# Beyond image-finiteness: labelled transition systems as a Stone space

Michael Huth
Department of Computing
Imperial College London
M.Huth@doc.imperial.ac.uk

## Abstract

*We study labelled transition systems over a finite set of events, modulo bisimulation, and prove that this quotient space has a computationally meaningful compact, zero-dimensional, and Hausdorff topology which is therefore ultra-metrizable and measures the degree of bisimilarity. In this space, labelled transition systems are approximated to any degree of precision by image-finite ones as the latter form a dense subset. As this is the 'maximal-points space' of a fully abstract domain for modal transition systems, modulo refinement, our results extend to those systems; unify denotational, operational, and metric semantics; and yield consistency measures for modal transition systems.*

**Keywords:** Labelled transition system, bisimulation, ultrametric, approximation, modal transition system.

## 1. Introduction

Labelled transition systems are a fundamental modelling formalism in many areas of computer science. Bisimulation is the established most general notion of equivalence[1] between labelled transition systems [26] and so any approximative notions, e.g. bounded testing [27], have to use bisimulation as a point of reference. Since bisimulation is an equivalence relation, the quotient of all labelled transition systems with respect to bisimulation is the right conceptual space for reasoning about and comparing qualitative aspects of labelled transition systems. But even quantitative aspects ought to be invariant under bisimulation.

If two labelled transition systems are not bisimilar, we may need to know to what *degree* this is so. This requires a quantitative measure of such differences and such a measure has many applications. We mention security protocols [29], where one system is the specification and the other is an implementation and where we may wish to quantify illicit information flow [10] or the effort needed to expose implementation flaws; modal specifications [23], where a specification captures a possibly infinite set of mutually non-bisimilar labelled transition systems; and requirements engineering [11], where each system may be the modal specification of a particular viewpoint and so *consistency measures on modal specifications* are sought.

Today's modelling needs increasingly require the use of labelled transition systems that are *no longer image-finite;* we mention time, probability, and continuous state spaces. But image-finite labelled transition systems are well understood and often have computable refinement and model checks, e.g. for finite-state systems and the propositional modal mu-calculus [22]. Therefore, the ability to approximate any labelled transition system with an image-finite one, to any degree of precision, is highly desirable. This brings us back to the question of how to measure the difference between two, not necessarily image-finite, labelled transition systems in quantitative terms (bisimulation being a qualitative measure).

A programme that develops such approximations and quantitative metrics should have concepts and results that are *robust under a change of representation*, e.g. if one encodes labelled transition systems as Kripke structures or vice versa. Such encodings are needed to create tool interfaces between event-based and state-based formalisms.

The account of systems and their refinement, given by such a programme, should also present a *unified theory* of operational, denotational, and metric semantics for these formalisms so that qualitative and quantitative reasoning is consistent with each other. In this paper we carry out such a programme and meet all the objectives mentioned above. It would be of interest to see whether similar results are obtainable for systems that explicitly represent time, probability (e.g. as done in [8, 10]) or other quantitative information.

*Outline of 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 results of this paper, showing that the maximal-points space of the fully abstract domain of Section 2 is a Stone space and the

[1] Weak bisimulation [26] on a labelled transition system is bisimulation on a modified transition relation.

quotient of all labelled transition systems with respect to bisimulation. In Section 4 we discuss the scope and significance of these results, Section 5 states related work, and Section 6 concludes.

## 2. Domain of modal transition systems

Larsen & Thomsen's modal transition systems and their refinement [24] are partial versions of labelled transition systems and bisimulation [26]. A modal transition system represents those labelled transition systems that refine it. This representation is sound, for if a modal transition system $M$ refines a modal transition system $N$, then all labelled transition systems that refine $M$ (the 'implementations' of $M$) also refine $N$.

In this section, we define modal transition systems, 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 [20]. Our results are shown within that domain.

Throughout this paper, let $Act$ be a fixed finite set of events and $Act^*$ the set of finite words over $Act$ with $\epsilon$ denoting the word of length zero; the labelled transition systems considered here have events from $Act$ only.

**Definition 1** 1. *A* mixed transition system *[6, 7] is a triple $M = (\Sigma, R^a, R^c)$ such that, for every* mode *$m \in \{a, c\}$, the pair $(\Sigma, R^m)$ is a* labelled transition system, *i.e. $R^m \subseteq \Sigma \times Act \times \Sigma$. If $R^a \subseteq R^c$, we call $M$ a* modal *transition system [24]. A mixed transition system $M$ with a designated initial state $i$ is* pointed, *written $(M, i)$; it is* 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. 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 *$M$ [24, 6]*[2] *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 $(s', t') \in Q$;*

   *(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.*

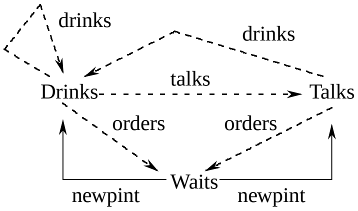

**Figure 1. An image-finite modal transition system specifying aspects of 'pub behavior.'**

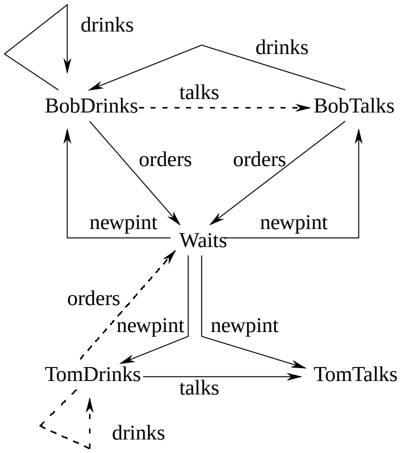

**Figure 2. An image-finite modal transition systems that refines the one in Figure 1.**

**Example 1** *Figures 1 and 2 depict modal transition systems, where dashed and solid lines depict may- and must-transitions, respectively. The refinement $Q$ identifies states with the same activity; e.g.* Drinks *with* TomDrinks *and* BobDrinks *etc.*

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. We may identify modal transition systems $(\Sigma, R, R)$ with labelled transition systems $(\Sigma, R)$ and refinement between such modal transition systems with bisimulation [24]. The reader familiar with domain theory [2] may safely skip the next definition.

