THIS DOCUMENT IS THE ONLINE-ONLY APPENDIX TO:

Proof Search Specifications of Bisimulation and Modal Logics for the π-calculus

Alwen Tiu
Logic and Computation Group
College of Engineering and Computer Science
The Australian National University
and
Dale Miller
INRIA-Saclay & LIX, École polytechnique

ACM Journal Name, Vol. V, No. N, 20YY, Pages 1–34.

A. PROPERTIES OF ONE-STEP TRANSITIONS

To prove the adequacy results for the encodings of bisimulation and modal logics, we shall consider some derived rules which allow us to enumerate all possible next states from a given process. In the following, we use the notation $\alpha^n \to \beta$ to denote the type $\underbrace{\alpha \to \cdots \to \alpha}_{n} \to \beta$, and we write $\alpha^* \to \beta$ to denote $\alpha^n \to \beta$ for some $n \geq 0$.

DEFINITION 29. The judgments $\sigma \triangleright P \xrightarrow{A} Q$ and $\sigma \triangleright P \xrightarrow{A} Q$ are *higher-order patterned judgments*, or patterned judgments for short, if

(1) every occurrence of the free variables in the judgment is applied to distinct names, which are either in σ or bound by λ-abstractions, *i.e.*, $M\ a_1 \cdots a_n$, where $a_i \in \sigma$ or it is bound by some λ-abstraction, and $a_1, \ldots, a_n$ are pairwise distinct,
(2) the only occurrences of free variables in P are those of type $n^n \to n$ where $n \geq 0$, and the only occurrences of free variables in A are those of type $n^n \to n$ or $n^n \to a$,
(3) and Q is of the form $(M\ \vec{\sigma})$ for some variable M.

The process term P in the transition predicate $P \xrightarrow{A} Q$ and $P \xrightarrow{A} Q$ is called a *primary* process term. The notion of patterned judgments extends to non-atomic judgments, which are defined inductively as follows:

—$\sigma \triangleright \top$ is a patterned judgment,

Permission to make digital/hard copy of all or part of this material without fee for personal or classroom use provided that the copies are not made or distributed for profit or commercial advantage, the ACM copyright/server notice, the title of the publication, and its date appear, and notice is given that copying is by permission of the ACM, Inc. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or a fee.
© 20YY ACM 0000-0000/YY/00-0001 $5.00

—if $\sigma \triangleright B$ and $\sigma \triangleright C$ are patterned judgments such that both judgments have no free variables in common which are of type $n^* \to p$, then $\sigma \triangleright B \wedge C$ is a patterned judgment,

—if $\sigma x \triangleright B$ is a patterned judgment, then $\sigma \triangleright \nabla x.B$ is a patterned judgment,

—and if $\sigma \triangleright B[h\,\vec{\sigma}/y]$ is a patterned judgment then $\sigma \triangleright \exists y.B$ is a patterned judgment, provided that h is of type $n^n \to a$ or $n^n \to p$, and h is not free in $\exists y.B$.

Two patterned judgments $\mathcal{A}$ and $\mathcal{B}$ are *p-compatible* if they do not have variables in common which are of type $n^* \to p$.

The restrictions on the occurences of free variables in patterned judgments are similar to the restrictions used in higher-order pattern unification. This is to ensure that proof search for patterned judgments involves only higher-order pattern unification.

Let ρ be a substitution and let Σ be a signature. We write $\Sigma \vdash \rho$ if for every $x \in \mathrm{dom}(\rho)$ of type τ, we have $\Sigma \vdash \rho(x) : \tau$. Two signatures Σ and Σ' are said to be compatible if whenever $x : \tau_1 \in \Sigma$ and $y : \tau_2 \in \Sigma'$, $x = y$ implies $\tau_1 = \tau_2$. Given two signature-and-substitution pairs (Σ_1, ρ_1) and (Σ_2, ρ_2) such that Σ_1 and Σ_2 are compatible, and $\Sigma_1 \vdash \rho_1$ and $\Sigma_2 \vdash \rho_2$, we write $(\Sigma_1, \rho_1) \circ (\Sigma_2, \rho_2)$ to denote the pair $(\Sigma_1\rho_2 \cup \Sigma_2, \rho_1 \circ \rho_2)$. This definition of composition extends straightforwardly to composition between a pair and a set or a list of pairs.

Let us call a signature-substitution pair (Σ, ρ) a *solution* for a patterned judgment $\mathcal{C}$ if $\Sigma \vdash \rho$ and $\Sigma\,;\,.\, \longmapsto \mathcal{C}\rho$ is provable. In proving the adequacy of the encoding of bisimulation and modal logics for the π calculus, we often want to find all possible solutions to a given transition relation, which corresponds to enumerating all possible continuations of a given process. For this purpose, we define a construction of "open" derivation trees for a given list of patterned judgments Δ. Open derivation trees are trees made of nodes which are instances of certain inference rules. This construction gives us a set of derivation trees for the sequent $\Delta \vdash \bot$, following a certain order of rule applications. As we shall see, the construction of the trees basically amounts to application of left-introduction rules to Δ. We are interested in collecting all the substitutions generated by the *def*$\mathcal{L}$ rule in these trees, which we will show to correspond to the solutions for the patterned judgments in Δ.

Definition 30. Let Δ be a list of patterned judgments such that its elements are pairwise p-compatible, and let (Σ, θ) be a pair such that $\Sigma \vdash \theta$, and that the free variables of Δ are in Σ. An *open inference rule* is an inference on triples of the form $(\Sigma', \Delta', \theta')$ where Σ' is a signature, Δ' is a list of patterned judgments and θ' is a substitution such that $\Sigma' \vdash \theta'$. We will use the notation $(\Sigma', \theta') \vdash \Delta'$ to denote such a triple. *Open derivation trees* are derivations constructed using the following open inference rules:

$$\frac{}{(\Sigma, \theta) \vdash [\,]}\ open \qquad \frac{(\Sigma, \theta) \vdash \Delta'}{(\Sigma, \theta) \vdash \bar{n} \triangleright \top, \Delta'}\ \top$$

$$\frac{(\Sigma, \theta) \vdash \bar{n} \triangleright A, \bar{n} \triangleright B, \Delta'}{(\Sigma, \theta) \vdash \bar{n} \triangleright A \wedge B, \Delta'}\ \wedge \qquad \frac{(\Sigma \cup \{h\}, \theta) \vdash \bar{n} \triangleright B\,(h\,\bar{n}), \Delta'}{(\Sigma, \theta) \vdash \bar{n} \triangleright \exists x.B\,x, \Delta'}\ \exists$$

$$\frac{\{(\Sigma\rho, \theta \circ \rho) \vdash \mathcal{B}\rho, \Delta\rho \mid \rho \in CSU(\mathcal{A}, \mathcal{H}),\ \mathcal{H} \triangleq \mathcal{B}\}}{(\Sigma, \theta) \vdash \mathcal{A}, \Delta}\ def$$

In the $\exists$-rule, the eigenvariable h is new, *i.e.*, it is not in Σ. In the *def*-rule, we require that for every $\rho \in CSU(\mathcal{A}, \mathcal{H})$, the judgments $\mathcal{B}\rho, \Delta\rho$ are patterned judgments. That is, we restrict the CSU's to those that preserves the pattern restrictions on judgments. The instances of the *open*-rule in an open derivation are called *open leaves* of the derivation. Given an open derivation Π, we denote with $\mathcal{L}(\Pi)$ the set of signature-substitution pairs in the open leaves of Π.

DEFINITION 31. The measure of a patterned judgment $\sigma \triangleright B$, written $|\sigma \triangleright B|$, is the number of process constructors occuring in the primary terms in B. The measure of a list of judgments Δ is the multiset of measures of the judgments in Δ.

LEMMA 32. *Let Δ be a list of patterned judgments such that its elements are pairwise p-compatible, and whose variables are in a given signature Σ. Let θ be a substitution such that $\Sigma \vdash \theta$. Then there exists an open derivation Π of $(\Sigma, \theta) \vdash \Delta$.*

LEMMA 33. *Let Σ_1, Σ_2, θ_1 and θ_2 be signatures and substitutions such that $\Sigma_1 \vdash \theta_1$ and $\Sigma_2 \vdash \theta_2$. Let Δ be a list of pairwise p-compatible patterned jugdments such that all its free variables are in Σ_2. If there exists an open derivation Π_1 of $(\Sigma_1\theta_2 \cup \Sigma_2, \theta_1 \circ \theta_2) \vdash \Delta$, then there exists an open derivation Π_2 of $(\Sigma_2, \theta_2) \vdash \Delta$ of the same height such that $\mathcal{L}(\Pi_1) = (\Sigma_1, \theta_1) \circ \mathcal{L}(\Pi_2)$ and vice versa.*

The following lemma states that the open leaves in an open derivation are solutions of the patterned judgments on the root of the derivation tree. This can be proved by induction on the height of derivation and case analysis on the definition clauses of one-step transitions.

LEMMA 34. *Let Δ be a list of patterned judgments such that its elements are pairwise p-compatible and whose variables are in a given signature Σ. Let Π be an open derivation of $(\Sigma, \epsilon) \vdash \Delta$. Then for every element $\mathcal{C} \in \Delta$ and every pair $(\Sigma', \theta) \in \mathcal{L}(\Pi)$, the sequent $\Sigma' ; . \longleftarrow \mathcal{C}\theta$ is provable.*

We are now ready to define the following derived rules. The rule one_f enumerates all possible free-actions that a process can perform. Given a patterned judgment $\bar{n} \triangleright P \xrightarrow{A} Q$ and an open derivation Π of $(\Sigma, \epsilon) \vdash \bar{n} \triangleright P \xrightarrow{A} Q$, the one_f rule, applied to this judgment, is as follows:

$$\frac{\{\Sigma' ; \Gamma\theta \longleftarrow \mathcal{C}\theta \mid (\Sigma', \theta) \in \mathcal{L}(\Pi)\}}{\Sigma ; \bar{n} \triangleright P \xrightarrow{A} Q, \Gamma \longleftarrow \mathcal{C}}\ one_f$$

The corresponding rule for bound input or bound output transition is defined analogously, *i.e.*,

$$\frac{\{\Sigma' ; \Gamma\theta \longleftarrow \mathcal{C}\theta \mid (\Sigma', \theta) \in \mathcal{L}(\Pi)\}}{\Sigma ; \bar{n} \triangleright P \xrightarrow{X} M, \Gamma \longleftarrow \mathcal{C}}\ one_b.$$

where Π is an open derivation of $(\Sigma, \epsilon) \vdash \bar{n} \triangleright P \xrightarrow{X} M$. Since open inference rules are essentially invertible left-rules of $FO\lambda^{\Delta\nabla}$, these derived rules are sound and invertible.

LEMMA 35. *The rules* one_f *and* one_b *are invertible and derivable in* $FO\lambda^{\Delta\nabla}$.

We can now prove Proposition 9.

