Quasi-Open Bisimilarity with Mismatch is Intuitionistic

Ross Horne
School of Computer Science and Engineering
Nanyang Technological University, Singapore
rhorne@ntu.edu.sg

Ki Yung Ahn
Department of Computer Engineering
Hannam University, Daejeon, Korea
kya@hnu.kr

Shang-wei Lin
School of Computer Science and Engineering
Nanyang Technological University, Singapore
shang-wei.lin@ntu.edu.sg

Alwen Tiu
Research School of Computer Science
Australian National University, Canberra
alwen.tiu@anu.edu.au

Abstract

Quasi-open bisimilarity is the coarsest notion of bisimilarity for the π-calculus that is also a congruence. This work extends quasi-open bisimilarity to handle mismatch (guards with inequalities). This minimal extension of quasi-open bisimilarity allows fresh names to be manufactured to provide constructive evidence that an inequality holds. The extension of quasi-open bisimilarity is canonical and robust — coinciding with open barbed bisimilarity (an objective notion of bisimilarity congruence) and characterised by an intuitionistic variant of an established modal logic. The more famous open bisimilarity is also considered, for which the coarsest extension for handling mismatch is identified. Applications to checking privacy properties are highlighted. Examples and soundness results are mechanised using the proof assistant Abella.

CCS Concepts • **Theory of computation → Process calculi**; **Modal and temporal logics**;

Keywords mismatch, bisimilarity, intuitionistic modal logic

ACM Reference format:
Ross Horne, Ki Yung Ahn, Shang-wei Lin, and Alwen Tiu. 2018. Quasi-Open Bisimilarity with Mismatch is Intuitionistic . In *Proceedings of LICS '18: 33rd Annual ACM/IEEE Symposium on Logic in Computer Science, Oxford, United Kingdom, July 9–12, 2018 (LICS '18),* 10 pages.
https://doi.org/10.1145/3209108.3209125

1 Introduction

The problem of logically characterising notions of bisimilarity that are congruences for the π-calculus was a long standing problem in concurrency theory until recently. We begin by explaining the historical context of this problem. We then explain how the insight gained leads to a solution to the long-debated problem of defining a bisimilarity for the π-calculus with mismatch that is a congruence.

The historical perspective. When Milner, Parrow and Walker announced the π-calculus [13], they introduced two notions of equivalence: *late bisimilarity* and *early bisimilarity*. They also provided modal logic characterisations of each of these bisimilarities in the style of Hennessey-Milner logic [9]; that is, two processes are equivalent if and only if they satisfy the same formulae. However, both late and early bisimilarity have the limitation that they are not fully compositional in the sense that, if two processes are bisimilar, it is not necessarily the case that they are bisimilar under an input prefix. Sangiorgi rectified this problem by introducing, first, *open bisimilarity* [18], and later, *quasi-open bisimilarity* [19] — both these notions of bisimilarity are automatically congruences. However, initially, no logical characterisation of either congruence was provided.

Some progress with the logical nature of open bisimilarity was made by Tiu and Miller [20]. When studying embeddings in an intuitionistic framework [12], they observe the law of excluded middle for name equality ($x = y$ or $x \neq y$) must be explicitly induced for late bisimilarity. By taking their embedding of late bisimilarity and dropping the distinct name assumption and the law of excluded middle we obtain open bisimilarity. This insight lead to intuitionistic modal logic $\mathcal{OM}$ [3], characterising open bisimilarity.

Quasi-open bisimilarity is also intuitionistic. This work extends the above story to cover *quasi-open bisimilarity* and mismatch. We discover that quasi-open bisimilarity is an intuitionistic variant of *early bisimilarity*, with a characteristic intuitionistic modal logic called intuitionistic $\mathcal{FM}$. As with $\mathcal{OM}$ the law of excluded middle is invalid for intuitionistic $\mathcal{FM}$.

In both $\mathcal{OM}$ and $\mathcal{FM}$, the law of excluded middle is invalidated by *intuitionistic hereditary*, which simply adds a proviso "for all reachable worlds" in front of connectives, where a reachable world is a process that can be reached by applying a substitution. For example, for $\overline{x}y \parallel z(w)$, by applying substitution $\{^z/_x\}$, we can reach "world" $\overline{z}y \parallel z(w)$. As in the classical case, $\overline{x}y \parallel z(w) \not\models \langle\tau\rangle\mathtt{tt}$, where $\mathtt{tt}$ here denotes the logical constant for truth, and $\langle\tau\rangle$ is the usual diamond modal operator indexed by the τ action. However, in contrast to the classical case, $\overline{x}y \parallel z(w) \not\models \neg\langle\tau\rangle\mathtt{tt}$, since in a "world" where $x = z$, $(\overline{x}y \parallel z(w))\{^z/_x\} \xrightarrow{\tau} 0$. Consequently, since neither formula can be satisfied, we have $\overline{x}y \parallel z(w) \not\models \langle\tau\rangle\mathtt{tt} \vee \neg\langle\tau\rangle\mathtt{tt}$, demonstrating that the law of excluded middle is invalidated. The insight that $x \neq y$ cannot automatically be assumed in an intuitionistic setting, assisted us in discovering a semantics for mismatch.

Why extend with mismatch? A mismatch guarded process of the form $[x \neq y]Q$ proceeds as Q only if we can provide evidence that x and y are not equal. Processes of the form $[x = y]P + [x \neq y]Q$ can

The authors acknowledge support from Ministry of Education, Singapore, Tier 2 grant MOE2014-T2-2-076. Ahn acknowledges support from NRF grant 2018R1C1B5046826 funded by Korea government (MSIT). Horne and Lin acknowledge support from National Research Foundation, Singapore, grant NRF2014NCR-NCR001-30.

LICS '18, July 9–12, 2018, Oxford, United Kingdom
© 2018 Association for Computing Machinery.
ACM ISBN 978-1-4503-5583-4/18/07…$15.00
https://doi.org/10.1145/3209108.3209125

be used to model protocols with control flow involving `if-then-else` branching [1]. Quasi-open bisimilarity allows equalities to be induced as required by applying substitutions, say $\{^{y}/_{x}\}$. However, the original definition of quasi-open bisimilarity has no mechanism enabling inequalities such as $x \neq y$ to be induced.

This work conservatively extends quasi-open bisimilarity to allow inequalities to be lazily induced, by manufacturing fresh names when more evidence is required. For example, observe that $[x \neq y]\tau$ is not quasi-open bisimilar to τ. Process τ can always act; but, without an explicit assumption guaranteeing x and y are distinct, $[x \neq y]\tau$ cannot perform any action. At first sight, since x and y are distinct variables it may be tempting to assume $[x \neq y]\tau$ can always act. This would be the **wrong** assumption for any bisimulation congruence, since there is a context $C\{\} \triangleq a(x).\{\,\cdot\,\} \parallel \overline{a}y$ such that $C\{[x \neq y]\tau\} \xrightarrow{\tau} [y \neq y]\tau$, but $C\{\tau\}$ only has transition $C\{\tau\} \xrightarrow{\tau} \tau$. Clearly $[y \neq y]\tau$ cannot perform any action hence is distinguished from τ. Thus distinguishing $[x \neq y]\tau$ and τ is essential to ensure a notion of bisimilarity is a congruence. Quasi-open bisimilarity, as defined in this work, does not a priori assume that $x \neq y$, but does ensure, whenever $x \neq y$ is enabled, it can never be disabled in the future. Thus, for example, $[x \neq y]\tau.[x = y]\tau$ and $[x \neq y]\tau$ are quasi-open bisimilar since, after the first transition, substitutions equating x and y are permanently disabled.

Subtleties of mismatch. Perhaps surprisingly, both open and quasi-open bisimilarity distinguish the following processes:

$$\tau \qquad \not\sim \qquad [x = y]\tau + [x \neq y]\tau$$

In the intuitionistic setting, recall that we do not a priori assume "$x = y$ or $x \neq y$" holds. The latter process must read the values of x and y, thereby deciding whether $x = y$ or $x \neq y$ in order to make progress; in contrast to τ which need not read anything to progress. Hence the latter process is stuck until a "world" is fixed. A distinguishing formula biased to the right is $\lceil\tau\rceil(x = y \vee x \neq y)$, i.e., in all worlds in which a τ transition is enabled either $x = y$ or $x \neq y$ has been fixed.

The above distinction is where we necessarily depart from previous work on mismatch [7, 8, 16, 17]. For readers accustomed to classical bisimulations, where all terms are grounded, distinguishing these terms may be contentious at first sight. However, dropping the law of excluded middle is necessary for any bisimilarity that is also a congruence.

Subtleties of quasi-open bisimilarity with mismatch. In contrast to the previous example, the following processes are equivalent according to quasi-open bisimilarity, but distinguished by open bisimilarity.

$$\nu x.\overline{z}x.z(y).\tau \qquad \sim \qquad \nu x.\overline{z}x.z(y).([x = y]\tau + [x \neq y]\tau)$$

This is due to quasi-open bisimilarity treating only private names classically. This feature makes quasi-open bisimilarity useful for verifying the privacy of protocols, where a decision based on private information cannot be observable. The above equivalence ensures there is no test an external observer can perform determining the second process above made a choice based on the private name x.

Outline. Section 2 introduces the conservative extension of quasi-open bisimilarity handling mismatch. Section 3 investigates the intuitionistic modal logic characterising quasi-open bisimilarity. Section 4 highlights the novel features of the mechanisation of proofs in proof assistant Abella [4]. Section 5 identifies the coarsest conservative extension of open bisimilarity handling mismatch. Section 6 justifies definitions in this work with respect to existing work on notions of bisimilarity handling mismatch.

2 Intuitionistic mismatch in the π-calculus

In order to define quasi-open bisimilarity with mismatch two small extensions are made in this section. Firstly, the labelled transition system, defining the operational semantics, must be made aware of environment information used to provide evidence for resolving mismatch guards. Secondly, the definition of quasi-open bisimilarity must be extended with the ability to manufacture fresh names.

