A Logical Viewpoint on Process-Algebraic Quotients

Antonín Kučera*
Faculty of Informatics
Masaryk University
Botanická 68a, 60200 Brno
Czech Republic
tony@fi.muni.cz

Javier Esparza†
Institut for Informatics
Technical University Munich
Arcisstr. 21, D-80290 Munich
Germany
esparza@in.tum.de

Abstract

We study the following problem: Given a transition system $\mathcal{T}$ and its quotient $\mathcal{T}/\!\sim$ under an equivalence $\sim$, which are the sets $\mathcal{L}$, $\mathcal{L}'$ of Hennessy-Milner formulae such that: if $\varphi \in \mathcal{L}$ and $\mathcal{T}$ satisfies φ, then $\mathcal{T}/\!\sim$ satisfies φ; if $\varphi \in \mathcal{L}'$ and $\mathcal{T}/\!\sim$ satisfies φ, then $\mathcal{T}$ satisfies φ.

1 Introduction

One of the main problems of automatic formal verification is that processes typically have a very large or even infinite state space. Formally, *processes* are understood as (being associated with) states in *transition systems*, a general and widely accepted model of systems with dynamics. Let $Act = \{a, b, c, \dots\}$ be a countably infinite set of *atomic actions* (which is fixed for the rest of this paper).

Definition 1 A transition system (T.S.) is a triple $\mathcal{T} = (S, \mathcal{A}, \rightarrow)$ where S is a set of *states* (or *processes*), $\mathcal{A} \subseteq Act$ a finite set of actions, and $\rightarrow \subseteq S \times \mathcal{A} \times S$ is a *transition relation*. We say that $\mathcal{T}$ is *image-finite* iff for all $s \in S$, $a \in \mathcal{A}$ the set $\{t \mid s \xrightarrow{a} t\}$ is finite.

In the rest of this paper we only consider image-finite transition systems. The reason is that the majority of studied process formalisms (like process algebras, Petri nets, pushdown automata, etc.) only define processes of image-finite transition systems. Moreover, common process equivalences admit a modal characterization in Hennessy-Milner logic (see below) only on the restricted class of image-finite processes (i.e., processes of image-finite transition systems).

As usual, we write $s \xrightarrow{a} t$ instead of $(s, a, t) \in \rightarrow$ and we extend this notation to elements of $\mathcal{A}^*$ in the standard way. A state t is *reachable* from a state s iff $s \xrightarrow{w} t$ for some $w \in \mathcal{A}^*$.

*On leave at the Institute for Informatics, Technical University Munich. Supported by the Alexander von Humboldt Foundation and by the Grant Agency of the Czech Republic, grant No. 201/03/1161.

†Partially supported by the Teilprojekt A3 of the Sonderforschungsbereich 342.

A natural idea how to decrease computational costs of formal verification is to replace a given 'large' process s with some smaller process t so that the original questions about s can be answered by examining the properties of t (we say that t is a *description* of s). In this paper we consider two classes of descriptions, introduced in the following definition:

Definition 2 Let $\sim$ be a process equivalence (i.e., an equivalence over the class of all processes). Let s be a process of a transition system $\mathcal{T} = (S, \mathcal{A}, \rightarrow)$.

- A process t is a $\sim$*-representation* of s iff $s \sim t$.
- The $\sim$*-quotient* of a process s is the process $[s]$ of $\mathcal{T}/\!\sim\; = (S/\!\sim, \mathcal{A}, \mapsto)$ where $S/\!\sim$ is the set of all $\sim$-classes of S (the class containing s is denoted by $[s]$) and $[s] \stackrel{a}{\mapsto} [t]$ iff there are $s' \in [s]$ and $t' \in [t]$ such that $s' \stackrel{a}{\rightarrow} t'$.

In fact, $\sim$-quotients are interesting only for those process equivalences which are preserved under quotients, i.e., such that $s \sim [s]$ for every process s. It has been shown in [12] that all process equivalences of the linear/branching time spectrum of [16] have this property. A generic sufficient condition for $\sim$ being preserved under quotients is given in Lemma 13.

It is intuitively clear that if we take process equivalences $\sim$ and $\approx$ such that $\sim\, \subseteq\, \approx$, then $\sim$-representations and $\sim$-quotients are larger but more "faithful" than $\approx$-representations and $\approx$-quotients, respectively. Moreover, we should also expect $\sim$-quotients to be more "faithful" than $\sim$-representations, at least for those process equivalences which are preserved under quotients. The reason is that the state-spaces of s and $[s]$ are the same up to $\sim$, while the states reachable from s and its $\sim$-representation t can be completely "unrelated" by $\sim$ in general.

Definition 3 Let P be a property of processes and $\sim$ a process equivalence. We say that P is

- *preserved* by $\sim$-representations (or $\sim$-quotients) iff whenever t is a $\sim$-representation (or the $\sim$-quotient) of s and s satisfies P, then t satisfies P;
- *reflected* by $\sim$-representations (or $\sim$-quotients) iff whenever t is a $\sim$-representation (or the $\sim$-quotient) of s and t satisfies P, then s satisfies P.

An immediate consequence of the previous definition is the following:

Lemma 4 Let $\sim$ a process equivalence. A property P is preserved by $\sim$-representations (or $\sim$-quotients) iff $\neg P$ is reflected by $\sim$-representations (or $\sim$-quotients).

In this paper we restrict ourselves to properties expressible in Hennessy-Milner (HM) logic. Formulae of HM logic have the following syntax (a ranges over Act):

$$\varphi \quad ::= \quad \mathtt{tt} \mid \varphi \wedge \varphi \mid \neg\varphi \mid \langle a \rangle \varphi$$

The *denotation* $[\![\varphi]\!]$ of a formula φ on a transition system $\mathcal{T} = (S, \mathcal{A}, \rightarrow)$ is defined as follows:

$$\begin{array}{rcl} [\![\mathtt{tt}]\!] & = & S \\ [\![\varphi \wedge \psi]\!] & = & [\![\varphi]\!] \cap [\![\psi]\!] \\ [\![\neg\varphi]\!] & = & S - [\![\varphi]\!] \\ [\![\langle a \rangle \varphi]\!] & = & \{s \in S \mid \exists t \in S : s \stackrel{a}{\rightarrow} t \wedge t \in [\![\varphi]\!]\} \end{array}$$

Instead of $s \in [\![\varphi]\!]$ we usually write $s \models \varphi$. The other boolean connectives are introduced in a standard way; we also define $\mathtt{ff} \equiv \neg\mathtt{tt}$ and $[a]\varphi \equiv \neg\langle a\rangle\neg\varphi$.

We say that a formula φ *distinguishes* between processes s and t iff either $s \models \varphi$ and $t \not\models \varphi$, or $s \not\models \varphi$ and $t \models \varphi$.

The question considered in this paper is what properties expressible in HM logic are preserved and reflected by $\sim$-representations and $\sim$-quotients for a given process equivalence $\sim$. Although the exact answer depends on the choice of $\sim$, it is possible to provide a generic solution by employing the notion of *modal characterization.* A modal characterization of $\sim$ is a set $\mathcal{H}$ of HM formulae such that for all processes s and t we have that $s \sim t$ iff s and t satisfy exactly the same subset of $\mathcal{H}$. Our main results (Theorem 1 and Theorem 2) classify all HM formulae which are preserved/reflected by $\sim$-representations and $\sim$-quotients. The classification is generic and depends only on a suitable modal characterization $\mathcal{H}$ of $\sim$. Here, the word "suitable" means that $\mathcal{H}$ must satisfy some specific closure properties. As we shall see, these conditions cannot be dropped because our theorems would be no longer valid; but they are "harmless" in the sense that many "reasonable" process equivalences have appropriate modal characterizations.

The paper is organized as follows. In Section 2.1, as a warm-up, we determine the set of HM formulae preserved/reflected by $\sim$-representations. In Section 2.2, the core of the paper, we determine the sets of formulae which are preserved/reflected by $\sim$-quotients. The obtained results are applied to the equivalences of the liner/branching time spectrum of [16] in Section 3. Finally, Section 4 contains conclusions and comments on related and future work.