PROOF. Suppose that $\mathtt{P} \xrightarrow{\alpha} \mathtt{Q}$ does not hold in the π-calculus. We show that the sequent $\neg\nabla\bar{n}.[\![\mathtt{P} \xrightarrow{\alpha} \mathtt{Q}]\!]$ is derivable in $FO\lambda^{\Delta\nabla}$. This is equivalent to proving the sequent $;\vec{n} \triangleright [\![\mathtt{P} \xrightarrow{\alpha} \mathtt{Q}]\!] \vdash \bot$. We apply either one_f or one_b to the sequent (bottom-up), depending on whether α is a free or a bound action. In both cases, if the premise of the one_f or one_b is empty, then we are done. Otherwise, there exists a substitution θ such that $(\nabla\vec{n}.[\![\mathtt{P} \xrightarrow{\alpha} \mathtt{Q}]\!])\theta$ is derivable in $FO\lambda^{\Delta\nabla}$. Since the transition judgment is ground, this would mean that $\nabla\vec{n}.[\![\mathtt{P} \xrightarrow{\alpha} \mathtt{Q}]\!]$ is derivable, and by Proposition 8, the transition $\mathtt{P} \xrightarrow{\alpha} \mathtt{Q}$ holds in the π-calculus, contradicting our assumption.

Conversely, suppose that $\neg\nabla\bar{n}.[\![\mathtt{P} \xrightarrow{\alpha} \mathtt{Q}]\!]$ is derivable in $FO\lambda^{\Delta\nabla}$. Then $\mathtt{P} \xrightarrow{\alpha} \mathtt{Q}$ cannot be a transition in the π-calculus, for otherwise, we would have $\vdash \nabla\bar{n}.[\![\mathtt{P} \xrightarrow{\alpha} \mathtt{Q}]\!]$ by Proposition 8, and by cut, we would have a proof of $\bot$, which is impossible. □

B. ADEQUACY OF THE SPECIFICATIONS OF BISIMULATIONS

We need some auxiliary lemmas that concern the structures of cut free proofs. The next three lemmas can be proved by simple permutations of inference rules.

LEMMA 36. *Let* Π *be a cut-free derivation of* $\cdot\,;\Gamma \vdash \mathcal{C}$, *where* $\mathcal{C}$ *contains a non-equality atomic formula and every judgment in* Γ *is in one of the following forms:*

$$\bar{n} \triangleright \forall x \forall y. x = y \lor x \neq y \qquad \bar{n} \triangleright \forall y. a = y \lor a \neq y \qquad \bar{n} \triangleright a = b \lor a \neq b$$

$$\bar{n} \triangleright a = a \lor a \neq a \qquad \bar{n} \triangleright a = a \qquad \bar{n} \triangleright a \neq b$$

for some $\bar{n}$ *and distinct names* a, b *in* $\bar{n}$. *Then there exists a derivation of the sequent which ends with a right-introduction rule on* $\mathcal{C}$.

LEMMA 37. *The* def$\mathcal{R}$ *rule, applied to lbisim* $P\ Q$, *for any* P *and* Q, *is invertible.*

LEMMA 38. *The* def$\mathcal{R}$ *rule, applied to ebisim* $P\ Q$, *for any* P *and* Q, *is invertible.*

B.1 Adequacy of the specification of late bisimulation

In the following, we use the notation $x_1 \neq x_2 \neq \cdots \neq x_{n-1} \neq x_n$ to abbreviate the conjunction

$$\bigwedge \{x_i \neq x_j \mid i, j \in \{1, \dots, n\}, i \neq j\}.$$

With a slight abuse of notation, we shall write $\mathcal{X} \supset B$, where $\mathcal{X}$ is a finite set of formula $\{B_1, \dots, B_n\}$, to mean $B_1 \land \cdots \land B_n \supset B$, and we shall write $\nabla y.\mathcal{X}$ to mean the formula $\nabla y.B_1 \land \cdots \land \nabla y.B_2$.

LEMMA 39. *Let* $\mathtt{P}$ *and* $\mathtt{Q}$ *be two late-bisimilar finite* π*-processes and let* $n_1, \dots, n_k$ *be the free names in* $\mathtt{P}$ *and* $\mathtt{Q}$. *Then for some finite set* $\mathcal{X} \subset \mathcal{E}$, *we have*

$$\vdash \forall n_1 \cdots \forall n_k.(\mathcal{X} \land n_1 \neq n_2 \neq \cdots \neq n_k \supset \mathit{lbisim}\ \mathtt{P}\ \mathtt{Q}). \qquad (3)$$

Proof. We construct a proof of formula (3) by induction on the size of P and Q, *i.e.*, the number of action prefixes in P and Q. It can be easily shown that the number of prefixes in a process is reduced by transitions, for finite processes. By applying the introduction rules for $\forall$, $\supset$ and unfolding the definition of *lbisim* (bottom up) to the formula (3), we get the following three sequents:

(1) $n_1, \cdots, n_k, A, P' \,;\, \mathcal{X}, n_1 \neq \cdots \neq n_k, \mathtt{P} \xrightarrow{A} P' \vdash \exists Q'.\mathtt{Q} \xrightarrow{A} Q' \wedge \mathit{lbisim}\ P'\ Q'$

(2) $n_1, \cdots, n_k, X, P' \,;\, \mathcal{X}, n_1 \neq \cdots \neq n_k, \mathtt{P} \xrightarrow{\downarrow X} P' \vdash \exists Q'.\ \mathtt{Q} \xrightarrow{\downarrow X} Q' \wedge \forall w.\mathit{lbisim}\ (P'w)\ (Q'w)$

(3) $n_1, \cdots, n_k, X, P' \,;\, \mathcal{X}, n_1 \neq \cdots \neq n_k, \mathtt{P} \xrightarrow{\uparrow X} P' \vdash \exists Q'.\ \mathtt{Q} \xrightarrow{\uparrow X} Q' \wedge \nabla w.\mathit{lbisim}\ (P'w)\ (Q'w)$

and their symmetric counterparts (obtained by exchanging the role of P and Q). The set $\mathcal{X}$ is left unspecified above, since it will be constructed by induction hypothesis (in the base case, where both P and Q are deadlocked processes, define $\mathcal{X}$ to be the empty set). We show here how to construct proofs for these three sequents; their symmetric counterparts can be proved similarly. In all these three cases, we apply either the one_f rule (for sequent 1) or the one_b rule (for sequent 2 and 3). If this application of one_f (or one_b) results in two distinct name-variables, say n_1 and n_2, to be identified, then the sequent is proved by using the assumption $n_1 \neq n_2$. Therefore the only interesting cases are when the name-variables $n_1, \cdots, n_k$ are instantiated to distinct name-variables, say, $m_1, \cdots, m_k$. In the following we assume that the substitution in the premises of one_f or one_b are non-trivial, meaning that they do not violate the assumption on name-distinction above.

Sequent 1. In this case, after applying the one_f rule bottom up and discharging the trivial premises, we need to prove, for each θ associated with the rule, the sequent

$$m_1, \cdots, m_k, \Sigma \,;\, \mathcal{X}, m_1 \neq \cdots \neq m_k \vdash \exists Q'.\mathtt{Q}\theta \xrightarrow{A\theta} Q' \wedge \mathit{lbisim}\ (P'\theta)\ Q'$$

for some signature Σ. We give a top-down construction of a derivation of this sequent as follows. By Lemma 34, we know that

$$\vdash m_1, \cdots, m_k, \Sigma \,;\, . \vdash \mathtt{P}\theta \xrightarrow{A\theta} P'\theta.$$

Since $m_1, \ldots, m_k$ are the only free names in $\mathtt{P}\theta$, we can show by induction on proofs that Σ in the sequent is redundant and can be removed, thus

$$\vdash m_1, \cdots, m_k \,;\, . \vdash \mathtt{P}\theta \xrightarrow{A\theta} P'\theta.$$

By the adequacy of one-step transition (Proposition 8), we have $\mathtt{P}\theta \xrightarrow{A\theta} P'\theta$. Notice that P is a renaming of $\mathtt{P}\theta$, since $m_1, \ldots, m_k$ are pairwise distinct. We recall that both one-step transitions and (late) bisimulation are closed under injective renaming (see, *e.g.*, [Milner et al. 1992]). Therefore, there exist α and R such that $\mathtt{P} \xrightarrow{\alpha} \mathtt{R}$, where α and R are obtained from $A\theta$ and $P'\theta$, respectively, under the same injective renaming. Since P and Q are bisimilar, there exists T such that $\mathtt{Q} \xrightarrow{\alpha} \mathtt{T}$, hence, by injective renaming and the adequacy result for one-step transitions, the sequent $m_1, \cdots, m_k \,;\, . \longmapsto \mathtt{Q}\theta \xrightarrow{A\theta} \mathtt{T}\theta$ is provable. It remains to show that

$$\vdash m_1, \cdots, m_k \,;\, \mathcal{X}, m_1 \neq \cdots \neq m_k \longmapsto \mathit{lbisim}\ (P'\theta)\ (\mathtt{T}\theta)$$

By induction hypothesis (note that the size of $(\mathtt{R}, \mathtt{T})$ is smaller than $(\mathtt{P}, \mathtt{Q})$), we have

$$\vdash \forall x_1 \cdots \forall x_j.\mathcal{X}' \wedge x_1 \neq \cdots \neq x_j \supset \mathit{lbisim}\ \mathtt{R}\ \mathtt{T}$$

where $\{x_1, \ldots, x_j\}$ is a subset of $\{n_1, \ldots, n_k\}$. We can weaken the formula with extra variables and assumptions to get

$$\vdash \forall n_1 \cdots \forall n_k.\mathcal{X}' \wedge n_1 \neq \cdots \neq n_k \supset \mathit{lbisim}\ \mathtt{R}\ \mathtt{T}.$$

Now since the $\forall R$ and $\supset R$ rules are invertible, this means

$$\vdash n_1, \ldots, n_k \,;\, \mathcal{X}', n_1 \neq \cdots \neq n_k \longmapsto \mathit{lbisim}\ \mathtt{R}\ \mathtt{T}.$$

Now define $\mathcal{X}$ to be $\mathcal{X}'$ and apply a renaming substitution which maps each n_i to m_i, we get a derivation of

$$m_1, \ldots, m_k \,;\, \mathcal{X}, m_1 \neq \cdots \neq m_k \longmapsto \mathit{lbisim}\ (P'\theta)\ (\mathtt{T}\theta).$$

Since provability is closed under weakening of signature, we have

$$\vdash m_1, \ldots, m_k, \Sigma \,;\, \mathcal{X}, m_1 \neq \cdots \neq m_k \longmapsto \mathit{lbisim}\ (P'\theta)\ (\mathtt{T}\theta),$$

and together with provability of $m_1, \ldots, m_k \,;\, . \longmapsto \mathtt{Q}\theta \xrightarrow{A\theta} \mathtt{T}\theta$, we get

$$\vdash m_1, \cdots, m_k, \Sigma \,;\, \mathcal{X}, m_1 \neq \cdots \neq m_k \longmapsto \mathtt{Q}\theta \xrightarrow{A\theta} \mathtt{T}\theta \wedge \mathit{lbisim}\ (P'\theta)\ \mathtt{T}\theta.$$