2.1 Open early labelled transitions

This section presents a dialect of the π-calculus with mismatch. The labelled transition semantics are extended in a minimal fashion in order to evaluate mismatch for open terms, where names are variables rather than distinct constants. In order to evaluate mismatch, we require a notion of *respectful substitution* critical throughout this work.

The grammar for processes extended with mismatch is presented.

$$P ::= 0 \mid \tau.P \mid x(y).P \mid \overline{x}y.P \mid \nu x.P \mid P \parallel P \mid P + P \mid [x = y]P \mid [x \neq y]P$$

A process can be prefixed by an action, where actions can be silent progress τ, or an input or output action. Input action $x(z)$ receives on channel x some value; while output actions $\overline{x}y$ sends y on the same channel. The private names are bound by the ν quantifier restricting their scope and freshness. Processes can be composed using parallel composition $\parallel$ and choice $+$. Further to the match guard that passes if two variables are the same, we include a mismatch that passes only if we have evidence two variables can never be equal. Note $[x = y]P + [x \neq y]Q$ encodes `if` $x{=}y$ `then` P `else` Q.

For (quasi-)open bisimilarity, there is no syntactic distinction between names and variables. The different semantic treatments of (input, bound, and extruded) variables are distinguished by an environment rather than the syntax. For quasi-open bisimilarity the *environment* is a set of names representing private names that have been extruded. This set of names is used in the open early labelled transition system in Fig. 1 as constructive evidence to determine whether a mismatch holds, using the following definition.

Definition 2.1 (respects). Given a set of variables $\mathcal{N}$ and substitution σ, we say σ respects $\mathcal{N}$ whenever for all $x \in \mathcal{N}$, $x\sigma = x$, and if $x \notin \mathcal{N}$ then $x\sigma \notin \mathcal{N}$. We say entailment $\mathcal{N} \models x \neq y$ holds whenever there is no σ respecting $\mathcal{N}$ such that $x\sigma = y\sigma$.

For example, $x \models x \neq y$ holds, since x is a private name hence cannot be unified with y by any respectful substitution. In contrast, $\varnothing \models x \neq y$ does **not** hold, since any substitution such that $x\sigma = y$ respects the empty set of private names. Entailment can be equivalently formulated as $\mathcal{N} \models x \neq y$ holds whenever, x and y are distinct variables and either $x \in \mathcal{N}$ or $y \in \mathcal{N}$.

The early transition semantics in Fig. 1 differs only slightly from the standard early transition semantics for the π-calculus. Each rule is tagged with an environment consisting of a set of names, which plays a significant role in the rules Mismatch and Res. The Open and Close rules have extra conditions that simply ensure that bound names on labels are fresh, by ensuring they not get confused with names in the environment. As standard for early labelled transitions, actions π range over grammar $\pi ::= \tau \mid \overline{x}y \mid xy \mid \overline{x}(z)$.

$$\dfrac{}{\mathcal{N}\colon x(z).P \xrightarrow{xy} P\{^{y}/_{z}\}}\,\textsc{Inp} \qquad \dfrac{}{\mathcal{N}\colon \pi.P \xrightarrow{\pi} P}\,\textsc{Act} \qquad \dfrac{\mathcal{N}\colon P \xrightarrow{\pi} Q}{\mathcal{N}\colon [x = x]P \xrightarrow{\pi} Q}\,\textsc{Mat} \qquad \dfrac{\mathcal{N}\colon P \xrightarrow{\pi} Q \quad \mathcal{N} \models x \neq y}{\mathcal{N}\colon [x \neq y]P \xrightarrow{\pi} Q}\,\textsc{Mismatch}$$

$$\dfrac{\mathcal{N}\colon P \xrightarrow{\overline{x}z} Q \quad z \notin \mathcal{N} \cup \{x\}}{\mathcal{N}\colon \nu z.P \xrightarrow{\overline{x}(z)} Q}\,\textsc{Open} \qquad \dfrac{\mathcal{N}, x\colon P \xrightarrow{\pi} Q \quad x \notin \mathcal{N} \cup \mathrm{n}(\pi)}{\mathcal{N}\colon \nu x.P \xrightarrow{\pi} \nu x.Q}\,\textsc{Res} \qquad \dfrac{\mathcal{N}\colon P \xrightarrow{\pi} Q \quad \text{if } \pi = \overline{x}(z) \text{ then } z \notin \mathrm{fv}(R)}{\mathcal{N}\colon P \parallel R \xrightarrow{\pi} Q \parallel R}\,\textsc{Par-l}$$

$$\dfrac{\mathcal{N}\colon P \xrightarrow{xz} P' \quad \mathcal{N}\colon Q \xrightarrow{\overline{x}(z)} Q' \quad z \notin \mathcal{N} \cup \mathrm{fv}(P)}{\mathcal{N}\colon P \parallel Q \xrightarrow{\tau} \nu z.(P' \parallel Q')}\,\textsc{Close-l} \qquad \dfrac{\mathcal{N}\colon P \xrightarrow{\overline{x}y} P' \quad \mathcal{N}\colon Q \xrightarrow{xy} Q'}{\mathcal{N}\colon P \parallel Q \xrightarrow{\tau} P' \parallel Q'}\,\textsc{Comm-l} \qquad \dfrac{\mathcal{N}\colon P \xrightarrow{\pi} R}{\mathcal{N}\colon P + Q \xrightarrow{\pi} R}\,\textsc{Sum-l}$$

Figure 1. An early transition semantics for the finite π-calculus processes with mismatch, plus the symmetric rules ($\star$-r). The variables of an action are defined such that: $\mathrm{n}(\overline{x}(z)) = \mathrm{n}(\overline{x}z) = \mathrm{n}(xz) = \{x, z\}$; and $\mathrm{n}(\tau) = \varnothing$; while α-conversion is such that $x(z).P$ and $\nu z.P$ bind z in P.

The Mismatch rule. Without the set of names in the environment, no process guarded with mismatch can make progress. An environment consisting of the single name z can be used to resolve a mismatch such as the following.

$$\dfrac{\dfrac{}{z\colon \tau \xrightarrow{\tau} 0} \qquad z \models x \neq z}{z\colon [x \neq z]\tau \xrightarrow{\tau} 0}$$

The Res rule. Notice that the Res rule extends the environment with a fresh name. This is essential for resolving a mismatch in which a variable is bound by a ν quantifier, as in the following example rule instance.

$$\dfrac{z\colon [x \neq z]\tau \xrightarrow{\tau} 0}{\varnothing\colon \nu z.[x \neq z]\tau \xrightarrow{\tau} \nu z.0}$$

Notice the premise holds by combining with the previous example.

2.2 Quasi-open bisimilarity with mismatch

This section introduces a conservative extension of quasi-open bisimilarity handling mismatch. The only change compared to the standard definition is an additional clause allowing new fresh names to be created.

A quasi-open bisimilarity is closed under all substitutions that do not involve private names. For example, $[x = y]\tau$ can act under substitution $\{^{y}/_{x}\}$, hence $[x = y]\tau$ is distinguished from 0.

The additional clause can be used to generate additional fresh names. These fresh names allow mismatches to be resolved by the labelled transition system. For example, given the empty environment, process $[x \neq y]\tau$ is inactive; however, turning x into a fresh name enables a transition $x\colon [x \neq y]\tau \xrightarrow{\tau} 0$. In this way, $[x \neq y]\tau$ is distinguished from 0. The first bullet point in the following definition induces (respectful) equalities, while the second is used to induce inequalities.

Definition 2.2 (quasi-open bisimilarity)**.** A symmetric relation indexed by an environment $\mathcal{R}$ is a quasi-open bisimulation whenever, if $P \mathrel{\mathcal{R}^{\mathcal{N}}} Q$ the following hold:

- If σ respects $\mathcal{N}$ then $P\sigma \mathrel{\mathcal{R}^{\mathcal{N}}} Q\sigma$.
- For any x, we have $P \mathrel{\mathcal{R}^{\mathcal{N},x}} Q$.
- If $\mathcal{N}\colon P \xrightarrow{\alpha} P'$, there exists Q' such that $\mathcal{N}\colon Q \xrightarrow{\alpha} Q'$ and $P' \mathrel{\mathcal{R}^{\mathcal{N}}} Q'$, where α is of the form τ, $\overline{x}y$ or xy.
- If $\mathcal{N}\colon P \xrightarrow{\overline{x}(z)} P'$, where z is fresh for P, Q and $\mathcal{N}$, there exists Q' such that $\mathcal{N}\colon Q \xrightarrow{\overline{x}(z)} Q'$ and $P' \mathrel{\mathcal{R}^{\mathcal{N},z}} Q'$.

Quasi-open bisimilarity $\sim$ is such that $P \sim Q$ whenever there exists quasi-open bisimulation $\mathcal{R}$ such that $P \mathrel{\mathcal{R}^{\varnothing}} Q$.

The above definition is standard except the second clause creating fresh names and the extra environment information for labelled transitions. At any point, a labelled transition enabled for a process, must be matched by a transition with the same label by the other process. In the final clause above, bound output transitions update the environment with a fresh private name.

Examples of quasi-open bisimilar processes. The following processes are quasi-open bisimilar.

$$\nu z.\overline{x}z.[x \neq z]\tau \sim \nu z.\overline{x}z.\tau$$

Since $\varnothing\colon \nu z.\overline{x}z.[x \neq z]\tau \xrightarrow{\overline{x}(z)} [x \neq z]\tau$ and $\varnothing\colon \nu z.\overline{x}z.\tau \xrightarrow{\overline{x}(z)} \tau$, we should check $[x \neq z]\tau \sim^{z} \tau$. This holds since $z \models x \neq z$, so, automatically without any further assumptions, $z\colon [x \neq z]\tau \xrightarrow{\tau} 0$, as required. A similar argument establishes $\nu z.[z \neq y]\tau \sim \tau$.

