Compositionality for Quantitative Specifications

Uli Fahrenberg, Jan Křetínský, Axel Legay, Louis-Marie Traonouez

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

Compositionality for Quantitative Specifications

Uli Fahrenberg · Jan Křetínský · Axel Legay · Louis-Marie Traonouez

the date of receipt and acceptance should be inserted later

Abstract We provide a framework for compositional and iterative design and verification of systems with quantitative information, such as rewards, time or energy. It is based on disjunctive modal transition systems where we allow actions to bear various types of quantitative information. Throughout the design process the actions can be further refined and the information made more precise. We show how to compute the results of standard operations on the systems, including the quotient (residual), which has not been previously considered for quantitative non-deterministic systems. Our quantitative framework has close connections to the modal nu-calculus and is compositional with respect to general notions of distances between systems and the standard operations.

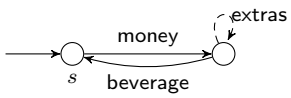

Fig. 1 Specification of a simple vending machine

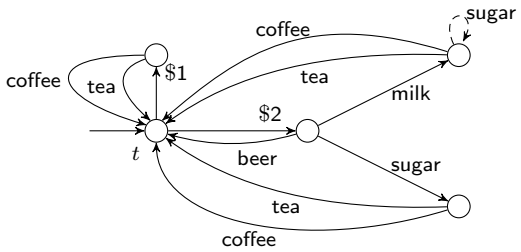

Fig. 2 Specification of another vending machine

1 Introduction

Specifications of systems come in two main flavors. *Logical* specifications are formalized as formulae of modal or temporal logics, such as the modal μ-calculus or LTL. A common way to verify them on a system is to translate them to automata and then analyze the composition of the system and the automaton. In contrast, in the *behavioral* approach, specifications are given, from the very beginning, in an automata-like formalism. Such properties can be verified using various equivalences and preorders, such as bisimilarity or refinement. Here we focus on the latter approach, but also show connections between the two.

Behavioral formalisms are particularly apt for component-based design. Indeed, specifications can be easily composed as well as separately refined into more concrete ones. The behavioral formalisms we work with here are *modal transition systems* (MTS) [46] and their extensions. MTS are like automata, but with two types of transitions: *must*-transitions represent behavior that has to be present in every implementation; *may*-transitions represent behavior that is allowed, but not required to be implemented.

A simple example of a vending machine specification, in Fig. 1, describes that any correct implementation must be ready to accept money, then may offer the customer to choose extras and must issue a beverage. While the must-transitions are preserved in the refinement process, the may-transitions can be either implemented and turned into must-transitions, or dropped.

This paper is based on the conference contribution [27] which has been presented at the 11th International Symposium on Formal Aspects of Component Software in Bertinoro, Italy.

Uli Fahrenberg · Axel Legay · Louis-Marie Traonouez
IRISA / Inria Rennes

Jan Křetínský
IST Austria

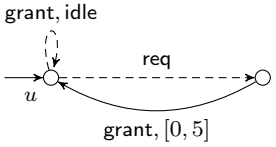

Fig. 3 A simple real-time specification

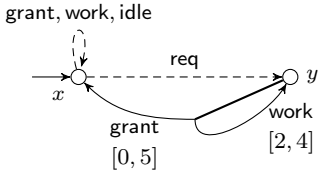

Fig. 4 A disjunctive modal transition system

$$\nu X.\Big([\mathsf{grant},\mathsf{idle},\mathsf{work}]X \wedge [\mathsf{req}]\nu Y.[\mathsf{idle},\mathsf{req}]\mathbf{ff} \wedge \big(\langle {}^{\mathsf{work}}_{[2,4]}\rangle Y \vee \langle {}^{\mathsf{grant}}_{[0,5]}\rangle X\big)\Big)$$

Fig. 5 The ν-calculus translation of the DMTS in Fig. 4

This low-level refinement process is, however, insufficient when the designer wants to get more specific about the implemented actions, such as going from the coarse specification just described to the more fine-grained specification of Fig. 2. In order to relate such specifications, MTS with *structured labels* have been introduced [5]. Given a preorder on labels, relating for instance coffee $\preccurlyeq$ beverage, we can refine a transition label into one which is below, for example implement "beverage" with its refinement "coffee".

This framework can be applied to various preorders. For example, one can use labels with a discrete component carrying the action information and an interval component to model time duration or energy consumption. As an example, consider the simple real-time property in Fig. 3: "after a req(uest), grant has to be executed within 5 time units without the process being idle meanwhile". The transition (grant, $[0,5]$) could be safely refined to (grant, $[l,r]$) for any $0 \le l \le r \le 5$.

We proceed to identify several shortcomings of the current approaches.

Expressive power. The current theory of structured labels [5, 30] is available only for the basic MTS. Very often one needs to use richer structures such as *disjunctive* MTS (DMTS) [10,47] or acceptance automata [34, 52]. While MTS generally cannot express disjunction of properties, DMTS and further related formalisms can and are, in fact, equivalent to the modal ν-calculus [8, 32].

This allows, for instance, to prohibit deadlocks as in the example in Fig. 4. The disjunctive must, depicted as a branching arrow, requires at least one of the transitions to be present. Thus we allow the deadline for grant to be reset if additional work is generated. Note that specifying grant and work as two separate must-transitions would not allow postponing the deadline; and two separate may-transitions would not guarantee any progress, as none of them has to be implemented. We hence propose *DMTS with structured labels* and also extend the equivalence between DMTS and the modal ν-calculus [8, 32] to our setting. Figure 5 shows a ν-calculus translation of the DMTS in Fig. 4.

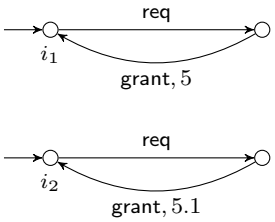

Fig. 6 Two implementations

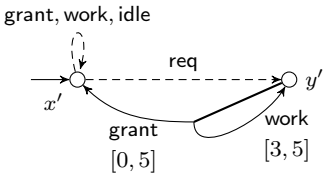

Fig. 7 Another DMTS specification

Robustness. Consider again the request-grant example in Fig. 4, together with the two labeled transition systems in Fig. 6. While i_1, issuing grant after precisely 5 time units, is a valid implementation of x, if there is but a small positive drift in the timing, like in i_2, it is not an implementation anymore. However, this drift might be easily mended or just might be due to measuring errors.

Therefore, when models and specifications contain such quantitative information, the standard Boolean notions of satisfaction and refinement are of limited utility [36, 55] and should be replaced by notions which are more robust to perturbations. For another example, the DMTS of Fig. 7 is *not* a refinement of the one in Fig. 4, but for all practical purposes, it is rather close.

One approach to robustness is to employ metric *distances* instead of Boolean relations; this has been done for example in [18–20, 25, 35, 45, 53, 54, 58, 59] and many other papers. An advantage of behavioral specification formalisms is that models and specifications are closely related, hence distances between models can easily be extended to distances between specifications. We have developed a distance-based approach for MTS in [4, 30] and shown in [29–31] that a good general setting is given

by recursively specified trace distances on an abstract quantale. Here we extend this to DMTS.

Compositionality. The framework should be compositional. In the quantitative setting, this in essence means that the operations we define on the systems should behave well with respect not only to satisfaction, but also to the distances. For instance, if s_1 is close to t_1 and s_2 close to t_2, then also the structural composition $s_1 \| s_2$ should be close to $t_1 \| t_2$. We prove this for the usual operations; in particular, we give a construction for such a well-behaved *quotient*.

The quotient of s by t is the most general specification that, when composed with t, refines s. This operation is thus useful for computing missing parts of a system to be implemented, when we already have several components at our disposal. The construction is complex already in the non-quantitative setting [8] and the extension of the algorithm to structured labels is non-trivial.

Our contribution. To sum up, we extend the framework of structured labels to DMTS and the modal ν-calculus. We equip this framework with distances and give constructions for the structured analogues of the standard operations, so that they behave compositionally with respect to the distances.

Further related work. Refinement of components is a frequently used design approach in various areas, ranging from subtyping [49] over the Java modeling language JML [38] or correct-by-design class diagram operations [26] to interface theories close to MTS such as interface automata [21] based on alternating simulation. A variant of alternating simulation called covariant-contravariant simulation has been compared to MTS modal refinement in [1]. The graphical representability of these variants was studied in [8, 12].

Quantitative specifications have been introduced in other settings. At first, the focus was on probabilities [37, 50, 51], but later, predicates with values in arbitrary metric spaces were also introduced [20]. Robustness of probabilistic specifications is considered in [18–20]. It is our hope that the close relationship between quantitative DMTS and the quantitative modal ν-calculus which we expose in this paper will aid in the development of theory and tools also for probabilistic specifications.

There are a number of extensions of MTS specifically designed for coping with real-time properties: the timed input-output specifications of [17], the timed interfaces of [22], and the modal event-clock specifications of [11]. Robustness for timed input-output specifications is considered in [43, 44, 56]. With only little extra work, our notions of distances and robustness can be applied to real-time specifications, see [28] for modal event-clock specifications.

Some other extensions of MTS have been developed for probabilistic properties: the constraint Markov chains of [13, 24, 39] and the abstract probabilistic automata of [13]. Distances for such specifications are used in [23], but no work on robustness is available.

2 Structured Labels

Let Σ be a poset with partial order $\preccurlyeq$. We think of $\preccurlyeq$ as *label refinement*, so that if $a \preccurlyeq b$, then a is less permissive (more restricted) than b.

We say that a label $a \in \Sigma$ is an *implementation label* if $b \preccurlyeq a$ implies $b = a$ for all $b \in \Sigma$, *i.e.*, if a cannot be further refined. The set of implementation labels is denoted Γ, and for $a \in \Sigma$, we let $[\![a]\!] = \{b \in \Gamma \mid b \preccurlyeq a\}$ denote the set of its implementations. Note that $a \preccurlyeq b$ implies $[\![a]\!] \subseteq [\![b]\!]$ for all $a, b \in \Sigma$.

Example 1 A trivial but important example of our label structure is the *discrete* one in which label refinement $\preccurlyeq$ is equality (and $\Gamma = \Sigma$). This is equivalent to the "standard" case of *unstructured* labels.

A typical label set in quantitative applications consists of a discrete component and real-valued weights. For specifications, weights are replaced by (closed) weight *intervals*, so that $\Sigma = U \times \{[l, r] \mid l \in \mathbb{R} \cup \{-\infty\}, r \in \mathbb{R} \cup \{\infty\}, l \leq r\}$ for a finite set U, *cf.* [4,5]. Label refinement is given by $(u_1, [l_1, r_1]) \preccurlyeq (u_2, [l_2, r_2])$ iff $u_1 = u_2$ and $[l_1, r_1] \subseteq [l_2, r_2]$, so that labels are more refined if they specify smaller intervals; thus, $\Gamma = U \times \{[x, x] \mid x \in \mathbb{R}\} \approx U \times \mathbb{R}$.

For a quite general setting, we can instead start with an arbitrary set Γ of implementation labels, let $\Sigma = 2^\Gamma$, the powerset, and $\preccurlyeq = \subseteq$ be subset inclusion. Then $[\![a]\!] = a$ for all $a \in \Sigma$. (Hence we identify implementation labels with one-element subsets of Σ.) □

2.1 Label operations

Specification theories come equipped with several standard operations that make compositional software design possible [3]: conjunction for merging viewpoints covering different system's aspects [7,57], structural composition for running components in parallel, and quotient to synthesize missing parts of systems [47]. In order to provide them for DMTS, we first need the respective atomic operations on their action labels.

We hence assume that Σ comes equipped with a partial conjunction, *i.e.*, an operator $\otimes : \Sigma \times \Sigma \rightharpoonup \Sigma$ for which it holds that

(1) if $a_1 \mathbin{⊘} a_2$ is defined, then $a_1 \mathbin{⊘} a_2 \preccurlyeq a_1$ and $a_1 \mathbin{⊘} a_2 \preccurlyeq a_2$, and
(2) if $a_3 \preccurlyeq a_1$ and $a_3 \preccurlyeq a_2$, then $a_1 \mathbin{⊘} a_2$ is defined and $a_3 \preccurlyeq a_1 \mathbin{⊘} a_2$.

Note that by these properties, any two partial conjunctions on Σ have to agree on elements for which they are both defined.

Example 2 For discrete labels, the unique conjunction operator is given by

$$a_1 \mathbin{⊘} a_2 = \begin{cases} a_1 & \text{if } a_1 = a_2\,, \\ \text{undef.} & \text{otherwise}\,. \end{cases}$$

Indeed, by property (2), $a_1 \mathbin{⊘} a_2$ must be defined for $a_1 = a_2$, and by (1), if $a_1 \mathbin{⊘} a_2 = a_3$ is defined, then $a_3 = a_1$ and $a_3 = a_2$.

For labels in $U \times \{[l, r] \mid l, r \in \mathbb{R}, l \le r\}$, the unique conjunction is

$$(u_1, [l_1, r_1]) \mathbin{⊘} (u_2, [l_2, r_2]) = \begin{cases} \text{undef.} & \text{if } u_1 \neq u_2 \text{ or } [l_1, r_1] \cap [l_2, r_2] = \emptyset\,, \\ (u_1, [l_1, r_1] \cap [l_2, r_2]) & \text{otherwise}\,. \end{cases}$$

To see uniqueness, let $a_i = (u_i, [l_i, r_i])$ for $i = 1, 2, 3$. Using property (2), we see that $a_1 \mathbin{⊘} a_2$ must be defined when $u_1 = u_2$ and $[l_1, r_1] \cap [l_2, r_2] \neq \emptyset$, and by (2), if $a_1 \mathbin{⊘} a_2 = a_3$ is defined, then $u_3 = u_1$ and $u_3 = u_2$, and $[l_3, r_3] \subseteq [l_1, r_1]$, $[l_3, r_3] \subseteq [l_2, r_2]$ imply $[l_1, r_1] \cap [l_2, r_2] \neq \emptyset$.

Finally, for the case of specification labels as sets of implementation labels, the unique conjunction is $a_1 \mathbin{⊘} a_2 = a_1 \cap a_2$. □

For structural composition and quotient of specifications, we assume a partial *label synchronization* operator $⊙ : \Sigma \times \Sigma \rightharpoonup \Sigma$ which specifies how to compose labels. We assume $⊙$ to be associative and commutative, with the following technical property which we shall need later: For all $a_1, a_2, b_1, b_2 \in \Sigma$ with $a_1 \preccurlyeq a_2$ and $b_1 \preccurlyeq b_2$, $a_1 ⊙ b_1$ is defined iff $a_2 ⊙ b_2$ is, and if both are defined, then $a_1 ⊙ b_1 \preccurlyeq a_2 ⊙ b_2$.

Example 3 For discrete labels, the conjunction of Example 2 is the same as CSP-style composition, *i.e.*, $a ⊙ b = a$ if $a = b$ and undefined otherwise, but other compositions can easily be defined.

For labels in $U \times \{[l, r] \mid l, r \in \mathbb{R}, l \le r\}$, several useful label synchronization operators may be defined for different applications. One is given by *addition* of intervals, *i.e.*,

$$(u_1, [l_1, r_1]) \overset{+}{⊙} (u_2, [l_2, r_2]) = \begin{cases} \text{undef.} & \text{if } u_1 \neq u_2\,, \\ (u_1, [l_1 + l_2, r_1 + r_2]) & \text{otherwise}\,, \end{cases}$$

for example modeling computation time of actions on a single processor. Another operator, useful in scheduling, uses maximum instead of addition:

$$(u_1, [l_1, r_1]) \overset{\max}{⊙} (u_2, [l_2, r_2]) = \begin{cases} \text{undef.} & \text{if } u_1 \neq u_2\,, \\ (u_1, [\max(l_1, l_2), \max(r_1, r_2)]) & \text{otherwise}\,. \end{cases}$$

For set-valued specification labels, we may take any synchronization operator $⊙$ given on implementation labels Γ and lift it to one on Σ by $a_1 ⊙ a_2 = \{b_1 ⊙ b_2 \mid b_1 \in [\![a_1]\!], b_2 \in [\![a_2]\!]\}$. □

3 Specification Formalisms

In this section we introduce the specification formalisms which we use in the rest of the paper. The universe of models for our specifications is the one of standard *labeled transition systems*. For simplicity of exposition, we work only with *finite* specifications and implementations, but most of our results extend to the infinite (but finitely branching) case.

A *labeled transition system* (LTS) is a structure $\mathcal{I} = (S, s^0, \longrightarrow)$ consisting of a finite set S of states, an initial state $s^0 \in S$, and a transition relation $\longrightarrow \subseteq S \times \Gamma \times S$. We usually write $s \xrightarrow{a} t$ instead of $(s, a, t) \in \longrightarrow$. Note that transitions are labeled with *implementation* labels.

3.1 Disjunctive Modal Transition Systems

A *disjunctive modal transition system* (DMTS) is a structure $\mathcal{D} = (S, S^0, \dashrightarrow, \longrightarrow)$ consisting of finite sets $S \supseteq S^0$ of states and initial states, respectively, may-transitions $\dashrightarrow \subseteq S \times \Sigma \times S$, and disjunctive must-transitions $\longrightarrow \subseteq S \times 2^{\Sigma \times S}$. It is assumed that for all $(s, N) \in \longrightarrow$ and $(a, t) \in N$ there is $(s, b, t) \in \dashrightarrow$ with $a \preccurlyeq b$.

Example 4 The specification x in Fig. 5 has a may-transition to y; from there we have a disjunctive must-transition with identical underlying may-transitions. The intuitive meaning of the transition, that either grant or work must be available, is formalized below using the modal refinement. □

Note that we allow multiple (or zero) initial states. We write $s \overset{a}{\dashrightarrow} t$ instead of $(s, a, t) \in \dashrightarrow$ and $s \longrightarrow N$ instead of $(s, N) \in \longrightarrow$. A DMTS $(S, S^0, \dashrightarrow, \longrightarrow)$ is an *implementation* if $\dashrightarrow \subseteq S \times \Gamma \times S$, $\longrightarrow = \{(s, \{(a, t)\}) \mid s \overset{a}{\dashrightarrow} t\}$, and $S^0 = \{s^0\}$ is a singleton; DMTS implementations are hence isomorphic to LTS.

DMTS were introduced in [47] in the context of equation solving, or *quotient* of specifications by processes and are used *e.g.*, in [10] for LTL model checking. They are a natural extension of *modal* transition systems [46], which are DMTS in which all disjunctive must-transitions $s \longrightarrow N$ lead to singletons $N = \{(a,t)\}$; in fact, DMTS are the closure of MTS under quotient [47].

We introduce a notion of modal refinement of DMTS with structured labels. For discrete labels, it coincides with the classical definition [47].

Definition 1 Let $\mathcal{D}_1 = (S_1, S_1^0, \dashrightarrow_1, \longrightarrow_1)$ and $\mathcal{D}_2 = (S_2, S_2^0, \dashrightarrow_2, \longrightarrow_2)$ be DMTS. A relation $R \subseteq S_1 \times S_2$ is a *modal refinement* if it holds for all $(s_1, s_2) \in R$ that

- for all $s_1 \overset{a_1}{\dashrightarrow}_1 t_1$ there is $s_2 \overset{a_2}{\dashrightarrow}_2 t_2$ such that $a_1 \preccurlyeq a_2$ and $(t_1, t_2) \in R$, and
- for all $s_2 \longrightarrow_2 N_2$ there is $s_1 \longrightarrow_1 N_1$ such that for all $(a_1, t_1) \in N_1$ there is $(a_2, t_2) \in N_2$ with $a_1 \preccurlyeq a_2$ and $(t_1, t_2) \in R$.

$\mathcal{D}_1$ *refines* $\mathcal{D}_2$, denoted $\mathcal{D}_1 \leq_{\mathsf{m}} \mathcal{D}_2$, if there exists an *initialized* modal refinement R, *i.e.*, one for which it holds that for every $s_1^0 \in S_1^0$ there is $s_2^0 \in S_2^0$ for which $(s_1^0, s_2^0) \in R$.

Note that this definition degrades to the one of [10, 47] for discrete labels (*cf.* Example 1).

We write $\mathcal{D}_1 \equiv_{\mathsf{m}} \mathcal{D}_2$ if $\mathcal{D}_1 \leq_{\mathsf{m}} \mathcal{D}_2$ and $\mathcal{D}_2 \leq_{\mathsf{m}} \mathcal{D}_1$. The *implementation semantics* of a DMTS $\mathcal{D}$ is $[\![\mathcal{D}]\!] = \{\mathcal{I} \leq_{\mathsf{m}} \mathcal{D} \mid \mathcal{I} \text{ implementation}\}$. This is, thus, the set of all LTS which satisfy the specification given by the DMTS $\mathcal{D}$. We say that $\mathcal{D}_1$ *thoroughly refines* $\mathcal{D}_2$, and write $\mathcal{D}_1 \leq_{\mathsf{th}} \mathcal{D}_2$, if $[\![\mathcal{D}_1]\!] \subseteq [\![\mathcal{D}_2]\!]$.

The below proposition, which follows directly from transitivity of modal refinement, shows that modal refinement is *sound* with respect to thorough refinement; in the context of specification theories, this is what one would expect. It can be shown that modal refinement is also *complete* for *deterministic* DMTS [9], but we will not need this here.

