General quantitative specification theories with modal transition systems

Uli Fahrenberg, Axel Legay

Noname manuscript No.
(will be inserted by the editor)

General Quantitative Specification Theories with Modal Transition Systems

Uli Fahrenberg · Axel Legay

the date of receipt and acceptance should be inserted later

Abstract This paper proposes a new theory of quantitative specifications. It generalizes the notions of step-wise refinement and compositional design operations from the Boolean to an arbitrary quantitative setting. Using a great number of examples, it is shown that this general approach permits to unify many interesting quantitative approaches to system design.

1 Introduction

Specification theories permit reasoning about behaviors of systems at the abstract level, which is needed in various application such as abstraction-based model checking for programming languages, or compositional reasoning. Such specification theories generally come with (1) a satisfaction relation that allows to decide whether an implementation is a model of the specification, (2) a notion of refinement for determining the relationship between specifications and their sets of implementations, (3) a structural composition which, at the abstract level, mimics the behavioral composition of systems, (4) a quotient that allows to synthesize specifications from refinements, and (5) a logical composition that allows to compute intersections of sets of implementations.

Prominent among specification theories is the one of *modal transition systems* [30–32, 36, 40], which are labeled transition systems equipped with two types of transitions: *must* transitions that are mandatory for any implementation, and *may* transitions which are optional. In recent work [7, 8, 10, 35], modal transition systems have been extended by adding richer information to the usual discrete label set of transition systems, permitting to reason about *quantitative* aspects of models and specifications. These quantitative labels can be used to model and analyze *e.g.* timing [19, 34], resource usage [8, 42], or energy consumption [15, 25].

This paper is based on the conference contributions [6, 26] which were presented at the 7th International Computer Science Symposium in Russia, CSR 2012, Nizhny Novgorod, Russia, and the 4th Workshop on Foundations of Interface Technologies, FIT 2012, Tallinn, Estonia.

Uli Fahrenberg · Axel Legay
Irisa/INRIA Rennes, France

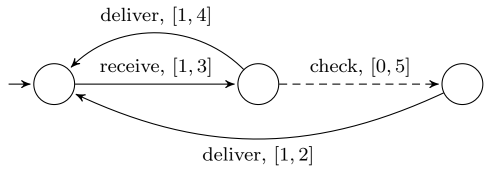


Fig. 1 Specification of a simple email system, with integer intervals modeling time constraints for performing the corresponding actions.

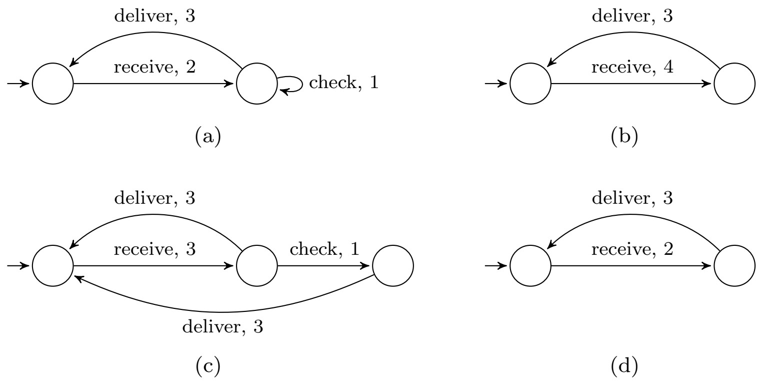


Fig. 2 Four implementations of the simple email system in Figure 1.

In particular, [35] extends modal transition systems with integer intervals and introduces corresponding extensions of the above operations which observe the added quantitative information, and [7] generalizes this theory to general *structured labels*. Both theories are, however, *fragile* in the sense that they rely on Boolean notions of satisfaction and refinement: as refinement either holds or does not, they are unable to *quantify* the impact of small variations in quantities.

An example of a quantitative specification, taken from [5], is shown in Figure 1. The intuition is that any concrete implementation *must* be able to receive and deliver email, within one to three and one to four time units, respectively; but it also *may* be able to check incoming email, *e.g.* for viruses, before delivering it. No other behavior is permitted.

Figure 2 shows four different implementation candidates for the specification of Figure 1. The first candidate in Figure 2(a), however, has an error in the discrete structure: after receiving an email, it may check the email indefinitely. Hence it does not satisfy the specification. The second candidate, in Figure 2(b), is also problematic: not implementing the checking part of the specification is entirely permissible, but it takes too long to receive email. Thus, if the timing constraints are abstracted from, it is a perfectly good implementation; but the quantitative timing constraints are off. The implementation candidate in Figure 2(c) has similar problems, as it takes too long to deliver emails after checking them. The transition system in Figure 2(d) is, finally, a true implementation of the specification.

An important observation is, now, that even though the systems in Figures 2(b) and 2(c) strictly are not implementations of the email system specification, they conform much better to it than the system in Figure 2(a). Intuitively, they "almost" comply with the specification; given some other engineering constraints, they might indeed be considered "good enough" given the specification. It is, then, this "almost" and "good enough" which we shall attempt to formalize in this work.

Our point of view is, more generally speaking, that *any* quantitative specification formalism falls short with a Boolean notion of satisfaction and refinement. If the specification formalism is intended to model quantitative properties, then it is of little use to know that a proposed implementation does not precisely adhere to a specification; much more useful information is obtained by knowing *how well* it implements the specification, or *how far* it is deviating. Of course, the answer to this "how far" question might be ∞, due to discrete errors as in Figure 2(a); but in case it is finite, useful knowledge may be gained *e.g.* as to how much more implementation effort is needed, or whether one can satisfy oneself with this slightly imperfect implementation.

A first quantitative specification theory which is not fragile is introduced in [4, 5]. This uses modal transition systems weighted with intervals as specifications, as in the examples in Figures 1 and 2. Quantitative satisfaction and refinement are measured using a *discounted accumulating distance*, which adds up discrepancies between transition weights, but discounts them so that differences in the further future matter less than differences incurred early. Coming back to our examples, and with a discounting factor of .9, the satisfaction distances of the four implementations in Figure 2 to the specification in Figure 1 are ∞ for system 2(a), 5.3 for system 2(b), 3.0 for system 2(c), and 0 for system 2(d). It will of course depend on the concrete application how these numbers are interpreted, and whether a distance of 5.3 or 3.0 will be considered "good enough".

Pertaining to the application at hand, specifications may be better given using some other formalism than interval-weighted modal transition systems, and satisfaction and refinement may be more realistically measured using other distances than the one given above. For quantifying differences between *systems* (*i.e.* without paying attention to specifications), a number of different distances have been used in different contexts [17,18,20,23,37,46,48], so one should indeed expect the same need for variation with quantitative specification theories.

What is needed is, thus, a quantitative specification theory that is independent of both the specific labels and the distance used to measure differences; this is what we introduce in this paper. Using the concept of distance iterator function from [27,29], we introduce a general notion of refinement distance between structured modal transition systems and a general quantitative specification theory. It turns out that there are some natural technical compatibility conditions relating the label composition operators with the distance which give rise to different properties of the specification theory.

We start out by introducing a general framework of quantitative refinement for quantitative specifications in Sections 2 and 3, together with a natural notion of *quantitative relaxation* of specifications. In Sections 4 and 5, we enrich this theory with generic operations which turn our framework into a *complete specification theory* in the sense of [3]. These operations are as follows:

– *Structural composition* composes two specifications to mimic parallel composition at implementation level; the structural composition $S \| T$ of two specifications S, T thus covers all parallel compositions of implementations of S with implementations of T. In our quantitative setting, this is expressed by a *quantitative independent implementability* property, Theorem 2 on page 17: for all specifications S, T, S', T', the distance from $S\|S'$ to $T\|T'$ is bounded above by a uniform function P on the distances from S to T and from S' to T'.

A prerequisite for our generic structural composition of specifications is a (partial) composition operator $\obar$ on *labels* which specifies which labels can synchronize, and what is the label produced by a synchronization. In the spirit of [49], this covers the most common label synchronizations such as CCS or CSP. In order for quantitative independent implementability to hold, some reasonable assumptions on $\obar$ are necessary which are quantitative generalizations of standard properties [7]. One of these is that composition of labels respects the bound function P we have adhered to above: intuitively, for labels k, ℓ, k', ℓ', the distance from $k \obar \ell$ to $k' \obar \ell'$ needs to be bounded by P applied to the distances from k to ℓ and from k' to ℓ'. Note that this is a completely static property which can easily be decided upon.

– *Quotient* is the adjoint to structural composition, *i.e.* it is used to solve equations of the form $S\|X \equiv T$ for X. This is useful for synthesizing *partial specifications*: if T is the specification of an overall system and S the specification of a part which has already been provided, then the quotient $X = T \bbslash S$ specifies the missing components. This is expressed by the *universal property* of quotient in Theorem 3 on page 20: for all specifications S, T and X, X refines $T \bbslash S$ if and only if $S\|X$ refines T. (Universality of the property refers to the fact that if quotient exists, it is uniquely defined.)

  To define quotient, one needs an operator $\obslash$ on labels which is adjoint to $\obar$. In order to extend quotient's universal property to the quantitative domain, we specify reasonable quantitative assumptions on the relation between $\obslash$ and $\obar$, more precisely, on the distance between m and $\ell \obslash k$ versus the one from $k \obar m$ to ℓ, for labels k, ℓ and m. Under these assumptions (more precisely, if $\obslash$ is *quantitatively exact* as we will define it later), we can show that for all specifications S, T, X, the distance from X to $T \bbslash S$ equals the one from $S\|X$ to T.

– *Conjunction* $\wedge$ of specifications is used to obtain implementations which must comply with both of two specifications. Similarly to the operations above, its prerequisite is a conjunction operator $\owedge$ on labels. It has been shown in [7] that if $\owedge$ is greatest lower bound for labels, then the operator $\wedge$ is greatest lower bound for specifications.

  In order to generalize the properties of $\wedge$ to the quantitative setting, we make an assumption of *boundedness* on $\owedge$, using a uniform bound function C similar to the function P for structural composition. Under this assumption, we can show in Theorem 4 on page 22 a quantitative generalization of the greatest lower bound property: for all specifications S, T, U, the distance from U to $S \wedge T$ is bounded above by C applied to the distances from U to S and from U to T. Motivated by an example which shows that for a common instantiation of our framework, $\owedge$ is *not* bounded, we also introduce a weaker variant of boundedness and show that also this can be lifted from labels to specifications (Theorem 5 on page 23).

Our general quantitative theory can be instantiated with a variety of different distances and operators, all useful for different applications; hence it can serve as a unifying framework for these applications. We develop one specific example in detail in the last section, using the modal event-clock automata of [12–14] for specifications and a distance suitable for real-time information. This *maximum-lead distance*, first introduced in [34], is fundamentally different from the one used in [4, 5], and so are the properties of the obtained quantitative specification theory. This shows the strength of our general approach.

2 Structured Modal Transition Systems

Labeled transition systems have long been established as the de-facto formalism for specifying formal semantics for discrete behavior and communication of programming languages and reactive systems. However, in order to capture meta-data and expectations about these, such as *e.g.* execution times of hardware platforms, cost of certain operations, or energy consumption, we require a richer formalism.

2.1 Labels and traces

We work with a poset Spec of *specification labels* with a partial order $\sqsubseteq_{\mathsf{Spec}}$ and denote by $\mathsf{Spec}^\infty = \mathsf{Spec}^* \cup \mathsf{Spec}^\omega$ the set of finite and infinite traces over Spec. In applications, Spec may be used to model data about the behavior of a system; for specifications this may be considered as legal parameters of operation, whereas for implementations it may be thought of as observed information.

The partial order $\sqsubseteq_{\mathsf{Spec}}$ is meant to model *refinement* of data; if $k \sqsubseteq_{\mathsf{Spec}} \ell$, then k is more refined (leaves fewer choices) than ℓ. The set $\mathsf{Imp} = \{k \in \mathsf{Spec} \mid k' \sqsubseteq_{\mathsf{Spec}} k \implies k' = k\}$ is called the set of *implementation labels*; these are the data which cannot be refined further. We let $[\![k]\!] = \{k' \in \mathsf{Imp} \mid k' \sqsubseteq_{\mathsf{Spec}} k\}$ and assume that $[\![k]\!] \neq \emptyset$ for all $k \in \mathsf{Spec}$.

2.2 Hemimetrics, pseudometrics and metrics

When $k \not\sqsubseteq_{\mathsf{Spec}} \ell$, we want to be able to quantify the impact of this difference in data on the systems in question, thus circumventing the fragility of the theory. To this end, we introduce a general notion of distance on sequences of data following the approach laid out in [29]. Before we can proceed however, we need to recall some terminology. Let $\mathbb{R}_{\geq 0} \cup \{\infty\}$ denote the extended positive reals, let X be a set and $d : X \times X \to \mathbb{R}_{\geq 0} \cup \{\infty\}$. Then d is called

- a *hemimetric* if $d(x, x) = 0$ for all $x \in X$ (indiscernibility of identicals) and $d(x, y) + d(y, z) \geq d(x, z)$ for all $x, y, z \in X$ (triangle inequality);
- a *pseudometric* if it is a hemimetric and additionally, $d(x, y) = d(y, x)$ for all $x, y \in X$ (symmetry);
- a *metric* if it is a pseudometric and additionally, $d(x, y) = 0$ implies $x = y$ for all $x, y \in X$ (identity of indiscernibles)

As our (hemi-, pseudo-)metrics may take the values ∞, some authors will refer to them as *extended* (hemi-, pseudo-)metrics.

Note that contrary to pseudometrics and metrics, hemimetrics are *asymmetric* distances: no relation is implied between $d(x, y)$ and $d(y, x)$. This will be useful for us, as we shall be considered with quantitative generalizations of *preorders* on specifications, which themselves by nature are asymmetric. Most of the distances we will consider are thus hemimetrics.

The *symmetrization* of a hemimetric d is the pseudometric $\bar d: X\times X \to \mathbb{R}_{\ge 0}\cup\{\infty\}$ given by $\bar d(x,y) = \max(d(x,y), d(y,x))$; this is the smallest of all pseudometrics d' on X for which $d \le d'$. Given hemimetrics d on X and d' on another set X', the *product distance* D on $X \times X'$ is defined by $D((x,x'),(y,y')) = d(x,y) + d(x',y')$.

The *Hausdorff hemimetric* associated with a hemimetric $d: X\times X \to \mathbb{R}_{\ge 0}\cup\{\infty\}$ is the function $d^{\mathrm{H}}: 2^X \times 2^X \to \mathbb{R}_{\ge 0} \cup \{\infty\}$ given for subsets $A, B \subseteq X$ by

$$d^{\mathrm{H}}(A,B) = \sup_{x\in A} \inf_{y\in B} d(x,y).$$

This is a well-known construction for metric spaces, *cf.* [1, 39]; there it is usually symmetrized and defined only for *closed* subsets, in which case it is a metric.

2.3 Trace distances

In order to build a framework for specification distances which is general enough to cover the distances commonly used, we introduce a notion of abstract trace distance which factors through a lattice on which it has a recursive characterization. We will show in Section 2.4 that this indeed covers the common scenarios.

Let M be an arbitrary set and $\mathbb{L} = (\mathbb{R}_{\ge 0}\cup\{\infty\})^M$ the set of functions from M to the extended non-negative real line. Then $\mathbb{L}$ is a complete lattice with partial order $\sqsubseteq_{\mathbb{L}}$ given by $\alpha \sqsubseteq_{\mathbb{L}} \beta$ if and only if $\alpha(x) \le \beta(x)$ for all $x \in M$, and with an addition $\oplus_{\mathbb{L}}$ given by $(\alpha \oplus_{\mathbb{L}} \beta)(x) = \alpha(x) + \beta(x)$. The bottom element of $\mathbb{L}$ is also the zero of $\oplus_{\mathbb{L}}$ and given by $\bot_{\mathbb{L}}(x) = 0$, and the top element is $\top_{\mathbb{L}}(x) = \infty$. We also define a metric on $\mathbb{L}$ by $d_{\mathbb{L}}(\alpha,\beta) = \sup_{x\in M} |\alpha(x) - \beta(x)|$.

Intuitively, the lattice $\mathbb{L}$ serves as a memory for more elaborate trace distances such as *e.g.* the limit-average distance, see Section 2.4. For simpler distances, it will suffice to let $M = \{*\}$ be the one-point set and thus $\mathbb{L} = \mathbb{R}_{\ge 0}\cup\{\infty\}$. We extend the notions of hemimetrics, pseudometrics and metrics from above to mappings $d: X\times X \to \mathbb{L}$, by replacing in their defining properties 0 by $\bot_{\mathbb{L}}$ and $+$ by $\oplus_{\mathbb{L}}$.

Let $d: \mathsf{Imp}\times\mathsf{Imp} \to \mathbb{L}$ be a hemimetric on implementation labels. We extend d to Spec by $d(k,\ell) = \sup_{m\in[\![k]\!]} \inf_{n\in[\![\ell]\!]} d(m,n)$. Hence also this distance is *asymmetric*; the intuition is that any label in $[\![k]\!]$ has to be matched as good as possible in $[\![\ell]\!]$. Note that this is the Hausdorff hemimetric associated with d on implementation labels.

We will assume given an abstract *trace distance* $d_T: \mathsf{Spec}^\infty \times \mathsf{Spec}^\infty \to \mathbb{L}$ which is a hemimetric and has a recursive expression using a *distance iterator* function $F: \mathsf{Imp}\times\mathsf{Imp}\times\mathbb{L} \to \mathbb{L}$, see below. This will allow us to recover many of the system distances found in the literature, while preserving key results. We will need to assume that F satisfies the following properties:

(1) F is *continuous* in the first two coordinates: $F(\cdot, n, \alpha)$ and $F(m, \cdot, \alpha)$ are continuous functions $\mathsf{Imp} \to \mathbb{L}$ for all $\alpha \in \mathbb{L}$.
(2) F is *monotone* in the third coordinate: $F(m,n,\cdot): \mathbb{L}\to\mathbb{L}$ is monotone for all $m, n \in \mathsf{Imp}$.
(3) F extends d: for all $m, n \in \mathsf{Imp}$, $F(m,n,\bot_{\mathbb{L}}) = d(m,n)$.

(4) Indiscernibility of identicals: $F(m, m, \alpha) = \alpha$ for all $m \in \mathsf{Imp}$.
(5) An extended triangle inequality: for all $m, n, o \in \mathsf{Imp}$ and $\alpha, \beta, \gamma \in \mathbb{L}$ with $\alpha \oplus_{\mathbb{L}} \beta \sqsupseteq_{\mathbb{L}} \gamma$, $F(m, n, \alpha) \oplus_{\mathbb{L}} F(n, o, \beta) \sqsupseteq_{\mathbb{L}} F(m, o, \gamma)$.

Note how the last two axioms are a generalization of the axioms for hemimetrics stated above.

We extend F to specification labels by defining

$$F(k, \ell, \alpha) = \sup_{m \in [\![k]\!]} \inf_{n \in [\![\ell]\!]} F(m, n, \alpha).$$

Then also the extended $F : \mathsf{Spec} \times \mathsf{Spec} \times \mathbb{L} \to \mathbb{L}$ is continuous in the first two and monotone in the third coordinates. Additionally, we assume that sets of implementation labels are *closed* with respect to F in the sense that for all $k, \ell \in \mathsf{Spec}$ and $\alpha \in \mathbb{L}$ with $F(k, \ell, \alpha) \neq \top_{\mathbb{L}}$, there are $m \in [\![k]\!]$, $n \in [\![\ell]\!]$ with $F(m, \ell, \alpha) = F(k, n, \alpha) = F(k, \ell, \alpha)$. Note that this implies that the sets $[\![k]\!]$ are closed under the hemimetric d on Spec.

Axioms (4) and (5) for F above now imply that for the extension, the following holds:

(4′) For all $k, \ell \in \mathsf{Spec}$ with $k \sqsubseteq_{\mathsf{Spec}} \ell$ and all $\alpha \in \mathbb{L}$, $F(k, \ell, \alpha) = \alpha$.
(5′) For all $k, \ell, m \in \mathsf{Spec}$ and $\alpha, \beta, \gamma \in \mathbb{L}$ with $\alpha \oplus_{\mathbb{L}} \beta \sqsupseteq_{\mathbb{L}} \gamma$, $F(k, \ell, \alpha) \oplus_{\mathbb{L}} F(\ell, m, \beta) \sqsupseteq_{\mathbb{L}} F(k, m, \gamma)$.

Let $\boldsymbol{\varepsilon} \in \mathsf{Spec}^\infty$ denote the empty sequence, and for any sequence $\sigma \in \mathsf{Spec}^\infty$, denote by σ_0 its first element and by σ^1 the tail of the sequence with the first element removed. We assume that d_T has a recursive characterization, using F, as follows:

$$d_T(\sigma, \tau) = \begin{cases} F(\sigma_0, \tau_0, d_T(\sigma^1, \tau^1)) & \text{if } \sigma, \tau \neq \boldsymbol{\varepsilon}, \\ \top_{\mathbb{L}} & \text{if } \sigma = \boldsymbol{\varepsilon}, \tau \neq \boldsymbol{\varepsilon} \text{ or } \sigma \neq \boldsymbol{\varepsilon}, \tau = \boldsymbol{\varepsilon}, \\ \bot_{\mathbb{L}} & \text{if } \sigma = \tau = \boldsymbol{\varepsilon}. \end{cases} \tag{1}$$

We remark that a recursive characterization such as the one above is quite natural. Not only does it cover all commonly used trace distances (see the examples in the next section), but recursion is central to computing, and any trace distance without a recursive characterization would strike us as being quite artificial. It is precisely this recursive characterization which allows us to lift the trace distance to *states* of specifications in Definition 3 below, see also [27, 29] where this relation was discovered.