Clearly $[x \neq z](\overline{x}y \parallel z(w)) \sim [x \neq z](\overline{x}y.z(w) + z(w).\overline{x}y)$ holds. This can be established directly; or by the properties $\overline{x}y \parallel z(w) \sim \overline{x}y.z(w) + z(w).\overline{x}y + [x = z]\tau$ combined with $[x = y][x \neq y]P \sim 0$ and $[x \neq y](P + Q) \sim [x \neq y]P + [x \neq y]Q$.

For $[x \neq z]\overline{x}y \parallel z(w)$ and $[x \neq z](\overline{x}y \parallel z(w))$, although the send and receive actions cannot interact, these processes are not quasi-open bisimilar. The former can always perform input action zw, even if x and z are equated; but the latter can only perform action zw in a context where x and y are guaranteed to be distinct.

Examples particular to quasi-open bisimilarity. The examples above also hold for any reasonable definition of open bisimilarity handling mismatch, as discussed later in Sec. 5. In contrast, the following equivalence holds only for quasi-open bisimilarity.

$$\nu x.\overline{z}x.z(y).\tau \;\sim\; \nu x.\overline{z}x.z(y).([x = y]\tau + [x \neq y]\tau)$$

The above equivalence is important for privacy properties. For example, suppose that a server only responds to a fixed key, represented by k or ℓ below, but does not disclose which key. In order to keep the internal key private, a dummy message is sent. The essence of this problem can be modelled by the following two processes.

$$\nu k.\nu\ell.\overline{x}k.\overline{x}\ell.x(y).([k = y]\tau + [k \neq y]\tau)$$
$$\nu k.\nu\ell.\overline{x}k.\overline{x}\ell.x(y).([\ell = y]\tau + [\ell \neq y]\tau)$$

Quasi-open bisimilarity, correctly, claims the above processes are equivalent (quasi-open bisimilar to $\nu k.\nu\ell.\overline{x}k.\overline{x}\ell.x(y).\tau$). Hence the server responding to k and the server responding to ℓ are indistinguishable to an external observer. Note this example is extracted from typical privacy problems in the applied π-calculus [2, 5, 6].

As a further example particular to quasi-open bisimilarity, observe the following process is quasi-open bisimilar to $[x \neq y]\tau$.

$$[x \neq y]([x \neq z]\tau + [y \neq z]\tau)$$

Notice that either x or y must be induced to be a private name, by the fresh name clause in quasi-open bisimulation; and either z is unified or not unified with the private name chosen. In all four scenarios one of the guards involving z is enabled.

2.3 The robustness of quasi-open bisimilarity

An essential property is that quasi-open bisimilarity is preserved by any context. For example, a notion of bisimilarity equating $[x \neq y]\tau$ and τ, **cannot** be a congruence, since these processes are distinguished by context $z(x).\{\,\cdot\,\} \parallel \overline{z}y$. Fortunately, having the insight to treat mismatches between variables intuitionistically, requiring constructive evidence of a mismatch, avoids this problem.

Theorem 2.3. *Quasi-open bisimilarity is a congruence.*

The above theorem has been mechanised using proof assistant Abella [4]. Details on the mechanisation appear in Section 4.

A barb represents the ability to observe an action on a channel. Barbs are typically used to define a notion called *barbed congruence* [14]. However, in the context of quasi-open bisimilarity an exact reference is *open barbed bisimilarity* [19]. Open barbed bisimilarity differs from barbed bisimilarity by closing by all contexts at every step. Here all transitions are in the empty environment.

Definition 2.4 (open barbed bisimilarity)**.** A process P has barb x, written $P{\downarrow}x$, whenever $P \xrightarrow{\overline{x}y} Q$, or $P \xrightarrow{\overline{x}(z)} Q$, or $P \xrightarrow{xy} Q$.

An open barbed bisimulation $\mathcal{R}$ is a symmetric relation over processes such that whenever $P \mathrel{\mathcal{R}} Q$ holds the following hold:

- For all contexts $C\{\}$, $C\{P\} \mathrel{\mathcal{R}} C\{Q\}$.
- If $P{\downarrow}x$ then $Q{\downarrow}x$.
- If $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $P' \mathrel{\mathcal{R}} Q'$ holds.

Open barbed bisimilarity is the greatest open barbed bisimulation.

The following result justifies the claim that our minimal extension of quasi-open bisimilarity, Definition 2.2, is canonical.

Theorem 2.5. *Quasi-open bisimilarity coincides with open barbed bisimilarity.*

The forward direction is a consequence of Theorem 2.3. The converse direction, shows each clause defining a quasi-open bisimulation can be induced by contexts. Thus, further to the established proof for quasi-open bisimilarity without mismatch [19], we need only construct contexts manufacturing fresh names.

Theorem 2.5 helps explain why some processes are not quasi-open bisimilar. Consider $\tau \not\sim [x = y]\tau + [x \neq y]\tau$ mentioned in the introduction. In the empty context, the former can perform a τ transition but the latter cannot perform any action. Hence the processes are not open barbed bisimilar and hence not quasi-open bisimilar. Note, in order for the branch with mismatch to act, we must close with a context such as $\nu y.\{\,\cdot\,\}$, forcing inequality $x \neq y$.

Situating quasi-open bisimilarity. It is easy to see that quasi-open bisimilarity is sound with respect to early bisimilarity. Early bisimilarity for processes extended with mismatch has been previously investigated [16]. In early bisimilarity, since all variables are distinct private names, a transition is always enabled for process $[x \neq y]\tau$. As mentioned above, consequently early bisimilarity is not a congruence — it must be artificially induced to be a congruence, yielding *early equivalence*. *Early equivalence* is well known [10, 19] to coincide with *barbed equivalence*.

Definition 2.6 (barbed equivalence)**.** A barbed bisimulation $\mathcal{R}$ is a symmetric relation over processes such that whenever $P \mathrel{\mathcal{R}} Q$ holds the following hold:

- If $P{\downarrow}x$ then $Q{\downarrow}x$.
- If $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $P' \mathrel{\mathcal{R}} Q'$ holds.

Barbed equivalence is defined to be the greatest congruence contained in the greatest barbed bisimulation.

Since any open barbed bisimulation is trivially a barbed bisimulation and a congruence, by Theorem 2.5, we have the following.

Corollary 2.7. *Quasi-open bisimilarity is sound with respect to barbed equivalence.*

The converse does not hold: $\tau + \tau.\tau$ and $\tau + \tau.[x \neq y]\tau + \tau.\tau$ are barbed congruent, but not quasi-open bisimilar.

As a sanity check, observe Definition 2.2 is conservative with respect to established definitions of quasi-open bisimulation without mismatch [18].

Proposition 2.8 (conservativity)**.** *For processes P and Q without mismatch, $P \sim Q$ iff P and Q are quasi-open bisimilar according to the original definition of quasi-open bisimulation [19].*

To see why the above holds, observe, for processes without mismatch: firstly, the open labelled transition systems, Fig. 1, coincides with the classic early labelled transition system for the π-calculus [13]; and, secondly, the additional clause manufacturing free names cannot disable any transition that was already enabled.

3 Intuitionistic modal logic $\mathcal{FM}$

In previous work [3], an intuitionistic modal logic called $\mathcal{OM}$ is proven to characterise open bisimilarity for the π-calculus (without mismatch). Here we present an intuitionistic version of the established modal logic $\mathcal{FM}$ (for $\mathcal{F}$ree input with $\mathcal{M}$atch [13]) that we prove to characterise quasi-open bisimilarity with mismatch.

A syntax of formulae is defined by the following grammar.

$$\begin{array}{rll} \phi ::= & \phi \wedge \phi \mid \phi \vee \phi \mid \phi \supset \phi \mid \mathtt{tt} \mid \mathtt{ff} \mid x = y & \} \text{ intuitionistic logic} \\ \mid & [\pi]\phi \mid \langle \pi \rangle \phi & \} \text{ modalities} \end{array}$$

In the syntax above, observe connectives cover the standard conjunction, disjunction, implication, top and bottom of intuitionistic logic with equalities. The two modalities box and diamond range over all observable actions. Observable actions π, as defined in Section 2.1, range over τ, free inputs, free outputs and bound outputs. Negative connectives and common constructs for Hennessy-Milner logic are defined by the following abbreviations.

$$\begin{array}{rr} \neg\phi \triangleq \phi \supset \mathtt{ff} & x \neq y \triangleq \neg(x = y) \\ [x = y]\phi \triangleq x = y \supset \phi & \langle x = y \rangle \phi \triangleq x = y \wedge \phi \\ [x \neq y]\phi \triangleq x \neq y \supset \phi & \langle x \neq y \rangle \phi \triangleq x \neq y \wedge \phi \end{array}$$

The semantics of intuitionistic $\mathcal{FM}$ is presented in Fig. 2. Satisfaction is defined as follows.

Definition 3.1. Process P satisfies formula ϕ, written $P \models \phi$, whenever, according to Fig. 2, $P \models^{\varnothing} \phi$ holds.

