Quantitative Refinement for Weighted Modal Transition Systems

Sebastian S. Bauer[1], Uli Fahrenberg[2], Line Juhl[3],
Kim G. Larsen[3], Axel Legay[2], and Claus Thrane[3]

[1] Ludwig-Maximilians-Universität München, Germany
[2] Irisa/INRIA Rennes, France
[3] Aalborg University, Denmark

Abstract. Specification theories as a tool in the development process of component-based software systems have recently attracted a considerable attention. Current specification theories are however qualitative in nature and hence fragile and unsuited for modern software systems. We propose the first specification theory which allows to capture quantitative aspects during the refinement and implementation process.

Keywords: reducing complexity of design, modal specifications, quantitative reasoning

1 Introduction

Rigorous design of modern computer systems faces the major challenge that the systems are too complex to reason about [16]. Hence it is necessary to reason at the level of specification rather than at the one of implementations. Such specifications, which act as finite and concise abstractions for possibly infinite sets of implementations, allow not only to decrease the complexity of the design, but also permit to reason on subsystems independently.

Any reasonable specification theory is equipped with a *satisfaction relation* to decide whether an implementation matches the requirements of a specification, and a *refinement relation* that allows to compare specifications (hence sets of implementations). Moreover, the theory needs a notion of *logical composition* which allows to infer larger specifications as logical combinations of smaller ones. Another important ingredient is a notion of *structural composition* that allows to build overall specifications from sub-specifications, mimicking at the implementation level *e.g.* the interaction of components in a distributed system. A partial inverse of this operation is given by the notion of *quotient* which allows to synthesize a sub-specification from an overall specification and an implementation which realizes a part of the overall specification.

Over the years, there have been a series of advances on specification theories [2, 14, 5, 13]. The predominant approaches are based on modal logics and process algebras but have the drawback that they cannot naturally embed both logical and structural composition within the same formalism. Moreover, such formalisms do not permit to reason from specification to implementation through stepwise refinement.

In order to leverage those problems, the concept of modal transition systems was introduced [12]. In short, modal transition systems are labeled transition systems equipped with two types of transitions: *must* transitions which are mandatory for any implementation, and *may* transitions which are optional for implementations. It is well admitted that modal transition systems match all the requirements of a reasonable specification theory (see *e.g.* [15] for motivations). Also, practical experience shows that the formalism is expressive enough to handle complex industrial problems [6, 17].

In a series of recent work [3, 10], the modal transition system framework has been extended in order to reason on *quantitative* aspects, hence providing a new specification theory for more elaborated structures, with the objective to better meet practical needs. In this quantitative setting however, the standard Boolean satisfaction and refinement relations are too fragile. Indeed, either an implementation satisfies a specification or it does not. This means that minor and major modifications in the implementation cannot be distinguished, as both of them may reverse the Boolean answer. As observed by de Alfaro *et al.* for the logical framework of CTL [1], this view is obsolete; engineers need quantitative notions on how modified implementations differ.

The main contribution of this paper is to mitigate the above problem by lifting the satisfaction and refinement relations into the quantitative framework, hence completing the quantitative approach to reason on modal transition systems. More precisely, and similarly to what has been proposed in the logical framework, we introduce a notion of *distance* between both specifications and implementations, which permits quantitative comparison. Given two implementations that do not necessarily satisfy a specification, we can decide through quantitative reasoning which one is the better match for the specification's requirements.

To facilitate this reasoning, we develop a notion of *modal* distance between specifications, which approximates the distances between their implementations. This preserves the relation between modal refinement and satisfaction checking in the Boolean setting. We show that computing distances between implementation sets is EXPTIME-hard, whereas modal distances are computable in NP $\cap$ CO-NP (which is higher than for Boolean modal refinement). Akin to *discounted games* [19] we can reason on behaviors in a discounted manner, giving more importance to differences that happen in the near future, while accumulating the amount by which the specifications fail to be compatible at each step. As for the games, the semantics of the outcome is considered application specific.

Modifying the semantic outcome of satisfaction has strong impact on operations between specifications. As a second contribution of this paper, we propose quantitative versions of structural composition and quotient which inherit the good properties from the Boolean setting. We also propose a new notion of *relaxation*, which is inherent to the quantitative framework and allows *e.g.* to calibrate the quotient operator.

However, there is no free lunch, and working with distances has a price: some of the properties of logical conjunction and determinization are not preserved in the quantitative setting. More precisely, conjunction is not the greatest lower bound with respect to refinement distance as it is in the Boolean setting, and deterministic overapproximation is too coarse. In fact we show that this is a fundamental limitation of *any* reasonable quantitative specification formalism.

Structure of the paper. We start out by introducing our quantitative formalism which has weighted transition systems as implementations and weighted modal transition systems as specifications. In Section 3 we introduce the distances we use for quantitative comparison of both implementations and specification. Section 4 is devoted to a formalization of the notion of relaxation which is of great use in quantitative design. In the next section we see some inherent limitations of the quantitative approach, and Section 6 finishes the paper by showing that structural composition works as expected in the quantitative framework and links relaxation to quotients. Note that proofs of all theorems in the paper can be found in an appendix.

Acknowledgment. The authors wish to thank Jiří Srba for fruitful discussions during the preparation of this work.

2 Weighted Modal Transition Systems

In this section we present the formalism we use for implementations and specifications. As implementations we choose the model of *weighted transition systems*, *i.e.* labeled transition systems with integer weights at transitions. Specifications both have a *modal* dimension, specifying discrete behavior which *must* be implemented and behavior which *may* be present in implementations, and a *quantitative* dimension, specifying intervals of weights on each transition which an implementation must choose from.

Let $\mathbb{I} = \big\{[x,y] \bigm| x \in \mathbb{Z} \cup \{-\infty\}, y \in \mathbb{Z} \cup \{\infty\}, x \le y\big\}$ be the set of closed extended-integer intervals and let Σ be a finite set of actions. Our set of *specification labels* is $\mathsf{Spec} = (\Sigma \times \mathbb{I}) \cup \{\bot\}$, where the special symbol $\bot$ models *inconsistency*. The set of *implementation labels* is defined as $\mathsf{Imp} = \Sigma \times \big\{[x,x] \bigm| x \in \mathbb{Z}\big\} \approx \Sigma \times \mathbb{Z}$. Hence a specification imposes labels and integer *intervals* which constrain the possible weights of an implementation.

We define a partial order on $\mathbb{I}$ (representing inclusion of intervals) by $[x,y] \sqsubseteq [x',y']$ if $x' \le x$ and $y \le y'$, and we extend this order to specification labels by $(a,I) \sqsubseteq (a',I')$ if $a = a'$ and $I \sqsubseteq I'$, and $\bot \sqsubseteq (a,I)$ for all $(a,I) \in \mathsf{Spec}$. The partial order on Spec is hence a *refinement* order; if $k_1 \sqsubseteq k_2$, then no more implementation labels are contained in k_1 than in k_2.

Specifications and implementations are defined as follows:

Definition 1. A *weighted modal transition system* (WMTS) is a four-tuple $(S, s^0, \dashrightarrow, \longrightarrow)$ consisting of a set of states S with an initial state $s^0 \in S$ and *may* and *must* transition relations satisfying $\longrightarrow \subseteq \dashrightarrow \subseteq S \times \mathsf{Spec} \times S$. A WMTS is an *implementation* if $\longrightarrow = \dashrightarrow \subseteq S \times \mathsf{Imp} \times S$.

A WMTS is *finite* if S and $\dashrightarrow$ (and hence also $\longrightarrow$) are finite sets, and it is *deterministic* if it holds that for any $s \in S$ and $a \in \Sigma$, $\big(s,(a,I_1),t_1\big), \big(s,(a,I_2),t_2\big) \in \dashrightarrow$ imply $I_1 = I_2$ and $t_1 = t_2$. Hence a deterministic specification allows at most one transition under each discrete action from every state. In the rest of the paper we will write $s \overset{k}{\dashrightarrow} s'$ for $(s,k,s') \in \dashrightarrow$ and similarly for $\longrightarrow$, and we will always write $S = (S, s^0, \dashrightarrow, \longrightarrow)$ or $S_i = (S_i, s_i^0, \dashrightarrow_i, \longrightarrow_i)$ for WMTS and $I = (I, i^0, \longrightarrow)$ for implementations.

The implementation semantics of a specification is given through modal refinement, as follows: A *modal refinement* of WMTS S_1, S_2 is a relation $R \subseteq S_1 \times S_2$ such that for any $(s_1,s_2) \in R$ and any *may* transition $s_1 \overset{k_1}{\dashrightarrow}_1 t_1$ in S_1, there exists $s_2 \overset{k_2}{\dashrightarrow}_2 t_2$ in S_2 for which $k_1 \sqsubseteq k_2$ and $(t_1,t_2) \in R$, and for any *must* transition $s_2 \xrightarrow{k_2}_2 t_2$ in S_2, there exists $s_1 \xrightarrow{k_1}_1 t_1$ in S_1 for which $k_1 \sqsubseteq k_2$ and $(t_1,t_2) \in R$. Hence in such a modal refinement, behavior which is required in S_2 is also required in S_1, no more behavior is allowed in S_1 than in S_2, and the quantitative requirements in S_1 are refinements of the ones in S_2. We write $S_1 \leq_m S_2$ if there is a modal refinement relation R for which $(s_1^0, s_2^0) \in R$. The implementation semantics of a specification can then be defined as the set of all implementations which are also refinements:

Definition 2. The *implementation semantics* of a WMTS S is the set $[\![S]\!] = \{I \mid I \leq_m S, I \text{ implementation}\}$.

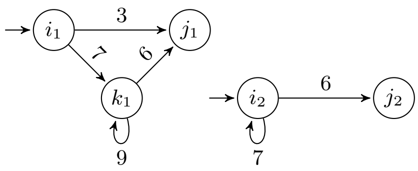
We say that a WMTS S is *consistent* if it has an implementation, *i.e.* if $[\![S]\!] \neq \emptyset$. A useful over-approximation of consistency is *local consistency*: a WMTS S is said to be locally consistent if $s \xrightarrow{k} t$ implies $k \neq \perp$, *i.e.* if no $\perp$-labeled *must* transitions appear in S. Local consistency implies consistency, but the inverse is not true; *e.g.* the WMTS $s_0 \xrightarrow{a,2} s_1 \overset{a,9}{\dashrightarrow} s_2 \xrightarrow{\perp} s_3$ has an implementation $i_0 \xrightarrow{a,2} i_1$. Local inconsistencies may be removed recursively as follows:

Definition 3. For a WMTS S, let $\text{pre} : 2^S \to 2^S$ be given by $\text{pre}(B) = \{s \in S \mid s \xrightarrow{k} t \in B \text{ for some } k\}$, and let $S^\perp = \{s \in S \mid s \xrightarrow{\perp} t \text{ for some } t \in S\}$. If $s^0 \notin \text{pre}^*(S^\perp)$, then the *pruning* $\rho(S) = (S_\rho, s^0, \dashrightarrow_\rho, \longrightarrow_\rho)$ is defined by $S_\rho = S \setminus \text{pre}^*(S^\perp)$, $\dashrightarrow_\rho = \dashrightarrow \cap \big(S_\rho \times (\mathsf{Spec} \setminus \{\perp\}) \times S_\rho\big)$ and $\longrightarrow_\rho = \longrightarrow \cap \big(S_\rho \times (\mathsf{Spec} \setminus \{\perp\}) \times S_\rho\big)$.

