Undecidability of 2-Label BPP Equivalences and Behavioral Type Systems for the π-Calculus

Naoki Kobayashi Takashi Suto
{koba,tsuto}@kb.ecei.tohoku.ac.jp
Tohoku University

Abstract

The trace equivalence of BPP was shown to be undecidable by Hirshfeld. We show that the trace equivalence remains undecidable even if the number of labels is restricted to two. The undecidability result holds also for the simulation of two-label BPP processes. These results imply undecidability of some behavioral type systems for the π-calculus.

1 Introduction

BPP [2] is a process calculus which has prefixes (lP), sum, parallel composition, and recursion as process constructors. Hirshfeld [3] has shown that the trace equivalence of two BPP processes is undecidable, by encoding the halting problem of a Minsky machine into the trace inclusion relation between two BPP processes. Hüttel [4] extended the undecidability result to other preorders between processes.

In this paper, we show that the trace inclusion of BPP processes remains undecidable even if we restrict the number of action labels to two. In the rest of the paper, we call the restriction of BPP to two labels *2-label BPP*. Hirshfeld's encoding of a Minsky machine requires 6 action labels, hence his result does not immediately extend to the case of 2-label BPP processes.

One may think that the undecidability for 2-label BPP processes can be easily obtained by encoding an action label into a sequence of the two labels, so that $P \leq_{tr} Q$ if and only if $[\![P]\!] \leq_{tr} [\![Q]\!]$, where $P \leq_{tr} Q$ means that the trace set of P is a subset of the trace set of Q, and $[\![P]\!]$ is the 2-label BPP process obtained from P by using the label encoding. Then, the undecidability of the trace inclusion for 2-label BPP (and hence also the undecidability of the trace equivalence) would follow from the undecidability for general BPP processes. We basically follow this approach, but there are two main difficulties. First, because of the existence of parallel composition, encoding of some action of a process may be simulated by interleaving execution of encodings of two or more actions of the other process. For example, consider two processes $P_1 = l_2 \,|\, l_2$ and $Q_1 = (l_2 \,|\, l_2) + l_3 l_1 l_1$ and choose the following label encoding: $[\![l_1]\!] = a, [\![l_2]\!] = ba, [\![l_3]\!] = bb$. Then, the trace sets of P_1 and Q_1 are of course different, but the trace sets of $[\![P_1]\!] = ba \,|\, ba$ and $[\![Q_1]\!] = (ba \,|\, ba) + bbaa$ are equivalent. Second, a naive encoding may also invalidate the equivalence of processes. For example, consider

$P_2 = l_2 \,|\, l_2$ and $Q_2 = l_2 l_2$. These have the same trace sets (and they are even bisimilar). With the above encoding, however, $[\![P_2]\!]$ has the trace *bbaa* while $[\![Q_2]\!]$ does not. To overcome the first problem, we choose an encoding of labels such that a shuffle of two or more encoded labels (i.e., a partial trace of $[\![l_1]\!] \,|\, \cdots \,|\, [\![l_m]\!]$) cannot be confused with encoding $[\![l]\!]$ of a single action. To avoid the second problem, we prepare a process *Inv* that simulates invalid sequences. With *Inv*, we can establish that $P \leq_{tr} Q$ if and only if $[\![P]\!] \leq_{tr} [\![Q]\!] \,|\, Inv$, since *Inv* simulates all the invalid sequences of $[\![P]\!]$ (which are generated by interleaving execution of more than one encoded actions). A similar (but a little more complicated) technique can also be used to show the undecidability of the simulation preorder of 2-label BPP processes.[1]

As an application of the undecidability results above, we show that the type checking problems for some behavioral type systems for the π-calculus are also undecidable.[2] In the behavioral type systems, channel types are augmented with *usage expressions* (usages, in short), describing how each communication channel is used. The usages can be regarded as 2-label BPP processes. Since the trace preorder between two usages can be reduced to the typability of a certain process, the type checking problem is undecidable.

The rest of this paper is structured as follows. Section 2 introduces BPP. Section 3 proves the undecidability of trace inclusion of 2-label BPP. Section 4 applies a similar technique to prove that the simulation preorder is also undecidable for 2-label BPP. Section 5 applies the undecidability results to show that certain behavioral type systems for the π-calculus are undecidable. Section 6 discusses related work, and Section 7 concludes.

2 Basic Parallel Processes (BPP)

BPP [2] is a calculus of processes consisting of prefixes, parallel composition, internal choice, and recursion. Unlike in CCS [16], there is no synchronization mechanism (such as the transition $a.P \,|\, \overline{a}.Q \xrightarrow{\tau} P \,|\, Q$).

The syntax of processes is given by:

$$P ::= \mathbf{0} \mid X \mid lP \mid (P|Q) \mid P + Q \mid \mu X.P$$

Here, X and l are meta-variables ranging over the sets of *process variables* and *action labels* respectively. We write **Act** for the set of action labels, and write $\mathbf{BPP}_{\mathbf{Act}}$ for the set of BPP processes whose action labels are in the set **Act**.

The process $\mathbf{0}$ does nothing. A process lP first performs l and then behaves like P. $P|Q$ is a parallel composition of P and Q, and $P + Q$ is an internal choice of P or Q. $\mu X.P$ stands for the recursive process X usually defined by the equation $X = P$.

We often omit $\mathbf{0}$ and just write a for $a\mathbf{0}$. We give a higher-precedence to unary prefixes, $+$, and $|$ in this order, so that $l_1P_1|l_2P_2 + l_3P_3$ means $(l_1P_1)|((l_2P_2) + (l_3P_3))$.

We say that P is guarded by l in lP. A recursive process $\mu X.P$ is *guarded* if X appears only in guarded positions of P. A process is *guarded* if all its recursive processes are guarded. In the rest of this paper, we consider only closed, guarded processes.[3]

[1] Note that the trace inclusion (as well as the simulation preorder) is decidable for 1-label BPP processes.

[2] Actually, investigation into the type checking problems lead us to the study of the trace and simu-

$$\frac{}{lP \xrightarrow{l} P} \quad (\textsc{Tr-Act}) \qquad \frac{[\mu X.P/X]P \xrightarrow{l} Q}{\mu X.P \xrightarrow{l} Q} \quad (\textsc{Tr-Rec})$$

$$\frac{P \xrightarrow{l} P'}{P \,|\, Q \xrightarrow{l} P' \,|\, Q} \quad (\textsc{Tr-ParL}) \qquad \frac{Q \xrightarrow{l} Q'}{P \,|\, Q \xrightarrow{l} P \,|\, Q'} \quad (\textsc{Tr-ParR})$$

$$\frac{P \xrightarrow{l} P'}{P + Q \xrightarrow{l} P'} \quad (\textsc{Tr-OrL}) \qquad \frac{Q \xrightarrow{l} Q'}{P + Q \xrightarrow{l} Q'} \quad (\textsc{Tr-OrR})$$

Figure 1: Transition rules of BPP processes

The transition relation $P \xrightarrow{l} Q$ is the least relation closed under the rules in Figure 1. We write $P \xrightarrow{l_1 \cdots l_n} Q$ if $P \xrightarrow{l_1} \cdots \xrightarrow{l_n} Q$.

2-label BPP is BPP where the set **Act** of action labels is restricted to the set $\{a, b\}$. Hence, the set of 2-label BPP processes is $\mathbf{BPP}_{\{a,b\}}$.

3 Undecidability of Trace Equivalence

In this section, we show that the trace equivalence of 2-label BPP processes is undecidable. As sketched in Section 1, we show an encoding of general BPP processes into 2-label BPP processes, so that the trace preorder is preserved. Then, the undecidability follows from the undecidability result for general BPP [3]. The undecidability of the trace equivalence can be shown also by using the encoding in Section 4, but the encoding presented in this section is simpler and easier to understand.

3.1 Trace Set, Trace Preorder, and Trace Equivalence

Definition 3.1 [trace set]: The *trace set* of P, written $\mathit{traces}(P)$, is defined by:

$$\mathit{traces}(P) = \{l_1 \dots l_n \mid P \xrightarrow{l_1} \cdots \xrightarrow{l_n} P_n\}$$

Definition 3.2: The *trace preorder* $\leq_{tr}$ and the *trace equivalence* $\sim_{tr}$ are defined by:

$$P \leq_{tr} Q \overset{\mathit{def}}{\Leftrightarrow} \mathit{traces}(P) \subseteq \mathit{traces}(Q)$$

$$P \sim_{tr} Q \overset{\mathit{def}}{\Leftrightarrow} P \leq_{tr} Q \wedge Q \leq_{tr} P$$

3.2 Encoding

We first define the encoding of labels. Since the number of labels occurring in a given process is finite, we assume here that the set **Act** of action labels is a finite set $\{l_0, \dots, l_{N-1}\}$. In the rest of this section and Section 4, we use meta-variables $P, Q, \dots$ for processes in $\mathbf{BPP}_{\{l_0,\dots,l_{N-1}\}}$,and use meta-variables $E, F, \dots$ for processes in $\mathbf{BPP}_{\{a,b\}}$.

lation preorders for 2-label BPP in this paper.

[3] Actually, any recursive process can be transformed to a bisimilar, guarded recursive process. For example, $\mu X.(X \,|\, lX)$ is equivalent to the guarded process $\mu X.l(X \,|\, X)$. $\mu X.X$ is bisimilar to $\mathbf{0}$.

Definition 3.3: A mapping $[\![\cdot]\!]$ from **Act** to $\{a,b\}^*$ is defined by:

$$[\![l_i]\!] = ab^i ab^{2N-1-i}$$

Here, a^i stands for the sequence of a of length i. For example, $a^3 = aaa$.