Proposition 1 *For all DMTS $\mathcal{D}_1$, $\mathcal{D}_2$, $\mathcal{D}_1 \leq_{\mathsf{m}} \mathcal{D}_2$ implies $\mathcal{D}_1 \leq_{\mathsf{th}} \mathcal{D}_2$.* □

3.2 Acceptance automata

A *non-deterministic acceptance automaton* (NAA) is a structure $\mathcal{A} = (S, S^0, \mathrm{Tran})$, with $S \supseteq S^0$ finite sets of states and initial states and $\mathrm{Tran} : S \to 2^{2^{\Sigma \times S}}$ an assignment of *transition constraints*. The intuition is that a transition constraint $\mathrm{Tran}(s) = \{M_1, \dots, M_n\}$ specifies a disjunction of n choices $M_1, \dots, M_n$ as to which transitions from s have to be implemented.

An NAA is an *implementation* if $S^0 = \{s^0\}$ is a singleton and it holds for all $s \in S$ that $\mathrm{Tran}(s) = \{M\} \subseteq 2^{\Gamma \times S}$ is a singleton; hence NAA implementations are isomorphic to LTS. Acceptance automata were first introduced in [52], based on the notion of acceptance trees in [34]; however, there they are restricted to be *deterministic*. We employ no such restriction here.

Let $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$ and $\mathcal{A}_2 = (S_2, S_2^0, \mathrm{Tran}_2)$ be NAA. A relation $R \subseteq S_1 \times S_2$ is a *modal refinement* if it holds for all $(s_1, s_2) \in R$ and all $M_1 \in \mathrm{Tran}_1(s_1)$ that there exists $M_2 \in \mathrm{Tran}_2(s_2)$ such that

$$\begin{aligned} &\forall (a_1, t_1) \in M_1 : \exists (a_2, t_2) \in M_2 : a_1 \preccurlyeq a_2, (t_1, t_2) \in R\,, \\ &\forall (a_2, t_2) \in M_2 : \exists (a_1, t_1) \in M_1 : a_1 \preccurlyeq a_2, (t_1, t_2) \in R\,. \end{aligned} \tag{1}$$

The definition reduces to the one of [52] in case labels are discrete. We will write $M_1 \preccurlyeq_R M_2$ if M_1, M_2, R satisfy (1).

In [8], translations were discovered between DMTS and NAA. For a DMTS $\mathcal{D} = (S, S^0, \dashrightarrow, \longrightarrow)$ and $s \in S$, let $\mathrm{Tran}(s) = \{M \subseteq \Sigma \times S \mid \forall (a,t) \in M : s \overset{a}{\dashrightarrow} t, \forall s \longrightarrow N : N \cap M \neq \emptyset\}$ and define the NAA $da(\mathcal{D}) = (S, S^0, \mathrm{Tran})$. For an NAA $\mathcal{A} = (S, S^0, \mathrm{Tran})$, define the DMTS $ad(\mathcal{A}) = (D, D^0, \dashrightarrow, \longrightarrow)$ by

$$\begin{aligned} D &= \{M \in \mathrm{Tran}(s) \mid s \in S\}\,, \\ D^0 &= \{M^0 \in \mathrm{Tran}(s^0) \mid s^0 \in S^0\}\,, \\ \longrightarrow &= \left\{\left(M, \{(a, M') \mid M' \in \mathrm{Tran}(t)\}\right) \;\middle|\; (a,t) \in M\right\}, \\ \dashrightarrow &= \{(M, a, M') \mid \exists M \longrightarrow N : (a, M') \in N\}\,. \end{aligned}$$

Similarly to a theorem of [8, 32], we can now show the following:

Theorem 1 *For all DMTS $\mathcal{D}_1$, $\mathcal{D}_2$ and NAA $\mathcal{A}_1$, $\mathcal{A}_2$, $\mathcal{D}_1 \leq_{\mathsf{m}} \mathcal{D}_2$ iff $da(\mathcal{D}_1) \leq_{\mathsf{m}} da(\mathcal{D}_2)$ and $\mathcal{A}_1 \leq_{\mathsf{m}} \mathcal{A}_2$ iff $ad(\mathcal{A}_1) \leq_{\mathsf{m}} ad(\mathcal{A}_2)$.* □

This structural equivalence will allow us to freely translate forth and back between DMTS and NAA in the rest of the paper. Note, however, that the state spaces of $\mathcal{A}$ and $ad(\mathcal{A})$ are not the same; the one of $ad(\mathcal{A})$ may be exponentially larger. [32] shows that this blow-up is unavoidable.

From a practical point of view, DMTS are a somewhat more useful specification formalism than NAA. This is because they are usually more compact and easily drawn and due to their close relation to the modal ν-calculus, see below.

3.3 The Modal ν-Calculus

In [8], translations were discovered between DMTS and the modal ν-calculus, and refining the translations in [32],

we could show that for discrete labels, these formalisms are *structurally equivalent*. We use the representation of the modal ν-calculus by equation systems in Hennessy-Milner logic developed in [42].

For a finite set X of variables, let $\mathcal{H}(X)$ be the set of *Hennessy-Milner formulae*, generated by the abstract syntax $\mathcal{H}(X) \ni \phi ::= \mathbf{tt} \mid \mathbf{ff} \mid x \mid \langle a\rangle\phi \mid [a]\phi \mid \phi \wedge \phi \mid \phi \vee \phi$, for $a \in \Sigma$ and $x \in X$. A *ν-calculus expression* is a structure $\mathcal{N} = (X, X^0, \Delta)$, with $X^0 \subseteq X$ sets of variables and $\Delta : X \to \mathcal{H}(X)$ a *declaration*.

We recall the greatest fixed point semantics of ν-calculus expressions from [42], but extend it to structured labels. Let $(S, S^0, \longrightarrow)$ be an LTS, then an *assignment* is a mapping $\sigma : X \to 2^S$. The set of assignments forms a complete lattice with order $\sigma_1 \sqsubseteq \sigma_2$ iff $\sigma_1(x) \subseteq \sigma_2(x)$ for all $x \in X$ and lowest upper bound $\big(\bigsqcup_{i\in I} \sigma_i\big)(x) = \bigcup_{i\in I} \sigma_i(x)$.

The semantics of a formula in $\mathcal{H}(X)$ is a function from assignments to subsets of S defined as follows: $(\!|\mathbf{tt}|\!)\sigma = S$, $(\!|\mathbf{ff}|\!)\sigma = \emptyset$, $(\!|x|\!)\sigma = \sigma(x)$, $(\!|\phi \wedge \psi|\!)\sigma = (\!|\phi|\!)\sigma \cap (\!|\psi|\!)\sigma$, $(\!|\phi \vee \psi|\!)\sigma = (\!|\phi|\!)\sigma \cup (\!|\psi|\!)\sigma$, and

$$(\!|\langle a\rangle\phi|\!)\sigma = \{s \in S \mid \exists s \xrightarrow{b} t : b \in [\![a]\!], t \in (\!|\phi|\!)\sigma\},$$

$$(\!|[a]\phi|\!)\sigma = \{s \in S \mid \forall s \xrightarrow{b} t : b \in [\![a]\!] \Longrightarrow t \in (\!|\phi|\!)\sigma\}.$$

The semantics of a declaration Δ is then the assignment defined by $(\!|\Delta|\!) = \bigsqcup\{\sigma : X \to 2^S \mid \forall x \in X : \sigma(x) \subseteq (\!|\Delta(x)|\!)\sigma\}$; the greatest (pre)fixed point of Δ.

An LTS $\mathcal{I} = (S, s^0, \longrightarrow)$ *implements* (or models) the expression $\mathcal{N}$, denoted $\mathcal{I} \models \mathcal{N}$, if there is $x^0 \in X^0$ such that $s^0 \in (\!|\Delta|\!)(x^0)$.

In [32] we have introduced another semantics for ν-calculus expressions, which is given by a notion of refinement, like for DMTS and NAA. For this we need a normal form for ν-calculus expressions:

Lemma 1 ([32]) *For any ν-calculus expression $\mathcal{N}_1 = (X_1, X_1^0, \Delta_1)$, there exists another $\mathcal{N}_2 = (X_2, X_2^0, \Delta_2)$ with $[\![\mathcal{N}_1]\!] = [\![\mathcal{N}_2]\!]$ and such that for any $x \in X$, $\Delta_2(x)$ is of the form*

$$\Delta_2(x) = \bigwedge_{i\in I} \Big(\bigvee_{j\in J_i} \langle a_{ij}\rangle x_{ij}\Big) \wedge \bigwedge_{a\in\Sigma} [a]\Big(\bigvee_{j\in J_a} y_{a,j}\Big)$$

for finite (possibly empty) index sets I, J_i, J_a and all $x_{ij}, y_{a,j} \in X_2$. □

As this is a type of *conjunctive normal form*, it is clear that translating a ν-calculus expression into normal form may incur an exponential blow-up. We introduce some notation for ν-calculus expressions in normal form. Let $\mathcal{N} = (X, X^0, \Delta)$ be such an expression and $x \in X$, with $\Delta(x) = \bigwedge_{i\in I} \big(\bigvee_{j\in J_i} \langle a_{ij}\rangle x_{ij}\big) \wedge \bigwedge_{a\in\Sigma} [a]\big(\bigvee_{j\in J_a} y_{a,j}\big)$ as in the lemma. Define $\Diamond(x) = \{\{(a_{ij}, x_{ij}) \mid j \in J_i\} \mid i \in I\}$ and, for each $a \in \Sigma$, $\Box^a(x) = \{y_{a,j} \mid j \in J_a\}$. Intuitively, $\Diamond(x)$ collects all $\langle a\rangle$-requirements from x, whereas $\Box^a(x)$ specifies the disjunction of $[a]$-properties which must hold from x. Note that now,

$$\Delta(x) = \bigwedge_{N\in\Diamond(x)} \Big(\bigvee_{(a,y)\in N} \langle a\rangle y\Big) \wedge \bigwedge_{a\in\Sigma} [a]\Big(\bigvee_{y\in\Box^a(x)} y\Big). \quad (2)$$

Let $\mathcal{N}_1 = (X_1, X_1^0, \Delta_1)$, $\mathcal{N}_2 = (X_2, X_2^0, \Delta_2)$ be ν-calculus expressions in normal form and $R \subseteq X_1 \times X_2$. The relation R is a *modal refinement* if it holds for all $(x_1, x_2) \in R$ that

- for all $a_1 \in \Sigma$ and $y_1 \in \Box_1^{a_1}(x_1)$ there is $a_2 \in \Sigma$ and $y_2 \in \Box_2^{a_2}(x_2)$ with $a_1 \preccurlyeq a_2$ and $(y_1, y_2) \in R$, and
- for all $N_2 \in \Diamond_2(x_2)$ there is $N_1 \in \Diamond_1(x_1)$ such that for all $(a_1, y_1) \in N_1$ there exists $(a_2, y_2) \in N_2$ with $a_1 \preccurlyeq a_2$ and $(y_1, y_2) \in R$.

We say that a ν-calculus expression (X, X^0, Δ) in normal form is an *implementation* if $X^0 = \{x^0\}$ is a singleton, $\Diamond(x) = \{\{(a, y)\} \mid y \in \Box^a(x), a \in \Sigma\}$ and $\Box^a(x) = \emptyset$ for all $a \notin \Gamma$, for all $x \in X$. We can translate a LTS $(S, S^0, \longrightarrow)$ to a ν-calculus expression (S, S^0, Δ) in normal form by setting $\Diamond(s) = \{\{(a, t)\} \mid s \xrightarrow{a} t\}$ and $\Box^a(s) = \{t \mid s \xrightarrow{a} t\}$ for all $s \in S$, $a \in \Sigma$. This defines a bijection between LTS and ν-calculus implementations, hence, like for DMTS and NAA, an embedding of LTS into ν-calculus.

One of the main results of [32] is that for discrete labels, the refinement semantics and the fixed point semantics of the modal ν-calculus agree; the proof can easily be extended to our case of structured labels:

Theorem 2 *For any LTS $\mathcal{I}$ and any ν-calculus expression $\mathcal{N}$ in normal form, $\mathcal{I} \models \mathcal{N}$ iff $\mathcal{I} \leq_{\mathsf{m}} \mathcal{N}$.* □

For a DMTS $\mathcal{D} = (S, S^0, \dashrightarrow, \longrightarrow)$ and all $s \in S$, let $\Diamond(s) = \{N \mid s \longrightarrow N\}$ and, for each $a \in \Sigma$, $\Box^a(s) = \{t \mid s \overset{a}{\dashrightarrow} t\}$. Define the (normal-form) ν-calculus expression $dn(\mathcal{D}) = (S, S^0, \Delta)$, with Δ given as in (2). For a ν-calculus expression $\mathcal{N} = (X, X^0, \Delta)$ in normal form, let $\dashrightarrow = \{(x, a, y) \in X \times \Sigma \times X \mid y \in \Box^a(x)\}$, $\longrightarrow = \{(x, N) \mid x \in X, N \in \Diamond(x)\}$ and define the DMTS $nd(\mathcal{N}) = (X, X^0, \dashrightarrow, \longrightarrow)$. Given that these translations are entirely syntactic, the following theorem is not a surprise:

Theorem 3 *For DMTS $\mathcal{D}_1$, $\mathcal{D}_2$ and ν-calculus expressions $\mathcal{N}_1$, $\mathcal{N}_2$, $\mathcal{D}_1 \leq_{\mathsf{m}} \mathcal{D}_2$ iff $dn(\mathcal{D}_1) \leq_{\mathsf{m}} dn(\mathcal{D}_2)$ and $\mathcal{N}_1 \leq_{\mathsf{m}} \mathcal{N}_2$ iff $nd(\mathcal{N}_1) \leq_{\mathsf{m}} nd(\mathcal{N}_2)$.* □

4 Specification theory

Structural specifications typically come equipped with operations which permit *compositional reasoning*, *viz.* conjunction, structural composition, and quotient, *cf.* [3].

On deterministic MTS, these operations can be given easily using simple structural operational rules (for such semantics of weighted systems, see for instance [40]). For non-deterministic specifications this is significantly harder; in [8] it is shown that DMTS and NAA permit these operations and, additionally but trivially, disjunction. Here we show how to extend these operations on non-deterministic systems to our quantitative setting with structured labels.

We remark that structural composition and quotient operators are well-known from some logics, such as, *e.g.*, linear [33] or spatial logic [14], and were extended to quite general contexts [15]. However, whereas these operators are part of the formal syntax in those logics, for us they are simply operations on logical expressions (or DMTS, or NAA). Consequently [32], structural composition is generally only a sound over-approximation of the semantic composition.

Given the equivalence of DMTS, NAA and the modal ν-calculus exposed in the previous section, we will often state properties for all three types of specifications at the same time, letting $\mathcal{S}$ stand for any of the three types.

4.1 Disjunction and conjunction

Disjunction of specifications is easily defined, as we allow for multiple initial states. For two DMTS $\mathcal{D}_1 = (S_1, S_1^0, \dashrightarrow_1, \longrightarrow_1)$ and $\mathcal{D}_2 = (S_2, S_2^0, \dashrightarrow_2, \longrightarrow_2)$, we can hence define $\mathcal{D}_1 \vee \mathcal{D}_2 = (S_1 \cup S_2, S_1^0 \cup S_2^0, \dashrightarrow_1 \cup \dashrightarrow_2, \longrightarrow_1 \cup \longrightarrow_2)$ (with all unions disjoint).

For conjunction, we let $\mathcal{D}_1 \wedge \mathcal{D}_2 = (S_1 \times S_2, S_1^0 \times S_2^0, \dashrightarrow, \longrightarrow)$, with

- $(s_1, s_2) \overset{a_1 \owedge a_2}{\dashrightarrow} (t_1, t_2)$ whenever $s_1 \overset{a_1}{\dashrightarrow}_1 t_1$, $s_2 \overset{a_2}{\dashrightarrow}_2 t_2$ and $a_1 \owedge a_2$ is defined,
- for all $s_1 \longrightarrow N_1$, $(s_1, s_2) \longrightarrow \{(a_1 \owedge a_2, (t_1, t_2)) \mid (a_1, t_1) \in N_1, s_2 \overset{a_2}{\dashrightarrow}_2 t_2, a_1 \owedge a_2 \text{ defined}\}$,
- for all $s_2 \longrightarrow N_2$, $(s_1, s_2) \longrightarrow \{(a_1 \owedge a_2, (t_1, t_2)) \mid (a_2, t_2) \in N_2, s_1 \overset{a_1}{\dashrightarrow}_1 t_1, a_1 \owedge a_2 \text{ defined}\}$.

Theorem 4 *For all specifications $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$,*

- *$\mathcal{S}_1 \vee \mathcal{S}_2 \leq_{\mathsf{m}} \mathcal{S}_3$ iff $\mathcal{S}_1 \leq_{\mathsf{m}} \mathcal{S}_3$ and $\mathcal{S}_2 \leq_{\mathsf{m}} \mathcal{S}_3$,*
- *$\mathcal{S}_1 \leq_{\mathsf{m}} \mathcal{S}_2 \wedge \mathcal{S}_3$ iff $\mathcal{S}_1 \leq_{\mathsf{m}} \mathcal{S}_2$ and $\mathcal{S}_1 \leq_{\mathsf{m}} \mathcal{S}_3$,*
- *$[\![\mathcal{S}_1 \vee \mathcal{S}_2]\!] = [\![\mathcal{S}_1]\!] \cup [\![\mathcal{S}_2]\!]$, and $[\![\mathcal{S}_1 \wedge \mathcal{S}_2]\!] = [\![\mathcal{S}_1]\!] \cap [\![\mathcal{S}_2]\!]$.*

Proof The proof that $\mathcal{S}_1 \vee \mathcal{S}_2 \leq_{\mathsf{m}} \mathcal{S}_3$ iff $\mathcal{S}_1 \leq_{\mathsf{m}} \mathcal{S}_3$ and $\mathcal{S}_2 \leq_{\mathsf{m}} \mathcal{S}_3$ is trivial: any modal refinement $R \subseteq (S_1 \cup S_2) \times S_3$ splits into two refinements $R_1 \subseteq S_1 \times S_3$, $R_2 \subseteq S_2 \times S_3$ and vice versa.

For the proof of the second claim, which we show for DMTS, we prove the back direction first. Let $R_2 \subseteq S_1 \times S_2$, $R_3 \subseteq S_1 \times S_3$ be initialized (DMTS) modal refinements and define $R = \{(s_1, (s_2, s_3)) \mid (s_1, s_2) \in R_2, (s_1, s_3) \in R_3\} \subseteq S_1 \times (S_2 \times S_3)$. Then R is initialized.

Now let $(s_1, (s_2, s_3)) \in R$, then $(s_1, s_2) \in R_2$ and $(s_1, s_3) \in R_3$. Assume that $s_1 \overset{a_1}{\dashrightarrow}_1 t_1$, then by $\mathcal{S}_1 \leq_{\mathsf{m}} \mathcal{S}_2$, we have $s_2 \overset{a_2}{\dashrightarrow}_2 t_2$ with $a_1 \preccurlyeq a_2$ and $(t_1, t_2) \in R_2$. Similarly, by $\mathcal{S}_1 \leq_{\mathsf{m}} \mathcal{S}_3$, we have $s_3 \overset{a_3}{\dashrightarrow}_3 t_3$ with $a_1 \preccurlyeq a_3$ and $(t_1, t_3) \in R_3$. But then also $a_1 \preccurlyeq a_2 \owedge a_3$ and $(t_1, (t_2, t_3)) \in R$, and $(s_2, s_3) \overset{a_2 \owedge a_3}{\dashrightarrow} (t_2, t_3)$ by definition.

Assume that $(s_2, s_3) \longrightarrow N$. Without loss of generality we can assume that there is $s_2 \longrightarrow_2 N_2$ such that $N = \{(a_2 \owedge a_3, (t_2, t_3)) \mid (a_2, t_2) \in N_2, s_3 \overset{a_3}{\dashrightarrow}_3 t_3\}$. By $S_1 \leq_{\mathsf{m}} S_2$, we have $s_1 \longrightarrow_1 N_1$ such that $\forall (a_1, t_1) \in N_1 : \exists (a_2, t_2) \in N_2 : a_1 \preccurlyeq a_2, (t_1, t_2) \in R_2$.

Let $(a_1, t_1) \in N_1$, then also $s_1 \overset{a_1}{\dashrightarrow}_1 t_1$, so by $S_1 \leq_{\mathsf{m}} S_3$, there is $s_3 \overset{a_3}{\dashrightarrow}_3 t_3$ with $a_1 \preccurlyeq a_3$ and $(t_1, t_3) \in R_3$. By the above, we also have $(a_2, t_2) \in N_2$ such that $a_1 \preccurlyeq a_2$ and $(t_1, t_2) \in R_2$, but then $(a_2 \owedge a_3, (t_2, t_3)) \in N$, $a_1 \preccurlyeq a_2 \wedge a_3$, and $(t_1, (t_2, t_3)) \in R$.

For the other direction of the second claim, let $R \subseteq S_1 \times (S_2 \times S_3)$ be an initialized (DMTS) modal refinement. We show that $S_1 \leq_{\mathsf{m}} S_2$, the proof of $S_1 \leq_{\mathsf{m}} S_3$ being entirely analogous. Define $R_2 = \{(s_1, s_2) \mid \exists s_3 \in S_3 : (s_1, (s_2, s_3)) \in R\} \subseteq S_1 \times S_2$, then R_2 is initialized.

