Convex Lattice Equation Systems

Giorgio Bacci, Giovanni Bacci, Mathias C. Jensen, and Kim G. Larsen

Department of Computer Science, Aalborg University

Abstract. In this paper we revisit the paradigm shift *"From Boolean to Quantitative Notions of Correctness"* proposed by Henzinger more than 10 years ago. In particular, we present the notion of Convex Lattice Equation Systems as a universal framework for encoding and inferring behavioural metrics between quantitative system behaviours. We demonstrate how the framework may be applied to infer bounds on values of stochastic games and distances between timed systems.

1 Introduction

In the seminal talk "*From Boolean to Quantitative Notions of Correctness*" [Hen10] at POPL10, Henzinger challenged the classical Boolean treatment of systems and properties: e.g. a property is either true or false of a system. In particular, within the well-established research field of concurrent and reactive systems, so-called implementation verification involves checking the behavioural equivalence (or preorder) between implementations and specifications. This approach requires a suitable model of the system and specification, as well as procedure for checking whether the two are related with respect to the given equivalence or preorder. And again the verdict is either true or false.

The "*Embedded Design Challenge*" [HS06] presented by Henzinger and Sifakis in 2006, emphasizes the importance of quantitative models in order to capture in an adequate manner physical constraints, timing requirements and probabilistic uncertainties, etc. Even in this quantitative setting, the Boolean view has been prevalent: two timed automata are either (timed) bisimilar [Yi90] or not, two Markov chains are either (probabilistic) bisimilar [LS89] or not. There has been some research into better describing inconsistent models of systems by extending the *true*-*false* dichotomy to being part of some larger lattice structure. E.g. Easterbrook and Chechik develop a general framework for reasoning about such inconsistent viewpoints using multi-valued logics [EC01] and Kupferman and Lustig give a notion of *latticed* simulation for multi-valued Kripke structures [KL10].

The paradigm shift to quantitative notions of correctness, as advocated by Henzinger [Hen10], was motivated by the need of a more refined view, where a system if not fully correct may still be correct up to a certain degree, and where two systems if not fully equivalent may still be close according to a behavioural distance. The proposed paradigm shift to quantitative verdicts has been pursued by several researchers, leading – among others – to notions of timed bisimulation distances [HMP05,TFL10,Ros19], weighted bisimulation distances

$x_1 = x_1 \wedge x_1$

$x_2 = x_1 \vee x_3$

$x_3 = ff$

(a) BES $\mathcal{E}$

$$\mathbf{A_1}\ \frac{x \in \Gamma}{\Gamma \vdash_{\mathcal{E}} x} \qquad \mathbf{A_2}\ \frac{}{\Gamma \vdash_{\mathcal{E}} tt}$$

$$\mathbf{A_3}\ \frac{\Gamma, x \vdash_{\mathcal{E}} \phi}{\Gamma \vdash_{\mathcal{E}} x} x =_{\mathcal{E}} \phi, x \notin \Gamma$$

$$\mathbf{A_4}\ \frac{\Gamma \vdash_{\mathcal{E}} x \ \ \Gamma \vdash_{\mathcal{E}} y}{\Gamma \vdash_{\mathcal{E}} x \wedge y}$$

$$\mathbf{A_5}\ \frac{\Gamma \vdash_{\mathcal{E}} x}{\Gamma \vdash_{\mathcal{E}} x \vee y} \qquad \mathbf{A_6}\ \frac{\Gamma \vdash_{\mathcal{E}} y}{\Gamma \vdash_{\mathcal{E}} x \vee y}$$

(b) Proof System $\mathcal{A}$

$$\cfrac{\cfrac{\cfrac{x_1 \in \{x_1\}}{\{x_1\} \vdash x_1}\ \mathbf{A_1} \quad \cfrac{x_1 \in \{x_1\}}{\{x_1\} \vdash x_1}\ \mathbf{A_1}}{\{x_1\} \vdash_{\mathcal{E}} x_1 \wedge x_1}\ \mathbf{A_4}}{\emptyset \vdash_{\mathcal{E}} x_1}\ \mathbf{A_3}$$

(c) Proof of $\vdash_{\mathcal{E}} x$

Fig. 1. A BES, the proof system $\mathcal{A}$ and proof of $\vdash_{\mathcal{E}} x$ from [Lar92]

[FTL11,LFT11], and probabilistic bisimulation metrics [DLT08,DGJP04]. Here a key question has been the design of complete proof systems respectively effective procedures for inferring respectively computing the distance between (timed, weighted or probabilistic) models, e.g. [CvBW12,BBLM13a,BBLM13b,BBLM16] [BBLM18,BBL$^+$21]. However, in this effort one is facing the very same challenge as for the corresponding Boolean equivalence checking problems: the *state-space explosion problem.* That is, in many cases enumeration of the full state-space may be infeasible. To deal with this problem, the development of *on-the-fly* algorithms have been made in the hope that answers about the degree of equivalence between systems behaviour can be made by exploring only a fraction of the state-space.

The idea of local or on-the-fly model checking was discovered simultaneously and independently by various people in the end of the 1980s all engaged in making (Boolean) model-checking and equivalence-checking tools for various process algebras and tools (Concurrency Workbench CWB [CPS89], CADP [GLMS11], VESAR [ACD$^+$93], TAV-EPSILON [CGL93]). In this process, it was realized that a very simple formalism, Boolean Equation Systems (BES), can provide a universal framework for efficiently encoding and solving (essentially) all model-checking and equivalence problems in a local manner. In a BES, a finite number of Boolean variables are defined recursively (maximally or minimally) by Boolean expressions over the variables. Whereas [Lar92] provides a complete proof system and the first local algorithms, the work in [And92,LS98] provides the first optimal (linear-time) local algorithms. See Fig. 1 for a BES, the proof system and its application from [Lar92]. Later extensions and adaptations of BES have been implemented in the tools CADP, muCRL [Man08] and the educational tool CAAL [AAE$^+$15].

Aiming at providing the foundation for a similar universal framework for computing behavioural metrics in a local manner, we introduce in this paper the notion of *Convex Lattice Equation Systems* (CLES). Here, variables $\mathcal{X} = \{x_1, \ldots, x_n\}$ range over values from a convex (complete) lattice (generalizing Boolean as well as a range of numeric domains) and are defined recursively by expressions $\{E_1, \ldots, E_n\}$ over $\mathcal{X}$ involving lattice constructs (join and meet) and convex combinations. We present a sound and complete proof system for checking consistency of statements of the form $E \leq \varepsilon$, where E is an expression over $\mathcal{X}$ and ε is an element from the complete lattice expressing a bound. As for BES, this proof system will provide the basis of a generic on-the-fly algorithm. Finally, we show how values of stochastic games and distances between timed systems may be encoded using CLES over the complete lattices $([0,1], \leq)$ respectively $([0,\infty], \leq)$.

2 Convex Lattice Equation Systems

A *convex (complete) lattice* is a structure $\langle \mathbb{D}, \sqsubseteq, \{+_\alpha \mid \alpha \in [0,1]\}\rangle$ consisting of a complete partial order $(\mathbb{D}, \sqsubseteq)$ (hence, with joins $\bigsqcup D$ and meets $\bigsqcap D$ for arbitrary subsets $D \subseteq \mathbb{D}$) and a convex space $\langle \mathbb{D}, \{+_\alpha \mid \alpha \in [0,1]\}\rangle$, where $w +_\alpha w'$ denotes the binary convex combination of two elements $w, w' \in \mathbb{D}$, subject to the following distributive laws

$$\bigsqcup D +_\alpha w = \bigsqcup \{w' +_\alpha w \mid w' \in D\}$$
$$\bigsqcap D +_\alpha w = \bigsqcap \{w' +_\alpha w \mid w' \in D\}$$

When the partial order and convex structure of $\langle \mathbb{D}, \sqsubseteq, \{+_\alpha \mid \alpha \in [0,1]\}\rangle$ are clear from the context, we will refer to the convex lattice simply as $\mathbb{D}$.

Simple examples of convex lattices are the unit interval $[0,1]$ and the extended non-negative reals $[0,\infty]$, with order $\leq$ and convex combination interpreted as $a +_\alpha b = \alpha a + (1-\alpha) b$. A less trivial example of convex lattice is the space of convex sets of probability distributions which have been used in the literature to combine non-determinism and probabilistic choice (see e.g. [Mis00,Gou08,TKP09,VW06]).

Note that, if $\mathbb{D}$ is a convex lattice, also the set $\mathbb{D}^X$ of functions from X to $\mathbb{D}$ can be turned into a convex lattice $\langle \mathbb{D}^X, \dot{\sqsubseteq}, \{\dot{+}_\alpha \mid \alpha \in [0,1]\}\rangle$ by point-wise extension of the order and convex combinator:

$$\dot{\sqsubseteq} = \{(f,g) \mid \forall x \in X. f(x) \sqsubseteq g(x)\}\,, \qquad (f \mathbin{\dot{+}_\alpha} g)(x) = f(x) +_\alpha g(x)\,.$$

Remark 1. Any complete partial order $(\mathbb{D}, \sqsubseteq)$ can be also seen as a (trivial) convex lattice by simply interpreting the convex combination as

$$w +_\alpha w' = w \sqcup w' \quad (\text{for } \alpha \in (0,1))\,, \qquad w +_1 w' = w\,, \qquad w +_0 w' = w'\,.$$

This means that the theory we shall develop in the following sections can be applied also on complete partial orders with no (nontrivial) convex structure.

Hereafter, we fix a convex lattice $\langle \mathbb{D}, \sqsubseteq, \{+_\alpha \mid \alpha \in [0,1]\}\rangle$ and denote by $\top = \bigsqcup \mathbb{D}$ and $\bot = \bigsqcap \mathbb{D}$ its top and bottom elements, respectively.