**Definition 2** 1. *A* topological space *$(X, \tau)$ consists of a set $X$ and a family $\tau$ of subsets of $X$ such that $\{\}$ and $X$ are in $\tau$, and $\tau$ is closed under finite intersections and arbitrary unions. Elements $O \in \tau$ are $\tau$-*open, *complements $X \setminus O$ with $O \in \tau$ are $\tau$-*closed, *and sets that are $\tau$-open and $\tau$-closed are $\tau$-*clopen.

2. *A partial order $(D, \leq)$ is a* dcpo *iff all its directed*

[2] We use the relational inverse of the $Q$ in [24, 6, 20], as done in [13].

*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. 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 $mub^1(F) = mub(F)$, $mub^{n+1}(F) = mub(mub^n(F))$ for all $n \geq 0$, and $mub^\infty(F) = \bigcup_{n\geq 1} mub^n(F)$. A 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 and contained in $\mathbf{K}(D)$ and $ub(F) = {\uparrow}mub(F)$, where we write ${\uparrow}X = \{d \in D \mid \exists x \in X : x \leq d\}$ and ${\downarrow}X = \{d \in D \mid \exists x \in X : d \leq x\}$ for any $X \subseteq D$. We call $X$* upper *iff $X = {\uparrow}X$;* lower *iff $X = {\downarrow}X$.*

3. *For a SFP-domain $D$, we define the* Scott-topology *$\sigma_D$ to consist of all subsets $U$ of $D$ satisfying $U = {\Uparrow}(U \cap \mathbf{K}(D))$; the* Lawson-topology *$\lambda_D$ 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 $\sigma_D$*-compact saturated *subsets of $D$ to be the $\lambda_D$-closed upper subsets of $D$*[3].

We use the *initial* solution to a domain equation presented in [20] as the domain whose set of maximal points we prove to be the Stone space of pointed labelled transition systems.

**Definition 3** 1. *The* mixed powerdomain *$\mathcal{M}[D]$ [16, 15] of a SFP-domain $D$ has as elements all pairs $(L, U)$ where $L$ is $\sigma_D$-closed and $U$ is $\sigma_D$-compact saturated such that $L$ and $U$ satisfy the* mix condition

$$L = {\Downarrow}(L \cap U)\ . \tag{1}$$

*The order on $\mathcal{M}[D]$ is defined by $(L, U) \leq (L', U')$ iff $(L \subseteq L'\ \&\ U' \subseteq U)$.*

2. *Since $\mathcal{M}[D]$ is a SFP-domain if $D$ is one and the functors $\mathcal{M}$ and $\prod$ are locally continuous [16, 2], we can solve the domain equation*

$$D = \prod_{\alpha \in Act} \mathcal{M}[D] \tag{2}$$

*over SFP-domains where $\prod_{\alpha\in Act}$ denotes the product over all events in $Act$, and write $\mathbb{D}$ for the SFP-domain and* initial solution *of that equation [20].*

3. *Every element $d \in \mathbb{D}$ may be* interpreted as a pointed mixed transition system *$(\mathcal{D}, d)$ where $d$ is the unique* initial state *and the recursion*

$$d = ((d^a_\alpha, d^c_\alpha))_{\alpha \in Act} \tag{3}$$

*of (2) specifies that all pointed mixed transition systems $(\mathcal{D}, d')$ with $d'$ in the set $d^a_\alpha$ ($d^c_\alpha$) are exactly the $\mathbb{R}^a$-successors ($\mathbb{R}^c$-successors) of $d$ for $\alpha$ in $(\mathcal{D}, d)$ (respectively). This makes $\mathbb{D}$ into a mixed transition system, which we denote by*

$$\mathcal{D} = (\mathbb{D}, \mathbb{R}^a, \mathbb{R}^c)\ . \tag{4}$$

By Proposition 1 in [20], the mix condition (1) guarantees that the *mixed* transition system $\mathcal{D}$ in (4) 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.

**Remark 1** *[20] Every image-finite pointed modal transition system $(M, i)$ has an embedding $\langle\!|\, M, i\,|\!\rangle \in \mathbb{D}$ such that $(M, i)$ and $(\mathcal{D}, \langle\!|\, M, i\,|\!\rangle)$ are refinement-equivalent. Moreover, the order on $\mathbb{D}$ is fully abstract: for all $d, e \in \mathbb{D}$, $d \leq e$ iff $(\mathcal{D}, d) \prec (\mathcal{D}, e)$.*

## 3. Stone space of labelled transition systems

In this section, 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 is therefore determined by a complete ultra metric. We define the required notions from topology.

**Definition 4** 1. *A topological space $(X, \tau)$ 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 $\tau$-open set is the union of $\tau$-clopens; and*

   (d) *a* Stone space *iff it is zero-dimensional, compact, and Hausdorff.*

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

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

[3] The definitions in item 3 are really characterizations [2]

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

6. *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 $\mathbb{X} = max(\mathbb{D})$ has a* maximal-points space topology

$$\tau_{\mathbb{X}} = \{U \cap \mathbb{X} \mid U \in \sigma_{\mathbb{D}}\}\,. \qquad (5)$$

7. *For $d \in \mathbb{D}$, we write $M(d)$ for the set $\twoheaduparrow d \cap max(\mathbb{D})$.*

Since $\mathbb{D}$ is a *SFP*-domain we have [25]

$$\tau_{\mathbb{X}} = \{V \cap \mathbb{X} \mid V \in \lambda_{\mathbb{D}}\}\,. \qquad (6)$$

Proposition 1 below holds for algebraic domains satisfying the Lawson condition of [25], which is (6) for $\mathbb{D}$. We state and prove that proposition for $\mathbb{D}$ for sake of completeness.