Let $(s_1, s_2) \in R_2$, then we must have $s_3 \in S_3$ such that $(s_1, (s_2, s_3)) \in R$. Assume that $s_1 \overset{a_1}{\dashrightarrow}_1 t_1$, then also $(s_2, s_3) \overset{a}{\dashrightarrow} (t_2, t_3)$ for some a with $a_1 \preccurlyeq a$ and $(t_1, (t_2, t_3)) \in R$. By construction we have $s_2 \overset{a_2}{\dashrightarrow}_2 t_2$ and $s_3 \overset{a_3}{\dashrightarrow}_3 t_3$ such that $a = a_2 \owedge a_3$, but then $a_1 \preccurlyeq a_2 \owedge a_3 \preccurlyeq a_2$ and $(t_1, t_2) \in R_2$.

Assume that $s_2 \longrightarrow_2 N_2$, then by construction we have $(s_2, s_3) \longrightarrow N = \{(a_2 \owedge a_3, (t_2, t_3)) \mid (a_2, t_2) \in N_2, s_3 \overset{a_3}{\dashrightarrow}_3 t_3\}$. By $\mathcal{S}_1 \leq_{\mathsf{m}} \mathcal{S}_2 \wedge \mathcal{S}_3$, there is $s_1 \longrightarrow_1 N_1$ such that $\forall (a_1, t_1) \in N_1 : \exists (a, (t_2, t_3)) \in N : a_1 \preccurlyeq a, (t_1, (t_2, t_3)) \in R$.

Let $(a_1, t_1) \in N_1$, then we have $(a, (t_2, t_3)) \in N$ for which $a_1 \preccurlyeq a$ and $(t_1, (t_2, t_3)) \in R$. By construction of N, this implies that there are $(a_2, t_2) \in N_2$ and $s_3 \overset{a_3}{\dashrightarrow}_3 t_3$ such that $a = a_2 \owedge a_3$, but then $a_1 \preccurlyeq a_2 \owedge a_3 \preccurlyeq a_2$ and $(t_1, t_2) \in R$.

As to the last claims of the theorem, $[\![\mathcal{S}_1 \wedge \mathcal{S}_2]\!] = [\![\mathcal{S}_1]\!] \cap [\![\mathcal{S}_2]\!]$ is clear from what we just proved: for all implementations $\mathcal{I}$, $\mathcal{I} \leq_{\mathsf{m}} \mathcal{S}_1 \wedge \mathcal{S}_2$ iff $\mathcal{I} \leq_{\mathsf{m}} \mathcal{S}_1$ and $\mathcal{I} \leq_{\mathsf{m}} \mathcal{S}_2$. For the other part, it is clear by construction that for any implementation $\mathcal{I}$, any witness R for $\mathcal{I} \leq_{\mathsf{m}} \mathcal{S}_1$ is also a witness for $\mathcal{I} \leq_{\mathsf{m}} \mathcal{S}_1 \vee \mathcal{S}_2$, and similarly for $\mathcal{S}_2$, hence $[\![\mathcal{S}_1]\!] \cup [\![\mathcal{S}_2]\!] \subseteq [\![\mathcal{S}_1 \vee \mathcal{S}_2]\!]$.

To show that also $[\![\mathcal{S}_1]\!] \cup [\![\mathcal{S}_2]\!] \supseteq [\![\mathcal{S}_1 \vee \mathcal{S}_2]\!]$, we note that an initialized refinement R witnessing $\mathcal{I} \leq_{\mathsf{m}} \mathcal{S}_1 \vee \mathcal{S}_2$ must relate the initial state of $\mathcal{I}$ either to an initial state of $\mathcal{S}_1$ or to an initial state of $\mathcal{S}_2$. In the first case, and

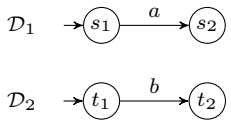

Fig. 8 Two simple DMTS

by disjointness, R witnesses $\mathcal{I} \leq_{\mathsf{m}} \mathcal{S}_1$, in the second, $\mathcal{I} \leq_{\mathsf{m}} \mathcal{S}_2$. □

With bottom and top elements given by $\bot = (\emptyset, \emptyset, \emptyset)$ and $\top = (\{s\}, \{s\}, \mathrm{Tran}_\top)$ with $\mathrm{Tran}_\top(s) = 2^{2^{\Sigma\times\{s\}}}$, our classes of specifications form *bounded distributive lattices* up to $\equiv_{\mathsf{m}}$.

4.2 Structural composition

For NAA $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$, $\mathcal{A}_2 = (S_2, S_2^0, \mathrm{Tran}_2)$, their *structural composition* is $\mathcal{A}_1 \| \mathcal{A}_2 = (S_1 \times S_2, S_1^0 \times S_2^0, \mathrm{Tran})$, with $\mathrm{Tran}((s_1, s_2)) = \{M_1 \oplus M_2 \mid M_1 \in \mathrm{Tran}_1(s_1), M_2 \in \mathrm{Tran}_2(s_2)\}$ for all $s_1 \in S_1$, $s_2 \in S_2$, where $M_1 \oplus M_2 = \{(a_1 \oplus a_2, (t_1, t_2)) \mid (a_1, t_1) \in M_1, (a_2, t_2) \in M_2, a_1 \oplus a_2 \text{ defined}\}$.

Remark a subtle difference between conjunction and structural composition, which we expose for discrete labels and CSP-style composition: for the DMTS $\mathcal{D}_1$, $\mathcal{D}_2$ shown in Fig. 8, both $\mathcal{D}_1 \wedge \mathcal{D}_2$ and $\mathcal{D}_1 \| \mathcal{D}_2$ have only one state, but $\mathrm{Tran}(s_1 \wedge t_1) = \emptyset$ and $\mathrm{Tran}(s_1 \| t_1) = \{\emptyset\}$, so that $\mathcal{D}_1 \wedge \mathcal{D}_2$ is inconsistent, whereas $\mathcal{D}_1 \| \mathcal{D}_2$ is not.

This definition extends the structural composition defined for modal transition systems, with structured labels, in [30]. For DMTS specifications (and hence also for ν-calculus expressions), the back translation from NAA to DMTS entails an exponential explosion.

Theorem 5 *Up to $\equiv_{\mathsf{m}}$, the operator $\|$ is associative, commutative and monotone.*

Proof Associativity and commutativity are clear by associativity and commutativity of $\oplus$. Monotonicity is equivalent to the assertion that (up to $\equiv_{\mathsf{m}}$) $\|$ distributes over the least upper bound $\vee$; one easily sees that for all specifications $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$, the identity is a two-sided modal refinement $\mathcal{S}_1 \| (\mathcal{S}_2 \vee \mathcal{S}_3) \equiv_{\mathsf{m}} \mathcal{S}_1 \| \mathcal{S}_2 \vee \mathcal{S}_1 \| \mathcal{S}_3$. □

Corollary 1 (Independent implementability) *For all specifications $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$, $\mathcal{S}_4$, $\mathcal{S}_1 \leq_{\mathsf{m}} \mathcal{S}_3$ and $\mathcal{S}_2 \leq_{\mathsf{m}} \mathcal{S}_4$ imply $\mathcal{S}_1 \| \mathcal{S}_2 \leq_{\mathsf{m}} \mathcal{S}_3 \| \mathcal{S}_4$.* □

4.3 Quotient

Because of non-determinism, we have to use a power set construction for the quotient, as opposed to conjunction and structural composition where product is sufficient.

For NAA $\mathcal{A}_3 = (S_3, S_3^0, \mathrm{Tran}_3)$, $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$, the quotient is $\mathcal{A}_3/\mathcal{A}_1 = (S, \{s^0\}, \mathrm{Tran})$, with $S = 2^{S_3 \times S_1}$ and $s^0 = \{(s_3^0, s_1^0) \mid s_3^0 \in S_3^0, s_1^0 \in S_1^0\}$. States in S will be written $\{s_3^1/s_1^1, \dots, s_3^n/s_1^n)\}$. Intuitively, this denotes that such state when composed with s_1^i conforms to s_3^i for each i; we call this *consistency* here.

We now define Tran. First, $\mathrm{Tran}(\emptyset) = 2^{\Sigma\times\{\emptyset\}}$, so $\emptyset$ is universal. For any other state $s = \{s_3^1/s_1^1, \dots, s_3^n/s_1^n\} \in S$, its set of *permissible labels* is defined by

$$pl(s) = \big\{a_2 \in \Sigma \;\big|\; \forall i = 1, \dots, n : \forall (a_1, t_1) \in\in \mathrm{Tran}_1(s_1^i) : \exists (a_3, t_3) \in\in \mathrm{Tran}_3(s_3^i) : a_1 \oplus a_2 \preccurlyeq a_3\big\},$$

that is, a label is permissible iff it cannot violate consistency. Here we use the notation $x \in\in z$ as a shortcut for $\exists y : x \in y \in z$.

Now for each $a \in pl(s)$ and each $i \in \{1, \dots, n\}$, let $\{t_1 \in S_1 \mid (a, t_1) \in\in \mathrm{Tran}_1(t_1^i)\} = \{t_1^{i,1}, \dots, t_1^{i,m_i}\}$ be an enumeration of all the possible states in S_1 after an a-transition. Then we define the set of all sets of possible assignments of next-a states from s_3^i to next-a states from s_1^i:

$$pt_a(s) = \big\{\{(t_3^{i,j}, t_1^{i,j}) \mid i = 1, \dots, n, j = 1, \dots, m_i\} \;\big|\; \forall i : \forall j : (a, t_3^{i,j}) \in\in \mathrm{Tran}_3(s_3^i)\big\}$$

These are all possible next-state assignments which preserve consistency. Now let $pt(s) = \bigcup_{a \in pl(s)} pt_a(s)$ and define

$$\mathrm{Tran}(s) = \big\{M \subseteq pt(s) \;\big|\; \forall i = 1, \dots, n : \forall M_1 \in \mathrm{Tran}_1(s_1^i) : \exists M_3 \in \mathrm{Tran}_3(s_3^i) : M \triangleright M_1 \preccurlyeq_R M_3\big\},$$

where $M \triangleright M_1 = \{(a_1 \oplus a, t_3^i) \mid (a, \{t_3^1/t_1^1, \dots, t_3^k/t_1^k)\}) \in M, (a_1, t_1^i) \in M_1\}$, to guarantee consistency no matter which element of $\mathrm{Tran}_1(s_1^i)$, s is composed with.

Example 5 Fig. 9 shows two simple specifications and their quotient under $\dot{\oplus}$, *i.e.*, using addition of intervals for label synchronization. Note that in order to have a finite representation of the quotient, we have to extend the label set to allow intervals which are not closed; for instance, the may-transition $(\mathsf{send},]1, \infty])$ from $\{s_0/t_0\}$ to $\emptyset$ comprises the fact that $pt_a(\{s_0/t_0\}) = \emptyset$ for all $a = (\mathsf{send}, [x, \infty])$ with $x > 1$. □

Theorem 6 *For all specifications $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$, $\mathcal{S}_1 \| \mathcal{S}_2 \leq_{\mathsf{m}} \mathcal{S}_3$ iff $\mathcal{S}_2 \leq_{\mathsf{m}} \mathcal{S}_3/\mathcal{S}_1$.*

Proof We show the proof for NAA; for DMTS and ν-calculus expressions it will follow through the translations. Let $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$, $\mathcal{A}_2 = (S_2, S_2^0, \mathrm{Tran}_2)$, $\mathcal{A}_3 = (S_3, S_3^0, \mathrm{Tran}_3)$; we show that $\mathcal{A}_1 \| \mathcal{A}_2 \leq_{\mathsf{m}} \mathcal{A}_3$ iff $\mathcal{A}_2 \leq_{\mathsf{m}} \mathcal{A}_3/\mathcal{A}_1$.

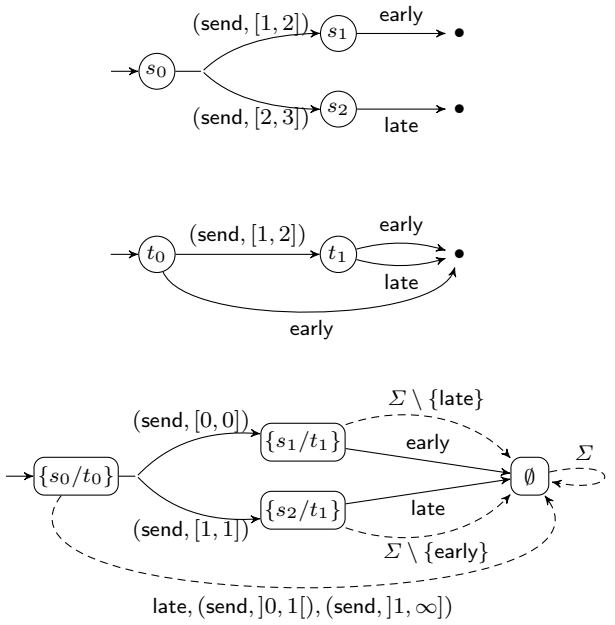

Fig. 9 Two DMTS (top and center) and their quotient (bottom)

We assume that the elements of $\mathrm{Tran}_1(s_1)$ are pairwise disjoint for each $s_1 \in S_1$; this can be achieved by, if necessary, splitting states.

First we note that by construction, $s \supseteq t$ implies $s \leq_{\mathsf{m}} t$ for all $s, t \in S$.

Assume that $\mathcal{A}_2 \leq_{\mathsf{m}} \mathcal{A}_3/\mathcal{A}_1$ and let $R = \{(s_1 \| s_2, s_3) \mid s_2 \leq_{\mathsf{m}} s_3/s_1\}$; we show that R is a witness for $\mathcal{A}_1 \| \mathcal{A}_2 \leq_{\mathsf{m}} \mathcal{A}_3$.

Let $(s_1 \| s_2, s_3) \in R$ and $M_\| \in \mathrm{Tran}_\|(s_1 \| s_2)$. Then $M_\| = M_1 \| M_2$ with $M_1 \in \mathrm{Tran}_1(s_1)$ and $M_2 \in \mathrm{Tran}_2(s_2)$. As $s_2 \leq_{\mathsf{m}} s_3/s_1$, we can pair M_2 with a set $M_/ \in \mathrm{Tran}_/(s_3/s_1)$, *i.e.*, such that the conditions in (1) are satisfied.

Let $M_3 = M_/ \triangleright M_1$. We show that (1) holds for the pair $M_\|, M_3$:

- Let $(a, t_1 \| t_2) \in M_\|$, then there are $a_1, a_2 \in \Sigma$ with $a = a_1 \oplus a_2$ and $(a_1, t_1) \in M_1$, $(a_2, t_2) \in M_2$. By (1), there is $(a_2', t) \in M_/$ such that $a_2 \preccurlyeq a_2'$ and $t_2 \leq_{\mathsf{m}} t$. Note that $a_3 = a_1 \oplus a_2'$ is defined and $a \preccurlyeq a_3$. Write $t = \{t_3^1/t_1^1, \ldots, t_3^n/t_1^n\}$. By construction, there is an index i for which $t_1^i = t_1$, hence $(a_3, t_3^i) \in M_3$. Also, $t \supseteq \{t_3^i/t_1^i\}$, hence $t_2 \leq_{\mathsf{m}} t_3^i/t_1^i$ and consequently $(t_1 \| t_2, t_3) \in R$.
- Let $(a_3, t_3) \in M_3$, then there are $(a_2', t) \in M_/$ and $(a_1, t_1) \in M_1$ such that $a_3 = a_1 \oplus a_2'$ and $t_3/t_1 \in t$. By (1), there is $(a_2, t_2) \in M_2$ for which $a_2 \preccurlyeq a_2'$ and $t_2 \leq_{\mathsf{m}} t$. Note that $a = a_1 \oplus a_2$ is defined and $a \preccurlyeq a_3$. Thus $(a, t_1 \| t_2) \in M_\|$, and by $t \supseteq \{t_3/t_1\}$, $t_2 \leq_{\mathsf{m}} t_3/t_1$.

Assume, for the other direction of the proof, that $\mathcal{A}_1 \| \mathcal{A}_2 \leq_{\mathsf{m}} \mathcal{A}_3$. Define $R \subseteq S_2 \times 2^{S_3 \times S_1}$ by

$$R = \big\{(s_2, \{s_3^1/s_1^1, \ldots, s_3^n/s_1^n\}) \;\big|\; \forall i = 1, \ldots, n : s_1^i \| s_2 \leq_{\mathsf{m}} s_3^i\big\};$$

we show that R is a witness for $\mathcal{A}_2 \leq_{\mathsf{m}} \mathcal{A}_3/\mathcal{A}_1$. Let $(s_2, s) \in R$, with $s = \{s_3^1/s_1^1, \ldots, s_3^n/s_1^n\}$, and $M_2 \in \mathrm{Tran}_2(s_2)$.

For every $i = 1, \ldots, n$, write the set $\mathrm{Tran}_1(s_1^i) = \{M_1^{i,1}, \ldots, M_1^{i,m_i}\}$. By assumption, $M_1^{i,j_1} \cap M_1^{i,j_2} = \emptyset$ for $j_1 \neq j_2$, hence every $(a_1, t_1) \in\in \mathrm{Tran}_1(s_1^i)$ is contained in a unique $M_1^{i,\delta_i(a_1,t_1)} \in \mathrm{Tran}_1(s_1^i)$.

For every $j = 1, \ldots, m_i$, let $M^{i,j} = M_1^{i,j} \| M_2 \in \mathrm{Tran}_\|(s_1^i \| s_2)$. By $s_1^i \| s_2 \leq_{\mathsf{m}} s_3^i$, we have $M_3^{i,j} \in \mathrm{Tran}_3(s_3^i)$ such that (1) holds for the pair $M^{i,j}, M_3^{i,j}$.

Now define

$$M = \big\{(a_2, t) \;\big|\; \exists (a_2, t_2) \in M_2 : \forall t_3/t_1 \in t : \exists i, a_1, a_3 : (a_1, t_1) \in\in \mathrm{Tran}_1(s_1^i), \; (a_3, t_3) \in M_3^{i,\delta_i(a_1,t_1)}, a_1 \oplus a_2 \preccurlyeq a_3, t_1 \| t_2 \leq_{\mathsf{m}} t_3\big\}. \tag{3}$$

We need to show that $M \in \mathrm{Tran}_/(s)$.

Let $i \in \{1, \ldots, n\}$ and $M_1^{i,j} \in \mathrm{Tran}_1(s_1^i)$; we claim that $M \triangleright M_1^{i,j} \preccurlyeq_R M_3^{i,j}$. Let $(a_3, t_3) \in M \triangleright M_1^{i,j}$, then $a_3 = a_1 \oplus a_2$ for some a_1, a_2 such that $t_3/t_1 \in t$, $(a_1, t_1) \in M_1^{i,j}$ and $(a_2, t) \in M$. By disjointness, $j = \delta_i(a_1, t_1)$, hence by definition of M, $(a_3, t_3) \in M_3^{i,j}$ as was to be shown.

For the reverse inclusion, let $(a_3, t_3) \in M_3^{i,j}$. By (1) and definition of $M^{i,j}$, there are $(a_1, t_1) \in M_1^{i,j}$ and $(a_2, t_2) \in M_2$ for which $a_1 \oplus a_2 \preccurlyeq a_3$ and $t_1 \| t_2 \leq_{\mathsf{m}} t_3$. Thus $j = \delta_i(a_1, t_1)$, so that there must be $(a_2, t) \in M$ for which $t_3/t_1 \in t$, but then also $(a_1 \oplus a_2, t_3) \in M \triangleright M_1^{i,j}$.

We show that $M_2 \preccurlyeq_R M$.

- Let $(a_2, t_2) \in M_2$. For every $i = 1, \ldots, n$ and every $(a_1, t_1) \in\in \mathrm{Tran}_1(t_1^i)$, we can use (1) to choose an element $(\eta_i(a_1, t_1), \tau_i(a_1, t_1)) \in M_3^{i,\delta_i(a_1,t_1)}$ for which $t_1 \| t_2 \leq_{\mathsf{m}} \tau_i(a_1, t_1)$ and $a_1 \oplus a_2 \preccurlyeq \eta_i(a_1, t_1)$. Let $t = \{\tau_i(a_1, t_1)/t_1 \mid i = 1, \ldots, n, (a_1, t_1) \in\in \mathrm{Tran}_1(t_1^i)\}$, then $(a_2, t) \in M$ and $(t_2, t) \in R$.
- Let $(a_2, t) \in M$, then we have $(a_2, t_2) \in M_2$ satisfying the conditions in (3). Hence $t_1 \| t_2 \leq_{\mathsf{m}} t_3$ for all $t_3/t_1 \in t$, so that $(t_2, t) \in R$. □

5 Robust Specification Theories

We proceed to lift the results of the previous sections to a *quantitative* setting, where the Boolean notions of modal and thorough refinement are replaced by refinement *distances*. We have shown in [29–31] that a

good setting for quantitative analysis is given by the one of *recursively specified trace distances* on an abstract commutative quantale as defined below; we refer to the above-cited papers for a detailed exposition of how this framework covers all common approaches to quantitative analysis.

Denote by $\Sigma^\infty = \Sigma^* \cup \Sigma^\omega$ the set of finite and infinite traces over Σ.

5.1 Recursively specified trace distances

Recall that a *(commutative) quantale* consists of a complete lattice $(\mathbb{L}, \sqsubseteq_\mathbb{L})$ and a commutative, associative addition operation $\oplus_\mathbb{L}$ which distributes over arbitrary suprema; we denote by $\bot_\mathbb{L}$, $\top_\mathbb{L}$ the bottom and top elements of $\mathbb{L}$. We call a function $d : X \times X \to \mathbb{L}$, for a set X and a quantale $\mathbb{L}$, an $\mathbb{L}$-*hemimetric* if it satisfies $d(x,x) = \bot_\mathbb{L}$ for all $x \in X$ and $d(x,z) \sqsubseteq_\mathbb{L} d(x,y) \oplus_\mathbb{L} d(y,z)$ for all $x,y,z \in X$.

