Math. Struct. in Comp. Science (2004), *vol.* 14, *pp.* 469–505. © 2004 Cambridge University Press
DOI: 10.1017/S0960129504004268 Printed in the United Kingdom

A domain equation for refinement of partial systems

MICHAEL R. A. HUTH[†], RADHA JAGADEESAN[‡]
and DAVID A. SCHMIDT[§]

[†]*Department of Computing, Imperial College London, South Kensington campus, London SW7 2AZ, England*
Email: M.Huth@doc.imperial.ac.uk

[‡]*School of Computer Science, Telecommunications, and Information Sciences, DePaul University, 243 S. Wabash Avenue, Chicago, Illinois 60604-2287*
Email: rjagadeesan@cs.depaul.edu

[§]*Department of Computing and Information Sciences, Kansas State University, 234 Nichols Hall, Manhattan, Kansas 66506*
Email: schmidt@cis.ksu.edu

Received 10 May 2002; revised 1 February 2003

A reactive system can be specified by a labelled transition system, which indicates static structure, along with temporal-logic formulas, which assert dynamic behaviour. But refining the former while preserving the latter can be difficult, because:

(i) Labelled transition systems are 'total' – characterised up to bisimulation – meaning that no new transition structure can appear in a refinement.
(ii) Alternatively, a refinement criterion not based on bisimulation might generate a refined transition system that violates the temporal properties.

In response, Larsen and Thomson proposed *modal transition systems*, which are 'partial', and defined a refinement criterion that preserved formulas in Hennessy–Milner logic. We show that modal transition systems are, up to a saturation condition, exactly the mixed transition systems of Dams that meet a mix condition, and we extend such systems to non-flat state sets. We then solve a domain equation over the mixed powerdomain whose solution is a bifinite domain that is universal for all saturated modal transition systems and is itself fully abstract when considered as a modal transition system. We demonstrate that many frameworks of partial systems can be translated into the domain: partial Kripke structures, partial bisimulation structures, Kripke modal transition systems, and pointer-shape-analysis graphs.

1. Introduction

A specification of a computing system typically consists of a segment that specifies static structure and a segment that describes dynamic behaviour. For example, a sequential program can be specified by a class diagram, which displays the structure of components to be written, and by sequence diagrams, which display behaviours that must be fulfilled by the executing program; the latter assert behaviours that must be satisfied by any implementation of the former. Refinements of the specification should lead to an

implementation that has the structure in the class diagram and preserves the behaviours stated by the sequence diagrams.

Reactive systems should also be specified and implemented with the assistance of structural and behavioural specifications, and indeed, it is common to employ labelled transition systems to specify the communication structure of a reactive system and to use temporal logic to assert the system's desired behaviours. Then, a model check can verify the consistency of structure with behaviour, a consistency that must be maintained in the refinements that lead to the implementation.

But what does it mean to refine a labelled transition system while preserving its desired behaviours? Labelled transition systems are 'total' entities – a transition from one state to another either can or cannot happen. This may seem innocuous, but the consequences are far-reaching, because labelled transition systems can be distinguished only up to bisimulation (Park 1989; Milner 1989), so it is impractical to use bisimulation to guide the refinement of a labelled-transition system into an implementation (Larsen 1989).

Alternatively, one might define refinement as a simulation (one-half of bisimulation) (Milner 1981) and 'refine' one labelled transition system into a second, such that all transitions in the second system are simulated by transitions in the first. But such a simulation does *not* preserve all the temporal-logic behaviours one might specify – behaviours that are existentially quantified can hold true in the specification transition system but fail in the refinement transition system. (And if we dualise the definition of simulation, the universally quantified properties can be lost.)

Similar problems arise when attempting to synthesise, from an implementation of a reactive system, its abstraction (*abstract interpretation* (Cousot and Cousot 1977)), which might be statically analysed for its temporal-logic properties.

The difficulty with employing a labelled transition system as a specification has its root in the way that negative capabilities are portrayed. A labelled transition system identifies a set of states Σ, a set of actions $\mathtt{Act}$ and a state transition relation, $R \subseteq \Sigma \times \mathtt{Act} \times \Sigma$, such that $(s, \alpha, s') \in R$ states the system is capable of performing action α in state s, producing s' as its successor. By force, $(t, \beta, t') \in (\Sigma \times \mathtt{Act} \times \Sigma) \setminus R$ implies that, at state t, action β either cannot be taken or cannot result in t'. But the human who specifies R might wish to express that some instances of $(\Sigma \times \mathtt{Act} \times \Sigma) \setminus R$ *are still possible* (but not required) in a correct implementation. Labelled transition systems do not provide this flexibility.

Larsen and Thomsen understood well the limitations of labelled transition systems and temporal logic as a specification methodology and proposed *modal transition systems* (Larsen and Thomsen 1988; Larsen 1989) as a solution. Simply stated, a modal transition system is a 'partial' variant of a labelled transition system that can express the *possibility* as well as the *necessity* of a state transition. Larsen and Thomsen revised the definition of bisimulation to accommodate refinement of modal transition systems into implementations and showed that temporal properties written in Hennessy–Milner logic (Hennessy and Milner 1985) are preserved by refinement (Larsen 1989).

Larsen and Thomsen's work applied to transition systems whose state set, Σ, was an unordered set. In this paper, we extend their results to state sets that are domains (Abramsky and Jung 1994), which are crucial to higher-order programming and abstract interpretation: we show that both modal transition systems and a large class of Dams's

consistent mixed transition systems (Dams 1996; Dams *et al.* 1997) are instances of 'saturated' transition systems. Inspired by Abramsky's result, which characterised labelled transition systems up to bisimulation as elements within a recursively defined convex powerdomain (Abramsky 1991), we characterise domain-based, saturated transition systems up to bi-refinement as elements within a reflexively defined product of *mixed powerdomains* (Heckmann 1990; Gunter 1992). This yields a sound treatment of refinement for a temporal logic with universal and existential quantification and negation. As a corollary, the reflexive product of mixed powerdomains generalises Kleene's strong semantics for propositional logic (Kleene 1952) to non-flat settings.

Outline of paper

In Section 2 we present modal transition systems for 'loosely' specifying reactive systems; such specifications may have many non-bisimilar implementations. Refinement and a property semantics (temporal logic) are defined; the latter is shown to be sound with respect to the former. Consistent mixed transition systems are related to modal transition systems by means of saturation, and we extend both to non-flat data domains by means of the mixed powerdomain. In Section 3, we solve a mixed powerdomain equation to obtain a saturated transition system that is universal (all saturated transition systems can be embedded into it) and fully abstract (its greatest abstraction relation coincides with the domain order). As a by-product, refinement of saturated transition systems is logically characterised by Hennessy–Milner logic. Section 4 testifies to the expressiveness of our framework and universal domain, by showing that various frameworks for modelling and analysing partial systems (which are used in concurrency theory, partial state-space model checking, and shape analysis) have linear translations into the domain. Finally, Section 5 discusses related work.

2. Modal transition systems

2.1. *Background*

Labelled transition systems play a prominent role in the specification, explanation and analysis of programs, as seen in structural operational semantics (Plotkin 1981), process algebras (Hoare 1985; Milner 1989) and model-checking (Holzmann 1997).

Definition 1. A *labelled transition system with signature* $\mathtt{Act}$ is a pair $\mathscr{L} = (\Sigma, R)$, where Σ is a set of *states* and $R \subseteq \Sigma \times \mathtt{Act} \times \Sigma$ is a *transition relation.* A labelled transition system is *pointed* if some $s_0 \in \Sigma$ is distinguished as the starting state.

Figure 1 presents the graphical representation of a labelled transition system, which specifies the structure of a system of two readers and one writer that share a file resource. Read a state such as *RSW* as 'first reader reads, second reader sleeps, writer writes'; the actions are *r* ('start read'), *er* ('end read'), *w* ('start write'), and *ew* ('end write'). We designate state *SSS* as the system's starting state.

If a transition system $\mathscr{L}$ is pointed, we can use its starting state and transition relation to generate a derivation tree of the process defined by $\mathscr{L}$ (Milner 1989).

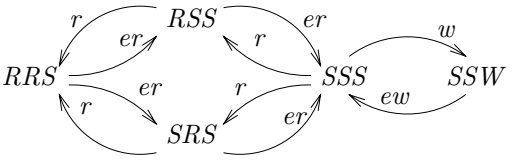


Fig. 1. A labelled transition system for two readers and one writer.

Throughout this paper, we assume that labelled transition systems are *image-finite*: $\{s' \in \Sigma \mid (s, \alpha, s') \in R\}$ is finite for all $s \in \Sigma$ and $\alpha \in \mathtt{Act}$. The intuitive meaning of $R_{s,\alpha} = \{s' \in \Sigma \mid (s, \alpha, s') \in R\} \neq \varnothing$ is:

'in state s, model $\mathscr{L}$ has the reactive capability to engage in action α which, if chosen and executed, results in a successor state $s' \in R_{s,\alpha}$'.

Despite the non-determinism present in labelled transition systems, the reactive capabilities in $R_{s,\alpha}$ are *firm guarantees*: although $\mathscr{L}$ cannot promise that action α will be chosen and executed – the resolution of such choices is accomplished by mechanisms external to the model, for example, a deterministic scheduler or a communication handshake – it does promise that an α-action *is executable* from state s and that the resulting state *can be chosen* from $R_{s,\alpha}$. Thus, labelled transition systems are *total* specifications in the information-theoretic sense: reactive capabilities are either present or absent and such capabilities cannot, up to bisimulation equivalence (Park 1989; Milner 1989), be modified by a correct implementation.

Larsen and Thomsen (Larsen and Thomsen 1988) noted that labelled transition systems have limited utility as specifications of computational systems, because a correct implementation of a labelled-transition-system specification must have bisimilar behaviour. This rules out the use of under-determined specifications and limits the flexibility needed for stepwise implementation. Dually, the analysis of legacy software typically faces the state-explosion problem and usually has to resort to aggressive abstraction techniques. However, state-space reduction is severely constrained if conducted within a fixed bisimulation-equivalence class.

Consequently, Larsen and Thomson proposed *modal transition systems* (Larsen and Thomsen 1988; Larsen 1989) as specification models that overcome these shortcomings. Their solution has a pleasant and free side effect in that it allows an extension of existing abstract-interpretation techniques (Cousot and Cousot 1977) to temporal logics that combine universal and existential path quantifiers (Larsen 1989).

2.2. *Refinement*

Dams developed, independently, mixed transition systems (Dams 1996), which can be seen as a more general notion of modal transition systems, so we define the two systems together.

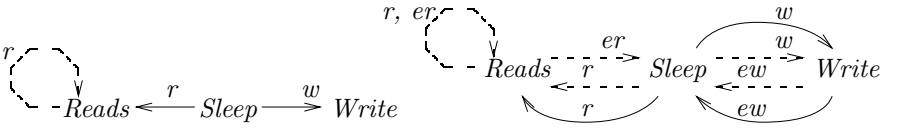


Fig. 2. A mixed transition system that is not a modal transition system (left) and a modal transition system (right).

Definition 2 (Mixed and modal transition systems).

1 A *mixed transition system* (Dams 1996) with signature $\mathtt{Act}$ is a triple $\mathscr{M} = (\Sigma, R^{\mathrm{a}}, R^{\mathrm{c}})$ such that (Σ, R^{m}) is a labelled transition system with signature $\mathtt{Act}$, for every *mode* $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$.
2 A *modal transition system* (Larsen and Thomsen 1988) with signature $\mathtt{Act}$ is a mixed transition system $\mathscr{M} = (\Sigma, R^{\mathrm{a}}, R^{\mathrm{c}})$ with signature $\mathtt{Act}$ such that $R^{\mathrm{a}} \subseteq R^{\mathrm{c}}$.
3 A mixed transition system is *pointed* if there is some $s_0 \in \Sigma$ distinguished as the starting state.
4 A modal transition system is *concrete* or *total* when $R^{\mathrm{a}} = R^{\mathrm{c}}$.

A mixed (modal) transition system is intended to be a 'loose' specification or an abstraction of concrete-system behaviour, and each of its labelled transition systems expresses a distinct 'aspect' or 'modality' of reactive capability:

— R^{a} lists firm guarantees of non-deterministic reactive capabilities – as is familiar from labelled transition systems;
— $R^{\mathrm{c}} \setminus R^{\mathrm{a}}$ lists capabilities that are possible but not guaranteed; the implementation of these reactive capabilities is optional; and
— in the case of a modal transition system, elements $(s, \alpha, s') \in (\Sigma \times \mathtt{Act} \times \Sigma) \setminus R^{\mathrm{c}}$ represent firm guarantees that, in state s, action α, if possible at all, cannot result in the successor state s'.

In Larsen and Thomsen's notation (Larsen and Thomsen 1988), elements of R^{a} are denoted by $s \longrightarrow_{\alpha}^{\Box} s'$ and elements of R^{c} by $s \longrightarrow_{\alpha}^{\Diamond} s'$, where $\Box$ denotes 'for all implementations' and $\Diamond$ 'for some implementation'. A modal transition system follows the philosophy that every firmly guaranteed transition can also be implemented.

Example 1. Figure 2 (left) shows a mixed transition system that abstracts just the read/write-acquisition structure of a one-or-more-readers/one-writer system. For brevity, R^{a}-transitions are drawn as solid arcs, while those from R^{c} are drawn as dashed arcs. State *Reads* represents the situation when one or more readers are engaged in reading; *Write* denotes that the writer is active; and *Sleep* asserts that no process uses the shared file.

The R^{a}-transitions from the *Sleep* state assert that read- and write-acquisition transitions are guaranteed in any correct implementation of the mixed-transition-system specification. The self-transition at *Reads* is possible but not guaranteed because, if all the readers are already engaged in reading, then yet another read acquisition is impossible. Since the

transitions (dashed lines) from the *Sleep* state are guaranteed and are not shadowed by any R^{c}-transitions, the transition system is not modal.

In contrast, Figure 2 (right) shows a modal transition system that shows the structure of both acquisition and release transitions for a system of readers and writer. Here, every firmly guaranteed transition is shadowed by one that is possible. The self-arcs on *Reads* admit the possibility of multiple readers. Note that the transition from *Reads* to *Sleep* is in $R^{\mathrm{c}} \setminus R^{\mathrm{a}}$, because *Reads* represents the state where one or many readers are reading the shared file – it is not guaranteed that the release of merely one reader will make the system return to *Sleep*.

Larsen's interpretation of $\Box$ and $\Diamond$ in mixed transition systems suggests that the refinement of one mixed transition system into another must refine the two forms of transitions in dual fashion.

Definition 3 (Refinement). Let $\mathscr{M} = (\Sigma, R^{\mathrm{a}}, R^{\mathrm{c}})$ be a mixed transition system with signature `Act`. A relation $Q \subseteq \Sigma \times \Sigma$ is a *refinement within* $\mathscr{M}$ (Larsen and Thomsen 1988; Dams 1996) iff $(s,t) \in Q$ implies for all $\alpha \in$ `Act`:

1 If $(t, \alpha, t') \in R^{\mathrm{a}}$, there exists some $s' \in \Sigma$ such that $(s, \alpha, s') \in R^{\mathrm{a}}$ and $(s', t') \in Q$.
2 If $(s, \alpha, s') \in R^{\mathrm{c}}$, there exists some $t' \in \Sigma$ such that $(t, \alpha, t') \in R^{\mathrm{c}}$ and $(s', t') \in Q$.

We write $s \prec_{\mathscr{M}} t$ or $s \prec t$ if there is some refinement Q with $(s,t) \in Q$. In that case, *s refines* (*is abstracted by*) *t*.

The union $\prec_{\mathscr{M}}$ of all refinements within a mixed transition system $\mathscr{M}$ is the greatest such refinement and a preorder.

In order to apply the above definition to the case of showing that one mixed transition system $\mathscr{M} = (\Sigma_1, R_1^{\mathrm{a}}, R_1^{\mathrm{c}})$ refines another system $\mathscr{N} = (\Sigma_2, R_2^{\mathrm{a}}, R_2^{\mathrm{c}})$, we can construct the disjoint union $\mathscr{M} + \mathscr{N} = (\Sigma_1 + \Sigma_2, R_1^{\mathrm{a}} + R_2^{\mathrm{a}}, R_1^{\mathrm{c}} + R_2^{\mathrm{c}})$. If $\mathscr{M}$ and $\mathscr{N}$ are pointed with start states i and j, respectively, we say that $(\mathscr{M}, j)$ *refines* (*is abstracted by*) $(\mathscr{N}, i)$ and write $(\mathscr{M}, j) \prec (\mathscr{N}, i)$ iff $(j,i) \in Q$ for some refinement Q within $\mathscr{M} + \mathscr{N}$.

The intuition behind $\mathscr{M}$ refining $\mathscr{N}$ is that all guaranteed reactive capabilities, R^{a}-transitions in $\mathscr{N}$, are preserved (up to simulation) within the more-concrete system $\mathscr{M}$; and $\mathscr{M}$ contains only those possible reactive capabilities, R^{c}-transitions in $\mathscr{M}$, (up to simulation) that were originally specified within $\mathscr{N}$.

Example 2 (Refinement of mixed transition systems). If we read the labelled transition system in Figure 1 as a total modal transition system (that is, each arc in the figure denotes an R^{c}- as well as an R^{a}-transition), then the system is a refinement of the modal transition system in Figure 2 (right) – given explicitly by $Q = \{(SSS, Sleep), (SS\,W, Write), (RSS, Reads), (SRS, Reads), (RRS, Reads)\}$ – but *not* of the mixed transition system, Figure 2 (left).

Figure 3 shows a modal transition system that is not total but is still a refinement of Figure 2 (right): the refinement depicts a specification of a system of at least two readers and a writer.

Finally, Figure 4 shows a system that does not refine either of the systems in Figure 2, because not all R^{a}-transitions are preserved and a new R^{c}-transition is added.

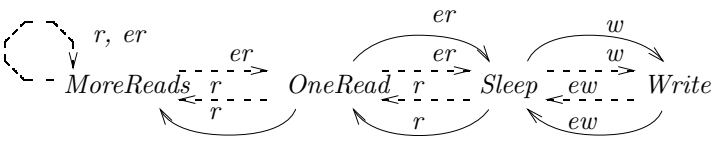


Fig. 3. A refinement of the modal transition system in Figure 2 (right).

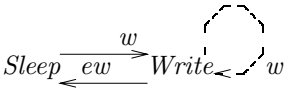


Fig. 4. A system that is not a refinement of any system in Figure 2.

$$
\begin{aligned}
[\![\ \mathtt{tt}\ ]\!]^{\mathrm{m}}_{\rho} &\stackrel{\text{def}}{=} \Sigma \\
[\![\ Z\ ]\!]^{\mathrm{m}}_{\rho} &\stackrel{\text{def}}{=} \rho^{\mathrm{m}}(Z) \\
[\![\ \neg\phi\ ]\!]^{\mathrm{m}}_{\rho} &\stackrel{\text{def}}{=} \Sigma \setminus [\![\ \phi\ ]\!]^{\neg\mathrm{m}}_{\rho} \\
[\![\ \phi_1 \wedge \phi_2\ ]\!]^{\mathrm{m}}_{\rho} &\stackrel{\text{def}}{=} [\![\ \phi_1\ ]\!]^{\mathrm{m}}_{\rho} \cap [\![\ \phi_2\ ]\!]^{\mathrm{m}}_{\rho} \\
[\![\ (\exists\alpha)\,\phi\ ]\!]^{\mathrm{m}}_{\rho} &\stackrel{\text{def}}{=} \mathrm{pre}^{\mathrm{m}}_{\alpha}([\![\ \phi\ ]\!]^{\mathrm{m}}_{\rho}) \\
[\![\ \mu Z.\phi\ ]\!]^{\mathrm{m}}_{\rho} &\stackrel{\text{def}}{=} \mathrm{lfp}\, F^{\mathrm{m}};\ \text{where } F^{\mathrm{m}}(A) \stackrel{\text{def}}{=} [\![\ \phi\ ]\!]^{\mathrm{m}}_{\rho[Z\mapsto A]}.
\end{aligned}
$$

Fig. 5. Property semantics over mixed transition systems (Huth *et al.* 2001) for mode $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$.

2.3. *Property logic*

We equip mixed and modal transition systems with a property logic $\mathbb{L}$, the modal mu-calculus (Kozen 1983), parametric in signature `Act`:

$$\phi ::= \mathtt{tt} \mid Z \mid \neg\phi \mid \phi \wedge \phi \mid (\exists\alpha)\phi \mid \mu Z.\phi, \tag{1}$$

where $\alpha \in \mathtt{Act}$, $Z \in \mathit{var}$ for a countable set of recursion variables var, and all free occurrences of Z in ϕ for $\mu Z.\phi$ are under an even scope of negations. We assume the standard embedding of `Act`-CTL (see, for example, Bradfield (1991)) into $\mathbb{L}$, for example, $\mathsf{EF}_{\alpha}\,\neg(\exists\beta)\mathtt{tt}$ ('there is an α-path on which, eventually, there is no β-successor state') translates into $\mu Z.(\neg(\exists\beta)\mathtt{tt}) \vee (\exists\alpha)Z$. We also make liberal use of `Act`-CTL connectives as abbreviations of their corresponding syntactic equivalents in $\mathbb{L}$.