Convex lattice expressions. Let $\mathcal{X}$ be a set of variables. The set $\mathcal{L}_{\mathcal{X}}$ of *convex lattice expressions* over $\mathcal{X}$ is given by the following grammar:

$$\phi ::= x \mid w \mid \phi_1 \sqcup \phi_2 \mid \phi_1 \sqcap \phi_2 \mid \phi_1 +_\alpha \phi_2 \,.$$

where $x \in \mathcal{X}$, $w \in \mathbb{D}$, and $\alpha \in [0,1]$. We say that an expression is *simple* if it is of the form, w, $x_1 \sqcup x_2$, $x_1 \sqcap x_2$, or $x_1 +_\alpha x_2$, where x_1 and x_2 are variables.

Semantically, we interpret convex lattice expressions with respect to an environment $\rho\colon \mathcal{X} \to \mathbb{D}$ mapping variables to elements in $\mathbb{D}$. Formally, for ρ and environment and ϕ a convex lattice expression we define the value $[\![\phi]\!]\rho \in \mathbb{D}$ inductively on ϕ as follows:

$$\begin{aligned}
[\![x]\!]\rho &= \rho(x) \\
[\![w]\!]\rho &= w \\
[\![\phi_1 \sqcup \phi_2]\!]\rho &= [\![\phi_1]\!]\rho \sqcup [\![\phi_2]\!]\rho \\
[\![\phi_1 \sqcap \phi_2]\!]\rho &= [\![\phi_1]\!]\rho \sqcap [\![\phi_2]\!]\rho \\
[\![\phi_1 +_\alpha \phi_2]\!]\rho &= [\![\phi_1]\!]\rho +_\alpha [\![\phi_2]\!]\rho
\end{aligned}$$

Example 1. Consider the convex lattice $\langle [0,1], \leq, \{+_\alpha \mid \alpha \in [0,1]\}$, where convex combinations are interpreted as $a +_\alpha b = \alpha a + (1-\alpha)b$. Under the environment $\rho = [x \mapsto 0.2, y \mapsto 0.5]$, the expression $x \sqcap y$, and $(x \sqcup y) +_{0.2} y$ are interpreted as follows

$$\begin{aligned}
[\![x \sqcap y]\!]\rho &= \min(0.2, 0.5) = 0.2\,, \\
[\![(x \sqcup y) +_{0.1} y]\!]\rho &= 0.1 \cdot \max(0.2, 0.5) + 0.9 \cdot 0.5 = 0.5\,.
\end{aligned}$$

The desired semantics of variables is specified recursively through the use of an equation system, which assigns with each variable $x \in \mathcal{X}$ a defining expression.

Definition 1. *A* convex lattice equation system *(CLES) is a pair $\mathcal{E} = (\mathcal{X}, E)$ where $\mathcal{X}$ is a finite set of variables and $E : \mathcal{X} \to \mathcal{L}_{\mathcal{X}}$ is a mapping from variables to expressions over $\mathcal{X}$. We will write $x =_{\mathcal{E}} \phi$ to indicate that $E(x) = \phi$.*

An equation system specifies a semantic requirement to an environment ρ. We say that ρ is a *model* of the equation system $\mathcal{E} = (\mathcal{X}, E)$ if and only if for all $x \in \mathcal{X}$, $[\![x]\!]\rho = [\![E(x)]\!]\rho$.

Example 2. Consider the convex lattice from Example 1. Let $\mathcal{E} = (\{x, y\}, E)$ be the CLES where $E(x) = 0.2 \sqcup (x \sqcap y)$ and $E(y) = (x \sqcup y) +_{0.1} y$. One can verify that, an interpretation ρ is a model of $\mathcal{E}$ whenever $0.2 \leq \rho(x) \leq \rho(y)$.

Given an equation system $\mathcal{E}$, we are interested in checking statements of the form $\phi \leq \varepsilon$, for for $\phi \in \mathcal{L}$ and $\varepsilon \in \mathbb{D}$.

Definition 2 (Consistency). *Let $\mathcal{E} = (\mathcal{X}, E)$ be a CLES. A statement $\phi \leq \varepsilon$ is consistent for $\mathcal{E}$, written $\models_{\mathcal{E}} \phi \leq \varepsilon$, if $[\![\phi]\!]\rho \sqsubseteq \varepsilon$ for some model ρ of $\mathcal{E}$.*

Example 3. Consider the CLES $\mathcal{E}$ from Example 2. The statement $x \sqcap y \leq 0.5$ is consistent for $\mathcal{E}$, and the model $\rho = [x \mapsto 0.2, y \mapsto 0.2]$ is a witnesses for that. In contrast, the statement $x \sqcap y \leq 0.1$ is not consistent for $\mathcal{E}$ because no model ρ of $\mathcal{E}$ satisfies $[\![x \sqcap y]\!]\rho \leq 0.1$.

The models of $\mathcal{E}$ are exactly the fixed points of functional $F_{\mathcal{E}} : \mathbb{D}^{\mathcal{X}} \to \mathbb{D}^{\mathcal{X}}$ defined as follows, for $\rho \colon \mathcal{X} \to \mathbb{D}$ an environment and $x \in \mathcal{X}$ a variable:

$$F_{\mathcal{E}}(\rho)(x) = [\![E(x)]\!]\rho\,.$$

It can be shown that $F_{\mathcal{E}}$ is monotone —this is an immediate consequence of the fact that, for all $\phi \in \mathcal{L}_{\mathcal{X}}$, $\rho \mathrel{\dot\sqsubseteq} \rho'$ implies $[\![\phi]\!]\rho \sqsubseteq [\![\phi]\!]\rho'$— therefore, since $\mathbb{D}^{\mathcal{X}}$ is a complete lattice, by Knaster-Tarski's fixed point theorem, the set of fixed points of $F_{\mathcal{E}}$ is also a complete lattice. In particular, there are least and greatest fixed points, denoted $\mu F_{\mathcal{E}}$ and $\nu F_{\mathcal{E}}$, respectively, and a model of $\mathcal{E}$ always exists. It is therefore clear that $\models_{\mathcal{E}} \phi \leq \varepsilon$ if and only if $[\![\phi]\!]\mu F_{\mathcal{E}} \sqsubseteq \varepsilon$.

Example 4. BESs as introduced in [Lar92] may be recast as CLESs over the complete lattice $\mathbb{B} = (\{\mathtt{tt}, \mathtt{ff}\}, \leq)$, with $\mathtt{tt} \leq \mathtt{ff}$. With this ordering, $\sqcup$ will be represented by conjunction and $\sqcap$ by disjunction. Given a Boolean expression ϕ (resp. equation system $\mathcal{E}$), we denote by ϕ^* (resp. $\mathcal{E}^*$) the corresponding complete lattice expression (resp. equation system)[1]. Moreover given a BES $\mathcal{E}$ the notion of *consistency* of a Boolean expression ϕ in [Lar92] is captured precisely by $\models_{\mathcal{E}^*} \phi^* \leq \mathtt{tt}$.

3 Complete Proof System for Consistency Checking

In Figure 2, we present the proof system $\mathcal{CL}$ for checking the (relative) consistency of a statement $\phi \leq \varepsilon$ by exploring the equation system $\mathcal{E} = (\mathcal{X}, E)$ in a minimal fashion. This is done by allowing one to make assumptions on the values of variables along the derivation proof when needed.

The statements of the proof system are of the form

$$\{x_1 \leq \varepsilon_1, \ldots, x_n \leq \varepsilon_n\} \vdash_{\mathcal{E}} \phi \leq \varepsilon\,. \tag{1}$$

where $x_1, \ldots, x_n \in \mathcal{X}$ are variables, $\varepsilon_1, \ldots, \varepsilon_n \in \mathbb{D}$, and $\phi \in \mathcal{L}_{\mathcal{X}}$.

The statement (1) may informally be interpreted as: $\phi \leq \varepsilon$ is consistent under the assumption of consistency of $x_i \leq \varepsilon_i$, for all $i = 1, \ldots, n$.

Most of the rules in Figure 2 are obvious. The only non-obvious one is (A_4) that allows one to infer the consistency of a variable x from the consistency of its definition $E(x)$, under an assumption set updated with a new assumption on the variable itself. The way we interpret a set of assumptions Γ is essential to understand how the rule (A_4) operates. Augmenting an assumption set Γ with a new assumption $x \leq \varepsilon$ should be interpreted as updating our belief on what the tightest bound should be for the value of x. In this respect, we see a set

[1] Note that convex combinations are treated as described in Remark 1.

$$(A_1)\ \frac{}{\Gamma \vdash_{\mathcal{E}} \phi \leq \top} \qquad (A_2)\ \frac{\Gamma \vdash_{\mathcal{E}} \phi \leq \varepsilon'}{\Gamma \vdash_{\mathcal{E}} \phi \leq \varepsilon}\ \text{ if } \varepsilon' \sqsubseteq \varepsilon$$

$$(A_3)\ \frac{}{\Gamma \vdash_{\mathcal{E}} x \leq \Gamma(x)} \qquad (A_4)\ \frac{\Gamma \cup \{x \leq \varepsilon\} \vdash_{\mathcal{E}} \Gamma(x) \sqcap E(x) \leq \varepsilon}{\Gamma \vdash_{\mathcal{E}} x \leq \varepsilon}$$

$$(A_5)\ \frac{}{\Gamma \vdash_{\mathcal{E}} w \leq w} \qquad (A_6)\ \frac{\Gamma \vdash_{\mathcal{E}} \phi_1 \leq \varepsilon \quad \Gamma \vdash_{\mathcal{E}} \phi_2 \leq \varepsilon}{\Gamma \vdash_{\mathcal{E}} \phi_1 \sqcup \phi_2 \leq \varepsilon}$$

$$(A_7)\ \frac{\Gamma \vdash_{\mathcal{E}} \phi_1 \leq \varepsilon_1 \quad \Gamma \vdash_{\mathcal{E}} \phi_2 \leq \varepsilon_2}{\Gamma \vdash_{\mathcal{E}} \phi_1 \sqcap \phi_2 \leq \varepsilon_1 \sqcap \varepsilon_2} \qquad (A_8)\ \frac{\Gamma \vdash_{\mathcal{E}} \phi_1 \leq \varepsilon_1 \quad \Gamma \vdash_{\mathcal{E}} \phi_2 \leq \varepsilon_2}{\Gamma \vdash_{\mathcal{E}} \phi_1 +_\alpha \phi_2 \leq \varepsilon_1 +_\alpha \varepsilon_2}$$

Fig. 2. The proof system $\mathcal{CL}$ for inferring the (relative) consistency of statements of the form $\phi \leq \varepsilon$ w.r.t. a CLES $\mathcal{E} = (\mathcal{X}, E)$.

of assumption as a function $\Gamma\colon \mathcal{X} \to \mathbb{D}$ mapping each $x \in \mathcal{X}$ to the tightest upper-bound $\Gamma(x) = \bigsqcap\{\varepsilon \mid (x \leq \varepsilon) \in \Gamma\}$ that can be inferred from Γ. In the following, we will use these two equivalent interpretations of Γ (as a function or a set of statements) interchangeably, as convenient.