In applications (see below), the lattice $\mathbb{L}$ comes equipped with a homomorphism $g : \mathbb{L} \to \mathbb{R}_{\geq 0} \cup \{\infty\}$ for which $g(d_T(\sigma, \sigma)) = 0$ for all $\sigma \in \mathsf{Spec}^\infty$. The actual trace distance of interest is then the composition $\tilde{d}_T = g \circ d_T$. The triangle inequality for F implies the usual triangle inequality for $\tilde{d}_T$: $\tilde{d}_T(\sigma, \tau) + \tilde{d}_T(\tau, \chi) \leq \tilde{d}_T(\sigma, \chi)$ for all $\sigma, \tau, \chi \in \mathsf{Spec}^\infty$, hence $\tilde{d}_T$ is a hemimetric on Spec^∞.

We need to work with distances which factor through $\mathbb{L}$, instead of plainly taking values in $\mathbb{R}_{\geq 0} \cup \{\infty\}$, because some distances which are useful in practice, as the ones in Examples 3 and 5 below, have no recursive characterization using $\mathbb{L} = \mathbb{R}_{\geq 0} \cup \{\infty\}$. Whether the theory works for more general intermediate lattices than $\mathbb{L} = (\mathbb{R}_{\geq 0} \cup \{\infty\})^M$ is an open question; we have had no occasion to use more general lattices in practice.

2.4 Examples

To give an application to the framework laid out above, we show here a few examples of specification labels and trace distances and how they fit into the framework. For a much more comprehensive application of the theory see Section 7.

Example 1 A good example of a set of specification labels, introduced in [4], is given by $\mathsf{Spec} = \Sigma \times \mathbb{I}$, where Σ is a finite set of discrete labels and $\mathbb{I} = \{[l, r] \mid l \in \mathbb{Z} \cup \{-\infty\}, r \in \mathbb{Z} \cup \{\infty\}, l \leq r\}$ is the set of extended-integer intervals. The partial order is defined by $(a, [l, r]) \sqsubseteq_{\mathsf{Spec}} (a', [l', r'])$ if and only if $a = a'$, $l' \leq l$ and $r' \geq r$. Hence refinement is given by restricting intervals, so that $\mathsf{Imp} = \Sigma \times \{[x, x] \mid x \in \mathbb{Z}\} \approx \Sigma \times \mathbb{Z}$.

The implementation label distance is given by

$$d((a, x), (a', x')) = \begin{cases} [c]|x - x'| & \text{if } a = a', \\ \infty & \text{otherwise,} \end{cases}$$

so that for specification labels $(a, [l, r])$, $(a', [l', r'])$,

$$\begin{aligned} d((a, [l, r]), (a', [l', r'])) &= \sup_{m \in [\![(a,[l,r])]\!]} \inf_{n \in [\![(a',[l',r'])]\!]} d(m, n) \\ &= \begin{cases} \max(l' - l, r - r', 0) & \text{if } a = a', \\ \infty & \text{otherwise.} \end{cases} \end{aligned}$$

Now let $\mathbb{L} = \mathbb{R}_{\geq 0} \cup \{\infty\}$ and $F(m, n, \alpha) = d(m, n) + \lambda\alpha$ for some fixed *discounting factor* $\lambda \in \mathbb{R}$ with $0 < \lambda < 1$, then $d_T(\sigma, \tau) = \sum_j \lambda^j d(\sigma_j, \tau_j)$ for implementation traces σ, τ of equal length. This distance hence accumulates individual distances on labels; it has been studied for weighted transition systems and games *e.g.* in [18, 20, 24, 37, 46, 48, 50]. The paper [4] then develops a complete specification theory around this specific distance; we will continue this example below to show how it fits in our present context.

Example 2 Using the same setting as above, with $\mathsf{Spec} = \Sigma \times \mathbb{I}$, $(a, [l, r]) \sqsubseteq_{\mathsf{Spec}} (a', [l', r'])$ if and only if $a = a'$, $l' \leq l$ and $r' \geq r$, and $d((a, x), (a', x')) = |x - x'|$ if $a = a'$ and ∞ otherwise, we can instantiate F to a *point-wise* instead of accumulating distance. Let again $\mathbb{L} = \mathbb{R}_{\geq 0} \cup \{\infty\}$, but $F(m, n, \alpha) = \max(d(m, n), \alpha)$. Then $d_T(\sigma, \tau) = \sup_j d(\sigma_j, \tau_j)$ for implementation traces σ, τ of equal length, hence measuring the biggest individual difference between the traces' symbols. This distance has been studied for weighted transition systems and games in [20–22, 37, 46] and other papers; we will also continue this example below to show how to develop a specification theory based on the point-wise distance.

Example 3 Again with the same instantiations of Imp and Spec as above, we can introduce *limit-average* distance. Here we let $\mathbb{L} = (\mathbb{R}_{\geq 0} \cup \{\infty\})^{\mathbb{N}}$, $g : \mathbb{L} \to \mathbb{R}_{\geq 0} \cup \{\infty\}$ given by $g(\alpha) = \liminf_j \alpha(j)$, and $F(m, n, \alpha)(j) = \frac{1}{j+1} d(m, n) + \frac{j}{j+1} \alpha(j - 1)$, then $\tilde{d}_T(\sigma, \tau) = g(d_T(\sigma, \tau)) = \liminf_j \frac{1}{j+1} \sum_{i=0}^{j} d(\sigma_j, \tau_j)$ for traces of equal length. This distance has been studied *e.g.* in [17, 18, 24, 50]; we show below how it, in the framework of the present paper, gives a limit-average specification theory.

Let us give some intuition on why it is quite natural to use $\mathbb{L} = (\mathbb{R}_{\geq 0} \cup \{\infty\})^{\mathbb{N}}$ for limit-average distance, and why the simple $\mathbb{L} = \mathbb{R}_{\geq 0} \cup \{\infty\}$ does not work in this case. Essentially, when we move along the traces σ and τ to compute there distance, we have to sum up the individual distances $d(\sigma_i, \tau_i)$. But the contribution of $\sum_{i=0}^{j} d(\sigma_j, \tau_j)$ is divided by $j+1$ to compute the end result, hence we have to keep track of where in the traces we currently are for computing distance recursively. This is naturally achieved by remembering and increasing the index j during the recursion, which we do using $M = \mathbb{N}$ and thus $\mathbb{L} = (\mathbb{R}_{\geq 0} \cup \{\infty\})^{\mathbb{N}}$.

Example 4 Examples 1 to 3 above are in a sense agnostic to the precise structure of implementation and specification labels. Indeed, the definitions only use the label distance $d : \mathsf{Imp} \times \mathsf{Imp} \to \mathbb{R}_{\geq 0} \cup \{\infty\}$, hence Imp (and Spec) can be any set. In particular, the theory put forward here (and also its specialization in [4]) works equally well in a *multi-weighted* setting as *e.g.* in [25], where $\mathsf{Imp} = \mathbb{Z}^k$, $\mathsf{Spec} = \mathbb{I}^k$ for some $k \in \mathbb{N}$.

Example 5 With the same instantiations of Imp and Spec as in Examples 1 to 3, we can introduce a distance which, instead of accumulating individual label differences, measures the long-run difference between *accumulated labels*. This *maximum-lead* distance is especially useful for real-time systems and has been considered in [34,46]. Unlike Examples 1 to 3, it does not use the distance d on implementation labels in the definition of the trace distance; rather it accumulates the labels itself before taking the distance.

Let $\mathbb{L} = (\mathbb{R}_{\geq 0} \cup \{\infty\})^{\mathbb{R}}$ and define $F : \mathsf{Imp} \times \mathsf{Imp} \times \mathbb{L} \to \mathbb{L}$ by

$$F((a, x), (a', x'), \alpha)(\delta) = \begin{cases} [c]\infty & \text{if } a \neq a', \\ \max(|\delta + x - x'|, \alpha(\delta + x - x')) & \text{if } a = a'. \end{cases}$$

Define $g : \mathbb{L} \to \mathbb{R}_{\geq 0} \cup \{\infty\}$ by $g(\alpha) = \alpha(0)$; the maximum-lead distance assuming the lead is zero. It can then be shown that for implementation traces $\sigma = ((a_0, x_0), (a_1, x_1), \dots)$, $\tau = ((a_0, y_0), (a_1, y_1), \dots)$,

$$\tilde{d}_T(\sigma, \tau) = g(d_T(\sigma, \tau)) = \sup_m \Big| \sum_{i=0}^{m} x_i - \sum_{i=0}^{m} y_i \Big|$$

is precisely the maximum-lead distance of [29,34].

We note that, like for limit-average distance, the simple lattice $\mathbb{L} = \mathbb{R}_{\geq 0} \cup \{\infty\}$ does not work for a recursive characterization of maximum-lead distance. This is due to the fact that during the computation of the distance from σ to τ, we have to keep track of the *lead* δ which we have accumulated until now, *i.e.* how much σ is ahead of τ; this is precisely what we achieve by using $M = \mathbb{R}$ and thus $\mathbb{L} = (\mathbb{R}_{\geq 0} \cup \{\infty\})^{\mathbb{R}}$. We will come back to this example in Section 7 in the context of modal event-clock specifications and their robust semantics.

Example 6 Specification labels different from the ones above can *e.g.* be *clock constraints*, or *zones* [2]. For a finite set Σ, let $\mathsf{Spec} = \Phi(\Sigma)$ be the set of closed clock constraints over Σ given by

$$\Phi(\Sigma) \ni \phi ::= a \leq k \mid a \geq k \mid \phi_1 \wedge \phi_2 \qquad (a \in \Sigma, k \in \mathbb{N}, \phi_1, \phi_2 \in \Phi(\Sigma)).$$

Clock constraints have a natural partial order given by $\phi \sqsubseteq_{\mathsf{Spec}} \phi'$ iff $\phi \implies \phi'$. Implementation labels are then clock constraints which impose a precise value for each $a \in \Sigma$, which can be seen as functions $u : \Sigma \to \mathbb{N}$. The natural distance between such *discrete clock valuations* is $d(u, u') = \max_{a \in \Sigma} |u(a) - u'(a)|$, and on top of this, any interesting trace distance can be imposed using our framework.

2.5 Structured Modal Transition Systems

Definition 1 A *structured modal transition system* (SMTS) is a tuple $(S, s_0, \dashrightarrow_S, \longrightarrow_S)$ consisting of a set S of states, an initial state $s_0 \in S$, and *must* and *may* transitions $\longrightarrow_S, \dashrightarrow_S \subseteq S \times \mathsf{Spec} \times S$ for which it holds that for all $s \xrightarrow{k}_S s'$ there is $s \overset{\ell}{\dashrightarrow}_S s'$ with $k \sqsubseteq_{\mathsf{Spec}} \ell$.

The last condition is one of *consistency*: everything which is required, is also allowed. If no confusion can arise, we will omit the subscripts S on the *must* and *may* transitions; we will also sometimes identify an SMTS $(S, s_0, \dashrightarrow_S, \longrightarrow_S)$ with its state set S.

Intuitively, a *may* transition $s \overset{k}{\dashrightarrow} s'$ specifies that an implementation I of S is *permitted* to have a corresponding transition $i \xrightarrow{m} i'$, for any $m \in [\![k]\!]$, whereas a *must* transition $s \xrightarrow{\ell} s'$ postulates that I is *required* to implement at least one corresponding transition $i \xrightarrow{n} i'$ for some $n \in [\![\ell]\!]$. We will make this precise below.

An SMTS S is an *implementation* if $\longrightarrow_S = \dashrightarrow_S \subseteq S \times \mathsf{Imp} \times S$; hence in an implementation, all optional behavior has been resolved, and all data has been refined to implementation labels.

Definition 2 An SMTS $(S, s_0, \dashrightarrow_S, \longrightarrow_S)$ is $\mathbb{L}$-*deterministic*, for a given lattice $\mathbb{L}$, if it holds for all $s \in S$, $s \overset{k_1}{\dashrightarrow} s_1$, $s \overset{k_2}{\dashrightarrow} s_2$ for which there is $k \in \mathsf{Spec}$ with $d(k, k_1) \neq \top_{\mathbb{L}}$ and $d(k, k_2) \neq \top_{\mathbb{L}}$ that $k_1 = k_2$ and $s_1 = s_2$.

Note that for the Boolean label distance given by $d(k, k') = \bot_{\mathbb{L}}$ if $k = k'$ and $\top_{\mathbb{L}}$ otherwise, the above definition reduces to the property that if $k_1 = k_2$, then also $s_1 = s_2$, hence $\mathbb{L}$-determinism is a generalization of usual determinism. In our quantitative case, we need to be more restrictive: not only do we not allow distinct transitions from s with the same label, but we forbid distinct transitions with labels which have a common quantitative refinement. Despite of this, we will generally omit the $\mathbb{L}$ and say deterministic instead of $\mathbb{L}$-deterministic.

Examples 1–3 (contd) For the label distance $d((a, x), (a', x')) = |x - x'|$ if $a = a'$ and ∞ otherwise of Examples 1 to 3 and 5, the above condition that there exist $k \in \mathsf{Spec}$ with $d(k, k_1) \neq \top_{\mathbb{L}}$ and $d(k, k_2) \neq \top_{\mathbb{L}}$ is equivalent, with $k_1 = (a_1, I_1)$ and $k_2 = (a_2, I_2)$, to saying that $a_1 = a_2$, hence our notion of determinism agrees with the one of [4].

A *modal refinement* of SMTS S, T is a relation $R \subseteq S \times T$ such that for any $(s, t) \in R$,

– whenever $s \overset{k}{\dashrightarrow}_S s'$, then also $t \overset{\ell}{\dashrightarrow}_T t'$ for some $k \sqsubseteq_{\mathsf{Spec}} \ell$ and $(s', t') \in R$,
– whenever $t \xrightarrow{\ell}_T t'$, then also $s \xrightarrow{k}_S s'$ for some $k \sqsubseteq_{\mathsf{Spec}} \ell$ and $(s', t') \in R$.

Thus any behavior which is permitted in S is also permitted in T, and any behavior required in T is also required in S. We write $S \leq_m T$ if there is a modal refinement $R \subseteq S \times T$ with $(s_0, t_0) \in R$.

The *implementation semantics* of a SMTS S is the set $[\![S]\!] = \{I \leq_m S \mid I \text{ is an implementation}\}$, and we write $S \leq_t T$ if $[\![S]\!] \subseteq [\![T]\!]$, saying that S *thoroughly refines* T. It follows by reflexivity of $\leq_m$ that $S \leq_m T$ implies $S \leq_t T$, hence modal refinement is a *syntactic over-approximation* of thorough refinement.

It can be shown for standard modal transition systems that $S \leq_t T$ does not imply $S \leq_m T$, unless T is deterministic, see [11]. We shall provide a quantitative generalization of this result in Theorem 1 below. Also, modal refinement for MTS can be decided in polynomial time, whereas deciding thorough refinement is EXPTIME-complete [11]. Essentially, thorough refinement—inclusion of implementation sets—is the relation one really is interested in, but modal refinement provides a useful over-approximation.

3 Refinement Distances

We define two distances between SMTS, one at the syntactic and one at the semantic level.

3.1 Modal and thorough refinement distance

Definition 3 The *modal refinement distance* $d_m : S \times T \to \mathbb{L}$ between the states of SMTS S, T is defined to be the least fixed point to the equations

$$d_m(s,t) = \max \begin{cases} \sup\limits_{s \overset{k}{\dashrightarrow}_S s'} \inf\limits_{t \overset{\ell}{\dashrightarrow}_T t'} F(k, \ell, d_m(s',t')), \\ \sup\limits_{t \overset{\ell}{\longrightarrow}_T t'} \inf\limits_{s \overset{k}{\longrightarrow}_S s'} F(k, \ell, d_m(s',t')). \end{cases}$$

We let $d_m(S,T) = d_m(s_0, t_0)$, and we write $S \leq_m^\alpha T$ if $d_m(S,T) \sqsubseteq_{\mathbb{L}} \alpha$.

Lemma 1 *The modal refinement distance is well-defined and a hemimetric. Also, $S \leq_m T$ implies $d_m(S,T) = \bot_{\mathbb{L}}$.*

Proof Let $I : \mathbb{L}^{S\times T} \to \mathbb{L}^{S \times T}$ be the endofunction defined by

$$I(h)(s,t) = \max \begin{cases} \sup\limits_{s \overset{k}{\dashrightarrow}_S s'} \inf\limits_{t \overset{\ell}{\dashrightarrow}_T t'} F(k, \ell, h(s',t')), \\ \sup\limits_{t \overset{\ell}{\longrightarrow}_T t'} \inf\limits_{s \overset{k}{\longrightarrow}_S s'} F(k, \ell, h(s',t')). \end{cases}$$

The lattice $\mathbb{L}^{S\times T}$ is complete because $\mathbb{L}$ is, and I is monotone because $F(k, \ell, \cdot) : \mathbb{L} \to \mathbb{L}$ is. By an application of Tarski's fixed point theorem [45], I has a unique least fixed point which hence defines d_m.

The property that $d_m(S,S) = 0$ for all SMTS S is clear, and the triangle inequality $d_m(S,T) \oplus_{\mathbb{L}} d_m(T,U) \sqsupseteq_{\mathbb{L}} d_m(S,U)$ can be shown inductively.

To show the last claim, assume $s \leq_m t$. Then for any $s \overset{k}{\dashrightarrow} s'$ there is $t \overset{\ell}{\dashrightarrow} t'$ for which $k \sqsubseteq_{\mathsf{Spec}} \ell$, hence $F(k, \ell, \alpha) = \alpha$ for all $\alpha \in \mathbb{L}$ by Axiom (4′). Similarly for *must* transitions, so the fixed point equations simplify to

$$d_m(s,t) = \max \Big(\sup_{s \dashrightarrow s'} \inf_{t \dashrightarrow t'} d_m(s',t'), \sup_{t \longrightarrow t'} \inf_{s \longrightarrow s'} d_m(s',t') \Big),$$

the least fixed point of which is $d_m(s,t) = \bot_{\mathbb{L}}$. □

One can also define a *linear distance* between states, analogous to trace inclusion. This is given by

$$d_T(s,t) = \max\Big(\sup_{\sigma\in \mathrm{Tr}(s)} \inf_{\tau\in \mathrm{Tr}(t)} d_T(\sigma,\tau), \sup_{\tau\in \mathrm{Tr}(t)} \inf_{\sigma\in \mathrm{Tr}(s)} d_T(\sigma,\tau)\Big),$$

where $\mathrm{Tr}(s)$ denotes the set of (*may* or *must*) traces emanating from s. It can then be shown [27, 29] that $d_T(s,t) \sqsubseteq_{\mathbb{L}} d_m(s,t)$ for all $s,t\in S$.

Definition 4 The *thorough refinement distance* from an SMTS S to an SMTS T is

$$d_t(S,T) = \sup_{I\in[\![S]\!]} \inf_{J\in[\![T]\!]} d_m(I,J),$$

and we write $S \le_t^\alpha T$ if $d_t(S,T)\sqsubseteq_{\mathbb{L}} \alpha$.

Lemma 2 *The thorough refinement distance is a hemimetric, and* $S\le_t T$ *implies* $d_t(S,T) = \bot_{\mathbb{L}}$.

Proof The equality $d_t(S,S) = \bot_{\mathbb{L}}$ is clear, and the triangle inequality $d_t(S,T) + d_t(T,U) \ge d_t(S,U)$ follows like in the proof of [1, Lemma 3.72]. If $S\le_t T$, then $[\![S]\!] \subseteq [\![T]\!]$ implies $d_t(S,T) = \bot_{\mathbb{L}}$. □

3.2 Refinement families

As is the case for ordinary (bi)simulation [41], there is a dual *relational* notion of refinement distance which is useful *e.g.* in proofs. Before we can introduce this, we need a notion similar to the *finite branching* assumption one needs to make for the case of bisimulation, *cf.* [38].

Definition 5 A SMTS S is said to be *compactly branching* if the sets $\{(s',k)\mid s \overset{k}{\dashrightarrow} s'\}, \{(s',k)\mid s \overset{k}{\longrightarrow} s'\}\subseteq S\times \mathsf{Spec}$ are compact under the symmetrized product distance $\bar d_m\times \bar d$ for every $s\in S$.

Recall that the pseudometric $\bar d_m\times\bar d$ is given by $\bar d_m\times\bar d((s,k),(s',k')) = \bar d_m(s,s') + \bar d(k,k') = \max(d_m(s,s'), d_m(s',s)) + \max(d(k,k'), d(k',k))$. We will need compactness of the sets $\{(s',k)\mid s \overset{k}{\dashrightarrow} s'\}, \{(s',k)\mid s \overset{k}{\longrightarrow} s'\}\subseteq S\times \mathsf{Spec}$ for the property that continuous functions on defined on them attain their infimum and supremum, see Lemma 3 and its proof below.

