Logical Methods in Computer Science
Vol. 1 (1:1) 2005, pp. 1–28
www.lmcs-online.org

Submitted Sep. 1, 2004
Published Jan. 26, 2005

LABELLED TRANSITION SYSTEMS AS A STONE SPACE

MICHAEL HUTH

Department of Computing, Imperial College London, South Kensington campus,
London SW7 2AZ, United Kingdom
e-mail address: M.Huth@doc.imperial.ac.uk

Abstract. A fully abstract and universal domain model for modal transition systems and refinement, developed in [27], is shown to be a maximal-points space model for the bisimulation quotient of labelled transition systems over a finite set of events. In this domain model we prove that this quotient is a Stone space whose compact, zero-dimensional, and ultra-metrizable Hausdorff topology measures the degree of bisimilarity and that image-finite labelled transition systems are dense. Using this compactness we show that the set of labelled transition systems that refine a modal transition system, its "set of implementations," is compact and derive a compactness theorem for Hennessy-Milner logic on such implementation sets. These results extend to systems that also have partially specified state propositions, unify existing denotational, operational, and metric semantics on partial processes, render robust consistency measures for modal transition systems, and yield an abstract interpretation of compact sets of labelled transition systems as Scott-closed sets of modal transition systems.

1. Introduction

Labelled transition systems are a fundamental modelling formalism in many areas of computer science and one often needs to compare two or more such systems in applications. For example, in doing state compression prior to model checking one wants to ensure that the compressed system yields the same model checks as the uncompressed one. Similarly, if one system is a specification and another one its implementation, then program correctness can be established by proving these systems to be equivalent. By the same token, if two systems are not equivalent, one may want to know to what degree this is so, e.g. in a risk analysis of a safety-critical system.

This paper chooses bisimulation as the notion of equivalence of labelled transition systems.[1] Bisimulation is an established, sufficiently fine-grained notion of equivalence between labelled transition systems [35] so any approximative notions, e.g. testing [37], have bisimulation as a well accepted point of reference. Since quantitative aspects ought to be invariant under bisimulation, we stipulate that the quotient of all labelled transition systems with

2000 ACM Subject Classification: 03B44, 06E15, 68Q85.

Key words and phrases: modal and labelled transition systems, refinement and bisimulation, Stone space, Hennessy-Milner logic.

[1]Weak bisimulation [35] is bisimulation on a modified transition relation and we don't consider fairness in this paper.

LOGICAL METHODS IN COMPUTER SCIENCE
DOI:10.2168/LMCS-1 (1:1) 2005

respect to bisimulation is the right conceptual space for reasoning about and comparing quantitative aspects of labelled transition systems.

If two labelled transition systems are not bisimilar, one may require a quantitative measure of such differences and such a measure has many applications. We mention security protocols [39], where one system is the specification and the other is an implementation and where we may wish to quantify illicit information flow [15] or the effort needed to expose implementation flaws; modal specifications [32], where a specification captures a possibly infinite set of mutually non-bisimilar labelled transition systems; and requirements engineering [16], where each system may be the modal specification of a particular viewpoint and *consistency measures on modal specifications* are sought.

One principal aim of this paper is to unify several strands of established work in one integrated framework: metric semantics of processes à la Bakker & Zucker [12]; use of Hennessy-Milner logic, domain theory and transition systems à la Abramsky [1]; means of under-specifying and refining processes à la Larsen & Thomsen [33]; and representations of classical topological spaces as maximal-point spaces of domains à la Lawson [34]. To that end, we use a domain $\mathbb{D}$, defined in [27] and shown to be a universal model for finitely-branching modal transition systems and fully abstract for their refinement in loc. cit.

Specifically, we discover that the metric induced by the Lawson topology on $\mathbb{D}$ is a generalization of the one in [12] to modal transition systems; that the subspace of maximal elements of $\mathbb{D}$ is a Stone space with respect to the Lawson (or Scott) topology; and that this Stone space is an isomorphic representation of the quotient of all labelled transition systems modulo bisimulation, so the topology and metric carry over to that quotient. Since a Stone space has a *complete* ultra-metric, our model has labelled transition systems that are not image-finite, allowing the modelling of continuous state spaces, but all labelled transition systems can be approximated by image-finite ones to any degree of precision.

The compactness of this quotient space then makes it possible to study the topological structure of sets of implementations for modal transition systems, the second principal aim of this paper. In particular, our topological analysis shows that 3-valued model checking [5, 6] reasons about compact sets of labelled transition systems, namely the set of all 2-valued refinements of a given 3-valued system. We propose two measures, a pessimistic and an optimistic one, for how close any refining labelled transition systems of two such 3-valued systems can be. Using compactness, we prove that the optimistic measure is zero iff the two 3-valued systems in question have a common refinement.

Our concepts and results are also *robust under a change of representation*, e.g. in moving from event-based to state-based systems or those that combine state and event information. It would be of interest to see whether results similar to the ones of this paper are obtainable for systems that explicitly represent time, probability (e.g. as done in [13, 15]) or other quantitative information.

Outline of this paper: In Section 2 we review modal transition systems, their refinement, and a fully abstract domain model for these notions. Section 3 establishes the central result of this paper, showing that the maximal-points space of the fully abstract domain of Section 2 is a Stone space and the quotient of all labelled transition systems with respect to bisimulation. In Section 4 we give three applications of the compactness of this maximal-points space: a compactness theorem for Hennessy-Milner logic on compact sets of implementations, an abstract interpretation of compact sets of implementations as Scott-closed

sets of modal transition systems, and a robust consistency measure for modal transition systems. Section 5 states related work, and Section 6 concludes.

2. Domain of modal transition systems

Modal transition systems [33] are defined like labelled transition systems, except that transitions come in two modes that specify whether such transitions must or may be implemented. A refinement relation between modal transition systems therefore associates to a modal transition system those refining labelled transition systems in which all implementation choices have been resolved. In this section we formalize these notions and present the domain of [27] as a faithful mathematical model of the model-checking framework of modal transition systems.

2.1. Mixed transition systems and refinement.

We define Larsen & Thomsen's modal transition systems [33], their refinement and other key concepts formally and present the domain $\mathbb{D}$ which is a fully abstract model of such systems and their refinement [27]. Our results are shown within that domain. In this paper, let $(\alpha, \beta, \cdots \in) Act$ be a fixed finite set of events and $(w, w', \cdots \in) Act^*$ the set of finite words over Act with ϵ denoting the word of length zero. The labelled transition systems considered here have events from Act only. The structural properties of our domain model require that we also define Dams' more general notion of mixed transition systems [9, 11].

A modal transition system M has two transition relations $R^a, R^c \subseteq \Sigma \times Act \times \Sigma$ on a set of states Σ. The sets R^a and $\Sigma \times Act \times \Sigma \setminus R^c$ specify *contractual promises or expectations* about the reactive capacity and incapacity of implementations, respectively. These guarantees are to be understood with respect to the refinement of states. We write "a" in R^a to denote **a**sserted behavior and "c" in R^c to denote **c**onsistent behavior and use these annotations in judgments $\models^a$ and $\models^c$ below with the same meaning.

Example 2.1. In Figure 1 we see a contractual guarantee that any state refining Drinks cannot have a transition labelled with newPint to a state refining Talks as the triple $(\text{Drinks}, \text{newPint}, \text{Talks})$ is not in R^c. There is a contractual guarantee that any state refining Waits has a R^a-transition labelled with newPint to all states that refine Drinks or Talks.

Definition 2.2.

(1)
- A *mixed transition system* [9, 11] is a triple $M = (\Sigma, R^a, R^c)$ such that, for every *mode* $m \in \{a, c\}$, the pair (Σ, R^m) is a *labelled transition system*, i.e. $R^m \subseteq \Sigma \times Act \times \Sigma$.
- If $R^a \subseteq R^c$, then M is a *modal* transition system [33].
- We call M *image-finite* iff for all $s \in \Sigma$, $\alpha \in Act$, and $m \in \{a, c\}$ the set $\{s' \in \Sigma \mid (s, \alpha, s') \in R^m\}$ is finite.
- A mixed transition system M with a designated initial state i is *pointed*, written (M, i).
- We call elements of R^a *must-transitions* and elements of $R^c \setminus R^a$ *may-transitions*.

(2) Let $M = (\Sigma, R^a, R^c)$ be a mixed transition system.
- A relation $Q \subseteq \Sigma \times \Sigma$ is a *refinement within* M [33, 9] iff $(s, t) \in Q$ implies, for all $\alpha \in Act$,
  (a) if $(s, \alpha, s') \in R^a$, there exists some $(t, \alpha, t') \in R^a$ such that $(s', t') \in Q$; and

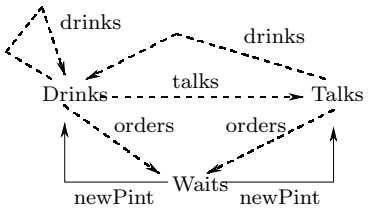

Figure 1: An image-finite modal transition system specifying aspects of "pub behavior."

(b) if $(t, \alpha, t') \in R^c$, there exists some $(s, \alpha, s') \in R^c$ such that $(s', t') \in Q$.

- We write $s \prec_M t$ or $s \prec t$ if there is some refinement Q with $(s, t) \in Q$. In that case, t *refines* (*is abstracted by*) s.
- States s and t are *refinement-equivalent* iff ($s \prec t$ and $t \prec s$).
- Let $(M, i) \prec (N, j)$ mean that j refines i in the mixed transition system that is the disjoint union of M and N; (M, i) and (N, j) are refinement-equivalent iff i and j are refinement-equivalent in that union.
- The *implementations* of (M, i) are those pointed modal transition systems without may-transitions that refine (M, i).

As the union $\prec_M$ of all refinements within M is also a refinement within M, $\prec_M$ is the greatest refinement relation within M. Please note that we use the relational inverse of the Q in [33, 9, 27], as done in [19], so our $(M, i) \prec (N, j)$ is written as $(N, j) \prec (M, i)$ in [27]. Larsen & Thomsen's modal transition systems and their refinement [33] are partial versions of labelled transition systems and bisimulation [35]. A modal transition system represents those labelled transition systems that refine it, the implementations of M. This representation is sound, for if a modal transition system M refines a modal transition system N, all labelled transition systems that refine M also refine N as $\prec$ is transitive.

Example 2.3.

(1) Figures 1 and 2 depict modal transition systems, where dashed and solid lines depict may-transitions and must-transitions, respectively. The refinement Q identifies states with the same activity; e.g. Drinks with TomDrinks and BobDrinks etc.
(2) The mixed transition system on the left of Figure 4 is not a modal transition system but is refinement-equivalent to the modal transition system on the right of Figure 4.

Remark 2.4. We may identify modal transition systems (Σ, R, R) with labelled transition systems (Σ, R) and refinement between such modal transition systems with bisimulation [33] and will freely move between these two representations of labelled transition systems and bisimulation subsequently.

2.2. **The interval domain as an allegory.** Before we present the domain model for refinement of modal transition systems we use Scott's interval domain [41] as a motivating example that features most of the desirable properties of our domain model.

Example 2.5. Figure 3 shows the interval domain and its ordering: $[r, s] \leq [r', s']$ iff ($r \leq r'$ and $s' \leq s$). In that case we say that $[r', s']$ refines $[r, s]$.

The interval domain nicely illustrates some of the properties we expect our domain model $\mathbb{D}$ to have.

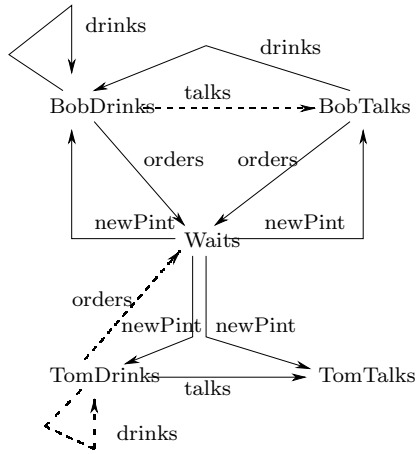

Figure 2: An image-finite modal transition system that refines the one in Figure 1.

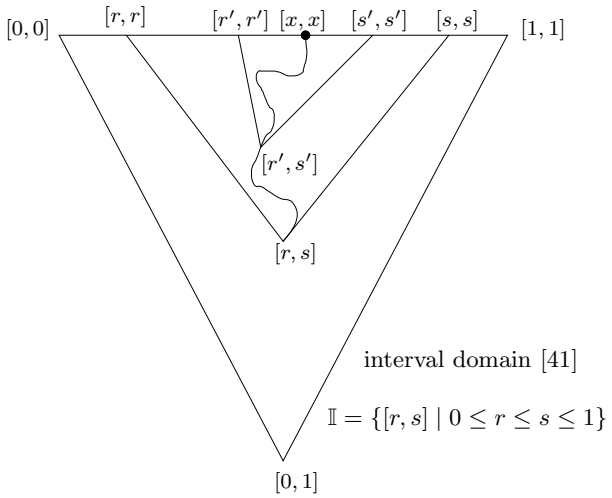

Figure 3: A schematic description of the interval domain and its order: $[r,s] \leq [r',s']$ iff $(r \leq r' \text{ and } s' \leq s)$.

(1) **Refinement is complete for implementations:** Real numbers $x \in [0,1]$ represented as intervals $[x,x]$ are the "implementations" of intervals, so $[r,s]$ has all $[x,x]$ with $x \in [r,s]$ as implementations. One can easily see that $[r,s]$ is refined by $[r',s']$ iff all implementations of $[r',s']$ are also implementations of $[r,s]$.
(2) **Universality:** The interval domain $\mathbb{I}$ is universal for worst/best-case abstractions of subsets of $[0,1]$. If we abstract $X \subseteq [0,1]$ by the interval $[\bigwedge X, \bigvee X] \in \mathbb{I}$, any element of $\mathbb{I}$ is the abstraction of at least one such X. In fact, there is a Galois connection $\alpha\colon \mathbb{P}([0,1])^{\mathrm{op}} \to \mathbb{I}$ and $\gamma\colon \mathbb{I} \to \mathbb{P}([0,1])^{\mathrm{op}}$ where $\alpha(X) = [\bigwedge X, \bigvee X]$ is the monotone abstraction function, $\gamma([r,s]) = [r,s]$ is the monotone "concretization" function, and $\alpha \circ \gamma = \mathrm{id}_{\mathbb{I}}$ and $\gamma \circ \alpha \leq \mathrm{id}_{\mathbb{P}([0,1])^{\mathrm{op}}}$.
(3) **Full abstraction:** The order on $\mathbb{I}$ coincides with the refinement relation as the latter means reverse containment of implementations by item (1) above.