Finally, applying an $\exists R$ to this sequent, we get

$$\vdash m_1, \cdots, m_k, \Sigma \,;\, \mathcal{X}, m_1 \neq \cdots \neq m_k \longmapsto \exists Q'.\mathtt{Q}\theta \xrightarrow{A\theta} Q' \wedge \mathit{lbisim}\ (P'\theta)\ Q'.$$

Sequent 2.. In this case, we need to prove the sequent

$$(*)\ m_1, \cdots, m_k, \Sigma \,;\, \mathcal{X}, m_1 \neq \cdots \neq m_k \longmapsto \exists Q'.\mathtt{Q}\theta \xrightarrow{\downarrow X\theta} Q' \wedge \forall w.\mathit{lbisim}\ ((P'\theta)w)\ (Q'w)$$

for each non-trivial θ in the premises of one_b rule. By the same reasoning as in the previous case, we obtain, for every transition $P\theta \xrightarrow{x(w)} \mathtt{R}$, where $\mathtt{R} = (P'\theta)\,w$, another transition $Q\theta \xrightarrow{x(w)} \mathtt{T}$ such that for all name z $\mathtt{R}[z/w] \sim_l \mathtt{T}[z/w]$. It is enough to consider $k{+}1$ cases for z, *i.e.*, those in which z is one of $m_1, \ldots, m_k$ and another where z is a new name, say m_{k+1}. By induction hypothesis, we have, for each $i \in \{1, \ldots, k\}$, a provable formula F_i

$$\forall m_1 \cdots \forall m_k.\mathcal{X}_1 \wedge m_1 \neq \cdots \neq m_k \supset \mathit{lbisim}\ (\mathtt{R}[m_i/w])\ (\mathtt{T}[m_i/w])$$

and a provable formula F_{k+1}:

$$\forall m_1 \cdots \forall m_{k+1}.\mathcal{X}_{k+1} \wedge m_1 \neq \cdots \neq m_{k+1} \supset \mathit{lbisim}\ (\mathtt{R}[m_{k+1}/w])\ (\mathtt{T}[m_{k+1}/w]).$$

Let $\mathcal{X}$ be the set $\{\forall x \forall y. x = y \vee x \neq y\} \cup \{\mathcal{X}_i \mid i \in \{1, \ldots, k+1\}\}$. Then the sequent $(*)$ is proved, in a bottom-up fashion, by instantiating Q' to $\lambda w.\mathtt{T}$, followed by an

$\wedge\mathcal{R}$-rule, resulting in the sequents:

$$m_1, \ldots, m_k, \Sigma\,;\, \mathcal{X}, m_1 \neq \cdots \neq m_k \longrightarrow \mathtt{Q}\theta \xrightarrow{A\theta} \lambda w.\mathtt{T} \qquad \text{and}$$

$$m_1, \ldots, m_k, \Sigma\,;\, \mathcal{X}, m_1 \neq \cdots \neq m_k \longrightarrow \forall w.\mathit{lbisim}\ \mathtt{R}\ \mathtt{T}$$

The first sequent is provable following the adequacy of one-step transition. For the second sequent, we apply the $\forall R$-rule to get the sequent

$$m_1, \ldots, m_k, m_{k+1}, \Sigma\,;\, \mathcal{X}, m_1 \neq \cdots \neq m_k \longrightarrow \mathit{lbisim}\ (\mathtt{R}[m_{k+1}/w])\ (\mathtt{T}[m_{k+1}/w]).$$

We then do a case analysis on the name m_{k+1}, using the assumption $\forall x \forall y. x = y \vee x \neq y$ in $\mathcal{X}$. Let $\mathtt{R}_{k+1} = \mathtt{R}[m_{k+1}/w]$ and let $\mathtt{T}_{k+1} = \mathtt{T}[m_{k+1}/w]$. We consider k instantiations, each instantiation compares m_{k+1} with m_i, for $i \in \{1, \ldots, k\}$. We thus get the following sequents:

(S_1) $\quad \Sigma'\,;\, \Delta, m_1 = m_{k+1} \longrightarrow \mathit{lbisim}\ \mathtt{R}_{k+1}\ \mathtt{T}_{k+1}$
(S_2) $\quad \Sigma'\,;\, \Delta, m_1 \neq m_{k+1}, m_2 = m_{k+1} \longrightarrow \mathit{lbisim}\ \mathtt{R}_{k+1}\ \mathtt{T}_{k+1}$
$\vdots$
(S_k) $\quad \Sigma'\,;\, \Delta, m_1 \neq m_{k+1}, \ldots, m_{k-1} \neq m_{k+1}, m_k = m_{k+1} \longrightarrow \mathit{lbisim}\ \mathtt{R}_{k+1}\ \mathtt{T}_{k+1}$
(S_{k+1}) $\quad \Sigma', m_{k+1}\,;\, \Delta, m_1 \neq m_2, \cdots, m_{k-1} \neq m_k, m_k \neq m_{k+1} \longrightarrow \mathit{lbisim}\ \mathtt{R}_{k+1}\ \mathtt{T}_{k+1}$

Here Σ' denotes the set $\{m_1, \ldots, m_{k+1}\} \cup \Sigma$ and Δ denotes the set $\{\mathcal{X}, m_1 \neq \cdots \neq m_k\}$. Provability of these sequents follow from provability of $F_1, \ldots, F_{k+1}$.

Sequent 3. In this case, we need to prove the sequent

$$(**) \qquad m_1, \cdots, m_k, \Sigma\,;\, \mathcal{X}, m_1 \neq \cdots \neq m_k \longrightarrow \begin{array}{l} \exists Q'.\mathtt{Q}\theta \xrightarrow{A\theta} Q' \wedge \\ \quad \nabla w.\mathit{lbisim}\ ((P'\theta)w)\ (Q'w) \end{array}$$

for each non-trivial θ in the premises of one_b rule. As in the previous case, we obtain $\mathtt{R}$ and $\mathtt{T}$ such that $\mathtt{P}\theta \xrightarrow{\bar{x}(w)} \mathtt{R}$ and $\mathtt{Q}\theta \xrightarrow{\bar{x}(w)} \mathtt{T}$ where $\lambda w.\mathtt{R} = P'\theta$. We assume, without loss of generality, that w is fresh. By the induction hypothesis, $\mathtt{R} \sim_l \mathtt{T}$ and

$$\vdash \forall m_1 \cdots \forall m_k \forall w. \mathcal{X}' \wedge m_1 \neq \cdots \neq m_k \neq w \supset \mathit{lbisim}\ \mathtt{R}\ \mathtt{T}.$$

Now apply Proposition 3 to replace $\forall w$ with ∇w,

$$\vdash \forall m_1 \cdots \forall m_k \nabla w. \mathcal{X}' \wedge m_1 \neq \cdots \neq m_k \neq w \supset \mathit{lbisim}\ \mathtt{R}\ \mathtt{T}.$$

And since ∇ distributes over all propositional connectives, we also have

$$\vdash \forall m_1 \cdots \forall m_k.(\nabla w \mathcal{X}') \wedge \nabla w.(m_1 \neq \cdots \neq m_k) \wedge \nabla w(\bar{m} \neq w) \supset \nabla w.\mathit{lbisim}\ \mathtt{R}\ \mathtt{T}.$$

Let $\mathcal{X} = \nabla w \mathcal{X}'$. Now, since the right-introduction rules for $\forall$, ∇ and $\supset$ are all invertible, we have that the sequent

$$(i) \qquad m_1, \ldots, m_k\,;\, \mathcal{X}, \nabla w.(m_1 \neq \cdots \neq m_k), \nabla w(\bar{m} \neq w) \longrightarrow \nabla w.\mathit{lbisim}\ \mathtt{R}\ \mathtt{T}$$

is provable. It can be easily checked that the following sequents are provable:

$\nabla w.m_i \neq m_j \longrightarrow m_i \neq m_j$, for any i and j.
$\longrightarrow \nabla w.m_i \neq w$, for any i (since w is in the scope of m_i).

By applying the cut rules to these sequents and sequent (i) above, we obtain

$$(ii) \qquad m_1, \ldots, m_k \,;\, \mathcal{X}, m_1 \neq \cdots \neq m_k \vdash \nabla w.\mathit{lbisim}\ \mathtt{R}\ \mathtt{T},$$

Provability of sequent $(**)$ then follows from provability of sequent (ii) above and the adequacy of the one-step transition (*i.e.*, by instantiating Q' with $\lambda w.\mathtt{T}$). □

The following lemma shows that *lbisim* is symmetric. Its proof is straightforward by induction on derivations.

LEMMA 40. *Let* $\mathtt{P}$ *and* $\mathtt{Q}$ *be two* π*-processes and let* $\bar{n}$ *be the list of all free names in* $\mathtt{P}$ *and* $\mathtt{Q}$. *If* $\vdash \mathcal{X} \supset \nabla\bar{n}.\mathit{lbisim}\ \mathtt{P}\ \mathtt{Q}$, *for some* $\mathcal{X} \subset \mathcal{E}$, *then* $\vdash \mathcal{X} \supset \nabla\bar{n}.\mathit{lbisim}\ \mathtt{Q}\ \mathtt{P}$.

B.2 Proof for Theorem 15 (adequacy of late bisimulation specification)

Soundness. We define a set $\mathcal{S}$ as

$$\mathcal{S} = \{(\mathtt{P},\mathtt{Q}) \mid \vdash \mathcal{X} \supset \nabla\bar{n}\ \mathit{lbisim}\ \mathtt{P}\ \mathtt{Q}, \text{ where } \mathrm{fn}(\mathtt{P},\mathtt{Q}) \subseteq \{\bar{n}\} \text{ and } \mathcal{X} \subseteq_f \mathcal{E}\}$$

and show that $\mathcal{S}$ is a bisimulation, *i.e.*, it is symmetric and closed with respect to the conditions 1, 2 and 3 in Definition 11. The symmetry of $\mathcal{S}$ follows from Lemma 40.

