UNIVERSITÄT AUGSBURG

Nondeterministic Modal Interfaces

Ferenc Bujtor, Sascha Fendrich,

Gerald Lüttgen, Walter Vogler

Report 2014-06 Oktober 2014

INSTITUT FÜR INFORMATIK
D-86135 AUGSBURG

Nondeterministic Modal Interfaces[*]

Ferenc Bujtor[†] Sascha Fendrich[‡] Gerald Lüttgen[‡] Walter Vogler[†]

October 14, 2014

Abstract

Interface theories are employed in the component-based design of concurrent systems. They often emerge as combinations of Interface Automata (IA) and Modal Transition Systems (MTS), e.g., Nyman et al.'s IOMTS, Bauer et al.'s MIO, Raclet et al.'s MI or our MIA. In this paper, we generalise MI to *nondeterministic* interfaces, for which we resolve the longstanding conflict between unspecified inputs being allowed in IA but forbidden in MTS. With this solution we achieve, in contrast to related work, an *associative* parallel composition, a *compositional* preorder, a conjunction on interfaces with *dissimilar alphabets* supporting perspective-based specifications, and a quotienting operator for decomposing *nondeterministic* specifications in a single theory.

1 Introduction

Interface theories [2, 7, 8, 16, 17, 22] support the component-based design of concurrent systems and offer a semantic framework for, e.g., software contracts [1] and web services [5]. Several such theories are based on de Alfaro and Henzinger's *Interface Automata* (IA) [11], whose distinguishing feature is a parallel composition on labelled transition systems with inputs and outputs, where receiving an unexpected input is regarded as an error, i.e., a communication mismatch. All states are pruned from which entering an error state cannot be prevented by the environment, rather than leaving the parallel composition fully undefined as in [2].

Various researchers have combined IA with Larsen's *Modal Transition Systems* (MTS) [15], which features may- and must-transitions to express allowed and required behaviour, resp. In a refinement of an interface, all required behaviour must be preserved and no disallowed behaviour may be added. Whereas in IA outputs are optional, they may now be enforced in theories combining IA and MTS, such as Nyman et al.'s IOMTS [16], Bauer et al.'s MIO [2], Raclet et al.'s *Modal Interfaces* (MI) [22] and our *Modal Interface Automata* (MIA) [17, 18]. In this paper we extend MI to nondeterministic systems, yielding the most general approach to date and permitting new applications, e.g., for dealing with races in networks. We built upon our prior work in [18], from which we adopt disjunctive must-transitions that are needed for operationally defining conjunction, which is another key operator in interface theories and supports perspective-based specification.

Combining IA and MTS is, however, problematic since unspecified inputs are forbidden in MTS, but allowed in IA with arbitrary behaviour afterwards. In IOMTS [16], the MTS-view was adopted and, as a consequence, compositionality of refinement wrt. the parallel operator $||$ was lost. In [18] we followed the

[*] Research support was provided by the DFG (German Research Foundation) under grants LU 1748/3-1 and VO 615/12-1.

[†] Institut für Informatik, University of Augsburg, Germany

[‡] Software Technologies Research Group, University of Bamberg, Germany

IA-view but found that resolving the conflict is essential for a more flexible conjunction. In our new MIA, we can optionally express the IA-view for state p and input i by an i-may-transition from p to a *special, universal state e* that can be refined in any way; we will need this option when defining $\|$. There is a similar idea in MI [22], but an ordinary state is used there with the consequence that $\|$ is not associative. In contrast to the somewhat related demonic completion as used, e.g., in [12], we do not enforce input-enabledness. With the new feature, our interface theory allows for a proper distinction between may- and must-transitions for inputs, unlike [17, 18]. This enables us to define conjunction also on interfaces with dissimilar alphabets via alphabet extension.

As in MI, our MIA is equipped with a multicast parallel composition, where one output can synchronise with several inputs. This is accompanied by a hiding operator for scoping actions as in [19]. These operators together are more expressive than the binary parallel composition of IA, which is used in [2, 16, 17, 18]. We also develop a quotienting operator as a kind of inverse of parallel composition $\|$. For a specification P and a given component D, quotienting constructs the most general component Q such that $Q \| D$ refines P. Quotienting is a very practical operator because it can be used for decomposing concurrent specifications stepwise, specifying contracts [4], and reusing components. In contrast to [22], our quotienting permits *nondeterministic* specifications and complements $\|$ rather than a simpler parallel product without pruning.

In summary, our new interface theory MIA generalises and improves upon existing theories combining IA and MTS: parallel composition is commutative and associative (cf. Sec. 3), quotienting also works for nondeterministic specifications (cf. Sec. 4), conjunction properly reflects perspective-based specification (cf. Secs. 5 and 6), and refinement (cf. Sec. 2) is compositional and permits alphabet extension (cf. Sec. 6).

2 Modal Interface Automata: The Setting

In this section we define *Modal Interface Automata* (MIA) and its supported operations. Essentially, MIAs are state machines with disjoint input and output alphabets, as in IA [11], and two transition relations, *may* and *must*, as in Modal Transition Systems [15]. May-transitions describe permitted behaviour, while must-transitions describe required behaviour. Unlike previous versions of MIA [17, 18] and also unlike other similar theories, we introduce the *universal state e* as an extra constituent.

Definition 1 (Modal Interface Automata)**.** *A* Modal Interface Automaton *(MIA) is a tuple* $(P, I, O, \longrightarrow, \dashrightarrow, p_0, e)$*, where*

- *P is the set of states containing the* initial state p_0 *and the* universal state e*,*
- *I and O are disjoint sets, the alphabets of* input *and* output actions*, not containing the special internal action τ, and $A =_{df} I \cup O$ is called the* alphabet*,*
- $\longrightarrow \subseteq P \times (A \cup \{\tau\}) \times (\mathscr{P}_{fin}(P) \setminus \emptyset)$ *is the* disjunctive must-transition *relation, with $\mathscr{P}_{fin}(P)$ being the set of finite subsets of P,*
- $\dashrightarrow \subseteq P \times (A \cup \{\tau\}) \times P$ *is the* may-transition *relation.*

We require the following conditions:

(a) For all $\alpha \in A \cup \{\tau\}$. $p \xrightarrow{\alpha} P'$ implies $\forall p' \in P'.\, p \overset{\alpha}{\dashrightarrow} p'$ (syntactic consistency)*,*

*(b) e appears in transitions only as the target state of input may-transitions (*sink condition*).*

Cond. (a) states that whatever is required should be allowed; this syntactic consistency is a natural and standard condition (cf. [15]). Cond. (b) matches the idea for e explained in the introduction. We use this state in the context of parallel composition to represent communication errors (see Def. 8). A MIA P is called *universal* if $P = (\{e\}, I, O, \emptyset, \emptyset, e, e)$, i.e., if $p_0 = e$. Note that our disjunctive must-transitions have a single label, in contrast to Disjunctive MTS [14].

In the sequel, we identify a MIA $(P, I, O, \longrightarrow, \dashrightarrow, p_0, e)$ with its state set P and, if needed, use index P when referring to one of its components, e.g., we write I_P for I. Similarly, we write, e.g., I_1 instead of I_{P_1} for MIA P_1. In addition, we let i, o, a, ω and α stand for representatives of the alphabets I, O, A, $O \cup \{\tau\}$ and $A \cup \{\tau\}$, resp.; we write $A = I/O$ when highlighting inputs I and outputs O in an alphabet A, and we define $\hat{a} =_{\mathrm{df}} a$ and $\hat{\tau} =_{\mathrm{df}} \varepsilon$ (the empty word). Furthermore, outputs and internal actions are called *local* actions since they are controlled locally by P. For convenience, we let $p \xrightarrow{a} p'$, $p \overset{a}{\not\longrightarrow}$ and $p \overset{a}{\not\dashrightarrow}$ denote $p \xrightarrow{a} \{p'\}$, $\nexists p'.\, p \xrightarrow{a} p'$ and $\nexists p'.\, p \overset{a}{\dashrightarrow} p'$, resp. In figures, we often refer to an action a as $a?$ if $a \in I$, and as $a!$ if $a \in O$, and omit the label of τ-transitions. Must-transitions (may-transitions) are drawn using solid, possibly splitting arrows (dashed arrows); any depicted must-transition also implicitly represents the underlying may-transition(s) due to syntactic consistency.

We now define *weak* must- and may-transition relations that abstract from transitions labelled by τ, as is needed for MIA refinement. It is an alternative but equivalent definition to the one presented in [18].

Definition 2 (Weak Transition Relations). *We define* weak *must-transition and* weak *may-transition relations, $\Longrightarrow$ and $=\Rightarrow$ resp., as the smallest relations satisfying the following conditions:*

(a) $P' \overset{\varepsilon}{\Longrightarrow} P'$ *for finite* $P' \subseteq P$,

(b) $P' \overset{\hat{\alpha}}{\Longrightarrow} P''$, $p'' \in P''$ *and* $p'' \xrightarrow{\tau} P'''$ *implies* $P' \overset{\hat{\alpha}}{\Longrightarrow} (P'' \setminus \{p''\}) \cup P'''$,

(c) $P' \overset{\varepsilon}{\Longrightarrow} P'' = \{p_1, \ldots, p_n\}$ *and* $\forall j.\, p_j \xrightarrow{a} P_j$, *implies* $P' \overset{a}{\Longrightarrow} \bigcup_{j=1}^{n} P_j$,

(d) $p \overset{\varepsilon}{=\Rightarrow} p$,

(e) $p \overset{\varepsilon}{=\Rightarrow} p'' \overset{\tau}{\dashrightarrow} p'$ *implies* $p \overset{\varepsilon}{=\Rightarrow} p'$,

(f) $p \overset{\varepsilon}{=\Rightarrow} p'' \overset{\alpha}{\dashrightarrow} p''' \overset{\varepsilon}{=\Rightarrow} p'$ *implies* $p \overset{\alpha}{=\Rightarrow} p'$.

For $\{p'\} \overset{\hat{\alpha}}{\Longrightarrow} P''$ we often write $p' \overset{\hat{\alpha}}{\Longrightarrow} P''$. Mostly for inputs a, we also use relation compositions $\xrightarrow{a}\overset{\varepsilon}{\Longrightarrow}$ and $\overset{a}{\dashrightarrow}\overset{\varepsilon}{=\Rightarrow}$ resp., i.e., where leading τs are disallowed. Observe that $p \xrightarrow{a}\overset{\varepsilon}{\Longrightarrow} P'$ implies $p \overset{a}{\Longrightarrow} P'$, and $p \overset{a}{\dashrightarrow}\overset{\varepsilon}{=\Rightarrow} p'$ implies $p \overset{a}{=\Rightarrow} p'$.

Lemma 3 ([18]). *Consider arbitrary MIAs P and Q.*

(a) Let $p \overset{\hat{\alpha}}{\Longrightarrow} P'$, $p' \in P'$ *and* $p' \overset{\varepsilon}{\Longrightarrow} P''$. *Then, there exists some* $\overline{P}$ *such that* $p \overset{\hat{\alpha}}{\Longrightarrow} \overline{P}$ *and* $P'' \subseteq \overline{P} \subseteq (P' \setminus \{p'\}) \cup P''$.

(b) Let $p \overset{\hat{\alpha}}{\Longrightarrow} P'$, $\{p_1, \ldots, p_n\} \subseteq P'$ *and* $p_i \overset{\varepsilon}{\Longrightarrow} P_i$ *for* $1 \leq i \leq n$. *Then, there exists some* $\overline{P}$ *such that* $p \overset{\hat{\alpha}}{\Longrightarrow} \overline{P} \subseteq (P' \setminus \{p_1, \ldots, p_n\}) \cup \bigcup_{i=1}^{n} P_i$.

(c) Let $p \overset{\hat{\alpha}}{\Longrightarrow} \bigcup_{i=1}^{n} P_i$ *and* $P_i \overset{\varepsilon}{\Longrightarrow} P_i'$ *for* $1 \leq i \leq n$. *Then, there exists some* $\overline{P}$ *such that* $p \overset{\hat{\alpha}}{\Longrightarrow} \overline{P}$ *and* $\overline{P} \subseteq \bigcup_{i=1}^{n} P_i'$.

(d) Let $P \stackrel{\varepsilon}{\Longrightarrow} P'$ and $P'' \subseteq P$. Then, there exists some $\overline{P}$ such that $P'' \stackrel{\varepsilon}{\Longrightarrow} \overline{P} \subseteq P'$.

(e) Let $p \stackrel{\varepsilon}{\Longrightarrow} P' = \{p_1, \dots, p_n\}$ and $p_i \stackrel{a}{\Longrightarrow} P_i$ for $1 \leq i \leq n$. Then, there exists some $\overline{P}$ such that $p \stackrel{a}{\Longrightarrow} \overline{P} \subseteq \bigcup_{i=1}^{n} P_i$.

Note that Parts (a)–(c) also hold for $\stackrel{a}{\longrightarrow}\stackrel{\varepsilon}{\Longrightarrow}$ in place of $\stackrel{\hat{\alpha}}{\Longrightarrow}$ with analogous proofs.

Proof. (a) We proceed by induction on the definition of $p' \stackrel{\varepsilon}{\Longrightarrow} P''$. The claim is trivial for $P'' = \{p'\}$. Now assume that $p' \stackrel{\varepsilon}{\Longrightarrow} P'''$, $\hat{p} \in P'''$, $\hat{p} \stackrel{\tau}{\longrightarrow} \hat{P}$ and $P'' = (P''' \setminus \{\hat{p}\}) \cup \hat{P}$. Further, by induction hypothesis, $p \stackrel{\hat{\alpha}}{\Longrightarrow} \overline{P}' \subseteq (P' \setminus \{p'\}) \cup P'''$ for some $\overline{P}'$ such that $P''' \subseteq \overline{P}'$. Applying Def. 2(b) to $p \stackrel{\hat{\alpha}}{\Longrightarrow} \overline{P}'$ and $\hat{p} \stackrel{\tau}{\longrightarrow} \hat{P}$ (observe $\hat{p} \in \overline{P}'$), we get $p \stackrel{\hat{\alpha}}{\Longrightarrow} \overline{P}$ with $\overline{P} =_{\text{df}} (\overline{P}' \setminus \{\hat{p}\}) \cup \hat{P} \subseteq (((P' \setminus \{p'\}) \cup P''') \setminus \hat{p}) \cup \hat{P} \subseteq (P' \setminus \{p'\}) \cup (P''' \setminus \{\hat{p}\}) \cup \hat{P} = (P' \setminus \{p'\}) \cup P''$; note that equality fails at the second inclusion if $\hat{p} \in P' \setminus (\{p'\} \cup \hat{P})$. Further, $P'' \subseteq \overline{P} = (\overline{P}' \setminus \{\hat{p}\}) \cup \hat{P}$ since $P''' \subseteq \overline{P}'$.

(b) We show by induction on k that there exists a $\overline{P}_k$ such that $p \stackrel{\hat{\alpha}}{\Longrightarrow} \overline{P}_k \subseteq (P' \setminus \{p_1, \dots, p_k\}) \cup \bigcup_{i=1}^{k} P_i$. Part (a) implies the case $k = 1$. Assume the claim holds for k. Now, there are two cases. If $p_{k+1} \notin \overline{P}_k$, then $\overline{P}_{k+1} = \overline{P}_k \subseteq (P' \setminus \{p_1, \dots, p_{k+1}) \cup \bigcup_{i=1}^{k+1} P_i$. Otherwise, $p \stackrel{\hat{\alpha}}{\Longrightarrow} \overline{P}_{k+1} \subseteq (\overline{P}_k \setminus \{p_{k+1}\}) \cup P_{k+1}$ by Part (a). As a consequence, $\overline{P}_{k+1} \subseteq (((P' \setminus \{p_1, \dots, p_k\}) \cup \bigcup_{i=1}^{k} P_i) \setminus \{p_{k+1}\}) \cup P_{k+1} \subseteq (P' \setminus \{p_1, \dots, p_{k+1}) \cup \bigcup_{i=1}^{k+1} P_i$.

(c) The proof proceeds by induction on the total number of applications of Def. 2(c). If this is 0, then $\overline{P} =_{\text{df}} \bigcup_{i=1}^{n} P_i$. Otherwise, assume w.l.o.g. that $P_1 \stackrel{\varepsilon}{\Longrightarrow} P_1''$, $p_1 \in P_1''$, $p_1 \stackrel{\tau}{\longrightarrow} P''$ and $P_1' = (P_1'' \setminus \{p_1\}) \cup P''$. By induction hypothesis, there exists a $\hat{P}$ such that $p \stackrel{\hat{\alpha}}{\Longrightarrow} \hat{P} \subseteq P_1'' \cup \bigcup_{i=2}^{n} P_i'$. If $p_1 \notin \hat{P}$, then $\hat{P} \subseteq \bigcup_{i=1}^{n} P_i'$ and we are done. Otherwise, $p \stackrel{\hat{\alpha}}{\Longrightarrow} \overline{P} =_{\text{df}} (\hat{P} \setminus \{p_1\}) \cup P''$. Since $\hat{P} \subseteq P_1'' \cup \bigcup_{i=2}^{n} P_i'$ implies $\hat{P} \setminus \{p_1\} \subseteq (P_1'' \setminus \{p_1\}) \cup \bigcup_{i=2}^{n} P_i'$, we obtain $\overline{P} \subseteq \bigcup_{i=1}^{n} P_i'$.

(d) The proof is by induction on the derivation of $P \stackrel{\varepsilon}{\Longrightarrow} P'$. For $P = P'$, choose $\overline{P} =_{\text{df}} P''$. Otherwise, assume $P \stackrel{\varepsilon}{\Longrightarrow} \hat{P}$, $p \in \hat{P}$, $p \stackrel{\tau}{\longrightarrow} \hat{P}'$ and $P' = (\hat{P} \setminus \{p\}) \cup \hat{P}'$. By induction hypothesis, there exists a $\overline{P}'$ such that $P'' \stackrel{\varepsilon}{\Longrightarrow} \overline{P}' \subseteq \hat{P}$. If $p \notin \overline{P}'$, then $\overline{P}' \subseteq P'$ and we are done. Otherwise, $\overline{P} =_{\text{df}} (\overline{P}' \setminus \{p\}) \cup \hat{P}' \subseteq P'$.

(e) For all $1 \leq i \leq n$, we have $p_i \stackrel{\varepsilon}{\Longrightarrow} P_i' = \{p_1^i, \dots, p_{k_i}^i\}$ such that $p_j^{\prime i} \stackrel{a}{\longrightarrow} P_j^i$ for $1 \leq j \leq k_i$, and can derive $p_i \stackrel{a}{\Longrightarrow} P_i$ from $p_i \stackrel{a}{\Longrightarrow} \bigcup_{j=1}^{k_i} P_j^i$ by repeated application of Def. 2(b), i.e., $\bigcup_{i=1}^{k_i} P_j^i \stackrel{\varepsilon}{\Longrightarrow} P_i$. By Part (d), we get for each P_j^i a $P_j^{\prime i}$ such that $P_j^i \stackrel{\varepsilon}{\Longrightarrow} P_j^{\prime i} \subseteq P_i \subseteq \bigcup_{i=1}^{n} P_i$. When applying Part (b), we obtain some $\hat{P}$ such that $p \stackrel{\varepsilon}{\Longrightarrow} \hat{P} \subseteq \bigcup_{i=1}^{n} P_i'$. With Def. 2(c) we get $p \stackrel{a}{\Longrightarrow} U$, where U is the union of some of the P_j^i. Taking these P_j^i as the P_i in Part (c) yields $p \stackrel{a}{\Longrightarrow} \overline{P}$ such that $\overline{P}$ is contained in the union of the resp. $P_j^{\prime i}$ and, thus, in $\bigcup_{i=1}^{n} P_i$. □

Now we define our refinement relation. It is a weak alternating simulation conceptually similar to the observational modal refinement found, e.g., in [13]. A notable aspect, originating from IA [11], is that inputs must be matched immediately, i.e., only trailing τs are allowed. Intuitively, this is due to parallel composition requiring that a signal sent from one system must be received immediately; otherwise, it is considered an error (a communication mismatch). Since one wishes not to introduce new errors during refinement, a refined system must immediately provide all specified inputs. This is discussed further in Remark 9.

We treat the universal state e as completely underspecified, i.e., we decree that any state refines it. This is only possible since e is not an ordinary state. We define our refinement preorder for MIAs with common input and output alphabets; we relax this in Sec. 6.

Definition 4 (MIA Refinement)**.** *Let P,Q be MIAs with common input and output alphabets. A relation $\mathscr{R} \subseteq P \times Q$ is a* MIA-refinement relation *if for all $(p,q) \in \mathscr{R}$ with $q \neq e_Q$:*

(i) $p \neq e_P$,

(ii) $q \xrightarrow{i} Q'$ *implies* $\exists P'.\, p \xrightarrow{i}\overset{\varepsilon}{\Longrightarrow} P'$ *and* $\forall p' {\in} P'\, \exists q' {\in} Q'.\, (p',q') \in \mathscr{R}$,

(iii) $q \xrightarrow{\omega} Q'$ *implies* $\exists P'.\, p \overset{\hat{\omega}}{\Longrightarrow} P'$ *and* $\forall p' {\in} P'\, \exists q' {\in} Q'.\, (p',q') \in \mathscr{R}$,

(iv) $p \overset{i}{\dashrightarrow} p'$ *implies* $\exists q'.\, q \overset{i}{\dashrightarrow}\overset{\varepsilon}{=\!\Rightarrow} q'$ *and* $(p',q') \in \mathscr{R}$,

(v) $p \overset{\omega}{\dashrightarrow} p'$ *implies* $\exists q'.\, q \overset{\hat{\omega}}{=\!\Rightarrow} q'$ *and* $(p',q') \in \mathscr{R}$.