Note that if $\rho(S)$ exists, then it is locally consistent, and if $\rho(S)$ does not exist ($s^0 \in \text{pre}^*(S^\perp)$), then S is inconsistent. Also, $\rho(S) \leq_m S$ and $[\![\rho(S)]\!] = [\![S]\!]$.

3 Thorough and Modal Refinement Distances

For the quantitative specification formalism we have introduced in the last section, the standard Boolean notions of satisfaction and refinement are too fragile. To be able to reason not only whether a given quantitative implementation satisfies a given quantitative specification, but also to what extent, we introduce a notion of *distance* between both implementations and specifications.



$$
\begin{aligned}
&d(j_1, j_2) = 0 \\
&d(i_1, j_2) = \infty \\
&d(j_1, i_2) = \infty \\
&d(k_1, j_2) = \infty \\
&d(k_1, i_2) = \max\{2 + .9\, d(k_1, i_2),\ .9\, \overbrace{d(j_1, j_2)}^{0}\} \\
&d(i_1, i_2) = \max\{3 + .9\, \underbrace{d(j_1, j_2)}_{0},\ .9\, d(k_1, i_2)\}
\end{aligned}
$$

Fig. 1. Two weighted transition systems with branching distance $d(I_1, I_2) = 18$.

We first define the distance between *implementations*; for this we introduce a distance on implementation labels by

$$d_{\mathsf{Imp}}\big((a_1, x_1), (a_2, x_2)\big) = \begin{cases} \infty & \text{if } a_1 \neq a_2, \\ |x_1 - x_2| & \text{if } a_1 = a_2. \end{cases} \tag{1}$$

In the rest of the paper, let $\lambda \in \mathbb{R}$ with $0 < \lambda < 1$ be a *discounting factor*.

Definition 4. Let I_1, I_2 be implementations (weighted transition systems). The *implementation distance* $d : I_1 \times I_2 \to \mathbb{R}_{\geq 0} \cup \{\infty\}$ between the states of I_1 and I_2 is the least fixed point of the equations

$$d(i_1, i_2) = \max \begin{cases} \sup\limits_{i_1 \xrightarrow{k_1}_1 j_1} \inf\limits_{i_2 \xrightarrow{k_2}_2 j_2} d_{\mathsf{Imp}}(k_1, k_2) + \lambda d(j_1, j_2), \\ \sup\limits_{i_2 \xrightarrow{k_2}_2 j_2} \inf\limits_{i_1 \xrightarrow{k_1}_1 j_1} d_{\mathsf{Imp}}(k_1, k_2) + \lambda d(j_1, j_2). \end{cases}$$

We define $d(I_1, I_2) = d(i_1^0, i_2^0)$.

Except for the symmetrizing max operation, this is precisely the *accumulating branching distance* which is introduced in [18]; see also [8, 9] for a thorough introduction to linear and branching distances as we use them here. As the equations in the definition define a *contraction*, they have indeed a unique least fixed point; note that $d(i_1, i_2) = \infty$ is also a fixed point, *cf.* [11].

We remark that besides this accumulating distance, other interesting system distances may be defined depending on the application at hand, but we concentrate here on this distance and leave a generalization to other distances for future work.

Example 1. Consider the two implementations I_1 and I_2 in Figure 1 with a single action (elided for simplicity) and with discounting factor $\lambda = .9$. The equations in the illustration have already been simplified by removing all expressions that evaluate to ∞. What remains to be done is to compute the least fixed point of the equation $d(k_1, i_2) = \max\big\{2 + .9\, d(k_1, i_2), 0\big\}$ which is $d(k_1, i_2) = 20$. Hence $d(i_1, i_2) = \max\{3, .9 \cdot 20\} = 18$.

To lift implementation distance to specifications, we need first to consider the distance between *sets* of implementations. Given implementation sets $\mathcal{I}_1, \mathcal{I}_2$, we define

$$d(\mathcal{I}_1, \mathcal{I}_2) = \sup_{I_1 \in \mathcal{I}_1} \inf_{I_2 \in \mathcal{I}_2} d(I_1, I_2)$$

Note that in case $\mathcal{I}_2$ is finite, we have that for all $\varepsilon \geq 0$, $d(\mathcal{I}_1, \mathcal{I}_2) \leq \varepsilon$ if and only if for each implementation $I_1 \in \mathcal{I}_1$ there exists $I_2 \in \mathcal{I}_2$ for which $d(I_1, I_2) \leq \varepsilon$, hence this is a natural notion of distance. Especially, $d(\mathcal{I}_1, \mathcal{I}_2) = 0$ if and only if $\mathcal{I}_1$ is a subset of $\mathcal{I}_2$ up to bisimilarity. For infinite $\mathcal{I}_2$, we have the slightly more complicated property that $d(\mathcal{I}_1, \mathcal{I}_2) \leq \varepsilon$ if and only if for all $\delta > 0$ and any $I_1 \in \mathcal{I}_1$, there is $I_2 \in \mathcal{I}_2$ for which $d(I_1, I_2) \leq \varepsilon + \delta$.

Note that in general, our distance on sets of implementations is *asymmetric*; we may well have $d(\mathcal{I}_1, \mathcal{I}_2) \neq d(\mathcal{I}_2, \mathcal{I}_1)$. We lift this distance to specifications as follows:

Definition 5. The *thorough refinement distance* between WMTS S_1 and S_2 is defined as $d_t(S_1, S_2) = d\big(\llbracket S_1 \rrbracket, \llbracket S_2 \rrbracket\big)$. We write $S_1 \leq_t^\varepsilon S_2$ if $d_t(S_1, S_2) \leq \varepsilon$.

Indeed this permits us to measure incompatibility of specifications. Also observe the special case where $S_1 = I_1$ is an implementation: then $d_t(I_1, S_2) = \inf_{I_2 \in \llbracket S_2 \rrbracket} d(I_1, I_2)$, which measures how close I_1 is to satisfy the specification S_2.

To facilitate computation and comparison of refinement distance, we introduce modal refinement distance as an overapproximation. We will show in Theorem 2 below that similarly to the Boolean setting [4], computation of thorough refinement distance is EXPTIME-hard, whereas modal refinement distance is computable in NP $\cap$ CO-NP. First we generalize the distance on implementation labels from Equation (1) to specification labels so that for $k, \ell \in \mathsf{Spec}$ we define

$$d_{\mathsf{Spec}}(k, \ell) = \sup_{k' \in \llbracket k \rrbracket} \inf_{\ell' \in \llbracket \ell \rrbracket} d_{\mathsf{Imp}}(k', \ell').$$

Note that d_{Spec} is asymmetric, and that $d_{\mathsf{Spec}}(k, \ell) = 0$ if and only if $k \sqsubseteq \ell$. Also, $d_{\mathsf{Spec}}(k, \ell) = d_{\mathsf{Imp}}(k, \ell)$ for all $k, \ell \in \mathsf{Imp}$. Using the $\dot{-}$ operation defined on integers by $x_1 \dot{-} x_2 = \max(x_1 - x_2, 0)$, we can express d_{Spec} as follows:

$$\begin{gathered} d_{\mathsf{Spec}}\big((a_1, I_1), (a_2, I_2)\big) = \infty \quad \text{if } a_1 \neq a_2 \\ d_{\mathsf{Spec}}\big((a, [x_1, y_1]), (a, [x_2, y_2])\big) = \max(x_2 \dot{-} x_1, y_1 \dot{-} y_2) \\ d_{\mathsf{Spec}}\big(\perp, (a, I_2)\big) = 0 \qquad\qquad d_{\mathsf{Spec}}\big((a, I_1), \perp\big) = \infty \end{gathered}$$

Definition 6. Let S_1, S_2 be WMTS. The *modal refinement distance* $d_m : S_1 \times S_2 \to \mathbb{R}_{\geq 0} \cup \{\infty\}$ from states of S_1 to states of S_2 is the least fixed point of the equations

$$d_m(s_1, s_2) = \max \begin{cases} \sup\limits_{s_1 \overset{k_1}{\dashrightarrow}_1 t_1} \inf\limits_{s_2 \overset{k_2}{\dashrightarrow}_2 t_2} d_{\mathsf{Spec}}(k_1, k_2) + \lambda d_m(t_1, t_2), \\ \sup\limits_{s_2 \overset{k_2}{\longrightarrow}_2 t_2} \inf\limits_{s_1 \overset{k_1}{\longrightarrow}_1 t_1} d_{\mathsf{Spec}}(k_1, k_2) + \lambda d_m(t_1, t_2). \end{cases}$$

We define $d_m(S_1, S_2) = d_m(s_1^0, s_2^0)$, and we write $S_1 \leq_m^\varepsilon S_2$ if $d_m(S_1, S_2) \leq \varepsilon$.

The argument for existence and uniqueness of the least fixed point is exactly the same as for implementation distance in Definition 4. Like thorough refinement distance, modal refinement distance may be asymmetric.

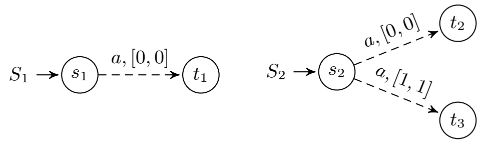


Fig. 2. Incompleteness of modal refinement distance.

The next theorem shows that modal refinement distance indeed overapproximates thorough refinement distance, and that it is exact for deterministic WMTS. Note that nothing general can be said about the precision of the overapproximation in the nondeterministic case; as an example observe the two specifications in Figure 2 for which $d_t(S_1, S_2) = 0$ but $d_m(S_1, S_2) = \infty$.

Theorem 1. *For WMTS S_1, S_2 we have $d_t(S_1, S_2) \le d_m(S_1, S_2)$. If S_1 is locally consistent and S_2 is deterministic, then $d_t(S_1, S_2) = d_m(S_1, S_2)$.*

The complexity results in the next theorem show that modal refinement distance can serve as a useful approximation of thorough refinement distance.

Theorem 2. *For finite WMTS S_1, S_2 and $\varepsilon \ge 0$, it is* EXPTIME*-hard to decide whether $S_1 \le_t^\varepsilon S_2$. The problem whether $S_1 \le_m^\varepsilon S_2$ is decidable in* NP $\cap$ CO-NP*.*

4 Relaxation

We introduce here a notion of *relaxation* which is specific to the quantitative setting. Intuitively, relaxing a specification means to weaken the quantitative constraints, while the discrete demands on which transitions may or must be present in implementations are kept. A similar notion of strengthening may be defined, but we do not use this here.

Definition 7. For WMTS S, S' and $\varepsilon \ge 0$, S' is an *ε-relaxation* of S if $S \le_m S'$ and $S' \le_m^\varepsilon S$.