Suppose that $(\mathtt{P},\mathtt{Q}) \in \mathcal{S}$, that is, $\vdash \mathcal{X} \supset \nabla\bar{n}\ \mathit{lbisim}\ \mathtt{P}\ \mathtt{Q}$ for some $\mathcal{X}$. Since $\mathit{def}\mathcal{R}$ on *lbisim* is invertible (Lemma 37), and since $\wedge\mathcal{R}$, $\supset\mathcal{R}$, $\nabla\mathcal{R}$ and $\forall\mathcal{R}$ are also invertible, there is a proof of the formula that ends with applications of these invertible rules. From this and the definition of *lbisim*, we can infer that provability of $\mathcal{X} \supset \nabla\bar{n}\ \mathit{lbisim}\ \mathtt{P}\ \mathtt{Q}$ implies provability of six other sequents, three of which are given in the following (the other three are symmetric counterparts of these):

$$(a)\ \ P', A \,;\, \mathcal{X}, \bar{n} \triangleright \mathtt{P} \xrightarrow{A\bar{n}} (P'\bar{n}) \vdash \bar{n} \triangleright \exists Q'.\mathtt{Q} \xrightarrow{A\bar{n}} Q' \ \wedge\ \mathit{lbisim}\ (P'\bar{n})\ Q'$$
$$(b)\ \ M, X \,;\, \mathcal{X}, \bar{n} \triangleright \mathtt{P} \xrightarrow{\downarrow(X\bar{n})} (M\bar{n}) \vdash \bar{n} \triangleright \exists N.\mathtt{Q} \xrightarrow{\downarrow(X\bar{n})} N \ \wedge\ \forall y.\mathit{lbisim}\ (M\bar{n}y)\ (Ny)$$
$$(c)\ \ M, X \,;\, \mathcal{X}, \bar{n} \triangleright \mathtt{P} \xrightarrow{\uparrow(X\bar{n})} (M\bar{n}) \vdash \bar{n} \triangleright \exists N.\mathtt{Q} \xrightarrow{\uparrow(X\bar{n})} N \ \wedge\ \nabla y.\mathit{lbisim}\ (M\bar{n}y)\ (Ny)$$

By examing the structure of proofs of these three sequents, we show that $\mathcal{S}$ is closed under all possible transitions from $\mathtt{P}$ and $\mathtt{Q}$. We examine the three cases in Definition 11:

(1) Suppose $\mathtt{P} \xrightarrow{\alpha} \mathtt{P}'$ for some free action α. Since $\mathtt{P} \xrightarrow{\alpha} \mathtt{P}'$, by the adequacy result for one-step transitions, we have that $\bar{n} \triangleright \mathtt{P} \xrightarrow{\alpha} \mathtt{P}'$ is derivable. Let $\rho = [\lambda\bar{n}.\alpha/A, \lambda\bar{n}.\mathtt{P}'/P']$. Applying ρ to the derivation of sequent (a), we get

$$\vdash \cdot\,;\, \mathcal{X}, \bar{n} \triangleright \mathtt{P} \xrightarrow{\alpha} \mathtt{P}' \vdash \bar{n} \triangleright \exists Q'.\mathtt{Q} \xrightarrow{\alpha} Q' \ \wedge\ \mathit{lbisim}\ \mathtt{P}'\ Q'.$$

By a cut between $\bar{n} \triangleright \mathtt{P} \xrightarrow{\alpha} \mathtt{P}'$ and this sequent, we obtain a derivation of

$$\cdot\,;\, \mathcal{X} \vdash \bar{n} \triangleright \exists Q'.\mathtt{Q} \xrightarrow{\alpha} Q' \ \wedge\ \mathit{lbisim}\ \mathtt{P}'\ Q'.$$

By Lemma 36, we know that there exists a derivation of this sequent which ends with a right-rule, hence, there exists a process $\mathtt{Q}'$ such that $\vdash \cdot\,;\, \mathcal{X} \vdash \bar{n} \triangleright \mathtt{Q} \xrightarrow{\alpha} \mathtt{Q}'$ and $\vdash \cdot\,;\, \mathcal{X} \vdash \bar{n} \triangleright \mathit{lbisim}\ \mathtt{P}'\ \mathtt{Q}'$. It is easy to show that $\mathcal{X}$ plays no part in the proof of the first sequent, so it can be removed from the sequent. Hence by the adequacy of one-step transitions, we have $\mathtt{Q} \xrightarrow{\alpha} \mathtt{Q}'$. Provability of the second sequent implies that $(\mathtt{P}', \mathtt{Q}')$ is in the set $\mathcal{S}$. Thus $\mathcal{S}$ is indeed closed under the α-transition.

(2) Suppose that $\mathtt{P} \xrightarrow{a(y)} \mathtt{P}'$. Applying a similar argument as in the previous case to sequent (b) with substitution $\rho = [\lambda\bar{n}.a/X, \lambda\bar{n}\lambda y.\mathtt{P}'/M]$, we obtain a provable sequent

$$\cdot\,;\, \mathcal{X} \vdash \bar{n} \triangleright \exists N.\mathtt{Q} \xrightarrow{\downarrow a} N \ \wedge\ \forall y.\mathit{lbisim}\ \mathtt{P}'\ (N y).$$

Again, as in the previous case, using Lemma 36, we can show that $\mathtt{Q} \xrightarrow{a(y)} \mathtt{Q}'$ for some process $\mathtt{Q}'$ such that $\vdash \cdot\,;\, \mathcal{X} \vdash \bar{n} \triangleright \forall y.\mathit{lbisim}\ \mathtt{P}'\ \mathtt{Q}'$. This implies that

$$\begin{array}{rl} (i) & \mathcal{X} \supset \nabla\bar{n}\forall y.\mathit{lbisim}\ \mathtt{P}'\ \mathtt{Q}', \\ (ii) & \mathcal{X} \supset \nabla\bar{n}.\mathit{lbisim}\ (\mathtt{P}'[w/y])\ (\mathtt{Q}'[w/y]), \text{ where } w \in \{\bar{n}\}, \\ (iii) & (\nabla y.\mathcal{X}) \supset \nabla y \nabla\bar{n}.\mathit{lbisim}\ \mathtt{P}'\ \mathtt{Q}' \end{array}$$

are all provable. The formula (ii) is obtained from (i) by instantiating y with one of $\bar{n}$. The formula (iii) is obtained from (i) as follows: Since

$$\nabla x \forall y.P\,x\,y \supset \forall y \nabla x.P\,x\,y \quad \text{and} \quad (A \supset \forall y.B) \supset (\forall y.(A \supset B)),$$

where y is not free in A, are theorems of $FO\lambda^{\Delta\nabla}$, we can enlarge the scope of y in (i) to the outermost level: hence, we have that $\forall y(\mathcal{X} \supset \nabla\bar{n}.\mathit{lbisim}\ \mathtt{P}'\ \mathtt{Q}')$ is provable. Now apply Proposition 3 to turn $\forall y$ into ∇y, then distribute the ∇y over the implication $\supset$ and conjunction $\wedge$, and we have (iii).

It remains to show that for every name w, the pair $(\mathtt{P}'[w/y], \mathtt{Q}'[w/y])$ is in $\mathcal{S}$. There are two cases to consider: The case where w is among $\bar{n}$ follows straightforwardly from (ii), the other case, where w is a new name, follows from (iii).

(3) Suppose $\mathtt{P} \xrightarrow{\bar{a}(y)} \mathtt{P}'$. Using the same argument as in the previous case, we can show that there exists a process $\mathtt{Q}'$ such that $\mathtt{Q} \xrightarrow{\bar{a}(y)} \mathtt{Q}'$ and such that

$$\vdash \cdot\,;\, \mathcal{X} \vdash \bar{n} \triangleright \nabla y.\mathit{lbisim}\ \mathtt{P}'\ \mathtt{Q}'.$$

The latter entails that $(\mathtt{P}', \mathtt{Q}') \in \mathcal{S}$, as required. □

B.3 Completeness

We are given $\mathtt{P} \sim_l \mathtt{Q}$ and we need to show that $\vdash \mathcal{X} \supset \nabla\bar{n}.\mathit{lbisim}\ \mathtt{P}\ \mathtt{Q}$, where $\mathcal{X} \subseteq_f \mathcal{E}$ and $\bar{n} = \{n_1, \dots, n_k\}$ includes all the free names in $\mathtt{P}$ and $\mathtt{Q}$. From Lemma 39 we have that

$$\vdash \forall n_1 \cdots \forall n_k (\mathcal{X}' \wedge n_1 \neq \cdots \neq n_k \supset \mathit{lbisim}\ \mathtt{P}\ \mathtt{Q})$$

for some $\mathcal{X}' \subseteq_f \mathcal{E}$. By Proposition 3, we can turn all the $\forall$ into ∇, hence

$$\vdash \nabla n_1 \cdots \nabla n_k (\mathcal{X}' \wedge n_1 \neq \cdots \neq n_k \supset \mathit{lbisim}\ \mathtt{P}\ \mathtt{Q}).$$

Since ∇ distributes over all propositional connectives, we have

$$\vdash (\nabla\bar{n}.\mathcal{X}') \wedge \nabla\bar{n}.(n_1 \neq \cdots \neq n_k) \supset \nabla\bar{n}.\mathit{lbisim}\ \mathtt{P}\ \mathtt{Q}.$$

Now, $\nabla\bar{n}.n_1 \neq \cdots \neq n_k$ is a theorem of $FO\lambda^{\Delta\nabla}$ (since any two distinct ∇-quantified names are not equal), therefore by modus ponens we have

$$\vdash \nabla\bar{n}.\mathcal{X}' \supset \nabla\bar{n}.\mathit{lbisim}\ \mathtt{P}\ \mathtt{Q}.$$

Let $\mathcal{X} = \nabla\bar{n}.\mathcal{X}'$, then we have $\mathcal{X} \supset \nabla\bar{n}.\mathit{lbisim}$ `P` `Q` as required. □

B.4 Adequacy of the specification of early bisimulation

The proof for the adequacy of the specification of early bisimulation follows a similar outline as that of late bisimulation. The proof is rather tedious and is not enlightening. We therefore omit the proof here.

B.5 Adequacy of the specification of open bisimulation

Proof of Lemma 18: The proof proceeds by induction on the length of the quantifier prefix $\mathcal{Q}\bar{x}$. At each stage of the induction, we construct a quantifier prefix $\mathcal{Q}\bar{y}$ such that $\mathcal{Q}\bar{x}.P \supset \mathcal{Q}\bar{y}.P\theta$ and $D\theta$ corresponds to the $\mathcal{Q}\bar{y}$-distinction. In the base case, where the quantifier prefix $\mathcal{Q}\bar{x}$ is empty, the quantifier $\mathcal{Q}\bar{y}$ is also the empty prefix. In this case we have $P\theta = P$, therefore $P \supset P\theta$ holds trivially. There are the following two inductive cases.
(1) Suppose $\mathcal{Q}\bar{x}.P = \mathcal{Q}'\bar{u}\nabla z.P$. Let D' be the distinction that corresponds to $\mathcal{Q}'\bar{u}$. Note that by definition, we have $D = D' \cup \{(z,v),(x,v) \mid v \in D'\}$. Let θ' be the substitution θ with domain restricted to $\{\bar{u}\}$. Since θ respects D, obviously θ' respects D' and $\theta(z) \neq \theta(v)$ for all $v \in D'$. By induction hypothesis, we have a proof of the formula $\mathcal{Q}\bar{u}(\nabla z.P) \supset \mathcal{Q}\bar{m}(\nabla z.P)\theta'$ for some quantifier prefix $\mathcal{Q}\bar{m}$ such that $D'\theta'$ is the $\mathcal{Q}\bar{m}$-distinction. Note that since z is not in the domain of θ', we have $(\nabla z.P)\theta' = \nabla z.(P\theta')$. Let $w = \theta(z)$. Since w is distinct from all other free names in $D'\theta'$, we can rename z with w, thus,

$$\vdash \mathcal{Q}\bar{u}\nabla z.P \supset \mathcal{Q}\bar{m}\nabla w.P(\theta' \circ [w/z])$$

