Modal Logics for Mobile Processes Revisited

Tiange Liu
School of Computing, The Australian National University, Canberra, Ngunnawal Country, Australia

Alwen Tiu
School of Computing, The Australian National University, Canberra, Ngunnawal Country, Australia

Jim de Groot
School of Computing, The Australian National University, Canberra, Ngunnawal Country, Australia

Abstract

We revisit the logical characterisations of various bisimilarity relations for the finite fragment of the π-calculus. Our starting point is the early and the late bisimilarity, first defined in the seminal work of Milner, Parrow and Walker, who also proved their characterisations in fragments of a modal logic (which we refer to as the MPW logic). Two important refinements of early and late bisimilarity, called open and quasi-open bisimilarity, respectively, were subsequently proposed by Sangiorgi and Walker. Horne, et. al., showed that open and quasi-bisimilarity are characterised by intuitionistic modal logics: OM (for open bisimilarity) and FM (for quasi-open bisimilarity). In this work, we attempt to unify the logical characterisations of these bisimilarity relations, showing that they can be characterised by different sublogics of a unifying logic. A key insight to this unification derives from a reformulation of the four bisimilarity relations (early, late, open and quasi-open) that uses an explicit name context, and an observation that these relations can be distinguished by the relative scoping of names and their instantiations in the name context. This name context and name substitution then give rise to an accessibility relation in the underlying Kripke semantics of our logic, that is captured logically by an S4-like modal operator. We then show that the MPW, the OM and the FM logics can be embedded into fragments of our unifying classical modal logic. In the case of OM and FM, the embedding uses the fact that intuitionistic implication can be encoded in modal logic $S4$.

2012 ACM Subject Classification Theory of computation → Process calculi; Theory of computation → Modal and temporal logics

Keywords and phrases pi-calculus, modal logic, intuitionistic logic, bisimilarity

Digital Object Identifier 10.4230/LIPIcs.CONCUR.2023.34

Acknowledgements We thank Ross Horne for various insightful discussions on the subtlety of the mismatch operator, and the anonymous reviewers for their careful reading of the paper and their helpful feedback on an earlier version of this paper.

1 Introduction

The π-calculus [14] is a process calculus originally developed by Milner, Parrow and Walker, aimed at modelling a notion of process mobility (called link mobility). It can be seen as an extension of the Calculus of Communicating Systems (CCS) [13], that allows the creation of channel names, and exchanges of names between processes. Unlike CCS, where there is a canonical notion of (strong/weak) bisimilarity defining process equivalence, there are several notions of (strong/weak) bisimilarity for the π-calculus that arise from different ways in which name quantification is scoped in the bisimulation game. We consider four important notions of bisimilarity in this work: the early and the late bisimilarity, that were first defined in [14], the open bisimilarity [20] and the quasi-open bisimilarity [22]. The latter two are chosen for our study for two reasons: they are full congruence relations (closed under all process constructs, something which is not true for early/late bisimilarity), and they are more amenable for automation, especially open bisimilarity. Quasi-open bisimilarity implies early bisimilarity and is implied by open bisimilarity, but is incomparable to late bisimilarity.

34th International Conference on Concurrency Theory (CONCUR 2023).
Editors: Guillermo A. Pérez and Jean-François Raskin; Article No. 34; pp. 34:1–34:17
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Our main interest is in the problem of characterising bisimilarity using (modal) logic. For a modal logic to characterise a notion of bisimilarity, bisimilar processes should satisfy precisely the same formulas (soundness), and conversely two processes satisfying the same formulas should be bisimilar (completeness). This type of results was pioneered by Hennessy and Milner, who characterised bisimilarity for CCS using a classical normal multi-modal logic [9]. Modal logics characterising early and late bisimilarity for the π-calculus were developed by Milner, Parrow and Walker [15]. The authors of that work show that early and late bisimilarity are characterised by the modal logic $\mathbb{EM}$ and $\mathbb{LM}$, respectively. Both $\mathbb{EM}$ and $\mathbb{LM}$ are sublogics of a classical modal logic, which we refer to here as MPW logic. Such a logical characterisation for open and quasi-open bisimilarity remained open until recently. In 2017, a characterisation of open bisimilarity was given using an intuitionistic modal logic $\mathbb{OM}$ [4, 5]. The intuitionistic nature of their logic, as opposed to MPW classical modal logic, was motivated by the fact that closure under certain name substitutions acts like intuitionistic persistence. Not long after, quasi-open bisimilarity was characterised using yet another intuitionistic modal logic called $\mathbb{FM}$ [10].

Early and late bisimilarity are distinguished in one important case involving an input transition. In a bisimulation game between a process P and another process Q, if P makes an input transition, e.g., $P \xrightarrow{a(x)} P'(x)$, then the move that Q plays can depend, or not depend, on the choice of the name x. In early bisimulation, the choice that Q makes is dependent on x, whereas in late bisimulation, it is independent of x. In open bisimulation, which refines late bisimulation, the choice of x is further delayed indefinitely – technically this is formalised by allowing input names to be *instantiated* at any point in the bisimulation game. In quasi-open bisimulation, the choice that Q makes is dependent on the name x, just like in early bisimulation. However, like open bisimulation, input names can be further instantiated at any point in the bisimulation game. Both open and quasi-open bisimulation impose a restriction on name substitutions, permitting only substitutions that do not identify certain pairs of names (typically those arising from names generated from bound-output transitions); they differ only in the extent on how certain names must remain *distinct* throughout the bisimulation game. The open nature of name instantiations is essentially what gives both open and quasi-open bisimiliarty their intuitionistic character: in the bisimulation game, equality between two (input) names cannot generally be decided, i.e. the classical tautology $(x = y) \vee (x \neq y)$ does not necessarily hold at every point in the bisimulation game [5, 10].

While the difference between early and late bisimilarity is reflected in MPW logic by the use of two modalities that capture precisely the difference in the scope of the name quantification arising from input transitions, the same cannot be said about $\mathbb{OM}$ and $\mathbb{FM}$, at least in their current formulations in [5, 10]. An obvious reason is that $\mathbb{OM}$ and $\mathbb{FM}$ are entirely separate logics, so not sublogics of a unifying logic like MPW logic. Another is a more fundamental one: the notions of *name distinctions* used in open and quasi-open bisimilarity are quite different, at least superficially, with open bisimulation adopting a more relax notion (that allows more names to be identified). This fundamental difference gives rise to seemingly incompatible logics and it is not obvious how they can be viewed as sublogics of a unifying logic. In this work, we show that these differences can be reconciled if the *context* in which these names are instantiated is taken into account. A (name) context here refers to information about how a name is created (as part of an input or a bound output), and the relative order in which names are created in a trace of a process. We refer to such a context as a *history*. By reformulating all four bisimilarity relations by explicitly accounting for histories of names, we are able to obtain a unifying (classical) modal logic, whose sublogics characterise all four bisimilarity relations. This reconciliation needs to account for the difference between intuitionistic and classical modal logics. We achieve this by viewing name substitutions as giving rise to an accessibility relation in a Kripke model, with a corresponding modal operator $\Box$ that behaves like a modal operator in the modal logic S4 (i.e., normal modal logics with reflexive and transitive frames). We can then encode intuitionistic implication (or negation) using this modal operator and classical implication. In particular, the notion of inequality $x \neq y$ in the intuitionistic logic $\mathbb{FM}$ becomes the modal formula $\Box\neg(x = y)$ in our logic. One notable consequence of our unifying logic, in the context of quasi-open bisimilarity, is that we obtain a much simpler construction of the distinguishing formulas for processes that are not quasi-bisimilar, in comparison to [10].

Our contributions can be summarised as follows:

- We give a uniform reformulation of four bisimilarity relations (early, late, open and quasi-open) using explicit name contexts.
- We give a unifying logic, whose sublogics characterise all four bisimilarity relations mentioned above.
- We provide a new construction of distinguishing formulae for quasi-open bisimilarity, simplifying a similar construction in [10], by making essential use of classical negation.

Outline of the paper. We set the stage in Section 2, where we recall the π-calculus, its late operational semantics with respect to a history, and the definitions of late, early, open and quasi-open bisimilarity. In Section 3 we introduce the logic that lies at the heart of this paper, together with its semantics. We showcase the distinguishing power by examples, and we state the main theorem of the paper, giving four fragments of the logic each of which characterises a notion of bisimilarity. Section 4 is devoted to proving the completeness part of the main theorem. Our results currently are established for the finite π-calculus with the match operator, but without the mismatch operator. In Section 5 discuss some key ideas on how to extend our results to handle the mismatch operator, leaving the details to future work. In Section 6 we discuss related work and we conclude in Section 7. Some detailed proofs are omitted but will be made available in a forthcoming technical report.

2 π-calculus and four notions of bisimulations

We give a brief overview of the operational semantics of the finite fragment of the π-calculus [14], and reformulate four notions of bisimulation: early [14], late [14], open [20] and quasi-open [22] bisimulation.

We assume a countably infinite set of *channel names* $\mathcal{N}$, elements of which are ranged over by lower-case letters such as x, y and z. Each name x has its dual *co-names*, denoted by $\bar{x}$. Informally, a name represents a communication channel where input can be received, and a co-name represents a channel where output can be sent. Processes can synchronise along channels with complementary names, i.e., a process inputting on channel x can synchronise with another process outputting on channel $\bar{x}$.