2 The classification

In this section we give a complete classification of HM properties which are preserved/reflected by $\sim$-representations and $\sim$-quotients for certain classes of process equivalences which satisfy some (abstractly formulated) conditions. From the very beginning, we restrict ourselves to those equivalences which have a *modal characterization.*

Definition 5 Let $\sim$ be a process equivalence. A *modal characterization* of $\sim$ is a set $\mathcal{H}$ of HM formulae such that for all processes s, t we have that $s \sim t$ iff s and t satisfy exactly the same formulae of $\mathcal{H}$.

Observe that the same equivalence can have many different modal characterizations.

Now we introduce some notions which will be frequently used in the subsequent sections.

Let φ be a HM formula. The (finite) set of all actions which are used in φ is denoted by $\mathcal{A}(\varphi)$, and the nesting depth of $\langle a\rangle$ operators in φ is denoted $\mathit{depth}(\varphi)$. (Note that $\mathit{depth}(\varphi)$ can be defined inductively by $\mathit{depth}(\mathtt{tt}) = 0$, $\mathit{depth}(\varphi \wedge \psi) = \max\{\mathit{depth}(\varphi), \mathit{depth}(\psi)\}$, $\mathit{depth}(\neg\varphi) = \mathit{depth}(\varphi)$, and $\mathit{depth}(\langle a\rangle\varphi) = 1 + \mathit{depth}(\varphi)$.)

Definition 6 Let $\mathcal{A} \subseteq \mathit{Act}$ be a finite set of actions. A *Tree* over $\mathcal{A}$ is any directed binary tree with root r whose edges are labelled by elements of $\mathcal{A}$ satisfying the following condition: if p, q are a-successors of a node s, where $a \in \mathcal{A}$, then the subtrees rooted by p, q are not isomorphic.

Tree-processes are associated with roots of Trees (we do not distinguish between Trees and Tree-processes in the rest of this paper). Note that for every $k \in \mathbf{N}_0$ and every finite $\mathcal{A} \subseteq Act$ there are only finitely many Trees over $\mathcal{A}$ whose depth is at most k (up to isomorphism). We denote this finite set of representatives by $\mathit{Tree}(\mathcal{A})_k$. Finally, for every node t of a Tree T, the subTree of T rooted by t is denoted $T(t)$.

It is a standard result that for every process s there is a Tree T (possibly of infinite depth) such that s and T satisfy exactly the same HM formulae (cf. [14]). One can also easily prove the following:

Lemma 7 HM formulae φ, ψ are equivalent iff they agree on every element of $\mathit{Tree}(\mathcal{A})_k$ where $\mathcal{A} = \mathcal{A}(\varphi) \cup \mathcal{A}(\psi)$ and $k = \max\{\mathit{depth}(\varphi), \mathit{depth}(\psi)\}$.

Sometimes we also use the following notation (where s is a process):

- $\mathcal{H}_\mathcal{A} := \{\varphi \mid \varphi \in \mathcal{H} \wedge \mathcal{A}(\varphi) \subseteq \mathcal{A}\}$,
- $\mathcal{H}^k_\mathcal{A} := \{\varphi \mid \varphi \in \mathcal{H}_\mathcal{A} \wedge \mathit{depth}(\varphi) \leq k\}$,
- $\mathcal{H}(s) := \{\varphi \mid \varphi \in \mathcal{H} \wedge s \models \varphi\}$,
- $\mathcal{H}_\mathcal{A}(s) := \{\varphi \mid \varphi \in \mathcal{H}_\mathcal{A} \wedge s \models \varphi\}$.

Note that if $\mathcal{A}$ is finite, then $\mathcal{H}^k_\mathcal{A}$ contains only finitely many pairwise nonequivalent formulae. In that case we can thus consider $\mathcal{H}^k_\mathcal{A}$ to be a *finite* set. Note that the '$\mathcal{H}(s)$' and '$\mathcal{H}_\mathcal{A}(s)$' notation as applicable also to Trees. For example, $\mathcal{H}(T(t))$ denotes the set of all HM formulae φ such that the subTree of T rooted by t satisfies φ.

2.1 HM properties preserved by $\sim$-representations

If $\mathcal{H}$ is a modal characterization of a process equivalence $\sim$, then every formula φ which is (equivalent to) a boolean combination of formulae from $\mathcal{H}$ is obviously preserved by $\sim$-representations. For this observation we do not need any additional assumptions about $\mathcal{H}$ or $\sim$. Now we would like to prove a kind of 'completeness' result saying no other HM properties are preserved by all $\sim$-representations. However, this does *not* hold in general, as it is demonstrated in the following counterexample:

Example 8 For every process s we define the set

$$\mathit{Ready}(s) = \{a \in Act \mid s \xrightarrow{a} t \text{ for some } t\}.$$

Now let $a \in Act$ be an (arbitrary but fixed) action, and let us define the equivalence $\sim_a$ as follows: $s \sim_a t$ iff $a \in \mathit{Ready}(s) \cap \mathit{Ready}(t)$, or $\mathit{Ready}(s) = \mathit{Ready}(t)$. The equivalence $\sim_a$ has a modal characterization

$$\mathcal{H}_a = \{\langle a \rangle \mathtt{tt} \vee \langle b \rangle \mathtt{tt} \mid b \in Act, a \neq b\}$$

Now observe that the formula $\langle a \rangle \mathtt{tt}$ is preserved by $\sim_a$-representations, but it is not equivalent to any boolean combination of formulae from $\mathcal{H}_a$.

If $\mathcal{H}$ is a modal characterization of $\sim$ and s, t are non-equivalent processes over $\mathcal{A}$, one intuitively expects that s and t are distinguished by some $\varphi \in \mathcal{H}$ such that $\mathcal{A}(\varphi) \subseteq \mathcal{A}$. Example 8 shows that it is not necessarily the case—the only formulae of $\mathcal{H}_a$ which distinguish between (non-equivalent) processes s and t with transitions $s \xrightarrow{a} s'$, $s \xrightarrow{b} s''$, $t \xrightarrow{b} t'$ are the formulae of the form $\langle a \rangle \mathtt{tt} \vee \langle c \rangle \mathtt{tt}$ where $c \neq b$. In general, if processes p and q over $\mathcal{A}$ are distinguished by some formula $\varphi \in \mathcal{H}$, then they are also distinguished by the formula φ' which is obtained from φ by substituting every subformula $\langle x \rangle \psi$, where $x \notin \mathcal{A}$, with $\mathtt{ff}$. Note that $\mathcal{A}(\varphi') \subseteq \mathcal{A}$. The problem is that φ' does not have to appear in $\mathcal{H}$ in general (as we have seen in Example 8). This motivates the following definition:

Definition 9 A modal characterization $\mathcal{H}$ of a process equivalence $\sim$ is *well-formed* iff whenever $\varphi \in \mathcal{H}$ and $\langle a \rangle \psi$ is an occurrence of a subformula in φ, then also $\varphi' \in \mathcal{H}$ where φ' is obtained from φ by substituting the occurrence of $\langle a \rangle \psi$ with $\mathtt{ff}$.

As we shall see in Section 3, all 'real' process equivalences which have a modal characterization also have a well-formed modal characterization. The same actually applies to the equivalence $\sim_a$ introduced in Example 8:

Example 10 The equivalence $\sim_a$ of Example 8 has a well-formed modal characterization $\mathcal{H} = \{\langle a \rangle \mathtt{tt}\} \cup \{\neg\langle a \rangle \mathtt{tt} \wedge \langle b \rangle \mathtt{tt} \mid b \in \mathit{Act}\}$.

For process equivalences with well-formed modal characterizations we can already establish the aforementioned completeness result. We start with an auxiliary lemma.

Lemma 11 Let $\sim$ be a process equivalence with a well-formed modal characterization $\mathcal{H}$. Let $\mathcal{A}$ be a finite subset of Act, and let $k \in \mathbf{N}_0$. For all $T, T' \in \mathit{Tree}(\mathcal{A})_k$ we have that $T \sim T'$ iff T and T' satisfy exactly the same formulae of $\mathcal{H}^k_{\mathcal{A}}$.

Proof The '$\Rightarrow$' direction is obvious. Now if suffices to realize that if T and T' are distinguished by some $\varphi \in \mathcal{H}$, then they are also distinguished by the formula $\varphi' \in \mathcal{H}^k_{\mathcal{A}}$ which is obtained form φ by substituting every occurrence of a subformula $\langle a \rangle \psi$, which is within the scope of k other $\langle b \rangle$-modalities or where $a \notin \mathcal{A}$, with $\mathtt{ff}$. The formulae φ and φ' agree on all Trees of $\mathit{Tree}(\mathcal{A})_k$, because the occurrences of subformulae in φ which have been substituted by $\mathtt{ff}$ during the construction of φ' are evaluated to false anyway.