The notion of compact branching was first introduced, for a formalism of *metric transition systems*, in [47]. It is a natural generalization of finite branching to a distance setting; we shall henceforth assume all our SMTS to be compactly branching.

Definition 6 A *modal refinement family* from S to T, for SMTS S, T, is an $\mathbb{L}$-indexed family of relations $R = \{R_\alpha\subseteq S\times T\mid \alpha\in\mathbb{L}\}$ with the property that for all $\alpha\in\mathbb{L}$ and all $(s,t)\in R_\alpha$,

- whenever $s \overset{k}{\dashrightarrow}_S s'$, then there is $\beta\in\mathbb{L}$ and $(s',t')\in R_\beta$ for which $t \overset{\ell}{\dashrightarrow}_T t'$ and $F(k,\ell,\beta)\sqsubseteq_{\mathbb{L}}\alpha$,
- whenever $t \overset{\ell}{\longrightarrow}_T t'$, then there is $\beta\in\mathbb{L}$ and $(s',t')\in R_\beta$ for which $s \overset{k}{\longrightarrow}_S s'$ and $F(k,\ell,\beta)\sqsubseteq_{\mathbb{L}}\alpha$.

Additionally we assume R to be *closed* in the sense that for all $s \in S$, $t \in T$, $(s,t) \in R_{\inf\{\alpha \mid (s,t) \in R_\alpha\}}$.

Lemma 3 *For all SMTS S, T and $\alpha \in \mathbb{L}$, $S \le_m^\alpha T$ if and only if there is a modal refinement family R from S to T with $(s_0,t_0) \in R_\alpha$.*

We say that a modal refinement family as in the lemma *witnesses* $S \le_m^\alpha T$; this is of course the same as saying that it witnesses $d_m(S,T) \sqsubseteq_{\mathbb{L}} \alpha$, which we sometimes shorten to say that it witnesses $d_m(S,T)$.

Proof Assume first that $S \le_m^\alpha T$, thus we know that $d_m(S,T) \sqsubseteq_{\mathbb{L}} \alpha$. We have to show that there is a modal refinement family R from S to T with $(s_0,t_0) \in R_\alpha$. Define a family $R = \{R_{\alpha'} \subseteq S \times T \mid \alpha' \in \mathbb{L}\}$ by

$$R_{\alpha'} = \{(s,t) \mid d_m(s,t) \sqsubseteq_{\mathbb{L}} \alpha'\}$$

for every $\alpha' \in \mathbb{L}$; note that R is closed in the sense above. Now let $\beta \in \mathbb{L}$ and $(s,t) \in R_\beta$.

– Assume $s \overset{k}{\dashrightarrow} s'$. By $d_m(s,t) \sqsubseteq_{\mathbb{L}} \beta$ and the definition of $d_m(s,t)$ it follows that $\inf_{t \overset{\ell}{\dashrightarrow} t'} F(k,\ell,d_m(s',t')) \sqsubseteq_{\mathbb{L}} \beta$. As T is compactly branching and F continuous, the set $\{F(k,\ell,d_m(s',t')) \mid t \overset{\ell}{\dashrightarrow} t'\}$ is compact, hence there exists a transition $t \overset{\ell}{\dashrightarrow} t'$ such that $F(k,\ell,d_m(s',t')) \sqsubseteq_{\mathbb{L}} \beta$.
– Assume $t \overset{\ell}{\longrightarrow} t'$. By $d_m(s,t) \sqsubseteq_{\mathbb{L}} \beta$ and the definition of $d_m(s,t)$ it follows that $\inf_{s \overset{k}{\longrightarrow} s'} F(k,\ell,d_m(s',t')) \sqsubseteq_{\mathbb{L}} \beta$. Again $\{F(k,\ell,d_m(s',t')) \mid s \overset{k}{\longrightarrow} s'\}$ is a compact set, whence there exists a transition $s \overset{k}{\longrightarrow} s'$ such that $F(k,\ell,d_m(s',t')) \sqsubseteq_{\mathbb{L}} \beta$.

For the other direction, assume a refinement family R from S to T with $(s_0,t_0) \in R_\alpha$. Define $h : S \times T \to \mathbb{L}$ by $h(s,t) = \inf\{\alpha \mid (s,t) \in R_\alpha\}$. Then $(s,t) \in R_\beta$ implies that $h(s,t) \sqsubseteq_{\mathbb{L}} \beta$. Let $s \in S$ and $t \in T$, then $(s,t) \in R_{h(s,t)}$ because R is closed, hence for all $s \overset{k}{\dashrightarrow} s'$ there is $t \overset{\ell}{\dashrightarrow} t'$ and $\alpha' \in \mathbb{L}$ for which $F(k,\ell,\alpha') \sqsubseteq_{\mathbb{L}} h(s,t)$ and $(s',t') \in R_{\alpha'}$, implying $h(s',t') \sqsubseteq_{\mathbb{L}} \alpha'$ and hence $F(k,\ell,h(s',t')) \sqsubseteq_{\mathbb{L}} h(s,t)$ by monotonicity and transitivity. Similarly, for all $t \overset{\ell}{\longrightarrow} t'$ there is $s \overset{k}{\longrightarrow} s'$ with $F(k,\ell,h(s',t')) \sqsubseteq_{\mathbb{L}} h(s,t)$. Hence h is a pre-fixed point for the equations in the definition of d_m, implying that $d_m(s,t) \sqsubseteq_{\mathbb{L}} h(s,t)$ for all $s \in S$, $t \in T$, thus especially $d_m(s_0,t_0) \sqsubseteq_{\mathbb{L}} \alpha$, because $(s_0,t_0) \in R_\alpha$ implies $h(s_0,t_0) \sqsubseteq_{\mathbb{L}} \alpha$ and $d_m(s_0,t_0) \sqsubseteq_{\mathbb{L}} h(s_0,t_0)$. □

3.3 Modal distance bounds thorough distance

The next theorem shows that the modal refinement distance overapproximates the thorough one, and that it is exact for deterministic SMTS. This is similar to the situation for standard modal transition systems [36]; note [36] that deterministic specifications generally suffice for applications.

Theorem 1 *For all SMTS S, T, $d_t(S,T) \sqsubseteq_{\mathbb{L}} d_m(S,T)$. If T is deterministic, then $d_t(S,T) = d_m(S,T)$.*

The counterexample for the Boolean version of this result given in [11] also works in our setting, to show that there exist (necessarily nondeterministic) SMTS S, T for which $d_t(S,T)=\bot_{\mathbb{L}}$, but $d_m(S,T)=\top_{\mathbb{L}}$.

Proof If $d_m(S,T)=\top_{\mathbb{L}}$, we have nothing to prove. Otherwise, let $R=\{R_\alpha\subseteq S\times T\mid \alpha\in\mathbb{L}\}$ be a modal refinement family which witnesses $d_m(S,T)$, then $(s_0,t_0)\in R_{d_m(S,T)}$. Let $I\in[\![S]\!]$; we will expose $J\in[\![T]\!]$ for which $d_m(I,J)\sqsubseteq_{\mathbb{L}} d_m(S,T)$.

Let $R^1\subseteq I\times S$ be a witness for $I\le_m S$, define $R'_\alpha=R^1\circ R_\alpha\subseteq I\times T$ for all $\alpha\in\mathbb{L}$, and let $R'=\{R'_\alpha\mid\alpha\in\mathbb{L}\}$. We let the states of J be $J=T$, with $j_0=t_0$, and define $\dashrightarrow_J=\longrightarrow_J$ as follows:

For any $i\xrightarrow{m}_I i'$ and any $t\in T$ for which $(i,t)\in R'_\alpha\in R'$ for some $\alpha\in\mathbb{L}$, $\alpha\ne\top_{\mathbb{L}}$, we have $t\overset{\ell}{\dashrightarrow}_T t'$ with $(i',t')\in R'_\beta\in R'$ for some $\beta\in\mathbb{L}$ with $F(m,\ell,\beta)\sqsubseteq_{\mathbb{L}}\alpha$. As $[\![\ell]\!]$ is closed under F, there is $n\in[\![\ell]\!]$ for which $F(m,n,\beta)=F(m,\ell,\beta)$, and we add a transition $t\xrightarrow{n}_J t'$ to J.

Similarly, for any $t\xrightarrow{\ell}_T t'$ and any $i\in I$ for which $(i,t)\in R'_\alpha\in R'$ for some $\alpha\in\mathbb{L}$, $\alpha\ne\top_{\mathbb{L}}$, we have $i\xrightarrow{m}_I i'$ with $(i',t')\in R'_\beta$ for some $\beta\in\mathbb{L}$ with $F(m,\ell,\beta)\sqsubseteq_{\mathbb{L}}\alpha$. Using again closedness of $[\![\ell]\!]$, we find $n\in[\![\ell]\!]$ for which $F(m,n,\beta)=F(m,\ell,\beta)$ and add a transition $t\xrightarrow{n}_J t'$ to J.

We show that the identity relation $\{(t,t)\mid t\in T\}\subseteq J\times T$ witnesses $J\le_m T$. Let first $t\xrightarrow{n}_J t'$; we must have used one of the two constructions above for creating this transition. In the first case, there is $t\overset{\ell}{\dashrightarrow}_T t'$ with $n\in[\![\ell]\!]$, and in the second case, there is $t\xrightarrow{\ell}_T t'$, hence also $t\overset{\ell'}{\dashrightarrow}_T t'$ with $\ell\sqsubseteq_{\mathsf{Spec}}\ell'$, thus $n\in[\![\ell]\!]\subseteq[\![\ell']\!]$. Now let $t\xrightarrow{\ell}_T t'$, then the second construction above has introduced $t\xrightarrow{n}_J t'$ with $n\in[\![\ell]\!]$.

To finish the proof, we show that the family R' is a witness for $d_m(I,J)\sqsubseteq_{\mathbb{L}} d_m(S,T)$. First, $(i_0,s_0)\in R^1$ and $(s_0,t_0)\in R_{d_m(S,T)}$ imply $(i_0,t_0)\in R'_{d_m(S,T)}$. Let $(i,t)\in R'_\alpha\in R'$ for some $\alpha\in\mathbb{L}$, $\alpha\ne\top_{\mathbb{L}}$, and assume first $i\xrightarrow{m}_I i'$. Then $t\overset{\ell}{\dashrightarrow}_T t'$ and $t\xrightarrow{n}_J t'$ by the first part of our above construction, and $(i',t')\in R'_\beta$ with $F(m,n,\beta)\sqsubseteq_{\mathbb{L}} F(m,\ell,\beta)\sqsubseteq_{\mathbb{L}}\alpha$. For the converse, and transition $t\xrightarrow{n}_J t'$ must have been introduced above, and in both cases, $i\xrightarrow{m}_I i'$ with $(i',t')\in R'_\beta$ and $F(m,n,\beta)\sqsubseteq_{\mathbb{L}} F(m,\ell,\beta)\sqsubseteq_{\mathbb{L}}\alpha$.

Now to the proof of the second assertion of the theorem. If $d_t(S,T)=\top_{\mathbb{L}}$, we are done. Otherwise we inductively construct a relation family $R=\{R_\alpha\subseteq S\times T\mid\alpha\in\mathbb{L}\}$ which satisfies $d_t((s,S),(t,T))\sqsubseteq\alpha$ for any $(s,t)\in R_\alpha$, as follows: Begin by letting $R_\alpha=\{(s_0,t_0)\}$ for all $\alpha\sqsupseteq_{\mathbb{L}} d_t(S,T)$, and let now $(s,t)\in R_\alpha$ with $d_t((s,S),(t,T))\sqsubseteq\alpha\ne\top_{\mathbb{L}}$.

Let $s\overset{k}{\dashrightarrow}_S s'$ and $t\overset{\ell}{\dashrightarrow}_T t'$ such that $d(k,\ell)\ne\top_{\mathbb{L}}$. Let $(i',I')\in[\![(s',S)]\!]$ and $m\in[\![k]\!]$, then there is $(i,I)\in[\![(s,S)]\!]$ for which $i\xrightarrow{m}_I i''$ and $(i'',I)\le_m (i',I')$. By the triangle inequality we have $d_t((i,I),(t,T))\sqsubseteq_{\mathbb{L}} d_t((i,I),(s,S))\oplus_{\mathbb{L}} d_t((s,S),(t,T))\sqsubseteq_{\mathbb{L}}\alpha$, hence there is $t\overset{\ell'}{\dashrightarrow} t''$ for which $d(m,\ell')\sqsubseteq_{\mathbb{L}}\alpha$. But we also have $d(m,\ell)\sqsubseteq_{\mathbb{L}} d(m,k)\oplus_{\mathbb{L}} d(k,\ell)=d(k,\ell)\ne\top_{\mathbb{L}}$, so by determinism of T it follows that $\ell=\ell'$ and $t'=t''$.

As $m\in[\![k]\!]$ was chosen arbitrarily above, we have $d(m,\ell)\sqsubseteq_{\mathbb{L}}\alpha$ for all $m\in[\![k]\!]$, hence $d(k,\ell)=F(k,\ell,\bot_{\mathbb{L}})\sqsubseteq\alpha$. Let $B=\{\beta'\in\mathbb{L}\mid F(k,\ell,\beta')\sqsubseteq_{\mathbb{L}}\alpha\}$ and $\beta=\sup B$, then $F(k,\ell,\beta)\sqsubseteq_{\mathbb{L}}\alpha$ as $\bot_{\mathbb{L}}\in S$. Add (s',t') to R_γ for all $\gamma\sqsupseteq_{\mathbb{L}}\beta$.

We miss to show that $d_t((s',S),(t',T)) \sqsubseteq_{\mathbb{L}} \beta$. By $d_t((s,S),(t,T)) \sqsubseteq_{\mathbb{L}} \alpha$ we must have $(j,J) \in [\![(t,T)]\!]$, $j \xrightarrow{n}_J j'$, and $\beta' \in \mathbb{L}$ for which $d_m((i',I'),(j',J)) \sqsubseteq_{\mathbb{L}} \beta'$ and $F(m,n,\beta') \sqsubseteq_{\mathbb{L}} \alpha$. Then $F(k,\ell,\beta') = F(m,\ell,\beta') \sqsubseteq_{\mathbb{L}} F(m,n,\beta') \sqsubseteq_{\mathbb{L}} \alpha$, hence $\beta' \in B$, implying that $d_t((s',S),(t',T)) \sqsubseteq_{\mathbb{L}} \beta' \sqsubseteq_{\mathbb{L}} \beta$.

We show that R is a refinement family which witnesses $d_m(S,T)$. Let $(s,t) \in R_\alpha \in R$ for some $\alpha \in \mathbb{L}$ and assume $s \overset{k}{\dashrightarrow}_S s'$. Let $m \in [\![k]\!]$, then there is $(i,I) \in [\![(s,S)]\!]$ with $i \xrightarrow{m}_I i'$. As $d_t((i,I),(t,T)) \sqsubseteq_{\mathbb{L}} \alpha$, this implies that there is $t \overset{\ell}{\dashrightarrow}_T t'$ with $d(m,\ell) \sqsubseteq_{\mathbb{L}} \alpha$. Also for any other $m' \in [\![k]\!]$ we have $t \overset{\ell'}{\dashrightarrow}_T t''$ with $d(m,\ell') \sqsubseteq_{\mathbb{L}} \alpha$, hence $\ell = \ell'$ and $t' = t''$ by determinism. As m was chosen arbitrarily, we have $d(m,\ell) \sqsubseteq \alpha$ for all $m \in [\![k]\!]$, hence $d(k,\ell) = F(k,\ell,\bot_{\mathbb{L}}) \sqsubseteq \alpha$. By construction of R, $(s',t') \in R_\beta$ for $\beta = \sup\{\beta' \in \mathbb{L} \mid F(k,\ell,\beta') \sqsubseteq_{\mathbb{L}} \alpha\}$.

Now assume $t \xrightarrow{\ell}_T t'$. Let $(i,I) \in [\![(s,S)]\!]$, then we have $(j,J) \in [\![(t,T)]\!]$ with $d_m((i,I),(j,J)) \sqsubseteq_{\mathbb{L}} \alpha$. We must have $j \xrightarrow{n}_J j'$ with $n \in [\![\ell]\!]$, hence there are $i \xrightarrow{m}_I i'$ and $\beta' \in \mathbb{L}$ with $d_m((i',I),(j',J)) \sqsubseteq_{\mathbb{L}} \beta'$ and $F(m,n,\beta') \sqsubseteq_{\mathbb{L}} \alpha$.

The above considerations hold for all $(i,I) \in [\![(s,S)]\!]$, hence there is $k \in \mathbb{L}$ with $m \in [\![k]\!]$, $s \xrightarrow{k}_S s'$, and $F(k,\ell,\beta') = F(m,\ell,\beta')$. But then $F(k,\ell,\beta') \sqsubseteq_{\mathbb{L}} F(m,n,\beta') \sqsubseteq_{\mathbb{L}} \alpha$, hence by construction of R, $(s',t') \in R_\beta$ for $\beta = \sup\{\beta' \in \mathbb{L} \mid F(k,\ell,\beta') \sqsubseteq_{\mathbb{L}} \alpha\}$. $\square$

3.4 Quantitative relaxation

In a quantitative framework, it can be useful to be able to *relax* and *strengthen* specifications during the development process. Which precise relaxations and strengthenings one wishes to apply will depend on the actual application, but we can here show three general relaxations which differ from each other in the *level* of the theory at which they are applied. For $\alpha \in \mathbb{L}$ and SMTS S, T,

- T is an α-*widening* of S if there is a relation $R \subseteq S \times T$ for which $(s_0,t_0) \in R$ and such that for all $(s,t) \in R$, $s \overset{k}{\dashrightarrow}_S s'$ if and only if $t \overset{\ell}{\dashrightarrow}_T t'$, and $s \xrightarrow{k}_S s'$ if and only if $t \xrightarrow{\ell}_T t'$, for $k \sqsubseteq_{\mathsf{Spec}} \ell$, $d(\ell,k) \sqsubseteq_{\mathbb{L}} \alpha$, and $(s',t') \in R$;
- T is an α-*relaxation* of S if $S \leq_m T$ and $T \leq_m^\alpha S$;
- the α-*extended implementation semantics* of S is

$$[\![S]\!]^{+\alpha} = \{I \leq_m^\alpha S \mid I \text{ implementation}\}.$$

Hence α-widening is an entirely *syntactic* notion: up to unweighted bisimulation, T is the same as S, but transition labels in T can be α "wider" than in S (hence also $S \leq_m T$). The second notion, α-relaxation, works at the level of semantics of specifications, whereas the last notion is at implementation level. A priori, there is no relation between the syntactic and semantic notions, even though one can be established in some special cases.

Examples 1–3 (contd) For the accumulated distance with discounting factor λ, any α-widening is also a $(1-\lambda)^{-1}\alpha$-relaxation. This is due to the fact that for traces $\sigma,\tau \in \mathsf{Spec}^\infty$ with $d(\sigma_j,\tau_j) \leq \alpha$ for all j, we have $\sum_j \lambda^j d(\sigma_j,\tau_j) \leq \sum_j \lambda^j \alpha \leq (1-\lambda)^{-1}\alpha$ by convergence of the geometric series, *cf.* [4].

For the point-wise distance, it is easy to see that any α-widening is also an α-relaxation, and the same holds for the limit-average distance:

$$\liminf_j \tfrac{1}{j+1} \sum_{i=0}^{j} d(\sigma_i, \tau_i) \le \liminf_j \tfrac{1}{j+1} j\alpha = \alpha$$

Example 5 (contd) For the maximum-lead distance on the other hand, it is easy to expose cases of α-widenings which are *not* β-relaxations for any β. One example consists of two one-state SMTS S, T with loops $s_0 \xrightarrow{a,1} s_0$ and $t_0 \xrightarrow{a,[0,2]} t_0$; then T is an α-widening of S for $\alpha(\delta) = |\delta + 1|$, but $d_m(T, S) = \top_{\mathbb{L}}$.

Proposition 1 *If T is an α-relaxation of S, then $[\![T]\!] \subseteq [\![S]\!]^{+\alpha}$.*

It can be shown for special cases that the inclusion in the proposition is strict [4]; for its proof one only needs the fact that $d_m(I, S) \sqsubseteq_{\mathbb{L}} d_m(I, T) \oplus d_m(T, S) \sqsubseteq_{\mathbb{L}} \alpha$ for all $I \in [\![T]\!]$.