▶ **Definition 1.** Processes are defined by the grammar

$$P ::= 0 \mid \tau.P \mid \bar{x}y.P \mid x(z).P \mid \nu x.P \mid (P \mid P) \mid P + P \mid [x = y]P.$$

A process of the form $\bar{x}y.P$ is an output-prefixed process, representing a process capable of outputting a free name y along channel x. We adopt here a syntactic sugar of the form $\bar{x}(z).P$ as an abbreviation of $\nu x.\bar{x}z.P$. Semantically, this represents a process capable of outputting a bound name z along channel x. A process of the form $x(z)$ is an input-prefixed process, with z acting as a placeholder for the received name. The prefix τ is a silent prefix, meaning that the transition can act without interaction with the environment, and $\nu x.P$ turns x into a bound name in P. The processes $P \mid Q$, $P+Q$ and $[x=y]P$ represent parallel processes, choice, and match, respectively.

▶ **Definition 2.** We recall some basic definitions.

- A name z in a prefix π is *binding* if π is of the form $\bar{x}(z)$ or $x(z)$. We write $\mathrm{bn}(\pi)$ for the binding names and $\mathrm{fn}(\pi)$ for all other names in π.
- An occurrence of a name z in a process P is *bound* if it lies in the scope of a prefix of the form $\bar{x}(z)$, $x(z)$, or of νz. Occurrences of names that are not bound are called *free*. We write $\mathrm{bn}(P)$ and $\mathrm{fn}(P)$ for the sets of bound and free names of a process, and we abbreviate $\mathrm{fn}(P,Q) = \mathrm{fn}(P) \cup \mathrm{fn}(Q)$.
- A *substitution* σ is a map that sends names to names such that the *support* $\mathsf{supp}(\sigma) := \{x \mid \sigma(x) \neq x\}$ of σ is finite. We sometimes write $\{{}^{z_1,\ldots,z_n}/_{x_1,\ldots,x_n}\}$ for the substitution σ with $\mathsf{supp}(\sigma) = \{x_1,\ldots,x_n\}$ and $x_i\sigma = z_i$ for all $i \in \{1,\ldots,n\}$. The application of a substitution to a variable x, prefix π or process P is defined as expected and denoted by $x\sigma$, $\pi\sigma$ and $P\sigma$. The composition $\sigma \cdot \theta$ of two substitutions is defined by $(\sigma \cdot \theta)(x) = \theta(\sigma(x))$.

2.1 History and operational semantics

Before defining our operational semantics of the π-calculus, we introduce the notion of a history and a respectful substitution, adapting the same notion from [20].

▶ **Definition 3** (Histories)**.** A history h is a list of names annotated with either i (denoting an input name) or o (denoting an output name). If x is any name then we write $x \in h$ if x^i or x^o appears in h, and if X is a set of names then we write $X \subseteq h$ if $x \in h$ for all $x \in X$.

When enumerating the list of annotated names in a history, we separate each name in the list with dots, e.g., $x^i \cdot y^o \cdot z^i$.

Intuitively, a history h represents the list of names that a process sends and receives during its transitions. The o-annotated names (denoted by z^o) correspond to output names extruded by a process in its bound output transitions. The names marked as input (denoted by z^i) represent symbolic inputs (i.e., variables) received by a process. The difference between these annotations is captured in the following definition of *respectful substitutions*.

▶ **Definition 4** (Respectful substitutions)**.** A substitution σ *respects* h if, for all h', h'' and x such that $h = h' \cdot x^o \cdot h''$, we have $x\sigma = x$ and $y\sigma \neq x$ for all $y \in h'$. If $h = x_1^{p_1} \cdots x_n^{p_n}$ is a history, where $p_1, \ldots, p_n \in \{i, o\}$, then we let $h\sigma := (x_1\sigma)^{p_1} \cdots (x_n\sigma)^{p_n}$ be the application of a respectful substitution σ to h.

▶ **Example 5.** Let $h = a^i \cdot b^o \cdot c^o \cdot x^i \cdot y^i$. Then $\sigma_1 = \{b/x, y/a\}$ is a substitution that respects h, and applying σ_1 to h results in $h\sigma_1 = a^i \cdot b^o \cdot c^o \cdot b^i \cdot a^i$. (Notice that we allow names to be repeated in a history). On the other hand, $\sigma_2 = \{a/b\}$ is not an h-respectful substitution, as it violates the condition that o-annotated names cannot be substituted, i.e., that $b\sigma_1 = b$ fails to hold. The substitution $\sigma_3 = \{c/a\}$ also does not respect h, as it substitutes an i-annotated name a with an o-annotated name that appears later in the history.

As the above example illustrates, the o-annotated names act like constants, while i-annotated names act like scoped variables, with their scoping determined by their relative positions in the history. Intuitively, when we consider a history as a trace of names inputted and outputted by a process, this scoping enforces the fact that a name received earlier in the

$$\frac{}{h : \pi.P \xrightarrow{\pi} P}\ (\textsc{Act}) \qquad \frac{h \cdot z^o : P \xrightarrow{\pi} Q \quad z \notin h \cup \mathrm{bn}(\pi) \cup \mathrm{fn}(\pi)}{h : \nu z.P \xrightarrow{\pi} \nu z.Q}\ (\textsc{Res})$$

$$\frac{h \cdot z^o : P \xrightarrow{\bar{x}z} Q \quad z \notin \{x\} \cup h}{h : \nu z.P \xrightarrow{\bar{x}(z)} Q}\ (\textsc{Open}) \qquad \frac{h : P \xrightarrow{\bar{x}(z)} P' \quad h : Q \xrightarrow{x(z)} Q'}{h : P|Q \xrightarrow{\tau} \nu z.(P'|Q')}\ (\textsc{Close})$$

$$\frac{h : P \xrightarrow{\pi} R}{h : P + Q \xrightarrow{\pi} R}\ (\textsc{Sum}) \qquad \frac{h : P \xrightarrow{\pi} Q \quad \mathrm{bn}(\pi) \cap \mathrm{fn}(R) = \emptyset}{h : P|R \xrightarrow{\pi} Q|R}\ (\textsc{Par})$$

$$\frac{h : P \xrightarrow{\pi} R}{h : [x = y]P \xrightarrow{\pi} R}\ (\textsc{Match}) \qquad \frac{h : P \xrightarrow{\bar{x}y} P' \quad h : Q \xrightarrow{x(z)} Q'}{h : P|Q \xrightarrow{\tau} P'|Q'\{{}^{y}/{}_{z}\}}\ (\textsc{L-Com})$$

Figure 1 The late transition semantics of the π-calculus with histories. Their symmetric variants are omitted. We require that $\mathrm{fn}(P) \subseteq h$ whenever $h : P \xrightarrow{\pi} Q$.

trace cannot be identified with a fresh name outputted later. The meaning of the annotations of names in a history and respectful substitutions will become clearer later when we define various notions of bisimilarity (Section 2.2).

We next define two orderings that will be useful later in the definitions of bisimulation. These orderings intend to constrain the possible identification of names in a history as a result of applying a respectful substitution.

▶ **Definition 6** (Orderings on histories). *We write $h \subseteq_o h'$ if h' can be obtained from h by adding o-annotated names to the end. Similarly, we write $h \subseteq_i h'$ if h' can be obtained from h by adding i-annotated names in front of h.*

The ordering $h \subseteq_i h'$ is intended to capture the fact that the new i-annotated names in h' cannot be identified with any o-annotated names in h (but may be identified with i-annotated names) after applying an h'-respectful substitution. This fact will be important later when defining quasi-open bisimulation. In the ordering $h \subseteq_o h'$ the new o-annotated names cannot be identified with any names appearing in h. This will be used later in the definition of early- and late-bisimulation.

The operational semantics of the π-calculus is given in Figure 1. Note that we use the *late variant* of the semantics [14], where bound input is not instantiated directly in the transition relation; its instantiation is defined in the definitions of bisimulation (see Section 2.2). Our semantics differs slightly from the standard late transition semantics, as each transition is indexed by a history. The history is strictly speaking not needed for the semantics in Figure 1. However, it will be important later when we discuss the handling of the mismatch operator (see Section 5). Note that in the Open and Res, the ν-binder in the process expression is interpreted as an o-annotated name in the history, reflecting the fact that this name is not affected by respectful substitutions.

We now state several lemmas for future reference.

▶ **Lemma 7.** *Let h be a history and suppose σ, θ are substitutions such that σ respects h. Then θ respects $h\sigma$ if and only if $\sigma \cdot \theta$ respects h.*

▶ **Lemma 8.** *Suppose $h : P \xrightarrow{\pi} Q$. If π is of the form τ or $\bar{x}y$ then $\mathrm{fn}(Q) \subseteq \mathrm{fn}(P)$. If π is of the form $x(z)$ or $\bar{x}(z)$ then $\mathrm{fn}(Q) \subseteq \mathrm{fn}(P) \cup \{z\}$.*

The following lemma helps prove that (quasi-)open bisimulations are closed under respectful substitutions. In a given transition $h : P \xrightarrow{\pi} Q$, without loss of generality, we may assume that $\mathrm{bn}(\pi)$ are chosen to be sufficiently fresh.

▶ **Lemma 9** (monotonicity). *Suppose $h : P \xrightarrow{\pi} Q$. Then $h\sigma : P\sigma \xrightarrow{\pi\sigma} Q\sigma$ for all σ that respect h and satisfy for all $x \in \mathrm{bn}(\pi)$, $y\sigma = x$ iff $x = y$.*

2.2 Four notions of bisimilarity

We augment early, late, open and quasi-open bisimilarity with histories. In each case, we first define a notion of bisimulation as a collection of relations indexed by the collection of histories. We write $\mathcal{H}$ for the collection of all histories, $\mathcal{H}^o$ for those consisting entirely of o-annotated names, and we similarly define $\mathcal{H}^i$. We let $\mathcal{H}^{i\text{-}o}$ denote the collection of histories in which every i-annotated name comes before all o-annotated names.