Example 5. Returning to BES and the proof system $\mathcal{A}$ from [Lar92]. Here judgements are of the form $\Gamma \vdash_{\mathcal{E}} \phi$, where ϕ is a Boolean formula, $\mathcal{E}$ is a BES and Γ is a set of Boolean variables (assumptions). Now let $\Gamma^* = \{x \leq \mathtt{tt} \mid x \in \Gamma\} \cup \{x \leq \mathtt{ff} \mid x \notin \Gamma\}$, we may consider $\Gamma^* \vdash_{\mathcal{E}^*} \phi^* \leq \mathtt{tt}$ as the corresponding judgment in $\mathcal{CL}$. With this correspondence it can be seen that the inference rules of $\mathcal{A}$ are captured by the rules of $\mathcal{CL}$ in the following way:

$$\begin{aligned}
&\mathbf{A_1} \equiv (A_3),\\
&\mathbf{A_2} \equiv (A5) \text{ with } \omega = \mathtt{tt},\\
&\mathbf{A_3} \equiv (A4),\\
&\mathbf{A4} \equiv (A6),\\
&\mathbf{A5} \equiv (A7) \text{ with } \varepsilon_2 = \mathtt{ff},\\
&\mathbf{A6} \equiv (A7) \text{ with } \varepsilon_1 = \mathtt{ff}.
\end{aligned}$$

It follows that $\Gamma \vdash_{\mathcal{E}} \phi$ are provable in $\mathcal{A}$ if and only if $\Gamma^* \vdash_{\mathcal{E}^*} \phi^* \leq \mathtt{tt}$ is provable in $\mathcal{CL}$.

To interpret semantically the conditional statements used in the proof system, we are looking for a notion of consistency that is relative to a set of assumptions. To this end we need to define what it means for an environment to be a model relative to some assumptions. We say that an environment ρ is a *model* of an equation system $\mathcal{E} = (\mathcal{X}, E)$ *relative to a set of assumptions* Γ, if for all $x \in \mathcal{X}$, $[\![x]\!]\rho = \Gamma(x) \sqcap [\![E(x)]\!]\rho$.

Definition 3 (Relative Consistency). *Let $\mathcal{E} = (\mathcal{X}, E)$ be a convex lattice equation system. A statement $\phi \leq \varepsilon$ is* consistent *for $\mathcal{E}$ relative to Γ, written $\Gamma \models_{\mathcal{E}} \phi \leq \varepsilon$, if there exists a model ρ of $\mathcal{E}$ relative to Γ such that $[\![\phi]\!]\rho \sqsubseteq \varepsilon$.*

Note that when the set of assumptions Γ is empty, relative consistency corresponds to standard consistency (i.e., $\emptyset \models_{\mathcal{E}} \phi \leq \varepsilon$ iff $\models_{\mathcal{E}} \phi \leq \varepsilon$).

The models of $\mathcal{E}$ relative to Γ are exactly the fixed points of the functional $F_{\mathcal{E},\Gamma} : \mathbb{D}^{\mathcal{X}} \to \mathbb{D}^{\mathcal{X}}$ defined as follows, for ρ an environment and $x \in \mathcal{X}$ a variable:

$$F_{\mathcal{E},\Gamma}(\rho)(x) = \Gamma(x) \sqcap [\![E(x)]\!]\rho \,.$$

Also $F_{\mathcal{E},\Gamma}$ is monotone, thus, by Knaster-Tarski's fixed point theorem, $F_{\mathcal{E},\Gamma}$ has least fixed point, denoted as $\mu F_{\mathcal{E},\Gamma}$. In particular, $\Gamma \models_{\mathcal{E}} \phi \leq \varepsilon$ is equivalent to $[\![\phi]\!]\mu F_{\mathcal{E},\Gamma} \sqsubseteq \varepsilon$.

The next two theorems prove the soundness and completeness of the proof system w.r.t. relative consistency.

Theorem 1 (Soundness). *If $\Gamma \vdash_{\mathcal{E}} \phi \leq \varepsilon$, then $\Gamma \models_{\mathcal{E}} \phi \leq \varepsilon$.*

Proof. By structural induction on the derivation tree for $\Gamma \vdash_{\mathcal{E}} \phi \leq \varepsilon$.
Case ($\mathbf{A_1}$): if $\Gamma \vdash_{\mathcal{E}} \phi \leq \varepsilon$ has been established using the axiom (A_1), then $\varepsilon = \top$. Clearly, $[\![\phi]\!]\mu F_{\mathcal{E},\Gamma} \sqsubseteq \top$. Thus, $\Gamma \models_{\mathcal{E}} \phi \leq \top$.

Case ($\mathbf{A_2}$): if $\Gamma \vdash_{\mathcal{E}} \phi \leq \varepsilon$ has been established using the axiom (A_2), then $\Gamma \vdash_{\mathcal{E}} \phi \leq \varepsilon'$ for some $\varepsilon' \sqsubseteq \varepsilon$. By inductive hypothesis, $\Gamma \models_{\mathcal{E}} \phi \leq \varepsilon'$. As this is equivalent to $[\![\phi]\!]\mu F_{\mathcal{E},\Gamma} \sqsubseteq \varepsilon'$, by transitivity of $\sqsubseteq$ we have $[\![\phi]\!]\mu F_{\mathcal{E},\Gamma} \sqsubseteq \varepsilon$. Thus, $\Gamma \models_{\mathcal{E}} \phi \leq \varepsilon$.

Case ($\mathbf{A_3}$): if $\Gamma \vdash_{\mathcal{E}} \phi \leq \varepsilon$ has been established using the axiom (A_3), then $\phi = x$ and $\varepsilon = \Gamma(x)$. Since $\mu F_{\mathcal{E},\Gamma}(x)$ is a fixed point of $F_{\mathcal{E},\Gamma}$, we have $\mu F_{\mathcal{E},\Gamma}(x) \sqsubseteq \Gamma(x)$. By definition, $[\![x]\!]\mu F_{\mathcal{E},\Gamma}(x) = \mu F_{\mathcal{E},\Gamma}(x)$ and, by transitivity of $\sqsubseteq$, we get $[\![x]\!]\mu F_{\mathcal{E},\Gamma}(x) \sqsubseteq \Gamma(x)$. Thus, $\Gamma \models_{\mathcal{E}} x \leq \Gamma(x)$.

Case ($\mathbf{A_4}$): if $\Gamma \vdash_{\mathcal{E}} \phi \leq \varepsilon$ has been established using the axiom (A_4), then $\phi = x$ and $\Gamma \cup \{x \leq \varepsilon\} \vdash_{\mathcal{E}} \Gamma(x) \sqcap E(x) \leq \varepsilon$. By inductive hypothesis, we have that $\Gamma \cup \{x \leq \varepsilon\} \models_{\mathcal{E}} \Gamma(x) \sqcap E(x) \leq \varepsilon$, which, in turn, it is equivalent to $\Gamma(x) \sqcap [\![E(x)]\!]\mu F_{\mathcal{E},\Gamma\cup\{x\leq\varepsilon\}} \sqsubseteq \varepsilon$. As $\mu F_{\mathcal{E},\Gamma\cup\{x\leq\varepsilon\}}$ is a fixed point of $F_{\mathcal{E},\Gamma\cup\{x\leq\varepsilon\}}$, we have $\mu F_{\mathcal{E},\Gamma\cup\{x\leq\varepsilon\}}(x) = \Gamma(x) \sqcap \varepsilon \sqcap [\![E(x)]\!]\mu F_{\mathcal{E},\Gamma\cup\{x\leq\varepsilon\}}$. Thus, $\mu F_{\mathcal{E},\Gamma\cup\{x\leq\varepsilon\}}(x) \sqsubseteq \varepsilon$. We prove that $[\![x]\!]\mu F_{\mathcal{E},\Gamma} = \mu F_{\mathcal{E},\Gamma}(x) \sqsubseteq \varepsilon$, by showing that $\mu F_{\mathcal{E},\Gamma\cup\{x\leq\varepsilon\}}$ is a prefix point of $F_{\mathcal{E},\Gamma}$, i.e., $F_{\mathcal{E},\Gamma}(\mu F_{\mathcal{E},\Gamma\cup\{x\leq\varepsilon\}})(y) \sqsubseteq \mu F_{\mathcal{E},\Gamma\cup\{x\leq\varepsilon\}}(y)$ for all $y \in \mathcal{X}$. We consider only the case $y = x$, since the others are trivial.

$$\begin{aligned}
F_{\mathcal{E},\Gamma}(\mu F_{\mathcal{E},\Gamma\cup\{x\leq\varepsilon\}})(x) &= \Gamma(x) \sqcap [\![E(x)]\!]\mu F_{\mathcal{E},\Gamma\cup\{x\leq\varepsilon\}} && \text{(def. } F_{\mathcal{E},\Gamma}) \\
&= \Gamma(x) \sqcap \varepsilon \sqcap [\![E(x)]\!]\mu F_{\mathcal{E},\Gamma\cup\{x\leq\varepsilon\}} && \text{(ind. hp.)} \\
&= \mu F_{\mathcal{E},\Gamma\cup\{x\leq\varepsilon\}}(x)\,. && \text{(fixed point of } F_{\mathcal{E},\Gamma\cup\{x\leq\varepsilon\}})
\end{aligned}$$

From the above, we conclude that $\Gamma \models_{\mathcal{E}} x \leq \varepsilon'$.

