On the Coincidence of Observational Equivalence and Labeled Bisimilarity in Applied Pi Calculus

Jia Liu
State Key Laboratory of Computer Science
Institute of Software Chinese Academy of Sciences
jliu@ios.ac.cn

1 Introduction

The applied pi calculus was introduced in [1] where two notions of equivalences, observational equivalence and labeled bisimilarity, are defined. A main result of the paper, Theorem 1, states that the two equivalences coincide. But the paper does not provide a proof for the theorem.

After the publication of the paper a counterexample to the theorem has been noted:

Let $A_r = \nu c. (c.a | \{c/x\})$ and $B_r = \nu c. (0 | \{c/x\})$. Obviously $A_r$ and $B_r$ are labeled bisimilar since their frames are the same and both have no transitions. However, they are not observational equivalence since for the context $x(y)$, $A_r | x(y) \Downarrow a$ but $B_r | x(y) \not\Downarrow a$.

However, this problem can be fixed by requiring active substitutions be defined on the base sort only (see, for instance, [2]).

The purpose of this note is to supply a proof for the theorem. In the original semantics in [1], the use of structural equivalence introduces the nondeterminism, which makes it difficult to write a rigorous proof. To overcome the difficulty we shall use intermediate semantics, originally proposed in [2] for symbolic semantics, as a bridge. Intermediate representation is aim to simply the rules for structural equivalence as much as possible, while keep the bisimilarity. Four equivalences will be discussed:

1. Observational Equivalence $\approx$
2. Labeled Bisimilarity $\approx_l$
3. Intermediate Observational Equivalence $\approx_i$
4. Intermediate Labeled Bisimilarity $\approx_{l,i}$

To show $\approx_l$ coincides with $\approx$, the proof is divided into three steps:

1. $\approx_l$ coincides with $\approx_{l,i}$ (Theorem 5.1 in Section 5)
2. $\approx_i$ coincides with $\approx$ (Theorem 6.2 and Theorem 6.3 in Section 6)
3. $\approx_{l,i}$ coincides with $\approx_i$ (Corollary 7.2 and Theorem 7.2 in Section 7)

To make the note self-contained, Sections 2, 3, 4, A and 5 are almost quoted from [3] (Section 2, Appendix A, Subsection 2.3, Section 2 and Appendix B.1 respectively).

The outline of the note is as follows: applied pi calculus and its semantics is reviewed in the following section. Section 3 introduces an alternative characterisation of the semantics, while Section 4 presents the intermediate representation. We study some properties of renamings in Section A. Section 5 states that intermediate labeled bisimilarity coincides with labeled bisimilarity. Section 6 states that intermediate observational equivalence coincides with observational equivalence. Section 7 states that intermediate observational equivalence coincides with intermediate labeled bisimilarity.
2 Applied Pi Calculus

2.1 syntax

We assume two disjoint, infinite sets \( N \) and \( V \) of names and variables, respectively. A signature is a finite set of function symbols, ranged over by \( f, g, h, enc, dec \), each having a non-negative arity. A function symbol with arity 0 is a constant symbol. Terms, ranged over by \( M, N \), are built up from names and variables by function applications:

\[
M, N ::= \quad \text{terms} \\
\quad a, b, c, \ldots, k, \ldots, m, n, \ldots, s \quad \text{names} \\
\quad x, y, z \quad \text{variables} \\
\quad f(M_1, \ldots, M_k) \quad \text{function application}
\]

We write \( \text{vars}(M) \) and \( \text{names}(M) \) for the variables and names in \( M \), respectively, and let \( \text{atoms}(M) = \text{vars}(M) \cup \text{names}(M) \). A ground term is a term containing no variables.

We rely on a sort system including a universal base sort and channel sort. The sort system splits \( N \) and \( V \) respectively into channel names \( N_{ch} \) and base names \( N_b \), channel variables \( V_{ch} \) and base variables \( V_b \). Function symbols are required to take arguments and produce results of the base types only. Terms are required to be well-sorted. Hence the set of terms of channel sort contains channel names and channel variables only. We will use \( a, b, c, d \) as channel names, \( s, k \) as base names, and \( x, y, z \) as variables; meta variables \( u, v, w \) are used to range over both names and variables. Tuples such as \( u, \ldots, u, \) and \( M_1 \cdots M_r \) will be denoted by \( \bar{u} \) and \( M \), respectively.

Plain processes are constructed using the standard operators 0 (nil), | (parallel composition), vn (name restriction), if-then-else (conditional), \( u(x) \) (input), \( \pi(N) \) (output), and ! (replication). Extended processes are created by extending plain processes with active substitutions that float and apply to any process coming into contact with it. The grammar for plain processes and extended processes are given below:

\[
P_r, Q_r, R_r ::= \text{plain processes} \\
P_r | Q_r \\
\nu n.P_r \\
\nu M = N \text{ then } P_r \text{ else } Q_r \\
u(x).P_r \\
\pi(N).P_r
\]

\[
A_r, B_r, C_r ::= \text{extended processes} \\
A_r | B_r \\
\nu n.A_r \\
\nu x.A_r \\
\nu M = \text{names}(M).L
\]

As in the pi calculus, \( u(x), \nu n \) and \( \nu x \) are binding, which lead to the usual notions of bound and free names and variables. We shall use \( \text{fn}(A_r), \text{fv}(A_r), \text{bn}(A_r) \) and \( \text{bv}(A_r) \) to denote the sets of free names, free variables, bound names and bound variables, respectively, of \( A_r \). In particular \( \text{fn}(M/x) = \text{vars}(M) \cup \{x\} \) and \( \text{fv}(\{M/x\}) = \text{names}(M) \). Let \( \text{fnw}(A_r) = \text{fn}(A_r) \cup \text{fn}(A_r) \) and \( \text{bnw}(A_r) = \text{bn}(A_r) \cup \text{bn}(A_r) \). We shall identify processes which are \( \alpha \)-convertible. Captures of bound names and bound variables are avoided by implicit \( \alpha \)-conversion.

Substitutions are sort-respecting finite partial mappings. Substitutions of terms for variables, ranged over by \( \sigma, \theta \), are always required to be cycle-free. Applications of substitutions to expressions will be written in postfix notation. The application of substitution \( \sigma \) to substitution \( \{M_1/x_1, \cdots, M_n/x_n\} \) is defined componentwise: \( \{M_1/x_1, \cdots, M_n/x_n\}\sigma = \{M_1\sigma/x_1, \cdots, M_n\sigma/x_n\} \). The domain and range of a substitution are defined thus: \( \text{dom}(\sigma) = \{x \mid x \neq \sigma x\} \) and \( \text{range}(\sigma) = \{M \mid x \in \text{dom}(\sigma), x\sigma = M\} \), respectively. We write \( \text{vars}(\sigma) \) and \( \text{names}(\sigma) \) for the sets of variables and names occurring in \( \sigma \), respectively. Also let

\[1\] We use subscript “r” (for “raw”) to distinguish the original processes from the intermediate processes to be introduced in Subsection 4.
2.2 Semantics

\( \text{atoms}(\sigma) = \text{vars}(\sigma) \cup \text{names}(\sigma) \). We say \( \sigma \) is idempotent if \( \text{dom}(\sigma) \cap \text{vars}(\text{range}(\sigma)) = \emptyset \). The functional composing of two substitutions \( \sigma_1 \) and \( \sigma_2 \) is denoted \( \sigma_1 \circ \sigma_2 \), and \( \sigma^* \) is the result of composing \( \sigma \) with itself repeatedly until an idempotent substitution is reached. We denote by \( \sigma|_v \) the restriction of \( \sigma \) on a set \( V \) of variables and names. Note that \( \sigma_1 \sigma_2 \), which is the application of \( \sigma_2 \) to \( \sigma_1 \), is in general different from \( \sigma_1 \circ \sigma_2 \) and \( \sigma_2 \circ \sigma_1 \); but when \( \sigma_1 = \sigma_2 \), they are all equal. If \( \text{dom}(\sigma_1) \cap \text{dom}(\sigma_2) = \emptyset \) then \( \sigma_1 \cup \sigma_2 \) denotes the union of \( \sigma_1 \) and \( \sigma_2 \). We also write \( \sigma_1 \subseteq \sigma_2 \) if there exists a \( \sigma \) such that \( \sigma_1 \cup \sigma = \sigma_2 \).

Active substitutions are required to be defined on the base sort only, for otherwise the coincidence between labeled bisimilarity and observational equivalence, which is the main result (Theorem 1) of \([1]\), will not hold.

In an extended process, active substitutions must be cycle-free and there is at most one substitution for each variable and exactly one when the variable is restricted. A frame is an extended process built up from 0 and active substitutions by parallel composition and restriction. The domain of frame \( \phi \), denoted by \( \text{dom}(\phi) \), is the set of variables \( x \) for which \( \phi \) contains a substitution \( \{ M/x \} \) not under \( \nu x \). The frame of an extended process \( A_r \), denoted by \( \phi(A_r) \), is obtained by replacing every plain process in \( A_r \) with 0. The domain of an extended process \( A_r \), written \( \text{dom}(A_r) \), is defined as \( \text{dom}(\phi(A_r)) \). We say \( A_r \) is closed if every variable is either bound or defined by an active substitution.

A renaming \( \rho \) is a partial mapping which maps names to names and variables to variables, and \( \text{dom}(\rho) \) and \( \text{range}(\rho) \) are defined as expected. The application of a renaming to an expression is written in prefix notation. Different from substitutions, when a renaming is applied to an extended process \( A_r \), it may replace some variables in \( \text{dom}(A_r) \). For instance, \( \{ y/x \}(a(c).0 | \{ b/y \}) = a\langle c \rangle.0 | \{ b/y \} \). We write \( \rho|_v \) for the restriction of \( \rho \) on the set \( V \) of variables and names. Given a finite set \( \xi \subseteq \mathcal{N} \cup \mathcal{V} \), we say \( \rho \) is well-formed on \( \xi \) if \( \text{dom}(\rho) \subseteq \xi \) and for any \( u, v \in \xi, u \neq v \) implies \( \rho(u) \neq \rho(v) \).

2.2 Semantics

A context is an extended process with a hole and an evaluation context is a context in which the hole is not under a replication, an input, an output or a conditional. A term context is a term with holes. Terms are equipped with an equational theory \( =_e \) that is an equivalence relation closed under substitutions of terms for variables, one-to-one renamings and term contexts. Structural equivalence, \( \equiv \), is the smallest equivalence relation on extended processes closed by evaluation context and \( \alpha \)-conversion, and satisfies the rules in Fig. 1.

The labeled operational semantics is given in Fig. 1. We denote by \( \Rightarrow \) the reflexive and transitive closure of \( \xrightarrow{\alpha} \), and write \( \xrightarrow{\alpha} \) for \( \xrightarrow{\alpha} \Rightarrow \), and \( \xrightarrow{\alpha} \) for \( \xrightarrow{\alpha} \Rightarrow \) if \( \alpha \) is not \( \tau \) and \( \Rightarrow \) otherwise.

We write \( A_r \Downarrow_a \) when \( A_r \) can send a message on \( a \), that is, when \( A_r \Rightarrow C[\pi(M).P] \) for some evaluation context \( C \) that does not bind \( a \).

**Definition 2.1.** Observational equivalence (\( \simeq \)) is the largest symmetric relation \( \mathcal{R} \) between closed extended processes with the same domain such that \( A_r \mathcal{R} B_r \) implies:

1. if \( A_r \Downarrow_a \) then \( B_r \Downarrow_a \);
2. if \( A_r \Rightarrow A'_r \), then \( B_r \Rightarrow B'_r \) and \( A'_r \mathcal{R} B'_r \) for some \( B'_r \);
3. \( C[A_r] \mathcal{R} C[B_r] \) for all closing evaluation contexts \( C \).

Since output messages are accumulated in the form of active substitutions which may affect subsequent behaviors, we need a reasonable way to comparing the effects of such messages. To this end the notion of a static equivalence is introduced to ensure that two processes expose the same information to the environment.

**Definition 2.2.** Two terms \( M \) and \( N \) are equal in the frame \( \phi \), written \( (M = N)\phi \), iff \( \phi \equiv \nu \tilde{n}.\sigma, \{ \tilde{n} \} \cap \text{names}(M, N) = \emptyset \), and \( M\sigma =_e N\sigma \), for some names \( \tilde{n} \) and substitution \( \sigma \).
\[
\begin{align*}
\text{Par-0} & \quad A_r \equiv A_r \mid 0 \\
\text{Par-A} & \quad A_r \mid (B_r \mid C_r) \equiv (A_r \mid B_r) \mid C_r \\
\text{Par-C} & \quad A_r \mid B_r \equiv B_r \mid A_r \\
\text{Repl} & \quad !P_r \equiv P_r \mid !P_r \\
\text{New-0} & \quad \nu u.0 \equiv 0 \\
\text{New-C} & \quad \nu u.\nu v. A_r \equiv \nu v.\nu u. A_r \\
\text{New-Par} & \quad A_r \mid \nu u. B_r \equiv \nu u. (A_r \mid B_r) \text{ when } u \notin \text{fv}(A_r) \\
\text{Alias} & \quad \nu x. \{M/x\} \equiv 0 \\
\text{Subst} & \quad \{M/x\} \mid A_r \equiv \{M/x\} \mid A_r \{M/x\} \\
\text{Rewrite} & \quad \{M/x\} \equiv \{N/x\} \text{ when } M \equiv N \\
\text{Then} & \quad \text{if } M = M \text{ then } P_r \text{ else } Q_r, \tau \rightarrow P_r \\
\text{Else} & \quad \text{if } M = N \text{ then } P_r \text{ else } Q_r, \tau \rightarrow Q_r \\
\text{Comm} & \quad \pi(M).P_r \mid a(x).Q_r \rightarrow P_r \mid Q_r \{M/x\} \\
\text{In} & \quad a(x).P_r \overset{a(M)}{\rightarrow} P_r \{M/x\} \\
\text{Out-Atom} & \quad \pi(u).P_r \overset{\pi(u)}{\rightarrow} P_r \text{ where } u \in N_{\text{lb}} \cup V_b \\
\text{Open-Atom} & \quad A_r \overset{\pi(u)}{\rightarrow} B_r, \quad a \neq u \\
\text{Scope} & \quad \nu u. A_r \overset{\pi(u)}{\rightarrow} \nu u. B_r, \quad u \text{ does not occur in } \alpha \\
\text{PAR} & \quad \text{bnv}(\alpha) \cap \text{fv}(B_r) = \emptyset \\
\text{STRUCT} & \quad A_r \equiv C_r \overset{\pi(A)}{\rightarrow} C_r' \equiv B_r \\
\end{align*}
\]

**Fig. 1.** Structural Equivalence and Labeled Transition Rules
Definition 2.3. Two closed frames \( \phi_1 \) and \( \phi_2 \) are statically equivalent, written \( \phi_1 \sim \phi_2 \), if \( \text{dom}(\phi_1) = \text{dom}(\phi_2) \), and for all terms \( M \) and \( N \) such that \( \text{vars}(M, N) \subseteq \text{dom}(\phi_1) \) we have \( (M = N) \phi_1 \), iff \( (M = N) \phi_2 \). Two closed extended processes \( A_r \) and \( B_r \) are statically equivalent, written \( A_r \sim B_r \), if their frames are.

Definition 2.4. Labeled bisimilarity \( (\approx_l) \) is the largest symmetric relation \( R \) on closed extended processes such that \( A_r R B_r \) implies:

1. \( A_r \sim B_r \)
2. if \( A_r \overset{\alpha}{\Rightarrow} A'_r \) and \( \text{fv}(\alpha) \subseteq \text{dom}(A_r) \) and \( \text{bn}(\alpha) \cap \text{fn}(B_r) = \emptyset \) then \( B_r \overset{\alpha}{\Rightarrow} B'_r \) and \( A'_r R B'_r \) for some \( B'_r \).

The following theorem is what we want to prove in this note:

Theorem 2.1. \( \approx \) coincides with \( \approx_l \).

3 An Alternative Semantics

The operational semantics of the applied pi calculus relies heavily on structural equivalence. This is because the analysis of complex data and “alias” mechanism introduced in the calculus depends on structural equivalence rules such as \text{SUBST} and \text{REWRITE} (see Fig. 1). However, structural equivalence makes it difficult to develop a proof for the coincidence between observational equivalence and labeled bisimilarity, as it introduces the nondeterminism. Thus, as a first step, similar to [2], we need to preprocess the original semantics in Fig. 1 and rewrite it to a more convenient form while preserving bisimilarity. In this section we replace the structural equivalence and transition rules in Fig. 1 with the rules in Fig. 2. The main change is replacing the two-directional rule \( !P_r \equiv P_r \parallel P_r \) with the one-directional \( !P_r \rightarrowrightarrow P_r \parallel P_r \). The rules \text{THEN}, \text{REP} and \text{OUTT} in Fig. 2 do not occur in Fig. 1. We shall show that the notions of labeled bisimilarities generated by the two sets of rules are exactly the same (Theorem 3.1), and also the observational equivalence.

In order to avoid confusion, in the following discussions we shall use \( \equiv_r, \rightarrowrightarrow_r, \rightarrowrightarrow_r, \sim_r, \approx_l \) and \( \approx_r \) to refer to structural equivalence, (strong and weak) transitions, static equivalence, labeled bisimilarity and observational equivalence respectively, defined in Section 2; and use \( \equiv, \rightarrowrightarrow, \rightarrowrightarrow, \sim, \approx \) and \( \approx_r \) for the corresponding ones defined by Fig. 2 here. To prove that \( \approx_l \) coincides with \( \approx \), and \( \approx_r \) coincides with \( \approx \), we need to construct bisimulations and explore the relationship between \( \rightarrowrightarrow_r \) and \( \rightarrowrightarrow_r \). Their transformations are mainly formalized by the following Lemma 3.2 and Lemma 3.3.

We write \( A_r \geq B_r \) if \( A_r \) can be transformed to \( B_r \) by applying to a subterm (which is not under a replication, an input, an output or a conditional) of \( A_r \) an axiom of structural equivalence \( \equiv \), other than \( !P_r \equiv P_r \parallel P_r \) from right to left; we write \( \geq \) for the reflexive and transitive closure of \( \geq \). We say a sequence \( A_1^1 \geq \cdots \geq A_1^r \) is a linear proof sequence of \( A_1^1 \rightarrowrightarrow A_1^r \).

There are only four inference rules with non-empty premises in the labelled transition rules in Fig. 1, namely \text{PAR}, \text{OPEN-ATOM}, \text{SCOPE} and \text{STRUCT}. Since each of the rules \text{PAR}, \text{OPEN-ATOM} and \text{SCOPE} commutes with \text{STRUCT}, and that two applications of \text{STRUCT} can be condensed to one, we can always obtain a derivation for any transition in which the application of \text{STRUCT} occurs only once and at the last step. We shall call such a derivation a normalized derivation.

For \( n \geq 1 \), an \( n \)-hole evaluation context \( C \) is an extended process with \( n \) holes which are not under a replication, an input, an output or a conditional. We write \( C[A_1^1, A_1^2, \cdots, A_1^n] \) for the extended process obtained by filling the holes with processes.