$\mathbb{L}$-hemimetrics are generalizations of distances: for $\mathbb{L} = \mathbb{R}_{\geq 0} \cup \{\infty\}$ the extended real line, an $(\mathbb{R}_{\geq 0} \cup \{\infty\})$-hemimetric is simply an extended hemimetric, and a symmetric extended hemimetric which satisfies indiscernibility of identicals, *i.e.*, for which $d(x,y) = 0$ implies $x = y$, is an extended metric. (These are called "extended" because they can take on the value ∞; usually, only non-negative real values are allowed for a (hemi)metric, but adding ∞ does not change much and gives nicer algebraic properties, *cf.* [48].)

A *recursive trace distance specification* $(\mathbb{L}, \mathsf{eval}, d^\mathbb{L}_\mathsf{tr}, F)$ consists of a quantale $\mathbb{L}$, a quantale morphism $\mathsf{eval} : \mathbb{L} \to \mathbb{R}_{\geq 0} \cup \{\infty\}$, an $\mathbb{L}$-hemimetric $d^\mathbb{L}_\mathsf{tr} : \Sigma^\infty \times \Sigma^\infty \to \mathbb{L}$ (called *lifted trace distance*), and a *distance iterator* function $F : \Sigma \times \Sigma \times \mathbb{L} \to \mathbb{L}$. F must be monotone in the third and anti-monotone in the second coordinate and satisfy an extended triangle inequality: for all $a,b,c \in \Sigma$ and $\alpha, \beta \in \mathbb{L}$, $F(a,b,\alpha) \oplus_\mathbb{L} F(b,c,\beta) \sqsupseteq_\mathbb{L} F(a,c,\alpha \oplus_\mathbb{L} \beta)$.

F is to specify $d^\mathbb{L}_\mathsf{tr}$ recursively in the sense that for all $a,b \in \Sigma$ and all $\sigma, \tau \in \Sigma^\infty$ (and with "." denoting concatenation),

$$d^\mathbb{L}_\mathsf{tr}(a.\sigma, b.\tau) = F(a, b, d^\mathbb{L}_\mathsf{tr}(\sigma, \tau)) \,. \tag{4}$$

The *trace distance* associated with such a distance specification is $d_\mathsf{tr} : \Sigma^\infty \times \Sigma^\infty \to \mathbb{R}_{\geq 0}$ given by $d_\mathsf{tr} = \mathsf{eval} \circ d^\mathbb{L}_\mathsf{tr}$.

Note that $d^\mathbb{L}_\mathsf{tr}$ specializes to a distance on labels (because $\Sigma \subseteq \Sigma^\infty$); we require that this is compatible with label refinement in the sense that $a \preccurlyeq b$ implies $d^\mathbb{L}_\mathsf{tr}(a,b) = \bot_\mathbb{L}$. Then (4) implies that whenever $a \preccurlyeq b$, then $F(a,b,\bot_\mathbb{L}) = d^\mathbb{L}_\mathsf{tr}(a,b) = \bot_\mathbb{L}$. As an inverse property, we say that F is *recursively separating* if $F(a,b,\alpha) = \bot_\mathbb{L}$ implies that $a \preccurlyeq b$ and $\alpha = \bot_\mathbb{L}$.

Example 6 It is shown in [29–31] that all commonly used trace distances obey recursive characterizations as above. We give a few examples, all of which are recursively separating:

The *point-wise* distance from [19], for example, has $\mathbb{L} = \mathbb{R}_{\geq 0} \cup \{\infty\}$, $\mathsf{eval} = \mathsf{id}$ and

$$d^\mathbb{L}_\mathsf{tr}(a.\sigma, b.\tau) = \max(d(a,b), d^\mathbb{L}_\mathsf{tr}(\sigma,\tau)) \,,$$

where $d : \Sigma \times \Sigma \to \mathbb{R}_{\geq 0} \cup \{\infty\}$ is a hemimetric on labels. For the label set $\Sigma = U \times \{[l,r] \mid l \in \mathbb{R} \cup \{-\infty\}, r \in \mathbb{R} \cup \{\infty\}, l \leq r\}$ from Example 1, one useful example of such a hemimetric is $d((u_1,[l_1,r_1]),(u_2,[l_2,r_2])) = \sup_{x_1 \in [l_1,r_1]} \inf_{x_2 \in [l_2,r_2]} |x_1 - x_2| = \max(l_2 - l_1, r_1 - r_2, 0)$ if $u_1 = u_2$ and ∞ otherwise, *cf.* [4].

The *discounting* distance, also used in [19], again uses $\mathbb{L} = \mathbb{R}_{\geq 0} \cup \{\infty\}$ and $\mathsf{eval} = \mathsf{id}$, but

$$d^\mathbb{L}_\mathsf{tr}(a.\sigma, b.\tau) = d(a,b) + \lambda d^\mathbb{L}_\mathsf{tr}(\sigma,\tau)$$

for a constant $\lambda \in [0,1[$.

For the limit-average distance used in [59] and other papers, $\mathbb{L} = (\mathbb{R}_{\geq 0} \cup \{\infty\})^\mathbb{N}$, $\mathsf{eval}(\alpha) = \liminf_{j \in \mathbb{N}} \alpha(j)$, and

$$d^\mathbb{L}_\mathsf{tr}(a.\sigma, b.\tau)(j) = \tfrac{1}{j+1} d(a,b) + \tfrac{j}{j+1} d^\mathbb{L}_\mathsf{tr}(\sigma,\tau)(j-1) \,.$$

The *discrete* trace distance is given by $d_\mathsf{tr}(\sigma,\tau) = 0$ if $\sigma \preccurlyeq \tau$ and ∞ otherwise (here we have extended $\preccurlyeq$ to traces in the obvious way). It has a recursive characterization with $\mathbb{L} = \mathbb{R}_{\geq 0} \cup \{\infty\}$, $\mathsf{eval} = \mathsf{id}$, and $d_\mathsf{tr}(a.\sigma, b.\tau) = d_\mathsf{tr}(\sigma,\tau)$ if $a \preccurlyeq b$ and ∞ otherwise. □

For the rest of this paper, we fix a recursively specified trace distance.

5.2 Refinement distances

We lift the notions of modal refinement, for all our formalisms, to distances. Conceptually, this is done by replacing "∀" quantifiers by "sup" and "∃" by "inf" in the definitions, and then using the distance iterator to introduce a recursive functional whose least fixed point is the distance.

Definition 2 The *lifted refinement distance* on the states of DMTS $\mathcal{D}_1 = (S_1, S_1^0, \dashrightarrow_1, \longrightarrow_1)$ and $\mathcal{D}_2 = (S_2, S_2^0, \dashrightarrow_2, \longrightarrow_2)$ is the least fixed point to the equations

$$d^\mathbb{L}_\mathsf{m}(s_1,s_2) = \max \begin{cases} \sup\limits_{s_1 \overset{a_1}{\dashrightarrow} t_1} \inf\limits_{s_2 \overset{a_2}{\dashrightarrow} t_2} F(a_1,a_2,d^\mathbb{L}_\mathsf{m}(t_1,t_2)) \,, \\ \sup\limits_{s_2 \longrightarrow N_2} \inf\limits_{s_1 \longrightarrow N_1} \\ \qquad \sup\limits_{(a_1,t_1) \in N_1} \inf\limits_{(a_2,t_2) \in N_2} F(a_1,a_2,d^\mathbb{L}_\mathsf{m}(t_1,t_2)) \,. \end{cases}$$

for $s_1 \in S_1$, $s_2 \in S_2$. For NAA $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$, $\mathcal{A}_2 = (S_2, S_2^0, \mathrm{Tran}_2)$, the right-hand side is replaced by

$$\sup_{M_1 \in \mathrm{Tran}_1(s_1)} \inf_{M_2 \in \mathrm{Tran}_2(s_2)} \max \begin{cases} \sup\limits_{(a_1,t_1)\in M_1} \inf\limits_{(a_2,t_2)\in M_2} F(a_1, a_2, d_{\mathsf{m}}^{\mathbb{L}}(t_1, t_2)), \\ \sup\limits_{(a_2,t_2)\in M_2} \inf\limits_{(a_1,t_1)\in M_1} F(a_1, a_2, d_{\mathsf{m}}^{\mathbb{L}}(t_1, t_2)), \end{cases}$$

and for ν-calculus expressions $\mathcal{N}_1 = (X_1, X_1^0, \Delta_1), \mathcal{N}_2 = (X_2, X_2^0, \Delta_2)$ in normal form, it is

$$\max \begin{cases} \sup\limits_{a_1 \in \Sigma, y_1 \in \Box_1^{a_1}(x_1)} \inf\limits_{a_2 \in \Sigma, y_2 \in \Box_2^{a_2}(x_2)} F(a_1, a_2, d_{\mathsf{m}}^{\mathbb{L}}(y_1, y_2)), \\ \sup\limits_{N_2 \in \Diamond_2(x_2)} \inf\limits_{N_1 \in \Diamond_1(x_1)} \sup\limits_{(a_1,y_1)\in N_1} \inf\limits_{(a_2,y_2)\in N_2} F(a_1, a_2, d_{\mathsf{m}}^{\mathbb{L}}(y_1, y_2)). \end{cases}$$

Using Tarski's fixed point theorem, one easily sees that the lifted refinement distances are indeed well-defined. (Here one needs monotonicity of F in the third coordinate, together with the fact that sup and inf are monotonic.)

Note that we define the distances using *least* fixed points, as opposed to the *greatest* fixed point definition of standard refinement. Informally, this is because our order is reversed: we are not interested in maximizing refinement relations, but in *minimizing* refinement distance.

The lifted refinement distance between specifications is defined by

$$d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{S}_1, \mathcal{S}_2) = \sup_{s_1^0 \in S_1^0} \inf_{s_2^0 \in S_2^0} d_{\mathsf{m}}^{\mathbb{L}}(s_1^0, s_2^0).$$

Analogously to thorough refinement, there is also a *lifted thorough refinement distance*, given by $d_{\mathsf{th}}^{\mathbb{L}}(\mathcal{S}_1, \mathcal{S}_2) = \sup_{\mathcal{I}_1 \in [\![\mathcal{S}_1]\!]} \inf_{\mathcal{I}_2 \in [\![\mathcal{S}_2]\!]} d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{I}_1, \mathcal{I}_2)$.

Using the eval function, one gets distances $d_{\mathsf{m}} = \mathsf{eval} \circ d_{\mathsf{m}}^{\mathbb{L}}$ and $d_{\mathsf{th}} = \mathsf{eval} \circ d_{\mathsf{th}}^{\mathbb{L}}$, with values in $\mathbb{R}_{\geq 0} \cup \{\infty\}$, which will be the ones one is interested in for concrete applications.

Example 7 We compute the *discounting* refinement distance between the DMTS x and x' in Figs. 4 and 7 on page 2, assuming sup-inf distance on quantitative labels (see Example 6). We have

$$d_{\mathsf{m}}(x, x') = \max(0 + \lambda d_{\mathsf{m}}(x, x'), 0 + \lambda d_{\mathsf{m}}(y, y')),$$
$$d_{\mathsf{m}}(y, y') = \max(0 + \lambda d_{\mathsf{m}}(x, x'), 1 + \lambda d_{\mathsf{m}}(y, y')),$$

the least fixed point of which is seen to be $d_{\mathsf{m}}(x, x') = \frac{\lambda}{1-\lambda}$. Similarly, $d_{\mathsf{m}}(x', x) = \frac{\lambda}{1-\lambda}$. Note that $x \not\leq_{\mathsf{m}} x'$ and $x' \not\leq_{\mathsf{m}} x$. □

We recall the notion of *refinement family* from [30] and extend it to specifications. We give the definition for NAA only; for DMTS and the modal ν-calculus it is similar.

Definition 3 A *refinement family* from $\mathcal{A}_1$ to $\mathcal{A}_2$, for NAA $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$, $\mathcal{A}_2 = (S_2, S_2^0, \mathrm{Tran}_2)$, is an $\mathbb{L}$-indexed family of relations $R = \{R_\alpha \subseteq S_1 \times S_2 \mid \alpha \in \mathbb{L}\}$ with the property that for all $\alpha \in \mathbb{L}$ with $\alpha \neq \top_{\mathbb{L}}$, all $(s_1, s_2) \in R_\alpha$, and all $M_1 \in \mathrm{Tran}_1(s_1)$, there is $M_2 \in \mathrm{Tran}_2(s_2)$ such that

- $\forall (a_1, t_1) \in M_1 : \exists (a_2, t_2) \in M_2, \beta \in \mathbb{L} : (t_1, t_2) \in R_\beta, F(a_1, a_2, \beta) \sqsubseteq \alpha$,
- $\forall (a_2, t_2) \in M_2 : \exists (a_1, t_1) \in M_1, \beta \in \mathbb{L} : (t_1, t_2) \in R_\beta, F(a_1, a_2, \beta) \sqsubseteq \alpha$.

Lemma 2 *For all NAA $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$, $\mathcal{A}_2 = (S_2, S_2^0, \mathrm{Tran}_2)$, there exists a refinement family R from $\mathcal{A}_1$ to $\mathcal{A}_2$ such that for all $s_1^0 \in S_1^0$, there is $s_2^0 \in S_2^0$ for which $(s_1^0, s_2^0) \in R_{d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_1, \mathcal{A}_2)}$.*

We say that a refinement family as in the lemma *witnesses* $d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_1, \mathcal{A}_2)$.

Proof Define R by $R_\alpha = \{(s_1, s_2) \mid d_{\mathsf{m}}^{\mathbb{L}}(s_1, s_2) \sqsubseteq_{\mathbb{L}} \alpha\}$. First, as $(s_1^0, s_2^0) \in R_{d_{\mathsf{m}}^{\mathbb{L}}(s_1^0, s_2^0)}$ for all $s_1^0 \in S_1^0$, $s_2^0 \in S_2^0$, it is indeed the case that for all $s_1^0 \in S_1^0$, there is $s_2^0 \in S_2^0$ for which

$$(s_1^0, s_2^0) \in R_{d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_1, \mathcal{A}_2)} = R_{\max_{s_1^0 \in S_1^0} \min_{s_2^0 \in S_2^0} d_{\mathsf{m}}^{\mathbb{L}}(s_1^0, s_2^0)}.$$

Now let $\alpha \in \mathbb{L}$ with $\alpha \neq \top_{\mathbb{L}}$ and $(s_1, s_2) \in R_\alpha$. Let $M_1 \in \mathrm{Tran}_1(s_1)$. We have $d_{\mathsf{m}}^{\mathbb{L}}(s_1, s_2) \sqsubseteq_{\mathbb{L}} \alpha$, hence there is $M_2 \in \mathrm{Tran}_2(s_2)$ such that

$$\alpha \sqsupseteq_{\mathbb{L}} \max \begin{cases} \sup\limits_{(a_1,t_1)\in M_1} \inf\limits_{(a_2,t_2)\in M_2} F(a_1, a_2, d_{\mathsf{m}}^{\mathbb{L}}(t_1, t_2)), \\ \sup\limits_{(a_2,t_2)\in M_2} \inf\limits_{(a_1,t_1)\in M_1} F(a_1, a_2, d_{\mathsf{m}}^{\mathbb{L}}(t_1, t_2)). \end{cases}$$

But this entails that for all $(a_1, t_1) \in M_1$, there is $(a_2, t_2) \in M_2$ and $\beta = d_{\mathsf{m}}^{\mathbb{L}}(t_1, t_2)$ with $F(a_1, a_2, \beta) \sqsubseteq_{\mathbb{L}} \alpha$, and that for all $(a_2, t_2) \in M_2$, there is $(a_1, t_1) \in M_1$ and $\beta = d_{\mathsf{m}}^{\mathbb{L}}(t_1, t_2)$ such that $F(a_1, a_2, \beta) \sqsubseteq_{\mathbb{L}} \alpha$. □

The following quantitative extension of Theorems 1 and 3 shows that our translations preserve and reflect refinement distances. Its proof is rather long and tedious, hence we present it in a separate appendix to this paper.

Theorem 7 *For all DMTS $\mathcal{D}_1, \mathcal{D}_2$, all NAA $\mathcal{A}_1$, $\mathcal{A}_2$ and all ν-calculus expressions $\mathcal{N}_1$, $\mathcal{N}_2$:*

$$d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{D}_1, \mathcal{D}_2) = d_{\mathsf{m}}^{\mathbb{L}}(da(\mathcal{D}_1), da(\mathcal{D}_2))$$
$$d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_1, \mathcal{A}_2) = d_{\mathsf{m}}^{\mathbb{L}}(ad(\mathcal{A}_1), ad(\mathcal{A}_2))$$
$$d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{D}_1, \mathcal{D}_2) = d_{\mathsf{m}}^{\mathbb{L}}(dn(\mathcal{D}_1), dn(\mathcal{D}_2))$$
$$d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{N}_1, \mathcal{N}_2) = d_{\mathsf{m}}^{\mathbb{L}}(nd(\mathcal{N}_1), nd(\mathcal{N}_2))$$

5.3 Properties

We sum up some important properties of our distances.

Proposition 2 *For all specifications $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_1 \leq_{\mathsf{m}} \mathcal{S}_2$ implies $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{S}_1,\mathcal{S}_2) = \bot_{\mathbb{L}}$, and $\mathcal{S}_1 \leq_{\mathsf{th}} \mathcal{S}_2$ implies $d^{\mathbb{L}}_{\mathsf{th}}(\mathcal{S}_1,\mathcal{S}_2) = \bot_{\mathbb{L}}$. If F is recursively separating, then $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{S}_1,\mathcal{S}_2) = \bot_{\mathbb{L}}$ implies $\mathcal{S}_1 \leq_{\mathsf{m}} \mathcal{S}_2$.*

Proof We show the proposition for NAA. First, if $\mathcal{A}_1 \leq_{\mathsf{m}} \mathcal{A}_2$, with $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$, $\mathcal{A}_2 = (S_2, S_2^0, \mathrm{Tran}_2)$, then there is an initialized refinement relation $R \subseteq S_1 \times S_2$, *i.e.*, such that for all $(s_1,s_2) \in R$ and all $M_1 \in \mathrm{Tran}_1(s_1)$, there is $M_2 \in \mathrm{Tran}_2(s_2)$ for which

- $\forall (a_1,t_1) \in M_1 : \exists (a_2,t_2) \in M_2 : a_1 \preccurlyeq a_2, (t_1,t_2) \in R$ and
- $\forall (a_2,t_2) \in M_2 : \exists (a_1,t_1) \in M_1 : a_1 \preccurlyeq a_2, (t_1,t_2) \in R$.

Defining $R' = \{R'_\alpha \mid \alpha \in \mathbb{L}\}$ by $R'_\alpha = R$ for all $\alpha \in \mathbb{L}$, we see that R' is an initialized refinement family which witnesses $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_1,\mathcal{A}_2) = \bot_{\mathbb{L}}$.

We have shown that $\mathcal{A}_1 \leq_{\mathsf{m}} \mathcal{A}_2$ implies $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_1,\mathcal{A}_2) = \bot_{\mathbb{L}}$. Now if $\mathcal{A}_1 \leq_{\mathsf{th}} \mathcal{A}_2$ instead, then for all $\mathcal{I} \in [\![\mathcal{A}_1]\!]$, also $\mathcal{I} \in [\![\mathcal{A}_2]\!]$, hence $d^{\mathbb{L}}_{\mathsf{th}}(\mathcal{A}_1,\mathcal{A}_2) = \bot_{\mathbb{L}}$.

To show the last property, assume F to be recursively separating. Define $R \subseteq S_1 \times S_2$ by $R = \{(s_1,s_2) \mid d^{\mathbb{L}}_{\mathsf{m}}(s_1,s_2) = \bot_{\mathbb{L}}\}$; we show that R is a witness for $\mathcal{A}_1 \leq_{\mathsf{m}} \mathcal{A}_2$. By $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_1,\mathcal{A}_2) = \bot_{\mathbb{L}}$, R is initialized.

Let $(s_1,s_2) \in R$ and $M_1 \in \mathrm{Tran}_1(s_1)$, then there is $M_2 \in \mathrm{Tran}_2(s_2)$ such that

$$\begin{aligned}
&\forall (a_1,t_1) \in M_1 : \exists (a_2,t_2) \in M_2, \beta_1 \in \mathbb{L} : \\
&\qquad d^{\mathbb{L}}_{\mathsf{m}}(t_1,t_2) \sqsubseteq_{\mathbb{L}} \beta_1, F(a_1,a_2,\beta_1) = \bot_{\mathbb{L}} , \\
&\forall (a_2,t_2) \in M_2 : \exists (a_1,t_1) \in M_1, \beta_1 \in \mathbb{L} : \\
&\qquad d^{\mathbb{L}}_{\mathsf{m}}(t_1,t_2) \sqsubseteq_{\mathbb{L}} \beta_1, F(a_1,a_2,\beta_1) = \bot_{\mathbb{L}} .
\end{aligned}$$

As F is recursively separating, we must have $a_1 \preccurlyeq a_2$ in both these equations and $\beta_1 = \beta_2 = \bot_{\mathbb{L}}$. But then $(t_1,t_2) \in R$, hence R is indeed a witness for $\mathcal{A}_1 \leq_{\mathsf{m}} \mathcal{A}_2$. □

Proposition 3 *The functions $d^{\mathbb{L}}_{\mathsf{m}}$ and $d^{\mathbb{L}}_{\mathsf{th}}$ are $\mathbb{L}$-hemimetrics, and d_{m}, d_{th} are hemimetrics.*

Proof We show the proof for NAA. The properties that $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A},\mathcal{A}) = \bot_{\mathbb{L}}$ and $d^{\mathbb{L}}_{\mathsf{th}}(\mathcal{A},\mathcal{A}) = \bot_{\mathbb{L}}$ follow from proposition 2.

