Compositionality for Quantitative Specifications

Uli Fahrenberg[1], Jan Křetínský[2], Axel Legay[1], and Louis-Marie Traonouez[1]

[1] IRISA / Inria Rennes
[2] IST Austria

Abstract. We consider the partial behavior model framework of disjunctive modal transition systems. We extend the framework to a general quantitative setting and show that also in this quantitative setting, modal transition systems and the modal nu-calculus are closely related. The main technical contribution is that our quantitative framework is compositional with respect to general notions of distances between systems and the standard operations. Moreover, we show how to compute the results of the operations, including the quotient, which has not been previously considered for quantitative non-deterministic systems. This allows for compositional and step-wise design and verification of systems with quantitative information, such as rewards, time or energy.

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 written, 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.

The behavioral formalism we work with is *modal transition systems* (MTS) [28] 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*-transition represent behavior that is allowed, but not required to be implemented. A simple example of a vending machine specification s, in Fig. 1 on the left, 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 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 on the right.

In order to relate such specifications, MTS with *structured labels* were introduced [5]. Given a preorder on labels, relating for instance coffee $\preccurlyeq$ beverage,

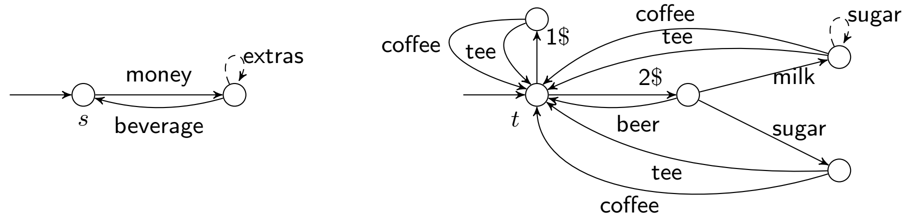


Fig. 1. Two specifications of a vending machine

we can refine a transition label into one which is below, for example implement "beverage" with its refinement "coffee". Then t will be a refinement of s.

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 durations or energy consumption. As an example, consider the simple real-time property to the left in Fig. 2: "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 $0 \leq l \leq r \leq 5$.

However, here we identify several shortcomings of the current approaches:

Expressive power. The current theory of structured labels is available only for the basic MTS. Very often one needs to use richer structures such as *disjunctive* MTS (DMTS) [8, 29] or acceptance automata [21, 31]. While MTS generally cannot express disjunction of properties, DMTS and further related formalisms can and are, in fact, equivalent to the ν-calculus [7]. This allows, for instance, to prohibit deadlocks as in the example to the right in Fig. 2. 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 [7] to our setting. Fig. 3 (left) shows a ν-calculus translation of the second quantitative specification of Fig. 2.

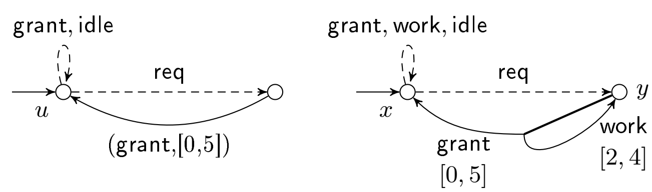


Fig. 2. Two simple quantitative specifications

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

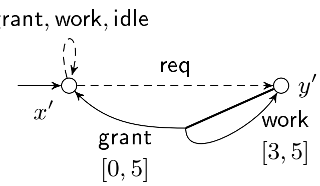


Fig. 3. A quantitative ν-calculus expression (left) and a quantitative DMTS

Robustness. Consider the grant issuing example u. While an implementation issuing grant after precisely 5 time units is a valid refinement, if there is but a small positive drift in the implementation, it is not a refinement 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 [23] and should be replaced by notions more robust to perturbations. As an example, the DMTS in Fig. 3 is *not* a refinement of the second one in Fig. 2, but for all practical purposes, it is very close.

One approach is to employ metric *distances* instead of Boolean relations; this has been done for example in [12–14, 16, 22, 27, 32, 33, 35, 36]. 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 [3, 4] and shown in [4, 18] 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 composition $s_1 \parallel s_2$ should be close to $t_1 \parallel t_2$. 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 system 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 [7] 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 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 [30] over the Java modeling language JML [24] or correct-by-design class diagrams operations [17] to interface theories close to MTS such as interface automata [15] 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 [7,9].

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 $\llbracket a \rrbracket = \{ b \in \Gamma \mid b \preccurlyeq a \}$. Note that $a \preccurlyeq b$ implies $\llbracket a \rrbracket \subseteq \llbracket b \rrbracket$ for all $a, b \in \Sigma$.

Example 1. A trivial but important example of our label structure is the *discrete* one in which label preorder $\preccurlyeq$ is equality. 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 $\llbracket a \rrbracket = a$ for all $a \in \Sigma$. (Hence we identify implementation labels with one-element subsets of Σ.) ☐

Label operations. Specification theories come equipped with several standard operations that make compositional software design possible [2]: conjunction for merging viewpoints covering different system's aspects [6,34], structural composition for running components in parallel, and quotient to synthesize missing parts of systems [29]. 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 $\owedge : \Sigma \times \Sigma \rightharpoonup \Sigma$ for which it holds that

(1) if $a_1 \owedge a_2$ is defined, then $a_1 \owedge a_2 \preccurlyeq a_1$ and $a_1 \owedge a_2 \preccurlyeq a_2$, and
(2) if $a_3 \preccurlyeq a_1$ and $a_3 \preccurlyeq a_2$, then $a_1 \owedge a_2$ is defined and $a_3 \preccurlyeq a_1 \owedge a_2$.

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

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

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

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

Finally, for the general case of specification labels as sets of implementation labels, the unique conjunction is $a_1 \owedge a_2 = a_1 \cap a_2$. □

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

Example 3. For discrete labels, the conjunction of Example 2 is the same as CSP-style composition, but other compositions may 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.*,

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

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

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

Yet another operator uses interval *intersection* instead, *i.e.*, $\overset{\cap}{\oplus} = \owedge$; this is useful if the intervals model deadlines.

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

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 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.

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 Section 1 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 [29] in the context of equation solving, or *quotient* of specifications by processes. They are a natural closure of *modal* transition systems [28], which are DMTS in which all disjunctive must-transitions $s \longrightarrow N$ lead to singletons $N = \{(a, t)\}$.

We introduce a notion of modal refinement of DMTS with structured labels. It coincides with the classical definition [29] on discrete labels.

Definition 5. *Let* $\mathcal{D}_1 = (S_1, S_1^0, \dashrightarrow_1, \longrightarrow_1)$, $\mathcal{D}_2 = (S_2, S_2^0, \dashrightarrow_2, \longrightarrow_2)$ *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 a modal refinement* R *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* $(s_1^0, s_2^0) \in R$.

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 $[\![\mathcal{D}]\!] = \{\mathcal{I} \leq_{\mathsf{m}} \mathcal{D} \mid \mathcal{I} \text{ implementation}\}$. 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.