We write $p \sqsubseteq q$ and say that p MIA-refines *q if there exists a MIA-refinement relation $\mathscr{R}$ such that $(p,q) \in \mathscr{R}$, and we let $p \sqsupseteq\sqsubseteq q$ stand for $p \sqsubseteq q$ and $q \sqsubseteq p$. Furthermore, we extend these notations to MIAs, write $P \sqsubseteq Q$ if $p_0 \sqsubseteq q_0$, and use $\sqsupseteq\sqsubseteq$ analogously.*

As we show next, Lem. 3 allows us to replace the transition in the premises of (ii) and (iii) above by a trailing weak and a weak one, resp.; the analogous replacement in (iv) and (v) is standard. This result is needed for proving that $\sqsubseteq$ is a preorder.

Proposition 5. *Let $\mathscr{R} \subseteq P \times Q$ be a MIA-refinement relation for MIAs P and Q, and let $(p,q) \in \mathscr{R}$ with $q \neq e_Q$.*

(ii) $q \xrightarrow{i}\overset{\varepsilon}{\Longrightarrow} Q'$ *implies* $\exists P'.\, p \xrightarrow{i}\overset{\varepsilon}{\Longrightarrow} P'$ *and* $\forall p' {\in} P'\, \exists q' {\in} Q'.\, (p',q') \in \mathscr{R}$.

(iii) $q \overset{\hat{\omega}}{\Longrightarrow} Q'$ *implies* $\exists P'.\, p \overset{\hat{\omega}}{\Longrightarrow} P'$ *and* $\forall p' {\in} P'\, \exists q' {\in} Q'.\, (p',q') \in \mathscr{R}$.

(iv) $p \overset{i}{\dashrightarrow}\overset{\varepsilon}{=\!\Rightarrow} p'$ *implies* $\exists q'.\, q \overset{i}{\dashrightarrow}\overset{\varepsilon}{=\!\Rightarrow} q'$ *and* $(p',q') \in \mathscr{R}$.

(v) $p \overset{\hat{\omega}}{=\!\Rightarrow} p'$ *implies* $\exists q'.\, q \overset{\hat{\omega}}{=\!\Rightarrow} q'$ *and* $(p',q') \in \mathscr{R}$.

Proof. The proof of Parts (iv) and (v) is standard; the proof of Part (ii) is very similar to that of Part (iii), although the third case is not relevant for Part (ii); thus, we focus on proving Part (iii) concerning weak disjunctive transitions. We proceed by induction on the definition of $q \overset{\hat{\omega}}{\Longrightarrow} Q'$:

- Let $\omega = \tau$ and $Q' = \{q\}$. Then, we choose $P' =_{\mathrm{df}} \{p\}$.
- Let $q \overset{\hat{\omega}}{\Longrightarrow} Q'$ due to Def. 2(b), i.e., we have $q \overset{\hat{\omega}}{\Longrightarrow} Q'''$, $q'' \in Q'''$, $q'' \xrightarrow{\tau} Q''$ and $Q' = (Q''' \setminus \{q''\}) \cup Q''$. By induction hypothesis, there is a P''' with $p \overset{\hat{\omega}}{\Longrightarrow} P'''$ and $\forall p''' {\in} P'''\, \exists q''' {\in} Q'''.\, (p''',q''') \in \mathscr{R}$. Further, for all $p'' \in P'''$ with $(p'',q'') \in \mathscr{R}$, there is a P'' with $p'' \overset{\varepsilon}{\Longrightarrow} P''$ and $\forall \overline{p} {\in} P''\, \exists \overline{q} {\in} Q''.\, (\overline{p},\overline{q}) \in \mathscr{R}$. Let $\hat{P}$ be the union of these P''. By Lem. 3(b), we have $p \overset{\hat{\omega}}{\Longrightarrow} P' \subseteq (P''' \setminus \{p'' \in P'' \mid (p'',q'') \in \mathscr{R}\}) \cup \hat{P}$. If $p' \in P'$, then either $p' \in \hat{P}$ with a matching $\overline{q} \in Q'' \subseteq Q'$, or there is a matching $q''' \in Q''' \setminus \{q''\} \subseteq Q'$.
- Let $q \overset{\hat{\omega}}{\Longrightarrow} Q'$ due to Def. 2(c), i.e., $\hat{\omega} = o$, $q \overset{\varepsilon}{\Longrightarrow} Q''' = \{q_1, \ldots, q_n\}$ with $q_j \xrightarrow{o} Q_j$ for all $1 \leq j \leq n$, and $Q' = \bigcup_{j=1}^{n} Q_j$. By induction hypothesis, there exists some P''' with $p \overset{\varepsilon}{\Longrightarrow} P'''$ and $\forall p''' {\in} P'''\, \exists q_j {\in} Q'''.\, (p''',q_j) \in \mathscr{R}$. For each $p''' \in P'''$, there exists some j and P'' with $p''' \overset{o}{\Longrightarrow} P''$ and $\forall \overline{p} {\in} P''\, \exists \overline{q} \in Q_j.\, (\overline{p},\overline{q}) \in \mathscr{R}$; let $\hat{P}$ be the union of all these P''. By Lem. 3(e), we obtain $p \overset{o}{\Longrightarrow} P' \subseteq \hat{P}$. For each $p' \in P'$, there exists a matching $\overline{q}$ in some $Q_j \subseteq Q'$. □

Corollary 6. *MIA refinement $\sqsubseteq$ is a preorder and the largest MIA-refinement relation.*

Proof. Reflexivity of $\sqsubseteq$ immediately follows from the fact that the identity relation on states is a MIA-refinement relation. For transitivity one shows that the composition of two MIA-refinement relations is again a MIA-refinement relation, using Prop. 5 and following the lines of [20]. The second claim follows since MIA-refinement relations are easily seen to be closed under union. □

3 Parallel Composition and Hiding

Interface Automata (IA) [10, 11] are equipped with an interleaving parallel operator, where an action occurring as an input in one interface is synchronised with the same action occurring as an output in some other interface; the synchronised action is hidden, i.e., labelled by τ. Since our work builds upon Modal Interfaces (MI) [22] we instead consider here a parallel composition, where the synchronisation of an interface's output action involves all concurrently running interfaces that have the action as input. Moreover, we include a separate operator for hiding outputs (cf. [19]). This properly generalises the binary communication of IA to multicast in MIA.

3.1 Parallel Composition

We present a parallel operator $\|$ on MIA in the same way as we did in [17, 18], except that common actions are not hidden immediately. Parallel composition is defined in two stages. First, a standard product $\otimes$ between two MIAs is introduced. Then, errors are identified, i.e., states where an output is not matched by an appropriate input, and, similarly as in IA, all states from which reaching an error cannot be prevented, are *pruned*, i.e., removed.

Definition 7 (Parallel Product)**.** *MIAs P_1, P_2 are* composable *if $O_1 \cap O_2 = \emptyset$. For such MIAs we define the* product $P_1 \otimes P_2 = ((P_1 \times P_2) \dot{\cup} \{e_{12}\}, I, O, \longrightarrow, \dashrightarrow, (p_{01}, p_{02}), e_{12})$*, where $I =_{df} (I_1 \cup I_2) \setminus (O_1 \cup O_2)$ and $O =_{df} O_1 \cup O_2$ and where $\longrightarrow$ and $\dashrightarrow$ are the smallest relations satisfying the following conditions:*

$$\begin{array}{llll}
\text{(PMust1)} & (p_1,p_2) \xrightarrow{\alpha} P_1' \times \{p_2\} & \textit{if} & p_1 \xrightarrow{\alpha} P_1' \textit{ and } \alpha \notin A_2 \\
\text{(PMust2)} & (p_1,p_2) \xrightarrow{\alpha} \{p_1\} \times P_2' & \textit{if} & p_2 \xrightarrow{\alpha} P_2' \textit{ and } \alpha \notin A_1 \\
\text{(PMust3)} & (p_1,p_2) \xrightarrow{a} P_1' \times P_2' & \textit{if} & p_1 \xrightarrow{a} P_1' \textit{ and } p_2 \xrightarrow{a} P_2' \textit{ for some } a \\
\text{(PMay1)} & (p_1,p_2) \overset{\alpha}{\dashrightarrow} (p_1',p_2) & \textit{if} & p_1 \overset{\alpha}{\dashrightarrow} p_1' \textit{ and } \alpha \notin A_2 \\
\text{(PMay2)} & (p_1,p_2) \overset{\alpha}{\dashrightarrow} (p_1,p_2') & \textit{if} & p_2 \overset{\alpha}{\dashrightarrow} p_2' \textit{ and } \alpha \notin A_1 \\
\text{(PMay3)} & (p_1,p_2) \overset{a}{\dashrightarrow} (p_1',p_2') & \textit{if} & p_1 \overset{a}{\dashrightarrow} p_1' \textit{ and } p_2 \overset{a}{\dashrightarrow} p_2' \textit{ for some } a.
\end{array}$$

From the parallel product, parallel composition is obtained by pruning, i.e., one removes errors and states leading up to errors via local actions, so called *illegal* states. This cuts all input transitions leading to an illegal state.

In [6] we have shown that de Alfaro and Henzinger have defined pruning in an inappropriate way in [10]. We remedied this by cutting not only an *i*-transition from some state p to an illegal state, but also all other *i*-transitions from p. Now, in [6, 10], p can be refined by a state with an *i*-transition and arbitrary behaviour afterward; we express this by introducing an *i*-may-transition to the universal state.

Definition 8 (Parallel Composition)**.** *Given a parallel product $P_1 \otimes P_2$, a state (p_1, p_2) is a* new error *if there is some $a \in A_1 \cap A_2$ such that (a) $a \in O_1$, $p_1 \overset{a}{\dashrightarrow}$ and $p_2 \overset{a}{\not\longrightarrow}$, or (b) $a \in O_2$, $p_2 \overset{a}{\dashrightarrow}$ and $p_1 \overset{a}{\not\longrightarrow}$. It is an* inherited error *if one of its components is a universal state, i.e., if it is of the form (e_1, p_2) or (p_1, e_2).*

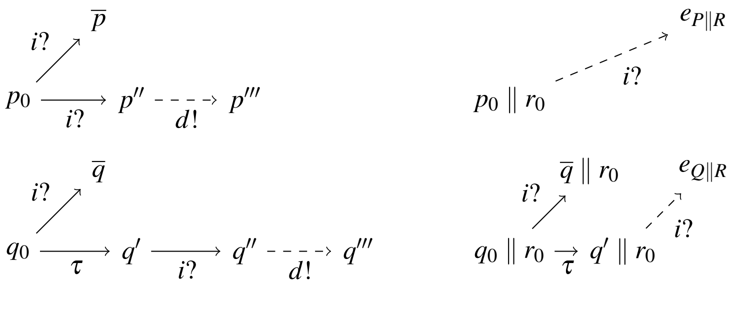

Figure 1: Illustration of the complications of pruning, where $A_P = A_Q = \{i\}/\{d\}$ and $A_R = \{d\}/\emptyset$.

We define the set $E \subseteq P_1 \times P_2$ of illegal *states as the least set such that $(p_1, p_2) \in E$ if (i) (p_1, p_2) is a new or inherited error or (ii) $(p_1, p_2) \overset{\omega}{\dashrightarrow} (p_1', p_2')$ and $(p_1', p_2') \in E$.*

Should the initial state be an illegal state, i.e., $(p_{01}, p_{02}) \in E$, then e_{12} becomes the initial – and thus the only reachable – state of the parallel composition *$P_1 \| P_2$. In this case, P_1 and P_2 are called* incompatible.

Otherwise, $P_1 \| P_2$ is obtained from $P_1 \otimes P_2$ by pruning *illegal states as follows. If there is a state $(p_1, p_2) \notin E$ with $(p_1, p_2) \overset{i}{\dashrightarrow} (p_1', p_2') \in E$ for some $i \in I$, then all must- and may-transitions labelled i and starting at (p_1, p_2) are removed, and a single transition $(p_1, p_2) \overset{i}{\dashrightarrow} e_{12}$ is added. Furthermore, all states in E, all unreachable states (except for e_{12}), and all their incoming and outgoing transitions are removed. If $(p_1, p_2) \in P_1 \| P_2$, we write $p_1 \| p_2$ and call p_1 and p_2* compatible.

Remark 9. *As mentioned before Def. 4, allowing leading τs when matching input may-transitions would render our pruning insufficient. When generalising Def. 4(iv) this way, we would have $P \sqsubseteq Q$ in Fig. 1 due to $\{(p_0, q_0), (\overline{p}, \overline{q}), (p, q'), (p'', q''), (p''', q''')\}$. Their parallel compositions with $R =_{df} (\{r_0, e_R\}, \{d\}, \emptyset, \emptyset, \emptyset, r_0, e_R)$ would, with our current pruning, no longer be in the refinement relation: $q_0 \| r_0$ would still have an i-must-transition, while $p_0 \| r_0$ would have lost both i-must-transitions during pruning. Thus, the refinement would not be a precongruence wrt. parallel composition.*

It is possible to repair this by a different pruning construction. For example, when cutting i-transitions at some state s, one can go backward from s along τ-transitions and cut all outgoing i-transitions; in the example, $q' \| r_0$ has an i-transition that is cut and, consequently, we would also remove every i-transition originating from $q_0 \| r_0$ since $q_0 \| r_0 \overset{\varepsilon}{\Longrightarrow} q' \| r_0$. This different parallel composition $\|'$ fixes the current counterexample as it removes $q_0 \| r_0 \xrightarrow{i} \overline{q} \| r_0$ and its underlying may-transition, replacing them with a i-may-transition to the universal state. □

In [22], Raclet et al. use a similar approach to pruning: they introduce a state we denote as tt, which has only input may-transitions as incoming transitions. Furthermore, it has a may-loop for every action of the parallel composition so that it can be refined by any state, much like our universal state (cf. Def. 4(i)). To see the difference, condsider the MIAs P, Q, R in Fig. 2, where we construct $(P \| Q) \| R$ according to [22]. Since tt is an ordinary state, it is combined with r_0 inheriting the j-must-loop. When refining the a-may-transition to this combined state by a must-transition, the target state of the latter necessarily has a j-must-transition. In our approach, the combination with r_0 is an inherited error, and e does not have any must-transitions.

More importantly, there is the severe problem that parallel composition in [22] is not associative. Consider again the systems P, Q and R in Fig. 2; their parallel compositions shown are not equivalent according

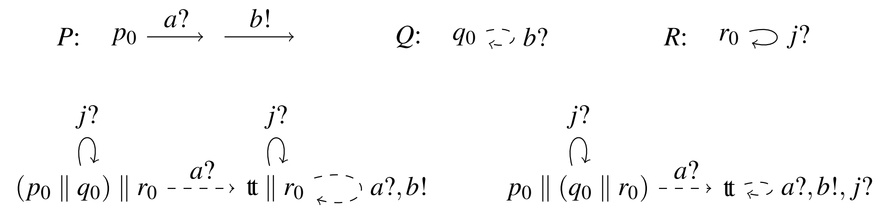

Figure 2: Differences of our state e to $\mathtt{tt}$ in [22], where $A_P = \{a\}/\{b\}$, $A_Q = \{b\}/\emptyset$ and $A_R = \{j\}/\emptyset$.

to $\sqsupseteq\sqsubseteq$ (and the equivalence in [22]). Note that our example does not rely on the multicast aspect of our parallel composition; it works just as well for IA parallel composition.

We prove now that parallel composition is associative, starting with two lemmas.

Lemma 10. *If P, Q are composable MIA and $p\|q \in P\|Q$, $o \in O_{P\|Q}$ and $i \in I_{P\|Q}$, then:*

1. *$p \| q \overset{o}{\dashrightarrow}$ iff $p \overset{o}{\dashrightarrow}$ and $o \in O_P$, or $q \overset{o}{\dashrightarrow}$ and $o \in O_Q$.*

2. *If $p \overset{i}{\not\longrightarrow}$ and $i \in I_P$ or if $q \overset{i}{\not\longrightarrow}$ and $i \in I_Q$, then $p \| q \overset{i}{\not\longrightarrow}$. The reverse implication does not hold in general.*

Proof. 1. Implication "⇒" is obvious. If implication "⇐" were false, (p,q) would be a new error or $(p,q) \overset{o}{\dashrightarrow} (p',q')$ in $P \otimes Q$ with $p' \| q'$ undefined. Both would render (p,q) illegal and $p \| q$ undefined, leading to a contradiction.

2. The implication is also obvious, but the reverse implication does not hold since the must-transition of $p \| q$ might have been cut during pruning. □

Lemma 11. *Given three MIAs P_1, P_2 and P_3, we have:*

(a) *$(P_1 \| P_2) \| P_3$ is defined iff P_1, P_2 and P_3 are pairwise composable iff $(P_1 \| P_2) \| P_3$ is defined as well.*

(b) *$(P_1 \| P_2) \| P_3$ is equal to S obtained from pruning $(P_1 \otimes P_2) \otimes P_3$ (up to the name of the respective universal state). For this purpose, a state $((p_1, p_2), p_3)$ is a new error if, for some $i \neq j$ with $i, j \in \{1,2,3\}$, there is some $a \in A_i \cap A_j$ such that $a \in O_i$, $p_i \overset{a}{\dashrightarrow}$ and $p_j \overset{a}{\not\longrightarrow}$; it is an inherited one, if $p_i = e_i$ for some $i \in \{1,2,3\}$.*

Proof. (a) is easy. (b) For reasons of readability we use P ,Q, R instead of P_1, P_2, P_3 and write (p,q,r) for $((p,q),r)$. Let E_{PQR} denote the illegal states of $(P \otimes Q) \otimes R$ as defined above for constructing S. We denote the illegal states of $P \otimes Q$ and $(P \| Q) \otimes R$ by E_{PQ} and $E_{(P\|Q)\otimes R}$ resp. Furthermore, let Err_{PQR}, Err_{PQ} and $Err_{(P\|Q)\otimes R}$ be the errors of the respective systems. We also say that two states p and q *produce an error*, if (p,q) is an error due to $p \overset{a}{\dashrightarrow}$ and $q \overset{a}{\not\longrightarrow}$ while $a \in O_P \cap I_Q$ or vice versa.

Our first aim is to show that $E_{PQR} = (E_{PQ} \times R) \cup (E_{(P\|Q)\otimes R} \setminus (\{e_{P\|Q}\} \times R))$.

⊆: We prove that $(p,q,r) \in E_{PQR}$ is contained in the r.h.s. by induction on the length of a local transition sequence from (p,q,r) to an error in Err_{PQR}. For the base case, we show $Err_{PQR} \subseteq (E_{PQ} \times R) \cup (E_{(P\|Q)\otimes R} \setminus (\{e_{P\|Q}\} \times R))$.

Consider $(p,q,r) \in Err_{PQR}$. If (p,q) is illegal in $P \otimes Q$ (this covers the cases that p or q is universal or that p and q produce an error), then $(p,q,r) \in E_{PQ} \times R$. Otherwise, $r = e_R$ and $(p,q,r) \in Err_{(P\|Q)\otimes R} \setminus (\{e_{P\|Q}\} \times R) \subseteq E_{(P\|Q)\otimes R} \setminus (\{e_{P\|Q}\} \times R)$, or r produces the error with p or q (possibly both). W.l.o.g. let p and r produce the error because $p \overset{a}{\dashrightarrow}$ and $r \not\xrightarrow{a}$ for some $a \in O_P \cap I_R$ or because $p \not\xrightarrow{a}$ and $r \overset{a}{\dashrightarrow}$ for some $a \in I_P \cap O_R$. By Lem. 10.1, this leads to $p \parallel q \overset{a}{\dashrightarrow}$ and – by Lem. 10.2 – to $r \not\xrightarrow{a}$ or $p \parallel q \not\xrightarrow{a}$ and $r \overset{a}{\dashrightarrow}$. Again, $(p,q,r) \in Err_{(P\|Q)\otimes R} \setminus (\{e_{P\|Q}\} \times R)$.

For the induction step, consider $(p,q,r) \in E_{PQR}$ with $(p,q,r) \overset{\omega}{\dashrightarrow} (p',q',r') \in E_{PQR}$ and $(p',q',r') \in (E_{PQ} \times R) \cup (E_{(P\|Q)\otimes R} \setminus (\{e_{P\|Q}\} \times R))$ by induction. By the argument at the beginning of the base case, we can assume that $p \parallel q$ is defined and, thus, $(p \parallel q, r)$ exists in $(P \parallel Q) \otimes R$. Thus, if $(p',q',r') \in E_{(P\|Q)\otimes R} \setminus (\{e_{P\|Q}\} \times R))$, then $(p,q,r) \in E_{(P\|Q)\otimes R} \setminus (\{e_{P\|Q}\} \times R))$ by definition of E.

Finally, consider $(p',q',r') \in E_{PQ} \times R$. If the ω-transition is only performed by r, then $(p',q',r') = (p,q,r')$ and thus $(p,q) \in E_{PQ}$, contradicting that (p,q) is not illegal. Otherwise, if $\omega \in O_{P\otimes Q} \cup \{\tau\}$, then $(p,q) \overset{\omega}{\dashrightarrow} (p',q') \in E_{PQ}$ and $(p,q){\in}E_{PQ}$, a contradiction. Thus, $\omega \in I_{P\otimes Q}$ and r performs ω as an output since, overall, it is an output. As $(p,q) \overset{\omega}{\dashrightarrow} (p',q') \in E_{PQ}$, this input transition is cut when pruning $P \otimes Q$, implying $p \parallel q \not\xrightarrow{\omega}$. This shows again that $(p,q,r) \in Err_{(P\|Q)\otimes R} \setminus (\{e_{P\|Q}\} \times R)$.

$\supseteq$: We show that $(E_{PQ} \times R) \cup (E_{(P\|Q)\otimes R} \setminus (\{e_{P\|Q}\} \times R)) \subseteq E_{PQR}$.