We now define encoding of a process. As mentioned in Section 1, we use different encodings for P and Q in $P \leq_{tr} Q$.

Definition 3.4:
Mappings $[\![\cdot]\!]_L$ and $[\![\cdot]\!]_R$ from $\mathbf{BPP}_{\{l_0,\ldots,l_{N-1}\}}$ to $\mathbf{BPP}_{\{a,b\}}$ are defined by:

$$\begin{array}{rclrcl} [\![\mathbf{0}]\!]_L & = & \mathbf{0} & [\![P \,|\, Q]\!]_L & = & [\![P]\!]_L \,|\, [\![Q]\!]_L \\ [\![X]\!]_L & = & X & [\![P + Q]\!]_L & = & [\![P]\!]_L + [\![Q]\!]_L \\ [\![lP]\!]_L & = & [\![l]\!][\![P]\!]_L & [\![\mu X.P]\!]_L & = & \mu X.[\![P]\!]_L \end{array}$$

$$[\![P]\!]_R = [\![P]\!]_L \,|\, \mathit{Inv}$$

$$\text{where } \mathit{Inv} = \sum_{k<N, k+l<2N-1} ab^k ab^l aG \text{ and } G = \mu X.(aX + bX)$$

The role of the process Inv in $[\![P]\!]_R$ is to simulate invalid transition sequences (caused by interleaving execution of $[\![l_i]\!]$ and $[\![l_j]\!]$).

3.3 Undecidability of Trace Equivalence

The main result of this section is stated as follows.

Theorem 3.5: $P \leq_{tr} Q$ if and only if $[\![P]\!]_L \leq_{tr} [\![Q]\!]_R$.

Since $P \leq_{tr} Q$ is undecidable for general BPP [3], we obtain the following corollary.

Corollary 3.6: The trace inclusion $E \leq_{tr} F$ and trace equivalence $E \sim_{tr} F$ are undecidable for 2-label BPP.

Proof: If the trace inclusion $\leq_{tr}$ were decidable for 2-label BPP, then we could decide $P \leq_{tr} Q$ for general BPP by deciding $[\![P]\!]_L \leq_{tr} [\![Q]\!]_R$, hence a contradiction. To see that $E \sim_{tr} F$ is also undecidable, it suffices to observe that $E \leq_{tr} F$ if and only if $E + F \sim_{tr} F$. □ □

The rest of this section is devoted to the proof of Theorem 3.5. The followings are key lemmas needed to prove Theorem 3.5.

Lemma 3.7: Let $m \in \{L, R\}$. If $P \xrightarrow{l} Q$, then $[\![P]\!]_m \xrightarrow{[\![l]\!]} [\![Q]\!]_m$.

Lemma 3.8: Let $m \in \{L, R\}$. If $[\![P]\!]_m \xrightarrow{[\![l]\!]} E$, then there exists a process Q such that $E = [\![Q]\!]_m$ and $P \xrightarrow{l} Q$.

Lemma 3.7, which follows by straightforward induction on the derivation of $P \xrightarrow{l} Q$, says that any transition of P can be simulated by $[\![P]\!]_L$ and $[\![P]\!]_R$. Lemma 3.8 says that any *valid* (in the sense that the transition label sequence corresponds to a label of P) transition sequence of $[\![P]\!]_L$ or $[\![P]\!]_R$ can be simulated by P.

Lemma 3.8 follows by induction on the derivation of the first transition of $[\![P]\!]_m \xrightarrow{[\![l]\!]} E$; See Appendix A for the full proof of Lemma 3.8. The proof makes use of the following key property, which essentially says that the first problem mentioned in Section 1 (that a single action may be simulated by interleaving execution of two or more actions) cannot occur.

Lemma 3.9: If $[\![P_1 \,|\, P_2]\!]_L \xrightarrow{[\![l]\!]} E$, then either (i) $[\![P_1]\!]_L \xrightarrow{[\![l]\!]} E_1$ and $E = E_1 \,|\, [\![P_2]\!]_L$ or (ii) $[\![P_2]\!]_L \xrightarrow{[\![l]\!]} E_2$ and $E = [\![P_1]\!]_L \,|\, E_2$

Proof sketch: By the transition rules, we have: (i) $[\![P_1]\!]_L \xrightarrow{s_1} E_1$, (ii) $[\![P_2]\!]_L \xrightarrow{s_2} E_2$, (iii) $E = E_1 \,|\, E_2$, and (iv) $[\![l]\!]$ is a shuffle of s_1 and s_2. It suffices to show that either s_1 or s_2 is an empty sequence. Suppose that s_1 and s_2 are not empty. Then s_1 and s_2 must be of the form ab^{j_1} and ab^{j_2} where $j_1, j_2 \leq N-1$. Then, $[\![l]\!]_L$ cannot be a shuffle of s_1 and s_2, since $[\![l]\!]_L$ contains $2N-1$ occurrences of b, whereas $j_1 + j_2 \leq 2N-2$. □

Proof: See Lemma A.6 in Appendix A. □

We state another key lemma below. Let $\mathbf{InvTr} = \{s \in \{a,b\}^* \mid \neg\exists s', l.(s = [\![l]\!]s')\}$. In other words, **InvTr** is the set of label sequences whose prefixes do not match $[\![l]\!]$.

Lemma 3.10: If $s \in \mathbf{InvTr} \cap \mathit{traces}([\![P]\!]_L)$, then $s \in \mathit{traces}(\mathit{Inv})$.

Proof: See Appendix A.2. □

Lemma 3.10 means that any initially invalid sequence generated by $[\![P]\!]_L$ can be simulated by Inv. Thus, the second problem mentioned in Section 1 is resolved.

We obtain the following lemma as an immediate corollary of Lemmas 3.7 and 3.8.

Lemma 3.11: Let $m \in \{L, R\}$. If $P \xrightarrow{l_{k_1} \cdots l_{k_n}} Q$, then $[\![P]\!]_m \xrightarrow{[\![l_{k_1}]\!] \cdots [\![l_{k_n}]\!]} [\![Q]\!]_m$. Conversely, if $[\![P]\!]_m \xrightarrow{[\![l_{k_1}]\!] \cdots [\![l_{k_n}]\!]} E$, then $P \xrightarrow{l_{k_1} \cdots l_{k_n}} Q$ and $[\![Q]\!]_m = E$.

We can now prove Theorem 3.5.

Proof of Theorem 3.5:

- "Only if": Suppose $P \leq_{tr} Q$ and $s \in \mathit{traces}([\![P]\!]_L)$. We need to show $s \in \mathit{traces}([\![Q]\!]_R)$. s must be of the form $[\![l_{k_1}]\!] \cdots [\![l_{k_n}]\!]s'$ where $s' \in \mathbf{InvTr}$. By Lemma 3.11, there exists P_1 such that $P \xrightarrow{l_{k_1} \cdots l_{k_n}} P_1$ and $s' \in \mathit{traces}([\![P_1]\!]_L)$. By the assumption, there must exist Q_1 such that $Q \xrightarrow{l_{k_1} \cdots l_{k_n}} Q_1$. By using Lemma 3.11 again, we get $[\![Q]\!]_R \xrightarrow{[\![l_{k_1} \cdots l_{k_n}]\!]} [\![Q_1]\!]_R$. By Lemma 3.10, we have $s' \in \mathit{traces}(\mathit{Inv}) \subseteq \mathit{traces}([\![Q_1]\!]_R)$. Thus, we have $s \in \mathit{traces}([\![Q]\!]_R)$ as required.
- "If": Suppose $[\![P]\!]_L \leq_{tr} [\![Q]\!]_R$ and $l_{k_1} \cdots l_{k_n} \in \mathit{traces}(P)$. By Lemma 3.11, $[\![l_{k_1}]\!] \cdots [\![l_{k_n}]\!] \in \mathit{traces}([\![P]\!]_L)$. By the assumption $[\![P]\!]_L \leq_{tr} [\![Q]\!]_R$, we have $[\![l_{k_1}]\!] \cdots [\![l_{k_n}]\!] \in \mathit{traces}([\![Q]\!]_R)$. By using Lemma 3.11 again, we obtain $l_{k_1} \cdots l_{k_n} \in \mathit{traces}(Q)$ as required.

□

4 Undecidability of Simulation Equivalence

In this section, we show that the simulation preorder and equivalence are also undecidable for 2-label BPP. We use the undecidability of the simulation preorder for the general BPP [4].[4]

Definition 4.1: A binary relation $\mathcal{R}$ on BPP processes is a *simulation* if, for any P, Q, l such that $P\mathcal{R}Q$ and $P \xrightarrow{l} P'$, there exists Q' such that $Q \xrightarrow{l} Q'$ and $P'\mathcal{R}Q'$. The *simulation preorder* $\leq_{sim}$ is the union of all simulations, i.e., $P \leq_{sim} Q$ if and only if there exists a simulation $\mathcal{R}$ such $P\mathcal{R}Q$. We write $P \sim_{sim} Q$ if $P \leq_{sim} Q \wedge Q \leq_{sim} P$.

Note that $\leq_{sim}$ itself is a simulation (hence, the largest simulation).

We show the undecidability of the simulation preorder for 2-label BPP, by reduction of the simulation preorder for general BPP into that for 2-label BPP. We first need to change the encoding $[\![\cdot]\!]_R$ of the right-hand side process.