Lemma 3.1. Assume \( A_r \geq B_r \) and \( A_r = C[|P_r|] \) with \( C \) an evaluation context. Then there exist an evaluation context \( C' \) and a plain process \( Q_r \) such that \( B_r = C'[|Q_r|] \) and \( C[P_r \parallel |P_r|] \geq C'[Q_r \parallel |Q_r|] \).
\[
A_r \equiv A_r \mid 0 \\
A_r \mid B_r \equiv B_r \mid A_r \\
A_r \mid (B_r \mid C_r) \equiv (A_r \mid B_r) \mid C_r
\]

\[
\nu x. \{M/x\} \equiv 0 \\
\{M/x\} \equiv \{N/x\} \quad \text{when } M =_E N \\
\nu u. \nu v. A_r \equiv \nu v. \nu u. A_r \\
\{M/x\} \mid A_r \equiv \{M/x\} \mid A_r \{M/x\} \\
A_r \mid \nu u. B_r \equiv \nu u. (A_r \mid B_r)
\]

when \( u \notin \text{fv}(A_r) \)

\begin{align*}
\text{Comm} & \quad \pi(A) . P_r \mid a(x). Q_r \xrightarrow{\tau} P_r \mid Q_r \{M/x\} \\
\text{Then} & \quad \text{if } M = N \text{ then } P_r \text{ else } Q_r \xrightarrow{\tau} P_r \quad \text{if } M =_E N \\
\text{Else} & \quad \text{if } M = N \text{ then } P_r \text{ else } Q_r \xrightarrow{\tau} Q_r \\
& \quad \text{if } M, N \text{ are ground terms and } M \neq_E N
\end{align*}

\begin{align*}
\text{Rep} & \quad \lnot P_r \xrightarrow{\tau} P_r \parallel P_r \\
\text{In} & \quad a(x). P_r \xrightarrow{a(M)} P_r \{M/x\}
\end{align*}

\begin{align*}
\text{Outch} & \quad \pi(c). P_r \xrightarrow{\pi(c)} P_r \\
\text{Out} & \quad \pi(M). P_r \xrightarrow{\nu x. \pi(x)} P_r \{M/x\} \quad \text{where } x \in V_b \text{ and } x \notin \text{fv}(\pi(M). P_r)
\end{align*}

\begin{align*}
\text{Opench} & \quad \frac{A_r \xrightarrow{\nu c. A_r} B_r \quad a \neq c}{\nu c. A_r \xrightarrow{\nu c. \pi(c)} B_r} \\
\text{Scope} & \quad \frac{A_r \xrightarrow{\nu c. A_r} B_r \quad u \text{ does not occur in } \alpha}{\nu u. A_r \xrightarrow{\nu u. B_r}}
\end{align*}

\begin{align*}
\text{Par} & \quad \frac{A_r \xrightarrow{\nu c. A_r} A_r' \quad \text{bnv}(\alpha) \cap \text{fv}(B_r) = \emptyset}{A_r \mid B_r \xrightarrow{\nu c. A_r} A_r' \mid B_r}
\end{align*}

\begin{align*}
\text{Struct} & \quad \frac{A_r \equiv C_r \xrightarrow{\alpha} D_r \equiv B_r}{A_r \xrightarrow{\alpha} B_r}
\end{align*}

Fig. 2. Structural Equivalence and Transition Rules
Proof. By induction on the length of the linear proof sequence for $\succ$. If the length is 0, the result holds immediately. Now assume $A_r \succ 1 \ A_r' \succ 1 \ A_r'' \succ 1 \ A_r^{\ell+1} = B_r$. By the induction hypothesis there exist a plain process $R_r$ and an evaluation context $C'''$ such that
\[ A_r' = C'''[R_r] \quad C[P_r || P_r] \succ C'''[R_r || R_r]. \tag{1} \]

We argue by case analysis on the axiom used in deriving $A_r' \succ 1 \ A_r^{\ell+1}$. We give the details only for two cases when $\succ$ is Rewrite and Subst. The other cases are similar.

1. $A_r' = C'''[\{M/x\}] \succ 1 \ C'''[\{N/x\}] = A_r^{\ell+1}$ with $M = _x N$. Since there is no way that active substitution $\{M/x\}$ can occur inside replications, it is easy to see that there exists a two-hole evaluation context $D$ such that $A_r' = D[R_r, \{M/x\}]$, $D[R_r, \{N/x\}] = C'''$ and $D[\cdot, \{M/x\}] = C''$. Using the Rewrite axiom, we know that $D[R_r || R_r, \{M/x\}] \succ 1 D[R_r || R_r, \{N/x\}]$. Let $C'' = D[\cdot, \{N/x\}]$ and $Q_r = R_r$. Clearly $A_r^{\ell+1} = C''[Q_r]$. Hence $C[P_r || P_r] \succ C''[R_r || R_r] \succ 1 C''[Q_r || Q_r]$ and the result holds.

2. (a) $A_r' = C'''[E_r \{M/x\}] \succ 1 \ C'''[E_r \{M/x\}] \succ 1 \ C''[\{M/x\}] = A_r^{\ell+1}$. Since the hole in any evaluation context has no chance to occur under any replication, $!R_r$ in (1) should occur in either $E_r$ or $C'''$.

The analysis for the latter case is similar to the above case. Now we consider the former case. Here there exists an evaluation context $D$ such that $E_r = D[R_r]$ and $C''[D[\cdot] || \{M/x\}] = C''$.

The substitution $\{M/x\}$ will apply to $D$ and $R_r$ while rewriting $A_r' \rightarrow A_r^{\ell+1}$. Let $D' = D[M/x]$ and $Q_r = R_r[M/x]$. We can easily see that $A_r^{\ell+1} = C'''[D'[\{Q_r\}] || \{M/x\}]$ and $C'''[D'[R_r] || R_r] || \{M/x\}]$. Let $C'' = C''[D'[\cdot] || \{M/x\}]$. Then $A_r^{\ell+1} = C''[Q_r]$ and $C[P_r || P_r] \succ C''[R_r || R_r] \succ C''[Q_r || Q_r]$.

(b) $A_r' = C'''[E_r \{M/x\}] \succ 1 \ C'''[E_r \{M/x\}] \succ 1 \ C''[\{M/x\}] = A_r^{\ell+1}$. When $!R_r$ in (1) occurs in $E_r[M/x]$, clearly there exist an evaluation context $D$ and a plain process $Q_r$ such that $E_r = D[Q_r]$ and $Q_r[M/x] = R_r$. The rest is similar to the above case.

3. $A_r' = C'''[P_r] \succ 1 \ C'''[P_r || P_r] = A_r^{\ell+1}$. When $!P_r$ is $!R_r$ in (1), the result holds trivially; otherwise $!R_r$ in (1) should occur in $C'''$ and the remaining analysis is similar.

Lemma 3.2. Assume $A_r \rightarrow_r A_r'$ where $A_r, A_r'$ are closed and $\alpha$ is not $\bar{\pi}(x)$ and $fv(\alpha) \subseteq dom(A_r)$. Then there exist closed $B_r, B_r'$ such that $A_r \rightarrow B_r \rightarrow B_r' \equiv A_r'$.

Proof. Consider the normalized derivation of transition $A_r \rightarrow_r A_r'$.

1. $\alpha$ is a $a(M)$. Then $A_r \equiv_r C[a(x).Q_r] \xrightarrow{a(M)} C[Q_r, \{M/x\}] \equiv_r A_r'$ with $C$ an evaluation context and $C[a(x).Q_r] \xrightarrow{a(M)} C[Q_r, \{M/x\}]$ derived by the rules in Fig. 1 without using $\equiv_r$.

We may assume $C[a(x).Q_r] \equiv_r C[Q_r, \{M/x\}]$ are both closed; for otherwise we can let $f = C[a(x).Q_r] - dom(C[a(x).Q_r]) = \{x_1, \ldots, x_n\}$ and choose $n$ fresh names $c_1, \ldots, c_n$ and let $\sigma = \{c_1/x_1, \ldots, c_n/x_n\}$. From the hypothesis, we know that $M\sigma = M, x \notin vars(\sigma)$, and $dom(A_r) = dom(C[a(x).P_r]) = dom(A_r')$. It is easy to see that $A_r = A_r \sigma \equiv_r C[X_\sigma][a(x).Q_r] \sigma \xrightarrow{a(M)} C[Q_r, \{M/x\}] = C\sigma[Q_r, \{M/x\}] \equiv_r A_r' \sigma \equiv A_r'$.

Since $C[a(x).Q_r] \xrightarrow{a(M)} C[Q_r, \{M/x\}]$ can be derived without using $\equiv_r$, $C[a(x).Q_r] \xrightarrow{a(M)} C[Q_r, \{M/x\}]$ can also be derived by rules in Fig. 2 without using $\equiv_r$. Thus $A_r \equiv_r C[a(x).Q_r] \xrightarrow{a(M)} C[Q_r, \{M/x\}] \equiv_r A_r'$. Now we proceed to construct the required $B_r$ and $B_r'$ as stated in the lemma. The rest of the proof goes by induction on the number of applications of $!P_r \equiv_r P_r || P_r$ to the proof sequence $A_r \equiv_r C[a(x).Q_r]$. If the number is 0, the result is immediate. So suppose the number is nonzero and consider the last application of $!P_r \equiv_r P_r || P_r$ from right to left (we write $\equiv_r$ for the application of an axiom of structural equivalence $\equiv_r$);

$$A_r \equiv_r C[P_r || P_r] \equiv_r C[|P_r|] = C[a(x).Q_r]$$
where $C'$ is also an evaluation context. From Lemma A.1, we know there exists $D'$ such that $C'[P_r \mid !P_r] \Rightarrow D'[R_r \mid !R_r]$ and $D'[R_r] = C[a(x), Q_r]$. Then there exists a two-hole evaluation context $D$ such that $D[R_r, !R_r] = C$ since $a(x), Q_r$ cannot occur inside the replication. Moreover $D[R_r, !R_r, a(x), Q_r] \xrightarrow{a(M)} D[R_r, !R_r, Q_r, \{M/x\}]$ can be derived by the rules in Fig. 2, and

$$A_r \equiv C'[P_r \mid !P_r] \Rightarrow D[R_r \mid !R_r, a(x), Q_r] \xrightarrow{a(M)} D[R_r \mid !R_r, Q_r, \{M/x\}] \equiv_r C[Q_r, \{M/x\}] \equiv_r A'_r.$$

Replacing $!R_r$ with $R_r$, $\mid !R_r$ does not introduce fresh variables. In other words $D[R_r \mid !R_r, a(x), Q_r]$ and $D[R_r \mid !R_r, Q_r, \{M/x\}]$ are also closed. By induction hypothesis, there exist closed $B_r, B'_r$ such that $A_r \Rightarrow B_r \xrightarrow{a(M)} B'_r \equiv_r A'_r$.

2. $\alpha$ is $\overline{\alpha}(c)$. Then $A_r \equiv_r C[\overline{\alpha}(c), Q_r] \xrightarrow{\overline{\alpha}(c)} C[Q_r] \equiv_r A'_r$ with $C$ an evaluation context. Clearly $C[\overline{\alpha}(c), Q_r] \xrightarrow{\overline{\alpha}(c)} C[Q_r]$. The rest of the proof is similar to the above case.

3. $\alpha = v_x \cdot \overline{\alpha}(x)$. Then $A_r \equiv_r v_x \cdot C[\overline{\alpha}(c), Q_r] \xrightarrow{v_x \cdot \overline{\alpha}(c)} C[Q_r] \equiv_r A'_r$ with $C$ an evaluation context. Clearly $v_x \cdot C[\overline{\alpha}(c), Q_r] \xrightarrow{v_x \cdot \overline{\alpha}(c)} C[Q_r]$. The rest of the proof is similar.

4. $\alpha = v_x \cdot \overline{\alpha}(x)$. Then $A_r \equiv_r v_x \cdot C[\overline{\alpha}(x), Q_r] \xrightarrow{v_x \cdot \overline{\alpha}(x)} C[Q_r] \equiv_r A'_r$ with $C$ an evaluation context. By the side-condition on extended process in Section 2.1, there is exactly one $\{M/x\}$ in $C$ for the restricted variable $x$. Thus there exists a two-hole evaluation context $D$ such that $C = D[\{M/x\}, \cdot]$. Since the side-condition for rule OUTT in Fig. 2 requires $x$ be fresh, we choose a fresh variable $y$ and let $g = \{y/x\}$. By $\alpha$-conversion, and structural equivalence $\equiv$, we can deduce that

$$v_x \cdot C[\overline{\alpha}(x), Q_r] = v_x \cdot D[\{M/x\}, \overline{\alpha}(x), Q_r] = v_y \cdot D[\{M/y\}, \overline{\alpha}(y), g(Q_r)]$$

$$v_x \cdot \overline{\alpha}(x) \xrightarrow{\overline{\alpha}(x)} v_y \cdot D[\{M/y\}, \overline{\alpha}(y), g(Q_r)]$$

$$\equiv v_y \cdot D[\{M/y\}, Q_r \mid \{y/x\}] \equiv \nu y \cdot D[\{M/y\} \mid \{y/x\}, Q_r]$$

$$\equiv \nu y \cdot D[\{M/y\} \mid \{M/x\}, Q_r] \equiv D[\nu y \cdot \{M/y\} \mid \{M/x\}, Q_r]$$

$$\equiv D[\{M/x\}, Q_r] = C[Q_r] \equiv_r A'_r.$$

5. $\alpha = \tau$. There are three cases:

(a) $A_r \equiv_r C$ if $M = M$ then $P_r$ else $Q_r$ $\xrightarrow{\tau} C[P_r] \equiv_r A'_r$ with $C$ an evaluation context.

(b) $A_r \equiv_r C$ if $M = N$ then $P_r$ else $Q_r$ $\xrightarrow{\tau} C[Q_r] \equiv_r A'_r$ with $M \neq N, M, N$ are ground terms and $C$ an evaluation context.

(c) $A_r \equiv_r C[\overline{\alpha}(M), P_r \mid a(x), Q_r] \xrightarrow{\tau} C[P_r \mid Q_r, \{M/x\}] \equiv_r A'_r$ with $C$ an evaluation context. The rest of the proof is similar.

Lemma 3.3. Assume $\alpha$ is not $\overline{\alpha}(x)$ and $A_r, A'_r$ are closed.

1. If $A_r \xrightarrow{\alpha} A'_r$ then there is a closed $A''_r$ such that $A_r \xrightarrow{\alpha} A''_r \equiv_r A'_r$.

2. If $A_r \xrightarrow{\alpha} A'_r$ then either $A_r \xrightarrow{\alpha} A''_r$ or $A_r \equiv_r A'_r$.

Proof. 1. Assume $A_r \xrightarrow{\alpha} A'_r$. By Lemma 3.2, there exist closed $B_r$ and $B'_r$ such that $A_r \Rightarrow B_r \xrightarrow{\alpha} B'_r \equiv_r A'_r$.

Replacing every left to right application of the rule $\overline{P_r} \equiv P_r \mid \overline{!P_r}$ in $A_r \Rightarrow B_r$ with $\overline{!P_r} \xrightarrow{\alpha} P_r \mid \overline{!P_r}$, we obtain $A_r \Rightarrow B_r \xrightarrow{\alpha} B'_r \equiv_r A'_r$. Letting $A''_r = B'_r$ gives the conclusion.

2. Assume $A_r \xrightarrow{\alpha} A'_r$ and apply transition induction.

(a) is $\alpha(M)$. Then $A_r \equiv C[a(x), P_r] \xrightarrow{a(M)} C[P_r \mid a(x)] \equiv A'_r$ where $C$ is an evaluation context.

Obviously we also have $A_r \xrightarrow{a(M)} A'_r$. 
(b) The cases for $\alpha$ is $\tau$, $\nu\beta(c)$ are similar as above case. For replication, we show that the result holds. $A_r \equiv C[|P_r|] \Rightarrow C[|P_r|] \equiv A_r$. We have $A_r \equiv C[|\pi(M).P|] \frac{\nu x.\pi(x)}{[\nu x.\pi(x)]} C[|\{M/x\}|] \equiv A_r$. Then we know that $A_r \equiv C[|\pi(M).P|] \frac{\nu x.\pi(x)}{[\nu x.\pi(x)]} C[|\{M/x\}|] \equiv A_r$.

Theorem 3.1. $\approx_{l.r}$ coincides with $\approx_l$.

Proof. 1. ($\Rightarrow$) We construct the set $S$ of pairs of closed extended processes such that $S = \{(A_r, B_r) | A_r \equiv_{l.r} B_r \}$ and show $S \subseteq \approx_l$. Assume $(A_r, B_r) \in S$ because of $A_r \equiv_{l.r} C_r \equiv_{l.r} D_r \equiv_{l.r} B_r$ for some $C_r$ and $D_r$. For the static equivalence part, although $\equiv_r$ has the rule $\text{REPL}$, while $\equiv$ does not, the rewriting $C[|P_r|] \equiv_r C[|P_r|]$ does not change the frames of processes, i.e. $\phi(C[|P_r|]) = \phi(C[|P_r|])$. Thus $\phi(C_r) \equiv_r \nu\nu.\sigma$ implies $\phi(A_r) \equiv \nu\nu.\sigma$, and similarly $\phi(D_r) \equiv \nu\nu.\sigma'$ implies $\phi(B_r) \equiv \nu\nu.\sigma'$. Hence $A_r \sim B_r$ holds by the definition of $\approx_l$.

Now assume $A_r \Rightarrow_\alpha A_r'$ with $fv(\alpha) \subseteq \text{dom}(A_r)$ and $bn(\alpha) \cap fn(B_r) = \emptyset$. By Lemma 3.3, we have $A_r \Rightarrow_\alpha A_r'$ or $A_r \equiv_{l.r} A_r'$.

When $A_r \Rightarrow_\alpha A_r'$, we have $C_r \Rightarrow_\alpha A_r'$. By the definition of $\approx_{l.r}$, there exists $D_r'$ such that $D_r \Rightarrow^*_{r} D_r' \approx_{l.r} A_r'$. Repeated applications of Lemma 3.3 gives a $B_r'$ such that $B_r \Rightarrow^*_{r} B_r' \equiv_{l.r} D_r'$. Hence $(A_r', B_r') \in S$.

When $A_r \equiv_{l.r} A_r'$, from the proof of Lemma 3.3, we can know that this could happen only when $\alpha$ is $\tau$. In this case, let $B_r' = B_r$. Then $B_r \Rightarrow_{r} B_r'$ and $A_r' \equiv_{r} B_r \equiv_{r} B_r'$. Hence $(A_r', B_r') \in S$.

2. ($\Leftarrow$) We construct the set $R$ of pairs of closed extended processes such that $R = \{(A_r, B_r) | \exists\{\tilde{y}\} \subseteq \text{dom}(A_r) : A_r \{|\tilde{y}/\tilde{y}\} \equiv_{\approx_l} B_r \{|\tilde{y}/\tilde{y}\} \}$ for any pairwise-distinct $\tilde{y}$ s.t. $\{\tilde{y}\} \cap \text{dom}(A_r) = \emptyset$ and $|\tilde{y}| = |\tilde{z}|$ and show that $R \subseteq \approx_{l.r}$. Note that when $A_r \approx_{l.r} B_r$, $\{|\tilde{y}\}$ is chosen to be empty. Assume $(A_r, B_r) \in R$. Then there exist $C_r, D_r$ and $\tilde{z}$ such that $A_r \{|\tilde{y}/\tilde{y}\} \equiv_{l.r} C_r \equiv_{l.r} D_r \equiv_{l.r} B_r \{|\tilde{y}/\tilde{y}\}$ for any pairwise-distinct $\tilde{y}$.

(a) For the static equivalence part, assume $(M = N)\phi(A_r)$ with $\text{vars}(M, N) \subseteq \text{dom}(A_r)$. As argued in 1, $\phi(C_r) \equiv \phi(A_r) \{|\tilde{z}/\tilde{y}\} \equiv \phi(A_r) \{|\tilde{z}/\tilde{y}\}$ and $\phi(D_r) \equiv \phi(B_r) \{|\tilde{z}/\tilde{y}\} \equiv \phi(B_r) \{|\tilde{z}/\tilde{y}\}$. Since $\{\tilde{y}\} \cap \text{vars}(M, N) = \emptyset$, we have $(M = N)\phi(C_r)$. From $\phi(C_r) \sim_{r} \phi(D_r)$, we obtain $(M = N)\phi(D_r)$. Now we show $(M = N)\phi(B_r)$. To this end, assume $\phi(B_r) \equiv \nu\nu.\sigma$ and $M' = \equiv_{e} N' \sigma$. Then $\phi(B_r) \{|\tilde{z}/\tilde{y}\} \equiv \nu\nu.\sigma \equiv \nu\nu.\sigma'$ and $M' = \equiv_{e} N' \sigma$. Since $\{\tilde{y}\} \cap \text{fn}(B_r) = \emptyset$ and $\{\tilde{z}\} \subseteq \text{dom}(B_r)$, we have $\phi(B_r) \equiv \nu\nu.\sigma$. Hence $M' = \equiv_{e} N' \sigma$. Thus $(M = N)\phi(B_r)$ holds, hence $A_r \sim_{r} B_r$.

