Computing and Informatics, Vol. 29, 2010, 1311–1324

A QUANTITATIVE CHARACTERIZATION OF WEIGHTED KRIPKE STRUCTURES IN TEMPORAL LOGIC

Uli Fahrenberg, Kim G. Larsen, Claus Thrane

Department of Computer Science
Aalborg University
Selma Lagerlöfs Vej 300
9220 Aalborg
Denmark
e-mail: {uli, kgl, crt}@cs.aau.dk

Revised manuscript received 11 May 2010

Abstract. We extend the usual notion of Kripke structures with a weighted transition relation and generalize the classical Boolean interpretation of CTL to a map which assigns to states and temporal formulae a real-valued distance describing the degree of satisfaction. We describe a general approach to obtaining quantitative interpretations for a generic extension of the CTL syntax and show that, for one such interpretation, the logic is both *adequate* and *expressive* with respect to quantitative bisimulation.

Keywords: Quantitative analysis, multi-valued CTL, weighted Kripke structures, bisimulation distances, system metrics

Mathematics Subject Classification 2000: 68Q85, 68Q60, 68N30

1 INTRODUCTION

Using logics for analysis of concurrent and reactive systems is a well-established approach [1], but the standard qualitative techniques are arguably insufficient when reasoning about *quantitative* aspects. Indeed, it can be argued that in a setting where system models and properties include both discrete and continuous, i.e. quantitative, information, e.g. real-time or probabilistic systems, a quantitative approach

is necessary. The focus of this paper is to provide insight as to how expressivity results may be obtained in a framework addressing this issue.

A number of extensions of temporal logics have been proposed with the purpose of providing verification techniques for real-world systems where the properties one is interested in go beyond behavioral quality, by addressing certain quantitative aspects such as *time*, *probabilities* or *cost* related to realizing the behavior.

Most notably, both probabilistic and timed versions of LTL and CTL [4] have been introduced, by allowing formulae to be interpreted over probabilistic or timed models. In these, satisfaction of path formulae is subject to constraints on quantitative information encoded in the models, by weights typically drawn from the set of real numbers. This allows specification and verification of properties such as "the probability of reaching state A is .5." or "P holds within 5.7 time units". This approach is utilized in verification tools such as PRISM [11, 16] and UPPAAL [12] to provide simple and expressive ways to represent properties of models.

From a more general perspective, multi-valued interpretations of CTL* and the μ-calculus have been proposed by interpreting formulae over models endowed with weights drawn from structures such as a *semirings* [13] or *quasi-Boolean lattices* [9]. This of course allows broader interpretation of weights, but more importantly allows truth values to be more descriptive, as formulae may take any value in the chosen weight domain as opposed to their Boolean counterparts. To see the benefits of this approach, we may simply consider devising a formula which evaluates to the number of times a classical property is violated over a path. In light of this, a number of recent papers [2, 3, 8] have been advocating the use of multi-valued interpretations of temporal logics for *games*, general *quantitative transition systems* and real-time systems.

A shared aim of most of the these extensions – e.g. [2, 8, 10, 13] – is to maintain a certain level of expressive power so as to be able to characterize bisimulation, generalizing the results from [5] for CTL. Hence one wants to show that the logic is in fact *adequate* to distinguish any non-bisimilar models and that the logic is *expressive* enough to build characteristic formulae of models.

In this paper we consider both properties, in the search of a generic approach to *discounted* multi-valued extensions of CTL and corresponding bisimulations, which likewise provide a measure on the relationship between states.

In addition to the multi-valued and annotative approach, both of which we refer to as *quantitative model checking*, there are different ways of extending the usual Kripke structures, and logics, with quantitative information. One can allow either a quantitative interpretation of atomic propositions, or extend the model with a weighted transition relation (in [9] referred to as an *accessibility* relation) [6, 7], or both. In this paper we choose the latter as it seems to admit more elegant proofs. Additionally, we retain the useful features from the syntax of timed and probabilistic CTL which allow specification of expected values along a path.

In [2], multi-valued (or quantitative) LTL and μ-calculus are presented in which propositions, instead, map states to weights in the interval $[0, 1]$, using a pointwise semantics similar to the one presented here. Because the syntax allows only

the evaluation of an atomic proposition at states, and not specifying its expected value, additional operators are required to gain expressiveness. On the other hand, the *discounted* CTL presented in [8] considers atomic propositions to be Boolean ($\bot = 0$ and $\top = 1$), and uses the time elapsed until a satisfying event occurs to discount the value of the formula.

In [2, 8, 10, 13], only adequacy of the respective logics is considered. In [2] it is shown that a restricted subset of the presented quantitative μ-calculus is adequate to characterize the distance relating states, in a variant of *point-wise bisimulation*. Similarly [8] shows that, for a given discounted CTL formula, *maximum-lead bisimulation* (another quantitative relation which we will not be concerned with here) provides an upper bound on the absolute difference of the formula evaluated at the corresponding states.

In the more general setting of [10], the authors consider the relationship of multi-valued CTL* and the notion of multi-valued bisimulation which (in the classical Boolean sense) relates states that allow the same (qualitative) behavior, and where the weights of atomic propositions at states are partitioned to be within some set of designated truth values. Finally [13] shows that strong bisimilarity of states implies that all formulae evaluate to the same element from the semiring considered for the corresponding pair of states.

As a final note on related subjects we note that, cf. also [3, 8], the present approach to quantitative analysis in terms of multi-valued or quantitative temporal logic and bisimulation is closely related to the notion of *robustness*, i.e. the tolerance for estimation errors and imprecision, see also [15, 18], which provides more realistic analysis for real-world applications than the idealized semantics otherwise considered. Treatment of these robustness issues is not within the scope of this paper.

