Acta Informatica manuscript No.
(will be inserted by the editor)

Richer Interface Automata with Optimistic and Pessimistic Compatibility

Gerald Lüttgen · **Walter Vogler** · **Sascha Fendrich**

Received: date / Accepted: date

Abstract Modal transition systems are a popular semantic underpinning of interface theories, such as Nyman et al.'s IOMTS and Bauer et al.'s MIO, which facilitate component-based reasoning for concurrent systems. Our interface theory MIA repaired a compositional flaw of IOMTS-refinement and introduced a conjunction operator. In this paper, we first modify MIA to properly deal with internal computations including internal must-transitions, which were largely ignored already in IOMTS. We then study a MIA variant that adopts MIO's pessimistic – rather than IOMTS' optimistic – view on component compatibility and define, for the first-time in a pessimistic, non-deterministic setting, conjunction and disjunction on interfaces. For both the optimistic and pessimistic MIA variant, we also discuss mechanisms for extending alphabets when refining interfaces, which is a desired feature for perspective-based specification. We illustrate our advancements via a small example.

Keywords Interface theory · disjunctive modal transitions system · modal interface automata · interface refinement · alphabet extension · perspective-based specification

1 Introduction

Interfaces play an important role for checking interoperability of system components, in particular in the component-based design of critical systems. Over the past two decades, research has focused on interface theories for *sequential* and object-oriented software systems.

An extended abstract of this article appeared in S. Schneider and H. Treharne, eds., 13th Intl. Workshop on *Automated Verification of Critical Systems* (AVoCS 2013), vol. 66 of Electronic Communications of the EASST. Research support was provided by the DFG (German Research Foundation) under grants LU 1748/3-1 and VO 615/12-1.

G. Lüttgen
Software Technologies Research Group, University of Bamberg, 96045 Bamberg, Germany
E-mail: gerald.luettgen@swt-bamberg.de

W. Vogler
Institut für Informatik, University of Augsburg, 86159 Augsburg, Germany
E-mail: walter.vogler@informatik.uni-augsburg.de

S. Fendrich
Software Technologies Research Group, University of Bamberg, 96045 Bamberg, Germany
E-mail: sascha.fendrich@uni-bamberg.de

These theories comprise behavioural types, which are often referred to as *contracts* [17] and express pre- and post-conditions as well as invariants of methods and classes; see [13] for a survey on contract languages and contract verification. More recently, interface theories describing behavioural/reactive types for *concurrent* systems [4,9,10,15,16,19] have emerged as a key technology, e.g., for specifying web services [6] and software contracts [3].

Many behavioural interface theories are inspired by de Alfaro and Henzinger's *Interface Automata* (IA) [1], which employs transition systems with input and output actions and alternating simulation for refinement. It is distinguished from classic process algebras by its parallel composition operator: an interface cannot block an incoming input in any state but, if an input arrives unexpectedly, this is treated as an error, i.e., as an incompatibility. IA suffers from the fact that outputs cannot be required since any interface may be implemented by a component that accepts all inputs and does not engage in any output, hence avoiding errors altogether. This is undesired in practice and has led researchers to base theories [4, 15, 16, 19] on Larsen's *modal* transition systems (MTS) [14]; these distinguish between must- and may-transitions and, thus, allow one to enforce outputs via output must-transitions.

In the light of errors that may arise when joining components in parallel, two schools on MTS-based interface theories have emerged, which treat compatibility either *optimistically* or *pessimistically*. To explain the difference, consider a component that offers an input a followed by an output b. If this component is composed in parallel with a component that does not offer an input on b, then an error state is reached after input a. Now, in the optimistic setting, the components are still considered to be (potentially) compatible since the system environment might refrain from sending an a and, thus, from forcing the parallel system into the error state. In the pessimistic setting, the components are deemed to be incompatible – with their parallel composition not being defined – because there exists a system environment – namely the environment initially offering the a – leading to the error state.

Therefore, the pessimistic school of Bauer et al. [4] only defines the composition of a restricted set of components; however, their MIO setting employs standard *modal refinement* as refinement preorder and standard weak transitions for abstracting from internal computation. In contrast, the optimistic school of Nyman et al. [15] follows IA in that parallel composition is still defined in the presence of error states, if some concrete system environment may prohibit such states to be reached. Their IOMTS setting is equipped with a customized preorder, which allows one to compose a much larger set of components than in MIO. Fatally, IOMTS-refinement does not require the matching of internal must-transitions of implementations and is not at all permissive wrt. abstracting from internal computation. Our interface theory *Modal Interface Automata* (MIA) [16] adopts IOMTS-refinement while repairing a compositional flaw regarding IOMTS parallel composition. It also adds conjunction on interfaces with common alphabets (i.e., action sets), which is a key operator allowing engineers to specify a concurrent system from different perspectives.