The logic's denotational semantics $[\![\ \cdot\ ]\!]^{\mathrm{m}}$ maps formulas ϕ and environments ρ into sets of states for a mode of analysis $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$; its definition, in Figure 5, uses a variable environment $\rho = (\rho^{\mathrm{a}}, \rho^{\mathrm{c}})$ such that $\rho^{\mathrm{m}} : \mathit{var} \to \mathscr{P}(\Sigma)$ for $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$. Note that $\neg\mathrm{a} \stackrel{\text{def}}{=} \mathrm{c}$, $\neg\mathrm{c} \stackrel{\text{def}}{=} \mathrm{a}$, and $\mathrm{pre}^{\mathrm{m}}_{\alpha}(A) \stackrel{\text{def}}{=} \{s \in \Sigma \mid \exists s' \in \Sigma,\ (s, \alpha, s') \in R^{\mathrm{m}},\ s' \in A\}$.

We write $s \models^{\mathrm{a}}_{\rho} \phi$ iff $s \in [\![\ \phi\ ]\!]^{\mathrm{a}}_{\rho}$ and say that ϕ is a (ρ-)*valid* assertion at s. Similarly, we write $s \models^{\mathrm{c}}_{\rho} \phi$ iff $s \in [\![\ \phi\ ]\!]^{\mathrm{c}}_{\rho}$, and say that ϕ is (ρ-)*consistent* at s. (If ϕ is closed, we elide ρ.)

The semantics in Figure 5 is the standard one for labelled transition systems with signature `Act`, *except* for the treatment of negation: to evaluate $\neg\phi$ in mode m, first evaluate ϕ in mode $\neg$m and then negate that result (Kelb 1994). Least fixed points $\mathrm{lfp}\, F^{\mathrm{m}}$ are computed in the complete lattice $(\mathscr{P}(\Sigma), \subseteq)$. For the standard syntactic approximations

of fixed-point formulas $\mu Z.\phi$

$$\mu_0 Z.\phi \stackrel{\text{def}}{=} \neg \mathtt{tt} \qquad \mu_{l+1} Z.\phi \stackrel{\text{def}}{=} \phi[Z \mapsto \mu_l Z.\phi] \qquad (l \geqslant 0) \tag{2}$$

we have $s \models^{\mathrm{m}}_{\rho} \mu Z.\phi$ in a mixed transition system iff $s \models^{\mathrm{m}}_{\rho} \mu_l Z.\phi$ for some $l \geqslant 0$; *provided* that Σ is finite or $\mu Z.\phi$ is unnested (Larsen 1990) – no fixed-point subformulas depend on an outer fixed point. (As is customary, $\phi[Z \mapsto \psi]$ denotes the formula obtained by replacing all free occurrences of Z in ϕ with ψ.)

Example 3 (Valid and consistent assertions). Consider the modal transition system in Figure 2 (right). The assertion $\neg(\exists w)(\exists r)\mathtt{tt}$ is valid at all states, because we fail to prove that $(\exists w)(\exists r)\mathtt{tt}$ is consistent – there is no sequence of two R^{c}-transitions labelled by w and then r.

The property $(\exists r)(\exists r)(\exists er)(\exists w)\mathtt{tt}$ is consistent at *Sleep*, because we can find (at *Sleep*) a sequence of four R^{c}-transitions labelled by these actions in that order. (The assertion is valid, however, at no state.)

Finally, we see that $\neg\mu Z.\neg(\exists w)(\exists ew)\neg Z$ is valid at *Sleep*, because the system allows arbitrarily many cycles of write acquisitions and releases along guaranteed arcs before a read is performed.

Environments ρ are *sound for* $\mathscr{M}$ iff for all $s \prec_{\mathscr{M}} t$ and $Z \in var$, $t \in \rho^{\mathrm{a}}(Z)$ implies $s \in \rho^{\mathrm{a}}(Z)$ and $s \in \rho^{\mathrm{c}}(Z)$ implies $t \in \rho^{\mathrm{c}}(Z)$.

Theorem 1 (Soundness of semantics with respect to refinement (Huth *et al.* 2001)). For any mixed transition system $\mathscr{M}$ with signature $\mathtt{Act}$, let $s, t \in \Sigma_{\mathscr{M}}$ and $s \prec_{\mathscr{M}} t$. For every $\phi \in \mathbb{L}$ with signature $\mathtt{Act}$ and every sound environment ρ:

1 If $t \models^{\mathrm{a}}_{\rho} \phi$, then $s \models^{\mathrm{a}}_{\rho} \phi$.
2 If $s \models^{\mathrm{c}}_{\rho} \phi$, then $t \models^{\mathrm{c}}_{\rho} \phi$.

Proof. The two items are proved by a nested induction: the outermost induction is on the fixed-point depth and the innermost induction on the structure of a formula ϕ.

— There is nothing to show for the clause $\mathtt{tt}$; for clause Z, we use the soundness of ρ.
— For $\neg\phi$:
  – Let $t \models^{\mathrm{a}}_{\rho} \neg\phi$. Then $t \not\models^{\mathrm{c}}_{\rho} \phi$. By induction on item 2, we infer $s \not\models^{\mathrm{c}}_{\rho} \phi$, that is, $s \models^{\mathrm{a}}_{\rho} \neg\phi$.
  – Let $s \models^{\mathrm{c}}_{\rho} \neg\phi$. Then $s \not\models^{\mathrm{a}}_{\rho} \phi$. By induction on item 1, we infer $t \not\models^{\mathrm{a}}_{\rho} \phi$, that is, $t \models^{\mathrm{c}}_{\rho} \neg\phi$.
— For $\phi_1 \wedge \phi_2$:
  – Let $t \models^{\mathrm{a}}_{\rho} \phi_1 \wedge \phi_2$. Then $t \models^{\mathrm{a}}_{\rho} \phi_i$ for $i = 1, 2$. By induction on item 1, we infer $s \models^{\mathrm{a}}_{\rho} \phi_i$ for $i = 1, 2$; that is, $s \models^{\mathrm{a}}_{\rho} \phi_1 \wedge \phi_2$.
  – Let $s \models^{\mathrm{c}}_{\rho} \phi_1 \wedge \phi_2$. Then $s \models^{\mathrm{c}}_{\rho} \phi_i$ for $i = 1, 2$. By induction on item 2, we infer $t \models^{\mathrm{c}}_{\rho} \phi_i$ for $i = 1, 2$; that is, $t \models^{\mathrm{c}}_{\rho} \phi_1 \wedge \phi_2$.

— For $(\exists\alpha)\,\phi$:
  - Let $t \models^{\mathrm{a}}_{\rho} (\exists\alpha)\,\phi$. Then there exists some $(t, \alpha, t') \in R^{\mathrm{a}}$ such that $t' \models^{\mathrm{a}}_{\rho} \phi$. Since $s \prec_{\mathscr{M}} t$, there exists some $s' \in \Sigma$ such that $(s, \alpha, s') \in R^{\mathrm{a}}$ and $s' \prec_{\mathscr{M}} t'$. By induction on item 1, $t' \models^{\mathrm{a}}_{\rho} \phi$ implies $s' \models^{\mathrm{a}}_{\rho} \phi$. But then $(s, \alpha, s') \in R^{\mathrm{a}}$ secures $s \models^{\mathrm{a}}_{\rho} (\exists\alpha)\,\phi$.
  - Let $s \models^{\mathrm{c}}_{\rho} (\exists\alpha)\,\phi$. Then there exists some $(s, \alpha, s') \in R^{\mathrm{c}}$ such that $s' \models^{\mathrm{c}}_{\rho} \phi$. Since $s \prec_{\mathscr{M}} t$, there exists some $t' \in \Sigma$ such that $(t, \alpha, t') \in R^{\mathrm{c}}$ and $s' \prec_{\mathscr{M}} t'$. By induction on item 2, $s' \models^{\mathrm{c}}_{\rho} \phi$ implies $t' \models^{\mathrm{c}}_{\rho} \phi$. But then $(t, \alpha, t') \in R^{\mathrm{c}}$ secures $t \models^{\mathrm{c}}_{\rho} (\exists\alpha)\,\phi$.

— For $\mu Z.\phi$, let $\mathsf{L}[\Sigma, \prec]$ be the collection of lower subsets L of Σ with respect to $\prec$: $t \in L$ and $s \prec t$ imply $s \in L$. Dually, $\mathsf{U}[\Sigma, \prec]$ is the collection of upper subsets U of Σ with respect to $\prec$: $s \in U$ and $s \prec t$ imply $t \in U$. We set $F^{\mathrm{m}}_0 \stackrel{\text{def}}{=} \varnothing$, $F^{\mathrm{m}}_{\gamma+1} \stackrel{\text{def}}{=} F^{\mathrm{m}}(F^{\mathrm{m}}_{\gamma})$, and $F^{\mathrm{m}}_{\lambda} \stackrel{\text{def}}{=} \bigcup_{\gamma<\lambda} F^{\mathrm{m}}_{\gamma}$ for limit ordinals λ.
  - By induction on ϕ and the fact that lower sets are closed under arbitrary unions, $F^{\mathrm{a}}_{\gamma} \in \mathsf{L}[\Sigma, \prec]$ for all ordinals γ. Since $\mathrm{lfp} F^{\mathrm{a}}$ is of that form, we have shown item 1.
  - Similarly, we infer $F^{\mathrm{c}}_{\gamma} \in \mathsf{U}[\Sigma, \prec]$ for all ordinals γ. Since $\mathrm{lfp} F^{\mathrm{c}}$ is of that form, this shows item 2. □

Theorem 1 is central to the utility of model-checking partial systems: item 1 says that all assertions that are valid at state t remain valid at all states that refine t. Dually, item 2 states that properties consistent at state s remain consistent for states that abstract s. Note that item 2 is required even if there is no need for explicit consistency checks – validating $\neg\phi$ at state t amounts to checking whether ϕ is consistent at t.

2.4. *De Morgan duals*

The propositional operators falsity ($\mathtt{ff}$), disjunction ($\phi \vee \phi$), implication ($\phi \to \phi$), universal branching ($(\forall\alpha)\,\phi$) and greatest fixed points ($\nu Z.\phi$) are expressed in $\mathbb{L}$ in the expected way:

$$\mathtt{ff} \stackrel{\text{def}}{=} \neg\mathtt{tt} \qquad \phi_1 \vee \phi_2 \stackrel{\text{def}}{=} \neg(\neg\phi_1 \wedge \neg\phi_2)$$
$$\phi_1 \to \phi_2 \stackrel{\text{def}}{=} \neg(\phi_1 \wedge \neg\phi_2) \qquad (\forall\alpha)\,\phi \stackrel{\text{def}}{=} \neg(\exists\alpha)\,\neg\phi$$
$$\nu Z.\phi \stackrel{\text{def}}{=} \neg\mu Z.\neg\phi[Z \mapsto \neg Z].$$

Remark 1 (Semantics of De Morgan duals). In every mixed transition system with state set Σ for every mode $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$, state $s \in \Sigma$, and environment ρ, we have

1 $s \not\models^{\mathrm{m}}_{\rho} \mathtt{ff}$.
2 $s \models^{\mathrm{m}}_{\rho} \phi_1 \vee \phi_2$ iff $s \models^{\mathrm{m}}_{\rho} \phi_1$ or $s \models^{\mathrm{m}}_{\rho} \phi_2$.
3 $s \models^{\mathrm{m}}_{\rho} \phi_1 \to \phi_2$ iff $s \not\models^{\neg\mathrm{m}}_{\rho} \phi_1$ or $s \models^{\mathrm{m}}_{\rho} \phi_2$.
4 $s \models^{\mathrm{m}}_{\rho} (\forall\alpha)\,\phi$ iff for all $s' \in \Sigma$, $(s, \alpha, s') \in R^{\neg\mathrm{m}}$ implies $s' \models^{\mathrm{m}}_{\rho} \phi$.
5 If Σ is finite or if $\nu Z.\phi$ is unnested (Larsen 1990), then $s \models^{\mathrm{m}}_{\rho} \nu Z.\phi$ iff for all $l \geqslant 0$ we have $s \not\models^{\neg\mathrm{m}}_{\rho} \mu_l Z.\neg\phi[Z \mapsto \neg Z]$.

The last three items of Remark 1 highlight the treatment of negation in mixed transition systems: in mode m, we can (3) verify an implication by refuting its premise in the dual mode or by verifying its conclusion in the original mode; (4) verify a universally branching formula $(\forall\alpha)\,\phi$ by showing that all $R^{\neg\mathrm{m}}$-successor states satisfy ϕ in mode m; and

(5) verify a greatest fixed point $\nu Z.\phi$ be refuting all syntactic approximations of a dual least fixed point in the dual mode. The derivation of (4) is instructive: $s \models^{\mathrm{m}} (\forall\alpha)\phi$ iff $s \models^{\mathrm{m}} \neg(\exists\alpha)\neg\phi$ iff not $(s \models^{\neg\mathrm{m}} (\exists\alpha)\neg\phi)$ iff not (for some s', $(s,\alpha,s') \in R^{\neg\mathrm{m}}$ and $s \models^{\neg\mathrm{m}} \neg\phi$) iff not (for some s', $(s,\alpha,s') \in R^{\neg\mathrm{m}}$ and not $(s \models^{\mathrm{m}} \phi)$) iff for all s', $(s,\alpha,s') \in R^{\neg\mathrm{m}}$ implies $s \models^{\mathrm{m}} \phi$.

2.5. *Totality*

Modal transition systems are partial systems whose total versions render an established model-checking framework.

Theorem 2 (Totality for modal transition systems). Let $\mathscr{M} = (\Sigma, R^{\mathrm{a}}, R^{\mathrm{c}})$ be a modal transition system with signature `Act` that is total: $R^{\mathrm{a}} = R^{\mathrm{c}}$. Then: for all $\phi \in \mathbb{L}$ and ρ with $\rho^{\mathrm{a}} = \rho^{\mathrm{c}}$: $[\![\phi]\!]^{\mathrm{a}}_{\rho}$ equals $[\![\phi]\!]^{\mathrm{c}}_{\rho}$; the semantics $[\![\phi]\!]^{\mathrm{m}}_{\rho}$ is the usual one for the labelled transition system (Σ, R^{m}); and every refinement in $\mathscr{M}$, in particular, $\prec_{\mathscr{M}}$, is a bisimulation.

Proof.

1 The proof that $[\![\phi]\!]^{\mathrm{a}}_{\rho} = [\![\phi]\!]^{\mathrm{c}}_{\rho}$ is a straightforward induction, which uses $\rho^{\mathrm{a}} = \rho^{\mathrm{c}}$ for clause Z and $R^{\mathrm{a}} = R^{\mathrm{c}}$ for clause $(\exists\alpha)\,\phi$.

2 If $[\![\phi]\!]^{\mathrm{a}}_{\rho} = [\![\phi]\!]^{\mathrm{c}}_{\rho}$ for all ϕ, then the semantics in Figure 5 is the standard one for labelled transition systems with signature `Act`.

3 If $R^{\mathrm{a}} = R^{\mathrm{c}}$, then Definition 3 is the definition of a bisimulation. □

Theorem 2 justifies our liberal use of $\models$ for $\models^{\mathrm{a}}$ and $\models^{\mathrm{c}}$ over total models.

2.6. *Maximal consistency*

For a pointed mixed transition system $(\mathscr{M}, i)$ with $i \models^{\mathrm{a}} \phi$, it is desirable that ϕ be satisfiable in a refining total model: $j \models \phi$ for a total model $(\mathscr{N}, j)$ with $(\mathscr{N}, j) \prec (\mathscr{M}, i)$.

Definition 4 (Consistent mixed transition systems). A mixed transition system $\mathscr{M}$ is *consistent* iff for all its states s and for all $\phi \in \mathbb{L}$, we have $s \models^{\mathrm{a}} \phi$ implies that ϕ is satisfiable over some total refining model: there is some state t in some labelled transition system $\mathscr{L}$ such that $t \models \phi$ and $(\mathscr{L}, t) \prec (\mathscr{M}, s)$.

Example 4 (An inconsistent mixed transition system). Consider the mixed transition system consisting of one state s and one $R^{\mathrm{a}} \setminus R^{\mathrm{c}}$ self-transition labelled by α: $\mathscr{M} = (\{s\}, \{(s,\alpha,s)\}, \varnothing)$.

Because of the guaranteed transition, we have that $s \models^{\mathrm{a}} (\exists\alpha)\mathtt{tt}$, but the lack of R^{c}-transitions implies that $s \not\models^{\mathrm{c}} (\exists\alpha)\mathtt{tt}$. By the semantics of negation and conjunction, we infer $s \models^{\mathrm{a}} (\exists\alpha)\mathtt{tt} \wedge \neg(\exists\alpha)\mathtt{tt}$, but the latter formula is clearly not satisfiable in labelled transition systems. In particular, it cannot be satisfied in some refining total model.

We now present a condition on mixed transition systems that guarantees their consistency and is met in all modal transition systems. This condition has an established domain-theoretic analogue (Heckmann 1990; Gunter 1992), which we will use in the next section to build a universal domain of consistent mixed transition systems.

Definition 5 (The mix condition (MC)). A mixed transition system

$$\mathscr{M} = (\Sigma, R^{\mathrm{a}}, R^{\mathrm{c}})$$

satisfies the *mix condition* (MC) iff for all $(s, \alpha, s') \in R^{\mathrm{a}}$, there is some $s'' \in \Sigma$ such that $(s, \alpha, s'') \in R^{\mathrm{a}} \cap R^{\mathrm{c}}$ and $s'' \prec s'$.

Condition (MC) is satisfied for all modal transition systems, since we may choose s'' to be s' whenever $R^{\mathrm{a}} \subseteq R^{\mathrm{c}}$. Conversely, any mixed transition system that satisfies (MC) has a modal transition system as a *saturated version.*

Definition 6 (Saturated mixed transition system). For every mixed transition system $\mathscr{M} = (\Sigma, R^{\mathrm{a}}, R^{\mathrm{c}})$, we define the *saturated mixed transition system* $\tilde{\mathscr{M}} = (\Sigma, \tilde{R}^{\mathrm{a}}, \tilde{R}^{\mathrm{c}})$, where $\tilde{R}^{\mathrm{a}} \stackrel{\mathrm{def}}{=} R^{\mathrm{a}} \cap R^{\mathrm{c}}$ and $\tilde{R}^{\mathrm{c}} \stackrel{\mathrm{def}}{=} R^{\mathrm{c}}$.

Unlike the definitions above, the alternative one of letting $\tilde{R}^{\mathrm{a}}$ be R^{a} and $\tilde{R}^{\mathrm{c}}$ be the union of R^{a} and R^{c} renders a modal transition system that is *not* equivalent to $\mathscr{M}$.

Proposition 1. Let $\mathscr{M} = (\Sigma, R^{\mathrm{a}}, R^{\mathrm{c}})$ be a mixed transition system with start state i satisfying condition (MC). Then $(\tilde{\mathscr{M}}, i)$ is a pointed modal transition system such that $(\tilde{\mathscr{M}}, i) \prec_{\mathscr{M}} (\mathscr{M}, i)$ and $(\mathscr{M}, i) \prec_{\mathscr{M}} (\tilde{\mathscr{M}}, i)$.

Proof. Let $s \prec_{\mathscr{M}} t$.

— We show that $(\tilde{\mathscr{M}}, i) \prec_{\mathscr{M}} (\mathscr{M}, i)$:
  - If $(t, \alpha, t') \in R^{\mathrm{a}}$, then $s \prec_{\mathscr{M}} t$ implies the existence of some $(s, \alpha, s') \in R^{\mathrm{a}}$ such that $s' \prec_{\mathscr{M}} t'$. Using the condition (MC), there exists some $(s, \alpha, s'') \in R^{\mathrm{a}} \cap R^{\mathrm{c}} = \tilde{R}^{\mathrm{a}}$ such that $s'' \prec_{\mathscr{M}} s'$. By transitivity of $\prec_{\mathscr{M}}$, we get $s'' \prec_{\mathscr{M}} t'$ and have $(s, \alpha, s'') \in \tilde{R}^{\mathrm{a}}$.
  - If $(s, \alpha, s') \in \tilde{R}^{\mathrm{c}} = R^{\mathrm{c}}$, then $s \prec_{\mathscr{M}} t$ implies $(t, \alpha, t') \in R^{\mathrm{c}}$ for some $t' \in \Sigma$ such that $s' \prec_{\mathscr{M}} t'$.