- $E_{PQ} \times R \subseteq E_{PQR}$: We prove that $(p,q,r) \in E_{PQ} \times R$ is contained in E_{PQR} by induction on the length of a local transition sequence from (p,q) to an error in Err_{PQ}. In the base case $(p,q) \in Err_{PQ}$, we have that p and q produce an error or one of them is an error state. In either case $(p,q,r) \in Err_{PQR} \subseteq E_{PQR}$. For the induction step, consider some $(p,q) \overset{\omega}{\dashrightarrow} (p',q') \in E_{PQ}$ where, by induction, $\{(p',q')\} \times R \subseteq E_{PQR}$. If $\omega \notin A_R$, then $(p,q,r) \overset{\omega}{\dashrightarrow} (p',q',r) \in E_{PQR}$ and we are done. If $\omega \in A_R$, we must have $\omega \in I_R$. Now either $(p,q,r) \in Err_{PQR}$ or $(p,q,r) \overset{\omega}{\dashrightarrow} (p',q',r') \in E_{PQR}$ for some r', and in either case we are done.
- $E_{(P\|Q)\otimes R} \setminus (\{e_{P\|Q}\} \times R) \subseteq E_{PQR}$: We prove that $(p,q,r) \in E_{(P\|Q)\otimes R} \setminus (\{e_{P\|Q}\} \times R)$ is contained in E_{PQR} by induction on the length of a local transition sequence from $(p \parallel q, r)$ to an error in $Err_{(P\|Q)\otimes R}$.
  In the base case $(p \parallel q, r) \in Err_{(P\|Q)\otimes R} \setminus (\{e_{P\|Q}\} \times R)$, we have that $r = e_R$ and, thus, $(p,q,r) \in Err_{PQR} \subseteq E_{PQR}$, or that $p \parallel q$ and r produce an error. The latter means: Either $p \parallel q \overset{a}{\dashrightarrow}$ and $r \not\xrightarrow{a}$ for some $a \in (O_P \cup O_Q) \cap I_R$, implying $p \overset{a}{\dashrightarrow}$ and $a \in O_P$ or $q \overset{a}{\dashrightarrow}$ and $a \in O_Q$ by Lem. 10.1, and hence $(p,q,r) \in Err_{PQR} \subseteq E_{PQR}$. Or $p \parallel q \not\xrightarrow{a}$ and $r \overset{a}{\dashrightarrow}$ for some $a \in (I_P \cup I_Q) \cap O_R$. Here $p \parallel q \not\xrightarrow{a}$ can have several reasons. We might have $p \not\xrightarrow{a}$ and $a \in I_P$ or $q \not\xrightarrow{a}$ and $a \in I_Q$ and in both cases $(p,q,r) \in Err_{PQR}$ due to $r \overset{a}{\dashrightarrow}$. Otherwise, $(p,q) \xrightarrow{a} (p',q') \in E_{PQ}$; in this case $(p,q,r) \overset{a}{\dashrightarrow} (p',q',r') \in E_{PQ} \times R \subseteq E_{PQR}$ by the above, implying $(p,q,r) \in E_{PQR}$, since $a \in O_{(P\otimes Q)\otimes R}$.

  For the induction step, consider some $(p \parallel q, r) \overset{\omega}{\dashrightarrow} (p' \parallel q', r') \in E_{(P\|Q)\otimes R}$; since $(p',q',r') \in E_{PQR}$ by induction, we are done with the '$\supseteq$'-case and thus with showing the desired equality.

We now show that the state space $(P \times Q \times R) \setminus E_{PQR} \cup \{e\}$ of S coincides with that of $(P \parallel Q) \parallel R$ (up to the name of the universal state). The states of $(P \parallel Q) \parallel R$ are:

$$\begin{aligned} &(((P\times Q)\setminus E_{PQ}\cup\{e_{P\|Q}\})\times R)\setminus E_{(P\|Q)\otimes R}\cup\{e\}\\ =&((P\times Q\times R)\setminus(E_{PQ}\times R)\cup\{e_{P\|Q}\}\times R)\setminus E_{(P\|Q)\otimes R}\cup\{e\}\\ =&\underbrace{(P\times Q\times R)\setminus(E_{PQ}\times R\cup E_{(P\|Q)\otimes R})}_{=(P\times Q\times R)\setminus E_{PQR}}\cup(\underbrace{\{e_{P\|Q}\}\times R\setminus E_{(P\|Q)\otimes R}}_{=\emptyset}\cup\{e\})\end{aligned}$$

For the last step, note that $(P\times Q\times R)\cap\{e_{P\|Q}\}\times R=\emptyset$.

Finally, we show that the transitions of S and $(P \parallel Q) \parallel R$ are the same. For transitions to e, consider $(p \parallel q) \parallel r \overset{i}{\dashrightarrow} e$ for some $i \in I_{(P\|Q)\|R}$. This transition exists, iff $(p \parallel q, r) \overset{i}{\dashrightarrow} (t, r') \in E_{(P\|Q)\otimes R}$. Now either $t = p' \parallel q'$ for some p' and q', and $(t, r') \in E_{(P\|Q)\otimes R} \setminus \{e_{P\|Q}\} \times R$. Or $(p \parallel q, r) \overset{i}{\dashrightarrow} (e_{P\|Q}, r')$, which holds iff $(p,q) \overset{i}{\dashrightarrow} (p',q') \in E_{PQ}$ and either $r \overset{i}{\dashrightarrow} r'$ or $i \notin A_R$ and $r = r'$. This is equivalent to $(p,q,r) \overset{i}{\dashrightarrow} (p',q',r') \in E_{PQ} \times R$. Both cases together show: $(p \parallel q) \parallel r \overset{i}{\dashrightarrow} e$ iff $(p,q,r) \overset{i}{\dashrightarrow}_{P\otimes Q\otimes R} (p',q',r') \in E_{PQR}$ iff $(p,q,r) \overset{i}{\dashrightarrow}_S e$ in S.

For transitions between the states of S (which are also the states of $(P \parallel Q) \parallel R$), observe that these are exactly the transitions inherited from $(P \otimes Q) \otimes R$ minus all i-transitions from any s with $s \overset{i}{\dashrightarrow} e$. In $(P \parallel Q) \parallel R$, all transitions are inherited indirectly from $(P \otimes Q) \otimes R$; if $s \overset{i}{\dashrightarrow} e$, s clearly has no other i-transitions.

It remains to show that no a-transition from some s is missing, if $s \overset{a}{\not\dashrightarrow} e$. Assume the contrary, namely that a transition $s = (p,q,r) \overset{a}{\dashrightarrow}_{P\otimes Q\otimes R} (p',q',r')$ of S is missing in $(P \parallel Q) \parallel R$ although $s \overset{a}{\not\dashrightarrow} e$. This can only be due to pruning; recall that $(p \parallel q) \parallel r$ and $(p' \parallel q') \parallel r'$ are states of $(P \parallel Q) \parallel R$.

If $(p,q) \overset{a}{\not\dashrightarrow}_{P\otimes Q}$, then $a \notin A_P \cup A_Q$, and the missing transition was lost when pruning $(P \parallel Q) \otimes R$, contradicting $s \overset{a}{\not\dashrightarrow} e$. Thus, $(p,q) \overset{a}{\dashrightarrow}_{P\otimes Q} (p',q')$.

If $p \parallel q \overset{a}{\not\dashrightarrow} p' \parallel q'$, then we have $p \parallel q \overset{a}{\dashrightarrow} e_{P\|Q}$ and $(p \parallel q, r)$ is illegal if $a \in O_R$ or $(p \parallel q) \parallel r \overset{a}{\dashrightarrow} e$, a contradiction in both cases. Thus, $(p \parallel q, r) \overset{a}{\dashrightarrow} (p' \parallel q', r')$ in $(P \parallel Q) \otimes R$. Again in this case, the transition was lost when pruning $(P \parallel Q) \otimes R$, a contradiction. □

This lemma immediately implies the desired associativity.

Theorem 12 (Associativity of Parallel Composition)**.** *Parallel composition is associative in the sense that, for MIAs P, Q and R, if $(P \parallel Q) \parallel R$ is defined, then $P \parallel (Q \parallel R)$ is defined as well and they are isomorphic, and vice versa.*

Now we proceed to show that MIA refinement is compositional wrt. parallel composition, which essentially means that $P \sqsubseteq Q$ implies $P \parallel R \sqsubseteq Q \parallel R$ for MIAs P, Q and R. The proof requires the following two lemmas.

Lemma 13 (Compatibility)**.** *For MIAs P_1, P_2 and Q_1, let E_P be the E-set of $P_1 \otimes P_2$ and E_Q be the one of $Q_1 \otimes P_2$. Further, let $p_1 \in P_1$, $p_2 \in P_2$ and $q_1 \in Q_1$ such that $p_1 \sqsubseteq q_1$. Then, $(p_1, p_2) \in E_P$ implies $(q_1, p_2) \in E_Q$.*

Proof. Let I_1/O_1 be the alphabets of P_1 and Q_1, let I_2/O_2 be the alphabets of P_2 and let I/O be the alphabets of the products. The proof is by induction on the length of a path from (p_1, p_2) to an error of $P_1 \otimes P_2$:

(Base) Let (p_1, p_2) be an error.

- Let $p_1 \overset{a}{\dashrightarrow}$ with $a \in O_1 \cap I_2$ and $p_2 \overset{a}{\not\longrightarrow}$. Then, for some q_1', we have $q_1 \overset{\varepsilon}{\Rightarrow} q_1' \overset{a}{\dashrightarrow}$ by $p_1 \sqsubseteq q_1$; hence, $(q_1, p_2) \overset{\varepsilon}{\Rightarrow} (q_1', p_2) \in E_Q$ and $(q_1, p_2) \in E_Q$ as well.
- Let $p_2 \overset{a}{\dashrightarrow}$ with $a \in O_2 \cap I_1$ and $p_1 \overset{a}{\not\longrightarrow}$. If $q_1 \overset{a}{\longrightarrow}$, we have a contradiction to $p_1 \sqsubseteq q_1$; otherwise, (q_1, p_2) is an error since $a \in I_1 \cap O_2$.
- If $p_1 = e_{P_1}$, then $q_1 = e_{Q_1}$ because of $p_1 \sqsubseteq q_1$, and thus $(q_1, p_2) \in E_Q$.
- Case $p_2 = e_{P_2}$ is obvious.

(Step) For a shortest path from (p_1, p_2) to an error, consider the first transition $(p_1, p_2) \overset{\omega}{\dashrightarrow} (p_1', p_2') \in E_P$, where $\omega \in O \cup \{\tau\}$. The transition is due to either Rule (PMay1), (PMay2) or (PMay3). In all cases we find some $q_1' \in Q_1$ such that (q_1', p_2') is locally reachable from (q_1, p_2) and $p_1' \sqsubseteq q_1'$. The latter implies $(q_1', p_2') \in E_Q$ by induction hypothesis.

(PMay1) $p_1 \overset{\omega}{\dashrightarrow} p_1'$, $p_2 = p_2'$, $\omega \notin A_2$. Due to $p_1 \sqsubseteq q_1$, there is a q_1' such that $q_1 \overset{\hat{\omega}}{\Rightarrow} q_1'$ and $p_1' \sqsubseteq q_1'$, and $(q_1, p_2) \overset{\hat{\omega}}{\Rightarrow} (q_1', p_2)$ by applications of (PMay1). By induction hypothesis, $(q_1', p_2) \in E_Q$ and, therefore, $(q_1, p_2) \in E_Q$.

(PMay2) $p_1 = p_1'$, $p_2 \overset{\omega}{\dashrightarrow} p_2'$ and $\omega \notin A_1$. Using (PMay2) we obtain $(q_1, p_2) \overset{\omega}{\dashrightarrow} (q_1, p_2')$, so that $(q_1, p_2') \in E_Q$ by induction hypothesis. Hence, $(q_1, p_2) \in E_Q$, too.

(PMay3) $\omega = o$, $p_1 \overset{o}{\dashrightarrow} p_1'$ and $p_2 \overset{o}{\dashrightarrow} p_2'$ with $o \in A_1 \cap A_2$. Note that o is an output for the product and one of its components, but an input for the other. By $p_1 \sqsubseteq q_1$ we have $q_1 \overset{\varepsilon}{\Rightarrow} q_1'' \overset{o}{\dashrightarrow} q_1''' \overset{\varepsilon}{\Rightarrow} q_1'$ for some q_1', q_1'', q_1''' with $p_1' \sqsubseteq q_1'$. (Note, that in case $o \in I_1$ we have $q_1 = q_1''$.) Therefore, we get $(q_1, p_2) \overset{\varepsilon}{\Rightarrow} (q_1'', p_2) \overset{o}{\dashrightarrow} (q_1''', p_2') \overset{\varepsilon}{\Rightarrow} (q_1', p_2')$ via (PMay1) and (PMay3). By induction hypothesis, $(q_1', p_2') \in E_Q$ and, hence, $(q_1, p_2) \in E_Q$, too. □

The next lemma generalises the synchronisation according to Rule (PMust3) to weak transitions.

Lemma 14 (Weak Must-Transitions)**.** *Let P, Q be composable MIAs. If $p \overset{a}{\Longrightarrow} P'$ (or $p \overset{a}{\longrightarrow}\overset{\varepsilon}{\Longrightarrow} P'$) and $q \overset{a}{\longrightarrow} Q'$ for some $a \in A_P \cap A_Q$, then $(p, q) \overset{a}{\Longrightarrow} P' \times Q'$ (or $(p, q) \overset{a}{\longrightarrow}\overset{\varepsilon}{\Longrightarrow} P' \times Q'$) in $P \otimes Q$.*

Proof. Consider $P'' \subseteq P$ and P''' with (i) $p \overset{\varepsilon}{\Longrightarrow} P'' = \{p_1, \ldots, p_n\}$ and $\forall i.\, p_i \overset{a}{\longrightarrow} P_i$ such that $P''' = \bigcup_{i=1}^{n} P_i$ and (ii) P' is obtained from P''' by repeated application of Def. 2(c) with $\alpha = \tau$. In $P \otimes Q$, we get $(p, q) \overset{\varepsilon}{\Longrightarrow} P'' \times \{q\}$ by the definition of $\overset{\varepsilon}{\Longrightarrow}$ and repeated application of (PMust1). Now, one can replace $(p_1, q), \ldots, (p_n, q)$ in $P'' \times \{q\}$ simultaneously by the elements of $P_1 \times Q', \ldots, P_n \times Q'$, whence $(p, q) \overset{a}{\Longrightarrow} P''' \times Q'$. The replacements of some $\overline{p}$ by $\overline{P}$ that transform P''' to P' can be applied to $P''' \times Q'$: each $(\overline{p}, q')$ with $q' \in Q'$ is replaced by the elements of $\overline{P} \times \{q'\}$.

The alternative claim for the trailing-weak transitions is a special case of the first claim, where $P'' = \{p\}$. □

Theorem 15 (Compositionality of Parallel Composition)**.** *Let P_1, P_2 and Q_1 be MIAs and $P_1 \sqsubseteq Q_1$. Assume that Q_1 and P_2 are composable, then:*

(a) *P_1 and P_2 are composable.*

(b) *$P_1 \parallel P_2 \sqsubseteq Q_1 \parallel P_2$, and $P_1 \parallel P_2$ is compatible if $Q_1 \parallel P_2$ is.*

Proof. Part (a) is trivial. Regarding Part (b), the second claim is immediate from the first with Lem. 13. We denote the universal state of $P_1 \parallel P_2$ and $Q_1 \parallel P_2$ as e_P and e_Q resp. E_P stand for the E-set of $P_1 \otimes P_2$ and E_Q for the one of $Q_1 \otimes P_2$, as in Lem. 13. To establish the first claim, we prove that

$$\mathscr{R} =_{\text{df}} \{(p_1 \parallel p_2,\ q_1 \parallel p_2) \mid p_1 \sqsubseteq q_1\} \cup (P_1 \parallel P_2) \times \{e_Q\}$$

is a MIA-refinement relation, for which we check the conditions of Def. 4; the second set obviously satisfies them. Then, we are done since $p_{01} \sqsubseteq q_{01}$ due to $P_1 \sqsubseteq Q_1$ and therefore $(p_{01} \parallel p_{02},\ q_{01} \parallel p_{02}) \in \mathscr{R}$. For the second subset, the check is trivial; so consider some $(p_1 \parallel p_2,\ q_1 \parallel p_2) \in \mathscr{R}$:

(i) Obvious, since $p_1 \parallel p_2 \neq e_P$.

(ii) Let $q_1 \parallel p_2 \xrightarrow{i} \overline{Q}$ due to either Rule (PMust1), (PMust2) or (PMust3). Note that $(q_1, p_2) \xrightarrow{i} \overline{Q}$ in $Q_1 \otimes P_2$ as well. If any state pair in $\overline{Q}$ was illegal, the transition would have been removed by pruning.

(PMust1) $q_1 \xrightarrow{i} Q'_1$ and $\overline{Q} = Q'_1 \times \{p_2\}$. By $p_1 \sqsubseteq q_1$, there is a $P'_1 \subseteq P_1$ such that $p_1 \xrightarrow{i}\overset{\varepsilon}{\Longrightarrow}_{P_1} P'_1$ and $\forall p'_1{\in}P'_1\, \exists q'_1{\in}Q'_1.\, p'_1 \sqsubseteq q'_1$. Now, $(p_1, p_2) \xrightarrow{i}\overset{\varepsilon}{\Longrightarrow} P'_1 \times \{p_2\}$ by repeated application of Rule (PMust1) and since $i \notin A_2$. For every $(p'_1, p_2) \in P'_1 \times \{p_2\}$, we have a suitable $(q'_1, p_2) \in Q'_1 \times \{p_2\}$; moreover, $(p'_1, p_2) \notin E_P$ since $(q'_1, p_2) \notin E_Q$ and due to Lem. 13. Thus, we have $(p'_1 \parallel p_2, q'_1 \parallel p_2) \in \mathscr{R}$.

It remains to show that $(p_1, p_2) \xrightarrow{i}\overset{\varepsilon}{\Longrightarrow} P'_1 \times \{p_2\}$ also exists in $P_1 \parallel P_2$, i.e., that no state (p''_1, p_2) along this weak transition is pruned. More generally, let us consider any $\overline{p}_1$ and p''_1 with $p_1 \overset{i}{\dashrightarrow} \overline{p}_1 \overset{\varepsilon}{\Longrightarrow} p''_1$, implying $(p_1, p_2) \overset{i}{\dashrightarrow} (\overline{p}_1, p_2) \overset{\varepsilon}{\Longrightarrow} (p''_1, p_2)$. Because of $p_1 \overset{i}{\dashrightarrow} \overline{p}_1$ and $p_1 \sqsubseteq q_1$, there must be some $\overline{q}_1$ with $q_1 \overset{i}{\dashrightarrow}\overset{\varepsilon}{\Longrightarrow} \overline{q}_1$ which implies $(q_1, p_2) \overset{i}{\dashrightarrow}\overset{\varepsilon}{\Longrightarrow} (\overline{q}_1, p_2)$, and $\overline{p}_1 \sqsubseteq \overline{q}_1$. If $(\overline{q}_1, p_2) \in E_Q$, then all outgoing i-transitions from $q_1 \parallel p_2$ would have been pruned, contradicting our assumptions. Thus, and by Lem. 13, $(\overline{p}_1, p_2) \notin E_P$, which means that $(p''_1, p_2) \notin E_P$, too.

(PMust2) $p_2 \xrightarrow{i} P'_2$ and $\overline{Q} = \{q_1\} \times P'_2$. Then, $(p_1, p_2) \xrightarrow{i} \overline{P} = \{p_1\} \times P'_2$ according to (PMust2) and since $i \notin A_1$. For $(p_1, p'_2) \in \overline{P}$, we get $(p_1, p'_2) \notin E_P$ because $(q_1, p'_2) \notin E_Q$ and due to Lem. 13. Thus, $p_1 \parallel p_2 \xrightarrow{i} \overline{P}$ and, for every $p_1 \parallel p'_2 \in \overline{P}$, we have $q_1 \parallel p'_2 \in \overline{Q}$ with $(p_1 \parallel p'_2, q_1 \parallel p'_2) \in \mathscr{R}$.

(PMust3) $q_1 \xrightarrow{i} Q'_1$, $p_2 \xrightarrow{i} P'_2$ and $\overline{Q} = Q'_1 \times P'_2$. (Note that $i \in I_1 \cap I_2$.) Then, by $p_1 \sqsubseteq q_1$, there is a set $P'_1 \subseteq P_1$ such that $p_1 \xrightarrow{i}\overset{\varepsilon}{\Longrightarrow} P'_1$ and $\forall p'_1{\in}P'_1\, \exists q'_1{\in}Q'_1.\, p'_1 \sqsubseteq q'_1$. By Lem. 14 we get that $(p_1, p_2) \xrightarrow{i}\overset{\varepsilon}{\Longrightarrow} P'_1 \times P'_2$.

Similarly to Case (PMust1), it remains to show that $(p_1, p_2) \xrightarrow{i}\overset{\varepsilon}{\Longrightarrow} P'_1 \times P'_2$ also exists in $P_1 \parallel P_2$, i.e., no state (p''_1, p'_2) along this weak transition is pruned. More generally, let us consider any $\overline{p_1}$ and p''_1 with $p_1 \overset{i}{\dashrightarrow} \overline{p_1} \overset{\varepsilon}{\Longrightarrow} p''_1$ and some p'_2 with $p_2 \overset{i}{\dashrightarrow} p'_2$, implying $(p_1, p_2) \overset{i}{\dashrightarrow} (\overline{p_1}, p'_2) \overset{\varepsilon}{\Longrightarrow} (p''_1, p'_2)$. Because of $p_1 \overset{i}{\dashrightarrow} \overline{p_1}$ and $p_1 \sqsubseteq q_1$, there must be some $\overline{q_1}$ with $q_1 \overset{i}{\dashrightarrow}\overset{\varepsilon}{\Longrightarrow} \overline{q_1}$, which implies $(q_1, p_2) \overset{i}{\dashrightarrow}\overset{\varepsilon}{\Longrightarrow} (\overline{q_1}, p'_2)$, and $\overline{p_1} \sqsubseteq \overline{q_1}$. If $(\overline{q_1}, p'_2) \in E_Q$, then all outgoing i-transitions from $q_1 \parallel p_2$ would have been pruned, contradicting our assumptions. Therefore, and by Lem. 13, $(\overline{p_1}, p'_2) \notin E_P$, which means that also $(p''_1, p'_2) \notin E_P$.

