FI MU

Faculty of Informatics
Masaryk University

A Logical Viewpoint on Process-Algebraic Quotients

by

Antonín Kučera
Javier Esparza

FI MU Report Series FIMU-RS-2000-01

January 2000

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.

Keywords: Verification, modal logics, transition systems, process equivalences.

1 Introduction

In the equivalence approach to formal verification, the specification and the implementation of a system are typically formalized as transition systems $\mathcal{S}$ and $\mathcal{I}$, and the informal statement 'the implementation satisfies the specification' is formalized as '$\mathcal{S}$ is equivalent to $\mathcal{I}$'. In the modal logic approach, the specification is a modal formula φ, and the statement is formalized as '$\mathcal{I}$ is a model of φ'.

In a seminal paper [7], Hennessy and Milner proved that bisimulation equivalence admits a *modal characterization*: Two (finitely branching) processes are bisimilar if and only if they satisfy exactly the same formulae

*Supported by a Research Fellowship granted by the Alexander von Humboldt Foundation and by a Post-Doc grant GA ČR No. 201/98/P046.

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

of Hennessy-Milner logic. This result was later extended to the modal μ-calculus, a much more powerful logic strictly containing many other logics, like CTL, CTL*, and LTL. This showed that it was possible to link the two different approaches to formal verification, based on equivalences and modal logics, respectively.

Modal characterizations play an important rôle in practice: Given a very large, or even infinite, transition system $\mathcal{T}$, we would like to obtain a smaller, or at least simpler, transition system $\mathcal{T}'$ which satisfies the specification if and only if $\mathcal{T}$ does. If the specification belongs to a set of formulae $\mathcal{H}$ characterizing an equivalence $\sim$, then we can safely take any $\mathcal{T}'$ satisfying $\mathcal{T} \sim \mathcal{T}'$.

An interesting possibility is to take $\mathcal{T}'$ as the *quotient* $\mathcal{T}/\!\sim$ of $\mathcal{T}$ under $\sim$, whose states are the equivalence classes of the states of $\mathcal{T}$, and whose transitions are given by $[s] \xrightarrow{a} [t]$ only if $s \xrightarrow{a} t$. This works for all equivalences in van Glabbeek's spectrum [19] because they satisfy $\mathcal{T} \sim \mathcal{T}/\!\sim$ (as proved in [14]). Quotients are particularly interesting for bisimulation equivalence for practical reasons, of which we give just two. First, in this case $\mathcal{T}/\!\sim$ can be very efficiently computed for finite transition systems, as shown in [17]. Second, for some classes of real-time and hybrid systems [2, 8], the quotient under bisimulation of an infinite transition system can be proved to be finite; this makes automatic verification possible, at least in principle.

$\mathcal{T}/\!\sim$ is guaranteed to satisfy a property of $\mathcal{H}$ if and only if $\mathcal{T}$ does, but maybe this holds for other properties as well? We study this question (in a slightly refined form) within the framework of Hennessy-Milner logic, for arbitrary equivalences. Given a set of formulae characterizing $\sim$, our results determine the sets $\mathcal{L}, \mathcal{L}' \supset \mathcal{H}$ such that $\mathcal{T}/\!\sim$ satisfies $\varphi \in \mathcal{L}$ if $\mathcal{T}$ does, and $\mathcal{T}$ satisfies $\varphi \in \mathcal{L}'$ if $\mathcal{T}/\!\sim$ does. As we shall see, $\mathcal{L} \cap \mathcal{L}' = \mathcal{H}$; the additional formulae of $\mathcal{L}, \mathcal{L}'$ which do not belong to $\mathcal{H}$ can be used by efficient verification semi-algorithms (which produce *yes/no/don't know* answers) – if we want to find out whether $\mathcal{T}$ satisfies some $\varphi \in \mathcal{L} \cup \mathcal{L}'$, we can first check if $\mathcal{T}/\!\sim$ satisfies φ; if it is the case and $\varphi \in \mathcal{L}'$, we can conclude that $\mathcal{T}$ satisfies φ. If $\mathcal{T}/\!\sim$ does not satisfy φ and $\varphi \in \mathcal{L}$, we conclude that $\mathcal{T}$ does not satisfy φ. In the other cases we 'don't know'.

The paper is organized as follows. Section 2 contains preliminary definitions. In Section 3.1, as a warm-up, we determine the set of Hennessy-Milner formulae preserved by *any* transition system $\mathcal{T}'$ satisfying $\mathcal{T} \sim \mathcal{T}'$. In Section 3.2, the core of the paper, we determine the sets $\mathcal{L}, \mathcal{L}'$ of formulae which are preserved/reflected by the quotient $\mathcal{T}/\!\sim$. In Section 4 we apply our results to the equivalences in van Glabbeek's hierarchy. Section 5 contains conclusions and comments on related and future work.

2 Definitions

Let $Act = \{a, b, c, \ldots\}$ be a countably infinite set of *atomic actions* (which is fixed for the rest of this paper).

Definition 2.1. *A transition system (T.S.) is a triple $\mathcal{T} = (S, \mathcal{A}, \rightarrow)$ where S is a set of* states, *$\mathcal{A} \subseteq Act$, and $\rightarrow \subseteq S \times \mathcal{A} \times S$ is a* transition relation*. We say that $\mathcal{T}$ is* finitely-branching *iff for every $s \in S$, $a \in \mathcal{A}$ the set $\{t \mid s \xrightarrow{a} t\}$ is finite.* Processes *are understood as (being associated with) states in transition systems.*

In the rest of this paper we only consider finitely-branching T.S. (this restriction is harmless from the 'practical' point of view, but it has important 'theoretical' consequences as it, e.g., allows to prevent the use of infinite conjunctions in our future constructions).

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 $w \in \mathcal{A}^*$. The set of actions which is used in the underlying transition system of a process p is denoted by $Act(p)$ (sometimes we work with processes whose associated transition system has not been explicitly defined). Properties which have been originally defined for transition systems are often also used for processes; in that case we always mean that the underlying transition system has the property (for example, we can speak about the set of states and actions of a given process).

Definition 2.2. *Let $\mathcal{T}_1 = (S_1, \mathcal{A}_1, \rightarrow_1)$, $\mathcal{T}_2 = (S_2, \mathcal{A}_2, \rightarrow_2)$ be transition systems. A (total) function $f : S_1 \rightarrow S_2$ is a* homomorphism *from $\mathcal{T}_1$ to $\mathcal{T}_2$ iff for all $s, t \in S_1$ and $a \in Act$ we have that $s \xrightarrow{a}_1 t \Longrightarrow f(s) \xrightarrow{a}_2 f(t)$.*

Definition 2.3. *A* renaming *is an (arbitrary) injective function $r : Act \rightarrow Act$. For every transition system $\mathcal{T} = (S, \mathcal{A}, \rightarrow)$ we define the r-*renamed *transition systems $r(\mathcal{T}) = (S, r(\mathcal{A}), \hookrightarrow)$ where $s \overset{r(a)}{\hookrightarrow} t$ iff $s \xrightarrow{a} t$.*

2.1 Process descriptions

In this section we briefly introduce and motivate the problem which is considered in this paper.

