On two-sided approximate model-checking: problem formulation and solution via finite topologies *

J.M. Davoren[1], T. Moor[2], R.P. Goré[3], V. Coulthard[3,1], and A. Nerode[4]

[1] Department of Electrical & Electronic Engineering
The University of Melbourne, VIC 3010 AUSTRALIA
davoren@unimelb.edu.au
[2] Lehrstuhl für Regelungstechnik
Friedrich-Alexander-Universität, Erlangen D-91058 GERMANY
thomas.moor@rt.eei.uni-erlangen.de
[3] Computer Sciences Laboratory, RSISE
The Australian National University, Canberra ACT 0200 AUSTRALIA
vaughan@discus.anu.edu.au
[4] Department of Mathematics Cornell University, Ithaca NY 14853 USA
anil@math.cornell.edu

Abstract. We give a general formulation of *approximate model-checking*, in which both under- and over-approximations are propagated to give two-sided approximations of the denotation set of an arbitrarily complex formula. As our specification language, we use the *modal μ-calculus*, since it subsumes standard linear and branching temporal logics over transition systems like **LTL**, **CTL** and **CTL***. We give a general construction of a *topological finite approximation scheme* for a Kripke model from a state-space discretization via an A/D-map and its induced finite topology. We further show that under natural *coherence conditions*, any finite approximation scheme can be refined by a topological one.

1 Introduction

It is now well established that exact symbolic model-checking of modal and/or temporal logic formulas in transition system models of hybrid and real-time systems is not computationally possible (recursively solvable) except when restricted to some tightly constrained sub-classes of systems. Given these limitations on exactness, a good deal of current research in formal methods for hybrid and real-time systems is devoted to developing algorithms for approximations of various backwards and forwards reachability operators on sets arising from differential inclusions and equations. Such approximations are typically based on a discretization of the state space by a finite partition or cover, e.g. consisting of a regular array of rectangular boxes, or of convex polyhedra or ellipsoids. Recent

* Research support from Aust. Research Council, Grants DP0208553, LX0242359. We thank Bryn Humberstone at Univ. of Melbourne for many valuable discussions.

contributions focus attention on application relevant classes of reachability relations and include algorithms for the efficient computation of over-approximations of sets of reachable states [1–3, 8, 10].

For example, in seeking to verify a safety property of a hybrid system model, such as expressed by "*From given initial conditions, the system never reaches a danger state*", one can use an *over-approximation* of the true reach-set and its disjointness from the danger states to conclude "*definitely* YES" to the verification question. Now suppose instead that one is asking *control* questions, such as "*From which set of states can the system be steered to reach a given target region, and up until then, always remain within designated safe states?*" Here, a guaranteed *under-approximation* of this backwards reachability set will let us identify a set of states of which we can answer "*definitely* YES" to this controllability question, with respect to the particular dynamics of the steered system.

In this paper, we address the task of giving *two-sided approximate evaluations* of the denotation set $[\![\varphi]\!]^{\mathcal{M}} \subseteq X$ of a logic formula φ, where $[\![\varphi]\!]^{\mathcal{M}}$ is the set of all states of a Kripke model $\mathcal{M}$ at which φ is satisfied – with $\mathcal{M} = (X, R, v)$, X the state space, $R \subseteq X \times X$ the transition relation, and $v : P \to 2^X$ a valuation of atomic propositions $p \in P$ as subsets of X. We consider the general problem of constructing maps $Un^{\mathcal{M}}$ and $Ov^{\mathcal{M}}$ which, when applied to a formula φ, return explicit computable descriptions of subsets of X with the property that $Un^{\mathcal{M}}(\varphi) \subseteq [\![\varphi]\!]^{\mathcal{M}} \subseteq Ov^{\mathcal{M}}(\varphi)$. As our specification language, we take the *modal μ-calculus*, since all the standard linear and branching temporal logics interpreted over transition systems (**LTL**, and **CTL** and **CTL***, respectively) are subsumed by the μ-calculus. We actually work with the *tense logic* extension, with modal operators for both the one-step future and past along the transition relation, as both constructs naturally rise in control and verification problems.

Building on the foundations of Cousot and Cousot's *abstract interpretation* [5], questions of approximation and abstraction for model-checking of large but finite state systems have been addressed by Grumberg and colleagues in [4, 6, 12]. In the recent [12], they develop a framework for abstraction using three-valued semantics, working say with $\mathbb{T} := \{\mathbf{yes}, \mathbf{no}, \mathbf{indf}\}$ (the latter abbreviating "*indefinite*"); working over bi-relational "must-may" Kripke models $\mathcal{M}$, they give a disjoint pair of affirmation and refutation denotation sets $[\![\varphi]\!]^{\mathcal{M}}_{\mathbf{yes}} \subseteq X$ and $[\![\varphi]\!]^{\mathcal{M}}_{\mathbf{no}} \subseteq X$ such that $[\![\varphi]\!]^{\mathcal{M}}_{\mathbf{yes}} \cap [\![\varphi]\!]^{\mathcal{M}}_{\mathbf{no}} = \varnothing$, and take $[\![\varphi]\!]^{\mathcal{M}}_{\mathbf{indf}} = X - ([\![\varphi]\!]^{\mathcal{M}}_{\mathbf{yes}} \cup [\![\varphi]\!]^{\mathcal{M}}_{\mathbf{no}})$. As we discuss below, the basic framework in [12] gives rise to a particular solution to our problem of two-sided approximate model-checking: given a standard Kripke model $\mathcal{M}$ that is abstracted under a suitable *mixed simulation relation* by a bi-relational "must-may" Kripke model $\mathcal{N}$, an under-approximation set $Un^{\mathcal{M}}(\varphi)$ can be obtained from $[\![\varphi]\!]^{\mathcal{N}}_{\mathbf{yes}}$ and an over-approximation set $Ov^{\mathcal{M}}(\varphi)$ can be obtained from the set-complement of $[\![\varphi]\!]^{\mathcal{N}}_{\mathbf{no}}$. The main results in [4, 6, 12] all assume that one has available an explicit first-order description of the true transition relation R on the concrete model $\mathcal{M}$, with exact point-wise knowledge of R. While these are reasonable assumptions for the very large but still finite state systems considered in these papers, they are quite restrictive in the setting of hybrid and real-time systems.

Technically, we develop a simple set-theoretic notion of a *finite approximation scheme* (f.a.s.) for μ-calculus formulas interpreted in a Kripke model, and establish the naturalness of our notion by showing that a model has a maximally refined f.a.s. if and only if it has a finite bisimulation quotient. We then give a general construction of an f.a.s. for a Kripke model from the topology generated from a finite cover or discretization of the state space under an A/D-map. In contrast to [4, 6, 12], we do not assume exact point-wise knowledge of the concrete transition relation R in order to construct approximations of the modal/tense operators; instead, we make do with a weaker assumption of having under- and over-approximations of the R-reachability (post-image) operator applied to the cells of the A/D map, which fits much better with current algorithms for approximating sets of reachable states in papers such as [1–3, 10]. We conclude the paper by proving a comprehensiveness result that every f.a.s. satisfying natural coherence conditions can be refined to give a topological f.a.s..

Structure of paper: Section 2 contains preliminaries from mathematics and logic. In Section 3, we formulate a general notion of a finite approximation scheme, and of refinements of schemes. Section 4 gives the basics of covers, A/D maps, and their Alexandroff topologies. The main results are in Section 5, and Section 6 gives a brief summary and discussion.

2 Preliminaries

2.1 Mathematical preliminaries

We write $r : X \rightsquigarrow Y$ to mean both that $r : X \to 2^Y$ is a *set-valued map*, with (possibly empty) set-values $r(x) \subseteq Y$ for each $x \in X$, and equivalently, that $r \subseteq X \times Y$ is a *relation*. (Total and single-valued) functions $r : X \to Y$ are a special case of set-valued maps. We write $r^{-1} : Y \rightsquigarrow X$ for the relational inverse/converse; $dom(r) := \{x \in X \mid r(x) \neq \varnothing\}$ and $ran(r) := dom(r^{-1})$. For maps $r_1 : X \rightsquigarrow Y$ and $r_2 : Y \rightsquigarrow Z$, we write their relational composition as $r_1 \bullet r_2 : X \rightsquigarrow Z$ given by $(r_1 \bullet r_2)(x) := \{z \in Z \mid (\exists y \in Y)\,[y \in r_1(x) \wedge z \in r_2(y)]\}$, in sequential left-to-right application order.

A relation $r : X \rightsquigarrow Y$ determines two *pre-image operators* (predicate transformers): the *existential* pre-image function $r^{-\exists} : 2^Y \to 2^X$ and the set-theoretic dual *universal* pre-image $r^{-\forall} : 2^Y \to 2^X$. Formally,

$$r^{-\exists}(W) := \{x \in X \mid W \cap r(x) \neq \varnothing\}$$
$$r^{-\forall}(W) := X - r^{-\exists}(Y - W) \;=\; \{x \in X \mid r(x) \subseteq W\}$$

for $W \subseteq Y$. The corresponding adjoint pair of *post-image operators* $r^{\forall}, r^{\exists} : 2^X \to 2^Y$ are given by $r^{\forall} := (r^{-1})^{-\forall}$ and $r^{\exists} := (r^{-1})^{-\exists}$, respectively. The adjoint relationships are: $r^{-\exists}(W) \subseteq V$ iff $W \subseteq r^{\forall}(V)$ and $r^{\exists}(V) \subseteq W$ iff $V \subseteq r^{-\forall}(W)$, for all $V \subseteq X$ and $W \subseteq Y$.