Proposition 6. *For all DMTS* $\mathcal{D}_1$, $\mathcal{D}_2$, $\mathcal{D}_1 \leq_{\mathsf{m}} \mathcal{D}_2$ *implies* $\mathcal{D}_1 \leq_{\mathsf{th}} \mathcal{D}_2$. □

Acceptance automata. A (non-deterministic) *acceptance automaton* (AA) 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 AA 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 AA implementations are isomorphic to LTS. Acceptance automata were first introduced in [31], based on the notion of acceptance trees in [21]; 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 AA. 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

$$\begin{aligned}&\text{for all } (a_1, t_1) \in M_1 \text{ there is } (a_2, t_2) \in M_2 \text{ with } a_1 \preccurlyeq a_2 \text{ and } (t_1, t_2) \in R\,,\\&\text{for all } (a_2, t_2) \in M_2 \text{ there is } (a_1, t_1) \in M_1 \text{ with } a_1 \preccurlyeq a_2 \text{ and } (t_1, t_2) \in R\,.\end{aligned} \tag{1}$$

The definition degrades to the one of [31] in case labels are discrete. We will write $M_1 \preccurlyeq_R M_2$ if M_1, M_2 satisfy (1).

In [7], the following translations were discovered between DMTS and AA: 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 AA $da(\mathcal{D}) = (S, S^0, \mathrm{Tran})$. For an AA $\mathcal{A} = (S, S^0, \mathrm{Tran})$, define the DMTS $ad(\mathcal{A}) = (D, D^0, \dashrightarrow, \longrightarrow)$ by

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

Similarly to a theorem of [7, 19], we can now show the following:

Theorem 7. *For DMTS $\mathcal{D}_1$, $\mathcal{D}_2$ and AA $\mathcal{A}_1$, $\mathcal{A}_2$, $\mathcal{D}_1 \leq_{\mathsf{m}} \mathcal{D}_2$ 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 AA 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. [19] shows that this blow-up is unavoidable.

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

The Modal ν-Calculus. In [7], translations were discovered between DMTS and the modal ν-calculus, and refining the translations in [19], we could show that for discrete labels, these formalisms are *structurally equivalent*. We use the representation by equation systems in Hennessy-Milner logic developed in [26]. 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*.

The semantics of ν-calculus expressions is usually given as a greatest fixed point to a declaration, *cf.* [26]. In [19] we have introduced another semantics, which is given by a notion of refinement, like for DMTS and AA. For this we need a normal form for ν-calculus expressions:

Lemma 8 ([19]). *For any ν-calculus expression $\mathcal{N}_1 = (X_1, X_1^0, \Delta_1)$, there exists another expression $\mathcal{N}_2 = (X_2, X_2^0, \Delta_2)$ 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,

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

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 $(y_1, y_2) \in R$.

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

It is shown in [19] that the refinement semantics and the standard fixed-point semantics for ν-calculus expressions agree, *i.e.*, that an LTS $\mathcal{I}$ is an implementation of an expression $\mathcal{N}$ iff $\mathcal{I} \le_{\mathsf{m}} \mathcal{N}$. Here we have used an embedding of LTS into ν-calculus similar to the one into DMTS or AA, *cf.* [19].

4 Specification theory

Structural specifications typically come equipped with operations which allow for *compositional reasoning*, *viz.* conjunction, structural composition, and quotient, *cf.* [2]. On deterministic MTS, these operations can be given easily using simple structural operational rules (for such semantics of weighted systems, see e.g. [25]). For non-deterministic systems this is significantly harder; in [7] it is shown that DMTS and AA 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 [20] or spatial logic [10], and were extended to very general contexts [11]. 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 AA). Consequently [19], structural composition is generally only a sound over-approximation of the semantic composition.

Given the equivalence of DMTS, AA 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.

Disjunction and conjunction. Disjunction of specifications is easily defined as we allow multiple initial states. For DMTS $\mathcal{D}_1 = (S_1, S_1^0, \dashrightarrow_1, \longrightarrow_1)$, $\mathcal{D}_2 = (S_2, S_2^0, \dashrightarrow_2, \longrightarrow_2)$, 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

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

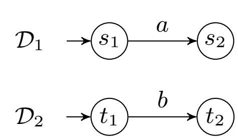
Theorem 10. *For all specifications $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$,*

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

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 $\equiv_{\mathsf{m}}$.

Structural composition. For AA $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$, $\mathcal{A}_2 = (S_2, S_2^0, \mathrm{Tran}_2)$, 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 to the right, 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 [4]. For DMTS specifications (and hence also for ν-calculus expressions), the back translation from AA to DMTS entails an exponential explosion.

Theorem 11. *Up to $\equiv_{\mathsf{m}}$, the operator $\|$ is associative, commutative and monotone, and $\bot \| \mathcal{S} \equiv_{\mathsf{m}} \bot$ for any specification $\mathcal{S}$.*

Corollary 12 (Independent implementability). *For all specifications $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$, $\mathcal{S}_4$, $\mathcal{S}_1 \le_{\mathsf{m}} \mathcal{S}_3$ and $\mathcal{S}_2 \le_{\mathsf{m}} \mathcal{S}_4$ imply $\mathcal{S}_1 \| \mathcal{S}_2 \le_{\mathsf{m}} \mathcal{S}_3 \| \mathcal{S}_4$.* □

Quotient. Because of non-determinism, we have to use a subset construction for the quotient, as opposed to conjunction and structural composition where product is sufficient. For AA $\mathcal{A}_3 = (S_3, S_3^0, \mathrm{Tran}_3)$, $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$, 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 $\{s_3^1/s_1^1, \dots, s_3^n/s_1^n)\}$ instead of $\{(s_3^1, s_1^1), \dots, (s_3^n, s_1^n))\}$. 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

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

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:

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

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

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

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 13. Consider the two simple systems in Fig. 4 and their quotient under $\overset{\cap}{\oplus}$, *i.e.*, where label synchronization is intersection. During the construction and the translation back to DMTS, many states were eliminated as they were inconsistent (their Tran-set was empty). For instance, there is no may transition to state $\{s_2/t_2\}$, because when it is composed with t_2 there is no guarantee of late-transition, hence no guarantee to refine s_2.

Theorem 14. *For all specifications $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$, $\mathcal{S}_1 \| \mathcal{S}_2 \le_{\mathsf{m}} \mathcal{S}_3$ iff $\mathcal{S}_2 \le_{\mathsf{m}} \mathcal{S}_3 / \mathcal{S}_1$.*

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

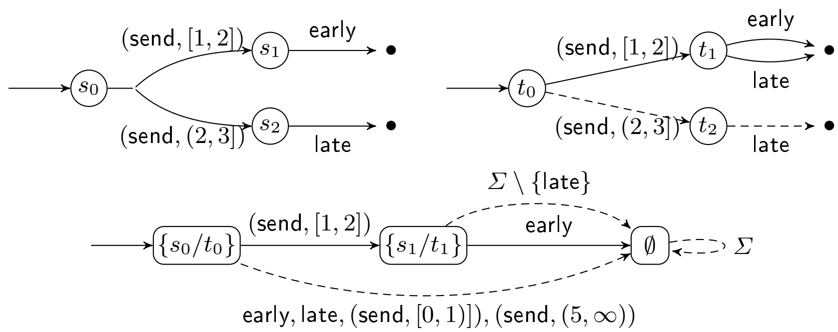


Fig. 4. Two DMTS and their quotient.

refinement *distances*. We have shown in [4, 18] that an appropriate 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.

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.