Definition 4.2: A mapping $[\![\cdot]\!]_{R'}$ from $\mathbf{BPP}_{\{l_0,\dots,l_{N-1}\}}$ to $\mathbf{BPP}_{\{a,b\}}$ is defined by:

$$
\begin{array}{rcl@{\qquad}rcl}
[\![\mathbf{0}]\!]_{R'} & = & \mathbf{0} & [\![P]\!]^{\epsilon,k_1,k_2} & = & [\![P]\!]_{R'} \\
[\![X]\!]_{R'} & = & X & [\![P]\!]^{as,1,k} & = & a[\![P]\!]^{s,2,k} + aH^{(2N-2-k)} \\
[\![lP]\!]_{R'} & = & a[\![P]\!]^{s,1,0} \quad (as = [\![l]\!]) & [\![P]\!]^{bs,1,k} & = & b[\![P]\!]^{s,1,k+1} + aH^{(2N-2-k)} \\
[\![P \,|\, Q]\!]_{R'} & = & [\![P]\!]_{R'} \,|\, [\![Q]\!]_{R'} & [\![P]\!]^{bs,2,k} & = & b[\![P]\!]^{s,2,k+1} + aG \\
[\![P + Q]\!]_{R'} & = & [\![P]\!]_{R'} + [\![Q]\!]_{R'} & H^{(k)} & = & \left\{ \begin{array}{ll} aG & (k = 0) \\ bH^{(k-1)} + aG & (k > 0) \end{array} \right. \\
[\![\mu X.P]\!]_{R'} & = & \mu X.[\![P]\!]_{R'} & & &
\end{array}
$$

Note that the process G has been defined in Definition 3.4.

Intuitively, $[\![P]\!]^{s,k_1,k_2}$ represents an intermediate state for simulating a single action of the original process. The sequence $s \in \{a, b\}^*$ is the remaining sequence of actions to be performed, and k_1 and k_2 are the numbers of a and b actions that have been already performed. The roles of $aH^{(2N-2-k)}$ and aG in the definitions of $[\![P]\!]^{s,k_1,k_2}$ are to simulate invalid transitions.

Theorem 4.3: $P \leq_{sim} Q$ if and only if $[\![P]\!]_L \leq_{sim} [\![Q]\!]_{R'}$.

To show the "if" part, it suffices to show that the relation $\{(P, Q) \mid [\![P]\!]_L \leq_{sim} [\![Q]\!]_{R'}\}$ is a simulation. To show the "only if" part, we use the following, standard up-to technique:

Lemma 4.4 [up-to technique]: Let $\mathcal{R}$ be a binary relation on BPP processes. If $\mathcal{R}$ satisfies:

$$\forall P, Q, P', l.((P\mathcal{R}Q \wedge P \xrightarrow{l} P') \Rightarrow \exists Q'.(Q \xrightarrow{l} Q' \wedge P' \leq_{sim} \mathcal{R} \leq_{sim} Q')),$$

then $\mathcal{R} \subseteq \leq_{sim}$.

Proof: This follows from the fact that $\mathcal{R} \cup (\leq_{sim} \mathcal{R} \leq_{sim})$ is a simulation. □

[4] The proofs in [4] contain some flaws, but the undecidability results are valid. Please refer to [15] for the flaws and corrected proofs of the undecidability for the general BPP.

To show the "only if" part of Theorem 4.3, it suffices to show that the following relation is a simulation up to $\leq_{sim}$ (i.e., satisfies the assumption of Lemma 4.4).

$$\begin{array}{rcl} [\![\leq_{sim}]\!] & = & \{(E,E) \mid E \in \mathbf{BPP}_{\{a,b\}}\} \\ & \cup & \{([\![P]\!]_L, [\![Q]\!]_{R'}) \mid P \leq_{sim} Q\} \\ & \cup & \{(E,F) \mid P \leq_{sim} Q \wedge P' \leq_{sim} Q' \wedge s_1 s_2 = [\![l]\!] \wedge s_1, s_2 \neq \epsilon \wedge \\ & & \quad [\![P]\!]_L \xrightarrow{s_1} E \xrightarrow{s_2} [\![P']\!]_L \wedge [\![Q]\!]_{R'} \xrightarrow{s_1} F \xrightarrow{s_2} [\![Q']\!]_{R'}\} \end{array}$$

E and F in the third set are intermediate states for simulating a single action of general BPP processes. If E performs a valid action and becomes E', then F can also perform a valid action to become F' so that the pair (E', F') is again in the second or third set. If E performs an invalid action to become E', then F can transit to a process containing $H^{(2N-2-k)}$ or G, which can simulate any transitions of E'. See Appendix A for the full proof.

As a corollary of the above theorem and the undecidability for general BPP [4, 15], we obtain the undecidability for 2-label BPP.

Corollary 4.5: The relations $\leq_{sim}$ and $\sim_{sim}$ are undecidable for 2-label BPP.

5 Application to Behavioral Type Systems

In this section, we apply the undecidability results of the previous sections to show the undecidability of certain behavioral type systems for the π-calculus.

Behavioral type systems [1, 5, 7, 10, 11, 19–21] use types to control how processes may interact with each other. They have been used for analyzing deadlocks [5, 7, 11], race conditions [5], termination [21], etc. The version of behavioral type systems we discuss below is a type system with *channel usages* [9–11, 17], which express how each communication channel is used for input and output.

5.1 Syntax of Usages, Types, and Processes

The syntax of usages and types are given by:

$$\begin{array}{l} U \text{ (usages)} ::= \mathbf{0} \mid ?U \mid !U \mid (U_1 \mid U_2) \mid U_1 + U_2 \mid X \mid \mu X.U \\ \tau \text{ (types)} ::= \mathbf{chan}_U[\tau_1, \ldots, \tau_n] \end{array}$$

The syntax of usages is almost the same as that of 2-label BPP, except that X may be unguarded in $\mu X.U$. For example, $\mu X.X$ is allowed and is sometimes distinguished from $\mathbf{0}$ [10, 11]. The transition relation $U \xrightarrow{l} U'$ (where $l \in \{?, !\}$) is the same as that of $\mathbf{BPP}_{\{?,!\}}$. We often omit $\mathbf{0}$ and just write ! and ? for $!\mathbf{0}$ and $?\mathbf{0}$. We write $FV(U)$ for the set of free variables in U.

Table 1 summarizes intuitive meaning of usages. For example, the usage $? \mid !$ describes a channel that should be used once for input and once for output in parallel.

The type $\mathbf{chan}_U[\tau_1, \ldots, \tau_n]$, abbreviated to $\mathbf{chan}_U[\widetilde{\tau}]$, describes a channel that should be used for passing a tuple of channels of types $\tau_1, \ldots, \tau_n$, and used according to U. For example, the type $\mathbf{chan}_{?!}[\,]$ describes a channel that should be first used for receiving, and then for sending a null tuple. A channel of type $\mathbf{chan}_?[\mathbf{chan}_![\,]]$ should be used for receiving a channel, and then the received channel should be used for sending a null tuple.

Table 1: Intuitive Meaning of Usages

$\mathbf{0}$	not used at all
$?U$	used for input, and then according to U
$!U$	used for output, and then according to U
$U_1 \,\vert\, U_2$	used according to U_1 and U_2, possibly in parallel
$U_1 + U_2$	used according to either U_1 or U_2
X	usage variable bound by μ.
$\mu X.U$	used recursively according to $X = U$.

The subtyping relation $\tau_1 \leq \tau_2$ (which means that a value of type τ may be used as a value of type τ') is inductively defined by:

$$\frac{U \leq U'}{\mathbf{chan}_U[\widetilde{\tau}] \leq \mathbf{chan}_{U'}[\widetilde{\tau}]} \qquad (\textsc{SubT})$$

Here, the *subusage* relation $U \leq U'$ means that U represents a more liberal usage of channels, so that a channel of usage U may be used as a channel of usage U'. For example, $?{+}! \leq ?$ should hold. There are several reasonable definitions of the subusage relation [8–11], depending on the property that should be ensured by the type system. The following definition is the simplest one among such reasonable definitions; other definitions are discussed later.

Definition 5.1: $U_1 \leq U_2 \overset{def}{\Leftrightarrow} U_2 \leq_{tr} U_1$.

Here, $\leq_{tr}$ is the trace inclusion relation for $\mathbf{BPP}_{\{?,!\}}$.

The syntax of processes is given by:

$$P ::= \mathbf{0} \mid x![y_1, \ldots, y_n].\, P \mid x?[y_1, \ldots, y_n].\, P \mid (P \,|\, Q) \mid *P \mid (\nu x : U)\, P$$

A sequence $y_1, \ldots, y_n$ is abbreviated to $\widetilde{y}$. The process $x![\widetilde{y}].\, P$ sends the tuple $[\widetilde{y}]$ of channels on channel x, and then behaves like P. The process $x?[\widetilde{y}].\, P$ waits to receive a tuple consisting of channels $\widetilde{z}$ on channel x, binds $\widetilde{y}$ to them, and then behaves like P. The process $P \,|\, Q$ runs P and Q in parallel, and the process $*P$ runs infinitely many copies of P in parallel. The process $(\nu x : U)\, P$ creates a fresh communication channel, binds x to it, and then behaves like P. An important point here is that x is annotated with a usage U, which specifies a programmer's intention on how x should be used. As observed later, this usage declaration makes the type system described below undecidable. We do not consider choice $P + Q$ and name matching $[x = y]P$; The type system remains undecidable in the presence of those constructors.

Example 5.2: In the π-calculus, a lock (i.e., a binary semaphore) can be expressed as a channel, where the locked (unlocked, resp.) state is represented by the absence (presence, resp.) of a message. For example, the process $\mathit{lck}?[\,].\, x?[y].\, \mathit{lck}![\,]$ locks lck, reads from x, and then releases lck. To enforce that the channel lck is indeed used as a lock (i.e., the channel is first used for output to initialize the lock, and then used according to $?!$ an arbitrary number of times), one can declare a usage of lck as $(\nu \mathit{lck} : (! \,|\, \mu X.(\mathbf{0} + (?! \,|\, X))))\, P$. The type system introduced in the next subsection ensures that P uses lck according to the declared usage.