(b) Assume $A_r \Rightarrow_{\alpha} A_r'$. We need to show that there exists $B_r'$ such that $B_r \Rightarrow_{\alpha} B_r'$ and $(A_r', B_r') \in R$. Consider the normalized derivation of transition of $A_r \Rightarrow_{\alpha} A_r'$. We distinguish two cases depending on whether $\alpha$ is $\pi(x)$ or not.

i. $\alpha$ is not $\pi(x)$. We can safely assume $\{|\tilde{y}\} \cap \text{fn}(A_r) = \emptyset$ since $\tilde{y}$ are arbitrary. From $A_r \Rightarrow_{\alpha} A_r'$, by $\text{PAR}$ in Fig. 1, we know that $C_r \equiv_{l.r} A_r \{|\tilde{y}/\tilde{y}\} \Rightarrow_{\alpha} A_r' \{|\tilde{y}/\tilde{y}\} = C_r'$. Using Lemma 3.3 several times, there exists $C_r'$ such that $C_r \Rightarrow^*_{r} C_r' \equiv_{l.r} C_r'$. By hypothesis $C_r \equiv_{l.r} D_r$, there exists $D_r'$ such that $D_r \Rightarrow^*_{r} D_r'$. Using Lemma 3.3 several times, we have $D_r \Rightarrow^*_{r} D_r'$.

We first check the case $D_r \Rightarrow^*_{r} D_r'$. From $C_r' \equiv_{l.r} C_r'$, we have $\phi(C_r) \equiv \phi(C_r')$, hence also $\phi(C_r) \equiv \phi(D_r')$. In other words, there exists $B_r'$ such that $D_r' \equiv_{r} B_r' \{|\tilde{y}/\tilde{y}\}$ with $\{|\tilde{y}\} \cap \text{fn}(B_r') = \emptyset$. 


(otherwise we can substitute them with the corresponding variables in $\bar{z}$). Adding restrictions $\nu \bar{y}$ to $B_r | \{\bar{z}/\bar{y}\} \equiv_r D_r \xrightarrow{\alpha} B'_r | \{\bar{z}/\bar{y}\}$, we have $B_r \xrightarrow{\alpha} B'_r$. From $A_r' | \{\bar{z}/\bar{y}\} \equiv_r C'_r \approx l \equiv D'_r \equiv B'_r | \{\bar{z}/\bar{y}\}$, we know that $(A_r', B'_r) \in \mathbb{R}$.

For the case when $D_r \equiv_r D'_r$, from the proof of Lemma 3.3, we can know that $D_r \equiv_r D'_r$ could happen only when $\alpha$ is $\tau$. Let $B'_r = B_r$. Then we have $B_r \xrightarrow{\alpha} B'_r$ and $A_r' | \{\bar{z}/\bar{y}\} \equiv_r C'_r \approx_l D'_r \equiv_r D_r \equiv_r B'_r | \{\bar{z}/\bar{y}\}$. Thus $(A_r', B'_r) \in \mathbb{R}$.

ii. $\alpha$ is $\pi(x)$. In this case $A_r \equiv_r C[\pi(x).P_r] \xrightarrow{\pi(x)} C[P_r] \equiv_r A'_r$ with $x \notin bv(C)$. Choose a fresh $y'$, then we have $C_r \equiv_r \nu y'.C[\pi(y').P_r | \{x/y\}] \equiv_r \nu y'.C[\pi(y').P_r | \{x/y\}] \equiv_r \nu y'.C[P_r | \{x/y\}] \equiv_r \nu y'.C[P_r | \{x/y\}] \equiv_r \nu y'.C[P_r | \{x/y\}]$ since $x$ is a free variable. From Lemma 3.3, there exists a closed $C'_r$ such that $C_r \equiv_r \nu y'.C'_r \equiv_r A'_r | \{\bar{z}, \bar{y}/\bar{y}, y\}$. By $C_r \approx_l D_r$, there exists $D'_r$ such that $D_r \equiv_r \nu y'.C'_r \approx_l C'_r$.

Assume $\phi(A_0) \equiv_r \nu \bar{m}.\sigma$. Then $\phi(C_r) \equiv_r \nu \bar{m}.\sigma | \{\bar{z}, \bar{y}/\bar{y}, y\} \equiv_r \nu \bar{m}.(\sigma \cup \{\bar{z}, \bar{y}/\bar{y}, y\})$. Hence $(\bar{z}, \bar{y}/\bar{y}, y \equiv \bar{y}, y | \{\bar{z}, \bar{y}/\bar{y}, y\}) \equiv_r (\bar{z}, \bar{y}/\bar{y}, y \equiv \bar{y}, y | \{\bar{z}, \bar{y}/\bar{y}, y\})$. Since $\phi(D'_r) \sim \phi(D'_r)$, we obtain $(\bar{z}, \bar{y}/\bar{y}, y \equiv \bar{y}, y | \{\bar{z}, \bar{y}/\bar{y}, y\})$. Thus there exists $B'_r$ such that $D'_r \equiv_r B'_r | \{\bar{z}, \bar{y}/\bar{y}, y \equiv \bar{y}, y | \{\bar{z}, \bar{y}/\bar{y}, y\}) \equiv_r \nu y.D_r \equiv_r \nu y'.C'[\pi(y'), Q_r] \equiv_r \nu y'.C'[\pi(y'), Q_r] \Rightarrow B'_r | \{x/y\}$ for some $C'$. Since static equivalence is closed under reduction (Lemma 1 in [1]), $C'[\pi(y'), Q_r] \Rightarrow B'_r | \{x/y\}$. Moreover, since $Q_r$ is a plain process which does not contain any active substitution, that is to say $C'$ can rewrite $y'$ with $x$. Hence we have $C'[\pi(y'), Q_r] \equiv_r C'[\pi(y'), Q_r]$, which implies $B_r \equiv_r B'_r | \{x/y\} \Rightarrow B'_r | \{x/y\} \equiv_r B'_r | \{x/y\}$.

\begin{align*}
\text{Theorem 3.2.} \quad \approx_r \text{ coincides with } \approx_r
\end{align*}

\textbf{Proof.} 1. $(\Rightarrow)$ We construct the following set

\begin{align*}
\{ (A_r, B_r) | A_r \equiv_r \approx_r B_r \}
\end{align*}

2. $(\Leftarrow)$ We construct the following set

\begin{align*}
\{ (A_r, B_r) | A_r \equiv_r \approx_r B_r \}
\end{align*}

The rest analysis are quite similar as above but much simpler.

Since the operational semantics defined by the rules in Fig.2 gives the same notion of a behavioural equivalence as that defined by the rules in Fig.1, in the rest part of this note we shall always use the operational semantics of Fig.2 instead of Fig.1.

4 Intermediate Representation

The notion of an intermediate representation was originally introduced in [2] as a means to circumvent the difficulties caused by structural equivalence in developing a symbolic semantics for the applied pi calculus. Here we use it to write a proof for the coincidence of observational equivalence and labeled bisimilarity. Intermediate representation can be regarded as an encoding which preserves both labeled bisimilarity and observational equivalence. The representation is a calculus by itself, which consists of, on the syntax side, intermediate processes, and, on the semantics side, intermediate transitions $\xrightarrow{H_i}$, intermediate static equivalence $\sim_i$, intermediate bisimilarity $\equiv_{i,t}$, and intermediate observational equivalence $\equiv_i$.

\footnote{\text{(\bar{z} = \bar{y})}\phi(C'_r) abbreviates (z_1 = y_1)\phi(C_r), \ldots (z_n = y_n)\phi(C'_r)}
The intermediate representation of replication is extended process with a hole not under a replication, an input, an output, or a conditional. For example, pulling name binders to the top level, applying active substitutions and eliminating variable restrictions.

Intermediate processes are required to be applied, namely each variable in dom(A) occurs only once in A. For example, \( \pi(f(k)) \mid \{k/x\} \) is applied while \( \pi(f(x)) \mid \{k/x\} \) is not. For an intermediate framed process \( F \), we write \( \varphi(F) \) for the substitution obtained by taking the union of the active substitutions in \( F \). For example, \( \varphi(\pi(f(k))) \mid \{k/x\} \mid \{h(k)/y\} = \{k/x, h(k)/y\}. \) An intermediate evaluation context is an intermediate extended process with a hole not under a replication, an input, an output, or a conditional.

Our setting is somewhat different from [2], but the essence remains the same. These intermediate processes are a selected subset of the original processes. The function \( \Gamma \) defined in Fig. 3 turns an extended processes into an intermediate extended process (“\( \triangleright \) in [2]) where we assume that bound names are pairwise-distinct and different from free names. It transforms an extended process into an intermediate extended process by pulling name binders to the top level, applying active substitutions and eliminating variable restrictions. For example, \( \Gamma(vx.(\pi(f(x)).vn.\pi(n) \mid \{k,h(k)/x\})) = vn.vk.(\pi(f(h(k))).\pi(n) \mid 0) \). For the parallel composition \( A_r \mid B_r \), \( A_r \) may use the variables defined by \( A_r \)'s active substitutions, and vice versa. To make sure \( \Gamma(A_r \mid B_r) \) to be applied, we have to apply the union of their active substitutions repeatedly until idempotent.

A replication \(!P_r\) implicitly contains infinitely many bound names, and we can not pull all of them to the top level at once. A feasible solution is to work “on-the-fly” and keep \(!P_r\) invariant under \( \Gamma \). In other words, the intermediate representation of replication \(!P_r\) is itself. It can be shown that \( \Gamma \) preserves \( \alpha \)-conversion.

Intermediate structural equivalence \( \equiv \), is the smallest equivalence relation on intermediate processes, closed by application of intermediate evaluation context and \( \alpha \)-conversion such that

\[
\text{PAR-0} \quad A \equiv A \mid 0
\]

\[
\text{PAR-A} \quad A \mid B \equiv B \mid A
\]

\[
\text{PAR-C} \quad A \mid (B \mid C) \equiv (A \mid B) \mid C
\]
Intermediate observational equivalence is the largest symmetric relation \( \simeq \) on closed intermediate processes defined by the rules in Fig. 4. In the \( \text{PAR}_i \) rule, when \( \alpha \) is an input \( a(M) \), \( M \) may use variables defined in the active substitutions in \( B \). To keep the result process applied, \( \varphi(B) \) is applied to \( \alpha \). For example, \( a(x).\overline{b}(x) \mid \{ k/y \} \xrightarrow{\alpha} \overline{b}(k) \mid \{ k/y \} \) can be derived from \( a(x).\overline{b}(x) \xrightarrow{a(k)} \overline{b}(k) \). Similar to Section 2.2, we denote by \( \Rightarrow_1 \), the reflexive and transitive closure of \( \xrightarrow{1} \), and write \( \Rightarrow_1, \Rightarrow_1, \Rightarrow_1, \) and \( \Rightarrow_1, \) for \( \Rightarrow_1, \Rightarrow_1, \) if \( \alpha \) is not \( \tau \) and \( \Rightarrow_1, \) otherwise.

We write \( A \Downarrow_1 \) when \( A \) can send a message on channel \( a \), namely \( A \Rightarrow_1 C[\pi(M),P] \) for some intermediate evaluation context that does not bind \( a \).

**Definition 4.1.** Intermediate observational equivalence is the largest symmetric relation \( \simeq \) on closed intermediate extended processes with the same domain such that \( A \simeq B \) implies:

1. If \( A \Downarrow_1 \) then \( B \Downarrow_1 \);
2. If \( A \Rightarrow_1 A' \), then \( B \Rightarrow_1 B' \) for some \( B' \) such that \( A' \simeq B' \);
3. For any names \( \tilde{l} \), variables \( \tilde{z} \subseteq \text{dom}(A) \), intermediate framed process \( E \) with \( \text{dom}(E) \subseteq \text{dom}(A) \), and \( \text{fv}(E) \subseteq \text{dom}(E) \), let \( A = \nu\tilde{v}.F, B = \nu\tilde{v}.H \) with \( \text{fv}(E) \cap (\tilde{v} \cup \tilde{m}) = \emptyset \). Then \( \nu\tilde{v}.\nu\tilde{m}.(E\varphi(F) \mid F[\tilde{z}]) \approx_1 \nu\tilde{v}.\nu\tilde{m}.(E\varphi(H) \mid H[\tilde{z}]) \).

**Definition 4.2.** Two intermediate extended processes \( A \) and \( B \) are intermediate statically equivalent, written \( A \sim B \), if
1. \( \text{dom}(A) = \text{dom}(B) \)

2. For any terms \( M \) and \( N \) such that \( \text{vars}(M, N) \subseteq \text{dom}(A) \), \( M \varphi(F_1) =_E N \varphi(F_1) \) iff \( M \varphi(F_2) =_E N \varphi(F_2) \), where \( A = \nu n_1.F_1, B = \nu n_2.F_2 \), and names \( (M, N) \cap \{n_1, n_2\} = \emptyset \).

**Definition 4.3.** Intermediate labeled bisimilarity \( \approx_{l,i} \) is the largest symmetric relation \( R \) on closed intermediate processes such that \( A R B \) implies,

1. \( A \sim_i B \)
2. If \( A \overset{\alpha}{\rightarrow} A' \) with \( \text{fv}(\alpha) \subseteq \text{dom}(A) \) and \( \text{bn}(\alpha) \cap \text{fn}(B) = \emptyset \), then \( B \overset{\alpha}{\rightarrow} B' \) and \( A' R B' \) for some \( B' \).

5 \( \approx_i \) coincides with \( \approx_{l,i} \)

The coincidence between labeled bisimilarity and intermediate labeled bisimilarity, namely the following Theorem 5.1, is proposed and proved in [2]. Our setting for intermediate semantics is slightly different from the original one [2]. For example, we have \( \alpha \)-conversion while they use naming environment, and we have replications while they don’t. In fact, the technical developed therein is also suitable for our setting. Although Theorem 5.1 is not introduced in this proof, we still give its proof in Appendix B in case some readers want to check it.

The proofs of the following Lemmas 5.1 is similar to Lemma A.4 in [2], while Lemma 5.2 and Lemma 5.4 are similar to Lemma 4.5 (the cases for \( \rightarrow_i \) and \( \overset{\alpha}{\rightarrow}_i \)) and Proposition 4.6 in [2] respectively. Although our framework differs slightly from theirs, the techniques developed there are still applicable. Thus we only sketch the proofs for these lemmas below.

We can extend the definition of \( \Gamma \) to the contexts by adding the rule for the hole \( \Gamma([\cdot]) = (\cdot)[\cdot] \), where \( \cdot \) will be treated as restrictions. For example \( \Gamma([\cdot] | \nu n.\tilde{c}(\cdot)) = (\cdot).\nu n.([\cdot] | \tilde{c}(\cdot)) \).

**Lemma 5.1.** Let \( C_r \) be an evaluation context in which bound names are pairwise-distinct and different from the free ones in \( C_r \). Let \( \tilde{x} \) be a tuple of pairwise-distinct variables such that the hole is in the scope of an occurrence of \( \nu x \) in \( C_r \). Then there exist some sequences of names \( \tilde{n}_1, \tilde{n}_2 \) and an intermediate framed evaluation context \( G \) such that \( \Gamma(C_r) = \nu \tilde{n}_1.\cdot.\nu \tilde{n}_2.G \).

For any extended process \( A_r \) such that \( C_r[A_r] \) is an extended process, if \( \Gamma(A_r) = \nu \tilde{m}.F \) for some of names \( \tilde{m} \) with \( \{\tilde{m}\} \cap (\{\tilde{n}_1, \tilde{n}_2\} \cup \text{fn}(C_r)) = \emptyset \) and some intermediate framed process \( F \), then

\[
\Gamma(C_r[A_r]) = \nu \tilde{n}_1.\nu \tilde{m}.\nu \tilde{n}_2.\cdot(G[F]\varphi(G[F]^\cdot)\cdot)_{\tilde{m}}
\]

As a corollary, we can see that when \( A_r \) is closed, no active substitution in \( C \) can apply to \( A_r \). In this case, we have \( \Gamma(C_r[A_r]) = \nu \tilde{n}_1.\nu \tilde{m}.\nu \tilde{n}_2.\cdot(G[F]\varphi(G[F]^\cdot)\cdot)_{\tilde{m}} \).

**Proof.** By induction on the structure of \( C \).

**Lemma 5.2.** Suppose \( B \simeq A \overset{\alpha}{\rightarrow}_i A' \) with \( \text{fv}(B, A) \cap \text{bn}(\alpha) = \emptyset \). There exists \( B' \) such that \( B \overset{\alpha}{\rightarrow}_i B' \simeq A' \).

**Proof.** By induction on the number of rewriting steps of \( \simeq \).

**Lemma 5.3.** Suppose \( B \simeq A \overset{\alpha}{\rightarrow}_i A' \) with \( \text{fv}(B, A) \cap \text{bn}(\alpha) = \emptyset \). There exists \( B' \) such that \( B \overset{\alpha}{\rightarrow}_i B' \simeq A' \).

**Proof.** By repeated applications of Lemma 5.2.
Lemma 5.4. If $A_r \xrightarrow{a} A_r'$ with $fv(A_r) \cap bv(\alpha) = \emptyset$, then $\Gamma(A_r) \xrightarrow{a} \sim B \simeq \Gamma(A_r')$ for some $B$.

Proof. See Appendix B.

Lemma 5.5. If $A_r \xrightarrow{a} A_r'$ with $fv(A) \cap bv(\alpha) = \emptyset$, then $\Gamma(A_r) \xrightarrow{a} \sim B \simeq \Gamma(A_r')$ for some $B$.

Proof. Using Lemma 5.4 and Lemma 5.2 several times.

Lemma 5.6. Assume $A_r$ is closed and $\Gamma(A_r) \xrightarrow{a} A$. Then there exists a closed $A_r'$ such that $A_r \xrightarrow{a} A_r'$ and $\Gamma(A_r') \simeq A$.

Proof. See Appendix B.

Lemma 5.7. Suppose $A_r$ is closed and $\Gamma(A_r) \xrightarrow{a} A$. Then there exists a closed $A_r'$ such that $A_r \xrightarrow{a} A_r'$ and $\Gamma(A_r') \simeq A$.

Proof. Using Lemma 5.2 and Lemma 5.6 several times.

Theorem 5.1. $A_r \approx_i B_r$ if and only if $\Gamma(A_r) \approx_{i, i} \Gamma(B_r)$.

Proof. See Appendix B.

6 \approx_i coincides with \approx_i

Lemma 6.1. If $\nu\tilde{\nu}.F \simeq \nu\tilde{\nu}.H$, then $\nu\tilde{\nu}.(E \varphi(F) \mid F_{\tilde{\nu}}) \simeq \nu\tilde{\nu}.(E \varphi(H) \mid H_{\tilde{\nu}})$ for any variables $\tilde{y}$ and intermediate framed process $E$ with $dom(E) \cap dom(F) = fn(E) \cap (\tilde{\nu} \cup \tilde{m}) = \emptyset$.

Proof. The proof goes by induction on the length of the linear proof sequence for $\simeq$. When the length is 0, the result holds trivially. For the inductive step, w.l.o.g., we may assume $\nu\tilde{\nu}.F \simeq \nu\tilde{\nu}.F' \simeq \nu\tilde{\nu}.H$. By the induction hypothesis, we have $\nu\tilde{\nu}.(E \varphi(F') \mid F'_{\tilde{\nu}}) \simeq \nu\tilde{\nu}.(E \varphi(F') \mid F'_{\tilde{\nu}})$. Now we show $\nu\tilde{\nu}.(E \varphi(F') \mid F'_{\tilde{\nu}}) \simeq \nu\tilde{\nu}.(E \varphi(H) \mid H_{\tilde{\nu}})$ as follows:

1. Assume the rewriting is $\nu\tilde{\nu}.F' = \nu\tilde{\nu}.G_1[A\{M/x\}] \simeq \nu\tilde{\nu}.G_1[A\{N/x\}] = \nu\tilde{\nu}.H$ where $G_1$ is an intermediate framed evaluation context. We can assume that $A$ does not contain restrictions, otherwise we can adjust the context part. We also can safely assume that $x$ is fresh and $\tilde{f} = \tilde{k} = \tilde{m}$ (otherwise we can use $\alpha$-conversion). Then $F' = G_1[A\{M/x\}] = (G_1[A]\{M/x\})$ and $H = G_1[A\{N/x\}] = (G_1[A]\{N/x\})$. Then $E \varphi(F') \mid F'_{\tilde{\nu}} = E \varphi((G_1[A]\{M/x\}) \mid ((G_1[A]\{M/x\}) \mid \tilde{y}})$ $\simeq E \varphi((G_1[A]\{M/x\}) \mid (G_1[A]\{M/x\}) \mid \tilde{y})$ $\simeq E \varphi((G_1[A]\{N/x\}) \mid ((G_1[A]\{N/x\}) \mid \tilde{y}) = E \varphi(H) \mid H_{\tilde{\nu}}$.