1.1 Contribution

We present a general approach to quantitative analysis and approximate characterizations of *weighted Kripke structures* (WKS) using formulae expressed in a weighted extension of CTL (WCTL). The theory presented here is an extension of a general framework for quantitative analysis of reactive systems presented in [17].

The goal of [17] was to set the scene for a generic approach to simulation-based analysis, measuring the degree with which one system may simulate another. Developing this paradigm, the current objective is to extend the analysis to verification of *specifications in temporal logic*. Thus we introduce here a matching quantitative semantics for WCTL which lifts the usual Boolean satisfaction relation of the logic to a function mapping formulae and states to $\mathbb{R}_{\geq 0} \cup \{\infty\}$, with $\top = 0$ and $\bot = \infty$. We show that with this semantics, WCTL is both *adequate* and *expressive* with respect to one of the quantitative bisimulation relations introduced in [17].

2 PRELIMINARIES

As in [17], the generalizations presented in this paper are based on metrics on sequences of real numbers. Let $a = (a_i)$ and $b = (b_i)$ be such sequence; we then define for $\lambda \in]0,1[$ the following basic distances:

$$d_+(a,b) = \sum_i \lambda^i |a_i - b_i| \tag{1}$$

$$d_\bullet(a,b) = \sup_i \{\lambda^i |a_i - b_i|\}. \tag{2}$$

Throughout the paper we will refer to (1) and (2), as well as to other distances based on these, as an *accumulating distance* and as a *point-wise distance*, respectively. For the rest of this paper we fix a discounting factor $\lambda \in]0,1[$.

The model which we shall consider is that of *weighted Kripke structures* (WKS), which represents a straight-forward extension of Kripke structures with a weighted transition relation labeling each transition. A natural interpretation is to view the labellings as the cost of taking transitions in the structure. This extension is similar to that one presented in [17] for labeled transition systems; thus the results presented in this paper are transferable to the current setting.

Definition 1. For a finite set $\mathcal{AP}$ of atomic propositions, a *weighted Kripke structure* is a quadruple $M = (S, T, \mathcal{L}, w)$ where

- S is a finite set of states
- $T \subseteq S \times S$ is a transition relation
- $\mathcal{L} : S \to 2^{\mathcal{AP}}$ is the proposition labeling, and
- $w : T \to \mathbb{R}_{\geq 0}$ assigns a positive real-valued weight to transitions.

We write $s \to s'$ instead of $(s,s') \in R$ and $s \xrightarrow{w} s'$ to indicate $w(s,s') = w$.

A *(weighted) path* in a WKS $M = (S, T, \mathcal{L}, w)$ is a (possibly infinite) sequence $\sigma = ((s_0,w_0),(s_1,w_1),(s_2,w_2),\ldots)$ with $(s_i,w_i) \in S \times \mathbb{R}_{\geq 0}$ and such that $s_i \to s_{i+1}$ and $w_i = w(s_i,s_{i+1})$ for all i. We denote by $\mathsf{P}(s)$ the set of paths in M starting at state s, and by $\mathsf{P}(M)$ the set of all paths in M. Given path σ, we write $\sigma(i) = (\sigma(i)_s, \sigma(i)_w)$ for its i-th state-weight pair, and σ^i for the suffix starting at $\sigma(i)$.

Notice that we have restricted ourselves to *finite* weighted Kripke structures here, i.e. structures with a finite set of states and finitely many atomic propositions. Our characterization results in Section 5 only hold for such finite structures.

Example 1. Figure 1 gives a model of a simple printer as a WKS which we shall come back to again later. Resource usage is modeled as atomic propositions, and transition weights model the combined cost of the operations. Turning on the machine, it moves from the state **Off** to **Ready**, from where it can **Suspend** and wake up at a much lower cost. Input is processed in the **Receiving** state, and the chosen output form incurs different costs related to resource usage, clean-up and reset.

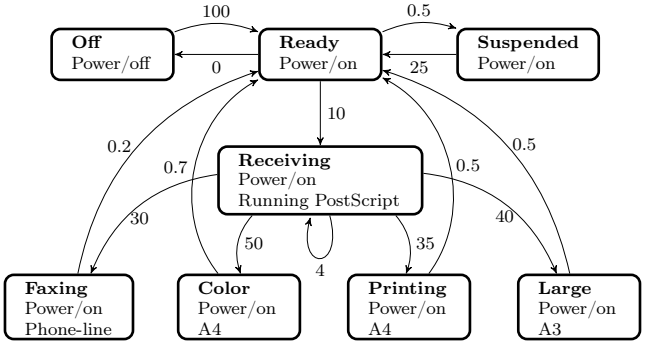

Fig. 1. The behavior and cost and resource usage of a simple printer

3 WEIGHTED CTL

We now consider two interpretations of *weighted CTL* (WCTL), based on (1) and (2), which will encompass quantitative information by two means. Firstly, as with TCTL and PCTL, syntactic extension of path operators, by annotation of real numbers (weights), modeling requirements on path weights (the exact meaning of these are deferred to the choice of semantics). Secondly, satisfaction of a formula by a system is no longer interpreted in the Boolean domain $\{\top, \bot\}$, but rather assigns to a state a truth value in the domain $\mathbb{R}_{\geq 0} \cup \{\infty\}$. We will interpret 0 as an exact match, whereas ∞ indicates an incompatibility between the system and the specified atomic propositions of a formula. Any intermediate value is interpreted as real-valued distance (from an exact match). That is, a smaller distance means a closer (better) match of the specified weights in the formula. We denote by $[\![\varphi]\!](s) \in \mathbb{R}_{\geq 0} \cup \{\infty\}$ the value obtained by evaluating formula φ at state s.

