt{fail}^{(\widetilde{z} \setminus x) \uplus \widetilde{y}} = \mathbb{N}' \tag{C.21}$$

where $\widetilde{y} = \mathsf{mfv}(B)$. From (C.20) and (C.21), we infer that $\mathbb{L}' = (\!|\mathbb{N}'|\!)^\circ$ and so the result follows.

(III) Suppose that $N'' \longrightarrow N'''$
This case follows by the IH.

(2) Otherwise we continue equation (C.14) as follows where $\#(x, M) = k$

$$\begin{aligned}(\!|\mathbb{N}|\!)^\circ &= (\!|N' \langle\!\langle B'/x \rangle\!\rangle|\!)^\bullet [x_{1k} \xleftarrow{\sim} x_{1k}] \\ &= (\!|N' \langle y_1 . \cdots, y_k / x \rangle|\!)^\bullet [y_1 . \cdots, y_k \leftarrow x] \langle\!\langle (\!|B'|\!)^\bullet / x \rangle\!\rangle [x_{1k} \xleftarrow{\sim} x_{1k}] \\ &= (\!|N''|\!)^\bullet [y_1 . \cdots, y_k \leftarrow x] \langle\!\langle (\!|B'|\!)^\bullet / x \rangle\!\rangle [x_{1k} \xleftarrow{\sim} x_{1k}]\end{aligned} \tag{C.22}$$

Let us consider the two possible cases:

(I) $\#(x, M) = \mathsf{size}(B) = k = 0$.
Then we have:

$$(\!|\mathbb{N}|\!)^\circ = (\!|N'|\!)^\bullet \langle\!\langle 1/x \rangle\!\rangle [x_{1k} \xleftarrow{\sim} x_{1k}] \tag{C.23}$$

Reductions can only appear in $(\!|N'|\!)^\bullet$ and the case follows by the IH.

(II) Otherwise we can perform the reduction:

$$(\!|\mathbb{N}|\!)^\circ = (\!|N''|\!)^\bullet[y_1.\cdots,y_k \leftarrow x]\langle\!\langle (\!|B'|\!)^\bullet/x\rangle\!\rangle[\widetilde{x_{1k} \leftarrow x_{1k}}] \longrightarrow \sum_{B_i \in \mathsf{PER}(B)} \mathtt{fail}^{\widetilde{z'}}[\widetilde{x_{1k} \leftarrow x_{1k}}] = \mathbb{L}' \tag{C.24}$$

where $\widetilde{z'} = \mathsf{fv}(N'') \uplus \mathsf{fv}(B')$. We also have that

$$\mathbb{N} = N\langle\!\langle B/x\rangle\!\rangle \longrightarrow \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{z}} = \mathbb{N}' \tag{C.25}$$

where $\widetilde{z} = \mathsf{mfv}(M) \uplus \mathsf{mfv}(B)$.

From (C.24) and (C.25), we infer that $\mathbb{L}' = (\!|\mathbb{N}'|\!)^\circ$ and so the result follows.

v) $\mathbb{N} = \mathtt{fail}^{\widetilde{y}}$
Then $(\!|\mathtt{fail}^{\widetilde{y}}|\!)^\circ = \mathtt{fail}^{\widetilde{y}}$, and no reductions can be performed.

vi) $\mathbb{N} = \mathbb{N}_1 + \mathbb{N}_2$:
This case holds by the IH. □

C.3. **Success Sensitiveness.**

Proposition 5.13 (Preservation of head term)**.** *The head of a term is preserved when applying the translation* $(\!|\cdot|\!)^\circ$*, i.e.,*

$$\forall M \in \lambda^{\mathsf{t}}_{\oplus}.\ \mathsf{head}(M) = \checkmark \iff \mathsf{head}_{\sum}((\!|M|\!)^\circ) = \checkmark.$$

Proof. By induction on the structure of M. We only need to consider terms of the following form.

(1) When $M = \checkmark$ the case is immediate.
(2) When $M = NB$ with $\mathsf{fv}(NB) = \{x_1, \cdots, x_k\}$ and $\#(x_i, M) = j_i$ we have that:

$$\begin{aligned}\mathsf{head}_{\sum}((\!|NB|\!)^\circ) &= \mathsf{head}_{\sum}((\!|NB\langle\widetilde{x_1}/x_1\rangle\cdots\langle\widetilde{x_k}/x_k\rangle|\!)^\bullet[\widetilde{x_1} \leftarrow x_1]\cdots[\widetilde{x_k} \leftarrow x_k]) \\ &= \mathsf{head}_{\sum}((\!|NB|\!)^\bullet) = \mathsf{head}_{\sum}((\!|N|\!)^\bullet)\end{aligned}$$

and $\mathsf{head}(NB) = \mathsf{head}(N)$, by the IH we have $\mathsf{head}(N) = \checkmark \iff \mathsf{head}_{\sum}((\!|N|\!)^\bullet) = \checkmark$.

(3) When $M = N\langle\!\langle B/x\rangle\!\rangle$, we must have that $\#(x, M) = \mathsf{size}(B)$ for the head of this term to be $\checkmark$. Let $\mathsf{fv}(N\langle\!\langle B/x\rangle\!\rangle) = \{x_1, \cdots, x_k\}$ and $\#(x_i, M) = j_i$. We have that:

$$\begin{aligned}\mathsf{head}_{\sum}((\!|N\langle\!\langle B/x\rangle\!\rangle|\!)^\circ) &= \mathsf{head}_{\sum}((\!|N\langle\!\langle B/x\rangle\!\rangle\langle\widetilde{x_1}/x_1\rangle\cdots\langle\widetilde{x_k}/x_k\rangle|\!)^\bullet[\widetilde{x_1} \leftarrow x_1]\cdots[\widetilde{x_k} \leftarrow x_k]) \\ &= \mathsf{head}_{\sum}((\!|N\langle\!\langle B/x\rangle\!\rangle|\!)^\bullet) \\ &= \mathsf{head}_{\sum}(\sum_{B_i \in \mathsf{PER}((\!|B|\!)^\bullet)} (\!|N\langle x_1, \cdots, x_k/x\rangle|\!)^\bullet\langle\!|B_i(1)/x_1|\!\rangle\cdots\langle\!|B_i(k)/x_k|\!\rangle) \\ &= \mathsf{head}_{\sum}((\!|N\langle x_1, \cdots, x_k/x\rangle|\!)^\bullet\langle\!|B_i(1)/x_1|\!\rangle\cdots\langle\!|B_i(k)/x_k|\!\rangle) \\ &= \mathsf{head}_{\sum}((\!|N\langle x_1, \cdots, x_k/x\rangle|\!)^\bullet)\end{aligned}$$

and $\mathsf{head}(N\langle\!\langle B/x\rangle\!\rangle) = \mathsf{head}(N)$, by the IH we have

$$\mathsf{head}(N) = \checkmark \iff \mathsf{head}_{\sum}((\!|N|\!)^\bullet) = \checkmark$$

□

Theorem 5.14 (Success Sensitivity)**.** *Let $\mathbb{M}$ be a well-formed $\lambda^{\natural}_{\oplus}$-expression. Then,*

$$\mathbb{M} \Downarrow_{\checkmark} \iff (\!|\mathbb{M}|\!)^{\circ} \Downarrow_{\checkmark} .$$

Proof. By induction on the structure of expressions $\lambda^{\natural}_{\oplus}$ and $\widehat{\lambda}^{\natural}_{\oplus}$. We proceed with the proof in two parts.

(1) Suppose that $\mathbb{M} \Downarrow_{\checkmark}$. We will prove that $(\!|\mathbb{M}|\!)^{\circ} \Downarrow_{\checkmark}$.
By operational completeness (Theorem 5.8) we have that if $\mathbb{M} \longrightarrow_{[\mathtt{R}]} \mathbb{M}'$ then
(1) If $[\mathtt{R}] = [\mathtt{R} : \mathtt{Beta}]$ then $(\!|\mathbb{M}|\!)^{\circ} \longrightarrow^{\leq 2} (\!|\mathbb{M}'|\!)^{\circ}$;
(2) If $[\mathtt{R}] = [\mathtt{R} : \mathtt{Fetch}]$ then $(\!|\mathbb{M}|\!)^{\circ} \longrightarrow^{+} (\!|\mathbb{M}''|\!)^{\circ}$, for some $\mathbb{M}''$ such that $\mathbb{M}' \equiv_{\lambda} \mathbb{M}''$.
(3) If $[\mathtt{R}] \neq [\mathtt{R} : \mathtt{Beta}]$ and $[\mathtt{R}] \neq [\mathtt{R} : \mathtt{Fetch}]$ then $(\!|\mathbb{M}|\!)^{\circ} \longrightarrow (\!|\mathbb{M}'|\!)^{\circ}$;
Notice that neither our reduction rules (in Figure 5), or our congruence $\equiv_{\lambda}$ (in Figure 18), or our encoding ($(\!|\checkmark|\!)^{\circ} = \checkmark$) create or destroy a $\checkmark$ occurring in the head of term. By Proposition 5.13 the encoding preserves the head of a term being $\checkmark$. The encoding acts homomorphically over sums, therefore, if a $\checkmark$ appears as the head of a term in a sum, it will stay in the encoded sum. We can iterate the operational completeness lemma and obtain the result.

(2) Suppose that $(\!|\mathbb{M}|\!)^{\circ} \Downarrow_{\checkmark}$. We will prove that $\mathbb{M} \Downarrow_{\checkmark}$.
From Def. 5.11 we have that $(\!|\mathbb{M}|\!)^{\circ} \Downarrow_{\checkmark} \implies \exists M_1, \cdots, M_k.\ \mathbb{M} \longrightarrow^{*} M_1 + \cdots + M_k$ and $\mathsf{head}(M_j) = \checkmark$, for some $j \in \{1, \ldots, k\}$.
Notice that if $(\!|\mathbb{M}|\!)^{\circ}$ is itself a term headed with $\checkmark$, say $\mathsf{head}((\!|\mathbb{M}|\!)^{\circ}) = \checkmark$, then $\mathbb{M}$ is itself headed with $\checkmark$, from Proposition 5.13.
Based on the shape of $(\!|\mathbb{M}|\!)^{\circ}$, we consider two cases. The first case, when $(\!|\mathbb{M}|\!)^{\circ} = M_1 + \ldots + M_k$, $k \geq 2$, and $\checkmark$ occurs in the head of an M_j, follows a similar reasoning. Then $\mathbb{M}$ has one of the forms:
(1) $\mathbb{M} = N_1$, then N_1 must contain the subterm $M\langle\!\langle {}^{B}/_{x} \rangle\!\rangle$ and $\mathsf{size}(B) = \#(x, M)$. Since,
$(\!|M\langle\!\langle {}^{B}/_{x} \rangle\!\rangle|\!)^{\circ} = \sum_{B_i \in \mathsf{PER}((\!|B|\!)^{\bullet})} (\!|M\langle {}^{\widetilde{x}}/_{x} \rangle|\!)^{\bullet} \langle\!| B_i(1)/x_i |\!\rangle \ldots \langle\!| B_i(k)/x_i |\!\rangle$, we can apply Proposition 5.13 as we may apply $\mathsf{head}_{\sum}((\!|M\langle\!\langle {}^{B}/_{x} \rangle\!\rangle|\!)^{\circ})$.
(2) $\mathbb{M} = N_1 + \ldots + N_l$ for $l \geq 2$.
The reasoning is similar and uses the fact that the encoding distributes homomorphically over sums.
The second case is when $(\!|\mathbb{M}|\!)^{\circ} \longrightarrow^{*} M_1 + \ldots + M_k$, and $\mathsf{head}(M_j) = \checkmark$, for some j and M_j. By operational soundness (Theorem 5.9) we have that if $(\!|\mathbb{M}|\!)^{\circ} \longrightarrow \mathbb{L}$ then there exist $\mathbb{M}'$ such that $\mathbb{M} \longrightarrow_{[\mathtt{R}]} \mathbb{M}'$ and
(1) If $[\mathtt{R}] = [\mathtt{R} : \mathtt{Beta}]$ then $\mathbb{L} \longrightarrow^{\leq 1} (\!|\mathbb{M}'|\!)^{\circ}$;
(2) If $[\mathtt{R}] \neq [\mathtt{R} : \mathtt{Beta}]$ then $\mathbb{L} \longrightarrow^{*} (\!|\mathbb{M}''|\!)^{\circ}$, for $\mathbb{M}''$ such that $\mathbb{M}' \equiv_{\lambda} \mathbb{M}''$.
The reasoning is similar to the previous case, since our reduction rules do not introduce/eliminate $\checkmark$ occurring in the head of terms and by taking $\mathbb{L}$ to be $M_1 + \ldots + M_k$ with $\mathsf{head}(M_j) = \checkmark$, for some j and M_j the result follows. □

Appendix D. Appendix to § 5.3

D.1. **Type Preservation.**

Proposition 5.22. *Suppose σ^j and σ^k are arbitrary strict types (Def. 2.15), for some $j, k \geq 0$. Following Fig. 17, consider their encoding into session types $[\![\sigma^j]\!]^{\lightning}_{(\tau_1,m)}$ and $[\![\sigma^k]\!]^{\lightning}_{(\tau_2,n)}$, respectively, where τ_1, τ_2 are strict types and $n, m \geq 0$.*
We have $[\![\sigma^j]\!]^{\lightning}_{(\tau_1,m)} = [\![\sigma^k]\!]^{\lightning}_{(\tau_2,n)}$ under the following conditions:

(1) *If $j > k$ then we take τ_1 to be an arbitrary strict type and $m = 0$; also, we take τ_2 to be σ and $n = j - k$.*
(2) *If $j < k$ then we take τ_1 to be σ and $m = k - j$; also, we take τ_2 to be an arbitrary strict type and $n = 0$.*
(3) *Otherwise, if $j = k$ then we take $m = n = 0$. Also, τ_1, τ_2 are arbitrary strict types.*

Proof. We shall prove the case of (1) and the case of (2) follows immediately. The case of (3) is immediate by the encoding on types defined in Definition 5.21. Hence we take $j > k$, τ_1 to be an arbitrary type and $m = 0$; also, we take τ_2 to be σ and $n = j - k$. Hence we want to show that $[\![\sigma^j]\!]^{\lightning}_{(\tau_1,0)} = [\![\sigma^k]\!]^{\lightning}_{(\sigma,n)}$. We have the following

$$
\begin{aligned}
[\![\sigma^k]\!]^{\lightning}_{(\sigma,n)} &= \oplus((\&\mathbf{1}) \parr (\oplus\&((\oplus[\![\sigma]\!]^{\lightning}) \otimes ([\![\sigma^{k-1}]\!]^{\lightning}_{(\sigma,n)}))))\\
[\![\sigma^{k-1}]\!]^{\lightning}_{(\sigma,n)} &= \oplus((\&\mathbf{1}) \parr (\oplus\&((\oplus[\![\sigma]\!]^{\lightning}) \otimes ([\![\sigma^{k-2}]\!]^{\lightning}_{(\sigma,n)}))))\\
&\vdots\\
[\![\sigma^{1}]\!]^{\lightning}_{(\sigma,n)} &= \oplus((\&\mathbf{1}) \parr (\oplus\&((\oplus[\![\sigma]\!]^{\lightning}) \otimes ([\![\omega]\!]^{\lightning}_{(\sigma,n)}))))
\end{aligned}
$$

and

$$
\begin{aligned}
[\![\sigma^j]\!]^{\lightning}_{(\tau_1,0)} &= \oplus((\&\mathbf{1}) \parr (\oplus\&((\oplus[\![\sigma]\!]^{\lightning}) \otimes ([\![\sigma^{j-1}]\!]^{\lightning}_{(\tau_1,0)}))))\\
[\![\sigma^{j-1}]\!]^{\lightning}_{(\tau_1,0)} &= \oplus((\&\mathbf{1}) \parr (\oplus\&((\oplus[\![\sigma]\!]^{\lightning}) \otimes ([\![\sigma^{j-2}]\!]^{\lightning}_{(\tau_1,0)}))))\\
&\vdots\\
[\![\sigma^{j-k+1}]\!]^{\lightning}_{(\tau_1,0)} &= \oplus((\&\mathbf{1}) \parr (\oplus\&((\oplus[\![\sigma]\!]^{\lightning}) \otimes ([\![\sigma^{j-k}]\!]^{\lightning}_{(\tau_1,0)}))))
\end{aligned}
$$

Notice that $n = j - k$, hence we wish to show that $[\![\sigma^n]\!]^{\lightning}_{(\tau_1,0)} = [\![\omega]\!]^{\lightning}_{(\sigma,n)}$. Finally we have that:

$$
\begin{aligned}
[\![\omega]\!]^{\lightning}_{(\sigma,n)} &= \oplus((\&\mathbf{1}) \parr (\oplus\&((\oplus[\![\sigma]\!]^{\lightning}) \otimes ([\![\omega]\!]^{\lightning}_{(\sigma,n-1)}))))\\
[\![\omega]\!]^{\lightning}_{(\sigma,n-1)} &= \oplus((\&\mathbf{1}) \parr (\oplus\&((\oplus[\![\sigma]\!]^{\lightning}) \otimes ([\![\omega]\!]^{\lightning}_{(\sigma,n-2)}))))\\
&\vdots\\
[\![\omega]\!]^{\lightning}_{(\sigma,1)} &= \oplus((\&\mathbf{1}) \parr (\oplus\&((\oplus[\![\sigma]\!]^{\lightning}) \otimes ([\![\omega]\!]^{\lightning}_{(\sigma,0)}))))\\
[\![\omega]\!]^{\lightning}_{(\sigma,0)} &= \oplus((\&\mathbf{1}) \parr (\oplus\&\mathbf{1}))
\end{aligned}
$$

and

$$\begin{aligned}
[\![\sigma^n]\!]^{\natural}_{(\tau_1,0)} &= \oplus((\&\mathbf{1}) \parr (\oplus\&((\oplus[\![\sigma]\!]^{\natural}) \otimes ([\![\sigma^{n-1}]\!]^{\natural}_{(\tau_1,0)}))))\\
[\![\sigma^{n-1}]\!]^{\natural}_{(\tau_1,0)} &= \oplus((\&\mathbf{1}) \parr (\oplus\&((\oplus[\![\sigma]\!]^{\natural}) \otimes ([\![\sigma^{n-2}]\!]^{\natural}_{(\tau_1,0)}))))\\
&\vdots\\
[\![\sigma^{1}]\!]^{\natural}_{(\tau_1,0)} &= \oplus((\&\mathbf{1}) \parr (\oplus\&((\oplus[\![\sigma]\!]^{\natural}) \otimes ([\![\omega]\!]^{\natural}_{(\tau_1,0)}))))\\
[\![\omega]\!]^{\natural}_{(\tau_1,0)} &= \oplus((\&\mathbf{1}) \parr (\oplus\&\mathbf{1}))
\end{aligned}$$

□

Theorem 5.23 (Type Preservation for $[\![\cdot]\!]^{\natural}_{u}$)**.** *Let B and $\mathbb{M}$ be a bag and an expression in $\widehat{\lambda}^{\natural}_{\oplus}$, respectively.*

(1) *If $\Gamma^{\dagger} \models B : \pi$ then $[\![B]\!]^{\natural}_{u} \vdash [\![\Gamma^{\dagger}]\!]^{\natural}, u : [\![\pi]\!]^{\natural}_{(\sigma,i)}$, for some strict type σ and index $i \geq 0$.*

(2) *If $\Gamma^{\dagger} \models \mathbb{M} : \tau$ then $[\![\mathbb{M}]\!]^{\natural}_{u} \vdash [\![\Gamma^{\dagger}]\!]^{\natural}, u : [\![\tau]\!]^{\natural}$.*

Proof. By mutual induction on the typing derivation of B and $\mathbb{M}$, with an analysis for the last rule applied. Recall that the encoding of types ($[\![-]\!]^{\natural}$) has been given in Definition 5.21.