**Proposition 1** *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 $\twoheaduparrow k$, $k \in \mathbf{K}(\mathbb{D})$, as $\mathbb{D}$ is algebraic. But each $\twoheaduparrow k$ is $\lambda_{\mathbb{D}}$-clopen as $\sigma_{\mathbb{D}} \subseteq \lambda_{\mathbb{D}}$ and $\twoheaduparrow k$ is $\lambda_{\mathbb{D}}$-closed. By (6), 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 $\tau_{\mathbb{X}}$-clopen containing $y$ and $x$ is in the $\tau_{\mathbb{X}}$-open $max(\mathbb{D}) \setminus M(k)$. ■

We need tools from temporal logic to develop a sufficient criterion for membership in $max(\mathbb{D})$.

**Definition 5** 1. *The set of formulas of* Hennessy-Milner logic *[17], $HML$, is generated by the grammar*

$$\phi ::= tt \;\mid\; \neg\phi \;\mid\; \langle\alpha\rangle\phi \;\mid\; \phi \wedge \phi \qquad (7)$$

*where $\alpha$ ranges over the finite set of events $Act$.*

2. *Larsen's* weak semantics *for a pointed modal transition system $(N,i) = ((\Sigma, R^a, R^c), i)$, denoted by $\models$ in [23] for $HML$ in negation normal form, is given by*

   *(a)* $(N,i) \models^m tt$

   *(b)* $(N,i) \models^m \neg\phi$ *iff* $(N,i) \not\models^{\neg m} \phi$

   *(c)* $(N,i) \models^m \langle\alpha\rangle\phi$ *iff for some* $(i, \alpha, i') \in R^m$, $(N,i') \models^m \phi$

   *(d)* $(N,i) \models^m \phi \wedge \psi$ *iff* $((N,i) \models^m \phi$ *and* $(N,i) \models^m \psi)$

   *where $m \in \{a, c\}$, $\neg a = c$, and $\neg c = a$.*

We write $[\alpha]$ for $\neg\langle\alpha\rangle\neg$ and $\phi \vee \psi$ for $\neg(\neg\phi \wedge \neg\psi)$ subsequently. For each $m \in \{a, c\}$ we have $(N,i) \models^m [\alpha]\phi$ iff for all $(i, \alpha, i') \in R^{\neg m}$, $(N,i') \models^m \phi$; and $(N,i) \models^m \phi \vee \psi$ iff $((N,i) \models^m \phi$ or $(N,i) \models^m \psi)$.

**Example 2** *Consider the modal transition system $N$ in Figure 1.*

1. *We have $(N, \mathrm{Talks}) \models^c \langle\mathrm{drinks}\rangle tt$ by virtue of the $R^c$-transition $(\mathrm{Talks}, \mathrm{drinks}, \mathrm{Drinks})$. By the semantics of negation, this implies $(N, \mathrm{Talks}) \not\models^a \neg\langle\mathrm{drinks}\rangle tt$. We also infer $(N, \mathrm{Talks}) \not\models^a \langle\mathrm{drinks}\rangle tt$ since there is no state $s$ with $(\mathrm{Talks}, \mathrm{drinks}, s) \in R^a$. By the semantics of disjunction, $(N, \mathrm{Talks}) \not\models^a \langle\mathrm{drinks}\rangle tt \vee \neg\langle\mathrm{drinks}\rangle tt$.*

2. *We have $(N, \mathrm{Waits}) \not\models^a \psi_{tt}^{\text{newpint talks, drinks}}$, for the formula $\psi_{tt}^{\text{newpint talks, drinks}}$ of $HML$ being $[\mathrm{newpint}][\mathrm{talks}](\langle\mathrm{drinks}\rangle tt \vee \neg\langle\mathrm{drinks}\rangle tt)$, as there is an $R^c$-path for the word $\mathrm{newpint\,talks} \in Act^*$, $(\mathrm{Waits}, \mathrm{newpint}, \mathrm{Drinks})(\mathrm{Drinks}, \mathrm{talks}, \mathrm{Talks})$, and $(N, \mathrm{Talks}) \not\models^a \langle\mathrm{drinks}\rangle tt \vee \neg\langle\mathrm{drinks}\rangle tt$ by item 1.*

We record some facts from [23] expressed within $\mathbb{D}$ in [20]:

**Remark 2** *[20] Let $d, e \in \mathbb{D}$ and $\phi, \psi \in HML$. Then $(\mathcal{D}, d) \models^a \phi$ implies $(\mathcal{D}, d) \models^c \phi$. We have $(\mathcal{D}, d) \prec (\mathcal{D}, e)$ iff (for all $\psi \in HML$, $(\mathcal{D}, e) \models^c \psi$ implies $(\mathcal{D}, d) \models^c \phi$) iff (for all $\psi \in HML$, $(\mathcal{D}, d) \models^a \psi$ implies $(\mathcal{D}, e) \models^a \phi$).*

Note that for pointed labelled transition systems $(L, l) = ((\Sigma, R, R), l)$, $\models^a$ equals $\models^c$ and is the standard semantics of $HML$ (e.g. see [26]) over labelled transition systems. This coincidence of $\models^a$ and $\models^c$ implies maximality in $\mathbb{D}$.