Recall that a *topology* $\mathcal{T} \subseteq 2^X$ on a set X is a family of subsets of X that is closed under arbitrary unions and finite intersections. So $\mathcal{T}$ is a distributive lattice of sets. The *interior operator* $int_{\mathcal{T}} : 2^X \to 2^X$ determined by $\mathcal{T}$ is given by $int_{\mathcal{T}}(W) := \bigcup \{U \in \mathcal{T} \mid U \subseteq W\}$. Sets $W \in \mathcal{T}$ are called *open* w.r.t. $\mathcal{T}$, and

this is so iff $W = int_{\mathcal{T}}(W)$. A sub-family of open sets $\mathcal{B} \subseteq \mathcal{T}$ constitutes a *basis* for the topology $\mathcal{T}$ on X if every open set $W \in \mathcal{T}$ is a union of basic opens in $\mathcal{B}$, and for every $x \in X$ and every pair of basic opens $U_1, U_2 \in \mathcal{B}$ such that $x \in U_1 \cap U_2$, there exists $U_3 \in \mathcal{B}$ such that $x \in U_3 \subseteq (U_1 \cap U_2)$.

A topology $\mathcal{T}$ on X is called Alexandroff if for every $x \in X$, there is a *smallest* open set $U \in \mathcal{T}$ such that $x \in U$. In particular, every *finite* topology (i.e. only finitely many open sets) is Alexandroff. There is a one-to-one correspondence between pre-orders on X and Alexandroff topologies on X. Any pre-order $\preccurlyeq$ on X induces an Alexandroff topology $\mathcal{T}_{\preccurlyeq}$ by taking $int_{\mathcal{T}_{\preccurlyeq}}(W) := (\preccurlyeq)^{-\forall}(W)$, which means $U \in \mathcal{T}_{\preccurlyeq}$ iff U is upwards-$\preccurlyeq$-closed, and V is closed in $\mathcal{T}_{\preccurlyeq}$ iff V is downwards-$\preccurlyeq$-closed, and $cl_{\mathcal{T}_{\preccurlyeq}}(W) = (\preccurlyeq)^{-\exists}(W)$. Conversely, for any topology, define a pre-order $\preccurlyeq_{\mathcal{T}}$ on X, known as the *specialisation pre-order*: $x \preccurlyeq_{\mathcal{T}} y$ iff $(\forall U \in \mathcal{T})\,[x \in U \Rightarrow y \in U]$. For any pre-order, $\preccurlyeq_{\mathcal{T}_{\preccurlyeq}} = \preccurlyeq$, and for any topology, $\mathcal{T}_{\preccurlyeq_{\mathcal{T}}} = \mathcal{T}$ iff $\mathcal{T}$ is Alexandroff.

Given two topological spaces $(X, \mathcal{T})$ and $(Y, \mathcal{S})$, a relation $R : X \rightsquigarrow Y$ is called: *lower semi-continuous* (l.s.c.) if for every $\mathcal{S}$-open set U in Y, $R^{-\exists}(U)$ is $\mathcal{T}$-open in X; *upper semi-continuous* (u.s.c.) if for every $\mathcal{S}$-open set U in Y, $R^{-\forall}(U)$ is $\mathcal{T}$-open in X; and *continuous* if it is both l.s.c. and u.s.c. [9].

2.2 Logic preliminaries: syntax

Fix a finite set P of atomic propositions, and let *Var* be a countable set of propositional variables. Let $\mathcal{F}^{\mathrm{t}}_{\mu}(P)$ be the μ-calculus (fixed-point) language generated by the grammar:

$$\varphi \ ::= \ p \mid z \mid \bot \mid \top \mid \neg\varphi \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \wedge \varphi_2 \mid \diamondsuit\varphi \mid \blacklozenge\varphi \mid \mu z.\varphi$$

where $p \in P$, $z \in \mathit{Var}$, and a least fixed-point formula $\mu z.\varphi$ is well-formed only when every occurrence of the variable z within φ occurs within the scope of an even number of negations. A formula φ is a *sentence* of the language $\mathcal{F}^{\mathrm{t}}_{\mu}(P)$ if every occurrence of a propositional variable in φ is bound by (within the scope of) a fixed-point operator μ; let $\mathcal{L}^{\mathrm{t}}_{\mu}(P)$ denote the set of all such sentences.

The superscript $^{\mathrm{t}}$ indicates our use of *tense logic*, with the temporally dual *future* and *past* modal diamond operators $\diamondsuit$ and $\blacklozenge$ operators, respectively, and their negation-dual box operators $\boxdot\varphi := \neg\diamondsuit\neg\varphi$ and $\blacksquare\varphi := \neg\blacklozenge\neg\varphi$. A formula $\diamondsuit\varphi$ is read "*At some state in the future, φ will hold*", while $\blacklozenge\varphi$ is read "*At some state in the past, φ has held*".

For formulas $\varphi, \psi \in \mathcal{F}^{\mathrm{t}}(P)$, and propositions $p \in P$, we write $\varphi[p := \psi]$ to mean the formula resulting from the simultaneous substitution of ψ for each occurrence of p in φ. Likewise, for propositional variables $z \in \mathit{Var}$, we write $\varphi[z := \psi]$ to mean the formula resulting from the simultaneous substitution of ψ for each occurrence of z in φ that is not bound by a μ, and with preliminary renaming of any occurrences of z in ψ that are bound by a μ. The μ operator is a *least* fixed-point constructor, and its dual *greatest* fixed-point constructor ν is defined by $\nu z.\varphi := \neg\mu z.\neg\varphi[z := \neg z]$.

2.3 Logic preliminaries: semantics

A *Kripke model* for the language $\mathcal{F}^{\mathrm{t}}_{\mu}(P)$ is a structure $\mathcal{M} = (X, R, v)$, where X is any non-empty set, $R : X \rightsquigarrow X$ is a binary relation, and $v : P \rightsquigarrow X$ is a set-valued map (atomic valuation). A *variable assignment* in $\mathcal{M}$ is a set-valued map $\xi : \mathit{Var} \rightsquigarrow X$. A model $\mathcal{M}$ and a variable assignment ξ together determine the (classical, two-valued) *denotation map* $[\![\cdot]\!]^{\mathcal{M}}_{\xi} : \mathcal{F}^{\mathrm{t}}_{\mu}(P) \rightsquigarrow X$, defined by induction on formulas:

$$
\begin{array}{rcl@{\qquad}rcl}
[\![p]\!]^{\mathcal{M}}_{\xi} & := & v(p) & [\![z]\!]^{\mathcal{M}}_{\xi} & := & \xi(z) \\
[\![\bot]\!]^{\mathcal{M}}_{\xi} & := & \varnothing & [\![\top]\!]^{\mathcal{M}}_{\xi} & := & X \\
[\![\neg\, \varphi]\!]^{\mathcal{M}}_{\xi} & := & X - [\![\varphi]\!]^{\mathcal{M}}_{\xi} & & & \\
[\![\varphi_1 \vee \varphi_2]\!]^{\mathcal{M}}_{\xi} & := & [\![\varphi_1]\!]^{\mathcal{M}}_{\xi} \cup [\![\varphi_2]\!]^{\mathcal{M}}_{\xi} & [\![\varphi_1 \wedge \varphi_2]\!]^{\mathcal{M}}_{\xi} & := & [\![\varphi_1]\!]^{\mathcal{M}}_{\xi} \cap [\![\varphi_2]\!]^{\mathcal{M}}_{\xi} \\
[\![\diamondsuit \varphi]\!]^{\mathcal{M}}_{\xi} & := & R^{-\exists}([\![\varphi]\!]^{\mathcal{M}}_{\xi}) & [\![\blacklozenge \varphi]\!]^{\mathcal{M}}_{\xi} & := & R^{\exists}([\![\varphi]\!]^{\mathcal{M}}_{\xi})
\end{array}
$$

$$
[\![\mu z.\varphi]\!]^{\mathcal{M}}_{\xi} := \bigcap \{\, W \in 2^X \mid [\![\varphi]\!]^{\mathcal{M}}_{\xi[z/W]} \subseteq W \,\}
$$

where $\xi[z/W]$ is the assignment that is the same as ξ except for assigning the set W to the variable z. For sentences $\varphi \in \mathcal{L}^{\mathrm{t}}_{\mu}(P)$, the denotation set is independent of the variable assignment: $[\![\varphi]\!]^{\mathcal{M}}_{\xi_1} = [\![\varphi]\!]^{\mathcal{M}}_{\xi_2}$ for any two assignments $\xi_1, \xi_2 : \mathit{Var} \rightsquigarrow X$. Thus a model determines a (sentence) denotation map $[\![\cdot]\!]^{\mathcal{M}} : \mathcal{L}^{\mathrm{t}}_{\mu}(P) \rightsquigarrow X$ by $[\![\varphi]\!]^{\mathcal{M}} := [\![\varphi]\!]^{\mathcal{M}}_{\xi}$ for any assignment ξ. A sentence $\varphi \in \mathcal{L}^{\mathrm{t}}_{\mu}(P)$ is *true* (respectively, *satisfiable*) in a model $\mathcal{M}$ if $[\![\varphi]\!]^{\mathcal{M}} = X$ (respectively, $[\![\varphi]\!]^{\mathcal{M}} \neq \varnothing$).

Let $\mathcal{M} = (X, R, v)$ and $\mathcal{N} = (Z, S, u)$ be two Kripke models for the tense language $\mathcal{F}^{\mathrm{t}}_{\mu}(P)$. A relation $h : X \rightsquigarrow Z$ constitutes a *simulation* (respectively, *tense simulation*) of model $\mathcal{M}$ by model $\mathcal{N}$ if:

- the set inclusion $h^{\exists}(v(p)) \subseteq u(p)$ holds for each $p \in P$, and
- the relational inclusion $(h^{-1} \bullet R) \subseteq (S \bullet h^{-1})$ holds (respectively, the relational inclusion $(R \bullet h) \subseteq (h \bullet S)$ also holds).

A relation $h : X \rightsquigarrow Z$ is a *bisimulation* (respectively, *tense bisimulation*) between models $\mathcal{M}$ and $\mathcal{N}$ if $h : X \rightsquigarrow Z$ is a simulation (respectively, tense simulation) of $\mathcal{M}$ by $\mathcal{N}$, and additionally $h^{-1} : Z \rightsquigarrow X$ is a simulation (respectively, tense simulation) of $\mathcal{N}$ by $\mathcal{M}$. In particular, for a single model $\mathcal{M} = (X, R, v)$, if h is an equivalence relation on X, then h is a tense bisimulation between $\mathcal{M}$ and itself iff for each equivalence class V of h, both $R^{-\exists}(V)$ and $R^{\exists}(V)$ are (possibly empty) unions of h-equivalence classes, and for each atomic $p \in P$, the set $v(p)$ is a (possibly empty) union of h-equivalence classes.