We show the triangle inequality for $d^{\mathbb{L}}_{\mathsf{m}}$. The triangle inequality for $d^{\mathbb{L}}_{\mathsf{th}}$ will then follow from standard arguments used to show that the Hausdorff metric satisfies the triangle inequality, see *e.g.*, [2, Lemma 3.72]. Let $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$, $\mathcal{A}_2 = (S_2, S_2^0, \mathrm{Tran}_2)$, $\mathcal{A}_3 = (S_3, S_3^0, \mathrm{Tran}_3)$ be NAA and $R^1 = \{R^1_\alpha \subseteq S_1 \times S_2 \mid \alpha \in \mathbb{L}\}$, $R^2 = \{R^2_\alpha \subseteq S_2 \times S_3 \mid \alpha \in \mathbb{L}\}$ refinement families such that $\forall s_1^0 \in S_1^0 : \exists s_2^0 \in S_2^0 : (s_1^0,s_2^0) \in R^1_{d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_1,\mathcal{A}_2)}$ and $\forall s_2^0 \in S_2^0 : \exists s_3^0 \in S_3^0 : (s_2^0,s_3^0) \in R^2_{d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_2,\mathcal{A}_3)}$.

Define $R = \{R_\alpha \subseteq S_1 \times S_3 \mid \alpha \in \mathbb{L}\}$ by

$$\begin{aligned}
R_\alpha = \big\{(s_1,s_3) \;\big|\; &\exists \alpha_1,\alpha_2 \in \mathbb{L}, s_2 \in S_2 : \\
&(s_1,s_2) \in R^1_{\alpha_1}, (s_2,s_3) \in R^2_{\alpha_2}, \alpha_1 \oplus_{\mathbb{L}} \alpha_2 = \alpha\big\} .
\end{aligned}$$

We see that for all $s_1^0 \in S_1^0$, there is $s_3^0 \in S_3^0$ such that $(s_1^0,s_3^0) \in R_{d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_1,\mathcal{A}_2) \oplus_{\mathbb{L}} d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_2,\mathcal{A}_3)}$; we show that R is a refinement family from $\mathcal{A}_1$ to $\mathcal{A}_2$.

Let $\alpha \in \mathbb{L}$ and $(s_1,s_3) \in R_\alpha$, then we have $\alpha_1,\alpha_2 \in \mathbb{L}$ and $s_2 \in S_2$ such that $\alpha_1 \oplus_{\mathbb{L}} \alpha_2 = \alpha$, $(s_1,s_2) \in R^1_{\alpha_1}$ and $(s_2,s_3) \in R^2_{\alpha_2}$. Let $M_1 \in \mathrm{Tran}_1(s_1)$, then we have $M_2 \in \mathrm{Tran}_2(s_2)$ such that

$$\begin{aligned}
&\forall (a_1,t_1) \in M_1 : \exists (a_2,t_2) \in M_2, \beta_1 \in \mathbb{L} : \\
&\qquad (t_1,t_2) \in R^1_{\beta_1}, F(a_1,a_2,\beta_1) \sqsubseteq_{\mathbb{L}} \alpha_1 , \qquad (5) \\
&\forall (a_2,t_2) \in M_2 : \exists (a_1,t_1) \in M_1, \beta_1 \in \mathbb{L} : \\
&\qquad (t_1,t_2) \in R^1_{\beta_1}, F(a_1,a_2,\beta_1) \sqsubseteq_{\mathbb{L}} \alpha_1 . \qquad (6)
\end{aligned}$$

This in turn implies that there is $M_3 \in \mathrm{Tran}_3(s_3)$ with

$$\begin{aligned}
&\forall (a_2,t_2) \in M_2 : \exists (a_3,t_3) \in M_3, \beta_2 \in \mathbb{L} : \\
&\qquad (t_2,t_3) \in R^2_{\beta_2}, F(a_2,a_3,\beta_2) \sqsubseteq_{\mathbb{L}} \alpha_2 , \qquad (7) \\
&\forall (a_3,t_3) \in M_3 : \exists (a_2,t_2) \in M_2, \beta_2 \in \mathbb{L} : \\
&\qquad (t_2,t_3) \in R^2_{\beta_2}, F(a_2,a_3,\beta_2) \sqsubseteq_{\mathbb{L}} \alpha_2 . \qquad (8)
\end{aligned}$$

Now let $(a_1,t_1) \in M_1$, then we get $(a_2,t_2) \in M_2$, $(a_3,t_3) \in M_3$ and $\beta_1,\beta_2 \in \mathbb{L}$ as in (5) and (7). Let $\beta = \beta_1 \oplus_{\mathbb{L}} \beta_2$, then $(t_1,t_3) \in R_\beta$, and by the extended triangle inequality for F, $F(a_1,a_3,\beta) \sqsubseteq_{\mathbb{L}} F(a_1,a_2,\beta_1) \oplus_{\mathbb{L}} F(a_2,a_3,\beta_2) \sqsubseteq_{\mathbb{L}} \alpha_1 \oplus_{\mathbb{L}} \alpha_2 = \alpha$.

Similarly, given $(a_3,t_3) \in M_3$, we can apply (8) and (6) to get $(a_1,t_1) \in M_1$ and $\beta \in \mathbb{L}$ such that $(t_1,t_3) \in R_\beta$ and $F(a_1,a_3,\beta) \sqsubseteq_{\mathbb{L}} \alpha$.

We have shown that $d^{\mathbb{L}}_{\mathsf{m}}$ and $d^{\mathbb{L}}_{\mathsf{tr}}$ are $\mathbb{L}$-hemimetrics. Using monotonicity of the eval function, it follows that d_{m} and d_{tr} are hemimetrics. □

Proposition 4 *For the* discrete *distances, $d_{\mathsf{m}}(\mathcal{S}_1,\mathcal{S}_2) = 0$ if $\mathcal{S}_1 \leq_{\mathsf{m}} \mathcal{S}_2$ and ∞ otherwise. Similarly, $d_{\mathsf{th}}(\mathcal{S}_1,\mathcal{S}_2) = 0$ if $\mathcal{S}_1 \leq_{\mathsf{th}} \mathcal{S}_2$ and ∞ otherwise.*

Proof We show the proposition for NAA. We already know that, also for the discrete distances, $\mathcal{A}_1 \leq_{\mathsf{m}} \mathcal{A}_2$ implies $d_{\mathsf{m}}(\mathcal{A}_1,\mathcal{A}_2) = 0$ and that $\mathcal{A}_1 \leq_{\mathsf{th}} \mathcal{A}_2$ implies $d_{\mathsf{th}}(\mathcal{A}_1,\mathcal{A}_2) = 0$. We show that $d_{\mathsf{m}}(\mathcal{A}_1,\mathcal{A}_2) = 0$ implies $\mathcal{A}_1 \leq_{\mathsf{m}} \mathcal{A}_2$. Let $R = \{R_\alpha \subseteq S_1 \times S_2 \mid \alpha \in \mathbb{L}\}$ be a refinement family such that $\forall s_1^0 \in S_1^0 : \exists s_2^0 \in S_2^0 : (s_1^0,s_2^0) \in R_0$. We show that R_0 is a witness for $\mathcal{A}_1 \leq_{\mathsf{m}} \mathcal{A}_2$; it is clearly initialized.

Let $(s_1, s_2) \in R_0$ and $M_1 \in \mathrm{Tran}_1(s_1)$, then we have $M_2 \in \mathrm{Tran}_2(s_2)$ such that

$$\begin{aligned} &\forall (a_1, t_1) \in M_1 : \exists (a_2, t_2) \in M_2, \beta \in \mathbb{L} : \\ &\qquad (t_1, t_2) \in R_\beta, F(a_1, a_2, \beta) = 0\,, \\ &\forall (a_2, t_2) \in M_2 : \exists (a_1, t_1) \in M_1, \beta \in \mathbb{L} : \\ &\qquad (t_1, t_2) \in R_\beta, F(a_1, a_2, \beta) = 0\,. \end{aligned} \tag{9}$$

Using the definition of the distance, we see that the condition $F(a_1, a_2, \beta) = 0$ is equivalent to $a_1 \preccurlyeq a_2$ and $\beta = 0$, hence (9) degenerates to

$$\begin{aligned} &\forall (a_1, t_1) \in M_1 : \exists (a_2, t_2) \in M_2 : (t_1, t_2) \in R_0, a_1 \preccurlyeq a_2\,, \\ &\forall (a_2, t_2) \in M_2 : \exists (a_1, t_1) \in M_1 : (t_1, t_2) \in R_0, a_1 \preccurlyeq a_2\,, \end{aligned}$$

which are exactly the conditions for R_0 to be a modal refinement.

Again by definition, we see that for any NAA $\mathcal{A}_1$, $\mathcal{A}_2$, either $d_{\mathsf{m}}(\mathcal{A}_1, \mathcal{A}_2) = 0$ or $d_{\mathsf{m}}(\mathcal{A}_1, \mathcal{A}_2) = \infty$, hence $\mathcal{A}_1 \not\leq_{\mathsf{m}} \mathcal{A}_2$ implies that $d_{\mathsf{m}}(\mathcal{A}_1, \mathcal{A}_2) = \infty$.

To show the last part of the proposition, we notice that

$$\begin{aligned} d_{\mathsf{th}}(\mathcal{A}_1, \mathcal{A}_2) &= \sup_{\mathcal{I}_1 \in [\![\mathcal{A}_1]\!]} \inf_{\mathcal{I}_2 \in [\![\mathcal{A}_2]\!]} d_{\mathsf{m}}(\mathcal{I}_1, \mathcal{I}_2) \\ &= \begin{cases} 0 & \text{if } \forall \mathcal{I}_1 \in [\![\mathcal{A}_1]\!] : \exists \mathcal{I}_2 \in [\![\mathcal{A}_2]\!] : \mathcal{I}_1 \leq_{\mathsf{m}} \mathcal{I}_2\,, \\ \infty & \text{otherwise}\,, \end{cases} \\ &= \begin{cases} 0 & \text{if } [\![\mathcal{A}_1]\!] \subseteq [\![\mathcal{A}_2]\!]\,, \\ \infty & \text{otherwise}\,. \end{cases} \end{aligned}$$

Hence $d_{\mathsf{th}}(\mathcal{A}_1, \mathcal{A}_2) = 0$ if $\mathcal{A}_1 \leq_{\mathsf{th}} \mathcal{A}_2$ and $d_{\mathsf{th}}(\mathcal{A}_1, \mathcal{A}_2) = \infty$ otherwise. □

As a quantitative analogy to the implication from (Boolean) modal refinement to thorough refinement (see Proposition 1), the next theorem shows that thorough refinement distance is bounded above by modal refinement distance. Note that for the discrete trace distance (and using Proposition 4), this is equivalent to the Boolean statement.

Theorem 8 *For all specifications $\mathcal{S}_1$, $\mathcal{S}_2$, $d^{\mathbb{L}}_{\mathsf{th}}(\mathcal{S}_1, \mathcal{S}_2) \sqsubseteq_{\mathbb{L}} d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{S}_1, \mathcal{S}_2)$.*

Proof We prove the statement for NAA; for DMTS and ν-calculus expressions it then follows from Theorem 7.

Let $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$, $\mathcal{A}_2 = (S_2, S_2^0, \mathrm{Tran}_2)$. We have a refinement family $R = \{R_\alpha \subseteq S_1 \times S_2 \mid \alpha \in \mathbb{L}\}$ such that for all $s_1^0 \in S_1^0$, there is $s_2^0 \in S_2^0$ with $(s_1^0, s_2^0) \in R_{d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_1, \mathcal{A}_2)}$. Let $\mathcal{I} = (S, S^0, T) \in [\![\mathcal{A}_1]\!]$, *i.e.*, $\mathcal{I} \leq_{\mathsf{m}} \mathcal{A}_1$.

Let $R^1 \subseteq S \times S_1$ be an initialized modal refinement, and define a relation family $R^2 = \{R^2_\alpha \subseteq S \times S_2 \mid \alpha \in \mathbb{L}\}$ by $R^2_\alpha = R^1 \circ R_\alpha = \{(s, s_2) \mid \exists s_1 \in S : (s, s_1) \in R^1, (s_1, s_2) \in R_\alpha\}$. We define a LTS $\mathcal{I}_2 = (S_2, S_2^0, T_2)$ as follows:

For all $\alpha \in \mathbb{L}$ with $\alpha \neq \top_{\mathbb{L}}$ and $(s, s_2) \in R^2_\alpha$: We must have $s_1 \in S_1$ with $(s, s_1) \in R^1$ and $(s_1, s_2) \in R_\alpha$. Then there is $M_1 \in \mathrm{Tran}_1(s_1)$ such that

- for all $s \xrightarrow{a} t$, there is $(a, t_1) \in M_1$ with $(t, t_1) \in R_1$,
- for all $(a_1, t_1) \in M_1$, there is $s \xrightarrow{a} t$ with $(t, t_1) \in R_1$.

This in turn implies that there is $M_2 \in \mathrm{Tran}_2(s_2)$ satisfying the conditions in Definition 3. For all $(a_2, t_2) \in M_2$: add a transition $s_2 \xrightarrow{a_2} t_2$ to T_2.

We show that the identity relation $\{(s_2, s_2) \mid s_2 \in S_2\}$ is a witness for $\mathcal{I}_2 \leq_{\mathsf{m}} \mathcal{A}_2$. Let $s_2 \in S_2$ and $s_2 \xrightarrow{a_2} t_2$. By construction, there is an $M_2 \in \mathrm{Tran}_2(s_2)$ with $(a_2, t_2) \in M_2$, and for all $(a_2', t_2') \in M_2$, $s_2 \xrightarrow{a_2'} t_2'$.

We show that R^2 is a witness for $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{I}, \mathcal{I}_2)$; clearly, R^2 is initialized. Let $\alpha \in \mathbb{L}$ with $\alpha \neq \top_{\mathbb{L}}$ and $(s, s_2) \in R^2_\alpha$, then there is $s_1 \in S_1$ with $(s, s_1) \in R^1$ and $(s_1, s_2) \in R_\alpha$. We also have $M_1 \in \mathrm{Tran}_1(s_1)$ such that

- for all $s \xrightarrow{a} t$, there is $(a, t_1) \in M_1$ with $(t, t_1) \in R^1$,
- for all $(a, t_1) \in M_1$, there is $s \xrightarrow{a} t$ with $(t, t_1) \in R^1$

and thus $M_2 \in \mathrm{Tran}_2(s_2)$ satisfying the conditions in Definition 3.

Let $s \xrightarrow{a} t$, then there is $(a, t_1) \in M_1$ with $(t, t_1) \in R^1$, hence also $(a_2, t_2) \in M_2$ and $\beta \in \mathbb{L}$ with $(t_1, t_2) \in R_\beta$ and $F(a, a_2, \beta) \sqsubseteq_{\mathbb{L}} \alpha$. But then $(t, t_2) \in R^2_\beta$, and $s_2 \xrightarrow{a_2} t_2$ by construction.

Let $s_2 \xrightarrow{a_2} t_2$. By construction, there is an $M_2 \in \mathrm{Tran}_2(s_2)$ with $(a_2, t_2) \in M_2$. This implies that there is $M_1 \in \mathrm{Tran}_1(s_1)$, $\beta \in \mathbb{L}$ and $(a_1, t_1) \in M_1$ with $(t_1, t_2) \in R_\beta$ and $F(a_1, a_2, \beta) \sqsubseteq \alpha$. But then there is also $s \xrightarrow{a_1} t$ with $(t, t_1) \in R^1$, hence $(t, t_2) \in R^2_\beta$. □

5.4 Disjunction and conjunction

In order to generalize the properties of Theorem 4 to our quantitative setting, we introduce a notion of relaxed implementation semantics:

Definition 4 The *α-relaxed implementation semantics* of $\mathcal{S}$, for a specification $\mathcal{S}$ and $\alpha \in \mathbb{L}$, is

$$[\![\mathcal{S}]\!]^\alpha = \{\mathcal{I} \text{ implementation} \mid d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{I}, \mathcal{S}) \sqsubseteq \alpha\}\,.$$

Hence, $[\![\mathcal{S}]\!]^\alpha$ comprises all labeled transition systems which are implementations of $\mathcal{S}$ *up to* α. Note that by Proposition 2 and for F recursively separating, $[\![\mathcal{S}]\!]^{\bot_{\mathbb{L}}} = [\![\mathcal{S}]\!]$.

Theorem 9 *For all specifications $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$ and $\alpha \in \mathbb{L}$,*

- $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{S}_1 \vee \mathcal{S}_2, \mathcal{S}_3) = \max(d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{S}_1, \mathcal{S}_3), d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{S}_2, \mathcal{S}_3))$,
- $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{S}_1, \mathcal{S}_2 \wedge \mathcal{S}_3) \sqsupseteq_{\mathbb{L}} \max(d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{S}_1, \mathcal{S}_2), d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{S}_1, \mathcal{S}_3))$,

– $[\![\mathcal{S}_1 \vee \mathcal{S}_2]\!]^\alpha = [\![\mathcal{S}_1]\!]^\alpha \cup [\![\mathcal{S}_2]\!]^\alpha$, *and*
– $[\![\mathcal{S}_1 \wedge \mathcal{S}_2]\!]^\alpha \subseteq [\![\mathcal{S}_1]\!]^\alpha \cap [\![\mathcal{S}_2]\!]^\alpha$.

Proof We show the proof for DMTS.

The proof that $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{D}_1 \vee \mathcal{D}_2, \mathcal{D}_3) = \max(d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{D}_1, \mathcal{D}_3), d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{D}_2, \mathcal{D}_3))$ is trivial: any refinement family witnessing $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{D}_1 \vee \mathcal{D}_2, \mathcal{D}_3)$ splits into two families witnessing $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{D}_1, \mathcal{D}_3)$ and $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{D}_2, \mathcal{D}_3)$ and vice versa.

To show that $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{D}_1, \mathcal{D}_2 \wedge \mathcal{D}_3) \sqsupseteq_{\mathbb{L}} \max(d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{D}_1, \mathcal{D}_2), d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{D}_1, \mathcal{D}_3))$, let $R = \{R_\alpha \subseteq S_1 \times (S_2 \times S_3) \mid \alpha \in \mathbb{L}\}$ be a witness for $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{D}_1, \mathcal{D}_2 \wedge \mathcal{D}_3)$ and define $R^2 = \{R^2_\alpha \subseteq S_1 \times S_2 \mid \alpha \in \mathbb{L}\}$ by $R^2_\alpha = \{(s_1, s_2) \mid \exists s_3 \in S_3 : (s_1, (s_2, s_3)) \in R_\alpha\}$ for all $\alpha \in \mathbb{L}$.

Let $s^0_1 \in S^0_1$, then we have $(s^0_2, s^0_3) \in S^0_2 \times S^0_3$ so that $(s^0_1, (s^0_2, s^0_3)) \in R_{d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{D}_1, \mathcal{D}_2 \wedge \mathcal{D}_3)}$, hence also $(s^0_1, s^0_2) \in R^2_{d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{D}_1, \mathcal{D}_2 \wedge \mathcal{D}_3)}$.

Let $\alpha \in \mathbb{L}$ and $(s_1, s_2) \in R^2_\alpha$, then we have $s_3 \in S_3$ for which $(s_1, (s_2, s_3)) \in R_\alpha$. Assume first that $s_1 \overset{a_1}{\dashrightarrow} t_1$, then there is $(s_2, s_3) \overset{a}{\dashrightarrow} (t_2, t_3)$ and $\beta \in \mathbb{L}$ such that $F(a_1, a, \beta) \sqsubseteq_{\mathbb{L}} \alpha$ and $(t_1, (t_2, t_3)) \in R_\beta$, hence $(t_1, t_2) \in R^2_\beta$. By construction of $\mathcal{D}_2 \wedge \mathcal{D}_3$, there are $s_2 \overset{a_2}{\dashrightarrow} t_2$ and $s_3 \overset{a_3}{\dashrightarrow} t_3$ such that $a = a_2 \oslash a_3$, but then by anti-monotonicity, $F(a_1, a_2, \beta) \sqsubseteq_{\mathbb{L}} F(a_1, a, \beta) \sqsubseteq \alpha$.

Now assume $s_2 \longrightarrow N_2$, then, by construction, $(s_2, s_3) \longrightarrow N = \{(a_2 \oslash a_3, (t_2, t_3)) \mid (a_2, t_2) \in N_2, s_3 \overset{a_3}{\dashrightarrow}_3 t_3\}$. Hence we have $s_1 \longrightarrow_1 N_1$ such that $\forall (a_1, t_1) \in N_1 : \exists (a, (t_2, t_3)) \in N, \beta \in \mathbb{L} : F(a_1, a, \beta) \sqsubseteq \alpha, (t_1, (t_2, t_3)) \in R_\beta$.