As standard for intuitionistic logic, there is no rule for bottom or equalities between distinct variables (there is no proof of the absurdity). Implication is interpreted intuitionistically by, as standard, checking that the implication holds in all *reachable worlds*. In this

$P \models^{\mathcal{N}} \mathtt{tt}$		always holds.
$P \models^{\mathcal{N}} x = x$		always holds.
$P \models^{\mathcal{N}} \phi_1 \wedge \phi_2$	iff	$P \models^{\mathcal{N}} \phi_1$ and $P \models^{\mathcal{N}} \phi_2$.
$P \models^{\mathcal{N}} \phi_1 \vee \phi_1$	iff	$P \models^{\mathcal{N}} \phi_1$ or $P \models^{\mathcal{N}} \phi_2$.
$P \models^{\mathcal{N}} \phi_1 \supset \phi_2$	iff	for any $\mathcal{M}$ and any σ respecting $\mathcal{N}$, we have $P\sigma \models^{\mathcal{M},\mathcal{N}} \phi_1\sigma$ implies $P\sigma \models^{\mathcal{M},\mathcal{N}} \phi_2\sigma$.
$P \models^{\mathcal{N}} \langle\alpha\rangle\phi$	iff	there exists Q such that $\mathcal{N} \colon P \xrightarrow{\alpha} Q$ and $Q \models^{\mathcal{N}} \phi$.
$P \models^{\mathcal{N}} \langle\overline{x}(z)\rangle\phi$	iff	there exists Q such that $\mathcal{N} \colon P \xrightarrow{\overline{x}(z)} Q$ and $Q \models^{\mathcal{N},z} \phi$.
$P \models^{\mathcal{N}} [\alpha]\phi$	iff	for any $Q, \mathcal{M}$ and any σ respecting $\mathcal{N}$, we have $\mathcal{M},\mathcal{N} \colon P\sigma \xrightarrow{\alpha\sigma} Q$ implies $Q \models^{\mathcal{M},\mathcal{N}} \phi\sigma$.
$P \models^{\mathcal{N}} [\overline{x}(z)]\phi$	iff	for any $Q, \mathcal{M}$ and any σ respecting $\mathcal{N}$, we have $\mathcal{M},\mathcal{N} \colon P\sigma \xrightarrow{\overline{x\sigma}(z)} Q$ implies $Q \models^{\mathcal{M},\mathcal{N},z} \phi\sigma$.

Figure 2. The semantics of intuitionistic modal logic $\mathcal{FM}$. Variable z is assumed to be fresh for bound output modalities.

setting a *world* is a pair consisting of set of names and a process, and reachability $\leq$ is defined such that:[1]

$\mathcal{N}, P \leq \mathcal{M}, Q$ whenever
$\quad\mathcal{N} \subseteq \mathcal{M}$ and, for some σ respecting $\mathcal{N}$, we have $P\sigma = Q$.

By the definition of implication, negation $0 \models^{\mathcal{N}} x = y \supset \mathtt{ff}$ holds only if there is no substitution respecting $\mathcal{N}$ unifying x and y (otherwise for some respectful σ, $x\sigma = y\sigma$, but $0 \models^{\mathcal{N}} \mathtt{ff}\sigma$ can never hold). Thus $0 \models^{\mathcal{N}} x = y \supset \mathtt{ff}$ coincides with the definition of entailment $\mathcal{N} \models x \neq y$ in Definition 2.1.

Like implication, modalities are assumed to hold in every reachable world. For the diamond modality the "all reachable worlds" proviso is redundant, since no respectful substitution or extra name distinction can disable a transition previously enabled. For the box modality, the "all reachable worlds" proviso is essential.

Observe that $[x \neq y]\tau \not\models \langle\tau\rangle\mathtt{tt}$, since, in the world with no assumptions about x and y, $[x \neq y]\tau$ cannot perform any actions. In contrast, $[x \neq y]\tau \models x \neq y \supset \langle\tau\rangle\mathtt{tt}$, by the following argument. All sets of names $\mathcal{N}$ such that $[x \neq y]\tau \models^{\mathcal{N}} x \neq y$ holds, are super sets of $\{x\}$ or $\{y\}$; therefore, for all such $\mathcal{N}$, we have $\mathcal{N} \colon [x \neq y]\tau \xrightarrow{\tau} 0$ and hence $[x \neq y]\tau \models^{\mathcal{N}} \langle\tau\rangle\mathtt{tt}$ holds, as required. In short, formula $[x \neq y]\langle\tau\rangle\mathtt{tt}$ reads "in all reachable worlds where x and y can never be equated, a τ transition is enabled."

3.1 Logically characterising quasi-open bisimilarity

The logical characterisation of quasi-open bisimulation is broken into a soundness and completeness result. Soundness states that if two processes are quasi-open bisimilar then they satisfy all the same formulae in intuitionistic $\mathcal{FM}$.

Theorem 3.2 (soundness)**.** *If $P \sim Q$, for all ϕ, $P \models \phi$ iff $Q \models \phi$.*

The proof of soundness proceeds by induction over the structure of formulae. The mechanisation in Abella is described in Section 4.

The interesting case is completeness. The contrapositive of completeness states: if two processes are not quasi-open bisimilar, then there is some formula that holds for one process but not the other process. For calculi such as the finite π-calculus with mismatch where quasi-open bisimulation is decidable, proving the contrapositive argument is sufficient to establish completeness.

Theorem 3.3 (completeness)**.** *If, for all ϕ, $P \models \phi$ iff $Q \models \phi$, $P \sim Q$.*

The next subsection explains the contrapositive to this theorem.

3.2 Distinguishing strategies and distinguishing formulae

We require a direct definition of "quasi-open non-bisimilarity" that holds whenever there is a distinguishing strategy in the quasi-open bisimulation game. Bisimulation is defined co-inductively; hence its dual definition "quasi-open non-bisimilarity" is defined inductively.

Definition 3.4 (quasi-open non-bisimilarity)**.** Inductively define the family of indexed relations $\not\sim_n$, for $n \in \mathbb{N}$. Base relation $\not\sim_0$ is the least symmetric relation such that $P \not\sim_0^{\mathcal{N}} Q$ whenever there exist process P', substitution σ respecting $\mathcal{N}$ and set of names $\mathcal{M}$ such that one of the following hold, where α is τ or $\overline{x}y$ or xy:

- $\mathcal{M},\mathcal{N} \colon P\sigma \xrightarrow{\alpha\sigma} P'$, and, for no Q', $\mathcal{M},\mathcal{N} \colon Q\sigma \xrightarrow{\alpha\sigma} Q'$.
- $\mathcal{M},\mathcal{N} \colon P\sigma \xrightarrow{\overline{x\sigma}(z)} P'$, where z is fresh for $P\sigma$, $Q\sigma$, $\mathcal{M}$ and $\mathcal{N}$, and there is no Q' such that $\mathcal{M},\mathcal{N} \colon Q\sigma \xrightarrow{\overline{x\sigma}(z)} Q'$.

Inductively, $\not\sim_{n+1}$ is the least symmetric relation extending $\not\sim_n$ such that $P \not\sim_{n+1}^{\mathcal{N}} Q$ whenever for some substitution σ respecting $\mathcal{N}$, and set of names $\mathcal{M}$, one of the following holds:

- $\mathcal{M},\mathcal{N} \colon P\sigma \xrightarrow{\alpha\sigma} P'$ and, for all Q_i, if $\mathcal{M},\mathcal{N} \colon Q\sigma \xrightarrow{\alpha\sigma} Q_i$, then we have $P' \not\sim_n^{\mathcal{M},\mathcal{N}} Q_i$.
- $\mathcal{M},\mathcal{N} \colon P\sigma \xrightarrow{\overline{a\sigma}(z)} P'$, and, for all Q_i and z fresh for $P\sigma$, $Q\sigma$, $\mathcal{M}$, $\mathcal{N}$, if $\mathcal{M},\mathcal{N} \colon Q\sigma \xrightarrow{\overline{a\sigma}(z)} Q_i$ then $P' \not\sim_n^{\mathcal{M},\mathcal{N},z} Q_i$.

The relation $\not\sim$, pronounced quasi-open non-bisimilarity, is defined to be the least relation containing $\not\sim_n$ for all $n \in \mathbb{N}$, i.e. $\bigcup_{n \in \mathbb{N}} \not\sim_n$, and $P \not\sim Q$ is defined as $P \not\sim^{\emptyset} Q$.

In the definition above, each stratum, indexed by n, contains all pairs of processes that can be distinguished by a strategy with depth at most n, i.e., at most n transitions are required to reach a world in which one process can move but the other cannot.

Given a strategy demonstrating that there is no quasi-open bisimulation containing a pair of processes, we can always construct a pair of distinguishing formulae in intuitionistic $\mathcal{FM}$.

Proposition 3.5 (distinguishing formulae)**.** *If $P \not\sim Q$ then there exists ϕ_L such that $P \models \phi_L$ and $Q \not\models \phi_L$, and also there exists ϕ_R such that $Q \models \phi_R$ and $P \not\models \phi_R$.*

The above proposition explicitly constructs two formulae: one biased to the left; another biased to the right. In contrast to classical modal logics where such formulae are de Morgan dual, in the intuitionistic setting, these formulae may be unrelated as illustrated by the following example.

Consider process $[x \neq y]\tau$ which is clearly not equivalent to 0. Now observe that $0 \models [\tau]\mathtt{ff}$ holds, since there is no world in which 0 can perform a τ transition; while $[x \neq y]\tau \not\models [\tau]\mathtt{ff}$, since there is a

[1] Note, for the π-calculus without mismatch, $\mathcal{M} = \mathcal{N}$ is sufficient in this definition.

"world" where $x \neq y$ and hence $[x \neq y]\tau$ can perform a τ transition. Hence $\left[\tau\right]\mathsf{ff}$ is a distinguishing formula biased to process 0. For a classical modal logic, we can simply negate a formula to obtain a distinguishing formula biased to $[x \neq y]\tau$. This construction **fails** in the intuitionistic setting, since $[x \neq y]\tau \not\models \neg\left[\tau\right]\mathsf{ff}$. The formula $\neg\left[\tau\right]\mathsf{ff}$ can be read as, "there is no world in which performing a τ transition is impossible." However, in the world where $x = y$, $([x \neq y]\tau)\{^{y}/_{x}\}$ indeed cannot perform a τ transition. The correct distinguishing formula biased to $[x \neq y]\tau$ is $\left[x \neq y\right]\left\langle\tau\right\rangle\mathsf{tt}$, i.e. whenever there is evidence that x and y are distinct, a τ transition is always enabled.

3.3 Examples of distinguishing formulae with mismatch

Since the proof of Proposition 3.5 is constructive, an algorithm generating distinguishing formulae for each pair of processes that are not quasi-open bisimilar can be extracted. We illustrate the result of applying this algorithm on examples of distinguished processes. Implementation details will appear in a companion paper.