Hence the quantitative constraints in S' may be more permissive than the ones in S, but no new discrete behavior may be introduced. Also note that any implementation of S is also an implementation of S', and no implementation of S' is further than ε away from an implementation of S. The following proposition relates specifications to relaxed specifications:

Proposition 1. *If S_1', S_2' are ε-relaxations of S_1 and S_2, then $d_m(S_1, S_2) - \varepsilon \le d_m(S_1, S_2') \le d_m(S_1, S_2)$ and $d_m(S_1, S_2) \le d_m(S_1', S_2) \le d_m(S_1, S_2) + \varepsilon$.*

On the syntactic level, we can introduce the following *widening* operator which relaxes all quantitative constraints in a systematic manner. We write $I \pm \delta = [x - \delta, y + \delta]$ for an interval $I = [x, y]$ and $\delta \in \mathbb{N}$.

Definition 8. Given $\delta \in \mathbb{N}$, the *δ-widening* of a WMTS S is the WMTS $S^{+\delta}$ with transitions $s \overset{a,I\pm\delta}{\dashrightarrow} t$ in $S^{+\delta}$ for all $s \overset{a,I}{\dashrightarrow} t$ in S, and $s \overset{a,I\pm\delta}{\longrightarrow} t$ in $S^{+\delta}$ for all $s \overset{a,I}{\longrightarrow} t$ in S.

Widening and relaxation are related as follows; note also that as widening is a global operation whereas relaxation may be achieved entirely locally, not all relaxations may be obtained as widenings.

Proposition 2. *The δ-widening of any WMTS S is a $(1-\lambda)^{-1}\delta$-relaxation.*

There is also an implementation-level notion which corresponds to relaxation:

Definition 9. The *ε-extended implementation semantics*, for $\varepsilon \geq 0$, of a WMTS S is $[\![S]\!]^{+\varepsilon} = \big\{ I \bigm| I \leq_m^\varepsilon S, I \text{ implementation} \big\}$.

Proposition 3. *If S' is an ε-relaxation of S, then $[\![S']\!] \subseteq [\![S]\!]^{+\varepsilon}$.*

It can be shown that there are WMTS S, S' such that S' is an ε-relaxation of S but the inclusion $[\![S']\!] \subseteq [\![S]\!]^{+\varepsilon}$ is strict.

5 Limitations of the Quantitative Approach

In this section we turn our attention towards some of the standard operators for specification theories; determinization and logical conjunction. Quite surprisingly, we show that in the quantitative setting, there are problems with these notions which do not appear in the Boolean theory. More specifically, we show that there is no determinization operator which always yields a *smallest* deterministic overapproximation, and there is no conjunction operator which acts as a greatest lower bound.

Theorem 3. *There is no unary operator $\mathcal{D}$ on WMTS for which it holds that*

(3.1) *$\mathcal{D}(S)$ is deterministic for any WMTS S,*
(3.2) *$S \leq_m \mathcal{D}(S)$ for any WMTS S,*
(3.3) *$S \leq_m^\varepsilon D$ implies $\mathcal{D}(S) \leq_m^\varepsilon D$ for any WMTS S, any deterministic WMTS D, and any $\varepsilon \geq 0$.*

In the standard Boolean setting, there is indeed a determinization operator which satisfies properties similar to the above, and which is useful because it enables checking thorough refinement, *cf.* Theorem 1. Likewise, the greatest-lower-bound property of logical conjunction in the Boolean setting ensures that the set of implementations of a conjunction of specifications is precisely the intersection of the implementation sets of the two specifications.

Theorem 4. *There is no partial binary operator $\wedge$ on WMTS for which it holds that*

(4.1) *$S_1 \wedge S_2 \leq_m S_1$ and $S_1 \wedge S_2 \leq_m S_2$ for all locally consistent WMTS S_1, S_2 for which $S_1 \wedge S_2$ is defined,* (4.2) *for any locally consistent WMTS S and all deterministic and locally consistent WMTS S_1, S_2 such that $S \leq_m S_1$ and $S \leq_m S_2$, $S_1 \wedge S_2$ is defined and $S \leq_m S_1 \wedge S_2$,*

(4.3) *for any $\varepsilon \geq 0$, there exist $\varepsilon_1 \geq 0$ and $\varepsilon_2 \geq 0$ such that for any locally consistent WMTS S and all deterministic and locally consistent WMTS S_1, S_2 for which $S_1 \wedge S_2$ is defined, $S \leq_m^{\varepsilon_1} S_1$ and $S \leq_m^{\varepsilon_2} S_2$ imply $S \leq_m^{\varepsilon} S_1 \wedge S_2$.*

The counterexamples used in the proofs of Theorems 3 and 4 are quite general and apply to a large class of distances, rather than only to the accumulating distance discussed in this paper. More precisely, it can be shown that Theorem 3 holds for *any* modal distance d_m for which there are label sequences (k_1^1, k_1^2), (k_2^1, k_2^2), (k_3^1, k_3^2) such that (using the obvious specialization of d_m to label sequences and $\sqcap$ as lowest upper bound on $(\mathsf{Spec}, \sqsubseteq)$)

$$\max\big(d_m\big((k_1^1, k_1^2), (k_3^1, k_3^2)\big), d_m\big((k_2^1, k_2^2), (k_3^1, k_3^2)\big)\big) \\ \neq d_m\big((k_1^1 \sqcap k_2^1, k_3^1), (k_1^2 \sqcap k_2^2, k_3^2)\big).$$

6 Structural Composition and Quotient

In this section we show that in our quantitative setting, notions of structural composition and quotient can be defined which obey the properties expected of such operations. In particular, structural composition satisfies independent implementability [2], hence the refinement distance between structural composites can be bounded by the distances between their respective components.

First we define partial synchronization operators $\oplus$ and $\ominus$ on specification labels which will be used for synchronizing transitions. We let $(a_1, I_1) \oplus (a_2, I_2)$ and $(a_1, I_1) \ominus (a_2, I_2)$ be undefined if $a_1 \neq a_2$, and otherwise

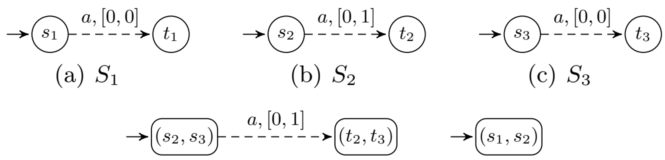
$$\big(a, [x_1, y_1]\big) \oplus \big(a, [x_2, y_2]\big) = \big(a, [x_1 + x_2, y_1 + y_2]\big), \\ (a, I_1) \oplus \bot = \bot \oplus (a, I_2) = \bot;$$

$$\big(a, [x_1, y_1]\big) \ominus \big(a, [x_2, y_2]\big) = \begin{cases} \bot & \text{if } x_1 - x_2 > y_1 - y_2, \\ \big(a, [x_1 - x_2, y_1 - y_2]\big) & \text{if } x_1 - x_2 \leq y_1 - y_2, \end{cases} \\ (a, I_1) \ominus \bot = \bot \ominus (a, I_2) = \bot.$$

Note that we use CSP-style synchronization, but other types of synchronization can easily be defined. Also, defining $\oplus$ to add intervals (and $\ominus$ to subtract them) is only one particular choice; depending on the application, one can also *e.g.* let $\oplus$ be intersection of intervals or some other operation.

Definition 10. Let S_1 and S_2 be WMTS. The *structural composition* of S_1 and S_2 is $S_1 \| S_2 = \big(S_1 \times S_2, (s_1^0, s_2^0), \mathsf{Spec}, \dashrightarrow, \longrightarrow\big)$ with transitions given as follows:

$$\frac{s_1 \overset{k_1}{\dashrightarrow}_1 t_1 \quad s_2 \overset{k_2}{\dashrightarrow}_2 t_2, \quad k_1 \oplus k_2 \text{ defined}}{(s_1, s_2) \overset{k_1 \oplus k_2}{\dashrightarrow} (t_1, t_2)} \qquad \frac{s_1 \xrightarrow{k_1}_1 t_1 \quad s_2 \xrightarrow{k_2}_2 t_2 \quad k_1 \oplus k_2 \text{ defined}}{(s_1, s_2) \xrightarrow{k_1 \oplus k_2} (t_1, t_2)}$$



(a) S_1 (b) S_2 (c) S_3

(d) $S_2 \| S_3$ (e) $S_1 \mathbin{\backslash\!\!\backslash} S_2$

Fig. 3. WMTS for which $d_m(S_3, S_1 \mathbin{\backslash\!\!\backslash} S_2) \neq d_m(S_2 \| S_3, S_1)$.

The *quotient* of S_1 by S_2 is $S_1 \mathbin{\backslash\!\!\backslash} S_2 = \rho\big(S_1 \times S_2 \cup \{u\}, (s_1^0, s_2^0), \mathsf{Spec}, \dashrightarrow, \longrightarrow\big)$ with transitions given as follows:

$$\frac{s_1 \overset{k_1}{\dashrightarrow}_1 t_1 \quad s_2 \overset{k_2}{\dashrightarrow}_2 t_2 \quad k_1 \ominus k_2 \text{ defined}}{(s_1, s_2) \overset{k_1 \ominus k_2}{\dashrightarrow} (t_1, t_2)} \qquad \frac{s_1 \xrightarrow{k_1}_1 t_1 \quad s_2 \xrightarrow{k_2}_2 t_2 \quad k_1 \ominus k_2 \text{ defined}}{(s_1, s_2) \xrightarrow{k_1 \ominus k_2} (t_1, t_2)}$$

$$\frac{s_1 \xrightarrow{k_1}_1 t_1 \quad \forall s_2 \xrightarrow{k_2}_2 t_2 : k_1 \ominus k_2 \text{ undefined}}{(s_1, s_2) \xrightarrow{\perp} (s_1, s_2)}$$

$$\frac{k \in \mathsf{Spec} \quad \forall s_2 \overset{k_2}{\dashrightarrow}_2 t_2 : k \oplus k_2 \text{ undefined}}{(s_1, s_2) \overset{k}{\dashrightarrow} u} \qquad \frac{k \in \mathsf{Spec}}{u \overset{k}{\dashrightarrow} u}$$

Note that we ensure that the quotient $S_1 \mathbin{\backslash\!\!\backslash} S_2$ is locally consistent by recursively removing $\perp$-labeled *must* transitions using pruning, see Definition 3. The following theorem shows that structural composition is well-behaved with respect to modal refinement distance in the sense that the distance between the composed systems is bounded by the distances of the individual systems. Note also the special case in the theorem of $S_1 \leq_m S_2$ and $S_3 \leq_m S_4$ implying $S_1 \| S_3 \leq_m S_2 \| S_4$.