2.4 Logic preliminaries: three-valued semantics

Let $\mathbb{T} := \{\mathbf{yes}, \mathbf{no}, \mathbf{indf}\}$ denote a set of three values, with partial order $\trianglelefteq$ defined by $\mathbf{indf} \trianglelefteq \omega$ and $\omega \trianglelefteq \omega$ for all $\omega \in \mathbb{T}$. A *three-valued must-may Kripke model* (in [7, 12], a *Kripke modal transition system* or *KMTS*) for the language $\mathcal{F}^{\mathrm{t}}_{\mu}(P)$ is a structure $\mathcal{M} = (X, R_{\mathrm{must}}, R_{\mathrm{may}}, v_{\mathbf{yes}}, v_{\mathbf{no}})$, where X is any non-empty set, R_{must} and R_{may} are two binary relations on X with $R_{\mathrm{must}} \subseteq R_{\mathrm{may}}$, and $v_{\mathbf{yes}}, v_{\mathbf{no}} : P \rightsquigarrow X$ are atomic valuations such that $v_{\mathbf{yes}}(p) \cap v_{\mathbf{no}}(p) = \varnothing$. A (standard)

Kipke model $\mathcal{M} = (X, R, v)$ can be viewed as a three-valued must-may Kripke model in which $R = R_{\text{must}} = R_{\text{may}}$ and $v(p) = v_{\mathbf{yes}}(p) = X - v_{\mathbf{no}}(p)$. A three-valued Kripke model $\mathcal{M}$ naturally determines two standard Kripke models $\mathcal{M}_{un} := (X, R_{\mathbf{must}}, v_{\mathbf{yes}})$ where $v_{un}(p) := v_{\mathbf{yes}}(p)$, and $\mathcal{M}_{ov} := (X, R_{\mathbf{may}}, v_{ov})$ where $v_{ov}(p) := X - v_{\mathbf{no}}(p)$, for all atomic $p \in P$.

Extending [12], §2.2, a three-valued must-may Kripke model $\mathcal{M}$ determines three sentence denotation maps $[\![\cdot]\!]^{\mathcal{M}}_{\omega} : \mathcal{L}^{\mathrm{t}}_{\mu}(P) \rightsquigarrow X$, one for each of the three values $\omega \in \mathbb{T}$, defined by induction on sentences:

$$
\begin{array}{rcl@{\qquad}rcl}
[\![p]\!]^{\mathcal{M}}_{\mathbf{yes}} & := & v_{\mathbf{yes}}(p) & [\![p]\!]^{\mathcal{M}}_{\mathbf{no}} & := & v_{\mathbf{no}}(p) \\
[\![\bot]\!]^{\mathcal{M}}_{\mathbf{yes}} & = & [\![\top]\!]^{\mathcal{M}}_{\mathbf{no}} := \varnothing & [\![\top]\!]^{\mathcal{M}}_{\mathbf{yes}} & = & [\![\bot]\!]^{\mathcal{M}}_{\mathbf{no}} := X \\
[\![\neg\varphi]\!]^{\mathcal{M}}_{\mathbf{yes}} & := & [\![\varphi]\!]^{\mathcal{M}}_{\mathbf{no}} & [\![\neg\varphi]\!]^{\mathcal{M}}_{\mathbf{no}} & := & [\![\varphi]\!]^{\mathcal{M}}_{\mathbf{yes}} \\
[\![\varphi_1 \vee \varphi_2]\!]^{\mathcal{M}}_{\mathbf{yes}} & := & [\![\varphi_1]\!]^{\mathcal{M}}_{\mathbf{yes}} \cup [\![\varphi_2]\!]^{\mathcal{M}}_{\mathbf{yes}} & [\![\varphi_1 \vee \varphi_2]\!]^{\mathcal{M}}_{\mathbf{no}} & := & [\![\varphi_1]\!]^{\mathcal{M}}_{\mathbf{no}} \cap [\![\varphi_2]\!]^{\mathcal{M}}_{\mathbf{no}} \\
[\![\varphi_1 \wedge \varphi_2]\!]^{\mathcal{M}}_{\mathbf{yes}} & := & [\![\varphi_1]\!]^{\mathcal{M}}_{\mathbf{yes}} \cap [\![\varphi_2]\!]^{\mathcal{M}}_{\mathbf{yes}} & [\![\varphi_1 \wedge \varphi_2]\!]^{\mathcal{M}}_{\mathbf{no}} & := & [\![\varphi_1]\!]^{\mathcal{M}}_{\mathbf{no}} \cup [\![\varphi_2]\!]^{\mathcal{M}}_{\mathbf{no}} \\
[\![\boxdot\varphi]\!]^{\mathcal{M}}_{\mathbf{yes}} & := & R^{-\exists}_{\mathbf{must}}([\![\varphi]\!]^{\mathcal{M}}_{\mathbf{yes}}) & [\![\boxdot\varphi]\!]^{\mathcal{M}}_{\mathbf{no}} & := & R^{-\forall}_{\mathbf{may}}([\![\varphi]\!]^{\mathcal{M}}_{\mathbf{no}}) \\
[\![\blacksquare\varphi]\!]^{\mathcal{M}}_{\mathbf{yes}} & := & R^{\exists}_{\mathbf{must}}([\![\varphi]\!]^{\mathcal{M}}_{\mathbf{yes}}) & [\![\blacksquare\varphi]\!]^{\mathcal{M}}_{\mathbf{no}} & := & R^{\forall}_{\mathbf{may}}([\![\varphi]\!]^{\mathcal{M}}_{\mathbf{no}}) \\
[\![\mu z.\varphi]\!]^{\mathcal{M}}_{\mathbf{yes}} & := & \bigcup_{\lambda<\eta_{\mathcal{M}}} W^{(\lambda)} & [\![\mu z.\varphi]\!]^{\mathcal{M}}_{\mathbf{no}} & := & \bigcap_{\lambda<\eta_{\mathcal{M}}} V^{(\lambda)}
\end{array}
$$

and $[\![\varphi]\!]^{\mathcal{M}}_{\mathbf{indf}} := X - ([\![\varphi]\!]^{\mathcal{M}}_{\mathbf{yes}} \cup [\![\varphi]\!]^{\mathcal{M}}_{\mathbf{no}})$ for all sentences $\varphi \in \mathcal{L}^{\mathrm{t}}_{\mu}(P)$. For the fixed-point constructor, one appeals as in [12] to the alternative iterative formulation of the Tarski fixed-point theorem for monotone operators on a complete lattice. The iteration bound $\eta_{\mathcal{M}}$ is the ordinal of the cardinality of 2^X; the affirming iteration sets $W^{(\lambda)}$ are defined by $W^{(0)} := \varnothing$, and $W^{(\eta)} := \bigcup_{\lambda<\eta} W^{(\lambda)}$ for limit ordinals $\eta \leq \eta_{\mathcal{M}}$, and for successor ordinals, $W^{(\lambda+1)} := \left([\![\varphi]\!]^{\mathcal{M}}_{\mathbf{yes}}\right)_{\xi}$, where ξ is any variable assignment such that $\xi(z) = W^{(\lambda)}$ (z is the *sole* free variable in φ). The refuting iteration sets $V^{(\lambda)}$ are defined by $V^{(0)} := X$, and $V^{(\eta)} := \bigcap_{\lambda<\eta} V^{(\lambda)}$ for limit ordinals $\eta \leq \eta_{\mathcal{M}}$, and for successor ordinals, $V^{(\lambda+1)} := ([\![\widetilde{\varphi}]\!]^{\mathcal{M}}_{\mathbf{no}})_{\xi}$, where ξ is any assignment such that $\xi(z) = V^{(\lambda)}$ and $\widetilde{\varphi} := \neg\varphi[z := \neg z]$.

Let $\mathcal{M} = (X, R_{\text{must}}, R_{\text{may}}, v_{\mathbf{yes}}, v_{\mathbf{no}})$ and $\mathcal{N} = (Z, S_{\text{must}}, S_{\text{may}}, u_{\mathbf{yes}}, u_{\mathbf{no}})$ be three-valued must-may Kripke models. A relation $h : X \rightsquigarrow Z$ is a *mixed simulation* (respectively, *mixed tense simulation*) of model $\mathcal{M}$ by model $\mathcal{N}$, or model $\mathcal{N}$ is a *three-valued abstraction* of $\mathcal{M}$ under h [7, 12] if: (a) $h : X \rightsquigarrow Z$ is a simulation (respectively, tense simulation) of $\mathcal{M}_{ov}$ by $\mathcal{N}_{ov}$; and (b) $h^{-1} : Z \rightsquigarrow X$ is a simulation (respectively, tense simulation) of $\mathcal{N}_{un}$ by $\mathcal{M}_{un}$. In particular, if $\mathcal{M} = (X, R, v)$ is a standard Kripke model, and $\mathcal{N}$ is a three-valued abstraction of $\mathcal{M}$ under mixed tense simulation $h : X \rightsquigarrow Z$, then for each $p \in P$, we have the two-sided approximation inclusions $h^{-\exists}(u_{\mathbf{yes}}(p) \subseteq v(p) \subseteq h^{-\forall}(Z - v_{\mathbf{no}}(p))$ for the atomic denotation sets $v(p)$ in the concrete model $\mathcal{M}$. Consequently, it follows by induction on sentences that if $\mathcal{N}$ is a *finite* three-valued abstraction of $\mathcal{M}$ under h, then for all μ-calculus sentences $\varphi \in \mathcal{L}^{\mathrm{t}}_{\mu}(P)$, we have:

$$h^{-\exists}([\![\varphi]\!]^{\mathcal{N}}_{\mathbf{yes}}) \;\subseteq\; [\![\varphi]\!]^{\mathcal{M}} \;\subseteq\; h^{-\forall}(Z - [\![\varphi]\!]^{\mathcal{N}}_{\mathbf{no}}) \tag{1}$$

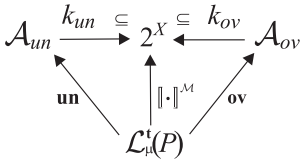
3 Finite approximation schemes for model-checking

We begin by developing a generic notion of a *scheme* for approximate evaluation of $[\![\varphi]\!]^{\mathcal{M}}$ which makes central the task of fulfilling the two-sided approximation inclusions.