Also of interest is the relation between relaxations of different specifications. An easy application of the triangle inequality for d_m shows that the distance between relaxations is bounded by the sum of the relaxation constants and the unrelaxed systems' distances:

Proposition 2 *Let T be an α-relaxation of S and T' an α'-relaxation of S'. Then $d_m(T, T') \sqsubseteq_{\mathbb{L}} \alpha \oplus_{\mathbb{L}} d_m(S, S')$ and $d_m(T', T) \sqsubseteq_{\mathbb{L}} \alpha' \oplus_{\mathbb{L}} d_m(S', S)$.* $\square$

4 Structural Composition and Quotient

We now introduce the different operations on SMTS which make up a specification theory. Firstly, we are interested in composing specifications S, S' into a specification $S \| S'$ by synchronizing on shared actions. Secondly, we need a quotient operator which solves equations of the form $S \| X \equiv T$, that is, the quotient synthesizes the most general specification $T \oslash S$ which describes all SMTS X satisfying the above equation.

4.1 Structural composition

To structurally compose SMTS, we assume given a generic partial *label composition* operator $\oplus : \mathsf{Spec} \times \mathsf{Spec} \hookrightarrow \mathsf{Spec}$ which specifies which labels can synchronize, *cf.* [49]. We will need to assume the following property:

– for all $\ell, \ell' \in \mathsf{Spec}$, $(\exists k \in \mathsf{Spec} : d(k, \ell) \ne \top_{\mathbb{L}}, d(k, \ell') \ne \top_{\mathbb{L}}) \iff (\exists m \in \mathsf{Spec} : \ell \oplus m, \ell' \oplus m$ are defined).

This operator permits to compose labels at transitions which are executed in parallel; the property required relates composability to distances in such a way that two labels have a common quantitative refinement if and only if they have a common synchronization. This is quite natural and holds for all our examples, and is needed to relate determinism to composition in the proof of Theorem 3 below.

Additionally, we must assume that there exists a function $P : \mathbb{L} \times \mathbb{L} \to \mathbb{L}$ which allows us to infer bounds on distances on synchronized labels. We assume that P is monotone in both coordinates, has $P(\bot_{\mathbb{L}}, \bot_{\mathbb{L}}) = \bot_{\mathbb{L}}$, $P(\alpha, \top_{\mathbb{L}}) = P(\top_{\mathbb{L}}, \alpha) = \top_{\mathbb{L}}$ for all $\alpha \in \mathbb{L}$, and that

$$F(k \oplus k', \ell \oplus \ell', P(\alpha, \alpha')) \sqsubseteq_{\mathbb{L}} P(F(k, \ell, \alpha), F(k', \ell', \alpha'))$$

for all $k, \ell, k', \ell' \in \mathsf{Spec}$ and $\alpha, \alpha' \in \mathbb{L}$ for which $k \oplus k'$ and $\ell \oplus \ell'$ are defined. Hence $d(k \oplus k', \ell \oplus \ell') \sqsubseteq_{\mathbb{L}} P(d(k, \ell), d(k', \ell'))$ for all such $k, \ell, k', \ell' \in \mathsf{Spec}$, thus P indeed bounds distances of synchronized labels.

Intuitively, P gives us a *uniform bound* on label composition: distances between composed labels can be bounded above using P and the individual labels' distances.

Definition 7 The *structural composition* of two SMTS S and T is the SMTS $S \| T = (S \times T, (s_0, t_0), \dashrightarrow_{S\|T}, \longrightarrow_{S\|T})$ with transitions defined as follows:

$$\frac{s \overset{k}{\dashrightarrow}_S s' \quad t \overset{\ell}{\dashrightarrow}_T t' \quad k \oplus \ell \text{ defined}}{(s,t) \overset{k \oplus \ell}{\dashrightarrow}_{S\|T} (s', t')} \qquad \frac{s \overset{k}{\longrightarrow}_S s' \quad t \overset{\ell}{\longrightarrow}_T t' \quad k \oplus \ell \text{ defined}}{(s,t) \overset{k \oplus \ell}{\longrightarrow}_{S\|T} (s', t')}$$

The next theorem shows that structural composition supports *quantitative independent implementability*: the distance between structural compositions can bounded above using P and the distances between the individual components.

Theorem 2 *For SMTS S, T, S', T', with $d_m(S\|S', T\|T') \neq \top_{\mathbb{L}}$, $d_m(S\|S', T\|T') \sqsubseteq_{\mathbb{L}} P(d_m(S,T), d_m(S',T'))$.*

Proof Let $R = \{R_\alpha \subseteq S \times T \mid \alpha \in \mathbb{L}\}$, $R' = \{R'_\alpha \subseteq S' \times T' \mid \alpha \in \mathbb{L}\}$ be witnesses for $d_m(S,T)$ and $d_m(S',T')$, respectively, and define

$$\begin{aligned} R^{\|}_\beta = \{((s,s'),(t,t')) \in S \times S' \times T \times T' \mid \\ \exists \alpha, \alpha' \in \mathbb{L} : (s,t) \in R_\alpha \in R, (s',t') \in R'_{\alpha'} \in R', P(\alpha, \alpha') \sqsubseteq_{\mathbb{L}} \beta\} \end{aligned}$$

for all $\beta \in \mathbb{L}$. We show that $R^{\|} = \{R^{\|}_\beta \mid \beta \in L\}$ is a witness for $d_m(S\|S', T\|T') \sqsubseteq_{\mathbb{L}} P(d_m(S,T), d_m(S',T'))$.

First, $((s_0, s'_0), (t_0, t'_0)) \in R^{\|}_{P(d_m(S,T), d_m(S',T'))}$. Let now $\beta \in \mathbb{L} \setminus \{\top_{\mathbb{L}}\}$ and $((s,s'),(t,t')) \in R^{\|}_\beta \in R^{\|}$, then we have $\alpha, \alpha' \in \mathbb{L} \setminus \{\top_{\mathbb{L}}\}$ with $(s,t) \in R_\alpha \in R$, $(s',t') \in R'_{\alpha'} \in R'$, and $P(\alpha, \alpha') \sqsubseteq_{\mathbb{L}} \beta$.

Let $(s,s') \overset{k \oplus k'}{\dashrightarrow}_{S\|S'} (\bar{s}, \bar{s}')$, then $s \overset{k}{\dashrightarrow}_S \bar{s}$ and $s' \overset{k'}{\dashrightarrow}_{S'} \bar{s}'$. As $(s,t) \in R_\alpha \in R$, we have $t \overset{\ell}{\dashrightarrow}_T \bar{t}$ and $\bar{\alpha} \in \mathbb{L}$ with $(\bar{s}, \bar{t}) \in R_{\bar{\alpha}} \in R$ and $F(k, \ell, \bar{\alpha}) \sqsubseteq_{\mathbb{L}} \alpha$. Similarly, $(s',t') \in R'_{\alpha'} \in R'$ implies that there is $t' \overset{\ell'}{\dashrightarrow}_{T'} \bar{t}'$ and $\bar{\alpha}' \in \mathbb{L}$ with $(\bar{s}', \bar{t}') \in R'_{\bar{\alpha}'} \in R'$ and $F(k', \ell', \bar{\alpha}') \sqsubseteq_{\mathbb{L}} \alpha'$.

Now if the composition $\ell \oplus \ell'$ is undefined, then $d_m(S\|S', T\|T') = \top_{\mathbb{L}}$. If it is defined, then we have $(t,t') \overset{\ell \oplus \ell'}{\dashrightarrow}_{T\|T'} (\bar{t}, \bar{t}')$ by definition of $S\|S'$. Also, $(\bar{t}, \bar{t}') \in R^{\|}_{P(\bar{\alpha}, \bar{\alpha}')} \in R^{\|}$ and $F(k \oplus k', \ell \oplus \ell', P(\bar{\alpha}, \bar{\alpha}')) \sqsubseteq_{\mathbb{L}} P(F(k, \ell, \bar{\alpha}), F(k', \ell', \bar{\alpha}')) \sqsubseteq_{\mathbb{L}} P(\alpha, \alpha')$.

The reverse direction, assuming a transition $(t,t') \overset{\ell \oplus \ell'}{\longrightarrow}_{T\|T'} (\bar{t}, \bar{t}')$, is similar. $\square$

Example 1 (contd) One popular label synchronization operator for the set $\mathsf{Spec} = \Sigma \times \mathbb{I}$ from our examples, also used in [4], is given by adding interval boundaries, *viz.*

$$(a, [l, r]) \oplus (a', [l', r']) = \begin{cases} (a, [l + l', r + r']) & \text{if } a = a', \\ \text{undefined} & \text{otherwise.} \end{cases}$$

It can then be shown [4] that

$$d(k \oplus k', \ell \oplus \ell') \le d(k, \ell) + d(k', \ell') \tag{2}$$

for all $k, \ell, k', \ell' \in \mathsf{Spec}$ for which $k \oplus k'$ and $\ell \oplus \ell'$ are defined.

For the accumulating distance, (2) implies that $\oplus$ is bounded above by $P(\alpha, \alpha') = \alpha + \alpha'$:

$$\begin{aligned} F(k \oplus k', \ell \oplus \ell', \alpha + \alpha') &= d(k \oplus k', \ell \oplus \ell') + \lambda(\alpha + \alpha') \\ &\le d(k, \ell) + \lambda\alpha + d(k', \ell') + \lambda\alpha' \\ &= F(k, \ell, \alpha) + F(k', \ell', \alpha') \end{aligned}$$

Theorem 2 thus specializes to [4, Thm. 5]: $\tilde{d}_m(S\|S', T\|T') \le \tilde{d}_m(S, T) + \tilde{d}_m(S', T')$ for all SMTS S, T, S', T'.

Example 2 (contd) Also for the point-wise distance, a bound is given by $P(\alpha, \alpha') = \alpha + \alpha'$:

$$\begin{aligned} F(k \oplus k', \ell \oplus \ell', \alpha + \alpha') &= \max(d(k \oplus k', \ell \oplus \ell'), \alpha + \alpha') \\ &\le \max(d(k, \ell) + d(k', \ell'), \alpha + \alpha') \\ &\le \max(d(k, \ell), \alpha) + \max(d(k', \ell'), \alpha') \\ &= F(k, \ell, \alpha) + F(k', \ell', \alpha'), \end{aligned}$$

the last inequality because of distributivity of addition over maximum. Thus also here, $\tilde{d}_m(S\|S', T\|T') \le \tilde{d}_m(S, T) + \tilde{d}_m(S', T')$ for all SMTS S, T, S', T'.

Example 3 (contd) For the limit-average distance, a similar bound $P(\alpha, \alpha') = \alpha \oplus \alpha'$ works: For all $j \in \mathbb{N}$,

$$\begin{aligned} F(k \oplus k', \ell \oplus \ell', \alpha \oplus \alpha')(j) &= \tfrac{1}{j+1} d(k \oplus k', \ell \oplus \ell') + \tfrac{j}{j+1}(\alpha(j-1) + \alpha'(j-1)) \\ &\le \tfrac{1}{j+1} d(k, \ell) + \tfrac{j}{j+1}\alpha(j-1) + \tfrac{1}{j+1} d(k', \ell') + \tfrac{j}{j+1}\alpha'(j-1) \\ &= F(k, \ell, \alpha)(j) + F(k', \ell', \alpha')(j). \end{aligned}$$

Hence also for the limit-average distance, $\tilde{d}_m(S\|S', T\|T') \le \tilde{d}_m(S, T) + \tilde{d}_m(S', T')$ for all SMTS S, T, S', T'.

In Section 7 we will introduce a different label synchronization operator with different properties.

4.2 Quotient

For *quotients* of SMTS, we need a partial label operator $\obslash : \mathsf{Spec} \times \mathsf{Spec} \hookrightarrow \mathsf{Spec}$ for which it holds that

- for all $k, \ell, m \in \mathsf{Spec}$, $\ell \obslash k$ is defined and $m \sqsubseteq_{\mathsf{Spec}} \ell \obslash k$ if and only if $k \obar m$ is defined and $k \obar m \sqsubseteq_{\mathsf{Spec}} \ell$;
- for all $\ell, \ell' \in \mathsf{Spec}$, $(\exists k \in \mathsf{Spec} : d(k,\ell) \neq \top_{\mathbb{L}}, d(k,\ell') \neq \top_{\mathbb{L}}) \iff (\exists m \in \mathsf{Spec} : m \obslash \ell, m \obslash \ell'$ are defined).

The first condition ensures that $\obslash$ is adjoint to $\obar$, and the second relates it to distances just as we did for $\obar$ above. Extending the first condition, we say that

- $\obslash$ is *quantitatively well-behaved* if it holds for all $k, \ell, m \in \mathsf{Spec}$ that $\ell \obslash k$ is defined and $d(m, \ell \obslash k) \neq \top_{\mathbb{L}}$ if and only if $k \obar m$ is defined and $d(k \obar m, \ell) \neq \top_{\mathbb{L}}$, and in that case, $F(m, \ell \obslash k, \alpha) \sqsupseteq_{\mathbb{L}} F(k \obar m, \ell, \alpha)$ for all $\alpha \in \mathbb{L}$, and that
- $\obslash$ is *quantitatively exact* if the inequality can be sharpened to $F(m, \ell \obslash k, \alpha) = F(k \obar m, \ell, \alpha)$.

Both of these are useful quantitative generalization of the adjunction between $\obslash$ and $\obar$; we will see examples below of quantitatively exact label quotients and in Section 7 of a quantitatively well-behaved one.

In the definition of quotient below, we denote by $\rho_B(S)$ the *pruning* of a SMTS S with respect to the states in $B \subseteq S$, which is obtained as follows. Define a *must*-predecessor operator $\mathsf{pre} : 2^S \to 2^S$ by $\mathsf{pre}(S') = \{s \in S \mid \exists k \in \mathsf{Spec}, s' \in S' : s \xrightarrow{k} s'\}$ and let pre^* be the reflexive, transitive closure of pre. Then $\rho_B(S)$ exists if $s_0 \notin \mathsf{pre}^*(B)$, and in that case, $\rho_B(S) = (S_\rho, s_0, \dashrightarrow_\rho, \longrightarrow_\rho)$ with $S_\rho = S \setminus \mathsf{pre}^*(B)$, $\dashrightarrow_\rho = \dashrightarrow \cap (S_\rho \times \mathsf{Spec} \times S_\rho)$, and $\longrightarrow_\rho = \longrightarrow \cap (S_\rho \times \mathsf{Spec} \times S_\rho)$.

Definition 8 For SMTS S, T, the *quotient* of T by S is the SMTS $T \mathbin{\backslash\!\!\backslash} S = \rho_B(T \times S \cup \{u\}, (t_0, s_0), \dashrightarrow_{T \backslash\!\backslash S}, \longrightarrow_{T \backslash\!\backslash S})$ given as follows (if it exists):

$$\frac{t \overset{\ell}{\dashrightarrow}_T t' \quad s \overset{k}{\dashrightarrow}_S s' \quad \ell \obslash k \text{ defined}}{(t,s) \overset{\ell \obslash k}{\dashrightarrow}_{T \backslash\!\backslash S} (t', s')} \qquad \frac{t \xrightarrow{\ell}_T t' \quad s \xrightarrow{k}_S s' \quad \ell \obslash k \text{ defined}}{(t,s) \xrightarrow{\ell \obslash k}_{T \backslash\!\backslash S} (t', s')}$$

$$\frac{t \xrightarrow{\ell}_T t' \quad \forall s \xrightarrow{k}_S s' : \ell \obslash k \text{ undefined}}{(t,s) \in B}$$

$$\frac{m \in \mathsf{Spec} \quad \forall s \overset{k}{\dashrightarrow}_S s' : k \obar m \text{ undefined}}{(t,s) \overset{m}{\dashrightarrow}_{T \backslash\!\backslash S} u} \qquad \frac{m \in \mathsf{Spec}}{u \overset{m}{\dashrightarrow}_{T \backslash\!\backslash S} u}$$

In the above definition, u is a new *universal* state from which everything is allowed and nothing required (last SOS rule). This state is reached from a quotient state (t,s) under label m whenever there is no *may* transition from s with whose label m can synchronize (next-to-last SOS rule), because in that case, any transition in the quotient will be canceled in the structural composition (*cf.* Theorem 3 below), and we need the quotient to be maximal. Similarly, if t specifies a *must* transition under a label ℓ which cannot be matched by any transition from s, then the quotient state (t,s) is *inconsistent*; hence we add it to B and remove it when pruning.

The next theorem shows that under certain standard conditions, quotient is *sound* and *maximal* with respect to structural composition.

Theorem 3 *Let S, T, X be SMTS such that S is deterministic and $T \mathbin{\backslash\!\!\backslash} S$ exists. Then $X \le_m T \mathbin{\backslash\!\!\backslash} S$ if and only if $S \| X \le_m T$. Also,*

- *if $\oslash$ is quantitatively well-behaved, then $d_m(X, T \mathbin{\backslash\!\!\backslash} S) \sqsupseteq_{\mathbb{L}} d_m(S \| X, T)$;*
- *if $\oslash$ is quantitatively exact and $d_m(X, T \mathbin{\backslash\!\!\backslash} S) \ne \top_{\mathbb{L}}$, then $d_m(X, T \mathbin{\backslash\!\!\backslash} S) = d_m(S \| X, T)$.*

The (Boolean) property that $X \le_m T \mathbin{\backslash\!\!\backslash} S$ iff $S \| X \le_m T$ implies *uniqueness* of quotient [28]. For the quantitative generalizations, the property induced by a well-behaved $\oslash$ means that distances to the quotient bound distances of structural compositions, which can be useful in further calculations; similarly for exact $\oslash$. Note that uniqueness implies that if a certain instantiation of our framework admits a quotient which is not quantitatively well-behaved, there is no hope that one can find another one which is.

Proof The proof that $X \le_m T \mathbin{\backslash\!\!\backslash} S$ if and only if $S \| X \le_m T$ is in [7]. For the other properties, assume first $\oslash$ to be quantitatively well-behaved; we show that $d_m(S \| X, T) \sqsubseteq_{\mathbb{L}} d_m(X, T \mathbin{\backslash\!\!\backslash} S)$. If $d_m(X, T \mathbin{\backslash\!\!\backslash} S) = \top_{\mathbb{L}}$, there is nothing to prove, so assume $d_m(X, T \mathbin{\backslash\!\!\backslash} S) \ne \top_{\mathbb{L}}$ and let $R = \{R_\alpha \subseteq X \times (T \times S \cup \{u\})\}$ be a witness for $d_m(X, T \mathbin{\backslash\!\!\backslash} S)$. Define $R'_\alpha = \{((s, x), t) \mid (x, (t, s)) \in R_\alpha\} \subseteq S \times X \times T$ for all $\alpha \in \mathbb{L}$ and collect these to a family $R' = \{R'_\alpha \mid \alpha \in \mathbb{L}\}$. We show that R' is a witness for $d_m(S \| X, T) \sqsubseteq_{\mathbb{L}} d_m(X, T \mathbin{\backslash\!\!\backslash} S)$.

We have $((s_0, x_0), t_0) \in R'_{d_m(X, T \mathbin{\backslash\!\!\backslash} S)} \in R'$, so let $\alpha \in \mathbb{L}$ and $((s, x), t) \in R'_\alpha \in R'$, and assume first that $(s, x) \overset{k \oplus m}{\dashrightarrow}_{S \| X} (s', x')$. Then $s \overset{k}{\dashrightarrow}_S s'$ and $x \overset{m}{\dashrightarrow}_X x'$ by definition of $S \| X$. Now $(x, (t, s)) \in R_\alpha \in R$ implies that there is $(t, s) \overset{\ell \oslash k'}{\dashrightarrow}_{T \mathbin{\backslash\!\!\backslash} S} (t', s'')$ and $\alpha' \in \mathbb{L}$ for which $F(m, \ell \oslash k', \alpha') \sqsubseteq_{\mathbb{L}} \alpha$ and $(x', (t', s'')) \in R_{\alpha'} \in R$. But then also $((s'', x'), t') \in R'_\alpha \in R'$, hence $k' \oplus m$ is defined and $F(k' \oplus m, \ell, \alpha') \sqsubseteq_{\mathbb{L}} F(m, \ell \oslash k', \alpha') \sqsubseteq_{\mathbb{L}} \alpha$.

Now $k \oplus m$ and $k' \oplus m$ being defined implies that there is k'' for which $d(k'', k) \ne \top_{\mathbb{L}}$ and $d(k'', k') \ne \top_{\mathbb{L}}$, and by definition of $T \mathbin{\backslash\!\!\backslash} S$, $s \overset{k'}{\dashrightarrow}_S s''$. As S is deterministic, this implies $k = k'$ and $s' = s''$. Hence $((s', x'), t') \in R'_{\alpha'} \in R'$ and $F(k \oplus m, \ell, \alpha') \sqsubseteq_{\mathbb{L}} \alpha$.

Assume now that $t \overset{\ell}{\longrightarrow}_T t'$. We must have $s \overset{k}{\longrightarrow}_S s'$ for which $\ell \oslash k$ is defined, for otherwise $(t, s) \in B$ and hence (t, s) would have been pruned in $T \mathbin{\backslash\!\!\backslash} S$. Thus $(t, s) \overset{\ell \oslash k}{\longrightarrow}_{T \mathbin{\backslash\!\!\backslash} S} (t', s')$, which by $(x, (t, s)) \in R_\alpha \in R$ implies that there is $x \overset{m}{\longrightarrow}_X x'$ and $\alpha' \in \mathbb{L}$ for which $F(m, \ell \oslash k, \alpha') \sqsubseteq_{\mathbb{L}} \alpha$ and $(x', (t', s')) \in R_{\alpha'} \in R$, hence $((s', x'), t') \in R'_{\alpha'} \in R'$. But then $k \oplus m$ is defined and $F(k \oplus m, \ell, \alpha') \sqsubseteq_{\mathbb{L}} F(m, \ell \oslash k, \alpha') \sqsubseteq_{\mathbb{L}} \alpha$, and $(s, x) \overset{k \oplus m}{\longrightarrow}_{S \| X} (s', x')$.