(1) We consider two cases:

(a) Rule [FS:wf-bag]:

In this case we have the following derivation:

$$[\texttt{FS:wf-bag}]\ \frac{\Gamma^{\dagger} \vdash B : \pi}{\Gamma^{\dagger} \models B : \pi}$$

There are two cases to be analyzed:

i) We may type bags with the [TS:bag] Rule.
This case is similar to that of [FS:bag]

ii) We may type bags with the [TS:1] Rule.
That is,

$$[\texttt{TS:1}]\ \frac{}{\vdash \mathtt{1} : \omega}$$

Our encoding gives us:

$$[\![\mathtt{1}]\!]^{\natural}_{x} = x.\mathtt{some}_{\emptyset}; x(y_n).(y_n.\overline{\mathtt{some}}; y_n.\overline{\mathtt{close}} \mid x.\mathtt{some}_{\emptyset}; x.\overline{\mathtt{none}})$$

and the encoding of ω can be either:

(A) $[\![\omega]\!]^{\natural}_{(\sigma,0)} = \overline{\&((\oplus\bot) \otimes (\& \oplus \bot))}$; or

(B) $[\![\omega]\!]^{\natural}_{(\sigma,i)} = \&((\oplus\bot) \otimes (\& \oplus ((\&\overline{[\![\sigma]\!]^{\natural}}) \parr (\overline{[\![\omega]\!]^{\natural}_{(\sigma,i-1)}}))))$

and one can build the following type derivation (rules from Figure 11):

$$[\mathtt{T}\oplus^{\mathtt{x}}_{\mathtt{w}}]\ \frac{[\mathtt{T}\&_{\mathtt{d}}^{\mathtt{x}}]\ \dfrac{[\mathtt{T}\,|]\ \dfrac{[\mathtt{T}\parr]\ \dfrac{[\mathtt{T}\&_{\mathtt{d}}^{\mathtt{x}}]\ \dfrac{[\mathtt{T1}]\ \dfrac{}{y_n.\overline{\mathtt{close}} \vdash y_n : \mathbf{1}}}{y_n.\overline{\mathtt{some}}; y_n.\overline{\mathtt{close}} \vdash y_n : \&\mathbf{1}} \qquad [\mathtt{T}\oplus^{\mathtt{x}}_{\mathtt{w}}]\ \dfrac{[\mathtt{T}\&^{\mathtt{x}}]\ \dfrac{}{x.\overline{\mathtt{none}} \vdash x : \&A}}{x.\mathtt{some}_{\emptyset}; x.\overline{\mathtt{none}} \vdash x : \oplus\,\&A}}{(y_n.\overline{\mathtt{some}}; y_n.\overline{\mathtt{close}} \mid x.\mathtt{some}_{\emptyset}; x.\overline{\mathtt{none}}) \vdash y_n : \&\mathbf{1}, x : \oplus\,\&A}}{x(y_n).(y_n.\overline{\mathtt{some}}; y_n.\overline{\mathtt{close}} \mid x.\mathtt{some}_{\emptyset}; x.\overline{\mathtt{none}}) \vdash x : (\&\mathbf{1}) \parr (\oplus\&A)}}{x.\mathtt{some}_{\emptyset}; x(y_n).(y_n.\overline{\mathtt{some}}; y_n.\overline{\mathtt{close}} \mid x.\mathtt{some}_{\emptyset}; x.\overline{\mathtt{none}}) \vdash x : \oplus\,((\&\mathbf{1}) \parr (\oplus\&A))}$$

Since A is arbitrary, we can take $A = \mathtt{1}$ for $[\![\omega]\!]^{\natural}_{(\sigma,0)}$ and $A = \overline{((\&\overline{[\![\sigma]\!]^{\natural}}) \parr (\overline{[\![\omega]\!]^{\natural}_{(\sigma,i-1)}}))}$ for $[\![\omega]\!]^{\natural}_{(\sigma,i)}$, in both cases, the result follows.

(b) Rule [FS:bag]:
Then $B = \wr M \wr \cdot A$ and we have the following derivation:

$$[\texttt{FS:bag}]\ \frac{\Gamma^\dagger \models M : \sigma \qquad \Delta^\dagger \models A : \sigma^k}{\Gamma^\dagger, \Delta^\dagger \models \wr M \wr \cdot A : \sigma^{k+1}}$$

To simplify the proof, we will consider $k = 2$ (the case $k > 2$ follows analogously). By IH we have

$$[\![M]\!]^\natural_{x_i} \vdash [\![\Gamma^\dagger]\!]^\natural, x_i : [\![\sigma]\!]^\natural$$
$$[\![A]\!]^\natural_{x} \vdash [\![\Delta^\dagger]\!]^\natural, x : [\![\sigma \wedge \sigma]\!]^\natural_{(\tau,j)}$$

By Definition 5.17,

$$\begin{aligned}[\![\wr M \wr \cdot A]\!]^\natural_x = & x.\texttt{some}_{\mathsf{fv}(\wr M \wr \cdot A)}; x(y_i).x.\texttt{some}_{y_i,\mathsf{fv}(\wr M \wr \cdot A)}; x.\overline{\texttt{some}}; \overline{x}(x_i).\\ & (x_i.\texttt{some}_{\mathsf{fv}(M)}; [\![M]\!]^\natural_{x_i} \mid [\![A]\!]^\natural_x \mid y_i.\overline{\texttt{none}})\end{aligned} \tag{D.1}$$

Let Π_1 be the derivation:

$$[\mathtt{T}\oplus^{\mathtt{x}}_{\mathtt{w}}]\ [\mathtt{T}\ |]\ \frac{\dfrac{[\![M]\!]^\natural_{x_i} \vdash [\![\Gamma^\dagger]\!]^\natural, x_i : [\![\sigma]\!]^\natural}{x_i.\texttt{some}_{\mathsf{fv}(M)}; [\![M]\!]^\natural_{x_i} \vdash [\![\Gamma^\dagger]\!]^\natural, x_i : \oplus[\![\sigma]\!]^\natural} \qquad [\mathtt{T}\&^{\mathtt{x}}]\ \dfrac{}{y_i.\overline{\texttt{none}} \vdash y_i : \&\mathbf{1}}}{\underbrace{x_i.\texttt{some}_{\mathsf{fv}(M)}; [\![M]\!]^\natural_{x_i} \mid y_i.\overline{\texttt{none}}}_{P_1} \vdash [\![\Gamma^\dagger]\!]^\natural, x_i : \oplus[\![\sigma]\!]^\natural, y_i : \&\mathbf{1}}$$

Let $P_1 = (x_i.\texttt{some}_{\mathsf{fv}(M)}; [\![M]\!]^\natural_{x_i} \mid y_i.\overline{\texttt{none}})$ in the the derivation Π_2 below:

$$[\mathtt{T}\&^{\mathtt{x}}_{\mathtt{d}}]\ \frac{[\mathtt{T}\otimes]\ \dfrac{\Pi_1 \qquad [\![A]\!]^\natural_x \vdash [\![\Delta^\dagger]\!]^\natural, x : [\![\sigma \wedge \sigma]\!]^\natural_{(\tau,j)}}{\overline{x}(x_i).(P_1 \mid [\![A]\!]^\natural_x) \vdash [\![\Gamma^\dagger]\!]^\natural, [\![\Delta^\dagger]\!]^\natural, y_i : \&\mathbf{1}, x : (\oplus[\![\sigma]\!]^\natural) \otimes ([\![\sigma \wedge \sigma]\!]^\natural_{(\tau,j)})}}{\underbrace{x.\overline{\texttt{some}}; \overline{x}(x_i).(P_1 \mid [\![A]\!]^\natural_x)}_{P_2} \vdash [\![\Gamma^\dagger]\!]^\natural, [\![\Delta^\dagger]\!]^\natural, y_i : \&\mathbf{1}, x : \&((\oplus[\![\sigma]\!]^\natural) \otimes ([\![\sigma \wedge \sigma]\!]^\natural_{(\tau,j)}))}$$

Let $P_2 = (x.\overline{\texttt{some}}; \overline{x}(x_i).(P_1 \mid [\![A]\!]^\natural_x))$ in the derivation below (the last two rules that were applied are $[\mathtt{T}\oplus^{\mathtt{x}}_{\mathtt{w}}]$ and $[\mathtt{T}\parr]$):

$$\cfrac{\cfrac{\cfrac{\cfrac{\Pi_2}{\vdots}}{P_2 \vdash [\![\Gamma^\dagger]\!]^\natural, [\![\Delta^\dagger]\!]^\natural, y_i : \&\mathbf{1}, x : \&((\oplus[\![\sigma]\!]^\natural) \otimes ([\![\sigma \wedge \sigma]\!]^\natural_{(\tau,j)}))}\,[\mathtt{T}\oplus^{\mathtt{x}}_{\mathtt{w}}]}{x.\texttt{some}_{y_i,\mathsf{fv}(\wr M \wr \cdot A)}; P_2 \vdash [\![\Gamma^\dagger]\!]^\natural, [\![\Delta^\dagger]\!]^\natural, y_i : \&\mathbf{1}, x : \oplus\&((\oplus[\![\sigma]\!]^\natural) \otimes ([\![\sigma \wedge \sigma]\!]^\natural_{(\tau,j)}))}}{x(y_i).x.\texttt{some}_{y_i,\mathsf{fv}(\wr M \wr \cdot A)}; P_2 \vdash [\![\Gamma^\dagger]\!]^\natural, [\![\Delta^\dagger]\!]^\natural, x : (\&\mathbf{1}) \parr (\oplus\&((\oplus[\![\sigma]\!]^\natural) \otimes ([\![\sigma \wedge \sigma]\!]^\natural_{(\tau,j)})))}$$
$$\underbrace{x.\texttt{some}_{\mathsf{fv}(\wr M \wr \cdot A)}; x(y_i).x.\texttt{some}_{y_i,\mathsf{fv}(\wr M \wr \cdot A)}; P_2}_{[\![\wr M \wr \cdot A]\!]^\natural_x} \vdash [\![\Gamma^\dagger]\!]^\natural, [\![\Delta^\dagger]\!]^\natural, x : \oplus((\&\mathbf{1}) \parr (\oplus\&((\oplus[\![\sigma]\!]^\natural) \otimes ([\![\sigma \wedge \sigma]\!]^\natural_{(\tau,j)}))))$$

From Definitions 4.5 (duality) and 5.21, we infer:

$$\oplus((\&\mathbf{1}) \parr (\oplus\&((\oplus[\![\sigma]\!]^\natural) \otimes ([\![\sigma \wedge \sigma]\!]^\natural_{(\tau,j)})))) = [\![\sigma \wedge \sigma \wedge \sigma]\!]^\natural_{(\tau,j)}$$

Therefore, $[\![\wr M \wr \cdot A]\!]^\natural_x \vdash [\![\Gamma^\dagger, \Delta^\dagger]\!]^\natural, x : [\![\sigma \wedge \sigma \wedge \sigma]\!]^\natural_{(\tau,j)}$ and the result follows.

(2) The proof of type preservation for expressions, relies on the analysis of nine cases:

(a) Rule [FS:wf-expr]:
Then we have the following derivation:

$$[\texttt{FS:wf-expr}]\ \frac{\Gamma^\dagger \vdash \mathbb{M} : \tau}{\Gamma^\dagger \models \mathbb{M} : \tau}$$

Cases follow from their corresponding case from [FS:-]. In the case of [TS:var] we have:

$$[\texttt{TS:var}]\ \frac{}{x : \tau \vdash x : \tau}$$

By Definition 5.21, $[\![x : \tau]\!]^{\not z} = x : \&\overline{[\![\tau]\!]^{\not z}}$, and by Figure 16, $[\![x]\!]^{\not z}_u = x.\overline{\texttt{some}}; [x \leftrightarrow u]$. The thesis holds thanks to the following derivation:

$$\frac{[(\texttt{Tid})]\ \dfrac{}{[x \leftrightarrow u] \vdash x : \overline{[\![\tau]\!]^{\not z}}, u : [\![\tau]\!]^{\not z}}}{[\texttt{T}\&^{\texttt{x}}_{\texttt{d}})]\ \dfrac{}{x.\overline{\texttt{some}}; [x \leftrightarrow u] \vdash x : \&\overline{[\![\tau]\!]^{\not z}}, u : [\![\tau]\!]^{\not z}}}$$

(b) Rule [FS:abs-sh]:
Then $\mathbb{M} = \lambda x.(M[\widetilde{x} \leftarrow x])$, and the derivation is:

$$\frac{[\texttt{FS:share}]\ \dfrac{\Delta^\dagger, x_1 : \sigma, \cdots, x_k : \sigma \models M : \tau}{\Delta^\dagger, x : \sigma \wedge \cdots \wedge \sigma \models M[x_1, \cdots, x_k \leftarrow x] : \tau \quad x \notin \Delta^\dagger}}{[\texttt{FS:abs-sh}]\ \Delta^\dagger \models \lambda x.(M[\widetilde{x} \leftarrow x]) : \sigma^k \to \tau}$$

To simplify the proof we will consider $k = 2$ ($k > 2$ follows similarly).
By the IH, we have

$$[\![M]\!]^{\not z}_u \vdash [\![\Delta^\dagger, x_1 : \sigma, x_2 : \sigma]\!]^{\not z}, u : [\![\tau]\!]^{\not z}.$$

From Def. 5.17 and Def. 5.21, it follows that

$$[\![\Delta^\dagger, x_1 : \sigma, x_2 : \sigma]\!]^{\not z} = [\![\Delta^\dagger]\!]^{\not z}, x_1 : \&\overline{[\![\sigma]\!]^{\not z}}, x_2 : \&\overline{[\![\sigma]\!]^{\not z}}$$

$$\begin{aligned}
[\![\lambda x.M[x_1, x_2 \leftarrow x]]\!]^{\not z}_u &= u.\overline{\texttt{some}}; u(x).[\![M[x_1, x_2 \leftarrow x]]\!]^{\not z}_u \\
&= u.\overline{\texttt{some}}; u(x).x.\overline{\texttt{some}}.\overline{x}(y_1).(y_1.\texttt{some}_\emptyset; y_1.\texttt{close}; \mathbf{0} \\
&\quad \mid x.\overline{\texttt{some}}; x.\texttt{some}_{u,(\mathsf{fv}(M)\setminus x_1,x_2)}; x(x_1).x.\overline{\texttt{some}}. \\
&\quad \overline{x}(y_2).(y_2.\texttt{some}_\emptyset; y_2.\texttt{close}; \mathbf{0} \mid x.\overline{\texttt{some}}; x.\texttt{some}_{u,(\mathsf{fv}(M)\setminus x_2)}; \\
&\quad x(x_2).x.\overline{\texttt{some}}; \overline{x}(y_3).(y_3.\texttt{some}_{u,\mathsf{fv}(M)}; y_3.\texttt{close}; [\![M]\!]^{\not z}_u \\
&\quad \mid x.\overline{\texttt{none}})))
\end{aligned}$$

We shall split the expression into three parts:

$$\begin{aligned}
N_1 &= x.\overline{\texttt{some}}; \overline{x}(y_3).(y_3.\texttt{some}_{u,\mathsf{fv}(M)}; y_3.\texttt{close}; [\![M]\!]^{\not z}_u \mid x.\overline{\texttt{none}}) \\
N_2 &= x.\overline{\texttt{some}}.\overline{x}(y_2).(y_2.\texttt{some}_\emptyset; y_2.\texttt{close}; \mathbf{0} \mid x.\overline{\texttt{some}}; x.\texttt{some}_{u,(\mathsf{fv}(M)\setminus x_2)}; \\
&\qquad x(x_2).N_1) \\
N_3 &= u.\overline{\texttt{some}}; u(x).x.\overline{\texttt{some}}.\overline{x}(y_1).(y_1.\texttt{some}_\emptyset; y_1.\texttt{close}; \mathbf{0} \mid x.\overline{\texttt{some}}; \\
&\qquad x.\texttt{some}_{u,(\mathsf{fv}(M)\setminus x_1,x_2)}; x(x_1).N_2)
\end{aligned}$$

and we obtain the derivation for term N_1 as follows:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\mathtt{T}\bot]\ \dfrac{[\![M]\!]^{\natural}_{u} \vdash [\![\Delta^{\dagger}, x_1 : \sigma, x_2 : \sigma]\!]^{\natural}, u : [\![\tau]\!]^{\natural}}{y_3.\mathtt{close}; [\![M]\!]^{\natural}_{u} \vdash [\![\Delta^{\dagger}, x_1 : \sigma, x_2 : \sigma]\!]^{\natural}, u : [\![f\tau]\!]^{\natural}, y_3 : \bot}}{[\mathtt{T}\oplus^{\mathtt{x}}_{\mathtt{w}}]\ \dfrac{}{y_3.\mathtt{some}_{u,\mathsf{fv}(M)}; y_3.\mathtt{close}; [\![M]\!]^{\natural}_{u} \vdash [\![\Delta^{\dagger}, x_1 : \sigma, x_2 : \sigma]\!]^{\natural}, u : [\![\tau]\!]^{\natural}, y_3 : \oplus \bot}} \quad [\mathtt{T}\&^{\mathtt{x}}]\ \dfrac{}{x.\overline{\mathtt{none}} \vdash x : \&A}}{[\mathtt{T}\otimes]\ \dfrac{}{\overline{x}(y_3).(y_3.\mathtt{some}_{u,\mathsf{fv}(M)}; y_3.\mathtt{close}; [\![M]\!]^{\natural}_{u} \mid x.\overline{\mathtt{none}}) \vdash [\![\Delta^{\dagger}, x_1 : \sigma, x_2 : \sigma]\!]^{\natural}, u : [\![\tau]\!]^{\natural}, x : (\oplus\bot) \otimes (\&A)}}}{[\mathtt{T}\&^{\mathtt{x}}_{\mathtt{d}}]\ \dfrac{}{\underbrace{x.\overline{\mathtt{some}}; \overline{x}(y_3).(y_3.\mathtt{some}_{u,\mathsf{fv}(M)}; y_3.\mathtt{close}; [\![M]\!]^{\natural}_{u} \mid x.\overline{\mathtt{none}})}_{N_1} \vdash [\![\Delta^{\dagger}, x_1 : \sigma, x_2 : \sigma]\!]^{\natural}, u : [\![\tau]\!]^{\natural}, x : \overline{[\![\omega]\!]^{\natural}_{(\sigma,i)}}}}$$