This paper advances the state-of-the-art of both schools. Regarding the optimistic MIA setting, we first re-consider IOMTS-refinement so that it properly deals with internal computation including internal must-transitions (cf. Sec. 2). Along the way we also permit general *disjunctive* must-transitions, thereby increasing expressiveness and enabling an intuitive definition of disjunction on interfaces. In particular, disjunctive must transitions are necessary to define a conjunction for nondeterministic systems in the presence of modalities (see Fig. 5 below). To the best of our knowledge, no existing work on disjunctive MTS considers weak transitions, and doing so turns out to be technically quite involved. In addition, we also extend MIA-refinement so as to allow alphabet changes during refinement along the lines of de Alfaro and Henzinger [1], which were also adopted by Chilton et al. [9,10]. Extending alphabets is useful in practice, firstly, when composing partial specification interfaces to an

overall interface conjunctively – in the sense of perspective-based specification employed in software engineering – and, secondly, since implementors may decide to add extra features that are not covered by the specification interface (cf. [19]). However, we demonstrate that the alphabet changes of de Alfaro and Henzinger are not suited for the first purpose and support the second only for inputs (cf. Sec. 2.4).

We then study a pessimistic variant of MIA, to which we add a powerful alphabet extension mechanism. Equally important, we define – for the first-time in a pessimistic, nondeterministic setting – conjunction and disjunction on interfaces (cf. Sec. 3). While Bauer [2] and Raclet et al. [19] also investigated conjunction, they did so only for deterministic interfaces not containing internal computation.

The interface theory of [19] additionally considers a quotient operator, which is a kind of inverse to parallel composition. It may be used for decomposing concurrent specifications stepwise and for component reuse. We leave the definition of a quotient operator for MIA to future work as this will be technically very challenging in the nondeterministic input/output setting of MIA, in contrast to the deterministic theories of [19] and [9].

In summary, we achieve a richer interface theory than related work does. In MIA, one may specify non-deterministic behaviour, enforce outputs, express disjunctive must-transitions, abstract from internal computation, interpret compatibility optimistically or pessimistically, compose interfaces conjunctively and disjunctively, and support perspective-based specification in the pessimistic setting. A small example dealing with a communication protocol illustrates our advancements for both the optimistic and the pessimistic MIA variant (cf. Secs. 2.3 and 3.4). Finally, Sec. 4 contains our conclusions and suggestions for future work.

2 Modal Interface Automata: The Optimistic Setting

This section fixes a severe shortcoming of MIA [16], which it inherited from IOMTS [15], namely that the refinement preorder ignores the matching of must-transitions labelled with the internal action τ. The MIA variant below also permits (in contrast to [16]) general disjunctive must-transitions, thus enabling a natural definition of disjunction on interfaces.

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

(i) P is the set of states,
(ii) $A =_{\mathrm{df}} I \cup O$ with $I \cap O = \emptyset$ is the alphabet consisting of disjoint inputs and outputs, resp., and not containing the special, silent action τ,
(iii) $\longrightarrow \subseteq P \times (A \cup \{\tau\}) \times (\mathscr{P}_{fin}(P) \setminus \emptyset)$ is the *must-transition* relation (with $\mathscr{P}_{fin}(P)$ being the set of finite subsets of P),
(iv) $\dashrightarrow \subseteq P \times (A \cup \{\tau\}) \times P$ is the *may-transition* relation,

such that the following conditions hold for all $i \in I$ and $\alpha \in A \cup \{\tau\}$:

(a) $p \xrightarrow{i} P'$ and $p \xrightarrow{i} P''$ implies $P' = P''$ *(input determinism)*,
(b) $p \overset{i}{\dashrightarrow} p'$ implies $\exists P'.\, p \xrightarrow{i} P'$ and $p' \in P'$ *(input must)*,
(c) $p \xrightarrow{\alpha} P'$ implies $\forall p' \in P'.\, p \overset{\alpha}{\dashrightarrow} p'$ *(syntactic consistency)*.

Conds. (a)–(c) are adapted from the corresponding definition in [16]. Input determinism is required for the MIA-refinement preorder (see below) to be a precongruence for parallel

composition and conjunction; this condition is already imposed by IA, but note that, here, an input must-transition is disjunctive, thus allowing nondeterminism within a transition. The *input must* condition is natural in the presence of IA-inspired parallel composition: a may-input in an interface specification may simply be left out by a refining implementation, and thus increase the potential for errors rather than decrease it. Finally, syntactic consistency is natural and inherited from modal transition systems [14].

In the sequel, we identify a MIA $(P, I, O, \longrightarrow, \dashrightarrow)$ 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., write $A = I/O$ when highlighting inputs I and outputs O in an alphabet A, and define $\hat{a} =_{\mathrm{df}} a$ and $\hat{\tau} =_{\mathrm{df}} \varepsilon$ (the empty word). 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 resp. may-transition(s).