(4) **Classical space as maximal-points space:** The set $[0,1]$ equipped with the compact Euclidean topology is isomorphic as a topological space to the set of maximal elements of $\mathbb{I}$ in the topology induced by the Scott- or Lawson-topology of $\mathbb{I}$.
(5) **Denseness of computable structures:** Intervals with rational endpoints approximate intervals to any degree of precision.
(6) **Consistency measure:** The map $c\colon \mathbb{I} \times \mathbb{I} \to \mathbb{I} \cup \{\bot\}$ defined by $c([r,s],[r',s']) = [\max(r,r'), \min(s,s')]$, where $[x,y]$ is understood to be $\bot$ if $x \not\leq y$, tells us whether its inputs are consistent with each other by checking whether its output is different from $\bot$. Non-overlapping intervals cannot possibly approximate the same real number.

The domain model $\mathbb{D}$ for refinement of modal transition systems [27] has similar properties which we discuss briefly here prior to their technical development in this paper. The completeness proof for implementations for refinement of modal transition systems does not depend on the compactness of $\max(\mathbb{D})$, is non-trivial, and presented elsewhere [28]. Universality amounts to showing that every modal transition system has a refinement-equivalent embedding in the domain $\mathbb{D}$. Full abstraction means that the order on $\mathbb{D}$ equals the greatest refinement relation on $\mathbb{D}$ interpreted as a modal transition system. The maximal-points space $\max(\mathbb{D})$ of $\mathbb{D}$ gives us a precise model of labelled transition systems and their notion of "nearness." This space turns out to be the quotient of labelled transition systems with respect to bisimulation such that the familiar metric based on tests expressed in Hennessy-Milner logic [37] induces the topology on that space. Finite-state labelled transition systems are shown to be dense in this space. Finally, the compactness of this space is proved and a monotone consistency measure

$$c\colon \mathbb{D} \times \mathbb{D} \to \mathbb{I} \tag{2.1}$$

between two modal transition systems is then derived thereof. Said compactness then renders a Galois connection between compact sets of implementations and Scott-closed sets of modal transition systems as shown in Theorem 4.6 below. Apart from these similarities with $\mathbb{I}$, a key difference is that $\mathbb{D}$ is algebraic and that the maximal-points space is therefore zero-dimensional.

2.3. **The domain model for refinement of modal transition systems.** The reader familiar with domain theory [2] may safely skip the next definition.

Definition 2.6.

(1)
- A *topological space* (X,τ) consists of a set X and a family τ of subsets of X such that $\{\}$ and X are in τ, and τ is closed under finite intersections and arbitrary unions.
- Elements $O \in \tau$ are *τ-open*, complements $X \setminus O$ with $O \in \tau$ are *τ-closed*, and sets that are τ-open and τ-closed are *τ-clopen*.

(2)
- A subset A of a partial order $(D,\leq)$ is *directed* iff (for all $a, a' \in A$ there is some $a'' \in A$ with $a, a' \leq a''$).
- A partial order $(D,\leq)$ is a *dcpo* iff all its directed subsets A have a least upper bound $\bigvee A$.
- We write
$$ub(A) \ = \{u \in D \mid \forall a \in A\colon a \leq u\}$$
for the set of *upper bounds* of A.

- We denote by
$$mub(A) = \{u \in ub(A) \mid \forall u' \in ub(A) \colon u' \leq u \Rightarrow u = u'\}$$
the set of *minimal upper bounds* of A.
- An element $k \in D$ is *compact* in a dcpo D iff (for all directed sets A of D with $k \leq \bigvee A$ there is some $a \in A$ with $k \leq a$). We write $\mathbf{K}(D)$ for the set of compact elements of D.
- A dcpo D is *algebraic* iff for all $d \in D$ the set $\{k \in \mathbf{K}(D) \mid k \leq d\}$ is directed with least upper bound d.
- For a finite subset F of D define, for all $n \geq 1$
$$\begin{aligned} mub^1(F) &= mub(F) \\ mub^{n+1}(F) &= mub(mub^n(F)) \\ mub^\infty(F) &= \bigcup_{n \geq 1} mub^n(F)\,. \end{aligned}$$
- A *bifinite domain*, also known as an *SFP*-domain, is an algebraic dcpo D such that for every finite subset $F \subseteq \mathbf{K}(D)$ the set $mub^\infty(F)$ is finite, contained in $\mathbf{K}(D)$, and $ub(F) = \uparrow mub(F)$ where for any $X \subseteq D$ we write
$$\uparrow X = \{d \in D \mid \exists x \in X \colon x \leq d\} \qquad \downarrow X = \{d \in D \mid \exists x \in X \colon d \leq x\}$$
- We call X *upper* iff $X = \uparrow X$; *lower* iff $X = \downarrow X$.

(3) For a bifinite domain D, we define
- the *Scott-topology* σ_D to consist of all subsets U of D satisfying
$$U = \uparrow\!(U \cap \mathbf{K}(D))$$
- the *Lawson-topology* λ_D to consist of all subsets V of D such that $x \in V$ implies the existence of some $k, l \in \mathbf{K}(D)$ with $x \in \uparrow k \setminus \uparrow l \subseteq V$; and
- the *σ_D-compact saturated* subsets of D to be the λ_D-closed upper subsets of D.

The definitions of item (3) above are really characterizations [2]. We use the *initial* solution $\mathbb{D}$ of a domain equation, presented in [27] and denoted by $\mathcal{D}$ in loc. cit., as the domain whose set of maximal points we prove to be the Stone space of pointed labelled transition systems modulo bisimulation. The items (2) and (3) of Definition 2.7 below are Definition 8 and 9 of [27], respectively.

Definition 2.7 ([27])**.**

(1) The *mixed powerdomain* $\mathcal{M}[D]$ [23, 22] of a bifinite domain D has as elements all pairs (L, U) where L is σ_D-closed and U is σ_D-compact saturated such that L and U satisfy the mix condition
$$L = \downarrow\!(L \cap U)\ . \tag{2.2}$$
The order on $\mathcal{M}[D]$ is defined by
$$(L, U) \leq (L', U') \qquad \text{iff} \qquad (L \subseteq L' \text{ and } U' \subseteq U)\,. \tag{2.3}$$

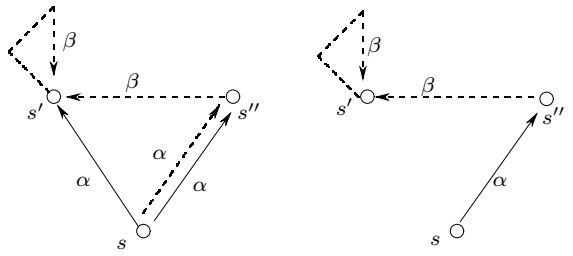

Figure 4: On the left: a mixed transition system (Σ, R^a, R^c) satisfying the mix condition (MC). Dashed lines denote elements of R^c and solid lines denote elements of R^a. For $(s, \alpha, s') \in R^a$ there is $(s, \alpha, s'') \in R^a \cap R^c$ with $s' \prec s''$. The other tuple in R^a is matched by itself as it is in $R^a \cap R^c$. On the right: a modal transition system that is refinement-equivalent to the mixed transition system on the left. Its set of must-transitions is $R^a \cap R^c$ (solid lines) and its set of may-transitions is R^c (solid or dashed lines).

(2) Since $\mathcal{M}[D]$ is a bifinite domain whenever D is bifinite and since the functors $\mathcal{M}$ and $\prod$ are locally continuous [23, 2], we can solve the domain equation

$$D = \prod_{\alpha \in Act} \mathcal{M}[D] \tag{2.4}$$

over bifinite domains where $\prod_{\alpha \in Act}$ denotes the product functor over all events in Act, and write $\mathbb{D}$ for the *initial solution* of that equation.

(3) The domain $\mathbb{D}$ may be *interpreted as a pointed mixed transition system*

$$\mathcal{D} = (\mathbb{D}, \mathbb{R}^a, \mathbb{R}^c) \tag{2.5}$$

where the recursion $d = ((d^a_\alpha, d^c_\alpha))_{\alpha \in Act}$ of the equation (2.4) for $\mathbb{D}$ specifies that all elements d' in the set d^a_α (d^c_α) are exactly the $\mathbb{R}^a$-successors ($\mathbb{R}^c$-successors) of d for α in $\mathcal{D}$ (respectively).

Thus, the L and U in (2.2) model $\mathbb{R}^a$- and $\mathbb{R}^c$-transitions within $\mathcal{D}$, respectively. The order-theoretic mix condition (2.2) has an equivalent version for mixed transition systems.

Definition 2.8 ([27])**.** A mixed transition system $M = (\Sigma, R^a, R^c)$ satisfies the *mix condition (MC)* iff (for all $(s, \alpha, s') \in R^a$ there is some $(s, \alpha, s'') \in R^a \cap R^c$ such that $s' \prec s''$).

As shown in Proposition 3 in [27], (2.2) ensures that $\mathcal{D}$ satisfies the mix condition (MC) since the order on $\mathbb{D}$ is a refinement within $\mathbb{D}$: for all $(e, \alpha, e') \in \mathbb{R}^a$ there is some $(e, \alpha, e'') \in \mathbb{R}^a \cap \mathbb{R}^c$ such that $(\mathcal{D}, e') \prec (\mathcal{D}, e'')$.

Example 2.9. Figure 4 demonstrates that mixed transition systems (Σ, R^a, R^c) that satisfy the mix condition (MC) are refinement-equivalent to modal transition systems $(\Sigma, R^a \cap R^c, R^c)$. Therefore, such mixed transition systems are merely modal transition systems in disguise [27].

Remark 2.10. By Proposition 1 in [27] and as seen in the previous example, the mix condition (MC) guarantees that the *mixed* transition system $(\mathbb{D}, \mathbb{R}^a, \mathbb{R}^c)$ is refinement-equivalent to the *modal* transition system $(\mathbb{D}, \mathbb{R}^a \cap \mathbb{R}^c, \mathbb{R}^c)$. Therefore all reasoning that is invariant

under refinement equivalence, as is the case in this paper, may be done with the latter modal transition system and we abuse notation to refer to that modal transition system as $\mathcal{D}$ as well.

The domain model $\mathbb{D}$ is *universal*: There is an embedding $(M, i) \mapsto \langle\!|\, M, i \,|\!\rangle$ from the class of image-finite pointed mixed transition system satisfying the mix-condition (MC) to elements of $\mathbb{D}$ such that (M, i) and $(\mathcal{D}, \langle\!|\, M, i \,|\!\rangle)$ are refinement-equivalent (Theorem 6.1 in [27]). The domain model $\mathbb{D}$ is *fully abstract*: For all $d, e \in \mathbb{D}$, we have $d \leq e$ iff $(\mathcal{D}, d) \prec (\mathcal{D}, e)$ (Theorem 5 in [27]). For sake of completeness, we sketch the construction of this embedding and needed aspects of the full abstraction proof in the next section.

3. Stone space of labelled transition systems

We show that the maximal elements of $\mathbb{D}$ are precisely the representations of pointed labelled transition systems modulo bisimulation; and that this quotient is a Stone space and therefore determined by a complete ultra metric.

3.1. **The maximal-points space.** We define the required notions from topology.

Definition 3.1.

(1) A topological space (X, τ) is
   (a) *compact* iff for all $\mathcal{U} \subseteq \tau$ with $X \subseteq \bigcup \mathcal{U}$ there is a finite subset $\mathcal{F} \subseteq \mathcal{U}$ with $X \subseteq \bigcup \mathcal{F}$;
   (b) *Hausdorff* iff for all $x \neq x'$ in X there are $O, O' \in \tau$ with $x \in O$, $x' \in O'$ and $O \cap O' = \{\}$;
   (c) *zero-dimensional* iff every τ-open set is the union of τ-clopens; and
   (d) a *Stone space* iff it is zero-dimensional, compact, and Hausdorff.

(2) A subset C of (X, τ) is *τ-compact* iff the topological space $(C, \{U \cap C \mid U \in \tau\})$ is compact.

(3) A subset A of X is *dense* in (X, τ) iff $A \cap O$ is non-empty for all non-empty $O \in \tau$.

(4) An *ultra-metric* on X is a function $d\colon X \times X \to [0, 1]$ such that for all $x, y, z \in X$
   (a) $d(x, y) = 0$ iff $x = y$;
   (b) $d(x, y) = d(y, x)$; and
   (c) $d(x, z) \leq \max(d(x, y), d(y, z))$.

(5) An ultra-metric $d\colon X \times X \to [0, 1]$ *determines a topology* τ_d on X whose elements are all those $O \subseteq X$ that are unions of sets of the form $B_\eta(x) = \{y \in X \mid d(x, y) < \eta\}$ for $x \in X$ and rational $\eta > 0$.

(6) A topological space (X, τ) is *ultra-metrizable* iff there is an ultra-metric $d\colon X \times X \to [0, 1]$ such that $\tau = \tau_d$.

(7) We denote by $\max(\mathbb{D}) = \{m \in \mathbb{D} \mid \forall d \in \mathbb{D}\colon m \leq d \Rightarrow m = d\}$ the set of *maximal elements* of $\mathbb{D}$. The set

$$\mathbb{X} = \max(\mathbb{D}) \tag{3.1}$$

has a *maximal-points space topology* [34]

$$\tau_{\mathbb{X}} = \{U \cap \mathbb{X} \mid U \in \sigma_{\mathbb{D}}\}\,. \tag{3.2}$$

(8) For $d \in \mathbb{D}$, we write

$$M(d) = \uparrow d \cap \max(\mathbb{D})\,. \tag{3.3}$$

$$
\begin{array}{lll}
(N,i) \models^m tt & & \\
(N,i) \models^m \neg\phi & \text{iff} & (N,i) \not\models^{\neg m} \phi \\
(N,i) \models^m \langle\alpha\rangle\phi & \text{iff} & \text{for some } (i,\alpha,i') \in R^m,\ (N,i') \models^m \phi \\
(N,i) \models^m \phi \wedge \psi & \text{iff} & ((N,i) \models^m \phi \text{ and } (N,i) \models^m \psi)
\end{array}
$$

Figure 5: Semantics of Hennessy-Milner logic with two judgments $(N,i) \models^m \phi$ where $m \in \{a,c\}$, $\neg a = c$, and $\neg c = a$.