— We show that $(\mathscr{M}, i) \prec_{\mathscr{M}} (\tilde{\mathscr{M}}, i)$:
  - If $(t, \alpha, t') \in \tilde{R}^{\mathrm{a}} = R^{\mathrm{a}} \cap R^{\mathrm{c}}$, then $s \prec_{\mathscr{M}} t$ implies $(s, \alpha, s') \in R^{\mathrm{a}}$ for some $s' \in \Sigma$ such that $s' \prec_{\mathscr{M}} t'$.
  - If $(s, \alpha, s') \in R^{\mathrm{c}}$, then $s \prec_{\mathscr{M}} t$ implies the existence of some $(t, \alpha, t') \in R^{\mathrm{c}} = \tilde{R}^{\mathrm{c}}$ such that $s' \prec_{\mathscr{M}} t'$. □

This result informs us that any mixed transition system that meets condition (MC) is merely an unsaturated version of a modal transition system and that these two systems cannot be distinguished *via* observations through $\models^{\mathrm{a}}$ or $\models^{\mathrm{c}}$ (by Theorem 1). In that sense, modal transition systems and mixed transition systems satisfying condition (MC) are equally expressive for the purposes of design and analysis; these systems are all consistent.

Theorem 3. Let $\mathscr{M}$ be a mixed transition system with signature `Act` that satisfies the mix condition (MC).

1 $\mathscr{M}$ is consistent.
2 For every ρ with $\rho^{\mathrm{a}}(Z) \subseteq \rho^{\mathrm{c}}(Z)$, $Z \in \mathit{var}$, and every $\phi \in \mathbb{L}$, we have $[\![\phi]\!]^{\mathrm{a}}_{\rho} \subseteq [\![\phi]\!]^{\mathrm{c}}_{\rho}$.
3 For every ρ with $\rho^{\mathrm{a}}(Z) \subseteq \rho^{\mathrm{c}}(Z)$, $Z \in \mathit{var}$, and every $\phi \in \mathbb{L}$, we have $[\![\phi \wedge \neg\phi]\!]^{\mathrm{a}}_{\rho} = \varnothing$.

Proof.

— For (1), let $\phi \in \mathbb{L}$ such that $(\mathscr{M}, s) \models^{\mathrm{a}}_{\rho} \phi$. Define $\mathscr{N} = (\Sigma, R^{\mathrm{a}} \cap R^{\mathrm{c}}, R^{\mathrm{a}} \cap R^{\mathrm{c}})$. An analogous reasoning to that given for the first part of Proposition 1 then renders $(\mathscr{N}, s) \prec_{\mathscr{M}} (\mathscr{M}, s)$. Thus, $(\mathscr{M}, s) \models^{\mathrm{a}}_{\rho} \phi$ implies $(\mathscr{N}, s) \models^{\mathrm{a}}_{\rho} \phi$ by Theorem 1. Applying Theorem 2 to $\mathscr{N}$, we infer that $s \models^{\mathrm{a}}_{\rho} \phi$ in the labelled transition system $\mathscr{L} \stackrel{\text{def}}{=} (\Sigma, R^{\mathrm{a}} \cap R^{\mathrm{c}})$, so $\mathscr{M}$ is consistent.

— We prove (2) by structural induction on ϕ; the clauses for $\mathtt{tt}$, $\neg$, $\wedge$ and $\mu Z.\phi$ are routine. For clause Z, we use the assumption that $\rho^{\mathrm{a}}(Z) \subseteq \rho^{\mathrm{c}}(Z)$ for every $Z \in \mathit{var}$. For $(\exists \alpha)$, let $s \in [\![(\exists \alpha)\, \phi]\!]^{\mathrm{a}}_{\rho}$, that is, $s \models^{\mathrm{a}}_{\rho} (\exists \alpha)\, \phi$. Then there exists some $(s, \alpha, s') \in R^{\mathrm{a}}$ such that $s' \models^{\mathrm{a}} \phi$. From (MC), we then infer the existence of some $s'' \in \Sigma$ such that $(s, \alpha, s'') \in R^{\mathrm{a}} \cap R^{\mathrm{c}}$ and $s'' \prec s'$. So $s' \models^{\mathrm{a}}_{\rho} \phi$ and $s'' \prec s'$ imply $s'' \models^{\mathrm{a}}_{\rho} \phi$ by Theorem 1. By induction, this gives us $s'' \models^{\mathrm{c}}_{\rho} \phi$. But then $(s, \alpha, s'') \in R^{\mathrm{c}}$ implies $s \models^{\mathrm{c}}_{\rho} (\exists \alpha) \phi$.

— (2) and (3) are equivalent: the set $[\![\phi \wedge \neg \phi]\!]^{\mathrm{a}}_{\rho}$ is non-empty iff there is some $s \in \Sigma$ such that $s \models^{\mathrm{a}}_{\rho}$ and $s \not\models^{\mathrm{c}}{}_{\rho} \phi$ iff there is an element in $[\![\phi]\!]^{\mathrm{a}}_{\rho} \setminus [\![\phi]\!]^{\mathrm{c}}_{\rho}$ iff $[\![\phi]\!]^{\mathrm{a}}_{\rho}$ is not a subset of $[\![\phi]\!]^{\mathrm{c}}_{\rho}$. □

Example 5 (More precise property semantics). Our property semantics loses precision in two places: the interpretation of disjunction in the assertion mode a, and the interpretation of conjunction in the consistency checking mode c. For example, any formula ϕ with $s \models^{\mathrm{c}}_{\rho} \phi$ and $s \not\models^{\mathrm{a}}_{\rho} \phi$ renders $s \models^{\mathrm{c}}_{\rho} \phi \wedge \neg \phi$ and $s \not\models^{\mathrm{a}}_{\rho} \phi \vee \neg \phi$. Such loss of precision may severely impact the quality of an analysis. Various techniques exist for obtaining more precise interpretations, although at a significant increase in complexity: we mention the focus operation of Ball *et al.* (2001) for program analysis and the generalised model checking of Bruns and Godefroid (2000).

2.7. *An extension: non-flat data*

Up to this point, the modal transition systems have had flat data sets: together, R^{a} and R^{c} partially specify a binary relation R over a *discrete* set Σ. We use the mixed powerdomain to generalise modal transition systems to non-flat sets, modelled as domains (Abramsky and Jung 1994).

Definition 7 (Mixed powerdomain (Gunter 1992; Heckmann 1990)). Let $(D, \leqslant)$ be a bifinite domain (Jung 1988) – a domain D such that its identity function id_D be the directed image of Scott-continuous functions $d : D \to D$ with finite image and $d = d \circ d \leqslant \mathrm{id}_D$. The *mixed powerdomain* $\mathsf{M}[D]$ of $(D, \leqslant)$ consists of the set of all pairs (L, U), where L is Scott-closed in $(D, \leqslant)$ and U is a Scott-compact upper set in $(D, \leqslant)$ such that L and U satisfy the consistency condition

$$L = \downarrow(L \cap U). \tag{3}$$

The order in $\mathsf{M}[D]$ is given by

$$(L, U) \leqslant (L', U') \quad \stackrel{\text{def}}{=} \quad L \subseteq L' \text{ and } U' \subseteq U. \tag{4}$$

This is why elements of a mixed powerdomain might be used as states in a mixed transition system: a state should be characterised by both the assertions L that are guaranteed to hold true for it and by the assertions U that are possibly true for it; the pair is consistent

if $L = \downarrow(L \cap U)$. A state (L, U) should refine state (L', U') when $(L, U) \leqslant (L', U')$. These intuitions are formalised in the next section, but a small example is in order.

Example 6 (Mixed powerdomains).

1 For the domain $D = \{*\}$, each subset is Scott-closed and a Scott-compact upper set. However, the pair $(L, U) = (\{*\}, \varnothing)$ does not satisfy the consistency condition (3) as the right-hand side of (3) is then empty. The three remaining pairs $\texttt{false} \stackrel{\text{def}}{=} (\varnothing, \varnothing)$, $\bot \stackrel{\text{def}}{=} (\varnothing, \{*\})$, and $\texttt{true} \stackrel{\text{def}}{=} (\{*\}, \{*\})$ satisfy (3) and comprise all elements of $\mathsf{M}[D]$. For the ordering, (4) informs us that $\bot \leqslant \texttt{false}$ and $\bot \leqslant \texttt{true}$ are the only non-reflexive instances of $\leqslant$ in $\mathsf{M}[D]$ (Heckmann 1990).
2 Let D be a finite set with a preorder $\leqslant$. Elements of $\mathsf{M}[D]$ are pairs (L, U), where L is a lower and U is an upper set with respect to $\leqslant$. If the ordering is flat, the consistency conditions reads as $L \subseteq U$.

As an element of a powerdomain, every $(L, U) \in \mathsf{M}[D]$ models a 'set' A. However, claims of the form, *"Element d is contained in the 'set' A"*, have *three*, instead of the conventional two, possible outcomes: `false` if $d \notin U$; `true` if $d \in L$; and $\bot$ otherwise, that is, if $d \in U \setminus L$. The Scott-closed set L specifies firm guarantees of membership, whereas the Scott-compact upper set U specifies the possibility of membership. Naturally, this three-valued interpretation of membership determines a three-valued interpretation of existential quantification, as worked out in Heckmann (1990). Non-flat data routinely arises in the framework of abstract interpretation (Cousot and Cousot 1977).

Example 7 (Multiple viewpoints). Non-flat applications of modal transition systems also occur in software engineering in the context of requirements analysis and consistency checking (Nuseibeh *et al.* 1994). In a simplified scenario, each element of a finite domain $(D, \leqslant)$ is a pointed modal transition system d, and $d \leqslant e$ expresses the fact that e has higher or equal priority to d. Each d is a different view of a software artifact. Assertions validated at a viewpoint are obliged to hold at viewpoints of lesser priority. In the light of Theorem 1, this means that properties consistent at a viewpoint are obliged to be consistent in viewpoints of higher priorities. A semantics collects these obligations of validity $\{\!|\mathscr{M}:\phi|\!\}^{\mathrm{a}}$ and consistency $\{\!|\mathscr{M}:\phi|\!\}^{\mathrm{c}}$ (Huth and Pradhan 2002)

$$\begin{aligned} \{\!|\mathscr{M}:\phi|\!\}^{\mathrm{a}} &\stackrel{\text{def}}{=} \{d \in D \mid \exists e \in D : d \leqslant e,\ e \models^{\mathrm{a}} \phi\} \\ \{\!|\mathscr{M}:\phi|\!\}^{\mathrm{c}} &\stackrel{\text{def}}{=} \{d \in D \mid \exists e \in D : e \leqslant d,\ e \models^{\mathrm{c}} \phi\} \\ \{\!|\mathscr{M}:\phi|\!\} &\stackrel{\text{def}}{=} (\{\!|\mathscr{M}:\phi|\!\}^{\mathrm{a}}, \{\!|\mathscr{M}:\phi|\!\}^{\mathrm{c}}). \end{aligned} \tag{5}$$

In general, $\{\!|\mathscr{M}:\phi|\!\}^{\mathrm{a}}$ will not be a subset of $\{\!|\mathscr{M}:\phi|\!\}^{\mathrm{c}}$, but $\{\!|\mathscr{M}:\phi|\!\}$ is an element of $\mathsf{M}[D]$, since $e \models^{\mathrm{a}} \phi$ implies $e \models^{\mathrm{c}} \phi$ for pointed modal transition systems e by Theorem 3.3. Given an inconsistent set Φ of properties, $\cap_{\phi \in \Phi} \{\!|\mathscr{M}:\phi|\!\}^{\mathrm{a}}$ identifies viewpoints that are impacted by this inconsistency. For a full exposition of this semantics and its usage in the detection, location and mitigation of inconsistencies, refer to Huth and Pradhan (2002).

3. A domain equation for modal transition systems

Powerdomains (Plotkin 1976; Smyth 1978; Abramsky and Jung 1994) are recognised and widely used as spaces of meaning for the denotational semantics of systems that exhibit non-determinism. Powerdomains that are the initial solution to a domain equation have also been used as internally fully abstract models of systems that specify concurrent systems and their abstraction order. For example, Abramsky (Abramsky 1991) used an adaptation of the convex powerdomain (Plotkin 1976) to model labelled transition systems and partial bisimulations. In this section, we apply the machinery of powerdomains and domain equations to provide a domain-theoretic model for mixed transition systems that meet condition (MC) and for their refinement. It is a pleasant surprise that the mixed powerdomain, discovered independently by Gunter (Gunter 1992) and Heckmann (Heckmann 1990), serves as a ready-to-use meaning space for this task. Throughout this section, we assume a fixed finite signature `Act` and use the well-known topological representations of powerdomains. For the purpose at hand, we work with countably based bifinite domains (Jung 1988).

For simplicity, the items described in the remark below represent Scott-closed subsets as sets of lower sets of compact elements. For $x \in (D, \leqslant)$ we write $\uparrow x = \{y \in D \mid x \leqslant y\}$.

Remark 2 (Universal property of the mixed powerdomain (Heckmann 1990)). For all countably based bifinite domains D and E:

1 $\mathsf{M}[D]$ is a countably based bifinite domain.
2 The map $d \mapsto \{\!|d|\!\} : D \to \mathsf{M}[D]$, defined by $\{\!|d|\!\} \stackrel{\text{def}}{=} (\{k \in D \mid k \leqslant d,\ k \text{ compact}\}, \uparrow d)$, is continuous.
3 The formal union operator $\bar{\cup} : \mathsf{M}[D] \times \mathsf{M}[D] \to \mathsf{M}[D]$, defined by

$$(L, U) \,\bar{\cup}\, (L', U') \stackrel{\text{def}}{=} (L \cup L', U \cup U') \tag{6}$$

is continuous.
4 For any continuous function $f : D \to \mathsf{M}[E]$, there exists a unique continuous map $\bar{f} : \mathsf{M}[D] \to \mathsf{M}[E]$ such that $\bar{f} \circ \bar{\cup} = \bar{\cup} \circ \bar{f} \times \bar{f}$ and $\bar{f} \circ \{\!|\cdot|\!\} = f$.
5 All compact elements of $\mathsf{M}[D]$ are obtained by a finite application of the constant $\bar{\varnothing} \stackrel{\text{def}}{=} (\varnothing, \varnothing)$ and the operations $\bar{\cup}$, $\{\!|\cdot|\!\}$, and $\{\!|\cdot ?|\!\}$ to compact elements of D; where $\{\!|d?|\!\} \stackrel{\text{def}}{=} (\varnothing, \uparrow d)$.

3.1. *The universal domain as a fully abstract mixed transition system*

For mixed transition systems, our discussion of membership in $\mathsf{M}[D]$ suggests we use Scott-closed sets as a model of the set of R^{a}-successors of a state, and Scott-compact upper sets as a model of the set of R^{c}-successors of a state. Fortunately, there is an intimate connection between the condition (MC), which guarantees consistency, and the domain-theoretic consistency condition (3).

Definition 8 (Universal domain). In the style of Abramsky's domain equation for partial bisimulation (Abramsky 1991), we let $\mathscr{D}_{\mathtt{Act}}$ be the initial solution to the domain equation

$$D = \prod_{\alpha \in \mathtt{Act}} \mathsf{M}[D] \tag{7}$$

over bifinite domains and Scott-continuous maps, where $\prod_{\alpha\in\mathtt{Act}} D_\alpha$ denotes the categorical product of the domains D_α whose elements are tuples $(d_\alpha)_{\alpha\in\mathtt{Act}}$ with $d_\alpha \in D_\alpha$ for all $\alpha \in \mathtt{Act}$. We write $\mathscr{D}$ for $\mathscr{D}_{\mathtt{Act}}$ if $\mathtt{Act}$ is determined by context or irrelevant. We write $\bot_{\mathscr{D}}$ for the bottom element $((\varnothing, \mathscr{D}))_{\alpha\in\mathtt{Act}}$ of $\mathscr{D}$.

We note that $\mathscr{D}$ is well defined since $\mathsf{M}[\cdot]$ and $\prod$ are locally continuous functors in the category of countably based bifinite domains and Scott-continuous maps (Heckmann 1990; Abramsky and Jung 1994). According to (7), any element d of $\mathscr{D}$ corresponds to a tuple of pairs $((L_\alpha, U_\alpha))_{\alpha\in\mathtt{Act}}$, where $(L_\alpha, U_\alpha) \in \mathsf{M}[D]$ for each $\alpha \in \mathtt{Act}$.

Definition 9 (Universal domain as a mixed transition system).

1 For every $d = ((L_\beta, U_\beta))_{\beta\in\mathtt{Act}} \in \mathscr{D}$ and $\alpha \in \mathtt{Act}$, we define

$$d_\alpha \stackrel{\text{def}}{=} (L_\alpha, U_\alpha), \qquad d^{\mathrm{a}}_\alpha \stackrel{\text{def}}{=} L_\alpha, \qquad d^{\mathrm{c}}_\alpha \stackrel{\text{def}}{=} U_\alpha. \tag{8}$$

2 We define state transition relations $\mathscr{R}^{\mathrm{m}} \subseteq \mathscr{D} \times \mathtt{Act} \times \mathscr{D}$:

$$\begin{aligned} \mathscr{R}^{\mathrm{a}} &\stackrel{\text{def}}{=} \{(d, \alpha, d') \mid \alpha \in \mathtt{Act},\ d' \in d^{\mathrm{a}}_\alpha\} \\ \mathscr{R}^{\mathrm{c}} &\stackrel{\text{def}}{=} \{(d, \alpha, d') \mid \alpha \in \mathtt{Act},\ d' \in d^{\mathrm{c}}_\alpha\}. \end{aligned} \tag{9}$$

We note that suprema in $\mathscr{D}$ are computed component-wise. Therefore, $d \in \mathscr{D}$ is compact in $\mathscr{D}$ iff for all $\alpha \in \mathtt{Act}$, d_α is compact in $\mathsf{M}[\mathscr{D}]$.

Remark 3 (Elements of $\mathscr{D}$ as pointed systems). Each element d of $\mathscr{D}$ represents a pointed mixed transition system. The start state is d, and its sets of $\mathscr{R}^{\mathrm{a}}$-reachable and $\mathscr{R}^{\mathrm{c}}$-reachable states are defined inductively in the standard manner *via* (9). Note that the operation $\prod_{\alpha\in\mathtt{Act}} \bar{\cup}$ has type $\mathscr{D} \times \mathscr{D} \to \mathscr{D}$, using the isomorphism implicit in the '=' of (7) as a casting and the general distributivity of products; it elegantly models the sum of pointed mixed transition systems.

As a mixed transition system, the domain $\mathscr{D}$ has a greatest refinement $\prec_{\mathscr{D}}$. We can already prove one half of the statement that the relational inverse of $\prec_{\mathscr{D}}$ is the order on the domain $\mathscr{D}$.

Proposition 2 (Order of universal domain as abstraction). The relational inverse of the ordering on $\mathscr{D}$ is a refinement in the mixed transition system $(\mathscr{D}, \mathscr{R}^{\mathrm{a}}, \mathscr{R}^{\mathrm{c}})$.

Proof. Let $e \leqslant^{\mathrm{op}} d$, that is, $d \leqslant e$ in $\mathscr{D}$. Let $\alpha \in \mathtt{Act}$.

1 If $(d, \alpha, d') \in \mathscr{R}^{\mathrm{a}}$, then $d' \in d^{\mathrm{a}}_\alpha$. But then $d \leqslant e$ implies $d' \in d^{\mathrm{a}}_\alpha \subseteq e^{\mathrm{a}}_\alpha$, that is, $(e, \alpha, d') \in \mathscr{R}^{\mathrm{a}}$; clearly, $d' \leqslant^{\mathrm{op}} d'$.

2 If $(e, \alpha, e') \in \mathscr{R}^{\mathrm{c}}$, then $e' \in e^{\mathrm{c}}_\alpha$ follows. But then $d \leqslant e$ implies $e' \in e^{\mathrm{c}}_\alpha \subseteq d^{\mathrm{c}}_\alpha$, that is, $(d, \alpha, e') \in \mathscr{R}^{\mathrm{c}}$; clearly, $e' \leqslant^{\mathrm{op}} e'$. □

$$\neg_{\mathrm{a}}\neg_{\mathrm{c}}\phi = \phi \qquad \neg_{\mathrm{c}}\neg_{\mathrm{a}}\phi = \phi$$
$$\phi \leqslant_{\mathrm{a}} \psi \Rightarrow \neg_{\mathrm{a}}\psi \leqslant_{\mathrm{c}} \neg_{\mathrm{a}}\phi \qquad \phi \leqslant_{\mathrm{c}} \psi \Rightarrow \neg_{\mathrm{c}}\psi \leqslant_{\mathrm{a}} \neg_{\mathrm{c}}\phi$$

Fig. 6. Axioms for AC-lattices.

The mixed transition system $(\mathscr{D}, \mathscr{R}^{\mathrm{a}}, \mathscr{R}^{\mathrm{c}})$ is not a modal transition system since the inclusion $\mathscr{R}^{\mathrm{a}} \subseteq \mathscr{R}^{\mathrm{c}}$ is a stronger condition than (3) for non-flat data. But condition (3) is simply the topological version of the mix condition (MC).