**Lemma 1** *Let $d \in \mathbb{D}$ such that, for all $\phi \in HML$, $(\mathcal{D}, d) \models^c \phi$ implies $(\mathcal{D}, d) \models^a \phi$. Then $d \in max(\mathbb{D})$.*

**Proof:** Consider such a $d$ and let $d \leq e$ in $\mathbb{D}$. Proof by contradiction: If $d \neq e$, then $e \not\leq d$ as $\mathbb{D}$ is a partial order. From $e \not\leq d$ we infer that there is some $k \in \mathbf{K}(\mathbb{D})$ with $k \leq e$ and $k \not\leq d$ as $\mathbb{D}$ is algebraic. For $\phi_k \in HML$ of [20], which satisfies

$$\forall f \in \mathbb{D}\colon \qquad (\mathcal{D}, f) \models^a \phi_k \qquad \text{iff} \qquad k \leq f\,, \qquad (8)$$

$k \leq e$ implies $(\mathcal{D}, e) \models^a \phi_k$ which implies $(\mathcal{D}, e) \models^c \phi_k$ by Remark 2. But $d \leq e$ means $(\mathcal{D}, d) \prec (\mathcal{D}, e)$ as $\mathbb{D}$ is fully abstract, and so $(\mathcal{D}, d) \models^c \phi_k$ by Remark 2 as $(\mathcal{D}, e) \models^c \phi_k$. By assumption on $d$, this renders $(\mathcal{D}, d) \models^a \phi_k$ and so $k \leq d$ by (8), a contradiction. ■

We sketch the definition of $\langle\!| M, i |\!\rangle \in \mathbb{D}$ for an image-finite modal transition system $(M, i)$ such that $(M, i)$ and $(\mathcal{D}, \langle\!| M, i |\!\rangle)$ are refinement-equivalent [20]. This construction follows ideas from algebraic semantics à la Nivat-Courcelle-Guessarian or à la Goguen-Thatcher-Wagner-Wright and is presented here via a simple process algebra.

**Definition 6** *1. The grammar for the* process algebra *$MPA$ is*

$$p ::= \mathbf{0} \mid \bot \mid \alpha_{tt}.p \mid \alpha_{\bot}.p \mid p + p \qquad (9)$$

*where $\alpha$ denotes any event in $Act$.*

2. *For each $p \in MPA$ let $\{\!| p |\!\} \in \mathbb{D}$ be as in Figure 3.*
3. *For all $p \in MPA$, the operational semantics in Figure 4 defines a pointed modal transition system $(\llbracket p \rrbracket, p)$.*

**Example 3** *Let $p \in MPA$ be* $\mathrm{drinks}_{\bot}.\bot + \mathrm{orders}_{\bot}.\bot + \mathrm{talks}_{tt}.\mathbf{0}$. *Then $(\llbracket p \rrbracket, p)$ is refinement-equivalent to the image-finite pointed modal transition system in Figure 5.*

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 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. It is rather obvious that this image-finite pointed modal transition system $(M[m], i)$ is the operational meaning of a term $p_m \in MPA$, and $m \leq m'$ implies that $\{\!| p_m |\!\} \leq \{\!| p_{m'} |\!\}$. Thus we can set $\langle\!| M, i |\!\rangle = \bigvee_{m \geq 0} \{\!| p_m |\!\}$ and note, shown in [16] for *SFP*-domains (without reference to a process algebra), that

$$\mathbf{K}(\mathbb{D}) = \{\{\!| p |\!\} \mid p \in MPA\}\,. \qquad (10)$$

**Example 4** *Figure 5 illustrates the construction of a finite approximation $(M[1], \mathrm{TomDrinks})$ to the pointed modal transition system $(M, \mathrm{TomDrinks})$ of Figure 2.*

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.

**Proposition 2** *The set of all embeddings of pointed image-finite labelled transition systems is dense in $(\mathbb{X}, \tau_{\mathbb{X}})$.*

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

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

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

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

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

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

$$\{\!| p + q |\!\}^a_\gamma = \{\!| p |\!\}^a_\gamma \cup \{\!| q |\!\}^a_\gamma,\ \gamma \in Act$$

$$\{\!| p + q |\!\}^c_\gamma = \{\!| p |\!\}^c_\gamma \cup \{\!| q |\!\}^c_\gamma,\ \gamma \in Act\,.$$

**Figure 3. Denotational semantics $\{\!| p |\!\}$ of the process algebra $MPA$ in $\mathbb{D}$; it interprets $0$ as deadlock in $\mathbb{D}$, $\bot$ as the least element of $\mathbb{D}$, $+$ as the mix union of [16], and the prefixes as expected (using saturations with $\downarrow$ and $\uparrow$ to ensure membership in $\mathbb{D}$).**

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

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

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

**Figure 4. Structural operational semantics of $MPA$: $p \longrightarrow^{\alpha}_{\bot} p'$ denotes a may-transition from $p$ to $p'$ and $p \longrightarrow^{\alpha}_{tt} p'$ denotes a must-transition from $p$ to $p'$, each labelled with some $\alpha \in Act$. A value $v$ stands for either $\bot$ or $tt$. There are no transitions out of $0$ and the free occurrence of $\gamma$ ranges over all events in $Act$.**

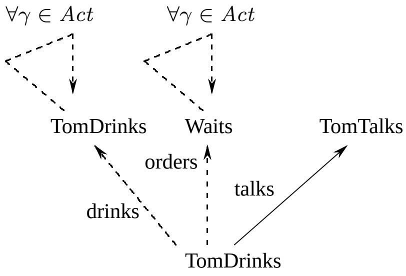

**Figure 5. The pointed modal transition system $(M[1], \mathrm{TomDrinks})$, an approximation of the pointed modal transition system $(M, \mathrm{TomDrinks})$ in Figure 2;** Waits **and the second** TomDrinks **turn into a may-stub.**

**Proof:** Let $(L, l)$ be a pointed image-finite labelled transition system. Then $(L, l)$ is refinement-equivalent to $(\mathcal{D}, (\!| L, l |\!))$ by Remark 1, so $d = (\!| L, l |\!)$ satisfies the assumptions of Lemma 1 and $(\!| L, l |\!)$ is in $max(\mathbb{D}) = \mathbb{X}$.