But $\theta' \circ [w/z]$ is exactly θ. Let $\mathcal{Q}\bar{y}$ be the prefix $\mathcal{Q}\bar{m}\nabla w$. It then follows that

$$\vdash \mathcal{Q}\bar{x}.P \supset \mathcal{Q}\bar{y}.P\theta.$$

Moreover, $D\theta$ can be easily shown to be the $\mathcal{Q}\bar{y}$-distinction.
(2) Suppose $\mathcal{Q}\bar{x} = \mathcal{Q}'\bar{u}\forall z.P$. Note that in this case, the $\mathcal{Q}\bar{x}$-distinction and $\mathcal{Q}'\bar{u}$-distinction co-incide, *i.e.*, both are the same distinction D. Moreover, $z \notin \mathrm{fv}(D)$. Let θ' be the substitution θ restricted to the domain $\{\bar{u}\}$. By induction hypothesis, we have that $\vdash \mathcal{Q}\bar{u}(\forall z.P) \supset \mathcal{Q}\bar{m}(\forall z.P)\theta'$, for some quantifier prefix $\mathcal{Q}\bar{m}$ such that $\mathcal{Q}\bar{m}$ corresponds to $D\theta'$. Note that $D\theta' = D\theta$, because $z \notin \mathrm{fv}(D)$. There are two cases to consider when constructing $\mathcal{Q}\bar{y}$. The first case is when z is identified, by θ, with some name in $\{\bar{u}\}$. In this case, by the property of universal quantification, we have that $\vdash \mathcal{Q}\bar{u}\forall z.P \supset \mathcal{Q}\bar{m}.P\theta$. In this case, we let $\mathcal{Q}\bar{y} = \mathcal{Q}\bar{m}$. Note that $D\theta'$ is the same as $D\theta$ in this case. Therefore $D\theta$ is the $\mathcal{Q}\bar{y}$-distinction. For the second case, we have that z is instantiated by θ to a new name, say w. Then following the same argument as the case with ∇, we have that $\vdash \mathcal{Q}\bar{u}\forall z.P \supset \mathcal{Q}\bar{m}\forall w.P\theta$. In this case, we let $\mathcal{Q}\bar{y} = \mathcal{Q}\bar{m}\forall w$. Note that in this case the $\mathcal{Q}\bar{y}$-distinction also coincides with $\mathcal{Q}\bar{m}$-distinction, *i.e.*, both are the same set $D\theta$. □

In the proof of soundness of open bisimulation to follow, we make use of a property of the structure of proofs of certain sequents. The following three lemmas state some meta-level properties of $FO\lambda^{\Delta\nabla}$. Their proofs are easy and are omited.

LEMMA 41. *Suppose the sequent $\Sigma\,;\Delta \longrightarrow \mathcal{C}$ is provable, where C is an existential judgment and Δ is a set of inequality between distinct terms,* i.e.*, every element of*

Δ is of the form $\bar{n} \triangleright s \neq t$, for some $\bar{n}$, s and t. Then there exists a proof of the sequent ending with $\exists\mathcal{R}$ applied to C.

LEMMA 42. *For any positive formula context $C[]$, $\vdash C[\forall x.B] \supset C[B[t/x]]$.*

LEMMA 43. *Let $\mathcal{Q}\bar{x}$ be a quantifier prefix. If $\mathcal{Q}\bar{x}.P$ and $\mathcal{Q}\bar{x}.P \supset Q$ are provable then $\mathcal{Q}\bar{x}.Q$ is provable.*

LEMMA 44. *Let D be a conjunction of inequalities between terms. If $\vdash \mathcal{Q}\bar{x}.D \supset \nabla y.P$, where y is not free in D, then $\vdash \mathcal{Q}\bar{x}\nabla y.D \supset P$.*

The following lemma is a simple corollary of Proposition 8 and Proposition 4.

LEMMA 45. $\mathtt{P} \xrightarrow{\alpha} \mathtt{Q}$ *if and only if* $\mathcal{Q}\bar{n}.[\![\mathtt{P} \xrightarrow{\alpha} \mathtt{Q}]\!]$ *is provable, where $\mathcal{Q}\bar{n}$ is a quantifier prefix and $\bar{n}$ are the free names of* $\mathtt{P}$.

To prove soundness of open bisimulation specification, we define a family of sets $\mathcal{S}$ in the following, and show that it is indeed an open bisimulation.

$$\mathcal{S}_D = \{(\mathtt{P},\mathtt{Q}) \mid \vdash \mathcal{Q}\bar{n}.[D'] \supset \mathit{lbisim}\ \mathtt{P}\ \mathtt{Q} \text{ and } \mathrm{fn}(\mathtt{P},\mathtt{Q},D') = \{\bar{n}\} \text{ and } D = D' \cup D'', \text{ where } D'' \text{ is the } \mathcal{Q}\bar{n}\text{-distinction. } \}$$

Suppose $(\mathtt{P},\mathtt{Q}) \in \mathcal{S}_D$. That is, $\vdash \mathcal{Q}\bar{n}.[D'] \supset \mathit{lbisim}\ \mathtt{P}\ \mathtt{Q}$. Let D'' be the distinction that corresponds to the prefix $\mathcal{Q}\bar{n}$. We have to show that for every name substitution θ which respects D, the set $\mathcal{S}$ is closed under conditions 1, 2, and 3 in Definition 14. Since θ respects D, it also respects D'' (since D'' is a subset of D). Therefore, it follows from Lemma 18 that there exists a prefix $\mathcal{Q}\bar{x}$ such that $D''\theta$ is the $\mathcal{Q}\bar{x}$-distinction, and $\vdash \mathcal{Q}\bar{x}.[D'\theta] \supset \mathit{lbisim}\ (\mathtt{P}\theta)\ (\mathtt{Q}\theta)$. By the invertibility of $\mathit{def}\mathcal{R}$ on lbisim and the right-introduction rules for $\forall$, ∇, $\supset$ and $\wedge$, we can infer that provability of the above formula implies provability of six other formulas, three of which are given in the following (the other three are symmetric variants of these formulas):

$$(a)\ \ \mathcal{Q}\bar{x}.[D'\theta] \supset \forall P'\forall A.\mathtt{P}\theta \xrightarrow{A} P' \supset \exists Q'.\mathtt{Q}\theta \xrightarrow{A} Q' \wedge \mathit{lbisim}\ P'\ Q'$$
$$(b)\ \ \mathcal{Q}\bar{x}.[D'\theta] \supset \forall M\forall X.\mathtt{P}\theta \xrightarrow{\downarrow X} M \supset \exists N.\mathtt{Q}\theta \xrightarrow{\downarrow X} N \wedge \forall w.\mathit{lbisim}\ (Mw)\ (Nw)$$
$$(c)\ \ \mathcal{Q}\bar{x}.[D'\theta] \supset \forall M\forall X.\mathtt{P}\theta \xrightarrow{\uparrow X} M \supset \exists N.\mathtt{Q}\theta \xrightarrow{\uparrow X} N \wedge \nabla w.\mathit{lbisim}\ (Mw)\ (Nw)$$

Using provability of these formulas, we show that $\mathcal{S}$ is closed under free actions, bound input actions and bound output actions.

—Suppose $\mathtt{P}\theta \xrightarrow{\alpha} \mathtt{R}$ where α is a free action. By Lemma 45, we have that

$$\vdash \mathcal{Q}\bar{x}.\mathtt{P}\theta \xrightarrow{\alpha} \mathtt{R}. \tag{4}$$

From formula (a) and Lemma 42, we have that

$$\vdash \mathcal{Q}\bar{x}.[D'\theta] \supset \mathtt{P}\theta \xrightarrow{\alpha} \mathtt{R} \supset \exists Q'.\mathtt{Q}\theta \xrightarrow{\alpha} Q' \wedge \mathit{lbisim}\ \mathtt{R}\ Q'. \tag{5}$$

Applying Lemma 43 to formula (4) and (5) above, we have that

$$\vdash \mathcal{Q}\bar{x}.[D'\theta] \supset \exists Q'.\mathtt{Q}\theta \xrightarrow{\alpha} Q' \wedge \mathit{lbisim}\ \mathtt{R}\ Q'.$$

The latter implies, by the invertibility of the right rules for ∇ and $\forall$, provability of the sequent

$$\Sigma\,;\ D_1 \Vdash \bar{m} \triangleright \exists Q'.\mathtt{Q}' \xrightarrow{\alpha'} Q' \wedge \mathit{lbisim}\ \mathtt{R}'\ Q'$$

where Σ are the eigenvariables corresponding to the universally quantified variables in $\mathcal{Q}\bar{x}$ (with appropriate raising) and $\bar{m}$ corresponds to the ∇-quantified variables in the same prefix. The terms $\mathtt{Q}'$, $\mathtt{R}'$, D_1 and α' are obtained from, respectively, $\mathtt{Q}\theta$, $\mathtt{R}$, $[D'\theta]$ and α by replacing their free names with their raised counterparts. Note that since θ respects D', the inequality in D_1 are those that relate distinct terms, hence, by Lemma 41, provability of the above sequent implies the existence of a term T such that $\vdash \Sigma\,;\ D_1 \Vdash \bar{m} \triangleright \mathtt{Q}' \xrightarrow{\alpha'} T'$ and

$$\vdash \Sigma\,;\ D_1 \Vdash \bar{m} \triangleright \mathit{lbisim}\ \mathtt{R}'\ T'. \tag{6}$$

It can be shown by induction on the height of derivations that D_1 in the first sequent can be removed, hence we have that

$$\vdash \Sigma\,;\ .\ \Vdash \bar{m} \triangleright \mathtt{Q}' \xrightarrow{\alpha'} T'.$$

Applying the appropriate introduction rules to this sequent (top down), we "unraise" the variables in Σ and obtain $\vdash \mathcal{Q}\bar{x}.\mathtt{Q}\theta \xrightarrow{\alpha} \mathtt{T}$, where $\mathtt{T}$ corresponds to T'. By Lemma 45, this means that $\mathtt{Q}\theta \xrightarrow{\alpha} \mathtt{T}$. It remains to show that $(\mathtt{R}, \mathtt{Q}) \in \mathcal{S}$. This is obtained from the sequent (6) above as follows. We apply the introduction rules for quantifiers and implication (top down) to sequent (6), hence unraising the variables in Σ and obtain the provable formula $\mathcal{Q}\bar{x}.[D'\theta] \supset \mathit{lbisim}\ \mathtt{R}\ \mathtt{T}$, from which it follows that $(\mathtt{R}, \mathtt{T}) \in \mathcal{S}_{D\theta}$.