Hence we can conclude that $\nu\tilde{\nu}.(E \varphi(F) \mid F_{\tilde{\nu}}) \simeq \nu\tilde{\nu}.(E \varphi(H) \mid H_{\tilde{\nu}})$.

2. The other cases are obvious.

Lemma 6.2. $A_r \approx B_r$ implies $\Gamma(A_r) \approx_i \Gamma(B_r)$.

Proof.

$$S = \{ (A, B) \mid A \simeq \Gamma(A_r), A_r \approx B_r, \Gamma(B_r) \simeq B \}$$

1. First we show that $A_r \approx_i B_r$. By Lemma 5.3 and Lemma 5.7, we can see that $A_r \not\approx_i B_r$. From $A_r \approx B_r$, we have $B_r \not\approx_i$. Then from Lemma 5.5 and Lemma 5.3, we have that $B \not\approx_i$.
2. Assume $A \implies B$ then we will show that there exists $B'$ such that $B \implies B'$ and $(A', B') \in S$. By Lemma 5.3 and Lemma 5.7, we have $A_r \implies A'_r$ with $\Gamma(A'_r) \simeq A$. From $A_r \implies B_r$ there exist $B'_r$ such that $B_r \implies B'_r \simeq A'_r$. By Lemma 5.5 and Lemma 5.3, we know that there exists $B'$ such that $B \implies B' \simeq \Gamma(B_r)$. Hence $(A', B') \in S$.

3. Assume $A = \nu\phi.H$ and $B = \rho_\phi.H$. For any $E, \tilde{\phi}, y$, let $C = \nu\nu.\nu.\nu.(E\varphi(F_1) \mid F_1 \varphi)$ and $D = \nu\nu.\nu.\nu.(E\varphi(H) \mid H_1 \varphi)$. We need to show that $(C, D) \in S$. Let $C_r = \nu\tilde{\phi}.\nu.(E \mid \cdot)$. Assume $\Gamma(A_r) = \nu\nu_1.F_1$ and $\Gamma(B_r) = \nu\nu_1.H_1$ and then $\Gamma(G[A_r]) = \nu\nu_1.(\nu\phi.H_1) \mid F_1 \varphi \simeq C$ and $\Gamma(C[B_r]) = \nu\nu_1.(E\varphi(H_1) \mid H_1 \varphi) \simeq D$ by Lemma 6.1. Since $\simeq$ is closed by context, namely $C_r[A_r] \simeq C_r[B_r]$, we know that $(C, D) \in S$.

**Lemma 6.3.** $\Gamma(A_r) \simeq_i \Gamma(B_r)$ implies $A_r \simeq B_r$.

**Proof.** We construct the following set

$$ R = \{ (A_r, B_r) \mid \Gamma(A_r) \simeq_i \Gamma(B_r) \}.$$ 

and will show that $R \subseteq S$. Assume $\Gamma(A_r) = \nu\nu_1.F \simeq \nu\nu_1.F_1 \simeq \nu\nu_1.H_1 \simeq \nu\nu_1.H = \Gamma(B_r)$.

1. First we prove that $A_r \Downarrow_{\alpha} \implies B_r \Downarrow_{\alpha}$. By Lemma 5.5 and Lemma 5.3, we know that $\nu\nu_1.F_1 \simeq \nu\nu_1.H_1$. Since $\nu\nu_1.F_1 \simeq \nu\nu_1.H_1$, we have $\nu\nu_1.H_1 \Downarrow_{\alpha}$ by Lemma 5.3 and Lemma 5.7 we have that $B_r \Downarrow_{\alpha}$.

2. Assume $A_r \implies A'_r$, we need to show there exists $B'_r$ such that $B_r \implies B'_r$ and $(A'_r, B'_r) \in R$. By Lemma 5.5 and Lemma 5.3, we know $\nu\nu_1.F_1 \implies \Delta$ such that $\Gamma(A'_r) \simeq A$. Since $\nu\nu_1.F_1 \simeq \nu\nu_1.H_1$, we have $\nu\nu_1.H_1 \implies B \simeq B_r$. By Lemma 5.3 and Lemma 5.7, there exists $B'_r$ such that $B_r \implies B'_r$ and $\Gamma(B'_r) \simeq B$. Thus $(A'_r, B'_r) \in R$.

3. For any evaluation context $C_r$, in case the bound names are not pairwise distinct or different from the free ones, we can use $\alpha$-conversion to $C_r[A_r] = C_r'[\nu\phi.H]$, $C_r[B_r] = C_r'[\nu\phi.H]$. Then we will have a new sequence $\Gamma(\alpha(A)) = \alpha(\Gamma(A)) \simeq \alpha(\nu\nu_1.F_1) \simeq \nu\nu_1.H_1 \simeq \alpha(\Gamma(B)) = \alpha(\Gamma(B_r))$. Hence we assume that the bound names of $C_r$ are not pairwise distinct or different from the free ones. By Lemma 5.1, we have $\Gamma(C_r[A_r]) = \nu\nu_1.\nu\nu_2.\nu\nu_3.\nu(\nu\alpha.H_1)[F_1 \varphi]$ and $\Gamma(C_r[B_r]) = \nu\nu_1.\nu\nu_2.\nu\nu_3.\nu(\nu\alpha.H_1)[F_1 \varphi]$ for some intermediate framed evaluation context $\varphi$. Since $\varphi$ is an intermediate framed evaluation context, we know that $\alpha \equiv E \mid \alpha$. Hence $\Gamma(C_r[B_r]) \simeq \nu\nu_1.\nu\nu_2.\nu\nu_3.\nu(\nu\alpha.H_1)[F_1 \varphi] \equiv_i \nu\nu_1.\nu\nu_2.\nu\nu_3.\nu(\nu\alpha.H_1)[F_1 \varphi]$.

Hence $(C_r[A_r], C_r[B_r]) \in R$.

7. $\simeq_i$ coincides with $\simeq_{l,i}$

**Lemma 7.1.** Assume $\text{dom}(E) \cap \text{fv}(F) = \text{fn}(E) \cap (\tilde{\phi} \cup \tilde{m}) = \text{vars}(\alpha) \cap \tilde{\varphi} = \emptyset$.

1. $\nu\phi.F \xrightarrow{\alpha(M(E))} \nu\nu.H$ implies $\nu\phi.\nu.\nu.(E\varphi(F) \mid F_1 \varphi) \xrightarrow{\alpha(M)} \nu\nu.\nu.\nu.(E\varphi(H) \mid H_1 \varphi)$;

2. $\nu\phi.F \xrightarrow{\alpha(M)} \nu\nu.H$ implies $\nu\phi.\nu.\nu.(E\varphi(F) \mid F_1 \varphi) \xrightarrow{\alpha(M)} \nu\nu.\nu.\nu.(E\varphi(H) \mid H_1 \varphi)$ when $\alpha$ is not input.

**Proof.** 1. Assume $\nu\phi.F \equiv_i \nu\phi.\nu.\nu.(E\varphi(F) \mid F_1 \varphi) \xrightarrow{\alpha(M)} \nu\nu.\nu.\nu.(E\varphi(H) \mid H_1 \varphi)$.

2. $\nu\phi.F \xrightarrow{\alpha(M)} \nu\nu.H$ implies $\nu\phi.\nu.\nu.(E\varphi(F) \mid F_1 \varphi) \xrightarrow{\alpha(M)} \nu\nu.\nu.\nu.(E\varphi(H) \mid H_1 \varphi)$ when $\alpha$ is not input.
2. We take the expansion of replication as the example. The other cases are similar. Assume $\nu\bar{m}.F \equiv_i, \nu\bar{m}.G[P] \equiv \nu\bar{m}.H$ with $\Gamma(P) = \nu.P$. Similarly as above we have $F_H \equiv_i \bar{G}_H[P] \equiv_i \nu\bar{m}.G(P)$ and $\varphi(F) = \varphi(G)$. Adding the parallel composition and restrictions, we have $\nu\bar{m}.(E\varphi(F) \mid F_H) \equiv_i \nu\bar{m}.(E\varphi(G) \mid G_H[P \mid P])$. Similarly as above input case, we can α-conver $\nu\bar{m}$ to $\nu\bar{m}.\nu.l$. and obtain $\nu\bar{m}.H = \nu\bar{m}.\nu.l.H'$. And also we get $G \equiv \bar{H}$ and $\varphi(G) = \varphi(H')$. Adding the parallel composition and restrictions, we have $\nu\bar{m}.\nu.l.(E\varphi(G) \mid \bar{G}_H[P \mid P]) \equiv_i \nu\bar{m}.\nu.l.(E\varphi(H) \mid \bar{H}_H[H \mid H])$. Finally we have $\nu\bar{m}.(E\varphi(F) \mid F_H) \equiv_i \nu\bar{m}.(E\varphi(G) \mid G_H[P]) \equiv, \nu\bar{m}.(E\varphi(H) \mid H_H[H \mid H])$.

Corollary 7.1. Assume $\text{dom}(E) \cap \text{fe}(F) = \text{fn}(E) \cap (\bar{n} \cup \bar{m}) = \text{vars}(\alpha) \cap \bar{z} = \emptyset$.

1. $\nu\bar{m}.F \equiv\alpha(M_E[\bar{z}])_l \nu\bar{m}.H$ implies $\nu\bar{m}.(E\varphi(F) \mid F_H) \equiv\alpha(M)_{l_1} \nu\bar{m}.(E\varphi(H) \mid H_H)$;

2. $\nu\bar{m}.F \equiv\alpha(M_E[\bar{z}])_l \nu\bar{m}.H$ implies $\nu\bar{m}.(E\varphi(F) \mid F_H) \equiv\alpha(M)_{l_1} \nu\bar{m}.(E\varphi(H) \mid H_H)$ when $\alpha$ is not input.

Proof. Using Lemma 7.1 several times.

Theorem 7.1. For any names $\bar{r}$, variables $\bar{y} \subseteq \text{dom}(F)$, intermediate framed process $E$ with $\text{fe}(E) \subseteq \text{dom}(E, F)$ and $\text{dom}(E) \cap \text{dom}(F) = \text{fn}(E) \cap (\bar{n} \cup \bar{m}) = \emptyset$. Then $\nu\bar{m}.F \approx_{l,1} \nu\bar{m}.H$ implies $\nu\bar{m}.\nu.l.(E\varphi(F) \mid F_H) \equiv_{l_1,1} \nu\bar{m}.\nu.l.(E\varphi(H) \mid H_H)$.

Proof. we construct the set $\mathcal{R}$ as follows:

$$\mathcal{R} = \{ \nu\bar{m}.\nu.l.(E\varphi(F) \mid F_H), \nu\bar{m}.\nu.l.(E\varphi(H) \mid H_H) \} \nu\bar{m}.F \approx_{l_1,1} \nu\bar{m}.H$$

where $\text{dom}(E) \cap \text{dom}(F) \neq \emptyset$, $\text{fe}(E) \subseteq \text{dom}(E, F)$ and we will prove $\mathcal{R} \subseteq \approx_{l,1}$.

First we show the intermediate static equivalence. According to the Def. 4.2, assume terms $M, N$ with $\text{vars}(M, N) \subseteq \text{dom}(E, F, \bar{g})$ and

$$M(\varphi(E\varphi(F)) \cup \varphi(F\bar{y})) = N(\varphi(E\varphi(F)) \cup \varphi(F\bar{y})) \quad (2)$$

We will prove that $M(\varphi(E\varphi(H)) \cup \varphi(F\bar{y})) = N(\varphi(E\varphi(H)) \cup \varphi(F\bar{y}))$. From $\text{dom}(E) \cap \text{dom}(F) = \emptyset$, we have that $M(\varphi(E\varphi(F)) \cup \varphi(F\bar{y})) = (M(\varphi(E\varphi(F))) \varphi(F\bar{y})) = (M(\varphi(E\varphi(F))) \varphi(F\bar{y}))$. Similarly we have $N(\varphi(E\varphi(F)) \cup \varphi(F\bar{y})) = (N(\varphi(E\varphi(F))) \varphi(F\bar{y}))$. And thus we can reduce the equation (2) to $M(\varphi(E\varphi(F))) \varphi(F\bar{y}) = N(\varphi(E\varphi(F))) \varphi(F\bar{y})$. From hypothesis $\nu\bar{m}.F \approx_{l,1} \nu\bar{m}.H$, we can easily know $(M(\varphi(E\varphi(F))) \varphi(F\bar{y})) = (M(\varphi(E\varphi(F))) \varphi(F\bar{y}))$. Similarly we can derive that $M(\varphi(E\varphi(F)) \cup \varphi(F\bar{y})) = (M(\varphi(E\varphi(F))) \varphi(F\bar{y})) = (M(\varphi(E\varphi(F))) \varphi(F\bar{y}))$. Hence $\nu\bar{m}.(E\varphi(F) \mid F_H) \approx_{l_1,1} \nu\bar{m}.(E\varphi(H) \mid H_H)$.

Now we proceed to show the behavior equivalence. Consider the normal derivation of the intermediate labeled transition.

1. $\nu\bar{m}.(E\varphi(F) \mid F_H) \equiv_i, \nu\bar{m}.(P(M \mid \bar{z})).P_2 \mid a(x).P_1 \mid F_1 \equiv_i \nu\bar{m}.(P_1(M \mid \bar{z}) \mid P_2 \mid F_1)$. The proof goes by a case analysis on the position of $a(x).P_1$ and $\bar{m}(M \mid \bar{z})$. P_2.

(a) $E\varphi(F) \equiv_i a(x).P_1 \mid F_1$ and $F_1 \equiv_i \bar{m}(M \mid \bar{z}).P_2 \mid F_1 \equiv_i \{ \bar{T} / \bar{y} \}$, with $F_1 \equiv_i F_1 \equiv_i F_1$. Since active substitutions are required to be defined on the base sort, $\varphi(F)$ does not contain $\alpha$. When $a(x).P_1$ occurs in $E\varphi(F)$, the only possibility is that $a$ is a free name of $E$. From the hypothesis $\text{fn}(E) \cap (\bar{n} \cup \bar{m}) = \emptyset$, we know that $a$ is not in $\bar{n}$ or $\bar{m}$. Assume $E \equiv_i a(x).Q_1 \mid E_1$ with $Q_1(\varphi(F)) = P_1$ and $E_1(\varphi(F)) = F_1$. We only detail the proof for the case when $M$ is of the base sort.

$$\nu\bar{m}.F \equiv_i, \nu\bar{m}.(P(M \mid \bar{z}) \mid P_2 \mid F_1 \equiv_i \{ \bar{T} / \bar{y} \})$$

From $\nu\bar{m}.F \approx_{l,1} \nu\bar{m}.H$, we can know that

$$\begin{align*}
\nu\bar{m}.H &\rightarrow_i \nu\bar{m}_1.(\bar{m}(N \mid \bar{z}) \mid H_1) \sim_{\nu,2}(\varphi(F)) \rightarrow_i \nu\bar{m}_1.(\bar{m}(N \mid \bar{z}) \mid H_1) \approx B_1 \approx_{l,1} A_1
\end{align*}$$
Using Corollary 7.1 to add $E \equiv_i a(x).Q_1 \mid E_1$ to and eliminate variables $\tilde{y}$ from the first $\Rightarrow_i$ in above transitions (3), we have

$$
\nu\tilde{m}.(E\varphi(H) \mid H_{\tilde{y}}) \equiv, \nu\tilde{m}.(a(x).Q_1\varphi(H) \mid E_1\varphi(H) \mid H_{\tilde{y}})
\Rightarrow_i \nu\tilde{m}_1.(E\varphi(H_1) \mid \pi(N).Q_2 \mid H_{\tilde{y}})
\equiv, \nu\tilde{m}_1.(a(x).Q_1\varphi(H_1) \mid E_1\varphi(H_1) \mid \pi(N).Q_2 \mid H_{\tilde{y}})
\Leftrightarrow_i \nu\tilde{m}_1.(Q_1\varphi(H_1))\{N/x\} \mid E_1\varphi(H_1) \mid Q_2 \mid H_{\tilde{y}})
$$

Then adding $Q_1\{z/x\} \mid E_1$ to and eliminating variables $\tilde{y} \cup z$ from the last $\Rightarrow_i$ in transitions (3), we obtain that

$$
\nu\tilde{m}.(E\varphi(H) \mid H_{\tilde{y}}) \Rightarrow_i \nu\tilde{m}'.(Q_1\varphi(H'))\{N/x\} \mid E_1\varphi(H') \mid H'_{\tilde{y}})
$$

Combining the transitions in (4) and (5), we obtain

$$
\nu\tilde{m}.(E\varphi(H) \mid H_{\tilde{y}}) \Rightarrow_i \nu\tilde{m}'.(Q_1\varphi(H'))\{N/x\} \mid E_1\varphi(H') \mid H'_{\tilde{y}})
$$

Adding name binders $\tilde{l}$ by $\text{Scope}_i$ in Fig. 4, we obtain that

$$
\nu\tilde{l}.\nu\tilde{m}.(E\varphi(H) \mid H_{\tilde{y}}) \Rightarrow_i \nu\tilde{l}.\nu\tilde{m}'.(Q_1\varphi(H'))\{N/x\} \mid E_1\varphi(H') \mid H'_{\tilde{y}}) = B
$$

Clearly $A, B$ can be obtained by adding $E_1 \mid Q_1\{z/x\}$ to $A_1, B_1$, removing $z, \tilde{y}$ and adding restrictions $\tilde{l}$. Hence $(A, B) \in \mathcal{R}$.

The analysis for channel sort $\mathcal{M}$ is similar. It is worth to point out that when $M$ is a channel name $\mathcal{C}$ and is bound by $\tilde{n}$, $\mathcal{C}$ will be free after the output $\nu\tilde{m}.F = \nu\tilde{m}_1.F'$, but it won’t be free after the internal communication performed by $\nu\tilde{m}_.(E\varphi(F) \mid F$. That is why we need to add the name restrictions $\tilde{l}$ in the construction of $\mathcal{R}$.

(b) $F \equiv_i a(x).P_1 \mid F_{11} \mid \{T/\tilde{y}\}$ and $E\varphi(F) \equiv, \pi(M).P_2 \mid F_{12}$, with $F_{11} \equiv_i F_{12} \equiv_i F_1$. Assume $E \equiv_i \pi(M).Q_2 \mid E_1$ with $M_1\varphi(F) = M, Q_2\varphi(F) = P_2$ and $E_1\varphi(F) = F_{12}$. Then $\nu\tilde{m}.F = a(M_1)_i, A_1 = \nu\tilde{m}.(P_1\{M_1\varphi(F)/x\} \mid F_{11} \mid \{T/\tilde{y}\})$. From $\nu\tilde{m}.F \approx_{i, \tilde{l}} \nu\tilde{m}.H$, we know that

$$
\nu\tilde{m}.H \Rightarrow_i \nu\tilde{m}_1.(a(x).Q_1 \mid H_1) \quad \frac{a(M_1)_i}{A_1}
\nu\tilde{m}_1.(Q_1\{M_1\varphi(H_1)/x\} \mid H_1) \Rightarrow_i B_1 = \nu\tilde{m}'.H' \approx_{i, \tilde{l}} A_1
$$

Adding $E \equiv_i \pi(M_1).Q_2 \mid E_1$ to and removing variables $\tilde{y}$ from the first $\Rightarrow_i$ in transitions (6), by Corollary 7.1, we obtain that

$$
\nu\tilde{m}_1.(E\varphi(H_1) \mid H_{\tilde{y}})
\Rightarrow_i \nu\tilde{m}_1.(E\varphi(H_1) \mid a(x).Q_1 \mid H_{\tilde{y}})
\equiv, \nu\tilde{m}_1.(\pi(M_1\varphi(H_1)).Q_2\varphi(H_1) \mid E_1\varphi(H_1) \mid a(x).Q_1 \mid H_{\tilde{y}})
\Leftrightarrow_i \nu\tilde{m}_1.(Q_2\varphi(H_1) \mid E_1\varphi(H_1) \mid Q_1\{M_1\varphi(H_1)/x\} \mid H_{\tilde{y}})
$$

17
Adding $Q_2 \mid E_1$ to the last $\implies_i$ and removing variables $\tilde{y}$ from transitions (6), we obtain that $v\tilde{m}(.Q_2{F}(H) \mid E_1{F}(H)) = Q_1({M}(M_1{F}(H)_1)/x) \mid H_1 \downarrow \gamma$. Combining with transitions (7) and adding $\tilde{l}$, we have that $v\tilde{m}(.E{F}(H) \mid H_\gamma) = v\tilde{m}(.Q_2{F}(H) \mid E_1{F}(H') \mid H' \downarrow \gamma)$. Adding $Q_2 \mid E_1$ and $\tilde{l}$ to $A$, $B$ and removing $\tilde{y}$, we can obtain $A$, $B$ and hence $(A, B) \in \mathcal{R}$.