Theorem 5 (Independent implementability). *For WMTS S_1, S_2, S_3, S_4 we have $d_m\big(S_1 \| S_3, S_2 \| S_4\big) \leq d_m(S_1, S_2) + d_m(S_3, S_4)$.*

The following theorem expresses the fact that quotient is a partial inverse to structural composition. Intuitively, the theorem shows that the quotient $S_1 \mathbin{\backslash\!\!\backslash} S_2$ is maximal among all WMTS S_3 with respect to any distance $S_2 \| S_3 \leq_m^\varepsilon S_1$; note the special case of $S_3 \leq_m S_1 \mathbin{\backslash\!\!\backslash} S_2$ if and only if $S_2 \| S_3 \leq_m S_1$.

Theorem 6 (Soundness and maximality of quotient). *Let S_1, S_2 and S_3 be locally consistent WMTS such that S_2 is deterministic and $S_1 \mathbin{\backslash\!\!\backslash} S_2$ is defined. If $d_m(S_3, S_1 \mathbin{\backslash\!\!\backslash} S_2) < \infty$, then $d_m(S_3, S_1 \mathbin{\backslash\!\!\backslash} S_2) = d_m(S_2 \| S_3, S_1)$.*

The example depicted in Figure 3 shows that the condition $d_m(S_3, S_1 \mathbin{\backslash\!\!\backslash} S_2) < \infty$ in Theorem 6 is necessary. Here $d_m(S_2 \| S_3, S_1) = 1$, but $d_m(S_3, S_1 \mathbin{\backslash\!\!\backslash} S_2) = \infty$ because of inconsistency between the transitions $s_1 \overset{a,[0,0]}{\dashrightarrow}_1 t_1$ and $s_2 \overset{a,[0,1]}{\dashrightarrow}_2 t_2$ for which $k_1 \ominus k_2$ is defined.

As a practical application, we notice that *relaxation* as defined in Section 4 can be useful when computing quotients. The quotient construction in Definition 10 introduces local inconsistencies (which afterwards are pruned) whenever there is a pair of transitions $s_1 \overset{k_1}{\dashrightarrow}_1 t_1$, $s_2 \overset{k_2}{\dashrightarrow}_2 t_2$ (or $s_1 \xrightarrow{k_1}_1 t_1$, $s_2 \xrightarrow{k_2}_2 t_2$) for which $k_1 \ominus k_2 = \bot$. Looking at the definition of $\ominus$, we see that this is the case if $k_1 = (a, [x_1, y_1])$ and $k_2 = (a, [x_2, y_2])$ are such that $x_1 - x_2 > y_1 - y_2$; hence these local inconsistencies can be avoided by *enlarging* k_1.

Enlarging quantitative constraints is exactly the intuition of relaxation, thus in practical cases where we get a quotient $S_1 \setminus\!\!\setminus S_2$ which is "too inconsistent", we may be able to solve this problem by constructing a suitable ε-relaxation S_1' of S_1. Theorems 5 and 6 can then be used to ensure that also $S_1' \setminus\!\!\setminus S_2$ is a relaxation of $S_1 \setminus\!\!\setminus S_2$.

7 Conclusion and Further Work

We have shown in this paper that within the quantitative specification framework of weighted modal transition systems, refinement and implementation distances provide a useful tool for robust compositional reasoning. Note that these distances permit us not only to reason about differences between implementations and from implementations to specifications, but they also provide a means by which we can compare specifications directly at the abstract level.

We have shown that for some of the ingredients of our specification theory, namely structural composition and quotient, our formalism is a conservative extension of the standard Boolean notions. We have also noted however, that for determinization and logical conjunction, the properties of the Boolean notions are not preserved, and that this is a fundamental limitation of any reasonable quantitative specification theory. The precise practical implications of this for the applicability of our quantitative specification framework are subject to future work.

References

1. Luca de Alfaro, Marco Faella, and Mariëlle Stoelinga. Linear and branching system metrics. *IEEE Trans. Software Eng.*, 35(2):258–273, 2009.
2. Luca de Alfaro and Thomas Henzinger. Interface-based design. In Manfred Broy, Johannes Grünbauer, David Harel, and Tony Hoare, editors, *Engineering Theories of Software Intensive Systems*, volume 195 of *NATO Science Series II: Mathematics, Physics and Chemistry*, pages 83–104. Springer-Verlag, 2005.
3. Sebastian S. Bauer, Line Juhl, Kim G. Larsen, Axel Legay, and Jiří Srba. Quantitative modal transition systems. 2011. Submitted.
4. Nikola Beneš, Jan Křetínský, Kim G. Larsen, and Jiří Srba. Checking thorough refinement on modal transition systems is EXPTIME-complete. In Martin Leucker and Carroll Morgan, editors, *ICTAC*, volume 5684 of *Lecture Notes in Computer Science*, pages 112–126. Springer-Verlag, 2009.
5. Arindam Chakrabarti, Luca de Alfaro, Thomas A. Henzinger, and Freddy Y. C. Mang. Synchronous and bidirectional component interfaces. In *Proc. 14th Int. Conference on Computer Aided Verification (CAV)*, volume 2404 of *Lecture Notes in Computer Science*, pages 414–427, 2002.

6. STREP COMBEST (COMponent-Based Embedded Systems design Techniques). `http://www.combest.eu/home/`.
7. Anne Condon. The complexity of stochastic games. *Information and Computation*, 96(2):203–224, 1992.
8. Uli Fahrenberg, Kim G. Larsen, and Claus Thrane. A quantitative characterization of weighted Kripke structures in temporal logic. *Computing and Informatics*, 29(6+):1311–1324, 2010.
9. Uli Fahrenberg, Claus Thrane, and Kim G. Larsen. Distances for weighted transition systems: Games and properties. In *Proc. QAPL'11*, Electronic Proceedings in Theoretical Computer Science, 2011. To be published.
10. Line Juhl, Kim G. Larsen, and Jiří Srba. Modal transition systems with weight intervals. *Journal of Logic and Algebraic Programming*, 2011. To be published.
11. Kim G. Larsen, Uli Fahrenberg, and Claus Thrane. Metrics for weighted transition systems: Axiomatization and complexity. *Theoretical Computer Science*, 2011. 10.1016/j.tcs.2011.04.003.
12. Kim Guldstrand Larsen. Modal specifications. In *Automatic Verification Methods for Finite State Systems*, volume 407 of *Lecture Notes in Computer Science*, pages 232–246. Springer, 1989.
13. Nancy Lynch and Mark R. Tuttle. An introduction to input/output automata. *CWI-Quarterly*, 2(3), 1989.
14. Ulrik Nyman. *Modal Transition Systems as the Basis for Interface Theories and Product Lines*. PhD thesis, Aalborg University, Department of Computer Science, September 2008.
15. Jean-Baptiste Raclet. Residual for component specifications. *Electr. Notes in Theor. Comput. Sci.*, 215:93–110, 2008.
16. Joseph Sifakis. A vision for computer science – the system perspective. *Central European Journal of Computer Science*, 1(1):108–116, 2011.
17. SPEEDS (SPEculative and Exploratory Design in Systems Engineering). `http://www.speeds.eu.com`.
18. Claus Thrane, Uli Fahrenberg, and Kim G. Larsen. Quantitative simulations of weighted transition systems. *Journal of Logic and Algebraic Programming*, 79(7):689–703, 2010.
19. Uri Zwick and Mike Paterson. The complexity of mean payoff games. In Ding-Zhu Du and Ming Li, editors, *COCOON*, volume 959 of *Lecture Notes in Computer Science*, pages 1–10. Springer-Verlag, 1995.

Appendix: Proofs for Section 3

There is a powerful proof technique introduced for branching distances between implementations in [18] that we here extend to modal refinement distance. We define a *modal refinement family* as an $\mathbb{R}_{\geq 0}$-indexed family of relations $R = \{R_\varepsilon \subseteq S_1 \times S_2 \mid \varepsilon \geq 0\}$ such that for any ε and any $(s_1, s_2) \in R_\varepsilon$,

- whenever $s_1 \overset{k_1}{\dashrightarrow} t_1$ then $s_2 \overset{k_2}{\dashrightarrow} t_2$ such that $d_{\mathsf{Spec}}(k_1, k_2) \leq \varepsilon$ and $(t_1, t_2) \in R_{\varepsilon'}$ for some $\varepsilon' \leq \lambda^{-1}\big(\varepsilon - d_{\mathsf{Spec}}(k_1, k_2)\big)$,
- whenever $s_2 \xrightarrow{k_2} t_2$ then $s_1 \xrightarrow{k_1} t_1$ such that $d_{\mathsf{Spec}}(k_1, k_2) \leq \varepsilon$ and $(t_1, t_2) \in R_{\varepsilon'}$ for some $\varepsilon' \leq \lambda^{-1}\big(\varepsilon - d_{\mathsf{Spec}}(k_1, k_2)\big)$.

It can then be shown, following the proof strategy in [18] developed for implementations, that $S_1 \leq_m^\varepsilon S_2$ if and only if there is a modal refinement family R with $(s_1^0, s_2^0) \in R_\varepsilon \in R$. Also note that modal refinement families are *upward closed* in the sense that $(s_1, s_2) \in R_\varepsilon$ implies that $(s_1, s_2) \in R_{\varepsilon'}$ for all $\varepsilon' \geq \varepsilon$.

Theorem A.1. *For WMTS S_1, S_2 we have $d_t(S_1, S_2) \leq d_m(S_1, S_2)$.*

Proof. If $d_m(S_1, S_2) = \infty$, we have nothing to prove. Otherwise, let $R = \{R_\varepsilon \subseteq S_1 \times S_2 \mid \varepsilon \geq 0\}$ be a modal refinement family which witnesses $d_m(S_1, S_2)$, *i.e.* such that $(s_1^0, s_2^0) \in R_{d_m(S_1,S_2)}$, and let $I_1 \in [\![S_1]\!]$. We have to expose $I_2 \in [\![S_2]\!]$ for which $d(I_1, I_2) \leq d_m(S_1, S_2)$.