Processes distinguished by early transition. Consider processes $\nu z.\overline{x}z.x(y).[z \neq y]\tau$ and $\nu z.\overline{x}z.x(y).\tau$ that are not quasi-open bisimilar. Both processes can perform actions $\overline{x}(z)$ and xz, to reach the pair of processes $[z \neq z]\tau \not\sim^{z} \tau$. Clearly, τ can perform a τ-transition but $[z \neq z]\tau$ is deadlocked. Thus, the following distinguishing formulae can be constructed:

$$\begin{aligned} \nu z.\overline{x}z.x(y).[z \neq y]\tau &\models \left[\overline{x}(z)\right]\left[xz\right]\left[\tau\right]\mathsf{ff} \\ \nu z.\overline{x}z.x(y).\tau &\models \left\langle\overline{x}(z)\right\rangle\left\langle xz\right\rangle\left\langle\tau\right\rangle\mathsf{tt} \end{aligned}$$

Processes distinguished by a specific world. Consider the following processes that are not quasi-open bisimilar.

$$[x \neq y]\tau.([y = z]\tau + [y \neq z]\tau) \not\sim [x \neq y]\tau.([x = z]\tau + [x \neq z]\tau)$$

In order to enable the first τ transitions, there are four (minimal) reachable worlds to consider, such that $x \neq y$.

- In the first two cases, we have private name x, and either $x = z$ or $x \neq z$ has been decided, depending on whether or not we apply substitution $\{^{z}/_{x}\}$ before introducing the private name x. Hence there are two sub scenarios:
  - In the case where $x = z$, since $x \neq y$, necessarily $y \neq z$.
  - In contrast, in the case where $x \neq z$, whether or not $y = z$ remains undecided. †
- There are two symmetric cases with private name y. In each sub-scenario, either $z = y$ or $z \neq y$ has been decided.

Notice, $y = z$ or $y \neq z$ is undecided only in scenario † above. Furthermore, in scenario †, we have $x \neq z$, and hence, in that world, $[x = z]\tau + [x \neq z]\tau$ can perform a τ transition. In contrast, $[y = z]\tau + [y \neq z]\tau$ cannot yet act with only private name x. Thus, assuming $x \neq y$, to force scenario †, we should also include $x \neq z$, leading to the following formulae distinguishing $[y = z]\tau + [y \neq z]\tau$ from $[x = z]\tau + [x \neq z]\tau$, respectively:

$$\left[\tau\right](y = z \vee y \neq z) \qquad \text{and} \qquad \left[x \neq z\right]\left\langle\tau\right\rangle$$

Assuming $x \neq y$, regardless of which of the four scenarios are chosen, each process above can be reached by a τ transition from the respective process below. Hence we can construct the corresponding distinguishing formulae.

$$[x \neq y]\tau.([y = z]\tau + [y \neq z]\tau) \models \left[\tau\right]\left[\tau\right](y = z \vee y \neq z)$$

$$[x \neq y]\tau.([x = z]\tau + [x \neq z]\tau) \models \left[x \neq y\right]\left\langle\tau\right\rangle\left[x \neq z\right]\left\langle\tau\right\rangle\mathsf{tt}$$

Note the above formulae would not be distinguishing in a classical setting with the law of excluded middle. Thus the use of an intuitionistic framework is necessary for this example.

Famous example demanding intuitionistic assumptions. Processes 0 and $[x \neq y]\tau$ are distinguished, since the latter can perform a τ action in a "world" where $x \neq y$, but the 0 can never perform a τ-transition. Thus we can constructing distinguishing formulae $0 \models \left[\tau\right]\mathsf{ff}$ and $[x \neq y]\tau \models \left[x \neq y\right]\left\langle\tau\right\rangle\mathsf{tt}$.

Processes τ and $[x \neq y]\tau$ are also distinguished, since τ can always perform a τ-transition, but $[x \neq y]\tau$ can only perform a τ-transition in worlds where $x \neq y$. This is also a base case of an algorithm for constructing distinguishing formulae, yielding $\tau \models \left\langle\tau\right\rangle\mathsf{tt}$ and $[x \neq y]\tau \models \left[\tau\right](x \neq y)$.

Now, consider $\tau + \tau.\tau \not\sim \tau + \tau.\tau + \tau.[x \neq y]\tau$ — a variant of a famous example [18]. The latter process can perform a τ-transition to reach process $[x \neq y]\tau$. However, the former process can only reach 0 or τ by a τ-transition. As noted above, neither 0 nor τ is quasi-open bisimilar to $[x \neq y]\tau$. Hence, by applying the inductive case of the algorithm, we can construct the following formulae from the conjunction and disjunction of the appropriate distinguishing formulae constructed above:

$$\begin{aligned} \tau + \tau.\tau &\models \left[\tau\right]\left(\left[\tau\right]\mathsf{ff} \vee \left\langle\tau\right\rangle\mathsf{tt}\right) \\ \tau + \tau.\tau + \tau.[x \neq y]\tau &\models \left\langle\tau\right\rangle.\left(\left[x \neq y\right]\left\langle\tau\right\rangle\mathsf{tt} \wedge \left[\tau\right](x \neq y)\right) \end{aligned}$$

Notably, if we exchange the above two processes and formulae, under classical assumptions, satisfiability would hold; and hence the above formulae would not distinguish the above processes. Thus the above example depends on interpreting $\mathcal{FM}$ in an intuitionistic meta-framework, i.e., without the law of excluded middle.

In the next section, we explain an embedding of a quasi-open bisimilarity and intuitionistic $\mathcal{FM}$ in the intuitionistic framework Abella. The embedding is used to formally mechanise theorems and examples in this work.

4 Mechanisation of Soundness in Abella

We describe the syntax for π-calculus and the logical specification of the labelled transition semantics and bisimilarity in Abella (Section 4.1), explain how the classical features of the quasi-open bisimulation is handled (Section 4.2), and briefly discuss the mechanisation of soundness theorems on quasi-open bisimilarity (Section 4.3) and the modal logic (Section 4.4).

4.1 Syntax, labelled transition steps, and bisimilarity

In Fig. 3, we define the syntax of process labels for the transition steps as Abella terms. Message in the π-calculus are atomic names, therefore, their type (`nm`) is declared without any term constructors. That is, they may either be globally declared or come from the name binding constructs (**⭣** and **𝝂**) of the π-calculus processes (`pr`). The constructors of `pr` are mostly formatted as bold faces of the symbols used in previous sections, except for input (**⭣**) and output (**⭡**) prefixes. For example, process $\nu y.([x{\neq}y]\overline{x}y \parallel x(z).[z{=}y]\tau)$ is transcribed as `(𝝂 y\ ‖ (≠ x y (⭡ x y)) (⭣ x z\ = z y (𝝉 𝟎)))` in Abella.

The constructors for labels (`lb`) are formatted as the non-bold symbols of the corresponding process constructors. Free-action labels τ, $\overline{x}y$, and xy are transcribed as `τ`, `↑x y`, and `↓x y`. A bound-output label $x(z)$ is transcribed as `z\↑x z`, or more simply as `↑x` by η-equivalence. Free and bound output labels share the same constructor (↑) but are distinguished by their types: `↑x y : lb` whereas

`↑x : nm →lb`. Accordingly, the transition rules are defined by two mutually inductive relations, 🡆 and ⇨, for free and bound steps. The corresponding transition-rule names in Fig. 1 from Section 2.1 are commented next to each definition clause of 🡆 and ⇨.

This style of logical specification for the pi-calculus and its characterizing modal logic has been used for studying properties of the late transition semantics and open bisimilarity [3, 20] – the key difference between the specification of early and late semantics is whether the input step is considered free or bound. Additionally, we specify the mismatch prefix (on lines 27-28 of Fig. 3), requiring at least one of the mismatching variables must be a private name (`name X ∨ name Y`), in addition to using the canonical intuitionistic negation via implication to absurdity (`X = Y → ⊥`). The coinductive definition of quasi-open bisimilarity is simpler than the Abella definition of open bisimilarity in previous work [3], in the sense that input actions are treated as other free actions.

```
1  Kind nm type. %%% names %%%%%%%%%%%%%%%
2  Kind pr type. %%% processes %%%%%%%%%%%
3  Type 𝛕        pr → pr.
4  Type 🠕        nm → nm → pr → pr.
5  Type 🠗        nm → (nm → pr) → pr.
6  Type +, ‖     pr → pr → pr.
7  Type 𝟎        pr.
8  Type 𝛎        (nm → pr) → pr.
9  Type =, ≠     nm → nm → pr → pr.
10 Kind lb type. %%% labels %%%%%%%%%%%%%
11 Type τ        lb.            % silent progress
12 Type ↑, ↓     nm → nm → lb.  % input and output
13
14 % a standard idiom requiring a variable be ∇-quantified
15 Define name : nm → prop  by  ∇ x, name x.
16
17 Define 🡆 : pr → lb → pr → prop                % free step
18      , ⇨ : pr → (nm → lb) → (nm → pr) → prop % bound step
19 by 🡆 (𝛕 P) τ P              % internal step (Act)
20  ; 🡆 (🠗 X P) (↓ X Y) (P Y)  % free input  (Inp)
21  ; 🡆 (🠕 X Y P) (↑ X Y) P    % free output (Act)
22  %% core process algebra for 🡆 ((*-r) rules omitted)
23  ; 🡆 (+ P Q) L R :=  🡆 P L R % (Choice-l)
24  ; 🡆 (‖ P Q) L (‖ R Q) :=  🡆 P L R % (Par-l)
25  ; 🡆 (𝛎 P) L (𝛎 Q) := ∇ x, 🡆 (P x) L (Q x) % (Res)
26  ; 🡆 (= X X P) L Q := 🡆 P L Q % (Mat)
27  ; 🡆 (≠ X Y P) L Q := % (Mismatch)
28         (name X ∨ name Y) ∧ (X = Y → ⊥) ∧ (🡆 P L Q)
29  %% communications
30  ; 🡆 (‖ P Q) τ (‖ PP QQ) :=                % (Comm)
31       (∃ X Y, 🡆 P (↓ X Y) PP ∧ 🡆 Q (↑ X Y) QQ)
32     ∨ (∃ X Y, 🡆 P (↑ X Y) PP ∧ 🡆 Q (↓ X Y) QQ)
33  ; 🡆 (‖ P Q) τ (𝛎 y\ ‖ (PP y) (QQ y)) :=  % (Close)
34       (∃ X, ⇨ Q (↑ X) QQ ∧ ∇ y, 🡆 P (↓ X y) (PP y))
35     ∨ (∃ X, ⇨ P (↑ X) PP ∧ ∇ y, 🡆 Q (↓ X y) (QQ y))
36   % bound output
37  ; ⇨ (𝛎 P) (↑ X) R := ∇ y, 🡆 (P y) (↑ X y) (R y) % (Act)
38  %% core process algebra for ⇨  (omitted)
39  /* (Choice-l), (Choice-r), (Par-l), (Par-r), (Mat), (Mismatch), and
40   (Res) for ⇨ are similar to those cases for 🡆 */ .
41
42 Theorem quasi-em : % The axiom of Quasi-Excluded Middle
43   ∀ (w : nm), ∇ x, (x = w) ∨ (x = w → ⊥).
44 skip. % Not a provable theorem but provided as an axiom
45
46 CoDefine q~ : pr → pr → prop
47 by q~ P Q
48    := (∀ L P₁, 🡆 P L P₁ →
49          ∃ Q₁, 🡆 Q L Q₁ ∧ q~ P₁ Q₁)
50    ∧ (∀ X P₁, ⇨ P (↑ X) P₁ →
51          ∃ Q₁, ⇨ Q (↑ X) Q₁ ∧ ∇ z, q~ (P₁ z) (Q₁ z))
52    ∧ /* ··· free step lead by Q omitted ··· */
53    ∧ /* ··· bound step lead by Q omitted ··· */ .
```