▶ **Definition 10** (Early bisimilarity). An *early bisimulation* is a family of symmetric relation $\{\mathcal{B}_e^h \mid h \in \mathcal{H}^o\}$ such that whenever $P\mathcal{B}_e^h Q$ we have:

- If $h : P \xrightarrow{\alpha} P'$ then $\exists Q'$ s.t. $h : Q \xrightarrow{\alpha} Q'$ and $P'\mathcal{B}_e^h Q'$, where α is of the form τ or $\bar{x}y$.
- If $h : P \xrightarrow{\bar{x}(z)} P'$ and z is fresh then $\exists Q'$ s.t. $h : Q \xrightarrow{\bar{x}(z)} Q'$ and $P'\mathcal{B}_e^{h\cdot z^o} Q'$.
- If $h : P \xrightarrow{x(z)} P'$ and z is fresh then for all $h' \supseteq_o h$ and $y \in h'$ there exists some Q' such that $h : Q \xrightarrow{x(z)} Q'$ and $P'\{y/z\}\mathcal{B}_e^{h'} Q'\{y/z\}$.

We write $\{\sim_e^h \mid h \in \mathcal{H}\}$ for the pointwise union of all early bisimulations and refer to $\sim_e^h$ as *early h-bisimilarity.* Two processes P and Q are called *early bisimilar* if they are early h-bisimilar for some $h \in \mathcal{H}^o$.

The third clause allows us to substitute z for any name y, including a name that does not appear in h (hence the need for the extension $h' \supseteq_o h$). The fact that we use only o-annotated histories in early (and late) bisimulation reflects the fact that names in these bisimulations cannot be instantiated, i.e., they are essentially constants. The definition of late bisimulation is similarly adapted from its original definition as follows.

▶ **Definition 11** (Late bisimilarity). A *late bisimulation* is a family $\{\mathcal{B}_\ell^h \mid h \in \mathcal{H}^o\}$ of symmetric relations indexed by a history consisting only of o-annotated names such that whenever $P\mathcal{B}_\ell^h Q$, we have:

- If $h : P \xrightarrow{\alpha} P'$ then $\exists Q'$ s.t. $h : Q \xrightarrow{\alpha} Q'$ and $P'\mathcal{B}_\ell^h Q'$, where α is of the form τ or $\bar{x}y$;
- If $h : P \xrightarrow{\bar{x}(z)} P'$ and z is fresh then $\exists Q'$ s.t. $h : Q \xrightarrow{\bar{x}(z)} Q'$ and $P'\mathcal{B}_\ell^{h\cdot z^o} Q'$;
- If $h : P \xrightarrow{x(z)} P'$ and z is fresh then $\exists Q'$ s.t. $h : Q \xrightarrow{x(z)} Q'$ and for all $y \in h'$ with $h' \supseteq_o h$ we have $P'\{y/z\}\mathcal{B}_\ell^{h'} Q'\{y/z\}$.

We write $\{\sim_\ell^h \mid h \in \mathcal{H}\}$ for the pointwise union of all late bisimulations and refer to $\sim_\ell^h$ as *late h-bisimilarity.* Two processes P and Q are called *late bisimilar* if they are late h-bisimlar for some $h \in \mathcal{H}^o$.

The notions of a late and early bisimilarity were originally defined in [14] without reference to a history. The original definition can be obtained from the above ones simply by omitting reference to the history, and in the third items letting y be an arbitrary name. We refer to this as *MPW late/early bisimulation*, and to the induced notion of bisimilarity as *MPW late/early bisimilarity.* The next proposition explains the connection between late/early bisimulations and MPW late/early bisimulations.

▶ **Proposition 12.** *Two processes are MPW late (resp. early) bisimilar if and only if they are late (resp. early) bisimilar.*

We now define analogues of open and quasi-open bisimulations [20, 22].

▶ **Definition 13** (Open bisimilarity). An *open bisimulation* is a history-indexed collection $\{\mathcal{B}_o^h \mid h \in \mathcal{H}\}$ of symmetric relations on processes such that whenever $P\mathcal{B}_e^h Q$:

- For all substitutions σ respecting h, we have $P\sigma\mathcal{B}_o^{h\sigma}Q\sigma$.
- If $h : P \xrightarrow{\alpha} P'$ then $\exists Q'$ s.t. $h : Q \xrightarrow{\alpha} Q'$ and $P'\mathcal{B}_o^h Q'$, where α is of the form τ or $\bar{x}y$;
- If $h : P \xrightarrow{\bar{x}(z)} P'$ and z is fresh, then $\exists Q'$ s.t. $h : Q \xrightarrow{\bar{x}(z)} Q'$ and $P'\mathcal{B}_o^{h\cdot z^o}Q'$;
- If $h : P \xrightarrow{x(z)} P'$ and z is fresh, then $\exists Q'$ s.t. $h : Q \xrightarrow{x(z)} Q'$ and $P'\mathcal{B}_o^{h\cdot z^i}Q'$.

The pointwise union of all open bisimulations is denoted by $\{\sim_o^h \mid h \in \mathcal{H}\}$. We refer to $\sim_o^h$ as *open h-bisimilarity.* We write $P \sim_o^{h'} Q$ if there exists an open bisimulation $\{\mathcal{B}_o^h \mid h \in \mathcal{H}\}$ and a history h' with only i-annotated names such that $P\mathcal{B}_o^{h'}Q$ and $\mathrm{fn}(P, Q) \subseteq h'$. We call P and Q *open bisimilar.*

Augmenting open bisimulations to account for a history does not affect the resulting notion of bisimilarity compared to the original definition, as was shown in [26, Corollary 22].

Quasi-open bisimilarity was originally defined in [22] using the early transition semantics. We adapt the original definition into late transition semantics indexed by history.

▶ **Definition 14** (Quasi-open bisimilarity). A *quasi-open bisimulation* is a history-indexed family $\{\mathcal{B}_q^h \mid h \in \mathcal{H}^{i\text{-}o}\}$ of symmetric relations on processes such that whenever $P\mathcal{B}_q^h Q$:

- For all substitutions σ respecting h, we have $P\sigma\mathcal{B}_q^{h\sigma}Q\sigma$;
- If $h : P \xrightarrow{\alpha} P'$ then $\exists Q'$ s.t. $h : Q \xrightarrow{\alpha} Q'$ and $P'\mathcal{B}_q^h Q'$, where $\alpha = \tau, \bar{x}y$;
- If $h : P \xrightarrow{\bar{x}(z)} P'$ and z is fresh, then $\exists Q'$ s.t. $h : Q \xrightarrow{\bar{x}(z)} Q'$ and $P'\mathcal{B}_q^{h\cdot z^o}Q'$;
- If $h : P \xrightarrow{x(z)} P'$ and z is fresh, then for all $h' \supseteq_i h$ and all $y \in h'$, $\exists Q'$ s.t. $h : Q \xrightarrow{x(z)} Q'$ and $P'\{y/z\}\mathcal{B}_q^{h'}Q'\{y/z\}$.

We write $\{\sim_q^h \mid h \in \mathcal{H}\}$ for the pointwise union of all quasi-open bisimulations and refer to $\sim_q^h$ as *quasi-open h-bisimilarity.* Two processes P and Q are called *quasi-open bisimilar* if there exists a history h with only i-annotated names such that $P \sim_q^h Q$ and $\mathrm{fn}(P, Q) \subseteq h$.

The first three conditions of an open and quasi-open bisimulation coincide. The last condition captures a subtle but important difference between open and quasi-open bisimulations: in quasi-open bisimulation, a bound output name must remain distinct from *all* other names produced during the bisimulation game, whereas in open bisimulation, the same bound output name only needs to be kept distinct from existing names in the history and future output names. This difference is captured technically by restricting the class of histories in quasi-open bisimulation to those where input names are always added to the front of output names, thereby preventing respectful substitutions from ever identifying output names with other (input/output) names.

Our definition relates to the original one in [22] as follows:

▶ **Proposition 15.** *Two processes are quasi-open bisimilar if and only if they are quasi-open bisimilar in the sense of [22].*

We use an example from [22] that distinguishes open and quasi-open bisimilarity to illustrate how to use histories.