Since $\mathbb{D}$ is a bifinite domain, the Lawson condition [34] holds for $\mathbb{D}$, namely that the topology $\tau_{\mathbb{X}}$ is also induced by the $\lambda_{\mathbb{D}}$-topology:

$$\tau_{\mathbb{X}} = \{V \cap \mathbb{X} \mid V \in \lambda_{\mathbb{D}}\}. \tag{3.4}$$

We remark that not all bifinite domains D enjoy the property that $\max(D)$ is compact in the topology induced by σ_D or λ_D.

3.2. **Maximal-points space is zero-dimensional and Hausdorff.** We first record that $\tau_{\mathbb{X}}$ is Hausdorff and zero-dimensional. Proposition 3.2 below holds for any algebraic domain satisfying the Lawson condition [34]. We state and prove that proposition for $\mathbb{D}$ for sake of completeness.

Proposition 3.2. *The topological space $(\mathbb{X}, \tau_{\mathbb{X}})$ is zero-dimensional and Hausdorff.*

Proof.

- Every $U \in \sigma_{\mathbb{D}}$ is the union of $\sigma_{\mathbb{D}}$-opens $\uparrow k$, $k \in \mathbf{K}(\mathbb{D})$, as $\mathbb{D}$ is algebraic. But each $\uparrow k$ is $\lambda_{\mathbb{D}}$-clopen as $\sigma_{\mathbb{D}} \subseteq \lambda_{\mathbb{D}}$ and $\uparrow k$ is $\lambda_{\mathbb{D}}$-closed. From the Lawson condition for $\mathbb{D}$, (3.4), we infer that $M(k)$ is $\tau_{\mathbb{X}}$-clopen and so $\tau_{\mathbb{X}}$ is zero-dimensional as every $O \in \tau_{\mathbb{X}}$ is the union of such sets.
- To show that $\tau_{\mathbb{X}}$ is Hausdorff, let $x \neq y$. Since $\mathbb{D}$ is a partial order we may assume $x \not\leq y$ without loss of generality. Since $\mathbb{D}$ is algebraic, $x \not\leq y$ implies $k \leq y$ and $k \not\leq x$ for some $k \in \mathbf{K}(\mathbb{D})$. But $M(k)$ is $\tau_{\mathbb{X}}$-open and contains y whereas x is in $\mathbb{X} \setminus M(k)$ which is $\tau_{\mathbb{X}}$-open since $M(k)$ is also $\tau_{\mathbb{X}}$-closed.

□

3.3. **Semantics of Hennessy-Milner logic.** We use tools from temporal logic to develop a sufficient criterion for membership in $\max(\mathbb{D})$.

Definition 3.3.

(1) The set of formulas of *Hennessy-Milner logic* [24] is generated by the grammar

$$\phi ::= tt \mid \neg\phi \mid \langle\alpha\rangle\phi \mid \phi \wedge \phi \tag{3.5}$$

where α ranges over the finite set of events Act.

(2) Let $(N,i) = ((\Sigma, R^a, R^c), i)$ be a pointed modal transition system. Larsen's semantics, denoted by $\models$ in [32] for Hennessy-Milner logic in negation normal form, is depicted in Figure 5.

(3) We write $[\alpha]$ for $\neg\langle\alpha\rangle\neg$ and $\phi \vee \psi$ for $\neg(\neg\phi \wedge \neg\psi)$ subsequently for all $\alpha \in Act$ and all ϕ and ψ of Hennessy-Milner logic.

Remark 3.4. For each $m \in \{a, c\}$ we have

$$\begin{array}{lll} (N,i) \models^m [\alpha]\phi & \text{iff} & \text{for all } (i,\alpha,i') \in R^{\neg m},\ (N,i') \models^m \phi \\ (N,i) \models^m \phi \vee \psi & \text{iff} & ((N,i) \models^m \phi \text{ or } (N,i) \models^m \psi)\ . \end{array}$$

Please note that $\models^m [\alpha]\phi$ universally quantifies over transitions in the *dual* mode $\neg m$.

Example 3.5. Consider the modal transition system N in Figure 1.

(1) We have $(N, \text{Talks}) \models^c \langle \text{drinks} \rangle tt$ because of the R^c-transition $(\text{Talks}, \text{drinks}, \text{Drinks})$. By the semantics of negation, this implies $(N, \text{Talks}) \not\models^a \neg\langle \text{drinks} \rangle tt$. We also infer $(N, \text{Talks}) \not\models^a \langle \text{drinks} \rangle tt$ as there is no state s with $(\text{Talks}, \text{drinks}, s) \in R^a$. By the semantics of disjunction, these two judgments render $(N, \text{Talks}) \not\models^a \langle \text{drinks} \rangle tt \vee \neg\langle \text{drinks} \rangle tt$. This judgment says that we can't determine that $\langle \text{drinks} \rangle tt \vee \neg\langle \text{drinks} \rangle tt$ is asserted in state Talks in N. As that formula is a tautology over labelled transition systems we see that judgments $(N, \text{Talks}) \models^a \phi$ under-approximate validity judgments "all refinements of (N, Talks) satisfy ϕ." As we show below, it turns out that the ability to capture these validity judgments for certain tautologies over labelled transition systems via $\models^a$ is what characterizes modal transition systems that are refinement-equivalent to labelled transition systems.

(2) We have $(N, \text{Waits}) \not\models^a [\text{newPint}][\text{talks}](\langle \text{drinks} \rangle tt \vee \neg\langle \text{drinks} \rangle tt)$ as there is an R^c-path $(\text{Waits}, \text{newPint}, \text{Drinks})(\text{Drinks}, \text{talks}, \text{Talks})$ for the word $\text{newPint talks} \in Act^*$ and $(N, \text{Talks}) \not\models^a \langle \text{drinks} \rangle tt \vee \neg\langle \text{drinks} \rangle tt$ by item (1). Therefore, the check $(N, \text{Waits}) \not\models^a [\text{newPint}][\text{talks}](\langle \text{drinks} \rangle tt \vee \neg\langle \text{drinks} \rangle tt)$ is unable to validate a tautology over labelled transition systems at state Waits in N.

3.4. **Denseness of image-finite labelled transition systems.** We sketch the definition of the embedding $(\!| M, i |\!) \in \mathbb{D}$ for an image-finite modal transition system (M, i) such that (M, i) and $(\mathcal{D}, (\!| M, i |\!))$ are refinement-equivalent [27]. This construction follows ideas from algebraic semantics à la Nivat-Courcelle-Guessarian [7] or à la Goguen-Thatcher-Wagner-Wright [21] in that we unfold pointed modal transition systems as finite trees for a fixed depth, adding a may-stub to all leaves of that tree for which there are still outgoing transitions in the pointed modal transition system. This unfolding is presented here via a simple process algebra.

Definition 3.6.

(1) The grammar for the *process algebra MPA* is

$$p ::= \mathbf{0} \mid \bot \mid \alpha_{tt}.p \mid \alpha_{\bot}.p \mid p + p \tag{3.6}$$

where α ranges over the finite set of events Act and no p in $p + p$ is allowed to be $\bot$ or $\mathbf{0}$.

(2) For each $p \in MPA$ let $\{\!| p |\!\} \in \mathbb{D}$ be as in Figure 6.

(3) For all $p \in MPA$, the structural operational semantics in Figure 7 defines a pointed modal transition system $(\llbracket p \rrbracket, p)$.

Example 3.7. Let $p \in MPA$ be $\text{drinks}_{\bot}.\bot + \text{orders}_{\bot}.\bot + \text{talks}_{tt}.\mathbf{0}$. Then $(\llbracket p \rrbracket, p)$ is refinement-equivalent to the image-finite pointed modal transition system in Figure 8.

We record that the denotational semantics of *MPA* in $\mathbb{D}$ matches the structural operational semantics. This proof is straightforward and amounts to showing that the saturations with $\downarrow$ and $\uparrow$ in $\mathbb{D}$ do not break refinement equivalence as they always occur in the right direction.

$$\{\!|\ \mathbf{0}\ |\!\} = ((\{\},\{\}))_{\alpha\in Act}$$

$$\{\!|\ \bot\ |\!\} = ((\{\},\mathbb{D}))_{\alpha\in Act}$$

$$(\{\!|\ \alpha_{tt}.p\ |\!\}^a_\alpha, \{\!|\ \alpha_{tt}.p\ |\!\}^c_\alpha) = (\downarrow\{\!|\ p\ |\!\}, \uparrow\{\!|\ p\ |\!\})$$

$$(\{\!|\ \alpha_{tt}.p\ |\!\}^a_\beta, \{\!|\ \alpha_{tt}.p\ |\!\}^c_\beta) = (\{\},\{\}),\ \alpha\neq\beta$$

$$(\{\!|\ \alpha_{\bot}.p\ |\!\}^a_\alpha, \{\!|\ \alpha_{\bot}.p\ |\!\}^c_\alpha) = (\{\}, \uparrow\{\!|\ p\ |\!\})$$

$$(\{\!|\ \alpha_{\bot}.p\ |\!\}^a_\beta, \{\!|\ \alpha_{\bot}.p\ |\!\}^c_\beta) = (\{\},\{\}),\ \alpha\neq\beta$$

$$\{\!|\ p+q\ |\!\}^m_\gamma = \{\!|\ p\ |\!\}^m_\gamma \cup \{\!|\ q\ |\!\}^m_\gamma,\ \gamma\in Act,\ m\in\{a,c\}$$

Figure 6: A denotational semantics of *MPA* in $\mathbb{D}$ that interprets $\mathbf{0}$ as deadlock, $\bot$ as the least element, $+$ as the mix union of [23], and the prefixes as expected using saturations with $\downarrow$ and $\uparrow$ to ensure membership in $\mathbb{D}$.

Lemma 3.8 ([28])**.** *For all $p\in MPA$, the modal transition system $(\|\ p\ \|, p)$ is refinement-equivalent to the mixed transition system $(\mathcal{D}, \{\!|\ p\ |\!\})$.*

To define the embedding $\langle\!|\, M,i\,|\!\rangle$ for an image-finite pointed modal transition system (M,i) consider $m\geq 0$, unwind M from i as a tree $M[m]$ such that all, and only, paths of length $\leq m$ of M are present. If a leaf of that tree has some R^c-successor in M, create R^c-loops on that leaf for *all* events in Act (a *may-stub*); otherwise, leave it as is (deadlock). By construction, this image-finite pointed modal transition system $(M[m],i)$ is the operational meaning $(\|\ p_m\ \|, p_m)$ of a term $p_m\in MPA$ so $m\leq m'$ and Lemma 3.8 imply that $\{\!|\ p_m\ |\!\}\leq\{\!|\ p_{m'}\ |\!\}$. Thus $\{\{\!|\ p_m\ |\!\}\mid m\geq 0\}$ is directed and we can set

$$\langle\!|\, M,i\,|\!\rangle = \bigvee_{m\geq 0} \{\!|\ p_m\ |\!\} \tag{3.7}$$

and note, shown in [23] for bifinite domains without reference to a process algebra, that

$$\mathbf{K}(\mathbb{D}) = \{\{\!|\ p\ |\!\}\mid p\in MPA\}\,. \tag{3.8}$$

We may thus represent all $k\in\mathbf{K}(\mathbb{D})$ in the form $\{\!|\ p\ |\!\}$ for some $p\in MPA$ subsequently.

Example 3.9. Figure 8 illustrates the construction of a finite approximation and depicts $(M[1], \mathrm{TomDrinks})$ for the pointed modal transition system $(M, \mathrm{TomDrinks})$ of Figure 2.

We define the characteristic formulas for terms p of the process algebra *MPA*, which will also be the characteristic formulas of the compact elements $\{\!|\ p\ |\!\}$ of $\mathbb{D}$.

Definition 3.10. For each $p\in MPA$, we define the formula ϕ_p of Hennessy-Milner logic in Figure 9.

These formulas characterize their terms, for one can interchange refinement checks $(\mathcal{D}, \{\!|\ p\ |\!\})\prec(\mathcal{D},d)$ with model checks $(\mathcal{D},d)\models^a\phi_p$ for all $d\in\mathbb{D}$.

$$\frac{}{\bot \longrightarrow^{\gamma}_{\bot} \bot}\ \text{MayStub}$$

$$\frac{}{\alpha_{tt}.p \longrightarrow^{\alpha}_{tt} p}\ \text{MustPrefix} \qquad \frac{}{\alpha_{\bot}.p \longrightarrow^{\alpha}_{\bot} p}\ \text{MayPrefix}$$

$$\frac{p \longrightarrow^{\alpha}_{v} p'}{p+q \longrightarrow^{\alpha}_{v} p'}\ \text{LChoice} \qquad \frac{q \longrightarrow^{\alpha}_{v} q'}{p+q \longrightarrow^{\alpha}_{v} q'}\ \text{RChoice}$$

Figure 7: Structural operational semantics of *MPA* in $\mathbb{D}$: $p \longrightarrow^{\alpha}_{\bot} p'$ and $p \longrightarrow^{\alpha}_{tt} p'$ denote a may-transition (respectively) must-transition from p to p', with label $\alpha \in Act$. There are no transitions out of $\mathbf{0}$; $v \in \{\bot, tt\}$; and the occurrence of γ ranges over all events in Act.