We now define *weak* must- and may-transition relations that abstract from transitions labelled by τ, as will be needed for MIA-refinement. This is the first definition of this kind which covers disjunctive must-transitions; it is also quite subtle as can be seen in Lemmas 4 and 11 below.

Definition 2 (Weak Transition Relations) *Weak* must-transition and *weak* may-transition relations $\stackrel{\hat{\omega}}{\Longrightarrow}$ and $\stackrel{\hat{\omega}}{=\!=\!\!\rightarrow}$, resp., are defined as the smallest relations satisfying $p \stackrel{\varepsilon}{\Longrightarrow} \{p\}$, $p \stackrel{\varepsilon}{=\!=\!\!\rightarrow} p$ and the following conditions, where $\hat{\omega} \in O \cup \{\varepsilon\}$ and $o \in O$:

(a) $p \stackrel{\hat{\omega}}{\Longrightarrow} P'$, $p' \in P'$ and $p' \stackrel{\tau}{\longrightarrow} P''$ implies $p \stackrel{\hat{\omega}}{\Longrightarrow} (P' \setminus \{p'\}) \cup P''$,
(b) $p \stackrel{\varepsilon}{\Longrightarrow} P' = \{p_1, \ldots, p_n\}$ and $\forall j.\, p_j \stackrel{o}{\longrightarrow} P_j$, implies $p \stackrel{o}{\Longrightarrow} \bigcup_{j=1}^{n} P_j$,
(c) $p \stackrel{\varepsilon}{=\!=\!\!\rightarrow} p'' \stackrel{\tau}{\dashrightarrow} p'$ implies $p \stackrel{\varepsilon}{=\!=\!\!\rightarrow} p'$,
(d) $p \stackrel{\varepsilon}{=\!=\!\!\rightarrow} p'' \stackrel{o}{\dashrightarrow} p''' \stackrel{\varepsilon}{=\!=\!\!\rightarrow} p'$ implies $p \stackrel{o}{=\!=\!\!\rightarrow} p'$.

The following extension of $\stackrel{\varepsilon}{\Longrightarrow}$ to sets of source states will also be useful and is defined as the smallest relation satisfying $P \stackrel{\varepsilon}{\Longrightarrow} P$ and

(a') $P \stackrel{\varepsilon}{\Longrightarrow} P'$, $p' \in P'$ and $p' \stackrel{\tau}{\longrightarrow} P''$ implies $P \stackrel{\varepsilon}{\Longrightarrow} (P' \setminus \{p'\}) \cup P''$.

An example of a weak disjunctive must-transition can be found in MIA P in Fig. 1. Here we have $p_0 \stackrel{o}{\Longrightarrow} \{p_5, p_4\}$ subsuming the transitions $p_0 \stackrel{\tau}{\longrightarrow} \{p_1, p_2\}$ due to Cond. (a), $p_1 \stackrel{o}{\longrightarrow} p_5$ and $p_2 \stackrel{o}{\longrightarrow} p_3$ due to Cond. (b), as well as $p_3 \stackrel{\tau}{\longrightarrow} p_4$ again due to Cond. (a). Our refinement relation which is based on the above definition and adapted from [15,16], is called *MIA-refinement*:

Definition 3 (MIA-Refinement) Let P, Q be MIAs with $I_P \supseteq I_Q$, $O_P \subseteq O_Q$ and $I_P \cap O_Q = \emptyset$. A Relation $\mathscr{R} \subseteq P \times Q$ is a *MIA-refinement relation* if for all $(p,q) \in \mathscr{R}$:

(i) $q \stackrel{i}{\longrightarrow} Q'$ implies $\exists P'.\, p \stackrel{i}{\longrightarrow} P'$ and $\forall p' \in P' \exists q' \in Q'.\, (p', q') \in \mathscr{R}$,
(ii) $q \stackrel{\omega}{\longrightarrow} Q'$ implies $\exists P'.\, p \stackrel{\hat{\omega}}{\Longrightarrow} P'$ and $\forall p' \in P' \exists q' \in Q'.\, (p', q') \in \mathscr{R}$,
(iii) $p \stackrel{\omega}{\dashrightarrow} p'$ implies $\exists q'.\, q \stackrel{\hat{\omega}}{=\!=\!\!\rightarrow} q'$ and $(p', q') \in \mathscr{R}$.

We write $p \sqsubseteq_{\smile} q$ and say that p *MIA-refines* q if there exists a MIA-refinement relation $\mathscr{R}$ such that $(p,q) \in \mathscr{R}$.