From here on, we fix a set $\mathcal{AP}$ of atomic propositions and a WKS $(S, T, \mathcal{L}, w)$. All definitions and results below will be given for the states of one single WKS, but we note that to relate states of different WKS, one can simply form the disjoint union.

Definition 2. For $\mathsf{p} \in \mathcal{AP}$, Φ generates the set of state formulae, and Ψ the set of path formulae, annotated by weights $c \in \mathbb{R}_{\geq 0}$, according to the following abstract syntax:

$$\Phi ::= \mathsf{p} \mid \neg\mathsf{p} \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid \mathsf{E}\Psi \mid \mathsf{A}\Psi$$
$$\Psi ::= \mathsf{X}_c\Phi \mid \mathsf{G}_c\Phi \mid \mathsf{F}_c\Phi \mid [\Phi_1 \mathsf{U}_c \Phi_2].$$

The WCTL logic is the set of state formulae, written $\mathcal{L}_w(\mathcal{AP})$ or simply $\mathcal{L}_w$.

Before presenting the formal semantics, let us consider the usual meaning of the CTL modalities, as well as how these may be generalized to ensure adherence to bisimulation variants considered in the following section:

Given CTL propositions on the form $M, s \models \mathsf{E}\psi$ and $M, s \models \mathsf{A}\psi$, we may interpret these as infinite *existential*, or *universal*, quantifications over paths in M from s satisfying ψ. Similarly, $M, \sigma \models \mathsf{F}\varphi$ and $M, \sigma \models \mathsf{G}\varphi$ may be interpreted as an infinite *disjunction*, or *conjunction*, over propositions on the form $M, s_i \models \varphi$ for $i \geq 0$, where s_i is a state on σ.

This observation is in line with some arguments given in [10], and we expect that a generic approach to defining quantitative (or multi-valued) semantics for WCTL over the truth domain $\mathbb{R}_{\geq 0} \cup \{\infty\}$ is obtainable. To this end, the standard sup and inf operators are reasonable generalization of E,A,F and G (interpreted as disjunction and conjunction over the standard Boolean domain) to the (complete) lattice $\mathbb{R}_{\geq 0} \cup \{\infty\}$.

Furthermore, this approach requires only modification to the evaluation (i.e. semantics) of path formulae. Our semantics specializes to the usual one in two different ways: either by mapping to the designated set of truth values (i.e. to $\top$), all $\varepsilon < \infty$ and ∞ to $\bot$, or by mapping only 0 to $\top$ and all $\varepsilon > 0$ to $\bot$.

3.1 Semantics

In the following we present two *discounted semantics*, derived from the distances d_+ from (1), and $d_\bullet$ from (2) where weights of transition are accumulated or considered point-wise. Formally, the semantics of $\varphi \in \mathcal{L}_w$ defines a map from the set of states S to the set $\mathbb{R}_{\geq 0} \cup \{\infty\}$. The first definition gives a general weighted semantics to state formulae:

Definition 3 (State semantics)**.** The semantics of state formulae is defined inductively as follows:

$$[\![\mathsf{p}]\!](s) = \begin{cases} 0 & \text{if } \mathsf{p} \in \mathcal{L}(s) \\ \infty & \text{otherwise} \end{cases} \qquad [\![\neg\mathsf{p}]\!](s) = \begin{cases} 0 & \text{if } \mathsf{p} \in \mathcal{AP} \setminus \mathcal{L}(s) \\ \infty & \text{otherwise} \end{cases}$$

$$[\![\varphi_1 \vee \varphi_2]\!](s) = \inf\{[\![\varphi_1]\!](s), [\![\varphi_2]\!](s)\} \qquad [\![\varphi_1 \wedge \varphi_2]\!](s) = \sup\{[\![\varphi_1]\!](s), [\![\varphi_2]\!](s)\}$$

$$[\![\mathsf{E}\psi]\!](s) = \inf\{[\![\psi]\!](\sigma) \mid \sigma \in \mathsf{P}(s)\} \qquad [\![\mathsf{A}\psi]\!](s) = \sup\{[\![\psi]\!](\sigma) \mid \sigma \in \mathsf{P}(s)\}.$$

In the last two formulae, $[\![\psi]\!](\sigma)$ is the accumulating or point-wise semantics of σ with respect to ψ as appropriate, see below.

In the next definition, we give the two different weighted semantics to path formulae; an accumulated and a point-wise one. Note that the only difference between the two is an interchange of maximum and sum, which supports the findings in [10, 13] which advocates abstracting away from concrete operators and interpreting the semantics over general algebraic structures.

Definition 4 (Path semantics)**.** The *accumulating* semantics of path formulae is defined inductively as follows:

$$\begin{aligned}
[\![\varphi]\!]_+(\sigma) &= [\![\varphi]\!](\sigma(0)_s)\\
[\![\mathsf{X}_c\varphi]\!]_+(\sigma) &= |\sigma(0)_w - c| + \lambda[\![\varphi]\!]_+(\sigma^1)\\
[\![\mathsf{F}_c\varphi]\!]_+(\sigma) &= \inf_k \left(\sum_{j=0}^{k-1} \lambda^j \Big|\sigma(j)_w - c\Big| + \lambda^k [\![\varphi]\!]_+(\sigma^k) \right)\\
[\![\mathsf{G}_c\varphi]\!]_+(\sigma) &= \sup_k \left(\sum_{j=0}^{k-1} \lambda^j \Big|\sigma(j)_w - c\Big| + \lambda^k [\![\varphi]\!]_+(\sigma^k) \right)\\
[\![\varphi_1 \mathsf{U}_c \varphi_2]\!]_+(\sigma) &= \inf_k \left(\sum_{j=0}^{k-1} \lambda^j \Big|[\![\varphi_1]\!]_+(\sigma^j) - c\Big| + \lambda^k [\![\varphi_2]\!]_+(\sigma^k) \right)
\end{aligned}$$