Operation on type environments:

$$(\Gamma_1 \,|\, \Gamma_2)(x) = \begin{cases} (\Gamma_1(x)) \,|\, (\Gamma_2(x)) & \text{if } x \in \mathit{dom}(\Gamma_1) \cap \mathit{dom}(\Gamma_2) \\ \Gamma_1(x) & \text{if } x \in \mathit{dom}(\Gamma_1) \setminus \mathit{dom}(\Gamma_2) \\ \Gamma_2(x) & \text{if } x \in \mathit{dom}(\Gamma_2) \setminus \mathit{dom}(\Gamma_1) \end{cases}$$

$$\text{where } \mathbf{chan}_{U_1}[\widetilde{\tau}] \,|\, \mathbf{chan}_{U_2}[\widetilde{\tau}] = \mathbf{chan}_{U_1 \,|\, U_2}[\widetilde{\tau}]$$

$$(*\Gamma)(x) = *(\Gamma(x))$$

$$\text{where } *\mathbf{chan}_U[\widetilde{\tau}] = \mathbf{chan}_{\mu X.(U \,|\, X)}[\widetilde{\tau}]$$

Typing:

$$\frac{}{\emptyset \vdash \mathbf{0}} \quad (\text{T-Zero}) \qquad \frac{\Gamma \vdash P}{*\Gamma \vdash *P} \quad (\text{T-Rep})$$

$$\frac{\Gamma \vdash P \qquad \Delta \vdash Q}{\Gamma \,|\, \Delta \vdash P \,|\, Q} \quad (\text{T-Par}) \qquad \frac{\Gamma, x : \tau \vdash P \qquad \tau' \leq \tau}{\Gamma, x : \tau' \vdash P} \quad (\text{T-Sub})$$

$$\frac{\Gamma, x : \mathbf{chan}_U[\widetilde{\tau}] \vdash P}{\Gamma \vdash (\nu x : U)\, P} \quad (\text{T-New}) \qquad \frac{\Gamma \vdash P \qquad x \notin \mathit{dom}(\Gamma) \qquad U \leq \mathbf{0}}{\Gamma, x : \mathbf{chan}_U[\widetilde{\tau}] \vdash P} \quad (\text{T-Weak})$$

$$\frac{\Gamma, x : \mathbf{chan}_U[\widetilde{\tau}] \vdash P}{(\Gamma, x : \mathbf{chan}_{!U}[\widetilde{\tau}]) \,|\, \widetilde{y} : \widetilde{\tau} \vdash x![\widetilde{y}].\, P} \quad (\text{T-Out}) \qquad \frac{\Gamma, x : \mathbf{chan}_U[\widetilde{\tau}], \widetilde{y} : \widetilde{\tau} \vdash P}{\Gamma, x : \mathbf{chan}_{?U}[\widetilde{\tau}] \vdash x?[\widetilde{y}].\, P} \quad (\text{T-In})$$

Figure 2: A Behavioral Type System

5.2 Type System

A type judgment for processes is of the form $\Gamma \vdash P$, where Γ is a type environment of the form $x_1 : \tau_1, \ldots, x_n : \tau_n$. It means that P behaves as specified by Γ. For example, $x : \mathbf{chan}_?[\mathbf{chan}_![\,]] \vdash P$ means that P uses x for receiving a channel of type $\mathbf{chan}_![\,]$, and then uses the received channel for sending a null tuple.

Typing rules and related definitions are given in Figure 2.

Remark 5.3: Although a usage of the form $U_1 + U_2$ does not appear in Figure 2, it can be introduced by rule T-Sub. For example, the process:
$x![y] \,|\, x?[z].\, z![\,] \,|\, x?[z].\, z?[\,].\, \mathbf{0}$ is typed under $x : \mathbf{chan}_{!\,|\,?\,|\,?}[\mathbf{chan}_{!+?}[\,]], y : \mathbf{chan}_{!+?}[\,]$.

5.3 Undecidability of Type Checking Problem

We show that the problem of deciding whether $\emptyset \vdash P$ holds or not is undecidable. The key observation for the proof is that, given two usages U_1 and U_2, we can construct a process P such that $\emptyset \vdash (\nu x : U_1)\, P$ if and only if $U_1 \leq U_2$. We use show the following key lemma.

Lemma 5.4: Let U be a usage and suppose $FV(U) \subseteq \{X_1, \ldots, X_n\}$. Then there exists a process P such that the followings are equivalent for any $U', U_1, \ldots, U_n$.

1. $U' \leq [U_1/X_1, \ldots, U_n/X_n]U$
2. $x_1 : \mathbf{chan}_{U_\bot}[\mathbf{chan}_{U_1}[\,]], \ldots, x_n : \mathbf{chan}_{U_\bot}[\mathbf{chan}_{U_n}[\,]], r : \mathbf{chan}_{U'}[\,] \vdash P$.

Here, $U_\bot = \mu X.(\mathbf{0} + ?X + !X)$.

We obtain the following result as a corollary of Lemma 5.4 and Corollary 3.6.

Theorem 5.5: The relation $\emptyset \vdash P$ is undecidable.

Proof: Let U_1, U_2 be usages. By Lemma 5.4, there exists a process P_1 such that $r : \mathbf{chan}_{U_1}[\,] \vdash P_1$ if and only if $U_1 \leq U_2$. Hence, $\emptyset \vdash (\nu r : U_1)\, P_1$ if and only if $U_1 \leq U_2$. Since the latter is undecidable, the type checking problem is also undecidable. □ □

Undecidability results for other definitions of $U_1 \leq U_2$ The above undecidability result holds for various other definitions of the subusage relation. For example, let $\leq \overset{def}{=} \geq_{sim}$. Since Lemma 5.4 remains valid, and $U_1 \leq_{sim} U_2$ is undecidable, the type checking problem is also undecidable. Here we sketch other definitions of subusage relations for which the type checking problem remains undecidable.

- Define a predicate $U\!\downarrow$ inductively by the rules:

  $$\frac{}{\mathbf{0}\!\downarrow} \qquad \frac{U_1 \downarrow \quad U_2\!\downarrow}{(U_1 \,|\, U_2)\!\downarrow} \qquad \frac{U_i\!\downarrow}{(U_1 + U_2)\!\downarrow} \qquad \frac{[\mu X.U/X]U\!\downarrow}{\mu X.U\!\downarrow}$$

  Then add the condition $U_1\!\downarrow \Rightarrow U_2\!\downarrow$ to the requirement for each element (U_1, U_2) in the simulation relation $\leq_{sim}$. Let $\leq_{sim}^{ex}$ be the extended simulation relation, and define $U_1 \leq U_2$ as $U_2 \leq_{sim}^{ex} U_1$.

- Extend the trace set using the above predicate:

  $$\mathit{extraces}(U) = \{l_1 \cdots l_n \mid U \xrightarrow{l_1} \cdots \xrightarrow{l_n} U'\} \cup \{l_1 \cdots l_n\!\downarrow \mid U \xrightarrow{l_1} \cdots \xrightarrow{l_n} U'\!\downarrow\}$$

  Then define $U_1 \leq U_2$ as $\mathit{extraces}(U_2) \subseteq \mathit{extraces}(U_1)$.

- Add a transition $U \xrightarrow{\tau} U'$ by introducing the synchronization rule:

  $$\frac{U_1 \xrightarrow{?} U_1' \quad U_2 \xrightarrow{!} U_2'}{U_1 \,|\, U_2 \xrightarrow{\tau} U_1' \,|\, U_2'}$$

  Then re-define the trace set, and define $\leq$ as the trace inclusion relation.

Remark 5.6: The undecidability results above may be disappointing, given that behavioral type systems are useful for checking various properties [1, 7, 10, 11, 19, 21] and that the above type system is one of the simplest forms of behavioral type systems. It should be noted, however, that the source of the undecidability result is the programmer's capability to declare arbitrary usages (by $(\nu x : U)$). In fact, Kobayashi's type systems for deadlock-freedom and information flow [10, 11] are much more complex, but the type checking problem is decidable (note that they do not allow type declaration). In order to allow declaration of usages as in this paper while keeping the decidability of type checking, we need to restrict the class of usages that can be declared by programmers. For example, type checking is decidable if the class of declared usages is restricted to the class of usages whose trace sets are deterministic Petri net languages [18].

6 Related Work

As already mentioned in Section 1, Hirshfeld [3] showed the undecidability of the trace equivalence for general BPP, and Hüttel [4] extended the result to show undecidability of other equivalence relations (except bisimilarity, which is decidable [2]). They [3, 4] both encode Minsky machines into BPP. Since their encoding uses more than two action labels, their results do not immediately imply the undecidability for 2-label BPP.

Srba [6] proposed a general method for encoding a labeled transition system into a transition system with a *single* label, so that certain properties are preserved by the encoding. His encoding is, however, not applicable to BPP.

A number of behavioral type systems for the π-calculus have been proposed recently for checking various properties including deadlock, race, liveness, termination, and information flow [1, 5, 7, 10, 11, 19–21]. Usage-based behavioral type systems studied in Section 5 were first proposed in [17] (in a less general form, without full recursion), and have been extended since then [1, 5, 10–13]. In some of the most recent type systems [1, 5, 13], CCS-like process calculi, which are more expressive than BPP, are used as usages or types. The undecidability result presented in this paper indicates that explicit usage or type declarations must be restricted in order to make those type systems decidable.