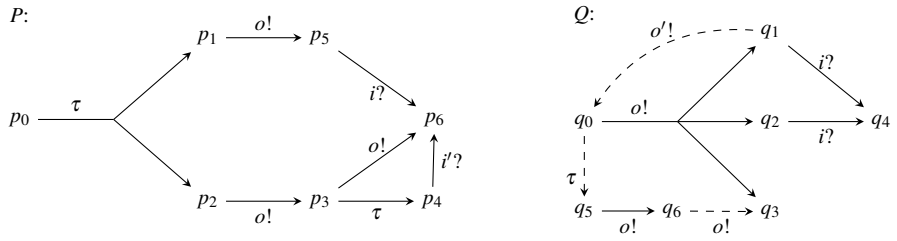

Fig. 1 MIA-refinement example: p_0 refines q_0 with input/output alphabets $P:\{i,i'\}/\{o\}$ and $Q:\{i\}/\{o,o'\}$.

One can immediately see that $\sqsubseteq$ is the largest MIA-refinement relation. The key difference to [16] is that our definition of MIA also allows τ-must-transitions, which must be considered in the refinement relation (Cond. (ii), for $\omega = \tau$). In addition, we now permit not only leading but also trailing τ-transitions when matching an output in Conds. (ii) and (iii); these were not allowed in [16] in the tradition of [1,15]. The reason why input must-transitions must be matched directly and not via a weak transition is due to MIA parallel composition, which we adopt from IA [1] and explain below.

Another difference to [16] is that we now permit the modification of a MIA's alphabet during refinement, along the lines of de Alfaro and Henzinger [1] and Chilton [10]. The three preconditions on the alphabets in Def. 3 mean that MIA-refinement allows one to extend the input alphabet and to restrict the output alphabet as far as action types are preserved, i.e., a dropped output action is not added as a new input action. Note that Cond. (ii) ensures that an output action o can only be removed from the alphabet if essentially no o-must-transitions are present. Also observe that the refining MIA may have additional input transitions with arbitrary subsequent behaviour, because input may-transitions are not considered in Cond. (iii). This will be crucial for establishing monotonicity wrt. parallel composition (see Thm. 12 below).

An example of a refinement is illustrated in Fig. 1, where it is easy to check that $\mathscr{R} = \{(p_0,q_0),(p_1,q_0),(p_2,q_5),(p_4,q_3),(p_5,q_1),(p_3,q_6),(p_6,q_4),(p_4,q_6),(p_6,q_3)\}$ is a MIA-refinement relation, i.e., $p_0 \sqsubseteq q_0$. It is important to note that the disjunctive must-transition $q_0 \xrightarrow{o} \{q_1,q_2,q_3\}$ must be matched by $p_0 \stackrel{o}{\Longrightarrow} \{p_4,p_5\}$ with $(p_4,q_3),(p_5,q_1) \in \mathscr{R}$, because $p_0 \stackrel{o}{\Longrightarrow} \{p_3,p_5\}$ is not a possible match due to $p_3 \stackrel{o}{\dashrightarrow}$.

This example also shows the intuition behind disjunctive must-transitions. They allow one to specify several alternatives for the behaviour after an action, from which at least one must be implemented. The disjunctive o-transition at state q_0 specifies the alternative behaviours at states q_1, q_2 and q_3. As a refinement of q_0, it is sufficient for state p_0 to implement only a subset of the behaviours described by q_1, q_2 and q_3 after action o, e.g., to implement q_1 by p_5 and q_3 by p_4 and not to implement q_2 at all. Thus, disjunctive transitions allow one to express choices of behaviours and a disjunction operator. In addition, they are necessary for being able to express conjunction on MIA. (See Sec. 2.2.)

As an aside, we wish to comment on another definition of refinement that may appear sensible at first glance, which is defined as MIA-refinement except that *new* inputs of the refining MIA are matched by "idling" as expressed by the following additional condition:

(iv) $p \xrightarrow{i} P'$ with $i \in I_P \setminus I_Q$ implies $\forall p' \in P'.\,(p',q) \in \mathscr{R}$.

However, the example in Fig. 8 (see Sec. 2.4) shows that the resulting refinement relation would not be transitive, since then $r_3 \sqsubseteq r_2 \sqsubseteq p$ but $r_3 \not\sqsubseteq p$.

Now that we have justified MIA-refinement intuitively, we focus our attention on proving that it is indeed a preorder. While reflexivity is trivial, transitivity requires that action types are preserved, i.e., $p \sqsubseteq_{\smile} q$ and $q \sqsubseteq_{\smile} r$ implies $p \sqsubseteq_{\smile} r$ if $I_P \cap O_R = \emptyset$. However, establishing transitivity is far from trivial due to the consideration of *weak* disjunctive must-transitions. We start off with a key lemma:

Lemma 4 *Consider arbitrary MIAs P and Q.*

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

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

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

Proof We only prove Part (a) here and postpone the proofs of the other parts to App. A. The proof of Part (a) proceeds 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, $p \stackrel{\hat{\omega}}{\Longrightarrow} \overline{P}' \subseteq (P' \setminus \{p'\}) \cup P'''$ for some $\overline{P}'$ such that $P''' \subseteq \overline{P}'$. Applying Def. 2(a) to $p \stackrel{\hat{\omega}}{\Longrightarrow} \overline{P}'$ and $\hat{p} \stackrel{\tau}{\longrightarrow} \hat{P}$ (observe $\hat{p} \in \overline{P}'$), we get $p \stackrel{\hat{\omega}}{\Longrightarrow} \overline{P}$ 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 $P''' \subseteq \overline{P}'$. □

This lemma allows us to replace the strong disjunctive must-transition in the premise of Def. 3(ii) by a weak one:

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

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

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

Proof The proof of Part (b) is standard; thus, we focus on proving Part (a) concerning weak disjunctive transitions. We proceed by induction on the definition of $q \stackrel{\hat{\omega}}{\Longrightarrow} Q'$:

- Let $\omega = \tau$ and $Q' = \{q\}$. Then, we choose $P' =_{\text{df}} \{p\}$.
- Let $q \stackrel{\hat{\omega}}{\Longrightarrow} Q'$ due to Def. 2(a), i.e., we have $q \stackrel{\hat{\omega}}{\Longrightarrow} Q'''$, $q'' \in Q'''$, $q'' \stackrel{\tau}{\longrightarrow} Q''$ and $Q' = (Q''' \setminus \{q''\}) \cup Q''$. By induction hypothesis, there exists some P''' with $p \stackrel{\hat{\omega}}{\Longrightarrow} P'''$ and $\forall p''' \in P'''\, \exists q''' \in Q'''.\, (p''',q''') \in \mathscr{R}$. Further, for each $p'' \in P'''$ with $(p'',q'') \in \mathscr{R}$, there exists a P'' with $p'' \stackrel{\varepsilon}{\Longrightarrow} P''$ 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 all these P''. By Lemma 4(b), we conclude $p \stackrel{\hat{\omega}}{\Longrightarrow} P' \subseteq (P''' \setminus \{p'' \in P'' \mid (p'',q'') \in \mathscr{R}\}) \cup \hat{P}$. 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(b), 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 a 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 Lemma 4(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 $\sqsubseteq_{\smile}$ is a preorder, where transitivity is understood as: $p \sqsubseteq_{\smile} q$ and $q \sqsubseteq_{\smile} r$ implies $p \sqsubseteq_{\smile} r$ if $I_P \cap O_R = \emptyset$.*

Proof Reflexivity 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 [18]. □

2.1 Parallel Composition

We define a parallel composition operator $|$ on MIA in analogy to IA [1, 15] in two stages: first a standard product $\otimes$ between two MIAs is introduced, where common actions are synchronized and hidden. Then, error states are identified, and all states are pruned from which reaching an error state is unavoidable in some implementation.

Definition 7 (Parallel Product) MIAs P_1 and P_2 are *composable* if $A_1 \cap A_2 = (I_1 \cap O_2) \cup (O_1 \cap I_2)$. For such MIAs we define the *product* $P_1 \otimes P_2 = (P_1 \times P_2, I, O, \longrightarrow, \dashrightarrow)$, where $I = (I_1 \cup I_2) \setminus (O_1 \cup O_2)$ and $O = (O_1 \cup O_2) \setminus (I_1 \cup I_2)$ and where $\longrightarrow$ and $\dashrightarrow$ are defined as follows:

(Must1)	$(p_1, p_2) \xrightarrow{\alpha} P_1' \times \{p_2\}$	if	$p_1 \xrightarrow{\alpha} P_1'$ and $\alpha \notin A_2$
(Must2)	$(p_1, p_2) \xrightarrow{\alpha} \{p_1\} \times P_2'$	if	$p_2 \xrightarrow{\alpha} P_2'$ and $\alpha \notin A_1$
(Must3)	$(p_1, p_2) \xrightarrow{\tau} P_1' \times P_2'$	if	$p_1 \xrightarrow{a} P_1'$ and $p_2 \xrightarrow{a} P_2'$ for some a
(May1)	$(p_1, p_2) \overset{\alpha}{\dashrightarrow} (p_1', p_2)$	if	$p_1 \overset{\alpha}{\dashrightarrow} p_1'$ and $\alpha \notin A_2$
(May2)	$(p_1, p_2) \overset{\alpha}{\dashrightarrow} (p_1, p_2')$	if	$p_2 \overset{\alpha}{\dashrightarrow} p_2'$ and $\alpha \notin A_1$
(May3)	$(p_1, p_2) \overset{\tau}{\dashrightarrow} (p_1', p_2')$	if	$p_1 \overset{a}{\dashrightarrow} p_1'$ and $p_2 \overset{a}{\dashrightarrow} p_2'$ for some a.