Transition systems are widely accepted as a convenient model of concurrent and distributed systems. A lot of verification problems (safety, liveness, etc.) can be thus reduced to certain properties of processes (states). A major difficulty is that in practice we often meet systems which have a very large or even infinite state-space. A natural idea how to decrease computational costs of formal verification is to replace a given process with some 'equivalent' and smaller one (which can be then seen as its 'description').

In this paper we consider two types of process descriptions ($\sim$-representations and $\sim$-characterizations) which are determined by a chosen *process equivalence* $\sim$. By a 'process equivalence' we mean an arbitrary equivalence on the class of all processes, i.e., states in finitely-branching T.S.

Definition 2.4. *Let $\sim$ be a process equivalence. A process t is a* $\sim$-representation *of a process s iff $s \sim t$.*

Definition 2.5. *Let $\sim$ be a process equivalence. The* $\sim$-characterization *of a process s of a transition system $\mathcal{T} = (S, \mathcal{A}, \rightarrow)$ 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 $\mapsto$ is the least relation satisfying $s \xrightarrow{a} t \Longrightarrow [s] \overset{a}{\mapsto} [t]$.*

Observe that the $\sim$-characterization of s is essentially the quotient of s under $\sim$. We use the word 'characterization' because for every 'reasonable' process equivalence $\sim$ (see Lemma 3.9) we have that $s \sim [s]$ for each process s; hence, the $\sim$-characterization of s describes not only the behavior of s (as $\sim$-representations of s do), but also the behavior of all reachable states of s, i.e., it *characterizes* the whole state-space of s. More precisely, for every state t of the process s there is an equivalent state $[t]$ of the process $[s]$. Therefore, we intuitively expect that $\sim$-characterizations should be more robust than $\sim$-representations. This intuition is confirmed by main theorems of Section 3. Also note that the same process can have many different $\sim$-representations, but its $\sim$-characterization is unique.

Definition 2.6. *Let P be a property of processes, $\sim$ a process equivalence. We say that P is*

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

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

An immediate consequence of the previous definition is the following:

Lemma 2.7. *Let $\sim$ a process equivalence. A property P is preserved by $\sim$-representations (or $\sim$-characterizations) iff $\neg P$ is reflected by $\sim$-representations (or $\sim$-characterizations).*

The question considered in this paper is what properties expressible in Hennessy-Milner logic (see the next section) are preserved and reflected by $\sim$-representations and $\sim$-characterizations for a given process equivalence $\sim$, i.e., to what extent are the two kinds of process descriptions 'robust' for a given $\sim$. As we shall see, we can give a complete classification of those properties if the equivalence $\sim$ satisfies certain (abstractly formulated) conditions. Intuitively, we put more and more restrictions on $\sim$ which allow us to prove more and more things; as we shall see in Section 4, all those restrictions are 'reasonable' in the sense that (almost) all existing (i.e., studied) process equivalences satisfy them. See Section 4 for details.

2.2 Hennessy-Milner Logic

Formulae of Hennessy-Milner (H.M.) 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:

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

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 $[a]\varphi \equiv \neg\langle a\rangle\neg\varphi$. The *depth* of a formula φ, denoted $depth(\varphi)$, is defined inductively by

- $depth(\mathtt{tt}) = 0$,
- $depth(\varphi \wedge \psi) = \max\{depth(\varphi), depth(\psi)\}$,
- $depth(\neg\varphi) = depth(\varphi)$,
- $depth(\langle a\rangle\varphi) = 1 + depth(\varphi)$.

The set of actions which are used in a formula φ is denoted by $Act(\varphi)$ (note that $Act(\varphi)$ is always finite).

Definition 2.8. *Let $\mathcal{A} \subseteq Act$. 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 $Tree(\mathcal{A})_k$.*

It is a standard result that for every process s there is a Tree T_s over $Act(s)$ (possibly of infinite depth) such that s and T_s satisfy exactly the same H.M. formulae (cf. [16]). One can also easily prove the following:

Lemma 2.9. *Formulae φ, ψ of H.M. logic are equivalent iff they agree on every $T \in Tree(\mathcal{A})_k$ where $\mathcal{A} = Act(\varphi) \cup Act(\psi)$ and $k = \max\{depth(\varphi), depth(\psi)\}$.*

For every renaming r and every H.M. formula φ we define the formula $r(\varphi)$ which is obtained from φ by substituting each $\langle a \rangle$ with $\langle r(a) \rangle$.

Lemma 2.10. *For every process s, renaming r, and H.M. formula φ we have that $s \models \varphi$ iff $r(s) \models r(\varphi)$.*

In the next section we also need the following tools:

Definition 2.11. *Let φ be a H.M. formula, s a process. For a given occurrence of a subformula ψ in φ we define its* diamond-depth, *denoted $d(\psi)$, to be the number of $\langle b \rangle$-modalities which have the occurrence of ψ in their scope. The set of all actions which are used in those modalities is denoted by $\mathcal{A}_d(\psi)$. Finally, we use $\mathcal{R}_s(\psi)$ to denote the set of all states which are reachable from s via a sequence of (exactly) $d(\psi)$ transitions whose actions are contained in $\mathcal{A}_d(\psi)$.*

Lemma 2.12. *Let φ be a H.M. formula. Let φ' be the formula obtained from φ by substituting (given occurrences of) its subformulae $\psi_1, \ldots, \psi_n$ by H.M. formulae $\xi_1, \ldots, \xi_n$, respectively. Let s be a process such that $s \models \varphi$ and for all $i \in \{1, \ldots, n\}$, $s' \in \mathcal{R}_s(\psi_i)$ one of the following conditions holds:*

1. $s' \models \psi_i \iff s' \models \xi_i$
2. $s' \models \xi_i$ *and the occurrence of ψ_i in φ is not within the scope of any negation.*

Then $s \models \varphi'$.

Proof. Immediate from Definition 2.11. □

3 The classification

In this section we give a complete classification of H.M. properties which are preserved/reflected by $\sim$-representations and $\sim$-characterizations 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 3.1. *Let $\sim$ be a process equivalence. We say that $\sim$ has a* modal characterization *iff there is a set $\mathcal{H}$ of H.M. 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. Sometimes we also use the following notation (where s is a process):

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

Note that if $\mathcal{A}$ is finite, then $\mathcal{H}^k_{\mathcal{A}}$ contains only finitely many pairwise non-equivalent formulae. In that case we can thus consider $\mathcal{H}^k_{\mathcal{A}}$ to be a *finite* set.