7 Conclusion

We have shown that the trace equivalence and simulation relation for 2-label BPP is undecidable. The undecidability result also implies the undecidability of certain behavioral type systems for the π-calculus.

Acknowledgments.

We would like to thank Hans Hüttel for discussions on the undecidability of BPP equivalences. We would also like to thank anonymous reviewers for useful comments.

References

[1] S. Chaki, S. Rajamani, and J. Rehof. Types as models: Model checking message-passing programs. In *Proceedings of ACM SIGPLAN/SIGACT Symposium on Principles of Programming Languages*, pages 45–57, 2002.

[2] S. Christensen, Y. Hirshfeld, and F. Moller. Decomposability, decidability and axiomatisability for bisimulation equivalence on basic parallel processes. In *Proceedings of IEEE Symposium on Logic in Computer Science*, pages 386–396, 1993.

[3] Y. Hirshfeld. Petri nets and the equivalence problem. In *Computer Science Logic*, volume 832 of *Lecture Notes in Computer Science*, pages 165–174. Springer-Verlag, 1993.

[4] H. Hüttel. Undecidable Equivalence for Basic Parallel Processes. In *Proceedings of TACS94*, volume 789 of *Lecture Notes in Computer Science*, pages 454–464. Springer-Verlag, 1994.

[5] A. Igarashi and N. Kobayashi. A generic type system for the pi-calculus. *Theoretical Computer Science*, 311(1-3):121–163, 2004.

[6] Jirí. On the power of labels in transition systems. In *Proceedings of CONCUR 2001*, volume 2154 of *Lecture Notes in Computer Science*, pages 277–291. Springer-Verlag, 2001.

[7] N. Kobayashi. TyPiCal: A type-based static analyzer for the pi-calculus. Tool available at `http://www.kb.ecei.tohoku.ac.jp/~koba/typical/`.

[8] N. Kobayashi. A type system for lock-free processes. *Information and Computation*, 177:122–159, 2002.

[9] N. Kobayashi. Type systems for concurrent programs. In *Proceedings of UNU/IIST 20th Anniversary Colloquium*, volume 2757 of *Lecture Notes in Computer Science*, pages 439–453. Springer-Verlag, 2003.

[10] N. Kobayashi. Type-based information flow analysis for the pi-calculus. *Acta Informatica*, 42(4-5):291–347, 2005.

[11] N. Kobayashi. A new type system for deadlock-free processes. In *Proceedings of CONCUR 2006*, volume 4137 of *Lecture Notes in Computer Science*, pages 233–247. Springer-Verlag, 2006.

[12] N. Kobayashi, S. Saito, and E. Sumii. An implicitly-typed deadlock-free process calculus. In *Proceedings of CONCUR2000*, volume 1877 of *Lecture Notes in Computer Science*, pages 489–503. Springer-Verlag, August 2000.

[13] N. Kobayashi, K. Suenaga, and L. Wischik. Resource usage analysis for the pi-calculus. *Logical Methods in Computer Science*, 2(3:4):1–42, 2006.

[14] N. Kobayashi and T. Suto. Undecidability of 2-label BPP equivalences and behavioural type systems for the π-calculus, 2007. Full version. Available from `http://www.kb.ecei.tohoku.ac.jp/~koba/publications.html`.

[15] N. Kobayashi and T. Suto. Undecidability of BPP equivalences revisited, 2007. Available from `http://www.kb.ecei.tohoku.ac.jp/~koba/publications.html`.

[16] R. Milner. *Communication and Concurrency.* Prentice Hall, 1989.

[17] E. Sumii and N. Kobayashi. A generalized deadlock-free process calculus. In *Proc. of Workshop on High-Level Concurrent Language (HLCL'98)*, volume 16(3) of *ENTCS*, pages 55–77, 1998.

[18] T. Suto and N. Kobayashi. Channel usage declaration for concurrent programming languages. *IPSJ Transaction on Programming*, 2007. to appear (in Japanese).

[19] N. Yoshida. Graph types for monadic mobile processes. In *FST/TCS'16*, volume 1180 of *Lecture Notes in Computer Science*, pages 371–387. Springer-Verlag, 1996.

[20] N. Yoshida. Type-based liveness guarantee in the presence of nontermination and nondeterminism. Technical Report 2002-20, MSC Technical Report, University of Leicester, April 2002.

[21] N. Yoshida, M. Berger, and K. Honda. Strong normalisation in the pi-calculus. *Information and Computation*, 191(2):145–202, 2004.

Appendix

A Proofs

We give proofs omitted in Sections 3–5. Section A.1 shows common properties of the encoding functions $\llbracket\cdot\rrbracket_L$, $\llbracket\cdot\rrbracket_R$, and $\llbracket\cdot\rrbracket_{R'}$. Section A.2 proves properties specific to each encoding. Section A.3 proves Theorem 4.3, and Section A.4 proves Lemma 5.4.

A.1 Common Properties of the Encoding Functions

Let $t \in \{a, b\}$ and $s \in \{a, b\}^*$. We write $\#t(s)$ for the number of occurrences of t in s.

The following lemma is a generalization of Lemma 3.7 to the case for $m \in \{L, R, R'\}$.

Lemma A.1: Let $m \in \{L, R, R'\}$. If $P \xrightarrow{l} Q$, then $\llbracket P\rrbracket_m \xrightarrow{\llbracket l\rrbracket} \llbracket Q\rrbracket_m$.

Proof: Straightforward induction on the derivation of $P \xrightarrow{l} Q$, with case analysis on the last rule used. To show the case where $m = R'$ and where Tr-Act has been used to derive $P \xrightarrow{l} Q$, observe that $\llbracket P_1\rrbracket^{s,k_1,k_2} \xrightarrow{s} \llbracket P_1\rrbracket_{R'}$ if $\#a(s) + k_1 = 2$ and $\#b(s) + k_2 = 2N - 1$. □

We define the set **Images** of 2-label processes that can appear as images of the encoding functions $\llbracket\cdot\rrbracket_L$, $\llbracket\cdot\rrbracket_R$, and $\llbracket\cdot\rrbracket_{R'}$:

Definition A.2: The set **Images** is defined by:

$$\begin{aligned}\mathbf{Images} \;=\; & \{\llbracket P\rrbracket_L \mid P \in \mathbf{BPP}_{\{l_0,\ldots,l_{N-1}\}}\} \cup \{\llbracket P\rrbracket_R \mid P \in \mathbf{BPP}_{\{l_0,\ldots,l_{N-1}\}}\} \\ & \cup \{\llbracket P\rrbracket_{R'} \mid P \in \mathbf{BPP}_{\{l_0,\ldots,l_{N-1}\}}\} \cup \{\mathit{Inv}\}\end{aligned}$$

Lemma A.3: If $E \in$ **Images**, then $E \not\xrightarrow{b}$ and $E \not\xrightarrow{ab^N}$.

Proof: $E \not\xrightarrow{b}$ follows immediately from the definition of the encoding functions. $\mathit{Inv} \not\xrightarrow{ab^N}$ also follows immediately from the definition of Inv. Suppose $E = \llbracket P\rrbracket_m$ and $E \xrightarrow{a} E'$. We show $E' \not\xrightarrow{b^N}$ by induction on the derivation of $E \xrightarrow{a} E'$.

- Case Tr-Act: In this case, $P = lP_1$ and $m \in \{L, R'\}$. If $m = L$, $E' \not\xrightarrow{b^N}$ follows immediately from the definition of the encoding. If $m = R'$, then $E' = \llbracket P_1\rrbracket^{b^i ab^j,1,0}$ with $ab^i ab^j = \llbracket l\rrbracket$. By induction on i, we can easily show that $\llbracket P_1\rrbracket^{b^i ab^j,1,0} \not\xrightarrow{b^{i+1}}$. Since $ab^i ab^j = \llbracket l\rrbracket$, we have $i \leq N - 1$ by the definition of the label encoding. Hence, we have $E' \not\xrightarrow{b^N}$ as required.
- Case Tr-OrL: In this case, $E = \llbracket P_1 + P_2\rrbracket_m$ and $\llbracket P_1\rrbracket_m \xrightarrow{a} E'$. Hence, the required result follows immediately from the induction hypothesis.
- Case Tr-OrR: Similar to the case above.

- Case Tr-ParL: In this case, $E = E_1 \,|\, E_2$ and $E' = E_1' \,|\, E_2$ with $E_1 \xrightarrow{a} E_1'$. Moreover, $E_1, E_2 \in \textbf{Images}$. By the induction hypothesis, $E_1' \overset{b^N}{\not\longrightarrow}$. We also have $E_2 \overset{b}{\not\longrightarrow}$. Therefore, we have $E' \overset{b^N}{\not\longrightarrow}$ as required.
- Case Tr-ParR: Similar to the case above.
- Case Tr-Rec: In this case, $P = \mu X.P_1$ and $[\![[P/X]P_1]\!]_m = [[\![P]\!]_m/X][\![P_1]\!]_m \xrightarrow{a} E'$, with $m \in \{L, R'\}$. The required result follows immediately from the induction hypothesis.

□

Lemma A.4: Suppose $m \in \{L, R'\}$. If $[\![P]\!]_m \xrightarrow{t} E$, then $t = a$ and there exists s, l and P' such that $[\![P]\!]_m \xrightarrow{a} E \xrightarrow{s} [\![P']\!]_m$ and $as = [\![l]\!]$.