Notice that the last rule applied $[\mathtt{T}\&^{\mathtt{x}}_{\mathtt{d}}]$ assigns $x : \&((\oplus\bot) \otimes (\&A))$. Again, since A is arbitrary, take $A = \oplus((\&\overline{[\![\sigma]\!]^{\natural}}) \parr (\overline{[\![\omega]\!]^{\natural}_{(\sigma,i-1)}}))$, obtaining $x : \overline{[\![\omega]\!]^{\natural}_{(\sigma,i)}}$. In order to obtain a type derivation for N_2, consider the derivation Π_1:

$$\dfrac{\dfrac{\dfrac{[\mathtt{T}\parr]\ \dfrac{N_1 \vdash [\![\Delta^{\dagger}]\!]^{\natural}, x_1 : \&\overline{[\![\sigma]\!]^{\natural}}, x_2 : \&\overline{[\![\sigma]\!]^{\natural}}, u : [\![\tau]\!]^{\natural}, x : \overline{[\![\omega]\!]^{\natural}_{(\sigma,i)}}}{x(x_2).N_1 \vdash [\![\Delta^{\dagger}]\!]^{\natural}, x_1 : \&\overline{[\![\sigma]\!]^{\natural}}, u : [\![\tau]\!]^{\natural}, x : (\&\overline{[\![\sigma]\!]^{\natural}}) \parr (\overline{[\![\omega]\!]^{\natural}_{(\sigma,i)}})}}{[\mathtt{T}\oplus^{\mathtt{x}}_{\mathtt{w}}]\ \dfrac{}{x.\mathtt{some}_{u,(\mathsf{fv}(M)\setminus x_2)}; x(x_2).N_1 \vdash [\![\Delta^{\dagger}]\!]^{\natural}, x_1 : \&\overline{[\![\sigma]\!]^{\natural}}, u : [\![\tau]\!]^{\natural}, x : \oplus((\&\overline{[\![\sigma]\!]^{\natural}}) \parr (\overline{[\![\omega]\!]^{\natural}_{(\sigma,i)}}))}}}{[\mathtt{T}\&^{\mathtt{x}}_{\mathtt{d}}]\ \dfrac{}{x.\overline{\mathtt{some}}; x.\mathtt{some}_{u,(\mathsf{fv}(M)\setminus x_2)}; x(x_2).N_1 \vdash [\![\Delta^{\dagger}]\!]^{\natural}, x_1 : \&\overline{[\![\sigma]\!]^{\natural}}, u : [\![\tau]\!]^{\natural}, x : \& \oplus ((\&\overline{[\![\sigma]\!]^{\natural}}) \parr (\overline{[\![\omega]\!]^{\natural}_{(\sigma,i)}}))}}$$

We take $P_1 = x.\overline{\mathtt{some}}; x.\mathtt{some}_{u,(\mathsf{fv}(M)\setminus x_2)}; x(x_2).N_1$ and $\Gamma^{\dagger}_1 = [\![\Delta^{\dagger}]\!]^{\natural}, x_1 : \&\overline{[\![\sigma]\!]^{\natural}}, u : [\![\tau]\!]^{\natural}$ and continue the derivation of N_2

$$\dfrac{\dfrac{[\mathtt{T}\bot]\ \dfrac{[\mathtt{T}\cdot]\ \dfrac{}{\mathbf{0} \vdash}}{y_2.\mathtt{close}; \mathbf{0} \vdash y_2 : \bot}}{[\mathtt{T}\oplus^{\mathtt{x}}_{\mathtt{w}}]\ \dfrac{}{y_2.\mathtt{some}_{\emptyset}; y_2.\mathtt{close}; \mathbf{0} \vdash y_2 : \oplus \bot}} \quad \begin{array}{c}\Pi_1\\ \vdots \\ P_1 \vdash \Gamma^{\dagger}_1, x : \& \oplus ((\&\overline{[\![\sigma]\!]^{\natural}}) \parr (\overline{[\![\omega]\!]^{\natural}_{(\sigma,i)}}))\end{array}}{[\mathtt{T}\otimes]\ \dfrac{}{\overline{x}(y_2).(y_2.\mathtt{some}_{\emptyset}; y_2.\mathtt{close}; \mathbf{0} \mid P_1) \vdash \Gamma^{\dagger}_1, x : (\oplus\bot) \otimes (\& \oplus ((\&\overline{[\![\sigma]\!]^{\natural}}) \parr (\overline{[\![\omega]\!]^{\natural}_{(\sigma,i)}})))}}{[\mathtt{T}\&^{\mathtt{x}}_{\mathtt{d}}]\ \dfrac{}{\underbrace{x.\overline{\mathtt{some}}.\overline{x}(y_2).(y_2.\mathtt{some}_{\emptyset}; y_2.\mathtt{close}; \mathbf{0} \mid P_1)}_{N_2} \vdash \Gamma^{\dagger}_1, x : \overline{[\![\sigma \wedge \omega]\!]^{\natural}_{(\sigma,i)}}}}$$

Finally, we type N_3 by first having the derivation Π_2:

$$\dfrac{\dfrac{\dfrac{[\mathtt{T}\parr]\ \dfrac{N_2 \vdash [\![\Delta^{\dagger}]\!]^{\natural}, x_1 : \&\overline{[\![\sigma]\!]^{\natural}}, u : [\![\tau]\!]^{\natural}, x : \overline{[\![\sigma \wedge \omega]\!]^{\natural}_{(\sigma,i)}}}{x(x_1).N_2 \vdash [\![\Delta^{\dagger}]\!]^{\natural}, u : [\![\tau]\!]^{\natural}, x : (\&\overline{[\![\sigma]\!]^{\natural}}) \parr \overline{[\![\sigma \wedge \omega]\!]^{\natural}_{(\sigma,i)}}}}{[\mathtt{T}\oplus^{\mathtt{x}}_{\mathtt{w}}]\ \dfrac{}{x.\mathtt{some}_{u,(\mathsf{fv}(M)\setminus x_1,x_2)}; x(x_1).N_2 \vdash [\![\Delta^{\dagger}]\!]^{\natural}, u : [\![\tau]\!]^{\natural}, x : \oplus((\&\overline{[\![\sigma]\!]^{\natural}}) \parr \overline{[\![\sigma \wedge \omega]\!]^{\natural}_{(\sigma,i)}})}}}{[\mathtt{T}\&^{\mathtt{x}}_{\mathtt{d}}]\ \dfrac{}{P_2 \vdash [\![\Delta^{\dagger}]\!]^{\natural}, u : [\![\tau]\!]^{\natural}, x : \& \oplus ((\&\overline{[\![\sigma]\!]^{\natural}}) \parr \overline{[\![\sigma \wedge \omega]\!]^{\natural}_{(\sigma,i)}})}}$$

We let $P_2 = x.\overline{\mathtt{some}}; x.\mathtt{some}_{u,(\mathsf{fv}(M)\setminus x_1,x_2)}; x(x_1).N_2$ and $\Gamma^{\dagger}_2 = [\![\Delta^{\dagger}]\!]^{\natural}, u : [\![\tau]\!]^{\natural}$. We continue the derivation of $N_3 = u.\overline{\mathtt{some}}; u(x).x.\overline{\mathtt{some}}.\overline{x}(y_1).(y_1.\mathtt{some}_{\emptyset}; y_1.\mathtt{close}; \mathbf{0} \mid P_2)$:

$$[\mathtt{T}\otimes]\ \dfrac{[\mathtt{T}\oplus^{\mathtt{x}}_{\mathtt{w}}]\ \dfrac{[\mathtt{T}\bot]\ \dfrac{[\mathtt{T}\cdot]\ \dfrac{}{\mathbf{0}\vdash}}{y_1.\mathtt{close};\mathbf{0}\vdash y_1:\bot}}{y_1.\mathtt{some}_\emptyset;y_1.\mathtt{close};\mathbf{0}\vdash y_1:\oplus\bot}\qquad \Pi_2}{\overline{x}(y_1).(y_1.\mathtt{some}_\emptyset;y_1.\mathtt{close};\mathbf{0}\mid P_2)\vdash \Gamma_2^\dagger, x:(\oplus\bot)\otimes(\&\oplus((\&\overline{[\![\sigma]\!]^\natural})\parr\overline{[\![\sigma\wedge\omega]\!]^\natural_{(\sigma,i)}}))}$$

$$[\mathtt{T}\&^{\mathtt{x}}_{\mathtt{d}}]\ \dfrac{x.\overline{\mathtt{some}}.\overline{x}(y_1).(y_1.\mathtt{some}_\emptyset;y_1.\mathtt{close};\mathbf{0}\mid P_2)\vdash [\![\Delta^\dagger]\!]^\natural, u:[\![\tau]\!]^\natural, x:\overline{[\![\sigma\wedge\sigma]\!]^\natural_{(\sigma,i)}}}{[\mathtt{T}\parr]\ \dfrac{u(x).x.\overline{\mathtt{some}}.\overline{x}(y_1).(y_1.\mathtt{some}_\emptyset;y_1.\mathtt{close};\mathbf{0}\mid P_2)\vdash [\![\Delta^\dagger]\!]^\natural, u:(\overline{[\![\sigma\wedge\sigma]\!]^\natural_{(\sigma,i)}})\parr([\![\tau]\!]^\natural)}{[\mathtt{T}\&^{\mathtt{x}}_{\mathtt{d}}]\ \dfrac{}{N_3\vdash [\![\Delta^\dagger]\!]^\natural, u:\&((\overline{[\![\sigma\wedge\sigma]\!]^\natural_{(\sigma,i)}})\parr([\![\tau]\!]^\natural))}}}$$

Since $[\![\sigma\wedge\sigma\to\tau]\!]^\natural = \&(\overline{[\![\sigma\wedge\sigma]\!]^\natural_{(\sigma,i)}}\parr[\![\tau]\!]^\natural)$, we have proven that $[\![\lambda x.M[\widetilde{x}\leftarrow x]]\!]^\natural_u \vdash [\![\Delta^\dagger]\!]^\natural, u:[\![\sigma\wedge\sigma\to\tau]\!]^\natural$ and the result follows.

(c) Rule [FS:app]:
Then $\mathbb{M} = M\ B$, and the derivation is

$$[\mathtt{FS{:}app}]\ \frac{\Gamma^\dagger\models M:\sigma^j\to\tau \qquad \Delta^\dagger\models B:\sigma^k}{\Gamma^\dagger,\Delta^\dagger\models M\ B:\tau}$$

By IH, we have both
- $[\![M]\!]^\natural_u \vdash [\![\Gamma^\dagger]\!]^\natural, u:[\![\sigma^j\to\tau]\!]^\natural$;
- and $[\![B]\!]^\natural_u \vdash [\![\Delta^\dagger]\!]^\natural, u:\overline{[\![\sigma^k]\!]^\natural_{(\tau_2,n)}}$, for some τ_2 and some n.

From the fact that $\mathbb{M}$ is well-formed and Def. 5.17 and Def. 5.21, we have:
- $B = \wr N_1,\cdots,N_k\wr$;
- $[\![M\ B]\!]^\natural_u = \bigoplus_{B_i\in\mathsf{PER}(B)} (\nu v)([\![M]\!]^\natural_v \mid v.\mathtt{some}_{u,\mathsf{fv}(B)};\overline{v}(x).([v\leftrightarrow u]\mid [\![B_i]\!]^\natural_x))$;
- $[\![\sigma^j\to\tau]\!]^\natural = \&(\overline{[\![\sigma^j]\!]^\natural_{(\tau_1,m)}}\parr[\![\tau]\!]^\natural)$, for some τ_1 and some m.

Also, since $[\![B]\!]^\natural_u \vdash [\![\Delta^\dagger]\!]^\natural, u:\overline{[\![\sigma^k]\!]^\natural_{(\tau_2,n)}}$, we have the following derivation Π_i:

$$[\mathtt{T}\oplus^{\mathtt{v}}_{\mathtt{w}}]\ \dfrac{[\mathtt{T}\otimes]\ \dfrac{[\![B_i]\!]^\natural_x\vdash [\![\Delta^\dagger]\!]^\natural, x:\overline{[\![\sigma^k]\!]^\natural_{(\tau_2,n)}} \qquad [\mathtt{Tid}]\ \dfrac{}{[v\leftrightarrow u]\vdash v:\overline{[\![\tau]\!]^\natural}, u:[\![\tau]\!]^\natural}}{\overline{v}(x).([v\leftrightarrow u]\mid [\![B_i]\!]^\natural_x)\vdash [\![\Delta^\dagger]\!]^\natural, v:\overline{[\![\sigma^k]\!]^\natural_{(\tau_2,n)}}\otimes\overline{[\![\tau]\!]^\natural}, u:[\![\tau]\!]^\natural}}{v.\mathtt{some}_{u,\mathsf{fv}(B)};\overline{v}(x).([v\leftrightarrow u]\mid [\![B_i]\!]^\natural_x)\vdash [\![\Delta^\dagger]\!]^\natural, v:\oplus(\overline{[\![\sigma^k]\!]^\natural_{(\tau_2,n)}}\otimes\overline{[\![\tau]\!]^\natural}), u:[\![\tau]\!]^\natural}$$

Notice that

$$\oplus(\overline{[\![\sigma^k]\!]^\natural_{(\tau_2,n)}}\otimes\overline{[\![\tau]\!]^\natural}) = \overline{[\![\sigma^k\to\tau]\!]^\natural}$$

Therefore, by one application of [Tcut] we obtain the derivations ∇_i, for each $B_i\in\mathsf{PER}(B)$:

$$[\mathtt{Tcut}]\ \frac{[\![M]\!]^\natural_v\vdash [\![\Gamma^\dagger]\!]^\natural, v:\&(\overline{[\![\sigma^j]\!]^\natural}_{(\tau_1,m)}\parr([\![\tau]\!]^\natural))\qquad \Pi_i}{(\nu v)([\![M]\!]^\natural_v\mid v.\mathtt{some}_{u,\mathsf{fv}(B)};\overline{v}(x).([v\leftrightarrow u]\mid [\![B_i]\!]^\natural_x))\vdash [\![\Gamma^\dagger]\!]^\natural, [\![\Delta^\dagger]\!]^\natural, u:[\![\tau]\!]^\natural}$$

In order to apply [Tcut], we must have that $[\![\sigma^j]\!]^\natural_{(\tau_1,m)} = [\![\sigma^k]\!]^\natural_{(\tau_2,n)}$, therefore, the choice of τ_1,τ_2,n and m, will consider the different possibilities for j and k, as in Proposition 5.22.
We can then conclude that $[\![MB]\!]^\natural_u\vdash [\![\Gamma^\dagger]\!]^\natural, [\![\Delta^\dagger]\!]^\natural, u:[\![\tau]\!]^\natural$:

$$[\texttt{T\&}]\ \frac{\text{For each } B_i \in \mathsf{PER}(B) \qquad \nabla_i}{\bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)(\llbracket M \rrbracket^{\natural}_{v} \mid v.\texttt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([v \leftrightarrow u] \mid \llbracket B_i \rrbracket^{\natural}_{x})) \vdash \llbracket \Gamma^{\dagger} \rrbracket^{\natural}, \llbracket \Delta^{\dagger} \rrbracket^{\natural}, u : \llbracket \tau \rrbracket^{\natural}}$$

and the result follows.

(d) Rule [FS:share]:
Then $\mathbb{M} = M[x_1, \dots x_k \leftarrow x]$ and

$$[\texttt{FS:share}]\ \frac{\Delta^{\dagger}, x_1 : \sigma, \cdots, x_k : \sigma \models M : \tau \quad x \notin \Delta^{\dagger} \quad k \neq 0}{\Delta^{\dagger}, x : \sigma_k \models M[x_1, \cdots, x_k \leftarrow x] : \tau}$$

The proof for this case is contained within 2(b).

(e) Rule [FS:weak]:
Then $\mathbb{M} = M[\leftarrow x]$ and

$$[\texttt{FS:weak}]\ \frac{\Gamma^{\dagger} \models M : \tau}{\Gamma^{\dagger}, x : \omega \models M[\leftarrow x] : \tau}$$

However $\Gamma^{\dagger}, x : \omega$ is not a core context hence we disallow the case.