The difference to the version of MIA in [16] is that we now have τ-must-transitions; in particular, this has led us to introduce Rule (Must3).

Definition 8 (Parallel Composition) Given a parallel product $P_1 \otimes P_2$, a state (p_1, p_2) is an *error state* if there is some $a \in A_1 \cap A_2$ such that (a) $a \in O_1$, $p_1 \overset{a}{\dashrightarrow}$ and $p_2 \not\xrightarrow{a}$, or (b) $a \in O_2$, $p_2 \overset{a}{\dashrightarrow}$ and $p_1 \not\xrightarrow{a}$. We define the set $E \subseteq P_1 \times P_2$ of *incompatible* states as the least set such that $(p_1, p_2) \in E$ if (i) (p_1, p_2) is an error state or (ii) $(p_1, p_2) \overset{\omega}{\dashrightarrow} (p_1', p_2')$ and $(p_1', p_2') \in E$.

The *parallel composition* $P_1|P_2$ of P_1 and P_2 is now obtained from $P_1 \otimes P_2$ by *pruning*, namely removing all states in E and every transition that involves such states as its source, its target or one of its targets; all may-transitions underlying a removed must-transition are deleted, too. If $(p_1, p_2) \in P_1|P_2$, we write $p_1|p_2$ and call p_1 and p_2 *compatible*.

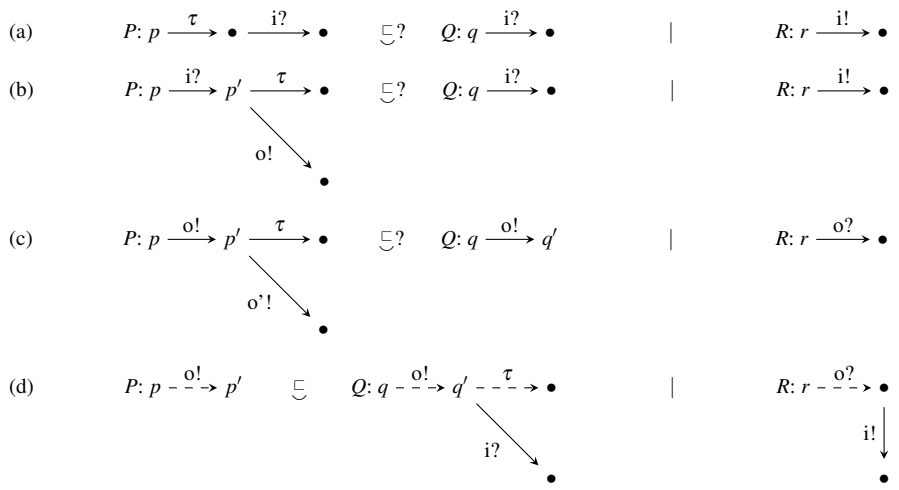

Fig. 2 Matching inputs with (a) leading and (b) trailing τ-transitions result in a compositionality bug. (c) The respective problem does not exist for outputs. (d) Trailing τ are unproblematic as well.

It is easy to see that parallel products and parallel compositions are well-defined MIAs and that the parallel composition operator is commutative and associative. Strictly speaking, associativity holds only if all components are mutually composable. To see what might go wrong, consider P, Q and R such that a is an input for P and R and an output for Q. While in $(P|Q)|R$ the former two MIAs synchronize on a, which is hidden as a result, the latter two MIAs synchronize on a in $P|(Q|R)$. In practice, this issue can be circumvented by a suitable renaming of actions; in our example, one could simply rename a to a fresh action b in P and Q.

In addition and as we will show below, MIA-refinement is compositional wrt. parallel composition, i.e., $\sqsubseteq$ is a precongruence. It is this desired property that requires us in Def. 3 to match input must-transitions strongly and to ignore input may-transitions when matching, both of which we discuss in the following.

To see the former, consider Fig. 2(a)–(c) with input/output alphabets $A_P =_{\text{df}} A_Q =_{\text{df}} \{i\}/\{o,o'\}$ and $A_R =_{\text{df}} \{o\}/\{i\}$. Firstly, leading τ-transitions are forbidden as one can see in Fig. 2(a): p should not refine q because q and r are compatible while p and r are not since (p,r) is an error. Therefore, one must not be able to match a transition $\xrightarrow{i}$ by a transition sequence $\left(\xrightarrow{\tau}\right)^+ \xrightarrow{i}$, unless the notion of error state originating from IA [1] is changed, as is done in [4]. Secondly, allowing trailing τ-transitions for P in Cond. (i) of Def. 3 would lead to a compositionality problem as illustrated in Fig. 2(b): p would refine q but, while q and r are compatible, p and r are not since they reach an error state after synchronizing on i. This problem does not occur with outputs as we can see in Fig. 2(c): p does not refine q since the underlying o-may-transition requires one to match p' with q' by Cond. (iii) of Def. 3. Fig. 2(d) illustrates that our trailing τ-transitions in Def. 3(iii) are unproblematic as well; here, neither p nor q is compatible with r.