Let $(a_1, t_1) \in N_1$, then we have $(a, (t_2, t_3)) \in N$ and $\beta \in \mathbb{L}$ for which $F(a_1, a, \beta) \sqsubseteq_{\mathbb{L}} \alpha$ and $(t_1, (t_2, t_3)) \in R_\beta$, hence $(t_1, t_2) \in R^2_\beta$. By construction of N, this implies that there are $(a_2, t_2) \in N_2$ and $s_3 \overset{a_3}{\dashrightarrow}_3 t_3$ such that $a = a_2 \oslash a_3$, but then by anti-monotonicity, $F(a_1, a_2, \beta) \sqsubseteq_{\mathbb{L}} F(a_1, a, \beta) \sqsubseteq \alpha$.

We have shown that $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{D}_1, \mathcal{D}_2 \wedge \mathcal{D}_3) \sqsubseteq_{\mathbb{L}} d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{D}_1, \mathcal{D}_2)$; the proof of $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{D}_1, \mathcal{D}_2 \wedge \mathcal{D}_3) \sqsubseteq_{\mathbb{L}} d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{D}_1, \mathcal{D}_3)$ is entirely analogous.

The inclusion $[\![\mathcal{D}_1 \wedge \mathcal{D}_2]\!]^\alpha \subseteq [\![\mathcal{D}_1]\!]^\alpha \cap [\![\mathcal{D}_2]\!]^\alpha$ is clear now: If $\mathcal{I} \in [\![\mathcal{D}_1 \wedge \mathcal{D}_2]\!]^\alpha$, *i.e.*, $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{I}, \mathcal{D}_1 \wedge \mathcal{D}_2) \sqsubseteq_{\mathbb{L}} \alpha$, then also $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{I}, \mathcal{D}_1) \sqsubseteq_{\mathbb{L}} \alpha$ and $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{I}, \mathcal{D}_2) \sqsubseteq_{\mathbb{L}} \alpha$, thus $\mathcal{I} \in [\![\mathcal{D}_1]\!]^\alpha \cap [\![\mathcal{D}_2]\!]^\alpha$.

To show that $[\![\mathcal{D}_1 \vee \mathcal{D}_2]\!]^\alpha = [\![\mathcal{D}_1]\!]^\alpha \cup [\![\mathcal{D}_2]\!]^\alpha$, one notices, like in the proof of Theorem 4, that for any LTS $\mathcal{I}$, any refinement family witnessing $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{I}, \mathcal{D}_1)$ or $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{I}, \mathcal{D}_2)$ is also a witness for $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{I}, \mathcal{D}_1 \vee \mathcal{D}_2)$ and vice versa. □

The below example shows why the inclusions above cannot be replaced by equalities. To sum up, disjunction is quantitatively sound and complete, whereas conjunction is only quantitatively sound.

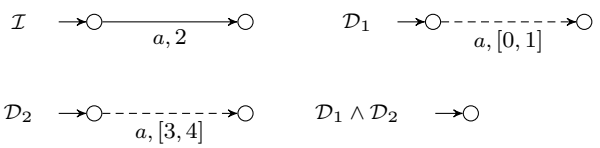

Fig. 10 LTS $\mathcal{I}$ together with DMTS $\mathcal{D}_1$, $\mathcal{D}_2$ and their conjunction. For the point-wise or discounting distances, $d_{\mathsf{m}}(\mathcal{I}, \mathcal{D}_1) = d_{\mathsf{m}}(\mathcal{I}, \mathcal{D}_2) = 1$, but $d_{\mathsf{m}}(\mathcal{I}, \mathcal{D}_1 \wedge \mathcal{D}_2) = \infty$

Example 8 For the point-wise or discounting distances, the DMTS in Fig. 10 are such that $d_{\mathsf{m}}(\mathcal{I}, \mathcal{D}_1) = 1$ and $d_{\mathsf{m}}(\mathcal{I}, \mathcal{D}_2) = 1$, but $d_{\mathsf{m}}(\mathcal{I}, \mathcal{D}_1 \wedge \mathcal{D}_2) = \infty$. Hence $d_{\mathsf{m}}(\mathcal{I}, \mathcal{D}_1 \wedge \mathcal{D}_2) \neq \max(d_{\mathsf{m}}(\mathcal{I}, \mathcal{D}_1), d_{\mathsf{m}}(\mathcal{I}, \mathcal{D}_2))$, and $\mathcal{I} \in [\![\mathcal{D}_1]\!]^1 \cap [\![\mathcal{D}_2]\!]^1$, but $\mathcal{I} \notin [\![\mathcal{D}_1 \wedge \mathcal{D}_2]\!]^1$. □

5.5 Structural composition and quotient

We proceed to devise a quantitative generalization of the properties of structural composition and quotient exposed in Section 4. To this end, we need to use a *uniform composition bound* on labels:

Let $P : \mathbb{L} \times \mathbb{L} \to \mathbb{L}$ be a function which is monotone in both coordinates, has $P(\alpha, \bot_{\mathbb{L}}) = P(\bot_{\mathbb{L}}, \alpha) = \alpha$ and $P(\alpha, \top_{\mathbb{L}}) = P(\top_{\mathbb{L}}, \alpha) = \top_{\mathbb{L}}$ for all $\alpha \in \mathbb{L}$. We require that for all $a_1, b_1, a_2, b_2 \in \Sigma$ and $\alpha, \beta \in \mathbb{L}$ with $F(a_1, a_2, \alpha) \neq \top$ and $F(b_1, b_2, \beta) \neq \top$, $a_1 \odot b_1$ is defined iff $a_2 \odot b_2$ is, and if both are defined, then

$$F(a_1 \odot b_1, a_2 \odot b_2, P(\alpha, \beta)) \sqsubseteq_{\mathbb{L}} P(F(a_1, a_2, \alpha), F(b_1, b_2, \beta)) \,. \quad (10)$$

Note that (10) implies that $d_{\mathsf{tr}}(a_1 \odot a_2, b_1 \odot b_2) \sqsubseteq_{\mathbb{L}} P(d_{\mathsf{tr}}(a_1, b_1), d_{\mathsf{tr}}(a_2, b_2))$. Hence P provides a *uniform bound* on distances between synchronized labels,[1] and (10) extends this property so that it holds recursively. Also, this is a generalization of the condition that we imposed on $\odot$ in Section 2; it is shown in [30] that it holds for all common label synchronizations.

The following theorems show that composition is uniformly continuous (*i.e.*, a quantitative generalization of independent implementability; Corollary 1) and that quotient preserves and reflects refinement distance (a quantitative generalization of Theorem 6).

Theorem 10 *For all specifications $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$, $\mathcal{S}_4$, $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{S}_1 \| \mathcal{S}_2, \mathcal{S}_3 \| \mathcal{S}_4) \sqsubseteq_{\mathbb{L}} P(d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{S}_1, \mathcal{S}_3), d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{S}_2, \mathcal{S}_4))$.*

Proof We show the proof for NAA. For $i = 1, 2, 3, 4$, let $\mathcal{A}_i = (S_i, S^0_i, \mathrm{Tran}_i)$. Let $R^1 = \{R^1_\alpha \subseteq S_1 \times S_3 \mid \alpha \in \mathbb{L}\}$, $R^2 = \{R^2_\alpha \subseteq S_2 \times S_4 \mid \alpha \in \mathbb{L}\}$ be refinement families such that $\forall s^0_1 \in S^0_1 : \exists s^0_3 \in S^0_3 : (s^0_1, s^0_3) \in R^1_{d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_1, \mathcal{A}_3)}$

[1] Indeed, P bears some similarity to the concept of *modulus of continuity* used in analysis.

and $\forall s_2^0 \in S_2^0 : \exists s_4^0 \in S_4^0 : (s_2^0, s_4^0) \in R^2_{d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_2,\mathcal{A}_4)}$. Define $R = \{R_\alpha \subseteq (S_1 \times S_2) \times (S_3 \times S_4) \mid \alpha \in \}$ by

$$R_\alpha = \big\{((s_1,s_2),(s_3,s_4)) \;\big|\; \exists \alpha_1, \alpha_2 \in \mathbb{L} : (s_1,s_3) \in R^1_{\alpha_1}, (s_2,s_4) \in R^2_{\alpha_2}, P(\alpha_1,\alpha_2) \sqsubseteq_{\mathbb{L}} \alpha\big\},$$

then it is clear that $\forall (s_1^0, s_2^0) \in S_1^0 \times S_2^0 : \exists (s_3^0, s_4^0) \in S_3^0 \times S_4^0 : ((s_1^0,s_2^0),(s_3^0,s_4^0)) \in R_{P(d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_1,\mathcal{A}_3), d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_2,\mathcal{A}_4))}$. We show that R is a refinement family from $\mathcal{A}_1 \| \mathcal{A}_2$ to $\mathcal{A}_3 \| \mathcal{A}_4$.

Let $\alpha \in \mathbb{L}$ and $((s_1,s_2),(s_3,s_4)) \in R_\alpha$, then we have $\alpha_1, \alpha_2 \in \mathbb{L}$ with $(s_1,s_3) \in R^1_{\alpha_1}$, $(s_2,s_4) \in R^2_{\alpha_2}$ and $P(\alpha_1,\alpha_2) \sqsubseteq_{\mathbb{L}} \alpha$. Let $M_{12} \in \mathrm{Tran}((s_1,s_2))$, then there must be $M_1 \in \mathrm{Tran}_1(s_1)$, $M_2 \in \mathrm{Tran}_2(s_2)$ for which $M_{12} = M_1 \oplus M_2$. Thus we also have $M_3 \in \mathrm{Tran}_3(s_3)$ and $M_4 \in \mathrm{Tran}_4(s_4)$ such that

$$\forall (a_1,t_1) \in M_1 : \exists (a_3,t_3) \in M_3, \beta_1 \in \mathbb{L} : (t_1,t_3) \in R^1_{\beta_1}, F(a_1,a_3,\beta_1) \sqsubseteq_{\mathbb{L}} \alpha_1, \quad (11)$$

$$\forall (a_3,t_3) \in M_3 : \exists (a_1,t_1) \in M_1, \beta_1 \in \mathbb{L} : (t_1,t_3) \in R^1_{\beta_1}, F(a_1,a_3,\beta_1) \sqsubseteq_{\mathbb{L}} \alpha_1, \quad (12)$$

$$\forall (a_2,t_2) \in M_2 : \exists (a_4,t_4) \in M_4, \beta_2 \in \mathbb{L} : (t_2,t_4) \in R^2_{\beta_2}, F(a_2,a_4,\beta_2) \sqsubseteq_{\mathbb{L}} \alpha_2, \quad (13)$$

$$\forall (a_4,t_4) \in M_4 : \exists (a_2,t_2) \in M_2, \beta_2 \in \mathbb{L} : (t_2,t_4) \in R^2_{\beta_2}, F(a_2,a_4,\beta_2) \sqsubseteq_{\mathbb{L}} \alpha_2. \quad (14)$$

Let $M_{34} = M_3 \oplus M_4$, then $M_{34} \in \mathrm{Tran}((s_3,s_4))$. Let $(a_{12},(t_1,t_2)) \in M_{12}$, then there are $(a_1,t_1) \in M_1$ and $(a_2,t_2) \in M_2$ for which $a_{12} = a_1 \oplus a_2$. Using (11) and (13), we get $(a_3,t_3) \in M_3$, $(a_4,t_4) \in M_4$ and $\beta_1, \beta_2 \in \mathbb{L}$ such that $(t_1,t_3) \in R^1_{\beta_1}$, $(t_2,t_4) \in R^2_{\beta_2}$, $F(a_1,a_3,\beta_1) \sqsubseteq_{\mathbb{L}} \alpha_1$, and $F(a_2,a_4,\beta_2) \sqsubseteq_{\mathbb{L}} \alpha_2$.

Let $a_{34} = a_3 \oplus a_4$ and $\beta = P(\beta_1,\beta_2)$, then we have $(a_{34},(t_3,t_4)) \in M_{34}$. Also, $(t_1,t_3) \in R^1_{\beta_1}$ and $(t_2,t_4) \in R^2_{\beta_2}$ imply that $((t_1,t_2),(t_3,t_4)) \in R_\beta$, and

$$\begin{aligned} F(a_{12},a_{34},\beta) &= F(a_1 \oplus a_2, a_3 \oplus a_4, P(\beta_1,\beta_2)) \\ &\sqsubseteq P(F(a_1,a_3,\beta_1), F(a_2,a_4,\beta_2)) \\ &\sqsubseteq_{\mathbb{L}} P(\alpha_1,\alpha_2) \sqsubseteq_{\mathbb{L}} \alpha. \end{aligned}$$

We have shown that for all $(a_{12},(t_1,t_2)) \in M_{12}$, there exists $(a_{34},(t_3,t_4)) \in M_{34}$ and $\beta \in \mathbb{L}$ such that $((t_1,t_2),(t_3,t_4)) \in R_\beta$ and $F(a_{12},a_{34},\beta) \sqsubseteq_{\mathbb{L}} \alpha$. To show the reverse property, starting from an element $(a_{34},(t_3,t_4)) \in M_{34}$, we can proceed entirely analogous, using (12) and (14). □

Theorem 11 *For all specifications $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$, we have $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{S}_1 \| \mathcal{S}_2, \mathcal{S}_3) = d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{S}_2, \mathcal{S}_3 / \mathcal{S}_1)$.*

Proof We show the proof for NAA. Let $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$, $\mathcal{A}_2 = (S_2, S_2^0, \mathrm{Tran}_2)$, $\mathcal{A}_3 = (S_3, S_3^0, \mathrm{Tran}_3)$; we show that $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_1 \| \mathcal{A}_2, \mathcal{A}_3) = d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_2, \mathcal{A}_3 / \mathcal{A}_1)$.

We assume that the elements of $\mathrm{Tran}_1(s_1)$ are pairwise disjoint for each $s_1 \in S_1$; this can be achieved by, if necessary, splitting states.

Define $R = \{R_\alpha \subseteq S_1 \times S_2 \times S_3 \mid \alpha \in \mathbb{L}\}$ by $R_\alpha = \{(s_1 \| s_2, s_3) \mid d^{\mathbb{L}}_{\mathsf{m}}(s_2, s_3/s_1) \sqsubseteq_{\mathbb{L}} \alpha\}$. We show that R is a witness for $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_1 \| \mathcal{A}_2, \mathcal{A}_3)$.

Let $s_1^0 \| s_2^0 \in S_1^0 \times S_2^0$, then there is $s_3^0 / s_1^0 \in s^0$ for which it holds that $d^{\mathbb{L}}_{\mathsf{m}}(s_2^0, s_3^0/s_1^0) \sqsubseteq_{\mathbb{L}} d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_2, \mathcal{A}_3/\mathcal{A}_1)$, hence $(s_1^0 \| s_1^0, s_3^0) \in R_{d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_2, \mathcal{A}_3/\mathcal{A}_1)}$.

Let $\alpha \in \mathbb{L} \setminus \{\top_{\mathbb{L}}\}$, $(s_1 \| s_2, s_3) \in R_\alpha$ and $M_\| \in \mathrm{Tran}_\|(s_1 \| s_2)$. Then $M_\| = M_1 \| M_2$ with $M_1 \in \mathrm{Tran}_1(s_1)$ and $M_2 \in \mathrm{Tran}_2(s_2)$. As $d^{\mathbb{L}}_{\mathsf{m}}(s_2, s_3/s_1) \sqsubseteq_{\mathbb{L}} \alpha$, we can pair M_2 with an $M_/ \in \mathrm{Tran}_/(s_3/s_1)$, *i.e.*, such that the conditions in Definition 3 are satisfied.

Let $M_3 = M_/ \triangleright M_1$. We show that the conditions in Definition 3 are satisfied for the pair $M_\|, M_3$:

- Let $(a, t_1 \| t_2) \in M_\|$, then there are $a_1, a_2 \in \Sigma$ with $a = a_1 \oplus a_2$ and $(a_1,t_1) \in M_1$, $(a_2,t_2) \in M_2$. Hence there is $(a_2', t) \in M_/$ and $\beta \in \mathbb{L}$ such that $F(a_2, a_2', \beta) \sqsubseteq_{\mathbb{L}} \alpha$ and $d^{\mathbb{L}}_{\mathsf{m}}(t_2, t) \sqsubseteq_{\mathbb{L}} \beta$.
  Note that $a_3 = a_1 \oplus a_2'$ is defined and $F(a, a_3, \beta) \sqsubseteq \alpha$. Write $t = \{t_3^1/t_1^1, \ldots, t_3^n/t_1^n\}$. By construction, there is an index i for which $t_1^i = t_1$, hence $(a_3, t_3^i) \in M_3$. Also, $t \supseteq \{t_3^i/t_1^i\}$, hence $d^{\mathbb{L}}_{\mathsf{m}}(t_2, t_3^i/t_1^i) \sqsubseteq \beta$ and consequently $(t_1 \| t_2, t_3) \in R_\beta$.
- Let $(a_3,t_3) \in M_3$, then there are $(a_2', t) \in M_/$ and $(a_1,t_1) \in M_1$ such that $a_3 = a_1 \oplus a_2'$ and $t_3/t_1 \in t$. Hence there are $(a_2,t_2) \in M_2$ and $\beta \in \mathbb{L}$ for which $F(a_2, a_2', \beta) \sqsubseteq_{\mathbb{L}} \alpha$ and $d^{\mathbb{L}}_{\mathsf{m}}(t_2, t) \sqsubseteq_{\mathbb{L}} \beta$. Note that $a = a_1 \oplus a_2$ is defined and $F(a, a_3, \beta) \sqsubseteq_{\mathbb{L}} \alpha$. Thus $(a, t_1 \| t_2) \in M$, and by $t \supseteq \{t_3/t_1\}$, $d^{\mathbb{L}}_{\mathsf{m}}(t_2, t_3/t_1) \sqsubseteq \beta$.

Assume, for the other direction of the proof, that $\mathcal{A}_1 \| \mathcal{A}_2 \leq_{\mathsf{m}} \mathcal{A}_3$. Define $R = \{R_\alpha \subseteq S_2 \times 2^{S_3 \times S_1} \mid \alpha \in \mathbb{L}\}$ by

$$R_\alpha = \big\{(s_2, \{s_3^1/s_1^1, \ldots, s_3^n/s_1^n\}) \;\big|\; \forall i = 1, \ldots, n : d^{\mathbb{L}}_{\mathsf{m}}(s_1^i \| s_2, s_3^i) \sqsubseteq_{\mathbb{L}} \alpha\big\};$$

we show that R is a witness for $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_2, \mathcal{A}_3/\mathcal{A}_1)$.

Let $s_2^0 \in S_2^0$. We know that for every $s_1^0 \in S_1^0$, there exists $\sigma(s_1^0) \in S_3^0$ such that $d^{\mathbb{L}}_{\mathsf{m}}(s_1^0 \| s_2^0, s_3^0) \sqsubseteq_{\mathbb{L}} d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_1 \| \mathcal{A}_2, \mathcal{A}_3)$. By $s^0 \supseteq \{\sigma(s_1^0)/s_1^0 \mid s_1^0 \in S_1^0\}$, we see that $(s_2^0, s^0) \in R_{d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_1 \| \mathcal{A}_2, \mathcal{A}_3)}$.

Let $\alpha \in \mathbb{L} \setminus \{\top_{\mathbb{L}}\}$ and $(s_2, s) \in R_\alpha$, with $s = \{s_3^1/s_1^1, \ldots, s_3^n/s_1^n\}$, and $M_2 \in \mathrm{Tran}_2(s_2)$.

For every $i = 1, \ldots, n$, let us write $\mathrm{Tran}_1(s_1^i) = \{M_1^{i,1}, \ldots, M_1^{i,m_i}\}$. By assumption, $M_1^{i,j_1} \cap M_1^{i,j_2} = \emptyset$ for $j_1 \neq j_2$, hence every $(a_1,t_1) \in\in \mathrm{Tran}_1(s_1^i)$ is contained in a unique $M_1^{i,\delta_i(a_1,t_1)} \in \mathrm{Tran}_1(s_1^i)$.

For every $j = 1, \ldots, m_i$, let $M^{i,j} = M_1^{i,j} \| M_2 \in \mathrm{Tran}_\|(s_1^i \| s_2)$. By $d^{\mathbb{L}}_{\mathsf{m}}(s_1^i \| s_2, s_3^i) \sqsubseteq_{\mathbb{L}} \alpha$, we have $M_3^{i,j} \in$

$\mathrm{Tran}_3(s_3^i)$ such that the conditions in Definition 3 hold for the pair $M^{i,j}, M_3^{i,j}$.

Now define

$$M = \big\{(a_2,t) \;\big|\; \exists (a_2,t_2) \in M_2 : \forall t_3/t_1 \in t : \exists i, a_1, a_3, \beta : (a_1,t_1) \in\!\in \mathrm{Tran}_1(s_1^i), (a_3,t_3) \in M_3^{i,\delta_i(a_1,t_1)}, F(a_1 \oslash a_2, a_3, \beta) \sqsubseteq_{\mathbb{L}} \alpha, d^{\mathbb{L}}_{\mathsf{m}}(t_1 \| t_2, t_3) \sqsubseteq_{\mathbb{L}} \beta \big\}. \quad (15)$$

We need to show that $M \in \mathrm{Tran}_/(s)$.

Let $i \in \{1,\dots,n\}$ and $M_1^{i,j} \in \mathrm{Tran}_1(s_1^i)$; we claim that $M \triangleright M_1^{i,j} \preccurlyeq_R M_3^{i,j}$. Let $(a_3,t_3) \in M \triangleright M_1^{i,j}$, then $a_3 = a_1 \oslash a_2$ for some a_1, a_2 such that $t_3/t_1 \in t$, $(a_1,t_1) \in M_1^{i,j}$ and $(a_2,t) \in M$. By disjointness, $j = \delta_i(a_1,t_1)$, hence by definition of M, $(a_3,t_3) \in M_3^{i,j}$ as was to be shown.