Definition 1. [Schemes for approximate model-checking]
Given a Kripke model $\mathcal{M} = (X, R, v)$ for the language $\mathcal{F}^{\mathrm{t}}_{\mu}(P)$ generated from a finite set P of atomic propositions, a finite approximation scheme (f.a.s.) *for $\mathcal{M}$ over P is a pair of structures $\Sigma = (\Sigma_{un}, \Sigma_{ov})$ with $\Sigma_{un} = (\mathcal{A}_{un}, \mathbf{un}, k_{un})$ and $\Sigma_{ov} = (\mathcal{A}_{ov}, \mathbf{ov}, k_{ov})$, where $\mathcal{A}_{un}$ and $\mathcal{A}_{ov}$ are non-empty finite sets, and the functions $\mathbf{un} : \mathcal{L}^{\mathrm{t}}_{\mu}(P) \to \mathcal{A}_{un}$ and $k_{un} : \mathcal{A}_{un} \to 2^X$, and $\mathbf{ov} : \mathcal{L}^{\mathrm{t}}_{\mu}(P) \to \mathcal{A}_{ov}$ and $k_{ov} : \mathcal{A}_{ov} \to 2^X$, are such that for all sentences $\varphi \in \mathcal{L}^{\mathrm{t}}_{\mu}(P)$:*

$$k_{un}\,(\mathbf{un}(\varphi)) \quad \subseteq \quad [\![\varphi]\!]^{\mathcal{M}} \quad \subseteq \quad k_{ov}\,(\mathbf{ov}(\varphi)) \tag{2}$$

The following diagram indicates the types of the maps (but it is not a commutative diagram):



The idea is that elements $a \in \mathcal{A}_{un}$ or $a \in \mathcal{A}_{ov}$ are *abstract* or *symbolic* representatives for state sets $W \subseteq X$, and the *concretization* maps $k_{un} : \mathcal{A}_{un} \to 2^X$ and $k_{ov} : \mathcal{A}_{ov} \to 2^X$ realize or decode the abstract representation. The propositional and modal operators on sentences should be semantically interpreted via **un** and **ov** by functions on the finite sets $\mathcal{A}_{un}$ or $\mathcal{A}_{ov}$. More specifically, these functions should constitute the semantics of computer programs implementing specific approximation algorithms for the various operators/functions on 2^X: the Boolean set-theoretic operations and the relational pre-/post-image operators $R^{-\exists}, R^{\exists} : 2^X \to 2^X$, and the least fixed points of $\subseteq$-monotone operators $F : 2^X \to 2^X$ built up from them.

Note that, as for the work on abstraction via three-valued must-may models in [7, 12], our two-sided approach of giving both under- and over-approximation values does provide substantial information about the unknown or unknowable denotation set $[\![\varphi]\!]^{\mathcal{M}}$. When we have values for both $k_{ov}\,(\mathbf{ov}(\varphi))$ and $k_{un}\,(\mathbf{un}(\varphi))$ from an f.a.s. Σ, then we know the true set $[\![\varphi]\!]^{\mathcal{M}}$ lies somewhere in between, and the set difference $k_{ov}\,(\mathbf{ov}(\varphi)) - k_{un}\,(\mathbf{un}(\varphi))$ is the set of all states in X at which the sentence φ does not have a determinate truth value under Σ. In contrast, if one has only a one-sided approximation scheme returning values $\mathit{Over}([\![\varphi]\!]^{\mathcal{M}})$ and satisfying the single inclusion $[\![\varphi]\!]^{\mathcal{M}} \subseteq \mathit{Over}([\![\varphi]\!]^{\mathcal{M}})$, then one has no further knowledge of accuracy when, *prima facie*, the exact set $[\![\varphi]\!]^{\mathcal{M}}$ is not known.

Clearly, there are better and worse approximation schemes, where the natural notion of "better" for a scheme is to return set values closer to that of the exact denotation set. We also identify further desirable properties of schemes, such as a scheme Σ behaving "reasonably" or "coherently".

Definition 2. *Given two finite approximation schemes* $\Sigma^1 = (\Sigma^1_{un}, \Sigma^1_{ov})$ *and* $\Sigma^2 = (\Sigma^2_{un}, \Sigma^2_{ov})$ *for a model* $\mathcal{M}$ *over* P*, we say that* Σ^2 *is a* refinement *of* Σ^1*, and we write* $\Sigma^1 \leqslant \Sigma^2$*, if for all sentences* $\varphi \in \mathcal{L}^{\mathrm{t}}_{\mu}(P)$*:*

$$k^1_{un}\left(\mathbf{un}^1(\varphi)\right) \subseteq k^2_{un}\left(\mathbf{un}^2(\varphi)\right) \subseteq [\![\,\varphi\,]\!]^{\mathcal{M}} \subseteq k^2_{ov}\left(\mathbf{ov}^2(\varphi)\right) \subseteq k^1_{ov}\left(\mathbf{ov}^1(\varphi)\right)$$

A refinement is proper*, written* $\Sigma^1 < \Sigma^2$*, if for some sentence* $\varphi \in \mathcal{L}^{\mathrm{t}}_{\mu}(P)$*, either* $k^1_{un}\left(\mathbf{un}^1(\varphi)\right) \subset k^2_{un}\left(\mathbf{un}^2(\varphi)\right)$*, or* $k^2_{ov}\left(\mathbf{ov}^2(\varphi)\right) \subset k^1_{ov}\left(\mathbf{ov}^1(\varphi)\right)$*.*
Two f.a. schemes Σ^1 *and* Σ^2 *will be called* bijectively equivalent *if there exist two bijective functions* $f_{un} : ran(\mathbf{un}^1) \to ran(\mathbf{un}^2)$ *and* $f_{ov} : ran(\mathbf{ov}^1) \to ran(\mathbf{ov}^2)$*, such that for all* $\varphi \in \mathcal{L}^{\mathrm{t}}_{\mu}(P)$*,* $k^1_{un}\left(\mathbf{un}^1(\varphi)\right) = k^2_{un}\left(f_{un}(\mathbf{un}^1(\varphi))\right)$*,* $k^2_{un}\left(\mathbf{un}^2(\varphi)\right) = k^1_{un}\left(f^{-1}_{un}(\mathbf{un}^2(\varphi))\right)$*,* $k^1_{ov}\left(\mathbf{ov}^1(\varphi)\right) = k^2_{ov}\left(f_{ov}(\mathbf{ov}^1(\varphi))\right)$*, and* $k^2_{ov}\left(\mathbf{ov}^2(\varphi)\right) = k^1_{ov}\left(f^{-1}_{ov}(\mathbf{ov}^2(\varphi))\right)$*.*
An f.a.s. Σ *is* non-degenerate *if both* $\mathcal{A}_{un}$ *and* $\mathcal{A}_{ov}$ *have at least two elements, and* $\mathbf{un}(\top) \neq \mathbf{un}(\bot)$ *and* $\mathbf{ov}(\top) \neq \mathbf{ov}(\bot)$*. A non-degenerate f.a.s.* Σ *is:*

- trivial *if both* $\mathcal{A}_{un}$ *and* $\mathcal{A}_{ov}$ *have exactly two elements;*
- extremal-coherent *if* $k_{un}\left(\mathbf{un}(\top)\right) = X$*, and* $k_{ov}\left(\mathbf{ov}(\bot)\right) = \varnothing$*;*
- full *if* $ran(\mathbf{un}) = \mathcal{A}_{un}$ *and* $ran(\mathbf{ov}) = \mathcal{A}_{ov}$*;*
- substitution-coherent *if for all sentences* $\varphi, \psi_1, \psi_2 \in \mathcal{L}^{\mathrm{t}}_{\mu}(P)$*, and all* $p \in P$*,*
  if $\mathbf{un}(\psi_1) = \mathbf{un}(\psi_2)$ *then* $\mathbf{un}\left(\varphi[p := \psi_1]\right) = \mathbf{un}\left(\varphi[p := \psi_2]\right)$*, and*
  if $\mathbf{ov}(\psi_1) = \mathbf{ov}(\psi_2)$ *then* $\mathbf{ov}\left(\varphi[p := \psi_1]\right) = \mathbf{ov}\left(\varphi[p := \psi_2]\right)$*;*
- exact *if* $k_{un}\left(\mathbf{un}(\varphi)\right) = [\![\,\varphi\,]\!]^{\mathcal{M}} = k_{ov}\left(\mathbf{ov}(\varphi)\right)$*, for all sentences* $\varphi \in \mathcal{L}^{\mathrm{t}}_{\mu}(P)$*.*

Henceforth, we will treat as equal any two schemes that are bijectively equivalent. Let $\mathsf{FAS}(\mathcal{M}, P)$ *denote the set of all extremal-coherent and substitution-coherent f.a.s. for* $\mathcal{M}$ *over* P*.*

The refinement relation $\leqslant$ defines a partial order on the set $\mathsf{FAS}(\mathcal{M}, P)$, under our standing convention of identifying bijectively equivalent schemes. There is a unique trivial f.a.s. $\Sigma_{\varnothing}$ that is non-degenerate, extremal-coherent, full, and substitution-coherent: each of $\mathcal{A}_{un}$ and $\mathcal{A}_{ov}$ have exactly two elements, and take $\mathbf{un}(\varphi) = \mathbf{un}(\bot)$ for all sentences $\varphi \neq \top$; $\mathbf{ov}(\varphi) = \mathbf{ov}(\top)$ for all sentences $\varphi \neq \bot$; $k_{un}\left(\mathbf{un}(\bot)\right) = \varnothing = k_{ov}\left(\mathbf{ov}(\bot)\right)$; and $k_{un}\left(\mathbf{un}(\top)\right) = X = k_{ov}\left(\mathbf{ov}(\top)\right)$. This scheme $\Sigma_{\varnothing}$ is the $\leqslant$-minimal element of the set $\mathsf{FAS}(\mathcal{M}, P)$.