(iii) Let $q_1 \parallel p_2 \xrightarrow{\omega} \overline{Q}$ due to either (PMust1), (PMust2) or (PMust3). Again the transition and the states exist in $Q_1 \otimes P_2$, too, for the same reasons as above.

(PMust1) $q_1 \xrightarrow{\omega} Q'_1$ and $\overline{Q} = Q'_1 \times \{p_2\}$. Then, by $p_1 \sqsubseteq q_1$, there exists $P'_1 \subseteq P_1$ such that $p_1 \overset{\hat{\omega}}{\Longrightarrow} P'_1$ and $\forall p'_1{\in}P'_1\, \exists q'_1{\in}Q'_1 .\, p'_1 \sqsubseteq q'_1$. Now, $(p_1, p_2) \overset{\hat{\omega}}{\Longrightarrow} P'_1 \times \{p_2\}$ according to (PMust1) and since $\omega \notin A_2$. Because p_1 and p_2 are compatible, this also holds for all pairs along this weak transition by the definition of E_P. For $p'_1 \in P'_1$ we have a suitable $q'_1 \in Q'_1$ such that, for the arbitrary $p'_1 \parallel p_2$, we also have $(p'_1 \parallel p_2, q'_1 \parallel q_2) \in \mathscr{R}$.

(PMust2) $p_2 \xrightarrow{\omega}_{P_2} P'_2$ and $\overline{Q} = \{q_1\} \times P'_2$. In this case we obtain that $(p_1, p_2) \xrightarrow{\omega} \overline{P} = \{p_1\} \times P'_2$ by (PMust2) and $\omega \notin A_1$. For $(p_1, p'_2) \in \overline{P}$ we get $(p_1, p'_2) \notin E_P$ since $(q_1, p'_2) \notin E_Q$ and due to Lem. 13. Thus, $p_1 \parallel p_2 \xrightarrow{\omega} \overline{P}$ and therefore also $p_1 \parallel p_2 \overset{\hat{\omega}}{\Longrightarrow} \overline{P}$. For $(p_1, p'_2) \in \overline{P}$ we also have $(p_1 \parallel p'_2, q_1 \parallel p'_2) \in \mathscr{R}$.

(PMust3) $\omega = o$, $q_1 \xrightarrow{o} Q'_1$, $p_2 \xrightarrow{o} P'_2$ for some action $o \in (O_1 \cap I_2) \cup (I_1 \cap O_2)$, and $\overline{Q} = Q'_1 \times P'_2$. By $p_1 \sqsubseteq q_1$, there exists some P'_1 with $p_1 \overset{o}{\Longrightarrow} P'_1$ (possibly $p_1 \xrightarrow{o}\overset{\varepsilon}{\Longrightarrow} P'_1$, if $o \in I_1$) such that $\forall p'_1{\in}P'_1\, \exists q'_1{\in}Q'_1 .\, p'_1 \sqsubseteq q'_1$. Now, $(p_1, p_2) \overset{o}{\Longrightarrow} R \subseteq P'_1 \times P'_2$ by Lem. 14 and, as in Case (PMust1) above, all pairs along this weak transition are compatible. Hence, $p_1 \parallel p_2 \overset{o}{\Longrightarrow} R$ and, for all $p'_1 \parallel p'_2 \in R$, we have some $q' \in Q'$ such that $(p'_1 \parallel p'_2, q'_1 \parallel p'_2) \in \mathscr{R}$.

(iv) First, we consider $p_1 \parallel p_2 \overset{i}{\dashrightarrow} e_P$ due to pruning, i.e., $(p_1, p_2) \overset{i}{\dashrightarrow} (p'_1, p'_2) \in E_P$.

(PMay1) $p_1 \overset{i}{\dashrightarrow}_{P_1} p'_1$ and $p'_2 = p_2$. By $p_1 \sqsubseteq q_1$, we have $q_1 \overset{i}{\dashrightarrow} q''_1 \overset{\varepsilon}{\Longrightarrow} q'_1$ for some q'_1, q''_1 such that $p'_1 \sqsubseteq q'_1$. Hence, $(q_1, p_2) \overset{i}{\dashrightarrow} (q''_1, p_2) \overset{\varepsilon}{\Longrightarrow} (q'_1, p_2)$ by repeated application of (PMay1) and since $i \notin A_2$. By Lem. 13 we get that $(q'_1, p_2) \in E_Q$ and thus $(q''_1, p_2) \in E_Q$. Therefore, $q_1 \parallel p_2 \overset{i}{\dashrightarrow} e_Q$ by pruning.

(PMay2) $p_2 \overset{i}{\dashrightarrow} p'_2$ and $p'_1 = p_1$. Then, $(q_1, p_2) \overset{i}{\dashrightarrow} (q_1, p'_2)$ by (PMay2). By Lem. 13 we get that $(q_1, p'_2) \in E_Q$. Therefore, $q_1 \parallel p_2 \overset{i}{\dashrightarrow} e_Q$ by pruning.

(PMay3) $p_1 \overset{i}{\dashrightarrow} p'_1$ and $p_2 \overset{i}{\dashrightarrow} p'_2$ for some action $i \in I_1 \cap I_2$. Due to $p_1 \sqsubseteq q_1$, we get $q_1 \overset{i}{\dashrightarrow} q''_1 \overset{\varepsilon}{\Longrightarrow} q'_1$ for some q'_1, q''_1 such that $p'_1 \sqsubseteq q'_1$. Hence, $(q_1, p_2) \overset{i}{\dashrightarrow} (q''_1, p'_2) \overset{\varepsilon}{\Longrightarrow} (q'_1, p'_2)$ by Rules (PMay1) and (PMay3). By Lem. 13 we get that $(q'_1, p'_2) \in E_Q$, and thus $(q''_1, p'_2) \in E_Q$ as well. Therefore, $q_1 \parallel p_2 \overset{i}{\dashrightarrow} e_Q$ by pruning.

Second, we consider $p_1 \parallel p_2 \overset{i}{\dashrightarrow} p'_1 \parallel p'_2$, due to one of the Rules (PMay1), (PMay2) or (PMay3).

(PMay1) $p_1 \overset{i}{\dashrightarrow} p'_1$ and $p'_2 = p_2$. By $p_1 \sqsubseteq q_1$, we have $q_1 \overset{i}{\dashrightarrow}\overset{\varepsilon}{\Longrightarrow} q'_1$ for some q'_1 such that $p'_1 \sqsubseteq q'_1$. Hence, $(q_1, p_2) \overset{i}{\dashrightarrow}\overset{\varepsilon}{\Longrightarrow} (q'_1, p_2)$ by repeated application of (PMay1) and since $i \notin A_2$. If any state along this weak transition is in E_Q, then we get $q_1 \parallel p_2 \overset{i}{\dashrightarrow} e_Q$ and $(p'_1 \parallel p'_2, e_Q) \in \mathscr{R}$. Otherwise, $q_1 \parallel p_2 \overset{i}{\dashrightarrow}\overset{\varepsilon}{\Longrightarrow} q'_1 \parallel p_2$ with $(p'_1 \parallel p_2, q'_1 \parallel p_2) \in \mathscr{R}$.

(PMay2) $p_2 \overset{i}{\dashrightarrow} p'_2$ and $p'_1 = p_1$. Then, $(q_1, p_2) \overset{i}{\dashrightarrow} (q_1, p'_2)$ by (PMay2). If the latter state (q_1, p'_2) is in E_Q, then we get $q_1 \parallel p_2 \overset{i}{\dashrightarrow} e_Q$ and are done. Otherwise we have $(p_1 \parallel p'_2, q_1 \parallel p'_2) \in \mathscr{R}$.

(PMay3) $p_1 \overset{i}{\dashrightarrow} p'_1$ and $p_2 \overset{i}{\dashrightarrow} p'_2$ for some action $i \in I_1 \cap I_2$: Due to $p_1 \sqsubseteq q_1$, we get $q_1 \overset{i}{\dashrightarrow} q''_1 \overset{\varepsilon}{\Longrightarrow} q'_1$ for some $q'_1, q''_1 \in Q$ such that $p'_1 \sqsubseteq q'_1$. Now, we obtain $(q_1, p_2) \overset{i}{\dashrightarrow} (q''_1, p'_2) \overset{\varepsilon}{\Longrightarrow} (q'_1, p'_2)$

by (PMay1) and (PMay3). If any state along $(q_1'', p_2') \overset{\varepsilon}{\Rightarrow} (q_1', p_2')$ is in E_Q, then we get $(q_1, p_2) \overset{i}{\dashrightarrow} e_Q$ and $(p_1' \parallel p_2', e_Q) \in \mathscr{R}$. Otherwise, we again have $(p_1' \parallel p_2', q_1' \parallel p_2') \in \mathscr{R}$.

(v) Let $p_1 \parallel p_2 \overset{\omega}{\dashrightarrow} p_1' \parallel p_2'$, due to one of the Rules (PMay1), (PMay2) or (PMay3).

(PMay1) $p_1 \overset{\omega}{\dashrightarrow} p_1'$ and $p_2' = p_2$. By $p_1 \sqsubseteq q_1$, we have $q_1 \overset{\hat{\omega}}{\Rightarrow} q_1'$ for some q_1' such that $p_1' \sqsubseteq q_1'$. Hence, $(q_1, p_2) \overset{\hat{\omega}}{\Rightarrow} (q_1', p_2)$ by repeated application of (PMay1) and since $\omega \notin A_2$. If any state along this weak transition was in E_Q, then also $(q_1, p_2) \in E_Q$, which contradicts $(p_1 \parallel p_2, q_1 \parallel p_2) \in \mathscr{R}$. Thus, $q_1 \parallel p_2 \overset{\hat{\omega}}{\Rightarrow} q_1' \parallel p_2$ with $(p_1' \parallel p_2, q_1' \parallel p_2) \in \mathscr{R}$.

(PMay2) $p_2 \overset{\omega}{\dashrightarrow} p_2'$ and $p_1' = p_1$. Then, $(q_1, p_2) \overset{\omega}{\dashrightarrow} (q_1, p_2')$ by (PMay2) and due to $p_1 \sqsubseteq q_1$. If the latter state (q_1, p_2') were in E_Q, then also the former state (q_1, p_2). Thus, we have $q_1 \| p_2 \overset{\omega}{\dashrightarrow} q_1 \| p_2'$ and $(p_1 \| p_2', q_1 \| p_2') \in \mathscr{R}$.

(PMay3) $\omega = o$, $p_1 \overset{o}{\dashrightarrow} p_1'$ and $p_2 \overset{o}{\dashrightarrow} p_2'$ for some action $o \in (O_1 \cap I_2) \cup (I_1 \cap O_2)$. Due to $p_1 \sqsubseteq q_1$, we get $q_1 \overset{\varepsilon}{\Rightarrow} q_1'' \overset{o}{\dashrightarrow} q_1''' \overset{\varepsilon}{\Rightarrow} q_1'$ (or $q_1 \overset{o}{\dashrightarrow} q_1''' \overset{\varepsilon}{\Rightarrow} q_1'$ if $o \in I_1$) for some $q_1', q_1'', q_1''' \in Q$ such that $p_1' \sqsubseteq q_1'$. Now, we obtain $(q_1, p_2) \overset{\varepsilon}{\Rightarrow} (q_1'', p_2) \overset{o}{\dashrightarrow} (q_1''', p_2') \overset{\varepsilon}{\Rightarrow} (q_1', p_2')$ (or $(q_1, p_2) \overset{o}{\dashrightarrow} (q_1''', p_2') \overset{\varepsilon}{\Rightarrow} (q_1', p_2')$) by (PMay1) and (PMay3). We get $q_1 \parallel p_2 \overset{o}{\Rightarrow} q_1' \parallel p_2'$ and $(p_1' \parallel p_2', q_1' \parallel p_2') \in \mathscr{R}$, as in Case (PMay1) above. □

3.2 Hiding and Restriction

We now introduce operators for scoping actions, as is usual in process algebra. In our setting, outputs are under the control of the system; when disconnected, they are still performed but the signal is no longer sent outside, i.e., the action is internal. In contrast, inputs are only performed because of an outside stimulus. Disconnecting an input rather blocks it and, therefore, we introduce a restriction operator for inputs. The same idea is used in the IA-setting of [9] but hiding and restriction are combined in one operation.

Definition 16 (Hiding)**.** *Given a MIA $P = (P, I, O, \longrightarrow_P, \dashrightarrow_P, p_0, e)$ and a set L of actions with $L \cap I = \emptyset$, then P* hiding *L is the MIA $P/L =_{df} (P, I, O \setminus L, \longrightarrow_{P/L}, \dashrightarrow_{P/L}, p_0, e)$, where all transition labels $o \in L$ are replaced by τ.*

Definition 17 (Restriction)**.** *Given a MIA $P = (P, I, O, \longrightarrow_P, \dashrightarrow_P, p_0, e)$ and a set L of actions such that $L \cap O = \emptyset$, then* restricting *L in P yields the MIA $P \setminus L =_{df} (P, I \setminus L, O, \longrightarrow_{P \setminus L}, \dashrightarrow_{P \setminus L}, p_0, e_P)$, where all transitions with label in L are deleted.*

Regarding weak must-transitions under hiding, it is important to note that, in analogy to Lem. 3, the transition's target set in P/L might be smaller than it is in P.

Lemma 18 (Weak Must-Transitions under Hiding)**.** *Let P be a MIA, $L \cap I = \emptyset$ and $o \in L \cap O$. If $p \overset{o}{\Longrightarrow}_P P'$, then $p \overset{\varepsilon}{\Longrightarrow}_{P/L} R \subseteq P'$. In general, $R \neq P'$.*

Proof. Consider $P'' \subseteq P$ and P''' with (i) $p \overset{\varepsilon}{\Longrightarrow}_P P'' = \{p_1, \ldots, p_n\}$ and $\forall i.\, p_i \xrightarrow{o}_P P_i$ such that $P''' = \bigcup_{i=1}^{n} P_i$ and (ii) P' is obtained from P''' by repeated application of Def. 2(e) with $\omega = \tau$. In P/L, we get $p \overset{\varepsilon}{\Longrightarrow}_{P/L} P''$ by the definition of $\overset{\varepsilon}{\Longrightarrow}$ and Def. 16. Now, according to the definition of $\overset{\varepsilon}{\Longrightarrow}$, one can replace $p_1, \ldots, p_n$

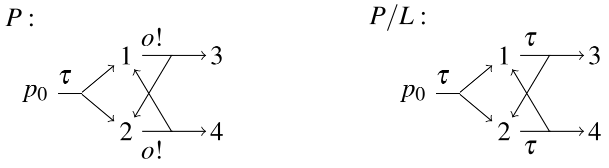

Figure 3: Example showing that set R in Lem. 18 is not always the full set P'.

in P'' one after the other by the elements of $P_1, \ldots, P_n$ such that we finally get $p \overset{\varepsilon}{\Longrightarrow}_{P/L} R'$ where $R' \subseteq P'''$. Note that R' can be a proper subset of P''', as is demonstrated by the example below.

The replacements of some $\overline{p}$ by $\overline{P}$ that transform P''' to P' can be applied to R' in P/L, as well, provided $\overline{p} \in R'$; if not, no replacement occurs. This results in R and, since the replacements preserve the inclusion, we have $p \overset{\varepsilon}{\Longrightarrow}_{P/L} R \subseteq P'$.

To see that $R \neq P'$ in general, consider Fig. 3 (see [18]), where $p_0 \overset{o}{\Longrightarrow}_P \{1,2,3,4\}$, but it is not possible to reach $\{1,2,3,4\}$ in P/L with a weak τ-must-transition. The reachable sets with maximal cardinality are $\{1,3,4\}$ and $\{2,3,4\}$. □

As desired, MIA refinement is a precongruence wrt. hiding and restriction.

Proposition 19. *Let P and Q be MIAs with $P \sqsubseteq Q$.*

1. *$P/L \sqsubseteq Q/L$ for any set L of actions with $L \cap I = \emptyset$.*
2. *$P \setminus L \sqsubseteq Q \setminus L$ for any set L of actions with $L \cap O = \emptyset$.*

Proof. Since $P \sqsubseteq Q$, there must be a MIA-refinement relation $\mathscr{R}$ with $(p,q) \in \mathscr{R}$. We show that $\mathscr{R}$ is also a MIA-refinement relation for $P/L \sqsubseteq Q/L$ and $P \setminus L \sqsubseteq Q \setminus L$.

In case of hiding, the only interesting case of Def. 4 is (iii), i.e., $q \xrightarrow{\tau}_{Q/L} Q'$ due to $q \xrightarrow{o}_Q Q'$ for some $o \in O \cap L$. The latter is matched by some transition $p \overset{o}{\Longrightarrow}_P P'$. By Lem. 18, this means $p \overset{\varepsilon}{\Longrightarrow}_{P/L} P'' \subseteq P'$. Since P' matches Q', P'' matches Q' as well. □

3.3 Parallel Composition with Hiding

We now turn our attention to parallel composition with immediate hiding on synchronised actions, enforcing binary communication. This parallel composition was used by de Alfaro and Henzinger for Interface Automata (IA) in [10, 11]. We show that the standard IA parallel composition can be expressed via our multicast parallel composition and hiding.

Definition 20 (Parallel Product and Composition with Hiding)**.** *MIAs P_1 and P_2 are* H-composable *if $O_1 \cap O_2 = \emptyset = I_1 \cap I_2$. We then define the* product with hiding *in the same way as the parallel product in Def. 7, except for $I =_{df} (I_1 \cup I_2) \setminus (O_1 \cup O_2)$ and*

(PMust3) $\quad (p_1, p_2) \xrightarrow{\tau} P_1' \times P_2' \quad$ *if* $\quad p_1 \xrightarrow{a} P_1'$ *and* $p_2 \xrightarrow{a} P_2'$ *for some a*

(PMay3) $\quad (p_1, p_2) \overset{\tau}{\dashrightarrow} (p_1', p_2') \quad$ *if* $\quad p_1 \overset{a}{\dashrightarrow} p_1'$ *and* $p_2 \overset{a}{\dashrightarrow} p_2'$ *for some a.*

From this parallel product with hiding, we get the parallel composition with hiding $P_1 \,|\, P_2$ *by the same pruning procedure as in Def. 8.*

It can easily be seen that the parallel product with hiding can be expressed by our parallel product without hiding and the hiding operator. Pruning does not change this since it treats outputs and internal actions equally.

Proposition 21. *Let P_1 and P_2 be MIAs and $S = A_1 \cap A_2$ be the set of synchronising actions. Then, $P_1 \,|\, P_2 = (P_1 \parallel P_2)/S$.*

For establishing the associativity of $|$, we first show some simple properties regarding hiding and parallel composition.

Proposition 22. *For MIAs P and Q we have the following laws, where $=$ means that the respective MIAs are identical (up to the naming of the resp. universal states in (iii)).*

(i) $P/L = P$ *if* $A_P \cap L = \emptyset$.

(ii) $P/L/L' = P/(L \cup L')$ *if* $L \cap I_P = L' \cap I_P = \emptyset$.

(iii) $(P \parallel Q)/L = (P/L) \parallel (Q/L)$ *if* $A_P \cap A_Q \cap L = \emptyset$.

Proof. Parts (i) and (ii) are straightforward. We thus focus on proving Part (iii). $P \otimes Q$ and $P/L \otimes Q/L$ are the same due to the condition $A_P \cap A_Q \cap L$, except that transition labels $o \in L$ in the former are replaced by τ in the latter; observe that (PMust3) and (PMay3) are never applicable to $o \in L$ by assumption, and the other rules work for $o \in L$ and τ in the same way. Also by assumption, the same states are considered as errors in both products. As a consequence and since pruning makes no difference between output- and τ-transitions, it deletes the same states in both systems and the same input transitions get redirected to the respective universal states of the parallel compositions. Finally, applying hiding to $P \parallel Q$ for the first system makes the MIAs identical. □

Associativity is a natural property of parallel composition, so one would expect that $(P \,|\, Q) \,|\, R = P \,|\, (Q \,|\, R)$ for some suitable equivalence = (e.g., equality up to isomorphism) provided that one side is defined. This law looks much less natural if we rewrite it according to Prop. 21; it is wrong in the version of $|$ in [10]. Here, associativity can be proved from Thm. 12 and Prop. 22:

Proposition 23. *Parallel composition with hiding is associative in the sense, that for pairwise H-composable MIAs P, Q and R, if $(P \,|\, Q) \,|\, R$ is defined, then $P \,|\, (Q \,|\, R)$ is defined as well and both are isomorphic, and vice versa.*

Proof. Let P, Q, R be pairwise H-composable MIAs. We use S_{PQ}, A_{PQ} etc. as above and let $S_{PQR} = S_{PQ} \cup S_{PR} \cup S_{QR}$. Note that $(*)$ $S_{PQ} \cap A_R = \emptyset$ since, otherwise A_R would contain an action that is an input in one of P and Q and an output in the other, contradicting H-composability of R with one of the other MIAs. Furthermore, $(**)$ $S_{PQ} \cup (A_{PQ} \cap A_R) = S_{PQ} \cup (((A_P \cup A_Q)/S_{PQ}) \cap A_R) \overset{(*)}{=} S_{PQ} \cup (((A_P \cup A_Q) \cap A_R)/S_{PQ}) = S_{PQ} \cup ((A_P \cup A_Q) \cap A_R) = S_{PQ} \cup (A_P \cap A_R) \cup (A_Q \cap A_R) = S_{PQR}$. We now obtain:

$$\begin{aligned}
(P \,|\, Q) \,|\, R &= ((P \parallel Q)/S_{PQ} \parallel R)/(A_{PQ} \cap A_R) && \text{(Prop. 21)}\\
&= ((P \parallel Q)/S_{PQ} \parallel R/S_{PQ})/(A_{PQ} \cap A_R) && \text{(Prop. 22.(i) and } (*))\\
&= ((P \parallel Q) \parallel R)/S_{PQ}/(A_{PQ} \cap A_R) && \text{(Prop. 22.(iii) and } (*))\\
&= ((P \parallel Q) \parallel R)/S_{PQR} && \text{(Prop. 22.(ii) and } (**))\\
&= (P \parallel (Q \parallel R))/S_{PQR} && \text{(Thm. 12)}\\
&= P \,|\, (Q \,|\, R) && \text{(by symmetric arguments)} \quad \square
\end{aligned}$$

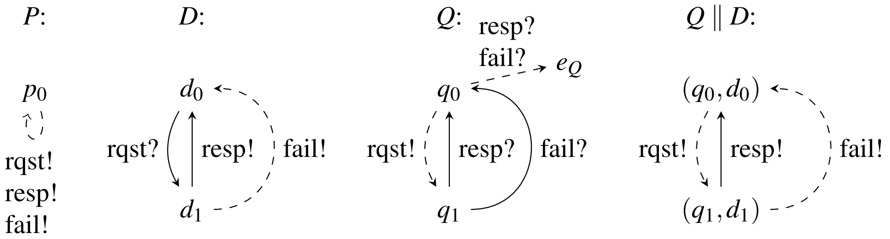

Figure 4: $Q = P /\!/ D$ with $q_0 = p_0 /\!/ d_0$ and $q_1 = p_0 /\!/ d_1$, where the alphabets are $A_P = \emptyset/\{\text{rqst, resp, fail}\}$, $A_D = \{\text{rqst}\}/\{\text{resp, fail}\}$, $A_Q = \{\text{resp, fail}\}/\{\text{rqst}\}$ and $A_{Q\parallel D} = \emptyset/\{\text{rqst, resp, fail}\}$.