A *recursive trace distance specification* $\mathcal{F} = (\mathbb{L}, \mathsf{eval}, d_\mathsf{t}^\mathbb{L}, F)$ consists of a quantale $\mathbb{L}$, a quantale morphism $\mathsf{eval} : \mathbb{L} \to \mathbb{R}_{\geq 0} \cup \{\infty\}$, an $\mathbb{L}$-hemimetric $d_\mathsf{t}^\mathbb{L} : \Sigma^\infty \times \Sigma^\infty \to \mathbb{L}$ (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 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 $d_\mathsf{t}^\mathbb{L}$ recursively in the sense that for all $a, b \in \Sigma$ and all $\sigma, \tau \in \Sigma^\infty$ (and with . denoting concatenation),

$$d_\mathsf{t}^\mathbb{L}(a.\sigma, b.\tau) = F(a, b, d_\mathsf{t}^\mathbb{L}(\sigma, \tau)) . \tag{3}$$

The *trace distance* associated with such a distance specification is $d_\mathsf{t} : \Sigma^\infty \times \Sigma^\infty \to \mathbb{R}_{\geq 0}$ given by $d_\mathsf{t} = \mathsf{eval} \circ d_\mathsf{t}^\mathbb{L}$. Note that $d_\mathsf{t}^\mathbb{L}$ 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 $d_\mathsf{t}^\mathbb{L}(a, b) = \bot_\mathbb{L}$. Then (3) implies that whenever $a \preccurlyeq b$, then $F(a, b, \bot_\mathbb{L}) = d_\mathsf{t}^\mathbb{L}(a, b) = \bot_\mathbb{L}$.

Example 15. It is shown in [4, 18] that all commonly used trace distances obey recursive characterizations as above. We give a few examples:

- The *point-wise* distance from [13], for example, has $\mathbb{L} = \mathbb{R}_{\geq 0} \cup \{\infty\}$, $\mathsf{eval} = \mathsf{id}$ and $d_{\mathsf{t}}^{\mathbb{L}}(a.\sigma, b.\tau) = \max(d(a,b), d_{\mathsf{t}}^{\mathbb{L}}(\sigma,\tau))$, 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 $d((u_1,[l_1,r_1]),(u_2,[l_2,r_2])) = \sup_{x_1 \in [l_1,r_1]} \inf_{x_2 \in [l_2,r_2]} |x_1 - x_2|$ if $u_1 = u_2$ and ∞ otherwise, *cf.* [3].
- The *discounting* distance, also used in [13], again uses $\mathbb{L} = \mathbb{R}_{\geq 0} \cup \{\infty\}$ and $\mathsf{eval} = \mathsf{id}$, but $d_{\mathsf{t}}^{\mathbb{L}}(a.\sigma, b.\tau) = d(a,b) + \lambda d_{\mathsf{t}}^{\mathbb{L}}(\sigma,\tau)$ for a constant $\lambda \in [0,1[$.
- For the limit-average distance used in [36] and others, $\mathbb{L} = (\mathbb{R}_{\geq 0} \cup \{\infty\})^{\mathbb{N}}$, $\mathsf{eval}(\alpha) = \liminf_{j \in \mathbb{N}} \alpha(j)$, $d_{\mathsf{t}}^{\mathbb{L}}(a.\sigma, b.\tau)(j) = \frac{1}{j+1} d(a,b) + \frac{j}{j+1} d_{\mathsf{t}}^{\mathbb{L}}(\sigma,\tau)(j-1)$.
- The *discrete* trace distance is given by $d_{\mathsf{t}}(\sigma,\tau) = 0$ 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 $d_{\mathsf{t}}(a.\sigma, b.\tau) = d_{\mathsf{t}}(\sigma,\tau)$ if $a \preccurlyeq b$ and ∞ otherwise.

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

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

Definition 16. *The* lifted refinement distance *on the states of DMTS $\mathcal{D}_1 = (S_1, S_1^0, \dashrightarrow_1, \longrightarrow_1)$, $\mathcal{D}_2 = (S_2, S_2^0, \dashrightarrow_2, \longrightarrow_2)$ is the least fixed point to the equations*

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

For AA $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$, $\mathcal{A}_2 = (S_2, S_2^0, \mathrm{Tran}_2)$, the equations are instead

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

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

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

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.)

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 $d^{\mathbb{L}}_{\mathsf{th}}(\mathcal{S}_1, \mathcal{S}_2) = \sup_{\mathcal{I}_1 \in [\![\mathcal{S}_1]\!]} \inf_{\mathcal{I}_2 \in [\![\mathcal{S}_2]\!]} d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{I}_1, \mathcal{I}_2)$. Using the eval function, one gets non-lifted distances $d_{\mathsf{m}} = \mathsf{eval} \circ d^{\mathbb{L}}_{\mathsf{m}}$ and $d_{\mathsf{th}} = \mathsf{eval} \circ d^{\mathbb{L}}_{\mathsf{th}}$, with values in $\mathbb{R}_{\geq 0} \cup \{\infty\}$, which will be the ones one is interested in for concrete applications.

Example 17. We compute the *discounted* refinement distance between the second DMTS in Figs. 2 and 3, assuming sup-inf distance on quantitative labels. We have $d_{\mathsf{m}}(x, x') = \max(0 + \lambda d_{\mathsf{m}}(x, x'), 0 + \lambda d_{\mathsf{m}}(y, y'))$ and $d_{\mathsf{m}}(y, y') = \max(0 + \lambda d_{\mathsf{m}}(x, x'), 1 + \lambda d_{\mathsf{m}}(y, y')$, whose least fixed point is $d_{\mathsf{m}}(x, x') = \frac{\lambda}{1-\lambda}$. Similarly, $d_{\mathsf{m}}(x', x) = \frac{\lambda}{1-\lambda}$. Note that $x \not\leq_{\mathsf{m}} x'$ and $x' \not\leq_{\mathsf{m}} x$.

The following quantitative extension of Theorems 7 and 9 shows that our translations preserve and reflect refinement distances.

Theorem 18. *For all DMTS $\mathcal{D}_1, \mathcal{D}_2$, all AA $\mathcal{A}_1$, $\mathcal{A}_2$ and all ν-calculus expressions $\mathcal{N}_1$, $\mathcal{N}_2$, $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{D}_1, \mathcal{D}_2) = d^{\mathbb{L}}_{\mathsf{m}}(da(\mathcal{D}_1), da(\mathcal{D}_2))$, $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{A}_1, \mathcal{A}_2) = d^{\mathbb{L}}_{\mathsf{m}}(ad(\mathcal{A}_1), ad(\mathcal{A}_2))$, $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{D}_1, \mathcal{D}_2) = d^{\mathbb{L}}_{\mathsf{m}}(dn(\mathcal{D}_1), dn(\mathcal{D}_2))$, and $d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{N}_1, \mathcal{N}_2) = d^{\mathbb{L}}_{\mathsf{m}}(nd(\mathcal{N}_1), nd(\mathcal{N}_2))$.*

Our distances behave as expected:

Proposition 19. *The functions $d^{\mathbb{L}}_{\mathsf{m}}$, $d^{\mathbb{L}}_{\mathsf{th}}$ are $\mathbb{L}$-hemimetrics, and d_{m}, d_{th} are hemimetrics. For 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 $d^{\mathbb{L}}_{\mathsf{th}}(\mathcal{S}_1, \mathcal{S}_2) = \bot_{\mathbb{L}}$.*

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.*

As a quantitative analogy to the implication from (Boolean) modal refinement to thorough refinement (Proposition 6), 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 19), this is equivalent to the Boolean statement.