—Suppose $\mathtt{P}\theta \xrightarrow{a(y)} \mathtt{R}$. As in the previous case, using Lemma 45, Lemma 42, Lemma 43 and formula (b) we can show that

$$\vdash \mathcal{Q}\bar{x}.[D'\theta] \supset \exists Q'.\mathtt{Q}\theta \xrightarrow{\downarrow a} N \wedge \forall w.\mathit{lbisim}\ (\mathtt{R}[w/y])\ (N\,y).$$

From this formula, we can show that there exists $\mathtt{T}$ such that $\mathcal{Q}\bar{x}.\mathtt{Q}\theta \xrightarrow{\downarrow a} \lambda z.\mathtt{T}$, therefore $\mathtt{Q}\theta \xrightarrow{a(z)} \mathtt{T}$, and that

$$\vdash \mathcal{Q}\bar{x}.[D'\theta] \supset \forall w.\mathit{lbisim}\ (\mathtt{R}[w/y])\ (\mathtt{T}[w/z]). \tag{7}$$

We need to show that for a fresh name w, $(\mathtt{R}[w/y], \mathtt{T}[w/z]) \in \mathcal{S}_{D\theta}$. From provability of formula (7), and the fact that $(A \supset \forall x.B) \supset \forall x(A \supset B)$, we obtain

$$\vdash \mathcal{Q}\bar{x}\forall w.[D'\theta] \supset \mathit{lbisim}\ (\mathtt{R}[w/y])\ (\mathtt{T}[w/z]).$$

Since the $\mathcal{Q}\bar{x}\forall w$-distinction is the same as $\mathcal{Q}\bar{x}$-distinction, the overal distinction encoded in the above formula is $D\theta$, therefore, by definition of $\mathcal{S}$, we have $(\mathtt{R}[w/y], \mathtt{T}[w/z]) \in \mathcal{S}_{D\theta}$.

—Suppose $\mathtt{P}\theta \xrightarrow{\bar{a}(y)} \mathtt{R}$. This case is similar to the bound input case. Applying the same arguments shows that there exists a process $\mathtt{T}$ such that $\mathtt{Q}\theta \xrightarrow{a(z)} \mathtt{T}$ and

$$\vdash \mathcal{Q}\bar{x}.[D'\theta] \supset \nabla w.\mathit{lbisim}\ (\mathtt{R}[w/y])\ (\mathtt{T}[w/z]). \tag{8}$$

We have to show that, for a fresh w, $(\mathtt{R}[w/y], \mathtt{T}[w/z]) \in \mathcal{S}_{D_2}$ where $D_2 = D\theta \cup \{w\} \times \mathrm{fn}(D\theta, \mathtt{P}\theta, \mathtt{Q}\theta)$. Note that the free names of $D\theta$, $\mathtt{P}\theta$ and $\mathtt{Q}\theta$ are all in $\bar{x}$ by definition. From formula (8) and Lemma 44, we have that

$$\vdash \mathcal{Q}\bar{x}\nabla w.[D'\theta] \supset \mathit{lbisim}\ (\mathtt{R}[w/y])\ (\mathtt{T}[w/z]).$$

Notice that the $\mathcal{Q}\bar{x}\nabla w$-distinction is $D''\theta \cup \{w\} \times \{\bar{x}\}$, and since $\bar{x}$ is the free names of $D\theta$, $\mathtt{P}\theta$ and $\mathtt{Q}\theta$, the overall distinction encoded by the above formula is exactly D_2, hence $(\mathtt{R}[w/y], \mathtt{T}[w/z]) \in \mathcal{S}_{D_2}$ as required. □

The proof of Theorem 21 is analogous to the completeness proof for Theorem 15. Suppose $\mathtt{P}$ and $\mathtt{Q}$ are open D-bisimilar. We construct a derivation of the formula

$$\forall n_1 \cdots \forall n_k([D] \supset \mathit{lbisim}\ \mathtt{P}\ \mathtt{Q}) \tag{9}$$

by induction on the number of action prefixes in $\mathtt{P}$ and $\mathtt{Q}$. By applying the introduction rules for $\forall$, $\supset$ and unfolding the definition of *lbisim* (bottom up) to the formula (9), we get the following sequents:

(1) $n_1, \cdots, n_k, A, P' ; [D], \mathtt{P} \xrightarrow{A} P' \vdash \exists Q'.\mathtt{Q} \xrightarrow{A} Q' \wedge \mathit{lbisim}\ P'\ Q'$

(2) $n_1, \cdots, n_k, X, P' ; [D], \mathtt{P} \xrightarrow{\downarrow X} P' \vdash \exists Q'.\mathtt{Q} \xrightarrow{\downarrow X} Q' \wedge \forall w.\mathit{lbisim}\ (P'w)\ (Q'w)$

(3) $n_1, \cdots, n_k, X, P' ; [D], \mathtt{P} \xrightarrow{\uparrow X} P' \vdash \exists Q'.\mathtt{Q} \xrightarrow{\uparrow X} Q' \wedge \nabla w.\mathit{lbisim}\ (P'w)\ (Q'w)$

and their symmetric counterparts. We show here how to construct proofs for these three sequents; the rest can be proved similarly. In all these three cases, we apply either the one_f rule (for sequent 1) or the one_b rule (for sequent 2 and 3). If this application of one_f (or one_b) results in two distinct name-variables, say n_1 and n_2, in D to be identified, then the sequent is proved by using the assumption $n_1 \neq n_2$ in D. Therefore the only interesting cases are when the instantiations of name-variables $n_1, \cdots, n_k$ respect the distinction D. In the following we assume the names $n_1, \ldots, n_k$ are instantiated to $m_1, \ldots, m_l$ and the distinction D is respected. Note that l may be smaller than k, depending on D, *i.e.*, it may allow some names to be identified.

Sequent 1. In this case, after applying the one_f rule bottom up and discharging the trivial premises (*i.e.*, those that violates the distinction D), we need to prove, for each θ associated with the rule, the sequent

$$m_1, \cdots, m_l, \Sigma ; [D\theta] \vdash \exists Q'.\mathtt{Q}\theta \xrightarrow{A\theta} Q' \wedge \mathit{lbisim}\ (P'\theta)\ Q' \tag{10}$$

for some signature Σ. By Lemma 34, we know that $m_1, \cdots, m_l, \Sigma ; . \vdash \mathtt{P}\theta \xrightarrow{A\theta} P'\theta$ is provable. Since $m_1, \ldots, m_l$ are the only free names in $\mathtt{P}\theta$, we can show by induction on proofs that Σ in the sequent is redundant and can be removed, thus the sequent $m_1, \cdots, m_l ; . \vdash \mathtt{P}\theta \xrightarrow{A\theta} P'\theta$ is also provable. By the adequacy of one-step transition (Proposition 8) and Proposition 4, we have $\mathtt{P}\theta \xrightarrow{\alpha} \mathtt{R}$ for some free action α and $\mathtt{R}$ where $\alpha = A\theta$ and $P'\theta = \mathtt{R}$. Let θ' be θ with domain restricted to $\{n_1, \ldots, n_k\}$. Obviously, θ' respects D and $D\theta' = D\theta$. Since $\mathtt{P}$ and $\mathtt{Q}$ are open D-bisimilar, we have that there exists $\mathtt{T}$ such that $\mathtt{Q}\theta \xrightarrow{\alpha} \mathtt{T}$ and $\mathtt{R} \sim_o^{D\theta'} \mathtt{T}$, hence by induction hypothesis, we have that

$$\vdash \forall m_1 \cdots \forall m_l.[D\theta] \supset \mathit{lbisim}\ P'\theta\ \mathtt{T}. \qquad (11)$$

Provability of sequent (10) follows from these facts, by instantiating Q' with $\mathtt{T}$.

Sequent 2.. In this case, we need to prove the sequent

$$m_1, \cdots, m_l, \Sigma\,;\ [D\theta] \vdash \exists Q'.\mathtt{Q}\theta \xrightarrow{\downarrow X\theta} Q' \wedge \forall w.\mathit{lbisim}\ ((P'\theta)w)\ (Q'w) \qquad (12)$$

for each non-trivial θ in the premises of one_b rule. By the same reasoning as in the previous case, we obtain, for every transition $\mathtt{P}\theta \xrightarrow{x(w)} \mathtt{R}$, where $\mathtt{R} = (P'\theta)\,w$, another transition $\mathtt{Q}\theta \xrightarrow{x(w)} \mathtt{T}$ such that (we assume w.l.o.g. that w is fresh) $\mathtt{R} \sim_o^{D\theta} \mathtt{T}$. The former implies that $\mathtt{Q}\theta \xrightarrow{\downarrow x} \lambda w.\mathtt{T}$ is derivable, and the latter implies, by induction hypothesis, that

$$\forall m_1 \cdots \forall m_l \forall w.[D\theta] \supset \mathit{lbisim}\ \mathtt{R}\ \mathtt{T}$$

is derivable. As in the previous case, from these two facts, we can prove the sequent (12) by instantiating Q' with $\lambda w.\mathtt{T}$.

Sequent 3. In this case, we need to prove the sequent

$$m_1, \cdots, m_l, \Sigma\,;\ [D\theta] \vdash \exists Q'.\mathtt{Q}\theta \xrightarrow{A\theta} Q' \wedge \nabla w.\mathit{lbisim}\ ((P'\theta)w)\ (Q'w) \qquad (13)$$

for each non-trivial θ in the premises of one_b rule. As in the previous case, we obtain $\mathtt{R}$ and $\mathtt{T}$ such that $\mathtt{P}\theta \xrightarrow{\bar{x}(w)} \mathtt{R}$ and $\mathtt{Q}\theta \xrightarrow{\bar{x}(w)} \mathtt{T}$ where $\lambda w.\mathtt{R} = P'\theta$. We assume, without loss of generality, that w is fresh, therefore since $\mathtt{P} \sim_o^D \mathtt{Q}$, by definition we have that $\mathtt{R} \sim_o^{D'} \mathtt{T}$, where $D' = D\theta \cup \{x\} \times \mathrm{fn}(D\theta, \mathtt{P}\theta, \mathtt{Q}\theta)$. Note that the free names of $D\theta$, $\mathtt{P}\theta$ and $\mathtt{Q}\theta$ are exactly $m_1, \dots, m_l$, so $D' = D\theta \cup \{x\} \times \{m_1, \dots m_l\}$. Thus by induction hypothesis, the formula

$$\forall m_1 \cdots \forall m_l \forall w.[D'] \supset \mathit{lbisim}\ \mathtt{R}\ \mathtt{T}.$$

Now apply Proposition 3 to replace $\forall w$ with ∇w,

$$\forall m_1 \cdots \forall m_k \nabla w.[D'] \supset \mathit{lbisim}\ \mathtt{R}\ \mathtt{T}.$$

And since ∇ distributes over all propositional connectives, we also have

$$\forall m_1 \cdots \forall m_k.(\nabla w.[D']) \supset \nabla w.\mathit{lbisim}\ \mathtt{R}\ \mathtt{T}.$$

It can be shown that $m_1, \dots, m_l\,;\ .\ \vdash \nabla w.[D'] \supset [D\theta]$ is provable, since the inequalities between w and $m_1, \dots, m_k$ trivially true. Therefore we have that

$$\vdash \forall m_1 \cdots \forall m_k.[D\theta] \supset \nabla w.\mathit{lbisim}\ \mathtt{R}\ \mathtt{T}. \qquad (14)$$

Now in order to prove sequent (13), we instantiate Q' with $\lambda w.\mathtt{T}$, and the rest of the proof proceeds as in the previous case, *i.e.*, with the help of formula (14). □