Case ($\mathbf{A_5}$): if $\Gamma \vdash_{\mathcal{E}} \phi \leq \varepsilon$ has been established using the axiom (A_5), then $\phi = w$ and $\varepsilon = w$. By definition, $[\![w]\!]\mu F_{\mathcal{E},\Gamma} = w$, thus $\Gamma \models_{\mathcal{E}} w \leq w$.

Case ($\mathbf{A_6}$): if $\Gamma \vdash_{\mathcal{E}} \phi \leq \varepsilon$ has been established using the axiom (A_6), then $\phi = \phi_1 \sqcup \phi_2$ and $\Gamma \vdash_{\mathcal{E}} \phi_i \leq \varepsilon$, for $i = 1, 2$. By inductive hypothesis, $\Gamma \models_{\mathcal{E}} \phi_i \leq \varepsilon$, for $i = 1, 2$. This is equivalent to $[\![\phi_1]\!]\mu F_{\mathcal{E},\Gamma} \sqcup [\![\phi_2]\!]\mu F_{\mathcal{E},\Gamma} \sqsubseteq \varepsilon$. By definition, $[\![\phi_1 \sqcup \phi_1]\!]\mu F_{\mathcal{E},\Gamma} = [\![\phi_1]\!]\mu F_{\mathcal{E},\Gamma} \sqcup [\![\phi_2]\!]\mu F_{\mathcal{E},\Gamma}$. Thus, $\Gamma \models_{\mathcal{E}} \phi_1 \sqcup \phi_2 \leq \varepsilon$.

Case ($\mathbf{A_7}$): if $\Gamma \vdash_{\mathcal{E}} \phi \leq \varepsilon$ has been established using the axiom (A_7), then $\phi = \phi_1 \sqcap \phi_2$, $\varepsilon = \varepsilon_1 \sqcap \varepsilon_2$, and $\Gamma \vdash_{\mathcal{E}} \phi_i \leq \varepsilon$, for $i = 1, 2$. By inductive hypothesis, $\Gamma \models_{\mathcal{E}} \phi_i \leq \varepsilon_i$, for $i = 1, 2$. This is equivalent to $[\![\phi_i]\!]\mu F_{\mathcal{E},\Gamma} \sqsubseteq \varepsilon_i$, for $i = 1, 2$. Therefore $[\![\phi_1]\!]\mu F_{\mathcal{E},\Gamma} \sqcap [\![\phi_2]\!]\mu F_{\mathcal{E},\Gamma} \sqsubseteq \varepsilon_1 \sqcap \varepsilon_2$. By definition and transitivity of $\sqsubseteq$, $[\![\phi_1 \sqcap \phi_1]\!]\mu F_{\mathcal{E},\Gamma} = [\![\phi_1]\!]\mu F_{\mathcal{E},\Gamma} \sqcap [\![\phi_2]\!]\mu F_{\mathcal{E},\Gamma} \sqsubseteq \varepsilon_1 \sqcap \varepsilon_2$. Thus, $\Gamma \models_{\mathcal{E}} \phi_1 \sqcap \phi_2 \leq \varepsilon_1 \sqcap \varepsilon_2$.

Case ($\mathbf{A_8}$): if $\Gamma \vdash_{\mathcal{E}} \phi \leq \varepsilon$ has been established using the axiom (A_8), then $\phi = \phi_1 +_p \phi_2$, $\varepsilon = \varepsilon_1 +_p \varepsilon_2$ and $\Gamma \vdash_{\mathcal{E}} \phi_i \leq \varepsilon_i$, for $i = 1, 2$. By inductive hypothesis, $\Gamma \models_{\mathcal{E}} \phi_i \leq \varepsilon_i$, which is equivalent to $[\![\phi_i]\!]\mu F_{\mathcal{E},\Gamma} \sqsubseteq \varepsilon_i$ for $i = 1, 2$. We show that $[\![\phi_1 +_p \phi_2]\!]\mu F_{\mathcal{E},\Gamma} \sqsubseteq \varepsilon_1 +_p \varepsilon_2$ in two steps.

$$\begin{aligned}
&[\![\phi_1]\!]\mu F_{\mathcal{E},\Gamma} +_p [\![\phi_2]\!]\mu F_{\mathcal{E},\Gamma} \\
&= ([\![\phi_1]\!]\mu F_{\mathcal{E},\Gamma} \sqcap \varepsilon_1) +_p [\![\phi_2]\!]\mu F_{\mathcal{E},\Gamma} && ([\![\phi_1]\!]\mu F_{\mathcal{E},\Gamma} \sqsubseteq \varepsilon_1) \\
&= ([\![\phi_1]\!]\mu F_{\mathcal{E},\Gamma} +_p [\![\phi_2]\!]\mu F_{\mathcal{E},\Gamma}) \sqcap (\varepsilon_1 +_p [\![\phi_2]\!]\mu F_{\mathcal{E},\Gamma}) && \text{(distributive law)}
\end{aligned}$$

Hence, $[\![\phi_1]\!]\mu F_{\mathcal{E},\Gamma} +_p [\![\phi_1]\!]\mu F_{\mathcal{E},\Gamma} \sqsubseteq \varepsilon_1 +_p [\![\phi_2]\!]\mu F_{\mathcal{E},\Gamma}$. Moreover,

$$\begin{aligned}
\varepsilon_1 +_p \varepsilon_2 &= \varepsilon_1 +_p (\varepsilon_2 \sqcup [\![\phi_2]\!]\mu F_{\mathcal{E},\Gamma}) && ([\![\phi_2]\!]\mu F_{\mathcal{E},\Gamma} \sqsubseteq \varepsilon_2) \\
&= (\varepsilon_1 +_p \varepsilon_2) \sqcup (\varepsilon_1 +_p [\![\phi_2]\!]\mu F_{\mathcal{E},\Gamma}) && \text{(distributive law)}
\end{aligned}$$

Hence, $\varepsilon_1 +_p [\![\phi_2]\!]\mu F_{\mathcal{E},\Gamma} \sqsubseteq \varepsilon_1 +_p \varepsilon_2$. Thus, by transitivity of $\sqsubseteq$ we have

$$[\![\phi_1 +_p \phi_2]\!]\mu F_{\mathcal{E},\Gamma} = [\![\phi_1]\!]\mu F_{\mathcal{E},\Gamma} +_p [\![\phi_1]\!]\mu F_{\mathcal{E},\Gamma} \sqsubseteq \varepsilon_1 +_p \varepsilon_2 \,.$$

Therefore, $\Gamma \models_{\mathcal{E}} \phi_1 +_p \phi_2 \leq \varepsilon_1 +_p \varepsilon_2$. □

Theorem 2 (Completeness). *If $\Gamma \models_{\mathcal{E}} \phi \leq \varepsilon$, then $\Gamma \vdash_{\mathcal{E}} \phi \leq \varepsilon$.*

Proof. In the following we will prove that $\Gamma \vdash_{\mathcal{E}} \phi \leq [\![\phi]\!]\mu F_{\mathcal{E},\Gamma}$. To simplify the exposition, we will make use of a semantically equivalent variant of the proof system in Figure 2 where we add the following rule derivable from (A_4)

$$(A_4^*)\ \frac{\Gamma' \cup \{\bar{x} \leq [\![x]\!]\mu F_{\mathcal{E},\Gamma}\} \vdash_{\mathcal{E}} \Gamma'(x) \sqcap E(x) \leq [\![x]\!]\mu F_{\mathcal{E},\Gamma}}{\Gamma' \vdash_{\mathcal{E}} x \leq [\![x]\!]\mu F_{\mathcal{E},\Gamma}}$$

Note that in the premise of (A_4^*), the variable x in the assumption set is "marked". The markings have no additional semantic meaning (i.e., $x = \bar{x}$). We will use them in our proof to keep track of the assumptions that have been introduced by applying (A_4^*).

We prove the following stronger statement: $\Gamma \cup \bar{\Gamma} \vdash_{\mathcal{E}} \phi \leq [\![\phi]\!]\mu F_{\mathcal{E},\Gamma}$ for all $\bar{\Gamma}$ containing only marked assumptions of the form $\bar{x} \leq [\![x]\!]\mu F_{\mathcal{E},\Gamma}$. We proceed by induction on $n = |\mathcal{X} \setminus \{x \mid (\bar{x} \leq \varepsilon) \in \bar{\Gamma}\}\,|$.

Base Case (n = 0). By hypothesis $(\bar{x} \leq [\![x]\!]\mu F_{\mathcal{E},\Gamma}) \in \bar{\Gamma}$ for all $x \in \mathcal{X}$. We proceed by induction on the structure of ϕ.

($\phi = w$) Recall that $[\![w]\!]\mu F_{\mathcal{E},\Gamma} = w$. By axiom ($A_5$), $\Gamma \cup \bar{\Gamma} \vdash_{\mathcal{E}} w \leq [\![w]\!]\mu F_{\mathcal{E},\Gamma}$.

($\phi = x$) Recall that $(\bar{x} \leq [\![x]\!]\mu F_{\mathcal{E},\Gamma}) \in \bar{\Gamma}$, hence $(\Gamma \cup \bar{\Gamma})(x) \sqsubseteq [\![x]\!]\mu F_{\mathcal{E},\Gamma}$. Thus, using ($A_3$) and ($A_2$) we prove $\Gamma \cup \bar{\Gamma} \vdash_{\mathcal{E}} x \leq [\![x]\!]\mu F_{\mathcal{E},\Gamma}$.