Theorem 20. *For all specifications $\mathcal{S}_1$, $\mathcal{S}_2$, $d^{\mathbb{L}}_{\mathsf{th}}(\mathcal{S}_1, \mathcal{S}_2) \sqsubseteq_{\mathbb{L}} d^{\mathbb{L}}_{\mathsf{m}}(\mathcal{S}_1, \mathcal{S}_2)$.*

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 $F(b_1, b_2, \beta) \neq \top$, $a_1 \oplus b_1$ is defined iff $a_2 \oplus b_2$ is, and if both are defined, then

$$F(a_1 \oplus b_1, a_2 \oplus b_2, P(\alpha, \beta)) \sqsubseteq_{\mathbb{L}} P(F(a_1, a_2, \alpha), F(b_1, b_2, \beta)) \,. \tag{4}$$

Note that (4) implies that $d_{\mathsf{t}}(a_1 \oplus a_2, b_1 \oplus b_2) \sqsubseteq_{\mathbb{L}} P(d_{\mathsf{t}}(a_1, b_1), d_{\mathsf{t}}(a_2, b_2))$. Hence P provides a uniform bound on distances between synchronized labels, and (4) extends this property so that it holds recursively. Also, this is a generalization of the condition that we imposed on $\oplus$ in Section 2; it is shown in [4] 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 12) and that quotient preserves and reflects refinement distance (a quantitative generalization of Theorem 14).

Theorem 21. *For all specifications* $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$, $\mathcal{S}_4$, $d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{S}_1 \| \mathcal{S}_2, \mathcal{S}_3 \| \mathcal{S}_4) \sqsubseteq_{\mathbb{L}} P(d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{S}_1, \mathcal{S}_3), d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{S}_2, \mathcal{S}_4))$.

Theorem 22. *For all specifications* $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$, $d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{S}_1 \| \mathcal{S}_2, \mathcal{S}_3) = d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{S}_2, \mathcal{S}_3 / \mathcal{S}_1)$.

6 Conclusion

We have presented a framework for compositional system development which supports quantities and system and action refinement. Moreover, it is robust, in that it uses distances to measure quantitative refinement and the compositional operations are uniformly continuous.

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 system development.

References

1. L. Aceto, I. Fábregas, D. de Frutos-Escrig, A. Ingólfsdóttir, and M. Palomino. On the specification of modal systems: A comparison of three frameworks. *Sci. Comput. Program.*, 78(12):2468–2487, 2013.
2. S. S. Bauer, A. David, R. Hennicker, K. G. Larsen, A. Legay, U. Nyman, and A. Wąsowski. Moving from specifications to contracts in component-based design. In *FASE*, vol. 7212 of *LNCS*. Springer, 2012.
3. S. S. Bauer, U. Fahrenberg, L. Juhl, K. G. Larsen, A. Legay, and C. Thrane. Weighted modal transition systems. *Form. Meth. Syst. Design*, 42(2):193–220, 2013.
4. S. S. Bauer, U. Fahrenberg, A. Legay, and C. Thrane. General quantitative specification theories with modalities. In *CSR*, vol. 7353 of *LNCS*. Springer, 2012.
5. S. S. Bauer, L. Juhl, K. G. Larsen, A. Legay, and J. Srba. Extending modal transition systems with structured labels. *Math. Struct. Comput. Sci.*, 22(4):581–617, 2012.
6. S. Ben-David, M. Chechik, and S. Uchitel. Merging partial behaviour models with different vocabularies. In *CONCUR*, vol. 8052 of *LNCS*. Springer, 2013.
7. N. Beneš, B. Delahaye, U. Fahrenberg, J. Křetínský, and A. Legay. Hennessy-Milner logic with greatest fixed points. In *CONCUR*, vol. 8052 of *LNCS*. Springer, 2013.
8. N. Beneš, I. Černá, and J. Křetínský. Modal transition systems: Composition and LTL model checking. In *ATVA*, vol. 6996 of *LNCS*. Springer, 2011.
9. G. Boudol and K. G. Larsen. Graphical versus logical specifications. *Th. Comp. Sci.*, 106(1):3–20, 1992.
10. L. Caires and L. Cardelli. A spatial logic for concurrency. *Inf. Comp.*, 186(2), 2003.

11. L. Cardelli, K. G. Larsen, and R. Mardare. Modular Markovian logic. In *ICALP (2)*, vol. 6756 of *LNCS*. Springer, 2011.
12. L. de Alfaro. Quantitative verification and control via the mu-calculus. In *CONCUR*, vol. 2761 of *LNCS*. Springer, 2003.
13. L. de Alfaro, M. Faella, T. A. Henzinger, R. Majumdar, and M. Stoelinga. Model checking discounted temporal properties. *Th. Comp. Sci.*, 345(1):139–170, 2005.
14. L. de Alfaro, M. Faella, and M. Stoelinga. Linear and branching system metrics. *IEEE Trans. Software Eng.*, 35(2):258–273, 2009.
15. L. de Alfaro and T. A. Henzinger. Interface automata. In *ESEC / SIGSOFT FSE*. ACM, 2001.
16. J. Desharnais, V. Gupta, R. Jagadeesan, and P. Panangaden. Metrics for labelled Markov processes. *Th. Comp. Sci.*, 318(3):323–354, 2004.
17. U. Fahrenberg, M. Acher, A. Legay, and A. Wąsowski. Sound merging and differencing for class diagrams. In *FASE*, vol. 8411 of *LNCS*. Springer, 2014.
18. U. Fahrenberg and A. Legay. The quantitative linear-time–branching-time spectrum. *Th. Comp. Sci.*, 2013. Online first: http://dx.doi.org/10.1016/j.tcs.2013.07.030.
19. U. Fahrenberg, A. Legay, and L.-M. Traonouez. Structural refinement for the modal nu-calculus. *CoRR*, 1402.2143, 2014. http://arxiv.org/abs/1402.2143.
20. J.-Y. Girard. Linear logic. *Th. Comp. Sci.*, 50:1–102, 1987.
21. M. Hennessy. Acceptance trees. *J. ACM*, 32(4):896–928, 1985.
22. T. A. Henzinger, R. Majumdar, and V. S. Prabhu. Quantifying similarities between timed systems. In *FORMATS*, vol. 3829 of *LNCS*. Springer, 2005.
23. T. A. Henzinger and J. Sifakis. The embedded systems design challenge. In *FM*, vol. 4085 of *LNCS*. Springer, 2006.
24. B. Jacobs and E. Poll. A logic for the Java modeling language JML. In *FASE*, vol. 2029 of *LNCS*. Springer, 2001.
25. B. Klin and V. Sassone. Structural operational semantics for stochastic and weighted transition systems. *Inf. Comput.*, 227:58–83, 2013.
26. K. G. Larsen. Proof systems for satisfiability in Hennessy-Milner logic with recursion. *Th. Comp. Sci.*, 72(2&3):265–288, 1990.
27. K. G. Larsen, R. Mardare, and P. Panangaden. Taking it to the limit: Approximate reasoning for Markov processes. In *MFCS*, vol. 7464 of *LNCS*. Springer, 2012.
28. K. G. Larsen and B. Thomsen. A modal process logic. In *LICS*. IEEE Computer Society, 1988.
29. K. G. Larsen and L. Xinxin. Equation solving using modal transition systems. In *LICS*. IEEE Computer Society, 1990.
30. B. Liskov and J. M. Wing. A behavioral notion of subtyping. *ACM Trans. Program. Lang. Syst.*, 16(6):1811–1841, 1994.
31. J.-B. Raclet. Residual for component specifications. Publication interne 1843, IRISA, Rennes, 2007.
32. D. Romero-Hernández and D. de Frutos-Escrig. Defining distances for all process semantics. In *FMOODS/FORTE*, vol. 7273 of *LNCS*. Springer, 2012.
33. D. Romero-Hernández and D. de Frutos-Escrig. Distances between processes: A pure algebraic approach. In *WADT*, vol. 7841 of *LNCS*. Springer, 2012.
34. S. Uchitel and M. Chechik. Merging partial behavioural models. In *SIGSOFT FSE*. ACM, 2004.
35. F. van Breugel and J. Worrell. A behavioural pseudometric for probabilistic transition systems. *Th. Comp. Sci.*, 331(1):115–142, 2005.
36. P. Černý, T. A. Henzinger, and A. Radhakrishna. Simulation distances. *Th. Comp. Sci.*, 413(1):21–35, 2012.