The *point-wise* semantics of path formulae is defined inductively as follows:

$$\begin{aligned}
[\![\varphi]\!]_\bullet(\sigma) &= [\![\varphi]\!](\sigma(0)_s)\\
[\![\mathsf{X}_c\varphi]\!]_\bullet(\sigma) &= \max\Big\{|\sigma(0)_w - c|,\ \lambda[\![\varphi]\!]_\bullet(\sigma^1)\Big\}\\
[\![\mathsf{F}_c\varphi]\!]_\bullet(\sigma) &= \inf_k \left(\max\Big\{ \max_{0\le j<k} \big\{\lambda^j |\sigma(j)_w - c|\big\},\ \lambda^k [\![\varphi]\!]_\bullet(\sigma^k)\Big\}\right)\\
[\![\mathsf{G}_c\varphi]\!]_\bullet(\sigma) &= \sup_k \left(\max\Big\{ \max_{0\le j<k} \big\{\lambda^j |\sigma(j)_w - c|\big\},\ \lambda^k [\![\varphi]\!]_\bullet(\sigma^k)\Big\}\right)\\
[\![\varphi_1 \mathsf{U}_c \varphi_2]\!]_\bullet(\sigma) &= \inf_k \left(\max\Big\{ \max_{0\le j<k} \big\{\lambda^j \big|[\![\varphi_1]\!]_\bullet(\sigma^j) - c\big|\big\},\ \lambda^k [\![\varphi_2]\!]_\bullet(\sigma^k)\Big\}\right)
\end{aligned}$$

Note that as usual, F_c can also be derived from U_c by $\mathsf{F}_c\varphi \triangleq \mathsf{tt}\mathsf{U}_c\varphi$ (where tt is a tautology).

Compared to e.g. TCTL, the annotated operators specify an expected value, hence $\mathsf{X}_c\varphi$ evaluated on σ means that c is expected of the first transition in σ. The difference is then added to (or the maximum is taken of it and) the value of φ over the remaining path σ^1.

Example 2. In the context of the example from Figure 1 we consider a useful property of printers, that of *having received a job, the printer cannot suspend before completing the job.* The formula $\varphi = \mathsf{A}(\neg\textbf{Suspended}\ \mathsf{U}_{10}\ \textbf{Ready})$ formalizes this qualitative property and also states that we expect to reach the **Ready** state using transitions with cost 10. With $\lambda = .9$, the point-wise interpretation $[\![\varphi]\!]_\bullet(\textbf{Receiving}) = 40$ is the cost (minus 10) of the transition in the computation tree which is furthest from 10. In the accumulating interpretation, $[\![\varphi]\!]_+(\textbf{Receiving}) = 48.37$ yields the sum of all such differences.

4 BISIMULATION

We now consider extensions of *strong bisimulation* [14] over WKS, based on (1) and (2). These are filling the gap between *unweighted* and *weighted* strong bisimulation as defined below:

Definition 5. Let $(S, T, \mathcal{L}, w)$ be a WKS on a set $\mathcal{AP}$ of atomic propositions. A relation $B \subseteq S \times S$ is

- an *unweighted bisimulation* provided that for all $(s,t) \in B$, $\mathcal{L}(s) = \mathcal{L}(t)$ and

  if $s \to s'$, then also $t \to t'$ and $(s', t') \in B$ for some $t' \in S'$,
  if $t \to t'$, then also $s \to s'$ and $(s', t') \in B$ for some $s' \in S$;

- a *(weighted) bisimulation* provided that for all $(s,t) \in B$, $\mathcal{L}(s) = \mathcal{L}(t)$ and

  if $s \xrightarrow{c} s'$, then also $t \xrightarrow{c} t'$ and $(s', t') \in B$ for some $t' \in S'$,
  if $t \xrightarrow{c} t'$, then also $s \xrightarrow{c} s'$ and $(s', t') \in B$ for some $s' \in S$.

We write $s \overset{u}{\sim} t$ if $(s,t) \in B$ for some unweighted bisimulation B, and $s \sim t$ if $(s,t) \in B$ for some weighted bisimulation B.

The motivation for the variants defined below is that, in order to relate structures, we do not always need perfect matching of transition weights; rather we would like to know how accurately weights are matched. As with the simulation distances of [17], we call a *bisimulation distance* any pseudometric on the states of a WKS which mediates between unweighted and weighted bisimilarity:

Definition 6. A *bisimulation distance* on a WKS $(S, T, \mathcal{L}, w)$ is a function $d : S \times S \to \mathbb{R}_{\geq 0} \cup \{\infty\}$ which satisfies the following for all $s_1, s_2, s_3 \in S$:

- $d(s_1, s_1) = 0$,
- $d(s_1, s_2) + d(s_2, s_3) \geq d(s_1, s_3)$,
- $d(s_1, s_2) = d(s_2, s_1)$,
- $s_1 \sim s_2$ implies $d(s_1, s_2) = 0$ and
- $d(s_1, s_2) \neq \infty$ implies $s_1 \overset{u}{\sim} s_2$

Our distances are based on distances of (infinite) sequences of real numbers, which is appropriate as for (s,t) in $\overset{u}{\sim}$ (or $\sim$), any path $(s, a, s_1, a_1 s_2, \dots) \in \mathsf{P}(s)$ must be matched by an equal-length path $(t, b, t_1, b_1, t_2, \dots) \in \mathsf{P}(t)$ with (s_i, t_i) in $\overset{u}{\sim}$ (or $\sim$).