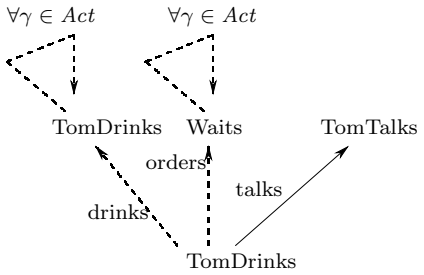

Figure 8: The pointed modal transition system $(M[1], \text{TomDrinks})$, an approximation of the pointed modal transition system $(M, \text{TomDrinks})$ in Figure 2. The states Waits and the second TomDrinks turn into may-stubs whereas the approximation recognizes TomTalks as a deadlocked state.

Lemma 3.11. *For all $d \in \mathbb{D}$ we have*

$$\{\!|\ p\ |\!\} \le d \qquad \textit{iff} \qquad (\mathcal{D}, d) \models^{a} \phi_p\,. \tag{3.9}$$

Proof. We prove this by structural induction on $p \in MPA$.

- We have $\{\!|\ \mathbf{0}\ |\!\} \le d$ iff (there are no $\mathbb{R}^c$-transitions out of d) iff $(\mathcal{D}, d) \models^{a} \psi_{\mathbf{0}}$.
- We have $\{\!|\ \bot\ |\!\} \le d$ for all $d \in \mathbb{D}$, but also $(\mathcal{D}, d) \models^{a} \psi_{\bot}$ for all $d \in \mathbb{D}$.
- Using induction on p, we have $(\mathcal{D}, d) \models^{a} \psi_{\alpha_{tt}.p}$ iff (there is a $\mathbb{R}^a$-transition (d, α, d') in $\mathbb{D}$ with $\{\!|\ p\ |\!\} \le d'$; all $\mathbb{R}^c$-transitions (d, α, d'') in $\mathbb{D}$ satisfy $\{\!|\ p\ |\!\} \le d''$; and there are no $\mathbb{R}^c$-transitions out of d in $\mathbb{D}$ for other events). This exactly captures $\{\!|\ \alpha_{tt}.p\ |\!\} \le d$.
- By induction on p, we have $(\mathcal{D}, d) \models^{a} \psi_{\alpha_{\bot}.p}$ iff (there are no $\mathbb{R}^c$-transitions out of d for events other than α, and all $\mathbb{R}^c$-transitions (d, α, d') satisfy $\{\!|\ p\ |\!\} \le d'$). But this captures $\{\!|\ \alpha_{\bot}.p\ |\!\} \le d$.
- Let $(\mathcal{D}, d) \models^{a} \psi_{p+q}$. Then $(\mathcal{D}, d) \models^{a} \bigwedge_{\alpha \in Act} \bigwedge_{p+q \longrightarrow^{\alpha}_{tt} r'} \langle \alpha \rangle \psi_{r'}$ and induction express that all $\mathbb{R}^a$-transitions out of $p+q$ to some r' can be answered by corresponding $(d, \alpha, d') \in \mathbb{R}^a$ with $\{\!|\ r\ |\!\}' \le d'$; whereas $(\mathcal{D}, d) \models^{a} \bigwedge_{\alpha \in Act} [\alpha] \big(\bigvee \{ \psi_{r'} \mid \exists v \in \{\bot, tt\} \colon p+q \longrightarrow^{\alpha}_{v} r' \} \big)$ states that all $(d, \alpha, d') \in \mathbb{R}^c$ can be answered in $(\{\!|\ p+q\ |\!\}, p+$

$$\phi_{\mathbf{0}} = \bigwedge_{\alpha \in Act} \neg\langle\alpha\rangle tt$$

$$\phi_{\perp} = tt$$

$$\phi_{\alpha_{tt}.p} = \langle\alpha\rangle\phi_p \wedge [\alpha]\phi_p \wedge \bigwedge_{\beta\neq\alpha} \neg\langle\beta\rangle tt$$

$$\phi_{\alpha_{\perp}.p} = [\alpha]\phi_p \wedge \bigwedge_{\beta\neq\alpha} \neg\langle\beta\rangle tt$$

$$\phi_{p+q} = \bigwedge\{\langle\alpha\rangle\phi_{r'} \mid \alpha \in Act,\ p+q \longrightarrow^{\alpha}_{tt} r'\}$$

$$\wedge \bigwedge_{\alpha\in Act} [\alpha](\bigvee_{v\in\{\perp,tt\}}\{\phi_{r'} \mid p+q \longrightarrow^{\alpha}_{v} r'\})$$

Figure 9: The characteristic formulas ϕ_p for terms p of the process algebra *MPA*.

q) by corresponding $\mathbb{R}^c$-transitions to some r' such that $r' \leq d'$ by induction. So $d \leq \{\!|\ p+q\ |\!\}$. □

This characterization is the key to proving that $\mathbb{D}$ is fully abstract and that refinement is characterized by the semantics for Hennessy-Milner logic.

Corollary 3.12 ([27])**.**

(1) *The order on $\mathbb{D}$ is the greatest refinement relation within $\mathcal{D}$.*
(2) *For all pointed modal transition systems (M,i) and (N,j) the following are equivalent:*
   (a) $(M,i) \prec (N,j)$
   (b) *for all ϕ of Hennessy-Milner logic,* $(M,i) \models^a \phi$ *implies* $(N,j) \models^a \phi$
   (c) *for all ϕ of Hennessy-Milner logic,* $(N,j) \models^c \phi$ *implies* $(M,i) \models^c \phi$.

Proof.

(1) That the order of $\mathbb{D}$ is a refinement follows directly from the definition of $\mathcal{D}$. For the converse, we show "$d \not\leq e$ implies that $(\mathcal{D}, e)$ does not refine $(\mathcal{D}, d)$:" First note that $\mathbf{K}(\mathbb{D})$ order-generates $\mathbb{D}$ so $d \not\leq e$ implies $k \leq d$ and $k \not\leq e$ for some $k \in \mathbf{K}(\mathbb{D})$. Then there is $p \in MPA$ with $k = \{\!|\ p\ |\!\}$ so that, by Lemma 3.11, for all $f \in \mathbb{D}$: $k \leq f$ iff $(\mathcal{D}, f) \models^a \phi_p$. Thus, $(\mathcal{D}, d) \models^a \phi_p$ and $(\mathcal{D}, e) \not\models^a \phi_p$ imply that e does not refine d in $\mathcal{D}$.
(2) Since $\models^a$ and $\models^c$ are dual with respect to negation, (b) and (c) are equivalent. The proof that (a) implies (b) is a straightforward structural induction on ϕ [26]. That (b) implies (a) follows from item (1), Lemma 3.11, and the fact that $\mathbb{D}$ is algebraic. □

We demonstrate that embeddings of pointed image-finite labelled transition systems are dense in $(\mathbb{X}, \tau_{\mathbb{X}})$, which we subsequently show to be the quotient space of all pointed

labelled transition systems with respect to bisimulation. The denseness argument rests on the fact that embeddings of implementations are maximal elements of $\mathbb{D}$.

Lemma 3.13. *Let $d \in \mathbb{D}$ be such that, for all ϕ of Hennessy-Milner logic, $(\mathcal{D}, d) \models^c \phi$ implies $(\mathcal{D}, d) \models^a \phi$. Then $d \in \max(\mathbb{D})$.*

Proof. Consider such a d and let $d \leq e$ in $\mathbb{D}$. Since $\leq$ is a partial order and since $\mathbb{D}$ is algebraic it suffices to show that $\mathop{\downarrow} e \cap \mathbf{K}(\mathbb{D}) \subseteq \mathop{\downarrow} d$. So let $\{\!|\, p \,|\!\} \in \mathbf{K}(\mathbb{D})$ with $\{\!|\, p \,|\!\} \leq e$. For ϕ_p of (3.9), $\{\!|\, p \,|\!\} \leq e$ implies $(\mathcal{D}, e) \models^a \phi_p$ which implies $(\mathcal{D}, e) \models^c \phi_p$ by Corollary 3.12 as $\mathbb{D}$ is fully abstract. But $d \leq e$ means $(\mathcal{D}, d) \prec (\mathcal{D}, e)$ as $\mathbb{D}$ is fully abstract, and so $(\mathcal{D}, d) \models^c \phi_p$ by Corollary 3.12 as $(\mathcal{D}, e) \models^c \phi_p$. By assumption on d, this renders $(\mathcal{D}, d) \models^a \phi_p$ and so $\{\!|\, p \,|\!\} \leq d$ by (3.9). □

Proposition 3.14. *The set of all embeddings of pointed image-finite labelled transition systems is dense in $(\mathbb{X}, \tau_{\mathbb{X}})$.*

Proof. As any pointed image-finite labelled transition system (L, l) is refinement-equivalent to $(\mathcal{D}, (\!|\, L, l \,|\!))$ [27], the embedding $(\!|\, L, l \,|\!)$ is in $\max(\mathbb{D}) = \mathbb{X}$ since it satisfies the assumptions of Lemma 3.13.

Let $O \in \tau_{\mathbb{X}}$ be non-empty, so $O = U \cap \max(\mathbb{D})$ for some $U \in \sigma_{\mathbb{D}}$ and there is some $k \in \mathbf{K}(\mathbb{D})$ with $M(k) \subseteq U \cap \max(\mathbb{D})$ since O is non-empty and $\mathbb{D}$ is algebraic. Let $q \in \mathit{MPA}$ be obtained by replacing all $\bot$ in p with $\mathbf{0}$ and, for all $\gamma \in \mathit{Act}$, all prefixes $\gamma_\bot.$ with γ_{tt}. Then $(\!|\, q \,|\!], q)$ refines $(\!|\, p \,|\!], p)$. Since $(\!|\, q \,|\!], q)$ is a pointed *labelled* transition system and $(\!|\, r \,|\!], r)$ is refinement-equivalent to $(\mathcal{D}, \{\!|\, r \,|\!\})$ for all $r \in \mathit{MPA}$ by Lemma 3.8, we conclude $\{\!|\, q \,|\!\} \in M(k) \subseteq O$ by Lemma 3.13 and $\{\!|\, q \,|\!\}$ is the embedding of a pointed image-finite labelled transition system. □

3.5. **Compactness of maximal-points space.** We show that $(\mathbb{X}, \tau_{\mathbb{X}})$ is compact by proving, indirectly, that $\max(\mathbb{D})$ is $\lambda_{\mathbb{D}}$-closed. Using results from [4] one could show that $\max(\mathbb{D})$ is $\lambda_{\mathbb{D}}$-closed by finding a subset T of $\mathbf{K}(\mathbb{D})$ that is a finitely branching tree and co-final in $\mathbf{K}(\mathbb{D})$. Given a candidate of such a T, the property that is difficult to ascertain is that any two elements of T that have an upper bound in $\mathbf{K}(\mathbb{D})$ are comparable. For example, consider the compact elements $\{\!|\, \alpha_{tt}.\bot + \beta_{tt}.\mathbf{0} \,|\!\}$ and $\{\!|\, \alpha_{tt}.\mathbf{0} + \beta_{tt}.\bot \,|\!\}$, both of which have the compact element $\{\!|\, \alpha_{tt}.\mathbf{0} + \beta_{tt}.\mathbf{0} \,|\!\}$ as an upper bound yet neither of them refines the other.

Faced with these difficulties, we therefore take a different route and realize $\max(\mathbb{D})$ as the set of those elements d of $\mathbb{D}$ that pass a set of judgments $(\mathcal{D}, d) \models^a \psi_p^{w,\alpha}$ where $\psi_p^{w,\alpha}$ are formulas of Hennessy-Milner logic.

Definition 3.15.

(1) Let $w = \delta_1 \delta_2 \dots \delta_n \in \mathit{Act}^*$, $\alpha \in \mathit{Act}$, and $p \in \mathit{MPA}$. Then we define the Hennessy-Milner logic formula

$$\psi_p^{w,\alpha} = [\delta_1][\delta_2] \dots [\delta_n](\langle\alpha\rangle\phi_p \vee \neg\langle\alpha\rangle\phi_p) \tag{3.10}$$

with ϕ_p as in Figure 9.

(2) Let Φ be the set of all Hennessy-Milner logic formulas $\psi_p^{w,\alpha}$ where $w \in \mathit{Act}^*$, $\alpha \in \mathit{Act}$, and $p \in \mathit{MPA}$.

(3) For ϕ of Hennessy-Milner logic and all $m \in \{a, c\}$ we define

$$[\!|\, \phi \,|\!]^m = \{d \in \mathbb{D} \mid (\mathcal{D}, d) \models^m \phi\}\,. \tag{3.11}$$

(4) Let $C_\Phi = \bigcap_{\phi\in\Phi} [\![\ \phi\ ]\!]^a$.

For each formula ϕ in Φ, the test $(\mathcal{D}, d)\models^a\phi$ checks whether there is a certain $\mathbb{R}^c$-reachable state from d with a certain outgoing may-transition that cannot be matched with a corresponding outgoing must-transition. Accordingly, C_Φ consists of those elements whose reachable states always find such a match. Intuitively, those should be the elements that represent labelled transition systems.

Example 3.16. The formulas in items (1) and (2) of Example 3.5 are in Φ as tt is $\phi_{\perp_\mathbb{D}}$, $\{\!|\ \perp\ |\!\} = \perp_\mathbb{D} \in \mathbf{K}(\mathbb{D})$, and $\epsilon \in Act^*$.

Rather than proving directly that $\max(\mathbb{D})$ is $\lambda_\mathbb{D}$-closed, we first establish that C_Φ is $\lambda_\mathbb{D}$-closed and then prove $\max(\mathbb{D}) = C_\Phi$. Whence maximal elements in $\mathbb{D}$ are exactly those elements whose reachable may-transitions have matching must-transitions. As C_Φ is the intersection of sets of the form $[\![\ \phi\ ]\!]^a$, we can show that the former is $\lambda_\mathbb{D}$-closed by proving that all latter sets are $\lambda_\mathbb{D}$-closed. We do this by structural induction on ϕ which requires a stronger induction hypothesis.