Let now $\oslash$ be quantitatively exact. To show that $d_m(X, T \mathbin{\backslash\!\!\backslash} S) \sqsubseteq_{\mathbb{L}} d_m(S \| X, T)$, assume that $d_m(S \| X, T) \ne \top_{\mathbb{L}}$ (otherwise there is nothing to prove), let $R = \{R_\alpha \subseteq S \times X \times T \mid \alpha \in \mathbb{L}\}$ be a witness for $d_m(S \| X, T)$, and define $R'_\alpha = \{(x, (t, s)) \mid ((s, x), t) \in R_\alpha\} \cup \{(x, u) \mid x \in X\} \subseteq X \times (T \times S \cup \{u\})$ for all $\alpha \in \mathbb{L}$. We show that $R' = \{R'_\alpha \mid \alpha \in \mathbb{L}\}$ is a witness for $d_m(X, T \mathbin{\backslash\!\!\backslash} S) \sqsubseteq_{\mathbb{L}} d_m(S \| X, T)$.

We have $(x_0, (t_0, s_0)) \in R'_{d_m(S \| X, T)} \in R'$. Let $\alpha \in \mathbb{L}$, $(x, u) \in R'_\alpha \in R'$ and $x \overset{m}{\dashrightarrow}_X x'$, then also $u \overset{m}{\dashrightarrow}_{T \mathbin{\backslash\!\!\backslash} S} u$, $F(m, m, \bot_{\mathbb{L}}) \sqsubseteq \alpha$, and $(x', u) \in R'_{\bot_{\mathbb{L}}} \in R'$. Now let $(x, (t, s)) \in R'_\alpha \in R'$ and $x \overset{m}{\dashrightarrow}_X x'$. If $k \oplus m$ is undefined for all $s \overset{k}{\dashrightarrow}_S s'$, then by definition of $T \mathbin{\backslash\!\!\backslash} S$, $(t, s) \overset{m}{\dashrightarrow}_{T \mathbin{\backslash\!\!\backslash} S} u$, $F(m, m, \bot_{\mathbb{L}}) \sqsubseteq \alpha$, and $(x', u) \in R'_{\bot_{\mathbb{L}}} \in R'$.

If there is a transition $s \overset{k}{\dashrightarrow}_S s'$ for which $k \oplus m$ is defined (by determinism there can be at most one), then also $(s,x) \overset{k\oplus m}{\dashrightarrow}_{S\|X} (s',x')$. As $((s,x),t) \in R_\alpha \in R$, we must have $t \overset{\ell}{\dashrightarrow} t'$ and $\alpha' \in \mathbb{L}$ with $F(k \oplus m, \ell, \alpha') \sqsubseteq_{\mathbb{L}} \alpha$ and $((s',x'),t') \in R_{\alpha'} \in R$, hence $(x',(t',s')) \in R'_{\alpha'} \in R'$. Then $\ell \oslash k$ is defined and $F(m, \ell \oslash k, \alpha') \sqsubseteq_{\mathbb{L}} \alpha$, and by definition of $T \setminus\!\!\setminus S$, $(t,s) \overset{\ell\oslash k}{\dashrightarrow}_{T\setminus\!\setminus S} (t',s')$.

Now assume that $(t,s) \xrightarrow{\ell\oslash k}_{T\setminus\!\setminus S} (t',s')$, then $t \xrightarrow{\ell}_T t'$ and $s \xrightarrow{k}_S s'$ by definition of $T \setminus\!\!\setminus S$. By $((s,x),t) \in R_\alpha \in R$, we have $(s,x) \xrightarrow{k'\oplus m}_{S\|X} (s'',x')$ and $\alpha' \in \mathbb{L}$ with $F(k' \oplus m, \ell, \alpha') \sqsubseteq_{\mathbb{L}} \alpha$ and $((s'',x'),t') \in R_{\alpha'} \in R$. This in turn implies that $s \xrightarrow{k'}_S s''$ and $x \xrightarrow{m}_X s'$ by definition of $S\|X$. We also see that $\ell \oslash k'$ is defined, which by determinism of S entails $k = k'$ and $s' = s''$. Hence $F(k \oplus m, \ell, \alpha') \sqsubseteq_{\mathbb{L}} \alpha$ and $(x',(t',s')) \in R'_{\alpha'} \in R'$. $\square$

Examples 1–3 (contd) For the label synchronization operator for $\mathsf{Spec} = \Sigma \times \mathbb{I}$ given by adding interval boundaries, a quotient can be defined by

$$(a',[l',r']) \oslash (a,[l,r]) = \begin{cases} (a,[l'-l, r'-r]) & \text{if } a = a' \text{ and } l'-l \le r'-r, \\ \text{undefined} & \text{otherwise.} \end{cases}$$

It can then be shown [4] that $d(m, \ell \oslash k) = d(k \oplus m, \ell)$ for all $k, \ell, m \in \mathsf{Spec}$ for which both $\ell \oslash k$ and $k \oplus m$ are defined. From this it easily follows that both for the accumulating, the point-wise, and the limit-average distance, $\oslash$ is quantitatively exact, hence for all three distances, Theorem 3 specializes to the theorem that $\tilde d_m(X, T \setminus\!\!\setminus S) = \tilde d_m(S\|X, T)$ for all SMTS S, T, X for which S is deterministic, $T \setminus\!\!\setminus S$ exists and $\tilde d_m(X, T \setminus\!\!\setminus S) \ne \infty$. For the accumulating distance, this is [4, Thm. 6].

Of course, different label synchronization operators give rise to different quotients with different properties; we refer again to Section 7.

5 Conjunction

Conjunction of SMTS can be used to merge two specifications into one. Let $\owedge : \mathsf{Spec} \times \mathsf{Spec} \hookrightarrow \mathsf{Spec}$ be a partial label operator for which it holds that

- for all $k, \ell \in \mathsf{Spec}$, if $k \owedge \ell$ is defined, then $k \owedge \ell \sqsubseteq_{\mathsf{Spec}} k$, $k \owedge \ell \sqsubseteq_{\mathsf{Spec}} \ell$, and
- for all $\ell, \ell' \in \mathsf{Spec}$, $(\exists k \in \mathsf{Spec} : d(k,\ell) \ne \top_{\mathbb{L}}, d(k,\ell') \ne \top_{\mathbb{L}}) \iff (\exists m \in \mathsf{Spec} : \ell \owedge m, \ell' \owedge m$ are defined).

The first requirement above ensures that conjunction acts as a lower bound, and the second one relates it to distances such that two labels have a common quantitative refinement if and only if they have a common conjunction. One also usually wants conjunction to be a *greatest* lower bound; we say that $\owedge$ is *conjunctively compositional* if it holds for all $k, \ell, m \in \mathsf{Spec}$ for which $m \sqsubseteq_{\mathsf{Spec}} k$ and $m \sqsubseteq_{\mathsf{Spec}} \ell$ that also $k \owedge \ell$ is defined and $m \sqsubseteq_{\mathsf{Spec}} k \owedge \ell$.

As a quantitative generalization, and analogously to what we did for structural composition, we say that $\owedge$ is *conjunctively bounded* by a function $C : \mathbb{L} \times \mathbb{L} \to \mathbb{L}$ if C is monotone in both coordinates, has $C(\bot_{\mathbb{L}}, \bot_{\mathbb{L}}) = \bot_{\mathbb{L}}$, $C(\alpha, \top_{\mathbb{L}}) = C(\top_{\mathbb{L}}, \alpha) = \top_{\mathbb{L}}$

for all $\alpha \in \mathbb{L}$, and if it holds for all $k, \ell, m \in \mathsf{Spec}$ for which $d(m,k) \neq \top_{\mathbb{L}}$ and $d(m,\ell) \neq \top_{\mathbb{L}}$ that $k \oslash \ell$ is defined and

$$F(m, k \oslash \ell, C(\alpha, \alpha')) \sqsubseteq_{\mathbb{L}} C(F(m,k,\alpha), F(m,\ell,\alpha'))$$

for all $\alpha, \alpha' \in \mathbb{L}$. Note that this implies that $d(m, k \oslash \ell) \sqsubseteq_{\mathbb{L}} C(d(m,k), d(m,\ell))$, hence conjunctive boundedness implies conjunctive compositionality. Like P for structural composition, C gives a uniform bound on label conjunction.

Definition 9 The *conjunction* of two SMTS S and T is the SMTS $S \wedge T = \rho_B(S \times T, (s_0, t_0), \dashrightarrow_{S\wedge T}, \longrightarrow_{S\wedge T})$ given as follows:

$$\frac{s \xrightarrow{k}_S s' \quad t \overset{\ell}{\dashrightarrow}_T t' \quad k \oslash \ell \text{ defined}}{(s,t) \xrightarrow{k \oslash \ell}_{S\wedge T} (s',t')} \qquad \frac{s \overset{k}{\dashrightarrow}_S s' \quad t \xrightarrow{\ell}_T t' \quad k \oslash \ell \text{ defined}}{(s,t) \xrightarrow{k \oslash \ell}_{S\wedge T} (s',t')}$$

$$\frac{s \overset{k}{\dashrightarrow}_S s' \quad t \overset{\ell}{\dashrightarrow}_T t' \quad k \oslash \ell \text{ defined}}{(s,t) \overset{k \oslash \ell}{\dashrightarrow}_{S\wedge T} (s',t')}$$

$$\frac{s \xrightarrow{k}_S s' \quad \forall t \overset{\ell}{\dashrightarrow}_T t' : k \oslash \ell \text{ undef.}}{(s,t) \in B} \qquad \frac{t \xrightarrow{\ell}_T t' \quad \forall s \overset{k}{\dashrightarrow}_S s' : k \oslash \ell \text{ undef.}}{(s,t) \in B}$$

Note that like for quotient, conjunction of SMTS may give inconsistent states which need to be pruned away after. As seen in the last two SOS rules above, this is the case when one SMTS specifies a *must* transition which the other SMTS cannot synchronize with. Hence, the demand on implementations of the conjunction is that they simultaneously *must* and *cannot* have a transition, which of course is unsatisfiable.

The next theorem shows the precise conditions under which conjunction is a greatest lower bound. Note that the greatest-lower-bound condition $U \leq_m S$, $U \leq_m T \Longrightarrow U \leq_m S \wedge T$ entails uniqueness.

Theorem 4 *Let S, T, U be SMTS. If $S \wedge T$ is defined, then $S \wedge T \leq_m S$ and $S \wedge T \leq_m T$. If, additionally, S or T are deterministic, then:*

- *If $\oslash$ is conjunctively compositional, $U \leq_m S$, and $U \leq_m T$, then $S \wedge T$ is defined and $U \leq_m S \wedge T$.*
- *If $\oslash$ is conjunctively bounded by C, $d_m(U,S) \neq \top_{\mathbb{L}}$, and $d_m(U,T) \neq \top_{\mathbb{L}}$, then $S \wedge T$ is defined and $d_m(U, S \wedge T) \sqsubseteq_{\mathbb{L}} C(d_m(U,S), d_m(U,T))$.*

Proof The proof of the two first claims is in [7]. For the third claim, let $R = \{R_\alpha \subseteq U \times S \mid \alpha \in \mathbb{L}\}$ and $R' = \{R'_\alpha \subseteq U \times T \mid \alpha \in \mathbb{L}\}$ be relation families witnessing $d_m(U,S)$ and $d_m(U,T)$, respectively, define $R^\wedge_\beta = \{(u,(s,t)) \mid \exists \alpha, \alpha' \in \mathbb{L} : (u,s) \in R_\alpha, (u,t) \in R'_{\alpha'}, C(\alpha,\alpha') \sqsubseteq_{\mathbb{L}} \beta\} \subseteq U \times S \times T$ for all $\beta \in \mathbb{L}$, and let $R^\wedge = \{R^\wedge_\beta \mid \beta \in \mathbb{L}\}$. We show that $R^\wedge$ is a witness for $d_m(U, S \wedge T) \sqsubseteq_{\mathbb{L}} C(d_m(U,S), d_m(U,T))$.

We have $(u_0, (s_0, t_0)) \in R^\wedge_{C(d_m(U,S), d_m(U,T))} \in R^\wedge$. Let $\beta \in \mathbb{L} \setminus \{\bot_{\mathbb{L}}\}$ and $(u,(s,t)) \in R^\wedge_\beta \in R^\wedge$, then we have $\alpha, \alpha' \in \mathbb{L} \setminus \{\bot_{\mathbb{L}}\}$ with $(u,s) \in R_\alpha \in R$, $(u,t) \in R'_{\alpha'} \in R'$, and $C(\alpha,\alpha') \sqsubseteq_{\mathbb{L}} \beta$.

Assume $u \overset{m}{\dashrightarrow}_U u'$, then there exist $s \overset{k}{\dashrightarrow}_S s'$ and $\bar\alpha \in \mathbb{L}$ for which $(u',s') \in R_{\bar\alpha} \in R$ and $F(m,k,\bar\alpha) \sqsubseteq_{\mathbb{L}} \alpha$, and similarly $t \overset{\ell}{\dashrightarrow}_T t'$ and $\bar\alpha'$ with $(u',t') \in R'_{\bar\alpha'} \in R'$ and

$F(m,\ell,\bar\alpha') \sqsubseteq \alpha'$. Then $d(m,k) \ne \top_{\mathbb{L}}$ and $d(m,\ell) \ne \top_{\mathbb{L}}$, so by conjunctive boundedness $k \oslash \ell$ is defined, and $(s,t) \overset{k\oslash\ell}{\dashrightarrow}_{S\wedge T} (s',t')$ by definition of $S\wedge T$. Also, $(u',(s',t')) \in R^{\wedge}_{C(\bar\alpha,\bar\alpha')} \in R^{\wedge}$ and $F(m, k\oslash\ell, C(\bar\alpha,\bar\alpha')) \sqsubseteq_{\mathbb{L}} C(F(m,k,\bar\alpha), F(m,\ell,\bar\alpha')) \sqsubseteq_{\mathbb{L}} C(\alpha,\alpha')$.

Assume $(s,t) \xrightarrow{k\oslash\ell}_{S\wedge T} (s',t')$, then $s \xrightarrow{k}_S s'$ and $t \xrightarrow{\ell}_T t'$ by definition of $S\wedge T$. We can without loss of generality postulate that T is deterministic. The fact that $(u,s) \in R_\alpha \in R$ implies that there are $u \xrightarrow{m}_U u'$ and $\bar\alpha \in \mathbb{L}$ for which $(u',s') \in R_{\bar\alpha} \in R$ and $F(m,k,\bar\alpha) \sqsubseteq_{\mathbb{L}} \alpha$. We must also have $u \overset{m'}{\dashrightarrow}_U u'$ for some $m' \sqsupseteq_{\mathsf{Spec}} m$, and then $(u,t) \in R'_{\bar\alpha} \in R'$ implies that there exist $t \overset{\ell'}{\dashrightarrow}_T t''$ and $\bar\alpha' \in \mathbb{L}$ with $(u',t'') \in R'_{\bar\alpha'} \in R'$ and $F(m',\ell',\bar\alpha') \sqsubseteq_{\mathbb{L}} \alpha'$.

The triangle inequality for F gives $F(m,\ell',\bar\alpha') \sqsubseteq_{\mathbb{L}} F(m,m',\bot_{\mathbb{L}}) \oplus F(m',\ell',\bar\alpha') \sqsubseteq_{\mathbb{L}} \alpha'$, hence $d(m,\ell') \ne \top_{\mathbb{L}}$. Together with $d(m,k) \ne \top_{\mathbb{L}}$, conjunctive boundedness allows us to conclude that $k \oslash \ell'$ is defined, but then both $k\oslash\ell$ and $k\oslash\ell'$ are defined, hence by determinism of T, $\ell = \ell'$ and $t' = t''$. $\square$

Examples 1–3 (contd) For the set $\mathsf{Spec} = \Sigma \times \mathbb{I}$ from our examples, the unique compositional conjunction operator on is given, on labels, by intersection of intervals [4]:

$$(a,[l,r]) \oslash (a',[l',r']) = \begin{cases} (a,[\max(l,l'),\min(r,r')]) & \text{if } a = a', \max(l,l') \le \min(r,r'), \\ \text{undefined} & \text{otherwise.} \end{cases}$$

We can easily show that $\oslash$ is *not* conjunctively bounded: with $m = (a,[2,2])$, $k = (a,[0,1])$ and $\ell = (a,[3,4])$, $d(m,k) = d(m,\ell) = 1$, but $k \oslash \ell$ is not defined. Noting that this statement does not involve the distance iterator F, we conclude that neither accumulating, point-wise nor limit-average distance admit a bounded conjunction operator. For the accumulating distance, this statement is [4, Thm. 4].

To deal with the problem that, as in the above example, conjunction may not be conjunctively bounded, we introduce another, weaker, property which ensures some compatibility of conjunction with distances. We say that $\oslash$ is *relaxed conjunctively bounded* by a function $C : \mathbb{L}\times\mathbb{L} \to \mathbb{L}$ if C is monotone in both coordinates, has $C(\bot_{\mathbb{L}},\bot_{\mathbb{L}}) = \bot_{\mathbb{L}}$, $C(\alpha,\top_{\mathbb{L}}) = C(\top_{\mathbb{L}},\alpha) = \top_{\mathbb{L}}$ for all $\alpha \in \mathbb{L}$, and such that for all $k,\ell \in \mathsf{Spec}$ for which there is $m \in \mathsf{Spec}$ with $d(m,k) \ne \top_{\mathbb{L}}$ and $d(m,\ell) \ne \top_{\mathbb{L}}$, there exist $k',\ell' \in \mathsf{Spec}$ with $k' \oslash \ell'$ defined, $k \sqsubseteq_{\mathsf{Spec}} k'$, $\ell \sqsubseteq_{\mathsf{Spec}} \ell'$, $d(k',k) \ne \top_{\mathbb{L}}$, and $d(\ell',\ell) \ne \top_{\mathbb{L}}$, such that for all $m' \in \mathsf{Spec}$, $\alpha,\alpha' \in \mathbb{L}$,

$$F(m', k'\oslash\ell', C(\alpha,\alpha')) \sqsubseteq_{\mathbb{L}} C(F(m',k,\alpha), F(m',\ell,\alpha')). \tag{3}$$

The following theorem shows that relaxed boundedness of $\oslash$ entails a similar property for SMTS conjunction.

Theorem 5 *Let S, T be SMTS with S or T deterministic and $\oslash$ relaxed conjunctively bounded by C. If there is an SMTS U for which $d_m(U,S) \ne \top_{\mathbb{L}}$ and $d_m(U,T) \ne \top_{\mathbb{L}}$, then there exist β- and γ-widenings S' of S and T' of T for which $S' \wedge T'$ is defined, and such that $d_m(U', S'\wedge T') \sqsubseteq_{\mathbb{L}} C(d_m(U',S), d_m(U',T))$ for all SMTS U'.*

Proof We start by constructing S' and T', almost as in the proof of the third claim of Theorem 4. The states of S' and T' will be the same as for S and T, and we start by letting $\beta = \bot_{\mathbb{L}}$, $\gamma = \bot_{\mathbb{L}}$.

Let U fulfill $d_m(U,S) \neq \top_{\mathbb{L}}$ and $d_m(U,T) \neq \top_{\mathbb{L}}$, let $R = \{R_\alpha \subseteq U \times S \mid \alpha \in \mathbb{L}\}$ and $R' = \{R'_\alpha \subseteq U \times T \mid \alpha \in \mathbb{L}\}$ be relation families witnessing $d_m(U,S)$ and $d_m(U,T)$, respectively, define $R^\wedge_\eta = \{(u,(s,t)) \mid \exists \alpha, \alpha' \in \mathbb{L} : (u,s) \in R_\alpha, (u,t) \in R'_{\alpha'}, C(\alpha,\alpha') \sqsubseteq_{\mathbb{L}} \eta\} \subseteq U \times S \times T$ for all $\eta \in \mathbb{L}$, and let $R^\wedge = \{R^\wedge_\eta \mid \eta \in \mathbb{L}\}$.