($\phi = \phi_1 \sqcap \phi_2$) By inductive hypothesis we have $\Gamma \cup \bar{\Gamma} \vdash_{\mathcal{E}} \phi_i \leq [\![\phi_i]\!]\mu F_{\mathcal{E},\Gamma}$ for $i = 1, 2$. Thus, by def. of $[\![\cdot]\!]$, via (A_7) we get $\Gamma \cup \bar{\Gamma} \vdash_{\mathcal{E}} \phi_1 \sqcap \phi_2 \leq [\![\phi_1 \sqcap \phi_2]\!]\mu F_{\mathcal{E},\Gamma}$.

($\phi = \phi_1 \sqcup \phi_2$) By inductive hypothesis we have $\Gamma \cup \bar{\Gamma} \vdash_{\mathcal{E}} \phi_i \leq [\![\phi_i]\!]\mu F_{\mathcal{E},\Gamma}$ for $i = 1, 2$. Thus, by def. of $[\![\cdot]\!]$, via (A_2) we get $\Gamma \cup \bar{\Gamma} \vdash_{\mathcal{E}} \phi_i \leq [\![\phi_1 \sqcup \phi_2]\!]\mu F_{\mathcal{E},\Gamma}$. Then, via ($A_6$) we get $\Gamma \cup \bar{\Gamma} \vdash_{\mathcal{E}} \phi_1 \sqcup \phi_2 \leq [\![\phi_1 \sqcup \phi_2]\!]\mu F_{\mathcal{E},\Gamma}$.

($\phi = \phi_1 +_\alpha \phi_2$) By inductive hypothesis we have $\Gamma \cup \bar{\Gamma} \vdash_{\mathcal{E}} \phi_i \leq [\![\phi_i]\!]\mu F_{\mathcal{E},\Gamma}$ for $i = 1, 2$. Thus, by def. of $[\![\cdot]\!]$, via (A_8) we get $\Gamma \cup \bar{\Gamma} \vdash_{\mathcal{E}} \phi_1 +_\alpha \phi_2 \leq [\![\phi_1 +_\alpha \phi_2]\!]\mu F_{\mathcal{E},\Gamma}$.

Inductive Case. Again, we proceed by induction on the structure of ϕ. We only show the case $\phi = x$. All other cases carry over exactly as in the base case.

We distinguish two cases: some marked assumption on x is present in $\bar{\Gamma}$, or not. In the former of the two cases we proceed exactly as done in the base case.

For the latter case, by inductive hypothesis on n we have that

$$\Gamma \cup \bar{\Gamma} \cup \{\bar{x} \leq [\![x]\!]\mu F_{\mathcal{E},\Gamma}\} \vdash_{\mathcal{E}} \Gamma(x) \sqcap E(x) \leq [\![\Gamma(x) \sqcap E(x)]\!]\mu F_{\mathcal{E},\Gamma} \,. \tag{2}$$

By def. of $[\![\cdot]\!]$ and the fact that $\mu F_{\mathcal{E},\Gamma}$ is a fixed point of $F_{\mathcal{E},\Gamma}$ we have

$$[\![\Gamma(x) \sqcap E(x)]\!]\mu F_{\mathcal{E},\Gamma} = \Gamma(x) \sqcap [\![E(x)]\!]\mu F_{\mathcal{E},\Gamma} = [\![x]\!]\mu F_{\mathcal{E},\Gamma} \,. \tag{3}$$

Therefore, by (2) and (3) via (A_4^*) we get $\Gamma \cup \bar{\Gamma} \vdash_{\mathcal{E}} x \leq [\![x]\!]\mu F_{\mathcal{E},\Gamma}$. □

4 Simple Stochastic Games

In this section we show how convex lattice equation systems encompass the powerful formalism of simple stochastic games [Con90,Con92].

A *simple stochastic game* (SSG) is a directed graph $G = (V, E)$ with the following properties. Vertices are partitioned into sets of *0-sinks*, *1-sinks*, *max vertices*, *min vertices*, and *average vertices*. Except the sink vertices, each vertex v of V, has two successors nodes that for convenience we call the left and the right successor of v, respectively denoted by *left*(v) and *right*(v).

The game is played by two players, the *max player* and the *min player*, with a single token. At each step of the game, the token is moved from a vertex to one of its two successors. At a min vertex the min player chooses the successor, at a max vertex the max player chooses the successor, and at an average vertex the successor is chosen at random by tossing a fair coin. The max player wins a play of the game if the token reaches a 1-sink and the min player wins if the play reaches a 0-sink or continues forever without reaching a sink. Since the game is stochastic, the max player tries to maximize the probability of reaching a 1-sink whereas the min player tries to minimize that probability.

A *strategy*, a.k.a. *policy*, for the min player is a function $\sigma \colon V_{\min} \to V$ that assigns the target of an outgoing edge to each min vertex, that is, for all $v \in V_{\min}$,

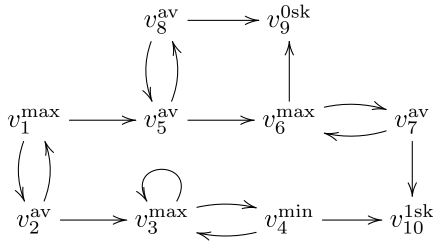

Fig. 3. A simple stochastic game (from [Con92]).

$(v, \sigma(v)) \in E$. Likewise, a strategy for the max player is a function $\tau \colon V_{\max} \to V$ that assigns the target of an outgoing edge to each max vertex. These strategies are known as *pure stationary* strategies. We can restrict ourselves to these strategies since both players of a simple stochastic game have optimal strategies of this type (see, for example, [LL69]).

Such strategies determine a sub-game in which each max vertex and each min vertex has out-degree one. We write $\nu_{\sigma,\tau} \colon V \to [0,1]$ for the function that gives the probability of a vertex in this sub-game to reach a 1-sink (see [Con92, Section 2] for details). The *value function* $\nu^* \colon V \to [0,1]$ of a SSG is defined as

$$\nu^* = \min_\sigma \max_\tau \nu_{\sigma,\tau} .$$

It is folklore that the value function of a simple stochastic game can be characterised as the least fixed point of the following function $\Psi_G \colon [0,1]^V \to [0,1]^V$ (see, for example, [Jub05, Section 2.2 and 2.3]) defined by

$$\Psi_G(\nu)(v) = \begin{cases} 0 & \text{if } v \text{ is a 0-sink} \\ 1 & \text{if } v \text{ is a 1-sink} \\ \max\{\nu(\mathit{left}(v)), \nu(\mathit{right}(v))\} & \text{if } v \text{ is a max vertex} \\ \min\{\nu(\mathit{left}(v)), \nu(\mathit{right}(v))\} & \text{if } v \text{ is a min vertex} \\ 1/2(\nu(\mathit{left}(v)) + \nu(\mathit{right}(v))) & \text{if } v \text{ is an average vertex} \end{cases}$$

4.1 Value function of an SSGs as a consistency checking

Let $G = (V, E)$ be a SSG. Consider the convex lattice $([0,1], \leq, \{+_\alpha \mid \alpha \in [0,1]\})$ where $a +_\alpha b = \alpha a + (1-\alpha) b$. We define the equation system $\mathcal{E}_G = (V, E_G)$ by

$$E_G(v) = \begin{cases} 0 & \text{if } v \text{ is a 0-sink} \\ 1 & \text{if } v \text{ is a 1-sink} \\ \mathit{left}(v) \sqcup \mathit{right}(v) & \text{if } v \text{ is a max vertex} \\ \mathit{left}(v) \sqcap \mathit{right}(v) & \text{if } v \text{ is a min vertex} \\ \mathit{left}(v) +_{1/2} \mathit{right}(v) & \text{if } v \text{ is an average vertex} \end{cases}$$

The following result relates the value of a SSG to consistency checking w.r.t. its corresponding corresponding equation system.

Theorem 3. *Let $G = (V, E)$ be a SSG and $\mathcal{E}_G = (V, E_G)$ the corresponding equation system. Then $\nu^*(v) \leq \varepsilon$ iff $\vdash_{\mathcal{E}_G} v \leq \varepsilon$.*

Proof. It is immediate to show that $F_{\mathcal{E}_G} = \Psi_G$, thus $\nu^* = \mu F_{\mathcal{E}_G}$. From this it follows that $\nu^*(v) \leq \varepsilon$ if and only if $\models_{\mathcal{E}_G} v \leq \varepsilon$, as $\models_{\mathcal{E}_G} v \leq \varepsilon$ is equivalent to $[\![v]\!]\mu F_{\mathcal{E}_G} = \mu F_{\mathcal{E}_G}(v) \leq \varepsilon$. The thesis follows by soundness and completeness of the proof system (Theorems 1 and 2). $\square$

We can now provide a first concrete application of the proof system in Fig. 2. Example 6 showcases a proof for a (tight) upper bound of the value of a vertex in a SSG made through consistency checking.

Example 6. Consider the SSG in Figure 3. In [Con92] it is shown that the value of the vertex v_3 under the strategies $\tau = (v_1 \mapsto v_5, v_3 \mapsto v_4, v_6 \mapsto v_7)$ and $\sigma = (v_4 \mapsto v_3)$ is $\nu_{\sigma,\tau}(v_3) = 0$. As these are optimal strategies for the players, we also have $\nu^*(v_3) = 0$. Next we show the inference tree for $\vdash_{\mathcal{E}_G} v_3 \leq 0$.

$$
\dfrac{
\dfrac{}{\{v_3 \leq 0\} \vdash_{\mathcal{E}_G} v_3 \leq 0}\,(A_3)
\qquad
\dfrac{
\dfrac{
\dfrac{}{\{v_3, v_4 \leq 0\} \vdash_{\mathcal{E}_G} v_3 \leq 0}\,(A_3)
\qquad
\dfrac{}{\{v_3, v_4 \leq 0\} \vdash_{\mathcal{E}_G} v_{10} \leq 1}\,(A_1)
}{\{v_3, v_4 \leq 0\} \vdash_{\mathcal{E}_G} v_3 \sqcap v_{10} \leq 0}\,(A_7)
}{\{v_3 \leq 0\} \vdash_{\mathcal{E}_G} v_4 \leq 0}\,(A_4)
}{
\dfrac{\{v_3 \leq 0\} \vdash_{\mathcal{E}_G} v_3 \sqcup v_4 \leq 0}{\vdash_{\mathcal{E}_G} v_3 \leq 0}\,(A_4)
}\,(A_6)
$$

Remarkably, the consistency of $v_3 \leq 0$ could be proven without exploring the entire equation system (only the equations for v_3, v_4 are used).