(c) The analysis for the cases when the input and output are both from $E$ or $F$ are similar and simpler.

2. $v\tilde{m}(.E{F}(F) \mid F_\gamma) \equiv v\tilde{m}(.E{F}(F) \mid F_\gamma)$, if $M = N$ then $P$ else $Q \mid F_1$. Then $v\tilde{m}(.E{F}(F) \mid F_\gamma) = v\tilde{m}(.E{F}(F) \mid F_1)$. From Corollary 7.1, we have $v\tilde{m}(.E{F}(F) \mid H_\gamma) = v\tilde{m}(.E{F}(F) \mid H_\gamma)$. Hence $(A, B) \in \mathcal{R}$.

3. $v\tilde{m}(.E{F}(F) \mid F_\gamma) \equiv v\tilde{m}(.E{F}(F) \mid F_\gamma)$, if $M = N$ then $P$ else $Q \mid F_1$. Then $v\tilde{m}(.E{F}(F) \mid F_\gamma) = v\tilde{m}(.E{F}(F) \mid F_1)$. From Corollary 7.1, we have $v\tilde{m}(.E{F}(F) \mid H_\gamma) = v\tilde{m}(.E{F}(F) \mid H_\gamma)$. Hence $(A, B) \in \mathcal{R}$.

4. $\tilde{v}\tilde{m}(.E{F}(F) \mid F_\gamma) \equiv \tilde{v}\tilde{m}(.E{F}(F) \mid F_\gamma)$, if $M = N$ then $P$ else $Q \mid F_1$. In this case $E \equiv \tilde{v}\tilde{m}(.E{F}(F) \mid F_\gamma) = \tilde{v}\tilde{m}(.E{F}(F) \mid F_1)$. From Corollary 7.1, we have $\tilde{v}\tilde{m}(.E{F}(F) \mid H_\gamma) = \tilde{v}\tilde{m}(.E{F}(F) \mid H_\gamma)$.

5. $v\tilde{m}(.E{F}(F) \mid F_\gamma) \equiv v\tilde{m}(.E{F}(F) \mid F_\gamma)$, if $M = N$ then $P$ else $Q \mid F_1$. Then $v\tilde{m}(.E{F}(F) \mid F_\gamma) = v\tilde{m}(.E{F}(F) \mid F_1)$. From Corollary 7.1, we have $v\tilde{m}(.E{F}(F) \mid H_\gamma) = v\tilde{m}(.E{F}(F) \mid H_\gamma)$.

18
Corollary 7.2. If $A \approx_{i,i} B$, then $A \approx_i B$.

Proof. This is a direct corollary of Theorem 7.1.

Theorem 7.2. If $A \approx_i B$, then $A \approx_{i,i} B$.

Proof. Assume $A = \nu \cdot F \approx_{i,i} \nu \cdot H = B$, to show $A \approx_{i,i} B$, we can construct the following set

$$\mathcal{R} = \{ (\nu \cdot F, \nu \cdot H) \mid \nu \cdot \nu \cdot (\prod_{i \in I} \bar{a}_i(M_i) \mid \prod_{j \in J} \bar{b}_j(c_j) \mid F_{\{\tilde{y}\}} \approx_{i,i} \nu \cdot \nu \cdot (\prod_{i \in I} \bar{a}_i(N_i) \mid \prod_{j \in J} \bar{b}_j(c_j) \mid H_{\{\tilde{y}\}}) \}$$

where (1) $\bar{c}$ is the sequence $c_1, c_2, \cdots, c_{|J|}$; (2) $a_i, b_j \notin fn(F, H)$ are pairwise-distinct names and are different from $\bar{c}, \bar{m}, \bar{n}$; (3) $\tilde{y} \subseteq dom(F)$, $\tilde{y} \subseteq dom(H)$.

For technical convenience and the readability of the proof, in the following discussion, we ignore the order between restrictions.
For notational convenience, we write if \( x \in V \) then 0 else \( P \), where \( V = \{ u_1, u_2, \ldots, u_k \} \), for

\[
\begin{align*}
  &\text{if } x = u_1 \text{ then 0} \\
  &\text{else if } x = u_2 \text{ then 0} \\
  &\quad \ldots \\
  &\text{else if } x = u_k \text{ then 0 else } P
\end{align*}
\]

Let \( C = \nu e.\nu \bar{M}.(\prod_{i \in I} \pi_i(M_i) \mid \prod_{j \in J} \bar{b}_j(c_j) \mid F_{\bar{y}}) \) and \( D = \nu e.\nu \bar{M}.(\prod_{i \in I} \pi_i(N_i) \mid \prod_{j \in J} \bar{b}_j(c_j) \mid H_{\bar{y}}) \).

Now we proceed to prove that \( \mathcal{R} \subseteq \approx_{\nu_e} \). Let \( C = \nu e.\nu \bar{M}.(\prod_{i \in I} \pi_i(M_i) \mid \prod_{j \in J} \bar{b}_j(c_j) \mid F_{\bar{y}}) \) and \( D = \nu e.\nu \bar{M}.(\prod_{i \in I} \pi_i(N_i) \mid \prod_{j \in J} \bar{b}_j(c_j) \mid H_{\bar{y}}) \). We will prove that \( \nu e.\bar{F} \approx_{\nu_e} \nu e.\bar{H} \).

First we show intermediate static equivalence between \( \nu e.\bar{F} \) and \( \nu e.\bar{H} \). According to the definition, assume \( M \varphi(F) = e N \varphi(F) \) with \( \text{vars}(M,N) \subseteq \text{dom}(F) \) and \( \text{names}(M,N) \cap (\nu \cup \bar{M}) = \emptyset \), we will prove that \( M \varphi(H) = e N \varphi(H) \). Consider \( E = a_1(x_1).a_2(x_2).\ldots.a_{|I|}(x_{|I|}) \). if \( M \{ \bar{x}/\bar{y} \} = N \{ \bar{x}/\bar{y} \} \) then \( \bar{d} \) else 0 where \( d \) is a fresh name. We put \( E \) inside \( C \) and have \( \nu e.\nu \bar{M}.(\prod_{i \in I} \pi_i(M_i) \mid \prod_{j \in J} \bar{b}_j(c_j) \mid F_{\bar{y}}) \) or \( \nu e.\nu \bar{M}.(\prod_{i \in I} \pi_i(M_i) \mid \prod_{j \in J} \bar{b}_j(c_j) \mid E \varphi(F_{\bar{y}})) \) \( \Rightarrow \) \( C_1 = \nu e.\nu \bar{M}.(\prod_{i \in I} \pi_i(M_i) \mid \prod_{j \in J} \bar{b}_j(c_j) \mid F_{\bar{y}}) \) or \( \nu e.\nu \bar{M}.(\prod_{i \in I} \pi_i(M_i) \mid \prod_{j \in J} \bar{b}_j(c_j) \mid E \varphi(F_{\bar{y}})) \) \( \Rightarrow \) \( D_1 = \nu e.\nu \bar{M}.(\prod_{i \in I} \pi_i(M_i) \mid \prod_{j \in J} \bar{b}_j(c_j) \mid H_{\bar{y}}) \) or \( \nu e.\nu \bar{M}.(\prod_{i \in I} \pi_i(M_i) \mid \prod_{j \in J} \bar{b}_j(c_j) \mid E \varphi(H_{\bar{y}})) \) \( \Rightarrow \) \( D_1 = \nu e.\nu \bar{M}.(\prod_{i \in I} \pi_i(M_i) \mid \prod_{j \in J} \bar{b}_j(c_j) \mid H_{\bar{y}}) \) if \( M \varphi(H_{\bar{y}})(\bar{M}/\bar{y}) = N \varphi(H_{\bar{y}})(\bar{M}/\bar{y}) \) then \( \bar{d} \) else 0 with \( D_1 \{ \bar{y}^d \} \) and \( D_1 \{ \bar{y}^d \} \). This requires \( M \varphi(H) = e N \varphi(H) \). Then \( \nu e.\bar{F} \approx_{\nu_e} \nu e.\bar{H} \).

1. \( \alpha = \pi.(c) \). Assume \( \nu e.\bar{F} \equiv \nu e.(\pi.(c)).P \mid F_1 \) and \( \pi.(c).P \mid F_1 \).

(a) \( a, c \notin \bar{c} \). Then consider the context \( \bar{d} \mid a(x). \) if \( x = c \) then \( d \) else 0, where \( d \) is fresh.

\[
\begin{align*}
  \nu e.\nu \bar{M}.(\prod_{i \in I} \pi_i(M_i) \mid \prod_{j \in J} \bar{b}_j(c_j) \mid \bar{d} \mid a(x). \text{if } x = c \text{ then } d \text{ else 0 } \mid F_{\bar{y}})
  \Rightarrow \nu e.\nu \bar{M}.(\prod_{i \in I} \pi_i(M_i) \mid \prod_{j \in J} \bar{b}_j(c_j) \mid P \mid F_1_{\bar{y}})
\end{align*}
\]

From the observational equivalence between \( C \) and \( D \), we can know that

\[
\nu e.\nu \bar{M}.(\prod_{i \in I} \pi_i(N_i) \mid \prod_{j \in J} \bar{b}_j(c_j) \mid \bar{d} \mid a(x). \text{if } x = c \text{ then } d \text{ else 0 } \mid H_{\bar{y}})
\Rightarrow D_1 \approx_{\nu_e} C_1
\]

For \( i \in I, j \in J \), we know that \( C_1 \{ \bar{y}^i_{a_j, b_j} \} \) and \( C_1 \{ \bar{y}^j_{a_i, b_i} \} \). Thus it should be \( D_1 \{ \bar{y}^i_{a_j, b_j} \} \) and \( D_1 \{ \bar{y}^j_{a_i, b_i} \} \). Since \( a \) is different from \( a_i, b_j \), the only possibility is that \( D_1 = \nu e.\nu \bar{M}.(\prod_{i \in I} \pi_i(N_i) \mid \prod_{j \in J} \bar{b}_j(c_j) \mid H') \) and \( H_{\bar{y}} \approx_{\nu e} H' \). Then \( \nu e.\bar{H} \approx_{\nu e} \nu e.\bar{H} \) with \( H_{\bar{y}} \approx_{\nu e} H' \). Hence we know that \( (\nu e.\bar{F}_1, \nu e.\bar{H}_1) \in \mathcal{R} \).

(b) When \( a = c_j \) with \( j \in J \) and \( c \notin \bar{c} \), consider the context \( \bar{d} \mid b_j(u).a(x). \) if \( x = c \) then \( d \mid \bar{b}_j(u) \) else 0 where \( d \) is fresh. Note that each time we consume a \( \bar{b}_j(u) \), we need to generate a new one since we require each name in \( \bar{c} \) has an output action.

(c) When \( c = c_k \) with \( k \in J \) and \( a \notin \bar{c} \), consider the context \( \bar{d} \mid b_k(v).a(x). \) if \( x = v \) then \( \bar{d} \mid \bar{b}_k(v) \) else 0 where \( d \) is fresh.

(d) When \( a = c_j \) and \( c = c_k \) with \( j, k \in J \), consider the context \( \bar{d} \mid b_j(u).b_k(v).a(x). \) if \( x = v \) then \( \bar{d} \mid \bar{b}_j(u) \mid \bar{b}_k(v) \) else 0 where \( d \) is fresh.

2. \( \alpha = nx.(\pi(x)) \). Assume \( \nu e.\bar{F} \equiv \nu e.(\pi(M)).P \mid F_1 \) and \( \nu e.(\pi(x)).P \mid \{ M/x \} \mid F_1 \) with \( x \notin \text{fv}(F, H) \).
(a) When $a \not\in \tilde{c}$, consider the context $\overline{d} \mid a(x). (d \mid \overline{a}_i(x))$ with $d, a_i$ are fresh, then

$$\nu \overline{c}. \nu \overline{m}. (\prod_{i \in I} \overline{a}_i(M_i) \mid \prod_{j \in J} \overline{b}_j(c_j) \mid \overline{d} \mid a(x).(d \mid \overline{a}_i(x)) \mid F_{\overline{y}})$$

$$\rightarrow_i C_1 = \nu \overline{c}. \nu \overline{m}. (\prod_{i \in I} \overline{a}_i(M_i) \mid \overline{a}_i(M) \mid \prod_{j \in J} \overline{b}_j(c_j) \mid P \mid F_1_{\overline{y}})$$

Similar as above analysis, we have $D \rightarrow_i D' = \nu \overline{c}. \nu \overline{m}. (\prod_{i \in I} \overline{a}_i(M_i) \mid \overline{a}_i(N) \mid \prod_{j \in J} \overline{b}_j(c_j) \mid H')$

and $H_{\overline{y}} \nu \overline{m}. \overline{a}_i (\nu \overline{m}. \overline{a}_i (\nu \overline{m}. H_1_{\overline{y}}))$. Hence we know that $(\nu \overline{m}. F_1, \nu \overline{m}. H_1) \in R$.

(b) When $a = c_j$, $j \in J$. Consider the context $\overline{d} \mid b_j(u).a(x).(d \mid \overline{a}_i(x) \mid \overline{b}_j(u))$ with $d, a_i$ are fresh.

3. $\alpha$ is a base input $a(M)$. Assume $\nu \overline{m}. F \equiv \nu \overline{m}. (a(x). P \mid F_1) \overset{a(c)}{\rightarrow_i} \nu \overline{m}. (P[M/x] \mid F_1)$.

(a) $a \not\in \tilde{c}$, consider the context $\overline{d}_i \mid \overline{a}_i(M_i) \mid d_i$ where $d_i$ is fresh;

(b) $a = c_j$ for some $j \in J$, consider the context $\overline{d}_i \mid b_j(u) \overline{a}_i(M_i) \mid d_i \mid \overline{b}_j(u)$, where $d_i$ is fresh;

(c) $a = c_j$ and $c = c_k$ with $j, k \in J$, consider the context $\overline{d}_i \mid b_j(u) b_k(v) \overline{a}_i(M_i) \mid d_i \mid \overline{b}_j(u) \mid \overline{b}_k(v)$, where $d_i$ is fresh.

4. $\alpha$ is a channel input $a(M)$. Assume $\nu \overline{m}. F \equiv \nu \overline{m}. (a(x). P \mid F_1) \overset{a(M)}{\rightarrow_i} \nu \overline{m}. (P[M/x] \mid F_1)$.

(a) $a \not\in \tilde{c}$, consider the context $\overline{d}_i \mid \overline{a}_i(M_i) \mid d_i$ where $d_i$ is fresh;

(b) $a = c_j$ for some $j \in J$, consider the context $\overline{d}_i \mid b_j(u) \overline{a}_i(M_i) \mid d_i \mid \overline{b}_j(u)$, where $d_i$ is fresh.

5. $\alpha$ is $vd. \overline{d}$. Assume $\nu \overline{m}. F \equiv \nu \overline{m}. (\overline{a}_i(M_i) \mid P \mid F_1) \overset{vd. \overline{d}}{\rightarrow_i} \nu \overline{m}_1. (P \mid F_1)$. Similar to the channel input case, whenever there is a conflict between $d$ and $a_i, b_j$, we can use Lemma A.12 to avoid it.

(a) When $a \not\in \tilde{c}$, consider the context $\overline{d} \mid a(x).f(x) \mid x \in fn(\nu \overline{m}. F, \nu \overline{m}. H)$ then 0 else $(d \mid \overline{b}_1(x))$, where $d, b_1$ are fresh, then

$$\nu \overline{c}. \nu \overline{m}. (\prod_{i \in I} \overline{a}_i(M_i) \mid \prod_{j \in J} \overline{b}_j(c_j) \mid E \mid F_{\overline{y}})$$

$$\rightarrow_i C_1 = \nu \overline{c}. \nu \overline{m}_1. (\prod_{i \in I} \overline{a}_i(M_i) \mid \prod_{j \in J} \overline{b}_j(c_j) \mid \overline{b}_1(d) \mid P \mid F_1_{\overline{y}})$$

Since $C \approx_i D$, there exist transitions

$$\nu \overline{c}. \nu \overline{m}. (\prod_{i \in I} \overline{a}_i(M_i) \mid \prod_{j \in J} \overline{b}_j(c_j) \mid E \mid H_{\overline{y}})$$

$$\rightarrow_i C_1 = \nu \overline{c}. \nu \overline{m}_1. (\prod_{i \in I} \overline{a}_i(M_i) \mid \prod_{j \in J} \overline{b}_j(c_j) \mid \overline{b}_1(d) \mid H')$$

and $H_{\overline{y}} \overset{vd. \overline{d}}{\rightarrow_i} H'$ and $\overline{m} = d, \overline{m}_1$. Thus we have $\nu \overline{m}. H \overset{vd. \overline{d}}{\rightarrow_i} \nu \overline{m}_1. H_1$ with $H_1_{\overline{y}} = H'$. Thus $(\nu \overline{m}. F_1, \nu \overline{m}_1. H_1) \in R$.

(b) When $a = c_j$ with $j \in J$, consider the context $\overline{d} \mid b_j(u).u(x).f(x) \mid x \in fn(\nu \overline{m}. F, \nu \overline{m}. H)$ then 0 else $(d \mid \overline{b}_1(x) \mid \overline{b}_j(u))$, where $d, b_j$ are fresh.
References

A Properties of Renamings

In this section we explore the closure properties w.r.t renamings which will be used in future. Technically, we need to use renamings to avoid capture caused by bound names and bound variables.

The following lemmas assert that intermediate transitions and intermediate static equivalence are closed w.r.t the application of well-formed renamings, which are used to cope with the problems caused by conflicting of bound names/variables in further discussions.

We begin this section by showing that part (2) of the Def. 4.2 (for \(\sim_i\)) is equivalent to the following statement: for any terms \(M \equiv N_1\) with \(\text{vars}(M, N) \subseteq \text{dom}(A)\), then for any \(\bar{I}, \bar{I}_2, H_1, H_2\) such that \(A = \nu \bar{I}, H_1\) and \(B = \nu \bar{I}_2, H_2\) and \(\text{names}(M, N) \cap \{\bar{I}, \bar{I}_2\} = \emptyset\), \(M \varphi(H_1) =_e N \varphi(H_2)\) iff \(M \varphi(H_2) =_e N \varphi(H_2)\).

**Lemma A.1.** Suppose \(\varphi\) is well-formed on \(\xi\) and \(\text{atoms}(M, N) \subseteq \xi\). Then \(M =_e N\) iff \(\varphi(M) =_e \varphi(N)\).

**Proof.** The \(\Rightarrow\) direction follows immediately from the fact that \(=_e\) is preserved by renaming, and we only detail the \(\Leftarrow\) direction here. Assume \(\varphi(u) = v\) for an arbitrary \(u \in \text{atoms}(M, N)\). Since \(\varphi\) is well-formed on \(\xi\),

1. if \(u \in \text{dom}(\varphi)\) then \(\{v/u\} \subseteq \varphi\).
2. if \(u \notin \xi \setminus \text{dom}(\varphi)\) then \(\varphi(u) = u = v\) and \(v \notin \text{atoms}(%\text{range}(\varphi))\)

Since \(\text{dom}(\varphi^{-1}) = \text{range}(\varphi)\), we obtain \(\varphi^{-1}(v) = u\) in either case. Hence \(\varphi^{-1}(\varphi(M)) = M\) and \(\varphi^{-1}(\varphi(N)) = N\). Since \(\varphi^{-1}\) is also a renaming, applying \(\varphi^{-1}\) to \(\varphi(M) =_e \varphi(N)\) we obtain \(\varphi^{-1}(\varphi(M)) =_e \varphi^{-1}(\varphi(N))\), namely \(M =_e N\).