Now let $\eta \in \mathbb{L} \setminus \{\top_{\mathbb{L}}\}$ and $(u,(s,t)) \in R^\wedge_\eta \in R^\wedge$, then we have $\alpha, \alpha' \in \mathbb{L} \setminus \{\bot_{\mathbb{L}}\}$ with $(u,s) \in R_\alpha \in R$, $(u,t) \in R'_{\alpha'} \in R'$, and $C(\alpha,\alpha') \sqsubseteq_{\mathbb{L}} \eta$. Let $u \overset{m}{\dashrightarrow}_U u'$, then also $s \overset{k}{\dashrightarrow}_S s'$ and $t \overset{\ell}{\dashrightarrow}_T t'$, and there are $\bar\alpha, \bar\alpha' \in \mathbb{L} \setminus \{\top_{\mathbb{L}}\}$ with $F(m,k,\bar\alpha) \sqsubseteq_{\mathbb{L}} \alpha$ and $F(m,\ell,\bar\alpha') \sqsubseteq_{\mathbb{L}} \alpha'$. Hence $d(m,k) \neq \top_{\mathbb{L}}$ and $d(m,\ell) \neq \top_{\mathbb{L}}$, and by relaxed conjunctive boundedness we have $k', \ell' \in \mathsf{Spec}$ with $k \sqsubseteq_{\mathsf{Spec}} k'$, $\ell \sqsubseteq_{\mathsf{Spec}} \ell'$, $d(k',k) \neq \top_{\mathbb{L}}$, $d(\ell',\ell) \neq \top_{\mathbb{L}}$, and $k' \oslash \ell'$ defined. We add the transitions $s \overset{k'}{\dashrightarrow}_{S'} s'$, $t \overset{\ell'}{\dashrightarrow}_{T'} t'$ to S' and T' and update $\beta := \max(\beta, d(k',k))$, $\gamma := \max(\gamma, d(\ell',\ell))$.

As the sets $\{k \in \mathsf{Spec} \mid s \overset{k}{\dashrightarrow}_S s'\}$, $\{\ell \in \mathsf{Spec} \mid t \overset{\ell}{\dashrightarrow}_T t'\}$ are compact, the above process converges to some $\beta, \gamma \neq \top_{\mathbb{L}}$. The *must* transitions we just copy from S to S' and from T to T', and then S' is a β-widening of S and T' is a γ-widening of T.

We must show that S' and T' satisfy the properties claimed. By construction $S' \wedge T'$ is defined, so let U' be an SMTS with $d_m(U',S) \neq \top_{\mathbb{L}}$ and $d_m(U',T) \neq \top_{\mathbb{L}}$ (otherwise we have nothing to prove). We must show that $d_m(U', S' \wedge T') \sqsubseteq_{\mathbb{L}} C(d_m(U',S), d_m(U',T))$. Let $R = \{R_\alpha \subseteq U' \times S \mid \alpha \in \mathbb{L}\}$ and $R' = \{R'_\alpha \subseteq U' \times T \mid \alpha \in \mathbb{L}\}$ be relation families witnessing $d_m(U',S)$ and $d_m(U',T)$, respectively, define $R^{\wedge'}_\eta = \{(u',(s,t)) \mid \exists \alpha,\alpha' \in \mathbb{L} : (u',s) \in R_\alpha, (u',t) \in R'_{\alpha'}, C(\alpha,\alpha') \sqsubseteq_{\mathbb{L}} \eta\} \subseteq U' \times S \times T$ for all $\eta \in \mathbb{L}$, and let $R^{\wedge'} = \{R^{\wedge'}_\eta \mid \eta \in \mathbb{L}\}$.

We have $(u'_0,(s_0,t_0)) \in R^{\wedge'}_{C(d_m(U',S),d_m(U',T))} \in R^{\wedge'}$. Let $\eta \in \mathbb{L} \setminus \{\bot_{\mathbb{L}}\}$ and $(u',(s,t)) \in R^{\wedge'}_\eta$, then we have $\alpha,\alpha' \in \mathbb{L} \setminus \{\bot_{\mathbb{L}}\}$ with $(u',s) \in R_\alpha \in R$, $(u',t) \in R'_{\alpha'} \in R'$, and $C(\alpha,\alpha') \sqsubseteq_{\mathbb{L}} \eta$. Let $u' \overset{m}{\dashrightarrow}_{U'} u''$, then also $s \overset{k}{\dashrightarrow}_S s'$ and $t \overset{\ell}{\dashrightarrow}_T t'$, and there are $\bar\alpha, \bar\alpha' \in \mathbb{L} \setminus \{\top_{\mathbb{L}}\}$ with $(u'',s') \in R_{\bar\alpha}$, $(u'',t') \in R'_{\bar\alpha'}$, $F(m,k,\bar\alpha) \sqsubseteq_{\mathbb{L}} \alpha$, and $F(m,\ell,\bar\alpha') \sqsubseteq_{\mathbb{L}} \alpha'$.

By construction of S' and T', we have $s \overset{k'}{\dashrightarrow}_{S'} s'$ and $t \overset{\ell'}{\dashrightarrow}_{T'} t'$ with $k \sqsubseteq_{\mathsf{Spec}} k'$, $\ell \sqsubseteq_{\mathsf{Spec}} \ell'$, $d(k',k) \sqsubseteq_{\mathbb{L}} \beta$, and $d(\ell',\ell) \sqsubseteq_{\mathbb{L}} \gamma$, and such that $k' \oslash \ell'$ is defined. Also, $(u'',(s',t')) \in R^{\wedge'}_{C(\bar\alpha,\bar\alpha')}$ and

$$F(m, k' \oslash \ell', C(\bar\alpha,\bar\alpha')) \sqsubseteq_{\mathbb{L}} C(F(m,k,\bar\alpha), F(m,\ell,\bar\alpha')) \sqsubseteq_{\mathbb{L}} C(\alpha,\alpha').$$

The other direction of the proof, starting with a transition $(s,t) \overset{k \oslash \ell}{\longrightarrow}_{S' \wedge T'} (s',t')$, is an exact copy of the corresponding part of the proof of Theorem 4. □

Example 1 (contd) For the set $\mathsf{Spec} = \Sigma \times \mathbb{I}$ from our examples, the following lemma shows a one-step version of relaxed conjunctive boundedness.

Lemma 4 *For all $k, \ell \in \mathsf{Spec}$ for which there is $m \in \mathsf{Spec}$ with $d(m,k) \neq \infty$ and $d(m,\ell) \neq \infty$, there exist $k', \ell' \in \mathsf{Spec}$ with $k \sqsubseteq_{\mathsf{Spec}} k'$, $\ell \sqsubseteq_{\mathsf{Spec}} \ell'$, $d(k',k) \neq \infty$, $d(\ell',\ell) \neq \infty$, and $k' \oslash \ell'$ defined, and then $d(m', k' \oslash \ell') \leq \max(d(m',k), d(m',\ell))$ for all $m' \in \mathsf{Spec}$.*

Proof Let $k, \ell \in \mathsf{Spec}$ such that there is $m \in \mathsf{Spec}$ with $d(m,k) \neq \infty$ and $d(m,\ell) \neq \infty$. This implies that $k = (a,[l,r])$ and $\ell = (a,[l',r'])$ for some $a \in \Sigma$, $k,l,k',l' \in \mathbb{Z} \cup \{-\infty,\infty\}$. Without loss of generality we can assume that $l \leq l'$.

If $r \geq l'$, then $k \oslash \ell = (a, [l', r])$ is defined, and we take $k' = k$, $\ell' = \ell$. Now let $m' = (a', [l'', r'']) \in \mathsf{Spec}$. If $a' \neq a$, the property to prove is trivially true. If $a' = a$, then we have

$$\begin{aligned} d(m', k' \oslash \ell') &= \max(0, l' - l'', r'' - r), \\ d(m', k) &= \max(0, l - l'', r'' - r), \\ d(m', \ell) &= \max(0, l' - l'', r'' - r'). \end{aligned}$$

Thus we need to show that

$$\max(0, l' - l'', r'' - r) \leq \max(0, l - l'', r'' - r, l' - l'', r'' - r'),$$

which is clear as all left-hand terms also appear on the right-hand side.

In case $r < l'$, we let $k' = (a, [l, l'])$ and $\ell' = (a, [r, r'])$. Then $k \sqsubseteq_{\mathsf{Spec}} k'$, $\ell \sqsubseteq_{\mathsf{Spec}} \ell'$, and $k' \oslash \ell' = (a, [r, l'])$ is defined. Also, $d(k', k) = d(\ell', \ell) = l' - r \neq \infty$.

Let $m' = (a', [l'', r''])$ as before, then the case $a' \neq a$ is again trivial. We have

$$d(m', k' \oslash \ell') = \max(0, r - l'', r'' - l'),$$

so we need to show that

$$\begin{aligned} \max(0, r - l'', r'' - l') &\leq \max(0, l - l'', r'' - r, l' - l'', r'' - r') \\ &= \max(0, r'' - r, l' - l''), \end{aligned}$$

where the equality follows from $l \leq l'$, hence $l - l'' \leq l' - l''$, and $r \leq r'$, hence $r'' - r' \leq r'' - r$. But $0 \leq l' - r$, $r - l'' < l' = l''$, and $r'' - l' < r'' - r$ because of $r < l'$, so the inequality follows. $\square$

For the accumulating distance, it then follows that $\oslash$ is relaxed conjunctively bounded by $C(\alpha, \alpha') = \alpha + \alpha'$: Using the notation from Lemma 4, we need to show (3), *i.e.* that $d(m', l' \oslash \ell') + \lambda(\alpha + \alpha') \leq d(m', k) + \lambda\alpha + d(m', \ell) + \lambda\alpha'$, which however is clear by $d(m', k' \oslash \ell') \leq \max(d(m', k), d(m', \ell)) \leq d(m', k) + d(m', \ell)$.

Example 2 (contd) For the pointwise distance, $\oslash$ is relaxed conjunctively bounded by $C(\alpha, \alpha') = \max(\alpha, \alpha')$: (3) is then equivalent to $\max(d(m', k' \oslash \ell'), \alpha, \alpha') \leq \max(d(m', k), d(m', \ell), \alpha, \alpha')$, which follows from Lemma 4.

Example 3 (contd) For the limit-average distance, $\oslash$ is relaxed conjunctively bounded by $C(\alpha, \alpha') = \alpha \oplus_{\mathbb{L}} \alpha'$: Again using the notation from Lemma 4, we need to show (3), so we need to see that for all $j \in \mathbb{N}_+$, $\frac{1}{j+1} d(m', k' \oslash \ell') + \frac{j}{j+1}\alpha(j-1) + \frac{j}{j+1}\alpha'(j-1) \leq \frac{1}{j+1} d(m', k) + \frac{j}{j+1}\alpha(j-1) + \frac{1}{j+1} d(m', \ell) + \frac{j}{j+1}\alpha'(j-1)$. This follows again from $d(m', k' \oslash \ell') \leq \max(d(m', k), d(m', \ell)) \leq d(m', k) + d(m', \ell)$.

6 Logical Characterizations

We show that quantitative refinement admits a logical characterization. Our results extend the logical characterization of modal transition systems in [36]. Our logic $\mathcal{L}$ is the smallest set of expressions generated by the following abstract syntax:

$$\phi, \phi_1, \phi_2 := \mathbf{tt} \mid \mathbf{ff} \mid \langle \ell \rangle \phi \mid [\ell]\phi \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2 \qquad (\ell \in \mathsf{Spec})$$

The semantics of a formula $\phi \in \mathcal{L}$ is a mapping $\phi@ : S \to \mathbb{L}$ given inductively as follows:

$$\mathbf{tt}@s = \bot \qquad \mathbf{ff}@s = \top$$
$$(\phi_1 \wedge \phi_2)@s = \max(\phi_1@s, \phi@_2 s) \qquad (\phi_1 \vee \phi_2)@s = \min(\phi_1@s, \phi_2@s)$$
$$\langle \ell \rangle \phi@s = \inf\{F(k, \ell, \phi@t) \mid s \xrightarrow{k} t, d(k, \ell) \neq \top_\mathbb{L}\}$$
$$[\ell]\phi@s = \sup\{F(k, \ell, \phi@t) \mid s \overset{k}{\dashrightarrow} t, d(k, \ell) \neq \top_\mathbb{L}\}$$

For a SMTS S we write $\phi@S = \phi@s_0$. The below theorems express the fact that $\mathcal{L}$ is *quantitatively sound* for refinement distance, *i.e.* the value of a formula in a specification is bounded by its value in any other specification together with their distance, and that the disjunction-free fragment of $\mathcal{L}$ is *quantitatively implementation complete*, *i.e.* the value of any disjunction-free formula in a specification S is bounded above by its value in any implementation of S. Note that disjunction-freeness is a very common assumption in this context, *cf.* [9].

Theorem 6 *For all $\phi \in \mathcal{L}$ and all SMTS S, T, $\phi@S \sqsubseteq_\mathbb{L} \phi@T \oplus_\mathbb{L} d_m(S, T)$.*

Proof Structural induction. The claim obviously holds for $\phi = \mathbf{tt}$ and $\phi = \mathbf{ff}$; if $\phi = \phi_1 \wedge \phi_2$, then $\phi_i@s_1 \sqsubseteq_\mathbb{L} \phi_i@s_2 \oplus_\mathbb{L} d_m(s_1, s_2)$ for $i = 1, 2$ imply that also $\max(\phi_1@s_1, \phi_2@s_1) \sqsubseteq_\mathbb{L} \max(\phi_1@s_2, \phi_2@s_2) \oplus_\mathbb{L} d_m(s_1, s_2)$, and similarly for $\phi = \phi_1 \vee \phi_2$.

For the case $\phi = \langle \ell \rangle \phi'$, there is nothing to prove if there are no transitions $s_2 \longrightarrow_2$ or if $d_m(s_1, s_2) = \top_\mathbb{L}$. Let thus $s_2 \xrightarrow{k_2}_2 t_2$, then there exist $s_1 \xrightarrow{k_1}_1 t_1$ with $F(k_1, k_2, d_m(t_1, t_2)) \sqsubseteq_\mathbb{L} d_m(s_1, s_2)$. Now by induction hypothesis, $\phi'@t_1 \sqsubseteq_\mathbb{L} d_m(t_1, t_2) \oplus_\mathbb{L} \phi'@t_2$, and then, using the triangle inequality,

$$\begin{aligned} F(k_1, \ell, \phi'@t_1) &\sqsubseteq_\mathbb{L} F(k_1, k_2, d_m(t_1, t_2)) \oplus_\mathbb{L} F(k_2, \ell, \phi'@t_2) \\ &\sqsubseteq_\mathbb{L} d_m(s_1, s_2) \oplus_\mathbb{L} F(k_2, \ell, \phi'@t_2). \end{aligned}$$

As $s_2 \xrightarrow{k_2}_2 t_2$ was arbitrary, this entails

$$\inf\{F(k_1, \ell, \phi'@t_1) \mid s_1 \xrightarrow{k_1}_1 t_1\} \sqsubseteq_\mathbb{L} \inf\{F(k_2, \ell, \phi'@t_2) \mid s_1 \xrightarrow{k_2}_2 t_2\} \oplus_\mathbb{L} d_m(s_1, s_2).$$

For the case $\phi = [\ell]\phi'$ the proof is similar: We have nothing to prove if $d_m(s_1, s_2) = \top_\mathbb{L}$ or if there are no transitions $s_1 \overset{k_1}{\dashrightarrow}_1 t_1$ with $F(k_1, \ell, \phi'@t_1) \neq \top_\mathbb{L}$, so assume there is such a transition. Then we also have $s_2 \overset{k_2}{\dashrightarrow}_2 t_2$ with $F(k_1, k_2, d_m(t_1, t_2)) \sqsubseteq_\mathbb{L} d_m(s_1, s_2)$, and

$$\begin{aligned} F(k_1, \ell, \phi'@t_1) &\sqsubseteq_\mathbb{L} F(k_1, k_2, d_m(t_1, t_2)) \oplus_\mathbb{L} F(k_2, \ell, \phi'@t_2) \\ &\sqsubseteq_\mathbb{L} d_m(s_1, s_2) \oplus_\mathbb{L} F(k_2, \ell, \phi'@t_2). \end{aligned} \qquad \square$$

Theorem 7 *For all disjunction-free $\phi \in \mathcal{L}$ and all SMTS S, $\phi@S = \sup_{I \in [\![S]\!]} \phi@I$.*

Proof Theorem 6 entails $\phi @ I \sqsubseteq_{\mathbb{L}} \phi @ S \oplus_{\mathbb{L}} d_m(I,S) = \phi @ S$ for all $I \in [\![S]\!]$, hence also $\sup_{I\in[\![S]\!]} \phi @ I \sqsubseteq_{\mathbb{L}} \phi @ S$. To show that $\phi @ S \sqsubseteq_{\mathbb{L}} \sup_{I\in[\![S]\!]} \phi @ I$ we use structural induction on ϕ. If $\phi = \mathbf{tt}$, both sides are $\bot_{\mathbb{L}}$, and if $\phi = \mathbf{ff}$, both sides are $\top_{\mathbb{L}}$, so the induction base is clear.

The case $\phi = \phi_1 \wedge \phi_2$ is also clear: By hypothesis, $\phi_1 @ S \sqsubseteq_{\mathbb{L}} \sup_{I\in[\![S]\!]} \phi_1 @ I$ and similarly for ϕ_2, hence

$$\begin{aligned} \phi @ S = \max(\phi_1 @ S, \phi_2 @ S) &\sqsubseteq_{\mathbb{L}} \max(\sup_{I\in[\![S]\!]} \phi_1 @ I, \sup_{I\in[\![S]\!]} \phi_2 @ I) \\ &= \sup_{I\in[\![S]\!]} \max(\phi_1 @ I, \phi_2 @ I). \end{aligned}$$

For the case $\phi = \langle \ell \rangle \phi'$, we are done if $\phi @ S = \bot_{\mathbb{L}}$. Otherwise, let $\alpha \sqsubset_{\mathbb{L}} \phi @ S$; we want to expose $I \in [\![S]\!]$ for which $\alpha \sqsubset_{\mathbb{L}} \phi @ I$. Start by letting $I = \{i_0\}$ and $\longrightarrow_I = \emptyset$.

Now for each transition $s_0 \xrightarrow{k}_S t$, we have $\alpha \sqsubset_{\mathbb{L}} F(k, \ell, \phi' @ t)$, so (assuming for the moment that $\phi' @ t \neq \bot_{\mathbb{L}}$) there is $\alpha'_k \sqsubset_{\mathbb{L}} \phi' @ t$ for which $F(k, \ell, \alpha'_k) \sqsupset_{\mathbb{L}} \alpha$. By induction hypothesis, there is $J \in [\![t, S]\!]$ for which $\alpha'_k \sqsubset_{\mathbb{L}} \phi' @ J$; let $n \in [\![k]\!]$ such that $F(n, \ell, \phi' @ J) = F(k, \ell, \phi' @ J)$, and add J together with a transition $i_0 \xrightarrow{n}_I j_0$ to I. In case $\phi' @ t = \bot_{\mathbb{L}}$, we just take an arbitrary $J \in [\![t, S]\!]$.

For the so-constructed implementation I we have

$$\begin{aligned} \phi @ I &= \inf\{F(m, \ell, \phi' @ j \mid i_0 \xrightarrow{m}_I j\} \\ &= \inf\{F(k, \ell, \phi' @ J) \mid s_0 \xrightarrow{k}_S t, J \in [\![t, S]\!], \phi' @ t = \bot_{\mathbb{L}} \text{ or } \alpha'_k \sqsubset_{\mathbb{L}} \phi' @ J\} \\ &\sqsupset_{\mathbb{L}} \inf(\{F(k, \ell, \alpha'_k) \mid s_0 \xrightarrow{k}_S t\} \cup \{F(k, \ell, \phi' @ t)\}) \sqsupseteq_{\mathbb{L}} \alpha, \end{aligned} \tag{4}$$

the strict inequality in (4) because S is compactly branching.

For the case $\phi = [\ell]\phi'$, let again $\alpha \sqsubset_{\mathbb{L}} \phi @ S$, and let $I \in [\![S]\!]$ be any implementation (there exists one because of local consistency of S). If $F(k, \ell, \phi' @ t) = \top_{\mathbb{L}}$ for all $s_0 \overset{k}{\dashrightarrow}_S t$, then $\phi @ S = \sup \emptyset = \bot_{\mathbb{L}}$ and we are done. Otherwise let $s_0 \overset{k}{\dashrightarrow}_S t$ be such that $\phi @ S = F(k, \ell, \phi' @ t)$, which exists because S is compactly branching. Then $\alpha \sqsubset_{\mathbb{L}} F(k, \ell, \phi' @ t)$, so (assuming that $\phi' @ t \neq \bot_{\mathbb{L}}$) we have $\alpha'_k \sqsubset_{\mathbb{L}} \phi' @ t$ with $F(k, \ell, \alpha'_k) \sqsupset_{\mathbb{L}} \alpha$.

Let $J \in [\![t, S]\!]$ such that $\alpha'_k \sqsubset_{\mathbb{L}} \phi' @ J$, let $n \in [\![k]\!]$ such that $F(n, \ell, \phi' @ J) = F(k, \ell, \phi' @ J)$, and add J together with a transition $i_0 \xrightarrow{n}_I j_0$ to I. Then

$$\begin{aligned} \phi @ I &= \sup\{F(m, \ell, \phi' @ n) \mid i_0 \xrightarrow{m}_I j\} \\ &\sqsupseteq_{\mathbb{L}} F(n, \ell, \phi' @ J) = F(k, \ell, \phi' @ J) \sqsupseteq_{\mathbb{L}} F(k, \ell, \alpha'_k) \sqsupset_{\mathbb{L}} \alpha. \end{aligned}$$

In case $\phi' @ t = \bot_{\mathbb{L}}$ instead, we again take an arbitrary $J \in [\![t, S]\!]$, and then $\phi @ I \sqsupseteq_{\mathbb{L}} F(k, \ell, \phi' @ t) \sqsupset_{\mathbb{L}} \alpha$. $\square$

7 Robust Semantics of Modal Event-Clock Specifications

As an application of the framework laid out in this paper, we consider the modal event-clock specifications (MECS) of [12–14] and give them a robust semantics as SMTS. We choose MECS instead of a more expressive real-time formalism such as *e.g.* timed automata [2] mainly for ease of exposition; it is certainly possible to extend the work presented here also to these formalisms.