▶ **Example 16.** Consider the processes

$$P = \nu u\bar{x}u.(x(z) + x(z).\tau + x(z).[z = u]\tau) \qquad Q = \nu u\bar{x}u.(x(z) + x(z).\tau)$$

We claim that P and Q are quasi-open bisimilar but not open bisimilar under the history $h = x^i$. After taking the transitions $\xrightarrow{\bar{x}(u)}\xrightarrow{x(z)}$ through the definition of open bisimilarity, we end up with the history $x^i \cdot u^o \cdot z^i$, while quasi-open bisimilarity yields history $y^i \cdot x^i \cdot u^o$ (if $y \notin \{x, u\}$) or $x^i \cdot u^o$ (if $y \in \{x, u\}$).

$$
\begin{array}{lll}
P \models^{h} \texttt{tt} & P \models^{h} x = x & P \models^{h} \neg\varphi \quad \text{iff} \quad P \not\models^{h} \varphi. \\
P \models^{h} \varphi_1 \wedge \varphi_2 & \text{iff} & P \models^{h} \varphi_1 \text{ and } P \models^{h} \varphi_2 \\
P \models^{h} \Diamond\varphi & \text{iff} & \exists\sigma \text{ respecting } h, P\sigma \models^{h\sigma} \varphi\sigma \\
P \models^{h} \langle\alpha\rangle\varphi & \text{iff} & \exists Q \text{ s.t. } h : P \xrightarrow{\alpha} Q \text{ and } Q \models^{h} \varphi, \text{ where } \alpha = \tau, \bar{x}y \\
P \models^{h} \langle\bar{x}(z)\rangle\varphi & \text{iff} & \exists Q \text{ s.t. } h : P \xrightarrow{\bar{x}(z)} Q \text{ and } Q \models^{h\cdot z^{o}} \varphi \\
P \models^{h} \langle x(z)\rangle\varphi & \text{iff} & \exists Q \text{ s.t. } h : P \xrightarrow{x(z)} Q \text{ and } \exists y \in h'(h' \supseteq_o h), Q\{{}^{y}/_{z}\} \models^{h'} \varphi\{{}^{y}/_{z}\} \\
P \models^{h} \langle x(z)\rangle_{\ell}\varphi & \text{iff} & \exists Q \text{ s.t. } h : P \xrightarrow{x(z)} Q \text{ and } \forall y \in h'(h' \supseteq_o h), Q\{y/z\} \models^{h'} \varphi\{y/z\} \\
P \models^{h} \langle x(z)\rangle_{e}\varphi & \text{iff} & \forall y \in h'(h' \supseteq_o h), \exists Q \text{ s.t. } h : P \xrightarrow{x(z)} Q \text{ and } Q\{y/z\} \models^{h'} \varphi\{y/z\} \\
P \models^{h} \langle x(z)\rangle_{o}\varphi & \text{iff} & \exists Q, h : P \xrightarrow{x(z)} Q \text{ and } Q \models^{h\cdot z^{i}} \varphi \\
P \models^{h} \langle x(z)\rangle_{q}\varphi & \text{iff} & \forall y \in h'(h' \supseteq_i h), \exists Q \text{ s.t. } h : P \xrightarrow{x(z)} Q \text{ and } Q\{y/z\} \models^{h'} \varphi\{y/z\}
\end{array}
$$

Figure 2 The semantics of logic $\mathbb{U}$. In each clause we require z to be fresh for h and σ, and that $\mathrm{fn}(P) \cup \mathrm{fn}(\varphi) \subseteq h$.

History $h = x^{i} \cdot u^{o} \cdot z^{i}$ indicates $x\sigma \neq u$ for all σ respecting it, while the substitution $\{{}^{u}/_{z}\}$ is allowed. After the transitions $\xrightarrow{\bar{x}(u)}\xrightarrow{x(z)}$, P can reach the state $[z = u]\tau$ and Q can reach either 0 or τ. Applying the substitution $\{{}^{u}/_{z}\}$ yields $[z = u]\tau \not\sim_{o}^{h} 0$, and applying $\{{}^{z}/_{z}\}$ gives $[z = u]\tau \not\sim_{o}^{h} \tau$. Therefore $P \not\sim_{o}^{h} Q$.

When considering quasi-open bisimilarity, if after the transitions $\xrightarrow{\bar{x}(u)}\xrightarrow{x(z)}$, $P' = 0$ or τ, then it is straightforward to show that P', Q' are quasi-open bisimilar. If $P' = [z = u]\tau$, we need to show that for all $h' \supseteq_i h$ and for all $y \in h'$, there exists a Q' such that $P'\{{}^{y}/_{z}\}$ is bisimilar to $Q'\{{}^{y}/_{z}\}$. Suppose $h' = h$ and $y \in \{x, u\}$. Then if $y = x$, we have that P' is bisimilar to $Q' = 0$, and if $y = u$ then P' is bisimilar to $Q' = \tau$. If $h' = y^{i} \cdot h$ and $y \notin \{x, u\}$ then P' is bisimilar to $Q' = 0$ because $y \neq u$. Therefore $P \sim_{q}^{h} Q$.

3 A universal logic

We define a universal logic $\mathbb{U}$ that characterises the four bisimilarities mentioned above.

▶ **Definition 17.** Let $\mathbb{U}$ be the language generated by the following grammar:

$$
\begin{array}{rl}
\varphi ::= & \texttt{tt} \mid x = y \mid \varphi \wedge \varphi \mid \neg\varphi \mid \Diamond\varphi \mid \langle\alpha\rangle\varphi \mid \langle\bar{x}(z)\rangle\varphi \\
& \mid \langle x(z)\rangle\varphi \mid \langle x(z)\rangle_{\ell}\varphi \mid \langle x(z)\rangle_{e}\varphi \mid \langle x(z)\rangle_{o}\varphi \mid \langle x(z)\rangle_{q}\varphi
\end{array}
$$

▶ **Definition 18.** Given a process P, a $\mathbb{U}$-formula φ and a history h, the satisfaction relation $P \models^{h} \varphi$ is defined in Figure 2.

▶ Remark. The modalities $\langle x(z)\rangle\varphi$, $\langle x(z)\rangle_{\ell}\varphi$ and $\langle x(z)\rangle_{e}\varphi$ correspond to the operators in MPW logic defined in [15]. The former is not used for our characterisations.

The dual logical propositional and modal connectives are defined as usual, via negation.

▶ **Definition 19** (Logical equivalence)**.** Two processes P and Q are *logically equivalent with respect to some* $\mathbb{S} \subseteq \mathbb{U}$ *and history* h, notation: $P \equiv_{\mathbb{S}}^{h} Q$, if $\mathrm{fn}(P) \cup \mathrm{fn}(Q) \subseteq h$ and for all $\varphi \in \mathbb{S}$ with $\mathrm{fn}(\varphi) \subseteq h$ we have $P \models^{h} \varphi$ iff $Q \models^{h} \varphi$.

We say that $\mathbb{S}$ characterises a history-indexed family $\{R^h \mid h \in \mathcal{H}\}$ of relations if: $P \equiv^h_{\mathbb{U}} Q$ iff PR^hQ. We define sublogics $\mathbb{E}$, $\mathbb{L}$, $\mathbb{Q}$ and $\mathbb{O}$ of $\mathbb{U}$ to characterise the late, early, open and quasi-open bisimilarity.

▶ **Definition 20** (Sublogics of $\mathbb{U}$)**.** The logics $\mathbb{E}$, $\mathbb{L}$, $\mathbb{Q}$ and $\mathbb{O}$ are the sublogics of $\mathbb{U}$ generated by the grammars with $\mathtt{tt}, \neg, \wedge$ and the modalities specified in Table 1.

Table 1 The modalities defining the logics $\mathbb{E}, \mathbb{L}, \mathbb{Q}$ and $\mathbb{O}$.

Logic	Modalities	Characterises
$\mathbb{E}$	$\langle\alpha\rangle$, $\langle\bar{x}(z)\rangle$, $\langle x(z)\rangle_e$	early bisimilarity
$\mathbb{L}$	$\langle\alpha\rangle$, $\langle\bar{x}(z)\rangle$, $\langle x(z)\rangle_\ell$	late bisimilarity
$\mathbb{Q}$	$\Diamond$, $\langle\alpha\rangle$, $\langle\bar{x}(z)\rangle$, $\langle x(z)\rangle_q$	quasi-open bisimilarity
$\mathbb{O}$	$\Diamond$, $\langle\alpha\rangle$, $\langle\bar{x}(z)\rangle$, $\langle x(z)\rangle_o$	open bisimilarity

▶ **Theorem 21.** *The various notions of bisimilarity can be characterised as follows:*

1. $P \equiv^h_{\mathbb{E}} Q$ *iff* $P \sim^h_e Q$
2. $P \equiv^h_{\mathbb{L}} Q$ *iff* $P \sim^h_\ell Q$
3. $P \equiv^h_{\mathbb{Q}} Q$ *iff* $P \sim^h_q Q$
4. $P \equiv^h_{\mathbb{O}} Q$ *iff* $P \sim^h_o Q$

Proof. We postpone the completeness proofs (i.e. $P \equiv^h Q$ implies $P \sim^h Q$) to Section 4. The soundness proofs are straightforward. As an example, we demonstrate part of the soundness proof for open bisimilarity.

Suppose $P \sim^h_o Q$. Then by definition $\mathrm{fn}(P, Q) \subseteq h$. Let φ be an $\mathbb{O}$-formula such that $\mathrm{fn}(\varphi) \subseteq h$ and assume $P \models^h \varphi$. We prove that $Q \models^h \varphi$ by induction on the structure of φ. The propositional cases are routine. We showcase the modal cases for $\varphi = \Diamond\psi$ and $\varphi = \langle\bar{x}(z)\rangle\psi$. If $\varphi = \Diamond\psi$ then there exists a substitution σ respecting h such that $P\sigma \models^{h\sigma} \psi\sigma$. By definition of open bisimulation we have $P\sigma \sim^{h\sigma}_o Q\sigma$. Besides, $\mathrm{fn}(\Diamond\psi) \subseteq h$ implies $\mathrm{fn}(\psi) \subseteq h$, so the induction hypothesis gives $Q\sigma \models^{h\sigma} \psi\sigma$ and hence $Q \models^h \Diamond\psi$.