**Lemma A.2.** Assume \(\text{dom}(A) = \text{dom}(B)\) and \(\varphi\) is well-formed on \(\text{fnv}(A, B)\). Then \(A \sim_i B\) iff \(\varphi(A) \sim_i \varphi(B)\).

**Proof.** 1. First we prove the \(\Rightarrow\) direction. Assume \(A \sim_i B\). We have \(\text{dom}(\varphi(A)) = \text{dom}(\varphi(B))\) since \(\text{dom}(A) = \text{dom}(B)\). Given two terms \(M, N\) with \(\text{vars}(M, N) \subseteq \text{dom}(\varphi(A))\), let \(\text{names}(M, N) \setminus \text{fnv}(\varphi(A), \varphi(B)) = \{c_1, \ldots, c_n\}\). Select \(n\) pairwise-distinct fresh names \(\{d_1, \ldots, d_n\}\) and construct a new renaming \(\hat{\varphi} = \{d_1/c_1, \ldots, d_n/c_n\}\). Let \(A = \nu n.F\) and \(B = \nu n.H\) with \(\{\bar{n}, \bar{m}\} \cap \text{names}(\varphi, M, N) = \emptyset\). We can easily verify that \(\varphi^{-1} \circ \hat{\varphi}\) is well-formed on \(\text{fnv}(\varphi(A), \varphi(B), M, N)\), \((\varphi^{-1} \circ \hat{\varphi})(\varphi(F)) = [(\varphi^{-1} \circ \hat{\varphi})(\varphi(F))], (\varphi^{-1} \circ \hat{\varphi})(\varphi(H)) = [(\varphi^{-1} \circ \hat{\varphi})(\varphi(H))].\) By Lemma A.1,

\[
M \varphi(F) =_e N \varphi(F) \\
\Leftrightarrow [(\varphi^{-1} \circ \hat{\varphi})(\varphi(F))] =_e [(\varphi^{-1} \circ \hat{\varphi})(\varphi(F))] \\
\Leftrightarrow [(\varphi^{-1} \circ \hat{\varphi})(\varphi(F))] =_e [(\varphi^{-1} \circ \hat{\varphi})(\varphi(F))] \\
\Leftrightarrow [(\varphi^{-1} \circ \hat{\varphi})(\varphi(F))] =_e [(\varphi^{-1} \circ \hat{\varphi})(\varphi(F))] \\
\Leftrightarrow M \varphi(F) =_e N \varphi(F)
\]

2. For the \(\Leftarrow\) direction, assume \(\varphi(A) \sim_i \varphi(B)\). Let \(M, N\) be two terms with \(\text{vars}(M, N) \subseteq \text{dom}(A, B)\). Let \(A = \nu n.F\) and \(B = \nu n.H\) with \(\{\bar{n}, \bar{m}\} \cap \text{names}(\varphi, M, N) = \emptyset\). Let \(\text{names}(M, N) \setminus \text{fnv}(A, B) = \{c_1, \ldots, c_n\}\) and select \(n\) pairwise-distinct fresh names \(\{d_1, \ldots, d_n\}\) to construct a new renaming as \(\hat{\varphi} = \{d_1/c_1, \ldots, d_n/c_n\}\). Then we have \(\varphi \circ \hat{\varphi}\) is well-formed on \(\xi \cup \text{fnv}(A, B, M, N)\). By Lemma A.1,

\[
M \varphi(F) =_e N \varphi(F) \\
\Leftrightarrow (\varphi \circ \hat{\varphi})(M \varphi(F)) =_e [(\varphi \circ \hat{\varphi})(N \varphi(F))] \\
\Leftrightarrow [(\varphi \circ \hat{\varphi})(M \varphi(F))] =_e [(\varphi \circ \hat{\varphi})(N \varphi(F))] \\
\Leftrightarrow [(\varphi \circ \hat{\varphi})(M \varphi(F))] =_e [(\varphi \circ \hat{\varphi})(N \varphi(F))] \\
\Leftrightarrow M \varphi(F) =_e N \varphi(F).
\]
Lemma A.3. Suppose $A \xrightarrow{\alpha} A'$, $\varrho$ is well-formed on $\xi$, $\text{fnv}(\alpha, A) \subseteq \xi$, and $\text{bnv}(\alpha) \cap \text{atoms}(\varrho) = \emptyset$. Then $\varrho(A) \xrightarrow{\beta} \varrho(A')$ where $\beta = \varrho(\alpha)$.

**Proof.** By transition induction on $A \xrightarrow{\alpha} A'$.

1. **ELSE.** If $M = N$ then $P$ else $Q \xrightarrow{\alpha} Q$ with $M, N$ are ground terms and $M \neq_N N$. Then by Lemma A.1 we obtain $\varrho(M) \neq_N \varrho(N)$ immediately.

2. **REP.** $\mu \xrightarrow{\nu n}. \nu n. (P \parallel P_r)$ where $\Gamma(P_r) = \nu n. P$. We may assume that $\{\vec{m}\} \cap \text{names}(\varrho) = \emptyset$ as capture can be avoided by $\alpha$-conversion. Then $\varrho(P_r) \xrightarrow{\alpha} \nu n. (\varrho(P) \parallel \varrho(P_r))$ follows from $\Gamma(\varrho(P_r)) = \nu n. \varrho(P)$.

3. **The cases for THEN, COMM, OUTCH, OUTT, and OPENCH.** are trivial.

4. **SCOPE.** $\nu n. A \xrightarrow{\alpha} \nu n. A'$ because $A \xrightarrow{\alpha} A'$ and $n \notin \text{names}(\alpha)$. Since $n$ may cause confliction, we select a fresh name $l$ so that $\varrho \circ \{l/n\}$ is well-formed on $\xi \cup \{n\}$. By the induction hypothesis we have $\varrho \circ \{l/n\}(A) \xrightarrow{\beta} \varrho \circ \{l/n\}(A')$ with $\beta = \varrho \circ \{l/n\}(\alpha) = \varrho(\alpha)$ and $l \notin \text{names}(\beta)$ since $n \notin \alpha$ and $l$ is fresh.

Finally we have $\varrho(\nu n. A) = \nu l. \varrho \circ \{l/n\}(A) \xrightarrow{\beta} \nu l. \varrho \circ \{l/n\}(A') = \varrho(\nu n. A')$.

5. **STRUCT.** We can easily verify that $\equiv$, is closed under $\varrho$, from which the conclusion follows immediately.

Lemma A.4. Suppose $A \xrightarrow{\alpha} A'$ and $\varrho$ is well-formed on $\xi$ and $\text{fnv}(\alpha, A) \subseteq \xi$ and $\text{bnv}(\alpha) \cap \text{atoms}(\varrho) = \emptyset$. Then $\varrho(A) \xrightarrow{\beta} \varrho(A')$ where $\beta = \varrho(\alpha)$.

**Proof.** Since $\text{fnv}(A') \subseteq \text{fnv}(A) \cup \text{atoms}(\alpha) \subseteq \xi \cup \text{bnv}(\alpha)$ and $\text{bnv}(\alpha) \cap \text{atoms}(\varrho) = \emptyset$, $\varrho$ is well-formed on $\xi \cup \text{bnv}(\alpha)$. The results holds by using Lemma A.3 several times.

Lemma A.5. Suppose $\text{fnv}(A) \subseteq \xi$, $\varrho$ is well-formed on $\xi$, and $\varrho(A) \xrightarrow{\alpha} B$, where $\text{fnv}(\beta) \subseteq \text{fnv}(\varrho)$ and $\text{bnv}(\beta) \cap \text{atoms}(\varrho) = \emptyset$. Then there exists exactly one $\alpha$ such that $\varrho(\alpha) = \beta$ and $\text{fnv}(\alpha) \subseteq \xi$. Moreover, $A \xrightarrow{\alpha} A'$ for some $A'$ such that $\varrho(A') = B$.

**Proof.** By transition induction on $\varrho(A) \xrightarrow{\beta} B$.

1. **IN.** Assume $A = a(x).P$ and $\varrho(A) = b(x).\varrho(P) \xrightarrow{b(N)} \varrho(P).\{N/x\}$ and $x$ is fresh. Since $\varrho$ is well-formed on $\xi$ and $\text{fnv}(\alpha) \subseteq \xi(\varrho)$, clearly there is exactly one $a(M)$ such that $\text{fnv}(a(M)) \subseteq \xi$, $\varrho(M) = N$. Also $A \xrightarrow{a(M)} P[M/x] = A'$ and $\varrho(A') = \varrho(P).\{N/x\}$.

2. **The cases for THEN, ELSE, REP, OUTCH, OUTT, and OPENCH.** are similar.

3. **COMM.** This case follows immediately from the fact that $\varrho$ never assign two different names in $A$ to a same name since $\varrho$ is well-formed.

4. **PAR.** Suppose $A = A_1 | A_2$ and $\varrho(A_1) \parallel \varrho(A_2) \xrightarrow{\beta_{1,2}} \nu n.(F \parallel \varrho(A_2)) = B$ from $\varrho(A_1) \parallel \varrho(A_2) \xrightarrow{\beta_{1,2}} \nu n. F$. W.I.O.G assume $\{\vec{n}\} \cap \text{names}(\varrho) = \emptyset$. By the induction hypothesis, there exists exactly one $\alpha$ such that $\varrho(\alpha) = \beta$ and $\text{fnv}(\alpha) \subseteq \xi$. Also $A_1 \xrightarrow{\alpha} \nu n. H$ with $\nu n. \varrho(H) = \nu n. F$. Hence by PAR, we obtain $A_1 | A_2 \xrightarrow{\alpha} \nu n.(H | A_2) = A'$ and $\varrho(A') = B$.

5. **SCOPE.** Assume $\varrho(A) = \nu n. D \xrightarrow{\beta_{1,2}} \nu n. D'$ because $D \xrightarrow{\beta_{1,2}} D'$ with $n \notin \text{names}(\beta)$. Since $n$ may appear in $\text{names}(\varrho)$, we need to avoid the confliction. Let

$$\vec{\beta} = \begin{cases} \varrho & \text{if } n \notin \text{range}(\varrho) \\ \varrho \circ \{l/d\} & \text{else if } \varrho(d) = n \text{ and } d \neq n \text{ and } l \text{ is fresh.} \end{cases}$$
Then ŝ is also well-formed on ξ.

If g(d) = n with d ≠ n, then we know that d /∈ fnv(A), for otherwise n ∈ g(A) which contradicts with g(A) = νn.D. Thus in either case we have g|fnv(A) = ŝ|fnv(A). Hence ŝ(A) = g(A).

Since n /∈ names(β) and fnv(β) ⊆ g(ξ), n /∈ range(ŝ) and fnv(β) ⊆ g(ξ). Let A = νm.C with m a fresh name. Then g(A) = ŝ(A) = νm.ĝ(C) = νm.|{n/m} ◦ ŝ}(C) = νm.D. Also {n/m} ◦ ŝ is well-formed on ξ ∪ {n}. By the induction hypothesis, C ≡ₐ C′ and |{n/m} ◦ ŝ}(C′) = D′, |{n/m} ◦ ŝ}(α) = β and fnv(α) ⊆ ξ ∪ {m}. Since l, n /∈ names(β), d, m /∈ names(α). Hence g(α) = |{n/m} ◦ ŝ}(α) = β. From fnv(C′) ⊆ fnv(C) ∪ atoms(α) and bnv(α) ∩ atoms(ĝ, ŝ) = ∅, we can infer |{n/m} ◦ ŝ}(C′) = |{n/m} ◦ ŝ}(C) = D′. Finally, by SCOPE, we obtain A = νm.C ≡ₚ, νm.C′ and g(νm.C′) = νm.(|{n/m} ◦ ŝ}(C′) = νm.D′.

6. STRUCT. A(α) ≡ C β , C′ ≡ B. Then there exists D such that D ≡_B A and g(D) = C. By the induction hypothesis, there exists D′ such that D ≡_B D′ and g(D′) = C′. Moreover, there exists A′ such that A′ ≡_B D′ and g(A′) = B. Hence A α , A′ for some A′ such that g(A′) = B.

Lemma A.6. Suppose fnv(A) ⊆ ξ, g is well-formed on ξ, and g(A) β , where fnv(β) ⊆ g(ξ) and bnv(β) ∩ atoms(ξ) = ∅. Then there exists exactly one α such that g(α) = β and fnv(α) ⊆ ξ. Moreover, A α , A′ for some A′ such that g(A′) = B.

Proof. Spelling out g(A) β , B we get

\[ g(A) \overset{β}{\Rightarrow}_1 B_1 \overset{β}{\Rightarrow}_1 \cdots \overset{β}{\Rightarrow}_1 B_i \overset{β}{\Rightarrow}_1 B_{i+1} \overset{β}{\Rightarrow}_1 \cdots \overset{β}{\Rightarrow}_1 B_n = B, \]

Note that \( \bigcup_{j=1}^{n} fnv(B_j) \subseteq fnv(A) \subseteq ξ \) and \( \bigcup_{j=1}^{n} fnv(B_j) \subseteq fnv(A, α) \cup bnv(α) \subseteq ξ \cup bnv(α). \) Since bnv(β) ∩ atoms(ξ) = ∅ and g(α) = β, bnv(α) ∩ atoms(ξ) = ∅. Thus g is well-formed on ξ ∪ bnv(α). Now we can use Lemma A.5 to obtain a sequence \( A \overset{β}{\Rightarrow}_1 C_n \overset{β}{\Rightarrow}_1 \cdots \overset{β}{\Rightarrow}_1 C_i \overset{β}{\Rightarrow}_1 C_{i+1} \overset{β}{\Rightarrow}_1 \cdots \overset{β}{\Rightarrow}_1 C_n = B_n; \) such that \( g(C_j) = B_j \) for each \( 1 \leq j \leq n. \) Therefore \( A \overset{α}{\Rightarrow}_1 A' \) where \( A' = C_n. \)

Lemma A.7.

1. Suppose \( A \overset{ν.π(x)}{\Rightarrow}_1 B, y ∈ V_b \) and \( y /∈ fnv(A). \) Then \( A \overset{ν.π(y)}{\Rightarrow}_1 \{y/x\}(B). \)

2. Suppose \( A \overset{ν.c.π(c)}{\Rightarrow}_1 B, d ∈ N_c \) and \( d /∈ fnv(A). \) Then \( A \overset{ν.d.π(d)}{\Rightarrow}_1 \{d/c\}(B). \)

Proof. Consider the linear proof sequence.

1. \( A ≡_B C[\overline{M}, P] \overset{ν.x.π(x)}{\Rightarrow}_1 C[P \mid \{M/x\}] ≡_B B \) and x is fresh. Then clearly we can see that \( A ≡_B C[\overline{M}, P] \overset{ν.y.π(y)}{\Rightarrow}_1 C[P \mid \{M/y\}] \equiv_1 \{y/x\}(B). \)

2. \( A ≡_B ν.ν.c. C[\overline{C}, C.P] \overset{ν.c.π(c)}{\Rightarrow}_1 C[P \mid \{M/c\}] \equiv_1 \{y/x\}(B). \)

Lemma A.8.

1. Suppose \( A \overset{ν.x.π(x)}{\Rightarrow}_1 B, y ∈ V_b \) and \( y /∈ fnv(A). \) Then \( A \overset{ν.y.π(y)}{\Rightarrow}_1 \{y/x\}(B). \)

2. Suppose \( A \overset{ν.d.π(d)}{\Rightarrow}_1 B, d ∈ N_c \) and \( d /∈ fnv(A). \) Then \( A \overset{ν.d.π(d)}{\Rightarrow}_1 \{d/c\}(B). \)

Proof. This is essentially a corollary of Lemma A.7 and Lemma A.3.

Lemma A.9. \( g(A_v) = g(Γ(A_v)) \) for any renaming g which is well-formed on fnv(A_v).

Lemma A.10. \( ≈_v \) and \( ≡_v \) are closed by well-formed renamings.
Lemma A.11. \(\approx_{i,i}\) is closed by well-formed renamings.

Proof. We construct the set:

\[
\mathcal{R} = \{ (\rho(A), \rho(B)) \mid A \approx_{i,i} B, \rho \text{ is well-formed on } fnv(A, B) \}
\]

and show that \(\mathcal{R} \subseteq \approx_{i,i}\). The intermediate static equivalence \(\rho(A) \sim_i \rho(B)\) holds immediately by Lemma A.2. For the behavior equivalence,

1. \(\rho(A) \sim_{i,i} C\). Using Lemma A.5 to remove \(\rho\), we obtain \(A \sim_{i,i} A'\) with \(\rho(A') = C\). From \(A \approx_{i,i} B\), there exist \(B \xrightarrow{\rho} B' \approx_{i,i} A'\). Applying \(\rho\) to the transition we obtain \(B \xrightarrow{\rho} B' \approx_{i,i} A'\). Let \(\rho' = \rho|_{\text{fnv}(A', B')}\). Then \(\rho'\) is well-formed on \(\text{fnv}(A', B')\) and \(\rho'(A') = C\) and \(\rho'(B') = D\) and \((C, D) \in \mathcal{R}\).

2. The analysis of the case when \(\alpha = \bar{\pi}(c)\) is similar as above.

3. \(\rho(A) \xrightarrow{b(N)}_{i,i} C\). Assume \(\text{names}(M) - \text{fn}(\rho(A), \rho(B)) = \{c_1, \ldots, c_n\}\). Choosing pairwise distinct fresh names \(d_1, \ldots, d_n\) and let \(\hat{\alpha} = \{d_1/c_1, \ldots, d_n/c_n\}\), \(\hat{\alpha}^{-1} = \{c_1/d_1, \ldots, c_n/d_n\}\) and \(N' = \hat{\alpha}(N)\). Applying \(\hat{\alpha}\) to the transition, by Lemma A.3, we have \(\rho(A) \xrightarrow{b(N')}_{i,i} \hat{\alpha}(C)\). Using Lemma A.5 to remove \(\rho\), then \(A \xrightarrow{a(M)}_{i,i} A'\) with \(\rho(a(M)) = b(N')\) and \(\rho(A') = \hat{\alpha}(C)\). From \(A \approx_{i,i} B\), there exist \(B \xrightarrow{a(M)}_{i,i} B' \approx_{i,i} A'\). Applying \(\rho\) to the transition we obtain \(B \xrightarrow{b(N')}_{i,i} B'\). Then applying \(\hat{\alpha}^{-1}\) we get \(B \xrightarrow{\hat{\alpha}^{-1}} D = \hat{\alpha}^{-1}(B')\). It is easy to verify that \(\rho' = (\hat{\alpha}^{-1} \circ \rho)|_{\text{fnv}(A', B')}\) is well-formed on \(\text{fnv}(A', B')\). And \(\rho'(A') = C\) and \(\rho'(B') = D\). Thus \((C, D) \in \mathcal{R}\).

4. \(\rho(A) \xrightarrow{\nu.x(z)}_{i,i} C\). In this case, \(x\) may occur in \(\text{fnv}(A, B)\). From \(x \notin \text{fnv}(\rho(A), \rho(B))\) and \(\text{dom}(\rho) \subseteq \text{fnv}(A, B)\), we have \(x \notin \text{range}(\rho)\). Choosing a fresh variable \(z\) and by Lemma A.7, we have \(\rho(A) \xrightarrow{\nu.z} \bar{\pi}(z)_{i,i} \{z/x\}(C)\). Now we can use Lemma A.5 to remove \(\rho\) and obtain that \(A \xrightarrow{\nu.z} B' \approx_{i,i} A'\). From \(A \approx_{i,i} B\), there exist \(B \xrightarrow{\nu.z} B' \approx_{i,i} A'\). By Lemma A.3, we have \(\rho(B) \xrightarrow{\nu.z} \rho(B')\). Then by Lemma A.8 we have \(\rho(B) \xrightarrow{\nu.z} (x/z)(\rho(B'))\). We can easily verify that \(\rho' = (x/z) \circ \rho|_{\text{fnv}(A', B')}\) is well-formed on \(\text{fnv}(A', B')\). From \(\rho'(A') = C\), we have \((C, D) \in \mathcal{R}\).

5. The analysis of the case when \(\alpha = \nu.c.\bar{\pi}(c)\) is similar as above.

Lemma A.12. \(\approx_i\) is closed by well-formed renamings.