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. By (10) there is some $p \in MPA$ with $\{\!| p |\!\} = k$. Let $q \in MPA$ be obtained by replacing all $\perp$ in $p$ with $\mathbf{0}$ and all prefixes $\gamma_\perp$ with $\gamma_{tt}$ $(\forall \gamma \in Act)$. Then $\{\!| p |\!\} \leq \{\!| q |\!\}$ as $(\mathcal{D}, \{\!| q |\!\})$ refines $(\mathcal{D}, \{\!| p |\!\})$. Since $(\| q \|, q)$ is a pointed *labelled* transition system and refinement-equivalent to $(\mathcal{D}, \{\!| q |\!\})$ (a straightforward structural induction on $q$), we conclude $\{\!| q |\!\} \in M(k) \subseteq O$ by Lemma 1 and $\{\!| q |\!\}$ is the embedding of a pointed image-finite labelled transition system. ∎

We show that $(\mathbb{X}, \tau_{\mathbb{X}})$ is compact by proving, indirectly, that $max(\mathbb{D})$ is $\lambda_{\mathbb{D}}$-closed.

**Definition 7** *1. Let $\Delta = \delta_1 \delta_2 \ldots \delta_n \in Act^*$, $\alpha \in Act$, and $k \in \mathbf{K}(\mathbb{D})$. Then $\psi_k^{\Delta, \alpha} \in HML$ is defined to be*

$$[\delta_1][\delta_2] \ldots [\delta_n](\langle\alpha\rangle\phi_k \vee \neg\langle\alpha\rangle\phi_k) \tag{11}$$

*with $\phi_k$ as in (8).*

*2. Let $\Phi$ $(\subseteq HML)$ be the set of all $\psi_k^{\Delta, \alpha}$ where $\Delta \in Act^*$, $\alpha \in Act$, and $k \in \mathbf{K}(\mathbb{D})$.*

*3. For $\phi \in HML$ and all $m \in \{a, c\}$ let*

$$\| \phi \|^m = \{d \in \mathbb{D} \mid (\mathcal{D}, d) \models^m \phi\} . \tag{12}$$

*4. Let $C_\Phi = \bigcap_{\phi \in \Phi} \| \phi \|^a$.*

**Example 5** *The formulas in items 1 and 2 of Example 2 are in $\Phi$ as $tt$ is $\phi_{\perp_{\mathbb{D}}}$, $\perp_{\mathbb{D}} \in \mathbf{K}(\mathbb{D})$, and $\epsilon \in Act^*$.*

We show that $C_\Phi$ is $\lambda_{\mathbb{D}}$-closed and prove $max(\mathbb{D}) = C_\Phi$.

**Lemma 2** *For each $\phi \in HML$, the sets $\| \phi \|^a$ and $\| \phi \|^c$ are $\lambda_{\mathbb{D}}$-clopen[4]. In particular, $C_\Phi$ is $\lambda_{\mathbb{D}}$-closed.*

**Proof:** We proceed with the first claim by structural induction on $\phi \in HML$. 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 $m \in \{a, c\}$

$$\| \langle\alpha\rangle\phi \|^m = \{d \in \mathbb{D} \mid d_\alpha^m \cap \| \phi \|^m \neq \{\}\} . \tag{13}$$

- Let $m = a$. By item 2 of Theorem 4 in [20], all $\| \psi \|^a$ $(\psi \in HML)$ are $\sigma_{\mathbb{D}}$-open, so $\| \langle\alpha\rangle\phi \|^a \in \sigma_{\mathbb{D}} \subseteq \lambda_{\mathbb{D}}$. Thus, 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 $F_\phi \subseteq \mathbf{K}(\mathbb{D})$ since $\mathbb{D}$ is algebraic. Inspecting (13), we have $e \in \| \langle\alpha\rangle\phi \|^a$ iff $e_\alpha^a \cap \uparrow F_\phi \neq \{\}$. Since $e_\alpha^a$ is a lower set, this is equivalent to $e_\alpha^a \cap F_\phi \neq \{\}$. For each $y \in F_\phi$ define $c(y) = (c(y)_\alpha)_{\alpha \in Act} \in \mathbb{D}$ 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 $y \in c(y)_\alpha^a \cap F_\phi$ for all $y \in C$, we get $\uparrow C \subseteq \| \langle\alpha\rangle\phi \|^a$ as the latter is upper. Note that for each $y \in F_\phi$ we have $c(y) \leq e$ in $\mathbb{D}$ iff $y \in e_\alpha^a$. 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 item 2 of Theorem 4 in [20] 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 this set is $\lambda_{\mathbb{D}}$-open. By induction, $\| \phi \|^c$ is $\lambda_{\mathbb{D}}$-open and so $D \setminus \| \phi \|^c = \| \neg\phi \|^a$ 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 (13), we infer $e \in \| \langle\alpha\rangle\phi \|^c$ iff there is some $x \in e_\alpha^c$ 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 $l = (l_\alpha)_{\alpha \in Act}$, 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 $e_\alpha^c \not\subseteq \uparrow F_{\neg\phi}$ iff (for some $x \in e_\alpha^c$, $x \notin \uparrow F_{\neg\phi}$). Therefore, $d \in \uparrow k \setminus \uparrow l \subseteq \| \langle\alpha\rangle\phi \|^c$.

Thus, $C_\Phi$ is $\lambda_{\mathbb{D}}$-closed as the intersection of $\lambda_{\mathbb{D}}$-closed sets. ∎

[4] That $\| \phi \|^a$ and $\| \phi \|^c$ are $\lambda_{\mathbb{D}}$-clopen allows one to prove the main result of [18] without requiring Theorem 1 below.

**Lemma 3** *The set $max(\mathbb{D})$ is contained in $C_\Phi$.*

**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 $(L, l)$ whenever $\langle\!| L, l |\!\rangle \in A$, $\alpha\langle\phi\rangle \vee \neg\alpha\langle\phi\rangle$ is valid over labelled transition systems, $[\delta_i]\phi$ is valid over labelled transition systems whenever $\phi$ is, and $\models^a$ is the standard semantics of *HML* over labelled transition systems.