Theorem 1 Let $\sim$ be a process equivalence and let $\mathcal{H}$ be a well-formed modal characterization of $\sim$. A formula φ of HM logic is preserved by $\sim$-representations iff φ is equivalent to a boolean combination of formulae from $\mathcal{H}$.

Proof For the '$\Longleftarrow$' direction, we show that if φ_1, φ_2 are preserved by $\sim$-representations, then $\varphi_1 \wedge \varphi_2$ and $\neg\varphi_1$ are also preserved. The $\varphi_1 \wedge \varphi_2$ subcase follows immediatelly. Now suppose that $\neg\varphi_1$ is *not* preserved, i.e., there are processes s, t such that $s \sim t$, $s \models \neg\varphi_1$, and $t \not\models \neg\varphi_1$. This means that $t \models \varphi_1$ and since s can be seen as a $\sim$-representation of t, we obtain that φ_1 is not preserved, which is a contradiction.

Now we prove the '$\Longrightarrow$' direction. Let φ be a formula preserved by $\sim$-representations, $k = \mathit{depth}(\varphi)$, and $\mathcal{A} = \mathcal{A}(\varphi)$. For every $T \in \mathit{Tree}(\mathcal{A})_k$ we construct the formula

$$\psi_T \quad \equiv \quad \bigwedge\{\varrho \mid \varrho \in \mathcal{H}^k_{\mathcal{A}}(T)\} \quad \wedge \quad \bigwedge\{\neg\varrho \mid \varrho \in \mathcal{H}^k_{\mathcal{A}} \smallsetminus \mathcal{H}^k_{\mathcal{A}}(T)\}$$

Now let

$$\psi \quad \equiv \quad \bigvee\{\psi_T \mid T \in \mathit{Tree}(\mathcal{A})_k, T \models \varphi\}$$

We prove that φ and ψ are equivalent. To do that, it suffices to show that φ and ψ agree on every $T_1 \in \mathit{Tree}(\mathcal{A})_k$ (see Lemma 7).

- Let $T_1 \in \mathit{Tree}(\mathcal{A})_k$ such that $T_1 \models \varphi$. As $T_1 \models \psi_{T_1}$, we also have $T_1 \models \psi$.
- Let $T_1 \in \mathit{Tree}(\mathcal{A})_k$ such that $T_1 \models \psi$. Then there is $T_2 \in \mathit{Tree}(\mathcal{A})_k$ such that $T_2 \models \varphi$ and $T_1 \models \psi_{T_2}$. As $T_1 \models \psi_{T_2}$, the Trees T_1, T_2 satisfy exactly the same formulae of $\mathcal{H}^k_{\mathcal{A}}$. Hence, $T_1 \sim T_2$ due to Lemma 11. As φ is preserved by $\sim$-representations, T_1 is a $\sim$-representation of T_2, and $T_2 \models \varphi$, we also have $T_1 \models \varphi$.

Theorem 1 gives a complete classification of those HM properties which are preserved and reflected (see Lemma 4) by $\sim$-representations for a process equivalence $\sim$ which has a well-formed modal characterization $\mathcal{H}$.

2.2 HM properties preserved by $\sim$-quotients

Now we establish analogous results for $\sim$-quotients. As we shall see, this problem is more complicated.

The first difficulty was indicated already in Section 1—it does not have much sense to consider $\sim$-quotients if we are not guaranteed that $s \sim [s]$ for every process s. Unfortunately, there *are* process equivalences (even with a well-formed modal characterization) which do not satisfy this basic requirement.

Example 12 Let $\sim_2$ be defined as follows: $s \sim_2 t$ iff for each $w \in \mathit{Act}^*$ such that $\mathit{length}(w) = 2$ we have that $s \stackrel{w}{\to} s'$ for some s' iff $t \stackrel{w}{\to} t'$ for some t'. The equivalence $\sim_2$ has a well-formed modal characterization

$$\mathcal{H} = \{\langle a\rangle\langle b\rangle\mathtt{tt} \mid a, b \in \mathit{Act}\}$$

Now let s be a process where $s \stackrel{a}{\to} t, s \stackrel{b}{\to} u, u \stackrel{c}{\to} v$, and t, u, v do not have any other transitions. Then $t \sim_2 u \sim_2 v$, hence $[s] \stackrel{ac}{\to} [v]$, and therefore $s \not\sim_2 [s]$.

However, there is a simple (and reasonable) condition which guarantees that a given $\sim$ is preserved under $\sim$-quotients. The next lemma can be seen as an instance of a well-known result of modal logic, stating that a model and its quotient through a filtration agree on every formula of the filtration [3]. We include a proof for the sake of completeness.

Lemma 13 Let $\sim$ be a process equivalence having a modal characterization $\mathcal{H}$ which is closed under subformulae (i.e., whenever $\varphi \in \mathcal{H}$ and ψ is a subformula of φ, then $\psi \in \mathcal{H}$). Then $s \sim [s]$ for every process s.

Proof Let $\mathcal{H}$ be a modal characterization of $\sim$ closed under subformulae. We prove that for every $\varphi \in \mathcal{H}$ and every process s we have $s \models \varphi \Longleftrightarrow [s] \models \varphi$ (i.e., $s \sim [s]$). By induction on the structure of φ.

- $\varphi \equiv \mathtt{tt}$. Immediate.

- $\varphi \equiv \neg\psi$. Then $\psi \in \mathcal{H}$ and $s \models \psi \iff [s] \models \psi$ by induction hypotheses. Hence also $s \models \neg\psi \iff [s] \models \neg\psi$ as required.

- $\varphi \equiv \psi \wedge \xi$. Then $\psi, \xi \in \mathcal{H}$. If $\psi \wedge \xi$ distinguishes between s and $[s]$, then ψ or ξ distinguishes between the two processes as well; we obtain a contradiction with induction hypotheses.

- $\varphi \equiv \langle a \rangle \psi$.

  - ($\Rightarrow$) Let $s \models \langle a \rangle \psi$. Then there is some t such that $s \xrightarrow{a} t$ and $t \models \psi$. Therefore, $[s] \overset{a}{\mapsto} [t]$ and as $\psi \in \mathcal{H}$, we can use induction hypothesis to conclude $[t] \models \psi$. Hence, $[s] \models \langle a \rangle \psi$.
  - ($\Leftarrow$) Let $[s] \models \langle a \rangle \psi$. Then $[s] \overset{a}{\mapsto} [t]$ for some $[t]$ such that $[t] \models \varphi$. By Definition 2, there are s', t' such that $s \sim s'$, $t \sim t'$, and $s' \xrightarrow{a} t'$. As $[t] = [t']$, we have $[t'] \models \psi$ and hence $t' \models \psi$ by induction hypothesis. Therefore, $s' \models \langle a \rangle \psi$. As $s \sim s'$ and $\langle a \rangle \psi \in \mathcal{H}$, we also have $s \models \langle a \rangle \psi$ as needed (remember that formulae of $\mathcal{H}$ cannot distinguish between equivalent processes by Definition 5).

Observe that the modal characterization of Example 12 is not closed under suformulae.

According to our intuition presented in Section 1, $\sim$-quotients should be more robust then $\sim$-representations, i.e., they should preserve more properties. The following definition gives a 'syntactical template' which allows to construct such properties.

Definition 14 Let $\mathcal{S}$ be a set of HM formulae. The set of *diamond* formulae over $\mathcal{S}$, denoted $\mathcal{D}(\mathcal{S})$, is defined by the following abstract syntax equation:

$$\varphi \quad ::= \quad \vartheta \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \langle a \rangle \varphi$$

Here a ranges over Act, and ϑ ranges over boolean combinations of formulae from $\mathcal{S}$. The set $\mathcal{B}(\mathcal{S})$ of *box* formulae over $\mathcal{S}$ is defined in the same way, but we use the $[a]$ modality instead of $\langle a \rangle$.

Definition 15 A modal characterization $\mathcal{H}$ of a process equivalence $\sim$ is *good* if it satisfies the following conditions:

- if $\varphi \in \mathcal{H}$, then also $\langle a \rangle \varphi \in \mathcal{H}$ for all $a \in Act$;

- if $\varphi \in \mathcal{H}$ and $\langle a \rangle \psi$ is an occurrence of a subformula in φ, then also $\varphi', \varphi'' \in \mathcal{H}$ where φ' and φ'' are obtained from φ by substituting the given occurrence of $\langle a \rangle \psi$ with `tt` and `ff`, respectively.