(f) Rule [FS:ex-sub]:
Then $\mathbb{M} = M[x_1, \cdots, x_k \leftarrow x]\ \langle\!\langle {}^{B}/_{x} \rangle\!\rangle$ and

$$[\texttt{FS:ex-sub}]\ \frac{\Delta^{\dagger} \models B : \sigma^{j} \qquad \Gamma^{\dagger}, x : \sigma^{k} \models M[x_1, \cdots, x_k \leftarrow x] : \tau}{\Gamma^{\dagger}, \Delta^{\dagger} \models M[x_1, \cdots, x_k \leftarrow x]\ \langle\!\langle {}^{B}/_{x} \rangle\!\rangle : \tau}$$

By Proposition 5.22 and IH we have both

$$\llbracket M[x_1, \cdots, x_k \leftarrow x] \rrbracket^{\natural}_{u} \vdash \llbracket \Gamma^{\dagger} \rrbracket^{\natural}, x : \overline{\llbracket \sigma_k \rrbracket^{\natural}_{(\tau,n)}}, u : \llbracket \tau \rrbracket^{\natural}$$

$$\llbracket B \rrbracket^{\natural}_{x} \vdash \llbracket \Delta^{\dagger} \rrbracket^{\natural}, x : \llbracket \sigma_j \rrbracket^{\natural}_{(\tau,m)}$$

From Def. 5.17, we have

$$\llbracket M[\widetilde{x} \leftarrow x]\ \langle\!\langle {}^{B}/_{x} \rangle\!\rangle \rrbracket^{\natural}_{u} = \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x)(\llbracket M[\widetilde{x} \leftarrow x] \rrbracket^{\natural}_{u} \mid \llbracket B_i \rrbracket^{\natural}_{x})$$

Therefore, for each $B_i \in \mathsf{PER}(B)$, we obtain the following derivation Π_i:

$$[\texttt{Tcut}]\ \frac{\llbracket M[\widetilde{x} \leftarrow x] \rrbracket^{\natural}_{u} \vdash \llbracket \Gamma^{\dagger} \rrbracket^{\natural}, x : \overline{\llbracket \sigma_k \rrbracket^{\natural}_{(\tau,n)}}, u : \llbracket \tau \rrbracket^{\natural} \qquad \llbracket B_i \rrbracket^{\natural}_{x} \vdash \llbracket \Delta^{\dagger} \rrbracket^{\natural}, x : \llbracket \sigma_j \rrbracket^{\natural}_{(\tau,m)}}{(\nu x)(\llbracket M[\widetilde{x} \leftarrow x] \rrbracket^{\natural}_{u} \mid \llbracket B_i \rrbracket^{\natural}_{x}) \vdash \llbracket \Gamma^{\dagger} \rrbracket^{\natural}, \llbracket \Delta^{\dagger} \rrbracket^{\natural}, u : \llbracket \tau \rrbracket^{\natural}}$$

We must have that $\llbracket \sigma^{j} \rrbracket^{\natural}_{(\tau,m)} = \llbracket \sigma^{k} \rrbracket^{\natural}_{(\tau,n)}$ which holds by the conditions in Proposition 5.22. Therefore, from Π_i and multiple applications of [T&] it follows that

$$[\texttt{T\&}]\ \frac{\forall \bigoplus_{B_i \in \mathsf{PER}(B)} \qquad \Pi_i}{\bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x)(\llbracket M[\widetilde{x} \leftarrow x] \rrbracket^{\natural}_{u} \mid x.\texttt{some}_{w}; \llbracket B_i \rrbracket^{\natural}_{x}) \vdash \llbracket \Gamma^{\dagger} \rrbracket^{\natural}, \llbracket \Delta^{\dagger} \rrbracket^{\natural}, u : \llbracket \tau \rrbracket^{\natural}}$$

that is, $\llbracket M[x_1, x_2 \leftarrow x] \langle\!\langle {}^{B}/_{x} \rangle\!\rangle \rrbracket^{\natural} \vdash \llbracket \Gamma^{\dagger}, \Delta^{\dagger} \rrbracket^{\natural}, u : \llbracket \tau \rrbracket^{\natural}$ and the result follows.

(g) Rule [FS:ex-lin-sub]:
Then $\mathbb{M} = M \langle\!| N/x |\!\rangle$ and

$$[\texttt{FS:ex-lin-sub}]\ \frac{\Delta^{\dagger} \models N : \sigma \qquad \Gamma^{\dagger}, x : \sigma \models M : \tau}{\Gamma^{\dagger}, \Delta^{\dagger} \models M \langle\!| N/x |\!\rangle : \tau}$$

By IH we have both

$$[\![N]\!]^{\lightning}_{x} \vdash [\![\Delta^{\dagger}]\!]^{\lightning}, x : [\![\sigma]\!]^{\lightning}$$
$$[\![M]\!]^{\lightning}_{x} \vdash [\![\Gamma^{\dagger}]\!]^{\lightning}, x : \&\overline{[\![\sigma]\!]^{\lightning}}, u : [\![\tau]\!]^{\lightning}.$$

From Def. 5.17, $[\![M\langle\!\langle N/x\rangle\!\rangle]\!]^{\lightning}_{u} = (\nu x)([\![M]\!]^{\lightning}_{u} \mid x.\mathtt{some}_{\mathsf{fv}(N)}; [\![N]\!]^{\lightning}_{x})$ and

$$[\mathtt{TCut}]\ \frac{[\![M]\!]^{\lightning}_{u} \vdash [\![\Gamma^{\dagger}]\!]^{\lightning}, u : [\![\tau]\!]^{\lightning}, x : \&\overline{[\![\sigma]\!]^{\lightning}} \qquad [\mathtt{T}\oplus^{\mathtt{x}}]\ \dfrac{[\![N]\!]^{\lightning}_{x} \vdash [\![\Delta^{\dagger}]\!]^{\lightning}, x : [\![\sigma]\!]^{\lightning}}{x.\mathtt{some}_{\mathsf{fv}(N)}; [\![N]\!]^{\lightning}_{x} \vdash [\![\Delta^{\dagger}]\!]^{\lightning}, x : \oplus[\![\sigma]\!]^{\lightning}}}{(\nu x)([\![M]\!]^{\lightning}_{u} \mid x.\mathtt{some}_{\mathsf{fv}(N)}; [\![N]\!]^{\lightning}_{x}) \vdash [\![\Gamma^{\dagger}]\!]^{\lightning}, [\![\Delta^{\dagger}]\!]^{\lightning}, u : [\![\tau]\!]^{\lightning}}$$

Observe that for the application of Rule [TCut] we used the fact that $\oplus\overline{[\![\sigma]\!]^{\lightning}} = \&\overline{[\![\sigma]\!]^{\lightning}}$. Therefore, $[\![M\langle\!\langle N/x\rangle\!\rangle]\!]^{\lightning}_{u} \vdash [\![\Gamma^{\dagger}]\!]^{\lightning}, [\![\Delta^{\dagger}]\!]^{\lightning}, u : [\![\tau]\!]^{\lightning}$ and the result follows.

(h) Rule [FS:fail]:
Then $\mathbb{M} = M\langle\!\langle N/x\rangle\!\rangle$ and

$$[\mathtt{FS{:}fail}]\ \frac{(x_1 : \sigma_1, \cdots, x_n : \sigma_n)^{\dagger} = x_1 : \sigma_1, \cdots, x_n : \sigma_n}{x_1 : \sigma_1, \cdots, x_n : \sigma_n \models \mathtt{fail}^{x_1,\cdots,x_n} : \tau}$$

From Definition 5.17, $[\![\mathtt{fail}^{x_1,\cdots,x_n}]\!]^{\lightning}_{u} = u.\overline{\mathtt{none}} \mid x_1.\overline{\mathtt{none}} \mid \cdots \mid x_k.\overline{\mathtt{none}}$ and

$$[\mathtt{T}\&^{\mathtt{u}}]\ [\mathtt{T}\mid]\ \frac{}{u.\overline{\mathtt{none}} \vdash u : [\![\tau]\!]^{\lightning}} \qquad \frac{[\mathtt{T}\&^{\mathtt{x_1}}]\ \dfrac{}{x_1.\overline{\mathtt{none}} \vdash_1 : \&\overline{[\![\sigma_1]\!]^{\lightning}}} \qquad \cdots \qquad [\mathtt{T}\&^{\mathtt{x_n}}]\ \dfrac{}{x_n.\overline{\mathtt{none}} \vdash x_n : \&\overline{[\![\sigma_n]\!]^{\lightning}}}}{x_1.\overline{\mathtt{none}} \mid \cdots \mid x_k.\overline{\mathtt{none}} \vdash x_1 : \&\overline{[\![\sigma_1]\!]^{\lightning}}, \cdots, x_n : \&\overline{[\![\sigma_n]\!]^{\lightning}}}$$
$$u.\overline{\mathtt{none}} \mid x_1.\overline{\mathtt{none}} \mid \cdots \mid x_k.\overline{\mathtt{none}} \vdash x_1 : \&\overline{[\![\sigma_1]\!]^{\lightning}}, \cdots, x_n : \&\overline{[\![\sigma_n]\!]^{\lightning}}, u : [\![\tau]\!]^{\lightning}$$

Therefore, $[\![\mathtt{fail}^{x_1,\cdots,x_n}]\!]^{\lightning}_{u} \vdash x_1 : \&\overline{[\![\sigma_1]\!]^{\lightning}}, \cdots, x_n : \&\overline{[\![\sigma_n]\!]^{\lightning}}, u : [\![\tau]\!]^{\lightning}$ and the result follows.

(i) Rule [FS:sum]:
This case follows easily by IH. □

D.2. **Completeness and Soundness.**

Theorem 5.26 (Consistency Stability Under ≡)**.** *Let $\mathbb{M}$ be a consistent $\widehat{\lambda}^{\lightning}_{\oplus}$-expression. If $\mathbb{M} \equiv \mathbb{M}'$ then $\mathbb{M}'$ is consistent.*

Proof. By induction on the structure of $\mathbb{M}$. Let us consider first two conditions 1 and 2 as other conditions are analogous. The congruence rules that concern the sharing construct of condition 1 are:

$$\begin{aligned}
M[\leftarrow x]\langle\!\langle \mathbf{1}/x\rangle\!\rangle &\equiv_{\lambda} M \\
MA[\widetilde{x} \leftarrow x]\langle\!\langle B/x\rangle\!\rangle &\equiv_{\lambda} (M[\widetilde{x} \leftarrow x]\langle\!\langle B/x\rangle\!\rangle)A && \text{with } x_i \in \widetilde{x} \Rightarrow x_i \notin \mathsf{fv}(A) \\
M[\widetilde{y} \leftarrow y]\langle\!\langle A/y\rangle\!\rangle[\widetilde{x} \leftarrow x]\langle\!\langle B/x\rangle\!\rangle &\equiv_{\lambda} (M[\widetilde{x} \leftarrow x]\langle\!\langle B/x\rangle\!\rangle)[\widetilde{y} \leftarrow y]\langle\!\langle A/y\rangle\!\rangle && \text{with } x_i \in \widetilde{x} \Rightarrow x_i \notin \mathsf{fv}(A)
\end{aligned}$$

Notice that these rules neither add or remove occurrences of shared variables neither do they allow shared variables to be extruded from their bindings by their side conditions. Also, they do not introduce new sharing on already shared variables. Hence, conditions 1(i) to 1(iv) are preserved by these rules.

Now consider the congruence rules concerning the explicit substitution of condition 2:

$$\begin{array}{rl} MB\langle\!|N/x|\!\rangle \equiv_\lambda (M\langle\!|N/x|\!\rangle)B & \text{with } x \notin \mathsf{fv}(B) \\ M\langle\!|N_2/y|\!\rangle\langle\!|N_1/x|\!\rangle \equiv_\lambda M\langle\!|N_1/x|\!\rangle\langle\!|N_2/y|\!\rangle & \text{with } x \notin \mathsf{fv}(N_2), y \notin \mathsf{fv}(N_1) \end{array}$$

As before, variables are not duplicated or eliminated from terms and by the side conditions of the rules they cannot extrude bound variables. Similarly, the rules do not introduce any sharing or new free variables. Hence conditions 2(i) to 2(iv) are satisfied. □

Proposition 5.29. *Suppose N is a well-formed, partially open $\widehat{\lambda}^{\natural}_{\oplus}$-term with $\mathsf{head}(N) = x$. Then, there exist an index set I, names $\widetilde{y}$ and n, and processes P_i such that the following four conditions hold:*

(1)
$$[\![N]\!]^{\natural}_u \longrightarrow^* \bigoplus_{i\in I} (\nu\widetilde{y})([\![x]\!]^{\natural}_n \mid P_i)$$

(2) *There exists a $\widehat{\lambda}^{\natural}_{\oplus}$-term N' such that $N \equiv_\lambda N'$ and:*
$$[\![N']\!]^{\natural}_u = \bigoplus_{i\in I} (\nu\widetilde{y})([\![x]\!]^{\natural}_n \mid P_i)$$

(3) *For any well-formed and partially open $\widehat{\lambda}^{\natural}_{\oplus}$-term M:*
$$[\![N\{\!|M/x|\!\}]\!]^{\natural}_u \longrightarrow^* \bigoplus_{i\in I} (\nu\widetilde{y})([\![M]\!]^{\natural}_n \mid P_i)$$

(4) *There exists a $\widehat{\lambda}^{\natural}_{\oplus}$-term M' such that $M' \equiv_\lambda N\{\!|M/x|\!\}$ and:*
$$[\![M']\!]^{\natural}_u = \bigoplus_{i\in I} (\nu\widetilde{y})([\![M]\!]^{\natural}_n \mid P_i)$$

Proof. Let us consider each part:

(1) We proceed by induction on the structure of N.

(I) $N = x$.
Then $[\![x]\!]^{\natural}_u$. Hence $I = \emptyset$ and $\widetilde{y} = \emptyset$.

(II) $N = (M\ B)$.
Then $\mathsf{head}(M\ B) = \mathsf{head}(M) = x$ and

$$[\![N]\!]^{\natural}_u = [\![M\ B]\!]^{\natural}_u = \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)([\![M]\!]^{\natural}_v \mid v.\mathtt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([v \leftrightarrow u] \mid [\![B_i]\!]^{\natural}_x))$$

and the result follows by induction on $[\![M]\!]^{\natural}_u$.

(III) $N = M[\widetilde{y} \leftarrow y]$. Not possible due to the assumption of partially open terms.

(IV) $N = (M[\widetilde{y} \leftarrow y])\langle\!\langle B/y \rangle\!\rangle$.
Then $\mathsf{head}((M[\widetilde{y} \leftarrow y])\langle\!\langle B/y \rangle\!\rangle) = \mathsf{head}((M[\widetilde{y} \leftarrow y])) = x$ when $\widetilde{y} = \emptyset$, $B = \mathtt{1}$ and $\mathsf{head}(M) = x$.

$$\begin{aligned} [\![N]\!]^{\natural}_u &= [\![(M[\leftarrow y])\langle\!\langle \mathtt{1}/y \rangle\!\rangle]\!]^{\natural}_u = (\nu y)([\![M[\leftarrow y]]\!]^{\natural}_u \mid [\![\mathtt{1}]\!]^{\natural}_y) \\ &= (\nu y)(y.\overline{\mathtt{some}}.\overline{y}(z).(z.\mathtt{some}_{u,\mathsf{fv}(M)}; z.\mathtt{close}; [\![M]\!]^{\natural}_u \mid y.\overline{\mathtt{none}}) \mid \\ &\qquad y.\mathtt{some}_\emptyset; y(z).(z.\overline{\mathtt{some}}; z.\overline{\mathtt{close}} \mid y.\mathtt{some}_\emptyset; y.\overline{\mathtt{none}})) \\ &\longrightarrow^* [\![M]\!]^{\natural}_u \end{aligned}$$

Then the result follows by induction on $[\![M]\!]^{\natural}_u$.

(V) When $N = M\langle\!\langle N'/y\rangle\!\rangle$, then $\mathsf{head}(M\langle\!\langle N'/y\rangle\!\rangle) = \mathsf{head}(M) = x$ and

$$[\![N]\!]^{\natural}_{u} = [\![M\langle\!\langle N'/y\rangle\!\rangle]\!]^{\natural}_{u} = (\nu y)([\![M]\!]^{\natural}_{u} \mid x.\mathtt{some}_{\mathsf{fv}(N')}; [\![N']\!]^{\natural}_{x})$$

Then true by induction on $[\![M]\!]^{\natural}_{u}$

(2) In this case, notice how reductions are only introduced when N has sub-term $(M[\leftarrow y])\langle\!\langle {}^{1}/_{y}\rangle\!\rangle$ from case 1(IV), however from the congruence of Fig. 18 we may rewrite this sub-term to be M which eliminates the need for reductions. Inductively, performing this application of $\equiv_{\lambda}$ provides the result.

(3) This case is similar to the first, with the clear difference that linear head substitution must also be used. However, we can inductively push the linear head substitution inside the term to reach the head variable. Consider the base case when $N = x$ and we have some well-formed partially open term M. Then $[\![N\{\!|M/x|\!\}]\!]^{\natural}_{u} = [\![x\{\!|M/x|\!\}]\!]^{\natural}_{u} = [\![M]\!]^{\natural}_{u}$. Hence $I = \emptyset$ and $\widetilde{y} = \emptyset$ matching that of case 1(i).

Next, let us consider the case of $N\{\!|M/x|\!\} = M'\langle\!\langle N'/y\rangle\!\rangle\{\!|M/x|\!\} = M'\{\!|M/x|\!\}\langle\!\langle N'/y\rangle\!\rangle$. By considering 1(V) we can see the evaluating the translation of creates the same process shape up to linear head substitution. Other cases follow analogously.

(4) This is a consequence of both (2) and (3). □

Notation D.1. We use the notation $\mathsf{fv}(M).\overline{\mathtt{none}}$ and $\widetilde{x}.\overline{\mathtt{none}}$ where $\mathsf{fv}(M)$ or $\widetilde{x}$ are equal to $x_1, \cdots, x_k$ to describe a process of the form $x_1.\overline{\mathtt{none}} \mid \cdots \mid x_k.\overline{\mathtt{none}}$

Theorem 5.30 (Operational Completeness)**.** *Let* $\mathbb{N}$ *and* $\mathbb{M}$ *be well-formed, partially open* $\widehat{\lambda}^{\natural}_{\oplus}$ *expressions. If* $\mathbb{N} \longrightarrow \mathbb{M}$ *then there exist* Q *and* $\mathbb{M}'$ *such that* $\mathbb{M}' \equiv_{\lambda} \mathbb{M}$, $[\![\mathbb{N}]\!]^{\natural}_{u} \longrightarrow^{*} Q = [\![\mathbb{M}']\!]^{\natural}_{u}$.

Proof. By induction on the reduction rule applied to infer $\mathbb{N} \longrightarrow \mathbb{M}$. We have five cases.

(1) Case [RS:Beta]:

Then $\mathbb{N} = (\lambda x.M[\widetilde{x} \leftarrow x])B \longrightarrow M[\widetilde{x} \leftarrow x]\ \langle\!\langle {}^{B}/_{x}\rangle\!\rangle = \mathbb{M}$.