Let $R^1 \subseteq I_1 \times S_1$ be a witness for $I_1 \leq_m S_1$, define $R'_\varepsilon = R^1 \circ R_\varepsilon \subseteq I_1 \times S_2$ for all $\varepsilon \geq 0$, and let $R' = \{R'_\varepsilon \mid \varepsilon \geq 0\}$. The states of $I_2 = (I_2, i_2^0, \mathsf{Imp}, \longrightarrow_{I_2})$ are $I_2 = S_2$ with $i_2^0 = s_2^0$, and the transitions we define as follows:

For any $i_1 \xrightarrow{k'_1}_{I_1} j_1$ and any $s_2 \in S_2$ for which $(i_1, s_2) \in R'_\varepsilon \in R'$ for some ε, we have $s_2 \overset{k_2}{\dashrightarrow}_2 t_2$ with $d_{\mathsf{Spec}}(k'_1, k_2) \leq \varepsilon$ and $(j_1, t_2) \in R'_{\varepsilon'} \in R'$ for some $\varepsilon' \leq \lambda^{-1}\big(\varepsilon - d_{\mathsf{Spec}}(k'_1, k_2)\big)$. Write $k'_1 = (a'_1, x'_1)$ and $k_2 = \big(a_2, [x_2, y_2]\big)$, then we must have $a'_1 = a_2$. Let

$$x'_2 = \begin{cases} x_2 & \text{if } x'_1 < x_2, \\ x'_1 & \text{if } x_2 \leq x'_1 \leq y_2, \\ y_2 & \text{if } x'_1 > y_2, \end{cases} \tag{2}$$

and $k'_2 = (a_2, x'_2)$, and put $s_2 \xrightarrow{k'_2}_{I_2} t_2$ in I_2. Note that

$$d_{\mathsf{Spec}}(k'_1, k'_2) = d_{\mathsf{Spec}}(k'_1, k_2). \tag{3}$$

Similarly, for any $s_2 \xrightarrow{k_2}_2 t_2$ and any $i_1 \in I_1$ with $(i_1, s_2) \in R'_\varepsilon \in R'$ for some ε, we have $i_1 \xrightarrow{k'_1}_{I_1} j_1$ with $d_{\mathsf{Spec}}(k'_1, k_2) \leq \varepsilon$ and $(j_1, t_2) \in R'_{\varepsilon'} \in R'$ for some $\varepsilon' \leq \lambda^{-1}\big(\varepsilon - d_{\mathsf{Spec}}(k'_1, k_2)\big)$. Write $k'_1 = (a'_1, x'_1)$ and $k_2 = (a_2, [x_2, y_2])$, define x'_2 as in (2) and $k'_2 = (a_2, x'_2)$, and put $s_2 \xrightarrow{k'_2}_{I_2} t_2$ in I_2.

We show that the identity relation $\mathrm{id}_{S_2} = \{(s_2, s_2) \mid s_2 \in S_2\} \subseteq S_2 \times S_2$ witnesses $I_2 \leq_m S_2$. Let first $s_2 \xrightarrow{k'_2}_{I_2} t_2$; we must have used one of the two constructions above for creating this transition. In the first case, we have $s_2 \overset{k_2}{\dashrightarrow}_2$

t_2 with $k_2' \sqsubseteq k_2$, and in the second case, we have $s_2 \xrightarrow{k_2}_2 t_2$, hence also $s_2 \overset{k_2}{\dashrightarrow}_2 t_2$, with the same property. For a transition $s_2 \xrightarrow{k_2}_2 t_2$ on the other hand, we have introduced $s_2 \xrightarrow{k_2'}_{I_2} t_2$ in the second construction above, with $k_2' \sqsubseteq k_2$.

We also want to show that the family R' is a witness for $d(I_1, I_2) \leq d_m(S_1, S_2)$. We have $(i_1^0, s_2^0) \in R'_{d_m(S_1,S_2)} = R_1 \circ R_{d_m(S_1,S_2)}$, so let $(i_1, s_2) \in R'_\varepsilon \in R'$ for some $\varepsilon \geq 0$. For any $i_1 \xrightarrow{k_1'}_{I_1} j_1$ we have $s_2 \overset{k_2}{\dashrightarrow}_2 t_2$ and $s_2 \xrightarrow{k_2'}_{I_2} t_2$ by the first part of our construction above, with $d_{\mathsf{Spec}}(k_1', k_2') = d_{\mathsf{Spec}}(k_1', k_2) \leq \varepsilon$ because of (3), and also $(j_1, t_2) \in R'_{\varepsilon'} \in R'$ for some $\varepsilon' \leq \lambda^{-1}\big(\varepsilon - d_{\mathsf{Spec}}(k_1', k_2)\big)$. For any $s_2 \xrightarrow{k_2'}_{I_2} t_2$, we must have used one of the constructions above to introduce this transition, and both give us $i_1 \xrightarrow{k_1'}_{I_1} j_1$ with $d_{\mathsf{Spec}}(k_1', k_2') \leq \varepsilon$ and $(j_1, t_2) \in R'_{\varepsilon'} \in R'$ for some $\varepsilon' \leq \lambda^{-1}\big(\varepsilon - d_{\mathsf{Spec}}(k_1', k_2)\big)$. □

Theorem A.2. *For WMTS S_1, S_2 with S_1 locally consistent and S_2 deterministic, we have $d_t(S_1, S_2) = d_m(S_1, S_2)$.*

Proof. If $d_t(S_1, S_2) = \infty$, we are done by Theorem 1. Otherwise, let $R = \{R_\varepsilon \mid \varepsilon \geq 0\}$ be the smallest relation family for which

- $(s_1^0, s_2^0) \in R_{d_t(S_1,S_2)}$ and
- whenever $(s_1, s_2) \in R_\varepsilon \in R$, $s_1 \overset{a,I_1}{\dashrightarrow}_1 t_1$, $s_2 \overset{a,I_2}{\dashrightarrow}_2 t_2$, then $(t_1, t_2) \in R_{\lambda^{-1}(\varepsilon - d_{\mathsf{Spec}}((a,I_1),(a,I_2)))}$.

We show below that this definition makes sense (especially that $\varepsilon - d_{\mathsf{Spec}}\big((a, I_1), (a, I_2)\big) \geq 0$ in all cases), and that R is a modal refinement family. We will use the convenient notation (s_1, S_1) for the WMTS S_1 with initial state s_1^0 replaced by s_1, similarly for (s_2, S_2).

We first show inductively that for any pair of states $(s_1, s_2) \in R_\varepsilon \in R$ we have $d_t\big((s_1, S_1), (s_2, S_2)\big) \leq \varepsilon$. This is obviously the case for $s_1 = s_1^0$ and $s_1 = s_2^0$, so assume now that $(s_1, s_2) \in R_\varepsilon \in R$ is such that $d_t\big((s_1, S_1), (s_2, S_2)\big) \leq \varepsilon$ and let $s_1 \overset{a,I_1}{\dashrightarrow}_1 t_1$, $s_2 \overset{a,I_2}{\dashrightarrow}_2 t_2$. Let $(q_1', P_1') \in [\![(t_1, S_1)]\!]$ and $x_1 \in I_1$.

There is an implementation $(p_1, P_1) \in [\![(s_1, S_1)]\!]$ for which $p_1 \xrightarrow{a,x_1} q_1$ and $(q_1, P_1) \leq_m (q_1', P_1')$. Now

$$d_t\big((p_1, P_1), (s_2, S_2)\big) \leq d_t\big((p_1, P_1), (s_1, S_1)\big) + d_t\big((s_1, S_1), (s_2, S_2)\big) \leq \varepsilon,$$

hence we must have $s_2 \overset{a_2',I_2'}{\dashrightarrow}_2 t_2'$ with $d_{\mathsf{Spec}}\big((a, x_1), (a_2', I_2')\big) \leq \varepsilon$. But then $a_2' = a$, hence by determinism of S_2, $I_2 = I_2'$ and $t_2 = t_2'$.

The above considerations hold for any $x_1 \in I_1$, hence $d_{\mathsf{Spec}}\big((a, I_1), (a, I_2)\big) \leq \varepsilon$. Thus $\varepsilon - d_{\mathsf{Spec}}\big((a, I_1), (a, I_2)\big) \geq 0$, and the definition of R above is justified. Now let $x_2 \in I_2$ such that $d_{\mathsf{Spec}}\big((a, x_1), (a, x_2)\big) = d_{\mathsf{Spec}}\big((a, x_1), (a, I_2)\big)$, then there is an implementation $(p_2, P_2) \in [\![(s_2, S_2)]\!]$ for which $p_2 \xrightarrow{a,x_2} q_2$, and

$$\begin{aligned} d\big((q_1', P_1'), (q_2, P_2)\big) &\leq \lambda^{-1}\big(\varepsilon - d_{\mathsf{Spec}}((a, x_1), (a, x_2))\big) \\ &= \lambda^{-1}\big(\varepsilon - d_{\mathsf{Spec}}((a, I_1), (a, I_2))\big), \end{aligned}$$

which, as $(q_1', P_1') \in [\![(t_1, S_1)]\!]$ was chosen arbitrarily, entails $d_t\big((s_1, S_1), (s_2, S_2)\big) \leq \lambda^{-1}\big(\varepsilon - d_{\mathsf{Spec}}((a, I_1), (a, I_2))\big)$.

We are ready to show that R is a refinement family. Let $(s_1, s_2) \in R_\varepsilon \in R$ for some ε, and assume $s_1 \overset{k_1}{\dashrightarrow}_1 t_1$; by local consistency of S we must have $k_1 \neq \bot$, hence $k_1 = (a, I_1)$. Let $x \in I_1$, then there is an implementation $(p, P^x) \in [\![(s_1, S_1)]\!]$ with a transition $p \xrightarrow{m} q$. Now $d_t\big((p, P^x), (s_2, S_2)\big) \leq \varepsilon$, hence we have a transition $s_2 \overset{a, I_2^x}{\dashrightarrow}_2 t_2^x$ with $d_{\mathsf{Spec}}\big((a, x), (a, I_2^x)\big) \leq \varepsilon$. Also for any other $x' \in I_1$ we have a transition $s_2 \overset{a, I_2^{x'}}{\dashrightarrow}_2 t_2^{x'}$ with $d_{\mathsf{Spec}}\big((a, x'), (a, I_2^{x'})\big) \leq \varepsilon$, hence by determinism of S_2, $I_2^x = I_2^{x'}$ and $t_2^x = t_2^{x'}$. It follows that there is a unique transition $s_2 \overset{a, I_2}{\dashrightarrow} t_2$, and as $d_{\mathsf{Spec}}\big((a, x), (a, I_2)\big) \leq \varepsilon$ for all $x \in I_1$, we have $d_{\mathsf{Spec}}\big((a, I_1), (a, I_2)\big) \leq \varepsilon$, and $(t_1, t_2) \in R_{\lambda^{-1}(\varepsilon - d_{\mathsf{Spec}}((a, I_1), (a, I_2)))}$ by definition.

Now assume $s_2 \xrightarrow{k_2}_2 t_2$. If $k_2 = \bot$, then there is a transition $s_1 \xrightarrow{\bot} t_1$ in S_1, in contradiction to local consistency of S_1. Hence $k_2 = (a, I_2)$. Let $(p_1, P_1) \in [\![(s_1, S_1)]\!]$, then we have $(p_2, P_2) \in [\![(s_2, S_2)]\!]$ with $d\big((p_1, P_1), (p_2, P_2)\big) \leq \varepsilon$. Now any $(p_2, P_2) \in [\![(s_2, S_2)]\!]$ has $p_2 \xrightarrow{a, x_2} q_2$ with $x_2 \in I_2$, thus there is also $p_1 \xrightarrow{a, x_1} q_1$ with $d_{\mathsf{Spec}}\big((a, x_1), (a, x_2)\big) \leq \varepsilon$ and $d\big((q_1, P_1), (q_2, P_2)\big) \leq \lambda^{-1}\big(\varepsilon - d_{\mathsf{Spec}}((a, x_1), (a, x_2))\big)$. This in turn implies that $s_1 \xrightarrow{a, I_1}_1 t_1$ for some $x_1 \in I_1$. We will be done once we can show $d_{\mathsf{Spec}}\big((a, I_1), (a, I_2)\big) \leq \varepsilon$, so assume to the contrary that there is $x_1' \in I_1$ with $d_{\mathsf{Spec}}\big((a, x_1), (a, I_2)\big) > \varepsilon$. Then there is an implementation $(p_1', P_1') \in [\![(s_1, S_1)]\!]$ with $p_1' \xrightarrow{a, x_1'} q_1'$, hence a transition $s_2 \overset{a, I_2'}{\dashrightarrow}_2 t_2'$ with $d_{\mathsf{Spec}}\big((a, x_1'), (a, I_2')\big) \leq \varepsilon$. But $I_2' = I_2$ by determinism of S_2, a contradiction. $\square$

Complexity Bounds

The fact that computing thorough refinement distance is EXPTIME-hard is easy. By [4], deciding thorough refinement for MTS (without weights) is EXPTIME-complete. By translating MTS to WMTS with weight 0 on all transitions, deciding thorough refinement for modal transition systems polynomial-time reduces to deciding whether thorough refinement distance is ≤ 0.