Figure 3. The syntax for processes (`pr`) and labels (`lb`) defined as terms in Abella, an inductive definition of the early labelled transition semantics (🡆, ⇨) for the finite π-calculus, the axiom of Quasi-Excluded Middle (`quasi-em`), and the coinductive definition of the quasi-open bisimilarity (`q~`).

4.2 Quasi-excluded middle for private names

The ∇-quantifier guarantees freshness from all previously introduced variables, ensuring mismatch against already known names to succeed (e.g., $\nu k.([x \neq k]\tau) \xrightarrow{\tau} 0$). However, it does not provide the classical properties on extruded private names, as required in quasi-open bisimulation, because Abella’s logic is intuitionistic. In particular, (mis)matching an input variable against an extruded name, e.g., $\nu k.\overline{a}k.a(x).[x = k]\tau$, can neither be satisfied nor be falsified in Abella because the input variable x is to be introduced *after* the private name k. To remedy this, we provide the axiom of *Quasi-Excluded Middle* (`quasi-em`), which empowers private names with the excluded middle for testing equality against any name.

Although `quasi-em` is applicable to any ∇-introduced names, not all private names become available to invoke the axiom during bisimulation steps but only those extruded by bound outputs. For example, one can prove in Abella

```
∀ a b y L P Q,
  🡆 (𝛎 x\ + (= x y (🠕 a y P)) (≠ x y (🠕 b y P))) L Q
    → L = (↑ b y)
```

which shows that only the mismatch guard is enabled. This suggests that the quasi-excluded middle does not affect the static scoping of names that are not extruded.

Interestingly, the bisimulation congruences are distinguished from their classical counterparts by the degree of availability regarding the excluded middle over name equalities. Tiu and Miller [20] discovered that a logical specification for late bisimilarity can be obtained from the specification of open bisimilarity just by enabling the excluded middle for arbitrary names. Similarly, we notice that a logical specification for early bisimilarity can be obtained from the specification of quasi-open bisimilarity by requiring all free names of processes be ground (i.e., `∀x, name x.` holds) so that the quasi-excluded middle become applicable everywhere.

4.3 Theorems on quasi-open bisimilarity

The equivalence theorems (reflexivity, symmetry, and transitivity) and most of the congruence theorems (closure under each `pr` constructor) are provable by straightforward coinduction. Showing congruence under parallel composition needs some extra steps due to bound communications (Close-l and -r). We prove congruence under ‖, adopting the method demonstrated in one of the π-calculus examples distributed with Abella, by defining an auxiliary inductive relation over both ‖ and 𝛎, and showing that the relation is closed under each bisimulation step. Some closure properties (for $\boldsymbol{\tau}$, ↓, and ↑) are bijective. In particular, the bijective closure property for input prefixes, `(∀Y, q~ (P Y) (Q Y)) ↔ q~ (↓ X P) (↓ X Q)`, is useful for generalizing coincidences of quasi-open bisimilarity with the logical equivalence (Section 4.4) to processes with arbitrary number of free variables.

4.4 Mechanisation of the modal logic

Fig. 4 defines the syntax and semantics of the intuitionistic $\mathcal{FM}$ in Abella. The definition is similar to the Abella definition in previous work on $\mathcal{OM}$, except the input action is free rather than bound.

Soundness (Theorem 3.2) is fully mechanised in Abella. Once `q~_sat`$_L$ in Fig. 4 is established, `q~_sat`$_R$ is a corollary of `q~_sat`$_L$ by `q~-sym`. Then, `q~_sat` is immediate from `q~_sat`$_L$ and $_R$. We prove `q~_sat`$_L$ by induction on the satisfaction derivation (`sat P F`).

Completeness (Theorem 3.3) is partly mechanised with a gap in establishing Proposition 3.5, which correspond to `sateq_➡`$_{L\text{ (and }R)}$ and `sateq_⇨`$_{L\text{ (and }R)}$ in Fig. 4. Once we assume that logical equivalence is closed under common transition steps, it is not difficult to prove `sat_q~` by coinduction. A sub-property of these closedness lemmas, logically equivalent processes must share the same transition step, stated by `sateq_➡∃`$_{L\text{ (and }R)}$ and `sateq_⇨∃`$_{L\text{ (and }R)}$, is mechanised. That is, if a process can make a step, the other process can also make a corresponding step with the same label.

Theorems `sat_q~` and `q~_sat` can be generalized to arbitrary number of free variables in Abella. That is, the following has been proven, where $\{x_1, \cdots, x_n\} = \mathrm{fv}(\mathtt{P}) \cup \mathrm{fv}(\mathtt{Q})$.

```
(∀x1···xn, q~ P Q)  ↔  (∀x1···xn, (∀F, sat P F ↔ sat Q F))
```

```
Type tt, ff                 o′ .
Type Υ, ⅄                   o′ → o′ → o′ .
Type □=, ◇=, □≠, ◇≠        nm → nm  → o′ → o′ .
Type □, ◇                   lb → o′ → o′ .
Type □↑, ◇↑                 nm → (nm → o′) → o′ .

Define sat : pr → o′ → prop       % sat P ϕ corresponds to
by sat P tt                       % P ⊨ ϕ in Section 3.
 ; ... % clauses for Υ, ⅄, □=, □≠, ◇≠, □, ◇ omitted
 ; sat P (□↑X A) :=
         ∀ Q, (⇨ P (↑ X) Q)  →  ∇ z, sat (Q z) (A z)
 ; sat P (◇↑X A) :=
         ∃ Q, (⇨ P (↑ X) Q)  ∧  ∇ z, sat (Q z) (A z).

Theorem q~_sat_L: ∀ P Q F, q~ P Q → sat P F → sat Q F.
Theorem q~_sat_R: ∀ P Q F, q~ P Q → sat Q F → sat P F.
Theorem q~_sat : ∀ P Q F, q~ P Q → (sat P F ↔ sat Q F).

Theorem sateq_➡∃_L: ∀ P Q A P1, (∀ F, sat P F ↔ sat Q F)
       → (➡ P A P1) → ∃ Q1, (➡ Q A Q1).
Theorem sateq_⇨∃_L: ···. % similar to above
Theorem sateq_➡_L : ∀ P Q A P1, (∀ F, sat P F ↔ sat Q F)
       → (➡ P A P1) → ∃ Q1, (➡ Q A Q1)
                                ∧ (∀ F, sat P1 F ↔ sat Q1 F).
Theorem sateq_⇨_L : ···. % similar to above
Theorem sat_q~ : ∀ P Q, (∀F, sat P F ↔ sat Q F) → q~ P Q.
```

Figure 4. The definition of intuitionistic $\mathcal{FM}$ in Abella and its properties on bisimilarity and logical equivalence (`q~_sat` for soundness and `sat_q~` for completeness) along with their key lemmas; $A \leftrightarrow B$ is an abbreviation for $(A \rightarrow B \wedge B \rightarrow A)$.

The above theorem makes use of the following closure property for inputs (proven in Abella), in addition to the closure property for inputs already mentioned in Section 4.3.

```
   (∀ F Y, sat   (P Y) F ↔ sat   (Q Y) F)
↔ (∀ F,  (sat (↓ X P) F ↔ sat (↓ X Q) F).
```

We emphasise, although `q~_sat` is not fully mechanised, the missing proposition has been manually checked. Furthermore, the proof is constructive, hence yields an algorithm constructing distinguishing formulae, which has been implemented.

5 What about open bisimilarity?

For the π-calculus without mismatch, the original definition of open bisimilarity [18] is strictly finer than quasi-open bisimilarity. For quasi-open bisimilarity there is a canonical extension handling mismatch, since there is an absolute reference point — open barbed bisimilarity — that quasi-open bisimilarity coincides with (Theorem 2.5). In contrast, an extension of open bisimilarity with mismatch must satisfy the following more complex criteria, that many subtle variants of open bisimilarity satisfy.

1. Conservative: for π-calculus processes without mismatch, the extension of open bisimilarity should coincide with the original definition of open bisimilarity [18].
2. Congruent: the extension of open bisimilarity should be a congruence, hence sound with respect to open barbed bisimilarity (Definition 2.4).
3. Late: the extension of open bisimilarity should be sound with respect to late bisimilarity with mismatch [16].