B.6 "Early" open bisimulation

The proof of Theorem 23 is by induction on the number of input prefixes in $\mathtt{P}$ and $\mathtt{Q}$. We prove a more general result: $\vdash \mathcal{Q}\bar{n}.\mathit{lbisim}\ \mathtt{P}\ \mathtt{Q}$ if and only if $\vdash \mathcal{Q}\bar{n}.\mathit{ebisim}\ \mathtt{P}\ \mathtt{Q}$, for any quantifier prefix $\mathcal{Q}\bar{n}$. By Lemma 37 and Lemma 38, and the invertibility of

$\nabla\mathcal{R}$ and $\forall\mathcal{R}$ rules, we know that if $\vdash \mathcal{Q}\bar{n}.lbisim\ \mathtt{P}\ \mathtt{Q}$ and $\vdash \mathcal{Q}\bar{n}.ebisim\ \mathtt{P}\ \mathtt{Q}$, then their unfolded instances are also provable. We show that one can construct a derivation for one instance from the other. The non-trivial case is when the bound input transition is involved. That is, given a derivation of

$$\mathcal{Q}\bar{n}.[\forall X \forall P'.\mathtt{P} \xrightarrow{\downarrow X} P' \supset \forall w \exists Q'.\mathtt{Q} \xrightarrow{\downarrow X} Q' \wedge ebisim\ (P'w)\ Q'w)]$$

we can construct a derivation of

$$\mathcal{Q}\bar{n}.[\forall X \forall P'.\mathtt{P} \xrightarrow{\downarrow X} P' \supset \exists Q'.\mathtt{Q} \xrightarrow{\downarrow X} Q' \wedge \forall w.ebisim\ (P'w)\ (Q'w)]$$

and vice versa. Note that we cannot do any analysis on the universally quantified name w in both formulas, since we do not have any assumptions on names (*e.g.*, the excluded middle on names as in the adequacy theorem for late bisimulation). It is then easy to check that the choice of Q' in both cases is independent of the name w, and their correspondence follows straightforwardly from the induction hypothesis. □

C. ADEQUACY OF THE SPECIFICATIONS OF MODAL LOGICS

The completeness proof of the modal logics specification shares similar structures with the completeness proofs for specifications of bisimulation. In particular, we use an analog of Lemma 39, given in the following.

LEMMA 46. *Let* $\mathtt{P}$ *be a process and* $\mathtt{A}$ *an assertion such that* $\mathtt{P} \models \mathtt{A}$. *Then*

$$\vdash \forall n_1 \cdots \forall n_k.\mathcal{X} \wedge n_1 \neq \cdots \neq n_k \supset [\![\mathtt{P} \models \mathtt{A}]\!]$$

for some $\mathcal{X} \subseteq_f \mathcal{E}$ *and some names* $n_1, \ldots, n_k$ *such that* $\mathrm{fn}(\mathtt{P}, \mathtt{A}) \subseteq \{n_1, \ldots, n_k\}$.

The proof of lemma proceeds by induction on the size of $\mathtt{A}$. The crucial step is when its interpretation in $FO\lambda^{\Delta\nabla}$ contains universal quantification over names, *e.g.*, when $\mathtt{A} = [a(y)]\mathtt{B}$. In this case, we again use the same technique as in the proof of Lemma 39, *i.e.*, using the excluded middle assumptions on names to enumerate all possible instances of the judgments.

Proof of Theorem 25 (Adequacy of the modal logic encoding)

First consider proving the soundness part of this theorem. Suppose we have a derivation Π of $\cdot\,;\,\mathcal{X} \vdash \nabla\bar{n}.[\![\mathtt{P} \models \mathtt{A}]\!]$. We want to show that $\mathtt{P} \models \mathtt{A}$. This is proved by induction on the size of $\mathtt{A}$. The proof also uses the property of invertible rules and the fact that applications of the excluded middles in $\mathcal{X}$ in deriving the sequent can be permuted up over all the right introduction rules. The latter is a consequence of Lemma 36. We look at a couple of interesting cases involving bound input and bound output.

out:. Suppose $\mathtt{A}$ is $[\bar{x}(y)]\mathtt{B}$. We need to show that for every $\mathtt{P}'$ such that $\mathtt{P} \xrightarrow{\bar{x}(y)} \mathtt{P}'$, we have $\mathtt{P}' \models \mathtt{B}$. (By α-conversion we can assume without loss of generality that y is not free in $\mathtt{P}$ and $\mathtt{A}$.) Note that here the occurrence of y in $\mathtt{P}'$ is bound in the transition judgment $\mathtt{P} \xrightarrow{\bar{x}(y)} \mathtt{P}'$. By Lemma 36 and the invertibility of certain inference rules, we can show that provability of $\cdot\,;\, \mathcal{X} \vdash \nabla \bar{n}.[\![\mathtt{P} \models \mathtt{A}]\!]$ implies the existence of a derivation Π' of

$$M\,;\, \mathcal{X}, \bar{n} \triangleright [\![\mathtt{P}]\!] \xrightarrow{\uparrow x} M\bar{n} \vdash \bar{n} \triangleright \nabla y.M\bar{n}y \models [\![\mathtt{B}]\!]$$

for some eigenvariable M. By the adequacy of one-step transitions, we have that $\vdash \nabla \bar{n}.[\![\mathtt{P}]\!] \xrightarrow{\uparrow x} \lambda y.[\![\mathtt{P}']\!]$. Let θ be the substitution $[(\lambda \bar{n} \lambda y.[\![\mathtt{P}']\!])/M]$. Applying θ to Π' we get the derivation $\Pi'\theta$ of $\cdot\,;\, \bar{n} \triangleright [\![\mathtt{P}]\!] \xrightarrow{\uparrow x} \lambda y.[\![\mathtt{P}']\!] \vdash \bar{n} \triangleright \nabla y.\mathtt{P}' \models [\![\mathtt{B}]\!]$. By cutting this derivation with the one-step transition judgment above, we obtain a derivation of $\cdot\,;\, . \vdash \bar{n} \triangleright \nabla y.\mathtt{P}' \models [\![\mathtt{B}]\!]$. Hence by induction hypothesis, we have that $\mathtt{P}' \models \mathtt{B}$.

in:. Suppose $\mathtt{A}$ is $[x(y)]^L\mathtt{B}$. We show that there exists a process $\mathtt{P}'$ such that $\mathtt{P} \xrightarrow{x(y)} \mathtt{P}'$ and for all name w, $\mathtt{P}'[w/y] \models \mathtt{B}[w/y]$. It is enough to consider the case where w is a name in $\mathrm{fn}(\mathtt{P}, \mathtt{A})$ and the case where w is a new name not in $\mathrm{fn}(\mathtt{P}, \mathtt{A})$. By Lemma 36 and the invertibility of some inference rules, we can show that provability of $\cdot\,;\, \mathcal{X} \vdash \bar{n} \triangleright [\![\mathtt{P}]\!] \models [\![[x(y)]^L\mathtt{B}]\!]$ implies the existence of two derivations Π_1 and Π_2, of the sequents $\cdot\,;\, \mathcal{X} \vdash \bar{n} \triangleright \mathtt{P} \xrightarrow{\downarrow x} N$ and $\cdot\,;\, \mathcal{X} \vdash \bar{n} \triangleright \forall y.Ny \models [\![\mathtt{B}]\!]$, respectively, for some closed term N.

By the adequacy result in Proposition 8, there exists a process $\mathtt{P}'$ such that $[\![\mathtt{P}']\!] = Ny$ and $\mathtt{P} \xrightarrow{x(y)} \mathtt{P}'$. By Proposition 5, we can instantiate y with any of the free names occurring in $\mathtt{P}$ or $\mathtt{A}$ (since they are all in the list $\bar{n}$), and hence for any name $w \in \mathrm{fn}(\mathtt{P}, \mathtt{A})$ by induction hypothesis we get $\mathtt{P}'[w/y] \models \mathtt{B}[w/z]$. The case where w is a new name is dealt with as follows. Without loss of generality we assume that $y = w$ (since we can always choose y to be sufficiently fresh). From Π_2 it follows that $\vdash \mathcal{X} \supset \nabla \bar{n}.\forall y.[\![\mathtt{P}']\!] \models [\![\mathtt{B}]\!]$. Using the $FO\lambda^{\Delta\nabla}$ theorems

$$(\nabla x \forall y.P) \supset \forall y \nabla x.P \quad \text{and} \quad (P \supset \forall z.Q) \supset \forall z(P \supset Q)$$

where z is not free in P, we can move the $\forall y$ quantification in $\mathcal{X} \supset \nabla \bar{n}.\forall y.[\![\mathtt{P}']\!] \models [\![\mathtt{B}]\!]$ to the outermost level and get the provable formula $\forall y(\mathcal{X} \supset \nabla \bar{n}.[\![\mathtt{P}']\!] \models [\![\mathtt{B}]\!])$. We then apply Proposition 3, to turn $\forall y$ into ∇y, thus obtaining a derivation of $\nabla y(\mathcal{X} \supset \nabla \bar{n}.[\![\mathtt{P}']\!] \models [\![\mathtt{B}]\!])$, and by distributing ∇ over $\supset$, we get $(\nabla y.\mathcal{X}) \supset \nabla y \nabla \bar{n}.[\![\mathtt{P}']\!] \models [\![\mathtt{B}]\!]$. We can now apply the induction hypothesis to get $\mathtt{P}' \models \mathtt{B}$.

Next we consider proving the completeness part of Theorem 25. Given $\mathtt{P} \models \mathtt{A}$, we would like to show that $\cdot\,;\, \mathcal{X} \vdash \nabla \bar{n}.[\![\mathtt{P} \models \mathtt{A}]\!]$ is provable. By Lemma 46, there are $m_1, \dots, m_k$ and $\mathcal{X}'$ such that

$$\vdash \forall m_1 \cdots \forall m_k.\mathcal{X}' \wedge m_1 \neq m_2 \cdots \neq m_k \supset [\![\mathtt{P} \models \mathtt{A}]\!].$$

Let $\bar{n} = m_1, \dots, m_k$ and let $\mathcal{X} = \nabla \bar{n}.\mathcal{X}'$. By Proposition 3, we have a derivation of

$$\nabla m_1 \cdots \nabla m_k.\mathcal{X}' \wedge m_1 \neq m_2 \cdots \neq m_k \supset [\![\mathtt{P} \models \mathtt{A}]\!].$$

By distributing the ∇'s over implication and conjunction we obtain

$$\mathcal{X} \wedge (\nabla \bar{n}.m_1 \neq m_2 \cdots \neq m_k) \supset \nabla \bar{n}.[\![\mathtt{P} \models \mathtt{A}]\!].$$

But since $\nabla \bar{n}.m_1 \neq m_2 \cdots \neq m_k$ is provable, by cut we obtain a derivation of

$$;\, \mathcal{X} \vdash \nabla \bar{n}.[\![\mathtt{P} \models \mathtt{A}]\!]. \qquad \square$$

D. CHARACTERISATION OF OPEN BISIMULATION

LEMMA 47. *Let* P *and* Q *be two processes. If for all* $\mathtt{A} \in \mathcal{LM}$, $\vdash (\mathcal{Q}\bar{n}.\mathtt{P} \models \mathtt{A})$ *if and only if* $\vdash (\mathcal{Q}\bar{n}.\mathtt{Q} \models \mathtt{A})$, *where* $\mathrm{fn}(\mathtt{P},\mathtt{Q},\mathtt{A}) \subseteq \{\bar{n}\}$, *then* $\mathtt{P} \sim_o^D \mathtt{Q}$, *where* D *is the* $\mathcal{Q}\bar{n}$*-distinction.*

PROOF. Let $\mathcal{S}$ be the following family of relations

$$\mathcal{S}_D = \{(\mathtt{P},\mathtt{Q}) \mid \text{for all } \mathtt{A}, \vdash (\mathcal{Q}\bar{n}.\mathtt{P} \models \mathtt{A}) \text{ iff } \vdash (\mathcal{Q}\bar{n}.\mathtt{Q} \models \mathtt{A}), \text{ where } \mathrm{fn}(\mathtt{P},\mathtt{Q},\mathtt{A}) \subseteq \{\bar{n}\} \text{ and } D \text{ is the } \mathcal{Q}\bar{n}\text{-distinction}\}$$

We then show that $\mathcal{S}$ is an open bisimulation. $\mathcal{S}$ is obviously symmetric, so it remains to show that it is closed under one-step transitions. We show here a case involving bound output; the rest are treated analogously.