- if $\varphi \in \mathcal{H}$ and ψ is a subformula of φ, then $\psi \in \mathcal{H}$. Moreover, if ψ is within the scope of a negation in φ, then also $\neg\psi \in \mathcal{H}$.

- if $\neg\psi_1, \cdots, \neg\psi_n \in \mathcal{H}$, then also $\neg\psi_1 \wedge \cdots \wedge \neg\psi_n \in \mathcal{H}$.

Note that a good modal characterization is also well-formed and closed under subformulae.

Before presenting our main result (Theorem 2), we formulate and prove two auxiliary lemmas.

Lemma 16 Let $\sim$ be a process equivalence with a good modal characterization $\mathcal{H}$. Let s, t be processes such that for every $a \in Act$ we have $\bigcup_{s \xrightarrow{a} s'} \mathcal{H}(s') = \bigcup_{t \xrightarrow{a} t'} \mathcal{H}(t')$. Then $s \sim t$.

Proof We show that for every $\varphi \in \mathcal{H}$ we have $s \models \varphi$ iff $t \models \varphi$. By induction on the structure of φ.

- $\varphi \equiv \mathtt{tt}$. Immediate.
- $\varphi \equiv \psi \wedge \xi$ or $\varphi \equiv \neg\psi$. Then $\psi, \xi \in \mathcal{H}$ and thus the result follows immediatelly by applying induction hypothesis.
- $\varphi \equiv \langle a \rangle \psi$. Suppose, e.g., $s \models \langle a \rangle \psi$ and $t \not\models \langle a \rangle \psi$. Then $\psi \in \mathcal{H}$, $\psi \in \bigcup_{s \xrightarrow{a} s'} \mathcal{H}(s')$, and $\psi \notin \bigcup_{t \xrightarrow{a} t'} \mathcal{H}(t')$, which is a contradiction.

Lemma 17 Let $\sim$ be a process equivalence with a good modal characterization $\mathcal{H}$. If there are processes s, t and $a \in Act$ such that

- $s \sim t$, and
- there is $s \xrightarrow{a} s'$ such that for every $t \xrightarrow{a} t'$ we have that $s' \not\sim t'$,

then there are processes p, q such that $\mathcal{H}(p) \subset \mathcal{H}(q)$.

Proof Let $\{t_1, \cdots, t_n\}$ be the set of all a-successors of t. Due to Lemma 16 we have that $\mathcal{H}(s') \subseteq \bigcup_{1 \le i \le n} \mathcal{H}(t_i)$. Now there are two possibilities:

- $\mathcal{H}(s') = \bigcup_{1 \le i \le n} \mathcal{H}(t_i)$. Since $s' \not\sim t_i$ for every $1 \le i \le n$, there must be some $1 \le j \le n$ such that $\mathcal{H}(t_j) \subset \mathcal{H}(s')$ are we are done.
- $\mathcal{H}(s') \subset \bigcup_{1 \le i \le n} \mathcal{H}(t_i)$. First we show that there is some t_j, $1 \le j \le n$, such that whenever $\neg\psi \in \mathcal{H}(s')$, then $\neg\psi \in \mathcal{H}(t_j)$. Suppose it is not the case, i.e., for each $1 \le i \le n$ there is a formula $\neg\psi_i \in \mathcal{H}(s')$ such that $\neg\psi_i \notin \mathcal{H}(t_i)$. Then $\bigwedge_{1 \le i \le n} \neg\psi_i$ is a formula of $\mathcal{H}$ (see Definition 15) which belongs to $\mathcal{H}(s')$ but not to $\bigcup_{1 \le i \le n} \mathcal{H}(t_i)$, and we have a contradiction. So, there must be such a t_j. If $\mathcal{H}(t_j) \subseteq \mathcal{H}(s')$, then also $\mathcal{H}(t_j) \subset \mathcal{H}(s')$ because $\mathcal{H}(t_j) \neq \mathcal{H}(s')$ and we are done. Otherwise, there is $\varrho \in \mathcal{H}(t_j)$ such that $\varrho \notin \mathcal{H}(s')$. Now let p, q be processes with transitions $p \xrightarrow{a} s'$, $q \xrightarrow{a} s'$, and $q \xrightarrow{a} t_j$, where $a \in Act$ is some action. We show that $\mathcal{H}(p) \subset \mathcal{H}(q)$. Clearly $\langle a \rangle \varrho$ is a formula of $\mathcal{H}$ which distinguishes between p and q, hence $\mathcal{H}(p) \neq \mathcal{H}(q)$. It remains to prove that $\mathcal{H}(p) \subseteq \mathcal{H}(q)$. Let $\varphi \in \mathcal{H}$. First, realize that φ can be viewed as a boolean combination of formulae of the form $\langle x \rangle \psi$. Now it suffices to show that for each (occurrence of) such a subformula $\langle x \rangle \psi$ we have that

  (1) if $\langle x \rangle \psi$ does not appear within the scope of any negation in φ, then $\langle x \rangle \psi \in \mathcal{H}(p)$ implies $\langle x \rangle \psi \in \mathcal{H}(q)$;

  (2) if $\langle x \rangle \psi$ appears within the scope of a negation in φ, then $\langle x \rangle \psi \in \mathcal{H}(p)$ iff $\langle x \rangle \psi \in \mathcal{H}(q)$.

If both (1) and (2) hold, then clearly $\varphi \in \mathcal{H}(p)$ implies $\varphi \in \mathcal{H}(q)$ as needed. A proof of (1) is easy—if $x \neq a$, then $\langle x \rangle \psi$ does not belong to $\mathcal{H}(p)$; and if $x = a$, then $\psi \in \mathcal{H}(s')$ and hence $\langle x \rangle \psi \in \mathcal{H}(q)$ as needed. The "$\Rightarrow$" direction of (2) is shown in the same way. It remains to demonstrate the "$\Leftarrow$" direction of (2). First realize that since $\langle x \rangle \psi$ appears within the scope of a negation in φ, we have that $\neg\psi \in \mathcal{H}$ (see Definition 15). Now, let us suppose that $\langle x \rangle \psi \in \mathcal{H}(q)$. That is, $\psi \in \mathcal{H}(s')$ or $\psi \in \mathcal{H}(t_j)$. If $\psi \in \mathcal{H}(s')$, we are done immediatelly; and if $\psi \in \mathcal{H}(t_j)$, we can conclude that $\psi \in \mathcal{H}(s')$ because otherwise $\neg\psi$ would be a formula of $\mathcal{H}(s')$ witnessing that t_j does not have the property specified above.

Theorem 2 Let $\sim$ be a process equivalence having a good modal characterization $\mathcal{H}$. A HM formula φ is preserved by $\sim$-quotients iff φ is equivalent to some formula of $\mathcal{D}(\mathcal{H})$.

Proof ($\Leftarrow$) Let $\varphi \in \mathcal{D}(\mathcal{H})$. By induction on the structure of φ:

- $\varphi \equiv \vartheta$. It suffices to realize that ϑ is preserved by $\sim$-representations (Theorem 1) and every $\sim$-quotient is also a $\sim$-representation (Lemma 13).
- $\varphi \equiv \varphi_1 \wedge \varphi_2$ or $\varphi \equiv \varphi_1 \vee \varphi_2$, where φ_1, φ_2 are preserved. Immediate.
- $\varphi \equiv \langle a \rangle \varphi_1$ where φ_1 is preserved. Let s be an arbitrary process such that $s \models \langle a \rangle \varphi_1$. Then there is $s \xrightarrow{a} s'$ such that $s' \models \varphi_1$. By definition of $\sim$-quotient we have $[s] \overset{a}{\mapsto} [s']$. Moreover, $[s'] \models \varphi_1$ as φ_1 is preserved. Hence, $[s] \models \langle a \rangle \varphi_1$ as needed.