To help select a definition of open bisimilarity from several reasonable choices, we introduce a further criteria. In order for open bisimulation to be suitable for verifying privacy properties, we require the following two processes to be equivalent.

$$\nu k.\nu \ell.\overline{x}k.\overline{x}\ell.x(y).([k = y]\tau + [k \neq y]\tau)$$

$$\nu k.\nu \ell.\overline{x}k.\overline{x}\ell.x(y).([\ell = y]\tau + [\ell \neq y]\tau)$$

As mentioned in Section 2.2, the above example contains the essence of privacy properties in the applied π-calculus.

To define open bisimilarity we require an open version of the late labelled transitions system in Fig. 5 and the notion of a *history*.

Definition 5.1 (history). A *history* is defined by the following grammar: $h \coloneqq \epsilon \mid h \cdot x^o \mid h \cdot x^i$. Substitution σ *respects* history h

$$\frac{z \notin \mathrm{n}(h)}{h\colon x(z).P \xrightarrow{x(z)} P}\ \textsc{Inp} \qquad \frac{h\colon P \xrightarrow{x(z)} Q \quad z \notin \mathrm{fv}(R)}{h\colon P \parallel R \xrightarrow{x(z)} Q \parallel R}\ \textsc{Par-l}$$

$$\frac{h \cdot z^o\colon P \xrightarrow{\pi} Q \quad z \notin \mathrm{n}(h) \cup \mathrm{n}(\pi)}{h\colon \nu z.P \xrightarrow{\pi} \nu z.Q}\ \textsc{Res}$$

$$\frac{h\colon P \xrightarrow{\overline{x}(z)} P' \quad h\colon Q \xrightarrow{x(z)} Q'}{h\colon P \parallel Q \xrightarrow{\tau} \nu z.\left(P' \parallel Q'\right)}\ \textsc{Close-l}$$

$$\frac{h\colon P \xrightarrow{\overline{x}y} P' \quad h\colon Q \xrightarrow{x(z)} Q'}{h\colon P \parallel Q \xrightarrow{\tau} P' \parallel Q'\left\{{}^{y}\!/\!{}_{z}\right\}}\ \textsc{Comm-l}$$

Figure 5. Rules for open late labelled transitions. All other rules are as for open early labelled transitions in Fig. 1, except all rules carry a history h instead of a set of names.

whenever for all h' and h'' such that $h = h' \cdot x^o \cdot h''$, $\sigma x = x$ and $y \in \mathrm{fv}(h')$ implies $x \neq y\sigma$. *Entailment* $h \models x \neq y$ holds whenever there is no σ respecting h such that $x\sigma = y\sigma$.

Entailment, used to resolve mismatch, is as defined earlier, except with respect to histories rather than of sets of names. For example, $x^i \cdot y^o \models x \neq y$, since history $x^i \cdot y^o$ represents that x was input before y was output. This leads us to the following definition of open bisimulation, satisfying all the above criteria.

Definition 5.2 (open bisimilarity)**.** A symmetric relation indexed by an environment $\mathcal{R}$ is an open bisimulation whenever, if $P \mathrel{\mathcal{R}^h} Q$ the following hold:

- If σ respects h, then $P\sigma \mathrel{\mathcal{R}^{h\sigma}} Q\sigma$.
- For any history h' we have $P \mathrel{\mathcal{R}^{h'\cdot h}} Q$.
- If $h\colon P \xrightarrow{\alpha} P'$, there exists Q' such that $h\colon Q \xrightarrow{\alpha} Q'$ and $P' \mathrel{\mathcal{R}^h} Q'$, where α is of the form τ or $\overline{x}y$.
- If $h\colon P \xrightarrow{x(z)} Q'$, where z is fresh for P, Q and h, then there exists Q' such that $h\colon Q \xrightarrow{x(z)} Q'$ and $P' \mathrel{\mathcal{R}^{h\cdot x^i}} Q'$.
- If $h\colon P \xrightarrow{\overline{x}(z)} P'$, where z is fresh for P, Q and h, then there exists Q' such that $h\colon Q \xrightarrow{\overline{x}(z)} Q'$ and $P' \mathrel{\mathcal{R}^{h\cdot x^o}} Q'$.

Open bisimilarity $\sim_o$ is defined such that $P \sim_o Q$ holds whenever there exists open bisimulation $\mathcal{R}$ such that $P \mathrel{\mathcal{R}^{x_1^i \cdot x_2^i \cdot \ldots \cdot x_n^i}} Q$ holds, where $\mathrm{fv}(P) \cup \mathrm{fv}(Q) \subseteq \{x_1, x_2, \ldots, x_n\}$.

The only difference compared to the standard definition of open bisimilarity is the second clause allowing histories to be extended in the past (there can be some extra activity before the first input or output action). This additional clause provides distinguishing power required to resolve mismatches, while at the same time being sufficiently coarse to respect the above privacy example.

Consider an example demonstrating the necessity of the additional clause to ensure open bisimilarity is a congruence. The following process are distinguished by open bisimilarity.

$$[x \neq y]\tau.\big(\,[z \neq x]([z{=}y]\tau + [z{\neq}y]\tau) + [z \neq y]([z{=}x]\tau + [z{\neq}x]\tau)\,\big)$$

$$[x \neq y]\tau.\big([z \neq x]\tau + [z \neq y]\tau\big)$$

The two weakest histories enabling $x \neq y$ are $x^i \cdot y^o$ and $y^i \cdot x^o$. Under either history, both process can perform a τ transition to reach the following pair of processes.

$$[z \neq x]([z = y]\tau + [z \neq y]\tau) + [z \neq y]([z = x]\tau + [z \neq x]\tau)$$

$$[z \neq x]\tau + [z \neq y]\tau$$

Without loss of generality, consider history prefix $y^i \cdot x^o$. At this point there is the possibility of prefixing the history further with z^i, at which point $z^i \cdot y^i \cdot x^o \models z \neq x$ holds and hence the second process above can perform a τ transition. In contrast, given history $z^i \cdot y^i \cdot x^o$, it remains undecided whether $z = y$ or $z \neq y$ and hence the first process above cannot yet perform a τ transition. Thus the processes are distinguished.

Notice that the prefixed history $z^i \cdot x^i \cdot y^o$ can be enforced by closing the initial processes by the context $w(z).w(y).\nu x.\overline{w}x.\,\{\,\cdot\,\}$. Under this context the former process can perform one τ-transition, but the latter process can perform two τ-transitions. Thus, without the clause pre-pending histories, open bisimilarity would not be a congruence.

By the above argument, any congruence extending open bisimilarity must have an extension with at least the discriminating power offered by the clause pre-pending histories. Since that clause is the only extension that we make to the standard definition of open bisimilarity we have the following.

Proposition 5.3. *Definition 5.2 is the coarsest notion of bisimilarity satisfying the criteria at the top of this section.*

Thus Def. 5.2 is a canonical conservative extension of open bisimilarity with mismatch, even if other definitions are possible.

Open bisimilarity as defined is indeed a congruence and hence sound with respect to open barbed congruence. Hence, appealing to Theorem 2.5, we have the following.

Corollary 5.4. *Open bisimilarity is sound with respect to quasi-open bisimilarity.*

To extend the characteristic modal logic $\mathcal{OM}$ to handle mismatch, we simply extend $\mathcal{OM}$ [3] according a Kripke semantics where $h, P \leq h', Q$ whenever for some σ respecting h and some history h'' we have $P\sigma = Q$ and $h'' \cdot h\sigma = h'$. Notice that entailment $h \models x \neq y$ is simply $0 \models^h x = y \supset \mathtt{ff}$ according to the Kripke semantics of $\mathcal{OM}$; hence for both open and quasi-open bisimilarity mismatch is treated as an intuitionistic negation, just under different intuitionistic logics ($\mathcal{OM}$ and $\mathcal{FM}$ respectively).

To illustrate a difference between $\mathcal{OM}$ and intuitionistic $\mathcal{FM}$, observe that we have the following in $\mathcal{OM}$.

$$\nu x.\overline{z}x.z(y).\tau \models \big\langle \overline{z}(x) \big\rangle \big\langle z(y) \big\rangle \big\langle \tau \big\rangle \mathtt{tt}$$

$$\nu x.\overline{z}x.z(y).([x \neq y]\tau + [x = y]\tau) \not\models \big\langle \overline{z}(x) \big\rangle \big\langle z(y) \big\rangle \big\langle \tau \big\rangle \mathtt{tt}$$

In contrast, in $\mathcal{FM}$, there is no distinguishing formula for the above processes. In contrast to quasi-open bisimilarity, even the coarsest open bisimilarity (Def. 5.2) distinguishes the following processes.

$$\nu x.\overline{z}x.z(y).\tau \qquad \not\sim_o \qquad \nu x.\overline{z}x.z(y).([x \neq y]\tau + [x = y]\tau)$$

This does not prevent open bisimilarity being used for proving privacy properties. However, it does mean more care is required than when modelling privacy properties using quasi-open bisimilarity.

6 Related work on quasi-open bisimilarity

Alternative approaches to open and quasi-open bisimulation with mismatch have been studied previously. However, the semantics in this paper resolves limitations of previous work [7, 8]. Crucially, previous approaches assume $[x \neq y]\tau$ and τ are indistinguishable; hence such definitions cannot define a congruence, as observed in the introduction.