3.1 H.M. properties preserved by $\sim$-representations

Theorem 3.2. *Let $\mathcal{H}$ be a modal characterization of a process equivalence $\sim$. Then every formula ϑ which is a Boolean combination of formulae from $\mathcal{H}$ is preserved by $\sim$-representations.*

The previous theorem is in fact a trivial consequence of Definition 3.1. Now we would like to prove a kind of 'completeness' result saying that nothing else (except for formulae which are equivalent to Boolean combinations of formulae from $\mathcal{H}$) is preserved by $\sim$-representations. However, this property does *not* hold for an arbitrary modal characterization $\mathcal{H}$; it is demonstrated by the following counterexample:

Example 3.3. *Let $\sim$ be defined as follows: $s \sim t$ iff $a \in Act(s) \cap Act(t)$, or $Act(s) = Act(t)$. Let*

$$\mathcal{M} = \{(\mathcal{A}_1, \mathcal{A}_2) \mid \mathcal{A}_1, \mathcal{A}_2 \textit{ are finite, nonempty, and disjoint subsets of } Act\}.$$

The equivalence $\sim$ has a modal characterization

$$\mathcal{H} = \{\langle a\rangle\, \mathtt{tt} \vee (\bigwedge_{b\in\mathcal{A}_1} \langle b\rangle\, \mathtt{tt} \wedge \bigwedge_{c\in\mathcal{A}_2} \neg\langle c\rangle\, \mathtt{tt}) \mid (\mathcal{A}_1, \mathcal{A}_2) \in \mathcal{M}\}$$

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

However, a simple assumption about $\mathcal{H}$ which is formulated in the next definition makes a completeness proof possible.

Definition 3.4. *We say that 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 4, all 'real' process equivalences which have a modal characterization also have a well-formed modal characterization. An important (and naturally-looking) property of those process equivalences which have a well-formed modal characterization is presented in the following lemma:

Lemma 3.5. *Let $\sim$ be a process equivalence having a well-formed modal characterization $\sim$. Let $\mathcal{A} \subseteq Act$, $k \in \mathbf{N}_0$. For all $T, T' \in Tree(\mathcal{A})_k$ 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 every element of $Tree(\mathcal{A})_k$, 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 3.6. *Let $\sim$ be a process equivalence having a well-formed modal characterization $\mathcal{H}$. Then every formula φ of H.M. logic which is preserved by $\sim$-representations is equivalent to a Boolean combination of formulae from $\mathcal{H}$.*

Proof. Let φ be a formula preserved by $\sim$-representations, $k = depth(\varphi)$, $\mathcal{A} = Act(\varphi)$ (note that $\mathcal{A}$ is *finite*). For every $T \in Tree(\mathcal{A})_k$ we construct the formula

$$\psi_T \equiv \bigwedge_{\substack{\varrho\in\mathcal{H}^k_{\mathcal{A}} \\ T\models\varrho}} \varrho \wedge \bigwedge_{\substack{\varrho\in\mathcal{H}^k_{\mathcal{A}} \\ T\not\models\varrho}} \neg\varrho$$

Now let

$$\psi \equiv \bigvee_{\substack{T \in Tree(\mathcal{A})_k \\ T \models \varphi}} \psi_T$$

We show that φ and ψ are equivalent. To do that, it suffices to show that φ and ψ agree on every $T_1 \in Tree(\mathcal{A})_k$ (see Lemma 2.9).

- Let $T_1 \in Tree(\mathcal{A})_k$ such that $T_1 \models \varphi$. As $T_1 \models \psi_{T_1}$, we also have $T_1 \models \psi$.
- Let $T_1 \in Tree(\mathcal{A})_k$ such that $T_1 \models \psi$. Then there is $T_2 \in Tree(\mathcal{A})_k$ 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 3.5. As φ is preserved by $\sim$-representations, T_1 is a $\sim$-representation of T_2, and $T_2 \models \varphi$, we also have $T_1 \models \varphi$. $\square$

Theorem 3.2 and 3.6 give a complete classification of those H.M. properties which are preserved and reflected (see Lemma 2.7) by $\sim$-representations for a process equivalence $\sim$ which has a well-formed modal characterization $\mathcal{H}$.

3.2 H.M. properties preserved by $\sim$-characterizations

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

The first difficulty has been indicated already in Section 2.1 – it does not have too much sense to speak about $\sim$-characterizations 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 3.7. *Let $\sim$ be defined as follows: $s \sim t$ iff for each $w \in Act^*$ such that $length(w) = 2$ we have that $s \stackrel{w}{\to} s'$ for some s' iff $t \stackrel{w}{\to} t'$ for some t'. The equivalence $\sim$ has a well-formed modal characterization*

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

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 $t \sim u \sim v$, hence $[s] \stackrel{ac}{\to} [v]$, and therefore $s \not\sim [s]$.

However, there is a simple (and reasonable) condition which guarantees what we need.

Definition 3.8. *Let $\sim$ be a process equivalence. We say that $\sim$ has a* closed *modal characterization iff it has a modal characterization $\mathcal{H}$ which is closed under subformula (i.e., whenever $\varphi \in \mathcal{H}$ and ψ is a subformula of φ, then $\psi \in \mathcal{H}$).*

A closed modal characterization is a particular case of a *filtration*. The next lemma is a well-known result of modal logic, stating that a model and its quotient through a filtration agree on every formula of the filtration [4]. We include a proof for the sake of completeness.

Lemma 3.9. *Let $\sim$ be a process equivalence having a closed modal characterization. Then $s \sim [s]$ for every process s.*

Proof. Let $\mathcal{H}$ be a closed modal characterization of $\sim$. We prove that for every $\varphi \in \mathcal{H}$ and every process s we have $s \models \varphi \iff [s] \models \varphi$ (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 2.5 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 hypotheses. 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 3.1). $\square$

According to our intuition presented in Section 2.1, $\sim$-characterizations 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 3.10. *Let $\mathcal{S}$ be a set of H.M. 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 $[a]$-modality instead of $\langle a \rangle$.*

Theorem 3.11. *Let $\sim$ be a process equivalence having a closed modal characterization $\mathcal{H}$. Then every formula of $\mathcal{D}(\mathcal{H})$ is preserved by $\sim$-characterizations.*

Proof. 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 3.6) and every $\sim$-characterization is also a $\sim$-representation (Lemma 3.9).
- $\varphi \equiv \varphi_1 \wedge \varphi_2$, 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 p be an arbitrary process such that $p \models \langle a \rangle \varphi_1$. Then there is $p \xrightarrow{a} p'$ such that $p' \models \varphi_1$. By definition of $\sim$-characterization we have $[p] \overset{a}{\mapsto} [p']$. Moreover, $[p'] \models \varphi_1$ as φ_1 is preserved. Hence, $[p] \models \langle a \rangle \varphi_1$ as needed. □

In order to prove the corresponding completeness result, we need some additional assumptions about $\sim$ and $\mathcal{H}$.