($\Rightarrow$) Let $k = \mathit{depth}(\varphi)$ and $\mathcal{A} = \mathcal{A}(\varphi)$. For every $T \in \mathit{Tree}(\mathcal{A})_k$ we define the formula ψ_T by induction on the depth of T:

- if the depth of T is 0, then $\psi_T \equiv \mathtt{tt}$,
- if the depth of T is $j \geq 1$, r is the root of T, and $r \xrightarrow{a_1} s_1, \cdots, r \xrightarrow{a_n} s_n$ are the outgoing arcs of r, then

$$\psi_T \quad \equiv \quad \bigwedge \{\varrho \mid \varrho \in \mathcal{H}^j_{\mathcal{A}}(T)\} \quad \wedge \quad \bigwedge \{\neg\varrho \mid \varrho \in \mathcal{H}^j_{\mathcal{A}} \smallsetminus \mathcal{H}^j_{\mathcal{A}}(T)\} \quad \wedge \quad \bigwedge_{1 \leq i \leq n} \langle a_i \rangle \psi_{T(s_i)}$$

  where $T(s_i)$ is the sub-Tree of T rooted by s_i.

We prove that for all $T_1, T_2 \in \mathit{Tree}(\mathcal{A})_k$ the following implication holds: If $T_2 \models \psi_{T_1}$ and $T_1 \models \varphi$, then $T_2 \models \varphi$. It clearly suffices for our purposes, because then one can easily show that φ is equivalent to the formula

$$\psi \quad \equiv \quad \bigvee \{\psi_T \mid T \in \mathit{Tree}(\mathcal{A})_k, T \models \varphi\}$$

(It suffices to check that φ and ψ agree on every $T \in \mathit{Tree}(\mathcal{A})_k$ which is straightforward.)

Assume the opposite, i.e., there are $T_1, T_2 \in \mathit{Tree}(\mathcal{A})_k$ such that $T_2 \models \psi_{T_1}$, $T_1 \models \varphi$, and $T_2 \models \neg\varphi$. We show that then φ is not preserved by $\sim$-quotients which is a contradiction.

We start by defining a homomorphism $f : T_1 \to T_2$ such that $f(s_1) \models \psi_{T(s_1)}$ for every node s_1 of T_1.

- $f(r_1) = r_2$, where r_1 and r_2 are the roots of T_1 and T_2, respectively;
- if $f(s_1)$ has been already defined (i.e., $f(s_1) = s_2$ where $s_2 \models \psi_{T(s_1)}$) and $s_1 \xrightarrow{a} t_1$ is an arc in T_1, then $f(t_1)$ is defined to be (one of the) t_2 such that $s_2 \xrightarrow{a} t_2$ and $t_2 \models \psi_{T(t_1)}$. Note that there must be at least one t_2 with this property, because $s_2 \models \langle a \rangle \psi_{T(t_1)}$ (see the definition of ψ_T above).

Observe that if the nodes of T_2 were pairwise non-equivalent, we could finish the proof as follows: Let $\mathcal{T}$ be the transition system obtained by taking the disjoint union of T_1 and T_2. Since the nodes of T_2 are pairwise non-equivalent and f preserves $\sim$, the $\sim$-quotient of $\mathcal{T}$ is isomorphic to T_2. Hence, we have the desired contradiction because the state r_1 of $\mathcal{T}$ (which is isomorphic to the root of T_1) satisfies φ, but the state $[r_1]$ of $\mathcal{T}/{\sim}$ (which is isomorphic to the root r_2 of T_2) does not satisfy φ.

Unfortunatelly, the nodes of T_2 do not have to be pairwise non-equivalent. Therefore, we first extend the tree T_2 into a transition system $\widehat{T_2}$ by adding certain states and transitions so that all states of $\widehat{T_2}$ (possibly except for the newly added ones) are pairwise non-equivalent. This extension is then "propagated" to T_1 via the homomorphism f. The newly added states and transitions do not influence the (in)validity of φ, but the homomorphism f still preserves $\sim$. Hence, we can finish the proof by taking $\mathcal{T}$ to be the disjoint union of $\widehat{T_1}$ and $\widehat{T_2}$ and arguing in the same way as above.

First, let us realize that there must be (some) processes p, q such that $\mathcal{H}(p) \subset \mathcal{H}(q)$. If it was not the case, we could employ Lemma 17 and prove by a strightforward induction on k that for all $T, T' \in \mathit{Tree}(\mathcal{A})_k$ we have that $T \sim T'$ iff T and T' are isomorphic. This would contradict our assumption that φ distinguishes between T_1 and T_2 which are equivalent (and thus isomorphic).

To extend the Tree T_2 into the system $\bar{T}_2$, for every $0 \le i \le k$ we do the following:

- Let Level_i be the set of all nodes of T_2 with the distance i from the root (hence, $\mathit{Level}_0 = \{r_2\}$). The set Level_i is split into two disjoint subsets
  - $A_i = \mathit{Level}_i \cap \Im(f)$
  - $B_i = \mathit{Level}_i \smallsetminus A_i$

  where $\Im(f)$ is the image of f.
- Let $A_i = \{t_1, \cdots, t_m\}$, $B_i = \{s_1, \cdots, s_n\}$, and let $a_1, \cdots, a_m$, $b_1, \cdots, b_n$ be fresh (i.e., previously unused) actions.
- For all $1 \le i \le m$ we add the transitions
  - $t_i \xrightarrow{a_i} q$,
  - $t_i \xrightarrow{a_k} p$ for every $1 \le k \le m$ such that $k \ne i$,
  - $t_i \xrightarrow{b_k} q$ for every $1 \le k \le n$.
- For all $1 \le j \le n$ we add the transitions
  - $s_j \xrightarrow{a_k} p$ for every $1 \le k \le m$,
  - $s_j \xrightarrow{b_j} q$,

- $s_j \stackrel{b_k}{\to} p$ for every $1 \leq k \leq n$ such that $k \neq j$.

This extension is now propagated back to T_1 via the homomorphism f—to every node s of T_1 we add exactly those transitions which have been just added to $f(s)$. Thus, we obtain the transition system $\widehat{T}_1$. Since we sometimes need to distinguish between a node s of T_1 (or T_2) and its corresponding "twin" in $\widehat{T}_1$ (or $\widehat{T}_2$), from now on we denote such a twin by $\widehat{s}$.

For all $0 \leq i \leq k$ and $s \in B_i$, let $w(s) \in Act^*$ be the sequence of actions associated to the path from the root r_2 of T_2 to s. We define the set $Neigh(s) \subseteq A_i$ by

$$Neigh(s) = \{t \in A_i \mid r_2 \stackrel{w(s)}{\to} t\}$$

Now we prove the three claims below.

i) For every node s of T_2 and every state t of $\widehat{T}_2$ we have that $\widehat{s} \not\sim t$.

   Let $\vartheta \in \mathcal{H}(q) \smallsetminus \mathcal{H}(p)$. It follows directly from the definition of $\widehat{T}_2$ that $\widehat{s}$ and t are distinguished by a formula $\langle a \rangle \xi$ for a suitable action $a \in Act$. In particular, if t is a state reachable from p or q, then we can choose a to be one of the fresh actions which have been used to connect p and q to $\widehat{s}$.

ii) For all $0 \leq i \leq k$ and $s \in B_i$ we have that $\mathcal{H}(s) \subseteq \bigcup_{t \in Neigh(s)} \mathcal{H}(t)$.

   Suppose the converse, i.e., there are $0 \leq i \leq k$, $s \in B_i$, and $\xi \in \mathcal{H}$ such that $\xi \notin \mathcal{H}(t)$ for every $t \in Neigh(s)$. Let $w(s) = a_0 \cdots a_{i-1}$, and let us consider the formula

   $$\vartheta \equiv \langle a_0 \rangle \cdots \langle a_{i-1} \rangle \xi$$

   Clearly $\vartheta \in \mathcal{H}$, $T_2 \models \vartheta$, and $T_1 \not\models \vartheta$. Hence, $T_1 \not\sim T_2$ and we have a contradiction.

iii) For all $0 \leq i \leq k$ and $s \in B_i$ we have that $\mathcal{H}(\widehat{s}) \subseteq \bigcup_{t \in Neigh(s)} \mathcal{H}(\widehat{t})$

   Let $s \in B_i$ for some $0 \leq i \leq k$. First we show that if for every $a \in Act$ we have that

   $$\bigcup_{\widehat{s} \stackrel{a}{\to} s'} \mathcal{H}(s') \quad \subseteq \quad \bigcup_{t \in Neigh(s)} \bigcup_{\widehat{t} \stackrel{a}{\to} t'} \mathcal{H}(t') \tag{1}$$

   then $\mathcal{H}(\widehat{s}) \subseteq \bigcup_{t \in Neigh(s)} \mathcal{H}(\widehat{t})$. It suffices for our purposes, because from the definitions of $\widehat{T}_2$ and $Neigh(s)$ we immediatelly obtain that

   - (1) is satisfied for all $s \in B_k$, hence for every $s \in B_k$ we have that $\mathcal{H}(\widehat{s}) \subseteq \bigcup_{t \in Neigh(s)} \mathcal{H}(\widehat{t})$;
   - if for all $s \in B_{i+1}$ we have that $\mathcal{H}(\widehat{s}) \subseteq \bigcup_{t \in Neigh(s)} \mathcal{H}(\widehat{t})$, then (1) is satisfied for all nodes of B_i.