Our work, lifts to the weak open barbed bisimilarity, permitting multiple τ transitions at each step. According to our semantics, processes P and Q, defined below, are **not** weak open barbed bisimilar.

$$\begin{aligned} P &\triangleq w(x).(\overline{w}w + [x = y]\tau.\overline{y}y) + w(x).(\overline{z}z + [x \neq y]\tau.\overline{y}y) \\ Q &\triangleq P + w(x).\overline{y}y \end{aligned}$$

To distinguish P from Q, consider context $C\{\,\cdot\,\} \triangleq \overline{w}x \parallel \{\,\cdot\,\}$. Now $C\{Q\} \xrightarrow{\tau} \overline{y}y$, but from $C\{P\}$, we cannot find any series of τ transitions to a state equivalent to $\overline{y}y$. In contrast, previous work [7, 8] claims the above processes are progressing quasi-open barbed bisimilar. The argument in previous work [7, 8] either: relies on the law of excluded middle for name equality ($C\{P\}$ can reach $\overline{y}y$, assuming either $x = y$ or $x \neq y$); or assumes mismatches with distinct variables can always be resolved. However, if we assume the law of excluded middle, or allow mismatch on distinct variables, open bisimulation fails to be a congruence. The resolution suggested in that related line of work is to artificially take the coarsest congruence contained in their proposed definition of quasi-open bisimilarity. In contrast, Definition 2.2 is already a congruence.

Note, in the weak setting, weak open barbed bisimilarity, coincides with progressing quasi-open bisimilarity, where each τ transition must be simulated by at least one τ transition. This problem was observed in classic work on CCS [15].

7 Conclusion

In the title we state: "quasi-open bisimilarity with mismatch is intuitionistic." This title refers to the following intertwined observations. In order for quasi-open bisimilarity to define a congruence, mismatch must be interpreted by intuitionistic negation, as in Definition 2.1; but not any intuitionistic negation; specifically, $x = y \supset \mathtt{ff}$ in the modal logic characterising quasi-open bisimilarity. That intuitionistic modal logic is based on a Kripke semantics extracted from the established definition of quasi-open bisimilarity [19]. Extending labelled transitions with an intuitionistic mismatch, in Fig. 1, allows open barbed bisimilarity, Def. 2.4, for the π-calculus with mismatch to be defined. Open barbed bisimilarity is used as a canonical reference point to extend quasi-open bisimilarity to handle mismatch leading to Def. 2.2. In turn, the extension of quasi-open bisimilarity leads to an extended Kripke semantics; and thereby the characteristic intuitionistic modal logic $\mathcal{FM}$ given in Fig. 2. Thus, not only is mismatch itself defined using intuitionistic negation, but also quasi-open bisimilarity is characterised by a (new) intuitionistic modal logic.

Although quasi-open bisimilarity is less famous than open bisimilarity, it is a natural choice of bisimulation congruence, situated between open bisimilarity and early equivalence as shown in Fig. 6. Open bisimilarity with mismatch (Def. 5.2) is also intuitionistic, but defined with respect to a different intuitionistic modal logic (a slight extension of $\mathcal{OM}$ in previous work [3]). As with quasi-open bisimilarity, the MISMATCH rule for open bisimilarity is defined as $x = y \supset \mathtt{ff}$, but in the intuitionistic logic $\mathcal{OM}$.

Most of this paper focuses on quasi-open bisimilarity due to the following properties that do not hold for open bisimilarity: firstly, there is a canonical extended definition of quasi-open bisimilarity handling mismatch; secondly, the classical variant of $\mathcal{FM}$ characterises an established classical bisimilarity (early bisimilarity [13]); thirdly, less machinery is required to define quasi-open bisimilarity. There is also a practical motivation for quasi-open bisimilarity: it correctly handles typical privacy properties. This contrasts to open bisimilarity, for which extra care is required in order to handle privacy properties.

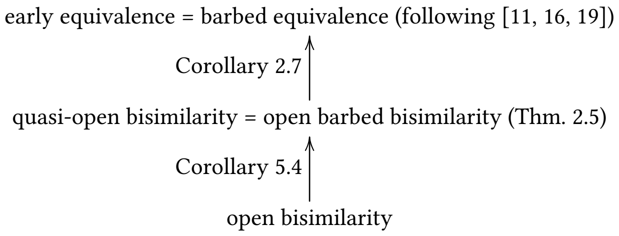
early equivalence = barbed equivalence (following [11, 16, 19])
Corollary 2.7
quasi-open bisimilarity = open barbed bisimilarity (Thm. 2.5)
Corollary 5.4
open bisimilarity

Figure 6. Summary of results comparing congruences for the π-calculus with mismatch.

A logical embedding of quasi-open bisimilarity in Abella, is used to mechanise soundness theorems and examples in this work. The mechanisation itself[2] is novel in how private names are handled. Indeed, the novelty of the techniques triggered untested features of Abella exposing a bug[3] in the implementation of the proof assistant. Additionally, a bisimulation checking algorithm following our constructive proof structure has been implemented in Haskell.[4]

As future work, we propose our extension of quasi-open bisimilarity as a reference specification for equivalence checkers. Furthermore, we propose the intuitionistic modal logic characterising quasi-open bisimilarity as a foundation for symbolic model checking invariant with respect to quasi-open bisimilarity.

Acknowledgements. We are grateful to Fu Yuxi and Björn Victor for sharing their insight into key examples.

References

[1] Martín Abadi, Bruno Blanchet, and Cédric Fournet. 2018. The Applied Pi Calculus: Mobile Values, New Names, and Secure Communication. *J. ACM* 65, 1 (2018), 1–41. https://doi.org/10.1145/3127586

[2] Martín Abadi and Cédric Fournet. 2004. Private authentication. *Theoretical Computer Science* 322, 3 (2004), 427 – 476. https://doi.org/10.1016/j.tcs.2003.12.023

[3] Ki Yung Ahn, Ross Horne, and Alwen Tiu. 2017. A Characterisation of Open Bisimilarity using an Intuitionistic Modal Logic. In *Proc. CONCUR 2017 (LIPIcs)*, Vol. 85. 7:1–7:17. https://doi.org/10.4230/LIPIcs.CONCUR.2017.7

[4] David Baelde, Kaustuv Chaudhuri, Andrew Gacek, Dale Miller, Gopalan Nadathur, Alwen Tiu, and Yuting Wang. 2014. Abella: A System for Reasoning about Relational Specifications. *J. Formalized Reasoning* 7, 2 (2014), 1–89. https://doi.org/10.6092/issn.1972-5787/4650

[5] Vincent Cheval, Hubert Comon-Lundh, and Stéphanie Delaune. 2017. A procedure for deciding symbolic equivalence between sets of constraint systems. *Inf. and Comput.* 255, Part 1 (2017), 94 – 125. https://doi.org/10.1016/j.ic.2017.05.004

[6] V. Cortier and B. Smyth. 2011. Attacking and Fixing Helios: An Analysis of Ballot Secrecy. In *2011 IEEE 24th Computer Security Foundations Symposium*. 297–311. https://doi.org/10.1109/CSF.2011.27

[7] Yuxi Fu. 2005. On quasi-open bisimulation. *Theor. Comput. Sci.* 338, 1-3 (2005), 96–126. https://doi.org/10.1016/j.tcs.2004.10.041

[8] Yuxi Fu and Zhenrong Yang. 2003. Tau laws for pi calculus. *Theoretical Computer Science* 308, 1 (2003), 55–130. https://doi.org/10.1016/S0304-3975(03)00202-0

[9] M. Hennessy and R. Milner. 1985. Algebraic Laws for Nondeterminism and Concurrency. *JACM* 32, 1 (1985), 137–161. https://doi.org/10.1145/2455.2460

[10] M. Johansson, J. Bengtson, J. Parrow, and B. Victor. 2010. Weak Equivalences in Psi-Calculi. In *2010 25th Annual IEEE Symposium on Logic in Computer Science*. 322–331. https://doi.org/10.1109/LICS.2010.30

[11] Magnus Johansson, Björn Victor, and Joachim Parrow. 2012. Computing strong and weak bisimulations for psi-calculi. *The Journal of Logic and Algebraic Programming* 81, 3 (2012), 162–180. https://doi.org/10.1016/j.jlap.2012.01.001

[12] Dale Miller and Alwen Tiu. 2005. A Proof Theory for Generic Judgments. *ACM Trans. Comput. Logic* 6, 4 (2005), 749–783. https://doi.org/10.1145/1094622.1094628

[13] Robin Milner, Joachim Parrow, and David Walker. 1993. Modal Logics for Mobile Processes. *Theoretical Computer Science* 114, 1 (1993), 149–171. https://doi.org/10.1016/0304-3975(93)90156-N

[14] Robin Milner and Davide Sangiorgi. 1992. *Barbed bisimulation*. Springer, Berlin, Heidelberg, 685–695. https://doi.org/10.1007/3-540-55719-9_114

[15] Ugo Montanari and Vladimiro Sassone. 1992. Dynamic congruence vs. progressing bisimulation for CCS. *Fundamenta informaticae* 16, 2 (1992), 171–199.

[16] Joachim Parrow and Davide Sangiorgi. 1995. Algebraic Theories for Name-Passing Calculi. *Information and Computation* 120, 2 (1995), 174 – 197. https://doi.org/10.1006/inco.1995.1108

[17] Joachim Parrow and Björn Victor. 1998. The Fusion Calculus: Expressiveness and Symmetry in Mobile Processes. In *Proc. LICS 1998*. IEEE Computer Society, 176–185. https://doi.org/10.1109/LICS.1998.705654

[18] Davide Sangiorgi. 1996. A theory of bisimulation for the π-calculus. *Acta Informatica* 33, 1 (01 Feb 1996), 69–97. https://doi.org/10.1007/s002360050036

[19] Davide Sangiorgi and David Walker. 2001. *On Barbed Equivalences in π-Calculus*. Springer, Berlin, Heidelberg, 292–304. https://doi.org/10.1007/3-540-44685-0_20

[20] Alwen Tiu and Dale Miller. 2010. Proof Search Specifications of Bisimulation and Modal Logics for the π-calculus. *ACM Trans. Comput. Logic* 11, 2, Article 13 (2010), 35 pages. https://doi.org/10.1145/1656242.1656248

[2] The mechanisation is available available at: https://github.com/kyagrd/NonBisim2DF

[3] issue #96, resolved in Abella 2.0.5 distribution

[4] https://github.com/kyagrd/hs-picalc-unbound-example/tree/quasi