By extending bisimulation with the d_+ and $d_\bullet$ distances, we collect a family of relations $\{\mathcal{R}_\varepsilon \subseteq S \times S\}$ (i.e. a map $\mathbb{R}_{\geq 0} \to 2^{S \times S}$) since, due to discounting, for each step the distance between each successor pair may grow:

Definition 7. A family of relations $\mathbf{R} = \{\mathcal{R}_\varepsilon \subseteq S \times S \mid \varepsilon > 0\}$ is

- an *accumulating bisimulation family* provided that for all $(s,t) \in \mathcal{R}_\varepsilon \in \mathbf{R}$, $\mathcal{L}(s) = \mathcal{L}(t)$ and
  - if $s \xrightarrow{c} s'$, then also $t \xrightarrow{d} t'$ with $|c-d| \leq \varepsilon$ for some $d \in \mathbb{R}_{\geq 0}$ and $(s',t') \in \mathcal{R}_{\varepsilon'} \in \mathbf{R}$ with $\varepsilon'\lambda \leq \varepsilon - |c-d|$, and
  - if $t \xrightarrow{c} t'$, then also $s \xrightarrow{d} s'$ with $|c-d| \leq \varepsilon$ for some $d \in \mathbb{R}_{\geq 0}$ and $(s',t') \in \mathcal{R}_{\varepsilon'} \in \mathbf{R}$ with $\varepsilon'\lambda \leq \varepsilon - |c-d|$;
- a *point-wise bisimulation family* provided that for all $(s,t) \in \mathcal{R}_\varepsilon \in \mathbf{R}$, $\mathcal{L}(s) = \mathcal{L}(t)$ and
  - if $s \xrightarrow{c} s'$, then also $t \xrightarrow{d} t'$ with $|c-d| \leq \varepsilon$ for some $d \in \mathbb{R}_{\geq 0}$ and $(s',t') \in \mathcal{R}_{\varepsilon'} \in \mathbf{R}$ with $\varepsilon'\lambda \leq \varepsilon$, and
  - if $t \xrightarrow{c} t'$, then also $s \xrightarrow{d} s'$ with $|c-d| \leq \varepsilon$ for some $d \in \mathbb{R}_{\geq 0}$ and $(s',t') \in \mathcal{R}_{\varepsilon'} \in \mathbf{R}$ with $\varepsilon'\lambda \leq \varepsilon$.

We write $s \overset{+}{\sim}_\varepsilon t$ and $s \dot{\sim}_\varepsilon t$, if $(s,t) \in \mathcal{R}_\varepsilon \in \mathbf{R}$ for an accumulating, or point-wise, bisimulation family $\mathbf{R}$.

Both variants of bisimulation families give rise to a bisimulation distance in the sense of Definition 6 by $d_+(s,t) = \inf\{\varepsilon \mid s \overset{+}{\sim}_\varepsilon t\}$ and $d_\bullet(s,t) = \inf\{\varepsilon \mid s \dot{\sim}_\varepsilon t\}$. Observe the following easy facts:

Lemma 8. 1. For $\varepsilon \leq \varepsilon'$ and members $\mathcal{R}_\varepsilon, \mathcal{R}_{\varepsilon'} \in \mathbf{R}$ of an accumulating or point-wise bisimulation family, $\mathcal{R}_\varepsilon \subseteq \mathcal{R}_{\varepsilon'}$.

2. Given $s \overset{+}{\sim}_\varepsilon t$, then every path $\sigma = (s_0, w_0, s_1, w_1 s_2, \dots) \in \mathsf{P}(s)$ has a corresponding path $\sigma' = (t_0, w_0', t_1, w_1' t_2, \dots) \in \mathsf{P}(t)$ such that $\varepsilon = \varepsilon_0$ and $s_i \overset{+}{\sim}_{\varepsilon_i} t_i$ for all i, where $\varepsilon_{i+1}\lambda = \varepsilon_i - |w_i - w_i'|$.

3. Given $s \dot{\sim}_\varepsilon t$, then every path $\sigma = (s_0, w_0, s_1, w_1 s_2, \dots) \in \mathsf{P}(s)$ has a corresponding path $\sigma' = (t_0, w_0', t_1, w_1' t_2, \dots) \in \mathsf{P}(t)$ such that $\varepsilon = \varepsilon_0$ and $s_i \dot{\sim}_{\varepsilon_i} t_i$ for all i, where $\varepsilon_{i+1}\lambda = \varepsilon_i$.

Note that as we only consider finite WKS, all $\mathcal{R}_\varepsilon$ relations are finite. Also, we shall speak of *corresponding paths* when referring to the second and third properties of the above lemma.

5 CHARACTERIZATION

In this section we show that the presented WCTL interpretations are adequate and expressive with respect to the appropriate bisimilarity variant.

5.1 Adequacy

The link between accumulating bisimilarity and our accumulating semantics for WCTL is as follows:

Theorem 9. For $s,t \in S$, $s \overset{+}{\sim}_\varepsilon t$ if and only if $\forall \varphi \in \mathcal{L}_w : \left|[\![\varphi]\!]_+(s) - [\![\varphi]\!]_+(t)\right| \leq \varepsilon$.

The proof follows from Lemmas 12 and 13 below. Observe that this provides us with the following corollary:

Corollary 10. For $s,t \in S$, $s \overset{+}{\sim}_0 t$ if and only if $[\![\varphi]\!]_+(s) = [\![\varphi]\!]_+(t)$ for all $\varphi \in \mathcal{L}_w$.

We obtain an equivalent result for the point-wise semantics:

Theorem 11. For $s,t \in S$, $s \dot{\sim}_\varepsilon t$ if and only if $\forall \varphi \in \mathcal{L}_w : \left|[\![\varphi]\!]_\bullet(s) - [\![\varphi]\!]_\bullet(t)\right| \leq \varepsilon$.