Regarding $\leqslant$-maximal schemes in $\mathsf{FAS}(\mathcal{M}, P)$, it is intuitively plausible that any scheme short of exact can always be further refined. The following result confirms the intuition: having an exact scheme is equivalent to having a finite bisimulation quotient.

Proposition 1. *For a model* $\mathcal{M}$ *over* P*, the following are equivalent:*
(**a**.) *there is an* $\leqslant$*-maximal scheme in* $\mathsf{FAS}(\mathcal{M}, P)$*;*
(**b**.) *there is an exact scheme in* $\mathsf{FAS}(\mathcal{M}, P)$*;*
(**c**.) $\mathcal{M}$ *has a finite tense bisimulation quotient.*

So for infinite models $\mathcal{M}$ that don't have finite bisimulation quotients, there will no maximal schemes in $\mathsf{FAS}(\mathcal{M}, P)$ under the refinement partial order $\leqslant$. This is a typical situation for hybrid systems and real-time systems, where the state-space is the product of a finite set and a real vector space.

As noted in the introduction, and developed in Section 2.4 leading to Equation 1, abstraction via three-valued must-may Kripke models in [12, 7] naturally gives rise to a finite approximation scheme.

Proposition 2. *If Z is a finite set, and $\mathcal{N} = (Z, S_{\text{must}}, S_{\text{may}}, u_{\mathbf{yes}}, u_{\mathbf{no}})$ is a three-valued must-may Kripke model that gives an abstraction of a standard Kripke model $\mathcal{M} = (X, R, v)$ under map $h : X \rightsquigarrow Z$, then $\Sigma^{\mathcal{N}}$ is in $\mathsf{FAS}(\mathcal{M}, P)$, where $\Sigma^{\mathcal{N}} := (\Sigma^{\mathcal{N}}_{un}, \Sigma^{\mathcal{N}}_{ov})$ with $\Sigma^{\mathcal{N}}_{un} = (\mathcal{A}_{un}, \mathbf{un}, k_{un})$ and $\Sigma^{\mathcal{N}}_{ov} = (\mathcal{A}_{ov}, \mathbf{ov}, k_{ov})$, where: $\mathbf{un}(\varphi) := [\![\, \varphi \,]\!]^{\mathcal{N}}_{\mathbf{yes}}$, and $\mathbf{ov}(\varphi) := X - [\![\, \varphi \,]\!]^{\mathcal{N}}_{\mathbf{no}}$; $\mathcal{A}_{un} := ran(\mathbf{un}) \subseteq 2^Z$ and $\mathcal{A}_{ov} := ran(\mathbf{ov}) \subseteq 2^Z$; and $k_{un} := h^{-\exists}$ and $k_{ov} := h^{-\forall}$.*

In the remainder of the paper, we focus on finite approximation schemes that arise from *finite topologies* $\mathcal{T}$ on the state space X of the target concrete model $\mathcal{M}$. We say that $\Sigma \in \mathsf{FAS}(\mathcal{M}, P)$ is *topological* with respect to a topology $\mathcal{T}$ on X if for each sentence $\varphi \in \mathcal{L}^{\mathrm{t}}_{\mu}(P)$, the set $k_{un}(\mathbf{un}(\varphi))$ is $\mathcal{T}$-open, and $k_{un}(\mathbf{un}(\varphi)) \subseteq int_{\mathcal{T}}([\![\, \varphi \,]\!]^{\mathcal{M}})$, and on the other side, $k_{ov}(\mathbf{ov}(\varphi))$ is $\mathcal{T}$-closed, and $cl_{\mathcal{T}}([\![\, \varphi \,]\!]^{\mathcal{M}}) \subseteq k_{ov}(\mathbf{ov}(\varphi))$.

4 Covers, A/D maps and their Alexandroff topologies

An initial study of covers, A/D maps (*analog-to-digital* maps) and their topologies was made by Nerode and Kohn in [11]. In this section, we build on that work to develop just enough of the general topology of A/D maps and their Alexandroff spaces for use in addressing the task of building approximation schemes.

Definition 3. *A* cover *of a set X is any total relation $\alpha \colon X \rightsquigarrow S$. We call S the* index set *or* observation set *of the cover. The* cells *of α are the subsets $\alpha^{-1}(s)$ of X; define $\mathsf{Cells}(\alpha) := \{\alpha^{-1}(s) \in 2^X \mid s \in ran(\alpha)\}$. Let $\mathcal{T}_\alpha$ be the topology generated by α, i.e. the smallest subset of 2^X containing $\mathsf{Cells}(\alpha)$ and closed under arbitrary unions and finite intersections.*

The totality condition on α ensures that $X = \bigcup_{s \in S} \alpha^{-1}(s)$, so the cells of α do constitute a *cover* of X in the usual sense. In general, the α-cells constitute a *sub-basis* for the topology $\mathcal{T}_\alpha$; i.e. every open set is a union of finite intersections of α-cells. In the special case where $\alpha \colon X \to S$ is actually a function, then α can be thinned, by eliminating any excess elements of S, to give a surjective quotient map. In this case, the α-cells constitute a partition of X, and we have the "classical collapse" of $\mathcal{T}_\alpha$ to a complete Boolean algebra.

Definition 4. *Given covers $\alpha \colon X \rightsquigarrow S$ and $\beta \colon X \rightsquigarrow T$, we say α is* refined by *β, and write $\alpha \leqslant \beta$ if there exists a map $\theta : S \rightsquigarrow T$ such that $\alpha = \beta \bullet \theta^{-1}$.*

This means $\alpha \leqslant \beta$ iff each α-cell indexed by $s \in ran(\alpha)$ breaks up into a union of β-cells indexed by $t \in \theta(s)$: $\alpha^{-1}(s) = \bigcup\{\beta^{-1}(t) \mid t \in \theta(s)\}$. Thus $\alpha \leqslant \beta$ iff $\mathcal{T}_\alpha \subseteq \mathcal{T}_\beta$. The transfer map θ describes how each cell/observation s of the original α is broken up into a union of β cells or converted into a set of observations $\theta(s) \subseteq T$. So β allows us to make at least as many distinctions between states in X, as does α.

The refinement relation $\leqslant$ is a *pre-order* on the collection (proper class) of all covers of X. One can have *equi-refinements* $\alpha \leqslant \beta$ and $\beta \leqslant \alpha$ for distinct covers $\alpha\colon X \rightsquigarrow S$ and $\beta\colon X \rightsquigarrow T$, related by transfer maps $\theta_0 : S \rightsquigarrow T$ and $\theta_1 : T \rightsquigarrow S$ such that $\alpha = \alpha \bullet \theta_1^{-1} \bullet \theta_0^{-1}$ and $\beta = \beta \bullet \theta_0^{-1} \bullet \theta_1^{-1}$, and having the same topology $\mathcal{T}_\alpha = \mathcal{T}_\beta$ on X.

For any cover α, we can find a minimally coarse refinement α' such that $\mathcal{T}_\alpha = \mathcal{T}_{\alpha'}$ and the α'-cells constitute a basis for the topology $\mathcal{T}_\alpha$: take the closure under non-empty finite intersections of the family $\mathsf{Cells}(\alpha)$. In our application to finite discretization and approximation, our interest is in *finite* covers: if $\mathsf{Cells}(\alpha)$ has finite cardinality k, then for such a topological refinement α', the cardinality of $\mathsf{Cells}(\alpha')$ is bounded by $2^k - 1$, and the cardinality of $\mathcal{T}_\alpha = \mathcal{T}_{\alpha'}$ is bounded by 2^{2^k-1}.

Definition 5. *An* A/D map *on a set X is a cover $\alpha : X \rightsquigarrow \mathbb{N}$ such that the converse map α^{-1} is injective and the family $\mathsf{Cells}(\alpha)$ is finite and constitutes a minimal basis for the topology $\mathcal{T}_\alpha$. Let $Z_\alpha := ran(\alpha) \subset \mathbb{N}$ be the finite range and let $A := \alpha^{-1} : \mathbb{N} \rightsquigarrow X$ denote the converse map, so $A(z) \subseteq X$ is the α-cell indexed by $z \in Z_\alpha$. Let $\mathsf{ADmap}(X)$ denote the set of all A/D maps on X.*

An A/D map α determines a topology $\mathcal{T}_\alpha$ on X that has only a finite number of open sets, and is thus Alexandroff. Further clarifying the definition, by *minimal basis* we mean that any proper sub-family of $\mathsf{Cells}(\alpha)$ fails to constitute a basis for $\mathcal{T}_\alpha$, which implies that no α-cell $A(z)$ is the union of two or more strictly smaller open sets of $\mathcal{T}_\alpha$. To see this, suppose otherwise, so $A(z) = U_1 \cup U_2$ where $U_1, U_2 \in \mathcal{T}_\alpha$ are both proper subsets of $A(z)$. Since $\mathsf{Cells}(\alpha)$ is a basis, each U_i is a union of basic opens in $\mathsf{Cells}(\alpha)$. But then $\mathsf{Cells}(\alpha) - \{A(z)\}$ will be a proper sub-family constituting a basis for $\mathcal{T}_\alpha$, contradicting the minimality of $\mathsf{Cells}(\alpha)$ as a basis. In particular, no α-cell is *disconnected*, by being a disjoint union of two smaller open sets of $\mathcal{T}_\alpha$. The requirement that $A = \alpha^{-1}$ be injective simply means that there is no redundancy in Z_α: $z \neq w$ implies $A(z) \neq A(w)$.

A pair of maps $\alpha, \beta \in \mathsf{ADmap}(X)$ are equi-refinements $\alpha \leqslant \beta$ and $\beta \leqslant \alpha$ iff there exists a bijective function $\tau : Z_\alpha \to Z_\beta$ such that $A(z) = B(\tau(z))$ and $B(w) = A(\tau^{-1}(w))$ for all $z \in Z_\alpha$ and $w \in Z_\beta$. Hence we can consider the set $\mathsf{ADmap}(X)$ to be *partially ordered* by the refinement relation $\leqslant$, up to re-labeling of cell indices via bijective functions.