Definition 3.12. *Let $\sim$ be a process equivalence. We say that $\sim$ has a* good *modal characterization iff it has a closed modal characterization $\mathcal{H}$ which satisfies the following conditions:*

- *if $\varphi \in \mathcal{H}$, then also $\langle a \rangle \varphi \in \mathcal{H}$ for every $a \in Act$;*
- *if $\varphi \in \mathcal{H}$, then also $r(\varphi) \in \mathcal{H}$ for every renaming r;*
- *if $\langle a \rangle \psi$ is an occurrence of a subformula in φ, then also $\varphi', \varphi'' \in \mathcal{H}$ where φ' and φ'' are the formulae obtained from φ by substituting the occurrence of $\langle a \rangle \psi$ with $\mathtt{tt}$ and $\mathtt{ff}$, respectively;*
- *if $\varphi \in \mathcal{H}$ and $\neg \psi$ is a subformula of φ, then also $\neg \xi \in \mathcal{H}$ for every subformula ξ of ψ;*
- *there are processes s, t such that $Act(s) \cup Act(t)$ is finite and $\mathcal{H}(s) \subset \mathcal{H}(t)$.*

The requirements of Definition 3.12 look strange at first glance. In fact, the first four of them only eliminate a lot of 'unnatural' process equivalences from our considerations. The last requirement is also no problem, because the majority of 'real' process equivalences are defined as kernels of certain preorders, and one can always find processes s, t such that s is 'strictly less' than t in the preorder.

Now we present a sequence of technical lemmas which are then used to prove the last main theorem of our paper.

Lemma 3.13. *Let $\mathcal{H}$ be a good modal characterization of a process equivalence $\sim$. For every $n \in \mathbf{N}$ and every finite $\mathcal{A} \subseteq Act$ there are processes $p_1, \cdots, p_n$ such that $Act(p_i)$ is finite, $Act(p_i) \cap \mathcal{A} = \emptyset$, and $\mathcal{H}(p_i) \supset \mathcal{H}(p_{i+1})$ for each $1 \leq i < n$.*

Proof. Let s and t be processes such that $\mathcal{H}(s) \subset \mathcal{H}(t)$. We can safely assume that $(Act(s) \cup Act(t)) \cap \mathcal{A} = \emptyset$, because otherwise we can consider processes $r(s), r(t)$ for an appropriate renaming r (observe that $\mathcal{H}(r(s)) \subset \mathcal{H}(r(t))$ due to Lemma 2.10 and Definition 3.12). Let $\xi \in \mathcal{H}$ be a formula such that $t \models \xi$ and $s \not\models \xi$. Let $a_1, \cdots, a_n$ be fresh (unused) actions. The process p_i has (exactly) the following transitions: $p_i \xrightarrow{a_j} s$ for every $1 \leq j < i \leq n$, and $p_i \xrightarrow{a_j} t$ for every $1 \leq i \leq j \leq n$. We prove that $\mathcal{H}(p_i) \supset \mathcal{H}(p_{i+1})$ for each $1 \leq i < n$. First, note that $\langle a_i \rangle \xi \in \mathcal{H}$, $p_i \models \langle a_i \rangle \xi$, and $p_{i+1} \not\models \langle a_i \rangle \xi$. It remains to prove that for every $\varphi \in \mathcal{H}$ such that $p_{i+1} \models \varphi$ we also have $p_i \models \varphi$. The formula φ can be viewed as a Boolean combination of formulae of the form $\langle a \rangle \psi$. We show that for each such $\langle a \rangle \psi$ we have that $p_{i+1} \models \langle a \rangle \psi \iff p_i \models \langle a \rangle \psi$, or $p_i \models \langle a \rangle \psi$ and $\langle a \rangle \psi$ is not within the scope of any negation in φ. It clearly suffices to conclude $p_i \models \varphi$. We distinguish two possibilities:

- $p_{i+1} \models \langle a \rangle \psi$. As $\psi \in \mathcal{H}$ and $\mathcal{H}(s) \subset \mathcal{H}(t)$, we also have $p_i \models \langle a \rangle \psi$ (see the construction of p_i above).

- $p_{i+1} \not\models \langle a \rangle \psi$. If $p_i \not\models \langle a \rangle \psi$, we are done immediately. If $p_i \models \langle a \rangle \psi$, then necessarily $a = a_i$; we obtain that $t \models \psi$ and $s \not\models \psi$. If the formula $\langle a \rangle \psi$ is within the scope of some negation in φ, we obtain $\neg\psi \in \mathcal{H}$. As $s \models \neg\psi$ and $t \not\models \neg\psi$, we have a contradiction with $\mathcal{H}(s) \subset \mathcal{H}(t)$. $\square$

Lemma 3.14. *Let $\sim$ be a process equivalence having a closed 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.

- $\varphi \equiv \psi \wedge \xi$. Suppose that $\psi \wedge \xi$ distinguishes between s and t. Then $\psi, \xi \in \mathcal{H}$ and at least one of those formulae must distinguish between s and t; we obtain a contradiction with induction hypotheses.

- $\varphi \equiv \neg\psi$. The same as above.

- $\varphi \equiv \langle a \rangle \psi$. 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 $\psi \notin \bigcup_{t \xrightarrow{a} t'} \mathcal{H}(t')$, a contradiction. □

Lemma 3.15. *Let $\sim$ be a process equivalence having a good modal characterization $\mathcal{H}$. Let $\mathcal{A}$ be a finite subset of Act, $k \in \mathbf{N}_0$. Let $T_1, T_2 \in Tree(\mathcal{A})_k$ such that there is a homomorphism f from T_2 to T_1 which preserves $\sim$. Then the Trees T_1, T_2 can be extended (by adding some new states and transitions) in such a way that the obtained transition systems T_1', T_2' satisfy the following:*

- *the homomorphism f can be extended to a homomorphism f' from T_2' to T_1' which also preserves $\sim$,*

- *for every H.M. formula φ such that $Act(\varphi) \subseteq \mathcal{A}$ we have $T_2' \models \varphi$ iff $T_2 \models \varphi$ and $T_1' \models \varphi$ iff $T_1 \models \varphi$,*

- *the 'old' states of T_1' (i.e., the ones which have not been added to T_1 during the extension procedure) are pairwise nonequivalent w.r.t. $\sim$.*

Proof. First we describe the extension of T_1 which yields the system T_1'. This extension is then 'propagated' back to T_2 via the homomorphism f—each state s of T_2 is extended in the same way as the state $f(s)$ of T_1. Finally, we show that the three requirements of our lemma are satisfied.

Let n be the number of states of T_1, and let m be the number of those states t of T_1 for which there is a state s of T_2 such that $f(s) = t$. Let $p_1, \ldots, p_n$ be processes over a finite $\mathcal{A}' \subseteq Act$ such that $\mathcal{H}(p_1) \supset \mathcal{H}(p_2) \supset \cdots \supset \mathcal{H}(p_n)$ and $\mathcal{A} \cap \mathcal{A}' = \emptyset$. Such processes must exist by Lemma 3.13. Now we take an arbitrary bijection b from the set of states of T_1 to $\{1, \ldots, n\}$ satisfying the following conditions:

- if $t = f(s)$ for some state s of T_2, then $b(t) \leq m$,

- if there is a (nonempty) path from t to t' in T_2, then $b(t) > b(t')$.

Now we add to T_1 all states of $p_1, \ldots, p_n$, and for each state t of T_1 and each transition $p_{b(s)} \xrightarrow{a} q$ we add the transition $t \xrightarrow{a} q$ (i.e., the state t has the same set of a-successors as $p_{b(s)}$ for every $a \in \mathcal{A}'$ after the modification). The described extension of T_1 is now 'propagated' to T_2 in the above indicated way, yielding the system T_2'.