Appendix: Proofs

Proof (of Theorem 10). The proof that $\mathcal{S}_1 \vee \mathcal{S}_2 \le_{\mathsf{m}} \mathcal{S}_3$ iff $\mathcal{S}_1 \le_{\mathsf{m}} \mathcal{S}_3$ and $\mathcal{S}_2 \le_{\mathsf{m}} \mathcal{S}_3$ 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 $R = \{(s_1, (s_2, s_3)) \mid (s_1, s_2) \in R_1, (s_1, s_3) \in R_3\} \subseteq S_1 \times (S_2 \times S_3)$. 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 $\mathcal{S}_1 \le_{\mathsf{m}} \mathcal{S}_2$, 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 $\mathcal{S}_1 \le_{\mathsf{m}} \mathcal{S}_3$, 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 $a_1 \preccurlyeq a_2 \oslash a_3$ and $(t_1, (t_2, t_3)) \in R$, and $(s_2, s_3) \overset{a_2 \oslash a_3}{\dashrightarrow} (t_2, t_3)$ 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 $N = \{(a_2 \oslash a_3, (t_2, t_3)) \mid (a_2, t_2) \in N_2, s_3 \overset{a_3}{\dashrightarrow}_3 t_3\}$. By $S_1 \le_{\mathsf{m}} S_2$, 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 $S_1 \le_{\mathsf{m}} S_3$, 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 $(a_2 \oslash a_3, (t_2, t_3)) \in N$, $a_1 \preccurlyeq a_2 \wedge a_3$, 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 $S_1 \le_{\mathsf{m}} S_2$, the proof of $S_1 \le_{\mathsf{m}} S_3$ 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 $a = a_2 \oslash a_3$, but then $a_1 \preccurlyeq a_2 \oslash a_3 \preccurlyeq a_2$ and $(t_1, t_2) \in R_2$.

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

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 $a = a_2 \oslash a_3$, but then $a_1 \preccurlyeq a_2 \oslash a_3 \preccurlyeq a_2$ 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 $\mathcal{I}$, $\mathcal{I} \le_{\mathsf{m}} \mathcal{S}_1 \wedge \mathcal{S}_2$ iff $\mathcal{I} \le_{\mathsf{m}} \mathcal{S}_1$ and $\mathcal{I} \le_{\mathsf{m}} \mathcal{S}_2$. For the other part, it is clear by construction that for any implementation $\mathcal{I}$, any witness R for $\mathcal{I} \le_{\mathsf{m}} \mathcal{S}_1$ is also a witness for $\mathcal{I} \le_{\mathsf{m}} \mathcal{S}_1 \vee \mathcal{S}_2$, and similarly for $\mathcal{S}_2$, hence $[\![\mathcal{S}_1]\!] \cup [\![\mathcal{S}_2]\!] \subseteq [\![\mathcal{S}_1 \vee \mathcal{S}_2]\!]$.

To show the other inclusion, we note that an initialized refinement R witnessing $\mathcal{I} \le_{\mathsf{m}} \mathcal{S}_1 \vee \mathcal{S}_2$ 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 by disjointness, R witnesses $\mathcal{I} \le_{\mathsf{m}} \mathcal{S}_1$, in the second, $\mathcal{I} \le_{\mathsf{m}} \mathcal{S}_2$. $\square$

Proof (of Theorem 11). Associativity and commutativity are clear. 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 $\mathcal{S}_1 \| (\mathcal{S}_2 \vee \mathcal{S}_3) \equiv_{\mathsf{m}} \mathcal{S}_1 \| \mathcal{S}_2 \vee \mathcal{S}_1 \| \mathcal{S}_3$. The assertion $\bot \| \mathcal{S} \equiv_{\mathsf{m}} \bot$ is also clear. $\square$

Proof (of Theorem 14). We show the proof for AA; 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 $\mathcal{A}_2 \leq_{\mathsf{m}} \mathcal{A}_3 / \mathcal{A}_1$.

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 $s, t \in S$.

Now 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 an $M_/ \in \mathrm{Tran}_/(s_3 / s_1)$, *i.e.*, such that the conditions in (1) are satisfied.

Let $M_3 = M_/ \rhd M_1$. 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 $t = \{t_3^1/t_1^1, \dots, t_3^n/t_1^n\}$. 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

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

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 $s = \{s_3^1/s_1^1, \dots, s_3^n/s_1^n\}$, and $M_2 \in \mathrm{Tran}_2(s_2)$.

For every $i = 1, \dots, n$, write $\mathrm{Tran}_1(s_1^i) = \{M_1^{i,1}, \dots, M_1^{i,m_i}\}$. 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 $j = 1, \dots, m_i$, 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

$$\begin{aligned} M = \{(a_2, t) \mid \exists (a_2, t_2) \in M_2 : \forall t_3/t_1 \in t : \exists i, a_1, a_3 : \\ (a_1, t_1) \in\in \mathrm{Tran}_1(s_1^i), (a_3, t_3) \in M_3^{i,\delta_i(a_1,t_1)}, a_1 \oplus a_2 \preccurlyeq a_3, t_1 \| t_2 \leq_{\mathsf{m}} t_3\}\,. \end{aligned} \tag{5}$$

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 $a_3 = a_1 \oplus a_2$ 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 $i = 1, \dots, n$ 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 $t = \{\tau_i(a_1, t_1)/t_1 \mid i = 1, \dots, n, (a_1, t_1) \in\in \mathrm{Tran}_1(t_1^i)\}$, then $(a_2, t) \in M$ and $(t_2, t) \in R$.
- Let $(a_2, t) \in M$, then we have $(a_2, t_2) \in M_2$ satisfying the conditions in (5). Hence $t_1 \| t_2 \leq_{\mathsf{m}} t_3$ for all $t_3/t_1 \in t$, so that $(t_2, t) \in R$. $\square$

Before we attempt any more proofs, we need to recall the notion of *refinement family* from [4] and extend it to AA. We give the definition for AA only; for DMTS and the modal ν-calculus it is similar.