4 Quotienting

The quotient operation is a kind of inverse or adjoined operation to parallel composition. It equips the theory with a means for component reuse and incremental, component-based specification. To describe the participants in a quotient operation we use the letters P for the specification, D for the divisor (the already implemented component) and Q for the quotient or its refinements. Given MIAs P and D, the quotient is the coarsest MIA Q such that $Q \parallel D \sqsubseteq P$ holds; we call this inequality the *defining inequality of the quotient*. We write $P /\!/ D$ for the quotient if it exists.

We demonstrate quotienting with the simple client-server application of Fig. 4. The server takes the role of the already given component D. It can receive a request and answers with a response. Additionally, the server may implement a failure as answer. When composed in parallel, client Q and server D are supposed to form a *closed* system, i.e., all shared actions are outputs. Thus, the parallel composition of client and server must refine the overall specification P. A specification for the client is then obtained as the quotient $Q = P /\!/ D$. Figure 4 gives a preview of this Q according to our construction below. Client Q may implement the sending of a request, and if so, it must be receptive for a response and a failure. If one of the latter two transitions were of may-modality, this would cause a communication mismatch in the parallel composition with D. The may-transitions resp? and fail! from q_0 to e_Q only exist to make Q as coarse as possible; they disappear in the parallel composition with D. Now, it is easy to check that the defining inequality $Q \parallel D \sqsubseteq P$ is satisfied. The example also shows that, in general, we do not have equality of $(P /\!/ D) \parallel D$ and P.

We define the quotient for a restricted set of MIAs, namely where the specification P has no τs and where the divisor D is may-deterministic and without τs. We call D *may-deterministic* if $d \overset{\alpha}{\dashrightarrow} d'$ and $d \overset{\alpha}{\dashrightarrow} d''$ implies $d' = d''$. Due to syntactic consistency, a may-deterministic MIA has no disjunctive must-transitions, i.e., the target sets of must-transitions are singletons. In addition, we exclude the pathological case where P has some state p and input i with $p \overset{i}{\dashrightarrow} e_P$ and $\exists p' \neq e_P .\, p \overset{i}{\dashrightarrow} p'$. Recall that transitions $p \overset{i}{\dashrightarrow} e_P$ are meant to express the following situation: (a) input i is not specified at p, but at the same time (b) p shall be refinable as in Interface Automata [11] by a state with an i-transition and arbitrary subsequent behaviour.

Despite these restrictions, our quotient significantly generalises that of Modal Interfaces [22], which considered deterministic specifications and deterministic divisors only. In the following, we call MIAs P and D satisfying our restrictions a *quotient pair*.

4.1 Definition and Main Result

Like most other operators we define the quotient in two stages, where $\text{may}_P(p,\alpha)$ stands for $\{p' \in P \mid p \overset{\alpha}{\dashrightarrow}_P p'\}$.

Definition 24 (Pseudo-Quotient)**.** *Let $(P, I_P, O_P, \longrightarrow_P, \dashrightarrow_P, p_0, e_P)$, $(D, I_D, O_D, \longrightarrow_D, \dashrightarrow_D, d_0, e_D)$ be a quotient pair with $A_D \subseteq A_P$ and $O_D \subseteq O_P$, and $I =_{df} I_P \cup O_D$ and $O =_{df} O_P \setminus O_D$. The* pseudo-quotient of P over D *is defined as the universal MIA $(\{(e_P, e_D)\}, I, O, \emptyset, \emptyset, (e_P, e_D), (e_P, e_D))$ if $p_0 = e_P$. Otherwise, $P \oslash D =_{df} (P \times D, I, O, \longrightarrow, \dashrightarrow, (p_0, d_0), (e_P, e_D))$, where the transition relations are defined by the following rules:*

$$
\begin{array}{llll}
\text{(QMust1)} & (p,d) \xrightarrow{a} P' \times \{d\} & \textit{if} & p \xrightarrow{a}_P P' \textit{ and } a \notin A_D \\
\text{(QMust2)} & (p,d) \xrightarrow{a} P' \times \{d'\} & \textit{if} & p \xrightarrow{a}_P P' \textit{ and } d \xrightarrow{a}_D d' \\
\text{(QMust3)} & (p,d) \xrightarrow{a} P' \times \{d'\} & \textit{if} & P' =_{df} \mathrm{may}_P(p,a) \neq \emptyset,\ e_P \notin P', \\
 & & & d \overset{a}{\dashrightarrow}_D d' \textit{ and } a \in O_D \\
\text{(QMay1)} & (p,d) \overset{a}{\dashrightarrow} (p',d) & \textit{if} & p \overset{a}{\dashrightarrow}_P p' \neq e_P \textit{ and } a \notin A_D \\
\text{(QMay2)} & (p,d) \overset{a}{\dashrightarrow} (p',d') & \textit{if} & p \overset{a}{\dashrightarrow}_P p' \neq e_P \textit{ and } d \xrightarrow{a}_D d' \\
\text{(QMay3)} & (p,d) \overset{a}{\dashrightarrow} (p',d') & \textit{if} & p \overset{a}{\dashrightarrow}_P p',\ e_P \notin \mathrm{may}_P(p,a), \\
 & & & d \overset{a}{\dashrightarrow}_D d' \textit{ and } a \notin O_P \cap I_D \\
\text{(QMay4)} & (p,d) \overset{a}{\dashrightarrow} (e_P,e_D) & \textit{if} & e_P \in \mathrm{may}_P(p,a) \quad \textit{(note: } a \in I_P \subseteq I\textit{)} \\
\text{(QMay5)} & (p,d) \overset{a}{\dashrightarrow} (e_P,e_D) & \textit{if} & p \neq e_P,\ d \overset{a}{\not\dashrightarrow}_D \textit{ and } a \in A_D \setminus (O_P \cap I_D) \\
 & & & \textit{(note: } A_D \setminus (O_P \cap I_D) = I \cap A_D\textit{)}
\end{array}
$$

Regarding the definition of the input and output alphabets we follow Chilton et al. [8] and Raclet et al. [22]; there is, however, a choice regarding the input alphabet, which we discuss in Sec. 4.2. The intuition behind a state (p,d) in $P \oslash D$ is that (p,d) composed in parallel with d refines state p, and that (p,d) should be coarsest wrt. MIA refinement satisfying this condition. With this in mind, we now justify the above rules intuitively. A formal proof is given in Lem. 26 and Thm. 27 below.

Rule (QMust1) is necessary due to the following consideration. If P has an a-must-transition where a is unknown to D, this can only originate from an a-must-transition in the quotient Q that we wish to construct; in order to be most permissive, each $p' \in P'$ must have a match in $Q \parallel D$. The corresponding consideration is true for Rule (QMay1), which also establishes syntactic consistency for Rule (QMust1).

Rule (QMust2) is obvious in the light of the choice of alphabet in Def. 24. As $P \oslash D$ has all actions of P and D in its alphabet, it also needs an a-must-transition to produce such a transition at $(p,d) \parallel d$. Here, Rule (QMay2) is the companion rule for guaranteeing syntactic consistency.

Rule (QMust3) ensures that (p,d) and d are compatible in case of an output of d. An application of this rule can be seen in Fig. 4 for action fail? at $q_1 = p_0 /\!/ d_1$. Syntactic consistency results from Rules (QMay2) and (QMay3); note that $a \in O_D$ implies $a \notin I_D$.

Observe how Rules (QMay2) and (QMay3) play together well. By the condition $a \notin O_P \cap I_D = O \cap I_D$, Rule (QMay3) does not generate an output a-may-transition in the pseudo-quotient that could make (p,d) and d illegal. These transitions are added by Rule (QMay2) if the a-transition at d is of must-modality and compatibility is ensured. This is exactly the situation in Fig. 4 for action rqst! at $q_0 = p_0 /\!/ d_0$.

Rule (QMay4) deals with the universal state in P. Obviously, $e_{P \oslash D}$ is the most general state of $P \oslash D$ that refines e_P in parallel composition with d. Implicitly, this rule replaces all states (e_P, d) by $e_{P \oslash D}$.

Rule (QMay5) makes $P \oslash D$ as coarse as possible. The input a-may-transitions introduced here just disappear in $(P \oslash D) \parallel D$, since a is blocked by D. This can be seen in Fig. 4 for actions resp? and fail? at $q_0 = p_0 /\!/ d_0$ and in $Q \parallel D$ at (q_0, d_0).

$P \oslash D$ is indeed a MIA. We have already argued for syntactic consistency. All rules ensure $p \neq e_P$; hence, $e_{P \oslash D}$ has no outgoing transitions. Incoming transitions of $e_{P \oslash D}$ can only arise from Rules (QMay4) or (QMay5), which are only applicable for $a \in I$.

Up to now, we have only defined the pseudo-quotient. Considering a candidate pair (p,d), for some combinations of modalities and assignments of actions to input or output, it is impossible that p is refined by a state resulting from a parallel composition with d. We call such states *impossible states* and remove them from the pseudo-quotient states. For example, consider states $p \xrightarrow{a}$ and $d \overset{a}{\dashrightarrow}$ such that $d \not\xrightarrow{a}$; no parallel composition with d refines p. While may-transitions can be refined by removing them and disjunctive transitions can be refined to subsets of their targets to prevent the reachability of impossible states, all states having a must-transition to only impossible states must also be removed. This pruning results in the quotient.

Definition 25 (Quotient)**.** *Let $P \oslash D$ be the pseudo-quotient of P over D. The set $G \subseteq P \times D$ of* impossible states *is defined as the least set refining the following rules:*

$$\begin{array}{lll@{\quad}l}
\text{(G1)} & p \xrightarrow{a}_P \textit{ and } d \not\xrightarrow{a}_D \textit{ and } a \in A_D & \textit{implies} & (p,d) \in G \\
\text{(G2)} & p \neq e_P \textit{ and } p \overset{a}{\not\dashrightarrow}_P \textit{ and } d \overset{a}{\dashrightarrow}_D \textit{ and } a \in O_D & \textit{implies} & (p,d) \in G \\
\text{(G3)} & p \neq e_P \textit{ and } d = e_D & \textit{implies} & (p,d) \in G \\
\text{(G4)} & (p,d) \xrightarrow{a}_{P \oslash D} R' \textit{ and } R' \subseteq G & \textit{implies} & (p,d) \in G
\end{array}$$

The quotient *$P//D$ is obtained from $P \oslash D$ by deleting all states $(p,q) \in G$. This also removes any may- or must-transition exiting and any may-transition entering a deleted state. Deleted states are also removed from targets of disjunctive must-transitions. If $(p,d) \in P//D$, then we write $p//d$. If $(p_0,d_0) \notin P//D$, then the quotient P over D is not defined.*

Rule (G1) is obvious since (p,d) cannot ensure that $p \xrightarrow{a}_P$ is matched if d has no a-must-transition, as an a-may-transition or even a forbidden action at d can in no case compose to a refinement of a must-transition at p. Rule (G2) captures the situation where d has an output a that is forbidden at p. Offering an a-must-input in the quotient would lead to a transition in the parallel composition with d, while not offering it would lead to an error; both would not refine p. Rule (G3) captures the division by e_D: state e_D in parallel with any state is universal and does not refine $p \neq e_P$. Finally, Rule (G4) propagates back all impossibilities that cannot be avoided by refining.

Observe that $P//D$ (i.e., the quotient is defined) is a MIA. Syntactic consistency and the universal state are preserved by pruning; in this case Rule (G4) is not applicable since $P \oslash D$ is a MIA. If the target set of a disjunctive must-transition became empty, it would be deleted. We show that the quotient operation above yields the coarsest MIA satisfying the defining inequality. For this proof, the next lemma ensures that the definedness of $\|$ and $//$ is mutually preserved across refinement.

Lemma 26. *Let P, D and Q be MIAs such that P and D is a quotient pair, $A_D \subseteq A_P$, $O_D \subseteq O_P$, $O_Q = O_P \setminus O_D$ and $I_Q = I_P \cup O_D$. Further, let p, d, q, be states in P, D, Q, resp. Then, the following statements hold:*

1. *If $q \parallel d \sqsubseteq p$, then $p//d$ is defined.*
2. *If $q \sqsubseteq p//d$ and $p \neq e_P$, then $q \parallel d$ is defined.*

Proof. We write $\longrightarrow_\otimes$, $\longrightarrow_\|$, $\longrightarrow_\oslash$ and $\longrightarrow_{//}$ as a shorthand for $\longrightarrow_{Q\otimes D}$, $\longrightarrow_{Q\|D}$, $\longrightarrow_{P\oslash D}$ and $\longrightarrow_{P//D}$, resp., and analogously for may-transitions. We show both claims by contraposition.

Claim 1: For all $(p,d) \in G$, the refinement $q \parallel d \sqsubseteq p$ does not hold for any $q \in Q$, possibly because $q \parallel d$ is not defined, i.e., $(q,d) \in E$ according to Def. 8. We prove this by induction on the derivation length according to the G-rules. In each case, we assume $q \parallel d \sqsubseteq p$ for some $q \in Q$ and derive a contradiction.

(G1) $p \xrightarrow{a}$, $d \not\xrightarrow{a}$ and $a \in A_D$: By $q \parallel d \sqsubseteq p$, we have $q \parallel d \xrightarrow{a}_\|$, which can only be due to (PMust2) or (PMust3); thus, $d \xrightarrow{a}$, which is a contradiction.

(G2) $p \neq e_P$, $p \overset{a}{\not\dashrightarrow}$, $d \overset{a}{\dashrightarrow}$ and $a \in O_D$: By $q \parallel d \sqsubseteq p$, we have $q \parallel d \overset{a}{\not\dashrightarrow}_{\parallel}$. Now, either $(q,d) \overset{a}{\dashrightarrow}_{\otimes}$ reaching an illegal state or $q \overset{a}{\not\dashrightarrow}$; in either case, $(q,d) \in E$, which is a contradiction.

(G3) $p \neq e_P$ and $d = e_D$: Here, $(q,d) \in E$ is an inherited error, which is a contradiction.

(G4) $(p,d) \xrightarrow{a}_{\oslash} R'$ with $R' \subseteq G$: Our claim holds for all $(p',d') \in R'$ by induction hypothesis, and the transition is due to one of the (QMust) rules:

(QMust1) $p \xrightarrow{a} P'$, $a \notin A_D$ and $R' = P' \times \{d\}$: By $q \parallel d \sqsubseteq p$, we have $q \parallel d \xrightarrow{a}_{\parallel} Q' \times \{d\}$ such that $\forall q' {\in} Q' \, \exists p' {\in} P'. \, q' \parallel d \sqsubseteq p'$. This is a contradiction, since $(p',d) \in R'$.

(QMust2) $p \xrightarrow{a} P'$, $d \xrightarrow{a} d'$ and $R' = P' \times \{d'\}$: $q \parallel d \sqsubseteq p$ implies the existence of a Q' with $q \xrightarrow{a} Q'$ and $\forall q' {\in} Q' \, \exists p' {\in} P'. \, q' \parallel d' \sqsubseteq p'$. This is again a contradiction since $(p',d') \in R'$.

(QMust3) $e_P \notin \mathrm{may}_P(p,a) \neq \emptyset$, $R' = \mathrm{may}_P(p,a) \times \{d'\}$, $d \overset{a}{\dashrightarrow} d'$ and $a \in O_D$: Since $q \parallel d$ is defined, we have some $q \xrightarrow{a} Q'$; otherwise, we would have $(q,d) \in E$. Thus, by definition of illegal states, also $q' \parallel d'$ must be defined for some (and in fact all) $q' \in Q'$. Now, $q \parallel d \overset{a}{\dashrightarrow}_{\parallel} q' \parallel d'$ must be matched by some $p \overset{a}{\dashrightarrow} p'$ due to $q \parallel d \sqsubseteq p$, and we have $q' \parallel d' \sqsubseteq p'$. This is again a contradiction since $(p',d') \in R'$.

Claim 2: For all $(q,d) \in E$, $q \sqsubseteq p/\!/d$ does not hold for any $p \in P$ with $p \neq e_P$, possibly because $p/\!/d$ is not defined. We prove this by induction on the length of a local path from (q,d) to an error in $Q \otimes D$; here, all actions on the path are outputs. In each case, we assume $q \sqsubseteq p/\!/d$ for some $p \in P$ with $p \neq e_P$ and derive a contradiction.

(Base) Let (q,d) be an error according to Def. 8.

(a) $q \overset{a}{\dashrightarrow} q'$, $d \not\xrightarrow{a}$ and $a \in O_Q \cap I_D$: Here, $q \sqsubseteq p/\!/d$ implies a transition $(p,d) \overset{a}{\dashrightarrow}_{\oslash} (p',d')$. But, such a transition cannot exist since none of the (QMay) rules applies; note that $a \in O_P \cap I_D$ for (QMay3) and (QMay5) and that $e_P \in \mathrm{may}_P(p,a)$ implies $a \in I_P$, which contradicts $a \in O_Q$, for (QMay4).

(b) $q \not\xrightarrow{a}$, $d \overset{a}{\dashrightarrow} d'$ and $a \in I_Q \cap O_D$: As just noted, $a \in O_P$ implies $e_P \notin \mathrm{may}_P(p,a)$. Since (G2) does not apply, we have $\mathrm{may}_P(p,a) \neq \emptyset$. Thus, we get $p/\!/d \xrightarrow{a}_{/\!/}$ by (QMust3), contradicting $q \sqsubseteq p/\!/d$ and $q \not\xrightarrow{a}$.

(c) (q,d) is an inherited error: If $q = e_Q$, then $p/\!/d = e_{P/\!/D}$ by $q \sqsubseteq p/\!/d$, and we have $p = e_P$. If $d = e_D$, then Rule (G3) and the definedness of $p/\!/d$ imply $p = e_P$. Both cases contradict $p \neq e_P$.

(Step) Assume $(q,d) \overset{a}{\dashrightarrow}_{\otimes} (q',d') \in E$ with $a \in O_{Q \otimes D}$ such that our claim holds for (q',d') by induction. We consider the different rules that resulted in this transition.

(PMay1) $a \notin A_D$, $d' = d$ and $q \overset{a}{\dashrightarrow} q'$: By $q \sqsubseteq p/\!/d$, there is a transition $p/\!/d \overset{a}{\dashrightarrow}_{/\!/} p'/\!/d''$ such that $q' \sqsubseteq p'/\!/d''$. The only applicable Rule (QMay1) (note that $a \in O_P$) implies $d'' = d$ and $p' \neq e_P$. Thus, we have $q' \sqsubseteq p'/\!/d$, contradicting the claim for (q',d').

(PMay2) $a \notin A_Q$, $q' = q$ and $d \overset{a}{\dashrightarrow} d'$: We have $a \in A_D \subseteq A_P = A_{P \oslash D} = A_Q$, which is a contradiction.

(PMay3) $q \overset{a}{\dashrightarrow} q'$ and $d \overset{a}{\dashrightarrow} d'$: By $q \sqsubseteq p/\!/d$, there is a transition $p/\!/d \overset{a}{\dashrightarrow}_{/\!/} p'/\!/d''$ such that $q' \sqsubseteq p'/\!/d''$. The only rules that are applicable are (QMay2) and (QMay3) (note that $a \in O_P$) both imply $d'' = d'$ and $p' \neq e_P$. Thus, we have $q' \sqsubseteq p'/\!/d'$, contradicting the claim for (q',d'). □

Theorem 27 ($/\!/$ is a Quotient Operator wrt. $\|$). *Let P and D be a quotient pair and Q be a MIA such that $A_D \subseteq A_P$, $O_D \subseteq O_P$, $O_Q = O_P \setminus O_D$ and $I_Q = I_P \cup O_D$. Then, $Q \sqsubseteq P/\!/D$ iff $Q \parallel D \sqsubseteq P$.*

Proof. We use the same shorthands as in Lem. 26. If $p_0 = e_P$, then $p_0/\!/d_0 = e_{P/\!/D}$ and both sides of the theorem's statement are simply true. For $p_0 \neq e_P$ we have: If $P/\!/D$ is defined, then also $p_0/\!/d_0$ and, by Lem. 26, $q_0 \parallel d_0$ is defined. If $Q \parallel D \sqsubseteq P$, then the initial state of $Q \parallel D$ is $q_0 \parallel d_0 \neq e_{Q\|D}$ because of $p_0 \neq e_P$; with $q_0 \parallel d_0$ also $p_0/\!/d_0$ is defined by Lem. 26. Therefore, it suffices to establish the refinements.