As $\mathcal{A} \cap \mathcal{A}' = \emptyset$, the new transitions which have been added to T_1 and T_2 cannot influence the (in)validity of any H.M. formula φ such that $Act(\varphi) \subseteq \mathcal{A}$. Hence, the second requirement of our lemma is satisfied. Moreover, it is easy to see that the third requirement is satisfied as well, because the 'old' states of T_1' now satisfy pairwise different subsets of $\mathcal{H}_{\mathcal{A}'}$. It remains to show that the first requirement is also valid.

The homomorphism f' is defined as a 'natural' extension of f – it agrees with f on the 'old' states of T_1', and behaves like an identity function on the 'new' ones. Observe that if s is a 'new' state of T_2', then the transition systems $T_2'(s)$ and $T_1'(f'(s))$ are the same (isomorphic). Hence, f' trivially preserves $\sim$ on all 'new' states of T_2'. To prove that $s \sim f'(s)$ for every 'old' state s of T_2', we first need to show the following auxiliary lemma: let $s_1, \ldots, s_j$ be 'old' states of T_2', t an 'old' state of T_1' such that

- there is no state s of T_2' such that $f'(s) = t$,
- $\mathcal{H}_{\mathcal{A}}(t) \subseteq \bigcup_{i=1}^{j} \mathcal{H}_{\mathcal{A}}(s_i)$.

Then $\mathcal{H}(t) \subseteq \bigcup_{i=1}^{j} \mathcal{H}(s_i)$.
A proof of the auxiliary lemma: Let $\varphi \in \mathcal{H}$ such that $t \models \varphi$. We show that $s_i \models \varphi$ for some $1 \leq i \leq j$. First we construct a formula $\varphi' \in \mathcal{H}_{\mathcal{A}}$ from φ in the following way (recall the notions introduced in Definition 2.11): every occurrence of a subformula $\langle a \rangle \psi$ in φ, $a \in \mathcal{A}'$, which is not within the scope of any $\langle b \rangle$-modality, where $b \in \mathcal{A}'$, is substituted by

- `tt` if $t \models \langle a \rangle \psi$ or there is some $t' \in \mathcal{R}_t(\langle a \rangle \psi)$ such that $t' \models \langle a \rangle \psi$,
- `ff` otherwise.

Clearly $\varphi' \in \mathcal{H}_{\mathcal{A}}$ (see Definition 3.12). We prove that $t \models \varphi'$, (i.e., $\varphi' \in \mathcal{H}_{\mathcal{A}}(t)$) by showing that the assumptions of Lemma 2.12 are satisfied for φ and the above defined substitution. Let $\langle a \rangle \psi$ be a formula whose occurrence has been substituted in φ to obtain φ'. First, let us realize that every state of $\mathcal{R}_t(\langle a \rangle \psi)$ is an 'old' one, because $\mathcal{A}_d(\langle a \rangle \psi) \subseteq \mathcal{A}$ (see above). We can distinguish two possibilities:

- the occurrence of $\langle a \rangle \psi$ has been substituted by `tt`. Then there are two subcases:
  - $t \models \langle a \rangle \psi$. Remember that each 'old' state q of T_1' has the same set of a-successors as $p_{b(q)}$ for every $a \in \mathcal{A}'$. Hence, $p_{b(t)} \models \langle a \rangle \psi$ because $t \models \langle a \rangle \psi$. Furthermore, for every $t' \in \mathcal{R}_t(\langle a \rangle \psi)$ we have

$\mathcal{H}(p_{b(t)}) \subset \mathcal{H}(p_{b(t')})$ (see the definition of b above). Therefore, $p_{b(t')} \models \langle a\rangle\psi$ and thus we get $t' \models \langle a\rangle\psi$. In other words, for every $t' \in \mathcal{R}_t(\langle a\rangle\psi)$ we obtain $t' \models \mathtt{tt} \Longleftrightarrow t' \models \langle a\rangle\psi$.

  – there is $t' \in \mathcal{R}_t(\langle a\rangle\psi)$ such that $t' \models \langle a\rangle\psi$. First, if $\langle a\rangle\psi$ is satisfied by *every* state of $\mathcal{R}_t(\langle a\rangle\psi)$, we are done immediately. Otherwise, there is $t'' \in \mathcal{R}_t(\langle a\rangle\psi)$ such that $t'' \not\models \langle a\rangle\psi$. Now it suffices to show that the occurrence of $\langle a\rangle\psi$ in φ cannot be within the scope of any negation (see the second condition of Lemma 2.12). Suppose the converse. As $\varphi \in \mathcal{H}$ and $\mathcal{H}$ is a good modal characterization, we know that both $\langle a\rangle\psi$ and $\neg\langle a\rangle\psi \in \mathcal{H}$. As the processes t' and t'' have the same a-successors as the processes $p_{b(t')}$ and $p_{b(t'')}$, respectively, we obtain $p_{b(t')} \models \langle a\rangle\psi$ and $p_{b(t'')} \not\models \langle a\rangle\psi$, hence also $p_{b(t')} \not\models \neg\langle a\rangle\psi$ and $p_{b(t'')} \models \neg\langle a\rangle\psi$. Therefore, it cannot be that $\mathcal{H}(p_{b(t')}) \subset \mathcal{H}(p_{b(t'')})$ or $\mathcal{H}(p_{b(t'')}) \subset \mathcal{H}(p_{b(t')})$, a contradiction.

- the occurrence of $\langle a\rangle\psi$ has been substituted by $\mathtt{ff}$. Then $t' \not\models \langle a\rangle\psi$ for each $t' \in \mathcal{R}_t(\langle a\rangle\psi)$, and we are done immediately.

Now we know that $\varphi' \in \mathcal{H}_{\mathcal{A}}(t)$, hence there must be some s_i such that $s_i \models \varphi'$. We prove that $s_i \models \varphi$, again by applying Lemma 2.12 (observe that φ can be obtained from φ' by a substitution which is 'inverse' to the previously considered one). We show that the assumptions of Lemma 2.12 are satisfied also for φ' and the 'inverse' substitution, distinguishing two possibilities:

- a given occurrence of $\mathtt{tt}$ is substituted 'back' to $\langle a\rangle\psi$. It means that we previously had $t \models \langle a\rangle\psi$ or $t' \models \langle a\rangle\psi$ for some $t' \in \mathcal{R}_t(\langle a\rangle\psi)$. As $\mathcal{H}(p_{b(f'(s))}) \supset \mathcal{H}(p_{b(v)})$ for every 'old' state s of T_2' and every 'old' state v of T_1' which is reachable from t (see the definition of b and the construction of T_2'), we can conclude that $\langle a\rangle\psi$ is satisfied by *each* 'old' state of T_2' (in particular, by all states of $\mathcal{R}_{s_i}(\mathtt{tt})$).