   Hence, $\mathcal{H}(\widehat{s}) \subseteq \bigcup_{t \in Neigh(s)} \mathcal{H}(\widehat{t})$ for all $s \in B_i$, $0 \leq i \leq k$ as required.

   So, let $\xi \in \mathcal{H}(\widehat{s})$. By induction on the structure of ξ we show that if (1) holds then $\xi \in \mathcal{H}(\widehat{t})$ for some $t \in Neigh(s)$.

- $\xi \equiv \mathtt{tt}$ or $\xi \equiv \xi_1 \wedge \xi_2$. Immediate.
- $\xi \equiv \langle a \rangle \xi_1$. Then $\xi_1 \in \mathcal{H}$ and hence we can use the assumption (1) to conclude that there is $t \in \mathit{Neigh}(s)$ such that $\widehat{t} \xrightarrow{a} t'$ where $t' \models \xi$.
- $\xi \equiv \neg \xi_1$. This requires more care. Let $\langle x \rangle \vartheta$ be an occurrence of a subformula in ξ_1, where $x \notin \mathcal{A}$[1], which appears within the scope of j other $\langle a_i \rangle$ operators, where all a_i's are in $\mathcal{A}$. For determining the validity of ξ in $\widehat{s}$ and all $\widehat{t}$, where $t \in \mathit{Neigh}(s)$, the only relevant information about $\langle x \rangle \vartheta$ is its (in)validity in those states which are reachable from $\widehat{s}$ and $\widehat{t}$ in exactly j transitions where the associated actions are in $\mathcal{A}$ (in particular, we can ignore p, q and their possible successors). Since $\langle x \rangle \vartheta$ appears within the scope of a negation in ξ, both ϑ and $\neg\vartheta$ belong to $\mathcal{H}$ (see Definition 15). Therefore, ϑ and $\neg\vartheta$ cannot distinguish between the processes p and q (otherwise, we would have a contradiction with $\mathcal{H}(p) \subset \mathcal{H}(q)$). From this and the definition of $\widehat{T_2}$ we obtain that $\langle x \rangle \vartheta$ is either valid or invalid in *all* of the aforementioned relevant states. This means that we can safely substitute each such subformula $\langle x \rangle \vartheta$ of ξ with $\mathtt{tt}$ or $\mathtt{ff}$ (depending on how the subformula evaluates). Thus we obtain a formula $\xi' \in \mathcal{H}$ (see Definition 15) which agrees with xi on $\widehat{s}$ and all $\widehat{t}$, where $t \in \mathit{Neigh}(s)$. Since $\mathcal{A}(\xi') \subseteq \mathcal{A}$, the newly added transitions and states of $\widehat{T_2}$ cannot influence the (in)validity of xi'. In other words, ξ' cannot distinguish between s and $\widehat{s}$, and between t and $\widehat{t}$ for every $t \in \mathit{Neigh}(s)$. Hence, $\widehat{s} \models \xi$ implies $\widehat{s} \models \xi'$ which implies $s \models \xi'$. Since $\mathcal{H}(s) \subseteq \bigcup_{t \in \mathit{Neigh}(s)} \mathcal{H}(t)$ (see above), we get that $t \models \xi'$ for some $t \in \mathit{Neigh}(s)$, hence $\widehat{t} \models \xi'$ and thus also $\widehat{t} \models \xi$ as required.

According to iii), the homomorphism $\widehat{f} : \widehat{T_1} \to \widehat{T_2}$ defined by

- $\widehat{f}(\widehat{s}) = \widehat{f(s)}$ for every node s of T_1,
- $\widehat{f}(u) = u$ for every node u reachable from p or q,

still preserves $\sim$. To see this, it suffices to show that $\widehat{s} \sim \widehat{f}(\widehat{s})$, which can be easily done by induction of the depth of $T_1(s)$ using the claim iii) above. (In fact, we prove that $\bigcup_{\widehat{s} \xrightarrow{a} s'} \mathcal{H}(s') = \bigcup_{\widehat{f}(\widehat{s}) \xrightarrow{a} t'} \mathcal{H}(t')$ for all $a \in \mathit{Act}$, and then use Lemma 16 to get $\widehat{s} \sim \widehat{f}(\widehat{s})$). Due to the claim i), all states of T_2 are pairwise non-equivalent (possibly except for some of the successors of p and q), and hence we obtain the desired contradiction in the way indicated above—we put $\mathcal{T}$ to be the disjoint union of $\widehat{T_1}$ and $\widehat{T_2}$. The $\sim$-quotient of $\mathcal{T}$ is isomorphic to $\widehat{T_2}$, the state $\widehat{r_1}$ of $\mathcal{T}$ (which is isomorphic to the root of $\widehat{T_1}$) satisfies φ, but the state $[\widehat{r_1}]$ of $\mathcal{T}/\!\sim$ (which is isomorphic to the root $\widehat{r_2}$ of $\widehat{T_2}$) does not satisfy φ. So, φ is not preserved under $\sim$-quotients and we have a contradiction.

Theorem 2 classifies all HM properties which are preserved by $\sim$-quotients where $\sim$ has a good modal characterization $\mathcal{H}$. Hence, HM properties which are *reflected* by $\sim$-quotients are exactly the formulae equivalent to box-formulae over boolean combinations of formulae of $\mathcal{H}$ (see Lemma 4).

[1]That is, x is one of the "new" actions which are used in $\widehat{T_2}$ but not in T_2.

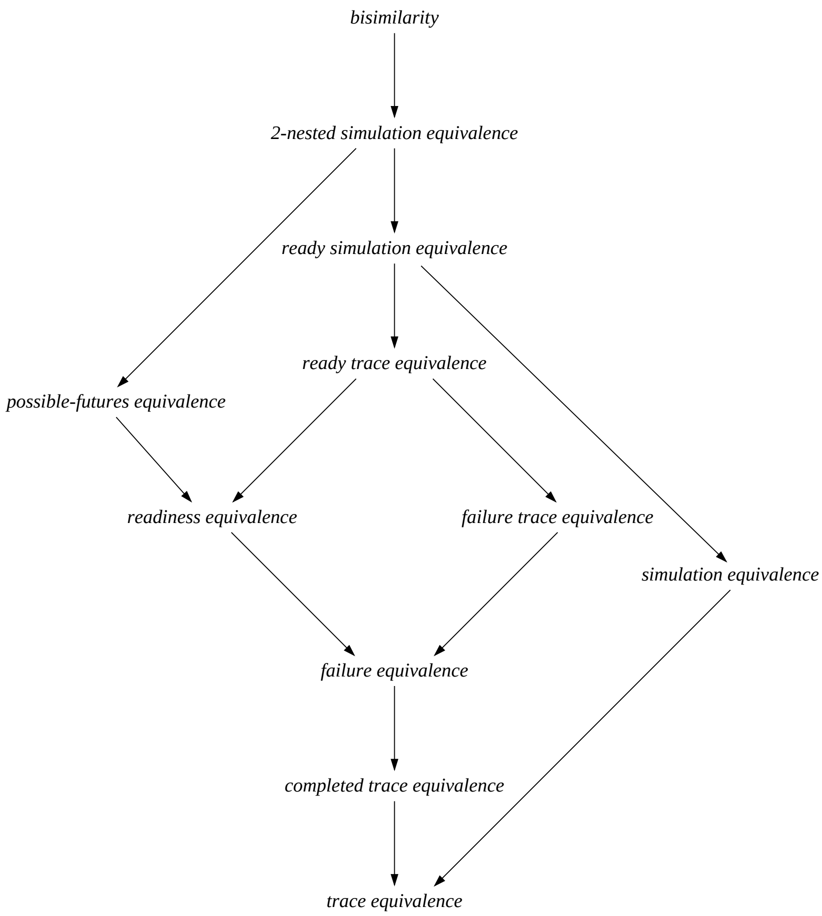

Figure 1: The linear time/branching time spectrum of [16]

3 Applications

In concurrency theory, many process equivalences expressing different 'levels' of semantical sameness of two processes have been designed and studied. A nice overview and comparison of possible approaches has been presented in [16]; in this paper, existing equivalences are ordered w.r.t. their coarseness (see Figure 1) and a kind of modal characterization is given for each of them (unfortunately, not a good one in the sense of Definition 15).