Motivated by the real-time framework, we use the maximum-lead distance from Example 5 to measure quantitative satisfaction and refinement and intersection of timing constraints for label composition. The so-defined quantitative specification theory has a bounded parallel composition and a well-behaved quotient. Conjunction is relaxed bounded. We will see later that "relaxed" or "robust" semantics of MECS as introduced *e.g.* in [16, 33, 43, 44], though very different from each other, all are restrictions of our semantics.

7.1 Modal event-clock specifications

We assume a fixed finite alphabet Σ and let $\delta \notin \Sigma$ denote a special symbol which signifies passage of time. Let, as in Example 6, $\Phi(\Sigma)$ denote the set of closed clock constraints over Σ, given by

$$\Phi(\Sigma) \ni \phi ::= a \le k \mid a \ge k \mid \phi_1 \wedge \phi_2 \qquad (a \in \Sigma, k \in \mathbb{N}, \phi_1, \phi_2 \in \Phi(\Sigma))\,.$$

A (real) clock valuation is a mapping $u : \Sigma \to \mathbb{R}_{\ge 0}$; we say that $u \models \phi$, for $\phi \in \Phi(\Sigma)$, if $u(a)$ satisfies ϕ for all $a \in \Sigma$, and we let $[\![\phi]\!] = \{u : \Sigma \to \mathbb{R}_{\ge 0} \mid u \models \phi\}$. For $d \in \mathbb{R}_{\ge 0}$ and $b \in \Sigma$ we define the *delay* and *reset* valuations $u + d$ and $u[b]$ by

$$(u + d)(a) = u(a) + d, \qquad\qquad u[b](a) = \begin{cases} [c]0 & \text{if } a = b, \\ u(a) & \text{otherwise.} \end{cases}$$

The initial valuation is u_0 given by $u_0(a) = 0$ for all $a \in \Sigma$.

We denote by $\mathbb{J} = \{[x, y] \mid x \in \mathbb{R}_{\ge 0}, y \in \mathbb{R}_{\ge 0} \cup \{\infty\}, x \le y\}$ the set of closed extended non-negative real intervals, and define addition of intervals, as before, by $[l, r] + [l', r'] = [l + l', r + r']$.

An *interval clock valuation* is a mapping $v : \Sigma \to \mathbb{J}$ associating with each symbol a a non-negative interval $v(a) = [l_a, r_a] \in \mathbb{J}$ of possible clock values. We say that $v \models \phi$, for $\phi \in \Phi(\Sigma)$, if there exists $u : \Sigma \to \mathbb{R}_{\ge 0}$ for which $u(a) \in v(a)$ for all $a \in \Sigma$ and $u \models \phi$. For $d \in \mathbb{J}$ and $b \in \Sigma$ we define the valuations $v + d$ and $v[b]$ by

$$(v + d)(a) = v(a) + [d, d], \qquad\qquad v[b](a) = \begin{cases} [c][0, 0] & \text{if } a = b, \\ u(a) & \text{otherwise.} \end{cases}$$

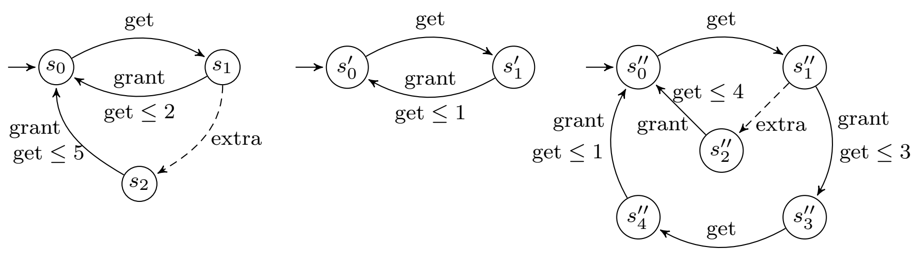
The initial valuation is v_0 given by $v_0(a) = [0, 0]$ for all $a \in \Sigma$.

Definition 10 A *modal event-clock specification* (MECS) is a tuple $A = (Q, q_0, \dashrightarrow_A, \longrightarrow_A)$ consisting of a finite set Q of locations, with initial location $q_0 \in Q$, and *may* and *must* edges $\dashrightarrow_A, \longrightarrow_A \subseteq Q \times \Sigma \times \Phi(\Sigma) \times Q$ which satisfy that for all $(q, a, g, q') \in \longrightarrow_A$ there exists $(q, a, g', q') \in \dashrightarrow_A$ with $[\![g]\!] \subseteq [\![g']\!]$.

As before we write $q \overset{a,g}{\dashrightarrow}_A q'$ instead of $(q, a, g, q') \in \dashrightarrow_A$, similarly for $\longrightarrow_A$. Figure 3 shows some examples of MECS.

To facilitate robust analysis of MECS, we give their semantics not as usual timed transition systems [2] (or as modal region automata as in [12]), but as *interval timed modal transition systems* (ITMTS). These are SMTS over

$$\mathsf{Spec} = (\Sigma \times \{[0, 0]\}) \cup (\{\delta\} \times \mathbb{J}) \subseteq (\Sigma \cup \{\delta\}) \times \mathbb{J},$$



S $\quad$ S' $\quad$ S''

Fig. 3 An MECS model S of a resource specification, *cf.* [12], and two refinement candidates S', S''. As customary, we omit *may* transitions which have an underlying *must* transition with the same label. Note that $S' \le_m S$ and $S'' \not\le_m S$, but $d_m(S'', S) = 1$.

with $(a, [l, r]) \sqsubseteq_{\mathsf{Spec}} (a', [l', r'])$ if and only if $a = a'$, $l \ge l'$, and $r \le r'$ (hence $[l, r] \subseteq [l', r']$ as in the examples), and thus with $\mathsf{Imp} = \Sigma \times \{0\} \cup \{\delta\} \times \mathbb{R}_{\ge 0}$. Hence an implementation is a usual timed transition system, with discrete transitions $s \xrightarrow{a,0} s'$ and delay transitions $s \xrightarrow{\delta,d} s'$.

Definition 11 The *semantics* of a MECS $A = (Q, q_0, \dashrightarrow_A, \longrightarrow_A)$ is the ITMTS $(\!|A|\!) = (S, s_0, \dashrightarrow_S, \longrightarrow_S)$ given as follows:

$$S = \{(q, v) \mid q \in Q, v : \Sigma \to \mathbb{J}\} \qquad\qquad s_0 = (q_0, v_0)$$

$$\begin{aligned}
\longrightarrow_S &= \{(q, v) \xrightarrow{a,0}_S (q', v') \mid q \xrightarrow{a,g}_A q', v \models g, v' = v[a]\} \\
&\qquad \cup \{(q, v) \xrightarrow{\delta,[l,r]}_S (q, v') \mid v' = v + [l, r]\} \\
\dashrightarrow_S &= \{(q, v) \overset{a,0}{\dashrightarrow}_S (q', v') \mid q \overset{a,g}{\dashrightarrow}_A q', v \models g, v' = v[a]\} \\
&\qquad \cup \{(q, v) \overset{\delta,[l,r]}{\dashrightarrow}_S (q, v') \mid v' = v + [l, r]\}
\end{aligned}$$

As we are using closed clock constraints for MECS, $(\!|A|\!)$ as defined above is compactly branching. Note that the "real", precise semantics of A as a timed transition system [2] is an implementation of $(\!|A|\!)$.

Refinement of MECS is defined semantically: $A \le_m B$ if $(\!|A|\!) \le_m (\!|B|\!)$. Note that the refinement of [12] is different (indeed it is not quantitative in our sense). By definition of modal refinement, a specification $S \le_m (\!|A|\!)$ is a *more precise*, or less relaxed, specification of the semantics of A: any delay intervals on transitions $s \overset{\delta,[l,r]}{\dashrightarrow}_S s'$ are contained in intervals $t \overset{\delta,[l',r']}{\dashrightarrow}_{(\!|A|\!)} t'$ (and similarly for *must* transitions).

7.2 Refinement distance

We are interested in *timing differences* of (refinements of) MECS, *i.e.* in expressing how much two ITMTS can differ in the timings of their behaviors. Given two finite traces $\sigma = (a_0, x_0), \dots, (a_n, x_n)$ and $\sigma' = (a_0, x'_0), \dots, (a_n, x'_n)$ (note that the discrete labels in $\Sigma \cup \{\delta\}$ are the same), their timing difference is $|(x_0 + x_1 + \dots + x_n) - (x'_0 + x'_1 + \dots + x'_n)|$, and what interests us is the *maximal* timing difference at any point of the runs. Hence we want the distance between σ and σ' to be $\max_{m=0,\dots,n} |\sum_{i=0}^m x_i - \sum_{i=0}^m x'_i|$, and with the $\max_{m=0,\dots,n}$ replaced by $\sup_{m\in\mathbb{N}}$ for infinite traces. This is precisely the *maximum-lead distance* of Example 5.

Note that the accumulating distance of [4] measures something entirely different: for the finite traces above, it is $|x_0 - x'_0| + \lambda|x_1 - x'_1| + \dots + \lambda^n |x_n - x'_n|$, hence measuring the sum of the differences in the individual timings of transitions rather than the overall timing difference. Thus the work laid out in [4] is not applicable to our setting, showing the strength of our more general approach.

Like in Example 5, we hence let $\mathbb{L} = (\mathbb{R}_{\ge 0} \cup \{\infty\})^{\mathbb{R}}$, the set of mappings from *leads* to distances, define $F : \mathsf{Imp} \times \mathsf{Imp} \times \mathbb{L} \to \mathbb{L}$ by

$$F((a,x),(a',x'),\alpha)(d) = \begin{cases} [c]\infty & \text{if } a \ne a' , \\ \max(|d+x-x'|, \alpha(d+x-x')) & \text{if } a = a' \end{cases}$$

and extend F to specifications by $F(k,\ell,\alpha) = \sup_{m\in[\![k]\!]} \inf_{n\in[\![\ell]\!]} F(m,n,\alpha)$. We also define $g : \mathbb{L} \to \mathbb{R}_{\ge 0} \cup \{\infty\}$ by $g(\alpha) = \alpha(0)$; the maximum-lead distance assuming the lead is zero.

We also instantiate our definitions of modal and thorough refinement distance for ITMTS; for MECS A, B we let $d_m(A,B) = d_m((\!|A|\!), (\!|B|\!))$, $d_t(A,B) = d_t((\!|A|\!), (\!|B|\!))$.

We already saw that in our special case, the notion of determinism from Definition 2 specializes to the condition, for all $s \in S$, that $s \overset{(a,[l_1,r_1])}{\dashrightarrow}_S s_1$ and $s \overset{(a,[l_2,r_2])}{\dashrightarrow}_S s_2$ imply $[l_1,r_1] = [l_2,r_2]$ and $s_1 = s_2$. For an MECS A, $(\!|A|\!)$ is hence deterministic if and only if for all locations q, $q \overset{a,g_1}{\dashrightarrow} q_1$ and $q \overset{a,g_2}{\dashrightarrow} q_2$ imply that $[\![g_1]\!] = [\![g_2]\!]$ and $q_1 = q_2$. This is a stronger notion of determinism than in [12]; we will call it *strong determinism* for differentiation.

7.3 Structural composition

For structural composition of ITMTS, the natural choice is to use CSP-style synchronization on discrete labels and *intersection* of intervals. As intervals signify timing constraints, composed intervals will then impose the conjunction of the timing constraints. Note that this is different from the synchronization used in Examples 1 to 3. Given $(a,[l,r]),(a',[l',r']) \in \mathsf{Spec}$ we hence define

$$(a,[l,r]) \oplus (a',[l',r']) = \begin{cases} (a, [\max(l,l'), \min(r,r')]) & \text{if } a = a', \max(l,l') \le \min(r,r'), \\ \text{undefined} & \text{otherwise.} \end{cases}$$

Lemma 5 *The operator $\oplus$ is bounded above by $P(\alpha,\alpha') = \max(\alpha,\alpha')$.*

Proof Let $k,k',\ell,\ell' \in \mathsf{Spec}$, $\alpha,\alpha' \in \mathbb{L}$ and $d \in \mathbb{R}$, and assume both $k \oplus k'$ and $\ell \oplus \ell'$ defined. Hence we can assume that the discrete parts of k, k', ℓ and ℓ' are all the same and ignore them from now on.

We need to show that

$$F(k \oplus k', \ell \oplus \ell', \max(\alpha,\alpha'))(d) \le \max(F(k,\ell,\alpha)(d), F(k',\ell',\alpha')(d)) .$$

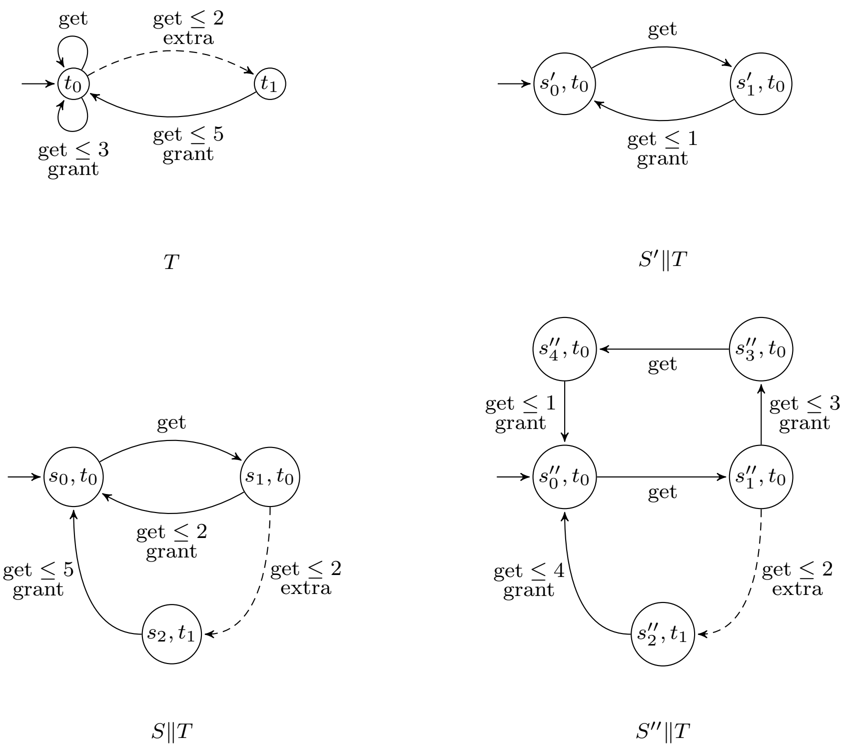


Fig. 4 A MECS model T of a process accessing the resource S from Figure 3, together with the structural compositions $S\|T$, $S'\|T$ and $S''\|T$. Note that $d_m(S''\|T, S\|T) = 1$.

Applying the definition of F, we see that this is equivalent to

$$\sup_{p\in[\![k\oplus k']\!]} \inf_{q\in[\![\ell\oplus\ell']\!]} \max(|d+p-q|, \max(\alpha(d+p-q), \alpha'(d+p-q)))$$
$$\le \max\begin{cases} \sup\limits_{m\in[\![k]\!]} \inf\limits_{n\in[\![\ell]\!]} \max(|d+m-n|, \alpha(d+m-n)) \\ \sup\limits_{m'\in[\![k']\!]} \inf\limits_{n'\in[\![\ell']\!]} \max(|d+m'-n'|, \alpha'(d+m'-n')); \end{cases}$$

note that we are abusing notation by identifying *e.g.* $p=(a,x)$ with x. This inequality in turn is equivalent to

$$\max\begin{cases} \sup\limits_{p\in[\![k\oplus k']\!]} \inf\limits_{q\in[\![\ell\oplus\ell']\!]} |d+p-q| \\ \sup\limits_{p\in[\![k\oplus k']\!]} \inf\limits_{q\in[\![\ell\oplus\ell']\!]} \alpha(d+p-q) \\ \sup\limits_{p\in[\![k\oplus k']\!]} \inf\limits_{q\in[\![\ell\oplus\ell']\!]} \alpha'(d+p-q) \end{cases} \le \max\begin{cases} \sup\limits_{m\in[\![k]\!]} \inf\limits_{n\in[\![\ell]\!]} |d+m-n| \\ \sup\limits_{m\in[\![k]\!]} \inf\limits_{n\in[\![\ell]\!]} \alpha(d+m-n) \\ \sup\limits_{m'\in[\![k']\!]} \inf\limits_{n'\in[\![\ell']\!]} |d+m'-n'| \\ \sup\limits_{m'\in[\![k']\!]} \inf\limits_{n'\in[\![\ell']\!]} \alpha'(d+m'-n'). \end{cases}$$

In this expression, the first line on the left-hand side is bounded by the right-hand side's first line, the second line on the left by the second line on the right, and the

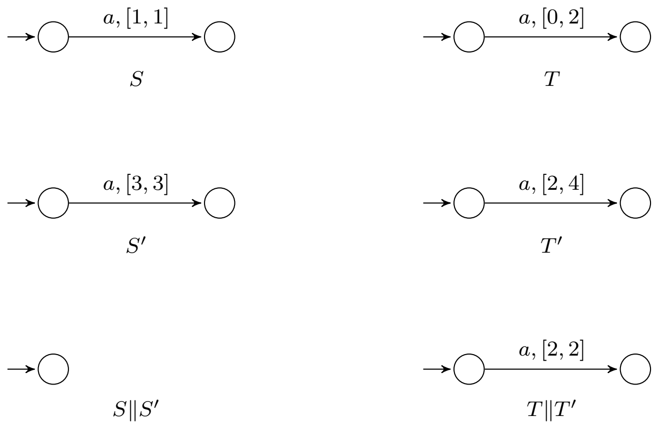


Fig. 5 Discrete failure in independent implementability. We have $d_m(S,T) = d_m(S',T') = \bot_{\mathbb{L}}$, but $d_m(S\|S', T\|T') = \top_{\mathbb{L}}$.

left-hand side's last line by the last line of the right-hand side, so that altogether, it holds. □

The notion of structural composition of ITMTS we obtain is consistent with the one of synchronized product of [12] (denoted $\otimes$ in that paper). Figure 4 depicts some examples of structural compositions.

Theorem 8 *Let A, B, A' and B' be MECS. With $\|$ the notion of synchronized product of MECS from [12], $(\!|A\|B|\!) \equiv_m (\!|A|\!)\|(\!|B|\!)$. Additionally, if $\tilde{d}_m(A\|A', B\|B') \neq \infty$, then $\tilde{d}_m(A\|A', B\|B') \le \max(\tilde{d}_m(A,B), \tilde{d}_m(A',B'))$.*

Proof $(\!|A\|B|\!) \equiv_m (\!|A|\!)\|(\!|B|\!)$ is clear from the definitions, and the second part follows directly from Theorem 2. □

We finish the section by a remark on the condition $\tilde{d}_m(A\|A', B\|B') \neq \infty$ in Theorem 8. As the proof of Theorem 2 shows, this is necessary to guard for what one may call *discrete failures*, where synchronized transitions may fail to exist due to incompatible timing constraints. The example in Figure 5 shows such a failure. When there are no such discrete failures, structural composition is bounded.

7.4 Quotient

For quotient of ITMTS we define, for labels $(a,[l,r]), (a',[l',r']) \in \mathsf{Spec}$,

$$(a',[l',r']) \oslash (a,[l,r]) = \begin{cases} \text{undefined} & \text{if } a \neq a'\,, \\ (a,[l',\infty]) & \text{if } a = a' \text{ and } l < l' \le r \le r'\,, \\ (a,[l',r']) & \text{if } a = a' \text{ and } l < l' \le r' < r\,, \\ \text{undefined} & \text{if } a = a' \text{ and } l \le r < l' \le r'\,, \\ (a,[0,\infty]) & \text{if } a = a' \text{ and } l' \le l \le r \le r'\,, \\ (a,[0,r']) & \text{if } a = a' \text{ and } l' \le l \le r < r'\,, \\ \text{undefined} & \text{if } a = a' \text{ and } l' \le r' < l \le r\,. \end{cases}$$

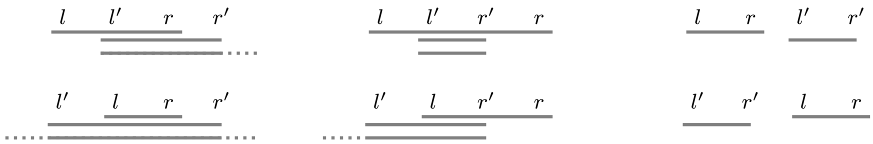


Fig. 6 Quotient $[l', r'] \oslash [l, r]$ of intervals, six cases. Top bar: $[l, r]$; middle bar: $[l', r']$; bottom bar: quotient. Note that for the two cases on the right, quotient is undefined.