"$\Rightarrow$": We show that $\mathscr{R} =_{\mathrm{df}} \{(q\|d, p) \in (Q\|D) \times P \mid q \sqsubseteq p/\!/d \text{ or } p = e_P\} \dot\cup \{(e_{Q\|D}, e_P)\}$ is a MIA-refinement relation. We only have to consider a $(q\|d, p) \in \mathscr{R}$ with $p \neq e_P$. Note that Cases (iii) and (v) are mostly analogous to Cases (ii) and (iv), resp.

(i) From $p \neq e_P$ we conclude, by $q \sqsubseteq p/\!/d$ and Lem. 26, that $q \parallel d$ exists, i.e., it is not the universal state.

(ii) $p \overset{i}{\longrightarrow} P'$ for $i \in I_P$:

1. If $i \in A_D$ and $d \overset{i}{\longrightarrow} d'$, then (QMust2) implies $(p,d) \overset{i}{\longrightarrow}_{\oslash} P' \times \{d'\}$. In $P/\!/D$, the target set might only be a subset $P'' \times \{d'\}$ of $P' \times \{d'\}$. By $q \sqsubseteq p/\!/d$, we have $q \overset{i}{\longrightarrow} Q'$ for some Q' such that $\forall q'{\in}Q'\, \exists p'{\in}P''.\, q' \sqsubseteq p'/\!/d'$, whence $(q'\|d', p') \in \mathscr{R}$; note that $p' \neq e_P$ since, otherwise, $e_P \in P'$. Now, by (PMust3) there is a transition $(q,d) \overset{i}{\longrightarrow}_{\otimes} Q' \times \{d'\}$. Since for all $(q',d') \in Q' \times \{d'\}$ there is some $p' \in P''$ with $q' \sqsubseteq p'/\!/d'$, we also have $q \parallel d \overset{i}{\longrightarrow}_{\|} Q' \times \{d'\}$ by Lem. 26.

   To see the latter, note that it is impossible that $(q,d) \overset{i}{\dashrightarrow}_{\oslash} (\overline{q}, d') \in E$, for some $\overline{q} \in D'$. This is because of the following reasons. If $(q,d) \overset{i}{\dashrightarrow}_{\oslash} (\overline{q}, d') \in E$, then $q \overset{i}{\dashrightarrow} \overline{q}$ by $I_P \subseteq I_Q$. Since $q \sqsubseteq p/\!/d$, we have $p/\!/d \overset{i}{\dashrightarrow}_{/\!/} \overline{p}/\!/\overline{d}$ for some $\overline{p}$ with $\overline{q} \sqsubseteq \overline{p}/\!/\overline{d}$, which can only be due to (QMay2). Observe that (QMay4) is excluded by P and D being a quotient pair, and that (QMay5) is excluded due to $i \in I_P$. In the remaining case (QMay2) we have $p \overset{i}{\dashrightarrow} \overline{p} \neq e_P$ and $\overline{d} = d'$; further, Lem. 26 implies $(\overline{q}, d') \notin E$.
2. If $i \in A_D$ and $d \overset{i}{\not\longrightarrow}$, then $(p,d) \in G$ by (G1), which is impossible since $p/\!/d$ is defined.
3. If $i \notin A_D$, the proof is analogous to Case 1 with $d = d'$, when replacing (QMust2) by (QMust1) and (PMust3) by (PMust1).

(iii) $p \overset{o}{\longrightarrow} P'$ for $o \in O_P$: Here, the same arguments as for (ii) apply.

(iv) $q \parallel d \overset{i}{\dashrightarrow}_{\|}$ and $i \in I_P$: Consider (a) $q \parallel d \overset{i}{\dashrightarrow}_{\|} q' \parallel d'$ or (b) $q \parallel d \overset{i}{\dashrightarrow}_{\|} e_{Q\|D}$ for $i \in I_{Q\|D}$. In both cases $(q,d) \overset{i}{\dashrightarrow}_{\otimes} (q',d')$ by one of (PMay1) or (PMay3) and $(q',d') \in E$ in case of (b). Rule (PMay2) is impossible as $A_Q = A_P \supseteq A_D$.

(PMay1) $q \overset{i}{\dashrightarrow} q'$ and $i \notin A_D$: We have $d = d'$, and $q \sqsubseteq p/\!/d$ implies $p/\!/d \overset{i}{\dashrightarrow}_{/\!/} p'/\!/d''$ for some p', d'' such that $q' \sqsubseteq p'/\!/d''$. Since $i \notin A_D$, we get either $d = d''$ and $p \overset{i}{\dashrightarrow} p' \neq e_P$ by (QMay1), or $p \overset{i}{\dashrightarrow} p' = e_P$ by (QMay4). In the latter case, we have $(q'\|d', e_P) \in \mathscr{R}$ for Case (a) and $(e_{Q\|D}, e_P) \in \mathscr{R}$ for Case (b). In the former case (QMay1), we have $(q'\| d', p') \in \mathscr{R}$ for Case (a) since $q' \sqsubseteq p'/\!/d'$. Case (b) is impossible because $q' \parallel d' \notin E$ by Lem. 26, $q' \sqsubseteq p'/\!/d'$ and $p' \neq e_P$.

(PMay3) $q \overset{i}{\dashrightarrow} q'$ and $d \overset{i}{\dashrightarrow} d'$: As $q \sqsubseteq p/\!/d$ we conclude $p/\!/d \overset{i}{\dashrightarrow}_{/\!/} p'/\!/d''$ for some p', d'' with $q' \sqsubseteq p'/\!/d''$. This can be due to (QMay2), (QMay3) or (QMay4); in all cases we have $p \overset{i}{\dashrightarrow} p'$. In case (QMay4), we have $p' = e_P$ and $(q' \| d', e_P) \in \mathscr{R}$ for Case (a) and $(e_{Q\|D}, e_P) \in \mathscr{R}$ for Case (b). In the other cases, we have $d'' = d'$ by may-determinism and $p' \neq e_P$; the proof now concludes like case (QMay1) above.

(v) $q \parallel d \overset{o}{\dashrightarrow}_{\|}$ and $a \in O_P$: This case is already covered by (iv)(a).

"$\Leftarrow$": We show that $\mathscr{R} =_{\text{df}} \{(q, p/\!/d) \in Q \times (P/\!/D) \mid q \parallel d \sqsubseteq p \text{ or } p/\!/d = e_{P/\!/D}\}$ is a MIA-refinement relation. It suffices to consider some $(q, p/\!/d) \in \mathscr{R}$ with $p/\!/d \neq e_P/\!/e_D$. In the following, the arguments for (iii) are analogous to those for (ii).

(i) Since $(q,d) \notin E$, we have $q \neq e_Q$.

(ii) $p/\!/d \xrightarrow{i}_{/\!/} R' \subseteq P' \times \{d'\}$ for $i \in I_{P/\!/D}$, where $(p,d) \xrightarrow{i}_{\oslash} P' \times \{d'\}$ is due to one of the (QMust) rules, and R' consists of the possible states of $P' \times \{d'\}$. In the following, we use $A_P = A_Q$ throughout.

(QMust1) $p \xrightarrow{i} P'$, $d = d'$ and $i \notin A_D$: By $q \parallel d \sqsubseteq p$ we get $q \parallel d \xrightarrow{i}_{\|} Q' \times \{d''\}$ for some Q', d'' with $\forall q' {\in} Q' \, \exists p' {\in} P'. \, q' \parallel d'' \sqsubseteq p'$. Since $i \notin A_D$, this transition can only be due to Rule (PMust1) and $d'' = d$. By Lem. 26, $q' \parallel d \sqsubseteq p'$ implies that $p'/\!/d$ is not impossible, hence $p'/\!/d \in R'$. Thus, we are done due to $q \xrightarrow{i} Q'$.

(QMust2) $p \xrightarrow{i} P'$ and $d \xrightarrow{i} d'$: By $q \parallel d \sqsubseteq p$, we get $q \parallel d \xrightarrow{i}_{\|} Q' \times \{d'\}$ for some Q' such that $\forall q' {\in} Q' \, \exists p' {\in} P'. \, q' \parallel d' \sqsubseteq p'$. The transition must result from (PMust3). Thus, we are done as in (QMust1).

(QMust3) $P' = \text{may}_P(p,a)$ and $d \overset{i}{\dashrightarrow} d'$ with $i \in O_D$: Since $i \in I_Q \cap O_D$ and $q \parallel d$ is defined, we have $q \xrightarrow{i} Q'$ for some Q'. Now, Rule (PMay3) gives us $(q,d) \overset{i}{\dashrightarrow}_{\otimes} (q',d')$ for all $q' \in Q'$. Since $i \in O_{Q \otimes D}$ and $(q,d) \notin E$, we also know that $(q',d') \notin E$, hence $q \parallel d \overset{i}{\dashrightarrow}_{\|} q' \parallel d'$. By $q \parallel d \sqsubseteq p$ we have $\forall q' \in Q' \exists p' \in P'. \, p \overset{i}{\dashrightarrow} p'$ and $q' \parallel d' \sqsubseteq p'$. As above, $p'/\!/d' \in R'$ and $q \xrightarrow{i} Q'$ matches $p/\!/d \xrightarrow{i}_{/\!/} R'$.

(iii) $p/\!/d \xrightarrow{o}_{/\!/} R'$ with $o \in O_{P/\!/D} = O_P \setminus O_D$: The same arguments as for (ii) apply, except that Rule (QMust3) is not applicable due to $o \notin O_D$.

(iv) $q \overset{i}{\dashrightarrow} q'$ for $i \in I_Q$:

1. $i \notin A_D$: By (PMay1) we have $(q,d) \overset{i}{\dashrightarrow}_{\otimes} (q',d)$. Thus, either $q \parallel d \overset{i}{\dashrightarrow}_{\|} e_{Q\|D}$ or $q \parallel d \overset{i}{\dashrightarrow}_{\|} q' \parallel d$. In the first case we get $p \overset{i}{\dashrightarrow} e_P$, because of $q \parallel d \sqsubseteq p$, and $(p,d) \overset{i}{\dashrightarrow}_{\oslash} (e_P, e_D)$ by (QMay4). Since (e_P, e_D) can never be impossible, we have $p/\!/d \overset{i}{\dashrightarrow}_{/\!/} e_P/\!/e_D$ and are done. For the second case, $q \parallel d \overset{i}{\dashrightarrow}_{\|} q' \parallel d$, we get $p \overset{i}{\dashrightarrow} p'$ for some p' with $q' \parallel d \sqsubseteq p'$, because of $q \parallel d \sqsubseteq p$. If $p \overset{i}{\dashrightarrow} e_P$, we are done as above. Otherwise, we get $(p,d) \overset{i}{\dashrightarrow}_{\oslash} (p',d)$ by (QMay1). Lem. 26 implies the definedness of $p'/\!/d$, hence $p/\!/d \overset{i}{\dashrightarrow}_{/\!/} p'/\!/d$, and we are done.

2. $i \in A_D$ and $d \overset{i}{\not\dashrightarrow}$: Since $p \neq e_P$ and $i \in A_D \setminus O_Q = A_D \setminus (O_P \cap I_D)$, we get $(p,d) \overset{i}{\dashrightarrow}_{\oslash} (e_P, e_D)$ by (QMay5). Since (e_P, e_D) can never be impossible, we have $p /\!/ d \overset{i}{\dashrightarrow}_{/\!/} e_P /\!/ e_D$ and are done.
3. $i \in A_D$ and $d \overset{i}{\dashrightarrow} d'$: By (PMay3), there is a transition $(q,d) \overset{i}{\dashrightarrow}_{\otimes} (q', d')$. Thus, either $q \parallel d \overset{i}{\dashrightarrow}_{\parallel} e_{Q\parallel D}$ (only possible, if $i \in I_D$) or $q \parallel d \overset{i}{\dashrightarrow}_{\parallel} q' \parallel d'$ (ensured, if $i \in O_D$, since $q \parallel d$ defined). The first case is as in (iv).1 and so is the second case, except for (QMay3) instead of (QMay1); for this, note that $i \in I_D$ implies $i \notin O_P$ by $i \in I_Q$.

(v) $q \overset{o}{\dashrightarrow} q'$ for $o \in O_Q$:

1. $o \in A_D$: We have $d \xrightarrow{o} d'$ for some d'; otherwise, $q \parallel d$ would not exist. By (PMay3), we have $(q,d) \overset{o}{\dashrightarrow}_{\otimes} (q', d')$, and hence $q \parallel d \overset{o}{\dashrightarrow}_{\parallel} q' \parallel d'$ by definedness of $q \parallel d$. By $q \parallel d \sqsubseteq p$, we have $p \overset{o}{\dashrightarrow} p'$ for some p' with $q' \parallel d' \sqsubseteq p'$. Since $o \in O_P$, we have $p' \neq e_P$, and we can apply (QMay2) to get $(p,d) \overset{o}{\dashrightarrow}_{\oslash} (p', d')$. Lem. 26 implies the definedness of $p' /\!/ d$, hence $p /\!/ d \overset{o}{\dashrightarrow}_{/\!/} p' /\!/ d'$ and we are done.
2. $o \notin A_D$: $q \parallel d \overset{o}{\dashrightarrow}_{\parallel} q' \parallel d$ by (PMay1) and definedness of $q \parallel d$; hence, due to $q \parallel d \sqsubseteq p$, there is a $p \overset{o}{\dashrightarrow} p'$ for some p' with $q' \parallel d \sqsubseteq p'$. Now we are done as in (v).1, applying (QMay1) instead of (QMay2). □

From this theorem, we can also conclude that $/\!/$ is monotonous wrt. $\sqsubseteq$ in the specification argument.

Theorem 28 (Monotonicity of $/\!/$ wrt. $\sqsubseteq$)**.** *Let P_1, P_2, D be MIAs with $P_1 \sqsubseteq P_2$. If $P_1 /\!/ D$ is defined and P_2 and D are a quotient pair, then $P_2 /\!/ D$ is defined and $P_1 /\!/ D \sqsubseteq P_2 /\!/ D$.*

Proof. If $P_1 /\!/ D$ is defined, then $(P_1 /\!/ D) \parallel D \sqsubseteq P_1$ by Thm. 27. Applying the assumption $P_1 \sqsubseteq P_2$, transitivity of $\sqsubseteq$ and Thm. 27 again, we conclude that $P_1 /\!/ D \sqsubseteq P_2 /\!/ D$; in particular, $P_2 /\!/ D$ is also defined. □

4.2 Discussion

In this section we discuss the choice of alphabet for the quotient $Q = P /\!/ D$, argue why its input alphabet may be chosen differently, and conclude with some remarks on quotienting for Modal Interfaces [22].

For $Q \parallel D \sqsubseteq P$ to hold, $Q \parallel D$ and P must have the same input alphabet and the same output alphabet. Thus, we must have $O_Q = O_P \setminus O_D$ and $I_Q \supseteq I_P \setminus I_D$. Concerning the input actions in D, quotient Q can listen to them but does not have to. Hence, $I_Q \subseteq I_P \setminus I_D \cup A_D = I_P \cup O_D$. The more inputs Q has, the easier it is to supply the behaviour ensuring $Q \parallel D \sqsubseteq P$. Thus, we have chosen the input alphabet $I_P \cup O_D$ for our quotient $P /\!/ D$, just as is done in [8] and [22]. When comparing some Q to $P /\!/ D$ in Thm. 27, Q necessarily has the same input and output alphabets as $P /\!/ D$, by Def. 4.

Quotient operators for interface theories have already been discussed by Raclet et al. [22] and Chilton et al. [7]. Our quotient $Q = P /\!/ D$ is most similar to [22], where D is assumed to be may-deterministic, P and D have no internal transitions, and $I_Q = I_P \cup O_D$. However, also P must be may-deterministic there, whereas we additionally allow nondeterminism and disjunctive must-transitions in P.

In addition, we have corrected some technical shortcomings of Modal Interfaces (MI) [22]. MI adapts the quotient operation for Modal Specifications from [21], with some additional rules defining the input and output alphabets of the quotient interface. However, compatibility is completely ignored for the quotient operation, which in [22] is an inverse or adjoint to their parallel product but *not* to parallel composition. This has been recognised in a technical report [4]. Unfortunately, that report employs a changed setting without a universal state. This is reflected by a different, non-compositional parallel composition that does not allow arbitrary behaviour in case of an inconsistency and that employs a more aggressive pruning strategy, where a mismatch can also occur if two systems share an input.

5 Conjunction and Disjunction

Besides parallel composition and quotienting, conjunction is one of the most important operators of interface theories. It allows one to specify different perspectives of a system separately, from which an overall specification can be determined. More formally, the conjunction should be the coarsest specification that refines the given perspective specifications, i.e., it should characterise the greatest lower bound of the refinement preorder. In the sequel, we define conjunction on MIAs with common alphabets, as we did for MIA refinement. Similar to parallel composition, we first present a conjunctive product and, in a second step, remove state pairs with contradictory specifications.

Definition 29 (Conjunctive Product)**.** *Consider two MIAs* $(P, I, O, \longrightarrow_P, \dashrightarrow_P, p_0, e_P)$ *and* $(Q, I, O, \longrightarrow_Q, \dashrightarrow_Q, q_0, e_Q)$ *with common alphabets. The* conjunctive product *is defined as* $P\&Q =_{df} (P \times Q, I, O, \longrightarrow, \dashrightarrow, (p_0, q_0), (e_P, e_Q))$ *by the following operational transition rules:*

(OMust1) $(p,q) \xrightarrow{\omega} \{(p',q') \,|\, p' \in P',\, q \overset{\hat{\omega}}{\Longrightarrow}_Q q'\}$ *if* $p \xrightarrow{\omega}_P P'$ *and* $q \overset{\hat{\omega}}{\Longrightarrow}_Q$
(OMust2) $(p,q) \xrightarrow{\omega} \{(p',q') \,|\, p \overset{\hat{\omega}}{\Longrightarrow}_P p',\, q' \in Q'\}$ *if* $p \overset{\hat{\omega}}{\Longrightarrow}_P$ *and* $q \xrightarrow{\omega}_Q Q'$
(IMust1) $(p,q) \xrightarrow{i} \{(p',q') \,|\, p' \in P',\, q \overset{i}{\dashrightarrow}\overset{\varepsilon}{\Longrightarrow}_Q q'\}$ *if* $p \xrightarrow{i}_P P'$ *and* $q \overset{i}{\dashrightarrow}\overset{\varepsilon}{\Longrightarrow}_Q$
(IMust2) $(p,q) \xrightarrow{i} \{(p',q') \,|\, p \overset{i}{\dashrightarrow}\overset{\varepsilon}{\Longrightarrow}_P p',\, q' \in Q'\}$ *if* $p \overset{i}{\dashrightarrow}\overset{\varepsilon}{\Longrightarrow}_P$ *and* $q \xrightarrow{i}_Q Q'$
(EMust1) $(p,e_Q) \xrightarrow{\alpha} P' \times \{e_Q\}$ *if* $p \xrightarrow{\alpha}_P P'$
(EMust2) $(e_P,q) \xrightarrow{\alpha} \{e_P\} \times Q'$ *if* $q \xrightarrow{\alpha}_Q Q'$
(May1) $(p,q) \overset{\tau}{\dashrightarrow} (p',q)$ *if* $p \overset{\tau}{\Longrightarrow}_P p'$
(May2) $(p,q) \overset{\tau}{\dashrightarrow} (p,q')$ *if* $q \overset{\tau}{\Longrightarrow}_Q q'$
(OMay) $(p,q) \overset{\omega}{\dashrightarrow} (p',q')$ *if* $p \overset{\omega}{\Longrightarrow}_P p'$ *and* $q \overset{\omega}{\Longrightarrow}_Q q'$
(IMay) $(p,q) \overset{i}{\dashrightarrow} (p',q')$ *if* $p \overset{i}{\dashrightarrow}\overset{\varepsilon}{\Longrightarrow}_P p'$ *and* $q \overset{i}{\dashrightarrow}\overset{\varepsilon}{\Longrightarrow}_Q q'$
(EMay1) $(p,e_Q) \overset{\alpha}{\dashrightarrow} (p',e_Q)$ *if* $p \overset{\alpha}{\dashrightarrow}_P p'$
(EMay2) $(e_P,q) \overset{\alpha}{\dashrightarrow} (e_P,q')$ *if* $q \overset{\alpha}{\dashrightarrow}_Q q'$

Note that this definition is similar to the one in [18], except for the treatment of inputs and the universal state. The conjunctive product is inherently different from the parallel product. Single transitions are defined through weak transitions, e.g., as in Rules (OMust), (IMust), (May), and τ-transitions synchronise by Rule (OMay). Furthermore, as given by Rules (EMust) and (EMay), a universal state is a neutral element for the conjunctive product, whereas it is absorbing for the parallel product.