In signal processing, analog-to-digital conversion is almost invariably modeled by a finite partition of the analog state space. This gives single-valued and total functions $\alpha : X \to \mathbb{N}$ with finite range, where the α-cells are partition blocks (and so will trivially form a minimal basis for the Boolean algebra $\mathcal{T}_\alpha$). One of the arguments in [11] is that in looking for *continuity* in the process of analog-to digital conversion, one won't find it in the Euclidean topology on the analog state space, so look instead at the finite topology on that space generated by the cells of an A/D map. The definition of an A/D map here is essentially equivalent to that in [11], which also briefly considers the non-finite case; there, a *generalized A/D map* has as its cells the fully join-irreducible elements in the lattice of open sets of an Alexandroff topology, which is equivalent to requiring the cells form a minimal basis.

For $\alpha \in \mathsf{ADmap}(X)$, we will write $\preccurlyeq_\alpha$ and $\approx_\alpha$, respectively, for the pre-order $\preccurlyeq_{\mathcal{T}_\alpha}$ on X, and equivalence relation $\approx_{\mathcal{T}_\alpha} := (\preccurlyeq_{\mathcal{T}_\alpha} \cap \succcurlyeq_{\mathcal{T}_\alpha})$ on X determined by $\mathcal{T}_\alpha$. We will also write int_α and cl_α for $int_{\mathcal{T}_\alpha}$ and $cl_{\mathcal{T}_\alpha}$. Let $s_\alpha : X \to X/\approx_\alpha$ be the Stone T_0 quotient map $s_\alpha(x) := [x]_{\approx_\alpha}$ mapping x to its topological equivalence class $[x]_{\approx_\alpha} \subseteq X$. The following result gives clean characterizations of the $\approx_\alpha$-classes, and of the topological operators int_α and cl_α.

Proposition 3. *Let $\alpha : X \rightsquigarrow Z_\alpha$ be any non-trivial A/D map on X.*

(1.) The function $F : X/\approx_\alpha \to Z_\alpha$ defined by

$$F(s_\alpha(x)) = z \quad \textit{iff} \quad s_\alpha(x) = A(z) - \bigcup\{\, A(w) \mid A(w) \subset A(z) \,\}$$

is a bijection, hence the function $q_\alpha : X \to Z_\alpha$ defined by $q_\alpha(x) := F(s_\alpha(x))$ is surjective. Let $Q_\alpha := q_\alpha^{-1} : Z_\alpha \rightsquigarrow X$ denote the converse map. Then for all $z \in Z_\alpha$, we have $Q_\alpha(z) \subseteq A(z)$, and $Q_\alpha(z)$ is the $\approx_\alpha$ partition block with the property that $x \in Q_\alpha(z)$ iff $A(z)$ is the smallest α-cell containing x.

(2.) The finite quotient space $(Z_\alpha, \mathcal{T}_\mathrm{q})$ under the surjection $q_\alpha : X \to Z_\alpha$ from $(X, \mathcal{T}_\alpha)$ has as its specialization pre-order $z \sqsubseteq w$ iff $A(w) \subseteq A(z)$.

(3.) For each $z \in Z_\alpha$, the α-cell $A(z)$ satisfies $A(z) = \bigcup\{\, Q_\alpha(w) \mid z \sqsubseteq w \,\}$; equivalently, $\alpha = \sqsubseteq \bullet q_\alpha$ and $A = Q_\alpha \bullet \sqsupseteq$.

(4.) The topological operators of $\mathcal{T}_\alpha$ are expressible in terms of unions of $\approx_\alpha$ equivalence classes. Specifically, for subsets $W \subseteq X$:

$$\begin{aligned} int_\alpha(W) &= \bigcup\{\, Q_\alpha(z) \mid A(z) \subseteq W \,\} \\ cl_\alpha(W) &= \bigcup\{\, Q_\alpha(z) \mid A(z) \cap W \neq \varnothing \,\} \\ bd_\alpha(W) &= \bigcup\{\, Q_\alpha(z) \mid A(z) \cap W \neq \varnothing \text{ and } A(z) \cap (X - W) \neq \varnothing \,\} \end{aligned} \tag{3}$$

(5.) The maps have the following semi-continuity properties respect to $(X, \mathcal{T}_\alpha)$ and $(Z_\alpha, \mathcal{T}_\mathrm{q})$:

- *$q_\alpha : X \to Z_\alpha$ is both l.s.c. and u.s.c., and a continuous function;*
- *$Q_\alpha = q_\alpha^{-1} : Z_\alpha \rightsquigarrow X$ is both l.s.c. and u.s.c., and thus continuous;*
- *$\alpha : X \rightsquigarrow Z_\alpha$ is l.s.c.; and*
- *$A = \alpha^{-1} : Z_\alpha \rightsquigarrow X$ is u.s.c.*

In Figure 1, we illustrate an A/D map α on a bounded region of $\mathbb{R}^2$, where the α-cells $A(z)$ consist of the following four types of sets:

basic larger squares:	$\mathbf{Sq}(i,j)$	for $i < 9$ and $j < 14$
horizontal overlaps:	$\mathbf{HO}(i,j) := \mathbf{Sq}(i,j) \cap \mathbf{Sq}(i,j+1)$	for $i < 9$ and $j < 13$
vertical overlaps:	$\mathbf{VO}(i,j) := \mathbf{Sq}(i,j) \cap \mathbf{Sq}(i+1,j)$	for $i < 8$ and $j < 14$
diagonal overlaps:	$\mathbf{DO}(i,j) := \mathbf{HO}(i,j) \cap \mathbf{VO}(i,j)$	for $i < 8$ and $j < 13$

Take the index set $Z_\alpha \subset \mathbb{N}$ to be the result of some coding of pairs and pairs of pairs. For this example, Z_α has cardinality 459; more generally, for a regular cover α of a bounded region of $\mathbb{R}^2$ such as this, of size $N \times M$, the cardinality of Z_α will be at most $3k^2$, where $k = \max\{N, M\}$.

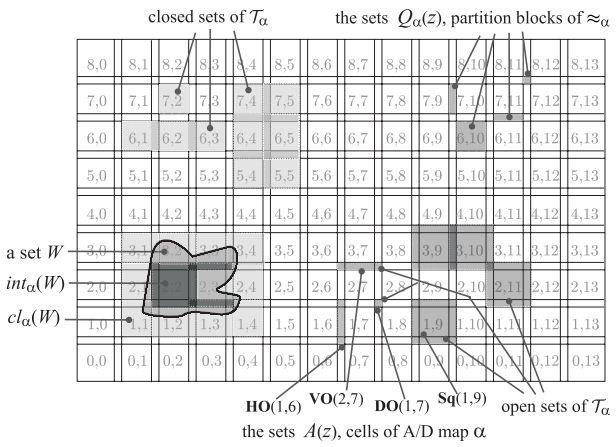


Fig. 1. *Example of A/D map α from regular cover of bounded region of $\mathbb{R}^2$.*

5 Topological f.a.s. from A/D maps

We will use an A/D map α and its topology $\mathcal{T}_\alpha$ to construct a topological finite approximation scheme Σ^α for a concrete Kripke model $\mathcal{M} = (X, R, v)$. To satisfy the conditions that $k_{un}(\mathbf{un}(\varphi))$ is $\mathcal{T}_\alpha$-open and $k_{ov}(\mathbf{ov}(\varphi))$ is $\mathcal{T}_\alpha$-closed, we will need to enforce various semi-continuity properties on relations $S_{un}, S_{ov} : Z_\alpha \rightsquigarrow Z_\alpha$ used in the approximation of R modal/tense operators, and need to draw on semi-continuity properties established in Proposition 3.

In what follows, we are given a model $\mathcal{M} = (X, R, v)$, and we need to have available an A/D map $\alpha \in \mathsf{ADmap}(X)$ and a pair of operators on sets $upo_\alpha, opo_\alpha : \mathsf{Cells}(\alpha) \to 2^X$ such that $upo_\alpha(A(z)) \subseteq R^\exists(A(z)) \subseteq opo_\alpha(A(z))$ for every α-cell $A(z) \in \mathsf{Cells}(\alpha)$. Moreover, we must be able to determine by finite computation whether $A(w) \subseteq upo_\alpha(A(z))$ and whether $A(w) \cap opo_\alpha(A(z)) \neq \varnothing$. So for example, if all the cells of the A/D map as well as the approximated values of upo_α and opo_α on cells are all first-order definable in a decidable structure (such as $\mathbb{R}$ as a real-closed field), then the computational pre-conditions will be met.