- a given occurrence of $\mathtt{ff}$ is substituted 'back' to $\langle a\rangle\psi$. If $\langle a\rangle\psi$ is not satisfied by any state of $\mathcal{R}_{s_i}(\mathtt{ff})$, we done immediately. We show that if there is some $s' \in \mathcal{R}_{s_i}(\mathtt{ff})$ such that $s' \models \langle a\rangle\psi$, then the occurrence of $\mathtt{ff}$ in φ' cannot be within the scope of any negation. Suppose the converse. Then there is an occurrence of $\langle a\rangle\psi$ in φ which is within the scope of some negation, hence $\neg\langle a\rangle\psi$ belong to $\mathcal{H}$. As $t \models \neg\langle a\rangle\psi$ and $\mathcal{H}(p_{b(t)}) \subset \mathcal{H}(p_{b(f'(s'))})$ (see above), we have $s' \models \neg\langle a\rangle\psi$, a contradiction.

Now we can continue with the main proof. We show that for each 'old' state s of T_2' we have that $s \sim f'(s)$. We proceed by induction on the depth of the subtree which is rooted by s in T_2 (denoted by d).

- $d = 0$. Then s is a leaf in T_2, hence the transition systems $T'_2(s)$ and $T'_1(f'(s))$ are isomorphic. Hence, we trivially have $s \sim f'(s)$.

- **Induction step:** We prove that $\bigcup_{s \xrightarrow{a} s'} \mathcal{H}(s') = \bigcup_{f'(s) \xrightarrow{a} t} \mathcal{H}(t)$ for each $a \in Act$ (hence $s \sim f'(s')$ by Lemma 3.14). If $a \in \mathcal{A}'$, the equality holds trivially because s and $f'(s)$ have the same set of a-successors. Now let $a \in \mathcal{A}$. By induction hypotheses we know that $\mathcal{H}(s') = \mathcal{H}(f'(s'))$ for each a-successor s' of s. To finish the proof, we need to show that for each a-successor t of $f'(s)$ for which there is no state q of T'_2 with $f'(q) = t$ we have that $\mathcal{H}(t) \subseteq \bigcup_{s \xrightarrow{a} s'} \mathcal{H}(s')$. However, it can be easily achieved with a help of the auxiliary lemma which has been proved above; all we need is to show that $\mathcal{H}_{\mathcal{A}}(t) \subseteq \bigcup_{s \xrightarrow{a} s'} \mathcal{H}_{\mathcal{A}}(s')$. Suppose it is not the case, i.e., there is some $\vartheta \in \mathcal{H}_{\mathcal{A}}$ such that $t \models \vartheta$ and $s' \not\models \vartheta$ for each a-successor s' of s. Hence $\langle a \rangle \vartheta \in \mathcal{H}_{\mathcal{A}}$, $s \not\models \langle a \rangle \vartheta$, and $f(s) \models \langle a \rangle \vartheta$; it contradicts the fact that the homomorphism f preserves $\sim$. □

Theorem 3.16. *Let $\sim$ be a process equivalence having a good modal characterization $\mathcal{H}$. Then every formula which is preserved by $\sim$-characterizations is equivalent to some formula of $\mathcal{D}(\mathcal{H})$.*

Proof. Let φ be a formula preserved by $\sim$-characterizations, $k = depth(\varphi)$, $\mathcal{A} = Act(\varphi)$. For every $T \in Tree(\mathcal{A})_k$ we define the formula ψ_T by induction on the depth of T:

- if the depth of T is 0, then $\psi_T \equiv \texttt{tt}$,

- if the depth of T is $j+1$, 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

$$\psi_T \;\equiv\; \bigwedge_{\substack{\varrho \in \mathcal{H}^{j+1}_{\mathcal{A}} \\ T \models \varrho}} \varrho \;\wedge\; \bigwedge_{\substack{\varrho \in \mathcal{H}^{j+1}_{\mathcal{A}} \\ T \not\models \varrho}} \neg\varrho \;\wedge\; \bigwedge_{i=1}^{n} \langle a_i \rangle \psi_{T(s_i)}$$

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

Let

$$\psi \;\equiv\; \bigvee_{\substack{T \in Tree(\mathcal{A})_k \\ T \models \varphi}} \psi_T$$

We prove that φ, ψ are equivalent by showing that they agree on every $T_1 \in Tree(\mathcal{A})_k$.

- Let $T_1 \in \mathit{Tree}(\mathcal{A})_k$ such that $T_1 \models \varphi$. As $T_1 \models \psi_{T_1}$, we immediately have $T_1 \models \psi$.

- Let $T_1 \in \mathit{Tree}(\mathcal{A})_k$ such that $T_1 \models \psi$. Then there is $T_2 \in \mathit{Tree}(\mathcal{A})_k$ with $T_2 \models \varphi$ and $T_1 \models \psi_{T_2}$. We need to prove that $T_1 \models \varphi$. Suppose the converse, i.e., $T_1 \models \neg\varphi$. Let r_1, r_2 be the roots of T_1, T_2, respectively. First we show that there is a homomorphism f from T_2 to T_1 such that for every node s of T_2 we have $f(s) \models \psi_{T(s)}$. The homomorphism f is defined by induction on the distance of s from r_2.

  - $s = r_2$. Then $f(r_2) = r_1$ (remember $T_1 \models \psi_{T_2}$).
  - s is the j^{th} successor of t where $t \xrightarrow{a_1} s_1, \cdots, t \xrightarrow{a_n} s_n$ are the outgoing arcs of t. The formula $\psi_{T(t)}$ looks as follows:

$$\psi_{T(t)} \;\equiv\; \bigwedge_{\substack{\varrho \in \mathcal{H}_{\mathcal{A}}^{k-d} \\ T(t) \models \varrho}} \varrho \;\wedge\; \bigwedge_{\substack{\varrho \in \mathcal{H}_{\mathcal{A}}^{k-d} \\ T(t) \not\models \varrho}} \neg\varrho \;\wedge\; \bigwedge_{i=1}^{n} \langle a_i \rangle \psi_{T(s_i)}$$

    where d is the distance of t from r_2. Let $f(t) = q$. As $q \models \psi_{T(t)}$ (by induction hypotheses), there is some $q \xrightarrow{a_j} q'$ such that $q' \models \psi_{T(s_j)}$. We put $f(s) = q'$.

  Observe that f also preserves $\sim$ because for every node s of T_2 we have that s and $f(s)$ satisfy exactly the same formulae of $\mathcal{H}_{\mathcal{A}}^{k-d}$ (d is the distance of s from r_2). Now we can apply Lemma 3.15—the Trees T_1, T_2 can be extended to transition systems T_1', T_2' in such a way that the 'old' states of T_1' are pairwise nonequivalent, φ is still valid (invalid) in r_2 (r_1), and the homomorphism f can be extended to a homomorphism f' which still preserves $\sim$. Let us define a transition system $\mathcal{T} = (S, \mathcal{A} \cup \mathcal{A}' \cup \{b\}, \rightarrow)$ where

  - S is a disjoint union of the sets of states of T_1' and T_2',
  - $\mathcal{A}'$ is the set of 'new' actions of T_1', T_2' (cf. the proof of Lemma 3.15), $b \notin \mathcal{A} \cup \mathcal{A}'$ is a fresh action,
  - $\rightarrow$ contains all transitions of T_1' and T_2'; moreover, we also have $r_2 \xrightarrow{b} r_2$, $r_1 \xrightarrow{b} r_1$, and $r_2 \xrightarrow{b} r_1$.