Proposition 3 (Universal domain satisfies mix condition). The mixed transition system $(\mathscr{D}, \mathscr{R}^{\mathrm{a}}, \mathscr{R}^{\mathrm{c}})$ satisfies the mix condition (MC).

Proof. Given (d, α, d') in $\mathscr{R}^{\mathrm{a}}$, we have $d' \in d^{\mathrm{a}}_{\alpha}$. By (3) and (7), there has to exist some $d'' \in d^{\mathrm{a}}_{\alpha} \cap d^{\mathrm{c}}_{\alpha}$ (that is, $(d, \alpha, d'') \in \mathscr{R}^{\mathrm{a}} \cap \mathscr{R}^{\mathrm{c}}$) such that $d' \leqslant d''$, that is, $d'' \prec d'$. □

That the relational inverse of the order in $\mathscr{D}$ equals $\prec_{\mathscr{D}}$ can be shown by a logical characterisation of refinement for a Hennessy–Milner logic (Hennessy and Milner 1985) $\mathbb{L}_{\mathrm{HM}}$, defined by the grammar

$$\phi ::= \mathtt{tt} \mid \neg\phi \mid \phi \wedge \phi \mid (\exists\alpha)\,\phi \tag{10}$$

where $\alpha \in \mathtt{Act}$. Since $\mathbb{L}_{\mathrm{HM}}$ is a sublogic of $\mathbb{L}$ without free variables, and since $(\mathscr{D}, \mathscr{R}^{\mathrm{a}}, \mathscr{R}^{\mathrm{c}})$ is a mixed transition system, we infer that the subsets $[\![\ \phi\ ]\!]^{\mathrm{a}}$ and $[\![\ \phi\ ]\!]^{\mathrm{c}}$ of $\mathscr{D}$ are well defined for all $\phi \in \mathbb{L}_{\mathrm{HM}}$, as specified in Figure 5. These meanings are elements of an assertion-consistency lattice (AC-lattice).

Definition 10 (AC-lattices (Huth and Pradhan 2002)). An *AC-lattice* is a tuple $(\mathscr{L}_{\mathrm{a}}, \leqslant_{\mathrm{a}}, \neg_{\mathrm{a}}, \mathscr{L}_{\mathrm{c}}, \leqslant_{\mathrm{c}}, \neg_{\mathrm{c}})$, where $(\mathscr{L}_{\mathrm{a}}, \leqslant_{\mathrm{a}})$ and $(\mathscr{L}_{\mathrm{c}}, \leqslant_{\mathrm{c}})$ are partial orders that induce lattices, and $\neg_{\mathrm{a}} : \mathscr{L}_{\mathrm{a}} \to \mathscr{L}_{\mathrm{c}}$ and $\neg_{\mathrm{c}} : \mathscr{L}_{\mathrm{c}} \to \mathscr{L}_{\mathrm{a}}$ are functions that meet the axioms of Figure 6.

A canonical example of AC-lattices are topological spaces X where $(\mathscr{L}^{\mathrm{a}}, \leqslant^{\mathrm{a}})$ and $(\mathscr{L}^{\mathrm{c}}, \leqslant^{\mathrm{c}})$ are the lattice of all closed and open subsets of X (respectively) – ordered by set inclusion; and $\neg^{\mathrm{a}}$ and $\neg^{\mathrm{c}}$ are set complementation. In Huth and Pradhan (2002), it is shown that – up to an order-isomorphism – this example is exhaustive for finite, distributive AC-lattices. The sets $[\![\ \phi\ ]\!]^{\mathrm{a}}$ and $[\![\ \phi\ ]\!]^{\mathrm{c}}$ of $\mathscr{D}$ form the elements of an AC-lattice within the canonical AC-lattice of the topological space $(\mathscr{D}, \sigma(\mathscr{D}))$, where $\sigma(\mathscr{D})$ denotes the Scott-topology of $\mathscr{D}$.

Definition 11 (AC-lattice operations in $\mathscr{D}$). For each $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$, we define the partial order $\mathbf{M}_{\mathrm{m}} \stackrel{\mathrm{def}}{=} \{[\![\ \phi\ ]\!]^{\mathrm{m}} \mid \phi \in \mathbb{L}_{\mathrm{HM}}\}$, ordered by inclusion, and a negation operation $\neg^{\mathrm{m}} : \mathbf{M}_{\mathrm{m}} \to \mathbf{M}_{\neg\mathrm{m}}$:

$$\neg^{\mathrm{m}}[\![\ \phi\ ]\!]^{\mathrm{m}} \stackrel{\mathrm{def}}{=} [\![\ \neg\phi\ ]\!]^{\neg\mathrm{m}}. \tag{11}$$

Theorem 4 (AC-lattice of $\mathscr{D}$).

1 The structure $(\mathbf{M}_{\mathrm{a}}, \subseteq, \neg^{\mathrm{a}}, \mathbf{M}_{\mathrm{c}}, \subseteq, \neg^{\mathrm{c}})$ is a distributive bounded AC-lattice, where $\neg^{\mathrm{a}}$ and $\neg^{\mathrm{c}}$ equal set complementation in the domain $\mathscr{D}$.
2 Each element of $\mathbf{M}_{\mathrm{a}}$ is Scott-open in $\mathscr{D}$ and each element of $\mathbf{M}_{\mathrm{c}}$ is Scott-closed in $\mathscr{D}$.

Proof.

1 Since $[\![\phi_1]\!]^{\mathrm{m}} \cap [\![\phi_2]\!]^{\mathrm{m}} = [\![\phi_1 \wedge \phi_2]\!]^{\mathrm{m}}$ and $[\![\phi_1]\!]^{\mathrm{m}} \cup [\![\phi_2]\!]^{\mathrm{m}} = [\![\neg(\neg\phi \wedge \neg\phi_2)]\!]^{\mathrm{m}}$, the partial orders $(\mathbf{M}_{\mathrm{m}}, \subseteq)$ determine lattices with bottom $[\![\neg\mathtt{tt}]\!]^{\mathrm{m}}$ and top $[\![\mathtt{tt}]\!]^{\mathrm{m}}$. Since $\neg\neg\mathrm{m} = \mathrm{m}$ and $[\![\neg\neg\phi]\!]^{\mathrm{m}} = [\![\phi]\!]^{\mathrm{m}}$, the first two axioms of Figure 6 are met. As for the remaining two axioms, let $d \in \neg^{\mathrm{m}}[\![\psi]\!]^{\mathrm{m}}$. Then $d \models^{\neg^{\mathrm{m}}} \neg\psi$ implies $d \not\models^{\mathrm{m}} \psi$ which, assuming $[\![\phi]\!]^{\mathrm{m}} \subseteq [\![\psi]\!]^{\mathrm{m}}$, implies $d \not\models^{\mathrm{m}} \phi$, that is, $d \in \neg^{\mathrm{m}}[\![\phi]\!]^{\mathrm{m}}$. The last claim about $\neg^{\mathrm{m}}$ follows since $d \models^{\neg^{\mathrm{m}}} \neg\phi$ iff $d \not\models^{\neg^{\neg^{\mathrm{m}}}} \phi$ iff $d \not\models^{\mathrm{m}} \phi$ iff $d \in \mathscr{D} \setminus [\![\phi]\!]^{\mathrm{m}}$.

2a To see that $[\![\phi]\!]^{\mathrm{a}}$ is an upper set in $\mathscr{D}$, let $d \in [\![\phi]\!]^{\mathrm{a}}$ and $d \leqslant e$ in $\mathscr{D}$. By Proposition 2, $e \prec d$. Since $d \models^{\mathrm{a}} \phi$, Theorem 1 implies $e \models^{\mathrm{a}} \phi$, that is, $e \in [\![\phi]\!]^{\mathrm{a}}$. An analogous proof shows that $[\![\phi]\!]^{\mathrm{c}}$ is a lower set in $\mathscr{D}$.

2b We show the remaining claims by simultaneous structural induction on (10):

(a) For $\mathtt{tt}$, this is clear as $\mathscr{D}$ is a Scott-closed and Scott-open subset of $\mathscr{D}$.

(b) For negation, this follows by induction from $[\![\neg\phi]\!]^{\mathrm{m}} = \mathscr{D} \setminus [\![\phi]\!]^{\neg^{\mathrm{m}}}$.

(c) For conjunction, this follows by induction since $[\![\phi_1 \wedge \phi_2]\!]^{\mathrm{m}} = [\![\phi_1]\!]^{\mathrm{m}} \cap [\![\phi_2]\!]^{\mathrm{m}}$.

(d) For $(\exists\alpha)\,\phi$, the proof for each mode is different and mode c makes use of the Hofmann–Mislove Theorem (Hofmann and Mislove 1981).

i Let $d \in [\![(\exists\alpha)\,\phi]\!]^{\mathrm{a}}$, which we know to be an upper set. Let D be the set of compact elements k in $\mathscr{D}$ such that $k \leqslant d$. For every $k \in D$ and $\alpha \in \mathtt{Act}$, k_α is compact and $k_\alpha \leqslant d_\alpha$ in $\mathsf{M}[D]$. Then $d^{\mathrm{a}}_\alpha \cap [\![\phi]\!]^{\mathrm{a}}$ equals the directed union $\bigcup_{k \in D} k^{\mathrm{a}}_\alpha \cap [\![\phi]\!]^{\mathrm{a}}$, using the fact that $\mathscr{D}$ is algebraic and that $[\![\phi]\!]^{\mathrm{a}}$ is Scott-open by induction. Since the former set is non-empty, there has to be some $k \in D$ for which $k^{\mathrm{a}}_\alpha \cap [\![\phi]\!]^{\mathrm{a}}$ is non-empty as well. But then $k \in [\![(\exists\alpha)\,\phi]\!]^{\mathrm{a}}$ for that k.

ii We already know that $[\![(\exists\alpha)\,\phi]\!]^{\mathrm{c}}$ is a lower set. For $D \subseteq [\![(\exists\alpha)\,\phi]\!]^{\mathrm{c}}$, where D is directed, let e be the supremum of D in $\mathscr{D}$. We use proof by contradiction. If e is not in $[\![(\exists\alpha)\,\phi]\!]^{\mathrm{c}}$, then e^{c}_α is contained in $\mathscr{D} \setminus [\![\phi]\!]^{\mathrm{c}}$, which is Scott-open by induction. Since $e^{\mathrm{c}}_\alpha = \bigcap_{d \in D} d^{\mathrm{c}}_\alpha$ is the filtered intersection of a family of Scott-compact upper (that is, saturated) sets in the bifinite domain $\mathscr{D}$, we may invoke the Hofmann–Mislove Theorem (Hofmann and Mislove 1981) as bifinite domains are sober spaces (Abramsky and Jung 1994). Therefore, there is some $d \in D$ for which d^{c}_α is contained in $\mathscr{D} \setminus [\![\phi]\!]^{\mathrm{c}}$ already. But then $d \in D \setminus [\![(\exists\alpha)\,\phi]\!]^{\mathrm{c}}$ is a contradiction. □

Sets of the form $[\![\phi]\!]^{\mathrm{a}}$ are model-based versions of valid assertions: the collection of elements in $\mathscr{D}$ for which property ϕ can be successfully verified. Sets of the form $\mathscr{D} \setminus [\![\phi]\!]^{\mathrm{c}}$, which equals $[\![\neg\phi]\!]^{\mathrm{a}}$, are model-based versions of inconsistent assertions: the set of elements in $\mathscr{D}$ for which property ϕ is not consistent. All of these sets are Scott-open observables.

To show internal full abstraction (that is, that the ordering of the domain equals the greatest abstraction relation of the domain viewed as a mixed transition system that meets condition (MC)), we need to prove that each upper set generated by a compact element of $\mathscr{D}$ is a denotation of a formula of Hennessy–Milner logic in assertion mode a.

Lemma 1 (Compact elements as denotations). For every compact element k in $\mathscr{D}$, there exists some $\phi_k \in \mathbb{L}_{\mathrm{HM}}$ such that $[\![\ \phi_k\ ]\!]^{\mathrm{a}}$ equals the upper set generated by k in $\mathscr{D}$.

Proof. For a domain E, we write $\mathbf{K}(E)$ for the partial order of compact elements of E. For $i \geqslant 0$, let $\mathscr{D}_i$ be the ith approximation of $\mathscr{D}$ via its defining domain equation in (7). We prove the lemma by induction on $i \geqslant 0$ for $\mathbf{K}(\mathscr{D}_i)$. This is sound since $\mathbf{K}(\mathscr{D}) = \bigcup_{i \geqslant 0} \mathbf{K}(\mathscr{D}_i)$ by (7).

— For $i = 0$, $\mathbf{K}(\mathscr{D}_0)$ is a singleton set $\{*\}$, so we may choose $\phi_* \stackrel{\text{def}}{=} \mathtt{tt}$.

— Let $k \in \mathbf{K}(\mathscr{D}_{i+1})$. Then each k_α is compact in $\mathsf{M}[\mathscr{D}_i]$. We invoke Theorem 6.4 of Heckmann (1990) to the approximating domain $\mathscr{D}_i$: each compact element of $\mathsf{M}[\mathscr{D}_i]$ is obtained by a finite application of the constant $\bar{\varnothing}$ and the operations $\bar{\cup}$, $\{\!|\cdot|\!\}$ and $\{\!|\cdot?|\!\}$ to compact elements of $\mathscr{D}_i$. Since $\{\!|l|\!\} = (\downarrow l, \uparrow l)$ and $\{\!|l?|\!\} = (\varnothing, \uparrow l)$, and $k_\alpha \in \mathbf{K}(\mathsf{M}[\mathscr{D}_i])$, we infer for all $\alpha \in \mathtt{Act}$ that $(k_\alpha^{\mathrm{a}}, k_\alpha^{\mathrm{c}}) = (\downarrow F_\alpha, \uparrow G_\alpha)$ for some finite sets $F_\alpha, G_\alpha \subseteq \mathbf{K}(\mathscr{D}_i)$. By induction, for each $x \in F_\alpha \cup G_\alpha$ there is some $\phi_x \in \mathbb{L}_{\mathrm{HM}}$ that satisfies the claim of the lemma for x. We use the abbreviations $(\forall\alpha)$ and $\bigvee$ to define

$$\psi_\alpha \stackrel{\text{def}}{=} \bigwedge_{l \in F_\alpha} (\exists\alpha)\, \phi_l$$

$$\eta_\alpha \stackrel{\text{def}}{=} (\forall\alpha) \bigvee_{m \in G_\alpha} \phi_m$$

$$\phi_k \stackrel{\text{def}}{=} \bigwedge_{\alpha \in \mathtt{Act}} \psi_\alpha \wedge \eta_\alpha.$$

Note that $\phi_k \in \mathbb{L}_{\mathrm{HM}}$ since $\mathtt{Act}$ is finite.

1 We show $k \in [\![\ \phi_k\ ]\!]^{\mathrm{a}}$, that is, $\uparrow k \subseteq [\![\ \phi_k\ ]\!]^{\mathrm{a}}$. Let $\alpha \in \mathtt{Act}$.

(a) For $l \in F_\alpha$ we have $\uparrow l = [\![\ \phi_l\ ]\!]^{\mathrm{a}}$ by induction, so $l \in k_\alpha^{\mathrm{a}} \cap [\![\ \phi_l\ ]\!]^{\mathrm{a}}$ since $l \in \downarrow F_\alpha = k_\alpha^{\mathrm{a}}$. But then $k \models^{\mathrm{a}} (\exists\alpha)\, \phi_l$. Therefore, $k \models^{\mathrm{a}} \psi_\alpha$.

(b) We have:

$$\begin{aligned} k \models^{\mathrm{a}} (\forall\alpha) \bigvee \phi_m \ \text{ iff } \ & k \not\models^{\mathrm{c}} (\exists\alpha) \neg \bigvee \phi_m \\ \text{iff } \ & k_\alpha^{\mathrm{c}} \cap [\![\ \neg \bigvee \phi_m\ ]\!]^{\mathrm{c}} = \varnothing \\ \text{iff } \ & k_\alpha^{\mathrm{c}} \subseteq \mathscr{D} \setminus [\![\ \neg \bigvee \phi_m\ ]\!]^{\mathrm{c}} = [\![\ \bigvee \phi_m\ ]\!]^{\mathrm{a}}. \end{aligned}$$

Since the latter is an upper set and since k_α^{c} equals $\uparrow G_\alpha$, it suffices to show $G_\alpha \subseteq [\![\ \bigvee_{m \in G_\alpha} \phi_m\ ]\!]^{\mathrm{a}}$. But

$$\uparrow G_\alpha = [\![\ \bigvee_{m \in G_\alpha} \phi_m\ ]\!]^{\mathrm{a}} \tag{12}$$

follows from induction and Remark 1.2. Thus, $k \models^{\mathrm{a}} \eta_\alpha$.

2 Let $d \in \mathscr{D}$ such that $d \models^{\mathrm{a}} \phi_k$. We have to show $k \leqslant d$ in $\mathscr{D}$, that is, $F_\alpha \subseteq d_\alpha^{\mathrm{a}}$ and $d_\alpha^{\mathrm{c}} \subseteq \uparrow G_\alpha$ for all $\alpha \in \mathtt{Act}$. For every $\alpha \in \mathtt{Act}$, $d \models^{\mathrm{a}} \phi_k$ implies

(a) $d \models^{\mathrm{a}} \psi_\alpha$, so for all $l \in F_\alpha$ there is some $l' \in d_\alpha^{\mathrm{a}}$ such that $l' \models^{\mathrm{a}} \phi_l$. By induction, $l \leqslant l'$ follows. Thus, $F_\alpha \subseteq \downarrow d_\alpha^{\mathrm{a}} = d_\alpha^{\mathrm{a}}$.

(b) $d \models^{\mathrm{a}} \eta_\alpha$, which is equivalent to $d^{\mathrm{c}}_\alpha \subseteq [\![\bigvee_{m \in G_\alpha} \phi_m]\!]^{\mathrm{a}}$. By (12), we get $d^{\mathrm{c}}_\alpha \subseteq \uparrow G_\alpha$.

□

Theorem 5 (Internal full abstraction and logical characterisation). The following are equivalent:

1 $d \leqslant e$ in the domain $\mathscr{D}$;
2 $e \prec_{\mathscr{D}} d$ in the mixed transition system $(\mathscr{D}, \mathscr{R}^{\mathrm{a}}, \mathscr{R}^{\mathrm{c}})$;
3 $\{\phi \in \mathbb{L}_{\mathrm{HM}} \mid d \models^{\mathrm{a}} \phi\} \subseteq \{\phi \in \mathbb{L}_{\mathrm{HM}} \mid e \models^{\mathrm{a}} \phi\}$; and
4 $\{\phi \in \mathbb{L}_{\mathrm{HM}} \mid e \models^{\mathrm{c}} \phi\} \subseteq \{\phi \in \mathbb{L}_{\mathrm{HM}} \mid d \models^{\mathrm{c}} \phi\}$.

Proof. We show (1) ⇒ (2) ⇒ (4) ⇒ (3) ⇒ (1). The first two implications follow from Proposition 2 and Theorem 1 (respectively). To show (4) ⇒ (3), let $d \models^{\mathrm{a}} \phi$. Then we have $d \not\models^{\mathrm{c}} \neg\phi$, which implies $e \not\models^{\mathrm{c}} \neg\phi$, by (4), that is, $e \models^{\mathrm{a}} \phi$. But (3) ⇒ (1) follows directly from Lemma 1, noting that $\mathscr{D}$ is algebraic. □

3.2. *Embedding modal transition systems into the universal domain*

We have already argued that the domain $\mathscr{D}$ is an internally fully abstract model of a mixed transition system that meets condition (MC). We now demonstrate its universality by embedding every mixed transition system that satisfies condition (MC) into $\mathscr{D}$ such that one system refines another iff this is the case for their corresponding embeddings in $\mathscr{D}$ – the embedding preserves and reflects refinements. As a by-product, we get that the assertion check semantics $\models^{\mathrm{a}}$ for Hennessy–Milner logic characterises refinement of mixed transition systems that meet condition (MC). Since elements of $\mathscr{D}$ correspond to pointed mixed transition systems, we work with pointed mixed transition systems $(\mathscr{M}, i)$.

We approximate pointed mixed transition systems $(\mathscr{M}, i)$ by a family of finite-state pointed mixed transition systems $(\mathscr{M}[n], i)$, $n \geqslant 0$. Our intention is to define the embedding $\langle\!| \mathscr{M}, i |\!\rangle$ as the directed supremum of the embeddings $\langle\!| \mathscr{M}[n], i |\!\rangle$ $(n \geqslant 0)$ in $\mathscr{D}$.

Definition 12 (Finite approximation systems). Let $(\mathscr{M}, i) = ((\Sigma, R^{\mathrm{a}}, R^{\mathrm{c}}), i)$ be a pointed mixed transition system. For each $n \geqslant 0$, we define a finite pointed mixed transition system $(\mathscr{M}[n], i) = ((\Sigma[n], R[n]^{\mathrm{a}}, R[n]^{\mathrm{c}}), i)$ by induction on n.