Definition 30 (Conjunction)**.** *Given a conjunctive product* $P\&Q$*, the set* $F \subseteq P \times Q$ *of (logically)* inconsistent states *is defined as the least set satisfying the following rules for all* $p \neq e_P$ *and* $q \neq e_Q$*:*

(F1) $p \xrightarrow{o}_P$ *and* $q \not\overset{o}{\Longrightarrow}_Q$ *implies* $(p,q) \in F$
(F2) $p \not\overset{o}{\Longrightarrow}_P$ *and* $q \xrightarrow{o}_Q$ *implies* $(p,q) \in F$
(F3) $p \xrightarrow{i}_P$ *and* $q \not\overset{i}{\dashrightarrow}_Q$ *implies* $(p,q) \in F$
(F4) $p \not\overset{i}{\dashrightarrow}_P$ *and* $q \xrightarrow{i}_Q$ *implies* $(p,q) \in F$
(F5) $(p,q) \xrightarrow{\alpha} R'$ *and* $R' \subseteq F$ *implies* $(p,q) \in F$

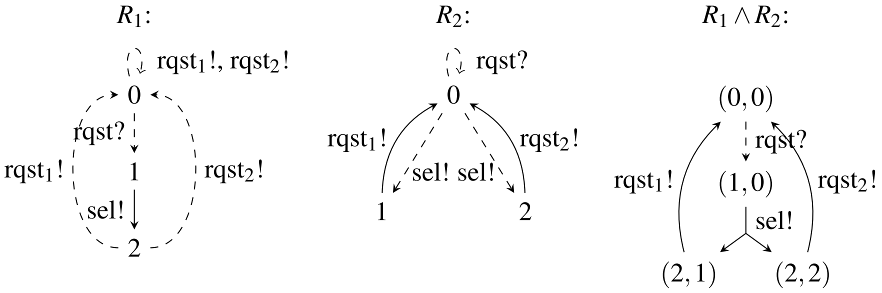

Figure 5: Conjunction on MIAs may lead to disjunctive transitions.

The conjunction $P \wedge Q$ is obtained by deleting all states $(p,q) \in F$ from P&Q. This also removes any may- or must-transition exiting a deleted state and any may-transition entering a deleted state; in addition, deleted states are removed from targets of disjunctive must-transitions. We write $p \wedge q$ for state (p,q) of $P \wedge Q$; all such states are defined – and consistent – by construction. However, if $(p_0,q_0) \in F$, then the conjunction of P and Q does not exist.

An example of conjunction is given in Fig. 5. MIAs R_1 and R_2 can be understood as requirements for a server front-end that routes between a client and at least one of two back-ends. MIA R_1 specifies that, after getting a client's request (rqst?), a back-end selection (sel!) must be performed, after which the request can be forwarded to one of the two back-ends (rqst$_1$!, rqst$_2$!). MIA R_2 specifies that, with the selection, it is decided to which one of the back-ends the request will be forwarded (rqst$_1$!, rqst$_2$!).

In $R_1 \wedge R_2$, the selection process (sel!) is given by a *disjunctive* must-transition. Such a requirement cannot be specified in a deterministic theory, such as Modal Interfaces [22] which our theory extends. Although one might approximate the disjunctive sel! by individual selection actions sel$_1$! and sel$_2$! for each back-end, the conjunction would either have both actions as may-transitions and thus allow one to omit both, or would have both actions as must-transitions, disallowing a server application with only one back-end.

Next, we prove that conjunction as defined above is the greatest lower bound wrt. MIA refinement. To this end, we introduce the notion of a witness as in [18].

Definition 31 (Witness)**.** *A* witness *W of P&Q is a subset of $P \times Q$ such that the following conditions hold for all $(p,q) \in W$:*

(W1) $p \xrightarrow{o}_P$ *implies* $q \overset{o}{\Longrightarrow}_Q$ *or* $q = e_Q$

(W2) $q \xrightarrow{o}_Q$ *implies* $p \overset{o}{\Longrightarrow}_P$ *or* $p = e_P$

(W3) $p \xrightarrow{i}_P$ *implies* $q \overset{i}{\dashrightarrow}\overset{\varepsilon}{\Longrightarrow}_Q$ *or* $q = e_Q$

(W4) $q \xrightarrow{i}_Q$ *implies* $p \overset{i}{\dashrightarrow}\overset{\varepsilon}{\Longrightarrow}_P$ *or* $p = e_P$

(W5) $(p,q) \xrightarrow{\alpha} R'$ *implies* $R' \cap W \neq \emptyset$

Intuitively, a witness is a set of state pairs that are consistent and thus witnesses the existence of a conjunction.

Lemma 32 (Concrete Witness)**.** *Let P, Q and R be MIAs with common alphabets.*

(i) *For any witness W of P&Q, we have $F \cap W = \emptyset$.*

(ii) *The set $\{(p,q) \in P \times Q \mid \exists r \in R.\, r \sqsubseteq p$ and $r \sqsubseteq q\}$ is a witness of $P\&Q$.*

Proof. While the first statement of the lemma is quite obvious, we prove here that $W =_{\text{df}} \{(p,q) \in P \times Q \mid \exists r \in R.\, r \sqsubseteq p \text{ and } r \sqsubseteq q\}$ is a witness of $P\&Q$:

(W1) $p \xrightarrow{o}_P P'$ implies $r \overset{o}{\Longrightarrow}_R R'$ by $r \sqsubseteq p$. Choose some $r' \in R'$. Then, $r \overset{o}{=\!\!\Rightarrow}_R r'$ by syntactic consistency and $q \overset{o}{=\!\!\Rightarrow}_Q$ or $q = e_Q$ by $r \sqsubseteq q$.

(W2) Analogous to (W1).

(W3) Similar to (W1) with o replaced by i, $\Longrightarrow$ by $\longrightarrow\overset{\varepsilon}{\Longrightarrow}$, and $=\!\!\Rightarrow$ by $\dashrightarrow\overset{\varepsilon}{=\!\!\Rightarrow}$.

(W4) Analogous to (W3).

(W5) First, consider $(p,q) \in W$ due to r, with $(p,q) \xrightarrow{\omega} S'$ because of $p \xrightarrow{\omega}_P P'$ and $S' = \{(p',q') \mid p' \in P',\, q \overset{\hat{\omega}}{=\!\!\Rightarrow}_Q q'\}$ by (OMust1). By $r \sqsubseteq p$ and since $p \neq e_P$, we get some $R' \subseteq R$ such that $r \overset{\hat{\omega}}{\Longrightarrow}_R R'$ and $\forall r' {\in} R'\, \exists p' {\in} P'.\, r' \sqsubseteq p'$. Choose $r' \in R'$; now, $r \overset{\hat{\omega}}{=\!\!\Rightarrow}_R r'$ due to syntactic consistency, and $q \overset{\hat{\omega}}{=\!\!\Rightarrow}_Q q'$ with $r' \sqsubseteq q'$ by $r \sqsubseteq q$; this also holds if $q = e_Q$ and $\omega = \tau$. Thus, we have $p' \in P'$ and q' such that $(p',q') \in W \cap S'$ due to r'. The same line of argument works for inputs with trailing-weak instead of weak transitions. The remaining case concerns transitions $(p,e_Q) \xrightarrow{\alpha} S'$ because of $p \xrightarrow{\alpha}_P P'$ and $S' = P' \times \{e_Q\}$ by (EMust1). Choose some $p' \in P'$; then, $(p',e_Q) \in W \cap S'$ due to $r = p'$. □

On the basis of this lemma we can now establish the desired greatest lower bound result for $\wedge$, which implies the compositionality of $\sqsubseteq$ wrt. $\wedge$ (cf. [18]).

Theorem 33 ($\wedge$ is And)**.** *Let P and Q be MIAs with common alphabets. Then, (i) ($\exists R.\, R \sqsubseteq P$ and $R \sqsubseteq Q$) iff $P \wedge Q$ defined. Further, in case $P \wedge Q$ is defined and for any R: (ii) $R \sqsubseteq P$ and $R \sqsubseteq Q$ iff $R \sqsubseteq P \wedge Q$.*

Note that R is implicitly required to have the same alphabets as P and Q by Def. 4.

Proof. (i) "$\Rightarrow$": This follows from Lem. 32.

(i), (ii) "$\Leftarrow$": It suffices to show that $\mathscr{R} =_{\text{df}} \{(r,p) \mid \exists q.\, r \sqsubseteq p \wedge q\}$ is a MIA-refinement relation. Then, in particular, (i) "$\Leftarrow$" follows by choosing $r_0 = p_0 \wedge q_0$. Furthermore, note that (EMust1) and (EMay1) essentially produce an isomorphic copy of P. The refinement conditions for states $(r,p) \in \mathscr{R}$ due to $q = e_Q$ hold by definition of $\mathscr{R}$, and we can ignore these rules in the rest of this proof.

We check the conditions of Def. 4 for some $(r,p) \in \mathscr{R}$ due to q, where $p \neq e_P$:

- $p \neq e_P$ implies $p \wedge q \neq e_P \wedge e_Q$. By $r \sqsubseteq p \wedge q$, we have $r \neq e_R$.
- Let $p \xrightarrow{\alpha}_P P'$; then, $q \overset{\hat{\alpha}}{=\!\!\Rightarrow}_Q$. For $\alpha \neq \tau$, this is because, otherwise, $p \wedge q$ would not be defined due to (F1). Hence, by (OMust1) (or similarly (IMust1)), $p \wedge q \xrightarrow{\alpha} \{p' \wedge q' \mid p' \in P',\, q \overset{\hat{\alpha}}{=\!\!\Rightarrow}_Q q',\, p' \wedge q'$ defined$\}$. By $r \sqsubseteq p \wedge q$, we get $r \overset{\hat{\alpha}}{\Longrightarrow}_R R'$ such that $\forall r' {\in} R'\, \exists p' {\wedge} q'.\, p' \in P',\, q \overset{\hat{\alpha}}{=\!\!\Rightarrow}_Q q'$ and $r' \sqsubseteq p' {\wedge} q'$. Thus, $\forall r' {\in} R'\, \exists p' {\in} P'.\, (r',p') \in \mathscr{R}$.
- $r \overset{\alpha}{\dashrightarrow}_R r'$ implies $\exists p' \wedge q'.\, p \wedge q \overset{\hat{\alpha}}{=\!\!\Rightarrow} p' \wedge q'$ and $r' \sqsubseteq p' \wedge q'$. The contribution of p in this weak transition sequence gives $p \overset{\hat{\alpha}}{=\!\!\Rightarrow}_P p'$, and we have $(r',p') \in \mathscr{R}$ due to q'.

(ii)"$\Longrightarrow$": Here, we show that $\mathscr{R} =_{\mathrm{df}} \{(r, p \wedge q) \mid r \sqsubseteq p \text{ and } r \sqsubseteq q\}$ is a MIA-refinement relation; by Part (i), $p \wedge q$ is defined whenever $r \sqsubseteq p$ and $r \sqsubseteq q$. As above, the (EMust) and (EMay) rules do not need to be checked, in particular, since $r' \sqsubseteq e_Q$ for all r'. We now verify the conditions of Def. 4:

- If $p \wedge q \neq e_P \wedge e_Q$, then w.l.o.g. $p \neq e_P$. By $r \sqsubseteq p$, we also have $r \neq e_R$.
- $p \wedge q \xrightarrow{\alpha} S'$; w.l.o.g. this is due to $p \xrightarrow{\alpha}_P P'$ and $S' = \{p' \wedge q' \mid p' \in P',\, q \overset{\hat{\alpha}}{\Longrightarrow}_Q q',\, p' \wedge q' \text{ defined}\}$. Because of $r \sqsubseteq p$, we have $r \overset{\hat{\alpha}}{\Longrightarrow}_R R'$ so that $\forall r'{\in}R'\, \exists p'{\in}P'.\ r' \sqsubseteq p'$. Consider some arbitrary $r' \in R'$ and the resp. $p' \in P'$. Then, $r \overset{\hat{\alpha}}{\Longrightarrow}_R r'$ by syntactic consistency and, due to $r \sqsubseteq q$, there exists some q' with $q \overset{\hat{\alpha}}{\Longrightarrow}_Q q'$ and $r' \sqsubseteq q'$. Thus, $p' \wedge q' \in S'$ and $(r', p' \wedge q') \in \mathscr{R}$. In case of $\alpha \in I$, we replace weak transitions by trailing-weak transitions.
- Let $r \overset{\alpha}{\dashrightarrow}_R r'$ and consider $p \overset{\hat{\alpha}}{\Longrightarrow}_P p'$ and $q \overset{\hat{\alpha}}{\Longrightarrow}_Q q'$ satisfying $r' \sqsubseteq p'$ and $r' \sqsubseteq q'$. Therefore, $(r', p' \wedge q') \in \mathscr{R}$. Further, if $\alpha \neq \tau$, we have $p \wedge q \overset{\alpha}{\dashrightarrow} p' \wedge q'$ by (OMay). Otherwise, either $p \overset{\tau}{\Longrightarrow}_P p'$ and $q \overset{\tau}{\Longrightarrow}_Q q'$ and we are done by (OMay), or w.l.o.g. $p \overset{\tau}{\Longrightarrow}_P p'$ and $q = q'$ and we are done by (May1), or $p = p'$ and $q = q'$. Again, in case of $\alpha \in I$, we replace weak transitions by trailing-weak transitions. □

Corollary 34. *MIA refinement is compositional wrt. conjunction.*

Clearly, conjunction is commutative. Furthermore, any conjunction operator that satisfies the statement of Thm. 33 for some preorder $\sqsubseteq$ is associative.

Lemma 35. *Let P, Q, R and S be MIAs.*

(1) $P \wedge (Q \wedge R)$ is defined iff $(P \wedge Q) \wedge R$ is defined.

(2) If $P \wedge (Q \wedge R)$ is defined, then $S \sqsubseteq P \wedge (Q \wedge R)$ iff $S \sqsubseteq (P \wedge Q) \wedge R$.

Proof. (1) Thm. 33(i), (ii) imply that $P \wedge (Q \wedge R)$ is defined iff $\exists S.\, S \sqsubseteq P$ and $S \sqsubseteq Q \wedge R$ iff $\exists S.\, S \sqsubseteq P$ and $S \sqsubseteq Q$ and $S \sqsubseteq R$ iff $\exists S.\, S \sqsubseteq P \wedge Q$ and $S \sqsubseteq R$ iff $(P \wedge Q) \wedge R$ is defined. Statement (2) follows directly from multiple applications of Thm. 33(ii). □

As a consequence of Lem. 35 we obtain strong associativity of conjunction.

Theorem 36 (Associativity of Conjunction). *Conjunction is strongly associative in the sense that, if one of $P \wedge (Q \wedge R)$ and $(P \wedge Q) \wedge R$ is defined, then both are defined and $P \wedge (Q \wedge R) \sqsupseteq\sqsubseteq (P \wedge Q) \wedge R$.*

We now turn our attention to disjunction $\vee$ on MIAs with the same alphabets and show that it corresponds to the least upper bound of MIA refinement.

Definition 37 (Disjunction). *Given two MIA $(P, I, O, \longrightarrow_P, \dashrightarrow_P, p_0, e_P)$ and $(Q, I, O, \longrightarrow_Q, \dashrightarrow_Q, q_0, e_Q)$ with common input and output alphabets. Writing also e for $e_P \vee e_Q$, the* disjunction *$P \vee Q$ is defined as $(\{e\}, I, O, \emptyset, \emptyset, e, e)$ if $p_0 = e_P$ or $q_0 = e_Q$. Otherwise, and assuming disjoint state sets, $P \vee Q = (\{p_0 \vee q_0, e\} \cup P \cup Q, I, O, \longrightarrow, \dashrightarrow, p_0 \vee q_0, e)$, where $\longrightarrow$ and $\dashrightarrow$ are the least sets satisfying the conditions $\longrightarrow_P \subseteq \longrightarrow$, $\dashrightarrow_P \subseteq \dashrightarrow$, $\longrightarrow_Q \subseteq \longrightarrow$, $\dashrightarrow_Q \subseteq \dashrightarrow$, and the following rules:*

(Must) $p_0 \vee q_0 \xrightarrow{\tau} \{p_0, q_0\}$ *if* $p_0 \neq e_P$ *and* $q_0 \neq e_Q$
(IMust) $p_0 \vee q_0 \xrightarrow{i} P' \cup Q'$ *if* $p_0 \xrightarrow{i}_P P'$ *and* $q_0 \xrightarrow{i}_Q Q'$
(May) $p_0 \vee q_0 \overset{\tau}{\dashrightarrow} p_0,\ p_0 \vee q_0 \overset{\tau}{\dashrightarrow} q_0$ *if* $p_0 \neq e_P$ *and* $q_0 \neq e_Q$
(IMay1) $p_0 \vee q_0 \overset{i}{\dashrightarrow} p'$ *if* $p_0 \overset{i}{\dashrightarrow}_P p'$
(IMay2) $p_0 \vee q_0 \overset{i}{\dashrightarrow} q'$ *if* $q_0 \overset{i}{\dashrightarrow}_Q q'$

Further, for each input may-transition to e_P or e_Q, the target is replaced by $e_P \vee e_Q$.

It is not difficult to see that disjunction is commutative and associative. The latter follows from the dual statement to Thm. 33, namely that $\vee$ is indeed disjunction.

Theorem 38 ($\vee$ is Or)**.** *Let P, Q and R be MIAs with common alphabets. Then, we have $P \vee Q \sqsubseteq R$ iff $P \sqsubseteq R$ and $Q \sqsubseteq R$.*

Proof. If, say, $p_0 = e_P$, then both sides imply $r_0 = e_R$, which implies $Q \sqsubseteq R$ in any case. So we can assume that neither $p_0 = e_P$ nor $q_0 = e_Q$.

"$\Longrightarrow$": We establish that $\mathscr{R} =_{\text{df}} \{(p_0, r) \mid p_0 \vee q_0 \sqsubseteq r\} \cup \sqsubseteq$ is a MIA-refinement relation. To do so, we let $(p_0, r) \in \mathscr{R}$ due to q_0 and check the conditions of Def. 4:

(i) If $r \neq e_R$, then $p_0 \vee q_0 \neq e$; thus, $p_0 \neq e_P$.

(ii) Let $r \xrightarrow{i}_R R'$. Because of $p_0 \vee q_0 \sqsubseteq r$ and by the only applicable Rule (IMust), we have $p_0 \vee q_0 \xrightarrow{i}\overset{\varepsilon}{\Longrightarrow} P' \cup Q'$, due to $p_0 \xrightarrow{i}\overset{\varepsilon}{\Longrightarrow}_P P'$ and $q_0 \xrightarrow{i}\overset{\varepsilon}{\Longrightarrow}_Q Q'$, such that $\forall p' {\in} P' \cup Q' \exists r' {\in} R'.\ p' \sqsubseteq r'$; recall $P \cap Q = \emptyset$. Hence, $\forall p' {\in} P' \exists r' {\in} R'.\ p' \sqsubseteq r'$ and

(iii) Let $r \xrightarrow{\omega}_R R'$. By $p_0 \vee q_0 \sqsubseteq r$, we get $p_0 \vee q_0 \overset{\hat{\omega}}{\Longrightarrow} S'$ for some S' such that $\forall s {\in} S'\ \exists r' {\in} R'.\ s \sqsubseteq r'$. If $p_0 \vee q_0 \overset{\omega}{\Longrightarrow} S'$, then the transition sequence underlying this weak transition starts with $p_0 \vee q_0 \xrightarrow{\tau} \{p_0, q_0\}$, and the remainder can be decomposed showing $p_0 \overset{\hat{\omega}}{\Longrightarrow}_P P'$, $q_0 \overset{\hat{\omega}}{\Longrightarrow}_Q Q'$ and $S' = P' \cup Q'$. As $\forall p' {\in} P' \exists r' {\in} R'.\, p' \sqsubseteq r'$, we are done now. The only remaining case is $\omega = \tau$ and $S' = \{p_0 \vee q_0\}$, in which there is some $r' \in R'$ such that $p_0 \vee q_0 \sqsubseteq r'$, i.e., $(p_0, r') \in \mathscr{R}$. Hence, we are done in this case, too, since $p_0 \overset{\hat{\tau}}{\Longrightarrow}_P p_0$.

(iv) Let $p_0 \overset{i}{\dashrightarrow}_P p'$. Then, $p_0 \vee q_0 \overset{i}{\dashrightarrow} p'$ and, due to $p_0 \vee q_0 \sqsubseteq r$, we obtain some r' with $r \overset{i}{\dashrightarrow}\overset{\varepsilon}{\Longrightarrow}_R r'$ and $p' \sqsubseteq r'$ by Def. 4 (iv).

(v) Let $p_0 \overset{\omega}{\dashrightarrow}_P p'$. Then, $p_0 \vee q_0 \overset{\tau}{\dashrightarrow} p_0$ and, due to $p_0 \vee q_0 \sqsubseteq r$, we apply Def. 4 (iv) twice to obtain some r' with $r \overset{\hat{\omega}}{\Longrightarrow}_R r'$ and $p' \sqsubseteq r'$.

"$\Longleftarrow$": We prove that $\mathscr{R} =_{\text{df}} \{(p_0 \vee q_0, r) \mid p_0 \sqsubseteq r \text{ and } q_0 \sqsubseteq r\} \cup \sqsubseteq$ is a MIA-refinement relation; consider $(p_0 \vee q_0, r)$ with $r \neq e_R$.

(i) Since $r \neq e_R$, we have $p_0 \neq e_P$ and $q_0 \neq e_Q$; thus, $p_0 \vee q_0 \neq e$.

(ii) Let $r \xrightarrow{i}_R R'$. By $p_0 \sqsubseteq r$ and $q_0 \sqsubseteq r$, we have P' and Q' satisfying $p_0 \xrightarrow{i}\overset{\varepsilon}{\Longrightarrow}_P P'$, $q_0 \xrightarrow{i}\overset{\varepsilon}{\Longrightarrow}_Q Q'$ such that $\forall p' {\in} P' \exists r' {\in} R'.\ p' \sqsubseteq r'$ and $\forall q' {\in} Q' \exists r' {\in} R'.\ q' \sqsubseteq r'$. Thus, $p_0 \vee q_0 \overset{i}{\Longrightarrow} P' \cup Q'$ using Rule (IMust) and interleaving the replacements involved in the weak transitions $p_0 \xrightarrow{i}\overset{\varepsilon}{\Longrightarrow}_P P'$ and $q_0 \xrightarrow{i}\overset{\varepsilon}{\Longrightarrow}_Q Q'$; recall that $P \cap Q = \emptyset$.