  The new b-transitions have been added just to make r_1 reachable from r_2. Observe that we still have $r_1 \sim r_2$, $r_1 \models \neg\varphi$, and $r_2 \models \varphi$. As T_2' can be 'embedded' into T_1' by f', the $\sim$-characterization of the process r_2

of $\mathcal{T}$ is the same (up to isomorphism) as the $\sim$-characterization of the process r_1 of T_1' with one additional arc $r_1 \xrightarrow{b} r_1$. As the 'old' states of T_1' (see Lemma 3.15) are pairwise non-equivalent w.r.t. $\sim$, and possible identification of the 'new' states of T_1' in the $\sim$-characterization of r_1 cannot influence (in)validity of any H.M. formula whose set of actions is contained in $\mathcal{A}$, we can conclude that φ is not satisfied by the process $[r_1]$ of $T_1'/\sim$. Hence, φ is not satisfied by the process $[r_1] = [r_2]$ of $\mathcal{T}/\sim$ either. As φ is satisfied by the process r_2 of $\mathcal{T}$, we can conclude that φ is not preserved by $\sim$-characterizations, and we have a contradiction. $\square$

Theorem 3.11 and 3.16 together say that a H.M. property P is preserved (reflected) by $\sim$-characterizations, where $\sim$ is a process equivalence having a good modal characterization $\mathcal{H}$, iff P is equivalent to some diamond formula (or box formula – see Lemma 2.7) over $\mathcal{H}$.

4 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 [19]; 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 3.12).

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 and bisimilarity—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 equivalences, but all these proofs are routine and therefore omitted.

The last requirement of Definition 3.12 says that there should be two processes s, t such that $\mathcal{H}(s) \subset \mathcal{H}(t)$. Examples of such processes for all equivalences of Figure 1 between ready simulation equivalence and trace equivalence are the processes p, q of Figure 2; in the case of 2-nested simulation equivalence and possible-futures equivalence we can use the processess r, u of the same figure.

In the subsequent paragraphs we employ the following notation:

- $\mathcal{P}(M)$ denotes the set of all subsets of M.

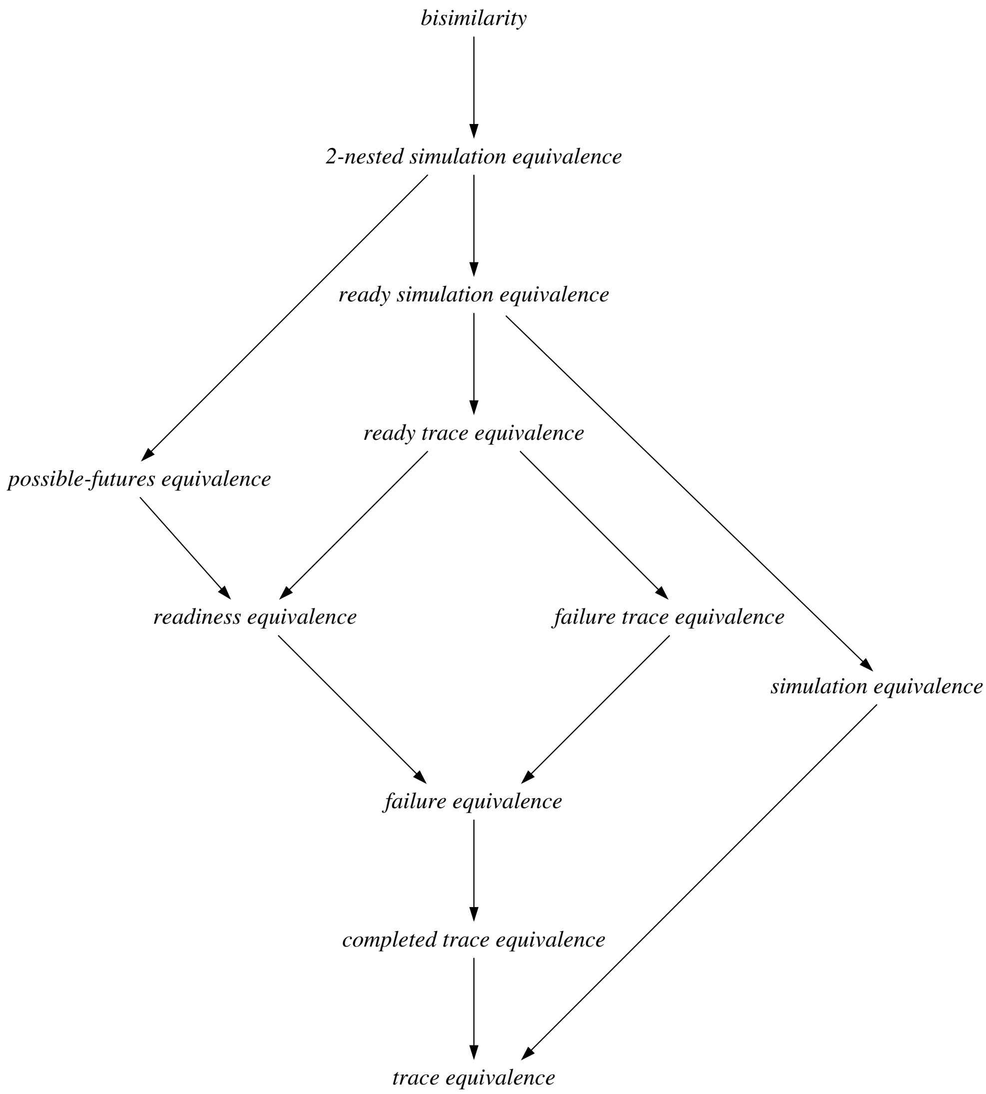

Figure 1: The linear time/branching time spectrum of [19]

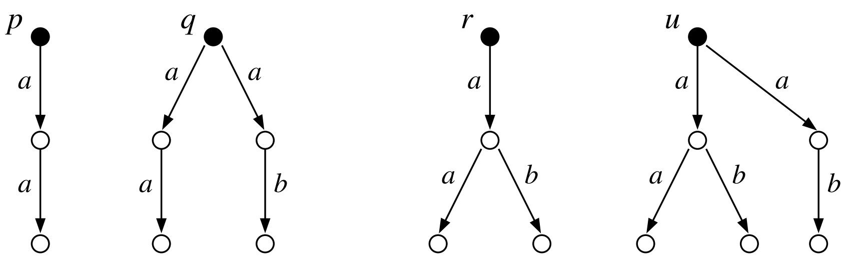

Figure 2: Processes satisfying $\mathcal{H}(s) \subset \mathcal{H}(t)$.