Remark 2. Many interesting optimization problems can be encoded as simple stochastic games. In particular, Tang and van Breugel [TvB16] showed that the probabilistic bisimilarity distance for Markov chains proposed by Desharnais et al. [DGJP04] can be characterized as the value of a simple stochastic game (without max vertices). Later, this result was generalised to the case of probabilistic automata [BBL+21] which combine non-determinism with probabilistic choice.

Thus, thanks to Theorem 3, one can prove upper bounds for the above mentioned probabilistic bisimilarity distances using the proof system of Fig. 2. $\square$

5 Timed Bisimulation Distance

In this section we introduce the novel notion of *timed bisimulation distance*, the natural extension of Wang Yi's timed bisimulation equivalence [Yi90] to a metric setting. We provide rudimentary results for this distance and we provide an encoding in terms of equation systems that allow us to check for upper-bounds of this distance for regular timed systems.

Towards this let us recall the basic notions of time domains and timed transition systems along with some properties regarding them.

Definition 4 (Time Domain). *A time domain is a monoid* $\langle \mathbb{T}, +, 0 \rangle$ *satisfying the following axioms*

$$\forall t, r, v \in \mathbb{T}: \quad t = t + r + v \implies t = t + r \qquad \text{(irreversibility)}$$
$$\forall t, r, v \in \mathbb{T}: \quad t + r = t + v \implies r = v \qquad \text{(left-cancellation)}$$

Time domains yield a canonical preorder $\leq$ given for $t, r \in \mathbb{T}$ by $t \leq r$ iff there exists $v \in \mathbb{T}$ such that $t + v = r$. Note that due to *left-cancellation* this v is unique and we can therefore derive substraction as $r - t = v$ whenever $t \leq r$. We can further generalize this substraction by truncating at 0 whenever $t > r$, i.e. $r \dot{-} t = 0$. A distance $d\colon \mathbb{T} \times \mathbb{T} \to [0, \infty]$ over $\mathbb{T}$ is said to respect the time domain $\langle \mathbb{T}, +, 0 \rangle$ if it makes $+$ non-expansive:

$$\forall t, r, v \in \mathbb{T}: \quad d(t, r) \geq d(t + v, r + v) \qquad \text{(non-expansiveness)}$$

The usual example of a time domain would be the non-negative reals, i.e. $\langle [0, \infty], +, 0 \rangle$, along with the distance given by the absolute difference, i.e. $|t - r|$.

For the remainder of this section we fix a time domain $\langle \mathbb{T}, +, 0 \rangle$ and a distance $d_{\mathbb{T}}\colon \mathbb{T} \times \mathbb{T} \to [0, \infty]$ respecting it.

Definition 5 (TTS). *A timed transition system is a tuple* $\mathcal{M} = (M, \mathbf{A}, \to)$ *where,* M *is a set of states,* $\mathbf{A}$ *is a countable set of action labels disjoint from* $\mathbb{T}$*,* $\to \subseteq (M \times \mathbb{T} \times M) \cup (M \times \mathbf{A} \times M)$ *is a transition relation describing timed and labelled behaviour, satisfying the following, for all* $m, m', m'' \in M$ *and* $t, t' \in \mathbb{T}$

$$m \xrightarrow{0} m \qquad \text{(zero delay)}$$
$$m \xrightarrow{t} m' \wedge t' \leq t \implies \exists n.\, m \xrightarrow{t'} n \xrightarrow{t-t'} m' \qquad \text{(time additivity)}$$
$$m \xrightarrow{t} m' \wedge m \xrightarrow{t} m'' \implies m' = m'' \qquad \text{(time determinism)}$$

We will use $\to^*$ to denote the transitive and reflexive closure of $\to$ and we write $m \not\to$ whenever there are no labelled transitions from the state $m \in M$.

Now, for a given $m \in M$, we define the set of possible timed behaviour of m, denoted $\delta_{\mathcal{M}}(m)$, by

$$\delta_{\mathcal{M}}(m) = \left\{ \langle t, \dagger, m' \rangle \in \mathbb{T} \times \{\dagger\} \times M \;\middle|\; m \xrightarrow{t} m' \not\to \right\}$$
$$\cup \left\{ \langle t, a, m' \rangle \in \mathbb{T} \times \mathbf{A} \times M \;\middle|\; m \xrightarrow{t}\xrightarrow{a} m' \right\}$$

where we use the special symbol $\dagger \notin \mathbf{A}$ to denote deadlocks. With this we can now define a preliminary distance between timed behaviour.

Definition 6. *Let* $d : M \times M \to [0, \infty]$ *be a distance over the states of* M*, then the behavioural distance of* $\mathcal{M}$ *wrt. to* d *is the distance* $\Lambda_{\mathcal{M}}(d) : (\mathbb{T} \times \mathbf{A}_{\dagger} \times M)^2 \to [0, \infty]$ *defined for arbitrary* $\langle t, a, m \rangle, \langle r, b, n \rangle \in \mathbb{T} \times \mathbf{A}_{\dagger} \times M$ *by*

$$\Lambda_{\mathcal{M}}(d)(\langle t, a, m \rangle, \langle r, b, n \rangle) = \max \{ d_{\mathbb{T}}(t, r), \iota(a, b), d(m, n) \}$$

where $\iota(a, b) = 0$ *if* $a = b$ *and* $\iota(a, b) = \infty$ *otherwise.*

We can now define the iterator of which we take the least fixed point to be our timed bisimilarity distance.

Definition 7 (Iterator). $\Psi_{\mathcal{M}} : [M \times M \to [0, \infty]] \to [M \times M \to [0, \infty]]$ *defined for arbitrary* $d : M \times M \to [0, \infty]$ *by*

$$\Psi_{\mathcal{M}}(d)(m, n) = \mathcal{H}(\Lambda_{\mathcal{M}}(d))(\delta_{\mathcal{M}}(m), \delta_{\mathcal{M}}(n))$$

where $\mathcal{H}(\Lambda_{\mathcal{M}}(d))$ *is the Hausdorff lifting of* $\Lambda_{\mathcal{M}}(d)$.

Lemma 1 (Monotonicity). *If* $d, d' : M \times M \to [0, \infty]$ *such that* $d \leq d'$*, then* $\Psi_{\mathcal{M}}(d) \leq \Psi_{\mathcal{M}}(d')$.

As the space of distances over M forms a complete lattice wrt. to pairwise comparison and as $\Psi_{\mathcal{M}}$ is monotonic over this space, we have by the Knaster-Tarski fixed point theorem [Tar55] that $\Psi_{\mathcal{M}}$ yields a unique least fixed point, denoted $\mu\Psi_{\mathcal{M}}$.

To justify our timed bisimilarity distance, we state the following two rudimentary results. Firstly, that $\mu\Psi_{\mathcal{M}}$ indeed behaves like a distance, in this case an (extended) pseudo-metric. Secondly, that $\mu\Psi_{\mathcal{M}}$ agrees with timed bisimilarity, that is whenever two states are bisimilar then $\mu\Psi_{\mathcal{M}}$ puts those states at distance zero.

Theorem 4. *If* $d_{\mathbb{T}}$ *is a pseudo-metric, then* $\mu\Psi_{\mathcal{M}}$ *is a pseudo-metric.*

Theorem 5. *If* m *and* n *are timed bisimilar then* $\mu\Psi_{\mathcal{M}}(m, n) = 0$.

5.1 Encoding for Regular Timed Processes

For the encoding we will only consider TTS induced by the regular fragment of TCCS (e.g. no use of parallel composition). We will not formally define TCCS here but instead refer to [Yi91]. The restriction to regular TCCS permits an easy characterisation of the timed bisimulation distance on a finite set of timed behaviour and thereby allowing us to encode it using convex lattice equation systems.

For any $m \in M$, let us define the minimal timed behaviour as

$$\delta^{\min}_{\mathcal{M}}(m) = \left\{ \langle t, a, m' \rangle \in \delta_{\mathcal{M}} \;\middle|\; t = \min_{\langle r, a, m' \rangle \in \delta_{\mathcal{M}}(m)} r \right\}$$

For TTS induced by TCCS expressions, the above set is finite regardless of choice of state. Furthermore, we have the following lemma stating that we only need to consider these finite subsets of timed behaviour for the timed bisimulation distance.

Lemma 2. *For arbitrary* $d : M \times M \to [0, \infty]$ *and* $m, n \in M$,

$$\Psi_{\mathcal{M}}(d)(m, n) = \mathcal{H}(\Lambda)(\delta^{\min}_{\mathcal{M}}(m), \delta^{\min}_{\mathcal{M}}(n))$$

Consider now the complete partial order $([0,\infty],\leq)$. For a given TTS $\mathcal{M}$ induced by a TTS expression we define the equation system $\langle \mathcal{X}_\mathcal{M}, E_\mathcal{M}\rangle$ where $\mathcal{X}_\mathcal{M}$ is given by $x_{m,n} \in \mathcal{X}_\mathcal{M}$ whenever $m,n \in M$ and $E_\mathcal{M}$ is given for $x_{m,n} \in \mathcal{X}_\mathcal{M}$ by

$$
\begin{aligned}
x_{m,n} =_{E_\mathcal{M}} & \bigsqcup_{\langle t,a,m'\rangle \in \delta^-(m)} \bigsqcap_{\langle r,b,n'\rangle \in \delta^-(n)} (d_\mathbb{T}(t,r) \sqcup \iota(a,b) \sqcup x_{m',n'}) \\
\sqcup & \bigsqcup_{\langle r,b,n'\rangle \in \delta^-(n)} \bigsqcap_{\langle t,a,m'\rangle \in \delta^-(m)} (d_\mathbb{T}(t,r) \sqcup \iota(a,b) \sqcup x_{m',n'})
\end{aligned}
$$

where $\bigsqcap \emptyset = \infty$ and $\bigsqcup \emptyset = 0$.