By Proposition 2, $A$ $(\subseteq max(\mathbb{D}))$ is dense in $(\mathbb{X}, \tau_\mathbb{X})$ 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 (6) since $C_\Phi$ is $\lambda_\mathbb{D}$-closed by Lemma 2. 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 $max(\mathbb{D}) \subseteq C_\Phi$. ■

We need to clarify the structure of elements in $C_\Phi$.

**Lemma 4** *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 $C_\Phi$ as well.*

2. *For all $\alpha \in Act$ we have $d^c_\alpha = \upharpoonleft(d^a_\alpha \cap d^c_\alpha)$.*

3. *For all $\phi \in HML$, $(\mathcal{D}, d)\models^c\phi$ implies $(\mathcal{D}, d)\models^a\phi$.*

**Proof:**

1. Let $d'$ be reachable from $d$ in $(\mathbb{D}, \mathbb{R}^c)$ and let $\Gamma \in Act^*$ be any word obtained by travelling from $d$ to $d'$ in $(\mathbb{D}, \mathbb{R}^c)$. Given $\psi^{\Delta,\,\alpha}_k \in \Phi$, the concatenation $\Gamma\Delta$ is in $Act^*$ and so $\psi^{\Gamma\Delta,\,\alpha}_k \in \Phi$. Thus the path for $\Gamma$ above and $d \in C_\Phi$ ensure $(\mathcal{D}, d')\models^a\psi^{\Delta,\,\alpha}_k$ and so $d' \in C_\Phi$.

2. Let $\alpha \in Act$. Since $\upharpoonleft(d^a_\alpha \cap d^c_\alpha) \subseteq \upharpoonleft d^c_\alpha = d^c_\alpha$, it suffices to show $d^c_\alpha \subseteq \upharpoonleft(d^a_\alpha \cap d^c_\alpha)$. Proof by contradiction: Let $x \in d^c_\alpha \setminus \upharpoonleft(d^a_\alpha \cap d^c_\alpha)$. Then $x \in d^c_\alpha$ and $d^a_\alpha \cap d^c_\alpha \subseteq \upharpoonleft(d^a_\alpha \cap d^c_\alpha)$ 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 $k \in \mathbf{K}(\mathbb{D})$ with $k \in \mathbb{D} \setminus d^a_\alpha$ and $k \leq x$ and so $\upharpoonleft k \cap d^a_\alpha = \{\}$ as $d^a_\alpha$ is a lower set. But $d \in C_\Phi$ implies $(\mathcal{D}, d)\models^a\langle\alpha\rangle\phi_k \vee \neg\langle\alpha\rangle\phi_k$, as that formula is $\psi^{\epsilon,\,\alpha}_k$, and so $\upharpoonleft k \cap d^a_\alpha = \{\}$ implies $\upharpoonleft k \cap d^c_\alpha = \{\}$ by (13), contradicting $x \in \upharpoonleft k \cap d^c_\alpha$.

3. We use structural induction on $\phi \in HML$. 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 Remark 2 as $\mathbb{D}$ is fully abstract. Since $d'' \in d^c_\alpha$ is reachable from $d$ in $(\mathbb{D}, \mathbb{R}^c)$ it is in $C_\Phi$ by item 1. Thus, we can apply induction and get $(\mathcal{D}, d'')\models^a\phi$. Since $d'' \in d^a_\alpha$, this renders $(\mathcal{D}, d)\models^a\langle\alpha\rangle\phi$. ■

The next two theorems state the main results of this paper.

**Theorem 1** *The set $max(\mathbb{D})$ equals $C_\Phi$. 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 4 and Lemma 1 we infer $C_\Phi \subseteq max(\mathbb{D})$. By Lemma 3 this implies $max(\mathbb{D}) = C_\Phi$. By Lemma 2, this means that $max(\mathbb{D})$ is $\lambda_\mathbb{D}$-closed. By Propositions 1 and 2, 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 (5) 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 *SFP*-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. ■

Next we show that $(\mathbb{X}, \tau_\mathbb{X})$ is precisely the quotient space of pointed labelled transition systems modulo bisimulation.

**Definition 8** *Given a topological space $(X, \tau)$ let $\mathcal{C}[X, \tau]$ be the* set of all $\tau$-compact subsets of $X$.

**Theorem 2**
1. *The embedding $(M, i) \mapsto \langle\!| M, i |\!\rangle$ for pointed image-finite modal transition systems 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*[5].

3. *Moreover, $\mathbb{X}$ satisfies the isomorphism*

$$\mathbb{X} = \prod_{\alpha \in Act} \mathcal{C}[\mathbb{X}, \tau_\mathbb{X}] \tag{14}$$

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

**Proof:**

1. We only sketch the idea. Whenever a state $s$ has infinitely many states $(s_i)_{i \in I}$ as $\alpha$-successors for $R^c$, choose a finite subset $F$ of $I$, retain transitions $(s, \alpha, s_i)$ and their must/may status for all $i \in F$, discard all $(s, \alpha, s_i)$ with $i \notin F$, and create a *may-stub* $s_F$ ($\langle\!| s_F |\!\rangle = \bot_\mathbb{D}$) and a may-transition $(s, \alpha, s_F)$. Doing this for all events while, at the same time,

[5] It doesn't 'type check' to ask whether $(\mathcal{D}, d)$ is *bisimilar* to a labelled transition system; but the saturation $\downharpoonleft$ is merely an artefact of the model.

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 1 whenever $(M, i)$ is a labelled transition system.