If $\varphi = \langle\bar{x}(z)\rangle\psi$ then there exists a P' such that $h : P \xrightarrow{\bar{x}(z)} P'$ and $P' \models^{h\cdot z^o} \psi$. By definition of $\models$ the name z is fresh for h. Therefore we can invoke the definition of open bisimulations to find a process Q' such that $h : Q \xrightarrow{\bar{x}(z)} Q'$ and $P' \sim^{h\cdot z^o}_o Q'$. Since $\mathrm{fn}(\langle\bar{x}(z)\rangle\psi) \subseteq h$ we have $\mathrm{fn}(\psi) \subseteq h \cdot z^o$, so we can use the induction hypothesis to derive $Q' \models^{h\cdot z^o} \psi$. Therefore $Q \models^h \langle\bar{x}(z)\rangle\psi$, as desired. ◀

We say a logic is sound and complete for a bisimilarity when: if two processes are bisimilar, then they satisfy the same set of formulas in the logic; and if two processes are not bisimilar, there exist some formulae in the logic that separate them, which we call the distinguishing formulae. A distinguishing formula holds for one process but not for the other, thus revealing a difference in their behavior. The distinguishing formulae can be used as efficiently checkable evidences to explain why two processes are not bisimilar.

The next examples illustrate how the modalities $\langle - \rangle_e$, $\langle - \rangle_\ell$, $\langle - \rangle_q$ and $\langle - \rangle_o$ can be used to recognise non-bisimilar processes.

▶ **Example 22** (Distinguishing processes that are not late bisimilar)**.** Consider the processes

$$P = x(z) + x(z).\tau + x(z).[z = u]\tau \qquad Q = x(z) + x(z).\tau$$

P and Q are early bisimilar but not late bisimilar (see e.g. [15, Section 2.3]). An induction on the structure of φ shows that we have $P \models^h \varphi$ iff $Q \models^h \varphi$ for all $h \in \mathcal{H}^o$ containing x^o and u^o and for all $\varphi \in \mathbb{E}$. However, if we bring $\langle x(z)\rangle_\ell$ into the picture then we can construct a formula which only holds at one of P and Q. For example, the formula

$$\varphi := \langle x(z)\rangle_\ell\big([\tau](z = u) \wedge ((z = u) \to \langle\tau\rangle\mathtt{tt})\big)$$

is true at P but not at Q.

To show that $P \models^{x^o \cdot u^o} \varphi$ we need to find a process P' such that $x^o \cdot u^o : P \xrightarrow{x(z)} P'$ and for all $h' \supseteq_o x^o \cdot u^o$ and all $y \in h'$ we have $P' \models^{h'} \big([\tau](z = u) \wedge ((z = u) \to \langle\tau\rangle\mathtt{tt})\big)\{{}^{y}\!/\!{}_{z}\}$. To this end, take $P' = [z = u]\tau$. Then we have $P'\{{}^{y}\!/\!{}_{z}\} \models^{h'} [\tau](z = u)\{{}^{y}\!/\!{}_{z}\}$, because if there is a τ-transition then we must have $(z = u)\{{}^{y}\!/\!{}_{z}\}$, and $P'\{{}^{y}\!/\!{}_{z}\} \models^{h'} ((z = u) \to \langle\tau\rangle\mathtt{tt})\{{}^{y}\!/\!{}_{z}\}$ because if $(z = u)\{{}^{y}\!/\!{}_{z}\}$ is true then there must exists a τ-transition from P'.

To see that $Q \not\models^{x^o \cdot u^o} \varphi$, note that there are only two processes that Q can $x(z)$-transition to, namely $Q' = 0$ and $Q' = \tau$. In the first case we have $0\{{}^{u}\!/\!{}_{z}\} \not\models^{x^o \cdot u^o} [\tau](z = u) \wedge \big((z = u) \to \langle\tau\rangle\mathtt{tt}\big)$ because the second conjoint is false, while in the second case we can take any $y \neq u$ to find $\tau \not\models^{x^o \cdot u^o \cdot y^o} [\tau](z = u) \wedge \big((z = u) \to \langle\tau\rangle\mathtt{tt}\big)$ because the first conjoint is false.

▶ **Example 23.** Recall from Example 16 that the processes

$$P = \nu u\bar{x}u.(x(z) + x(z).\tau + x(z).[z = u]\tau), \qquad Q = \nu u\bar{x}u.(x(z) + x(z).\tau)$$

are quasi-open bisimilar but not open bisimilar. We construct a distinguishing formula using the modality $\langle x(z)\rangle_o$. First observe the difference between $[z = u]\tau$ and τ. The latter can always make a τ-transition while the former cannot do that without a suitable substitution. Therefore $[z = u]\tau \not\models^{x^i \cdot u^o \cdot z^i} \langle\tau\rangle\mathtt{tt}$ while $\tau \models^{x^i \cdot u^o \cdot z^i} \langle\tau\rangle\mathtt{tt}$. Similarly, the processes 0 and $[z = u]\tau$ can be distinguished by $[z = u]\tau \models^{x^i \cdot u^o \cdot z^i} \Diamond\langle\tau\rangle\mathtt{tt}$ while $0 \not\models^{x^i \cdot u^o \cdot z^i} \Diamond\langle\tau\rangle\mathtt{tt}$. Observe that both P and Q both can perform the transitions $\xrightarrow{\bar{x}(u)}\xrightarrow{x(z)}$ to arrive at states that are distinguishable by a formula. Thus, if we define $\varphi := \langle\bar{x}(u)\rangle\langle x(z)\rangle_o(\neg\langle\tau\rangle\mathtt{tt} \wedge \Diamond\langle\tau\rangle\mathtt{tt})$ then we have $P \models^{x^i} \varphi$ while $Q \not\models^{x_i} \varphi$.

4 Completeness for quasi-open and open bisimilarity

We now detail completeness for quasi-open bisimilarity. We first list here some useful lemmas that will be used in the main completeness proof. Most of these are straightforward to prove, except for Lemma 26, for which we outline a proof.

▶ **Definition 24.** Let h be a history and σ a substitution. Then we define

$$e(h, \sigma) := \bigwedge\{(x = y) \mid x, y \in h \text{ distinct}, \sigma(x) = \sigma(y)\} \wedge \bigwedge\{(x \neq y) \mid x, y \in h, \sigma(x) \neq \sigma(y)\}$$

This is a finite conjunction because h is finite.

▶ **Lemma 25.** *Let P be a process, h a history such that $\mathrm{fn}(P) \subseteq h$ and θ a renaming that respects h. Then for all formulas φ such that $\mathrm{fn}(\varphi) \subseteq h$ we have $P \models^h \varphi$ iff $P\theta \models^{h\theta} \varphi\theta$.*

▶ **Lemma 26.** *Let P be a process, h a history and σ a substitution that respects h. Then $P\sigma \models^{h\sigma} \varphi\sigma$ if and only if $P \models^h \Diamond(e(h, \sigma) \wedge \varphi)$.*

Proof. Suppose $P\sigma \models^{h\sigma} \varphi\sigma$. Since σ respects h, by definition of $e(h, \sigma)$ we have $P\sigma \models^{h\sigma} e(h, \sigma)\sigma$. Therefore $P\sigma \models^{h\sigma} (e(h, \sigma) \wedge \varphi)\sigma$, hence $P \models^h \Diamond(e(h, \sigma) \wedge \varphi)$.

For the conversely, suppose $P \models^{h} \Diamond(e(h,\sigma) \wedge \varphi)$. Then by definition of $\Diamond$, there exists substitution θ respecting h such that $P\theta \models^{h\theta} e(h,\sigma)\theta \wedge \varphi\theta$. Then we have $P\theta \models^{h\theta} e(h,\sigma)\theta$ and $P\theta \models^{h\theta} \varphi\theta$. By $P\theta \models^{h\theta} e(h,\sigma)\theta$ we have $x\sigma = y\sigma$ iff $x\theta = y\theta$ for all $x, y \in h$, and hence we can find a renaming θ' such that σ coincides with $\theta \cdot \theta'$ on h (i.e. $z\sigma = (z\theta)\theta'$ for all $z \in h$). Moreover we may assume that θ' respects h. Then we can use Lemma 25 and the assumption $P\theta \models^{h\theta} \varphi\theta$ to find that $P\sigma \models^{h\sigma} \varphi\sigma$. ◀

▶ **Lemma 27.**

1. *If $h\sigma : P\sigma \xrightarrow{\pi} P'$, then there exists an action π' such that $\pi = \pi'\sigma$.*
2. *If $P\sigma \models^{h\sigma} \varphi$ then there exists a formula φ' using the same connectives as φ s.t. $\varphi'\sigma = \varphi$.*

▶ **Lemma 28** (image finiteness)**.** *For any process P and action π there are finitely many P_i, up to renaming of* $\mathrm{bn}(\pi)$*, such that $P \xrightarrow{\pi} P_i$.*

To prove the completeness is equivalent to prove that if two processes are not bisimilar then there must be some distinguishing formulae that can be satisfied by one of the processes but by not the other. The proof will provide a strategy on constructing distinguishing formulae for any processes that are not quasi-open bisimilar. On the basis of the image finiteness, we are able to define distinguishability, which is a negation of bisimilarity. Note that the subscript of $\sim_0$ below is the number zero instead of the letter o for open bisimilarity.

▶ **Definition 29** (distinguishability)**.** Let $\not\sim_0^h$ be the smallest symmetric relation satisfying $P \not\sim_0^h Q$ whenever there exists a substitution σ respecting h and an action π such that

- There exists a P' such that $h\sigma : P\sigma \xrightarrow{\pi} P'$ but no Q' satisfying $h\sigma : Q\sigma \xrightarrow{\pi} Q'$.

If π is of the shape $\bar{x}(z)$ or $x(z)$ then we assume that z is fresh for h and σ.