Here $\mathcal{X}_\mathcal{M}$ may be infinite, but the formulae given by $E_\mathcal{M}$ are finite and depend only on finite subsets of $\mathcal{X}_\mathcal{M}$. This is because you can only describe finite branching using TCCS and that the target states of labelled transitions remain the same regardless of further delays due to the TTS induced by TCCS expressions satisfying persistency. Hence, one need only consider a finite sub-equation system of $E_\mathcal{M}$ when checking for consistency.

Example 7. As an example, consider the two TCCS expressions

$$P = \epsilon(4).a.P + b.\mathrm{Nil} \quad \text{and} \quad Q = \epsilon(3).(a.Q + b.\mathrm{Nil})$$

over the time domain $\mathbb{T} = \mathbb{R}_{\geq 0}$. Let $d_\mathbb{T}$ be given by the absolute difference, then P and Q have distance $\mu\Psi_\mathcal{M}(P,Q) = \max(d_\mathbb{T}(4,3), d_\mathbb{T}(0,3)) = 3$. For the given TCCS expressions we have that their minimal time behaviour is

$$\delta^{\min}_\mathcal{M}(P) = \{\langle 4, a, \mathrm{Nil}\rangle, \langle 0, b, \mathrm{Nil}\rangle\}$$

$$\delta^{\min}_\mathcal{M}(Q) = \{\langle 3, a, \mathrm{Nil}\rangle, \langle 3, b, \mathrm{Nil}\rangle\}$$

and hence the formula associated with them is

$$
\begin{aligned}
x_{P,Q} = & ((d_\mathbb{T}(4,3) \sqcup \iota(a,a) \sqcup x_{P,Q}) \sqcap (d_\mathbb{T}(4,3) \sqcup \iota(a,b) \sqcup x_{P,\mathrm{Nil}})) \\
& \sqcup ((d_\mathbb{T}(0,3) \sqcup \iota(b,a) \sqcup x_{\mathrm{Nil},Q}) \sqcap (d_\mathbb{T}(0,3) \sqcup \iota(b,b) \sqcup x_{\mathrm{Nil},\mathrm{Nil}})) \\
& \sqcup ((d_\mathbb{T}(4,3) \sqcup \iota(a,a) \sqcup x_{P,Q}) \sqcap (d_\mathbb{T}(0,3) \sqcup \iota(b,a) \sqcup x_{\mathrm{Nil},Q})) \\
& \sqcup ((d_\mathbb{T}(4,3) \sqcup \iota(a,b) \sqcup x_{P,\mathrm{Nil}}) \sqcap (d_\mathbb{T}(0,3) \sqcup \iota(b,b) \sqcup x_{\mathrm{Nil},\mathrm{Nil}}))
\end{aligned}
$$

As $\iota(a,b) = \iota(b,a) = \infty$, $\iota(a,a) = \iota(b,b) = 0$, and $d_\mathbb{T}(4,3) \leq d_\mathbb{T}(0,3) = 3$ we can even reduce the above formulae to the semantically equivalent formulae

$$3 \sqcup x_{\mathrm{Nil},\mathrm{Nil}} \sqcup x_{P,Q}$$

Of course it is no coincidence that we arrive at more less the exact distance between P and Q, as the equations of $E_\mathcal{M}$ exactly encode the definition of $\Psi_\mathcal{M}$. Hence, we can even state the following lemma

Lemma 3. *If $d(m,n) = \rho(x_{m,n})$ for arbitrary $m,n \in M$, then $[\![E(x_{m,n})]\!]\rho = \Psi(d)(m,n)$*

Using this, one quickly arrives at the main result of this section, namely that we can encode our timed bisimilarity distance using Convex Lattice Equation Systems.

Theorem 6. $\mu\Psi_{\mathcal{M}}(m,n) \leq \varepsilon$ *iff* $\models_{E_{\mathcal{M}}} x_{m,n} \leq \varepsilon$.

Corollary 1. $\mu\Psi_{\mathcal{M}}(m,n) \leq \varepsilon$ *iff* $\vdash_{E_{\mathcal{M}}} x_{m,n} \leq \varepsilon$.

Example 8. Let us finally reconsider the TCCS processes P and Q from Example 7. Here we give the proof tree for $\vdash_{E_{\mathcal{M}}} x_{P,Q} \leq 3$ under the reduced defining Convex Lattice Equation System:

$$\begin{aligned} x_{P,Q} &= 3 \sqcup x_{\mathrm{Nil,Nil}} \sqcup x_{P,Q} \\ x_{\mathrm{Nil,Nil}} &= 0 \end{aligned}$$

$$\dfrac{\dfrac{\dfrac{}{x_{P,Q} \leq 3 \vdash_{E_{\mathcal{M}}} 3 \leq 3}\,(A_5) \qquad \dfrac{\dfrac{\dfrac{}{x_{\mathrm{Nil,Nil}}, x_{P,Q} \leq 3 \vdash_{E_{\mathcal{M}}} 0 \leq 0}\,(A_5)}{x_{\mathrm{Nil,Nil}}, x_{P,Q} \leq 3 \vdash_{E_{\mathcal{M}}} 0 \leq 3}\,(A_2)}{x_{P,Q} \leq 3 \vdash_{E_{\mathcal{M}}} x_{\mathrm{Nil,Nil}} \leq 3}\,(A_4)}{x_{P,Q} \leq 3 \vdash_{E_{\mathcal{M}}} 3 \sqcup x_{\mathrm{Nil,Nil}} \leq 3}\,(A_6) \qquad \dfrac{}{x_{P,Q} \leq 3 \vdash_{E_{\mathcal{M}}} x_{P,Q} \leq 3}\,(A_3)}{\dfrac{x_{P,Q} \leq 3 \vdash_{E_{\mathcal{M}}} (3 \sqcup x_{\mathrm{Nil,Nil}}) \sqcup x_{P,Q} \leq 3}{\vdash_{E_{\mathcal{M}}} x_{P,Q} \leq 3}\,(A_4)}\,(A_6)$$

□

6 Conclusion

More than 10 years ago, Henzinger advocated the use of *quantitative* notions of correctness, as opposed to *Boolean*, for a more refined view of a quantitative system which, if not fully correct, can still be correct up to a certain degree. Taking to hear Henzinger's suggestion, in this paper we proposed a quantitative extension of [Lar92]. The result of this effort is *Convex Lattice Equation Systems* (CLES), a universal framework for encoding abstract quantitative notions of correctness, such as behavioral metrics for probabilistic and timed systems. We presented a sound and complete proof system for checking consistency of statements of the form $E \leq \varepsilon$ over a CLES, where E is an convex lattice expression expressing some property of the CLES and ε is an element from the complete lattice expressing a bound. To demonstrate the generality of this framework, we showed how value functions of Simple Stochastic Games and behavioural distances between timed systems may be encoded using CLES. We also showed examples of proof derivations which exploits the local exploration of the equations of a CLES to check consistency statements. As in [Lar92], this proof system paves the way for an on-the-fly algorithm for checking consistency statements over a CLES.

References

[AAE+15] Jesper Rank Andersen, Nicklas Andersen, Søren Enevoldsen, Mathias M. Hansen, Kim G. Larsen, Simon R. Olesen, Jirí Srba, and Jacob K. Wortmann. CAAL: concurrency workbench, aalborg edition. In Martin Leucker, Camilo Rueda, and Frank D. Valencia, editors, *Theoretical Aspects of Computing - ICTAC 2015 - 12th International Colloquium Cali, Colombia, October 29-31, 2015, Proceedings*, volume 9399 of *Lecture Notes in Computer Science*, pages 573–582. Springer, 2015.

[ACD+93] Bernard Algayres, Veronigue Coelho, Laurent Doldi, Hubert Garavel, Yves Lejeune, and Carlos Rodríguez. VESAR: A pragmatic approach to formal specification and verification. *Comput. Networks ISDN Syst.*, 25(7):779–790, 1993.

[And92] Henrik Reif Andersen. Model checking and boolean graphs. In Bernd Krieg-Brückner, editor, *ESOP '92, 4th European Symposium on Programming, Rennes, France, February 26-28, 1992, Proceedings*, volume 582 of *Lecture Notes in Computer Science*, pages 1–19. Springer, 1992.

[BBL+21] Giorgio Bacci, Giovanni Bacci, Kim G. Larsen, Radu Mardare, Qiyi Tang, and Franck van Breugel. Computing Probabilistic Bisimilarity Distances for Probabilistic Automata. *Log. Methods Comput. Sci.*, 17(1), 2021.

[BBLM13a] Giorgio Bacci, Giovanni Bacci, Kim G. Larsen, and Radu Mardare. Computing behavioral distances, compositionally. In Krishnendu Chatterjee and Jirí Sgall, editors, *Mathematical Foundations of Computer Science 2013 - 38th International Symposium, MFCS 2013, Klosterneuburg, Austria, August 26-30, 2013. Proceedings*, volume 8087 of *Lecture Notes in Computer Science*, pages 74–85. Springer, 2013.

[BBLM13b] Giorgio Bacci, Giovanni Bacci, Kim G. Larsen, and Radu Mardare. On-the-fly exact computation of bisimilarity distances. In Nir Piterman and Scott A. Smolka, editors, *Tools and Algorithms for the Construction and Analysis of Systems - 19th International Conference, TACAS 2013, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2013, Rome, Italy, March 16-24, 2013. Proceedings*, volume 7795 of *Lecture Notes in Computer Science*, pages 1–15. Springer, 2013.