To see why input may-transitions are ignored when matching, observe that prescribing their matching as in Def. 3(iii) for output may-transitions would also yield a compositionality defect. For example, for the MIAs in Fig. 3 with alphabets $A_P =_{\text{df}} \{o\}/\emptyset$ and $A_Q =_{\text{df}} A_{Q'} =_{\text{df}} \{i\}/\{o\}$, we would have $q' \sqsubseteq q$ but $p|q' \not\sqsubseteq p|q$. As an aside, observe that

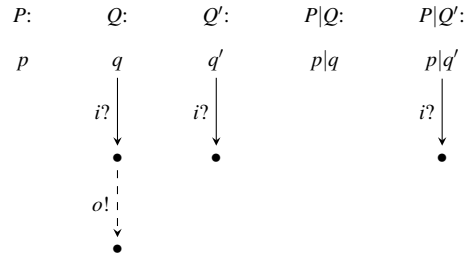

Fig. 3 Necessity of ignoring input may-transitions when matching. Here, p and $p|q$ are deadlocked processes, i.e., they do not have an outgoing transition.

MIA-refinement is powerful enough to model STG-bisimulation [21] *with* internal actions by considering only must-transitions; in that setting, it is practically important to allow unspecified inputs in an implementation.

We are now going to prove compositionality of MIA-refinement wrt. parallel composition, which requires us to establish a couple of auxiliary properties regarding the preservation of composability and consistency under refinement, as well as a property of weak must-transitions.

Lemma 9 (Composability) *Let P_1, P_2 and Q be MIAs with $p_1 \in P_1$, $q \in Q$ and $p_1 \sqsubseteq q$ such that Q and P_2 are composable and $A_1 \cap A_2 \subseteq A_Q \cap A_2$. Then, P_1 and P_2 are composable, $I_Q \cap O_2 = I_1 \cap O_2$ and $O_Q \cap I_2 \supseteq O_1 \cap I_2$.*

The intuition behind $A_1 \cap A_2 \subseteq A_Q \cap A_2$ is that no new synchronizations may be introduced, while existing synchronizations may be removed.

Proof Since Q and P_2 are composable we have $(I_1 \cap I_2) \cup (I_1 \cap O_2) \cup (O_1 \cap I_2) \cup (O_1 \cap O_2) = A_1 \cap A_2 \subseteq A_Q \cap A_2 = (I_Q \cap O_2) \cup (O_Q \cap I_2)$; in particular, $(I_1 \cap I_2) \cup (I_1 \cap O_2) \subseteq (I_Q \cap O_2) \cup (O_Q \cap I_2)$. Since the first intersection is contained in I_1 and $I_1 \cap O_Q = \emptyset$ by preservation of action types, we get $(I_1 \cap I_2) \cup (I_1 \cap O_2) \subseteq I_Q \cap O_2 \subseteq I_1 \cap O_2$. Since I_2 and O_2 are disjoint, we conclude $I_1 \cap I_2 = \emptyset$ and, as a first consequence, $I_Q \cap O_2 = I_1 \cap O_2$. Since $O_1 \subseteq O_Q$, we also have $O_1 \cap O_2 = \emptyset$ by composability of Q and P_2. Therefore, $A_1 \cap A_2 = (I_1 \cap O_2) \cup (O_1 \cap I_2)$. Finally, $O_Q \cap I_2 \supseteq O_1 \cap I_2$ is obvious, as $O_1 \subseteq O_Q$. □

Lemma 10 (Consistency) *Let E_P be the E-set of $P_1 \otimes P_2$ and E_Q be the one of $Q \otimes P_2$, for MIAs P_1, P_2 and Q such that Q and P_2 are composable and $A_1 \cap A_2 \subseteq A_Q \cap A_2$. Further, let $p_1 \in P_1$, $p_2 \in P_2$ and $q \in Q$ such that $p_1 \sqsubseteq q$. Then, $(p_1, p_2) \in E_P$ implies $(q, p_2) \in E_Q$.*

Proof The proof is by induction on the length of a path from (p_1, p_2) to an error state of $P_1 \otimes P_2$:

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

- Let $p_1 \overset{a}{\dashrightarrow}_{P_1}$ with $a \in O_1 \cap I_2 \subseteq O_Q \cap I_2$ and $p_2 \overset{a}{\not\longrightarrow}_{P_2}$. Then, for some q', we have $q \overset{\varepsilon}{=\!=\!\twoheadrightarrow}_Q q' \overset{a}{\dashrightarrow}_Q$ by $p_1 \sqsubseteq q$; hence, $(q, p_2) \overset{\varepsilon}{=\!=\!\twoheadrightarrow} (q', p_2) \in E_Q$ and $(q, p_2) \in E_Q$ as well.
- Let $p_2 \overset{a}{\dashrightarrow}_{P_2}$ with $a \in O_2 \cap I_1$ and $p_1 \overset{a}{\not\longrightarrow}_{P_1}$. If $q \overset{a}{\longrightarrow}_Q$, we have a contradiction to $p_1 \sqsubseteq q$; otherwise, (q, p_2) is an error state since $a \in I_1 \cap O_2 = I_Q \cap O_2$ by Lemma 9.