We inductively define $\not\sim_{n+1}^h$ as the smallest symmetric relation containing $\not\sim_n^h$ such that $P \not\sim_{n+1}^h Q$ holds if there exists a σ respecting h and a process P' such that either

- $h\sigma : P\sigma \xrightarrow{\alpha} P'$ and for all Q' such that $h\sigma : Q\sigma \xrightarrow{\alpha} Q'$ we have $P' \not\sim_n^{h\sigma} Q'$, where α is of the form τ or $\bar{x}y$; or
- $h\sigma : P\sigma \xrightarrow{\bar{x}(z)} P'$ for some $z \notin h$ and for all Q' such that $h\sigma : Q\sigma \xrightarrow{\bar{x}(z)} Q'$ we have $P' \not\sim_n^{h\sigma \cdot z^o} Q'$; or
- $h\sigma : P\sigma \xrightarrow{x(z)} P'$ for some $z \notin h$ and there exists some $h' \supseteq_i h$ and $y \in h'$ such that for all Q' with $h\sigma : Q\sigma \xrightarrow{x(z)} Q'$ we have $P'\{{}^{y}/_{z}\} \not\sim_n^{h'\sigma} Q'\{{}^{y}/_{z}\}$.

Again, if π is of the shape $\bar{x}(z)$ or $x(z)$ then we assume that z is fresh for h and σ.

▶ **Lemma 30.** *Let P and Q be processes and $h \in \mathcal{H}^{i\text{-}o}$ a history such that* $\mathrm{fn}(P,Q) \subseteq h$*. Then $P \not\sim_q^h Q$ if and only if there exists some n such that $P \not\sim_n^h Q$.*

Theorem 21(3), that is, completeness of quasi-open bisimilarity with respect to $\mathbb{Q}$, follows immediately from the next lemma.

▶ **Lemma 31.** *If $P \not\sim_q^h Q$, then there exists $\varphi \in \mathbb{Q}$ such that $P \models_{\mathbb{Q}}^{h} \varphi$ and $Q \not\models_{\mathbb{Q}}^{h} \varphi$.*

Proof. If $P \not\sim_q^h Q$ then there exists some n such that $P \not\sim_n^h Q$ by Lemma 30. We now construct a distinguishing formula using induction on n. The base case is straightforward. We show here a non-trivial inductive case.

Suppose $P \not\sim_{n+1}^h Q$. Without loss of generality assume that there exists a substitution σ respecting h and a process P such that on of the three cases from Definition 29 holds.

Case 1: $P\sigma \xrightarrow{\alpha} P'$ and for all Q' that satisfy $h\sigma : Q\sigma \xrightarrow{\alpha} Q'$ we have $P' \not\sim_n^{h\sigma} Q'$, where α is of the form τ or $\bar{x}y$. The case is similar to case 2 below.

Case 2: $P\sigma \xrightarrow{\bar{x}(z)} P'$ for some $z \notin h$ and for all Q' that satisfy $h\sigma : Q\sigma \xrightarrow{\bar{x}(z)} Q'$ we have $P' \not\sim_n^{h\sigma \cdot z^o} Q'$. By Lemma 28 there are finitely many such Q' (up to renaming of bound names in π) such that $Q\sigma \xrightarrow{\bar{x}(z)} Q'$, so we can enumerate them $Q'_1, \ldots, Q'_m$. Since $P' \not\sim_n^{h\sigma \cdot z^o} Q'_i$, the induction hypothesis yields a formula φ_i such that $P' \models^{h\sigma \cdot z^o} \varphi_i$ while $Q'_i \not\models^{h\sigma \cdot z^o} \varphi_i$, for all $i \in \{1, \ldots, m\}$. We claim that

$$P \models^h \Diamond(e(h,\sigma) \wedge \langle \bar{x}(z) \rangle \bigwedge_i \varphi'_i) \quad \text{and} \quad Q \not\models^h \Diamond(e(h,\sigma) \wedge \langle \bar{x}(z) \rangle \bigwedge_i \varphi'_i)$$

where $\varphi'_i\sigma = \varphi_i$. By Lemma 27, we have $P\sigma \xrightarrow{\overline{x\sigma}(z)} P'$, and $P' \models^{h\sigma \cdot z^o} \varphi'_i\sigma$, where $\varphi'_i\sigma = \varphi_i$. Then $P\sigma \models^{h\sigma} \langle \overline{x\sigma}(z) \rangle \varphi'_i\sigma$. Since the above holds for all i, $P\sigma \models^{h\sigma} \langle \overline{x\sigma}(z) \rangle \bigwedge_i \varphi'_i\sigma$. Lemma 26 then gives we have $P \models^h \Diamond(e(h,\sigma) \wedge \langle \bar{x}(z) \rangle \bigwedge_i \varphi'_i)$.

For the latter, assume otherwise that $Q \models^h \Diamond(e(h,\sigma) \wedge \langle \bar{x}(z) \rangle \bigwedge_i \varphi'_i)$, then by Lemma 26, $Q\sigma \models^{h\sigma} \langle \overline{x\sigma}(z) \rangle \bigwedge_i \varphi'_i\sigma)$, then there exists Q'_i such that $Q\sigma \xrightarrow{\overline{x\sigma}(z)} Q'_i$ and $Q'_i \models^{h\sigma \cdot z^o} \bigwedge_i \varphi_i$, contradicting the condition that no such Q'_i exists.

Case 3: $h\sigma : P\sigma \xrightarrow{x(z)} P'$ for some $z \notin h\sigma$ and there exists a $h' \supseteq_i h\sigma$ and a $y_0 \in h'$ such that for all Q' that satisfy $h\sigma : Q\sigma \xrightarrow{x(z)} Q'$ we have $P'\{y_0/z\} \not\sim_n^{h'} Q'\{y_0/z\}$. We may assume that $h' = h\sigma$ if $y_0 \in h\sigma$ and $h' = y_0^i \cdot h\sigma$ otherwise. By Lemma 28 there are finitely many such Q' (up to renaming of bound names in π), so we can enumerate them $Q'_1, \ldots, Q'_m$. Since $P'\{y_0/z\} \not\sim_n^{h'\sigma} Q'_i\{y_0/z\}$ by the induction hypothesis we can find a formula φ_i such that

$$P'\{y_0/z\} \models^{h'} \varphi_i \quad \text{while} \quad Q'_i\{y_0/z\} \not\models^{h'} \varphi_i,$$

for all $i \in \{1, \ldots, m\}$. Let $\varphi'_i = \varphi_i\{z/y_0\}$ (so obviously $\varphi_i = \varphi'_i\{y_0/z\}$).

Setting $\varphi := \varphi'_1 \wedge \cdots \wedge \varphi'_m$, we have

$$P'\{y_0/z\} \models^{h'} \varphi\{y_0/z\} \quad \text{while} \quad Q'_i\{y_0/z\} \not\models^{h'} \varphi\{y_0/z\}, \tag{1}$$

for all $i \in \{1, \ldots, m\}$. We now consider two subcases:

Case 3A: $y_0 \in h\sigma$. We now claim that

$$P\sigma \models^{h\sigma} \langle x(z) \rangle_q ((z = y_0) \to \varphi) \quad \text{but} \quad Q\sigma \not\models^{h\sigma} \langle x(z) \rangle_q ((z = y_0) \to \varphi). \tag{2}$$

For the former, let h'' be any history such that $h'' \supseteq_i h\sigma$ and let $y \in h''$. We need to find some P'' such that $h\sigma : P \xrightarrow{x(z)} P''$ and $P'' \models^{h''} ((z = y_0) \to \varphi)\{y/z\}$. Again, we may assume that $h'' = h$ if $y \in h$ and $h'' = y^i \cdot h$ otherwise. Take $P'' = P'$. Then we know that $h\sigma : P\sigma \xrightarrow{x(z)} P'$, so we only need to show that $P' \models^{h''} (z = y_0)\{y/z\} \to \varphi\{y/z\}$. If $y \neq y_0$ then $(z = y_0)\{y/z\}$ is false so the implication is true. If $y = y_0$ then $h'' = h'$ and $\varphi\{y/z\} = \varphi\{y_0/z\}$ so that (1) implies $P'\{y/z\} \models^{h''} \varphi\{y/z\}$, as desired.

Now for the latter, consider history h' and $y_0 \in h'$. Then (clearly) for all Q'_i we have $Q'_i \models^{h'} (z = y_0)\{y_0/z\}$. But $Q'_i \not\models^{h'} \varphi\{y_0/z\}$ by (1), so $Q'_i \not\models^{h'} ((z = y_0) \to \varphi)\{y_0/z\}$. Since the Q'_i range over the $x(z)$-successors of Q (up to renaming of bound names in π), this implies $Q \not\models^{h\sigma} \langle x(z) \rangle_q ((y_0 = z) \to \varphi)$.

Now by Lemma 27 we can find a ψ such that $\psi\sigma = \langle x(z) \rangle_q ((x = y_0) \to \varphi)$, so $P\sigma \models^{h\sigma} \psi\sigma$ and $Q\sigma \not\models^{h\sigma} \psi\sigma$. Lemma 26 then a distinguishing formula which is true at P but false at Q.

Case 3B: $y_0 \notin h\sigma$. Let φ' be $\varphi\{z/y_0\}$. We now claim that

$$P\sigma \models^{h\sigma} \langle x(z) \rangle_q (z \notin h\sigma \to \varphi) \quad \text{but} \quad Q\sigma \not\models^{h\sigma} \langle x(z) \rangle_q (z \notin h\sigma \to \varphi). \tag{3}$$

where $z \notin h\sigma$ refers to $\bigwedge\{z \neq w \mid w \in h\sigma\}$. This case follows a similar reasoning as in 3A, with the inequality guard $(z \notin h\sigma)$ replacing the role of $(z = y_0)$ in 3A.