To demonstrate practical applicability of our abstract results, we present a good modal characterization for each equivalence of Figure 1 (except for completed trace equivalence—see below). Formally, we should also prove that each of the given modal characterizations is good and that it is indeed a modal characterization of the associated equivalence, but all these proofs are routine and therefore omitted.

In the subsequent paragraphs we use the following notation:

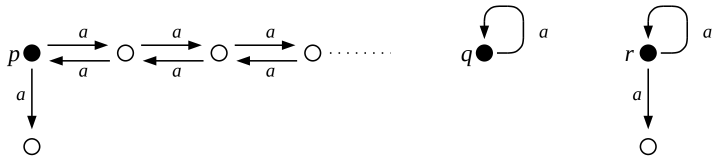

Figure 2: An infinite-state process having a finite $=_t$-representation and a finite $=_t$-quotient.

- $\mathcal{P}(M)$ denotes the set of all subsets of M.
- In all definitions we assume a fixed transition system $\mathcal{T} = (S, \mathcal{A}, \rightarrow)$. If $s \in S$, then
$$I(s) = \{a \in \mathcal{A} \mid \exists t \in S \text{ such that } s \xrightarrow{a} t\}$$
- θ ranges over the set of formulae defined by
$$\theta \quad ::= \quad \texttt{tt} \;\mid\; \texttt{ff} \;\mid\; \neg\langle a\rangle\texttt{tt} \;\mid\; \theta \wedge \theta$$
where $a \in Act$.
- λ ranges over the set of formulae defined by
$$\lambda \quad ::= \quad \texttt{tt} \;\mid\; \texttt{ff} \;\mid\; \langle a\rangle\texttt{tt} \;\mid\; \lambda \wedge \lambda$$
where $a \in Act$.

Trace equivalence. The set of *traces* of a process s, denoted $Tr(s)$, is defined by

$$Tr(s) = \{w \in \mathcal{A}^* \mid \exists t \text{ such that } s \xrightarrow{w} t\}$$

We say that s, t are *trace equivalent*, written $s =_t t$, iff $Tr(s) = Tr(t)$. A good modal characterization $\mathcal{H}$ for trace equivalence is given by

$$\varphi \quad ::= \quad \texttt{tt} \;\mid\; \texttt{ff} \;\mid\; \langle a\rangle\varphi$$

where a ranges over Act.

Before we continue with the other equivalences, let us have a look at a small example which shows that (and how) our abstract results work. Consider the process p of Fig. 2. The process q is a $=_t$-representation of p, and the process r is the $=_t$-characterization of p. According to our results, the formula $\langle a\rangle\neg\langle a\rangle\texttt{tt}$ which is satisfied by p is not generally preserved by $=_t$-representations, but it is preserved by $=_t$-characterizations. Indeed, we have $q \not\models \langle a\rangle\neg\langle a\rangle\texttt{tt}$, while $r \models \langle a\rangle\neg\langle a\rangle\texttt{tt}$.

Failure equivalence. A pair $(w, \Phi) \in \mathcal{A}^* \times \mathcal{P}(\mathcal{A})$ is a *failure pair* of a process $s \in S$, if there is a state $t \in S$ such that $s \xrightarrow{w} t$ and $I(s) \cap \Phi = \emptyset$. Let $F(s)$ denote the set of all failure pairs of s. Processes s, t are *failure equivalent*, written $s =_f t$, iff $F(s) = F(t)$.

A good modal characterization for $=_f$ is given by the following equation (where a ranges over Act):

$$\varphi \quad ::= \quad \mathtt{tt} \;\mid\; \mathtt{ff} \;\mid\; \theta \;\mid\; \langle a\rangle\varphi$$

Readiness equivalence. A pair $(w, \Phi) \in \mathcal{A}^* \times \mathcal{P}(\mathcal{A})$ is a *ready pair* of a process $s \in S$, if there is a state $t \in S$ such that $s \xrightarrow{w} t$ and $I(t) = \Phi$. Let $R(s)$ denote the set of all ready pairs of s. Processes s, t are *readiness equivalent*, written $s =_r t$, iff $R(s) = R(t)$. A good modal characterization for $=_r$ is given by the following equation (where a ranges over Act):

$$\varphi \quad ::= \quad \mathtt{tt} \;\mid\; \mathtt{ff} \;\mid\; \theta \wedge \lambda \;\mid\; \langle a\rangle\varphi$$

Failure trace equivalence. The *refusal relations* $\xrightarrow{\Phi}$ for $\Phi \in \mathcal{P}(\mathcal{A})$ are defined by:

$$s \xrightarrow{\Phi} t \text{ iff } s = t \text{ and } I(s) \cap \Phi = \emptyset$$

The *failure trace relations* $\xrightarrow{\delta}$ for $\delta \in (\mathcal{A} \cup \mathcal{P}(\mathcal{A}))^*$ are defined as the reflexive and transitive closure of both the transition and the refusal relations. $\delta \in (Act \cup \mathcal{P}(\mathcal{A}))^*$ is a *failure trace* of a process $s \in S$, if there is a state $t \in S$ such that $s \xrightarrow{\delta} t$. Let $FT(s)$ denote the set of failure traces of s. Processes s, t are *failure trace equivalent*, written $s =_{ft} t$, iff $FT(s) = FT(t)$. A good modal characterization for $=_{ft}$ is given by the following equation (where a ranges over Act):

$$\varphi \quad ::= \quad \mathtt{tt} \;\mid\; \mathtt{ff} \;\mid\; \theta \;\mid\; \langle a\rangle(\theta \wedge \varphi)$$

Ready trace equivalence. The *ready trace relations* $\overset{\delta}{\Rightarrow}$ for $\delta \in (\mathcal{A} \cup \mathcal{P}(\mathcal{A}))^*$ are defined inductively by:

1. $s \overset{\epsilon}{\Rightarrow} s$ for any $s \in S$.
2. $s \xrightarrow{a} t$ implies $s \overset{a}{\Rightarrow} t$.
3. $s \overset{\Phi}{\Rightarrow} t$ with $\Phi \in \mathcal{P}(\mathcal{A})$ whenever $s = t$ and $I(s) = \Phi$.
4. $s \overset{\delta}{\Rightarrow} t \overset{\rho}{\Rightarrow} u$ implies $s \overset{\delta\rho}{\Rightarrow} u$.

$\delta \in (\mathcal{A} \cup \mathcal{P}(\mathcal{A}))^*$ is a *ready trace* of a process $s \in S$ if there is a state $t \in S$ such that $s \overset{\delta}{\Rightarrow} t$. Let $RT(s)$ denote the set of ready traces of s. Processes s, t are *ready trace equivalent*, written $s =_{rt} t$, iff $RT(s) = RT(t)$. A good modal characterization for $=_{rt}$ is given by the following equation (where a ranges over Act):

$$\varphi \quad ::= \quad \mathtt{tt} \;\mid\; \mathtt{ff} \;\mid\; \theta \wedge \lambda \;\mid\; \langle a\rangle(\theta \wedge \lambda \wedge \varphi)$$

Simulation equivalence. A binary relation $R \subseteq S \times S$ is a *simulation* if whenever sRt then

$$\forall a \in \mathcal{A}: \; s \xrightarrow{a} s' \;\Rightarrow\; \exists t': \; t \xrightarrow{a} t' \wedge s'Rt'$$

A process $s \in S$ is *simulated* by a process $t \in S$, written $s \sqsubseteq_s t$, iff there is a simulation R such that $(s,t) \in R$. Moreover, we say that s,t are *simulation equivalent*, written $s =_s t$, iff $s \sqsubseteq_s t$ and $t \sqsubseteq_s s$. A good modal characterization for $=_s$ is given by the following equation (where a ranges over Act):

$$\varphi \quad ::= \quad \mathtt{tt} \;\mid\; \mathtt{ff} \;\mid\; \langle a \rangle \varphi \;\mid\; \varphi \wedge \varphi$$