Lemma 3.17. *For each ϕ of Hennessy-Milner logic, the sets $[\![\ \phi\ ]\!]^a$ and $[\![\ \phi\ ]\!]^c$ are $\lambda_\mathbb{D}$-clopen. In particular, C_Φ is $\lambda_\mathbb{D}$-closed.*

Proof. We proceed with the first claim by structural induction on ϕ. This is evident for the clauses tt, negation, and conjunction since $[\![\ tt\ ]\!]^m = \mathbb{D}$ is $\lambda_\mathbb{D}$-clopen and clopens are closed under set complement ($[\![\ \neg\phi\ ]\!]^a = \mathbb{D}\setminus [\![\ \phi\ ]\!]^c$ and $[\![\ \neg\phi\ ]\!]^c = \mathbb{D}\setminus [\![\ \phi\ ]\!]^a$) and finite intersections. We still require proofs for $\langle\alpha\rangle\phi$, where for each $m \in \{a, c\}$ we have

$$[\![\ \langle\alpha\rangle\phi\ ]\!]^m = \{d \in \mathbb{D} \mid d^m_\alpha \cap [\![\ \phi\ ]\!]^m \neq \{\}\}\,. \tag{3.12}$$

- Let $m = a$. By Theorem 4.2 in [27], $[\![\ \psi\ ]\!]^a$ is $\sigma_\mathbb{D}$-open for all ψ of Hennessy-Milner logic, so $[\![\ \langle\alpha\rangle\phi\ ]\!]^a \in \sigma_\mathbb{D} \subseteq \lambda_\mathbb{D}$ and it suffices to show that $[\![\ \langle\alpha\rangle\phi\ ]\!]^a$ is $\lambda_\mathbb{D}$-closed, i.e. $\sigma_\mathbb{D}$-compact as an upper set. By induction, $[\![\ \phi\ ]\!]^a$ is $\lambda_\mathbb{D}$-clopen; it is also $\sigma_\mathbb{D}$-open so $[\![\ \phi\ ]\!]^a = \uparrow F_\phi$ for a finite subset $F_\phi \subseteq \mathbf{K}(\mathbb{D})$ as $\mathbb{D}$ is algebraic. By the definition of $[\![\ \langle\alpha\rangle\phi\ ]\!]^a$, we have $e \in [\![\ \langle\alpha\rangle\phi\ ]\!]^a$ iff $e^a_\alpha \cap \uparrow F_\phi \neq \{\}$ iff $e^a_\alpha \cap F_\phi \neq \{\}$ (as e^a_α is a lower set). For each $y \in F_\phi$ define $c(y) = (c(y)_\gamma)_{\gamma\in Act} \in \mathbb{D}$ by $c(y)_\beta = (\{\}, \mathbb{D})$ for all $\beta \neq \alpha$; and $c(y)_\alpha = (\downarrow y, \mathbb{D})$. Then $C = \{c(y) \mid y \in F_\phi\}$ is finite and $C \subseteq \mathbf{K}(\mathbb{D})$. Since $y \in c(y)^a_\alpha \cap F_\phi$ for all $y \in C$, we get $\uparrow C \subseteq [\![\ \langle\alpha\rangle\phi\ ]\!]^a$ as the latter set is upper. Note that for each $y \in F_\phi$ we have $c(y) \leq e$ in $\mathbb{D}$ iff $y \in e^a_\alpha$. Therefore, $e \in [\![\ \langle\alpha\rangle\phi\ ]\!]^a$ implies $e \in \uparrow C$. Thus, $[\![\ \langle\alpha\rangle\phi\ ]\!]^a$ equals $\uparrow C$ for the finite subset C of $\mathbf{K}(\mathbb{D})$.
- Let $m = c$. From Theorem 4.2 in [27] we already know that $[\![\ \langle\alpha\rangle\phi\ ]\!]^c$ is $\sigma_\mathbb{D}$-closed and therefore $\lambda_\mathbb{D}$-closed. Thus, it suffices to show that $[\![\ \langle\alpha\rangle\phi\ ]\!]^c$ is $\lambda_\mathbb{D}$-open. By induction, $[\![\ \phi\ ]\!]^c$ is $\lambda_\mathbb{D}$-open and therefore $D\setminus [\![\ \phi\ ]\!]^c = [\![\ \neg\phi\ ]\!]^a$ is $\lambda_\mathbb{D}$-closed (and $\sigma_\mathbb{D}$-open), i.e. $\sigma_\mathbb{D}$-compact upper. Since $\mathbb{D}$ is algebraic, $[\![\ \neg\phi\ ]\!]^a = \uparrow F_{\neg\phi}$ for a finite subset $F_{\neg\phi}$ of $\mathbf{K}(\mathbb{D})$. Thus, $[\![\ \phi\ ]\!]^c = \mathbb{D}\setminus\uparrow F_{\neg\phi}$. Inspecting the definition of $[\![\ \langle\alpha\rangle\phi\ ]\!]^c$, we infer $e \in [\![\ \langle\alpha\rangle\phi\ ]\!]^c$ iff there is some $x \in e^c_\alpha$ such that $x \notin \uparrow F_{\neg\phi}$. Now let $d \in [\![\ \langle\alpha\rangle\phi\ ]\!]^c$. We claim that there are compact elements k and l with $d \in \uparrow k \setminus \uparrow l \subseteq [\![\ \langle\alpha\rangle\phi\ ]\!]^c$, which concludes the proof since $\uparrow k \setminus \uparrow l$ is $\lambda_\mathbb{D}$-open. Choose any $k \in \downarrow d \cap \mathbf{K}(\mathbb{D})$. As for $l = (l_\gamma)_{\gamma\in Act}$, set $l_\beta = (\{\}, \mathbb{D})$ for all $\beta \neq \alpha$; and $l_\alpha = (\{\}, \uparrow F_{\neg\phi})$; in particular, $l \in \mathbf{K}(\mathbb{D})$. Note that $l \not\leq e$ in $\mathbb{D}$ iff $e^c_\alpha \not\subseteq \uparrow F_{\neg\phi}$ iff (for some $x \in e^c_\alpha$, $x \notin \uparrow F_{\neg\phi}$). Therefore, $d \in \uparrow k \setminus \uparrow l \subseteq [\![\ \langle\alpha\rangle\phi\ ]\!]^c$.

So C_Φ is $\lambda_\mathbb{D}$-closed as the intersection of $\lambda_\mathbb{D}$-closed sets. □

In [43] open sets are thought of as observable properties, so the denotations of Hennessy-Milner logic formulas in $\mathbb{D}$ (and in $\mathbb{X}$) are closed under negation as observations. If we extend these denotations to the modal mu-calculus [31], we expect observable properties to correspond to sets in the Borel algebra generated by $\sigma_{\mathbb{D}}$.

Using the denseness of embeddings of image-finite labelled transition systems in $\mathbb{X}$, we can prove the inclusion $\max(\mathbb{X}) \subseteq C_\Phi$.

Lemma 3.18. *The set* $\max(\mathbb{D})$ *is contained in* C_Φ.

Proof. Let A be the set of all embeddings $\langle\!|\, L, l \,|\!\rangle$ of pointed image-finite labelled transition systems (L, l). Then $A \subseteq C_\Phi$ follows as

- $(\mathcal{D}, \langle\!|\, L, l \,|\!\rangle)$ is refinement-equivalent to (L, l),
- $\alpha\langle\phi\rangle \vee \neg\alpha\langle\phi\rangle$ is valid over labelled transition systems for all ϕ of Hennessy-Milner logic,
- $[\delta_i]\phi$ is valid over labelled transition systems whenever ϕ is, and
- $\models^a$ is the standard semantics of Hennessy-Milner logic over labelled transition systems.

By Proposition 3.14, A is a dense subset of $(\mathbb{X}, \tau_{\mathbb{X}})$ and so its superset $C_\Phi \cap \max(\mathbb{D})$ is also dense in $(\mathbb{X}, \tau_{\mathbb{X}})$ and is $\tau_{\mathbb{X}}$-closed by the Lawson condition for $\mathbb{D}$ since C_Φ is $\lambda_{\mathbb{D}}$-closed by Lemma 3.17. But the only dense $\tau_{\mathbb{X}}$-closed subset of $(\mathbb{X}, \tau_{\mathbb{X}})$ is $\mathbb{X}$ itself and so $C_\Phi \cap \max(\mathbb{D}) = \max(\mathbb{D})$ follows which implies $\max(\mathbb{D}) \subseteq C_\Phi$. □

For a proof of the reverse inclusion $C_\Phi \subseteq \max(\mathbb{X})$ we need to clarify the structure of elements in C_Φ.

Lemma 3.19. *Let* $d \in C_\Phi$. *Then:*

1. *All* $d' \in \mathbb{D}$ *that are reachable from* d *in the labelled transition system* $(\mathbb{D}, \mathbb{R}^c)$ *are in* C_Φ *as well.*
2. *For all* $\alpha \in Act$ *we have* $d^c_\alpha = \uparrow\!(d^a_\alpha \cap d^c_\alpha)$.
3. *For all* ϕ *of Hennessy-Milner logic,* $(\mathcal{D}, d) \models^c \phi$ *implies* $(\mathcal{D}, d) \models^a \phi$.

Proof.

1. Let d' be reachable from d in $(\mathbb{D}, \mathbb{R}^c)$ and let $w' \in Act^*$ be the word obtained by travelling from d to d' on such a path. Given $\psi_p^{w,\alpha} \in \Phi$, the concatenation $w'w$ is in Act^* and so $\psi_p^{w'w,\alpha} \in \Phi$. Thus the path for w' above and $d \in C_\Phi$ ensure $(\mathcal{D}, d') \models^a \psi_p^{w,\alpha}$ and so $d' \in C_\Phi$.
2. Let $\alpha \in Act$. Since $\uparrow\!(d^a_\alpha \cap d^c_\alpha) \subseteq \uparrow\! d^c_\alpha = d^c_\alpha$, it suffices to show $d^c_\alpha \subseteq \uparrow\!(d^a_\alpha \cap d^c_\alpha)$. Proof by contradiction: Let $x \in d^c_\alpha \setminus \uparrow\!(d^a_\alpha \cap d^c_\alpha)$. Then $x \in d^c_\alpha$ and $d^a_\alpha \cap d^c_\alpha \subseteq \uparrow\!(d^a_\alpha \cap d^c_\alpha)$ imply $x \notin d^a_\alpha$ and so $x \in \mathbb{D} \setminus d^a_\alpha$. As $\mathbb{D}$ is algebraic and $\mathbb{D} \setminus d^a_\alpha \in \sigma_{\mathbb{D}}$, there is some $\{\!|\, p \,|\!\} \in \mathbf{K}(\mathbb{D})$ with $\{\!|\, p \,|\!\} \in \mathbb{D} \setminus d^a_\alpha$ and $\{\!|\, p \,|\!\} \leq x$ and so $\uparrow\!\{\!|\, p \,|\!\} \cap d^a_\alpha = \{\}$ as d^a_α is a lower set. But $d \in C_\Phi$ implies $(\mathcal{D}, d) \models^a \langle\alpha\rangle\phi_p \vee \neg\langle\alpha\rangle\phi_p$, as $\langle\alpha\rangle\phi_p \vee \neg\langle\alpha\rangle\phi_p$ is $\psi_p^{\epsilon,\alpha}$, and so $\uparrow\!\{\!|\, p \,|\!\} \cap d^a_\alpha = \{\}$ implies $\uparrow\!\{\!|\, p \,|\!\} \cap d^c_\alpha = \{\}$ by the definition of $[\![\, \langle\alpha\rangle\phi \,]\!]^m$ in (3.12), contradicting $x \in \uparrow\!\{\!|\, p \,|\!\} \cap d^c_\alpha$.
3. We use structural induction on ϕ. The cases for tt, negation, and conjunction are straightforward. Let $(\mathcal{D}, d) \models^c \langle\alpha\rangle\phi$, so $(\mathcal{D}, d') \models^c \phi$ for some $d' \in d^c_\alpha$. By item (2), there is some $d'' \in d^a_\alpha \cap d^c_\alpha$ with $d'' \leq d'$. But then $(\mathcal{D}, d') \models^c \phi$ and $d'' \leq d'$ imply $(\mathcal{D}, d'') \models^c \phi$ by Corollary 3.12. Since $d'' \in d^c_\alpha$ is reachable from d in $(\mathbb{D}, \mathbb{R}^c)$ it is in C_Φ by item (1). Thus, we can apply induction on d'' and get $(\mathcal{D}, d'') \models^a \phi$. Since $d'' \in d^a_\alpha$, this renders $(\mathcal{D}, d) \models^a \langle\alpha\rangle\phi$. □

We have now all the machinery at our disposal for stating and proving our main results in the next two theorems.

Theorem 3.20. *The set* $\max(\mathbb{D})$ *equals* C_Φ. *In particular,* $\max(\mathbb{D})$ *is* $\lambda_{\mathbb{D}}$*-closed and* $(\mathbb{X}, \tau_{\mathbb{X}})$ *is a Stone space in which the set of embeddings of pointed image-finite labelled transition systems is dense.*

Proof. From item (3) of Lemma 3.19 and Lemma 3.13 we infer $C_\Phi \subseteq \max(\mathbb{D})$. Lemma 3.18 then renders $\max(\mathbb{D}) = C_\Phi$. By Lemma 3.17, this means that $\max(\mathbb{D})$ is $\lambda_{\mathbb{D}}$-closed. By Propositions 3.2 and 3.14, it suffices to show that $(\mathbb{X}, \tau_{\mathbb{X}})$ is compact. Let $\mathbb{X} = \bigcup \mathcal{U}$ for $\mathcal{U} \subseteq \tau_{\mathbb{X}}$. By the definition of $\tau_{\mathbb{X}}$, each $U \in \mathcal{U}$ is of the form $V_U \cap \max(\mathbb{D})$ for some $V_U \in \sigma_{\mathbb{D}}$. Since $\mathbb{D}$ is a bifinite domain, $(\mathbb{D}, \lambda_{\mathbb{D}})$ is compact [2]. Since $\max(\mathbb{D})$ is $\lambda_{\mathbb{D}}$-closed it is $\lambda_{\mathbb{D}}$-compact as a $\lambda_{\mathbb{D}}$-closed subset of the compact space $(\mathbb{D}, \lambda_{\mathbb{D}})$. From $\mathbb{X} = \bigcup \mathcal{U}$ and $\sigma_{\mathbb{D}} \subseteq \lambda_{\mathbb{D}}$ we infer that $\max(\mathbb{D}) \subseteq \bigcup\{V_U \mid U \in \mathcal{U}\} \subseteq \lambda_{\mathbb{D}}$. The $\lambda_{\mathbb{D}}$-compactness of $\max(\mathbb{D})$ therefore implies the existence of a finite set $\mathcal{F} \subseteq \mathcal{U}$ with $\max(\mathbb{D}) \subseteq \bigcup\{V_U \mid U \in \mathcal{F}\}$. But then $\mathbb{X} \subseteq \bigcup \mathcal{F}$ follows. □

3.6. **Maximal-points space as quotient space of labelled transition systems.** Theorem 3.20 is of interest in its own right since $\max(D)$ is not λ_D-closed for bifinite domains D in general. But we also have to demonstrate that $\mathbb{X}$ is the desired quotient space of labelled transition systems modulo bisimulation.