Proof. We construct the set:

\[
\mathcal{R} = \{ (\rho(A), \rho(B)) \mid A \approx_i B, \rho \text{ is well-formed on } fnv(A, B) \}
\]

and prove \(\mathcal{R} \subseteq \approx_i\). The first two requirements in Def. 4.1 are satisfied by \(\mathcal{R}\) according to the analysis in the above proof. Now we will prove that \(\mathcal{R}\) satisfies the third requirement. Consider \(E\) with \(\text{dom}(E) \cap \text{dom}(\rho(A)) = \emptyset\) and \(\text{fn}(E) \subseteq \text{dom}(E, \rho(A))\). Now let \(A = \nu.M.F\) and \(B = \nu.M.H\) with \(\tilde{M}, \tilde{M}\) fresh. Assume \(\text{fn}(E) - \text{fnv}(\rho(A), \rho(B)) = \{v_1, \ldots, v_n\}\). Choose fresh \(v_1, \ldots, v_n\) and let \(\hat{\alpha} = \{v_1/v_1, \ldots, v_n/v_n\}\). Let \(E' = \rho^{-1}(\rho(E))\). Since \(\text{dom}(\rho(E)) \cap \text{dom}(\rho(A)) = \emptyset\) and \(\text{fnv}(\rho(E)) \subseteq \{v_1, \ldots, v_n\} \cup \text{fnv}(\rho(A), \rho(B))\), we can deduce that \(\text{dom}(E') \cap \text{dom}(A) = \emptyset\) and \(\text{fn}(E') \subseteq \{v_1, \ldots, v_n\} \cup \text{fnv}(A, B)\). Thus we have \(C = \nu.M.(E' \varphi(F) | F) \approx_i \nu.M.(E' \varphi(H) | H) = D\) and \(\text{fn}(C, D) \subseteq \{v_1, \ldots, v_n\} \cup \text{fnv}(A, B)\). Let \(\rho' = \rho^{-1} \circ \rho|_{\text{fnv}(C, D)}\). We can easily know that \(\rho'\) is well-formed on \(\text{fnv}(C, D)\) and \(\rho(C) = \nu.M.(E \varphi(F) | \rho(F))\) and \(\rho(D) = \nu.M.(E \varphi(H) | \rho(H))\). Thus \((\nu.M.(E \varphi(F) | \rho(F)), \nu.M.(E \varphi(H) | \rho(H)) \in \mathcal{R}\).

B Proofs in Section 5

The proofs of the following Lemmas B.1 and B.2 are similar to Lemma 4.5 (the case for \(\equiv_i\)) and Proposition A.6 in [2] respectively.
Lemma B.1. \( \simeq \equiv \) is the same as \( \equiv \simeq \).

Proof. Consider the linear proof sequences of \( \simeq \) and \( \equiv \). We use \( \simeq^1 \) and \( \equiv^1 \) to denote a single step of rewriting. First we can prove that \( A \simeq^1 C \equiv^1 B \) then there exists \( D \) such that \( A \equiv^1 D \simeq^1 B \) by case analysis. Then if \( A \simeq^1 \cdots \simeq^1 \equiv^1 \cdots \equiv^1 B \), using the above result several times we can swap all the \( \simeq^1 \) and \( \equiv^1 \) and obtain that \( A \equiv^1 \cdots \equiv^1 \simeq^1 \cdots \simeq^1 B \).

Lemma B.2. If \( A_r \equiv B_r \) then \( \Gamma(A_r) \equiv \Gamma(B_r) \).

Proof. By induction on the number of rewriting steps of \( \equiv \). The base step is straightforward. For the inductive step, assume \( A_r \equiv C_r \equiv B_r \). By induction hypothesis we have \( \Gamma(A_r) \equiv \Gamma(C_r) \equiv \Gamma(B_r) \). An application of Lemma B.1 gives \( \Gamma(A_r) \equiv \Gamma(B_r) \).

Lemma 5.4 If \( A_r \overset{\sigma}{\to} A'_r \) with \( f\nu(A_r) \cap \nu(\alpha) = \emptyset \), then \( \Gamma(A_r) \overset{\sigma}{\to} \Gamma(A'_r) \) for some \( B_r \).

Proof. Consider the normalized derivation of transition of \( A_r \overset{\sigma}{\to} A'_r \).

1. \( A_r \equiv C[\pi(c).P_r] \overset{\pi\langle c \rangle}{\longrightarrow} C[\pi(c).P_r] \equiv A'_r \). By Lemma 5.1 and Lemma B.2, we have that

\[
\Gamma(A_r) \equiv \equiv \nu\nu_1,\nu\nu_2,\nu[\pi(c).P\phi(G)] \overset{\pi\langle c \rangle}{\longrightarrow} \Gamma(A'_r)
\]

where \( \Gamma(C) = \nu\nu_1,\nu\nu_2,\nu P \), \( \Gamma(P_r) = \nu\nu P \) and \( \Gamma[\pi(c).P_r] = \nu\nu\nu[\pi(c).P] \). Using Lemma 5.1 again, we have \( \Gamma(A'_r) \equiv \equiv \Gamma[C[\pi(c).P_r]] = \nu\nu_1,\nu\nu_2,\nu[\pi(c).P\phi(G)] \). Using Lemma B.1 to swap \( \equiv \), and \( \simeq \), then

\[
\Gamma(A_r) \equiv \equiv \nu\nu_1,\nu\nu_2,\nu[\pi(c).P\phi(G)] \overset{\pi\langle c \rangle}{\longrightarrow} \Gamma(A'_r)
\]

that is to say there exist \( A \) and \( A' \) such that \( \Gamma(A_r) \equiv A \overset{\pi\langle c \rangle}{\longrightarrow} \Gamma(A'_r) \). By Lemma 5.2, there exists \( B \) such that \( \Gamma(A_r) \overset{\pi\langle c \rangle}{\longrightarrow} \Gamma(A'_r) \). The result holds.

2. The other cases are similar.

Lemma B.3. Assume \( \sigma = \sigma_1 \cup \sigma_2 \) is cycle-free. Then

1. \( \sigma^* \circ \sigma_1^* = \sigma^* \circ \sigma_2^* = \sigma^* \).
2. \( \sigma = (\sigma_1^* \cup \sigma_2^*) = (\sigma_1^* \sigma_2^*)^* \cup (\sigma_1^* \sigma_2^*)^* \).
3. \( \sigma, \sigma^* = (\sigma_1 \sigma_2^*)^* \) and \( \sigma, \sigma^* = (\sigma_1^* \sigma_2)^* \).

Proof. 1. For any \( x \in \text{dom}(\sigma) \), we have \( (x\sigma_1)\sigma^* = x\sigma^* \). In other words \( \sigma^* = \sigma^* \circ \sigma_1 \). Hence \( \sigma^* = \sigma^* \circ \sigma_1 = \sigma^* \circ \sigma_1 \circ \sigma_1 = \cdots = \sigma^* \circ \sigma_1 \). The proof for \( \sigma^* \circ \sigma_2^* = \sigma^* \) is similar.

2. We first show \( \sigma^* \circ (\sigma_1^* \cup \sigma_2^*) = \sigma^* \). Suppose \( x \in \text{dom}(\sigma_1) \). Then \( x(\sigma^* \circ (\sigma_1^* \cup \sigma_2^*)) = x(\sigma_1^* \cup \sigma_2^*)\sigma^* = (x\sigma_1^*)\sigma^* = x(\sigma^* \circ \sigma_1^*) = x\sigma^* \). Similarly we can derive \( x(\sigma^* \circ (\sigma_1^* \cup \sigma_2^*)) = x\sigma^* \) when \( x \in \text{dom}(\sigma_2) \). Hence \( \sigma^* \circ (\sigma_1^* \cup \sigma_2^*) = \sigma^* \). From this we have \( \sigma^* = \sigma^* \circ (\sigma_1^* \cup \sigma_2^*) = \sigma^* \circ (\sigma_1^* \cup \sigma_2^*)^* = (\sigma_1 \cup \sigma_2^*)^* \). Therefore,

\[
(\sigma_1^* \cup \sigma_2^*)^* = (\sigma_1^* \cup \sigma_2^* \sigma_1^*) = (\sigma_1 \cup \sigma_2^*)^* \circ (\sigma_1^* \cup \sigma_2^*) = (\sigma_1 \cup \sigma_2^*)^* \circ (\sigma_1^* \cup \sigma_2^*) = (\sigma_1^* \sigma_2^*)^* \cup (\sigma_1 \sigma_2^*)^*.
\]

3. Since \( \sigma = \sigma_1 \cup \sigma_2 \), \( \sigma^* = \sigma^* \circ (\sigma_1 \cup \sigma_2) = \sigma_1 \sigma_2 \sigma^* \). The result follows immediately using 2.

Lemma B.4. Suppose \( \theta \) and \( \sigma \) are idempotent substitutions such that \( \text{dom}(\theta) \cap \text{dom}(\sigma) = \emptyset \) and \( \theta \cup \sigma \) is cycle-free. Then

1. \( (\sigma \theta)^* = \sigma(\theta \sigma)^* \) and \( (\theta \sigma)^* = \theta(\sigma \theta)^* \).
Lemma B.5.

Proof. 1. As shown in the proof of the above lemma and the hypothesis that $\theta$ and $\sigma$ are idempotent, we have $(\theta \cup \sigma)^* = (\theta \cup \sigma)^* \cup (\theta \cup \sigma)^*$, as well as $(\theta \cup \sigma)^* \circ (\theta \cup \sigma) = \theta(\theta \cup \sigma)^* \cup \sigma(\theta \sigma)^*$. Hence $(\theta \sigma \cup \theta \theta)^* = \theta(\theta \sigma)^*$ and $(\sigma \theta)^* = \sigma(\theta \sigma)^*$.

2. Let $\hat{\theta} = (\theta \sigma)^*$. Then

$$
\hat{\theta} \circ [\theta(\sigma_1 \cup \sigma_2)] = [\theta(\sigma_1 \cup \sigma_2)] \hat{\theta} = (\theta(\sigma_1 \cup \sigma_2) \hat{\theta}) = (\theta(\sigma_1 \cup \sigma_2) \hat{\theta} \circ (\theta \sigma) \hat{\theta}) = \hat{\theta} \circ (\theta \sigma) \hat{\theta} = \hat{\theta} \circ (\theta \sigma) = \hat{\theta}.
$$

Therefore $\hat{\theta} = \hat{\theta} \circ (\theta(\sigma_1 \cup \sigma_2)) = \hat{\theta} \circ (\theta(\sigma_1 \cup \sigma_2))^* = (\theta(\sigma_1 \cup \sigma_2))^*$. Moreover $(\hat{\theta} \sigma_1)^* = (\theta \sigma_1)^*$ for $(\theta \sigma_1)^* = (\theta \sigma_1 \cup \sigma_2)^* = (\theta(\sigma_1 \cup \sigma_2))^*$. Observing that $(\hat{\theta} \sigma_1)(\theta \sigma_1) = ((\hat{\theta} \sigma_1)(\theta \sigma_1)) \sigma_2 = (\theta(\sigma_1 \cup \sigma_2)(\theta(\sigma_1 \cup \sigma_2))^*$, then we have $(\hat{\theta} \sigma_1)^* \sigma_2 = (\theta(\sigma_1 \cup \sigma_2))^*$. Furthermore we have $\hat{\theta} \circ [(\theta \sigma_1)^* \sigma_2] = [(\theta \sigma_1)^* \sigma_2] \hat{\theta} = [(\theta \sigma_1)^*] \sigma_2 \hat{\theta} = [\theta(\sigma_1 \cup \sigma_2)]^* \hat{\theta} = \hat{\theta}$. Hence $\hat{\theta} = \hat{\theta} \circ (\theta \sigma_1)^* \sigma_2 = (\theta \sigma_1)^* \sigma_2$.

Lemma B.5. For any open process $A_r$, $A_r \equiv A_r \varphi(A_r)^*$.

Proof. Assume $A_r$ contains $n$ active substitutions each is of the form $\{M/x\}$. Since the active substitutions in $A_r$ are required to be cycle-free, they can be ordered as $\sigma_1, \ldots, \sigma_n$, where $\sigma_i = \{M_i/x_i\}$, in such a way that $x_j \not\in \text{range}(\sigma_i)$ for any $1 \leq i \leq n$ and $j \geq i$. Then $\varphi(A_r)^* = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_n$. Therefore $A_r \equiv A_r \sigma_n \equiv (A_r \sigma_n) \sigma_{n-1} \cdots \equiv \cdots \equiv (A_r \sigma_{n-1}) \cdots \sigma_1 = A_r \varphi(A_r)^*$.

Now we proceed to prove Lemma 5.6, which requires some preparation. We need to decompose function $\Gamma$ (transforming an extended process into an intermediate one, as defined in Fig. 3) into two independent steps, namely functions $A$ and $S$ given below. We say an extended process $A_r$ is open when it contains no restricted variable and every name binder is under an input, an output, or a conditional. For example $a(x).\nu n.\pi(M) \mid \{M/y\}$ is an open process while $\nu n.\{a(x), a(y) \mid \{M/y\}\}$ is not. We write $\varphi(A_r)$ for the union of active substitutions of an open process $A_r$. We say $A_r$ is applied when each variable in $\text{dom}(A_r)$ occurs only once.

The function $A$ is similar to $\Gamma$, but yields an applied process which is still structurally equivalent to the original one. The purpose of $A$ is to apply all the active substitutions in an extended process, while the purpose of $S$ is to pull out all name binders in an extended process.

Definition B.1 (Applied function $A$).

\[
\begin{align*}
A(0) &= 0, & A(u.x,P_r) &= u(x).P_r, & A(!P_r) &= !P_r, \\
A(\pi(N),P_r) &= \pi(N).P_r, & A(A_r | B_r) &= U_n.\nu n.(C_r | D_r) \varphi(C_r | D_r)^* & \text{where } A(A) = \nu n. C_r 	ext{ and } A(B) = \nu n. D_r, \\
A(\nu n. A_r) &= \nu n. A(A_r), & A(\{M/x\}) &= \{M/x\}, & A(\nu x. A_r) &= A(A_r) \times x.
\end{align*}
\]

Definition B.2 (Scope function $S$).

\[
\begin{align*}
S(0) &= 0, & S(!P_r) &= !P_r, \\
S(u.x,P_r) &= \nu n. u(x).Q_r, & \text{where } S(P_r) &= \nu n. Q_r, \\
S(\pi(N),P_r) &= \nu n. \pi(N).Q_r, & \text{where } S(P_r) &= \nu n. Q_r, \\
S(\text{if } M = N \text{ then } P_r \text{ else } Q_r) &= \nu n. \nu m.(\text{if } M = N \text{ then } P_r \text{ else } Q_r)^* & \text{where } S(P_r) &= \nu n. P_r^* 	ext{ and } S(Q_r) &= \nu n. Q_r, \\
S(A_r | B_r) &= \nu n. \nu m.(C_r | D_r), & \text{where } S(A_r) &= \nu n. C_r \text{ and } S(B_r) &= \nu n. D_r, \\
S(\nu n. A_r) &= \nu n. S(A_r), & S(\{M/x\}) &= \{M/x\}, \\
S(\nu x. A_r) &= \nu n. \nu x. B_r, & \text{where } S(A_r) &= \nu n. B_r.
\end{align*}
\]

28
Lemma B.6. \( A_r \equiv A(A_r) \) for any extended process \( A_r \).

Proof. By induction on the structure of \( A_r \). It suffices to prove that for any extended process \( A_r \), \( A_r \equiv A(A_r) \) and \( A(A_r) \) is of the form \( νn.A'_r \) for some open and applied process \( A'_r \). We focus on parallel composition and restriction here as other cases are trivial.

1. Suppose the extended process has the form \( A_r | B_r \). By the induction hypothesis, we get \( A_r \equiv A(A_r) = νn.A'_r \) and \( B_r \equiv A(A_r) = νn.B'_r \). By the definition of \( A \) on parallel composition, we obtain \( A(A_r \mid B_r) = νn.A'_r \mid B'_r \). [\ref{lemma:A_parallel}]. By Lemma B.5, \( A_r \mid B_r \equiv νn.νm.(A'_r \mid B'_r)^* \). By the induction hypothesis \( A_r \equiv A(A_r) \) and \( C_r \mid \{M/x\} \mid D_r \) are open and applied processes, i.e. \( x \) does not occur in \( C_r \) or \( D_r \). Hence

\[
νx.A_r \equiv νx.νn.(C_r \mid \{M/x\} \mid D_r) = νn.(C_r \mid νx.\{M/x\} \mid D_r) = A(νx.A_r).
\]

Lemma B.7. Let \( A_r \) be an open extended process. Then \( Γ(A_r) = Γ(A_r,φ(A_r)^* = S(A_r,φ(A_r)^*) \).

Proof. Observe that \( S(\sigma.A) = S(\sigma.A) \). We now prove \( Γ(A_r) = S(\sigma.A_r,φ(A_r)^* = νn.G \) and \( φ(A_r)^* = φ(G) \) by induction on the structure of \( A_r \). We only consider the parallel composition here as the other cases are easier. Assume \( A_r = A'_r \mid A''_r \). By the induction hypothesis we have

\[
Γ(A'_r) = S(\sigma.A'_r,φ(A'_r)^* = /n.F \quad φ(A'_r)^* = φ(F) \quad Γ(A''_r) = S(\sigma.A''_r,φ(A''_r)^* = νm.H \quad φ(A''_r)^* = φ(H).
\]

By Lemma B.3 (1) we have \( φ(A'_r \mid A''_r)^* = φ(A'_r \mid A''_r)^* \) and also \( φ(A'_r \mid A''_r)^* \times φ(A''_r)^* = φ(A''_r \mid A''_r)^* \). Thus

\[
S((A'_r \mid A''_r)^* \times φ(A'_r))^* = S(A'_r,φ(A'_r)^* \mid A''_r,φ(A''_r)^*),φ(F \mid H)^*
= νn.νr.(F \mid H)φ(F \mid H)^* = Γ(A'_r \mid A''_r).
\]

Hence \( Γ(A_r) = S(\sigma.A_r,φ(A_r)^* = Γ(A_r,φ(A_r)^*) \).

Note that we can extend the definition of \( S \) to context by defining \( S(\{\} = (\cdot\{\} \) where \( (\cdot \) is a hole for restrictions. For example, assume \( C_r = νn.\pi(b) | \{\} | νm.\pi(c) \) \( S(\pi(c)) = νn.\pi.νm.\pi(\pi(b) | \{\} | \pi(c)) \). Assume \( P_r = νl.a(x) \) then \( S(C_r[P_r]) = νn.νl.νm.\pi(\pi(b) | a(x) | \pi(c)) \).

Lemma B.8. Let \( Γ(A_r) = νn.G[F] \) where \( G \) is an intermediate framed evaluation context. Then

1. \( A(A_r) = C_r[A_r] \) where \( C_r \) is open and applied and \( C_r \) is an applied evaluation context.
2. \( S(B_r) = νl.F, S(\pi(c)) = νn.\pi.νm.\pi, \{\pi(c)\} = \{\pi(c)\} \).

Proof. The results are direct consequences of the following three statements:

1. Suppose the extended process has the form \( A_r \mid B_r \). By the definition of \( Γ(-) \) we have

\[
Γ(A'_r) = νn.F_r \quad Γ(A''_r) = νm.F_r 
\]

To prove these statements, we apply induction on the structure of \( A_r \). We shall only detail the proof for parallel composition here as the other cases are easier. Let \( A_r = A'_r \mid A''_r \). By the definition of \( Γ(-) \) we have

\[
Γ(A'_r) = νn_1,F_1, Γ(A''_r) = νm_2,F_2 
\]

\[
(\pi(c) \equiv \{\pi(c)\}) = G[F]
\]

Since \( G \) has only one hole, there are only three possibilities for the position of \( F \):
Case 1 $F = (F_1 | F_2)\varphi(F_1 | F_2)^*$. Then $\mathcal{G} = [\cdot]$. By the induction hypothesis, there exist $\tilde{n}_{11}, \tilde{n}_{12}, \tilde{n}_{21}, \tilde{n}_{22}, B^1_r, B^2_r$ such that

\[
\begin{align*}
\mathcal{A}(A_r^1) &= \nu\tilde{n}_{11}.B^1_r \\
\mathcal{S}(B^1_r) &= \nu\tilde{n}_{12}.F_1 \\
\{\tilde{n}_{11}, \tilde{n}_{12}\} &= \{\tilde{m}_1\} \\
\varphi(B^1_r) &= \varphi(F_1) \\
\mathcal{G}^1_r &= [\cdot] \\
\mathcal{A}(A_r^2) &= \nu\tilde{n}_{21}.B^2_r \\
\mathcal{S}(B^2_r) &= \nu\tilde{n}_{22}.F_2 \\
\{\tilde{n}_{21}, \tilde{n}_{22}\} &= \{\tilde{m}_2\} \\
\varphi(B^2_r) &= \varphi(F_2) \\
\mathcal{G}^2_r &= [\cdot]
\end{align*}
\]

Hence $\mathcal{A}(A_r) = \nu\tilde{n}_{11}.\nu\tilde{n}_{12}.(B^1_r | B^2_r)\varphi(B^1_r | B^2_r)^*$, which shows (1) (taking $\tilde{t} = \nu\tilde{n}_{11}.\nu\tilde{n}_{21}, \mathcal{G}_r$ as the empty context, and $B_r = (B^1_r | B^2_r)\varphi(B^1_r | B^2_r)^*$).