Example 3. We consider again the printer from Figure 1. When ignoring Color and Printing as atomic propositions, we have Color $\overset{+}{\sim}_{.2}$ Printing, as the two initial transition are the only difference. As a formula which realizes this bisimulation distance one can take $\varphi = \text{power/on} \wedge \text{A4} \wedge \mathsf{AX}_{0.5}\text{Ready}$; then $[\![\varphi]\!]_+(\text{Printing}) = 0$ and $[\![\varphi]\!]_+(\text{Color}) = .2$.

The proofs of adequacy, and also of expressivity below, for the accumulating and point-wise cases are similar, hence we concentrate on the accumulating case below. In the proof we will repeatedly make use of the lesser-known little brother of the triangle inequality

$$\big||x-y| - |x-z|\big| \leq |y-z|$$

Lemma 12. Let $s,t \in S$ with $s \overset{+}{\sim}_\varepsilon t$, and let $\sigma = (s,u,s_1,u_1,\ldots) \in \mathsf{P}(s)$, $\tau = (t,v,t_1,v_1,\ldots) \in \mathsf{P}(t)$ be corresponding paths. Then $\left|[\![\varphi]\!]_+(s) - [\![\varphi]\!]_+(t)\right| \leq \varepsilon$ for all state formulae φ, and $\left|[\![\varphi]\!]_+(\sigma) - [\![\varphi]\!]_+(\tau)\right| \leq \varepsilon$ for all path formulae φ.

Proof. We prove the lemma by structural induction in φ. The induction base is clear, as $s \overset{+}{\sim}_\varepsilon t$ implies that $\mathsf{p} \in \mathcal{L}(s)$ if and only if $\mathsf{p} \in \mathcal{L}(t)$, hence $[\![\varphi]\!]_+(s) = [\![\varphi]\!]_+(t)$ for $\varphi = \mathsf{p}$ or $\varphi = \neg\mathsf{p}$. For the inductive step, we examine each syntactic construction in turn:

1. $\varphi = \varphi_1 \vee \varphi_2$

   There are four cases to consider, corresponding to whether $[\![\varphi_1]\!]_+(s) \leq [\![\varphi_2]\!]_+(s)$ or $[\![\varphi_1]\!]_+(s) > [\![\varphi_2]\!]_+(s)$ and similarly for $[\![\varphi_1]\!]_+(t)$ and $[\![\varphi_2]\!]_+(t)$. We show the proof for one of the "mixed" cases; the other three ones are similar or easier:

   Assume $[\![\varphi_1]\!]_+(s) \leq [\![\varphi_2]\!]_+(s)$ and $[\![\varphi_1]\!]_+(t) > [\![\varphi_2]\!]_+(t)$. Then $[\![\varphi_1 \vee \varphi_2]\!]_+(s) - [\![\varphi_1 \vee \varphi_2]\!]_+(t) = [\![\varphi_1]\!]_+(s) - [\![\varphi_2]\!]_+(t)$, and $[\![\varphi_1]\!]_+(s) - [\![\varphi_1]\!]_+(t) \leq [\![\varphi_1]\!]_+(s) - [\![\varphi_2]\!]_+(t) \leq [\![\varphi_2]\!]_+(s) - [\![\varphi_2]\!]_+(t)$, and by induction hypothesis, $-\varepsilon \leq [\![\varphi_1]\!]_+(s) - [\![\varphi_1]\!]_+(t)$ and $[\![\varphi_2]\!]_+(s) - [\![\varphi_2]\!]_+(t) \leq \varepsilon$.
2. $\varphi = \varphi_1 \wedge \varphi_2$. This is similar to the previous case.

3. $\varphi = \mathsf{E}\varphi_1$

   By definition of $[\![\mathsf{E}\varphi_1]\!]_+$ there is a path $\sigma \in \mathsf{P}(s)$ for which $[\![\varphi_1]\!]_+(\sigma) = [\![\varphi]\!]_+(s)$. By Lemma 8 there is a corresponding path $\tau \in \mathsf{P}(t)$, and from the induction hypothesis we know that $|[\![\varphi_1]\!]_+(\sigma) - [\![\varphi_1]\!]_+(\tau)| \leq \varepsilon$. Thus $|[\![\varphi]\!]_+(s) - [\![\varphi]\!]_+(t)| \leq \varepsilon$.

4. $\varphi = \mathsf{A}\varphi_1$. This is similar to the previous case.

5. $\varphi = \mathsf{X}_c\varphi_1$

   By definition, $[\![\varphi]\!]_+(\sigma) = \lambda[\![\varphi_1]\!]_+(\sigma^1) + |c-u|$ and $[\![\varphi]\!]_+(\tau) = \lambda[\![\varphi_1]\!]_+(\tau^1) + |c-v|$, where $\sigma = s \xrightarrow{u} \sigma^1$ and $\tau = t \xrightarrow{v} \tau^1$. Since $s \overset{+}{\sim}_\varepsilon t$ and σ and τ correspond, we have $\sigma(1) \overset{+}{\sim}_{\varepsilon'} \tau(1)$ with $\varepsilon'\lambda \leq \varepsilon - |u - v|$, and by induction hypothesis $|[\![\varphi_1]\!]_+(\sigma^1) - [\![\varphi_1]\!]_+(\tau^1)| \leq \varepsilon'$. Hence $\big|[\![\varphi]\!]_+(\sigma) - [\![\varphi]\!]_+(\tau)\big| \leq \big||c-u| - |c-v|\big| + \lambda\big|[\![\varphi_1]\!]_+(\sigma^1) - [\![\varphi_2]\!]_+(\tau^1)\big| \leq |u-v| + \varepsilon - |u-v| = \varepsilon$.