[BBLM16] Giorgio Bacci, Giovanni Bacci, Kim G. Larsen, and Radu Mardare. Complete axiomatization for the bisimilarity distance on markov chains. In Josée Desharnais and Radha Jagadeesan, editors, *27th International Conference on Concurrency Theory, CONCUR 2016, August 23-26, 2016, Québec City, Canada*, volume 59 of *LIPIcs*, pages 21:1–21:14. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2016.

[BBLM18] Giorgio Bacci, Giovanni Bacci, Kim G. Larsen, and Radu Mardare. Complete axiomatization for the total variation distance of markov chains. In Sam Staton, editor, *Proceedings of the Thirty-Fourth Conference on the Mathematical Foundations of Programming Semantics, MFPS 2018, Dalhousie University, Halifax, Canada, June 6-9, 2018*, volume 341 of *Electronic Notes in Theoretical Computer Science*, pages 27–39. Elsevier, 2018.

[CGL93] Karlis Cerans, Jens Chr. Godskesen, and Kim G Larsen. Timed modal specification – theory and tools. In *Proceedings of Computer Aided Verification, CAV 1993*, 1993.

[Con90] Anne Condon. On Algorithms for Simple Stochastic Games. In *Advances In Computational Complexity Theory*, volume 13 of *DIMACS Series in*

Discrete Mathematics and Theoretical Computer Science, pages 51–72. DIMACS/AMS, 1990.

[Con92] Anne Condon. The Complexity of Stochastic Games. *Inf. Comput.*, 96(2):203–224, 1992.

[CPS89] Rance Cleaveland, Joachim Parrow, and Bernhard Steffen. The concurrency workbench. In Joseph Sifakis, editor, *Automatic Verification Methods for Finite State Systems, International Workshop, Grenoble, France, June 12-14, 1989, Proceedings*, volume 407 of *Lecture Notes in Computer Science*, pages 24–37. Springer, 1989.

[CvBW12] Di Chen, Franck van Breugel, and James Worrell. On the complexity of computing probabilistic bisimilarity. In Lars Birkedal, editor, *Foundations of Software Science and Computational Structures - 15th International Conference, FOSSACS 2012, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2012, Tallinn, Estonia, March 24 - April 1, 2012. Proceedings*, volume 7213 of *Lecture Notes in Computer Science*, pages 437–451. Springer, 2012.

[DGJP04] Josée Desharnais, Vineet Gupta, Radha Jagadeesan, and Prakash Panangaden. Metrics for labelled markov processes. *Theor. Comput. Sci.*, 318(3):323–354, 2004.

[DLT08] Josée Desharnais, François Laviolette, and Mathieu Tracol. Approximate analysis of probabilistic processes: Logic, simulation and games. In *Fifth International Conference on the Quantitative Evaluaiton of Systems (QEST 2008), 14-17 September 2008, Saint-Malo, France*, pages 264–273. IEEE Computer Society, 2008.

[EC01] Steve M. Easterbrook and Marsha Chechik. A framework for multi-valued reasoning over inconsistent viewpoints. In Hausi A. Müller, Mary Jean Harrold, and Wilhelm Schäfer, editors, *Proceedings of the 23rd International Conference on Software Engineering, ICSE 2001, 12-19 May 2001, Toronto, Ontario, Canada*, pages 411–420. IEEE Computer Society, 2001.

[FTL11] Uli Fahrenberg, Claus R. Thrane, and Kim G. Larsen. Distances for weighted transition systems: Games and properties. In Mieke Massink and Gethin Norman, editors, *Proceedings Ninth Workshop on Quantitative Aspects of Programming Languages, QAPL 2011, Saarbrücken, Germany, April 1-3, 2011*, volume 57 of *EPTCS*, pages 134–147, 2011.

[GLMS11] Hubert Garavel, Frédéric Lang, Radu Mateescu, and Wendelin Serwe. CADP 2010: A toolbox for the construction and analysis of distributed processes. In Parosh Aziz Abdulla and K. Rustan M. Leino, editors, *Tools and Algorithms for the Construction and Analysis of Systems - 17th International Conference, TACAS 2011, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2011, Saarbrücken, Germany, March 26-April 3, 2011. Proceedings*, volume 6605 of *Lecture Notes in Computer Science*, pages 372–387. Springer, 2011.

[Gou08] Jean Goubault-Larrecq. Prevision domains and convex powercones. In *FoSSaCS*, volume 4962 of *Lecture Notes in Computer Science*, pages 318–333. Springer, 2008.

[Hen10] Thomas A. Henzinger. From boolean to quantitative notions of correctness. In Manuel V. Hermenegildo and Jens Palsberg, editors, *Proceedings of the 37th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2010, Madrid, Spain, January 17-23, 2010*, pages 157–158. ACM, 2010.

[HMP05] Thomas A. Henzinger, Rupak Majumdar, and Vinayak S. Prabhu. Quantifying similarities between timed systems. In Paul Pettersson and Wang Yi, editors, *Formal Modeling and Analysis of Timed Systems, Third International Conference, FORMATS 2005, Uppsala, Sweden, September 26-28, 2005, Proceedings*, volume 3829 of *Lecture Notes in Computer Science*, pages 226–241. Springer, 2005.

[HS06] Thomas A. Henzinger and Joseph Sifakis. The embedded systems design challenge. In Jayadev Misra, Tobias Nipkow, and Emil Sekerinski, editors, *FM 2006: Formal Methods, 14th International Symposium on Formal Methods, Hamilton, Canada, August 21-27, 2006, Proceedings*, volume 4085 of *Lecture Notes in Computer Science*, pages 1–15. Springer, 2006.

[Jub05] Brendan Juba. On the Hardness of Simple Stochastic Games. Master's thesis, Carnegie Mellon University, Pittsburgh, PA, USA, May 2005.

[KL10] Orna Kupferman and Yoad Lustig. Latticed simulation relations and games. *Int. J. Found. Comput. Sci.*, 21(2):167–189, 2010.

[Lar92] Kim Guldstrand Larsen. Efficient local correctness checking. In *CAV*, volume 663 of *Lecture Notes in Computer Science*, pages 30–43. Springer, 1992.

[LFT11] Kim G. Larsen, Uli Fahrenberg, and Claus R. Thrane. Metrics for weighted transition systems: Axiomatization and complexity. *Theor. Comput. Sci.*, 412(28):3358–3369, 2011.

[LL69] Thomas Liggett and Steven A. Lippman. Stochastic Games with Perfect Information and Time Average Payoff. *SIAM Review*, 11(4):604–607, 1969.

[LS89] Kim Guldstrand Larsen and Arne Skou. Bisimulation through probabilistic testing. In *Conference Record of the Sixteenth Annual ACM Symposium on Principles of Programming Languages, Austin, Texas, USA, January 11-13, 1989*, pages 344–352. ACM Press, 1989.

[LS98] Xinxin Liu and Scott A. Smolka. Simple linear-time algorithms for minimal fixed points (extended abstract). In Kim Guldstrand Larsen, Sven Skyum, and Glynn Winskel, editors, *Automata, Languages and Programming, 25th International Colloquium, ICALP'98, Aalborg, Denmark, July 13-17, 1998, Proceedings*, volume 1443 of *Lecture Notes in Computer Science*, pages 53–66. Springer, 1998.

[Man08] K.L. Man. mucrl: A computer science based approach for specification and verification of hardware circuits. 01:I–387–I–390, 2008.

[Mis00] Michael W. Mislove. Nondeterminism and probabilistic choice: Obeying the laws. In *CONCUR*, volume 1877 of *Lecture Notes in Computer Science*, pages 350–364. Springer, 2000.

[Ros19] Amnon Rosenmann. On the distance between timed automata. In Étienne André and Mariëlle Stoelinga, editors, *Formal Modeling and Analysis of Timed Systems - 17th International Conference, FORMATS 2019, Amsterdam, The Netherlands, August 27-29, 2019, Proceedings*, volume 11750 of *Lecture Notes in Computer Science*, pages 199–215. Springer, 2019.

[Tar55] Alfred Tarski. A lattice-theoretical fixpoint theorem and its applications. *Pacific journal of Mathematics*, 5(2):285–309, 1955.

[TFL10] Claus R. Thrane, Uli Fahrenberg, and Kim G. Larsen. Quantitative analysis of weighted transition systems. *J. Log. Algebraic Methods Program.*, 79(7):689–703, 2010.

[TKP09] Regina Tix, Klaus Keimel, and Gordon D. Plotkin. Semantic domains for combining probability and non-determinism. *Electron. Notes Theor. Comput. Sci.*, 222:3–99, 2009.

[TvB16] Qiyi Tang and Franck van Breugel. Computing probabilistic bisimilarity distances via policy iteration. In *CONCUR*, volume 59 of *LIPIcs*, pages 22:1–22:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2016.

[VW06] Daniele Varacca and Glynn Winskel. Distributing probability over non-determinism. *Math. Struct. Comput. Sci.*, 16(1):87–113, 2006.

[Yi90] Wang Yi. Real-time behaviour of asynchronous agents. In Jos C. M. Baeten and Jan Willem Klop, editors, *CONCUR '90, Theories of Concurrency: Unification and Extension, Amsterdam, The Netherlands, August 27-30, 1990, Proceedings*, volume 458 of *Lecture Notes in Computer Science*, pages 502–520. Springer, 1990.

[Yi91] Wang Yi. CCS + time = an interleaving model for real time systems. In Javier Leach Albert, Burkhard Monien, and Mario Rodríguez-Artalejo, editors, *Automata, Languages and Programming, 18th International Colloquium, ICALP91, Madrid, Spain, July 8-12, 1991, Proceedings*, volume 510 of *Lecture Notes in Computer Science*, pages 217–228. Springer, 1991.