Definition 23. *A* refinement family *from $\mathcal{A}_1$ to $\mathcal{A}_2$, for AA $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$, $\mathcal{A}_2 = (S_2, S_2^0, \mathrm{Tran}_2)$, 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 24. *For all AA $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$, $\mathcal{A}_2 = (S_2, S_2^0, \mathrm{Tran}_2)$, 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

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

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

Proof (of Theorem 18).

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

Let $\mathcal{D}_1 = (S_1, S_1^0, \dashrightarrow_1, \longrightarrow_1)$, $\mathcal{D}_2 = (S_2, S_2^0, \dashrightarrow_2, \longrightarrow_2)$ 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 $(s_1^0, s_2^0) \in R_{d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{D}_1, \mathcal{D}_2)}$. We show that R is an AA 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

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

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 $(a_2, t_2) \in M_2$.

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

Let $\mathcal{D}_1 = (S_1, S_1^0, \dashrightarrow_1, \longrightarrow_1)$, $\mathcal{D}_2 = (S_2, S_2^0, \dashrightarrow_2, \longrightarrow_2)$ be DMTS. There exists an AA 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 $(s_1^0, s_2^0) \in R_{d_{\mathsf{m}}^{\mathbb{L}}(da(\mathcal{D}_1), da(\mathcal{D}_2))}$. 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.

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

Let $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$, $\mathcal{A}_2 = (S_2, S_2^0, \mathrm{Tran}_2)$ be AA, with DMTS translations $(D_1, D_1^0, \longrightarrow_1, \dashrightarrow_1)$, $(D_2, D_2^0, \longrightarrow_2, \dashrightarrow_2)$. There is an AA 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 $(s_1^0, s_2^0) \in R_{d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_1, \mathcal{A}_2)}$.

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

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

We show that R' is a witness for $d_{\mathsf{m}}^{\mathbb{L}}(ad(\mathcal{A}_1), ad(\mathcal{A}_2)) \sqsubseteq_{\mathbb{L}} d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_1, \mathcal{A}_2)$. 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 $(s_1^0, s_2^0) \in R_{d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_1, \mathcal{A}_2)}$, which gives us $M_2^0 \in \mathrm{Tran}_2(s_2^0)$ which satisfies the conditions in the definition of $R'_{d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_1, \mathcal{A}_2)}$, whence $(M_1^0, M_2^0) \in R'_{d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_1, \mathcal{A}_2)}$.

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

Let $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$, $\mathcal{A}_2 = (S_2, S_2^0, \mathrm{Tran}_2)$ be AA, with DMTS translations $(D_1, D_1^0, \longrightarrow_1, \dashrightarrow_1)$, $(D_2, D_2^0, \longrightarrow_2, \dashrightarrow_2)$. 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 $(M_1^0, M_2^0) \in R_{d_{\mathsf{m}}^{\mathbb{L}}(ad(\mathcal{A}_1), ad(\mathcal{A}_2))}$.

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

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

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

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

Let $(a_2, t_2) \in M_2$ and define $N_2 = \{(a_2, M_2') \mid M_2' \in \text{Tran}_2(t_2)\}$, 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 $N_1 = \{(a_1, M_1') \mid M_1' \in \text{Tran}_1(t_1)\}$; we only miss to show that $(t_1, t_2) \in R'_\beta$ for some $\beta \in \mathbb{L}$ with $F(a_1, a_2, \beta) \sqsubseteq_{\mathbb{L}} \alpha$. Let $M_1' \in \text{Tran}_1(t_1)$, 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 $M_2' \in \text{Tran}_2(t_2)$.

Let $(a_1, t_1) \in M_1$ and define $N_1 = \{(a_1, M_1') \mid M_1' \in \text{Tran}_1(t_1)\}$, 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 $N_2 = \{(a_2, M_2'') \mid M_2'' \in \text{Tran}_2(t_2)\}$. Now if $M_1'' \in \text{Tran}_1(t_1)$, 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 $M_2'' \in \text{Tran}_2(t_2)$.

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

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

Let $\mathcal{D}_1 = (S_1, S_1^0, \dashrightarrow_1, \longrightarrow_1)$, $\mathcal{D}_2 = (S_2, S_2^0, \dashrightarrow_2, \longrightarrow_2)$ be DMTS, with ν-calculus translations $dn(\mathcal{D}_1) = (S_1, S_1^0, \Delta_1)$, $dn(\mathcal{D}_2) = (S_2, S_2^0, \Delta_2)$. 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 $(s_1^0, s_2^0) \in R_{d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{D}_1, \mathcal{D}_2)}$.

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 $N_1 \in \Diamond_1(s_1)$.

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

Let $\mathcal{D}_1 = (S_1, S_1^0, \dashrightarrow_1, \longrightarrow_1)$, $\mathcal{D}_2 = (S_2, S_2^0, \dashrightarrow_2, \longrightarrow_2)$ be DMTS, with ν-calculus translations $dn(\mathcal{D}_1) = (S_1, S_1^0, \Delta_1)$, $dn(\mathcal{D}_2) = (S_2, S_2^0, \Delta_2)$. 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 $(s_1^0, s_2^0) \in R_{d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{D}_1, \mathcal{D}_2)}$.

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 $t_1 \in \square_1^{a_1}(s_1)$, so that there is $a_2 \in \Sigma$, $t_2 \in \square_2^{a_2}(s_2)$ 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 $N_2 \in \lozenge_2(s_2)$. Hence there is $N_1 \in \lozenge_1(s_1)$ 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 $s_1 \longrightarrow_1 N_1$.

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

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 $nd(\mathcal{N}_1) = (X_1, X_1^0, \dashrightarrow_1, \longrightarrow_1)$, $nd(\mathcal{N}_2) = (X_2, X_2^0, \dashrightarrow_2, \longrightarrow_2)$. 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 $(x_1^0, x_2^0) \in R_{d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{N}_1, \mathcal{N}_2)}$.

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 $y_1 \in \square_1^{a_1}(x_1)$, hence there are $a_2 \in \Sigma$, $y_2 \in \square_2^{a_2}$ 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 $N_2 \in \lozenge_2(x_2)$. Hence there must be $N_1 \in \lozenge_1(x_1)$ 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 $x_1 \longrightarrow_1 N_1$.

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

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 $nd(\mathcal{N}_1) = (X_1, X_1^0, \dashrightarrow_1, \longrightarrow_1)$, $nd(\mathcal{N}_2) = (X_2, X_2^0, \dashrightarrow_2, \longrightarrow_2)$. 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 $(x_1^0, x_2^0) \in R_{d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{N}_1, \mathcal{N}_2)}$.

Let $\alpha \in \mathbb{L}$, $(x_1, x_2) \in R_\alpha$, $a_1 \in \Sigma$, and $y_1 \in \square_1^{a_1}(x_1)$. 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 $y_1 \in \square_2^{a_2}(x_2)$.

Let $N_2 \in \lozenge_2(x_2)$, 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 $N_1 \in \lozenge_1(x_1)$. $\square$

Proof (of Proposition 19, first part). We show the proposition for AA. First, if $\mathcal{A}_1 \le_{\mathsf{m}} \mathcal{A}_2$, 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 $d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_1, \mathcal{A}_2) = \bot_{\mathbb{L}}$.