(iii) Let $r \xrightarrow{\omega}_R R'$. By $p_0 \sqsubseteq r$ and $q_0 \sqsubseteq r$ we have P' and Q' such that $p_0 \overset{\hat{\omega}}{\Longrightarrow}_P P'$, $q_0 \overset{\hat{\omega}}{\Longrightarrow}_Q Q'$ and $\forall p' \in P' \cup Q' \, \exists r' \in R'.\ p' \sqsubseteq r'$. Hence, $p_0 \vee q_0 \overset{\hat{\omega}}{\Longrightarrow} P' \cup Q'$ due to Rule (Must).

(iv) Let $p_0 \vee q_0 \overset{i}{\dashrightarrow}_Q$. Then, w.l.o.g., we only need to consider $p_0 \overset{i}{\dashrightarrow}_P p'$, and as $p_0 \sqsubseteq r$ we have $r \overset{i}{\dashrightarrow} \overset{\varepsilon}{\Longrightarrow}_R r'$ for some r' satisfying $p' \sqsubseteq r'$.

(v) Let $p_0 \vee q_0 \overset{\omega}{\dashrightarrow}$. This is only possible for $\omega = \tau$. W.l.o.g. we only need to consider $p_0 \vee q_0 \overset{\tau}{\dashrightarrow} p_0$. This transition is matched with $r \overset{\varepsilon}{\Longrightarrow}_R r$ since $p_0 \sqsubseteq r$. □

Corollary 39. *MIA refinement is compositional wrt. disjunction.*

6 Alphabet Extension

So far, MIA refinement is only defined on MIAs with the same alphabets. This is insufficient for supporting perspective-based specification, where an overall specification is conjunctively composed of smaller specifications, each addressing one 'perspective' (e.g., a single system requirement) and referring only to actions that are relevant to that perspective. Hence, it is useful to extend conjunction and thus MIA refinement to dissimilar alphabets in such a way that we can add new inputs and outputs in a refinement step. For this purpose we introduce alphabet extension as an operation on MIAs, similar to [18] and also to *weak extension* in [22]. More precisely, we add may-loops for all new actions to each state, except the universal state. Conjunction and also disjunction are easily generalised by applying alphabet extension to the operands. These two and parallel composition are compositional wrt. the extended refinement preorder. For the quotient, however, the situation is more difficult as we discuss below.

Definition 40 (Alphabet Extension & Refinement)**.** *Given a MIA $(P, I, O, \longrightarrow, \dashrightarrow, p_0, e)$ and disjoint action sets I' and O' satisfying $I' \cap A = \emptyset = O' \cap A$, where $A =_{df} I \cup O$, the* alphabet extension of P by I' and O' *is given by $[P]_{I',O'} =_{df} (P, I \cup I', O \cup O', \longrightarrow, \dashrightarrow', p_0, e)$ for $\dashrightarrow' =_{df} \dashrightarrow \cup \{(p, a, p) \mid p \in P \setminus \{e\}, a \in I' \cup O'\}$. We often write $[p]_{I',O'}$ for p as state of $[P]_{I',O'}$, or conveniently $[p]$ in case I', O' are understood from the context.*

For MIAs P and Q with $p \in P$, $q \in Q$, $I_P \supseteq I_Q$ and $O_P \supseteq O_Q$, we define $p \sqsubseteq' q$ if $p \sqsubseteq [q]_{I_P \setminus I_Q, O_P \setminus O_Q}$. Since $\sqsubseteq'$ extends $\sqsubseteq$ to MIAs with different alphabets, we write $\sqsubseteq$ for $\sqsubseteq'$ and abbreviate $[q]_{I_P \setminus I_Q, O_P \setminus O_Q}$ by $[q]_P$; the same notations are used for P and Q.

As an aside we remark that our alphabet extension is different to the one proposed by Ben-David et al. for Modal Transition Systems in [3], where unknown actions are treated as internal actions. This has the consequence, however, that a state with an *a*-must-transition can be refined by a state that offers a *b*-must-transition followed by an *a*-must-transition, where *b* is a new action. In the context of interface theories, this is undesirable, particularly, if *a* is an input.

Compositionality of parallel composition as in Thm. 15 is preserved by the extended refinement relation as long as alphabet extension does not yield new communications.

Theorem 41 (Compositionality of Parallel Composition)**.** *Let P_1, P_2, Q be MIAs such that Q and P_2 are composable and $P_1 \sqsubseteq Q$. Assume further that, for $I' =_{df} I_1 \setminus I_Q$ and $O' =_{df} O_1 \setminus O_Q$, we have $(I' \cup O') \cap A_2 = \emptyset$. Then:*

(a) *P_1 and P_2 are composable.*

(b) *If Q and P_2 are compatible, then so are P_1 and P_2 and $P_1 \parallel P_2 \sqsubseteq Q \parallel P_2$.*

Proof. It is easy to see that $[Q]_{I',O'}$ and P_2 are composable due to $(I' \cup O') \cap A_2 = \emptyset$, which implies (a). Furthermore, $[Q]_{I',O'} \otimes P_2$ is isomorphic to $[Q \otimes P_2]_{I',O'}$ via mapping $[q] \otimes p_2 \mapsto [q \otimes p_2]$. This is because of (PMay1) in the definition of $\otimes$, since we only add "fresh" may-transitions to each $q \in Q$. The mapping also respects errors as new may-transitions with label $o \in O'$ cannot create new errors since $o \notin I_2$, and no new $i \in I'$ has to have a must-transition since $i \notin O_2$. Thus, $[q_0]$ and p_{02} are compatible if q_0 and p_{02} are; moreover, $p_{01} \sqsubseteq [q_0]$. Now, the result follows from Thm. 15. □

For outputs it is obvious that new communications might result in an error and, therefore, must be disallowed. Although a new shared input $i \in I' \cap I_2$ does not raise errors in synchronisation, it can break compositionality for multicast communication: if $p_{01} \sqsubseteq q_0$, $p_{02} \xrightarrow{i}$ and $p_{01} \not\xrightarrow{i}$, then $q_0 \parallel p_{02} \xrightarrow{i}$ but $p_{01} \parallel p_{02} \not\xrightarrow{i}$.

We lift our conjunction operator to conjuncts with dissimilar alphabets.

Definition 42 (Lifting Conjunction)**.** *Let P, Q be MIAs, $p \in P$ and $q \in Q$ such that $I_P \cap O_Q = \emptyset = I_Q \cap O_P$. Then, $p \wedge' q =_{df} [p]_Q \wedge [q]_P$ and similarly for $P \wedge' Q$. We simply write $\wedge$ for $\wedge'$.*

To be able to lift our main result, Thm. 33, it is sufficient to establish that the alphabet extension operation is a homomorphism for conjunction. The proof of Thm. 33 follows exactly the line of argument in [18].

Lemma 43. *Let P with $p \in P$ and Q with $q \in Q$ be MIAs with common alphabets. Consider the alphabet extensions by some I' and O'. Then:*

(a) *p and q are consistent iff $[p]$ and $[q]$ are.*

(b) *Given consistency, $[p \wedge q] \sqsupseteq\sqsubseteq [p] \wedge [q]$.*

Proof. For proving (a), consider the mapping $\beta : (p,q) \mapsto ([p],[q])$, which is a bijection between $P\&Q$ and $[P]\&[Q]$. We have $(p,q) \in F_{P\&Q}$ due to $a \in A$ and (F1), (F2), (F3) or (F4) iff $([p],[q]) \in F_{[P]\&[Q]}$ due to $a \in A$ and (F1), (F2), (F3) or (F4). Observe that (F1), (F2), (F3) and (F4) never apply to $([p],[q])$ and $a \in I' \cup O'$, since there are no must-transitions labelled a. For the same reason, Rules (OMust1), (OMust2), (IMust1), (IMust2), (EMust1) and (EMust2) are never applicable for a and, thus, β is an isomorphism regarding must-transitions; hence, (F5) is applicable exactly in the corresponding cases according to β. Therefore, β is also a bijection between $F_{P\&Q}$ and $F_{[P]\&[Q]}$.

For (b), we can regard β also as a bijection between $[P \wedge Q]$ and $[P] \wedge [Q]$, and establish each direction of $\sqsupseteq\sqsubseteq$ separately:

- "$\sqsubseteq$"*:* We show that β is a MIA-refinement relation, for which we consider $[p \wedge q]$ and $[p] \wedge [q]$. Cond. (i) of Def. 4 is trivial. Conds. (ii) and (iii) are clear, because β is still an isomorphism on must-transitions. Regarding Conds. (iv) and (v), we only have to consider $\alpha \in I' \cup O'$ and $[p \wedge q] \overset{\alpha}{\dashrightarrow} [p \wedge q]$. This transition can be matched by the transition $[p] \wedge [q] \overset{\alpha}{\dashrightarrow} [p] \wedge [q]$, which exists by (IMay), (OMay), (EMay1) or (EMay2).

- "$\sqsupseteq$"*:* We show that also β^{-1} is a MIA-refinement relation. Take $[p] \wedge [q]$ and $[p \wedge q]$; again, Conds. (i), (ii) and (iii) are clear. Thus, we only have to consider $\alpha \in I' \cup O'$ for establishing Conds. (iv) and (v), so that $[p] \wedge [q] \overset{\alpha}{\dashrightarrow} r$ iff $r = [p'] \wedge [q']$ for $p \overset{\varepsilon}{\Longrightarrow} p'$ and $q \overset{\varepsilon}{\Longrightarrow} q'$. Such a transition can be matched by the transition $[p \wedge q] \overset{\alpha}{\dashrightarrow} [p \wedge q] \overset{\varepsilon}{\Longrightarrow} [p' \wedge q']$, where the weak may-transition exists by (May1), (May2), (OMay), (IMay), (EMay1) or (EMay2), or because $p = p'$ and $q = q'$. □

Theorem 44 ($\wedge$ is And)**.** *Let P, Q and R be MIAs such that $I_P \cap O_Q = \emptyset = I_Q \cap O_P$, $I_R \supseteq I_P \cup I_Q$ and $O_R \supseteq O_P \cup O_Q$. Then, (i) there exists such an R with $R \sqsubseteq P$ and $R \sqsubseteq Q$ iff $P \wedge Q$ is defined. In case $P \wedge Q$ is defined: (ii) $R \sqsubseteq P$ and $R \sqsubseteq Q$ iff $R \sqsubseteq P \wedge Q$.*

Proof. Recall that we denote by $[\cdot]_P$ an extension with the additional actions of P, and similarly for Q and R. Also note that, in the context of this theorem, $[[p_0]_Q]_R = [p_0]_R$ and $[[q_0]_P]_R = [q_0]_R$.

(i) If $r_0 \sqsubseteq [p_0]_R$ and $r_0 \sqsubseteq [q_0]_R$, then $[p_0]_R \wedge [q_0]_R$ is defined by Thm. 33. The latter conjunction equals $[[p_0]_Q]_R \wedge [[q_0]_P]_R$; hence, $[p_0]_Q \wedge [q_0]_P$ is defined by Lem. 43, and this conjunction is $p_0 \wedge q_0$ by definition. If $[p_0]_Q \wedge [q_0]_P$ is defined, there exists R with the common alphabets of $[P]_Q$ and $[Q]_P$ with $r_0 \sqsubseteq [p_0]_Q$ and $r_0 \sqsubseteq [q_0]_P$ by Thm. 33. For this R, we have $[p_0]_Q = [p_0]_R$ and $[q_0]_P = [q_0]_R$; thus, $r_0 \sqsubseteq p_0$ and $r_0 \sqsubseteq q_0$ by definition.

(ii) Let $p_0 \wedge q_0$ be defined. We reason as follows:

$$\begin{array}{lll}
 & r_0 \sqsubseteq p_0 \text{ and } r_0 \sqsubseteq q_0 & \\
\text{iff} & r_0 \sqsubseteq [p_0]_R \text{ and } r_0 \sqsubseteq [q_0]_R & \text{(by definition)} \\
\text{iff} & r_0 \sqsubseteq [p_0]_R \wedge [q_0]_R & \text{(by Thm. 33)} \\
\text{iff} & r_0 \sqsubseteq [[p_0]_Q \wedge [q_0]_P]_R & \text{(by Lem. 43 and note above)} \\
\text{iff} & r_0 \sqsubseteq p_0 \wedge q_0 & \text{(by Defs. 40 and 42)} \qquad \Box
\end{array}$$

The situation for disjunction under alphabet extension is analogous to the one above, but exploiting monotonicity of the alphabet extension operation wrt. $\sqsubseteq$.

Definition 45 (Lifting Disjunction)**.** *Let P, Q be MIAs, $p \in P$ and $q \in Q$ such that $I_P \cap O_Q = \emptyset = I_Q \cap O_P$. Then, $p \vee' q =_{df} [p]_Q \vee [q]_P$ and similarly for $P \vee' Q$. Once again, we simply write $\vee$ for $\vee'$.*

Lemma 46 (Monotonicity of $[\cdot]$)**.** *Let P with $p \in P$ and R with $r \in R$ be MIAs having the same alphabets, as well as I' and O' be suitable action sets for extending them. Then, $p \sqsubseteq r$ iff $[p] \sqsubseteq [r]$.*

Proof. Since we only add may-loops with a fresh label a for the extension, it suffices to observe for direction ”$\Longrightarrow$” and $p \sqsubseteq r$ that each may-transition $[p] \overset{a}{\dashrightarrow} [p]$ can be matched by $[r] \overset{a}{\dashrightarrow} [r]$, or $r = e_R$. □

Theorem 47 ($\vee$ is Or)**.** *Let P, Q and R be MIAs such that $I_P \cap O_Q = \emptyset = I_Q \cap O_P$, $I_R \subseteq I_P \cup I_Q$ and $O_R \subseteq O_P \cup O_Q$. Then, $P \vee Q \sqsubseteq R$ iff $P \sqsubseteq R$ and $Q \sqsubseteq R$.*

Proof. The proof proceeds along the following chain of equivalences:

$$\begin{array}{lll}
 & p_0 \vee q_0 \sqsubseteq r_0 & \\
\text{iff} & [p_0]_Q \vee [q_0]_P \sqsubseteq [[r_0]_P]_Q & \text{(by definition)} \\
\text{iff} & [p_0]_Q \sqsubseteq [[r_0]_P]_Q \text{ and } [q_0]_P \sqsubseteq [[r_0]_P]_Q & \text{(by Thm. 38)} \\
\text{iff} & p_0 \sqsubseteq [r_0]_P \text{ and } q_0 \sqsubseteq [r_0]_Q & \text{(by Lem. 46)} \\
\text{iff} & p_0 \sqsubseteq r_0 \text{ and } q_0 \sqsubseteq r_0 & \text{(by definition)} \qquad \Box
\end{array}$$

We conclude this section by reconsidering our quotient operator. As discussed in Sec. 4.2, there is some freedom in choosing the input alphabet of the quotient $P /\!/ D$ of a specification P and a divisor D, namely $I_P \setminus I_D \subseteq I_{P/\!/D} \subseteq I_P \cup O_D$. Since our extended refinement allows us to compare MIAs with different alphabets, one could aim for a generalisation of Thm. 27 where Q and $P /\!/ D$ may have different alphabets.

Because $Q \sqsubseteq P /\!/ D$, the quotient would have a minimal alphabet in this version, in contrast to our choice of $I_{P/\!/D} = I_P \cup O_D$. However, this leads to complications as one can see from the example in Fig. 6. A MIA Q satisfying $Q \parallel D \sqsubseteq P$ must have $O_Q = \{x, y\}$, but $I_Q = I_P \setminus I_D = \emptyset$ clearly does not suffice because

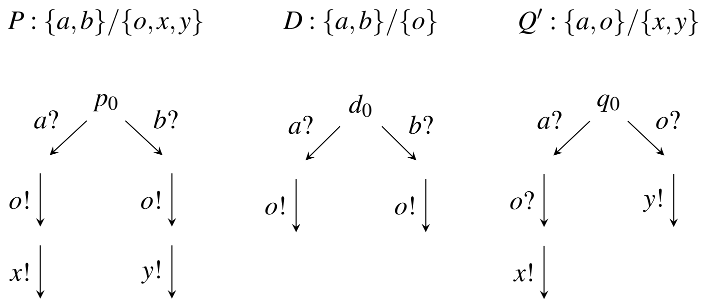

Figure 6: Complications of quotienting in the context of alphabet extension.

Q is allowed to produce x or y only after o. Furthermore, Q must see a or b to distinguish between the branches. Solutions are possible for $I_Q = \{a,o\}$ and $I_Q = \{b,o\}$; a solution Q' for $\{a,o\}$ is also shown in Fig. 6, where transitions to the universal state are not drawn for simplicity. It looks like there are several maximal solutions. Note, however, that Thm. 27 in its present form still holds for our extended refinement preorder.

Another aspect of alphabet extension for quotienting is that we can generalise the problem by permitting D to have actions unknown to P. A straightforward generalisation of our approach in Sec. 4 would make these actions inputs for the quotient, but there can also be solutions to $Q \parallel D \sqsubseteq P$ where Q has some new inputs of D as outputs. We leave a further investigation of these aspects to future work.

7 Conclusions and Future Work

We presented an extension of Raclet et al.'s modal interface theory [22] to *nondeterministic* systems. To do so we resolved, for the first time properly, the conflict between unspecified inputs being allowed in interface theories derived from de Alfaro and Henzinger's Interface Automata [11] but forbidden in Modal Transition Systems [15]. To this end, we introduced a special universal state, which enabled us to achieve compositionality (in contrast to [16]) as well as associativity (in contrast to [22]) for parallel composition; this also allowed for a more practical support of perspective-based specification when compared to [17, 18]. In addition, we defined a quotienting operator that permits the decomposition of *nondeterministic* specifications and takes *pruning* in parallel composition into account (in contrast to [22]).

Regarding future work, we wish to explore the choice of alphabets for quotienting and relax the determinism requirement on divisors. We also intend to implement our theory in MICA (see `http://www.irisa.fr/s4/tools/mica/`) or the MIO Workbench [2].

References

[1] S. S. Bauer, A. David, R. Hennicker, K. G. Larsen, A. Legay, U. Nyman, and A. Wasowski. Moving from specifications to contracts in component-based design. In *FASE*, volume 7212 of *LNCS*, pages 43–58. Springer, 2012.

[2] S. S. Bauer, P. Mayer, A. Schroeder, and R. Hennicker. On weak modal compatibility, refinement, and the MIO Workbench. In *TACAS*, volume 6015 of *LNCS*, pages 175–189. Springer, 2010.

[3] S. Ben-David, M. Chechik, and S. Uchitel. Merging partial behaviour models with different vocabularies. In *CONCUR*, volume 8052 of *LNCS*, pages 91–105. Springer, 2013.

[4] A. Benveniste, B. Caillaud, D. Nickovic, R. Passerone, J.-B. Raclet, P. Reinkemeier, A. Sangiovanni-Vincentelli, W. Damm, T. A. Henzinger, and K. G. Larsen. Contracts for system design. Technical Report 8147, INRIA, November 2012.

[5] D. Beyer, A. Chakrabarti, T. A. Henzinger, and S. A. Seshia. An application of web-service interfaces. In *ICWS*, pages 831–838. IEEE, 2007.

[6] F. Bujtor and W. Vogler. Error-pruning in interface automata. In *SOFSEM*, volume 8327 of *LNCS*, pages 162–173. Springer, 2014.

[7] T. Chen, C. Chilton, B. Jonsson, and M. Z. Kwiatkowska. A compositional specification theory for component behaviours. In *ESOP*, volume 7211 of *LNCS*, pages 148–168. Springer, 2012.

[8] C. Chilton. *An Algebraic Theory of Componentised Interaction*. PhD thesis, Oxford, 2013.

[9] C. Chilton, B. Jonsson, and M. Kwiatkowska. An algebraic theory of interface automata. Technical Report RR-13-02, Oxford, 2013.

[10] L. de Alfaro and T. A. Henzinger. Interface automata. In *FSE*, pages 109–120. ACM, 2001.

[11] L. de Alfaro and T. A. Henzinger. Interface-based design. In *Engineering Theories of Software-Intensive Systems*, volume 195 of *NATO Science Series*. Springer, 2005.

[12] R. De Nicola and R. Segala. A process algebraic view of input/output automata. *Theor. Comput. Sci.*, 138(2):391–423, 1995.

[13] H. Hüttel and K. G. Larsen. The use of static constructs in a modal process logic. In *Logic at Botik*, volume 363 of *LNCS*, pages 163–180. Springer, 1989.

[14] K. Larsen and L. Xinxin. Equation solving using modal transition systems. In *LICS*, pages 108–117. IEEE, 1990.

[15] K. G. Larsen. Modal specifications. In *Automatic Verification Methods for Finite State Systems*, volume 407 of *LNCS*, pages 232–246. Springer, 1989.

[16] K. G. Larsen, U. Nyman, and A. Wasowski. Modal I/O automata for interface and product line theories. In *ESOP*, volume 4421 of *LNCS*, pages 64–79. Springer, 2007.

[17] G. Lüttgen and W. Vogler. Modal interface automata. *LMCS*, 9(3), 2013.

[18] G. Lüttgen and W. Vogler. Richer interface automata with optimistic and pessimistic compatibility. *ECEASST*, 66, 2013. An extended version has been submitted to Acta Informatica.

[19] N. A. Lynch. *Distributed Algorithms*. Morgan Kaufmann, 1996.

[20] R. Milner. *Communication and concurrency*. Prentice Hall, 1989.

[21] J.-B. Raclet. Residual for component specifications. *ENTCS*, 215:93–110, 2008.

[22] J.-B. Raclet, E. Badouel, A. Benveniste, B. Caillaud, A. Legay, and R. Passerone. A modal interface theory for component-based design. *Fund. Inform.*, 108(1-2):119–149, 2011.