The symmetric cases, with the role of P and Q reversed, can be obtained by taking the negated distinguishing formula constructed above. ◀

The proofs for early and late bisimilarity resemble the one above. For open bisimilarity, the definition for $P \not\sim_{n+1}^{h} Q$ (Definition 29) differs in the third clause, which is changed to

$$\exists P', h\sigma : P\sigma \xrightarrow{x\sigma(z)} P' \text{ and } \forall Q_i \text{ such that } h\sigma : Q\sigma \xrightarrow{x\sigma(z)} Q_i, P' \not\sim_{n}^{h\sigma\cdot z^i} Q_i$$

as the name z^i is added at a different location in history compared to quasi-open bisimilarity. The remainder of the proof proceeds along the line of the completeness proof for quasi-open bisimulation, but with all three inductive steps resembling cases 1 and 2. In fact, the proof can also be derived from the connection with [5] outlined in Section 6 below.

5 Handling mismatch

So far our language does not include the mismatch prefix $[x \neq y]$, with the interpretation that $[x \neq y]P$ can proceed as P only if x and y are not equal. Adding mismatch is problematic because doing so naively may invalidate Lemma 9 (monotonicity), which requires that "any name-substitution to a process does not diminish its capabilities for action" [23, Chapter 1.1]. In the context of open and quasi-open bisimulation, since names in a process may be subjected to instantiations, the operational semantics for mismatch need to account for all possible instantiations. This is easy to accommodate when the semantics is augmented with histories. The following rule for mismatch is an adaptation of a similar rule in [10]:

$$\frac{h : P \xrightarrow{\pi} Q \quad h \models x \neq y}{h : [x \neq y]P \xrightarrow{\pi} Q} \ (\textsc{Mismatch})$$

where $h \models x \neq y$ iff $x\sigma \neq y\sigma$ for all substitutions σ respecting h.

The monotonicity lemma (Lemma 9) still holds even in the presence of the Mismatch rule. We sketch here a proof for the inductive step. Let σ be any substitution which is respectful with respect to h. First observe that Lemma 7 implies that $h\sigma \models x\sigma \neq y\sigma$. (Indeed, if $h\sigma \not\models x\sigma \neq y\sigma$ then there exists a respectful substitution θ such that $(x\sigma)\theta = (y\sigma)\theta$, but then $\sigma\theta$ respects h and identifies x and y, a contradiction.) By induction hypothesis we have $h\sigma : P\sigma \xrightarrow{\pi\sigma} Q\sigma$. Thus we can use the mismatch rule to find $h\sigma : ([x \neq y]P)\sigma \xrightarrow{\pi\sigma} Q\sigma$.

Monotonicity aside, there is still a problem with mismatch: closure of (quasi-)open bisimilarity under restriction no longer holds. For example, under current definitions, the process $[x \neq y]\tau$ under the history $h = x^i \cdot y^i$ is open and quasi-open bisimilar with 0, since there is a respectful substitution that could invalidate $x \neq y$ (i.e., $\{x/y\}$) so that the τ-transition is not possible from $[x \neq y]\tau$. But neither open-bisimilarity nor quasi-open bisimilarity holds for $\nu y.[x \neq y]\tau$ and 0 under the history $h' = x^i$, since $[x \neq y]$ is always true when y is restricted. To solve this problem, we need to close the (quasi-)open bisimilarity with *rigidisation of names*, i.e., turning an i-annotated name into o-annotated. We extend our logic $\mathbb{U}$ with another accessibility relation that is induced by rigidisation, in addition to the accessibility relation induced by respectful substitution.

We first define the rigidisation relations.

▶ **Definition 32** (Rigidisation relations)**.** The relations $\subseteq_{ro}$ and $\subseteq_{rq}$ are the smallest relations on histories such that:

- $h \subseteq_{ro} h'$ iff $h = h_1 \cdot x^i \cdot h_2$ and $h' = h_1 \cdot x^o \cdot h_2$.
- $h \subseteq_{rq} h'$ iff $h = h_1 \cdot x^i \cdot h_2$ and $h' = h_1 \cdot h_2 \cdot x^o$.
- $h \subseteq_{ro} h \subseteq_{rq} h$.
- Both $\subseteq_{ro}$ and $\subseteq_{rq}$ are transitively closed.

We extend our logic $\mathbb{U}$ with new modal operators $\Diamond_{ro}$ and $\Diamond_{rq}$ for rigidisation of names in open and quasi-open bisimilarities respectively. The semantics are defined as follows.

$$\begin{array}{lll} P \models^h \Diamond_{ro}\varphi & \text{iff} & \exists h' \supseteq_{ro} h, P \models^{h'} \varphi \\ P \models^h \Diamond_{rq}\varphi & \text{iff} & \exists h' \supseteq_{rq} h, P \models^{h'} \varphi \end{array}$$

Accordingly, the definitions of open and quasi-open bisimilarity also need to be extended. For open bisimilarity, we add an additional clause to Definition 13:

For any $h' \supseteq_{ro} h$, we have $P\mathcal{B}_o^{h'}Q$.

For quasi-open bisimilarity, we add an additional clause to Definition 14:

For any $h' \supseteq_{rq} h$, we have $P\mathcal{B}_q^{h'}Q$.

We conjecture that the extensions of bisimilarities we defined here are the same as the definitions given by [10], and that they are characterised by our extended logic $\mathbb{U}$.

6 Related work

The idea of accounting of history of names in process transitions has been considered in other settings, notably in the automata theoretic model called *history-dependent automata* [16, 17]. In the case of bisimilarity relations, indexing the relations with a context more general than distinctions has also been considered in work on *environmental bisimulation* [21], and bisimulations for cryptographic calculi,e.g., [3, 6, 24]. In particular, our notion of histories is a special instance of that used in [24]. None of these works consider specifically the problem of characterising bisimulations via logic. We discuss next two other closest related works.

Relations between sublogic $\mathbb{O}$ and the intuitionistic modal logic $\mathbb{OM}$

In [5], open bisimilarity is characterised $\mathbb{OM}$, which extends intuitionistic logic with modalities of the form $\langle\pi\rangle\varphi$ and $[\pi]\varphi$ where π is of the form τ, $\bar{x}y$, $\bar{x}(z)$ or $x(z)$. The diamonds are interpreted with respect to a process and a history as in Definition 18 above, with $\langle x(z)\rangle$ being interpreted as $\langle x(z)\rangle_o$. The box operators are interpreted as the duals of the diamonds, with the additional condition that they be closed under respectful substitutions. For example,

$$P \models^h_{\mathbb{OM}} [\bar{x}(z)]\varphi \quad \text{iff} \quad \forall\sigma \text{ respecting } h, \forall Q,\ P\sigma \xrightarrow{\overline{x\sigma}z} Q \text{ implies } Q \models^{h\sigma}_{\mathbb{OM}} \varphi\sigma.$$

The logic $\mathbb{OM}$ can faithfully be embedded in $\mathbb{O}$ via a variation of the Gödel-McKinsey-Tarski translation of intuitionistic logic into the modal logic **S4** (see e.g. [7, §3.9]).

▶ **Definition 33.** Define the translation $t : \mathbb{OM} \to \mathbb{O}$ on propositional connectives as the Gödel-McKinsey-Tarski translation:

$$\begin{array}{lll} t(\mathtt{tt}) = \mathtt{tt} & t(\varphi_1 \wedge \varphi_2) = t(\varphi_1) \wedge t(\varphi_2) & t(x = y) = (x = y) \\ t(\mathtt{ff}) = \mathtt{ff} & t(\varphi_1 \vee \varphi_2) = t(\varphi_1) \vee t(\varphi_2) & t(\varphi_1 \supset \varphi_2) = \Box(t(\varphi_1) \to t(\varphi_2)) \end{array}$$

This is extended to modalities as follows:

$$\begin{array}{lll} t(\langle\pi\rangle\varphi) = \langle\pi\rangle t(\varphi) & t([\pi]\varphi) = \Box([\pi]t(\varphi)) & \text{for } \pi = \tau, \bar{x}y, \bar{x}(z) \\ t(\langle\pi\rangle\varphi) = \langle\pi\rangle_o t(\varphi) & t([\pi]\varphi) = \Box([\pi]_o t(\varphi)) & \text{for } \pi = x(z) \end{array}$$

The correctness of the translation relies of the following lemma.

▶ **Lemma 34.** *For all P and all $\varphi \in \mathbb{OM}$ we have $P \models^h_{\mathbb{OM}} \varphi$ iff $P \models^h t(\varphi)$.*

Completeness for open bisimilarity now follows from [5, Theorem 3.3]: If $P \not\sim^h_o Q$ then there exists a formula $\varphi \in \mathbb{OM}$ such that $P \models^h_{\mathbb{OM}} \varphi$ while $Q \not\models^h_{\mathbb{OM}} \varphi$ or vice versa. Lemma 34 implies that $t(\varphi) \in \mathbb{O}$ satisfies $P \models^h t(\varphi)$ while $Q \not\models^h t(\varphi)$ (or vice versa), so that $P \not\equiv^h_o Q$.