2. Let $d \in max(\mathbb{D})$ $(= C_\Phi)$. By Lemma 4, for all $\alpha \in Act$, the set $d^a_\alpha \cap d^c_\alpha$ is in $C_\Phi$ $(= max(\mathbb{D}))$ and $d^c_\alpha = {\Uparrow}(d^a_\alpha \cap d^c_\alpha)$. Combining this, we infer $d = (({\Downarrow}(d^a_\alpha \cap d^c_\alpha), d^a_\alpha \cap d^c_\alpha))_{\alpha \in Act}$. But since $C_\Phi$ 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 labelled transition system that replaces ${\Downarrow}(e^a_\alpha \cap e^c_\alpha)$ with $e^a_\alpha \cap e^c_\alpha$ for all $e$ reachable from $d$ in $(\mathbb{D}, \mathbb{R}^c)$.

3. The equation (14) follows from (2), Lemmas 34.5 and 25 of [4]; the latter is stated for $SFP^M$-domains $D$ but only requires that $max(D)$ is $\lambda_D$-closed. ∎

The compactness of $\mathbb{X}$ has an interpretation in terms of Hennessy-Milner logic.

**Corollary 1** *Let $(\phi_i)_{i \in I}$ be a family of formulas of Hennessy-Milner logic such that every pointed labelled transition system satisfies at least one of these $\phi_i$. Then there is a finite set $F \subseteq I$ such that the formula $\bigvee_{i \in F} \phi_i \in HML$ is valid over all labelled transition systems.*

**Proof:** Since bisimulation-equivalent labelled transition systems satisfy the same formulas of $HML$, items 1 and 2 of Theorem 2 and the assumptions on $(\phi_i)_{i \in I}$ above imply $\mathbb{X} = \bigcup \mathcal{U}$ where $\mathcal{U} = \{\llbracket \phi_i \rrbracket^a \cap max(\mathbb{D}) \mid i \in I\}$ is in $\tau_\mathbb{X}$ as all $\llbracket \phi_i \rrbracket^a$ are in $\sigma_\mathbb{D}$. Since $(\mathbb{X}, \tau_\mathbb{X})$ is compact by Theorem 1, there is a finite $\mathcal{F} \subseteq \mathcal{U}$ with $\mathbb{X} \subseteq \bigcup \mathcal{F}$, i.e $\mathbb{X} \subseteq \bigcup_{i \in F} \llbracket \phi_i \rrbracket^a = \llbracket \bigvee_{i \in F} \phi_i \rrbracket^a$ for a finite set $F \subseteq I$. Thus all labelled transition systems satisfy $\bigvee_{i \in F} \phi_i$ by Theorem 2 as the embedding of labelled transition systems into $\mathbb{D}$ reflects and preserves refinement. ∎

## 4. Discussion

The scope of these results, including Corollary 1, is wider than that of labelled and modal transition systems. Godefroid & Jagadeesan [14] show that many three-valued models, their refinement, and temporal logic semantics are equivalent in expressiveness and that the translations that witness this equivalence preserve and reflect refinements and impose no complexity penalties. Thus, our results also apply to Kripke structures and their notion of bisimulation. To define the distance between *partial* Kripke structures [5] $(K_1, i_1)$ and $(K_2, i_2)$, compute their translations as pointed modal transition systems $(T_1, t_1)$ and $(T_2, i_2)$, respectively, as in [14], and then compute the distance between these two modal transition systems. This is meaningful as these translations preserve and reflect refinement, so they are well defined on equivalence classes; in particular, the maximality of elements is preserved and reflected.

We explicitly state the metrics $d_\mathbb{D}$ for pointed modal transition systems and $d_\mathbb{X}$ for pointed labelled transition systems. Fix an enumeration $k_0, k_1, \ldots$ of $\mathbf{K}(\mathbb{D})$ and set

$$\begin{aligned} d_\mathbb{D}(d, e) &= inf\{2^{-n} \mid \forall i \leq n\colon k_i \leq d \Leftrightarrow k_i \leq e\} \\ d_\mathbb{X}(x, y) &= inf\{2^{-n} \mid \forall i \leq n\colon k_i \leq x \Leftrightarrow k_i \leq y\}\,. \end{aligned}$$

Then the topology determined by $d_\mathbb{D}$ and $d_\mathbb{X}$ is $\lambda_\mathbb{D}$ and $\tau_\mathbb{X}$, respectively. The practical utility of these metrics may depend on a wise choice of the enumeration above. Ideally, we wish to enumerate compact elements $k$ in increasing modal depth of $\phi_k$ in (8), corresponding to the iterative unfolding of the functional for bisimulation [26].

We define the *consistency measure* $[c_1(d, e), c_2(d, e)]$ by

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

and use this as an alternative way of comparing the pointed modal transition systems $(\mathcal{D}, d)$ and $(\mathcal{D}, e)$. Since $M(f)$ is $\tau_\mathbb{X}$-compact for all $f \in \mathbb{D}$ ($\lambda_\mathbb{D}$-closed as the intersection of two $\lambda_\mathbb{D}$-closed sets), $c_1(d, e)$ 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 $M(e)$ is the symmetric $\forall\exists$-lift of $d_\mathbb{X}$ to $\tau_\mathbb{X}$-compact subsets and satisfies $c_1(d, e) \leq c(d, e) \leq c_2(d, e)$.

Such measures are of particular interest if $d$ and $e$ represent different viewpoints [28, 21, 30] of the same system such that the degree of consistency between these descriptions needs to be explored. Let us say that $(\mathcal{D}, d)$ and $(\mathcal{D}, e)$ are *consistent with each other* iff they have some common refinement $(\mathcal{D}, f)$. Using Theorems 1 and 2 and equation (3) of [23] for finite-state systems we can show:

**Theorem 3** *Let $d, e \in \mathbb{D}$. Then $c_1(d, e) = 0$ iff $(\mathcal{D}, d)$ and $(\mathcal{D}, e)$ are consistent with each other. Moreover, "$c_1(\langle\!| M, i |\!\rangle, \langle\!| N, j |\!\rangle) = 0?$," ranging over finite-state modal transition systems $(M, i)$ and $(N, j)$, is in EXPTIME.*

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, and $c_2(d, e)$ is an upper bound on such a difference. From item 4 of Definition 4, $c_1$ satisfies only (b) and $c_2$ satisfies only (b) and (c).