Suppose $(\mathtt{P},\mathtt{Q}) \in \mathcal{S}_D$. Then we have that for all $\mathtt{A}$, $\vdash \mathcal{Q}\bar{n}.\mathtt{P} \models \mathtt{A}$ iff $\vdash \mathcal{Q}\bar{n}.\mathtt{Q} \models \mathtt{A}$, for some prefix $\mathcal{Q}\bar{n}$. Let θ be a substitution that respects D. Suppose $\mathtt{P}\theta \xrightarrow{\bar{x}(y)} \mathtt{P}'$. We need to show that there exists a $\mathtt{Q}'$ such that $\mathtt{Q}\theta \xrightarrow{\bar{x}(y)} \mathtt{Q}'$ and $\mathtt{P}' \sim_o^{D'} \mathtt{Q}'$ where $D' = D\theta \cup \{y\} \times \mathrm{fn}(\mathtt{P},\mathtt{Q},D)$. (Here we assume w.l.o.g. that y is chosen to be sufficiently fresh.) Suppose θ identifies the following pairs of names in P and Q: $(x_1,y_1),\ldots,(x_k,y_k)$, and suppose that $\theta(z) = x$. Then by the definition of $\mathcal{S}_D$:

$$\vdash \mathcal{Q}\bar{n}.\mathtt{P} \models [x_1 = y_2][x_2 = y_2]\cdots[x_k = y_k]\langle\bar{z}(y)\rangle\mathtt{B}$$

if and only if for all B,

$$\vdash \mathcal{Q}\bar{n}.\mathtt{Q} \models [x_1 = y_2][x_2 = y_2]\cdots[x_k = y_k]\langle\bar{z}(y)\rangle\mathtt{B}.$$

Note that the statement cannot hold vacuously, since for at least one instance of B, *i.e.*, B = true, both judgments must be true. By analysis on the (supposed) cut-free proofs of both judgments, for any B, the above statement reduces to

$$\vdash \mathcal{Q}\bar{m}.\mathtt{P}\theta \models \langle\bar{x}(y)\rangle\mathtt{B}\theta \qquad \text{iff} \qquad \vdash \mathcal{Q}\bar{m}.\mathtt{Q}\theta \models \langle\bar{x}(y)\rangle\mathtt{B}\theta,$$

for some prefix $\mathcal{Q}\bar{m}$ such that $\mathcal{Q}\bar{m}$-distinction is the result of applying θ to the $\mathcal{Q}\bar{n}$-distinction.

Now let $\{\mathtt{Q}_i\}_{i\in I}$ be the set of all $\mathtt{Q}'$ such that $\mathtt{Q}\theta \xrightarrow{\bar{x}(y)} \mathtt{Q}'$, and suppose that for all $i \in I$, $\mathtt{P}' \not\sim_o^{D'} \mathtt{Q}_i$. That means that there exists an $\mathtt{A}_i$, for each $i \in I$, that separates $\mathtt{P}'$ and $\mathtt{Q}_i$, *i.e.*, $\vdash (\mathcal{Q}\bar{m}\nabla y.\mathtt{P}' \models \mathtt{A}_i)$ but $\not\vdash (\mathcal{Q}\bar{m}\nabla y.\mathtt{Q}' \models \mathtt{A}_i)$. Note that we can assume w.l.o.g. that $\bar{m}$ include all the free names of $\mathtt{A}_i$ (recall that $\bar{n}$ is really a schematic list of names, dependent on the choice of A in the first place). Let $\mathtt{B}\theta$ be $\bigwedge_{i\in I}\mathtt{A}_i$. Then, by analysis of cut-free proofs, we can show that $\vdash (\mathcal{Q}\bar{m}.\mathtt{P}\theta \models \langle\bar{x}(y)\rangle\mathtt{B}\theta)$ but $\not\vdash (\mathcal{Q}\bar{m}.\mathtt{Q} \models \langle\bar{x}(y)\rangle\mathtt{B}\theta)$, which contradicts our initial assumption. Therefore, there must be one $\mathtt{Q}'$ such that $\mathtt{Q} \xrightarrow{\bar{x}(y)} \mathtt{Q}'$ and $\mathtt{P}' \sim_o^{D'} \mathtt{Q}'$. □

LEMMA 48. *Let* P *and* Q *be two processes such that* $\mathtt{P} \sim_o^D \mathtt{Q}$ *for some distinction* D. *Then for all* $\mathtt{A} \in \mathcal{LM}$ *and for all prefix* $\mathcal{Q}\bar{n}$ *such that* D *corresponds to the* $\mathcal{Q}\bar{n}$*-distinction and* $\mathrm{fn}(\mathtt{P},\mathtt{Q},D) \subseteq \{\bar{n}\}$, $\vdash \mathcal{Q}\bar{n}.\mathtt{P} \models \mathtt{A}$ *if and only if* $\vdash \mathcal{Q}\bar{n}.\mathtt{Q} \models \mathtt{A}$.

PROOF. Suppose that $\mathtt{P} \sim_o^D \mathtt{Q}$ and $\vdash \mathcal{Q}\bar{n}.\mathtt{P} \models \mathtt{A}$. We show, by induction on the size of A, that $\vdash \mathcal{Q}\bar{n}.\mathtt{Q} \models \mathtt{A}$. The other direction is proved symmetrically, since open bisimulation is symmetric. We look at the interesting cases.

—Suppose $\mathtt{A} = \langle \bar{x}(y) \rangle \mathtt{B}$ for some $\mathtt{B}$. By analysis on the cut free derivations of $\mathcal{Q}\bar{n}.\mathtt{P} \models \mathtt{A}$, it can be shown that

$$\vdash \mathcal{Q}\bar{n}.\exists M.\mathtt{P} \xrightarrow{\uparrow x} M \wedge \nabla y.(M\, y) \models \mathtt{B}.$$

This entails that there exists a process $\mathtt{P}'$ such that

$$\vdash \mathcal{Q}\bar{n}.\mathtt{P} \xrightarrow{\uparrow x} \lambda y.\mathtt{P}' \wedge \nabla y.\mathtt{P}' \models \mathtt{B}.$$

And by the invertibility of the right-introduction rules for $\forall$, ∇ and $\wedge$, this in turn entails that $\vdash \mathcal{Q}\bar{n}.\mathtt{P} \xrightarrow{\uparrow x} \lambda y.\mathtt{P}'$ and $\vdash \mathcal{Q}\bar{n}\nabla y.\mathtt{P}' \models \mathtt{B}$. The former implies, by the adequacy of one-step transition, that $\mathtt{P} \xrightarrow{\bar{x}(y)} \mathtt{P}'$. Since $\mathtt{P} \sim_o^D \mathtt{Q}$, this means that there exists $\mathtt{Q}'$ such that $\mathtt{Q} \xrightarrow{\bar{x}(y)} \mathtt{Q}'$ and $\mathtt{P}' \sim_o^{D'} \mathtt{Q}'$, where $D' = D \cup \{y\} \times \mathrm{fn}(\mathtt{P}, \mathtt{Q}, D)$. At this point we are almost ready to apply the induction hypothesis to $\mathcal{Q}\bar{n}\nabla y.\mathtt{P}' \models \mathtt{B}$, except that D' may not corresponds to the $\mathcal{Q}\bar{n}\nabla y$-distinction, since the latter may contain more inequal pairs than D'. However, since open bisimulation is closed under extensions of distinctions (see Lemma 6.3. in [Sangiorgi 1996]), we can assume without loss of generality that D' is indeed the $\mathcal{Q}\bar{n}\nabla y$-distinction. Therefore by the adequacy of one-step transition and induction hypothesis, we conclude that $\vdash \mathcal{Q}\bar{n}.\mathtt{Q} \xrightarrow{\uparrow x} \lambda x.\mathtt{Q}'$ and $\vdash \mathcal{Q}\bar{n}\nabla y.\mathtt{Q}' \models \mathtt{B}$, and from these, it follows that $\mathcal{Q}\bar{n}.\mathtt{P} \models \mathtt{A}$ is also provable.

—Suppose $\mathtt{A} = \langle x(y) \rangle \mathtt{B}$. This case is analogous to the previous case. The only difference is that the bound input is universally quantified, instead of ∇-quantified. So we apply the induction hypothesis to $\mathcal{Q}\bar{n}\forall y.\mathtt{P}' \models \mathtt{B}$, which can be done without resorting to extensions of the distinction D, since in this case the $\mathcal{Q}\bar{n}\forall y$-distinction is exactly D.

—For the cases where $\mathtt{A}$ is prefixed by either $[x(y)]^L$ or $[\bar{x}(y)]$, the proof follows a similar argument as in the completeness proof of open bisimulation (Theorem 21). For instance, for the case where $\mathtt{A} = [x(y)]^L\mathtt{B}$, from the fact that $\vdash \mathcal{Q}\bar{n}.\mathtt{P} \models \mathtt{A}$, it follows that

$$\vdash \mathcal{Q}\bar{n}.\forall M(\mathtt{P} \xrightarrow{\downarrow x} M \supset \exists y.(M\, y) \models \mathtt{B}).$$

As in the proof of Theorem 21, we can further show that there is a derivation of this formula that ends with one_b-rule, such that every θ in this premise is a D-respecting substitution. Since $\mathtt{P} \sim_o^D \mathtt{Q}$, we can show that every bound input action of $\mathtt{P}\theta$, for any D-respecting θ, can be imitated by $\mathtt{Q}\theta$ and vice versa. From this and induction hypothesis, we can therefore obtain a derivation of

$$\mathcal{Q}\bar{n}.\forall N(\mathtt{Q} \xrightarrow{\downarrow x} N \supset \exists y.(N\, y) \models \mathtt{B}),$$

hence $\vdash \mathcal{Q}\bar{n}.\mathtt{Q} \models \mathtt{A}$. □

Finally, the proof of Theorem 26 now follows immediately from Lemma 47 and Lemma 48. □