We have shown that $\mathcal{A}_1 \le_{\mathsf{m}} \mathcal{A}_2$ implies $d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_1, \mathcal{A}_2) = \bot_{\mathbb{L}}$; as a special case, we see that $d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}, \mathcal{A}) = \bot_{\mathbb{L}}$ for all AA $\mathcal{A}$. Now if $\mathcal{A}_1 \le_{\mathsf{th}} \mathcal{A}_2$ instead, then for all

$\mathcal{I} \in [\![\mathcal{A}_1]\!]$, also $\mathcal{I} \in [\![\mathcal{A}_2]\!]$, hence $d_{\mathsf{th}}^{\mathbb{L}}(\mathcal{A}_1, \mathcal{A}_2) = \perp_{\mathbb{L}}$. As a special case, we conclude that $d_{\mathsf{th}}^{\mathbb{L}}(\mathcal{A}, \mathcal{A}) = \perp_{\mathbb{L}}$ for all AA $\mathcal{A}$.

Next we show the triangle inequality for $d_{\mathsf{m}}^{\mathbb{L}}$. The triangle inequality for $d_{\mathsf{th}}^{\mathbb{L}}$ will then follow from standard arguments used to show that the Hausdorff metric satisfies the triangle inequality. 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 AA and $R^1 = \{R_\alpha^1 \subseteq S_1 \times S_2 \mid \alpha \in \mathbb{L}\}$, $R^2 = \{R_\alpha^2 \subseteq S_2 \times S_3 \mid \alpha \in \mathbb{L}\}$ refinement families such that $\forall s_1^0 \in S_1^0 : \exists s_2^0 \in S_2^0 : (s_1^0, s_2^0) \in R^1_{d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_1, \mathcal{A}_2)}$ and $\forall s_2^0 \in S_2^0 : \exists s_3^0 \in S_3^0 : (s_2^0, s_3^0) \in R^2_{d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_2, \mathcal{A}_3)}$.

Define $R = \{R_\alpha \subseteq S_1 \times S_3 \mid \alpha \in \mathbb{L}\}$ by $R_\alpha = \{(s_1, s_3) \mid \exists \alpha_1, \alpha_2 \in \mathbb{L}, s_2 \in S_2 : (s_1, s_2) \in R^1_{\alpha_1}, (s_2, s_3) \in R^2_{\alpha_2}, \alpha_1 \oplus_{\mathbb{L}} \alpha_2 = \alpha\}$. We see that $\forall s_1^0 \in S_1^0 : \exists s_3^0 \in S_3^0 : (s_1^0, s_3^0) \in R_{d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_1, \mathcal{A}_2) \oplus_{\mathbb{L}} d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_2, \mathcal{A}_3)}$; 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

$$\forall (a_1, t_1) \in M_1 : \exists (a_2, t_2) \in M_2, \beta_1 \in \mathbb{L} : (t_1, t_2) \in R^1_{\beta_1}, F(a_1, a_2, \beta_1) \sqsubseteq_{\mathbb{L}} \alpha_1, \quad (6)$$
$$\forall (a_2, t_2) \in M_2 : \exists (a_1, t_1) \in M_1, \beta_1 \in \mathbb{L} : (t_1, t_2) \in R^1_{\beta_1}, F(a_1, a_2, \beta_1) \sqsubseteq_{\mathbb{L}} \alpha_1. \quad (7)$$

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

$$\forall (a_2, t_2) \in M_2 : \exists (a_3, t_3) \in M_3, \beta_2 \in \mathbb{L} : (t_2, t_3) \in R^2_{\beta_2}, F(a_2, a_3, \beta_2) \sqsubseteq_{\mathbb{L}} \alpha_2, \quad (8)$$
$$\forall (a_3, t_3) \in M_3 : \exists (a_2, t_2) \in M_2, \beta_2 \in \mathbb{L} : (t_2, t_3) \in R^2_{\beta_2}, F(a_2, a_3, \beta_2) \sqsubseteq_{\mathbb{L}} \alpha_2. \quad (9)$$

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 (6) and (8). 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 (9) and (7) 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 $d_{\mathsf{m}}^{\mathbb{L}}$ and $d_{\mathsf{t}}^{\mathbb{L}}$ are $\mathbb{L}$-hemimetrics. Using monotonicity of the eval function, it follows that d_{m} and d_{t} are hemimetrics. ☐

Proof (of Proposition 19, second part). 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

$$\begin{aligned} &\forall (a_1, t_1) \in M_1 : \exists (a_2, t_2) \in M_2, \beta \in \mathbb{L} : (t_1, t_2) \in R_\beta, F(a_1, a_2, \beta) = 0, \\ &\forall (a_2, t_2) \in M_2 : \exists (a_1, t_1) \in M_1, \beta \in \mathbb{L} : (t_1, t_2) \in R_\beta, F(a_1, a_2, \beta) = 0. \end{aligned} \quad (10)$$

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 (10) degenerates to

$$\forall (a_1, t_1) \in M_1 : \exists (a_2, t_2) \in M_2 : (t_1, t_2) \in R_0, a_1 \preccurlyeq a_2,$$
$$\forall (a_2, t_2) \in M_2 : \exists (a_1, t_1) \in M_1 : (t_1, t_2) \in R_0, a_1 \preccurlyeq a_2,$$

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

Again by definition, we see that for any AA $\mathcal{A}_1$, $\mathcal{A}_2$, 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. □

Proof (of Theorem 20). We prove the statement for AA; for DMTS and ν-calculus expressions it then follows from Theorem 18.

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 $(s_1^0, s_2^0) \in R_{d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_1, \mathcal{A}_2)}$. 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 $R^2 = \{R_\alpha^2 \subseteq S \times S_2 \mid \alpha \in \mathbb{L}\}$ by $R_\alpha^2 = R^1 \circ R_\alpha = \{(s, s_2) \mid \exists s_1 \in S : (s, s_1) \in R^1, (s_1, s_2) \in R_\alpha\}$. 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 $(s, s_2) \in R_\alpha^2$: 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 23. 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 $M_2 \in \mathrm{Tran}_2(s_2)$ 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 $d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{I}, \mathcal{I}_2)$; clearly, R^2 is initialized. Let $\alpha \in \mathbb{L}$ with $\alpha \neq \top_{\mathbb{L}}$ and $(s, s_2) \in R_\alpha^2$, 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 $(a_1, t_1) \in M_1$, there is $s \xrightarrow{a_1} t$ with $(t, t_1) \in R^1$

and thus $M_2 \in \mathrm{Tran}_2(s_2)$ satisfying the conditions in Definition 23.