To show an upper bound on the complexity of computing modal refinement distance, we need to introduce *discounted values of weighted games*, *cf.* [19]. A weighted game graph is a finite real-weighted bipartite digraph $(V_1, V_2, \longrightarrow)$, *i.e.* with $V_1 \cap V_2 = \emptyset$ and $\longrightarrow \in (V_1 \times \mathbb{R} \times V_2) \cup (V_2 \times \mathbb{R} \times V_1)$ a finite set of edges. These are assumed to be non-blocking in the sense that each $v \in V_1 \cup V_2$ has at least one outgoing edge $v \xrightarrow{r} w$ (which is the shorthand for $(v, r, w) \in \longrightarrow$).

A Player-1 strategy in such a weighted game graph is a mapping $\theta_1 : V_1 \to \mathbb{R} \times V_2$ for which $\big(v_1, \theta_1(v_1)\big) \in \longrightarrow$ for each $v_1 \in V_1$. Similarly, a Player-2 strategy is a mapping $\theta_2 : V_2 \to \mathbb{R} \times V_1$ such that $\big(v_2, \theta_2(v_2)\big) \in \longrightarrow$ for each $v_2 \in V_2$. The sets of all Player-1 and Player-2 strategies are denoted Θ_1 and Θ_2, respectively.

Denote by $tgt(e) = w$ the target of an edge $e = (v, r, w) \in \longrightarrow$ and by $wt(e) = r$ its weight. A vertex $v_0 \in V_1$ and a pair $(\theta_1, \theta_2) \in \Theta_1 \times \Theta_2$ of strategies determine a unique infinite sequence $\big(e_j(\theta_1, \theta_2)\big)_{j \geq 0}$ of edges $e_j(\theta_1, \theta_2) \in \longrightarrow$ for which

$$\begin{aligned} e_0(\theta_1,\theta_2) &= \big(v_0, \theta_1(v_0)\big), \\ e_{2j+1}(\theta_1,\theta_2) &= \big(tgt(e_{2j}), \theta_2(tgt(e_{2j}))\big), \\ e_{2j}(\theta_1,\theta_2) &= \big(tgt(e_{2j-1}, \theta_1(tgt(e_{2j-1}))\big). \end{aligned}$$

In other words, the two players alternate to pick edges in $\longrightarrow$ according to their strategies. The *discounted value* of the game $(V_1, V_2, \longrightarrow)$ played from $v_0 \in V_1$ with discounting factor λ, $0 \le \lambda < 1$, is defined to be

$$p(v_0,\lambda) = \sup_{\theta_1\in\Theta_1} \inf_{\theta_2\in\Theta_2} \sum_{j=0}^{\infty} \lambda^j\, wt\big(e_j(\theta_1,\theta_2)\big).$$

We recall the following theorem from [19]; the complexity result is obtained by reduction to simple stochastic games [7].

Lemma 1 ([19]). *The discounted value $p(v_0,\lambda)$ may be computed as the unique fixed point to the equations*

$$p(v,\lambda) = \begin{cases} \max\limits_{v \xrightarrow{r} w} r + \lambda p(w,\lambda) & \text{if } v \in V_1, \\ \min\limits_{v \xrightarrow{r} w} r + \lambda p(w,\lambda) & \text{if } v \in V_2. \end{cases}$$

The decision problem corresponding to computing $p(v_0)$ is contained in NP$\cap$coNP*.*

Next we present a reduction from modal refinement distance of WMTS to discounted values of weighted games, *cf.* [11].

Lemma 2. *For WMTS S_1, S_2 one can construct in polynomial time a weighted game $(V_1, V_2, \longrightarrow)$ with a vertex $v_0 \in V_1$ such that $d_m(S_1,S_2) = p(v_0,\sqrt{\lambda})$.*

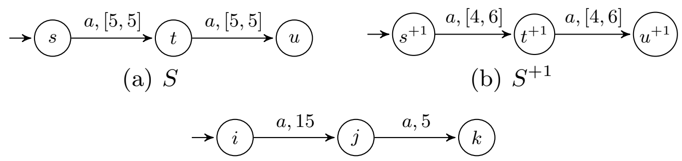
Proof. Let $V_1 = S_1 \times S_2$, $V_2 = S_1 \times S_2 \times \mathsf{Spec} \times \{may, must\}$, and define the transitions as follows:

$$\begin{aligned} (s_1,s_2) &\xrightarrow{0} (t_1,s_2,k_1,may) && \text{if} \quad s_1 \overset{k_1}{\dashrightarrow}_1 t_1 \\ (s_1,s_2) &\xrightarrow{0} (s_1,t_2,k_2,must) && \text{if} \quad s_2 \xrightarrow{k_2}_2 t_2 \\ (t_1,s_2,k_1,may) &\xrightarrow{d_{\mathsf{Spec}}(k_1,k_2)} (t_1,t_2) && \text{if} \quad s_2 \overset{k_2}{\dashrightarrow}_2 t_2 \\ (s_1,t_2,k_2,must) &\xrightarrow{d_{\mathsf{Spec}}(k_1,k_2)} (t_1,t_2) && \text{if} \quad s_1 \xrightarrow{k_1}_1 t_1 \end{aligned}$$

Setting $v_0 = (s_1^0, s_2^0)$ finishes the construction. $\square$

In [11] it is also shown that conversely, computing discounted values of weighted games may be polynomial-time reduced to computing simulation distance for weighted transition systems, hence we can conclude the following.

Lemma 3. *The decision problem corresponding to computing modal refinement distance for WMTS is polynomial-time equivalent to the decision problem corresponding to computing discounted values of weighted games.*



(a) S (b) S^{+1}

(c) I

Fig. 4. WMTS S for which $\llbracket S' \rrbracket \subsetneq \llbracket S \rrbracket^{+\varepsilon}$.

Appendix: Proofs for Section 4

Proof (of Proposition 1). By the triangle inequality we have

$$\begin{aligned} d_m(S_1, S_2') &\le d_m(S_1, S_2) + d_m(S_2, S_2'), \\ d_m(S_1, S_2) &\le d_m(S_1, S_2') + d_m(S_2', S_2), \\ d_m(S_1, S_2) &\le d_m(S_1, S_1') + d_m(S_1', S_2), \\ d_m(S_1', S_2) &\le d_m(S_1', S_1) + d_m(S_1, S_2). \end{aligned} \qquad \square$$

Proof (of Proposition 2). For the first claim, the identity relation $\mathrm{id}_S = \{(s, s) \mid s \in S\} \subseteq S \times S$ is a witness for $S \le_m S^{+\delta}$: if $s \overset{k}{\dashrightarrow} t$, then by construction $s \overset{k_2}{\dashrightarrow}_{+\delta} t$ with $k \sqsubseteq k_2$, and if $s \xrightarrow{k_2}_{+\delta} t$, then again by construction $s \xrightarrow{k} t$ for some $k \sqsubseteq k_2$.

Now to prove $d_m(S^{+\delta}, S) \le (1-\lambda)^{-1}\delta$, we define a family of relations $R = \{R_\varepsilon \mid \varepsilon \ge 0\}$ by $R_\varepsilon = \emptyset$ for $\varepsilon < (1-\lambda)^{-1}\delta$ and $R_\varepsilon = \mathrm{id}_S$ for $\varepsilon \ge (1-\lambda)^{-1}\delta$. We show that R is a modal refinement family.

Let $(s, s) \in R_\varepsilon$ for some $\varepsilon \ge (1-\lambda)^{-1}\delta$, and assume $s \overset{k_2}{\dashrightarrow}_{+\delta} t$. By construction there is a transition $s \overset{k}{\dashrightarrow} t$ with $d_{\mathsf{Spec}}(k_2, k) \le \delta \le \varepsilon$. Now

$$\frac{1}{\lambda}\Big(\varepsilon - d_{\mathsf{Spec}}(k_2, k)\Big) \ge \frac{1}{\lambda}\Big(\frac{\delta}{1-\lambda} - \delta\Big) = \frac{\delta}{1-\lambda} \ge \varepsilon$$

and $(t, t) \in R_\varepsilon$, which settles this part of the proof. The other direction, starting with a transition $s \xrightarrow{k} t$, is similar. $\square$

Proof (of Proposition 3). If $I \in \llbracket S' \rrbracket$, then $d_m(I, S') = 0$, hence $d_m(I, S) \le \varepsilon$ by Proposition 1, which in turn implies that $I \in \llbracket S \rrbracket^{+\varepsilon}$. The example in Figure 4 then shows that in general, $\llbracket S' \rrbracket \subsetneq \llbracket S \rrbracket^{+\varepsilon}$. For $\delta = 1$ and $\lambda = .9$, we have $I \in \llbracket S \rrbracket^{+(1-\lambda)^{-1}\delta}$, but $I \notin \llbracket S^{+\delta} \rrbracket$. $\square$

Appendix: Proofs for Section 5

Theorem A.3. *There is no unary operator $\mathcal{D}$ on WMTS for which it holds that*

(3.1) *$\mathcal{D}(S)$ is deterministic for any WMTS S,*

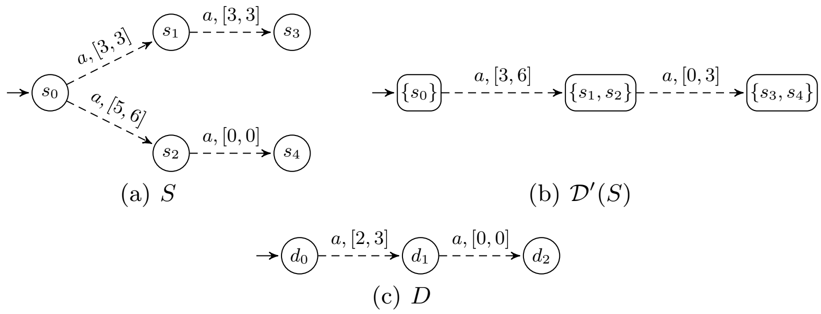


Fig. 5. WMTS for which $d_m\big(\mathcal{D}'(S), D\big) \not\leq d_m(S, D)$.