Proof: Straightforward induction on the derivation of $[\![P]\!]_m \xrightarrow{t} E$. □

Lemma A.5: If $E_1, E_2 \in \textbf{Images}$ and $E_1 \,|\, E_2 \xrightarrow{s_1} E' \xrightarrow{s_2} E''$ with $s_1 s_2 = [\![l]\!]$, then $E' = E_1' \,|\, E_2'$ and $E'' = E_1'' \,|\, E_2''$, with either (i) $E_1 \xrightarrow{s_1} E_1' \xrightarrow{s_2} E_1''$ and $E_2 = E_2' = E_2''$ or (ii) $E_1 = E_1' = E_1''$ and $E_2 \xrightarrow{s_1} E_2' \xrightarrow{s_2} E_2''$.

Proof: By the definition of the transition relation, we have:

$$\begin{array}{l} E_1 \xrightarrow{s_{11}} E_1' \xrightarrow{s_{21}} E_1'' \\ E_2 \xrightarrow{s_{12}} E_2' \xrightarrow{s_{22}} E_2'' \\ s_1 \text{ is a shuffle of } s_{11} \text{ and } s_{12} \\ s_2 \text{ is a shuffle of } s_{21} \text{ and } s_{22} \end{array}$$

By the definition of $[\![l]\!]$, the label a must occur twice in $[\![l]\!]$. If $s_{1i}s_{2i}$ contains no a, then by Lemma A.3, $s_{1i}s_{2i}$ must be the empty sequence ϵ, so that the result follows immediately. Suppose that each of $s_{11}s_{21}$ and $s_{12}s_{22}$ contains one a. Then, by Lemma A.3, $s_{11}s_{21} = ab^{x_1}$ and $s_{12}s_{22} = ab^{x_2}$ with $x_1, x_2 \leq N-1$. This contradicts with the fact that $[\![l]\!]$ is a shuffle of $s_{11}s_{21}$ and $s_{12}s_{22}$, since the number of b in $[\![l]\!]$ is $2N-1$ but $x_1 + x_2 \leq 2N-2$.
□

We are now ready to show a generalization of Lemma 3.8 to also the case for $[\![P]\!]_{R'}$.

Lemma A.6: Let $m \in \{L, R, R'\}$. If $[\![P]\!]_m \xrightarrow{[\![l]\!]} E$, then there exists a process Q such that $E = [\![Q]\!]_m$ and $P \xrightarrow{l} Q$.

Proof: We first prove the case for $m \in \{L, R'\}$ by induction on the derivation of the first transition step of $[\![P]\!]_L \xrightarrow{[\![l]\!]} E$, with case analysis on the last rule used.

- Case Tr-Act: In this case, $[\![P]\!]_m$ must be of the form aE_1. By the definition of the encoding, P must be of the form lP_1. If $m = L$, then $[\![P]\!]_m = [\![l]\!][\![P_1]\!]_m$, so that $Q = P_1$ satisfies the required property. For the case $m = R'$, it suffices to show that if $[\![P_1]\!]^{s,k_1,k_2} \xrightarrow{s} E$ with $\#a(s) + k_1 = 2$ and $\#b(s) + k_2 = 2N-1$, then $E = [\![P_1]\!]_{R'}$. This follows by induction on the length of s, using the fact $H^{(k)} \overset{k+1}{\not\longrightarrow}$.

- Case Tr-ParL: In this case, $P = P_1 \mid P_2$. By Lemma A.5, it must be the case that $[\![P_1]\!]_m \xrightarrow{[\![l]\!]} E_1$ and $E = E_1 \mid [\![P_2]\!]_m$. By the induction hypothesis, there exists Q_1 such that $P_1 \xrightarrow{l} Q_1$ and $E_1 = [\![Q_1]\!]_m$. Hence, $Q = Q_1 \mid P_2$ satisfies the required condition.

- Case Tr-ParR: Similar to the above case.

- Case Tr-OrL: In this case, $P = P_1 + P_2$, with $[\![P_1]\!]_m \xrightarrow{[\![l]\!]} E$. By the induction hypothesis, there exists Q such that $P_1 \xrightarrow{l} Q$ and $[\![Q]\!]_m = E$. By using Tr-OrL, we obtain $P \xrightarrow{l} Q$ as required.

- Case Tr-OrR: Similar to the above case.

- Case Tr-Rec: In this case, $P = \mu X.P'$ and $[[\![\mu X.P']\!]_m/X][\![P']\!]_m = [\![[\mu X.P'/X]P']\!]_m \xrightarrow{[\![l]\!]} E$. By the induction hypothesis, there exists Q such that $[\mu X.P'/X]P' \xrightarrow{l} Q$ and $[\![Q]\!]_m = E$. By using Tr-Rec, we obtain $P \xrightarrow{l} Q$ as required.

Now we show the case for $m = R$ using the result for the case $m = L$. Suppose $[\![P]\!]_R = [\![P]\!]_L \mid \mathit{Inv} \xrightarrow{[\![l]\!]} E$. Then by Lemma A.5, $E = E_1 \mid E_2$ and either (i) $[\![P]\!]_L \xrightarrow{[\![l]\!]} E_1$ and $E_2 = \mathit{Inv}$, or (ii) $\mathit{Inv} \xrightarrow{[\![l]\!]} E_2$ and $E_1 = [\![P]\!]_L$. The latter case is, however, impossible by the definition of Inv. Hence, it must be the case that $[\![P]\!]_L \xrightarrow{[\![l]\!]} E_1$ and $E = E_1 \mid \mathit{Inv}$. By the result for the case $m = L$, there exists Q such that $P \xrightarrow{l} Q$ and $[\![Q]\!]_L = E_1$. Thus, we have $[\![Q]\!]_R = E$ and $P \xrightarrow{l} Q$ as required. □

A.2 Properties Specific to Each Encoding

Proof of Lemma 3.10: Suppose $s \in \mathbf{InvTr} \cap [\![P]\!]_L$. By the definition of **InvTr** and Lemma A.3, s must be one of the following forms.

1. the empty sequence ϵ
2. ab^i where $i < N$
3. $s = ab^i ab^j$ where $i < N$ and $i + j < 2N - 1$
4. $s = ab^i ab^j as'$ where $i < N$ and $i + j < 2N - 1$

In all the cases, s is a trace of Inv. □

The rest of the lemmas proved in this subsection will be used in the proof of Theorem 4.3.

Lemma A.7: If $E \in \mathbf{BPP}_{\{a,b\}}$ and $E \overset{b^{k+1}}{\not\longrightarrow}$, then $E \leq_{sim} H^{(k)}$.

Proof: This follows from the fact that

$$\mathcal{R} = \{(E, H^{(k)}) \mid E \in \mathbf{BPP}_{\{a,b\}} \wedge E \overset{b^{k+1}}{\not\longrightarrow}\} \cup \{(E, G) \mid E \in \mathbf{BPP}_{\{a,b\}}\}$$

is a simulation. □

Lemma A.8: If $[\![lP]\!]_{R'} \xrightarrow{s_1} E \xrightarrow{s_2} F$ and $s_1 s_2 = [\![l]\!]$ with $s_1, s_2 \neq \epsilon$, then $E = [\![P]\!]^{s_2,k_1,k_2}$ where $k_1 = \#a(s_1)$ and $k = \#b(s_1)$.

Proof: The proof proceeds by induction on the length of s_1.

- Case where the length of s_1 is 1: By the definition of the encoding, s_1 must be a and $E = [\![P]\!]^{s_2,1,0}$ as required.

- Case where $s_1 = s_1' t$ with $s_1' \neq \epsilon$ and $t \in \{a, b\}$. In this case, there exists E_1 such that $[\![lP]\!]_{R'} \xrightarrow{s_1'} E_1 \xrightarrow{t} E$. Let $\#a(s_1') = k_1'$ and $\#b(s_1') = k_2'$. By the induction hypothesis, $E_1 = [\![P]\!]^{ts_2,k_1',k_2'}$. Hence, (i) $E = [\![P]\!]^{s_2,k_1,k_2}$, (ii) $t = a$, $k_1' = 1$ and $E = H^{(2N-2-k_2')}$, or (iii) $t = a$, $k_1' = 2$ and $E = G$. In the second case, $\#a(s_1) = 2$ and $\#b(s_1) = k_2'$ but $E \not\xrightarrow{b^{2N-1-k_2'}}$. This contradicts with the assumption $E \xrightarrow{s_2}$ and $s_1 s_2 = [\![l]\!]$. In the third case, $\#a(s_1 s_2) = 3$, which contradicts with the assumption $s_1 s_2 = [\![l]\!]$. Hence, it must be the case that $E = [\![P]\!]^{s_2,k_1,k_2}$.

□

Lemma A.9: If $[\![P]\!]_{R'} \xrightarrow{s_1} E \xrightarrow{s_2} F$ and $s_1 s_2 = [\![l]\!]$ with $s_1, s_2 \neq \epsilon$, then $[\![P']\!]^{s_2,k_1,k_2} \leq_{sim} E$ for some P', where $k_1 = \#a(s_1)$ and $k_2 = \#b(s_1)$.

Proof: We show this by induction on the derivation of the first step of the transition sequence $[\![P]\!]_{R'} \xrightarrow{s_1} E$, with case analysis on the last rule used.

- Case Tr-Act: The required result follows immediately from Lemma A.8.

- Case Tr-OrL: In this case, we have $P = P_1 \,|\, P_2$ and $[\![P_1]\!]_{R'} \xrightarrow{s_1} E \xrightarrow{s_2} F$. Therefore, the required result follows immediately from the induction hypothesis.

- Case Tr-OrR: Similar to the above case.