Definition 3.21. Given a topological space (X, τ) let $\mathcal{C}[X, \tau]$ be the *poset of all* τ*-compact subsets of* X, ordered by reverse inclusion: $C \sqsubseteq C'$ iff $C' \subseteq C$.

Theorem 3.22.

(1) *The embedding* $(M, i) \mapsto \langle\!|\, M, i \,|\!\rangle$ *for pointed image-finite modal transition systems given in* [27] *extends to pointed modal transition systems such that labelled transition systems are embedded into* $\max(\mathbb{D})$.

(2) *Conversely, for any* $d \in \max(\mathbb{D})$ *the pointed mixed transition system* $(\mathcal{D}, d)$ *is refinement-equivalent to a labelled transition system. (It doesn't "type check" to ask whether* $(\mathcal{D}, d)$ *is* bisimilar *to a labelled transition system; but* $\downarrow$ *and* $\uparrow$ *are merely saturation artifacts of the model.)*

(3) *We have the isomorphism*

$$\mathbb{X} = \prod_{\alpha \in Act} \mathcal{C}[\mathbb{X}, \tau_{\mathbb{X}}] \tag{3.13}$$

of sets where $x = (x_\alpha)_{\alpha \in Act}$ *models the* α*-successors of* x *as the* $\tau_{\mathbb{X}}$*-compact set* x_α*, for each* $\alpha \in Act$.

Proof.

(1) Whenever a state s has infinitely many states $\{s_i \mid i \in I\}$ as α-successors for R^c, choose a finite subset F of I, retain transitions (s, α, s_i) and their must/may status for all $i \in F$, discard all (s, α, s_i) with $i \notin F$, and create a *may-stub* s_F ($\{\!|\, s_F \,|\!\} = \bot_{\mathbb{D}}$) and a may-transition (s, α, s_F). Doing this for all events while, at the same time, unfolding (M, i) as a tree ensures that all approximations are image-finite with limit $\langle\!|\, M, i \,|\!\rangle$ such that $(\mathcal{D}, \langle\!|\, M, i \,|\!\rangle)$ is refinement-equivalent to (M, i). In particular, $\langle\!|\, M, i \,|\!\rangle \in \max(\mathbb{D})$ by Lemma 3.13 whenever (M, i) is a labelled transition system.

(2) Let $d \in \max(\mathbb{D})$ and $\alpha \in Act$. The set $d^a_\alpha \cap d^c_\alpha$ is in C_Φ, which equals $\max(\mathbb{D})$, and $d^c_\alpha = \uparrow\!(d^a_\alpha \cap d^c_\alpha)$ by Lemma 3.19 and Theorem 3.20. Combining this with (2.2), we infer $d = ((\downarrow\!(d^a_\alpha \cap d^c_\alpha), d^a_\alpha \cap d^c_\alpha))_{\alpha \in Act}$. But since C_Φ is closed under states reachable in $(\mathbb{D}, \mathbb{R}^c)$, we may assume this representation for all elements e reachable from d in $(\mathbb{D}, \mathbb{R}^c)$. Therefore, $(\mathcal{D}, d)$ is refinement-equivalent to the modal transition system with no may-transitions that replaces $\downarrow\!(e^a_\alpha \cap e^c_\alpha)$ with $e^a_\alpha \cap e^c_\alpha$ for all $\alpha \in Act$ and all e reachable from d in $(\mathbb{D}, \mathbb{R}^c)$.

(3) The isomorphism follows from the equation for $\mathbb{D}$ and Lemmas 34.5 and 25 of [4]; the latter is stated for SFP^M-domains D, which are bifinite, but its proof only requires that $\max(D)$ is λ_D-closed. □

An immediate consequence of these two main theorems is that sets of implementations of modal transition systems are compact in the quotient space modulo bisimulation.

Corollary 3.23. *For each pointed modal transition system (M, s), its set of implementations is compact in the quotient space of labelled transition systems modulo bisimulation.*

Proof. The set of implementations of (M, s) in $\mathbb{X}$ is $M(\langle\!|\, M, s \,|\!\rangle) = \uparrow\!\langle\!|\, M, s \,|\!\rangle \cap \max(\mathbb{D})$ which is $\lambda_{\mathbb{D}}$-closed as the intersection of two $\lambda_{\mathbb{D}}$-closed sets and so it is $\tau_{\mathbb{X}}$-compact. □

4. Applications of compactness

We now discuss some of the consequences of the compactness of $\tau_{\mathbb{X}}$: a compactness theorem for Hennessy-Milner logic on compact sets of implementations, an abstract interpretation of compact sets of implementations as Scott-closed sets of modal transition systems, and a robust consistency measure for modal transition systems.

4.1. **A compactness theorem for sets of implementations.** Compactness of $(\mathbb{X}, \tau_{\mathbb{X}})$, stated in terms of Hennessy-Milner logic, is familiar from first-order logic but here secured without appeal to a complete proof system. Such semantic techniques for proving compactness are not new, we mention model-theoretic techniques based on ultra-filters. A compactness theorem for Hennessy-Milner logic alone already follows from its standard encoding in first-order logic. However, we prove a compactness result that goes beyond Hennessy-Milner logic as it applies to compact sets of labelled transition systems, in particular to the set of common implementations of finitely-many pointed modal transition systems. For a single such system, $(\mathcal{D}, \bot_{\mathbb{D}})$, we then regain the familiar compactness theorem for Hennessy-Milner logic. Our result is stronger than this familiar theorem as the sets of implementations of pointed modal transition systems are not expressible through Hennessy-Milner logic. In Theorem 4.8(2) below we see that these sets are expressible in Hennessy-Milner logic extended with greatest fixed points for finite-state modal transition systems.

Corollary 4.1.

(1) *Let Γ be a set of formulas of Hennessy-Milner logic and C a $\tau_{\mathbb{X}}$-compact set such that for all finite subsets Δ of Γ there is some $c_\Delta \in C$ that satisfies $\bigwedge \Delta$. Then there is some $c_\Gamma \in C$ that satisfies all formulas of Γ.*

(2) *In particular, let Γ be a set of formulas of Hennessy-Milner logic and $\{(M_i, s_i) \mid 1 \leq i \leq k\}$ a finite set of pointed modal transition systems such that for all finite subsets Δ of Γ there is a pointed labelled transition system that refines all (M_i, s_i) and satisfies $\bigwedge \Delta$. Then there is a pointed labelled transition system that refines all (M_i, s_i) and satisfies all formulas of Γ.*

Proof. By Corollary 3.23 it suffices to prove item (1). By duality of consistency (i.e. satisfiability) and validity, it suffices to prove the dual statement of item (1): assume that every $c \in C$ satisfies as least one $\phi \in \Gamma$ and show that there is a finite set $\Delta \subseteq \Gamma$ such that $\bigvee \Delta$ is valid over the set C. By this assumption, we have

$$C \subseteq \bigcup \mathcal{U} \tag{4.1}$$

where $\mathcal{U} = \{ [\![\phi]\!]^a \cap \max(\mathbb{D}) \mid \phi \in \Gamma \}$ is a subset of $\tau_{\mathbb{X}}$ as all $[\![\phi]\!]^a$ are in $\sigma_{\mathbb{D}}$ by Theorem 4.2 in [27]. As C is $\tau_{\mathbb{X}}$-compact, there is a finite $\mathcal{F} \subseteq \mathcal{U}$ with $C \subseteq \bigcup \mathcal{F}$, i.e. $C \subseteq \bigcup_{\phi \in \Delta} [\![\phi]\!]^a = [\![\bigvee \Delta]\!]^a$ for a finite set $\Delta \subseteq \Gamma$. Thus all $c \in C$ satisfy $\bigvee \Delta$. □

Example 4.2. Figure 10 depicts schematically the set of common implementations of two pointed modal transition systems $(\mathcal{D}, d)$ and $(\mathcal{D}, e)$, the intersection of the implementations of d and e. This is a compact subset of $\mathbb{X}$ and so we get a compactness theorem for Hennessy-Milner logic on that set.

4.2. **Abstract interpretation of $\tau_{\mathbb{X}}$-compact sets of implementations.** Cousot & Cousot's abstract interpretation framework [8] approximates concrete objects and their transformations by abstract objects and transformations such that reasoning on abstract objects is sound for their concretizations. In a simple setting, one has given a set C of concrete objects (e.g. computer programs) and a partial order $(A, \leq)$ of abstract objects, a monotone abstraction function $\alpha\colon (\mathbb{P}(C), \subseteq) \to (A, \leq)$, and a monotone concretization function $\gamma\colon (A, \leq) \to (\mathbb{P}(C), \subseteq)$. The value $a = \alpha(X)$ should represent the best approximation of $X \subseteq C$ within the partial order $(A, \leq)$ and $\gamma(a)$ should represent the set of those concrete objects that are abstracted by a. One can encode these intuitions by making α and γ a Galois connection [8], a notion we define below.

Example 4.3. Let C be the set of natural numbers and $A = \{\top, O, E\}$ where $\top$ is the top element and O and E are incomparable. Define $\alpha(X)$ to be O if all elements of X are odd; E if all elements of X are even; and $\top$ otherwise. Then $\alpha(\{2, 46, 128\}) = O$ and $\alpha(\{2, 4, 7\}) = \top$ etc. Define $\gamma(E) = \{0, 2, 4, \dots\}$, $\gamma(O) = \{1, 3, 5, \dots\}$, and $\gamma(\top) = C$. Then $\alpha(\{2, 46, 128\}) = O$ says that O is the least element that soundly represents the set $\{2, 46, 128\}$. The equation $\gamma(\alpha(\{2, 46, 128\})) = \{0, 2, 4, \dots\}$ shows that the abstract value of $\{2, 46, 128\}$ has a larger set of concrete objects.

We want to apply this framework in our setting. From the compactness of $\tau_{\mathbb{X}}$ Corollary 3.23 infers that the set $M(\langle\!| M, s |\!\rangle)$ is $\tau_{\mathbb{X}}$-compact for all pointed modal transition systems (M, s). Said $\tau_{\mathbb{X}}$-compact set comprises all the implementations of (M, i). Conversely, a $\tau_{\mathbb{X}}$-compact set C of labelled transition system can be approximated by any pointed modal transition system (M, s) satisfying $C \subseteq M(\langle\!| M, s |\!\rangle)$. Ideally, one wants an *optimal* such (M, s), one for which the difference $M(\langle\!| M, s |\!\rangle) \setminus C$ is minimal. Of course, this optimality is ensured for any C of the form $M(\langle\!| M, s |\!\rangle)$. The next example shows that there is no optimal (M, s) in general.

Example 4.4. Consider two pointed modal transition trees (M_1, s_1) and (M_2, s_2) that have a common refinement but do not refine each other. In general, there will be more than one minimal upper bound of the set $\{\langle\!| M_1, s_1 |\!\rangle, \langle\!| M_2, s_2 |\!\rangle\}$ in $\mathbb{D}$ so there cannot be a $d \in \mathbb{D}$ such that $M(d)$ equals the $\tau_{\mathbb{X}}$-compact set $M(\langle\!| M_1, s_1 |\!\rangle) \cap M(\langle\!| M_2, s_2 |\!\rangle)$.

The fact that modal transition systems cannot be such optimal abstractions of $\tau_{\mathbb{X}}$-compact sets seems to be related to the incompleteness of modal transition systems for

abstraction-based model checking [10] since $\mathbb{D}$ is not bounded complete. But there is a Galois connection between $\tau_{\mathbb{X}}$-compact subsets of $\mathbb{X}$ and $\sigma_{\mathbb{D}}$-closed subsets of $\mathbb{D}$. For a $\tau_{\mathbb{X}}$-compact set C its set of concretizations is the Scott-closed set of all (M, s) for which $C \subseteq M(\langle\!| M, s |\!\rangle)$. Conversely, a Scott-closed subset L of pointed modal transition systems is abstracted as the set of those pointed labelled transition systems that implement all elements of L.

Definition 4.5.

(1) Let $\mathcal{L}[\mathbb{D}] = \{L \mid L \ \sigma_{\mathbb{D}}\text{-closed}\}$ be the set of $\sigma_{\mathbb{D}}$-closed subsets of $\mathbb{D}$, ordered by set inclusion: L is less than or equal to L' iff $L \subseteq L'$.

(2) Let L_1 and L_2 be complete lattices. A *Galois connection* [17] is a pair of monotone maps $\alpha\colon L_1 \to L_2$ and $\gamma\colon L_2 \to L_1$ such that for all $x \in L_1$ we have $\gamma(\alpha(x)) \geq x$ and for all $y \in L_2$ we have $\alpha(\gamma(y)) \leq y$. In that case, α is the *upper adjoint* of γ.

Theorem 4.6. *The maps $\gamma\colon \mathcal{C}[\mathbb{X}, \tau_{\mathbb{X}}] \to \mathcal{L}[\mathbb{D}]$ and $\alpha\colon \mathcal{L}[\mathbb{D}] \to \mathcal{C}[\mathbb{X}, \tau_{\mathbb{X}}]$ defined by*

$$\begin{aligned} \gamma(C) &= \{d \in \mathbb{D} \mid C \subseteq M(d)\} \\ \alpha(L) &= \bigcap_{d \in L} M(d) \end{aligned} \tag{4.2}$$

form a Galois connection, where α is the upper adjoint of γ.

Proof.