(3.2) *$S \leq_m \mathcal{D}(S)$ for any WMTS S,*
(3.3) *$S \leq_m^\varepsilon D$ implies $\mathcal{D}(S) \leq_m^\varepsilon D$ for any WMTS S, any deterministic WMTS D, and any $\varepsilon \geq 0$.*

Proof. There is a determinization operator $\mathcal{D}'$ on WMTS, introduced in [3], which satisfies Property (3.2) above and a weaker version of Property (3.3) with $\varepsilon = 0$:

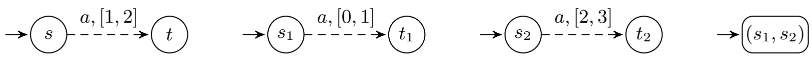
(3.3′) $S \leq_m D$ implies $\mathcal{D}'(S) \leq_m D$ for any WMTS S and any deterministic WMTS D.

Assume now that there is an operator $\mathcal{D}$ as in the theorem. Then for any WMTS S, $S \leq_m \mathcal{D}'(S)$ and thus $\mathcal{D}(S) \leq_m \mathcal{D}'(S)$ by (3.3), and $S \leq_m \mathcal{D}(S)$ and hence $\mathcal{D}'(S) \leq_m \mathcal{D}(S)$ by (3.3′). We finish the proof by showing that the operator $\mathcal{D}'$ from [3] does not satisfy (3.3). The example in Figure 5 shows a WMTS S and a deterministic WMTS D for which $d_m\big(\mathcal{D}'(S), D\big) = 3 + 3\lambda$ and $d_m(S, D) = \max(3, 3\lambda) = 3$, hence $d_m\big(\mathcal{D}'(S), D\big) \not\leq d_m(S, D)$. ☐

Theorem A.4. *There is no partial binary operator $\wedge$ on WMTS for which it holds that*

(4.1) *$S_1 \wedge S_2 \leq_m S_1$ and $S_1 \wedge S_2 \leq_m S_2$ for all locally consistent WMTS S_1, S_2 for which $S_1 \wedge S_2$ is defined,*
(4.2) *for any locally consistent WMTS S and all deterministic and locally consistent WMTS S_1, S_2 such that $S \leq_m S_1$ and $S \leq_m S_1$, $S_1 \wedge S_2$ is defined and $S \leq_m S_1 \wedge S_2$,*
(4.3) *for any $\varepsilon \geq 0$, there exist $\varepsilon_1 \geq 0$ and $\varepsilon_2 \geq 0$ such that for any locally consistent WMTS S and all deterministic and locally consistent WMTS S_1, S_2 for which $S_1 \wedge S_2$ is defined, $S \leq_m^{\varepsilon_1} S_1$ and $S \leq_m^{\varepsilon_2} S_2$ imply $S \leq_m^\varepsilon S_1 \wedge S_2$.*

Proof. We follow the same strategy as in the proof of Theorem 3. There is a conjunction operator $\wedge'$ defined for WMTS in [3] which satisfies Properties (4.1)



(a) S (b) S_1 (c) S_2 (d) $S_1 \wedge S_2$

Fig. 6. WMTS for which $d_m(S, S_1 \wedge S_2) \not\leq \max\big(d_m(S, S_1), d_m(S, S_2)\big)$.

and (4.2) and a version (4.3′) for $\varepsilon = 0$ of Property (4.3). Using these properties, one can see that for all deterministic and locally consistent WMTS S_1 and S_2 for which $S_1 \wedge S_2$ and $S_1 \wedge' S_2$ are locally consistent, $S_1 \wedge S_2 \leq_m S_1 \wedge' S_2$ and $S_1 \wedge' S_2 \leq_m S_1 \wedge S_2$. The WMTS depicted in Figure 6 then show that $d_m(S, S_1 \wedge S_2) \leq \max\big(d_m(S, S_1), d_m(S, S_2)\big)$ does not hold in general. Indeed, $d_m(S, S_1) = d_m(S, S_2) = 1$, but $d_m(S, S_1 \wedge S_2) = \infty$. □

Appendix: Proofs for Section 6

Lemma 4. *For $k_1, k_2, k_3, k_4 \in \mathsf{Spec}$ with $k_1 \oplus k_3$ and $k_2 \oplus k_4$ defined, we have $d_{\mathsf{Spec}}(k_1 \oplus k_3, k_2 \oplus k_4) \leq d_{\mathsf{Spec}}(k_1, k_2) + d_{\mathsf{Spec}}(k_3, k_4)$.*

Proof (of Lemma 4). If $k_1 = \bot$ or $k_3 = \bot$, then the left-hand side of the inequality is 0, and if $k_2 = \bot$ or $k_4 = \bot$, then the right-hand side is ∞, hence in both cases the proof is complete. We are left with the case where all $k_i \neq \bot$; write $k_i = \big(a, [x_i, y_i]\big)$ for all i. We have

$$\begin{aligned} d_{\mathsf{Spec}}(k_1 \oplus k_3, k_2 \oplus k_4) &= \max\big((x_2 + x_4) \dot{-} (x_1 + x_3), (y_1 + y_3) \dot{-} (y_2 + y_4)\big), \\ d_{\mathsf{Spec}}(k_1, k_2) + d_{\mathsf{Spec}}(k_3, k_4) &= \max(x_2 \dot{-} x_1, y_1 \dot{-} y_2) + \max(x_4 \dot{-} x_3, y_3 \dot{-} y_4) \\ &\geq \max\big((x_2 \dot{-} x_1) + (x_4 \dot{-} x_3), (y_1 \dot{-} y_2) + (y_3 \dot{-} y_4)\big). \end{aligned}$$

But

$$\begin{aligned} (x_2 + x_4) \dot{-} (x_1 + x_3) &= \max\big((x_2 + x_4) - (x_1 + x_3), 0\big) \\ &= \max\big((x_2 - x_1) + (x_4 - x_3), 0\big) \\ &\leq \max(x_2 - x_1, 0) + \max(x_4 - x_3, 0) \\ &= (x_2 \dot{-} x_1) + (x_4 \dot{-} x_3), \end{aligned}$$

and similarly one shows $(y_1 + y_3) \dot{-} (y_2 + y_4) \leq (y_1 \dot{-} y_2) + (y_3 \dot{-} y_4)$. □

Proof (of Theorem 5). If $d_m(S_1, S_2) = \infty$ or $d_m(S_3, S_4) = \infty$, we have nothing to prove. Otherwise, let $R^1 = \{R^1_\varepsilon \subseteq S_1 \times S_2 \mid \varepsilon \geq 0\}$, $R^2 = \{R^2_\varepsilon \subseteq S_3 \times S_4 \mid \varepsilon \geq 0\}$ be witnesses for $d_m(S_1, S_2)$ and $d_m(S_3, S_4)$, respectively; hence $(s_1^0, s_2^0) \in R^1_{d_m(S_1,S_2)} \in R^1$ and $(s_3^0, s_4^0) \in R^2_{d_m(S_3,S_4)} \in R^2$. Define

$$\begin{aligned} R_\varepsilon = \big\{\big((s_1, s_3), (s_2, s_4)\big) \in S_1 \times S_3 \times S_2 \times S_4 \mid \\ (s_1, s_2) \in R^1_{\varepsilon_1} \in R^1, (s_3, s_4) \in R^2_{\varepsilon_2} \in R^2, \varepsilon_1 + \varepsilon_2 \leq \varepsilon\big\} \end{aligned}$$

for all $\varepsilon \geq 0$ and let $R = \{R_\varepsilon \mid \varepsilon \geq 0\}$. We show that R is a witness for $d_m\big(S_1\|S_3, S_2\|S_4\big) \leq d_m(S_1, S_2) + d_m(S_3, S_4)$.

We have $\big((s_1^0, s_3^0), (s_2^0, s_4^0)\big) \in R_{d_m(S_1,S_2)+d_m(S_3,S_4)} \in R$. Now let $\big((s_1, s_3), (s_2, s_4)\big) \in R_\varepsilon \in R$ for some ε, then $(s_1, s_2) \in R^1_{\varepsilon_1} \in R^1$ and $(s_3, s_4) \in R^2_{\varepsilon_2} \in R^2$ for some $\varepsilon_1 + \varepsilon_2 \leq \varepsilon$.

Assume $(s_1, s_3) \overset{k_1 \oplus k_3}{\dashrightarrow} (t_1, t_3)$, then $s_1 \overset{k_1}{\dashrightarrow}_1 t_1$ and $s_3 \overset{k_3}{\dashrightarrow}_3 t_3$. By $(s_1, s_2) \in R^1_{\varepsilon_1} \in R^1$, we have $s_2 \overset{k_2}{\dashrightarrow}_2 t_2$ with $d_{\mathsf{Spec}}(k_1, k_2) \leq \varepsilon_1$ and $(t_1, t_2) \in R^1_{\varepsilon_1'} \in R^1$ for some $\varepsilon_1' \leq \lambda^{-1}\big(\varepsilon_1 - d_{\mathsf{Spec}}(k_1, k_2)\big)$; similarly, $s_4 \overset{k_4}{\dashrightarrow}_4 t_4$ with $d_{\mathsf{Spec}}(k_3, k_4) \leq \varepsilon_2$ and $(t_3, t_4) \in R^2_{\varepsilon_2'} \in R^2$ for some $\varepsilon_2' \leq \lambda^{-1}\big(\varepsilon_2 - d_{\mathsf{Spec}}(k_3, k_4)\big)$. Let $\varepsilon' = \varepsilon_1' + \varepsilon_2'$, then the sum $k_2 \oplus k_4$ is defined, and

$$\begin{aligned} \varepsilon' &\leq \lambda^{-1}\big(\varepsilon_1 + \varepsilon_2 - (d_{\mathsf{Spec}}(k_1, k_2) + d_{\mathsf{Spec}}(k_3, k_4))\big) \\ &\leq \lambda^{-1}\big(\varepsilon - d_{\mathsf{Spec}}(k_1 \oplus k_3, k_2 \oplus k_4)\big) \end{aligned}$$

by Lemma 4. We have $(s_2, s_4) \overset{k_2 \oplus k_4}{\dashrightarrow} (t_2, t_4)$, $d_{\mathsf{Spec}}(k_1 \oplus k_3, k_2 \oplus k_4) \leq \varepsilon_1 + \varepsilon_2 \leq \varepsilon$ again by Lemma 4, and $\big((t_1, t_3), (t_2, t_4)\big) \in R_{\varepsilon'} \in R$.