6. $\varphi = \mathsf{F}_c\varphi_1$

   Pick any $\delta > 0$, then there is $k \in \mathbb{N}$ for which $S_k = \sum_{j=0}^{k-1} \lambda^j |\sigma(j)_w - c| + \lambda^k [\![\varphi]\!]_+(\sigma^k) \leq [\![\varphi]\!]_+(\sigma) + \delta$. As the paths σ and τ correspond, we also have $T_k = \sum_{j=0}^{k-1} \lambda^j |\tau(j)_w - c| + \lambda^k [\![\varphi]\!]_+(\tau^k) \leq [\![\varphi]\!]_+(\tau) + \delta$. Repeated use of the definition of $\overset{+}{\sim}_\varepsilon$ yields $\sigma(k) \overset{+}{\sim}_{\varepsilon'} \tau(k)$ with $\varepsilon'\lambda^k \leq \varepsilon - \sum_{j=0}^{k-1} \lambda^j \big|\sigma(j)_w - \tau(j)_w\big|$, hence by induction hypothesis, $\big|[\![\varphi]\!]_+(\sigma^k) - [\![\varphi]\!]_+(\tau^k)\big| \leq \varepsilon'$. Thus $\big|[\![\varphi]\!]_+(\sigma) - [\![\varphi]\!]_+(\tau)\big| \leq \big|S_k - T_k\big| + \delta \leq \sum_{j=0}^{k-1} \lambda^j \big||\sigma(j)_w - c| - |\tau(j)_w - c|\big| + \lambda^k \big|[\![\varphi]\!]_+(\sigma^k) - [\![\varphi]\!]_+(\tau^k)\big| + \delta \leq \varepsilon + \delta$. As these considerations hold for any $\delta > 0$, we must have $\big|[\![\varphi]\!]_+(\sigma) - [\![\varphi]\!]_+(\tau)\big| \leq \varepsilon$.

7. $\varphi = \mathsf{G}_c\varphi_1$; $\varphi = \varphi_1 \mathsf{U}_c \varphi_2$. These are similar to the previous case. □

Lemma 13. Let $s, t \in S$ and assume that $\big|[\![\varphi]\!]_+(s) - [\![\varphi]\!]_+(t)\big| \leq \varepsilon$ for all state formulae $\varphi \in \mathcal{L}_w$. Then $s \overset{+}{\sim}_\varepsilon t$.

Proof. This follows directly from Theorem 14 below, but one can also observe that the accumulating family $\mathbf{R} = \{\mathcal{R}_\varepsilon\}$ defined by

$$\mathcal{R}_\varepsilon = \big\{(s,t) \mid s,t \in S, \forall \varphi \in \mathcal{L}_w : \big|[\![\varphi]\!]_+(s) - [\![\varphi]\!]_+(t)\big| \leq \varepsilon\big\}$$

is indeed an accumulating bisimulation in terms of Definition 7. □

5.2 Expressivity

We show that WCTL with accumulating semantics is expressive with respect to accumulating bisimulation in the following sense:

Theorem 14. For each $s \in S$ and every $\gamma \in \mathbb{R}_+$, there exists a state formula $\varphi^s_\gamma \in \mathcal{L}_w$, interpreted over the accumulating semantics, which characterizes s up to accumulating bisimulation and up to γ, i.e. such that for all $s' \in S$, $s \overset{+}{\sim}_\varepsilon s'$ if and only if $[\![\varphi^s_\gamma]\!]_+(s') \in [\varepsilon - \gamma, \varepsilon + \gamma]$ for all γ.

Proof. We define characteristic formulae of unfoldings as follows: For each $s \in S$ and $n \in \mathbb{N}$, denote $\mathcal{L}(s) = \{\mathsf{p}_1, \dots, \mathsf{p}_k\}$ and $\mathcal{AP} \setminus \mathcal{L}(s) = \{\mathsf{q}_1, \dots, \mathsf{q}_\ell\}$ and let $\varphi(s,n)$ be the WCTL formula defined inductively as follows:

$$\varphi(s,0) = (\mathsf{p}_1 \wedge \dots \wedge \mathsf{p}_k) \wedge (\neg\mathsf{q}_1 \wedge \dots \wedge \neg\mathsf{q}_\ell)$$
$$\varphi(s,n+1) = \bigwedge_{s \xrightarrow{w} s'} \mathsf{EX}_w \varphi(s',n) \;\wedge \bigwedge_{w : s \xrightarrow{w} s'} \mathsf{AX}_w \Big(\bigvee_{s \xrightarrow{w} s'} \varphi(s',n) \Big) \wedge \varphi(s,0)$$

It is easy to see that $[\![\varphi(s,n)]\!]_+(s) = 0$ for all n.

To complete the proof, one observes that for each $\gamma > 0$, there is $n(\gamma) \in \mathbb{N}$ such that $\varphi(s, n(\gamma))$ can play the role of φ^s_γ in the theorem. Intuitively this is due to discounting: The further the unfolding in $\varphi(s,n)$, the higher are the weights discounted, hence from some $n(\gamma)$ on, maximum weight difference is below γ. □

Theorem 15. For each $s \in S$ and every $\gamma \in \mathbb{R}_+$, there exists a state formula $\varphi^s_\gamma \in \mathcal{L}_w$ interpreted over the point-wise semantics, which characterizes s up to point-wise bisimulation and up to γ, i.e. such that for all $s' \in S$, $s \mathrel{\dot{\sim}_\varepsilon} s'$ if and only if $[\![\varphi^s_\gamma]\!]_\bullet(s') \in [\varepsilon - \gamma, \varepsilon + \gamma]$ for all γ.

6 CONCLUSION AND FINAL REMARKS

We have shown in this paper that weighted CTL with an accumulating semantics is adequate and expressive for accumulating bisimulation for weighted Kripke structures. We have also seen that the same holds for the point-wise semantics for WCTL with respect to point-wise bisimulation.