1 The mixed transition system $(M[0], i)$ has no R^{a}-transitions and state set $\Sigma[0] = \{i\}$; its set of R^{c}-transitions equals $\{(i, \alpha, i) \mid \alpha \in \mathtt{Act}\}$.
2 Assume that $(M[n], i)$ is defined for all mixed transition systems (M, i). Let $\alpha \in \mathtt{Act}$, and A_α and C_α be the set of R^{a}_α-successors and R^{c}_α-successors of i in (M, i), respectively. In $(M[n+1], i)$, state i has as R^{a}_α-successors all pointed mixed transition systems $(M[n], a)$ with $a \in A_\alpha$, where transitions are interpreted between pointed systems. Similarly, in $(M[n+1], i)$ state i has all pointed mixed transition systems $(M[n], c)$ with $c \in C_\alpha$ as R^{c}_α-successors. The state set $\Sigma[n+1]$ is the disjoint sum of $\{i\}$ and the state sets of $(M[n], l)$ for all $l \in \bigcup_\alpha A_\alpha \cup C_\alpha$.

Note that $(M[n+1], i)$ has no transitions whatsoever for all $n \geqslant 0$ if i has no successor state in (M, i).

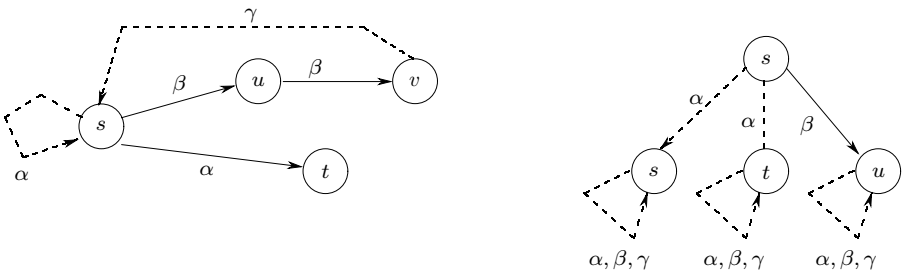


Fig. 7. The left-hand diagram shows a pointed modal transition system $(\mathscr{M}, s)$. The right-hand diagram shows its finite approximation $(\mathscr{M}[1], s)$, where s is unfolded once. (R^{c}-transitions that shadow R^{a}-transitions are omitted.)

Example 8 (The first two approximations).

1 Our embedding will map the initial approximation $(\mathscr{M}[0], i)$ to the least element $((\varnothing, \mathscr{D}))_{\alpha \in \mathtt{Act}}$ of $\mathscr{D}$, where $\varnothing$ models the absence of R^{a}-transitions and $\mathscr{D}$ models the set of R^{c}-transitions $\{(i, \alpha, i') \mid \alpha \in \mathtt{Act}\}$.
2 Figure 7 depicts a pointed modal transition system $(\mathscr{M}, s)$ and its approximation $(\mathscr{M}[1], s)$. In $\mathscr{M}[1]$, there are no transitions out of t. State v is not present/reachable.

Our finite approximations have the expected and desired properties.

Proposition 4 (Finite approximations are monotone). Let $(\mathscr{N}, j)$ and $(\mathscr{M}, i)$ be mixed transition systems.

1 For all $n \geqslant 0$, $(\mathscr{M}, i) \prec (\mathscr{M}[n], i)$.
2 For all $n \geqslant 0$, $(\mathscr{M}[n+1], i) \prec (\mathscr{M}[n], i)$.
3 $(\mathscr{N}, j) \prec (\mathscr{M}, i)$ iff for all $n \geqslant 0$, $(\mathscr{N}[n], j) \prec (\mathscr{M}[n], i)$ iff for all $n \geqslant 0$, $(\mathscr{N}, j) \prec (\mathscr{M}[n], i)$.

Proof.

1 Let $(s, t) \in \Sigma \times \Sigma[n]$ be in Q iff:
   — $t \in \Sigma[n]$ is an unfolded version of $s \in \Sigma$ and t does not occur as the nth state on any path in $\mathscr{M}[n]$ beginning in i; or
   — t is the nth state for some path in $\mathscr{M}[n]$ beginning in i, $\bar{s}$ is the folded version of t, and either $\bar{s} = s$ or there is a path in $\mathscr{M}$ beginning in i on which s occurs after $\bar{s}$.

   We claim that Q is a refinement. Let $(s, t) \in Q$.

   (a) Given $(t, \alpha, t') \in R[n]^{\mathrm{a}}$:
      — Let t be an unfolded version of s such that t does not occur as the nth state on any path in $\mathscr{M}[n]$ beginning in i. Then $(s, \alpha, s') \in R^{\mathrm{a}}$, where s' is the folded version of t'. Regardless of whether t' is 'an nth state' or not, we infer $(s', t') \in Q$ by the definition of Q.
      — Then t cannot be the nth state for some path in $\mathscr{M}[n]$ beginning in i.

(b) Given $(s, \alpha, s') \in R^{\mathrm{c}}$:

— Let t be an unfolded version of s such that t does not occur as the nth state on any path in $\mathscr{M}[n]$ beginning in i. Then $(t, \alpha, t') \in R[n]^{\mathrm{c}}$, where t' is the unfolded version of s'. Regardless of whether t' is 'an nth state' or not, we infer $(s', t') \in Q$ by the definition of Q.

— If t is the nth state for some path in $\mathscr{M}[n]$ beginning in i, $\bar{s}$ is the folded version of t, and either $\bar{s} = s$ or there is a path in $\mathscr{M}$ on which s occurs after $\bar{s}$, then $(t, \alpha, t) \in R[n]^{\mathrm{c}}$ by the definition of $\mathscr{M}[n]$. We readily infer $(s', t) \in Q$ since s' occurs after $\bar{s}$ on some path in $\mathscr{M}$.

2 This proof is identical to the one given for the previous item, except that we replace $(\mathscr{M}, i)$ by $(\mathscr{M}[n+1], i)$.

3 Since all mixed transition systems in this paper are image-finite, the greatest refinement $\prec$ between $(\mathscr{N}, j)$ and $(\mathscr{M}, i)$ is the intersection of its finite approximants $\prec_n$ $(n \geqslant 0)$ of the greatest fixed-point iterations. Thus, it suffices to show, for all $n \geqslant 0$, that $(\mathscr{N}, j) \prec_n (\mathscr{M}, i)$ iff $(\mathscr{N}[n], j) \prec_n (\mathscr{M}[n], i)$ iff $(\mathscr{N}, j) \prec_n (\mathscr{M}[n], i)$ – this is routine.

□

Next, we need to define the embeddings $\langle\!| \mathscr{M}[n], i |\!\rangle$ for all $n \geqslant 0$.

Proposition 5 (Embedding approximants into $\mathscr{D}$). Let $(\mathscr{M}, i)$ be a pointed mixed transition system that satisfies condition (MC) and has state set Σ. For every $s \in \Sigma$ and $n \geqslant 0$, we can construct a compact element $\langle\!| \mathscr{M}[n], s |\!\rangle$ in $\mathscr{D}$ such that

$$(\mathscr{M}[n], s) \prec (\mathscr{D}, \langle\!| \mathscr{M}[n], s |\!\rangle) \qquad \text{and} \qquad (\mathscr{D}, \langle\!| \mathscr{M}[n], s |\!\rangle) \prec (\mathscr{M}[n], s). \tag{13}$$

Proof. We proceed by induction on n for all approximants of the form $(\mathscr{M}[n], i)$. In each inductive step, we construct concrete refinements $Q_1^i \subseteq \Sigma[n] \times \mathscr{D}$ and $Q_2^i \subseteq \mathscr{D} \times \Sigma[n]$ that verify (13).

— Let $n = 0$. We set $\langle\!| \mathscr{M}[0], i |\!\rangle \stackrel{\text{def}}{=} \bot_{\mathscr{D}}$, $Q_1^i \stackrel{\text{def}}{=} \{(i, \bot_{\mathscr{D}})\}$, and $Q_2^i \stackrel{\text{def}}{=} \{(\bot_{\mathscr{D}}, i)\}$. The element $\langle\!| \mathscr{M}[0], i |\!\rangle$ is compact in $\mathscr{D}$.

— Let such embeddings be well defined for approximants of pointed systems for all $k < n$. To define $\langle\!| \mathscr{M}[n], i |\!\rangle$, we need to define $\mathrm{i}_\alpha \in \mathsf{M}[\mathscr{D}]$ for each $\alpha \in \mathtt{Act}$ and set $\langle\!| \mathscr{M}[n], i |\!\rangle \stackrel{\text{def}}{=} (\mathrm{i}_\alpha)_{\alpha \in \mathtt{Act}}$. Consider the approximant $(\mathscr{M}[n], i)$. Define

$$\begin{aligned} F_\alpha &\stackrel{\text{def}}{=} \{s' \in \Sigma[n] \mid (i, \alpha, s') \in R[n]^{\mathrm{a}}\} \\ G_\alpha &\stackrel{\text{def}}{=} \{s' \in \Sigma[n] \mid (i, \alpha, s') \in R[n]^{\mathrm{c}}\}. \end{aligned} \tag{14}$$

For every $s' \in F_\alpha \cup G_\alpha$, we have $\langle\!| \mathscr{M}[n-1], s' |\!\rangle$ is already defined by induction. We set

$$\begin{aligned} \mathrm{i}_\alpha^{\mathrm{a}} &\stackrel{\text{def}}{=} \downarrow\{\langle\!| \mathscr{M}[n-1], l |\!\rangle \mid l \in F_\alpha\} \\ \mathrm{i}_\alpha^{\mathrm{c}} &\stackrel{\text{def}}{=} \uparrow\{\langle\!| \mathscr{M}[n-1], m |\!\rangle \mid m \in G_\alpha\} \end{aligned} \tag{15}$$

for each $\alpha \in \mathtt{Act}$. (Note that $\mathrm{i}_\alpha^{\mathrm{a}}$ is empty if i has no R_α^{a}-successors in $(\mathscr{M}[n], i)$. Similarly, $\mathrm{i}_\alpha^{\mathrm{c}}$ is empty without any R_α^{c}-successors in $(\mathscr{M}[n], i)$. Thus, $\mathrm{i}_\alpha = \bar{\varnothing}$ if there are no transitions out of i in $(\mathscr{M}[n], i)$.) It suffices to show that $\mathrm{i}_\alpha^{\mathrm{a}} \subseteq \downarrow(\mathrm{i}_\alpha^{\mathrm{a}} \cap \mathrm{i}_\alpha^{\mathrm{c}})$ for each $\alpha \in \mathtt{Act}$.

Given $d \in \mathrm{i}^{\mathrm{a}}_{\alpha}$, there is some $l \in F_\alpha$ such that $d \leqslant \langle\!|\, \mathscr{M}[n-1], l \,|\!\rangle$. But $l \in F_\alpha$ means $(\mathrm{i}, \alpha, l) \in R^{\mathrm{a}}$. By condition (MC), there exists some $m \in \Sigma$ such that $(\mathrm{i}, \alpha, m) \in R^{\mathrm{a}} \cap R^{\mathrm{c}}$ and $(\mathscr{M}, m) \prec (\mathscr{M}, l)$. Using induction, the latter gives us

$$(\mathscr{D}, \langle\!|\, \mathscr{M}[n-1], m \,|\!\rangle) \prec (\mathscr{M}[n-1], m) \prec (\mathscr{M}[n-1], l) \prec (\mathscr{D}, \langle\!|\, \mathscr{M}[n-1], l \,|\!\rangle), \tag{16}$$

which implies $\langle\!|\, \mathscr{M}[n-1], l \,|\!\rangle \leqslant \langle\!|\, \mathscr{M}[n-1], m \,|\!\rangle$ by Theorem 5, and so, by transitivity, $d \leqslant \langle\!|\, \mathscr{M}[n-1], m \,|\!\rangle$ follows. From $(\mathrm{i}, \alpha, m) \in R^{\mathrm{a}} \cap R^{\mathrm{c}}$, we infer $m \in F_\alpha \cap G_\alpha$, and therefore $\langle\!|\, \mathscr{M}[n-1], m \,|\!\rangle \in \mathrm{i}^{\mathrm{a}}_{\alpha} \cap \mathrm{i}^{\mathrm{c}}_{\alpha}$ shows the claim. Since $\mathrm{i}^{\mathrm{a}}_{\alpha}$ and $\mathrm{i}^{\mathrm{c}}_{\alpha}$ in (15) are order-generated by finitely many elements (which are compact by induction), we infer that i_α is compact in $\mathsf{M}[\mathscr{D}]$ for each $\alpha \in \mathtt{Act}$. Therefore, $\langle\!|\, \mathscr{M}[n], i \,|\!\rangle$ is compact in $\mathscr{D}$. As for the refinement relations Q^i_1 and Q^i_2, we define

$$\begin{aligned}
Q^i_1 \stackrel{\text{def}}{=}\ & \{(i, \langle\!|\, \mathscr{M}[n], i \,|\!\rangle)\} \\
& \cup \Big(\bigcup_{x \in F_\alpha \cup G_\alpha} Q^x_1 \Big) \\
& \cup \{(s, d) \in \Sigma[n] \times \mathscr{D} \mid d \leqslant \langle\!|\, \mathscr{M}[n-1], s \,|\!\rangle,\ \langle\!|\, \mathscr{M}[n-1], s \,|\!\rangle \in \mathrm{i}^{\mathrm{c}}_{\alpha}\} \\
Q^i_2 \stackrel{\text{def}}{=}\ & \{(\langle\!|\, \mathscr{M}[n-1], i \,|\!\rangle, \mathrm{i})\} \\
& \cup \Big(\bigcup_{x \in F_\alpha \cup G_\alpha} Q^x_2 \Big) \\
& \cup \{(e, t) \in \mathscr{D} \times \Sigma[n] \mid \langle\!|\, \mathscr{M}[n-1], t \,|\!\rangle \leqslant e,\ \langle\!|\, \mathscr{M}[n-1], t \,|\!\rangle \in \mathrm{i}^{\mathrm{a}}_{\alpha}\}.
\end{aligned}$$

□

Definition 13 (General embedding). Let $(\mathscr{M}, i)$ be a pointed mixed transition system that meets condition (MC). By Proposition 5, $\langle\!|\, \mathscr{M}[n], i \,|\!\rangle \in \mathscr{D}$ is defined for all $n \geqslant 0$. By Propositions 4.2 and 5 and Theorem 5, these elements form an ascending chain in $\mathscr{D}$ and therefore

$$\langle\!|\, \mathscr{M}, i \,|\!\rangle \stackrel{\text{def}}{=} \bigvee_{n \geqslant 0} \langle\!|\, \mathscr{M}[n], i \,|\!\rangle \tag{17}$$

exists.

The properties of this embedding allow us to prove important facts about mixed transition systems that meet condition (MC).

Theorem 6 (Logical and domain-theoretic characterisation of refinement). Let $(\mathscr{N}, j)$ and $(\mathscr{M}, i)$ be mixed transition systems that satisfy condition (MC).

1 $(\mathscr{N}, j) \prec (\mathscr{M}, i)$ iff $\langle\!|\, \mathscr{M}, i \,|\!\rangle \leqslant \langle\!|\, \mathscr{N}, j \,|\!\rangle$ in $\mathscr{D}$.
2 $(\mathscr{N}, j) \prec (\mathscr{M}, i)$ iff $\{\phi \in \mathbb{L}_{\mathrm{HM}} \mid (\mathscr{M}, i) \models^{\mathrm{a}} \phi\} \subseteq \{\phi \in \mathbb{L}_{\mathrm{HM}} \mid (\mathscr{N}, j) \models^{\mathrm{a}} \phi\}$.

Proof.

1 By Proposition 4, we have $(\mathscr{N}, j) \prec (\mathscr{M}, i)$ iff for all $n \geqslant 0$, $(\mathscr{N}[n], j) \prec (\mathscr{M}[n], i)$ iff (by Proposition 5) for all $n \geqslant 0$, $(\mathscr{D}, \langle\!|\, \mathscr{N}[n], j \,|\!\rangle) \prec (\mathscr{D}, \langle\!|\, \mathscr{M}[n], i \,|\!\rangle)$ iff (by internal full abstraction) for all $n \geqslant 0$, $\langle\!|\, \mathscr{M}[n], i \,|\!\rangle \leqslant \langle\!|\, \mathscr{N}[n], j \,|\!\rangle$ in $\mathscr{D}$. Thus, $(\mathscr{N}, j) \prec (\mathscr{M}, i)$ implies

$$\langle\!|\, \mathscr{M}, i \,|\!\rangle = \bigvee_{n \geqslant 0} \langle\!|\, \mathscr{M}[n], i \,|\!\rangle \leqslant \bigvee_{n \geqslant 0} \langle\!|\, \mathscr{N}[n], j \,|\!\rangle = \langle\!|\, \mathscr{N}, j \,|\!\rangle. \tag{18}$$

Conversely, let $\langle\!|\mathscr{M},i|\!\rangle \leqslant \langle\!|\mathscr{N},j|\!\rangle$. We use proof by contradiction. If $(\mathscr{N},j) \not\prec (\mathscr{M},i)$, then Proposition 4.3. implies

$$(\mathscr{N},j) \not\prec (\mathscr{M}[n],i) \tag{19}$$

for some $n \geqslant 0$. We claim that

$$\forall m \geqslant 0 : (\mathscr{N}[m],j) \not\prec (\mathscr{M}[n],i). \tag{20}$$

If there is some $m \geqslant 0$ with $(\mathscr{N}[m],j) \prec (\mathscr{M}[n],i)$, then $(\mathscr{N},j) \prec (\mathscr{N}[m],j)$ holds by Proposition 4.1, for (N,j), and this implies $(\mathscr{N},j) \prec (\mathscr{M}[n],i)$ since $\prec$ is transitive, which contradicts (19).
For every $m \geqslant 0$, we have $(\mathscr{N}[m],j) \prec (\mathscr{D}, \langle\!|\mathscr{N}[m],j|\!\rangle)$ and $(\mathscr{D}, \langle\!|\mathscr{M}[n],i|\!\rangle) \prec (\mathscr{M}[n],i)$ follow from Proposition 5. But then (20) and the transitivity of $\prec$ imply that the pointed mixed transition system $(\mathscr{D}, \langle\!|\mathscr{N}[m],j|\!\rangle)$ does not refine $(\mathscr{D}, \langle\!|\mathscr{M}[n],i|\!\rangle)$. Since $m \geqslant 0$ was arbitrary, Proposition 2 renders

$$\forall m \geqslant 0 : \langle\!|\mathscr{M}[n],i|\!\rangle \not\leqslant \langle\!|\mathscr{N}[m],i|\!\rangle \tag{21}$$

which contradicts (18) since $\langle\!|\mathscr{M}[n],i|\!\rangle$ is compact in $\mathscr{D}$ by Proposition 5 and

$$\langle\!|\mathscr{M}[n],i|\!\rangle \leqslant \langle\!|\mathscr{M},i|\!\rangle \leqslant \langle\!|\mathscr{N},j|\!\rangle = \bigvee_{m \geqslant 0} \langle\!|\mathscr{N}[m],j|\!\rangle,$$

where the supremum is directed.

2 One implication follows from Theorem 1. Conversely, the relation $(\mathscr{N},j) \not\prec (\mathscr{M},i)$ implies $\langle\!|\mathscr{M},i|\!\rangle \not\leqslant \langle\!|\mathscr{N},j|\!\rangle$ in $\mathscr{D}$ by the previous item. Since $\mathscr{D}$ is algebraic, there exists some compact element k in $\mathscr{D}$ such that $k \leqslant \langle\!|\mathscr{M},i|\!\rangle$ and $k \not\leqslant \langle\!|\mathscr{N},j|\!\rangle$. By Lemma 1, there exists some $\phi_k \in \mathbb{L}_{\mathrm{HM}}$ with $\uparrow k = [\![\, \phi_k \,]\!]^{\mathrm{a}}$. Thus, $\langle\!|\mathscr{M},i|\!\rangle \models^{\mathrm{a}} \phi_k$ and $\langle\!|\mathscr{N},j|\!\rangle \not\models^{\mathrm{a}} \phi_k$ follow. By Proposition 5 and Theorem 1, we then get $(\mathscr{M},i) \models^{\mathrm{a}} \phi_k$ and $(\mathscr{N},j) \not\models^{\mathrm{a}} \phi_k$. □

3.3. *Complementary processes*

The universal domain $\mathscr{D}$ models processes whose reactive capabilities are either firmly guaranteed, possible or firmly disallowed (that is, impossible). One may wonder whether such processes have a *complement* whose reactive capabilities are the logical negations of those of the original process. Given a modal transition system $\mathscr{M} = (\Sigma, R^{\mathrm{a}}, R^{\mathrm{c}})$, a complementary process is evidently defined by $\bar{\mathscr{M}} = (\Sigma, \bar{R}^{\mathrm{a}}, \bar{R}^{\mathrm{c}})$, where

$$(s,\alpha,s') \in \bar{R}^{\mathrm{m}} \quad \text{iff} \quad (s,\alpha,s') \notin R^{\neg \mathrm{m}} \qquad (\mathrm{m} \in \{\mathrm{a},\mathrm{c}\}). \tag{22}$$

Specification (22) can be modelled in our universal domain $\mathscr{D}$. Since we can embed modal transition systems into $\mathscr{D}$, this follows readily from the fact that $\bar{\mathscr{M}}$ is a modal transition system if $\mathscr{M}$ is one, for $\bar{R}^{\mathrm{a}}$ equals $(\Sigma \times \Sigma) \setminus R^{\mathrm{c}}$, which is contained in $(\Sigma \times \Sigma) \setminus R^{\mathrm{a}}$, since $\mathscr{M}$ is a modal transition system. But $(\Sigma \times \Sigma) \setminus R^{\mathrm{a}} = \bar{R}^{\mathrm{c}}$.