- Case Tr-ParL: In this case, we have $P = P_1 \,|\, P_2$. By Lemma A.5, it must be the case that $E = E_1 \,|\, [\![P_2]\!]_{R'}$ and $F = F_1 \,|\, [\![P_2]\!]_{R'}$ with $[\![P_1]\!]_{R'} \xrightarrow{s_1} E_1 \xrightarrow{s_2} F_1$. By the induction hypothesis, $[\![P']\!]^{s_2,k_1,k_2} \leq_{sim} E_1$ for some P'. Since $E_1 \leq_{sim} E_1 \,|\, [\![P_2]\!]_{R'} = E$, we have $[\![P']\!]^{s_2,k_1,k_2} \leq_{sim} E$ as required.

- Case Tr-ParR: Similar to the above case.

- Case Tr-Rec: In this case, we have $P = \mu X.P_1$ and $[\![[P/X]P_1]\!]_{R'} = [[\![P]\!]_{R'}/X][\![P_1]\!]_{R'} \xrightarrow{s_1} E \xrightarrow{s_2} F$. Therefore, the required result follows immediately from the induction hypothesis.

□

Lemma A.10: Suppose that the following conditions hold.

1. $[\![P]\!]_L \xrightarrow{s_1} E \xrightarrow{s_2} F$ with $s_1 s_2 = [\![l]\!]$ and $s_1, s_2 \neq \epsilon$.

2. $E \xrightarrow{t} E'$ for some $t \in \{a, b\}$.

3. There is no s_2' such that $E' \xrightarrow{s_2'} F$ and $ts_2' = s_2$.

Then, $t = a$ and either (i) $\#a(s_1) = 2$ or (ii) $\#a(s_1) = 1$ and $E' \not\xrightarrow{b^{2N-1-\#b(s_1)}}$.

Proof: We show this by induction on the derivation of the first step of the transition sequence $\llbracket P \rrbracket_{R'} \xrightarrow{s_1} E$, with case analysis on the last rule used.

- Case Tr-Act: In this case, it must be the case that $\llbracket P \rrbracket_L = s_1 s_2 \llbracket P_1 \rrbracket_L$, $E = s_2 \llbracket P_1 \rrbracket_L$, and $F = \llbracket P_1 \rrbracket_L$. The required property holds vacuously, since the third assumption of the lemma does not hold.

- Case Tr-OrL: In this case, we have $P = P_1 + P_2$ and $\llbracket P_1 \rrbracket_L \xrightarrow{s_1} E \xrightarrow{s_2} F$. The required property follows immediately from the induction hypothesis.

- Case Tr-OrR: Similar to the above case.

- Case Tr-ParL: In this case, we have $P = P_1 \,|\, P_2$. By Lemma A.5 and the first condition, it must be the case that $E = E_1 \,|\, \llbracket P_2 \rrbracket_L$ and $F = F_1 \,|\, \llbracket P_2 \rrbracket_L$ with $\llbracket P_1 \rrbracket_L \xrightarrow{s_1} E_1 \xrightarrow{s_2} F_1$. By the condition $E \xrightarrow{t} E'$, we have either (i) $E' = E'_1 \,|\, \llbracket P_2 \rrbracket_L$ and $E_1 \xrightarrow{t} E'_1$, or (ii) $E' = E_1 \,|\, E'_2$ and $\llbracket P_2 \rrbracket_L \xrightarrow{t} E'_2$.

  - Case $E' = E'_1 \,|\, \llbracket P_2 \rrbracket_L$ and $E_1 \xrightarrow{t} E'_1$: Suppose $E'_1 \xrightarrow{s'_2} F_1$. Then, we have $E' \xrightarrow{s'_2} F$, which contradicts with the third condition of the lemma. Therefore we have $E'_1 \not\xrightarrow{s'_2} F_1$. By the induction hypothesis, we have $t = a$ and either (i-1) $\#a(s_1) = 2$, or (i-2) $\#a(s_1) = 1$ and $E'_1 \not\xrightarrow{b^{2N-1-\#b(s_1)}}$. In the latter case, by $\llbracket P_2 \rrbracket_L \not\xrightarrow{b}$ (Lemma A.3), we have $E \not\xrightarrow{b^{2N-1-\#b(s_1)}}$ as required.

  - Case $E' = E_1 \,|\, E'_2$ and $\llbracket P_2 \rrbracket_L \xrightarrow{t} E'_2$: By Lemma A.3, we have $t = a$. By the condition $s_1 \neq \epsilon$ and Lemma A.3, $\#a(s_1)$ is either 1 or 2. Suppose $\#a(s_1) = 1$ but $E' \xrightarrow{b^{2N-1-\#b(s_1)}}$. Then, there must exist i and j such that $E_1 \xrightarrow{b^i}$ and $E'_2 \xrightarrow{b^j}$ with $i + j = 2N - 1 - \#b(s_1)$. However, by Lemma A.3, it must be the case that $\#b(s_1) + i \leq N - 1$ and $j \leq N - 1$, which implies $i + j \leq 2N - 2 - \#b(s_1)$; hence a contradiction. Thus, we have either (ii-1) $\#a(s_1) = 2$, or (ii-2) $\#a(s_1) = 1$ and $E' \not\xrightarrow{b^{2N-1-\#b(s_1)}}$.

- Case Tr-ParR: Similar to the above case.

- Case Tr-Rec: In this case, we have $P = \mu X.P_1$ and $\llbracket [P/X]P_1 \rrbracket_L = [\llbracket P \rrbracket_L / X] \llbracket P_1 \rrbracket_L \xrightarrow{s_1} E \xrightarrow{s_2} F$. The required property follows immediately from the induction hypothesis.

□

A.3 Proof of Theorem 4.3

We now give a full proof of Theorem 4.3.

Proof: This follows from the fact that $\mathcal{R} \cup (\leq_{sim} \mathcal{R} \leq_{sim})$ is a simulation. □

Proof of Theorem 4.3:

- "Only if" : Define the relation $\llbracket \leq_{sim} \rrbracket$ by:

  $$\begin{array}{rcl} \llbracket \leq_{sim} \rrbracket & = & \{(E,E) \mid E \in \mathbf{BPP}_{\{a,b\}}\} \\ & \cup & \{(\llbracket P \rrbracket_L, \llbracket Q \rrbracket_{R'}) \mid P \leq_{sim} Q\} \\ & \cup & \{(E,F) \mid P \leq_{sim} Q \wedge P' \leq_{sim} Q' \wedge s_1 s_2 = \llbracket l \rrbracket \wedge s_1, s_2 \neq \epsilon \wedge \\ & & \quad \llbracket P \rrbracket_L \xrightarrow{s_1} E \xrightarrow{s_2} \llbracket P' \rrbracket_L \wedge \llbracket Q \rrbracket_{R'} \xrightarrow{s_1} F \xrightarrow{s_2} \llbracket Q' \rrbracket_{R'}\} \end{array}$$

  It suffices to show that $\llbracket \leq_{sim} \rrbracket$ satisfies the condition of Lemma 4.4. Suppose $(E,F) \in \llbracket \leq_{sim} \rrbracket$. We perform case analysis on which set contains (E,F). The case (E,F) is in the first set is trivial.

  - Case where (E,F) is in the second set: In this case, $E = \llbracket P \rrbracket_L$ and $F = \llbracket Q \rrbracket_{R'}$, with $P \leq_{sim} Q$. Suppose $E \xrightarrow{t} E'$. Then by Lemma A.4, there exist s, l and P' such that $P \xrightarrow{l} P'$ and $E \xrightarrow{t} E' \xrightarrow{s} \llbracket P' \rrbracket_L$ with $ts = \llbracket l \rrbracket$. By the condition $P \leq_{sim} Q$, there exists Q' such that $Q \xrightarrow{l} Q'$ with $P' \leq_{sim} Q'$. By Lemma A.1, there exists F' such that $\llbracket Q \rrbracket_{R'} \xrightarrow{t} F' \xrightarrow{s} \llbracket Q' \rrbracket_{R'}$. The required result follows, since (E', F') is in the third set of $\llbracket \leq_{sim} \rrbracket$.
  - Case where (E,F) is in the third set: In this case, we have:

    $$\begin{array}{llll} P \leq_{sim} Q & P' \leq_{sim} Q' & s_1 s_2 = \llbracket l \rrbracket & s_1, s_2 \neq \epsilon \\ \multicolumn{2}{l}{\llbracket P \rrbracket_L \xrightarrow{s_1} E \xrightarrow{s_2} \llbracket P' \rrbracket_L} & \multicolumn{2}{l}{\llbracket Q \rrbracket_{R'} \xrightarrow{s_1} F \xrightarrow{s_2} \llbracket Q' \rrbracket_{R'}} \end{array}$$

    Suppose $E \xrightarrow{t} E'$. There are two cases to consider:

    - Case $E \xrightarrow{t} E' \xrightarrow{s_2'} \llbracket P' \rrbracket_L$ where $s_2 = ts_2'$. By the condition $F \xrightarrow{s_2} \llbracket Q' \rrbracket_{R'}$, there exists F' such that $F \xrightarrow{t} F' \xrightarrow{s_2'} \llbracket Q' \rrbracket_{R'}$. The required result follows, since (E', F') is in either the second or the third set.
    - Case where $E \xrightarrow{t} E' \xrightarrow{s_2'} \llbracket P' \rrbracket_L$ does not hold for s_2' such that $ts_2' = s_2$. By Lemma A.9 and the condition $\llbracket Q \rrbracket_{R'} \xrightarrow{s_1} F \xrightarrow{s_2} \llbracket Q' \rrbracket_{R'}$, $\llbracket Q_1 \rrbracket^{s_2, k_1, k_2} \leq_{sim} F$ for some Q_1, where $k_1 = \#a(s_1)$ and $k_2 = \#b(s_1)$. By Lemma A.10, we also have $t = a$ and either (i) $\#a(s_1) = 2$ or (ii) $E' \overset{b^{2N-1-k}}{\not\longrightarrow}$ and $\#a(s_1) = 1$. In case (i), by $\llbracket Q_1 \rrbracket^{s_2, 2, k_2} \leq_{sim} F$, there exists F' such that $F \xrightarrow{t} F'$ and $G \leq_{sim} F'$. Since $\mathcal{R}$ contains the identity relation, we have $E' \leq_{sim} G \mathcal{R} G \leq_{sim} F'$ as required. In case (ii), by $\llbracket Q_1 \rrbracket^{s_2, 1, k_2} \leq_{sim} F$, there exists F' such that $F \xrightarrow{t} F'$ and $H^{(2N-2-k_2)} \leq_{sim} F'$. Moreover, by Lemma A.7 and $E' \overset{b^{2N-1-k_2}}{\not\longrightarrow}$, we have $E' \leq_{sim} H^{(2N-2-k_2)}$. Hence, we have $E' \leq_{sim} H^{(2N-2-k_2)} \mathcal{R} H^{(2N-2-k_2)} \leq_{sim} F'$ as required.