On the one hand, we have:

$$\begin{aligned}
[\![\mathbb{N}]\!]^{\natural}_{u} &= [\![(\lambda x.M[\widetilde{x} \leftarrow x])B]\!]^{\natural}_{u} \\
&= \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)([\![\lambda x.M[\widetilde{x} \leftarrow x]]\!]^{\natural}_{v} \mid v.\mathtt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([\![B_i]\!]^{\natural}_{x} \mid [v \leftrightarrow u])) \\
&= \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)(v.\overline{\mathtt{some}}; v(x).[\![M[\widetilde{x} \leftarrow x]]\!]^{\natural}_{v} \mid v.\mathtt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([\![B_i]\!]^{\natural}_{x} \mid [v \leftrightarrow u])) \\
&\longrightarrow \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)(v(x).[\![M[\widetilde{x} \leftarrow x]]\!]^{\natural}_{v} \mid \overline{v}(x).([\![B_i]\!]^{\natural}_{x} \mid [v \leftrightarrow u])) \\
&\longrightarrow \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v, x)([\![M[\widetilde{x} \leftarrow x]]\!]^{\natural}_{v} \mid [\![B_i]\!]^{\natural}_{x} \mid [v \leftrightarrow u]) \\
&\longrightarrow \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x)([\![M[\widetilde{x} \leftarrow x]]\!]^{\natural}_{u} \mid [\![B_i]\!]^{\natural}_{x})
\end{aligned} \tag{D.2}$$

On the other hand, we have:

$$[\![\mathbb{M}]\!]^{\natural}_{u} = [\![M[\widetilde{x} \leftarrow x]\ \langle\!\langle {}^{B}/_{x}\rangle\!\rangle]\!]^{\natural}_{u} = \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x)([\![M[\widetilde{x} \leftarrow x]]\!]^{\natural}_{u} \mid [\![B_i]\!]^{\natural}_{x}) \tag{D.3}$$

Therefore, by (D.2) and (D.3) the result follows.

(2) Case [RS:Ex-Sub]:

Then $N = M[x_1, \cdots, x_k \leftarrow x]\ \langle\!\langle {}^{B}/_{x} \rangle\!\rangle$, with $B = \wr N_1, \ldots, N_k \wr$, $k \geq 1$ and $M \neq \mathtt{fail}^{\widetilde{y}}$. The reduction is

$$\mathbb{N} = M[x_1, \cdots, x_k \leftarrow x]\ \langle\!\langle {}^{B}/_{x} \rangle\!\rangle \longrightarrow \sum_{B_i \in \mathsf{PER}(B)} M\ \langle\!| B_i(1)/x_1 |\!\rangle \cdots \langle\!| B_i(k)/x_k |\!\rangle = \mathbb{M}.$$

We detail the encodings of $[\![\mathbb{N}]\!]_u^{\natural}$ and $[\![\mathbb{M}]\!]_u^{\natural}$. To simplify the proof, we will consider $k = 1$ (the case $k > 1$ follows analogously).

On the one hand, we have:

$$\begin{aligned}
[\![\mathbb{N}]\!]_u^{\natural} &= [\![M[x_1 \leftarrow x]\ \langle\!\langle {}^{B}/_{x} \rangle\!\rangle]\!]_u^{\natural} = \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x)([\![M[x_1 \leftarrow x]]\!]_u^{\natural} \mid [\![B_i]\!]_x^{\natural}) \\
&= \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x)(x.\overline{\mathtt{some}}.\overline{x}(y_1).(y_1.\mathtt{some}_{\emptyset}; y_1.\mathtt{close}; \mathbf{0} \mid x.\overline{\mathtt{some}}; x.\mathtt{some}_{u,(\mathsf{fv}(M)\setminus x_1)}; \\
&\quad x(x_1).x.\overline{\mathtt{some}}; \overline{x}(y_2).(y_2.\mathtt{some}_{u,\mathsf{fv}(M)}; y_2.\mathtt{close}; [\![M]\!]_u^{\natural} \mid x.\overline{\mathtt{none}})) \mid \\
&\quad x.\mathtt{some}_{\mathsf{fv}(B_i(1))}; x(y_1).x.\mathtt{some}_{y_1,\mathsf{fv}(B_i(1))}; x.\overline{\mathtt{some}}; \overline{x}(x_1).(x_1.\mathtt{some}_{\mathsf{fv}(B_i(1))}; \\
&\quad [\![B_i(1)]\!]_{x_1}^{\natural} \mid y_1.\overline{\mathtt{none}} \mid x.\mathtt{some}_{\emptyset}; x(y_2).(y_2.\overline{\mathtt{some}}; y_2.\overline{\mathtt{close}} \mid x.\mathtt{some}_{\emptyset}; x.\overline{\mathtt{none}}))) \\
&\longrightarrow^* \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x, y_1, x_1, y_2)(y_1.\mathtt{some}_{\emptyset}; y_1.\mathtt{close}; \mathbf{0} \mid y_1.\overline{\mathtt{none}} \mid y_2.\mathtt{some}_{u,\mathsf{fv}(M)}; y_2.\mathtt{close}; \\
&\quad [\![M]\!]_u^{\natural} \mid y_2.\overline{\mathtt{some}}; y_2.\overline{\mathtt{close}} \mid x.\overline{\mathtt{none}} \mid x.\mathtt{some}_{\emptyset}; x.\overline{\mathtt{none}} \mid x_1.\mathtt{some}_{\mathsf{fv}(B_i(1))}; [\![B_i(1)]\!]_{x_1}^{\natural}) \\
&\longrightarrow^* \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x_1)([\![M]\!]_u^{\natural} \mid x_1.\mathtt{some}_{\mathsf{fv}(B_i(1))}; [\![B_i(1)]\!]_{x_1}^{\natural})
\end{aligned} \tag{D.4}$$

On the other hand, we have:

$$\begin{aligned}
[\![\mathbb{M}]\!]_u^{\natural} &= [\![\sum_{B_i \in \mathsf{PER}(B)} M\ \langle\!| B_i(1)/x_1 |\!\rangle]\!]_u^{\natural} = \bigoplus_{B_i \in \mathsf{PER}(B)} [\![M\ \langle\!| B_i(1)/x_1 |\!\rangle]\!]_u^{\natural} \\
&= \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x_1)([\![M]\!]_u^{\natural} \mid x_1.\mathtt{some}_{\mathsf{fv}(B_i(1))}; [\![B_i(1)]\!]_{x_1}^{\natural})
\end{aligned} \tag{D.5}$$

Therefore, by (D.4) and (D.5) the result follows.

(3) Case [RS:Lin-Fetch]:

Then we have $\mathbb{N} = M\ \langle\!| N'/x |\!\rangle$ with $\mathsf{head}(M) = x$ and $\mathbb{N} \longrightarrow M\{\!|N'/x|\!\} = \mathbb{M}$.

On the one hand, we have:

$$\begin{aligned}
[\![N]\!]_u^{\natural} = [\![M\ \langle\!| N'/x |\!\rangle]\!]_u^{\natural} &= (\nu x)([\![M]\!]_u^{\natural} \mid x.\mathtt{some}_{\mathsf{fv}(N')}; [\![N']\!]_x^{\natural}) \\
&\longrightarrow^* (\nu x)(\bigoplus_{i \in I} (\nu \widetilde{y})([\![x]\!]_j^{\natural} \mid P_i) \mid x.\mathtt{some}_{\mathsf{fv}(N')}; [\![N']\!]_x^{\natural}) \qquad (*) \\
&= (\nu x)(\bigoplus_{i \in I} (\nu \widetilde{y})([\![x]\!]_j^{\natural} \mid P_i) \mid x.\mathtt{some}; [\![N']\!]_x^{\natural}) \\
&\longrightarrow (\nu x)(\bigoplus_{i \in I} (\nu \widetilde{y})([x \leftrightarrow j] \mid P_i) \mid [\![N']\!]_x^{\natural}) \\
&\longrightarrow \bigoplus_{i \in I} (\nu \widetilde{y})(P_i \mid [\![N']\!]_j^{\natural}) = Q
\end{aligned} \tag{D.6}$$

where the reductions denoted by $(*)$ are inferred via Proposition 5.29.

On the other hand, we have by Proposition 5.29 :

$$[\![\mathbb{M}]\!]^{\natural}_{u} = [\![M\{\!|N'/x|\!\}]\!]^{\natural}_{u} \longrightarrow^{*} \bigoplus_{i\in I}(\nu\widetilde{y})(P_i \mid [\![N']\!]^{\natural}_{j}) \tag{D.7}$$

We also have by Proposition 5.29 and (D.7) that there exists M' such that $M' \equiv_{\lambda} M\{\!|N'/x|\!\}$ with:

$$[\![M']\!]^{\natural}_{u} = \bigoplus_{i\in I}(\nu\widetilde{y})(P_i \mid [\![N']\!]^{\natural}_{j}) \tag{D.8}$$

Therefore, by (D.6) and (D.8) the result follows.

(4) Case [RS:TCont] and [RS:ECont]: These cases follow by IH.

(5) Case [RS:Fail]:

Then, $\mathbb{N} = M[x_1, \cdots, x_k \leftarrow x]\ \langle\!\langle {}^{B}/_{x} \rangle\!\rangle$ with $k \neq \mathsf{size}(B)$ and

$$\mathbb{N} \longrightarrow \sum_{B_i\in \mathsf{PER}(B)} \mathtt{fail}^{\widetilde{y}} = \mathbb{M},$$

where $\widetilde{y} = (\mathsf{fv}(M) \setminus \{x_1, \cdots, x_k\}) \cup \mathsf{fv}(B)$.

Let us assume that $k > l$ and we proceed similarly for $k > l$. Hence $k = l + m$ for some $m \geq 1$. On the one hand, we have (D.9), this can be seen in Fig. 20.

On the other hand, we have:

$$\begin{aligned}[\![\mathbb{M}]\!]^{\natural}_{u} &= [\![\sum_{B_i\in \mathsf{PER}(B)} \mathtt{fail}^{\widetilde{y}}]\!]^{\natural}_{u} = \bigoplus_{B_i\in \mathsf{PER}(B)} [\![\mathtt{fail}^{\widetilde{y}}]\!]^{\natural}_{u} \\ &= \bigoplus_{B_i\in \mathsf{PER}(B)} u.\overline{\mathtt{none}} \mid (\mathsf{fv}(M) \setminus \{x_1, \cdots, x_k\}) \cup \mathsf{fv}(B).\overline{\mathtt{none}}\end{aligned} \tag{D.10}$$

Therefore, by (D.9) and (D.10) the result follows.

(6) Case [RS:Cons$_1$]:

Then, $\mathbb{N} = \mathtt{fail}^{\widetilde{x}}\ B$ with $B = \wr N_1, \ldots, N_k \wr$ and $\mathbb{N} \longrightarrow \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{x}\cup\widetilde{y}} = \mathbb{M}$, where $\widetilde{y} = \mathsf{fv}(B)$.

On the one hand, we have:

$$\begin{aligned}[\![N]\!]^{\natural}_{u} &= [\![\mathtt{fail}^{\widetilde{x}}\ B]\!]^{\natural}_{u} \\ &= \bigoplus_{B_i\in \mathsf{PER}(B)} (\nu v)([\![\mathtt{fail}^{\widetilde{x}}]\!]^{\natural}_{v} \mid v.\mathtt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([v \leftrightarrow u] \mid [\![B_i]\!]^{\natural}_{x})) \\ &= \bigoplus_{B_i\in \mathsf{PER}(B)} (\nu v)(v.\overline{\mathtt{none}} \mid \widetilde{x}.\overline{\mathtt{none}} \mid v.\mathtt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([v \leftrightarrow u] \mid [\![B_i]\!]^{\natural}_{x})) \\ &\longrightarrow \bigoplus_{B_i\in \mathsf{PER}(B)} u.\overline{\mathtt{none}} \mid \widetilde{x}.\overline{\mathtt{none}} \mid \widetilde{y}.\overline{\mathtt{none}} \\ &= \bigoplus_{\mathsf{PER}(B)} u.\overline{\mathtt{none}} \mid \widetilde{x}.\overline{\mathtt{none}} \mid \widetilde{y}.\overline{\mathtt{none}}\end{aligned} \tag{D.11}$$

$$
\begin{aligned}
[\![\mathbb{N}]\!]^{\natural}_{u} &= [\![M[x_1,\cdots,x_k \leftarrow x]\ \langle\!\langle B/x \rangle\!\rangle]\!]^{\natural}_{u} \\
&= \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x)([\![M[x_1,\cdots,x_k \leftarrow x]]\!]^{\natural}_{u} \mid [\![B_i]\!]^{\natural}_{x}) \\
&= \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x)(x.\overline{\mathtt{some}}.\overline{x}(y_1).(y_1.\mathtt{some}_{\emptyset}; y_1.\mathtt{close}; \mathbf{0} \mid x.\overline{\mathtt{some}}; x.\mathtt{some}_{u,(\mathsf{fv}(M)\setminus x_1,\cdots,x_k)}; \\
&\qquad x(x_1).\cdots x.\overline{\mathtt{some}}.\overline{x}(y_k).(y_k.\mathtt{some}_{\emptyset}; y_k.\mathtt{close}; \mathbf{0} \mid x.\overline{\mathtt{some}}; x.\mathtt{some}_{u,(\mathsf{fv}(M)\setminus x_k)}; \\
&\qquad x(x_k).x.\overline{\mathtt{some}}; \overline{x}(y_{k+1}).(y_{k+1}.\mathtt{some}_{u,\mathsf{fv}(M)}; y_{k+1}.\mathtt{close}; [\![M]\!]^{\natural}_{u} \mid x.\overline{\mathtt{none}}))\cdots) \\
&\qquad \mid x.\mathtt{some}_{\mathsf{fv}(B)}; x(y_1).x.\mathtt{some}_{y_1,\mathsf{fv}(B)}; x.\overline{\mathtt{some}}; \overline{x}(x_1).(x_1.\mathtt{some}_{\mathsf{fv}(B_i(1))}; [\![B_i(1)]\!]^{\natural}_{x_1} \\
&\qquad \mid y_1.\overline{\mathtt{none}} \mid \cdots x.\mathtt{some}_{\mathsf{fv}(B_i(l))}; x(y_l).x.\mathtt{some}_{y_l,\mathsf{fv}(B_i(l))}; x.\overline{\mathtt{some}}; \overline{x}(x_l).(x_l.\mathtt{some}_{\mathsf{fv}(B_i(l))}; \\
&\qquad [\![B_i(l)]\!]^{\natural}_{x_l} \mid y_l.\overline{\mathtt{none}} \mid x.\mathtt{some}_{\emptyset}; x(y_{l+1}).(y_{l+1}.\overline{\mathtt{some}}; y_{l+1}.\overline{\mathtt{close}} \mid x.\mathtt{some}_{\emptyset}; x.\overline{\mathtt{none}}))))) \\
&\longrightarrow^{*} \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x, y_1, x_1, \cdots y_l, x_l)(y_1.\mathtt{some}_{\emptyset}; y_1.\mathtt{close}; \mathbf{0} \mid \cdots \mid y_l.\mathtt{some}_{\emptyset}; y_l.\mathtt{close}; \mathbf{0} \\
&\qquad x.\overline{\mathtt{some}}.\overline{x}(y_{l+1}).(y_{l+1}.\mathtt{some}_{\emptyset}; y_{l+1}.\mathtt{close}; \mathbf{0} \mid x.\overline{\mathtt{some}}; x.\mathtt{some}_{u,(\mathsf{fv}(M)\setminus x_{l+1},\cdots,x_k)}; \\
&\qquad x(x_{l+1}).\cdots x.\overline{\mathtt{some}}.\overline{x}(y_k).(y_k.\mathtt{some}_{\emptyset}; y_k.\mathtt{close}; \mathbf{0} \mid x.\overline{\mathtt{some}}; x.\mathtt{some}_{u,(\mathsf{fv}(M)\setminus x_k)}; x(x_k). \\
&\qquad x.\overline{\mathtt{some}}; \overline{x}(y_{k+1}).(y_{k+1}.\mathtt{some}_{u,\mathsf{fv}(M)}; y_{k+1}.\mathtt{close}; [\![M]\!]^{\natural}_{u} \mid x.\overline{\mathtt{none}}))\cdots) \mid \\
&\qquad x_1.\mathtt{some}_{\mathsf{fv}(B_i(1))}; [\![B_i(1)]\!]^{\natural}_{x_1} \mid \cdots \mid x_l.\mathtt{some}_{\mathsf{fv}(B_i(l))}; [\![B_i(l)]\!]^{\natural}_{x_l} \mid y_1.\overline{\mathtt{none}} \mid \cdots \mid y_l.\overline{\mathtt{none}} \\
&\qquad x.\mathtt{some}_{\emptyset}; x(y_{l+1}).(y_{l+1}.\overline{\mathtt{some}}; y_{l+1}.\overline{\mathtt{close}} \mid x.\mathtt{some}_{\emptyset}; x.\overline{\mathtt{none}})) \\
&\longrightarrow^{*} \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x, x_1, \cdots, x_l)(x.\mathtt{some}_{u,(\mathsf{fv}(M)\setminus x_{l+1},\cdots,x_k)}; x(x_{l+1}).\cdots \\
&\qquad x.\overline{\mathtt{some}}.\overline{x}(y_k).(y_k.\mathtt{some}_{\emptyset}; y_k.\mathtt{close}; \mathbf{0} \mid x.\overline{\mathtt{some}}; x.\mathtt{some}_{u,(\mathsf{fv}(M)\setminus x_k)}; x(x_k). \\
&\qquad x.\overline{\mathtt{some}}; \overline{x}(y_{k+1}).(y_{k+1}.\mathtt{some}_{u,\mathsf{fv}(M)}; y_{k+1}.\mathtt{close}; [\![M]\!]^{\natural}_{u} \mid x.\overline{\mathtt{none}})) \mid \\
&\qquad x_1.\mathtt{some}_{\mathsf{fv}(B_i(1))}; [\![B_i(1)]\!]^{\natural}_{x_1} \mid \cdots \mid x_l.\mathtt{some}_{\mathsf{fv}(B_i(l))}; [\![B_i(l)]\!]^{\natural}_{x_l} \mid x.\overline{\mathtt{none}}) \\
&\longrightarrow \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x_1, \cdots, x_l)(u.\overline{\mathtt{none}} \mid x_1.\overline{\mathtt{none}} \mid \cdots \mid x_l.\overline{\mathtt{none}} \mid (\mathsf{fv}(M) \setminus x_1, \cdots, x_k).\overline{\mathtt{none}} \mid \\
&\qquad x_1.\mathtt{some}_{\mathsf{fv}(B_i(1))}; [\![B_i(1)]\!]^{\natural}_{x_1} \mid \cdots \mid x_l.\mathtt{some}_{\mathsf{fv}(B_i(l))}; [\![B_i(l)]\!]^{\natural}_{x_l}) \\
&\longrightarrow^{*} \bigoplus_{B_i \in \mathsf{PER}(B)} u.\overline{\mathtt{none}} \mid (\mathsf{fv}(M) \setminus \{x_1, \cdots, x_k\}) \cup \mathsf{fv}(B).\overline{\mathtt{none}}
\end{aligned}
\tag{D.9}
$$

Figure 20: Reductions of an encoded explicit substitution

On the other hand, we have:

$$
\begin{aligned}
[\![\mathbb{M}]\!]^{\natural}_{u} = [\![\sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{x} \cup \widetilde{y}}]\!]^{\natural}_{u} &= \bigoplus_{\mathsf{PER}(B)} [\![\mathtt{fail}^{\widetilde{x} \cup \widetilde{y}}]\!]^{\natural}_{u} \\
&= \bigoplus_{\mathsf{PER}(B)} u.\overline{\mathtt{none}} \mid \widetilde{x}.\overline{\mathtt{none}} \mid \widetilde{y}.\overline{\mathtt{none}}
\end{aligned}
\tag{D.12}
$$

Therefore, by (D.11) and (D.12) the result follows.