The reverse direction, starting with a transition $(s_2, s_4) \xrightarrow{k_2 \oplus k_4} (t_2, t_4)$, is similar. □

Lemma 5. *If $k_1, k_2, k_3 \in \mathsf{Spec}$ are such that $k_1 \ominus k_2$ and $k_2 \oplus k_3$ are defined and $k_1 \ominus k_2 \neq \perp$, $k_2 \oplus k_3 \neq \perp$, then $d_{\mathsf{Spec}}(k_3, k_1 \ominus k_2) = d_{\mathsf{Spec}}(k_2 \oplus k_3, k_1)$.*

Proof (of Lemma 5). We can write $k_i = \big(a, [x_i, y_i]\big)$ for some $a \in \Sigma$. Then

$$\begin{aligned} d_{\mathsf{Spec}}(k_3, k_1 \ominus k_2) &= \max\big((x_1 - x_2) \dot{-} x_3, y_3 \dot{-} (y_1 - y_2)\big) \\ &= \begin{cases} x_1 - x_2 - x_3 & \text{if } \begin{array}{l} x_1 - x_2 - x_3 \geq 0 \\ x_1 - x_2 - x_3 \geq y_3 - y_1 + y_2 \end{array} \\ y_3 - y_1 + y_2 & \text{if } \begin{array}{l} y_3 - y_1 + y_2 \geq 0 \\ y_3 - y_1 + y_2 \geq x_1 - x_2 - x_3 \end{array} \\ 0 & \text{if } \begin{array}{l} x_1 - x_2 - x_3 \leq 0 \\ y_3 - y_1 + y_2 \leq 0 \end{array} \end{cases} \end{aligned}$$

and similarly

$$\begin{aligned} d_{\mathsf{Spec}}(k_2 \oplus k_3, k_1) &= \max\big(x_1 \dot{-} (x_2 + x_3), (y_2 + y_3) \dot{-} y_1\big) \\ &= \begin{cases} x_1 - x_2 - x_3 & \text{if } \begin{array}{l} x_1 - x_2 - x_3 \geq 0 \\ x_1 - x_2 - x_3 \geq y_2 + y_3 - y_1 \end{array} \\ y_2 + y_3 - y_1 & \text{if } \begin{array}{l} y_2 + y_3 - y_1 \geq 0 \\ y_2 + y_3 - y_1 \geq x_1 - x_2 - x_3 \end{array} \\ 0 & \text{if } \begin{array}{l} x_1 - x_2 - x_3 \leq 0 \\ y_2 + y_3 - y_1 \leq 0 \end{array} \end{cases} \end{aligned}$$

□

Proof (of Theorem 6). To avoid confusion, we write $\dashrightarrow_{\mathbin{\backslash\!\!\backslash}}$ and $\longrightarrow_{\mathbin{\backslash\!\!\backslash}}$ for transitions in $S_1 \mathbin{\backslash\!\!\backslash} S_2$ and $\dashrightarrow_{\|}$ and $\longrightarrow_{\|}$ for transitions in $S_2\|S_3$. The inequality $d_m(S_3, S_1 \mathbin{\backslash\!\!\backslash} S_2) \geq d_m(S_2\|S_3, S_1)$ is trivial if $d_m(S_2\|S_3, S_1) = \infty$, so assume the opposite and let $R^1 = \big\{R^1_\varepsilon \subseteq S_3 \times \big(S_1 \times S_2 \cup \{u\}\big) \bigm| \varepsilon \geq 0\big\}$ be a witness for $d_m(S_3, S_1 \mathbin{\backslash\!\!\backslash} S_2)$. Define $R^2_\varepsilon = \big\{\big((s_2,s_3),s_1\big) \bigm| \big(s_3,(s_1,s_2)\big) \in R^1_\varepsilon\big\} \subseteq S_2 \times S_3 \times S_1$ for all $\varepsilon \ge 0$, and let $R^2 = \{R^2_\varepsilon \mid \varepsilon \ge 0\}$. Certainly $\big((s^0_2,s^0_3),s^0_1\big) \in R^2_{d_m(S_3,S_1 \mathbin{\backslash\!\!\backslash} S_2)} \in R^2$, so let now $\big((s_2,s_3),s_1\big) \in R^2_\varepsilon \in R^2$ for some $\varepsilon \ge 0$.

Assume $(s_2,s_3) \overset{k_2 \oplus k_3}{\dashrightarrow}_{\|} (t_2,t_3)$, then also $s_2 \overset{k_2}{\dashrightarrow}_2 t_2$ and $s_3 \overset{k_3}{\dashrightarrow}_3 t_3$, and by local consistency, $k_3 \ne \perp$. By $\big(s_3,(s_1,s_2)\big) \in R^1_\varepsilon$, there is $(s_1,s_2) \overset{k_1 \ominus k'_2}{\dashrightarrow}_{\mathbin{\backslash\!\!\backslash}} (t_1,t'_2)$ for which $d_{\mathsf{Spec}}(k_3, k_1 \ominus k'_2) = d_{\mathsf{Spec}}(k'_2 \oplus k_3, k_1) \le \varepsilon$ and such that $\big(t_3,(t_1,t'_2)\big) \in R^1_{\varepsilon'} \in R^1$, hence $\big((t'_2,t_3),t_1\big) \in R^2_{\varepsilon'} \in R^2$, for some $\varepsilon' \le \lambda^{-1}\big(\varepsilon - d_{\mathsf{Spec}}(k'_2 \oplus k_3, k_1)\big)$. By definition of quotient we must have $s_1 \overset{k_1}{\dashrightarrow}_1 t_1$ and $s_2 \overset{k'_2}{\dashrightarrow}_2 t'_2$, and by determinism of S_2, $k'_2 = k_2$ and $t'_2 = t_2$.

Assume $s_1 \xrightarrow{k_1}_1 t_1$, then we have $k_1 \ne \perp$ by local consistency of S_1. We must have a transition $s_2 \xrightarrow{k_2}_2 t_2$ for which $k_1 \ominus k_2$ is defined and $k_1 \ominus k_2 \ne \perp$, for otherwise the state (s_1,s_2) would have been pruned from $S_1 \mathbin{\backslash\!\!\backslash} S_2$. Hence $(s_1,s_2) \xrightarrow{k_1 \ominus k_2}_{\mathbin{\backslash\!\!\backslash}} (t_1,t_2)$. This in turn implies that there is $s_3 \xrightarrow{k_3}_3 t_3$ for which $d_{\mathsf{Spec}}(k_3, k_1 \ominus k_2) = d_{\mathsf{Spec}}(k_2 \oplus k_3, k_1) \le \varepsilon$ and such that $\big(t_3,(t_1,t_2)\big) \in R^1_{\varepsilon'} \in R^1$, hence $\big((t_2,t_3),t_1\big) \in R^2_{\varepsilon'} \in R^2$, for some $\varepsilon' \le \lambda^{-1}\big(\varepsilon - d_{\mathsf{Spec}}(k_2 \oplus k_3, k_1)\big)$, and by definition of parallel composition, $(s_2,s_3) \xrightarrow{k_2 \oplus k_3}_{\|} (t_2,t_3)$.

To show that $d_m(S_3, S_1 \mathbin{\backslash\!\!\backslash} S_2) \le d_m(S_2 \| S_3, S_1)$, let $R^2 = \{R^2_\varepsilon \subseteq S_2 \times S_3 \times S_1 \mid \varepsilon \ge 0\}$ be a witness for $d_m(S_2 \| S_3, S_1)$, define $R^1_\varepsilon = \big\{\big(s_3,(s_1,s_2)\big) \bigm| \big((s_2,s_3),s_1\big) \in R^2_\varepsilon\big\} \cup \big\{(s_3,u) \bigm| s_3 \in S_3\big\}$ for all $\varepsilon \ge 0$, and let $R^1 = \{R^1_\varepsilon \mid \varepsilon \ge 0\}$, then $\big(s^0_3,(s^0_1,s^0_2)\big) \in R^1_{d_m(S_2 \| S_3, S_1)} \in R^1$.

For any $(s_3,u) \in R^1_\varepsilon$ for some $\varepsilon \ge 0$, any transition $s_3 \overset{k_3}{\dashrightarrow}_3 t_3$ can be matched by $u \overset{k_3}{\dashrightarrow}_{\mathbin{\backslash\!\!\backslash}} u$, and then $(t_3,u) \in R^1_0$. Let now $\big(s_3,(s_1,s_2)\big) \in R^1_\varepsilon$ for some $\varepsilon \ge 0$, and assume $s_3 \overset{k_3}{\dashrightarrow}_3 t_3$. If $k_2 \oplus k_3$ is undefined for all transitions $s_2 \overset{k_2}{\dashrightarrow}_2 t_2$, then by definition $(s_1,s_2) \overset{k_3}{\dashrightarrow} u$, and again $(t_3,u) \in R^1_0$. If there is a transition $s_2 \overset{k_2}{\dashrightarrow}_2 t_2$ such that $k_2 \oplus k_3$ is defined, then also $(s_2,s_3) \overset{k_2 \oplus k_3}{\dashrightarrow}_{\|} (t_2,t_3)$. Hence we have $s_1 \overset{k_1}{\dashrightarrow}_1 t_1$ with $d_{\mathsf{Spec}}(k_2 \oplus k_3, k_1) \le \varepsilon$, implying that $(s_1,s_2) \overset{k_1 \ominus k_2}{\dashrightarrow}_{\mathbin{\backslash\!\!\backslash}} (t_1,t_2)$. We must have $k_1 \ominus k_2 \ne \perp$, for otherwise $d_{\mathsf{Spec}}(S_3, S_1 \mathbin{\backslash\!\!\backslash} S_2) = \infty$, hence $d_{\mathsf{Spec}}(k_3, k_1 \ominus k_2) = d_{\mathsf{Spec}}(k_2 \oplus k_3, k_1) \le \varepsilon$. Also, $\big((t_2,t_3),t_1\big) \in R^2_{\varepsilon'} \in R^2$, hence $\big(t_3,(t_1,t_2)\big) \in R^1_{\varepsilon'} \in R^1$, for some $\varepsilon' \le \lambda^{-1}\big(\varepsilon - d_{\mathsf{Spec}}(k_3, k_1 \ominus k_2)\big)$.

Assume $(s_1,s_2) \xrightarrow{k_1 \ominus k_2}_{\mathbin{\backslash\!\!\backslash}} (t_1,t_2)$, then $k_1 \ominus k_2 \ne \perp$ by local consistency of $S_1 \mathbin{\backslash\!\!\backslash} S_2$, hence we have $s_1 \xrightarrow{k_1}_1 t_1$ and $s_2 \xrightarrow{k_2}_2 t_2$. It follows that $(s_2,s_3) \xrightarrow{k'_2 \oplus k_3}_{\|} (t'_2,t_3)$ with $d_{\mathsf{Spec}}(k'_2 \oplus k_3, k_1) = d_{\mathsf{Spec}}(k_3, k_1 \ominus k'_2) \le \varepsilon$ and such that $\big((t'_2,t_3),t_1\big) \in R^2_{\varepsilon'} \in R^2$, hence $\big(t_3,(t_1,t'_2)\big) \in R^1_{\varepsilon'} \in R^1$, for some $\varepsilon' \le \lambda^{-1}\big(\varepsilon - d_{\mathsf{Spec}}(k_3, k_1 \ominus k'_2)\big)$. By definition of parallel composition we must have $s_2 \xrightarrow{k'_2}_2 t'_2$ and $s_3 \xrightarrow{k_3}_3 t_3$, and by determinism of S_2, $k'_2 = k_2$ and $t'_2 = t_2$. $\square$