Definition 6. *For a Kripke model $\mathcal{M} = (X, R, v)$ over P, a triple $(\alpha, upo_\alpha, opo_\alpha)$ will be called* A/D adequate *if $\alpha : X \rightsquigarrow Z_\alpha$ is a non-degenerate A/D map on X, and the operators on sets $upo_\alpha, opo_\alpha : \mathsf{Cells}(\alpha) \to 2^X$ satisfy:*

(i) *for all $p \in P$, either $v(p) = \varnothing$, or there exists $z \in Z_\alpha$ such that $A(z) \subseteq v(p)$;*

(ii) *for all $z, w \in Z_\alpha$, if $A(z) \subseteq A(w)$ (i.e. $w \sqsubseteq z$), then $upo_\alpha(A(z)) \subseteq upo_\alpha(A(w))$, and $opo_\alpha(A(z)) \subseteq opo_\alpha(A(w))$;*

(iii) *$upo_\alpha(A(z)) \subseteq R^\exists(A(z)) \subseteq opo_\alpha(A(z))$ for every α-cell $A(z) \in \mathsf{Cells}(\alpha)$;*

(iv) *for all $z, z', w \in Z_\alpha$, if $A(z') \subseteq A(z)$ and $A(w) \subseteq upo_\alpha(A(z))$, then there exists $w' \in Z_\alpha$ such that $A(w') \subseteq A(w) \cap upo_\alpha(A(z'))$.*

The first adequacy condition (i) says that α has to be fine enough to fit a cell inside every non-empty atomic denotation set. Condition (ii) asks that the operators upo_α and opo_α should be inclusion-monotone on α-cells, and (iii) requires

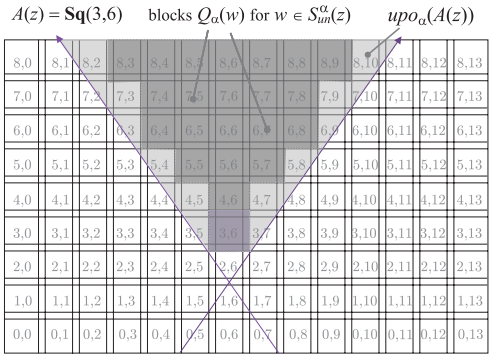


Fig. 2. *Finite relation S^α_{un} from A/D map α and known operator upo_α on α-cells.*

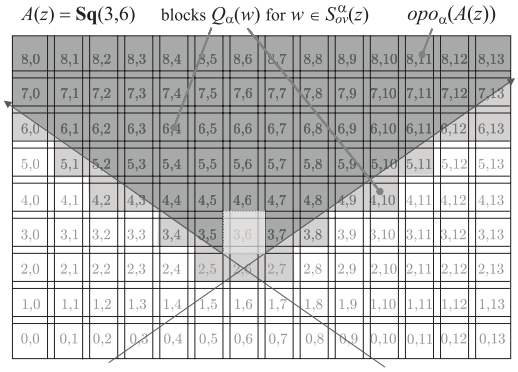


Fig. 3. *Finite relation S^α_{ov} from A/D map α and known operator opo_α on α-cells.*

that they give correct approximations of the post-image operator $R^\exists$ applied to α-cells. Condition (iv) amounts to asking for a semi-continuity property of a relation on the finite index set Z_α derived from upo_α.

Proposition 4. [Construction of finite approximating Kripke models]
Given a Kripke model $\mathcal{M} = (X, R, v)$ over P, suppose $(\alpha, upo_\alpha, opo_\alpha)$ is A/D adequate for $\mathcal{M}$. Define two finite Kripke models $\mathcal{N}^\alpha_{un} = (Z_\alpha, S^\alpha_{un}, u_{un})$ and $\mathcal{N}^\alpha_{ov} = (Z_\alpha, S^\alpha_{ov}, u_{ov})$ by:

$$S^\alpha_{un}(z) := \{w \in Z_\alpha \mid A(w) \subseteq upo_\alpha(A(z))\} \quad u_{ov}(p) := \{z \in Z_\alpha \mid A(z) \cap v(p) \neq \varnothing\}$$
$$S^\alpha_{ov}(z) := \{w \in Z_\alpha \mid A(w) \cap opo_\alpha(A(z)) \neq \varnothing\} \quad u_{un}(p) := \{z \in Z_\alpha \mid A(z) \subseteq v(p)\}$$

Consider the set Z_α equipped with the quotient topology $\mathcal{T}_\mathrm{q} = \mathcal{T}_\sqsubseteq$. Then the maps $S_{un} : Z_\alpha \rightsquigarrow Z_\alpha$ and $S^{-1}_{un} : Z_\alpha \rightsquigarrow Z_\alpha$ are both l.s.c. and each atomic set $u_{un}(p)$ is $\mathcal{T}_\mathrm{q}$-open, and the maps $S_{ov} : Z_\alpha \rightsquigarrow Z_\alpha$ and $S^{-1}_{ov} : Z_\alpha \rightsquigarrow Z_\alpha$ are both u.s.c. and each atomic set $u_{ov}(p)$ is $\mathcal{T}_\mathrm{q}$-closed.

In Figures 2 and 3, we illustrate the process of "blockifying" a pair of known approximating operators upo_α and opo_α through an A/D map α to produce the relations S^α_{un} and S^α_{ov} in the models $\mathcal{N}^\alpha_{un}$ and $\mathcal{N}^\alpha_{ov}$, as defined in Proposition 4.

Proposition 5. [Topological f.a.s. from A/D maps]
Given a Kripke model $\mathcal{M} = (X, R, v)$ for $\mathcal{L}^{\mathrm{t}}_\mu(P)$, suppose $(\alpha, upo_\alpha, opo_\alpha)$ is A/D adequate for $\mathcal{M}$, and let $\mathcal{N}^\alpha_{un} = (Z_\alpha, S^\alpha_{un}, u_{un})$ and $\mathcal{N}^\alpha_{ov} = (Z_\alpha, S^\alpha_{ov}, u_{ov})$ be the finite models defined in Proposition 4. Define two maps $\mathbf{un} : \mathcal{L}^{\mathrm{t}}_\mu(P) \to 2^{Z_\alpha}$ and $\mathbf{ov} : \mathcal{L}^{\mathrm{t}}_\mu(P) \to 2^{Z_\alpha}$ by mutual induction on sentences:

$$
\begin{array}{rcl@{\qquad}rcl}
\mathbf{un}(p) & := & u_{un}(p) & \mathbf{ov}(p) & := & u_{ov}(p) \\
\mathbf{un}(\bot) & := & \varnothing & \mathbf{ov}(\bot) & := & \varnothing \\
\mathbf{un}(\top) & := & Z_\alpha & \mathbf{ov}(\top) & := & Z_\alpha \\
\mathbf{un}(\neg\varphi) & := & Z_\alpha - \mathbf{ov}(\varphi) & \mathbf{ov}(\neg\varphi) & := & Z_\alpha - \mathbf{un}(\varphi) \\
\mathbf{un}(\varphi_1 \vee \varphi_2) & := & \mathbf{un}(\varphi_1) \cup \mathbf{un}(\varphi_2) & \mathbf{ov}(\varphi_1 \vee \varphi_2) & := & \mathbf{ov}(\varphi_1) \cup \mathbf{ov}(\varphi_2) \\
\mathbf{un}(\varphi_1 \wedge \varphi_2) & := & \mathbf{un}(\varphi_1) \cap \mathbf{un}(\varphi_2) & \mathbf{ov}(\varphi_1 \wedge \varphi_2) & := & \mathbf{ov}(\varphi_1) \cap \mathbf{ov}(\varphi_2) \\
\mathbf{un}(\diamondsuit\varphi) & := & (S^\alpha_{un})^{-\exists}(\mathbf{un}(\varphi)) & \mathbf{ov}(\diamondsuit\varphi) & := & (S^\alpha_{ov})^{-\exists}(\mathbf{ov}(\varphi)) \\
\mathbf{un}(\blacklozenge\varphi) & := & (S^\alpha_{un})^{\exists}(\mathbf{un}(\varphi)) & \mathbf{ov}(\blacklozenge\varphi) & := & (S^\alpha_{ov})^{\exists}(\mathbf{ov}(\varphi)) \\
\mathbf{un}(\mu z.\varphi) & := & \bigcup_{n \le K_\alpha} \mathbf{un}(\varphi^n) & \mathbf{ov}(\mu z.\varphi) & := & \bigcup_{n \le K_\alpha} \mathbf{ov}(\varphi^n)
\end{array}
$$

where $\varphi^0 := \bot$ and $\varphi^{n+1} := \varphi[z := \varphi^n]$ and the iteration bound is $K_\alpha := |\mathcal{T}_{\mathrm{q}}|$.

Then $\Sigma_\alpha := (\Sigma^\alpha_{un}, \Sigma^\alpha_{ov})$ is in $\mathsf{FAS}(\mathcal{M}, P)$, and is a topological f.a.s. with respect to the finite topology $\mathcal{T}_\alpha$ on X, where $\Sigma^\alpha_{un} := (\mathcal{T}_\sqsubseteq, \mathbf{un}, k^\alpha_{un})$ and $\Sigma^\alpha_{ov} := (\mathcal{T}_\sqsupseteq, \mathbf{ov}, k^\alpha_{ov})$, and $k^\alpha_{un} : \mathcal{T}_\sqsubseteq \to 2^X$ and $k^\alpha_{ov} : \mathcal{T}_\sqsupseteq \to 2^X$ are given by $k^\alpha_{un} := q^{-1}_\alpha$ and $k^\alpha_{ov} := q^{-1}_\alpha$.

In addition, if $\beta \in \mathsf{ADmap}(X)$, $\alpha \leqslant \beta$, $(\beta, upo_\beta, opo_\beta)$ is A/D adequate for $\mathcal{M}$, and $upo_\alpha(B(w)) \subseteq upo_\beta(B(w)) \subseteq R^\exists(B(w)) \subseteq opo_\beta(B(w)) \subseteq opo_\alpha(B(w))$ for all β-cells $B(w)$ for $w \in Z_\beta$, then $\Sigma_\alpha \leqslant \Sigma_\beta$.

This work emerged from a study by the authors of topological semantics for intuitionistic modal and tense logics, and their relationship under the *Gödel translation* to classical multi-modal logics equipped with additional **S4** modal operators $\Box$ and $\Diamond$ interpreted by topological interior and closure, respectively. In the light of this background, we are led to consider Gödel-inspired translation maps from the base language $\mathcal{L}^{\mathrm{t}}_\mu(P)$ into a multi-modal extension, which allows us to formally express and reason about not only the "real thing", but also our under- and over-approximations.

Let $\mathcal{L}^\star_\Box(P)$ be the multi-modal language which extends $\mathcal{L}^{\mathrm{t}}(P)$ (the tense language generated from P *without* the μ operator) by the addition of further pairs of tense diamonds, $\diamondsuit_\circ$ and $\blacklozenge_\circ$, and $\diamondsuit^\bullet$ and $\blacklozenge^\bullet$, and a plain box modality $\Box$. As before, we treat $\to$, $\Diamond$, and the now three pairs of tense box modalities $\boxdot$ and $\blacksquare$, $\boxdot_\circ$ and $\blacksquare_\circ$, and $\boxdot^\bullet$ and $\blacksquare^\bullet$, as all classically definable.