- The map γ is well defined. First $d \leq e$ implies $M(e) \subseteq M(d)$ and so $\gamma(C)$ is a lower set. Second let $(d_i)_{i \in I}$ be directed in $\gamma(C)$. Then $C \subseteq \bigcap_{i \in I} M(d_i)$ and the latter equals $M(\bigvee_{i \in I} d_i)$, so $\gamma(C)$ is $\sigma_{\mathbb{D}}$-closed.
- The map α is well defined. For if L is empty, then $\alpha(L) = \mathbb{X}$ is $\tau_{\mathbb{X}}$-compact; and if L is non-empty, $\alpha(L)$ is the intersection of $\lambda_{\mathbb{D}}$-closed elements and so $\lambda_{\mathbb{D}}$-closed whence $\tau_{\mathbb{X}}$-compact.
- The map γ is monotone. Let $C \sqsubseteq C'$, i.e. $C' \subseteq C$. Then $d \in \gamma(C)$ means $C \subseteq M(d)$ and so $C' \subseteq M(d)$ follows. Therefore $d \in \gamma(C')$ and so $\gamma(C) \subseteq \gamma(C')$.
- The map α is monotone. Let $L \subseteq L'$. Then $\alpha(L') = \bigcap_{d \in L'} M(d) \subseteq \bigcap_{d \in L} M(d) = \alpha(L)$ and so $\alpha(L) \sqsubseteq \alpha(L')$.
- To see $\gamma \circ \alpha \geq \mathrm{id}_{\mathcal{L}[\mathbb{D}]}$ let $L \in \mathcal{L}[\mathbb{D}]$. Then $\gamma(\alpha(L)) = \{e \in \mathbb{D} \mid \alpha(L) \subseteq M(e)\} = \{e \in \mathbb{D} \mid \bigcap_{d \in L} M(d) \subseteq M(e)\}$ clearly contains L.
- To see $\alpha \circ \gamma \leq \mathrm{id}_{\mathcal{C}[\mathbb{X}, \tau_{\mathbb{X}}]}$ let $C \in \mathcal{C}[\mathbb{X}, \tau_{\mathbb{X}}]$. Then $\alpha(\gamma(C)) = \alpha(\{d \in \mathbb{D} \mid C \subseteq M(d)\}) = \bigcap\{M(d) \mid C \subseteq M(d)\}$ obviously contains C. □

Theorem 4.6 remains to be valid if we reverse the orders on the domains $\mathcal{C}[\mathbb{X}, \tau_{\mathbb{X}}]$ and $\mathcal{L}[\mathbb{D}]$ and swap the names α and β throughout the theorem and its proof. In that case, a $\tau_{\mathbb{X}}$-compact set C is abstracted by a set L of pointed modal transition systems and any such L has a set of pointed labelled transition systems as concretizations. This view is perhaps more natural.

4.3. **Consistency measure for modal transition systems.** We explicitly state the metrics $d_{\mathbb{D}}$ for pointed modal transition systems and $d_{\mathbb{X}}$ for pointed labelled transition systems. The latter is then used to define a consistency measure on modal transition systems as an alternative to the metric $d_{\mathbb{D}}$. Fix an enumeration $p_0, p_1, \ldots$ of *MPA* and set

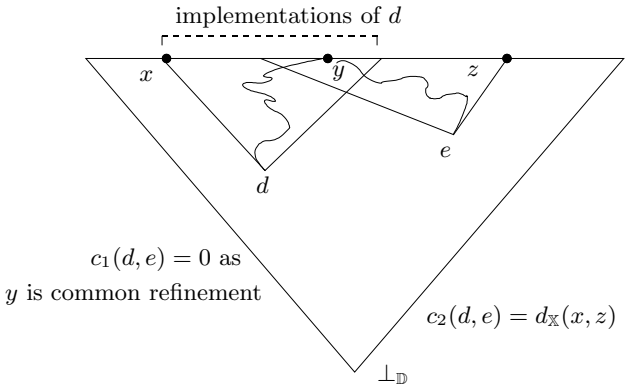

Figure 10: Two pointed modal transition systems $(\mathcal{D}, d)$ and $(\mathcal{D}, e)$ that have a common refinement.

$$\begin{aligned} d_{\mathbb{D}}(d,e) &= \mathit{inf}\{2^{-n} \mid \forall i \leq n\colon \{\!|\ p_i\ |\!\} \leq d \text{ iff } \{\!|\ p_i\ |\!\} \leq e\} \\ d_{\mathbb{X}}(x,y) &= \mathit{inf}\{2^{-n} \mid \forall i \leq n\colon \{\!|\ p_i\ |\!\} \leq x \text{ iff } \{\!|\ p_i\ |\!\} \leq y\}\,. \end{aligned}$$

Then the topology determined by $d_{\mathbb{D}}$ and $d_{\mathbb{X}}$ is $\lambda_{\mathbb{D}}$ and $\tau_{\mathbb{X}}$, respectively. For practical purposes we wish to enumerate $p \in \mathit{MPA}$ in increasing modal depth of ϕ_p in (3.9), corresponding to the iterative unfolding of the functional for bisimulation [35]. In that case, $d_{\mathbb{X}}$ is essentially the metric in [12]. These metrics are standard and well understood but result in consistency measures if lifted to compact sets of implementations.

We define the *consistency measure* $c = \lambda(d,e) \cdot [c_1(d,e), c_2(d,e)]\colon \mathbb{D} \times \mathbb{D} \to \mathbb{I}$ by

$$\begin{aligned} c_1(d,e) &= \mathit{inf}\{d_{\mathbb{X}}(x,y) \mid x \in M(d),\ y \in M(e)\} \\ c_2(d,e) &= \mathit{sup}\,\{d_{\mathbb{X}}(x,y) \mid x \in M(d),\ y \in M(e)\} \end{aligned}$$

and use this as an alternative to the metric $d_{\mathbb{D}}$ for comparing the pointed modal transition systems $(\mathcal{D}, d)$ and $(\mathcal{D}, e)$. Note that c_1 and c_2 are optimistic and pessimistic measures (respectively) from the point of view of an implementor.

Example 4.7. Figure 10 shows a scenario where two pointed modal transition systems $(\mathcal{D}, d)$ and $(\mathcal{D}, e)$ have a common refinement, and so $c_1(d,e) = 0$.

Since $M(f)$ is $\tau_{\mathbb{X}}$-compact for all $f \in \mathbb{D}$ by Corollary 3.23, $c_1(d,e)$ and $c_2(d,e)$ are the metric analogue of symmetric $\forall\forall$ and $\exists\exists$ lifts of relations from elements to subsets, here of $d_{\mathbb{X}}$ to $\tau_{\mathbb{X}}$-compact subsets, respectively. The standard metric $c(d,e)$ between compact subsets $M(d)$ and $M(e)$, the Hausdorff distance, is the symmetric $\exists\forall$-lift of $d_{\mathbb{X}}$ to $\tau_{\mathbb{X}}$-compact subsets and so

$$c_1(d,e) \leq c(d,e) \leq c_2(d,e)\,. \tag{4.3}$$

Such consistency measures are of particular interest if d and e represent different viewpoints [38, 30, 42] of the same system such that the degree of consistency between these descriptions needs to be explored.

We prove that c_1 is a robust measure in that its kernel consists of those pairs of pointed modal transition systems that have a common refinement.

Theorem 4.8.

(1) *For all $d, e \in \mathbb{D}$, we have $c_1(d,e) = 0$ iff $(\mathcal{D}, d)$ and $(\mathcal{D}, e)$ have a common refinement.*
(2) *Deciding whether two finite-state modal transition systems have a common refinement is reducible to checking the satisfiability of a modal mu-calculus formula with greatest fixed points only.*

Proof.

(1) We use Theorems 3.20 and 3.22 repeatedly. If $(\mathcal{D}, d)$ and $(\mathcal{D}, e)$ have a common refinement, there is some $m \in M(d) \cap M(e)$ and so $c_1(d,e) = 0$ as $d_{\mathbb{X}}(m,m) = 0$. Conversely, let $c_1(d,e) = 0$. Then for each $n \geq 0$ there are $m^d_n \in M(d)$ and $m^e_n \in M(e)$ with $d_{\mathbb{X}}(m^d_n, m^e_n) < 1/n$. Since $(\mathbb{X}, \tau_{\mathbb{X}})$ is compact, there is a convergent subsequence $(m^d_{n_j})_{j\geq 0}$ of $(m^d_n)_{n\geq 0}$ with limit m^d and so $m^d \in M(d)$ as the latter is $\tau_{\mathbb{X}}$-closed. Since $d_{\mathbb{X}}(m^d_{n_j}, m^e_{n_j}) < 1/n_j$ for each $j \geq 0$, this implies $inf\{d_{\mathbb{X}}(m^d, m^e_{n_j}) \mid j \geq 0\} = 0$ and so m^d is in all $\tau_{\mathbb{X}}$-closed sets that contain $\{m^e_{n_j} \mid j \geq 0\}$. Therefore, m^d is in $M(e)$ and so $(\mathcal{D}, m^d)$ is a common refinement of $(\mathcal{D}, d)$ and $(\mathcal{D}, e)$.
(2) If (M, i) and (N, j) are finite-state, we show that there are formulas $X_{(M,i)}$ and $X_{(N,j)}$ of the modal mu-calculus with greatest fixed points only such that the modal mu-calculus formula $X_{(M,i)} \wedge X_{(N,j)}$ is satisfiable over labelled transition systems iff (M, i) and (N, j) have a common refinement. Larsen & Thomsen implicitly define these formulas in the system of recursive equations (3) of [32] where, for each state s in $M = (\Sigma, R^a, R^c)$,

$$X_{(M,s)} = (\bigwedge_{(s,\alpha,s')\in R^a} \langle\alpha\rangle X_{(M,s')}) \wedge (\bigwedge_{\alpha\in Act} [\alpha](\bigvee_{(s,\alpha,s')\in R^c} X_{(M,s')})) \tag{4.4}$$

as a greatest fixed point. If s has finitely many reachable states in M, then $X_{(M,s)}$ is expressible in the modal mu-calculus, using a "calling context" on the set of states t that are R^c-reachable from s and static scoping of the greatest fixed-point operators $\nu Z_t.\phi$. Now for all pointed labelled transition systems (L, l) we have $(L, l) \models^a X_{(M,s)}$ iff $(M, s) \prec (L, l)$ where we can use the proof of (3) in [32] which works in our setting as conjunctions and disjunctions need not be finite. □

Example 4.9. Let M be the modal transition system from Figure 1. We write $X_{(M,\mathrm{Drinks})}$ as a formula of the modal mu-calculus with greatest fixed points only. Let

$$\begin{aligned}
X_{(M,\mathrm{Dr})} &= \nu Z_{\mathrm{Dr}}.[\mathrm{drinks}]Z_{\mathrm{Dr}} \wedge [\mathrm{talks}]X^{\mathrm{Dr}}_{(M,\mathrm{Ta})} \wedge [\mathrm{orders}]X^{\mathrm{Dr}}_{(M,\mathrm{Wa})} \qquad (4.5)\\
X^{\mathrm{Dr}}_{(M,\mathrm{Ta})} &= \nu Z_{\mathrm{Ta}}.[\mathrm{drinks}]Z_{\mathrm{Dr}} \wedge [\mathrm{orders}]X^{\mathrm{Dr\,Ta}}_{(M,\mathrm{Wa})}\\
X^{\mathrm{Dr}}_{(M,\mathrm{Wa})} &= \nu Z_{\mathrm{Wa}}.\langle\mathrm{newPint}\rangle Z_{\mathrm{Dr}} \wedge \langle\mathrm{newPint}\rangle X^{\mathrm{Dr}}_{(M,\mathrm{Ta})} \wedge [\mathrm{newPint}](Z_{\mathrm{Dr}} \vee X^{\mathrm{Dr\,Wa}}_{(M,\mathrm{Ta})})\\
X^{\mathrm{Dr\,Wa}}_{(M,\mathrm{Ta})} &= \nu Z_{\mathrm{Ta}}.[\mathrm{drinks}]Z_{\mathrm{Dr}} \wedge [\mathrm{orders}]Z_{\mathrm{Wa}}\\
X^{\mathrm{Dr\,Ta}}_{(M,\mathrm{Wa})} &= \nu Z_{\mathrm{Wa}}.\langle\mathrm{newPint}\rangle Z_{\mathrm{Dr}} \wedge \langle\mathrm{newPint}\rangle Z_{\mathrm{Ta}} \wedge [\mathrm{newPint}](Z_{\mathrm{Dr}} \vee Z_{\mathrm{Ta}})
\end{aligned}$$

where the superscripts in $X_{(M,s)}$ record the "calling context" of the recursions.

So $c_1(d, e)$ measures the *degree of inconsistency* of $(\mathcal{D}, d)$ and $(\mathcal{D}, e)$, a lower bound on the difference between their implementations, $c_2(d, e)$ is an upper bound on such a difference, and none of them is a metric: From item (4) of Definition 3.1, c_1 satisfies only (b) and c_2 satisfies only (b) and (c). The reducibility of common refinement checks to satisfiability checks in the modal mu-calculus yields EXPTIME as a weak upper bound on its complexity. Since the formulas are defined in terms of greatest fixed points only, one can indeed show a stronger result: the decision problem of common refinements is in PTIME [25].

4.4. **Scope of these results.** Our results also apply to 3-valued model checking frameworks in which system observables are state propositions or a combination of state propositions and events. This is so since Godefroid & Jagadeesan's translation between modal transition systems (events only), partial Kripke structures [5] (state propositions only), and Kripke modal transition systems [26] (events and state propositions) and their translations of the respective temporal logic formulas is shown to preserve and reflect refinement and the meaning of model checks [20].

5. Related work

Bakker & Zucker use domain equations and metric completions for a metric and denotational treatment of concurrency in [12].

Lawson proposes the notion of a maximal-point space to represent classical topological spaces as maximal points of a domain in the topology induced by the domain's Lawson- and Scott-topology [34].

Abramsky [1] provides a fully abstract domain of synchronization trees for *partial* bisimulation between labelled transition systems that have a divergence predicate. The domain equation of loc. cit. uses a sum construction on the convex powerdomain. Maximal points are not part of that paper's agenda and are therefore not discussed therein. Labelled transition systems with a divergence predicate and partial bisimulation are recognized as certain modal transition systems and their refinement in [26].