(7) Cases [RS:Cons$_2$] and [RS:Cons$_3$]: These cases follow by IH similarly to Case 7. □

Theorem 5.33 (Operational Soundness)**.** *Let $\mathbb{N}$ be a well-formed, partially open $\widehat{\lambda}^{\natural}_{\oplus}$ expression. If $[\![\mathbb{N}]\!]^{\natural}_{u} \longrightarrow^{*} Q$ then there exist Q' and $\mathbb{N}'$ such that $Q \longrightarrow^{*} Q'$, $\mathbb{N} \longrightarrow^{*}_{\equiv_\lambda} \mathbb{N}'$ and $[\![\mathbb{N}']\!]^{\natural}_{u} = Q'$.*

Proof. By induction on the structure of $\mathbb{N}$ and then induction on the number of reductions of $[\![\mathbb{N}]\!]^{\natural} \longrightarrow^{*}_{\equiv_\lambda} Q$

(1) $\mathbb{N} = x$, $\mathbb{N} = \mathtt{fail}^{\emptyset}$ and $\mathbb{N} = \lambda x.(M[\widetilde{x} \leftarrow x])$.
These cases are trivial since no reduction can take place.

(2) $\mathbb{N} = (M\ B)$.
Then,

$$[\![(M\ B)]\!]^{\natural}_{u} = \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)([\![M]\!]^{\natural}_{v} \mid v.\mathtt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([v \leftrightarrow u] \mid [\![B_i]\!]^{\natural}_{x}))$$

and we are able to perform the reductions from $[\![(M\ B)]\!]^{\natural}_{u}$.
We now proceed by induction on k, with $[\![\mathbb{N}]\!]^{\natural}_{u} \longrightarrow^{k} Q$.
The interesting case is when $k \geq 1$ (the case $k = 0$ is trivial).
Then, for some process R and n, m such that $k = n + m$, we have the following:

$$\begin{aligned}
[\![\mathbb{N}]\!]^{\natural}_{u} &= \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)([\![M]\!]^{\natural}_{v} \mid v.\mathtt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([\![B_i]\!]^{\natural}_{x} \mid [v \leftrightarrow u])) \\
&\longrightarrow^{m} \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)(R \mid v.\mathtt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([\![B_i]\!]^{\natural}_{x} \mid [v \leftrightarrow u])) \\
&\longrightarrow^{n} Q
\end{aligned}$$

Thus, the first $m \geq 0$ reduction steps are internal to $[\![M]\!]^{\natural}_{v}$; type preservation in $\mathsf{s}\pi$ ensures that, if they occur, these reductions do not discard the possibility of synchronizing with $v.\mathtt{some}$. Then, the first of the $n \geq 0$ reduction steps towards Q is a synchronization between R and $v.\mathtt{some}_{u,\mathsf{fv}(B)}$.
We consider two sub-cases, depending on the values of m and n:

(I) When $m = 0$ and $n \geq 1$:
Thus $R = [\![\mathbb{M}]\!]^{\natural}_{v}$, and there are two possibilities of having an unguarded $v.\overline{\mathtt{some}}$ or $v.\overline{\mathtt{none}}$ without internal reductions. By the diamond property (Proposition 3.10) we will be reducing each non-deterministic choice of a process simultaneously. Then we have the following for each case:

(A) $M = (\lambda x.M'[\widetilde{x} \leftarrow x])\langle\!|N_1/y_1|\!\rangle \cdots \langle\!|N_p/y_p|\!\rangle \qquad (p \geq 0)$.

$$\begin{aligned}
[\![M]\!]^{\natural}_{v} &= [\![(\lambda x.M'[\widetilde{x} \leftarrow x])\langle\!|N_1/y_1|\!\rangle \cdots \langle\!|N_p/y_p|\!\rangle]\!]^{\natural}_{v} \\
&= (\nu \widetilde{y})([\![(\lambda x.M'[\widetilde{x} \leftarrow x])]\!]^{\natural}_{v} \mid y_1.\mathtt{some}_{\mathsf{fv}(N_1)}; [\![N_1]\!]^{\natural}_{y_1} \mid \cdots \mid y_p.\mathtt{some}_{\mathsf{fv}(N_p)}; [\![N_p]\!]^{\natural}_{y_p}) \\
&= (\nu \widetilde{y})([\![(\lambda x.M'[\widetilde{x} \leftarrow x])]\!]^{\natural}_{v} \mid Q''), \text{ for } \widetilde{y} = y_1, \cdots, y_p \\
&= (\nu \widetilde{y})(v.\overline{\mathtt{some}}; v(x).[\![M'[\widetilde{x} \leftarrow x]]\!]^{\natural}_{v} \mid Q'')
\end{aligned}$$

where $Q'' = y_1.\mathtt{some}_{\mathsf{fv}(N_1)}; [\![N_1]\!]^{\natural}_{y_1} \mid \cdots \mid y_p.\mathtt{some}_{\mathsf{fv}(N_p)}; [\![N_p]\!]^{\natural}_{y_p}$.

With this shape for M, the encoding of $\mathbb{N}$ becomes:

$$
\begin{aligned}
[\![\mathbb{N}]\!]^{\not z}_u &= [\![(M\ B)]\!]^{\not z}_u \\
&= \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)([\![M]\!]^{\not z}_v \mid v.\mathtt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([\![B_i]\!]^{\not z}_x \mid [v \leftrightarrow u])) \\
&= \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)((\nu \widetilde{y})(v.\overline{\mathtt{some}}; v(x).[\![M'[\widetilde{x} \leftarrow x]]\!]^{\not z}_v \mid Q'') \mid \\
&\qquad\qquad v.\mathtt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([\![B_i]\!]^{\not z}_x \mid [v \leftrightarrow u])) \\
&\longrightarrow \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v, \widetilde{y})(v(x).[\![M'[\widetilde{x} \leftarrow x]]\!]^{\not z}_v \mid \overline{v}(x).([\![B_i]\!]^{\not z}_x \mid [v \leftrightarrow u]) \mid Q'') = Q_1 \\
&\longrightarrow \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v, \widetilde{y}, x)([\![M'[\widetilde{x} \leftarrow x]]\!]^{\not z}_v \mid [\![B_i]\!]^{\not z}_x \mid [v \leftrightarrow u] \mid Q'') = Q_2 \\
&\longrightarrow \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x, \widetilde{y})([\![M'[\widetilde{x} \leftarrow x]]\!]^{\not z}_u \mid [\![B_i]\!]^{\not z}_x \mid Q'') = Q_3
\end{aligned}
$$

We also have that

$$
\begin{aligned}
\mathbb{N} &= (\lambda x.M'[\widetilde{x} \leftarrow x])\langle\!\langle N_1/y_1 \rangle\!\rangle \cdots \langle\!\langle N_p/y_p \rangle\!\rangle\ B \\
&\equiv_\lambda ((\lambda x.M'[\widetilde{x} \leftarrow x])B)\langle\!\langle N_1/y_1 \rangle\!\rangle \cdots \langle\!\langle N_p/y_p \rangle\!\rangle \\
&\longrightarrow M'[\widetilde{x} \leftarrow x]\langle\!\langle {}^B/_x \rangle\!\rangle\langle\!\langle N_1/y_1 \rangle\!\rangle \cdots \langle\!\langle N_p/y_p \rangle\!\rangle = \mathbb{M}
\end{aligned}
$$

Furthermore, we have:

$$
\begin{aligned}
[\![\mathbb{M}']\!]^{\not z}_v &= [\![M'[\widetilde{x} \leftarrow x]\langle\!\langle {}^B/_x \rangle\!\rangle\langle\!\langle N_1/y_1 \rangle\!\rangle \cdots \langle\!\langle N_p/y_p \rangle\!\rangle]\!]^{\not z}_v \\
&= \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x)([\![M'[\widetilde{x} \leftarrow x]]\!]^{\not z}_v \mid [\![B_i]\!]^{\not z}_x \mid Q'')
\end{aligned}
$$

We consider different possibilities for $n \geq 1$; in all of the thesis holds:

(i) $n = 1$:
Then $Q = Q_1$ and $[\![\mathbb{N}]\!]^{\not z}_u \longrightarrow^1 Q_1$. In addition,
(a) $Q_1 \longrightarrow^2 Q_3 = Q'$,
(b) $\mathbb{N} \longrightarrow^1 M'[\widetilde{x} \leftarrow x]\langle\!\langle {}^B/_x \rangle\!\rangle = \mathbb{N}'$,
(c) $[\![M'[\widetilde{x} \leftarrow x]\langle\!\langle {}^B/_x \rangle\!\rangle]\!]^{\not z}_u = Q_3$.
and the result follows.

(ii) $n = 2$:
Then $Q = Q_2$ and $[\![\mathbb{N}]\!]^{\not z}_u \longrightarrow^2 Q_2$. In addition,
- $Q_2 \longrightarrow^1 Q_3 = Q'$,
- $\mathbb{N} \longrightarrow^1 M'[\widetilde{x} \leftarrow x]\langle\!\langle {}^B/_x \rangle\!\rangle = \mathbb{N}'$
- $[\![M'[\widetilde{x} \leftarrow x])\langle\!\langle {}^B/_x \rangle\!\rangle]\!]^{\not z}_u = Q_3$

and the result follows.

(iii) $n \geq 3$:
Then $[\![\mathbb{N}]\!]^{\not z}_u \longrightarrow^3 Q_3 \longrightarrow^l Q$, for $l \geq 0$. In addition, $\mathbb{N} \longrightarrow \mathbb{M}'$ and $Q_3 = [\![\mathbb{M}']\!]^{\not z}_u$. By the IH, there exist Q' and $\mathbb{N}'$ such that $Q \longrightarrow^i Q'$, $\mathbb{M}' \longrightarrow^j_{\equiv_\lambda} \mathbb{N}'$ and $[\![\mathbb{N}']\!]^{\not z}_u = Q'$. Finally, $[\![\mathbb{N}]\!]^{\not z}_u \longrightarrow^3 Q_3 \longrightarrow^l Q \longrightarrow^i Q'$ and $\mathbb{N} \to \mathbb{M}' \longrightarrow^j_{\equiv_\lambda} \mathbb{N}'$, and the result follows.

(B) $M = \mathtt{fail}^{\widetilde{z}}$.

$$[\![M]\!]^{\natural}_{v} = [\![\mathtt{fail}^{\widetilde{z}}]\!]^{\natural}_{v} = v.\overline{\mathtt{none}} \mid \widetilde{z}.\overline{\mathtt{none}}$$

With this shape for M, the encoding of $\mathbb{N}$ becomes:

$$\begin{aligned}
[\![\mathbb{N}]\!]^{\natural}_{u} &= [\![(M\ B)]\!]^{\natural}_{u} \\
&= \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)([\![M]\!]^{\natural}_{v} \mid v.\mathtt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([\![B_i]\!]^{\natural}_{x} \mid [v \leftrightarrow u])) \\
&= \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)(v.\overline{\mathtt{none}} \mid \widetilde{z}.\overline{\mathtt{none}} \mid v.\mathtt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([\![B_i]\!]^{\natural}_{x} \mid [v \leftrightarrow u])) \\
&\longrightarrow \bigoplus_{B_i \in \mathsf{PER}(B)} u.\overline{\mathtt{none}} \mid \widetilde{z}.\overline{\mathtt{none}} \mid \mathsf{fv}(B).\overline{\mathtt{none}} \\
&= \bigoplus_{\mathsf{PER}(B)} u.\overline{\mathtt{none}} \mid \widetilde{z}.\overline{\mathtt{none}} \mid \mathsf{fv}(B).\overline{\mathtt{none}}
\end{aligned}$$

Also,

$$\mathbb{N} = \mathtt{fail}^{\widetilde{z}}\ B \longrightarrow \sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{z} \cup \mathsf{fv}(B)} = \mathbb{M}.$$

Furthermore,

$$\begin{aligned}
[\![\mathbb{M}]\!]^{\natural}_{u} &= [\![\sum_{\mathsf{PER}(B)} \mathtt{fail}^{\widetilde{z} \cup \mathsf{fv}(B)}]\!]^{\natural}_{u} \\
&= \bigoplus_{\mathsf{PER}(B)} [\![\mathtt{fail}^{\widetilde{z} \cup \mathsf{fv}(B)}]\!]^{\natural}_{u} \\
&= \bigoplus_{\mathsf{PER}(B)} u.\overline{\mathtt{none}} \mid \widetilde{z}.\overline{\mathtt{none}} \mid \mathsf{fv}(B).\overline{\mathtt{none}}
\end{aligned}$$

(II) When $m \geq 1$ and $n \geq 0$, the distinguish two cases:

(A) $n = 0$:

Then,

$$\bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)(R \mid v.\mathtt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([\![B_i]\!]^{\natural}_{x} \mid [v \leftrightarrow u])) = Q,$$

and $[\![M]\!]^{\natural}_{u} \longrightarrow^{m} R$.

By the IH there exist R' and $\mathbb{M}'$ such that $R \longrightarrow^{i} R'$, $M \longrightarrow^{j}_{\equiv_\lambda} \mathbb{M}'$, and $[\![\mathbb{M}']\!]^{\natural}_{u} = R'$. Hence,

$$\begin{aligned}
[\![\mathbb{N}]\!]^{\natural}_{u} &= \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)([\![M]\!]^{\natural}_{v} \mid v.\mathtt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([\![B_i]\!]^{\natural}_{x} \mid [v \leftrightarrow u])) \\
&\longrightarrow^{m} \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)(R \mid v.\mathtt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([\![B_i]\!]^{\natural}_{x} \mid [v \leftrightarrow u])) = Q \\
&\longrightarrow^{i} \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)(R' \mid v.\mathtt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([\![B_i]\!]^{\natural}_{x} \mid [v \leftrightarrow u])) = Q'
\end{aligned}$$

and so the $\widehat{\lambda}^{\natural}_{\oplus}$ term can reduce as follows: $\mathbb{N} = (M\ B) \longrightarrow^{j}_{\equiv_\lambda} M'\ B = \mathbb{N}'$ and $[\![\mathbb{N}']\!]^{\natural}_{u} = Q'$.

(B) $n \geq 1$:
Then R has an occurrence of an unguarded $v.\overline{\texttt{some}}$ or $v.\overline{\texttt{none}}$, which implies it is of the form $[\![(\lambda x.M'[\widetilde{x} \leftarrow x])\langle\!\langle N_1/y_1 \rangle\!\rangle \cdots \langle\!\langle N_p/y_p \rangle\!\rangle]\!]^{\natural}_{v}$ or $[\![\texttt{fail}]\!]^{\natural}_{v}$, and the case follows by IH.

This concludes the analysis for the case $\mathbb{N} = (M\,B)$.

(3) $\mathbb{N} = M[\widetilde{x} \leftarrow x]$.
The sharing variable x is not free and the result follows by vacuity.

(4) $\mathbb{N} = (M[\widetilde{x} \leftarrow x])\langle\!\langle B/x \rangle\!\rangle$. Then,

$$[\![\mathbb{N}]\!]^{\natural}_{u} = [\![(M[\widetilde{x} \leftarrow x])\langle\!\langle B/x \rangle\!\rangle]\!]^{\natural}_{u} = \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x)([\![M[\widetilde{x} \leftarrow x]]\!]^{\natural}_{u} \mid [\![B_i]\!]^{\natural}_{x})$$

(I) $\mathsf{size}(\widetilde{x}) = \mathsf{size}(B)$.
Then let us consider the shape of the bag B.

(A) When $B = 1$
We have the following

$$\begin{aligned}
[\![\mathbb{N}]\!]^{\natural}_{u} &= (\nu x)([\![M[\leftarrow x]]\!]^{\natural}_{u} \mid [\![1]\!]^{\natural}_{x}) \\
&= (\nu x)(x.\overline{\texttt{some}}.\overline{x}(y_i).(y_i.\texttt{some}_{u,\mathsf{fv}(M)}; y_i.\texttt{close}; [\![M]\!]^{\natural}_{u} \mid x.\overline{\texttt{none}}) \mid \\
&\quad x.\texttt{some}_{\emptyset}; x(y_n).(y_n.\overline{\texttt{some}}; y_n.\overline{\texttt{close}} \mid x.\texttt{some}_{\emptyset}; x.\overline{\texttt{none}})) \\
&\longrightarrow (\nu x)(\overline{x}(y_i).(y_i.\texttt{some}_{u,\mathsf{fv}(M)}; y_i.\texttt{close}; [\![M]\!]^{\natural}_{u} \mid x.\overline{\texttt{none}}) \mid \\
&\quad x(y_n).(y_n.\overline{\texttt{some}}; y_n.\overline{\texttt{close}} \mid x.\texttt{some}_{\emptyset}; x.\overline{\texttt{none}})) \qquad = Q_1 \\
&\longrightarrow (\nu x, y_i)(y_i.\texttt{some}_{u,\mathsf{fv}(M)}; y_i.\texttt{close}; [\![M]\!]^{\natural}_{u} \mid x.\overline{\texttt{none}} \mid y_n.\overline{\texttt{some}}; \\
&\quad y_n.\overline{\texttt{close}} \mid x.\texttt{some}_{\emptyset}; x.\overline{\texttt{none}}) \qquad = Q_2 \\
&\longrightarrow (\nu x, y_i)(y_i.\texttt{close}; [\![M]\!]^{\natural}_{u} \mid x.\overline{\texttt{none}} \mid y_n.\overline{\texttt{close}} \mid x.\texttt{some}_{\emptyset}; x.\overline{\texttt{none}}) \qquad = Q_3 \\
&\longrightarrow (\nu x)([\![M]\!]^{\natural}_{u} \mid x.\overline{\texttt{none}} \mid x.\texttt{some}_{\emptyset}; x.\overline{\texttt{none}}) \qquad = Q_4 \\
&\longrightarrow [\![M]\!]^{\natural}_{u} \qquad = Q_5
\end{aligned}$$

Notice how Q_2 has a choice however the x name can be closed at any time so for simplicity we only perform communication across this name once all other names have completed their reductions.

Now proceed by induction on the number of reductions $[\![\mathbb{N}]\!]^{\natural}_{u} \longrightarrow^{k} Q$.