Ready simulation equivalence. A binary relation $R \subseteq S \times S$ is a *ready simulation* if whenever sRt then:

- $\forall a \in \mathcal{A}: \; s \xrightarrow{a} s' \;\Rightarrow\; \exists t': \; t \xrightarrow{a} t' \wedge s'Rt'$
- $I(s) = I(t)$

A process $s \in S$ is *ready simulated* by a process $t \in S$, written $s \sqsubseteq_{rs} t$, iff there is a ready simulation R such that $(s,t) \in R$. Moreover, we say that s,t are *ready simulation equivalent*, written $s =_{rs} t$, iff $s \sqsubseteq_{rs} t$ and $t \sqsubseteq_{rs} s$. A good modal characterization for $=_{rs}$ is given by the following equation (where a ranges over Act):

$$\varphi \quad ::= \quad \mathtt{tt} \;\mid\; \mathtt{ff} \;\mid\; \theta \wedge \lambda \;\mid\; \langle a \rangle (\theta \wedge \lambda \wedge \varphi) \;\mid\; \varphi \wedge \varphi$$

Possible futures equivalence. A pair $(w, \Phi) \in \mathcal{A}^* \times \mathcal{P}(\mathcal{A}^*)$ is *a possible future* of a process $s \in S$ iff there is a state $t \in S$ such that $s \xrightarrow{w} t$ and $Tr(t) = \Phi$. The set of all possible futures of s is denoted $PF(s)$. Processes s,t are *possible-futures equivalent*, written $s =_{pf} t$, iff $PF(s) = PF(t)$. A good modal characterization for $=_{pf}$ is given by the following equation (where a ranges over Act):

$$\varphi \quad ::= \quad \mathtt{tt} \;\mid\; \mathtt{ff} \;\mid\; \bigwedge_{i=1}^{n} \psi_i \wedge \bigwedge_{i=1}^{m} \neg \psi_i \;\mid\; \langle a \rangle \varphi$$

where $m, n \in \mathbf{N}_0$, and ψ ranges over the set of formulae defined by $\psi \;\; ::= \;\; \mathtt{tt} \mid \mathtt{ff} \mid \langle a \rangle \psi$ (where a ranges over Act).

2-nested simulation equivalence. A binary relation $R \subseteq S \times S$ is a *2-nested simulation* if whenever sRt then

- $\forall a \in \mathcal{A}: \; s \xrightarrow{a} s' \;\Rightarrow\; \exists t': \; t \xrightarrow{a} t' \wedge s'Rt'$
- $s =_s t$

A process $s \in S$ is *2-nested simulated* by a process $t \in S$, written $s \sqsubseteq_2 t$, iff there is a 2-nested simulation R such that $(s,t) \in R$. Moreover, we say that s,t are *2-nested simulation equivalent*, written $s =_2 t$, iff $s \sqsubseteq_2 t$ and $t \sqsubseteq_2 s$. A good modal characterization for $=_2$ is given by the following equation (where a ranges over Act):

$$\varphi \quad ::= \quad \mathtt{tt} \ \mid \ \mathtt{ff} \ \mid \ \bigwedge_{i=1}^{n} \psi_i \wedge \bigwedge_{i=1}^{m} \neg\psi_i \ \mid \ \langle a \rangle \Big(\bigwedge_{i=1}^{n} \psi_i \wedge \bigwedge_{i=1}^{m} \neg\psi_i \wedge \varphi \Big) \ \mid \ \varphi \wedge \varphi$$

where $m,n \in \mathbf{N}_0$, and ψ ranges over the set of formulae defined by

$$\psi \quad ::= \quad \mathtt{tt} \ \mid \ \mathtt{ff} \ \mid \ \langle a \rangle \psi \ \mid \ \psi \wedge \psi$$

Bisimilarity. A binary relation $R \subseteq S \times S$ is a *bisimulation* if R as well as the reverse of R are simulations. Processes s and t are *bisimilar*, written $s \sim_b t$, iff there is a bisimulation R such that $(s,t) \in R$. A good modal characterization for $\sim_b$ is the set of all formulae of HM logic.

An interesting related problem is whether a given infinite-state state process has for a given $\sim$ any finite $\sim$-representation, and whether its $\sim$-characterization is finite. It is also known as the *regularity* and *strong regularity* problem (see also [12]). Some decidability results for various equivalences and various classes of infinite-state processes have already been established [2, 11, 7, 9, 13, 8], but this area still contains a number of open problems.

The only equivalence of [16] which does not have a good modal characterization is completed trace equivalence. The problem is that this equivalence requires a simple infinite conjunction, or a generalized $\langle \cdot \rangle$ modality (which can be phrased 'after any action'), which are not at our disposal.

4 Related and future work

In the context of process theory, modal characterizations were introduced by Hennessy and Milner in their seminal paper [6]. The paper provides characterizations of bisimulation, simulation, and trace equivalence as full, conjunction-free, and negation-free Hennessy-Milner logic, respectively. The result stating that bisimulation equivalence is also characterized by the modal μ-calculus seems to be folklore. In [16], van Glabbeek introduces the equivalences of his hierarchy by means of sets of formulae, in a style close to modal characterizations.

In [10], Kaivola and Valmari determine weakest equivalences preserving certain fragments of linear time temporal logic. In [5], Goltz, Kuiper, and Penczek study the equivalences characterized by various logics in a partial order setting.

An interesting open problem is whether it is possible to give a similar classification for some richer (more expressive) logic. Also, we are not sufficiently acquainted with work on modal logic outside of computer science (or before computer science was born). Work on filtrations [3] or partial isomorphisms [4] should help us to simplify and streamline our proofs.

References

[1] *Proceedings of CONCUR'92*, volume 630 of *LNCS*. Springer, 1992.

[2] O. Burkart, D. Caucal, and B. Steffen. Bisimulation collapse and the process taxonomy. In *Proceedings of CONCUR'96*, volume 1119 of *LNCS*, pages 247–262. Springer, 1996.

[3] B.F. Chellas. *Modal Logic—An Introduction*. Cambridge University Press, 1980.

[4] J. Flum. First-order logic and its extensions. In *Proceedings of the International Summer Institute and Logic Colloquium*, volume 499 of *Lecture Notes in Mathematics*, pages 248–310. Springer, 1975.

[5] U. Goltz, R. Kuiper, and W. Penczek. Propositional temporal logics and equivalences. In *Proceedings of CONCUR'92* [1], pages 222–236.

[6] M. Hennessy and R. Milner. Algebraic laws for nondeterminism and concurrency. *Journal of the Association for Computing Machinery*, 32(1):137–161, 1985.

[7] P. Jančar and J. Esparza. Deciding finiteness of Petri nets up to bisimilarity. In *Proceedings of ICALP'96*, volume 1099 of *LNCS*, pages 478–489. Springer, 1996.

[8] P. Jančar, A. Kučera, and F. Moller. Simulation and bisimulation over one-counter processes. In *Proceedings of STACS 2000*, volume 1770 of *LNCS*, pages 334–345. Springer, 2000.

[9] P. Jančar and F. Moller. Checking regular properties of Petri nets. In *Proceedings of CONCUR'95*, volume 962 of *LNCS*, pages 348–362. Springer, 1995.

[10] R. Kaivola and A. Valmari. The weakest compositional semantic equivalence preserving nexttime-less linear temporal logic. In *Proceedings of CONCUR'92* [1], pages 207–221.

[11] A. Kučera. Regularity is decidable for normed PA processes in polynomial time. In *Proceedings of FST&TCS'96*, volume 1180 of *LNCS*, pages 111–122. Springer, 1996.

[12] A. Kučera. On finite representations of infinite-state behaviours. *Information Processing Letters*, 70(1):23–30, 1999.

[13] A. Kučera and R. Mayr. Simulation preorder over simple process algebras. *Information and Computation*, 173(2):184–198, 2002.

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

[15] D.M.R. Park. Concurrency and automata on infinite sequences. In *Proceedings 5^{th} GI Conference*, volume 104 of *LNCS*, pages 167–183. Springer, 1981.

[16] R. van Glabbeek. The linear time—branching time spectrum. *Handbook of Process Algebra*, pages 3–99, 1999.