- "If" : Define the relation $\mathcal{S}$ by:

  $$\mathcal{S} \quad = \quad \{(P,Q) \mid \llbracket P \rrbracket_L \leq_{sim} \llbracket Q \rrbracket_{R'}\}$$

  We prove that $\mathcal{S}$ is simulation. Suppose $(P,Q) \in \mathcal{S}$ and $P \xrightarrow{l} P'$. Then $\llbracket P \rrbracket_L \xrightarrow{\llbracket l \rrbracket} \llbracket P' \rrbracket_L$ holds by Lemma 3.7. By the definition of $\mathcal{S}$, $\llbracket P \rrbracket_L \leq_{sim} \llbracket Q \rrbracket_{R'}$, so that there exists some F such that $[\![Q]\!]_{R'} \xrightarrow{[\![l]\!]} F$ and $[\![P']\!]_L \leq_{sim} F$. By Lemma A.6, there exists some Q' such that $F = [\![Q']\!]_{R'}$ and $Q \xrightarrow{l} Q'$. We have $(P', Q') \in \mathcal{S}$ as required, since $[\![P']\!]_L \leq_{sim} [\![Q']\!]_{R'}$ holds.

□

A.4 Proof of Lemma 5.4

Proof: We show this by induction on the structure of U.

- $U = \mathbf{0}$: Let $P = \mathbf{0}$. Then, $x_1 : \mathbf{chan}_{U_\perp}[\mathbf{chan}_{U_1}[\,]], \dots, x_n : \mathbf{chan}_{U_\perp}[\mathbf{chan}_{U_n}[\,]], r : \mathbf{chan}_{U'}[\,] \vdash P$ if and only if $U' \leq U$ as required.
- $U = X_i$: Let $P = x_i![r].\,\mathbf{0}$. Then,

$$\begin{aligned}&x_1 : \mathbf{chan}_{U_\perp}[\mathbf{chan}_{U_1}[\,]], \dots, x_n : \mathbf{chan}_{U_\perp}[\mathbf{chan}_{U_n}[\,]], r : \mathbf{chan}_{U'}[\,] \vdash P\\ &\Longleftrightarrow U' \leq U_i \,|\, \mathbf{0}\\ &\Longleftrightarrow U' \leq U_i\end{aligned}$$

- $U = !V$: By the induction hypothesis, there exists P_1 such that

$$\begin{aligned}&x_1 : \mathbf{chan}_{U_\perp}[\mathbf{chan}_{U_1}[\,]], \dots, x_n : \mathbf{chan}_{U_\perp}[\mathbf{chan}_{U_n}[\,]], r : \mathbf{chan}_{V'}[\,] \vdash P_1\\ &\Longleftrightarrow V' \leq [U_1/X_1, \dots, U_n/X_n]V\end{aligned}$$

  Let $P = x![\,].\,P_1$. Then,

$$\begin{aligned}&x_1 : \mathbf{chan}_{U_\perp}[\mathbf{chan}_{U_1}[\,]], \dots, x_n : \mathbf{chan}_{U_\perp}[\mathbf{chan}_{U_n}[\,]], r : \mathbf{chan}_{U'}[\,] \vdash P\\ &\Longleftrightarrow U' \leq ![U_1/X_1, \dots, U_n/X_n]V = [U_1/X_1, \dots, U_n/X_n]U\end{aligned}$$

- $U = ?V$: Similar to the above case.
- $U = V_1 \,|\, V_2$: By the induction hypothesis, there exist P_1 and P_2 such that

$$\begin{aligned}&x_1 : \mathbf{chan}_{U_\perp}[\mathbf{chan}_{U_1}[\,]], \dots, x_n : \mathbf{chan}_{U_\perp}[\mathbf{chan}_{U_n}[\,]], r : \mathbf{chan}_{V_1'}[\,] \vdash P_1\\ &\Longleftrightarrow V_1' \leq [U_1/X_1, \dots, U_n/X_n]V_1\\ &x_1 : \mathbf{chan}_{U_\perp}[\mathbf{chan}_{U_1}[\,]], \dots, x_n : \mathbf{chan}_{U_\perp}[\mathbf{chan}_{U_n}[\,]], r : \mathbf{chan}_{V_2'}[\,] \vdash P_2\\ &\Longleftrightarrow V_2' \leq [U_1/X_1, \dots, U_n/X_n]V_2\end{aligned}$$

  Let $P = P_1 \,|\, P_2$. Then,

$$\begin{aligned}&x_1 : \mathbf{chan}_{U_\perp}[\mathbf{chan}_{U_1}[\,]], \dots, x_n : \mathbf{chan}_{U_\perp}[\mathbf{chan}_{U_n}[\,]], r : \mathbf{chan}_{U'}[\,] \vdash P\\ &\Longleftrightarrow U' \leq [U_1/X_1, \dots, U_n/X_n]V_1 \,|\, [U_1/X_1, \dots, U_n/X_n]V_2 = [U_1/X_1, \dots, U_n/X_n]U\end{aligned}$$

- $U = V_1 + V_2$: By the induction hypothesis, there exist P_1 and P_2 such that

$$\begin{aligned}&x_1 : \mathbf{chan}_{U_\perp}[\mathbf{chan}_{U_1}[\,]], \dots, x_n : \mathbf{chan}_{U_\perp}[\mathbf{chan}_{U_n}[\,]], r : \mathbf{chan}_{V_1'}[\,] \vdash P_1\\ &\Longleftrightarrow V_1' \leq [U_1/X_1, \dots, U_n/X_n]V_1\\ &x_1 : \mathbf{chan}_{U_\perp}[\mathbf{chan}_{U_1}[\,]], \dots, x_n : \mathbf{chan}_{U_\perp}[\mathbf{chan}_{U_n}[\,]], r : \mathbf{chan}_{V_2'}[\,] \vdash P_2\\ &\Longleftrightarrow V_2' \leq [U_1/X_1, \dots, U_n/X_n]V_2\end{aligned}$$

Let $P = (\nu u : U_\perp)\,(u![r].\,\mathbf{0} \mid u?[r].\,P_1 \mid u?[r].\,P_2)$. Then,

$$\begin{array}{l} x_1 : \mathbf{chan}_{U_\perp}[\mathbf{chan}_{U_1}[\,]], \dots, x_n : \mathbf{chan}_{U_\perp}[\mathbf{chan}_{U_n}[\,]], r : \mathbf{chan}_{U'}[\,] \vdash P \\ \Longleftrightarrow U' \leq [U_1/X_1, \dots, U_n/X_n]V_1 \wedge U' \leq [U_1/X_1, \dots, U_n/X_n]V_2 \\ \Longleftrightarrow U' \leq [U_1/X_1, \dots, U_n/X_n]U \end{array}$$

Here, note that $U \leq U_1 \wedge U \leq U_2$ if and only if $U \leq U_1 + U_2$.

- $U = \mu X_{n+1}.V$: By the induction hypothesis, there exists P_1 such that

$$\begin{array}{l} x_1 : \mathbf{chan}_{U_\perp}[\mathbf{chan}_{U_1}[\,]], \dots, x_n : \mathbf{chan}_{U_\perp}[\mathbf{chan}_{U_n}[\,]], \\ \quad x_{n+1} : \mathbf{chan}_{U_\perp}[\mathbf{chan}_{U_{n+1}}[\,]], r : \mathbf{chan}_{V'}[\,] \vdash P_1 \\ \Longleftrightarrow V' \leq [U_1/X_1, \dots, U_n/X_n, U_{n+1}/X_{n+1}]V \end{array}$$

Let $P = (\nu x_{n+1} : U_\perp)\,(x_{n+1}?[r].\,P_1 \mid x_{n+1}![r].\,\mathbf{0})$. Then,

$$\begin{array}{l} x_1 : \mathbf{chan}_{U_\perp}[\mathbf{chan}_{U_1}[\,]], \dots, x_n : \mathbf{chan}_{U_\perp}[\mathbf{chan}_{U_n}[\,]], r : \mathbf{chan}_{U'}[\,] \vdash P \\ \Longleftrightarrow \exists U_{n+1}.(U' \leq U_{n+1} \wedge U_{n+1} \leq [U_1/X_1, \dots, U_n/X_n, U_{n+1}/X_{n+1}]V) \\ \Longleftrightarrow U' \leq U \end{array}$$

Here, we have used the fact that $V_1 \leq [V_1/X]V_2$ if and only if $V_1 \leq \mu X.V_2$.

□