Our maximal-points space $\mathbb{D}$ enables modelling and reasoning about labelled transition systems *that are not necessarily image-finite*. Such systems are increasingly required and some approximation results are found in the literature (e.g. [8]). Our results and techniques offer a uniform way of approximating such systems and embedding them into $\mathbb{D}$.

As pointed out by Di Pierro et al. in [10], a quantitative measure of non-bisimilarity between two (probabilistic) labelled transition systems $L_1$ and $L_2$ can assess whether an implementation $L_2$ is secure enough with respect to a specification $L_1$, the idea being that bisimulation ensures a non-interference property and that non-bisimulation implies information leaks that need to be quantified. Since $\tau_{\mathbb{X}}$ is determined by a complete ultra-metric, such a programme is within reach for labelled transition systems. Two issues emerge. First, different ultra-metrics $d$ may determine $\tau_{\mathbb{X}}$ but any such choice fixes a quantitative scale. Second, having found a practically meaningful scale and definition of this metric, $d$ may not be (feasibly) computable and so algorithms for suitable approximations of values $d(x, y)$ may have to be designed.

In [20] the sets $\llbracket \phi \rrbracket^m$ of (12), indexed with a consistent environment for recursion variables, are defined for formulas $\phi$ of the propositional modal mu-calculus $\mu M$ [22]. For all $\phi \in \mu M$, one can show that these sets are upper (for $m = a$) and lower (for $m = c$) sets in $\mathbb{D}$ [20]. In fact, all of these sets are elements of the Borel algebra of $\sigma_{\mathbb{D}}$, the sigma-algebra generated by $\sigma_{\mathbb{D}}$. Which upper and lower sets of that Borel algebra have such a representation? Answers would shed light on the topology of abstraction-based model-checking [12].

## 5. Related work

Abramsky [1] provides a fully abstract domain of synchronization trees for labelled transition systems that have a divergence predicate and *partial* bisimulation. 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 [19].

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 *SFP*-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 1 but we suspect it is not a $SFP^M$-domain since $\mathcal{M}[D_1]$ is not a $SFP^M$-domain for the $SFP^M$-domain $D_1 = \{\bot < \mathit{ff}, \mathit{tt}\}$ [3], although $\mathcal{M}[D_1]$ is the second iteration of the domain equation (2) for $Act = \{\alpha\}$.

The paper [20] 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 [18] the model $\mathbb{D}$ is used to show that an image-finite pointed modal transition system $(N, j)$ refines an image-finite pointed modal transition system $(M, i)$ iff all image-finite labelled transition systems that refine $(N, j)$ also refine $(M, i)$.

Di Pierro et al. [10] develop a quantitative notion of process equivalence that forms 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 and show that one soundly abstracts the other.

Desharnais et al. [8] show that each continuous-state labelled Markov process has a sequence of finite acyclic labelled Markov processes as abstractions such that this sequence is, in a technical sense, 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. [9] 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 [20]. 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 then revealed the fine-structure of $\mathbb{X}$, notably we proved that its topology $\tau_{\mathbb{X}}$ inherited from $\sigma_{\mathbb{D}}$ and $\lambda_{\mathbb{D}}$ is compact, zerodimensional, and Hausdorff (a Stone space). In particular, $\tau_{\mathbb{X}}$ is determined by a complete ultra-metric $d_{\mathbb{X}}$ for which image-finite labelled transition systems approximate labelled transition systems to any degree of precision[6]. Thus our results unify denotational, operational, and metric semantics of labelled and modal transition systems. We then discussed the scope and significance of these results and pointed to their potential applications in security, requirements engineering, and under-specification.

## 7. Acknowledgments

Glenn Bruns, Alessandra Di Pierro, Patrice Godefroid, Chris Hankin, Radha Jagadeesan, Achim Jung, Ralph Kop-

[6] 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 $\lambda_{\mathbb{D}}$ and $d_{\mathbb{D}}$.

perman, David Schmidt, and Herbert Wiklicky commented on the general research programme underlying this work.

## 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 *Proceedings of the 11th Conference on Computer Aided Verification*, volume 1633 of *Lecture Notes in Computer Science*, pages 274–287. Springer Verlag, July 1999.

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

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

[8] J. Desharnais, V. Gupta, R. Jagadeesan, and P. Panangaden. Approximating Labeled Markov Processes. In *15th Annual IEEE Symposium on Logic in Computer Science (LICS'00)*, Santa Barbara, California, 26-29 June 2000. IEEE Computer Society Press.

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

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

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

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

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

[14] 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 4th Conference on Verification, Model Checking and Abstract Interpretation (VMCAI'2003)*, volume 2575 of *LNCS*, pages 206–222, New York, January 2003. Springer Verlag.

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

[16] R. Heckmann. Set Domains. In *European Symposium on Programming*, pages 177–196, 1990.

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

[18] M. Huth. Refinement is complete for implementations. Invited submission to the special issue for the Third International Workshop on Automated Verification of Critical Systems. Under review, January 2004.

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

[20] M. Huth, R. Jagadeesan, and D. A. Schmidt. A domain equation for refinement of partial systems. Accepted for publication in the journal Mathematical Structures in Computer Science. In press; 1 February, 2003.

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

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

[23] 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.

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

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

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

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

[28] 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.

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

[30] I. Sommerville, P. Sawyer, and S. Viller. Viewpoints for requirements elicitation: a practical approach. In *Proc. 1998 International Conference on Requirements Engineering (ICRE'98)*, Colorado Springs, Colorado, April 6-10 1998. IEEE Computer Society Press.