The intuition is that to obtain the maximal solution $[p, q]$ to an equation $[l, r] \oplus [p, q] \sqsubseteq_{\mathsf{Spec}} [l', r']$, whether p and q must restrain the interval in the intersection, or can be 0 and ∞, respectively, depends on the position of $[l, r]$ relative to $[l', r']$, *cf.* Figure 6.

Lemma 6 *The operator $\oslash$ is quantitatively well-behaved.*

Proof We need to show that for all $k, \ell, m \in \mathsf{Spec}$, $\alpha \in \mathbb{L}$ and $d \in \mathbb{R}$, $F(m, \ell \ominus k, \alpha)(d) \geq F(k \oplus m, \ell, \alpha)(d)$. The proof is somewhat complicated by the large number of cases due to different placement of the intervals in k, ℓ and m, so, denoting the left and right interval bounds in k by k^- and k^+ (similarly for ℓ and m), we only show the case where $\ell^- \leq k^- \leq \ell^+ \leq m^- \leq k^+ \leq m^+$. In this case, the assertion that $F(m, \ell \ominus k, \alpha)(d) \geq F(k \oplus m, \ell, \alpha)(d)$ is equivalent to

$$\sup_{m^- \leq x \leq m^+} \inf_{y \leq \ell^+} \max(|d + x - y|, \alpha(d + x - y)) \geq \sup_{m^- \leq x \leq k^+} \inf_{\ell^- \leq y \leq \ell^+} \max(|d + x - y|, \alpha(d + x - y)),$$

which is clear as $m^- \leq x \leq k^+$ implies $m^- \leq x \leq m^+$. □

We can lift our quotient from the semantic ITMTS level to MECS as follows: A clock constraint in $\Phi(\Sigma)$ is equivalent to a mapping $\Sigma \to \mathbb{J}$, where $\mathbb{J} = \{[x, y] \mid x \in \mathbb{N}, y \in \mathbb{N} \cup \{\infty\}, x \leq y\} \subseteq \mathbb{J}$ denotes the set of closed extended non-negative integer intervals, and then we can define $\phi' \oslash \phi$ by $(\phi' \oslash \phi)(a) = \phi'(a) \oslash \phi(a)$ with $\oslash$ defined on intervals as above. Our quotient of MECS is then defined as in [12], but with their guard operation replaced by our $\oslash$ (hence our quotient is different from theirs, which is to be expected as the notions of refinement are different).

Theorem 9 *Let A, B, X be MECS for which $B \setminus\!\!\setminus A$ exists, then $(\!|B \setminus\!\!\setminus A|\!) \equiv (\!|B|\!) \setminus\!\!\setminus (\!|A|\!)$. If A is strongly deterministic, then $\tilde{d}_m(X, B \setminus\!\!\setminus A) \leq \tilde{d}_m(A \| X, B)$, and $X \leq_m B \setminus\!\!\setminus A$ if and only if $A \| X \leq_m B$.*

Proof $(\!|B \setminus\!\!\setminus A|\!) \equiv (\!|B|\!) \setminus\!\!\setminus (\!|A|\!)$ is clear from the definitions. For the second part, $X \leq_m B \setminus\!\!\setminus A$ if and only if $A \| X \leq_m B$ by Theorem 3, and by the same theorem, $d_m(X, B \setminus\!\!\setminus A) \sqsubseteq d_m(A \| X, B)$, so as $g : \mathbb{L} \to \mathbb{R}_{\geq 0} \cup \{\infty\}$ is a homomorphism, the claim follows. □

7.5 Conjunction

The conjunction operator on labels of ITMTS is defined using intersection of intervals like for structural composition, hence we let $k \owedge \ell = k \oplus \ell$ for $k, \ell \in \mathsf{Spec}$. The intuition is that transition intervals give constraints on timings; hence a transition in the conjunction has to satisfy both interval constraints. Like in Examples 1 to 3, it can be shown that $\owedge$ is *not* bounded.

Lemma 7 *The operator $\owedge$ is relaxed conjunctively bounded by $C(\alpha, \alpha') = \alpha + \alpha'$.*

Proof We use Lemma 4 and the constructions in its proof. We need to show that for all $\alpha, \alpha' \in \mathbb{L}$ and all $d \in \mathbb{R}$,

$$\begin{aligned} \sup_{l'' \le z \le r''} \inf_{r \le w \le l'} & \max(|d + z - w|, \alpha(d + z - w) + \alpha'(d + z - w)) \\ & \le \sup_{l'' \le z \le r''} \inf_{l \le x \le r} \max(|d + z - x|, \alpha(d + z - x)) \\ & \quad + \sup_{l'' \le z \le r''} \inf_{l' \le y \le r'} \max(|d + z - y|, \alpha'(d + z - y)) \end{aligned} \tag{5}$$

Now for all $z \in [l'', r'']$, we have

$$\inf_{r \le w \le l'} |d + z - w| \le \inf_{l \le x \le r} |d + z - x| + \inf_{l' \le y \le r'} |d + z - y|$$

and

$$\begin{aligned} \inf_{r \le w \le l'} & (\alpha(d + z - w) + \alpha'(d + z - w)) \\ & \le \inf_{l \le x \le r} \alpha(d + z - x) + \inf_{l' \le y \le r'} \alpha'(d + z - y); \end{aligned}$$

both can be shown by simply considering all cases of the placement of the infima. But then also

$$\begin{aligned} \max(& \inf_{r \le w \le l'} |d + z - w|, \inf_{r \le w \le l'} (\alpha(d + z - w) + \alpha'(d + z - w))) \\ & \le \max \begin{cases} \inf_{l \le x \le r} |d + z - x| + \inf_{l' \le y \le r'} |d + z - y| \\ \inf_{l \le x \le r} \alpha(d + z - x) + \inf_{l' \le y \le r'} \alpha'(d + z - y)) \end{cases} \\ & \le \max(\inf_{l \le x \le r} |d + z - x|, \inf_{l \le x \le r} \alpha(d + z - x)) \\ & \quad + \max(\inf_{l' \le y \le r'} |d + z - y|, \inf_{l' \le y \le r'} \alpha'(d + z - y)), \end{aligned}$$

the last inequality by distributivity of $+$ over max. As this holds for all z, we have proven (5). $\square$

Our notion of conjunction is consistent with the one for MECS in [12], and to make use of relaxed boundedness, we need to lift the notion of quantitative widening from the semantic ITMTS level to MECS. This is done by defining, for a clock constraint $\phi : \Sigma \to \mathbb{J}$ and $n \in \mathbb{N}$, the n-extended constraint ϕ_{+n} by $\phi_{+n}(a) = \phi(a) + [-n, n]$ (this is similar to a construction in [16]), and then saying that a MECS B is an n-widening of another MECS A if there is a relation $R \subseteq Q_A \times Q_B$ for which $(q_0^A, q_0^B) \in R$, and for all $(q_A, q_B) \in R$, $q_A \overset{a,g}{\dashrightarrow}_A q'_A$ if and only if $q_B \overset{a,g_{+n}}{\dashrightarrow} q'_B$ with $(q_B, q'_B) \in R$ and similarly for *must* transitions.

Theorem 10 *Let A, B be MECS. With $\wedge$ the notion of greatest lower bound from [12], $(\!|A \wedge B|\!) \equiv (\!|A|\!) \wedge (\!|B|\!)$. If A or B is strongly deterministic and there is a MECS C for which $\tilde{d}_m(C, A) \neq \infty$ and $\tilde{d}_m(C, B) \neq \infty$, then there are an n-widening A' of A and an m-widening B' of B for which $A' \wedge B'$ is defined, and such that $\tilde{d}_m(C', A' \wedge B') \leq \tilde{d}_m(C', A) + \tilde{d}_m(C', B)$ for all MECS C'.*

Proof $(\!|A \wedge B|\!) \equiv (\!|A|\!) \wedge (\!|B|\!)$ by definition, and the second claim follows from Theorem 5 and the homomorphism property of $g : \mathbb{L} \to \mathbb{R}_{\geq 0} \cup \{\infty\}$. $\square$

8 Conclusion

This paper constitutes the first general and complete quantitative theory for modal specifications. We have shown not only how to introduce such a general quantitative framework, but also the general conditions one needs to impose on the interplay between the system distance and the operators such as composition and quotient for the quantitative theory to work properly.

Using [4, 5] and our final example of modal event-clock specifications, we have seen two different instantiations of the general framework, using different distances for measuring variations of systems and specifications and different operators for structural composition and quotient. Other applications of our framework, *e.g.* to hybrid systems, in programming languages or quantitative logics, will require other distances and other operators, but as shown in [27, 29], they all stay within the unifying framework introduced in this paper.

Acknowledgements The authors wish to thank Sebastian S. Bauer and Claus Thrane for numerous discussions on the subject of this work, and a number of anonymous referees for useful comments and improvements.

References

1. Charalambos D. Aliprantis and Kim C. Border. *Infinite Dimensional Analysis: A Hitchhiker's Guide*. Springer-Verlag, 2007.
2. Rajeev Alur and David Dill. A theory of timed automata. *Theoretical Computer Science*, 126(2):183–235, 1994.
3. Sebastian S. Bauer, Alexandre David, Rolf Hennicker, Kim G. Larsen, Axel Legay, Ulrik Nyman, and Andrzej Wąsowski. Moving from specifications to contracts in component-based design. In Juan de Lara and Andrea Zisman, editors, *FASE*, volume 7212 of *Lecture Notes in Computer Science*, pages 43–58. Springer-Verlag, 2012.
4. Sebastian S. Bauer, Uli Fahrenberg, Line Juhl, Kim G. Larsen, Axel Legay, and Claus Thrane. Quantitative refinement for weighted modal transition systems. In Filip Murlak and Piotr Sankowski, editors, *MFCS*, volume 6907 of *Lecture Notes in Computer Science*, pages 60–71. Springer-Verlag, 2011.
5. Sebastian S. Bauer, Uli Fahrenberg, Line Juhl, Kim G. Larsen, Axel Legay, and Claus Thrane. Weighted modal transition systems. *Formal Methods in System Design*, 42(2):193–220, 2013.
6. Sebastian S. Bauer, Uli Fahrenberg, Axel Legay, and Claus Thrane. General quantitative specification theories with modalities. In Edward A. Hirsch, Juhani Karhumäki, Arto Lepistö, and Michail Prilutskii, editors, *CSR*, volume 7353 of *Lecture Notes in Computer Science*, pages 18–30. Springer-Verlag, 2012.
7. Sebastian S. Bauer, Line Juhl, Kim G. Larsen, Axel Legay, and Jiří Srba. Extending modal transition systems with structured labels. *Mathematical Structures in Computer Science*, 22(4):581–617, 2012.

8. Sebastian S. Bauer, Line Juhl, Kim G. Larsen, Jiří Srba, and Axel Legay. A logic for accumulated-weight reasoning on multiweighted modal automata. In Tiziana Margaria, Zongyan Qiu, and Hongli Yang, editors, *TASE*, pages 77–84. IEEE, 2012.
9. Nikola Beneš, Ivana Černá, and Jan Křetínský. Modal transition systems: Composition and LTL model checking. In Tevfik Bultan and Pao-Ann Hsiung, editors, *ATVA*, volume 6996 of *Lecture Notes in Computer Science*, pages 228–242. Springer-Verlag, 2011.
10. Nikola Beneš, Jan Křetínský, Kim G. Larsen, Mikael H. Møller, and Jiří Srba. Dual-priced modal transition systems with time durations. In Nikolaj Bjørner and Andrei Voronkov, editors, *LPAR*, volume 7180 of *Lecture Notes in Computer Science*, pages 122–137. Springer-Verlag, 2012.
11. Nikola Beneš, Jan Křetínský, Kim G. Larsen, and Jiří Srba. On determinism in modal transition systems. *Theoretical Computer Science*, 410(41):4026–4043, 2009.
12. Nathalie Bertrand, Axel Legay, Sophie Pinchinat, and Jean-Baptiste Raclet. A compositional approach on modal specifications for timed systems. In Karin Breitman and Ana Cavalcanti, editors, *ICFEM*, volume 5885 of *Lecture Notes in Computer Science*, pages 679–697. Springer-Verlag, 2009.
13. Nathalie Bertrand, Axel Legay, Sophie Pinchinat, and Jean-Baptiste Raclet. Modal event-clock specifications for timed component-based design. *Science of Computer Programming*, 77(12):1212–1234, 2012.
14. Nathalie Bertrand, Sophie Pinchinat, and Jean-Baptiste Raclet. Refinement and consistency of timed modal specifications. In Adrian Horia Dediu, Armand-Mihai Ionescu, and Carlos Martín-Vide, editors, *LATA*, volume 5457 of *Lecture Notes in Computer Science*, pages 152–163. Springer-Verlag, 2009.
15. Patricia Bouyer, Uli Fahrenberg, Kim G. Larsen, and Nicolas Markey. Quantitative analysis of real-time systems using priced timed automata. *Communications of the ACM*, 54(9):78–87, 2011.
16. Patricia Bouyer, Kim G. Larsen, Nicolas Markey, Ocan Sankur, and Claus R. Thrane. Timed automata can always be made implementable. In Joost-Pieter Katoen and Barbara König, editors, *CONCUR*, volume 6901 of *Lecture Notes in Computer Science*, pages 76–91. Springer-Verlag, 2011.
17. Pavol Černý, Thomas A. Henzinger, and Arjun Radhakrishna. Simulation distances. In Paul Gastin and François Laroussinie, editors, *CONCUR*, volume 6269 of *Lecture Notes in Computer Science*, pages 253–268. Springer-Verlag, 2010.
18. Krishnendu Chatterjee, Laurent Doyen, and Thomas A. Henzinger. Quantitative languages. *ACM Transactions on Computational Logic*, 11(4), 2010.
19. Alexandre David, Kim G. Larsen, Axel Legay, Ulrik Nyman, and Andrzej Wąsowski. Timed I/O automata: a complete specification theory for real-time systems. In Karl Henrik Johansson and Wang Yi, editors, *HSCC*, pages 91–100. ACM, 2010.
20. Luca de Alfaro, Marco Faella, and Mariëlle Stoelinga. Linear and branching system metrics. *IEEE Transactions on Software Engineering*, 35(2):258–273, 2009.
21. Luca de Alfaro, Thomas A. Henzinger, and Rupak Majumdar. Discounting the future in systems theory. In Jos C. M. Baeten, Jan Karel Lenstra, Joachim Parrow, and Gerhard J. Woeginger, editors, *ICALP*, volume 2719 of *Lecture Notes in Computer Science*, pages 1022–1037. Springer-Verlag, 2003.
22. Josée Desharnais, François Laviolette, and Mathieu Tracol. Approximate analysis of probabilistic processes. In *QEST*, pages 264–273. IEEE Computer Society, 2008.
23. Laurent Doyen, Thomas A. Henzinger, Axel Legay, and Dejan Ničković. Robustness of sequential circuits. In Luís Gomes, Victor Khomenko, and João M. Fernandes, editors, *ACSD*, pages 77–84. IEEE Computer Society, 2010.
24. Andrzej Ehrenfeucht and Jan Mycielski. Positional strategies for mean payoff games. *International Journal of Game Theory*, 8:109–113, 1979.
25. Uli Fahrenberg, Line Juhl, Kim G. Larsen, and Jiří Srba. Energy games in multiweighted automata. In Antonio Cerone and Pekka Pihlajasaari, editors, *ICTAC*, volume 6916 of *Lecture Notes in Computer Science*, pages 95–115. Springer-Verlag, 2011.
26. Uli Fahrenberg and Axel Legay. A robust specification theory for modal event-clock automata. In Sebastian S. Bauer and Jean-Baptiste Raclet, editors, *FIT*, volume 87 of *Electronic Proceedings in Theoretical Computer Science*, pages 5–16, 2012.
27. Uli Fahrenberg, Axel Legay, and Claus Thrane. The quantitative linear-time–branching-time spectrum. In Supratik Chakraborty and Amit Kumar, editors, *FSTTCS*, volume 13 of *Leibniz International Proceedings in Informatics*, pages 103–114. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2011.

28. Uli Fahrenberg, Axel Legay, and Andrzej Wąsowski. Make a difference! (Semantically). In Jon Whittle, Tony Clark, and Thomas Kühne, editors, *MoDELS*, volume 6981 of *Lecture Notes in Computer Science*, pages 490–500. Springer-Verlag, 2011.
29. Uli Fahrenberg, Claus Thrane, and Kim G. Larsen. Distances for weighted transition systems: Games and properties. In Mieke Massink and Gethin Norman, editors, *QAPL*, volume 57 of *Electronic Proceedings in Theoretical Computer Science*, pages 134–147, 2011.
30. Patrice Godefroid, Michael Huth, and Radha Jagadeesan. Abstraction-based model checking using modal transition systems. In Kim G. Larsen and Mogens Nielsen, editors, *CONCUR*, volume 2154 of *Lecture Notes in Computer Science*, pages 426–440. Springer-Verlag, 2001.
31. Alexander Gruler, Martin Leucker, and Kathrin D. Scheidemann. Modeling and model checking software product lines. In Gilles Barthe and Frank S. de Boer, editors, *FMOODS*, volume 5051 of *Lecture Notes in Computer Science*, pages 113–131. Springer-Verlag, 2008.
32. Orna Grumberg, Martin Lange, Martin Leucker, and Sharon Shoham. Don't know in the μ-calculus. In Radhia Cousot, editor, *VMCAI*, volume 3385 of *Lecture Notes in Computer Science*, pages 233–249. Springer-Verlag, 2005.
33. Vineet Gupta, Thomas A. Henzinger, and Radha Jagadeesan. Robust timed automata. In Oded Maler, editor, *HART*, volume 1201 of *Lecture Notes in Computer Science*, pages 331–345. Springer-Verlag, 1997.
34. Thomas A. Henzinger, Rupak Majumdar, and Vinayak S. Prabhu. Quantifying similarities between timed systems. In Paul Pettersson and Wang Yi, editors, *FORMATS*, volume 3829 of *Lecture Notes in Computer Science*, pages 226–241. Springer-Verlag, 2005.
35. Line Juhl, Kim G. Larsen, and Jirí Srba. Modal transition systems with weight intervals. *Journal of Logic and Algebraic Programming*, 81(4):408–421, 2012.
36. Kim G. Larsen. Modal specifications. In Joseph Sifakis, editor, *Automatic Verification Methods for Finite State Systems*, volume 407 of *Lecture Notes in Computer Science*, pages 232–246. Springer-Verlag, 1989.
37. Kim G. Larsen, Uli Fahrenberg, and Claus Thrane. Metrics for weighted transition systems: Axiomatization and complexity. *Theoretical Computer Science*, 412(28):3358–3369, 2011.
38. Robin Milner. *Communication and Concurrency.* Prentice Hall, 1989.
39. James R. Munkres. *Topology.* Prentice Hall, 2000.
40. Ulrik Nyman. *Modal Transition Systems as the Basis for Interface Theories and Product Lines.* PhD thesis, Aalborg University, September 2008.
41. David M. R. Park. Concurrency and automata on infinite sequences. In *Theoretical Computer Science*, volume 104 of *Lecture Notes in Computer Science*, pages 167–183. Springer-Verlag, 1981.
42. Jacob Illum Rasmussen, Kim G. Larsen, and K. Subramani. On using priced timed automata to achieve optimal scheduling. *Formal Methods in System Design*, 29(1):97–114, 2006.
43. Mani Swaminathan and Martin Fränzle. A symbolic decision procedure for robust safety of timed systems. In *TIME*, page 192. IEEE Computer Society, 2007.
44. Mani Swaminathan, Martin Fränzle, and Joost-Pieter Katoen. The surprising robustness of (closed) timed automata against clock-drift. In Giorgio Ausiello, Juhani Karhumäki, Giancarlo Mauri, and C.-H. Luke Ong, editors, *IFIP TCS*, volume 273 of *IFIP*, pages 537–553. Springer-Verlag, 2008.
45. Alfred Tarski. A lattice-theoretical fixpoint theorem and its applications. *Pacific Journal of Mathematics*, 5:285–309, 1955.
46. 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.
47. Franck van Breugel. A theory of metric labelled transition systems. *Annals of the New York Academy of Sciences*, 806(1):69–87, 1996.
48. Franck van Breugel. A behavioural pseudometric for metric labelled transition systems. In Martín Abadi and Luca de Alfaro, editors, *CONCUR*, volume 3653 of *Lecture Notes in Computer Science*, pages 141–155. Springer-Verlag, 2005.
49. Glynn Winskel and Mogens Nielsen. Models for concurrency. In Samson Abramsky, Dov M. Gabbay, and Thomas S.E. Maibaum, editors, *Handbook of Logic in Computer Science*, volume 4, pages 1–148. Clarendon Press, Oxford, 1995.
50. Uri Zwick and Michael Paterson. The complexity of mean payoff games. In *Computing and Combinatorics*, volume 959 of *Lecture Notes in Computer Science*, pages 1–10. Springer-Verlag, 1995.