Modal logics for nominal transition systems

In [18], Parrow et. al., defines a general framework for defining transition systems, called nominal transition systems, that subsumes most of name-passing calculi, including the π-calculus. They then define a general modal logic that characterises bisimilarity relations defined on nominal transition systems. They show several examples of how their framework can be instantiated to provide logical characterisations of bisimilarity relations; these include the π-calculus (without mismatch) and early, late and open bisimilarity. Of particular interests in the context of the current paper is the way in which they capture the notion of respectful substitutions, which is formalised as a notion of effects. In the modal logic for open bisimilarity, their logic considers an operator @ that applies an effect to the state (i.e., a process) of their semantic judgment, e.g., $P \models f@\varphi$ iff $f(P) \models \varphi$. This resembles our operator $\Diamond$, however there are a couple of crucial differences: we apply the substitution (effect f in this example) to both the state and the modal formula, and our logic contains the equality predicate whereas their logic (for this particular example involving the π-calculus) does not allow equality (or any state predicates). The equality predicate becomes quite crucial when mismatch is present and at this stage, it is not clear whether quasi-open bisimilarity with mismatch can be similarly defined in the framework of nominal transition systems.

7 Conclusion

In this paper we considered early, late, open and quasi-open bisimilarity for the finite fragment of the π-calculus extended with the mismatch operator. We provided a unified presentation of each of these notions in the late transition semantics, using the notion of a history to capture the name context of a process. We then defined a unifying modal logic, and identified four fragments charaterising the four notions of bisimilarity. That is, for each type of bisimilarity we gave a sublogic of the unifying logic such that two processes are bisimilar if and only if they satisfy precisely the same formulas in the fragment.

As a consequence of the fact that our unifying logic is classical, we obtain a simple construction of distinguishing formulas for non-bisimilar processes in the context of open and quasi-open bisimilarity, compared to [5, 10].

An interesting direction for further research is to investigate to what extend our unifying logic can be used for extensions of our fragment of the π-calculus to include e.g. replication or recursion, or to cryptographic calculi such as the spi-calculus [2] or the applied π-calculus [1]. Some work in this direction can be found in [8, 12, 19, 25, 11].

References

1 Martín Abadi, Bruno Blanchet, and Cédric Fournet. The applied pi calculus: Mobile values, new names, and secure communication. *J. ACM*, 65(1):1:1–1:41, 2018. doi:10.1145/3127586.

2 Martín Abadi and Andrew D. Gordon. A calculus for cryptographic protocols: The spi calculus. In Richard Graveman, Philippe A. Janson, Clifford Neuman, and Li Gong, editors, *CCS '97, Proceedings of the 4th ACM Conference on Computer and Communications Security, Zurich, Switzerland, April 1-4, 1997*, pages 36–47. ACM, 1997. doi:10.1145/266420.266432.

3 Martín Abadi and Andrew D. Gordon. A bisimulation method for cryptographic protocols. *Nord. J. Comput.*, 5(4):267, 1998.

4 Ki Yung Ahn, Ross Horne, and Alwen Tiu. A characterisation of open bisimilarity using an intuitionistic modal logic. In Roland Meyer and Uwe Nestmann, editors, *28th International Conference on Concurrency Theory, CONCUR 2017, September 5-8, 2017, Berlin, Germany*, volume 85 of *LIPIcs*, pages 7:1–7:17. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2017. doi:10.4230/LIPIcs.CONCUR.2017.7.

5 Ki Yung Ahn, Ross Horne, and Alwen Tiu. A characterisation of open bisimilarity using an intuitionistic modal logic. *Logical Methods in Computer Science*, 17, 2021.

6 Johannes Borgström and Uwe Nestmann. On bisimulations for the spi calculus. In Hélène Kirchner and Christophe Ringeissen, editors, *Algebraic Methodology and Software Technology, 9th International Conference, AMAST 2002, Saint-Gilles-les-Bains, Reunion Island, France, September 9-13, 2002, Proceedings*, volume 2422 of *Lecture Notes in Computer Science*, pages 287–303. Springer, 2002. doi:10.1007/3-540-45719-4_20.

7 A. Chagrov and M. Zakharyaschev. *Modal Logic.* Oxford University Press, Oxford, 1997.

8 Ulrik Frendrup, Hans Hüttel, and Jesper Nyholm Jensen. Modal logics for cryptographic processes. In Uwe Nestmann and Prakash Panangaden, editors, *9th International Workshop on Expressiveness in Concurrency, EXPRESS 2002, Satellite Workshop from CONCUR 2002, Brno, Czech Republic, August 19, 2002*, volume 68 of *Electronic Notes in Theoretical Computer Science*, pages 124–141. Elsevier, 2002. doi:10.1016/S1571-0661(05)80368-8.

9 Matthew Hennessy and Robin Milner. Algebraic laws for nondeterminism and concurrency. *J. ACM*, 32(1):137–161, 1985. doi:10.1145/2455.2460.

10 Ross Horne, Ki Yung Ahn, Shang-Wei Lin, and Alwen Tiu. Quasi-open bisimilarity with mismatch is intuitionistic. In Anuj Dawar and Erich Grädel, editors, *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2018, Oxford, UK, July 09-12, 2018*, pages 26–35. ACM, 2018. doi:10.1145/3209108.3209125.

11 Ross Horne and Sjouke Mauw. Discovering epassport vulnerabilities using bisimilarity. *Log. Methods Comput. Sci.*, 17(2):24, 2021. doi:10.23638/LMCS-17(2:24)2021.

12 Hans Hüttel and Michael D. Pedersen. A logical characterisation of static equivalence. In Marcelo Fiore, editor, *Proceedings of the 23rd Conference on the Mathematical Foundations of Programming Semantics, MFPS 2007, New Orleans, LA, USA, April 11-14, 2007*, volume 173 of *Electronic Notes in Theoretical Computer Science*, pages 139–157. Elsevier, 2007. doi:10.1016/j.entcs.2007.02.032.

13 Robin Milner. *A Calculus of Communicating Systems*, volume 92 of *Lecture Notes in Computer Science*. Springer, 1980. doi:10.1007/3-540-10235-3.

14 Robin Milner, Joachim Parrow, and David Walker. A calculus of mobile processes, II. *Information & Computation*, 100:41–77, 1992. doi:10.1016/0890-5401(92)90009-5.

15 Robin Milner, Joachim Parrow, and David Walker. Modal logics for mobile processes. *Theor. Comput. Sci.*, 114(1):149–171, 1993. doi:10.1016/0304-3975(93)90156-N.

16 Ugo Montanari and Marco Pistore. An introduction to history dependent automata. In Andrew D. Gordon, Andrew M. Pitts, and Carolyn L. Talcott, editors, *Second Workshop on Higher-Order Operational Techniques in Semantics, HOOTS 1997, Stanford, CA, USA, December 8-12, 1997*, volume 10 of *Electronic Notes in Theoretical Computer Science*, pages 170–188. Elsevier, 1997. doi:10.1016/S1571-0661(05)80696-6.

17 Ugo Montanari and Marco Pistore. History dependent automata. Technical report, Università di Pisa, 1998.

18 Joachim Parrow, Johannes Borgström, Lars-Henrik Eriksson, Ramunas Gutkovas, and Tjark Weber. Modal logics for nominal transition systems. *Log. Methods Comput. Sci.*, 17(1), 2021. URL: https://lmcs.episciences.org/7137.

19 Michael David Pedersen. Logics for the applied pi calculus. *BRICS Report Series*, 13(19), December 2006. doi:10.7146/brics.v13i19.21923.

20 Davide Sangiorgi. A theory of bisimulation for the pi-calculus. In Eike Best, editor, *CONCUR '93, 4th International Conference on Concurrency Theory, Hildesheim, Germany, August 23-26, 1993, Proceedings*, volume 715 of *Lecture Notes in Computer Science*, pages 127–142. Springer, 1993. doi:10.1007/3-540-57208-2_10.

21 Davide Sangiorgi, Naoki Kobayashi, and Eijiro Sumii. Environmental bisimulations for higher-order languages. *ACM Trans. Program. Lang. Syst.*, 33(1):5:1–5:69, 2011. doi:10.1145/1889997.1890002.

22 Davide Sangiorgi and David Walker. On barbed equivalences in pi-calculus. In Kim Guldstrand Larsen and Mogens Nielsen, editors, *CONCUR 2001 – Concurrency Theory, 12th International Conference, Aalborg, Denmark, August 20-25, 2001, Proceedings*, volume 2154 of *Lecture Notes in Computer Science*, pages 292–304. Springer, 2001. doi:10.1007/3-540-44685-0_20.

23 Davide Sangiorgi and David Walker. *The pi-calculus: a Theory of Mobile Processes*. Cambridge university press, 2003.

24 Alwen Tiu. A trace based bisimulation for the spi calculus: An extended abstract. In Zhong Shao, editor, *Programming Languages and Systems, 5th Asian Symposium, APLAS 2007, Singapore, November 29-December 1, 2007, Proceedings*, volume 4807 of *Lecture Notes in Computer Science*, pages 367–382. Springer, 2007. doi:10.1007/978-3-540-76637-7_25.

25 Alwen Tiu and Jeremy E. Dawson. Automating open bisimulation checking for the spi calculus. In *Proceedings of the 23rd IEEE Computer Security Foundations Symposium, CSF 2010, Edinburgh, United Kingdom, July 17-19, 2010*, pages 307–321. IEEE Computer Society, 2010. doi:10.1109/CSF.2010.28.

26 Alwen Tiu and Dale Miller. Proof search specifications of bisimulation and modal logics for the pi-calculus. *ACM Trans. Comput. Log.*, 11(2):13:1–13:35, 2010. doi:10.1145/1656242.1656248.