Mislove et al. present a fully abstract domain model, which combines the probabilistic power domain with a convex variant of the Plotkin powerdomain, for finite-state processes with non-deterministic and probabilistic choice [36].

Alessi et al. [4] introduce a category of SFP^M-domains with a compositional maximal-points space functor to Stone spaces. They show that all bifinite domains D for which $\max(D)$ is a Stone space are Scott-continuous retracts of SFP^M-domains. In particular, $\mathbb{D}$ is such a retract by Theorem 3.20. We suspect that $\mathbb{D}$ is not an SFP^M-domain since $\mathcal{M}[D_1]$ is not an SFP^M-domain for the SFP^M-domain $D_1 = \{\bot < ff, tt\}$ [3], although $\mathcal{M}[D_1]$ is the second iteration of the domain equation (2.4) for $\mathbb{D}$ when $Act = \{\alpha\}$.

The paper [27] presents the domain $\mathbb{D}$ and its modal transition system $\mathcal{D}$, both denoted as $\mathcal{D}$ in loc. cit., and proves full abstraction and a characterization of $\mathbb{D}$'s compact elements in terms of formulas of Hennessy-Milner logic.

In [28] it is shown that the co-inductive refinement of modal transition systems has an extensional description: a pointed modal transition system (M, i) refines a pointed modal transition system (N, j) if, and only if, the set of implementations of (M, i) is a subset of the implementations of (N, j).

Dams & Namjoshi [10] show that finite-state modal transition systems are incomplete as abstractions of infinite-state modal transition systems for modal mu-calculus checking. They propose focused transition systems as a generalization of modal transition systems,

show completeness for this class of models, and define a game semantics for refinement of focused transition systems and a game semantics for model checks of alternating tree automata on focused transition systems. It is straightforward to write down a domain equation for focused transition systems but a programme of maximal-points spaces won't directly render pointed Kripke structures since, as noted in [10], focused transition systems can have maximal refinements that have inconsistent constraints on propositions at states.

In [25] consistency, satisfiability, and validity problems are studied for collectively model checking a set of views endowed with labelled transitions, hybrid constraints on states, and atomic propositions. A PTIME algorithm for deciding whether a set of views has a common refinement (consistency) is given. It is proved that deciding whether a common refinement satisfies a formula of the hybrid mu-calculus [40] (satisfiability), and its dual (validity), are EXPTIME-complete. Two generically generated "summary" views are defined that constitute informative and consistent common refinements and abstractions of a set of views (respectively).

Di Pierro et al. [15] develop a quantitative notion of process equivalence as the basis for an approximative version of non-interference and precise quantifications of information leakage. They present two semantics-based analyzes for approximative non-interference where one soundly abstracts the other.

Desharnais et al. [13] show that each continuous-state labelled Markov process has a sequence of finite acyclic labelled Markov processes as abstractions which is precise for a probabilistic modal logic; an equivalence between the category of Markov processes and simulation morphisms and a recursively defined domain, viewed as a category, is given.

Desharnais et al. [14] define a pseudo metric between labelled concurrent Markov chains where zero distance means weak bisimilarity. The metric is characterized in a real-valued modal logic and shown to allow for compositional quantitative reasoning.

6. Conclusions

We presented the fully abstract and universal domain model $\mathbb{D}$ for pointed modal transition systems and refinement of [27]. Using techniques from concurrency theory and topology, we demonstrated that $\mathbb{D}$ is the right fully abstract and universal model for labelled transition systems and bisimulation since the quotient space of all pointed labelled transition systems with respect to bisimulation, $(\mathbb{X}, \tau_{\mathbb{X}})$, is obtained as the maximal-points space of $\mathbb{D}$. We furthermore revealed the fine-structure of $\mathbb{X}$, notably we proved that its topology $\tau_{\mathbb{X}}$ inherited from the Scott- and Lawson-topology of $\mathbb{D}$ is compact, zero-dimensional, and Hausdorff (a Stone space). In particular, $\tau_{\mathbb{X}}$ is determined by a computationally meaningful, complete ultra-metric $d_{\mathbb{X}}$ for which image-finite labelled transition systems approximate labelled transition systems to any degree of precision. Modulo refinement, $(\mathcal{D}, k)$ is image-finite for all $k \in \mathbf{K}(\mathbb{D})$, so this denseness also applies to modal transition systems for the Lawson-topology and its metric $d_{\mathbb{D}}$. Thus our results unify denotational, operational, and metric semantics of labelled and modal transition systems. We finally derived consequences of this compact representation: a compactness theorem for Hennessy-Milner logic on compact sets of implementations, an abstract interpretation of compact sets of implementations as Scott-closed sets of modal transition systems, and a robust consistency measure for modal transition systems.

Acknowledgment

Radha Jagadeesan suggested working with the mixed powerdomain in [27]. Glenn Bruns, Alessandra Di Pierro, Patrice Godefroid, Dimitar Guelev, Chris Hankin, Radha Jagadeesan, Achim Jung, Ralph Kopperman, David Schmidt, and Herbert Wiklicky are thanked for helpful comments and discussions. This paper is an extended journal version of [29] and reflects the thorough and thoughtful comments made by the anonymous referees of the LICS 2004 conference and the journal Logical Methods in Computer Science.

References

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

[2] S. Abramsky and A. Jung. Domain theory. In S. Abramsky, D. M. Gabbay, and T. S. E. Maibaum, editors, *Handbook of Logic in Computer Science*, volume 3, pages 1–168. Oxford Univ. Press, 1994.

[3] F. Alessi, P. Baldan, and F. Honsell. Partializing Stone spaces using SFP domains. In M. Bidoit and M. Dauchet, editors, *TAPSOFT'97 Conference Proceedings*, volume 1214 of *Lecture Notes in Computer Science*, pages 478–489, Lille, France, 14-18 April 1997. Springer Verlag.

[4] F. Alessi, P. Baldan, and F. Honsell. A Category of Compositional Domain-Models for Separable Stone Spaces. *Theoretical Computer Science*, 290(1):599–635, January 2003.

[5] G. Bruns and P. Godefroid. Model Checking Partial State Spaces with 3-Valued Temporal Logics. In *Proc. of the 11th International Conference on Computer Aided Verification*, volume 1633 of *Lecture Notes in Computer Science*, pages 274–287. Springer Verlag, July 1999.

[6] G. Bruns and P. Godefroid. Generalized Model Checking: Reasoning about Partial State Spaces. In *Proc. of the 11th International Conference on Concurrency Theory*, volume 1877 of *Lecture Notes in Computer Science*, pages 168–182. Springer Verlag, August 2000.

[7] B. Courcelle and M. Nivat. Algebraic families of interpretations. In *Proc. of the 17th IEEE Symposium on Foundations of Computer Science*, pages 137–146, October 1976.

[8] P. Cousot and R. Cousot. Abstract interpretation: a unified lattice model for static analysis of programs. In *Proc. of the 4th ACM Symposium on Principles of Programming Languages*, pages 238–252, Los Angeles, California. ACM Press, 1977.

[9] D. Dams. *Abstract interpretation and partition refinement for model checking*. PhD thesis, Technische Universiteit Eindhoven, The Netherlands, 1996.

[10] D. Dams and K. Namjoshi. The Existence of Finite Abstractions for Branching Time Model Checking. In *Proc. of the Nineteenth Annual IEEE Symposium on Logic in Computer Science*, pages 335–344, 13-17 July, Turku, Finland. IEEE Computer Society Press, 2004.

[11] D. Dams, R. Gerth, and O. Grumberg. Abstract interpretation of reactive systems. *ACM TOPLAS*, 19:253–291, 1997.

[12] J. W. de Bakker and J. I. Zucker. Denotational Semantics Of Concurrency. In *Proc. 14th Annual ACM Symposium on Theory of Computing*, pages 153–158, New York, New York, 1982. ACM Press.

[13] J. Desharnais, V. Gupta, R. Jagadeesan, and P. Panangaden. Approximating Labeled Markov Processes. In *Proc. of the 15th Annual IEEE Symposium on Logic in Computer Science*, pages 95–106, Santa Barbara, California, 26-29 June 2000. IEEE Computer Society Press.

[14] J. Desharnais, V. Gupta, R. Jagadeesan, and P. Panangaden. The Metric Analogue of Weak Bisimulation for Probabilistic Processes. In *Proc. of the 17th Annual IEEE Symposium on Logic in Computer Science*, pages 413–422, Copenhagen, Denmark, July 2002. IEEE Computer Society.

[15] A. Di Pierro, C. Hankin, and H. Wiklicky. Approximate Non-Interference. *Journal of Computer Security*, 12(1):37–82, 2004.

[16] D. C. Gause and G. M. Weinberg. *Exploring Requirements: Quality Before Design*. Dorset House Publishing, 353 West 12th Street, New York, NY 10014, 1989.

[17] G. Gierz, K. H. Hofmann, K. Keimel, J. D. Lawson, M. Mislove, and D. S. Scott. A Compendium of Continuous Lattices. Springer Verlag, 1980.

[18] P. Godefroid, M. Huth, and R. Jagadeesan. Abstraction-based Model Checking using Modal Transition Systems. In *Proc. of the 12th International Conference on Theory and Practice of Concurrency*, volume 2154 of *Lecture Notes in Computer Science*, pages 426–440. Springer Verlag, August 2001.

[19] P. Godefroid and R. Jagadeesan. Automatic Abstraction Using Generalized Model Checking. In E. Brinksma and K. G. Larsen, editors, *Proc. of the 14th International Conference on Computer Aided Verification*, volume 2404 of *Lecture Notes in Computer Science*, pages 137–150, Copenhagen, Denmark, July 2002. Springer Verlag.

[20] P. Godefroid and R. Jagadeesan. On The Expressiveness of 3-Valued Models. In L. D. Zuck, P. C. Attie, A. Cortesi, and S. Mukhopadhyay, editors, *Proc. of the 4th International Conference on Verification, Model Checking and Abstract Interpretation*, volume 2575 of *LNCS*, pages 206–222, New York, January 2003. Springer Verlag.

[21] J. A. Goguen, J. W. Thatcher, E. G. Wagner, and J. B. Wright. Initial algebra semantics and continuous algebras. *Journal of the ACM*, 24(1):44–67, 1977.

[22] C. Gunter. The mixed power domain. *Theoretical Computer Science*, 103:311–334, 1992.

[23] R. Heckmann. Set Domains. In *Proc. of the 3rd European Symposium on Programming*, volume 432 of *Lecture Notes in Computer Science*, pages 177–196. Springer Verlag, 1990.

[24] M. Hennessy and R. Milner. Algebraic laws for nondeterminism and concurrency. *Journal of the ACM*, 32(1):137–161, January 1985.

[25] A. Hussain and M. Huth. On model checking multiple hybrid views. *Preliminary Proc. of the First International Symposium on Leveraging Applications of Formal Method*, 15 pages, 30 October - 2 November, Paphos, Cyprus, 2004.

[26] M. Huth, R. Jagadeesan, and D. A. Schmidt. Modal transition systems: a foundation for three-valued program analysis. In D. Sands, editor, *Proc. of ESOP'2001*, pages 155–169. Springer Verlag, April 2001.

[27] M. Huth, R. Jagadeesan, and D. A. Schmidt. A domain equation for refinement of partial systems. *Mathematical Structures in Computer Science*, 14(4):469–505, Cambridge University Press, August 2004.

[28] M. Huth. Refinement is complete for implementations. Revised version submitted, 27 pages, August 2004. Under review.

[29] M. Huth. Beyond image-finiteness: labelled transition systems as a Stone space. In: *Proc. of the Nineteenth Annual IEEE Symposium on Logic in Computer Science*, pages 222–231, 13-17 July, Turku, Finland, IEEE Computer Society Press, 2004.

[30] D. Jackson. Structuring Z Specifications With Views. *ACM Transactions on Software Engineering and Methodology*, 4(4):365–389, October 1995.

[31] D. Kozen. Results on the propositional mu-calculus. *Theoretical Computer Science*, 27:333–354, 1983.

[32] K. G. Larsen. Modal Specifications. In J. Sifakis, editor, *Automatic Verification Methods for Finite State Systems*, number 407 in Lecture Notes in Computer Science, pages 232–246. Springer Verlag, June 12–14 1989. International Workshop, Grenoble, France.

[33] K. G. Larsen and B. Thomsen. A Modal Process Logic. In *Proc. of the Third Annual IEEE Symposium on Logic in Computer Science*, pages 203–210. IEEE Computer Society Press, 1988.

[34] J. Lawson. Spaces of Maximal Points. *Mathematical Structures in Computer Science*, 7(5):543–555, October 1997.

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

[36] M. Mislove, J. Ouaknine, and J. Worrell. Axioms for Probability and Nondeterminism. *Electronic Notes in Theoretical Computer Science*, 65(1):21 pages, 2003.

[37] R. D. Nicola and M. Hennessy. Testing equivalences for processes. *Theoretical Computer Science*, 34:83–133, 1984.

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

[39] P. Ryan, S. Schneider, M. Goldsmith, G. Lowe, and B. Roscoe. *modelling and analysis of security protocols*. Addison Wesley, 2001.

[40] U. Sattler and M. Vardi. The Hybrid μ-calculus. In R. Goré, A. Leitsch, and T. Nipkov *Proc. of the First International Joint Conference on Automated Reasoning*. Lecture Notes in Computer Science 2083, pages 76–91, Siena, Italy, 18-23 June, Springer Verlag, 2001.

[41] D. S. Scott. *Formal semantics of programming languages*, volume 2 of *Courant Computer Science Symposia*, chapter: *Lattice theory, data types and semantics*, pages 65–106. Prentice-Hall, 1972.

[42] I. Sommerville, P. Sawyer, and S. Viller. Viewpoints for requirements elicitation: a practical approach. In *Proc. of the 1998 International Conference on Requirements Engineering*, Colorado Springs, Colorado, April 6-10 1998. IEEE Computer Society Press.
[43] S. Vickers. *Topology via Logic*. Cambridge Tracts in Theoretical Computer Science 5, 1989.