By Lemma B.7,

\[
\mathcal{S}((B^1_r | B^2_r)\varphi(B^1_r | B^2_r)^*) = \Gamma(B^1_r | B^2_r) = \nu\tilde{n}_{12}.\nu\tilde{n}_{22}.(F_1 | F_2)\varphi(F_1 | F_2)^*.
\]

Moreover all the bound names of an open process can not appear in its active substitutions, we have $\varphi(B^1_r | B^2_r)^* = \varphi(F_1 | F_2)^*$, which gives (3).

Case 2 $F$ is inside $F_1\varphi(F_1 | F_2)^*$. For simplicity assume $\sigma = \varphi(F_1 | F_2)^*$. Then $F_1 = \mathcal{G}_r[H_1]$ where $H_1\sigma = F$ and $(\mathcal{G}_r[\cdot] | F_2)\sigma = \mathcal{G}[\cdot]$. By the induction hypothesis we have

\[
\begin{align*}
\mathcal{A}(A_r^1) &= \nu\tilde{k}_1.\nu\tilde{n}_{12}.(\mathcal{G}_r[\cdot] | B^1_r)\varphi(\mathcal{G}_r[\cdot] | B^1_r)^* \\
\mathcal{S}(B^1_r) &= \nu\tilde{k}_1.H_1 \\
\mathcal{S}(\mathcal{G}_r) &= \nu\tilde{n}_{12}.\mathcal{G}_r \\
\{\tilde{n}_{11}, \tilde{n}_{12}, \tilde{k}_1, \tilde{k}_2\} &= \{\tilde{m}_1\}
\end{align*}
\]

Hence

\[
\mathcal{A}(A_r^1 | A_r^2) = \nu\tilde{k}_1.\nu\tilde{n}_{12}.(\mathcal{G}_r[\cdot] | B^1_r | B^2_r)\varphi(\mathcal{G}_r[\cdot] | B^1_r | B^2_r)^* = \nu\tilde{k}_1.\nu\tilde{n}_{12}.(\mathcal{G}_r[\cdot] | B^2_r)\sigma.
\]

This shows (1).

\[
\mathcal{S}((\mathcal{G}_r[\cdot] | B^1_r | B^2_r)\sigma) = \mathcal{S}(\mathcal{G}_r[\cdot] | B^1_r | B^2_r)\sigma = \nu\tilde{n}_{12}.\nu\tilde{k}_2.\nu\tilde{n}_{12}.\nu\tilde{n}_{22}.(\mathcal{G}_r[H_1] | F_2).
\]

Since $\{\tilde{n}_{11}, \tilde{n}_{12}, \tilde{n}_{21}, \tilde{n}_{22}, \tilde{k}_1, \tilde{k}_2\} = \{\tilde{m}_1, \tilde{m}_2\}$, this shows (2).

Here we have $\varphi(\mathcal{G}_r[\cdot] | B^1_r | B^2_r)^* = \varphi(F_1 | F_2)^*$, which gives (3).

Case 3 $F$ is inside $F_2\varphi(F_1 | F_2)^*$. This case is similar.

**Lemma B.9.** Suppose $\Gamma(A_r) \equiv \nu\tilde{m}.\mathcal{G}[\cdot]$. There exists an applied process $B_r$ such that

1. $A_r \equiv B_r$ and $B_r = \mathcal{C}_r[D_r]$ where $D_r$ is open and applied and $\mathcal{C}_r$ is an applied evaluation context.
2. $S(D_r) = \nu\tilde{l}.F$, $S(\mathcal{C}_r) = \nu\tilde{n}_{1,2}.(\cdot).\nu\tilde{n}_{1,2}.\mathcal{G}$, $\{\tilde{n}_{1,2}, \tilde{m}_{1,2}\} = \{\tilde{m}\}$.

**Proof.** By induction on the length of the linear proof sequence for $\Gamma(A_r) \equiv \nu\tilde{m}.\mathcal{G}[\cdot]$. The base step when the length is 0 follows from Lemma B.8. For the inductive step, we discuss by case analysis on the last axiom used in deriving $\equiv$. We only detail the proof for the case when the last axiom is the commutative law. The other cases are similar. Assume $\Gamma(A_r) \equiv [\mathcal{C}[A | B] \equiv \mathcal{C}[B | A] = \nu\tilde{m}.\mathcal{G}[\cdot]$. By the induction hypothesis, we can deduce that there exists an applied process $C_r[A_r | B_r]$ such that

\[
\begin{align*}
A_r &\equiv [C_r[A_r | B_r]] \\
S(A_r^1) &= \nu\tilde{n}_{1,2}.A \\
S(B_r^1) &= \nu\tilde{n}_{2,2}.B \\
S(C_r) &= \nu\tilde{n}_{1,2}.(\cdot).\nu\tilde{n}_{1,2}.\mathcal{G} \\
\nu\tilde{l}.\nu\tilde{n}_{1,2}.\nu\tilde{n}_{1,2}.\nu\tilde{l}_{2,2}.\mathcal{G} &\equiv \mathcal{C}
\end{align*}
\]

30
where $A'_r, B'_r$ are open and applied processes, $C'_r$ is an applied evaluation context and $G'$ is an intermediate framed evaluation context.

We construct a process $B_r$ by letting $B_r = C'_r[B'_r | A'_r]$ and clearly $B_r$ is also applied and $B_r \equiv A_r$. Moreover according to Lemma B.7, $\Gamma(B_r) = S(B_r) = \nu l, \nu \bar{m}_2, \nu \bar{m}_1, \nu l, G'[B | A]$. Since $C[B | A] = \nu \bar{m}_n G[F] and \nu l_1, \nu \bar{m}_1, \nu \bar{m}_2, \nu l_2, G' = C$, it means there is $k$ such that $S(B_r) = \nu k, G[F]$ and $\{k\} = \{\bar{m}\}$. Using Lemma B.8, there exist $C_r, D_r$ such that $B_r = C_r[D_r]$ such that $S(D_r) = \Gamma(D_r) = \nu l, F$, $S(C_r) = \Gamma(C_r) = \nu \bar{s}_1, (\cdot), \nu \bar{s}_2, G'$ and $\{\bar{s}, \bar{l}, \bar{s}_1\} = \{k\} = \{\bar{m}\}$. This concludes the proof.

**Lemma B.10.** Suppose $\Gamma(A_r) = \nu \bar{m}, G$ where $G$ is an intermediate framed process. Then $\nu \bar{m}, \varphi(G) \equiv \phi(A_r)$.

**Proof.** The proof proceeds by induction on the structure of $A_r$ (which is an extended process). The case when $A_r$ is a plain process is trivial.

1. $A_r = C_r | D_r$ for some extended processes $C_r, D_r$. Assume $\Gamma(C_r) = \nu \bar{m}, F$ and $\Gamma(D_r) = \nu \bar{m}, H$. By the induction hypothesis, $\phi(C_r) \equiv \nu \bar{m}, \varphi(F)$ and $\phi(D_r) \equiv \nu \bar{m}, \varphi(H)$. Hence $\phi(A_r) = \phi(C_r) \ | \ \phi(D_r) \equiv \nu \bar{m}, \nu \bar{m}, \varphi(F) \ | \ \varphi(H)) \equiv \nu \bar{m}, \varphi(F) | H)$. From $\Gamma(A_r) = \nu \bar{m}, \nu \bar{m}, G(F \ | \ H), \varphi(F \ | \ H)^\ast$, the conclusion holds.

2. $A_r = v x . C_r$. Assume $\Gamma(C_r) = \nu \bar{m}, F$. Then $\Gamma(A_r) = \nu \bar{m}, F_x \nu$. By the induction hypothesis, $\phi(C_r) \equiv \nu \bar{m}, \varphi(F)$. Hence $\phi(A_r) = v x . \phi(C_r) \equiv \nu \bar{m}, \nu \bar{m}, \varphi(F) \equiv \nu \bar{m}, \varphi(F) \ \nu (note\ that\ x\ occurs\ only\ once\ in\ F)$.

3. $A_r = v m . C_r$. Assume $\Gamma(C_r) = \nu \bar{m}, F$. Then $\Gamma(A_r) = \nu m, \nu \bar{m}, F$. By the induction hypothesis, $\phi(C_r) \equiv \nu \bar{m}, \varphi(F)$. Hence $\phi(A_r) = v m . \phi(C_r) \equiv \nu m, \nu \bar{m}, \varphi(F)$.

**Lemma 5.6** Assume $A_r$ is closed and $\Gamma(A_r) \stackrel{\alpha_r}{\Rightarrow} A$. Then there exists a closed $A'_r$ such that $A_r \stackrel{\alpha_r}{\Rightarrow} A'$ and $\Gamma(A'_r) \simeq A$.

**Proof.** By induction on the normalized derivation of $\Gamma(A_r) \stackrel{\alpha_r}{\Rightarrow} A$. In the following $G$ denotes a framed evaluation context.

1. $\Gamma(A_r) \equiv \nu \bar{m}, G(a(x).P) \overset{a(M)}\Rightarrow, \nu \bar{m}, G[P \{M \varphi(G)/x\}] \equiv, A$. By Lemma B.9, there exists an applied $B_r$ such that $B_r \equiv A_r and B_r = C_1[a(x).P]$ where $S(P_r) = \nu l \cdot P$, $S(C_r) = \nu \bar{m}, (\cdot), \nu \bar{m}, G$ and $\{\bar{m}, \bar{m}, \bar{l}\} = \{\bar{m}\}$. Hence dom$(A_r) = dom(B_r)$ and $fv(A_r) = fv(B_r)$. Let $B'_r = C_1[P_r \{M/x\}]$. Then clearly we can deduce $B_r \overset{a(M)}\Rightarrow B'_r$ from the rules in Fig. 2. Observing that $\Gamma(P_r) = S(P_r) = \nu l, P \Gamma(C_r) = S(C_r) = \nu \bar{m}, (\cdot), \nu \bar{m}, G$, by Lemma 5.1 we have that

$$\Gamma(B'_r) = \nu \bar{m}, \nu \bar{m}, \nu \bar{m}, G \{M \varphi(G)/x\} \simeq \nu \bar{m}, G[P \{M \varphi(G)/x\}] \equiv, A$$

By Lemma B.1, there exists $C = \nu k, H$ such that $\Gamma(B'_r) \equiv, C \simeq A$.

2. $\Gamma(A_r) \equiv \nu \bar{m}, G[P_r] \overset{\rho_r}{\Rightarrow}, \nu \bar{m}, \nu \bar{m}, G[P \{P_r\}] \equiv, A$ with $\Gamma(P_r) = \nu \bar{m}, P$. Then there exists an applied $B_r$ such that $B_r \equiv A_r and B_r = C_1[P_r]$ and $S(C_r) = \nu \bar{m}, (\cdot), \nu \bar{m}, G$ with $\{\bar{m}, \bar{m}, \bar{m}\} = \{\bar{m}\}$. Obviously $\Gamma(P_r) = S(P_r) = \nu \bar{m}, P$. Hence $B_r \overset{\rho_r}{\Rightarrow} C_r[P_r \{P_r\} = B'_r and \Gamma(B'_r) = \nu \bar{m}, \nu \bar{m}, \nu \bar{m}, \nu \bar{m}, G[P \{P_r\}] \simeq \nu \bar{m}, \nu \bar{m}, G[P \{P_r\}] \equiv, A$. Similarly there exists a closed $A'_r$ such that $A_r \equiv B'_r and \Gamma(A'_r) \simeq A$.

3. The other cases are similar.

The definitions of labeled bisimilarity $\simeq$ and intermediate labeled bisimilarity $\simeq_{i}$ encompass not only behavioral equivalence on process dynamics, but also static equivalence for the partial environmental knowledge exposed by processes. Before proving Theorem 5.1, we need to establish some important properties of static equivalence, as stated in the following Lemma B.11, Lemma B.10 and Lemma B.12.

**Lemma B.11.** $\sim_i$ is an equivalence relation closed w.r.t. $\simeq$ and $\equiv$. 31
Proof. For \(\equiv\), we observe that when \(A \equiv B\), \(\nu \nu. F = \nu \nu. H\) and \(\varphi(F) = \varphi(H)\). Since \(\equiv\), is an equivalence, we know that \(\sim_i\) is an equivalence relation closed w.r.t. \(\equiv\).

For \(\sim\), the proof goes by induction on the length of the linear proof sequence for \(\sim\). When the length is 0, the result holds trivially. For the inductive step, w.l.o.g., we may assume \(A \sim A' \sim B \sim C\). By the induction hypothesis, we have \(A \sim B\). Now we show \(A \sim C\) as follows:

1. \(B = C[D[M/z]] \simeq C[D[N/z]] = C\) and \(M =_\nu N\). Assume \(C[D] = \nu \nu. F\). Then for each \(x \in \text{dom}(A)\) we have \(x \varphi(F[M/z]) =_\nu x \varphi(F[N/z])\). Let \(A = \nu \nu. H\). Since \(A \sim B\), for any \(N_1, N_2\) with \(\text{names}(N_1, N_2) \cap \{\tilde{m}_1, \tilde{m}_2\} = \emptyset\), \(N_1 \varphi(H) =_\nu N_2 \varphi(H)\) iff \(N_1 \varphi(F[M/z]) =_\nu N_2 \varphi(F[N/z])\). Since \(M =_\nu N\), \(N_1 \varphi(F[M/z]) =_\nu N_1 \varphi(F[N/z])\) and \(N_2 \varphi(F[M/z]) =_\nu N_2 \varphi(F[N/z])\). Thus \(N_1 \varphi(H) =_\nu N_2 \varphi(H)\) iff \(N_1 \varphi(F[N/z]) =_\nu N_2 \varphi(F[N/z])\). Therefore \(A \sim C\).

2. According to Def. 4.2 for \(\sim_{i}\), \(A \sim_{i} C\) holds immediately for the cases when \(B = \nu \nu. \nu. D = \nu \nu. D\) and when \(B = \nu \nu. \nu. D. D\). Hence from Def. 2.3 we know that \(A \sim_{i} B\).

Lemma B.12. Let \(A_r\) and \(B_r\) be two closed extended processes. Then \(A_r \sim B_r\) iff \(\Gamma(A_r) \sim_{i} \Gamma(B_r)\).

Proof. 1. \(\Longleftarrow\) Let \(M, N\) be two arbitrary terms with \(\text{vars}(M, N) \subseteq \text{dom}(A_r)\). Let also \(\Gamma(A_r) = \nu \nu. F\) and \(\Gamma(B_r) = \nu \nu. G\) with \(\{\tilde{m}_1, \tilde{m}_2\} \cap \text{fn}(M, N) = \emptyset\). Since \(\Gamma(A_r) \sim_{i} \Gamma(B_r)\), \(M \varphi(F) =_\nu N \varphi(G)\). By Lemma B.10 we have \(\varphi(A_r) \equiv \nu \nu. \varphi(F)\) and \(\varphi(B_r) \equiv \nu \nu. \varphi(G)\). Hence from Def. 2.3 we know that \(A_r \sim_{i} B_r\).

2. \(\Longrightarrow\) Let \(M, N\) be two arbitrary terms. Let also \(\Gamma(A_r) = \nu \nu. F_1\) and \(\Gamma(B_r) = \nu \nu. F_2\) with \(\{\tilde{m}_1, \tilde{m}_2\} \cap \text{names}(M, N) = \emptyset\). W.l.o.g. we may assume \(M \varphi(F_1) =_\nu N \varphi(F_2)\). We need to show \(M \varphi(F_1) =_\nu N \varphi(F_2)\).

By Lemma B.10, we obtain \(\nu \nu. \varphi(F_1) \equiv \phi(A_r)\). By the hypothesis \(A_r \sim_{i} B_r\), there exist \(\tilde{m}_1, \tilde{m}_2\) such that \(\phi(B_r) \equiv \nu \nu. \sigma\) and \(M \sigma =_\nu N \sigma\). Since \(\tilde{m}_1, \tilde{m}_2\) is closed under substitution, it holds that \(M \sigma =_\nu N \sigma\). By Lemma B.5 and Lemma B.10, we have \(\nu \nu. \sigma \equiv \nu \nu. \phi(B_r) \equiv \nu \nu. \varphi(F_2)\). From Lemma B.2 we can infer \(\nu \nu. \sigma \equiv_{\equiv} \nu \nu. \varphi(F_2)\). By Lemma B.11 we obtain \(\nu \nu. \sigma \equiv_{\equiv} \nu \nu. \varphi(F_2)\). Hence \(M \varphi(F_1) =_\nu N \varphi(F_2)\).

Theorem 5.1 \(A_r \equiv_{i} B_r\) if and only if \(\Gamma(A_r) \equiv_{i, i} \Gamma(B_r)\).

Proof. 1. \(\Longleftarrow\) We construct a set \(\mathbb{R}\) on closed extended processes thus

\[\mathbb{R} = \{ (A_r, B_r) \mid \Gamma(A_r) \equiv_{i, i} \Gamma(B_r) \}\]

We show \(\mathbb{R} \subseteq_{\equiv_{i, i}}\). Suppose \(\Gamma(A_r) \equiv C \equiv_{i, i} D \equiv \Gamma(B_r)\). In combination with Lemma B.12 and Lemma B.11 we obtain the static equivalence part \(A_r \sim_{i} B_r\) immediately. We are left to show the agreement between transitions. Suppose \(A_r \xrightarrow{\sigma} A'_r\) with \(f\sigma(\alpha) \subseteq \text{dom}(A_r)\). Clearly \(A_r, A'_r, C, D\) are all closed. From Lemma 5.4 and Lemma 5.2, there exists \(C'\) such that \(C \xrightarrow{\sigma} C' \equiv \Gamma(A'_r)\), where \(C'\) is closed because \(C\) is closed and \(f\sigma(\alpha) \subseteq \text{dom}(C) = \text{dom}(A_r)\). From \(D \equiv_{i, i} C\), there exists \(D'\) such that \(D \equiv_{i, i} D' \equiv_{i, i} C'\).

By Lemma 5.3 and Lemma 5.7 we can deduce that there exists a closed \(B'_r\) such that \(B_r \equiv_{i, i} B'_r\) and \(\Gamma(B'_r) \equiv D'\). Hence \(A'_r, B'_r \in \mathbb{R}\).

2. \(\Longrightarrow\) This direction is proved by constructing a set \(\mathbb{S}\) on closed intermediate extended processes thus

\[\mathbb{S} = \{ (A, B) \mid A \equiv \Gamma(A_r), \ A_r \equiv_{i} B_r, \ \Gamma(B_r) \equiv B \}\]

We show \(\mathbb{S} \subseteq_{\equiv_{i, i}}\). First, \(A \sim_{i} B\) follows from Lemma B.12 and Lemma B.11. Suppose \(A \xrightarrow{\sigma} A'\). By Lemma 5.2 we have \(\Gamma(A) \xrightarrow{\sigma} \Gamma(A')\). By Lemma 5.6 we have \(A_r \xrightarrow{\sigma} A'_r\) and \(\Gamma(A'_r) \equiv A'_r\). Since \(A_r \equiv_{i} B_r\), there is some \(B'_r\) such that \(B_r \xrightarrow{\sigma} B'_r \equiv_{i} A'_r\). By Lemma 5.5 and Lemma 5.3 we have \(B \equiv_{i, i} B'_r\). Hence \((A', B') \in \mathbb{S}\).