For the reverse inclusion, let $(a_3,t_3) \in M_3^{i,j}$. By definition of $M^{i,j}$, there are $(a_1,t_1) \in M_1^{i,j}$, $(a_2,t_2) \in M_2$ and $\beta \in \mathbb{L}$ for which $F(a_1 \oslash a_2, a_3, \beta) \sqsubseteq_{\mathbb{L}} \alpha$ and $d^{\mathbb{L}}_{\mathsf{m}}(t_1 \| t_2, t_3) \sqsubseteq_{\mathbb{L}} \beta$. Thus $j = \delta_i(a_1,t_1)$, so that there must be $(a_2,t) \in M$ for which $t_3/t_1 \in t$, but then also $(a_1 \oslash a_2, t_3) \in M \triangleright M_1^{i,j}$.

We show that the pair M_2, M satisfies the conditions of Definition 3.

- Let $(a_2,t_2) \in M_2$. For every $i = 1,\dots,n$ and every $(a_1,t_1) \in\!\in \mathrm{Tran}_1(t_1^i)$, we can use Definition 3 applied to the pair $M_1^{i,\delta_i(a_1,t_1)} \| M_2, M_3^{i,\delta_i(a_1,t_1)}$ to choose an element $(\eta_i(a_1,t_1), \tau_i(a_1,t_1)) \in M_3^{i,\delta_i(a_1,t_1)}$ and $\beta_i(a_1,t_1) \in \mathbb{L}$ for which $d^{\mathbb{L}}_{\mathsf{m}}(t_1 \| t_2, \tau_i(a_1,t_1)) \sqsubseteq_{\mathbb{L}} \beta_i(a_1,t_1)$ and $F(a_1 \oslash a_2, \eta_i(a_1,t_1), \beta_i(a_1,t_1)) \sqsubseteq_{\mathbb{L}} \alpha$. Let $t = \{\tau_i(a_1,t_1)/t_1 \mid i = 1,\dots,n, (a_1,t_1) \in\!\in \mathrm{Tran}_1(t_1^i)\}$, then $(a_2,t) \in M$ and $(t_2,t) \in R_\beta$.
- Let $(a_2,t) \in M$, then we have $(a_2,t_2) \in M_2$ satisfying the conditions in (15). Hence for all $t_3/t_1 \in t$, there are i, a_1, a_3, and $\beta(t_3/t_1)$ such that $(a_3,t_3) \in M_3^{i,\delta_i(a_1,t_1)}$, $F(a_1 \oslash a_2, a_3, \beta(t_3/t_1)) \sqsubseteq_{\mathbb{L}} \alpha$ and $d^{\mathbb{L}}_{\mathsf{m}}(t_1 \| t_2, t_3) \sqsubseteq_{\mathbb{L}} \beta(t_3/t_1)$. Let $\beta = \sup\{\beta(t_3/t_1) \mid t_3/t_1 \in t\}$, then $d^{\mathbb{L}}_{\mathsf{m}}(t_1 \| t_2, t_3) \sqsubseteq_{\mathbb{L}} \beta$ for all $t_3/t_1 \in t$, hence $(t_2,t) \in R_\beta$. □

6 Conclusion

We have presented a framework for compositional and iterative design and verification of systems which supports quantities and system and action refinement. Moreover, it is robust, in that it uses distances to measure quantitative refinement and the operations preserve distances.

The framework is very general. It can be applied to a large variety of quantities (energy, time, resource consumption etc.) and implement the robustness notions associated with them. It is also agnostic with respect to the type of specifications used, as it applies equally to behavioral and logical specifications. This means that logical and behavioral quantitative specifications can be freely combined in quantitative system development.

As to future work, we believe that that the close relationship between DMTS and the modal ν-calculus which we expose here should be helpful for relating our robust semantics of the modal ν-calculus to other quantitative logics [18,37,50]. We also plan to implement the operations detailed here within the graphical tool MoTraS [41].

References

1. Luca Aceto, Ignacio Fábregas, David de Frutos-Escrig, Anna Ingólfsdóttir, and Miguel Palomino. On the specification of modal systems: A comparison of three frameworks. *Sci. Comput. Program.*, 78(12):2468–2487, 2013.
2. Charalambos D. Aliprantis and Kim C. Border. *Infinite Dimensional Analysis: A Hitchhiker's Guide*. Springer-Verlag, 2007.
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 *Lect. Notes Comput. Sci.*, pages 43–58. Springer, 2012.
4. Sebastian S. Bauer, Uli Fahrenberg, Line Juhl, Kim G. Larsen, Axel Legay, and Claus Thrane. Weighted modal transition systems. *Form. Meth. Syst. Design*, 42(2):193–220, 2013.
5. Sebastian S. Bauer, Line Juhl, Kim G. Larsen, Axel Legay, and Jiří Srba. Extending modal transition systems with structured labels. *Math. Struct. Comput. Sci.*, 22(4):581–617, 2012.
6. Sebastian S. Bauer and Jean-Baptiste Raclet, editors. *Foundations of Interface Technologies, FIT 2012*, volume 87 of *EPTCS*, 2012.
7. Shoham Ben-David, Marsha Chechik, and Sebastián Uchitel. Merging partial behaviour models with different vocabularies. In D'Argenio and Melgratti [16], pages 91–105.
8. Nikola Beneš, Benoît Delahaye, Uli Fahrenberg, Jan Křetínský, and Axel Legay. Hennessy-Milner logic with greatest fixed points. In D'Argenio and Melgratti [16], pages 76–90.
9. Nikola Beneš, Jan Křetínský, Kim G. Larsen, and Jiří Srba. On determinism in modal transition systems. *Theor. Comput. Sci.*, 410(41):4026–4043, 2009.
10. 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 *Lect. Notes Comput. Sci.*, pages 228–242. Springer-Verlag, 2011.
11. Nathalie Bertrand, Axel Legay, Sophie Pinchinat, and Jean-Baptiste Raclet. Modal event-clock specifications for timed component-based design. *Sci. Comput. Program.*, 77(12):1212–1234, 2012.
12. Gérard Boudol and Kim G. Larsen. Graphical versus logical specifications. *Theor. Comput. Sci.*, 106(1):3–20, 1992.
13. Benoît Caillaud, Benoît Delahaye, Kim G. Larsen, Axel Legay, Mikkel L. Pedersen, and Andrzej Wąsowski. Constraint Markov chains. *Theor. Comput. Sci.*, 412(34):4373–4404, 2011.

14. Luís Caires and Luca Cardelli. A spatial logic for concurrency (part I). *Inf. Comp.*, 186(2):194–235, 2003.
15. Luca Cardelli, Kim G. Larsen, and Radu Mardare. Modular Markovian logic. In Luca Aceto, Monika Henzinger, and Jiří Sgall, editors, *ICALP (2)*, volume 6756 of *Lect. Notes Comput. Sci.*, pages 380–391. Springer-Verlag, 2011.
16. Pedro R. D'Argenio and Hernán C. Melgratti, editors. *CONCUR 2013 - Concurrency Theory - 24th Int. Conf.*, volume 8052 of *Lect. Notes Comput. Sci.* Springer-Verlag, 2013.
17. Alexandre David, Kim G. Larsen, Axel Legay, Ulrik Nyman, Louis-Marie Traonouez, and Andrzej Wąsowski. Real-time specifications. *Int. J. Softw. Tools Techn. Transfer*, 2013. Online first. `http://dx.doi.org/10.1007/s10009-013-0286-x`.
18. Luca de Alfaro. Quantitative verification and control via the mu-calculus. In Roberto M. Amadio and Denis Lugiez, editors, *CONCUR*, volume 2761 of *Lect. Notes Comput. Sci.*, pages 102–126. Springer-Verlag, 2003.
19. Luca de Alfaro, Marco Faella, Thomas A. Henzinger, Rupak Majumdar, and Mariëlle Stoelinga. Model checking discounted temporal properties. *Theor. Comput. Sci.*, 345(1):139–170, 2005.
20. Luca de Alfaro, Marco Faella, and Mariëlle Stoelinga. Linear and branching system metrics. *IEEE Trans. Software Eng.*, 35(2):258–273, 2009.
21. Luca de Alfaro and Thomas A. Henzinger. Interface automata. In *ESEC / SIGSOFT FSE*, pages 109–120. ACM, 2001.
22. Luca de Alfaro, Thomas A. Henzinger, and Mariëlle Stoelinga. Timed interfaces. In Alberto L. Sangiovanni-Vincentelli and Joseph Sifakis, editors, *EMSOFT*, volume 2491 of *Lect. Notes Comput. Sci.*, pages 108–122. Springer-Verlag, 2002.
23. Benoît Delahaye, Uli Fahrenberg, Kim G. Larsen, and Axel Legay. Refinement and difference for probabilistic automata. *Logical Methods in Computer Science*, 10(3), 2014.
24. Benoît Delahaye, Kim G. Larsen, Axel Legay, Mikkel L. Pedersen, and Andrzej Wąsowski. Consistency and refinement for interval Markov chains. *J. Log. Algebr. Program.*, 81(3):209–226, 2012.
25. Josee Desharnais, Vineet Gupta, Radha Jagadeesan, and Prakash Panangaden. Metrics for labelled Markov processes. *Theor. Comput. Sci.*, 318(3):323–354, 2004.
26. Uli Fahrenberg, Mathieu Acher, Axel Legay, and Andrzej Wąsowski. Sound merging and differencing for class diagrams. In Stefania Gnesi and Arend Rensink, editors, *FASE*, volume 8411 of *Lect. Notes Comput. Sci.*, pages 63–78. Springer-Verlag, 2014.
27. Uli Fahrenberg, Jan Křetínský, Axel Legay, and Louis-Marie Traonouez. Compositionality for quantitative specifications. In *FACS*, Lect. Notes Comput. Sci. Springer-Verlag, 2014. To be published.
28. Uli Fahrenberg and Axel Legay. A robust specification theory for modal event-clock automata. In Bauer and Raclet [6], pages 5–16.
29. Uli Fahrenberg and Axel Legay. Generalized quantitative analysis of metric transition systems. In Chung-chieh Shan, editor, *APLAS*, volume 8301 of *Lect. Notes Comput. Sci.*, pages 192–208. Springer-Verlag, 2013.
30. Uli Fahrenberg and Axel Legay. General quantitative specification theories with modal transition systems. *Acta Inf.*, 51(5):261–295, 2014.
31. Uli Fahrenberg and Axel Legay. The quantitative linear-time–branching-time spectrum. *Theor. Comput. Sci.*, 538:54–69, 2014.
32. Uli Fahrenberg, Axel Legay, and Louis-Marie Traonouez. Structural refinement for the modal nu-calculus. In Gabriel Ciobanu and Dominique Méry, editors, *ICTAC*, volume 8687 of *Lect. Notes Comput. Sci.*, pages 169–187. Springer-Verlag, 2014.
33. Jean-Yves Girard. Linear logic. *Theor. Comput. Sci.*, 50:1–102, 1987.
34. Matthew Hennessy. Acceptance trees. *J. ACM*, 32(4):896–928, 1985.
35. 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 *Lect. Notes Comput. Sci.*, pages 226–241. Springer-Verlag, 2005.
36. Thomas A. Henzinger and Joseph Sifakis. The embedded systems design challenge. In Jayadev Misra, Tobias Nipkow, and Emil Sekerinski, editors, *FM*, volume 4085 of *Lect. Notes Comput. Sci.*, pages 1–15. Springer-Verlag, 2006.
37. Michael Huth and Marta Z. Kwiatkowska. Quantitative analysis and model checking. In *LICS*, pages 111–122. IEEE Computer Society, 1997.
38. Bart Jacobs and Erik Poll. A logic for the Java modeling language JML. In Heinrich Hußmann, editor, *FASE*, volume 2029 of *Lect. Notes Comput. Sci.*, pages 284–299. Springer-Verlag, 2001.
39. Bengt Jonsson and Kim G. Larsen. Specification and refinement of probabilistic processes. In *LICS*, pages 266–277. IEEE Computer Society, 1991.
40. Bartek Klin and Vladimiro Sassone. Structural operational semantics for stochastic and weighted transition systems. *Inf. Comput.*, 227:58–83, 2013.
41. Jan Křetínský and Salomon Sickert. MoTraS: A tool for modal transition systems and their extensions. In Dang Van Hung and Mizuhito Ogawa, editors, *ATVA*, volume 8172 of *Lect. Notes Comput. Sci.*, pages 487–491. Springer-Verlag, 2013. Tool accessible at `https://www7.in.tum.de/~kretinsk/motras.html`.
42. Kim G. Larsen. Proof systems for satisfiability in Hennessy-Milner logic with recursion. *Theor. Comput. Sci.*, 72(2&3):265–288, 1990.
43. Kim G. Larsen, Axel Legay, Louis-Marie Traonouez, and Andrzej Wąsowski. Robust specification of real time components. In Uli Fahrenberg and Stavros Tripakis, editors, *FORMATS*, volume 6919 of *Lect. Notes Comput. Sci.*, pages 129–144. Springer-Verlag, 2011.
44. Kim G. Larsen, Axel Legay, Louis-Marie Traonouez, and Andrzej Wąsowski. Robust synthesis for real-time systems. *Theor. Comput. Sci.*, 515:96–122, 2014.
45. Kim G. Larsen, Radu Mardare, and Prakash Panangaden. Taking it to the limit: Approximate reasoning for Markov processes. In Branislav Rovan, Vladimiro Sassone, and Peter Widmayer, editors, *MFCS*, volume 7464 of *Lect. Notes Comput. Sci.*, pages 681–692. Springer-Verlag, 2012.
46. Kim G. Larsen and Bent Thomsen. A modal process logic. In *LICS*, pages 203–210. IEEE Computer Society, 1988.
47. Kim G. Larsen and Liu Xinxin. Equation solving using modal transition systems. In *LICS*, pages 108–117. IEEE Computer Society, 1990.
48. F. William Lawvere. Metric spaces, generalized logic, and closed categories. *Rendiconti del seminario matématico e fisico di Milano*, XLIII:135–166, 1973.
49. Barbara Liskov and Jeannette M. Wing. A behavioral notion of subtyping. *ACM Trans. Program. Lang. Syst.*, 16(6):1811–1841, 1994.
50. Matteo Mio. Probabilistic modal mu-calculus with independent product. In Martin Hofmann, editor, *FOSSACS*, volume 6604 of *Lect. Notes Comput. Sci.*, pages 290–304. Springer-Verlag, 2011.

51. Carroll Morgan and Annabelle McIver. A probabilistic temporal calculus based on expectations. In *Formal Methods Pathific*, 1997.
52. Jean-Baptiste Raclet. Residual for component specifications. Publication interne 1843, IRISA, Rennes, 2007.
53. David Romero-Hernández and David de Frutos-Escrig. Defining distances for all process semantics. In Holger Giese and Grigore Rosu, editors, *FMOODS/FORTE*, volume 7273 of *Lect. Notes Comput. Sci.*, pages 169–185. Springer-Verlag, 2012.
54. David Romero-Hernández and David de Frutos-Escrig. Distances between processes: A pure algebraic approach. In Narciso Martí-Oliet and Miguel Palomino, editors, *WADT*, volume 7841 of *Lect. Notes Comput. Sci.*, pages 265–282. Springer-Verlag, 2012.
55. Joseph Sifakis. A vision for computer science - the system perspective. *Central Europ. J. Comput. Sci.*, 1(1):108–116, 2011.
56. Louis-Marie Traonouez. A parametric counterexample refinement approach for robust timed specifications. In Bauer and Raclet [6], pages 17–33.
57. Sebastián Uchitel and Marsha Chechik. Merging partial behavioural models. In Richard N. Taylor and Matthew B. Dwyer, editors, *SIGSOFT FSE*, pages 43–52. ACM, 2004.
58. Franck van Breugel and James Worrell. A behavioural pseudometric for probabilistic transition systems. *Theor. Comput. Sci.*, 331(1):115–142, 2005.
59. Pavol Černý, Thomas A. Henzinger, and Arjun Radhakrishna. Simulation distances. *Theor. Comput. Sci.*, 413(1):21–35, 2012.

Appendix: Proof of Theorem 7

$\underline{d^{\mathbb{L}}_{\mathsf{m}}(da(\mathcal{D}_1), da(\mathcal{D}_2)) \sqsubseteq_{\mathbb{L}} d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{D}_1, \mathcal{D}_2)}$:

Let $\mathcal{D}_1 = (S_1, S_1^0, \dashrightarrow_1, \longrightarrow_1)$ and $\mathcal{D}_2 = (S_2, S_2^0, \dashrightarrow_2, \longrightarrow_2)$ be DMTS. There exists a DMTS refinement family $R = \{R_\alpha \subseteq S_1 \times S_2 \mid \alpha \in \mathbb{L}\}$ such that for all $s_1^0 \in S_1^0$, there is $s_2^0 \in S_2^0$ with $(s_1^0, s_2^0) \in R_{d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{D}_1,\mathcal{D}_2)}$. We show that R is an NAA refinement family.

Let $\alpha \in \mathbb{L}$ and $(s_1, s_2) \in R_\alpha$. Let $M_1 \in \mathrm{Tran}_1(s_1)$ and define

$$M_2 = \big\{(a_2, t_2) \mid s_2 \overset{a_2}{\dashrightarrow}_2 t_2, \exists (a_1, t_1) \in M_1 : \exists \beta \in \mathbb{L} : (t_1, t_2) \in R_\beta, F(a_1, a_2, \beta) \sqsubseteq_{\mathbb{L}} \alpha\big\}.$$

The condition

$$\forall (a_2, t_2) \in M_2 : \exists (a_1, t_1) \in M_1, \beta \in \mathbb{L} : (t_1, t_2) \in R_\beta, F(a_1, a_2, \beta) \sqsubseteq \alpha$$

is satisfied by construction. For the inverse condition, let $(a_1, t_1) \in M_1$, then $s_1 \overset{a_1}{\dashrightarrow}_1 t_1$, and as R is a DMTS refinement family, this implies that there is $s_2 \overset{a_2}{\dashrightarrow}_2 t_2$ and $\beta \in \mathbb{L}$ for which $(t_1, t_2) \in R_\beta$ and $F(a_1, a_2, \beta) \sqsubseteq_{\mathbb{L}} \alpha$, so that $(a_2, t_2) \in M_2$ by construction.

We are left with showing that $M_2 \in \mathrm{Tran}_2(s_2)$. First we notice that by construction, indeed $s_2 \overset{a_2}{\dashrightarrow}_2 t_2$ for all $(a_2, t_2) \in M_2$. Now let $s_2 \longrightarrow N_2$; we need to show that $N_2 \cap M_2 \neq \emptyset$.

We have $s_1 \longrightarrow N_1$ such that $\forall (a_1, t_1) \in N_1 : \exists (a_2, t_2) \in N_2, \beta \in \mathbb{L} : (t_1, t_2) \in R_\beta, F(a_1, a_2, \beta) \sqsubseteq_{\mathbb{L}} \alpha$. We know that $N_1 \cap M_1 \neq \emptyset$, so let $(a_1, t_1) \in N_1 \cap M_1$. Then there is $(a_2, t_2) \in N_2$ and $\beta \in \mathbb{L}$ such that $(t_1, t_2) \in R_\beta$ and $F(a_1, a_2, \beta) \sqsubseteq_{\mathbb{L}} \alpha$. But $(a_2, t_2) \in N_2$ implies $s_2 \overset{a_2}{\dashrightarrow}_2 t_2$, hence $(a_2, t_2) \in M_2$.

$\underline{d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{D}_1, \mathcal{D}_2) \sqsubseteq_{\mathbb{L}} d^{\mathbb{L}}_{\mathsf{m}}(da(\mathcal{D}_1), da(\mathcal{D}_2))}$:

Let $\mathcal{D}_1 = (S_1, S_1^0, \dashrightarrow_1, \longrightarrow_1)$ and $\mathcal{D}_2 = (S_2, S_2^0, \dashrightarrow_2, \longrightarrow_2)$ be DMTS. There exists an NAA refinement family $R = \{R_\alpha \subseteq S_1 \times S_2 \mid \alpha \in \mathbb{L}\}$ such that for all $s_1^0 \in S_1^0$, there is $s_2^0 \in S_2^0$ for which $(s_1^0, s_2^0) \in R_{d^{\mathbb{L}}_{\mathsf{m}}(da(\mathcal{D}_1),da(\mathcal{D}_2))}$. We show that R is a DMTS refinement family. Let $\alpha \in \mathbb{L}$ and $(s_1, s_2) \in R_\alpha$.

Let $s_1 \overset{a_1}{\dashrightarrow}_1 t_1$, then we cannot have $s_1 \longrightarrow \emptyset$. Let $M_1 = \{(a_1, t_1)\} \cup \bigcup\{N_1 \mid s_1 \longrightarrow N_1\}$, then $M_1 \in \mathrm{Tran}_1(s_1)$ by construction. This implies that there is $M_2 \in \mathrm{Tran}_2(s_2)$, $(a_2, t_2) \in M_2$ and $\beta \in \mathbb{L}$ such that $(t_1, t_2) \in R_\beta$ and $F(a_1, a_2, \beta) \sqsubseteq_{\mathbb{L}} \alpha$, but then also $s_2 \overset{a_2}{\dashrightarrow} t_2$ as was to be shown.