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 $M_2 \in \mathrm{Tran}_2(s_2)$ 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 $(t, t_2) \in R^2_\beta$. □

Proof (of Theorem 21). We show the proof for AA. For $i = 1, 2, 3, 4$, let $\mathcal{A}_i = (S_i, S_i^0, \mathrm{Tran}_i)$. 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 $\forall s_1^0 \in S_1^0 : \exists s_3^0 \in S_3^0 : (s_1^0, s_3^0) \in R^1_{d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_1, \mathcal{A}_3)}$ and $\forall s_2^0 \in S_2^0 : \exists s_4^0 \in S_4^0 : (s_2^0, s_4^0) \in R^2_{d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_2, \mathcal{A}_4)}$. Define $R = \{R_\alpha \subseteq (S_1 \times S_2) \times (S_3 \times S_4) \mid \alpha \in \}$ by

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

then it is clear that $\forall (s_1^0, s_2^0) \in S_1^0 \times S_2^0 : \exists (s_3^0, s_4^0) \in S_3^0 \times S_4^0 : ((s_1^0, s_2^0), (s_3^0, s_4^0)) \in R_{P(d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_1, \mathcal{A}_3), d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_2, \mathcal{A}_4))}$. 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

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

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

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

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

Let $M_{34} = M_3 \oplus M_4 \in \mathrm{Tran}((s_3, s_4))$. 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 $(a_{34}, (t_3, t_4)) \in M_{34}$. 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 $\forall(a_{12},(t_1,t_2)) \in M_{12} : \exists(a_{34},(t_3,t_4)) \in M_{34}, \beta \in \mathbb{L} : ((t_1,t_2),(t_3,t_4)) \in R_\beta, F(a_{12},a_{34},\beta) \sqsubseteq_{\mathbb{L}} \alpha$. 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). □

Proof (of Theorem 22). We show the proof for AA. 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 $d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_1 \| \mathcal{A}_2, \mathcal{A}_3) = d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_2, \mathcal{A}_3/\mathcal{A}_1)$.

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 $R_\alpha = \{(s_1 \| s_2, s_3) \mid d_{\mathsf{m}}^{\mathbb{L}}(s_2, s_3/s_1) \sqsubseteq_{\mathbb{L}} \alpha\}$. We show that R is a witness for $d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_1 \| \mathcal{A}_2, \mathcal{A}_3)$.

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 $d_{\mathsf{m}}^{\mathbb{L}}(s_2^0, s_3^0/s_1^0) \sqsubseteq_{\mathbb{L}} d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_2, \mathcal{A}_3/\mathcal{A}_1)$, hence $(s_1^0 \| s_1^0, s_3^0) \in R_{d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_2, \mathcal{A}_3/\mathcal{A}_1)}$.

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 $d_{\mathsf{m}}^{\mathbb{L}}(s_2, s_3/s_1) \sqsubseteq_{\mathbb{L}} \alpha$, we can pair M_2 with an $M_/ \in \mathrm{Tran}_/(s_3/s_1)$, *i.e.*, such that the conditions in Definition 23 are satisfied.

Let $M_3 = M_/ \triangleright M_1$. We show that the conditions in Definition 23 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 $d_{\mathsf{m}}^{\mathbb{L}}(t_2, t) \sqsubseteq_{\mathbb{L}} \beta$.
  Note that $a_3 = a_1 \oplus a_2'$ is defined and $F(a, a_3, \beta) \sqsubseteq \alpha$. Write $t = \{t_3^1/t_1^1, \dots, t_3^n/t_1^n\}$. 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 $d_{\mathsf{m}}^{\mathbb{L}}(t_2, t_3^i/t_1^i) \sqsubseteq \beta$ 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 $d_{\mathsf{m}}^{\mathbb{L}}(t_2, t) \sqsubseteq_{\mathbb{L}} \beta$. 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 $t \supseteq \{t_3/t_1\}$, $d_{\mathsf{m}}^{\mathbb{L}}(t_2, t_3/t_1) \sqsubseteq \beta$.

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

$$R_\alpha = \{(s_2, \{s_3^1/s_1^1, \dots, s_3^n/s_1^n\}) \mid \forall i = 1, \dots, n : d_{\mathsf{m}}^{\mathbb{L}}(s_1^i \| s_2, s_3^i) \sqsubseteq_{\mathbb{L}} \alpha\}\,;$$

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

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 $d_{\mathsf{m}}^{\mathbb{L}}(s_1^0 \| s_2^0, s_3^0) \sqsubseteq_{\mathbb{L}} d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_1 \| \mathcal{A}_2, \mathcal{A}_3)$. By $s^0 \supseteq \{\sigma(s_1^0)/s_1^0 \mid s_1^0 \in S_1^0\}$, we see that $(s_2^0, s^0) \in R_{d_{\mathsf{m}}^{\mathbb{L}}(\mathcal{A}_1 \| \mathcal{A}_2, \mathcal{A}_3)}$.

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

For every $i = 1, \dots, n$, write $\mathrm{Tran}_1(s_1^i) = \{M_1^{i,1}, \dots, M_1^{i,m_i}\}$. 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 $j = 1, \dots, m_i$, let $M^{i,j} = M_1^{i,j} \| M_2 \in \mathrm{Tran}_\|(s_1^i \| s_2)$. By $d_{\mathsf{m}}^{\mathbb{L}}(s_1^i \| s_2, s_3^i) \sqsubseteq_{\mathbb{L}} \alpha$, we have $M_3^{i,j} \in \mathrm{Tran}_3(s_3^i)$ such that the conditions in Definition 23 hold for the pair $M^{i,j}, M_3^{i,j}$.

Now define

$$\begin{aligned} M = \{(a_2, t) \mid \exists (a_2, t_2) \in M_2 : \forall t_3/t_1 \in t : \exists i, a_1, a_3, \beta : (a_1, t_1) \in\in \mathrm{Tran}_1(s_1^i), \\ (a_3, t_3) \in M_3^{i, \delta_i(a_1, t_1)}, F(a_1 \oplus a_2, a_3, \beta) \sqsubseteq_{\mathbb{L}} \alpha, d_{\mathsf{m}}^{\mathbb{L}}(t_1 \| t_2, t_3) \sqsubseteq_{\mathbb{L}} \beta\}\,. \end{aligned} \tag{15}$$

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 $a_3 = a_1 \oplus a_2$ 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 definition of $M^{i,j}$, there are $(a_1, t_1) \in M_1^{i,j}$, $(a_2, t_2) \in M_2$ and β for which $F(a_1 \oplus a_2, a_3, \beta) \sqsubseteq_{\mathbb{L}} \alpha$ and $d_{\mathsf{m}}^{\mathbb{L}}(t_1 \| t_2, t_3) \sqsubseteq_{\mathbb{L}} \beta$. 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 $(a_1 \oplus a_2, t_3) \in M \triangleright M_1^{i,j}$.

We show that the pair M_2, M satisfies the conditions of Definition 23.

- 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 23 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 $d_{\mathsf{m}}^{\mathbb{L}}(t_1 \| t_2, \tau_i(a_1, t_1)) \sqsubseteq_{\mathbb{L}} \beta_i(a_1, t_1)$ and $F(a_1 \oplus a_2, \eta_i(a_1, t_1), \beta_i(a_1, t_1)) \sqsubseteq_{\mathbb{L}} \alpha$. 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 $i, a_1, a_3, \beta(t_3/t_1)$ such that $(a_3, t_3) \in M_3^{i,\delta_i(a_1,t_1)}$, $F(a_1 \oplus a_2, a_3, \beta(t_3/t_1)) \sqsubseteq_{\mathbb{L}} \alpha$ and $d_{\mathsf{m}}^{\mathbb{L}}(t_1 \| t_2, t_3) \sqsubseteq_{\mathbb{L}} \beta(t_3/t_1)$. Let $\beta = \sup\{\beta(t_3/t_1) \mid t_3/t_1 \in t\}$, then $d_{\mathsf{m}}^{\mathbb{L}}(t_1 \| t_2, t_3) \sqsubseteq_{\mathbb{L}} \beta$ for all $t_3/t_1 \in t$, hence $(t_2, t) \in R_\beta$. $\square$