Remark 4 (Complementary process in $\mathscr{D}$). For every pointed modal transition system $(\mathscr{M},i)$, the complementary process $\langle\!|\bar{\mathscr{M}},i|\!\rangle \in \mathscr{D}$ is well defined.

4. Expressiveness of modal transition systems

Domain equation (7) for refinement in partial systems chooses modal transition systems to represent partial, under-determined aspects of a system in its state-transition capabilities. However, systems may also be under-determined in state observables – atomic propositions such as 'the network cable is plugged in', or 'pointer `x` may point to location `l` in the heap'. Therefore, we formulate notions of partial systems (Kripke modal transition systems), refinement and property semantics that allow for under-determined aspects in state transitions and state observables and prove that Kripke modal transition systems can be translated into modal transition systems such that refinements and property semantics are preserved and reflected. In particular, the results obtained for our universal domain in (7) apply to Kripke modal transition systems as well. Since this translation is linear in the size of models and formulas, no real overhead is involved in this representational shift.

The ability of modal transition systems to faithfully represent partial systems, their operational refinement, and property semantics is not limited to Kripke MTSs. In this section, we also show that labelled transition systems with a divergence predicate – the extended transition systems in Bruns and Godefroid (1999) – and partial Kripke structures (Bruns and Godefroid 1999), as well as their operational abstraction preorders and three-valued semantics of modal logic, have such faithful embeddings into the model checking framework for modal transition systems.

4.1. *Kripke modal transition systems*

A *doubly labelled transition system* (de Nicola and Vaandrager 1995) with signature $(\mathtt{Act}, \mathtt{AP})$ is comprised of a non-empty set of states Σ, a set $\mathtt{Act}$ of action labels, a set $\mathtt{AP}$ of (atomic) state propositions, a state transition relation $R \subseteq \Sigma \times \mathtt{Act} \times \Sigma$, and a labelling function $L : \Sigma \to \mathscr{P}(\mathtt{AP})$. (Throughout, we assume that, for every $s \in \Sigma$ and $\alpha \in \mathtt{Act}$, the sets $L(s)$ and $\{s' \mid (s, \alpha, s') \in R\}$ are finite.) Such structures are expressive and flexible models since they allow for state ($\mathtt{AP}$) and state transition ($\mathtt{Act}$) observables. Kripke modal transition systems are partial versions of doubly labelled transition systems in the same way that modal transition systems are partial versions of labelled transition systems.

Definition 14 (Kripke modal transition systems (Huth *et al.* 2001)). A *Kripke modal transition system* (Kripke MTS) $\mathscr{K}$ with signature $(\mathtt{Act}, \mathtt{AP})$ is a tuple

$$(\Sigma, R^{\mathrm{a}}, R^{\mathrm{c}}, L^{\mathrm{a}}, L^{\mathrm{c}})$$

such that $(\Sigma, R^{\mathrm{a}}, L^{\mathrm{a}})$ and $(\Sigma, R^{\mathrm{c}}, L^{\mathrm{c}})$ form *doubly labelled transition systems* with the same signature, $R^{\mathrm{a}} \subseteq R^{\mathrm{c}}$, and $L^{\mathrm{a}}(s) \subseteq L^{\mathrm{c}}(s)$ for all $s \in \Sigma$.

Of course, one may define Kripke mixed transition systems and their version of the consistency condition (MC). However, in practical applications modellers will want to rely on a consistency condition that is enforced by the underlying specification language, and in a transparent manner: Kripke modal transition systems are such a specification language. Refinements of Kripke modal transition systems are generalisations of refinements of

modal transition systems in that state proposition observables are preserved (for mode a) and reflected (for mode c).

Definition 15 (Refinement of Kripke modal transition systems (Huth *et al.* 2001)). A *refinement* within a Kripke MTS $\mathscr{K} = (\Sigma, R^{\mathrm{a}}, R^{\mathrm{c}}, L^{\mathrm{a}}, L^{\mathrm{c}})$ with signature $(\mathtt{Act}, \mathtt{AP})$ is a relation $Q \subseteq \Sigma \times \Sigma$ such that $(s,t) \in Q$ implies for all $\alpha \in \mathtt{Act}$:

1 For all $(t, \alpha, t') \in R^{\mathrm{a}}$, there is some $s' \in \Sigma$ with $(s, \alpha, s') \in R^{\mathrm{a}}$ and $(s', t') \in Q$.
2 For all $(s, \alpha, s') \in R^{\mathrm{c}}$, there is some $t' \in \Sigma$ with $(t, \alpha, t') \in R^{\mathrm{c}}$ and $(s', t') \in Q$.
3 $L^{\mathrm{a}}(t) \subseteq L^{\mathrm{a}}(s)$.
4 $L^{\mathrm{c}}(s) \subseteq L^{\mathrm{c}}(t)$.

We write $s \prec_{\mathscr{M}} t$ or $s \prec t$ if there is some refinement Q with $(s,t) \in Q$. In that case, *s refines* (*is abstracted by*) *t*.

Remark 5 (Refinement for pointed models). Let $\mathscr{K}_1$ and $\mathscr{K}_2$ be two Kripke MTSs with start states i_1 and i_2 (respectively). Since the set-theoretic sum of these two Kripke MTSs is a Kripke MTS with the sum of their respective signatures, we say that $(\mathscr{K}_1, i_1)$ refines (is abstracted by) $(\mathscr{K}_2, i_2)$ iff there is a refinement Q on their sum such that $(i_1, i_2) \in Q$.

The logic for Kripke MTSs, $\mathbb{L}_{\mathrm{K}}$, is the modal mu-calculus as in (1), except that one replaces the clause for $\mathtt{tt}$ with a clause for atomic propositions ($p \in \mathtt{AP}$). (We may re-express $\mathtt{tt}$ as $\neg(p \wedge \neg p)$ since Kripke MTSs are consistent.) The semantics of this logic over Kripke MTSs is the same as the one in Figure 5, expect that clause $\mathtt{tt}$ is replaced by (23).

$$[\![\ p\ ]\!]^{\mathrm{m}}_{\rho} \stackrel{\mathrm{def}}{=} \{s \in \Sigma \mid p \in L^{\mathrm{m}}(s)\} \tag{23}$$

The additional capability of Kripke MTSs to express state observables may be encoded in state transition observables. We translate Kripke MTSs into modal transition systems over an extended signature and show that this translation preserves and reflects refinement and the property semantics. In particular, Kripke MTSs can be embedded into our universal domain (for the appropriately extended signature).

Definition 16 (Translating Kripke MTSs). Let $\mathscr{K} = (\Sigma, R^{\mathrm{a}}, R^{\mathrm{c}}, L^{\mathrm{a}}, L^{\mathrm{c}})$ be a Kripke MTS with signature $(\mathtt{Act}, \mathtt{AP})$. This determines a mixed transition system $\mathbf{M}[\mathscr{K}]$ with signature $\mathtt{AP} + \mathtt{Act}$, state space Σ, and transition relations $\bar{R}^{\mathrm{m}} \subseteq \Sigma \times (\mathtt{AP} + \mathtt{Act}) \times \Sigma$, where

$$\bar{R}^{\mathrm{m}} \stackrel{\mathrm{def}}{=} \{(s, \beta, s') \mid \beta \in L^{\mathrm{m}}(s) \text{ and } s = s';\ \text{or } (s, \beta, s') \in R^{\mathrm{m}}\} \qquad (\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}). \tag{24}$$

Note that the resulting mixed transition system is image-finite. We define a translation from $\mathbb{L}_{\mathrm{K}}$ to $\mathbb{L}$ by:

$$\begin{array}{ll} T(p) \stackrel{\mathrm{def}}{=} (\exists p)\, \neg(p \wedge \neg p) & T(Z) \stackrel{\mathrm{def}}{=} Z \\ T(\neg\phi) \stackrel{\mathrm{def}}{=} \neg T(\phi) & T(\phi_1 \wedge \phi_2) \stackrel{\mathrm{def}}{=} T(\phi_1) \wedge T(\phi_2) \\ T((\exists\alpha)\,\phi) \stackrel{\mathrm{def}}{=} (\exists\alpha)\, T(\phi) & T(\mu Z.\phi) \stackrel{\mathrm{def}}{=} \mu Z.T(\phi). \end{array}$$

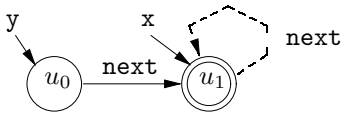
The transformations of models ($\mathscr{K} \mapsto \mathbf{M}[\mathscr{K}]$) and properties ($\phi \mapsto T(\phi)$) preserve and reflect refinement, abstraction, and model checks.

Theorem 7 (Soundness and completeness of translation). Let $\mathscr{K}$ be a Kripke MTS $(\Sigma, R^{\mathrm{a}}, R^{\mathrm{c}}, L^{\mathrm{a}}, L^{\mathrm{c}})$ with signature $(\mathtt{Act}, \mathtt{AP})$. Then:

1 $\mathbf{M}[\mathscr{K}]$ is a modal transition system with signature $\mathtt{AP} + \mathtt{Act}$.
2 For $s, t \in \Sigma$, we have $s \prec t$ in $\mathscr{K}$ iff $s \prec t$ in $\mathbf{M}[\mathscr{K}]$.
3 For all $\phi \in \mathbb{L}_{\mathrm{K}}$, ρ, and m, we have $[\![\phi]\!]^{\mathrm{m}}_{\rho} = [\![T(\phi)]\!]^{\mathrm{m}}_{\rho}$.

Proof.

1 Let $(s, \beta, s') \in \bar{R}^{\mathrm{a}}$. If $\beta \in L^{\mathrm{a}}(s)$, then $L^{\mathrm{a}}(s) \subseteq L^{\mathrm{c}}(s)$ implies $s' = s$ and $(s, \beta, s) \in \bar{R}^{\mathrm{c}}$. Otherwise, $(s, \beta, s') \in R^{\mathrm{a}} \subseteq R^{\mathrm{c}}$, so $(s, \beta, s') \in \bar{R}^{\mathrm{c}}$.
2 Let $s, t \in \Sigma$.
   (a) Let $s \prec t$ in $\mathscr{K}$. We show $s \prec t$ in $\mathbf{M}[\mathscr{K}]$:
      i Let $(t, \beta, t') \in \bar{R}^{\mathrm{a}}$. If $(t, \beta, t') \in R^{\mathrm{a}}$, then $s \prec t$ in $\mathscr{K}$ implies the existence of some $s' \in \Sigma$ with $s' \prec t'$ in $\mathscr{K}$ and $(s, \beta, s') \in R^{\mathrm{a}}$, that is, $(s, \beta, s') \in \bar{R}^{\mathrm{a}}$. Otherwise, $\beta \in L^{\mathrm{a}}(t)$ and $s' = s$, so $s \prec t$ in $\mathscr{K}$ implies $\beta \in L^{\mathrm{a}}(s)$ and $s' = s$, that is, $(s, \beta, s) \in \bar{R}^{\mathrm{a}}$.
      ii Let $(s, \beta, s') \in \bar{R}^{\mathrm{c}}$. If $(s, \beta, s') \in R^{\mathrm{c}}$, then $s \prec t$ in $\mathscr{K}$ implies the existence of some $t' \in \Sigma$ with $s' \prec t'$ and $(t, \beta, t') \in R^{\mathrm{c}}$, that is, $(t, \beta, t') \in \bar{R}^{\mathrm{c}}$. Otherwise, $\beta \in L^{\mathrm{c}}(s)$ and $t' = t$, so $s \prec t$ in $\mathscr{K}$ implies $\beta \in L^{\mathrm{c}}(t)$ and $t' = t$, that is, $(t, \beta, t) \in \bar{R}^{\mathrm{c}}$.
   (b) Let $s \prec t$ in $\mathbf{M}[\mathscr{K}]$. We show $s \prec t$ in $\mathscr{K}$:
      i Given $(t, \alpha, t') \in R^{\mathrm{a}}$, we have $(t, \alpha, t') \in \bar{R}^{\mathrm{a}}$, so $s \prec t$ in $\mathbf{M}[\mathscr{K}]$ implies the existence of some $s' \in \Sigma$ with $s' \prec t'$ in $\mathbf{M}[\mathscr{K}]$ and $(s, \alpha, s') \in \bar{R}^{\mathrm{a}}$, that is, $(s, \alpha, s') \in R^{\mathrm{a}}$ since $\mathtt{AP}$ and $\mathtt{Act}$ are disjoint in $\mathtt{AP} + \mathtt{Act}$.
      ii Given $(s, \alpha, s') \in R^{\mathrm{c}}$, we have $(s, \alpha, s') \in \bar{R}^{\mathrm{c}}$, so $s \prec t$ in $\mathbf{M}[\mathscr{K}]$ implies the existence of some $t' \in \Sigma$ with $s' \prec t'$ in $\mathbf{M}[\mathscr{K}]$ and $(t, \alpha, t') \in \bar{R}^{\mathrm{c}}$, that is, $(t, \alpha, t') \in R^{\mathrm{c}}$ since $\mathtt{AP}$ and $\mathtt{Act}$ are disjoint in $\mathtt{AP} + \mathtt{Act}$.
      iii Given $p \in L^{\mathrm{a}}(t)$, we have $(t, p, t) \in \bar{R}^{\mathrm{a}}$, so $s \prec t$ in $\mathbf{M}[\mathscr{K}]$ implies the existence of some $s' \in \Sigma$ such that $(s, p, s') \in \bar{R}^{\mathrm{a}}$. Since $\mathtt{AP}$ and $\mathtt{Act}$ are disjoint in $\mathtt{AP} + \mathtt{Act}$, we infer $s' = s$ and $p \in L^{\mathrm{a}}(s)$.
      iv Given $p \in L^{\mathrm{c}}(s)$, we have $(s, p, s) \in \bar{R}^{\mathrm{c}}$, so $s \prec t$ in $\mathbf{M}[\mathscr{K}]$ implies the existence of some $t' \in \Sigma$ such that $(t, p, t') \in \bar{R}^{\mathrm{c}}$. Since $\mathtt{AP}$ and $\mathtt{Act}$ are disjoint in $\mathtt{AP} + \mathtt{Act}$, we have $t' = t$ and $p \in L^{\mathrm{c}}(t)$.
3 This statement is proved by the same induction as in the proof of Theorem 1:
   (a) For variables Z, $[\![\phi]\!]^{\mathrm{m}}_{\rho} = \rho^{\mathrm{m}}(Z) = [\![T(Z)]\!]^{\mathrm{m}}_{\rho}$.
   (b) For p, we have $[\![\phi]\!]^{\mathrm{m}}_{\rho} = \{s \in \Sigma \mid p \in L^{\mathrm{m}}(s)\} = \{s \in \Sigma \mid \exists s' \in \Sigma,\ (s, p, s') \in \bar{R}^{\mathrm{m}}\} = [\![(\exists p)\, \neg(p \wedge \neg p)]\!]^{\mathrm{m}}_{\rho}$ since $\mathtt{AP}$ and $\mathtt{Act}$ are disjoint in $\mathtt{AP} + \mathtt{Act}$.
   (c) For $\neg\phi$, $[\![\neg\phi]\!]^{\mathrm{m}}_{\rho} = \Sigma \setminus [\![\phi]\!]^{\neg\mathrm{m}}_{\rho} = \Sigma \setminus [\![T(\phi)]\!]^{\neg\mathrm{m}}_{\rho} = [\![\neg T(\phi)]\!]^{\mathrm{m}}_{\rho} = [\![T(\neg\phi)]\!]^{\mathrm{m}}_{\rho}$.
   (d) For $\phi_1 \wedge \phi_2$, $[\![\phi_1 \wedge \phi_2]\!]^{\mathrm{m}}_{\rho} = [\![\phi_1]\!]^{\mathrm{m}}_{\rho} \cap [\![\phi_2]\!]^{\mathrm{m}}_{\rho} = [\![T(\phi_1)]\!]^{\mathrm{m}}_{\rho} \cap [\![T(\phi_2)]\!]^{\mathrm{m}}_{\rho}$, which equals $[\![T(\phi_1 \wedge \phi_2)]\!]^{\mathrm{m}}_{\rho}$.
   (e) For $(\exists\alpha)\,\phi$, $[\![(\exists\alpha)\,\phi]\!]^{\mathrm{m}}_{\rho} = \{s \in \Sigma \mid \exists s'\ (s, \alpha, s') \in R^{\mathrm{m}},\ s' \in [\![\phi]\!]^{\mathrm{m}}_{\rho}\} = \{s \in \Sigma \mid \exists s'\ (s, \alpha, s') \in \bar{R}^{\mathrm{m}},\ s' \in [\![T(\phi)]\!]^{\mathrm{m}}_{\rho}\} = [\![T((\exists\alpha)\,\phi)]\!]^{\mathrm{m}}_{\rho}$ since $\mathtt{AP}$ and $\mathtt{Act}$ are disjoint in $\mathtt{AP} + \mathtt{Act}$.



$$
\begin{array}{ll}
x(u_0) = 0 & next(u_0, u_0) = 0 \\
x(u_1) = 1 & next(u_0, u_1) = 1 \\
y(u_0) = 1 & next(u_1, u_0) = 0 \\
y(u_1) = 0 & next(u_1, u_1) = 1/2 \\
sm(u_0) = 0 & \\
sm(u_1) = 1 &
\end{array}
$$

Fig. 8. A shape graph and its representation through predicates.

(f) For $\mu Z.\phi$, $[\![\ T(\mu Z.\phi)\ ]\!]^{\mathrm{m}}_{\rho}$ is defined to be $[\![\ \mu Z.T(\phi)\ ]\!]^{\mathrm{m}}_{\rho}$, which is the least fixed point of the function $A \mapsto [\![\ T(\phi)\ ]\!]^{\mathrm{m}}_{\rho[Z \mapsto A]}$. By induction, this function equals $A \mapsto [\![\ \phi\ ]\!]^{\mathrm{m}}_{\rho[Z \mapsto A]}$ and so its least fixed point is $[\![\ \mu Z.\phi\ ]\!]^{\mathrm{m}}_{\rho}$. □

4.2. *Shape analysis with Kripke modal transition systems*

An important form of pointer analysis is *shape analysis* (Chase *et al.* 1990; Ghiya and Hendren 1996; Jones and Muchnick 1979; Sagiv *et al.* 1999; Whaley and Rinard 1999), where the contents of heap storage are approximated by a graph whose nodes denote objects and whose arcs denote the values of the objects' fields. Local ('stack') variables that point into the heap are drawn as arcs pointing to the nodes.

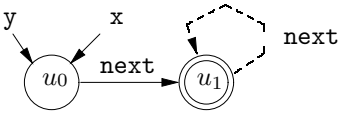
Figure 8 displays the syntax of such *shape graphs*. The example in the Figure depicts an approximation to a singly linked list of length at least two: objects are circles; a double-circled object is a 'summary node', meaning that it possibly represents more than one concrete object. Since the objects were constructed from a class/struct that owns a `next` field, objects have `next`-labelled arcs. For the sake of our discussion, the objects are named u_0 and u_1, and local variables `x` and `y` point to the objects. A solid arc denotes that a field definitely points to an object; a dotted arc means the field possibly points to it. Thus, the self-arc on u_1 must be dotted because u_1 possibly denotes multiple nodes, meaning that a `next` dereference possibly points to one of the concrete objects denoted by the node.

Shape graphs can be encoded in various ways; in Figure 8, we display a coding due to Sagiv, Reps and Wilhelm (Sagiv *et al.* 1999), who define local-variable points-to information with unary predicates and field points-to information with binary ones. The predicates produce the answers 'guaranteed to point to' (1), 'possibly points to' (1/2), and 'not points to' (0), where the values are ordered $0 \leqslant 1/2 \leqslant 1$. Similarly, the predicate *sm* notes which nodes are summary nodes; those s for which $sm(s) = 1$.

Shape graphs can be used as data values for a data-flow analysis, where a program's transfer functions transform an input shape graph to an output one. The transfer functions for assignment and object construction appear in Figure 9, where p' denotes predicate p updated by the transfer function $T[\![\mathtt{C}]\!]$ for command `C`. The transfer functions are written as predicate-logic formulas and interpreted on top of Kleene's strong semantics for propositional logic.