Let $s_2 \longrightarrow N_2$ and assume, for the sake of contradiction, that there is no $s_1 \longrightarrow N_1$ for which $\forall (a_1, t_1) \in N_1 : \exists (a_2, t_2) \in N_2, \beta \in \mathbb{L} : (t_1, t_2) \in R_\beta, F(a_1, a_2, \beta) \sqsubseteq_{\mathbb{L}} \alpha$ holds. Then for each $s_1 \longrightarrow N_1$, there is an element $(a_{N_1}, t_{N_1}) \in N_1$ such that $\exists (a_2, t_2) \in N_2, \beta \in \mathbb{L} : (t_{N_1}, t_2) \in R_\beta, F(a_{N_1}, a_2, \beta) \sqsubseteq_{\mathbb{L}} \alpha$ does *not* hold.

Let $M_1 = \{(a_{N_1}, t_{N_1}) \mid s_1 \longrightarrow N_1\}$, then $M_1 \in \mathrm{Tran}_1(s_1)$ by construction. Hence we have $M_2 \in \mathrm{Tran}_2(s_2)$ such that $\forall (a_2, t_2) \in M_2 : \exists (a_1, t_2) \in M_1, \beta \in \mathbb{L} : (t_1, t_2) \in R_\beta, F(a_1, a_2, \beta) \sqsubseteq \alpha$. Now $N_2 \cap M_2 \neq \emptyset$, so let $(a_2, t_2) \in N_2 \cap M_2$, then there is $(a_1, t_1) \in M_1$ and $\beta \in \mathbb{L}$ such that $(t_1, t_2) \in R_\beta$ and $F(a_1, a_2, \beta) \sqsubseteq_{\mathbb{L}} \alpha$, in contradiction to how M_1 was constructed.

$\underline{d^{\mathbb{L}}_{\mathsf{m}}(ad(\mathcal{A}_1), ad(\mathcal{A}_2)) \sqsubseteq_{\mathbb{L}} d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_1, \mathcal{A}_2)}$:

Let $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$, $\mathcal{A}_2 = (S_2, S_2^0, \mathrm{Tran}_2)$ be NAA, with DMTS translations $ad(\mathcal{A}_1) = (D_1, D_1^0, \longrightarrow_1, \dashrightarrow_1)$, $ad(\mathcal{A}_2) = (D_2, D_2^0, \longrightarrow_2, \dashrightarrow_2)$. There is an NAA refinement family $R = \{R_\alpha \subseteq S_1 \times S_2 \mid \alpha \in \mathbb{L}\}$ such that for all $s_1^0 \in S_1^0$, there is $s_2^0 \in S_2^0$ with $(s_1^0, s_2^0) \in R_{d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_1,\mathcal{A}_2)}$.

Define a relation family $R' = \{R'_\alpha \subseteq D_1 \times D_2 \mid \alpha \in \mathbb{L}\}$ by

$$\begin{aligned} R'_\alpha = \big\{(M_1, M_2) \;\big|\; & \exists (s_1, s_2) \in R_\alpha : \\ & M_1 \in \mathrm{Tran}_1(s_1), M_2 \in \mathrm{Tran}(s_2), \\ & \forall (a_1, t_1) \in M_1 : \exists (a_2, t_2) \in M_2, \beta \in \mathbb{L} : \\ & \qquad (t_1, t_2) \in R_\beta, F(a_1, a_2, \beta) \sqsubseteq_{\mathbb{L}} \alpha, \\ & \forall (a_2, t_2) \in M_2 : \exists (a_1, t_1) \in M_1, \beta \in \mathbb{L} : \\ & \qquad (t_1, t_2) \in R_\beta, F(a_1, a_2, \beta) \sqsubseteq_{\mathbb{L}} \alpha\big\}. \end{aligned}$$

We show that R' is a witness for $d^{\mathbb{L}}_{\mathsf{m}}(ad(\mathcal{A}_1), ad(\mathcal{A}_2)) \sqsubseteq_{\mathbb{L}} d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_1, \mathcal{A}_2)$. Let $\alpha \in \mathbb{L}$ and $(M_1, M_2) \in R'_\alpha$.

Let $M_2 \longrightarrow_2 N_2$. By construction of $\longrightarrow$, there is $(a_2, t_2) \in M_2$ such that $N_2 = \{(a_2, M_2') \mid M_2' \in \mathrm{Tran}_2(t_2)\}$. Then $(M_1, M_2) \in R'_\alpha$ implies that there must be $(a_1, t_1) \in M_1$ and $\beta \in \mathbb{L}$ such that $(t_1, t_2) \in R_\beta$ and $F(a_1, a_2, \beta) \sqsubseteq_{\mathbb{L}} \alpha$. Let $N_1 = \{(a_1, M_1') \mid M_1' \in \mathrm{Tran}_1(t_1)\}$, then $M_1 \longrightarrow_1 N_1$.

We show that $\forall (a_1, M_1') \in N_1 : \exists (a_2, M_2') \in N_2 : (M_1', M_2') \in R'_\beta$: Let $(a_1, M_1') \in N_1$, then $M_1' \in \mathrm{Tran}_1(t_1)$. From $(t_1, t_2) \in R_\beta$ we get $M_2' \in \mathrm{Tran}_2(t_2)$ such that

$$\begin{aligned}\forall (b_1, u_1) \in M_1' : \exists (b_2, u_2) \in M_2', \gamma \in \mathbb{L} :\\ (u_1, u_2) \in R_\gamma, F(b_1, b_2, \gamma) \sqsubseteq_{\mathbb{L}} \beta\,,\\ \forall (b_2, u_2) \in M_2' : \exists (b_1, u_1) \in M_1', \gamma \in \mathbb{L} :\\ (u_1, u_2) \in R_\gamma, F(b_1, b_2, \gamma) \sqsubseteq_{\mathbb{L}} \beta\,,\end{aligned}$$

hence $(M_1', M_2') \in R'_\beta$; also, $(a_2, M_2') \in N_2$ by construction of N_2.

Let $M_1 \overset{a_1}{\dashrightarrow}_1 M_1'$, then we have $M_1 \longrightarrow_1 N_1$ for which $(a_1, M_1') \in N_1$ by construction of $\dashrightarrow_1$. This in turn implies that there must be $(a_1, t_1) \in M_1$ such that $N_1 = \{(a_1, M_1'') \mid M_1'' \in \mathrm{Tran}_1(t_1)\}$. By $(M_1, M_2) \in R'_\alpha$, we get $(a_2, t_2) \in M_2$ and $\beta \in \mathbb{L}$ such that $(t_1, t_2) \in R_\beta$ and $F(a_1, a_2, \beta) \sqsubseteq_{\mathbb{L}} \alpha$. Let $N_2 = \{(a_2, M_2') \mid M_2' \in \mathrm{Tran}_2(t_2)\}$, then $M_2 \longrightarrow_2 N_2$ and hence $M_2 \overset{a_2}{\dashrightarrow}_2 M_2'$ for all $(a_2, M_2') \in N_2$. By the same arguments as above, there is $(a_2, M_2') \in N_2$ for which $(M_1', M_2') \in R'_\beta$.

We miss to show that R' is initialized. Let $M_1^0 \in D_1^0$, then we have $s_1^0 \in S_1^0$ with $M_1^0 \in \mathrm{Tran}_1(s_1^0)$. As R is initialized, this entails that there is $s_2^0 \in S_2^0$ with $(s_1^0, s_2^0) \in R_{d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_1, \mathcal{A}_2)}$, which gives us $M_2^0 \in \mathrm{Tran}_2(s_2^0)$ which satisfies the conditions in the definition of $R'_{d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_1, \mathcal{A}_2)}$, whence $(M_1^0, M_2^0) \in R'_{d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_1, \mathcal{A}_2)}$.

$\underline{d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_1, \mathcal{A}_2) \sqsubseteq_{\mathbb{L}} d^{\mathbb{L}}_{\mathsf{m}}(ad(\mathcal{A}_1), ad(\mathcal{A}_2))}$:

Let $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$, $\mathcal{A}_2 = (S_2, S_2^0, \mathrm{Tran}_2)$ be NAA, with DMTS translations $ad(\mathcal{A}_1) = (D_1, D_1^0, \longrightarrow_1, \dashrightarrow_1)$, $ad(\mathcal{A}_2) = (D_2, D_2^0, \longrightarrow_2, \dashrightarrow_2)$. There is a DMTS refinement family $R = \{R_\alpha \subseteq D_1 \times D_2 \mid \alpha \in \mathbb{L}\}$ such that for all $M_1^0 \in D_1^0$, there exists $M_2^0 \in D_2^0$ with $(M_1^0, M_2^0) \in R_{d^{\mathbb{L}}_{\mathsf{m}}(ad(\mathcal{A}_1), ad(\mathcal{A}_2))}$.

Define a relation family $R' = \{R'_\alpha \subseteq S_1 \times S_2 \mid \alpha \in \mathbb{L}\}$ by

$$R'_\alpha = \big\{(s_1, s_2) \;\big|\; \forall M_1 \in \mathrm{Tran}_1(s_1) : \exists M_2 \in \mathrm{Tran}_2(s_2) : (M_1, M_2) \in R_\alpha\big\}\,;$$

we will show that R' is a witness for $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_1, \mathcal{A}_2) \sqsubseteq_{\mathbb{L}} d^{\mathbb{L}}_{\mathsf{m}}(ad(\mathcal{A}_1), ad(\mathcal{A}_2))$.

Let $\alpha \in \mathbb{L}$, $(s_1, s_2) \in R'_\alpha$ and $M_1 \in \mathrm{Tran}_1(s_1)$, then by construction of R', we have $M_2 \in \mathrm{Tran}_2(s_2)$ with $(M_1, M_2) \in R_\alpha$.

Let $(a_2, t_2) \in M_2$ and define $N_2 = \{(a_2, M_2') \mid M_2' \in \mathrm{Tran}_2(t_2)\}$, then $M_2 \longrightarrow_2 N_2$. Now $(M_1, M_2) \in R_\alpha$ implies that there must be $M_1 \longrightarrow_1 N_1$ satisfying $\forall (a_1, M_1') \in N_1 : \exists (a_2, M_2') \in N_2, \beta \in \mathbb{L} : (M_1', M_2') \in R_\beta, F(a_1, a_2, \beta) \sqsubseteq_{\mathbb{L}} \alpha$. We have $(a_1, t_1) \in M_1$ such that $N_1 = \{(a_1, M_1') \mid M_1' \in \mathrm{Tran}_1(t_1)\}$; we only miss to show that $(t_1, t_2) \in R'_\beta$ for some $\beta \in \mathbb{L}$ for which $F(a_1, a_2, \beta) \sqsubseteq_{\mathbb{L}} \alpha$. Let $M_1' \in \mathrm{Tran}_1(t_1)$, then $(a_1, M_1') \in N_1$, hence there is $(a_2, M_2') \in N_2$ and $\beta \in \mathbb{L}$ such that $(M_1', M_2') \in R_\beta$ and $F(a_1, a_2, \beta) \sqsubseteq \alpha$, but $(a_2, M_2') \in N_2$ also entails $M_2' \in \mathrm{Tran}_2(t_2)$.

Let $(a_1, t_1) \in M_1$ and define $N_1 = \{(a_1, M_1') \mid M_1' \in \mathrm{Tran}_1(t_1)\}$, then $M_1 \longrightarrow_1 N_1$. Now let $(a_1, M_1') \in N_1$, then $M_1 \overset{a_1}{\dashrightarrow}_1 M_1'$, hence we have $M_2 \overset{a_2}{\dashrightarrow}_2 M_2'$ and $\beta \in \mathbb{L}$ such that $(M_1', M_2') \in R_\beta$ and $F(a_1, a_2, \beta) \sqsubseteq_{\mathbb{L}} \alpha$. By construction of $\dashrightarrow_2$, this implies that there is $M_2 \longrightarrow_2 N_2$ with $(a_2, M_2') \in N_2$, and we have $(a_2, t_2) \in M_2$ for which $N_2 = \{(a_2, M_2'') \mid M_2'' \in \mathrm{Tran}_2(t_2)\}$. Now if $M_1'' \in \mathrm{Tran}_1(t_1)$, then $(a_1, M_1'') \in N_1$, hence there is $(a_2, M_2'') \in N_2$ with $(M_1'', M_2'') \in R_\beta$, but $(a, M_2'') \in N_2$ also gives $M_2'' \in \mathrm{Tran}_2(t_2)$.

We miss to show that R' is initialized. Let $s_1^0 \in S_1^0$ and $M_1^0 \in \mathrm{Tran}_1(s_1^0)$. As R is initialized, this gets us $M_2^0 \in D_2$ with $(M_1^0, M_2^0) \in R_{d^{\mathbb{L}}_{\mathsf{m}}(ad(\mathcal{A}_1), ad(\mathcal{A}_2))}$, but $M_2^0 \in \mathrm{Tran}_2(s_2^0)$ for some $s_2^0 \in S_2^0$, and then $(s_1^0, s_2^0) \in R'_{d^{\mathbb{L}}_{\mathsf{m}}(ad(\mathcal{A}_1), ad(\mathcal{A}_2))}$.

$\underline{d^{\mathbb{L}}_{\mathsf{m}}(dn(\mathcal{D}_1), dn(\mathcal{D}_2)) \sqsubseteq_{\mathbb{L}} d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{D}_1, \mathcal{D}_2)}$:

Let $\mathcal{D}_1 = (S_1, S_1^0, \dashrightarrow_1, \longrightarrow_1)$ and $\mathcal{D}_2 = (S_2, S_2^0, \dashrightarrow_2, \longrightarrow_2)$ be DMTS, with ν-calculus translations $dn(\mathcal{D}_1) = (S_1, S_1^0, \Delta_1)$ and $dn(\mathcal{D}_2) = (S_2, S_2^0, \Delta_2)$. There is a DMTS refinement family $R = \{R_\alpha \subseteq S_1 \times S_2 \mid \alpha \in \mathbb{L}\}$ such that for all $s_1^0 \in S_1^0$, there exists $s_2^0 \in S_2^0$ for which $(s_1^0, s_2^0) \in R_{d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{D}_1, \mathcal{D}_2)}$.

Let $\alpha \in \mathbb{L}$, $(s_1, s_2) \in R_\alpha$, $a_1 \in \Sigma$, and $t_1 \in \Box_1^{a_1}(s_1)$. Then $s_1 \overset{a_1}{\dashrightarrow}_1 t_1$, hence we have $s_2 \overset{a_2}{\dashrightarrow}_2 t_2$ and $\beta \in \mathbb{L}$ with $(t_1, t_2) \in R_\beta$ and $F(a_1, a_2, \beta) \sqsubseteq_{\mathbb{L}} \alpha$, but then also $t_2 \in \Box_2^{a_2}(s_2)$.

Let $N_2 \in \Diamond_2(s_2)$, then also $s_2 \longrightarrow_2 N_2$, so that there must be $s_1 \longrightarrow_1 N_1$ such that $\forall (a_1, t_1) \in N_1 : \exists (a_2, t_2) \in N_2, \beta \in \mathbb{L} : (t_1, t_2) \in R_\beta, F(a_1, a_2, \beta) \sqsubseteq_{\mathbb{L}} \alpha$, but then also $N_1 \in \Diamond_1(s_1)$.

$\underline{d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{D}_1, \mathcal{D}_2) \sqsubseteq_{\mathbb{L}} d^{\mathbb{L}}_{\mathsf{m}}(dn(\mathcal{D}_1), dn(\mathcal{D}_2))}$:

Let $\mathcal{D}_1 = (S_1, S_1^0, \dashrightarrow_1, \longrightarrow_1)$ and $\mathcal{D}_2 = (S_2, S_2^0, \dashrightarrow_2, \longrightarrow_2)$ be DMTS, with ν-calculus translations $dn(\mathcal{D}_1) = (S_1, S_1^0, \Delta_1)$ and $dn(\mathcal{D}_2) = (S_2, S_2^0, \Delta_2)$. There is a ν-calculus refinement family $R = \{R_\alpha \subseteq S_1 \times S_2 \mid \alpha \in \mathbb{L}\}$ such that for all $s_1^0 \in S_1^0$, there exists $s_2^0 \in S_2^0$ for which $(s_1^0, s_2^0) \in R_{d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{D}_1, \mathcal{D}_2)}$.

Let $\alpha \in \mathbb{L}$ and $(s_1, s_2) \in R_\alpha$, and assume that $s_1 \overset{a_1}{\dashrightarrow}_1 t_1$. Then $t_1 \in \Box_1^{a_1}(s_1)$, so that there is $a_2 \in \Sigma$, $t_2 \in \Box_2^{a_2}(s_2)$ and $\beta \in \mathbb{L}$ for which $(t_1, t_2) \in R_\beta$ and $F(a_1, a_2, \beta) \sqsubseteq_{\mathbb{L}} \alpha$, but then also $s_2 \overset{a_2}{\dashrightarrow}_2 t_2$.

Assume that $s_2 \longrightarrow_2 N_2$, then $N_2 \in \Diamond_2(s_2)$. Hence there is $N_1 \in \Diamond_1(s_1)$ so that $\forall (a_1,t_1) \in N_1 : \exists (a_2,t_2) \in N_2, \beta \in \mathbb{L} : (t_1,t_2) \in R_\beta, F(a_1,a_2,\beta) \sqsubseteq_{\mathbb{L}} \alpha$, but then also $s_1 \longrightarrow_1 N_1$.

$\underline{d^{\mathbb{L}}_{\mathsf{m}}(nd(\mathcal{N}_1), nd(\mathcal{N}_2)) \sqsubseteq_{\mathbb{L}} d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{N}_1,\mathcal{N}_2)}$:

Let $\mathcal{N}_1 = (X_1, X_1^0, \Delta_1)$, $\mathcal{N}_2 = (X_2, X_2^0, \Delta_2)$ be ν-calculus expressions in normal form, with DMTS translations $nd(\mathcal{N}_1) = (X_1, X_1^0, \dashrightarrow_1, \longrightarrow_1)$ and $nd(\mathcal{N}_2) = (X_2, X_2^0, \dashrightarrow_2, \longrightarrow_2)$. There is a ν-calculus refinement family $R = \{R_\alpha \subseteq X_1 \times X_2 \mid \alpha \in \mathbb{L}\}$ such that for all $x_1^0 \in X_1^0$, there is $x_2^0 \in X_2^0$ for which $(x_1^0, x_2^0) \in R_{d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{N}_1,\mathcal{N}_2)}$.

Let $\alpha \in \mathbb{L}$ and $(x_1,x_2) \in R_\alpha$, and assume that $x_1 \overset{a_1}{\dashrightarrow}_1 y_1$. Then $y_1 \in \Box_1^{a_1}(x_1)$, hence there are $a_2 \in \Sigma$, $y_2 \in \Box_2^{a_2}$ and $\beta \in \mathbb{L}$ such that $(y_1,y_2) \in R_\beta$ and $F(a_1,a_2,\beta) \sqsubseteq_{\mathbb{L}} \alpha$, but then also $x_2 \overset{a_2}{\dashrightarrow}_2 y_2$.

Assume that $x_2 \longrightarrow_2 N_2$, then $N_2 \in \Diamond_2(x_2)$. Hence there must be $N_1 \in \Diamond_1(x_1)$ such that $\forall (a_1,y_1) \in N_1 : \exists (a_2,y_2) \in N_2, \beta \in \mathbb{L} : (y_1,y_2) \in R_\beta, F(a_1,a_2,\beta) \sqsubseteq_{\mathbb{L}} \alpha$, but then also $x_1 \longrightarrow_1 N_1$.

$\underline{d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{N}_1,\mathcal{N}_2) \sqsubseteq_{\mathbb{L}} d^{\mathbb{L}}_{\mathsf{m}}(nd(\mathcal{N}_1), nd(\mathcal{N}_2))}$:

Let $\mathcal{N}_1 = (X_1, X_1^0, \Delta_1)$, $\mathcal{N}_2 = (X_2, X_2^0, \Delta_2)$ be ν-calculus expressions in normal form, with DMTS translations $nd(\mathcal{N}_1) = (X_1, X_1^0, \dashrightarrow_1, \longrightarrow_1)$ and $nd(\mathcal{N}_2) = (X_2, X_2^0, \dashrightarrow_2, \longrightarrow_2)$. There is a DMTS refinement family $R = \{R_\alpha \subseteq X_1 \times X_2 \mid \alpha \in \mathbb{L}\}$ such that for all $x_1^0 \in X_1^0$, there is $x_2^0 \in X_2^0$ for which $(x_1^0, x_2^0) \in R_{d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{N}_1,\mathcal{N}_2)}$.

Let $\alpha \in \mathbb{L}$, $(x_1,x_2) \in R_\alpha$, $a_1 \in \Sigma$, and $y_1 \in \Box_1^{a_1}(x_1)$. Then $x_1 \overset{a_1}{\dashrightarrow}_1 y_1$, hence we have $x_2 \overset{a_2}{\dashrightarrow}_2 y_2$ and $\beta \in \mathbb{L}$ so that $(y_1,y_2) \in R_\beta$ and $F(a_1,a_2,\beta) \sqsubseteq_{\mathbb{L}} \alpha$, but then also $y_1 \in \Box_2^{a_2}(x_2)$.

Let $N_2 \in \Diamond_2(x_2)$, then also $x_2 \longrightarrow_2 N_2$. Hence we must have $x_1 \longrightarrow_1 N_1$ with $\forall (a_1,y_1) \in N_1 : \exists (a_2,y_2) \in N_2, \beta \in \mathbb{L} : (y_1,y_2) \in R_\beta, F(a_1,a_2,\beta) \sqsubseteq_{\mathbb{L}} \alpha$, but then also $N_1 \in \Diamond_1(x_1)$. $\square$