We believe that these results can be lifted to a common abstract framework, but notice that this framework will be different from the one proposed in [10] as our truth domain $\mathbb{R}_{\geq 0} \cup \{\infty\}$ is not a quasi-Boolean lattice. This generalization should also encompass other weighted bisimulations such as the maximum-lead bisimulation of [8, 17], and we expect to see some synergies between the weighted-automata and quantitative-verification communities.

REFERENCES

[1] Aceto, L.—Ingólfsdóttír, A.—Larsen, K. G.—Srba, J.: Reactive Systems: Modelling, Specification and Verification. Cambridge University Press 2007.

[2] de Alfaro, L.—Faella, M.—Stoelinga, M.: Linear and Branching Metrics for Quantitative Transition Systems. In Proc. ICALP '04, LNCS 3142, pp. 97–109, Springer-Verlag 2004.

[3] de Alfaro, L.—Henzinger, T. A.—Majumdar, R.: Discounting the Future in Systems Theory. In Proc. ICALP '03, LNCS 2719, pp. 1022–1037, Springer 2003.

[4] Baier, C.—Katoen, J. P.: Principles of Model Checking. MIT Press 2008.

[5] Browne, M. C.—Clarke, E. M.—Grumberg, O.: Characterizing Kripke Structures in Temporal Logic. In Proc. TAPSOFT '87, LNCS 249, pp. 256–270, Springer 1987.

[6] Fitting, M.: Many-Valued Modal Logics. Fundam. Inform., Vol. 15, 1991, Nos. 3–4, pp. 235–254.

[7] Fitting, M.: Many-Valued Modal Logics II. Fundam. Inform., Vol. 17, 1992, Nos. 1–2, pp. 55–73.

[8] Henzinger, T. A.—Majumdar, R.—Prabhu, V.: Quantifying Similarities Between Timed Systems. In Proc. FORMATS '05, LNCS 3829, pp. 226–241, Springer 2005.

[9] Konikowska, B.—Penczek, W.: Model Checking for Multi-Valued Computation Tree Logics. In: M. Fitting, E. Orłowska (Eds.): Beyond Two: Theory and Applications of Multiple-Valued Logic, Springer 2003.

[10] Konikowska, B.—Penczek, W.: On Designated Values in Multi-Valued CTL* Model Checking. Fundam. Inform., Vol. 60, 2004, Nos. 1–4, pp. 211–224.

[11] Kwiatkowska, M.—Norman, G.—Parker, D.—Qu, H.: Assume-Guarantee Verification for Probabilistic Systems. In Proc. TACAS '10, LNCS 6105, pp. 23–37. Springer 2010.

[12] Larsen, K. G.—Pettersson, P.—Yi, W.: UPPAAL in a Nutshell. Software Tools for Technology Transfer, Vol. 1, 1997, Nos. 1–2, pp. 134–152.

[13] Lluch-Lafuente, A.–Montanari, U.: Quantitative-Calculus and CTL Based on Constraint Semirings. ENTCS 112, pp. 37–59, 2005.

[14] Milner, R.: Communication and Concurrency. Prentice Hall 1989.

[15] Puri, A.: Dynamical Properties of Timed Automata. Discrete Event Dynamic Systems, Vol. 10, 2000, Nos. 1–2, pp. 87–113.

[16] Rutten, J.—Kwiatkowska, M.—Norman, G.—Parker, D.: Mathematical Techniques for Analyzing Concurrent and Probabilistic Systems. Vol. 23 of CRM Monograph Series, American Mathematical Society 2004.

[17] Thrane, C.—Fahrenberg, U.—Larsen, K. G.: Quantitative Analysis of Weighted Transition Systems. Journal of Logic and Algebraic Programming, 2010 (to appear).

[18] de Wulf, M.—Doyen, L.—Markey, N.—Raskin, J. F.: Robustness and Implementability of Timed Automata. In Proc. FORMATS/FTRTFT '04, LNCS 3253, pp. 118–133, 2004.

Uli Fahrenberg holds an MSc in mathematics and computer science and a Ph. D. in mathematics from Aalborg University, Denmark. He is currently a Postdoc at the Distributed and Embedded Systems (DES) unit in the Department of Computer Science at Aalborg University and a member of the Centre for Embedded Software Systems (CISS), the Danish VKR Centre of Excellence MT-LAB, and the European research projects Quasimodo and GASICS.

Kim G. Larsen holds an M. Sc. in mathematics and computer science from Aalborg University, Denmark and a Ph. D. in computer science from Edinburgh University, Scotland. He is a Professor of computer science at Aalborg University, Industrial Professor at Twente University, The Netherlands, Director of the Centre for Embedded Software Systems (CISS), and Co-director of the Danish VKR Centre of Excellence MT-LAB. He became Honorary Doctor (Honoris causa) at Uppsala University in 1999 for his outstanding contributions to the popular verification tool UPPAAL. In 2005 he received the Danish Citation Laureates Award, Thomson Scientific, as the most cited Danish computer scientist in the period of 1990–2004. In 2007 he became Honorary Doctor (Honoris causa) at Laboratoire Specification et Verification, Ecole Normale Supérieure Cachan, France. He has an H-number of 49 and is prime investigator in the real-time verification tool UPPAAL and main contributor to the engine of the tool visualSTATE.

Claus Thrane holds an M. Sc. in computer science from Aalborg University, Denmark. He is currently a Ph. D. student with the Distributed and Embedded Systems (DES) unit in the Department of Computer Science at Aalborg University. He is a member of the Centre for Embedded Software Systems (CISS), of the Danish VKR Centre of Excellence MT-LAB, and of the European research project Quasimodo.