$T[\texttt{x = y}] : x'(v) = y(v)$; all other predicates $p' = p$
$T[\texttt{x.next = y}] : next'(v_1, v_2) = (next(v_1, v_2) \wedge (sm(v_1) \vee \neg x(v_1)) \vee (x(v_1) \wedge y(v_2))$;
all other $p' = p$
$T[\texttt{x = y.next}] : x'(v) = \exists v_1.y(v_1) \wedge next(v_1, v)$; all other $p' = p$
$T[\texttt{x = new Node()}]$: let v_{new} be a fresh node, in $x'(v) = (v = v_{new})$;
all other $p'(v) = (p(v) \wedge (v \neq v_{new}))$

Effect of x = y on Figure 8:



Effect of x .next = y on Figure 8:

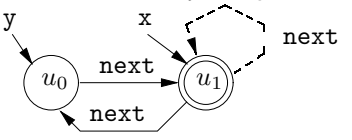


Fig. 9. Transfer functions on shape graphs.

A shape graph is in fact a Kripke MTS $(\Sigma, R^{\mathrm{a}}, R^{\mathrm{c}}, L^{\mathrm{a}}, L^{\mathrm{c}})$, where:

— Σ is the shape graph's nodes;
— $\mathtt{Act} = \{\mathtt{next}\}$;
— AP contains the symbol *sm* and all identifiers of the program's pointer variables;
— R^{a} contains the solid labelled arcs between nodes;
— $R^{\mathrm{c}} \setminus R^{\mathrm{a}}$ contains the dashed labelled arcs between nodes;
— $\mathtt{x} \in L^{\mathrm{a}}(s)$ when a solid arc shows that x points to object s;
— $\mathtt{x} \in L^{\mathrm{c}}(s) \setminus L^{\mathrm{a}}(s)$ when a dashed arc shows that x points to object s;
— when s is a summary node, $sm \in L^{\mathrm{a}}(s)$.

Given a shape graph/Kripke MTS, we check the graph for correctness properties that are expressible in the CTL-subset (Burch *et al.* 1990; Dam 1994) of the modal mu-calculus. In Sagiv *et al.* (1999), such properties are encoded in predicate logic augmented with a transitive closure operator.

Here are some examples: the direction relationship (Ghiya and Hendren 1996), stating that an access path exists from the object named by x to an object named by y, is written $\mathtt{D}(\mathtt{x},\mathtt{y}) \stackrel{\text{def}}{=} \mathtt{x} \wedge \mathsf{EF}_{\mathtt{next}}\mathtt{y}$ – an object s has atomic property x iff x points to s. Recall that $\mathsf{EF}_\alpha\phi$ states, 'there exists a path of α-labelled transitions such that, at some state in the future, ϕ holds true'. To validate the fact that there is a *guaranteed* (*possible*) path from s, we check whether $s \models^a \mathtt{D}(\mathtt{x},\mathtt{y})$ ($s \models^c \mathtt{D}(\mathtt{x},\mathtt{y})$); to refute the existence of a path, we check $s \models^a \neg\mathtt{D}(\mathtt{x},\mathtt{y})$.

The interference relationship (Ghiya and Hendren 1996), saying that pointers x and y have access paths to a common heap node, is written with *inverse* transition relationships of R^{a}: $\mathtt{I}(\mathtt{x},\mathtt{y}) \stackrel{\text{def}}{=} (\mathsf{EF}_{\mathtt{next}^{-1}}\mathtt{x}) \wedge (\mathsf{EF}_{\mathtt{next}^{-1}}\mathtt{y})$. We check $s \models^c \mathtt{I}(\mathtt{x},\mathtt{y})$ to see if aliasing of object s by x and y is possible.

Aliasing of pointers can be expressed: for $\mathtt{aliasing} \stackrel{\text{def}}{=} \mathsf{EF}_{\mathtt{next}}(\bigvee_{\mathtt{x}\neq\mathtt{y}} \mathtt{x}\wedge\mathtt{y})$, the formulas:

(a) $\mathsf{AG}_{\mathtt{next}}\neg\mathtt{aliasing}$,
(b) $\mathsf{AG}_{\mathtt{next}}\neg(\mathtt{x} \wedge \bigvee_{\mathtt{x}\neq\mathtt{y}} \mathtt{y})$, and
(c) $\mathsf{AG}_{\mathtt{next}}\neg(\mathtt{x} \wedge \mathtt{y})$

can then be used to check:

(a) the absence of any kind of aliasing;
(b) that x has no alias; and that
(c) x and y never point to the same heap node.

(Recall that $\mathtt{AG}_\alpha\phi$ states, 'for all α-paths, it is globally true that ϕ holds for all states along the path'.)

We can check for possibly cyclic data structures. The predicate $\mathtt{cyclic} \stackrel{\text{def}}{=} \bigvee_{\mathtt{x}\in\mathtt{AP}} \mathtt{x} \wedge \mathsf{EX}_{\mathtt{next}}\mathsf{EF}_{\mathtt{next}}\mathtt{x}$ states that a heap node is pointed to by some x that has an access path to, presumably the same, heap node pointed to by x. (Recall that $\mathsf{EX}_\alpha\phi$ says, 'there exists an α-transition to a next state where ϕ holds'.)

A full exposition of shape analysis based on shape graphs is beyond the scope of this paper. However, we note that the modal transition systems for shape graphs may have total refinements that have no correspondence to shapes that may occur at run-time. For example, a variable cannot point to two distinct locations in the heap at the same time. Thus, one may need to use techniques for restricting the set of total refinements of a graph in order to conclude that properties are valid or consistent. One such technique is assume-guarantee reasoning for branching-time logics (Kupferman and Vardi 1998).

4.3. *Extended transition systems*

In Section 2, we have already discussed how labelled transition systems give rise to partial systems whose under-determined aspects are represented explicitly. Modelling under-determinacy in systems through a pair of labelled transition systems, connected with a consistency constraint, is not the only way of enriching labelled transition systems with explicit under-determined aspects. Bruns and Godefroid define an extended transition system $\mathscr{E}$ (Bruns and Godefroid 1999) with signature Act as a labelled transition system (Σ, R) with the same signature, endowed with a divergence predicate $\uparrow \subseteq \Sigma \times \mathtt{Act}$ (Milner 1981; Walker 1990). The intuitive meaning of $s \uparrow \alpha$ is that 'some of the α-transitions from s in the full model may be missing at s in the ETS $\mathscr{E}$' (Bruns and Godefroid 1999). As is usual, we write $s \downarrow \alpha$ when $s \uparrow \alpha$ fails to hold, meaning that all α-transitions from s in the full model (possibly none at all) are present in the ETS $\mathscr{E}$. Partial bisimulations (Milner 1981; Walker 1990) are the operational abstraction preorder for extended transition systems.

Definition 17 (Partial bisimulation (Milner 1981)). A *partial bisimulation* in an extended transition system $\mathscr{E} = (\Sigma, R, \uparrow)$ is a relation $Q \subseteq \Sigma \times \Sigma$ such that $(t, s) \in Q$ implies for all $\alpha \in \mathtt{Act}$:

1 If $(t, \alpha, t') \in R$, there exists some $s' \in \Sigma$ such that $(s, \alpha, s') \in R$ and $(t', s') \in Q$.
2 If $t \downarrow \alpha$, then:
   (i) $s \downarrow \alpha$.
   (ii) Whenever $(s, \alpha, s') \in R$, there exists $t' \in \Sigma$ such that $(t, \alpha, t') \in R$ and $(t', s') \in Q$.

One can form the sum of two extended transition systems by forming the sum of their underlying labelled transition systems, the sum of their respective divergence predicates,

$$
\begin{aligned}
[\![\ \mathtt{tt}\ ]\!]^{\downarrow} s &\stackrel{\text{def}}{=} 1 \\
[\![\ \neg\phi\ ]\!]^{\downarrow} s &\stackrel{\text{def}}{=} 1 - ([\![\ \phi\ ]\!]^{\downarrow} s) \\
[\![\ \phi_1 \wedge \phi_2\ ]\!]^{\downarrow} s &\stackrel{\text{def}}{=} ([\![\ \phi_1\ ]\!]^{\downarrow} s) \wedge ([\![\ \phi_2\ ]\!]^{\downarrow} s) \\
[\![\ (\exists\alpha)\,\phi\ ]\!]^{\downarrow} s &\stackrel{\text{def}}{=} \bigvee(\{1/2 \mid s \uparrow \alpha\} \cup \{[\![\ \phi\ ]\!]^{\downarrow} s' \mid (s,\alpha,s') \in R\}).
\end{aligned}
$$

Fig. 10. Property semantics for Hennessy–Milner logic $\mathbb{L}_{\mathrm{HM}}$ over extended transition systems (Bruns and Godefroid 1999), where $s \in \Sigma$ and $\wedge$ and $\bigvee$ are defined for $0 < 1/2 < 1$. The set $\{1/2 \mid s \uparrow \alpha\}$ is empty iff $s \downarrow \alpha$.

and the sum of their signatures. In this manner, Definition 17 also defines partial bisimulations between pointed extended transition systems. The intuitive readings of $s \uparrow \alpha$ and $s \downarrow \alpha$ suggest that extended transition systems can be represented as modal transition systems, and therefore embed into our universal domain. What is perhaps more surprising is that partial bisimulations in an extended transition system turn out to be the relational inverses of refinements of the representing modal transition systems. Moreover, the three-valued semantics for Hennessy–Milner logic in Bruns and Godefroid (1999) corresponds to the assertion checking semantics of the representing modal transition system.

Definition 18 (Translating extended transition systems (Huth *et al.* 2001)). Let $\mathscr{E}$ be an extended transition system $(\Sigma, R, \uparrow)$ with signature $\mathtt{Act}$. We define a modal transition system $\mathbf{E}[\mathscr{E}] = (\Sigma, R, R^{\mathrm{c}})$ with the same signature $\mathtt{Act}$, where

$$R^{\mathrm{c}} \stackrel{\text{def}}{=} R \cup \{(s,\alpha,s') \in \Sigma \times \mathtt{Act} \times \Sigma \mid s \uparrow \alpha\}. \tag{25}$$

Note that the state variable s' is free in (25), meaning that the modal transition system represents each instance of $s \uparrow \alpha$ conservatively in that it adds R^{c}-transitions of type α from *s to all states in* Σ. In Bruns and Godefroid (1999), formulas of $\mathbb{L}_{\mathrm{HM}}$ are interpreted over extended transition systems with signature $\mathtt{Act}$; the semantics is given in Figure 10. We use the truth ordering $0 < 1/2 < 1$ as a representation instead of the false $< \perp <$ true of Bruns and Godefroid (1999).

Theorem 8 (Soundness and completeness of translation). Let $\mathscr{E} = (\Sigma, R, \uparrow)$ be an extended transition system with signature $\mathtt{Act}$.

1 The structure $\mathbf{E}[\mathscr{E}]$ is a modal transition system with signature $\mathtt{Act}$.
2 For all $\phi \in \mathbb{L}_{\mathrm{HM}}$, we have $[\![\ \phi\ ]\!]^{\downarrow} s = 1$ iff $s \in [\![\ \phi\ ]\!]^{\mathrm{a}}$; $[\![\ \phi\ ]\!]^{\downarrow} s = 0$ iff $s \notin [\![\ \phi\ ]\!]^{\mathrm{c}}$. In particular, $[\![\ \phi\ ]\!]^{\downarrow} s = 1/2$ iff $s \in [\![\ \phi\ ]\!]^{\mathrm{c}} \setminus [\![\ \phi\ ]\!]^{\mathrm{a}}$.
3 The relational inverse of a reflexive partial bisimulation in $\mathscr{E}$ is a refinement in the modal transition system $\mathbf{E}[\mathscr{E}]$. Conversely, if $\mathbf{E}[\mathscr{E}]$ is such that

$$s \prec_{\mathscr{M}} t \text{ and } t \downarrow \alpha \;\Rightarrow\; s \downarrow \alpha \tag{26}$$

then the relational inverse of every refinement in $\mathbf{E}[\mathscr{E}]$ is a partial bisimulation in $\mathscr{E}$. In that case, the relational inverse of the greatest partial bisimulation equals the greatest refinement in $\mathbf{E}[\mathscr{E}]$.

Proof.

1 Since R^{a} equals R, equation (25) enforces the consistency condition $R^{\mathrm{a}} \subseteq R^{\mathrm{c}}$.

2 By the previous item and Theorem 3.2, it suffices to show the claims about 0 and 1, which we prove by structural induction:

(a) We have $[\![\mathtt{tt}]\!]^{\downarrow} s = 1$ and $s \in [\![\mathtt{tt}]\!]^{\mathrm{m}}$ for $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$.

(b) For negation, $x \stackrel{\text{def}}{=} [\![\neg\phi]\!]^{\downarrow} s = 1 - [\![\phi]\!]^{\downarrow} s$. By induction, x equals 1 iff $s \notin [\![\phi]\!]^{\mathrm{c}}$ iff $s \in [\![\neg\phi]\!]^{\mathrm{a}}$. By induction, x equals 0 iff $s \in [\![\phi]\!]^{\mathrm{a}}$ iff $s \notin [\![\neg\phi]\!]^{\mathrm{c}}$.

(c) For conjunction, $y \stackrel{\text{def}}{=} [\![\phi_1 \wedge \phi_2]\!]^{\downarrow} s = ([\![\phi_1]\!]^{\downarrow} s) \wedge ([\![\phi_2]\!]^{\downarrow} s)$. By induction, y equals 1 iff $s \in [\![\phi_i]\!]^{\mathrm{a}}$ for $i = 1, 2$ iff $s \in [\![\phi_1 \wedge \phi_2]\!]^{\mathrm{a}}$. By induction, y equals 0 iff $s \notin [\![\phi_i]\!]^{\mathrm{c}}$ for some $i = 1, 2$ iff $s \notin [\![\phi_1 \wedge \phi_2]\!]^{\mathrm{c}}$.

(d) For the modalities,

$$z \stackrel{\text{def}}{=} [\![(\exists\alpha)\,\phi]\!]^{\downarrow} s = \bigvee(\{1/2 \mid s \uparrow \alpha\} \cup \{[\![\phi]\!]^{\downarrow} s' \mid (s, \alpha, s') \in R\}).$$

By induction, z equals 1 iff there is some s' with $(s, \alpha, s') \in R$ and $s' \in [\![\phi]\!]^{\mathrm{a}}$ iff $s \in [\![(\exists\alpha)\,\phi]\!]^{\mathrm{a}}$. By induction, z equals 0 iff $s \downarrow \alpha$ and $s' \notin [\![\phi]\!]^{\mathrm{c}}$ for all s' with $(s, \alpha, s') \in R$ iff $s \notin [\![(\exists\alpha)\,\phi]\!]^{\mathrm{c}}$ by (25).

3 (a) Let $\sqsubseteq$ be a reflexive, partial bisimulation in $\mathscr{E}$. We show that Q, the relational inverse of $\sqsubseteq$, is a refinement in $\mathbf{E}[\mathscr{E}]$. Let $(s, t) \in Q$, that is, $t \sqsubseteq s$.

i If $(t, \alpha, t') \in R^{\mathrm{a}}$, that is, $(t, \alpha, t') \in R$, then $t \sqsubseteq s$ implies the existence of some $s' \in \Sigma$ such that $(s, \alpha, s') \in R = R^{\mathrm{a}}$ and $t' \sqsubseteq s'$, that is, $(s', t') \in Q$.

ii If $(s, \alpha, s') \in R^{\mathrm{c}}$, there are two cases to consider:

A If $t \uparrow \alpha$, then $(t, \alpha, s') \in R^{\mathrm{c}}$ by (25). But $s' \sqsubseteq s'$, that is, $(s', s') \in Q$, as $\sqsubseteq$ is reflexive.

B If $t \downarrow \alpha$, then $t \sqsubseteq s$ implies $s \downarrow \alpha$, which, in turn, implies $(s, \alpha, s') \in R$ by (25) since $(s, \alpha, s') \in R^{\mathrm{c}}$. But then $t \sqsubseteq s$ implies the existence of some $t' \in \Sigma$ such that $(t, \alpha, t') \in R \subseteq R^{\mathrm{c}}$ and $t' \sqsubseteq s'$, that is, $(s', t') \in Q$.

(b) Let Q be a refinement in $\mathbf{E}[\mathscr{E}]$ and $(t, s) \in Q^{-1}$, that is, $(s, t) \in Q$.

i If $(t, \alpha, t') \in R$, then $(t, \alpha, t') \in R^{\mathrm{a}}$ and $(s, t) \in Q$ imply the existence of some $s' \in \Sigma$ such that $(s, \alpha, s') \in R^{\mathrm{a}} = R$ and $(s', t') \in Q$, that is, $(t', s') \in Q^{-1}$.

ii If $t \downarrow \alpha$, then:

A If (26) holds, then $s \downarrow \alpha$ as $(s, t) \in Q$, which is contained in $\prec$ as a refinement.

B If $(s, \alpha, s') \in R \subseteq R^{\mathrm{c}}$, then $(s, t) \in Q$ implies the existence of some $t' \in \Sigma$ such that $(t, \alpha, t') \in R^{\mathrm{c}}$ and $(s', t') \in Q$. But then $(t, \alpha, t') \in R^{\mathrm{c}}$ and $t \downarrow \alpha$ imply $(t, \alpha, t') \in R$. □

This result not only states that extended transition systems and their partial bisimulation can be seen as modal transition systems with their abstraction order. Since the latter models can be embedded into our universal domain, the former models are themselves embedable into the same domain by the composition of these transformations. Inspecting the work in Abramsky (1991), this suggests that there is an embedding of Abramsky's universal domain (Abramsky 1991), which is based on an extended Plotkin powerdomain,

into our universal domain $\mathscr{D}$. Since the divergence predicate in Abramsky (1991) is state-wide, this is false. However, an embedding can be given for the action-dependent divergence predicate of this section by modifying the domain in Abramsky (1991) to a recursive solution of products of lifted Plotkin powerdomains. This embedding is based on the embedding of the Plotkin powerdomain $\mathscr{C}_D$ of a domain D into the mixed powerdomain $\mathsf{M}[D]$: every compact, convex set C, even the empty set used in Abramsky (1991), is mapped to the pair (L, U), where L and U are the lower and upper closure of C, respectively (Heckmann 1990).

4.4. *Partial Kripke structures*

Bruns and Godefroid (Bruns and Godefroid 1999) also devise partial Kripke structures as under-determined models for partial-state-space model checking. In *loc. cit.* they specify an abstraction preorder between such models, give a three-valued semantics over such models for the branching-time temporal logic CTL (Clarke and Emerson 1981), and present a model-checking algorithm for that semantics (Bruns and Godefroid 1999). Since partial Kripke structures are special Kripke MTSs, we may use the translation of Section 4.1 to represent these models as modal transition systems. This translation preserves and reflects the abstraction preorder and the three-valued semantics of propositional modal logic.

Definition 19 (Partial Kripke structures (Bruns and Godefroid 1999)).

1 Let $\mathbf{K}$ be the *partial information order* $\{0, 1/2, 1\}$ with $1/2 \sqsubseteq 0$ and $1/2 \sqsubseteq 1$, which is an isomorphic copy of $\mathsf{M}[*]$.
2 A *partial Kripke structure* $\mathscr{P}$ (Bruns and Godefroid 1999) with signature $\mathtt{AP}$ is a triple (Σ, R, L), where Σ is a set of states, $R \subseteq \Sigma \times \Sigma$ a state transition relation, and $L : \Sigma \times \mathtt{AP} \to \mathbf{K}$ is a labelling function.
3 A *completeness order* (Bruns and Godefroid 1999) in a partial Kripke structure $\mathscr{P}$ with signature $\mathtt{AP}$ is a relation $Q \subseteq \Sigma \times \Sigma$ such that $(s, t) \in Q$ implies:
   (a) For all $p \in \mathtt{AP}$, we have $L(s, p) \sqsubseteq L(t, p)$ in the information order of $\mathbf{K}$.
   (b) If $(s, s') \in R$, then there exists some $t' \in \Sigma$ with $(t, t') \in R$ and $(s', t') \in Q$.
   (c) If $(t, t') \in R$, then there exists some $s' \in \Sigma$ with $(s, s') \in R$ and $(s', t') \in Q$.

Intuitively, $L(s, p) = 1/2$ expresses the fact that 'p is true at state s' is a consistent statement; whereas $L(s, p) = 1$ ($L(s, p) = 0$) expresses the fact that 'p is true at state s' ('p is false at state s') is a valid assertion (respectively). For a completeness order Q, $(s, t) \in Q$ implies that valid assertions for s are also valid for t, and consistent statements for s are consistent for t as well; this correspondence is preserved in a co-inductive manner, which is familiar from bisimulations (Park 1989; Milner 1989). In Bruns and Godefroid (1999), a three-valued semantics for propositional modal logic is given over partial Kripke structures; see Figure 11.