- In all definitions we assume a fixed transition system $\mathcal{T} = (S, Act, \rightarrow)$. If $s \in S$, then

$$I(s) = \{a \in Act \mid \exists t \in S \text{ such that } s \xrightarrow{a} t\}$$

- θ ranges over the set of formulae defined by

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

  where $a \in Act$.

- λ ranges over the set of formulae defined by

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

  where $a \in Act$.

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

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

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

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

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. 3. 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 $\langle a\rangle\neg\langle a\rangle\mathtt{tt}$ which is satisfied by p is not generally preserved by $=_t$-representations, but it is preserved by $=_t$-characterizations. Indeed, we have $q \not\models \langle a\rangle\neg\langle a\rangle\mathtt{tt}$, while $r \models \langle a\rangle\neg\langle a\rangle\mathtt{tt}$.

Failure equivalence. A pair $(w, \Phi) \in Act^* \times \mathcal{P}(Act)$ 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*,

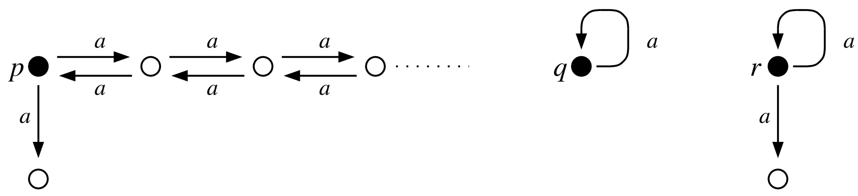

Figure 3: An infinite-state process having finite $=_t$-representation and $=_t$-characterization

written $s =_f t$, iff $F(s) = F(t)$. A good modal characterization for $=_f$ is given by

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

Readiness equivalence. A pair $(w, \Phi) \in Act^* \times \mathcal{P}(Act)$ 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

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

Failure trace equivalence. The *refusal relations* $\xrightarrow{\Phi}$ for $\Phi \in \mathcal{P}(Act)$ 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 $\delta \in (Act \cup \mathcal{P}(Act))^*$ are defined as the reflexive and transitive closure of both the transition and the refusal relations. $\delta \in (Act \cup \mathcal{P}(Act))^*$ 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

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

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

1. $s \stackrel{\epsilon}{\Rightarrow} s$ for any $s \in S$.

2. $s \stackrel{a}{\rightarrow} t$ implies $s \stackrel{a}{\Rightarrow} t$.

3. $s \stackrel{\Phi}{\Rightarrow} t$ with $\Phi \in \mathcal{P}(Act)$ whenever $s = t$ and $I(s) = \Phi$.

4. $s \stackrel{\delta}{\Rightarrow} t \stackrel{\rho}{\Rightarrow} u$ implies $s \stackrel{\delta\rho}{\Rightarrow} u$.

$\delta \in (Act \cup \mathcal{P}(Act))^*$ is a *ready trace* of a process $s \in S$ if there is a state $t \in S$ such that $s \stackrel{\delta}{\Rightarrow} t$. 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

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

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

$$\forall a \in Act: \ s \stackrel{a}{\rightarrow} s' \ \Rightarrow \ \exists t': \ t \stackrel{a}{\rightarrow} t' \wedge s'Rt'$$

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

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

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

- $\forall a \in Act: \ s \stackrel{a}{\rightarrow} s' \ \Rightarrow \ \exists t': \ t \stackrel{a}{\rightarrow} t' \wedge s'Rt'$
- $I(s) = I(t)$

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

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

Possible futures equivalence. A pair $(w, \Phi) \in Act^* \times \mathcal{P}(Act^*)$ 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

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

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

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

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

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

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

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

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

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

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 [14]). Some decidability results for various equivalences and various classes of infinite-state processes have already been established [3, 13, 9, 11, 15, 10], but this area still contains a number of open problems.

The only equivalences of [19] which do not have a good modal characterization are bisimilarity [18] and completed trace equivalence. Bisimilarity is not a 'real' problem, in fact (only the last requirement of Definition 3.12 cannot be satisfied); a modal characterization of bisimilarity is formed by *all* H.M. formulae, and therefore *each* H.M. formula is trivially preserved and reflected by $\sim$-representations and $\sim$-characterizations. As for 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 disposal.

5 Related and future work

In the context of process theory, modal characterizations were introduced by Hennessy and Milner in their seminal paper [7]. The paper provides characterizations of bisimulation, simulation, and trace equivalence as full, conjunction-free, and negation-free H.M. logic, respectively. The result stating that bisimulation equivalence is also characterized by the modal μ-calculus seems to be folklore. In [19], van Glabbeek introduces the equivalences of his hierarchy by means of sets of formulae, in a style close to modal characterizations.

In [12], Kaivola and Valmari determine weakest equivalences preserving certain fragments of linear time temporal logic. In [6], 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 [4] or partial isomorphisms [5] should help us to simplify and streamline our proofs.

References

[1] *Proceedings of CONCUR'92*, volume 630 of *Lecture Notes in Computer Science*. Springer, 1992.

[2] R. Alur and D. Dill. A theory of timed automata. *Theoretical Computer Science*, 126(2):183–235, 1994. Fundamental Study.

[3] O. Burkart, D. Caucal, and B. Steffen. Bisimulation collapse and the process taxonomy. In *Proceedings of CONCUR'96*, volume 1119 of *Lecture Notes in Computer Science*, pages 247–262. Springer, 1996.

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

[5] 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.

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

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

[8] T. Henzinger. Hybrid automata with finite bisimulations. In *Proceedings of ICALP'95*, volume 944 of *Lecture Notes in Computer Science*, pages 324–335. Springer, 1995.

[9] P. Jančar and J. Esparza. Deciding finiteness of Petri nets up to bisimilarity. In *Proceedings of ICALP'96*, volume 1099 of *Lecture Notes in Computer Science*, pages 478–489. Springer, 1996.

[10] P. Jančar, A. Kučera, and F. Moller. Simulation and bisimulation over one-counter processes. In *Proceedings of STACS 2000*, Lecture Notes in Computer Science. Springer, 2000. To appear.

[11] P. Jančar and F. Moller. Checking regular properties of Petri nets. In *Proceedings of CONCUR'95*, volume 962 of *Lecture Notes in Computer Science*, pages 348–362. Springer, 1995.

[12] 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.

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

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

[15] A. Kučera and R. Mayr. Simulation preorder on simple process algebras. In *Proceedings of ICALP'99*, volume 1644 of *Lecture Notes in Computer Science*, pages 503–512. Springer, 1999.

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

[17] R. Paige and R. Tarjan. Three partition refinement algorithms. *SIAM Journal of Computing*, 16(6):973–989, 1987.

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

[19] R.J. van Glabbeek. The linear time—branching time spectrum. In *Proceedings of CONCUR'90*, volume 458 of *Lecture Notes in Computer Science*, pages 278–297. Springer, 1990.

Publications in the FI MU Report Series are in general accessible
via WWW and anonymous FTP:

`http://www.fi.muni.cz/informatics/reports/`
`ftp  ftp.fi.muni.cz (cd pub/reports)`

Copies may be also obtained by contacting:

Faculty of Informatics
Masaryk University
Botanická 68a
602 00 Brno
Czech Republic