(i) $k = 0$:
This case is trivial.

(ii) $k = 1$: ($2 \leq k \leq 4$: is similar.)
Then, $Q = Q_1$ and $[\![\mathbb{N}]\!]^{\natural}_{u} \longrightarrow^{1} Q_1$. In addition, $Q_1 \longrightarrow^{4} Q_5 = Q'$, $\mathbb{N} \longrightarrow^{0} M[\leftarrow x]\langle\!\langle 1/x \rangle\!\rangle \equiv_\lambda M$ and $[\![M]\!]^{\natural}_{u} = Q_5$, and the result follows.

(iii) $k \geq 5$:
Then $[\![\mathbb{N}]\!]^{\natural}_{u} \longrightarrow^{5} Q_5 \longrightarrow^{l} Q$, for $l \geq 0$. Since $Q_5 = [\![M]\!]^{\natural}_{u}$, by the IH it follows that there exist Q' and $\mathbb{N}'$ such that $Q \longrightarrow^{i} Q', M \longrightarrow^{j}_{\equiv_\lambda} \mathbb{N}'$ and $[\![\mathbb{N}']\!]^{\natural}_{u} = Q'$.

$$
\begin{aligned}
[\![\mathbb{N}]\!]^{\natural}_{u} &= [\![(M[\widetilde{x} \leftarrow x])\langle\!\langle B/x \rangle\!\rangle]\!]^{\natural}_{u} \\
&= \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x)([\![M[\widetilde{x} \leftarrow x]]\!]^{\natural}_{u} \mid [\![B_i]\!]^{\natural}_{x}) \\
&= \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x)(x.\overline{\mathtt{some}}.\overline{x}(y_1).(y_1.\mathtt{some}_{\emptyset}; y_1.\mathtt{close}; \mathbf{0} \mid x.\overline{\mathtt{some}}; x.\mathtt{some}_{u,(\mathsf{fv}(M)\setminus x_1,\cdots,x_l)}; \\
&\quad x(x_1).\cdots x.\overline{\mathtt{some}}.\overline{x}(y_l).(y_l.\mathtt{some}_{\emptyset}; y_l.\mathtt{close}; \mathbf{0} \mid x.\overline{\mathtt{some}}; x.\mathtt{some}_{u,(\mathsf{fv}(M)\setminus x_l)}; x(x_l). \\
&\quad x.\overline{\mathtt{some}}; \overline{x}(y_{l+1}).(y_{l+1}.\mathtt{some}_{u,\mathsf{fv}(M)}; y_{l+1}.\mathtt{close}; [\![M]\!]^{\natural}_{u} \mid x.\overline{\mathtt{none}})) \cdots) \mid \\
&\quad x.\mathtt{some}_{\mathsf{fv}(B)}; x(y_1).x.\mathtt{some}_{y_1,\mathsf{fv}(B)}; x.\overline{\mathtt{some}}; \overline{x}(x_1).(x_1.\mathtt{some}_{\mathsf{fv}(B_i(1))}; [\![B_i(1)]\!]^{\natural}_{x_1} \\
&\quad \mid y_1.\overline{\mathtt{none}} \mid \cdots x.\mathtt{some}_{\mathsf{fv}(B_i(l))}; x(y_l).x.\mathtt{some}_{y_l,\mathsf{fv}(B_i(l))}; x.\overline{\mathtt{some}}; \overline{x}(x_l).(x_l.\mathtt{some}_{\mathsf{fv}(B_i(l))}; \\
&\quad [\![B_i(l)]\!]^{\natural}_{x_l} \mid y_l.\overline{\mathtt{none}} \mid x.\mathtt{some}_{\emptyset}; x(y_{l+1}).(y_{l+1}.\overline{\mathtt{some}}; y_{l+1}.\overline{\mathtt{close}} \mid x.\mathtt{some}_{\emptyset}; x.\overline{\mathtt{none}})))) \\
&\longrightarrow^{5l} \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x, x_1, y_1, \cdots, x_l, y_1)(y_1.\mathtt{some}_{\emptyset}; y_1.\mathtt{close}; \mathbf{0} \mid \cdots y_l.\mathtt{some}_{\emptyset}; y_l.\mathtt{close}; \mathbf{0} \mid \\
&\quad x.\overline{\mathtt{some}}; \overline{x}(y_{l+1}).(y_{l+1}.\mathtt{some}_{u,\mathsf{fv}(M)}; y_{l+1}.\mathtt{close}; [\![M]\!]^{\natural}_{u} \mid x.\overline{\mathtt{none}}) \mid \\
&\quad x_1.\mathtt{some}_{\mathsf{fv}(B_i(1))}; [\![B_i(1)]\!]^{\natural}_{x_1} \mid y_1.\overline{\mathtt{none}} \mid \cdots x_l.\mathtt{some}_{\mathsf{fv}(B_i(l))}; [\![B_i(l)]\!]^{\natural}_{x_l} \mid y_l.\overline{\mathtt{none}} \mid \\
&\quad x.\mathtt{some}_{\emptyset}; x(y_{l+1}).(y_{l+1}.\overline{\mathtt{some}}; y_{l+1}.\overline{\mathtt{close}} \mid x.\mathtt{some}_{\emptyset}; x.\overline{\mathtt{none}})) \\
&\longrightarrow^{5} \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x_1, y_1, \cdots, x_l, y_1)(y_1.\mathtt{some}_{\emptyset}; y_1.\mathtt{close}; \mathbf{0} \mid \cdots y_l.\mathtt{some}_{\emptyset}; y_l.\mathtt{close}; \mathbf{0} \\
&\quad \mid [\![M]\!]^{\natural}_{u} \mid x_1.\mathtt{some}_{\mathsf{fv}(B_i(1))}; [\![B_i(1)]\!]^{\natural}_{x_1} \mid y_1.\overline{\mathtt{none}} \mid \cdots x_l.\mathtt{some}_{\mathsf{fv}(B_i(l))}; [\![B_i(l)]\!]^{\natural}_{x_l} \mid y_l.\overline{\mathtt{none}}) \\
&\longrightarrow^{l} \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x_1, \cdots, x_l)([\![M]\!]^{\natural}_{u} \mid x_1.\mathtt{some}_{\mathsf{fv}(B_i(1))}; [\![B_i(1)]\!]^{\natural}_{x_1} \mid \cdots \mid x_l.\mathtt{some}_{\mathsf{fv}(B_i(l))}; [\![B_i(l)]\!]^{\natural}_{x_l}) \\
&= Q_{6l+5}
\end{aligned}
$$

Figure 21: Reductions of encoded explicit substitution

Then, $[\![\mathbb{N}]\!]^{\natural}_{u} \longrightarrow^{5} Q_5 \longrightarrow^{l} Q \longrightarrow^{i} Q'$ and by the contextual reduction one has $\mathbb{N} = (M[\leftarrow x])\langle\!\langle 1/x \rangle\!\rangle \longrightarrow^{j}_{\equiv_\lambda} \mathbb{N}'$ and the case holds.

(B) $B = \wr N_1, \cdots, N_l \wr$, for $l \geq 1$.
Then, consider the reductions in Fig. 21.
The proof follows by induction on the number of reductions $[\![\mathbb{N}]\!]^{\natural}_{u} \longrightarrow^{k} Q$.

(i) $k = 0$:
This case is trivial. Take $[\![\mathbb{N}]\!]^{\natural}_{u} = Q = Q'$ and $\mathbb{N} = \mathbb{N}'$.

(ii) $1 \leq k \leq 6l + 5$:
Then, $[\![\mathbb{N}]\!]^{\natural}_{u} \longrightarrow^{k} Q_k$. Observing the reductions in Fig. 21, one has $Q_k \longrightarrow^{6l+5-k} Q_{6l+5} = Q'$,
$\mathbb{N} \longrightarrow^{1} \sum_{B_i \in \mathsf{PER}(B)} M \ \langle\!\langle B_i(1)/x_1 \rangle\!\rangle \cdots \langle\!\langle B_i(l)/x_l \rangle\!\rangle = \mathbb{N}'$ and
$[\![\sum_{B_i \in \mathsf{PER}(B)} M \ \langle\!\langle B_i(1)/x_1 \rangle\!\rangle \cdots \langle\!\langle B_i(l)/x_l \rangle\!\rangle]\!]^{\natural}_{u} = Q_{6l+5}$, and the result follows.

(iii) $k > 6l + 5$:
Then, $[\![\mathbb{N}]\!]^{\natural}_{u} \longrightarrow^{6l+5} Q_{6l+5} \longrightarrow^{n} Q$, for $n \geq 1$. In addition,
$\mathbb{N} \longrightarrow^{1} \sum_{B_i \in \mathsf{PER}(B)} M \ \langle\!\langle B_i(1)/x_1 \rangle\!\rangle \cdots \langle\!\langle B_i(l)/x_l \rangle\!\rangle$ and

$Q_{6l+5} = [\![\sum_{B_i \in \mathsf{PER}(B)} M \ \langle\!\langle B_i(1)/x_1 \rangle\!\rangle \cdots \langle\!\langle B_i(l)/x_l \rangle\!\rangle]\!]^{\not\downarrow}_u$. By the IH there exist Q' and $\mathbb{N}'$ such that $Q \longrightarrow^i Q'$,

$$\sum_{B_i \in \mathsf{PER}(B)} M \ \langle\!\langle B_i(1)/x_1 \rangle\!\rangle \cdots \langle\!\langle B_i(l)/x_l \rangle\!\rangle \longrightarrow^j_{\equiv_\lambda} \mathbb{N}'$$

and $[\![\mathbb{N}']\!]^{\not\downarrow}_u = Q'$. Finally,
$[\![\mathbb{N}]\!]^{\not\downarrow}_u \longrightarrow^{6l+5} Q_{6l+5} \longrightarrow^n Q \longrightarrow^i Q'$ and
$\mathbb{N} \to \sum_{B_i \in \mathsf{PER}(B)} M \ \langle\!\langle B_i(1)/x_1 \rangle\!\rangle \cdots \langle\!\langle B_i(l)/x_l \rangle\!\rangle \longrightarrow^j_{\equiv_\lambda} \mathbb{N}'$.

(II) $\mathsf{size}(\widetilde{x}) > \mathsf{size}(B)$.
Then, $\mathbb{N} = M[x_1, \cdots, x_k \leftarrow x] \ \langle\!\langle {}^B\!/_x \rangle\!\rangle$ with $B = \wr N_1, \cdots, N_l \wr$, for $k > l$. Also,

$$\mathbb{N} \longrightarrow \sum_{B_i \in \mathsf{PER}(B)} \mathtt{fail}^{\widetilde{z}} = \mathbb{M} \quad \text{and} \quad \widetilde{z} = (\mathsf{fv}(M) \setminus \{x_1, \cdots, x_k\}) \cup \mathsf{fv}(B).$$

On the one hand, we have Fig. 22. Hence $k = l + m$ for some $m \geq 1$
Now we proceed by induction on the number of reductions $[\![\mathbb{N}]\!]^{\not\downarrow}_u \longrightarrow^j Q$.

(A) $j = 0$:
This case is trivial.

(B) $1 \leq j \leq 7l + 6$:
Then,
$[\![\mathbb{N}]\!]^{\not\downarrow}_u \longrightarrow^j Q_j \longrightarrow^{7l+6-j} Q_{7l+6} = Q'$, $\mathbb{N} \longrightarrow^1 \sum_{B_i \in \mathsf{PER}(B)} \mathtt{fail}^{\widetilde{z}} = \mathbb{N}'$
and $[\![\sum_{B_i \in \mathsf{PER}(B)} \mathtt{fail}^{\widetilde{z}}]\!]^{\not\downarrow}_u = Q_{7l+6}$, and the result follows.

(C) $j > 7l + 6$:
Then, $[\![\mathbb{N}]\!]^{\not\downarrow}_u \longrightarrow^{7l+6} Q_{7l+6} \longrightarrow^n Q$, for $n \geq 1$. Also, $\mathbb{N} \longrightarrow^1 \sum_{B_i \in \mathsf{PER}(B)} \mathtt{fail}^{\widetilde{z}}$.
However no further reductions can be performed.

(III) $\mathsf{size}(\widetilde{x}) < \mathsf{size}(B)$.
Proceeds similarly to the previous case.

(5) $\mathbb{N} = M\langle\!\langle N'/x \rangle\!\rangle$.
Then,

$$[\![M\langle\!\langle N'/x \rangle\!\rangle]\!]^{\not\downarrow}_u = (\nu x)([\![M]\!]^{\not\downarrow}_u \mid x.\mathtt{some}_{\mathsf{fv}(N')}; [\![N']\!]^{\not\downarrow}_x)$$

Then we have

$$\begin{aligned} [\![\mathbb{N}]\!]^{\not\downarrow}_u &= (\nu x)([\![M]\!]^{\not\downarrow}_u \mid x.\mathtt{some}_{\mathsf{fv}(N')}; [\![N']\!]^{\not\downarrow}_x) \\ &\longrightarrow^m (\nu x)(R \mid x.\mathtt{some}_{\mathsf{fv}(N')}; [\![N']\!]^{\not\downarrow}_x) \\ &\longrightarrow^n Q \end{aligned}$$

for some process R, where $\longrightarrow^n$ is a reduction that initially synchronizes with $x.\mathtt{some}_{\mathsf{fv}(N')}$ when $n \geq 1$, $n + m = k \geq 1$. Type preservation in $\mathsf{s}\pi$ ensures reducing $[\![M]\!]^{\not\downarrow}_v \longrightarrow^m$ does not consume possible synchronizations with $x.\mathtt{some}$ if they occur. Let us consider the the possible sizes of both m and n.

(I) For $m = 0$ and $n \geq 1$.
In this case $R = [\![M]\!]^{\not\downarrow}_u$ and there are two possibilities of having an unguarded $x.\overline{\mathtt{some}}$ or $x.\overline{\mathtt{none}}$ without internal reductions.

(A) $M = \mathtt{fail}^{x,\widetilde{y}}$

$$
\begin{aligned}
[\![N]\!]^{\natural}_{u} &= [\![M[x_1,\cdots,x_k \leftarrow x]\ \langle\!\langle B/x \rangle\!\rangle]\!]^{\natural}_{u} \\
&= \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x)([\![M[x_1,\cdots,x_k \leftarrow x]]\!]^{\natural}_{u} \mid [\![B_i]\!]^{\natural}_{x}) \\
&= \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x)(x.\overline{\mathtt{some}}.\overline{x}(y_1).(y_1.\mathtt{some}_{\emptyset}; y_1.\mathtt{close}; \mathbf{0} \mid x.\overline{\mathtt{some}}; x.\mathtt{some}_{u,(\mathsf{fv}(M)\setminus x_1,\cdots,x_k)}; \\
&\quad x(x_1).\cdots x.\overline{\mathtt{some}}.\overline{x}(y_k).(y_k.\mathtt{some}_{\emptyset}; y_k.\mathtt{close}; \mathbf{0} \mid x.\overline{\mathtt{some}}; x.\mathtt{some}_{u,(\mathsf{fv}(M)\setminus x_k)}; x(x_k). \\
&\quad x.\overline{\mathtt{some}}; \overline{x}(y_{k+1}).(y_{k+1}.\mathtt{some}_{u,\mathsf{fv}(M)}; y_{k+1}.\mathtt{close}; [\![M]\!]^{\natural}_{u} \mid x.\overline{\mathtt{none}}))\cdots) \mid \\
&\quad x.\mathtt{some}_{\mathsf{fv}(B)}; x(y_1).x.\mathtt{some}_{y_1,\mathsf{fv}(B)}; x.\overline{\mathtt{some}}; \overline{x}(x_1).(x_1.\mathtt{some}_{\mathsf{fv}(B_i(1))}; [\![B_i(1)]\!]^{\natural}_{x_1} \\
&\quad \mid y_1.\overline{\mathtt{none}} \mid \cdots x.\mathtt{some}_{\mathsf{fv}(B_i(l))}; x(y_l).x.\mathtt{some}_{y_l,\mathsf{fv}(B_i(l))}; x.\overline{\mathtt{some}}; \overline{x}(x_l).(x_l.\mathtt{some}_{\mathsf{fv}(B_i(l))}; \\
&\quad [\![B_i(l)]\!]^{\natural}_{x_l} \mid y_l.\overline{\mathtt{none}} \mid x.\mathtt{some}_{\emptyset}; x(y_{l+1}).(y_{l+1}.\overline{\mathtt{some}}; y_{l+1}.\overline{\mathtt{close}} \mid x.\mathtt{some}_{\emptyset}; x.\overline{\mathtt{none}}))))) \\
&\longrightarrow^{5l} \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x, y_1, x_1, \cdots y_l, x_l)(y_1.\mathtt{some}_{\emptyset}; y_1.\mathtt{close}; \mathbf{0} \mid \cdots \mid y_l.\mathtt{some}_{\emptyset}; y_l.\mathtt{close}; \mathbf{0} \\
&\quad x.\overline{\mathtt{some}}.\overline{x}(y_{l+1}).(y_{l+1}.\mathtt{some}_{\emptyset}; y_{l+1}.\mathtt{close}; \mathbf{0} \mid x.\overline{\mathtt{some}}; x.\mathtt{some}_{u,(\mathsf{fv}(M)\setminus x_{l+1},\cdots,x_k)}; \\
&\quad x(x_{l+1}).\cdots x.\overline{\mathtt{some}}.\overline{x}(y_k).(y_k.\mathtt{some}_{\emptyset}; y_k.\mathtt{close}; \mathbf{0} \mid x.\overline{\mathtt{some}}; x.\mathtt{some}_{u,(\mathsf{fv}(M)\setminus x_k)}; x(x_k). \\
&\quad x.\overline{\mathtt{some}}; \overline{x}(y_{k+1}).(y_{k+1}.\mathtt{some}_{u,\mathsf{fv}(M)}; y_{k+1}.\mathtt{close}; [\![M]\!]^{\natural}_{u} \mid x.\overline{\mathtt{none}}))\cdots) \mid \\
&\quad x_1.\mathtt{some}_{\mathsf{fv}(B_i(1))}; [\![B_i(1)]\!]^{\natural}_{x_1} \mid \cdots \mid x_l.\mathtt{some}_{\mathsf{fv}(B_i(l))}; [\![B_i(l)]\!]^{\natural}_{x_l} \mid \\
&\quad y_1.\overline{\mathtt{none}} \mid \cdots \mid y_l.\overline{\mathtt{none}} \\
&\quad x.\mathtt{some}_{\emptyset}; x(y_{l+1}).(y_{l+1}.\overline{\mathtt{some}}; y_{l+1}.\overline{\mathtt{close}} \mid x.\mathtt{some}_{\emptyset}; x.\overline{\mathtt{none}})) \\
&\longrightarrow^{l+5} \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x, x_1, \cdots, x_l)(x.\mathtt{some}_{u,(\mathsf{fv}(M)\setminus x_{l+1},\cdots,x_k)}; x(x_{l+1}).\cdots \\
&\quad x.\overline{\mathtt{some}}.\overline{x}(y_k).(y_k.\mathtt{some}_{\emptyset}; y_k.\mathtt{close}; \mathbf{0} \mid x.\overline{\mathtt{some}}; x.\mathtt{some}_{u,(\mathsf{fv}(M)\setminus x_k)}; x(x_k). \\
&\quad x.\overline{\mathtt{some}}; \overline{x}(y_{k+1}).(y_{k+1}.\mathtt{some}_{u,\mathsf{fv}(M)}; y_{k+1}.\mathtt{close}; [\![M]\!]^{\natural}_{u} \mid x.\overline{\mathtt{none}})) \mid \\
&\quad x_1.\mathtt{some}_{\mathsf{fv}(B_i(1))}; [\![B_i(1)]\!]^{\natural}_{x_1} \mid \cdots \mid x_l.\mathtt{some}_{\mathsf{fv}(B_i(l))}; [\![B_i(l)]\!]^{\natural}_{x_l} \mid x.\overline{\mathtt{none}}) \\
&\longrightarrow \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x_1, \cdots, x_l)(u.\overline{\mathtt{none}} \mid x_1.\overline{\mathtt{none}} \mid \cdots \mid x_l.\overline{\mathtt{none}} \mid (\mathsf{fv}(M) \setminus \{x_1,\cdots,x_k\}).\overline{\mathtt{none}} \mid \\
&\qquad x_1.\mathtt{some}_{\mathsf{fv}(B_i(1))}; [\![B_i(1)]\!]^{\natural}_{x_1} \mid \cdots \mid x_l.\mathtt{some}_{\mathsf{fv}(B_i(l))}; [\![B_i(l)]\!]^{\natural}_{x_l}) \\
&\longrightarrow^{l} \bigoplus_{B_i \in \mathsf{PER}(B)} u.\overline{\mathtt{none}} \mid (\mathsf{fv}(M) \setminus \{x_1,\cdots,x_k\}).\overline{\mathtt{none}} \mid \mathsf{fv}(B).\overline{\mathtt{none}} \\
&= Q_{7l+6}
\end{aligned}
$$