Lemma 2 (Correspondence to Kripke MTSs (Huth *et al.* 2001)). Partial Kripke structures $\mathscr{P} = (\Sigma, R, L)$ with signature $\mathtt{AP}$ are in one-to-one correspondence to Kripke MTSs $\mathscr{K} = (\Sigma, R^{\mathrm{a}}, R^{\mathrm{c}})$ with signature $(\{*\}, \mathtt{AP})$ such that $R^{\mathrm{a}} = R^{\mathrm{c}} = \{(s, *, s') \mid (s, s') \in R\}$, $L^{\mathrm{a}}(s) = \{p \in \mathtt{AP} \mid L(s, p) = 1\}$, and $L^{\mathrm{c}}(s) = \{p \in \mathtt{AP} \mid L(s, p) \neq 0\}$.

$$
\begin{aligned}
[\![\ p\ ]\!]^{\mathbf{K}}\, s &\stackrel{\text{def}}{=} L(s,p)\\
[\![\ \neg\phi\ ]\!]^{\mathbf{K}}\, s &\stackrel{\text{def}}{=} 1-([\![\ \phi\ ]\!]^{\mathbf{K}}\, s)\\
[\![\ \phi_1\wedge\phi_2\ ]\!]^{\mathbf{K}}\, s &\stackrel{\text{def}}{=} ([\![\ \phi_1\ ]\!]^{\mathbf{K}}\, s)\wedge([\![\ \phi_2\ ]\!]^{\mathbf{K}}\, s)\\
[\![\ \Diamond\phi\ ]\!]^{\mathbf{K}}\, s &\stackrel{\text{def}}{=} \bigvee\{[\![\ \phi\ ]\!]^{\mathbf{K}}\, s' \mid (s,s')\in R\}.
\end{aligned}
$$

Fig. 11. Property semantics for propositional modal logic over partial Kripke structures (Bruns and Godefroid 1999), where $s\in\Sigma$ and $\wedge$ and $\bigvee$ are defined for $0<1/2<1$, which is the *truth ordering* of $\mathbf{K}$.

Proof. Relations of type $\Sigma\times\Sigma$ are in one-to-one correspondence to relations of type $\Sigma\times\{*\}\times\Sigma$. As for the labelling functions, $L^{\mathrm{a}}(s)\subseteq L^{\mathrm{c}}(s)$ follows since $0\neq 1$. Conversely, any pair $(L^{\mathrm{a}},L^{\mathrm{c}})$ with $L^{\mathrm{a}}(s)\subseteq L^{\mathrm{c}}(s)$ for all $s\in\Sigma$ determines a function $L:\Sigma\times\mathtt{Act}\to\mathbf{K}$ such that $L(s,p)=1$ iff $p\in L^{\mathrm{a}}(s)$; and $L(s,p)=0$ iff $p\notin L^{\mathrm{c}}(s)$. These transformations are clearly inverses of each other. □

Definition 20 (Translating partial Kripke structures). Let $\mathscr{P}=(\Sigma,R,L)$ be a partial Kripke structure with signature AP and let $\mathscr{K}$ be its corresponding Kripke MTSs as in Lemma 2. We then define $\mathbf{P}[\mathscr{P}]\stackrel{\text{def}}{=}\mathbf{M}[\mathscr{K}]$. Given a formula ϕ of propositional modal logic, let $K(\phi)$ be the formula obtained by replacing each occurrence of $\Diamond$ in ϕ with $(\exists *)$.

Theorem 9 (Soundness and completeness of translation). Let $\mathscr{P}=(\Sigma,R,L)$ be a partial Kripke structure with signature AP.

1 The modal transition system $\mathbf{P}[\mathscr{P}]$ has signature $\mathtt{AP}+\{*\}$.
2 The relational inverse of the greatest completeness order in $\mathscr{P}$, which is the union of all completeness orders in $\mathscr{P}$ (Bruns and Godefroid 1999), is the greatest refinement in $\mathbf{P}[\mathscr{P}]$.
3 For all ϕ of propositional modal logic, $[\![\ \phi\ ]\!]^{\mathbf{K}}\, s=1$ iff $s\in[\![\ T(K(\phi))\ ]\!]^{\mathrm{a}}$; $[\![\ \phi\ ]\!]^{\mathbf{K}}\, s=0$ iff $s\notin[\![\ T(K(\phi))\ ]\!]^{\mathrm{c}}$.

Proof.

1 This is an immediate consequence of Theorem 7.
2 By Theorem 7, it suffices to show the statement for the corresponding Kripke MTS $\mathscr{K}$ instead of for $\mathbf{P}[\mathscr{P}]$. Inspecting Definition 15 and the third part of Definition 19, this is now clear.
3 By Theorem 7, it suffices to show the statement for $[\![\ K(\phi)\ ]\!]^{\mathrm{m}}$ over $\mathscr{K}$ instead of $[\![\ T(K(\phi))\ ]\!]^{\mathrm{m}}$ over $\mathbf{P}[\mathscr{P}]$, which we prove by structural induction:
   (a) We have $[\![\ p\ ]\!]^{\mathbf{K}}\, s=1$ iff $L(s,p)=1$ iff $p\in L^{\mathrm{a}}(s)$ iff $s\in[\![\ K(p)\ ]\!]^{\mathrm{a}}$; dually, $[\![\ p\ ]\!]^{\mathbf{K}}\, s=0$ iff $L(s,p)=0$ iff $p\notin L^{\mathrm{c}}(s)$ iff $s\notin[\![\ K(p)\ ]\!]^{\mathrm{c}}$.
   (b) For negation, $x\stackrel{\text{def}}{=}[\![\ \neg\phi\ ]\!]^{\mathbf{K}}\, s=1-[\![\ \phi\ ]\!]^{\mathbf{K}}\, s$. By induction, x equals 1 iff $s\notin[\![\ K(\phi)\ ]\!]^{\mathrm{c}}$ iff $s\in[\![\ K(\neg\phi)\ ]\!]^{\mathrm{a}}$. By induction, x equals 0 iff $s\in[\![\ K(\phi)\ ]\!]^{\mathrm{a}}$ iff $s\notin[\![\ K(\neg\phi)\ ]\!]^{\mathrm{c}}$.
   (c) For conjunction, $y\stackrel{\text{def}}{=}[\![\ \phi_1\wedge\phi_2\ ]\!]^{\mathbf{K}}\, s=([\![\ \phi_1\ ]\!]^{\mathbf{K}}\, s)\wedge([\![\ \phi_2\ ]\!]^{\mathbf{K}}\, s)$. By induction, y equals 1 iff $s\in[\![\ K(\phi_i)\ ]\!]^{\mathrm{a}}$ for $i=1,2$ iff $s\in[\![\ K(\phi_1\wedge\phi_2)\ ]\!]^{\mathrm{a}}$. By induction, y equals 0 iff $s\notin[\![\ K(\phi_i)\ ]\!]^{\mathrm{c}}$ for some $i=1,2$ iff $s\notin[\![\ K(\phi_1\wedge\phi_2)\ ]\!]^{\mathrm{c}}$.

(d) For modalities, $z \stackrel{\text{def}}{=} [\![\Diamond \phi]\!]^{\mathbf{K}} s = \bigvee\{[\![\phi]\!]^{\mathbf{K}} s' \mid (s, s') \in R\}$). By induction, z equals 1 iff there is some s' with $(s, s') \in R$ (that is, $(s, *, s) \in R^{\mathrm{a}}$) and $s' \in [\![K(\phi)]\!]^{\mathrm{a}}$ iff $s \in [\![K(\Diamond \phi)]\!]^{\mathrm{a}}$. By induction, z equals 0 iff $s' \notin [\![K(\phi)]\!]^{\mathrm{c}}$ for all s' with $(s, *, s') \in R$ iff $s \notin [\![K(\Diamond \phi)]\!]^{\mathrm{c}}$. □

5. Related work

Models and abstraction. Modal transition systems were introduced in Larsen and Thomsen (1988). A logical characterisation of refinement can be found in Larsen (1989). The models developed in Dams' thesis (Dams 1996) and in Dams *et al.* (1997) correspond to the 'mixed' Kripke MTSs of Section 4.1. (We presented a more special class of mixed transition systems, informed by our choice of domain equation in Section 3.) Partial Kripke structures (Morikawa 1989) were studied in Bruns and Godefroid (1999). They showed that their three-valued property semantics can be computed by conventional model checks over two Kripke structures (Bruns and Godefroid 2000) – this is also possible for modal transition systems (Godefroid *et al.* 2001) and Kripke modal transition systems (Huth 2002a). In Bruns and Godefroid (2000), generalised model checking specifies a more precise semantics for such models and reduces such property verification to the non-emptiness problem of alternating Büchi word automata over a one-letter alphabet. The account of extended transition systems and partial bisimulations (Milner 1981; Walker 1990) was based on Bruns and Godefroid (1999). In Schmidt (2001), it is shown how a concrete and naive trace-set semantics is transformed, by stepwise abstract interpretation (Cousot and Cousot 1977), into a modal transition system that is then subject to property checks for branching-time logics. This transformation of models makes use of the existential and universal abstractions presented in Cousot and Cousot (2000). In Huth (1999; 2001; 2002b), the modalities of modal transition systems are generalised to a wider class of models and sound abstractions are developed. The paper Huth *et al.* (2001) is the original rendition of portions of Sections 2 and 4. In Godefroid *et al.* (2001), a calculus for the computation and representation of incremental abstractions is presented for modal transition systems. Loose specifications are also considered for variations of first-order logic; we can mention the semantics of Alloy Jackson *et al.* (2000) and Jackson *et al.* (2001), the use of the Smyth powerdomain in Huth and Pradhan (2001), and the Kleene semantics of an extended first-order logic in Sagiv *et al.* (1999) used for shape analysis.

Domains and logic. In Abramsky (1991), Abramksy studies a domain of synchronisation trees and describes its logical counterpart, using Stone duality. This logic serves as a 'rational reconstruction' (Abramsky 1991) of Hennessy–Milner logic. In this domain, a fully abstract semantics for terms of the process algebra SCCS is given. The mixed powerdomain was discovered independently by Heckmann (Heckmann 1990) and Gunter (Gunter 1992). The former contains a concise axiomatisation of the mix algebras. Three-valued logic historically emphasised the development of proof theory; see, for example, Segerberg (1967) and Morikawa (1989). The three-valued interpretation of set-theory used in this paper is Kleene's strong interpretation of propositional logic (Kleene 1952). It appears that the mixed powerdomain generalises this semantics to non-flat data settings.

Acknowledgments

We gratefully thank the anonymous referees for their detailed corrections and most helpful suggestions on improving the presentation of this material. Part of this research was carried out with the generous support of the U.S. National Science Foundation under grants CCR-99010171, 9970679, 02030716, ITR-0085949, 0086154, and INT-9981558. We would like to dedicate this paper to Dana Scott on the occasion of his 70th birthday.

References

Abramsky, S. (1991) A domain equation for bisimulation. *Information and Computation* **92** (2) 161–218.

Abramsky, S. and Jung, A. (1994) Domain theory. In: Abramsky, S., Gabbay, D. M. and Maibaum, T. S. E. (eds.) *Handbook of Logic in Computer Science*, Oxford University Press, **3** 1–168.

Ball, T., Podelski, A. and Rajamani, S. K. (2001) Boolean and Cartesian Abstraction for Model Checking C Programs. In: Margaria, T. and Yi, W. (eds.) Proceedings of TACAS'2001, Genova, Italy. *Springer-Verlag Lecture Notes in Computer Science* **2031** 268–283.

Bradfield, J. C. (1991) *Verifying Temporal Properties of Systems*, Birkhäuser, Boston, Mass.

Bruns, G. and Godefroid, P. (1999) Model Checking Partial State Spaces with 3-Valued Temporal Logics. In: Proceedings of the 11th Conference on Computer Aided Verification. *Springer-Verlag Lecture Notes in Computer Science* **1633** 274–287.

Bruns, G. and Godefroid, P. (2000) Generalized Model Checking: Reasoning about Partial State Spaces. In: Proceedings of CONCUR'2000 (11th International Conference on Concurrency Theory). *Springer-Verlag Lecture Notes in Computer Science* **1877** 168–182.

Burch, J. R., Clarke, E. M., Dill, D. L., McMillan, K. L. and Hwang, J. (1990) Symbolic model checking: 10^{20} states and beyond. Proceedings of the Fifth Annual Symposium on Logic in Computer Science.

Chase, D., Wegman, M. and Zadeck, F. (1990) Analysis of pointers and structures. In: *SIGPLAN Conf. on Prog. Lang. Design and Implementation*, ACM Press 296–310.

Clarke, E. M. and Emerson, E. A. (1981) Synthesis of synchronization skeletons for branching time temporal logic. In: Kozen, D. (ed.) Logic of Programs Workshop. *Springer-Verlag Lecture Notes in Computer Science* **131** 52–71.

Cousot, P. and Cousot, R. (1977) Abstract interpretation: a unified lattice model for static analysis of programs. In: *Proc. 4th ACM Symp. on Principles of Programming Languages*, ACM Press 238–252.

Cousot, P. and Cousot, R. (2000) Temporal abstract interpretation. In: *Conference Record of the 27th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, Boston, Mass., ACM Press.

Dam, M. (1994) CTL* and ECTL* as Fragments of the Modal mu-Calculus. *Theoretical Computer Science* **126** 77–96.

Dams, D. (1996) *Abstract interpretation and partition refinement for model checking*, Ph.D. thesis, Technische Universiteit Eindhoven, The Netherlands.

Dams, D., Gerth, R. and Grumberg, O. (1997) Abstract interpretation of reactive systems. *ACM Transactions on Programming Languages and Systems* **19** (2) 253–291.

Ghiya, R. and Hendren, L. J. (1996) Is it a Tree, a DAG, or a Cyclic Graph? A Shape Analysis for Heap-Directed Pointers in C. In: *Proceedings of the 23rd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages* 1–15.

Godefroid, P., Huth, M. and Jagadeesan, R. (2001) Abstraction-based Model Checking using Modal Transition Systems. In: Proceedings of the International Conference on Theory and Practice of Concurrency. *Springer-Verlag Lecture Notes in Computer Science* **2154** 426–440.

Gunter, C. (1992) The mixed power domain. *Theoretical Computer Science* **103** 311–334.

Heckmann, R. (1990) Set Domains. In: Jones, N. D. (ed.) European Symposium on Programming. *Springer-Verlag Lecture Notes in Computer Science* **432** 177–196.

Hennessy, M. C. B. and Milner, R. (1985) Algebraic laws for non-determinism and concurrency. *JACM* **32** 137–161.

Hoare, C. A. R. (1985) *Communicating Sequential Processes*, Prentice-Hall.

Hofmann, K. H. and Mislove, M. (1981) Local compactness and continuous lattices. In: Banaschewski, B. and Hoffmann, R.-E. (eds.) Continuous Lattices. *Springer-Verlag Lecture Notes in Computer Science* **871** 209–248.

Holzmann, G. (1997) The model checker SPIN. *IEEE Transactions on Software Engineering* **23** 279–295.

Huth, M. (1999) A Unifying Framework for Model Checking Labeled Kripke Structures, Modal Transition Systems, and Interval Transition Systems. In: Proceedings of the 19th International Conference on the Foundations of Software Technology & Theoretical Computer Science, IIT Chennai, India. *Springer-Verlag Lecture Notes in Computer Science* **1738** 369–380.

Huth, M. (2001) Domains of view: a foundation for specification and analysis. Chapter in: *Domains and Processes*, Kluwer Academic Press 183–218.

Huth, M. (2002a) Model checking modal transition systems using Kripke structures. In: Third International Workshop on Verification, Model Checking and Abstract Interpretation, Venice, Italy. *Springer-Verlag Lecture Notes in Computer Science* **2294** 302–316.

Huth, M. (2002b) Possibilistic and Probabilistic Abstraction-Based Model Checking. In: Hermanns, H. and Segala, R. (eds.) Process Algebra and Probabilistic Methods, Performance Modeling and Verification, Second Joint International Workshop PAPM-PROBMIV 2002, Copenhagen, Denmark. *Springer-Verlag Lecture Notes in Computer Science* **2399** 115–134.

Huth, M., Jagadeesan, R. and Schmidt, D. (2001) Modal transition systems: a foundation for three-valued program analysis. In: Sands, D. (ed.) *Proceedings of the European Symposium on Programming (ESOP'2001)*, Springer Verlag 155–169.

Huth, M. and Pradhan, S. (2001) Model-Checking View-Based Partial Specifications. In: Brookes, S. and Mislove, M. (eds.) *Electronic Notes in Theoretical Computer Science*, Elsevier Science Publishers **45**.

Huth, M. and Pradhan, S. (2002) Lifting assertion and consistency checkers from single to multiple viewpoints. Technical Report TR 2002/11, Imperial College London, Department of Computing.

Jackson, D., Schechter, I. and Shlyakhter, I. (2000) Alcoa: the alloy constraint analyser. In: *Proc. International Conference on Software Engineering*, Limerick, Ireland.

Jackson, D., Shlyakhter, I. and Sridharan, M. (2001) A Micromodularity Mechanism. In *Proceedings of the ACM SIGSOFT Conference on the Foundations of Software Engineering/European Software Engineering Conference (FSE/ESEC'01)*.

Jones, N. D. and Muchnick, S. (1979) Flow analysis and optimization of LISP-like structures. In: *Proc. 6th ACM Symp. Principles of Programming Languages* 244–256.

Jung, A. (1988) *Cartesian Closed Categories of Domains*, Ph.D. thesis, Fachbereich Mathematik, Technische Hochschule Darmstadt.

Kelb, P. (1994) Model checking and abstraction: a framework preserving both truth and failure information. Technical Report OFFIS, University of Oldenburg, Germany.

Kleene, S. C. (1952) *Introduction to Metamathematics*, Van Nostrand.

Kozen, D. (1983) Results on the propositional mu-calculus. *Theoretical Computer Science* **27** 333–354.

Kupferman, O. and Vardi, M. Y. (1998) Modular model checking. In: Proc. Compositionality Workshop. *Springer-Verlag Lecture Notes in Computer Science* **1536** 381–401.

Larsen, K. G. (1989) Modal Specifications. In: Sifakis, J. (ed.) Automatic Verification Methods for Finite State Systems, International Workshop, Grenoble, France. *Springer-Verlag Lecture Notes in Computer Science* **407** 232–246.

Larsen, K. (1990) Proof systems for satisfiability in Hennessy–Milner logic with recursion. *Theoretical Computer Science* **72** 265–288.

Larsen, K. G. and Thomsen, B. (1988) A Modal Process Logic. In: *Third Annual Symposium on Logic in Computer Science*, IEEE Computer Society Press 203–210.

Milner, R. (1981) A modal characterisation of observable machine behaviours. In: Astesiano, G. and Böhm, C. (eds.) CAAP '81. *Springer-Verlag Lecture Notes in Computer Science* **112** 25–34.

Milner, R. (1989) *Communication and Concurrency*, Prentice-Hall.

Morikawa, O. (1989) Some modal logics based on a three-valued logic. *Notre Dame J. of Formal Logic* **30** 130–137.

de Nicola, R. and Vaandrager, F. (1995) Three Logics for Branching Bisimulation. *Journal of the Association of Computing Machinery* **42** (2) 458–487.

Nuseibeh, B., Kramer, J. and Finkelstein, A. (1994) A Framework for Expressing the Relationships Between Multiple Views in Requirements Specification. *IEEE Transactions on Software Engineering* **20** (10) 760–773.

Park, D. M. R. (1989) Concurrency and automata on infinite sequences. In: Deussen, P. (ed.) In: Proc. of the 5th GI Conference. *Springer-Verlag Lecture Notes in Computer Science* **104** 167–183.

Plotkin, G. D. (1976) A powerdomain construction. *SIAM Journal on Computing* **5** 452–487.

Plotkin, G. D. (1981) A Structural Approach to Operational Semantics. Technical Report FN-19, DAIMI, Computer Science Department, Aarhus University, Ny Munkegade, Building 540, DK-8000 Aarhus, Denmark. (Reprinted April 1991.)

Sagiv, M., Reps, T. and Wilhelm, R. (1999) Parametric Shape Analysis via 3-Valued Logic. In: *Proceedings of the 26th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, San Antonio, Texas 105–118.

Schmidt, D. A. (2001) From Trace Sets to Modal-Transition Systems by Stepwise Abstract Interpretation. (Submitted for publication.)

Segerberg, K. (1967) Some modal logics based on a three-valued logic. *Theoria* **33** 53–71.

Smyth, M. B. (1978) Powerdomains. *Journal of Computer and Systems Sciences* **16** 23–36.

Walker, D. J. (1990) Bisimulation and divergence. *Information and Computation* **85** (2) 202–241.

Whaley, J. and Rinard, M. (1999) Compositional pointer and escape analysis for Java programs. In: *Proc. OOPSLA'99*, ACM 187–206.