Proposition 6. *Given a Kripke model $\mathcal{M} = (X, R, v)$ over P, suppose the triple $(\alpha, upo_\alpha, opo_\alpha)$ is A/D adequate for $\mathcal{M}$, and let $\mathcal{N}^\alpha_{un} = (Z_\alpha, S^\alpha_{un}, u_{un})$, and $\mathcal{N}^\alpha_{ov} = (Z_\alpha, S^\alpha_{ov}, u_{ov})$ be the finite models defined in Proposition 4.*

Define a multi-relational topological model $\mathcal{M}^\star_\alpha := (X, \mathcal{T}_\alpha, R, R^\alpha_{un}, R^\alpha_{ov}, v)$ *for the language* $\mathcal{L}^\star_\Box(P)$*, with* int_α *interpreting* $\Box$*, relation* R *interpreting* $\diamondsuit$ *and* $\blacklozenge$*, and relations* R^α_{un} *interpreting* $\diamondsuit_\circ$ *and* $\blacklozenge_\circ$*, and* R^α_{ov} *interpreting* $\diamondsuit^\bullet$ *and* $\blacklozenge^\bullet$*, where:*

$$R^\alpha_{un} := q_\alpha \bullet S^\alpha_{un} \bullet q_\alpha^{-1} \qquad \textit{and} \qquad R^\alpha_{ov} := q_\alpha \bullet S^\alpha_{ov} \bullet q_\alpha^{-1}$$

Then there are two Gödel-like translation maps $\mathrm{UT}, \mathrm{OT}\colon \mathcal{L}^{\mathrm{t}}_\mu(P) \to \mathcal{L}^\star_\Box(P)$ *such that the approximation values generated by the f.a.s.* Σ_α *are (classically) expressible in* $\mathcal{L}^\star_\Box(P)$*, over the model* $\mathcal{M}^\star_\alpha$*, in the sense that, for all sentences* $\varphi \in \mathcal{L}^{\mathrm{t}}_\mu(P)$*:*

$$q_\alpha^{-1}(\mathbf{un}(\varphi)) = [\![\, \mathrm{UT}(\varphi) \,]\!]^{\mathcal{M}^\star_\alpha} \qquad \textit{and} \qquad q_\alpha^{-1}(\mathbf{ov}(\varphi)) = [\![\, \mathrm{OT}(\varphi) \,]\!]^{\mathcal{M}^\star_\alpha}$$
$$\mathcal{M}^\star_\alpha \models \mathrm{UT}(\varphi) \to \varphi \qquad \textit{and} \qquad \mathcal{M}^\star_\alpha \models \varphi \to \mathrm{OT}(\varphi)$$
$$\mathcal{M}^\star_\alpha \models \mathrm{UT}(\varphi) \leftrightarrow \Box\,\mathrm{UT}(\varphi) \qquad \textit{and} \qquad \mathcal{M}^\star_\alpha \models \mathrm{OT}(\varphi) \leftrightarrow \Diamond\,\mathrm{OT}(\varphi)$$

The mutually recursive translation maps are defined as follows:

$$\begin{array}{rlrl}
\mathrm{UT}(p) &:= \Box p & \mathrm{OT}(p) &:= \Diamond p \\
\mathrm{UT}(\bot) &:= \bot & \mathrm{OT}(\bot) &:= \bot \\
\mathrm{UT}(\top) &:= \top & \mathrm{OT}(\top) &:= \top \\
\mathrm{UT}(\neg\varphi) &:= \neg\,\mathrm{OT}(\varphi) & \mathrm{OT}(\neg\varphi) &:= \neg\,\mathrm{UT}(\varphi) \\
\mathrm{UT}(\varphi_1 \vee \varphi_2) &:= \mathrm{UT}(\varphi_1) \vee \mathrm{UT}(\varphi_2) & \mathrm{OT}(\varphi_1 \vee \varphi_2) &:= \mathrm{OT}(\varphi_1) \vee \mathrm{OT}(\varphi_2) \\
\mathrm{UT}(\varphi_1 \wedge \varphi_2) &:= \mathrm{UT}(\varphi_1) \wedge \mathrm{UT}(\varphi_2) & \mathrm{OT}(\varphi_1 \wedge \varphi_2) &:= \mathrm{OT}(\varphi_1) \wedge \mathrm{OT}(\varphi_2) \\
\mathrm{UT}(\diamondsuit\varphi) &:= \diamondsuit_\circ\,\mathrm{UT}(\varphi) & \mathrm{OT}(\diamondsuit\varphi) &:= \diamondsuit^\bullet\,\mathrm{OT}(\varphi) \\
\mathrm{UT}(\blacklozenge\varphi) &:= \blacklozenge_\circ\,\mathrm{UT}(\varphi) & \mathrm{OT}(\blacklozenge\varphi) &:= \blacklozenge^\bullet\,\mathrm{OT}(\varphi) \\
\mathrm{UT}(\mu z.\varphi) &:= \bigvee_{n \le K_\alpha} \mathrm{UT}(\varphi^n) & \mathrm{OT}(\mu z.\varphi) &:= \bigvee_{n \le K_\alpha} \mathrm{OT}(\varphi^n)
\end{array}$$

where the iteration bound is $K_\alpha = |\mathcal{T}_{\mathrm{q}}|$*.*

For example, in the extended language $\mathcal{L}^\star_\Box(P)$, the formula $\mathrm{OT}(\varphi) \wedge \neg\mathrm{UT}(\varphi)$ denotes in $\mathcal{M}^\star_\alpha$ the set of all states $x \in X$ that do not have a determinate truth value under the scheme Σ_α.

We conclude the paper with a comprehensiveness result: from any finite approximation scheme $\Sigma \in \mathsf{FAS}(\mathcal{M}, P)$, we can construct an A/D map α and a topological f.a.s. Σ_α that is a refinement of the given scheme Σ.

Proposition 7. [Comprehensiveness of topological finite approximation schemes] *Given any f.a.s.* $\Sigma \in \mathsf{FAS}(\mathcal{M}, P)$ *for a model* $\mathcal{M} = (X, R, v)$*, there exists an A/D map* $\alpha : X \rightsquigarrow Z_\alpha$*, and a pair of finite models* $\mathcal{N}^\alpha_{un} = (Z_\alpha, S^\alpha_{un}, u_{un})$ *and* $\mathcal{N}^\alpha_{ov} = (Z_\alpha, S^\alpha_{ov}, u_{ov})$ *which determine a topological finite approximation scheme* Σ_α*, as given in Proposition 5, such that* $\Sigma \leqslant \Sigma_\alpha$*.*
Moreover, the A/D map α *and the models* $\mathcal{N}^\alpha_{un}$ *and* $\mathcal{N}^\alpha_{ov}$ *are such that the construction and conclusions of Proposition 6 hold of them.*

6 Conclusions

This paper gives clear focus to the problem of approximate model-checking in modal and tense logics, calling for two-sided approximations propogated to arbitrarily complex formulas. We have developed a generic notion of a finite approximation scheme for a model, and of a partial ordering on such schemes, and we have established the naturalness of the notion by proving that a model has a maximally refined finite approximation scheme if and only if it has a finite bisimulation quotient. We then gave a general construction of finite approximation schemes from A/D maps and their finite topologies plus a pair of basic approximation operators defined on the cells of the A/D map. We showed this sub-class of topological schemes to be comprehensive in the sense that, given any finite approximation scheme Σ satisfying minimal coherence conditions, we can construct an A/D map α and a topological finite approximation scheme Σ_α that refines the given scheme Σ. Future work will investigate efficient implementation for reasonable classes of continuous dynamics based on [10, 1–3, 8].

References

1. R. Alur, T. Dang, and F. Ivancic. Progress on reachability analysis of hybrid systems. In *Hybrid Systems: Computation and Control* (HSCC'03), LNCS 2623, pages 20–35. Springer.
2. E. Asarin, T. Dang, and O. Maler. The d/dt tool for verification of hybrid systems. In *Computer Aided Verification 2002*, LNCS 2404, pages 365–370. Springer.
3. A. Chutinam and B. Krogh. Computational techniques for hybrid system verification. *IEEE Transactions on Automatic Control*, 48:64–75, 2003.
4. E. M. Clarke, O. Grumberg, and D. Long. Model checking and abstraction. *ACM Trans. on Prog. Lang. and Systems*, 16(5):1512–, 1994.
5. P. Cousot and R. Cousot. Abstract interpretation: a unified lattice model for static analysis of programs by construction of fixpoints. In *Proc. 4th ACM Symp on Principles of Prog Lang* (POPL'77), pages 238–252. ACM Press, 1977.
6. D.Dams, R.Gerth, and O.Grumberg. Abstract interpretation of reactive systems. *ACM Trans on Prog Langs and Systems (TOPLAS)*, 19(2), 1997.
7. P. Godefroid, M. Huth, and R. Jagadeesan. Abstraction-based model checking using modal transition systems. In *Proc International Conf on Concurrency* (CONCUR 2001), LNCS 2154, pages 426–440. Springer-Verlag, 2001.
8. B.H Krogh and O. Stursberg. Efficient representation and computation of reachable sets for hybrid systems. In *Hybrid Systems: Computation and Control* (HSCC'03), volume 2623 of *LNCS*, pages 498–513. Springer, 2003.
9. K. Kuratowski. *Topology.* Academic Press, 1966. (Vol 1, 1966; Vol 2, 1968.).
10. A.B. Kurzhanski and P. Varaiya. Reachability analysis for uncertain systems—the ellipsoidal technique. *Control and optimization. Dyn. Contin. Discrete Impuls. Syst. Ser. B Appl. Algorithms*, 9(3):347–367, 2002.
11. A. Nerode and W. Kohn. Models for hybrid systems: Automata, topologies, controllability, observability. In R. L. Grossman, editor, *Hybrid Systems* (HSI), LNCS 736, pages 297–316. Springer-Verlag, 1993.
12. S. Shoham and O. Grumberg. Monotonic abstraction-refinement for **CTL**. In *Proc Int Conf on Tools and Algorithms for the Construction and Analysis of Systems* (TACAS'04), LNCS 2988, pages 546 – 560. Springer, 2004.