Figure 22: Reductions of an encoded explicit substitution that leads to failure

$$
\begin{aligned}
[\![\mathbb{N}]\!]^{\natural}_{u} &= (\nu x)([\![M]\!]^{\natural}_{u} \mid x.\mathtt{some}_{\mathsf{fv}(N')}; [\![N']\!]^{\natural}_{x}) \\
&= (\nu x)([\![\mathtt{fail}^{x,\widetilde{y}}]\!]^{\natural}_{u} \mid x.\mathtt{some}_{\mathsf{fv}(N')}; [\![N']\!]^{\natural}_{x}) \\
&= (\nu x)(u.\overline{\mathtt{none}} \mid x.\overline{\mathtt{none}} \mid \widetilde{y}.\overline{\mathtt{none}} \mid x.\mathtt{some}_{\mathsf{fv}(N')}; [\![N']\!]^{\natural}_{x}) \\
&\longrightarrow u.\overline{\mathtt{none}} \mid \widetilde{y}.\overline{\mathtt{none}} \mid \mathsf{fv}(N').\overline{\mathtt{none}}
\end{aligned}
$$

Notice that no further reductions can be performed.

Thus,

$$[\![\mathbb{N}]\!]^{\not\zeta}_u \longrightarrow u.\overline{\texttt{none}} \mid \widetilde{y}.\overline{\texttt{none}} \mid \mathsf{fv}(N').\overline{\texttt{none}} = Q'.$$

We also have that

$$\mathbb{N} \longrightarrow \texttt{fail}^{\widetilde{y}\cup\mathsf{fv}(N')} = \mathbb{N}' \text{ and } [\![\texttt{fail}^{\widetilde{y}\cup\mathsf{fv}(N')}]\!]^{\not\zeta}_u = Q',$$

and the result follows.

(B) $\mathsf{head}(M) = x$

By the diamond property (Proposition 3.10) we will be reducing each non-deterministic choice of a process simultaneously. Then by Proposition 5.29 we have the following:

$$\begin{aligned}
[\![\mathbb{N}]\!]^{\not\zeta}_u &\longrightarrow^* (\nu x)(\bigoplus_{i\in I}(\nu\widetilde{y})([\![x]\!]^{\not\zeta}_j \mid P_i) \mid x.\texttt{some}_{\mathsf{fv}(N')}; [\![N']\!]^{\not\zeta}_x) \\
&= (\nu x)(\bigoplus_{i\in I}(\nu\widetilde{y})(x.\overline{\texttt{some}}; [x \leftrightarrow j] \mid P_i) \mid x.\texttt{some}_{\mathsf{fv}(N')}; [\![N']\!]^{\not\zeta}_x) \\
&\longrightarrow (\nu x)(\bigoplus_{i\in I}(\nu\widetilde{y})([x \leftrightarrow j] \mid P_i) \mid [\![N']\!]^{\not\zeta}_x) && = Q_1 \\
&\longrightarrow \bigoplus_{i\in I}(\nu\widetilde{y})([\![N']\!]^{\not\zeta}_j \mid P_i) && = Q_2
\end{aligned}$$

We also have that

$$\mathbb{N} = M\langle\!\langle N'/x \rangle\!\rangle \longrightarrow M\{\!|N'/x|\!\} = \mathbb{M}'.$$

where by Proposition 5.29 we obtain

$$[\![M\{\!|N'/x|\!\}]\!]^{\not\zeta}_u \longrightarrow^* \bigoplus_{i\in I}(\nu\widetilde{y})([\![N']\!]^{\not\zeta}_j \mid P_i) = Q_2.$$

and finally from Proposition 5.29 there exists an $\mathbb{M}$ with $\mathbb{M} \equiv_\lambda \mathbb{M}'$ such that:

$$[\![\mathbb{M}]\!]^{\not\zeta}_u = \bigoplus_{i\in I}(\nu\widetilde{y})([\![N']\!]^{\not\zeta}_j \mid P_i) \quad = Q_2.$$

for simplicity we assume that $[\![\mathbb{N}]\!]^{\not\zeta}_u \longrightarrow Q_1$

(i) $n = 1$: Then $Q = Q_1$ and $[\![\mathbb{N}]\!]^{\not\zeta}_u \longrightarrow^1 Q_1$. Since, $Q_1 \longrightarrow^1 Q_2 = Q'$, $\mathbb{N} \longrightarrow^1 M\{\!|N'/x|\!\} \equiv_\lambda \mathbb{M} = \mathbb{N}'$ and $[\![\mathbb{M}]\!]^{\not\zeta}_u = Q_2$, the result follows.

(ii) $n \geq 2$: Then, $[\![\mathbb{N}]\!]^{\not\zeta}_u \longrightarrow^2 Q_2 \longrightarrow^l Q$, for $l \geq 0$. Also, $\mathbb{N} \to \mathbb{M}$, $Q_2 = [\![\mathbb{M}]\!]^{\not\zeta}_u$. By the IH there exist Q' and $\mathbb{N}'$ such that $Q \longrightarrow^i Q'$, $\mathbb{M} \longrightarrow^j_{\equiv_\lambda} \mathbb{N}'$ and $[\![\mathbb{N}']\!]^{\not\zeta}_u = Q'$. Finally, $[\![\mathbb{N}]\!]^{\not\zeta}_u \longrightarrow^2 Q_2 \longrightarrow^l Q \longrightarrow^i Q'$ and $\mathbb{N} \to \mathbb{M} \longrightarrow^j_{\equiv_\lambda} \mathbb{N}'$, and the result follows.

(II) For $m \geq 1$ and $n \geq 0$.

(A) $n = 0$:

Then,

$$(\nu x)(R \mid x.\texttt{some}_{\mathsf{fv}(N')}; [\![N']\!]^{\not\zeta}_x) = Q \text{ and } [\![M]\!]^{\not\zeta}_u \longrightarrow^m R.$$

By the IH there exist R' and $\mathbb{M}'$ such that $R \longrightarrow^{i} R'$, $M \longrightarrow^{j}_{\equiv_\lambda} \mathbb{M}'$ and $[\![\mathbb{M}']\!]^{\not\zeta}_{u} = R'$. Hence,

$$[\![\mathbb{N}]\!]^{\not\zeta}_{u} = (\nu x)([\![M]\!]^{\not\zeta}_{u} \mid x.\mathtt{some}_{\mathsf{fv}(N')}; [\![N']\!]^{\not\zeta}_{x}) \longrightarrow^{m} (\nu x)(R \mid x.\mathtt{some}_{\mathsf{fv}(N')}; [\![N']\!]^{\not\zeta}_{x}) = Q.$$

Also,

$$Q \longrightarrow^{i} (\nu x)(R' \mid x.\mathtt{some}_{\mathsf{fv}(N')}; [\![N']\!]^{\not\zeta}_{x}) = Q'$$

and the term can reduce as follows:
$\mathbb{N} = M\langle\!\langle N'/x \rangle\!\rangle \longrightarrow^{j}_{\equiv_\lambda} \sum_{M'_i \in \mathbb{M}'} M'_i\langle\!\langle N'/x \rangle\!\rangle = \mathbb{N}'$ and $[\![\mathbb{N}']\!]^{\not\zeta}_{u} = Q'$.

(B) When $n \geq 1$
Then R has an occurrence of an unguarded $x.\overline{\mathtt{some}}$ or $x.\overline{\mathtt{none}}$, and the case follows by IH. □

D.3. **Success Sensitiveness.**

Proposition 5.37 (Preservation of Success)**.** *The ✓ at the head of a partially open term is preserved to an unguarded occurrence of ✓ when applying the translation $[\![\cdot]\!]^{\not\zeta}_{u}$ up to reductions and vice-versa. That is to say:*

(1) $\forall M \in \widehat{\lambda}^{\not\zeta}_{\oplus}$: $\quad \mathsf{head}(M) = ✓ \implies [\![M]\!]^{\not\zeta}_{u} \longrightarrow^{*} (P \mid ✓) \oplus Q$
(2) $\forall M \in \widehat{\lambda}^{\not\zeta}_{\oplus}$: $\quad [\![M]\!]^{\not\zeta}_{u} = (P \mid ✓) \oplus Q \implies \mathsf{head}(M) = ✓$

Proof. In both cases, by induction on the structure of M.

(1) We only need to consider terms of the following form:
- $M = ✓$.
  This case is immediate.
- $M = N\ B$.
  By definition, $\mathsf{head}(N\ B) = \mathsf{head}(N)$. Hence we consider that $\mathsf{head}(N) = ✓$. Then,

$$[\![N\ B]\!]^{\not\zeta}_{u} = \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)([\![N]\!]^{\not\zeta}_{v} \mid v.\mathtt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([v \leftrightarrow u] \mid [\![B_i]\!]^{\not\zeta}_{x}))$$

  and by the IH ✓ is unguarded in $[\![N]\!]^{\not\zeta}_{u}$ after a sequence of reductions.
- $M = (N[\widetilde{x} \leftarrow x])\langle\!\langle B/x \rangle\!\rangle$.
  By definition, $\mathsf{head}((N[\widetilde{x} \leftarrow x])\langle\!\langle B/x \rangle\!\rangle) = \mathsf{head}(N[\widetilde{x} \leftarrow x]) = \mathsf{head}(N) = ✓$ where $\widetilde{x} = x_1, \cdots, x_k$ and $\#(x, M) = \mathsf{size}(B)$.

$$[\![(N[\widetilde{x} \leftarrow x])\langle\!\langle B/x \rangle\!\rangle]\!]^{\not\zeta}_{u} = \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x)([\![N[\widetilde{x} \leftarrow x]]\!]^{\not\zeta}_{u} \mid [\![B_i]\!]^{\not\zeta}_{x}) \longrightarrow^{*} \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu \widetilde{x})([\![N]\!]^{\not\zeta}_{u} \mid x_1.\mathtt{some}_{\mathsf{fv}(B_i(1))}; [\![B_i(1)]\!]^{\not\zeta}_{x_1} \mid \cdots \mid x_k.\mathtt{some}_{\mathsf{fv}(B_i(k))}; [\![B_i(k)]\!]^{\not\zeta}_{x_k})$$

  and by the IH ✓ is unguarded in $[\![N]\!]^{\not\zeta}_{u}$ after a sequence of reductions.

- $M = M'\langle\!\langle N/x \rangle\!\rangle$.
  By definition, $\mathsf{head}(M'\langle\!\langle N/x \rangle\!\rangle) = \mathsf{head}(M')\checkmark$. Then,
  $$[\![M'\langle\!\langle N/x \rangle\!\rangle]\!]^{\lightning}_u = (\nu x)([\![M']\!]^{\lightning}_u \mid x.\mathtt{some}_{\mathsf{fv}(N)}; [\![N]\!]^{\lightning}_x)$$
  and by the IH $\checkmark$ is unguarded in $[\![N]\!]^{\lightning}_u$.

(2) We only need to consider terms of the following form:
- $M = \checkmark$.
  This case is trivial.
- $M = N\ B$.
  Then,
  $$[\![N\ B]\!]^{\lightning}_u = \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu v)([\![N]\!]^{\lightning}_v \mid v.\mathtt{some}_{u,\mathsf{fv}(B)}; \overline{v}(x).([v \leftrightarrow u] \mid [\![B_i]\!]^{\lightning}_x)).$$
  The only occurrence of an unguarded $\checkmark$ is within $[\![N]\!]^{\lightning}_v$. By the IH we have that $\mathsf{head}(N) = \checkmark$ and finally $\mathsf{head}(N\ B) = \mathsf{head}(N)$.
- $M = (N[\widetilde{x} \leftarrow x])\langle\!\langle {}^{B}/_{x} \rangle\!\rangle$.
  Then,
  $$[\![(N[\widetilde{x} \leftarrow x])\langle\!\langle {}^{B}/_{x} \rangle\!\rangle]\!]^{\lightning}_u = \bigoplus_{B_i \in \mathsf{PER}(B)} (\nu x)([\![N[\widetilde{x} \leftarrow x]]\!]^{\lightning}_u \mid [\![B_i]\!]^{\lightning}_x)$$
  However in both $[\![N[\widetilde{x} \leftarrow x]]\!]^{\lightning}_u$ and $[\![B_i]\!]^{\lightning}_x$ we have that both are guarded and hence $\checkmark$ cannot occur without synchronizations.
- $M = M'\langle\!\langle N/x \rangle\!\rangle$.
  Then,
  $$[\![M'\langle\!\langle N/x \rangle\!\rangle]\!]^{\lightning}_u = (\nu x)([\![M']\!]^{\lightning}_u \mid x.\mathtt{some}_{\mathsf{fv}(N)}; [\![N]\!]^{\lightning}_x),$$
  an unguarded occurrence of $\checkmark$ can only occur within $[\![M']\!]^{\lightning}_u$. By the IH we have $\mathsf{head}(M') = \checkmark$ and hence $\mathsf{head}(M'\langle\!\langle N/x \rangle\!\rangle) = \mathsf{head}(M')$. □

Theorem 5.38 (Success Sensitivity)**.** *Let $\mathbb{M}$ be a closed well-formed $\widehat{\lambda}^{\lightning}_{\oplus}$-expression. Then,*
$$\mathbb{M} \Downarrow_{\checkmark} \iff [\![\mathbb{M}]\!]^{\lightning}_u \Downarrow_{\checkmark} .$$

Proof. We proceed with the proof in two parts.

(1) Suppose that $\mathbb{M} \Downarrow_{\checkmark}$. We will prove that $[\![\mathbb{M}]\!]^{\lightning} \Downarrow_{\checkmark}$.
  By Def. 5.11, there exists $\mathbb{M}' = M_1 + \cdots + M_k$ such that $\mathbb{M} \longrightarrow^* \mathbb{M}'$ and with $\mathsf{head}(M_j) = \checkmark$, for some $j \in \{1, \ldots, k\}$. By completeness there exists Q such that $[\![\mathbb{M}]\!]^{\lightning}_u \longrightarrow^* Q = [\![\mathbb{M}']\!]^{\lightning}_u$.
  We wish to show that there exists Q' such that $Q \longrightarrow^* Q'$ and Q' has an unguarded occurrence of $\checkmark$.
  Since $Q = [\![\mathbb{M}']\!]^{\lightning}_u$ and due to compositionality and the homormorphic preservation of non-determinism, we have that
  $$Q = [\![M_1]\!]^{\lightning}_u \oplus \cdots \oplus [\![M_k]\!]^{\lightning}_u$$
  By Proposition 5.37 (1) we have that
  $$\mathsf{head}(M_j) = \checkmark \implies [\![M_j]\!]^{\lightning}_u \longrightarrow^* (P \mid \checkmark) \oplus Q''$$
  for some Q''. Hence, $Q \longrightarrow^* (P \mid \checkmark) \oplus Q'' = Q'$, as wanted.

(2) Suppose that $[\![\mathbb{M}]\!]_u^{\not\downarrow} \Downarrow_{\checkmark}$. We will prove that $\mathbb{M} \Downarrow_{\checkmark}$.

By operational soundness (Theorem 5.33): if $[\![\mathbb{N}]\!]_u^{\not\downarrow} \longrightarrow^* Q$ then there exist Q' and $\mathbb{N}'$ such that $Q \longrightarrow^* Q'$, $\mathbb{N} \longrightarrow^*_{\equiv_\lambda} \mathbb{N}'$ and $[\![\mathbb{N}']\!]_u^{\not\downarrow} = Q'$. Since $[\![\mathbb{M}]\!]_u^{\not\downarrow} \longrightarrow^* P_1 \oplus \ldots \oplus P_k$, and $P_j = P_j'' \mid \checkmark$, for some j.

Notice that if $[\![\mathbb{M}]\!]_u^{\not\downarrow}$ is itself a term with unguarded $\checkmark$, say $[\![\mathbb{M}]\!]_u^{\not\downarrow} = P \mid \checkmark$, then $\mathbb{M}$ is itself headed with $\checkmark$, from Proposition 5.13 (2).

In the case $[\![\mathbb{M}]\!]_u^{\not\downarrow} = P_1 \oplus \ldots \oplus P_k$, $k \geq 2$, and $\checkmark$ occurs unguarded in an P_j, The encoding acts homomorphically over sums and the reasoning is similar. We have that $P_j = P_j' \mid \checkmark$ we apply Proposition 5.13 (2). □