(Step) For a shortest path from (p_1,p_2) to an error state, consider the first transition $(p_1,p_2) \overset{\omega}{\dashrightarrow} (p_1',p_2') \in E_P$ with $\omega \in O \cup \{\tau\}$. The transition is due to either Rule (May1), (May2) or (May3). In all cases we show $p_1' \sqsubseteq q'$ for some $q' \in Q$, which implies $(q',p_2') \in E_Q$ by induction hypothesis.

(May1) $p_1 \overset{\omega}{\dashrightarrow}_{P_1} p_1'$, $p_2 = p_2'$, $\omega \notin A_2$, and $\omega \in O_1 \cup \{\tau\}$ by $\omega \in O \cup \{\tau\}$. Due to $p_1 \sqsubseteq q$ and Def. 3(iii), there is a q' such that $q \overset{\hat{\omega}}{\Longrightarrow}_Q q'$ and $p_1' \sqsubseteq q'$, and $(q,p_2) \overset{\hat{\omega}}{\Longrightarrow} (q',p_2)$ by applications of Rule (May1). By induction hypothesis, $(q',p_2) \in E_Q$ and, therefore, $(q,p_2) \in E_Q$.

(May2) $p_1 = p_1'$, $p_2 \overset{\omega}{\dashrightarrow}_{P_2} p_2'$ and $\omega \notin A_1$. Since $\omega \notin I_1$ implies $\omega \notin I_Q$ and since $\omega \notin O_Q$ by composability, we can apply Rule (May2) again and obtain $(q,p_2) \overset{\omega}{\dashrightarrow} (q,p_2')$, so that $(q,p_2') \in E_Q$ by induction hypothesis. Hence, $(q,p_2) \in E_Q$, too.

(May3) $\omega = \tau$, and we distinguish the following cases:

- $p_1 \overset{a}{\dashrightarrow}_{P_1} p_1'$ with $a \in O_1$, and $p_2 \overset{a}{\dashrightarrow}_{P_2} p_2'$ with $a \in I_2$. By $p_1 \sqsubseteq q$ we have $q \overset{\varepsilon}{\Longrightarrow}_Q q'' \overset{a}{\dashrightarrow}_Q q''' \overset{\varepsilon}{\Longrightarrow}_Q q'$ for some q',q'',q''' with $p_1' \sqsubseteq q'$. Therefore, we get $(q,p_2) \overset{\varepsilon}{\Longrightarrow} (q'',p_2) \overset{\tau}{\dashrightarrow} (q''',p_2') \overset{\varepsilon}{\Longrightarrow} (q',p_2')$ via Rules (May1) and (May3). By induction hypothesis, $(q',p_2') \in E_Q$ and, hence, $(q,p_2) \in E_Q$, too.
- $p_1 \overset{a}{\dashrightarrow}_{P_1} p_1'$ with $a \in I_1$, and $p_2 \overset{a}{\dashrightarrow}_{P_2} p_2'$ with $a \in O_2$. Note that $a \in I_Q$ since $I_1 \cap O_2 = I_Q \cap O_2$ by Lemma 9. If $q \not\overset{a}{\dashrightarrow}_Q$, then $q \not\overset{a}{\longrightarrow}_Q$ by syntactic consistency and (q,p_2) is thus an error state. If $q \overset{a}{\dashrightarrow}_Q$, then there exist unique $p_1 \overset{a}{\longrightarrow}_{P_1} P'$ and $q \overset{a}{\longrightarrow}_Q Q'$ by input determinism. We have $p_1' \in P'$ by Def. 1(b) and $\exists q' \in Q'.\, p_1' \sqsubseteq q'$ since $p_1 \sqsubseteq q$. Hence, $q \overset{a}{\dashrightarrow}_Q q'$ by syntactic consistency and $(q,p_2) \overset{\tau}{\dashrightarrow} (q',p_2')$ due to Rule (May3). By induction hypothesis, $(q',p_2') \in E_Q$ and, therefore, $(q,p_2) \in E_Q$. □

Lemma 11 (Weak Must-Transitions) *Let P and Q be composable MIAs. If $p \overset{a}{\Longrightarrow}_P P'$ and $q \overset{a}{\longrightarrow}_Q Q'$ for some $a \in (O_P \cap I_Q) \cup (I_P \cap O_Q)$, then $(p,q) \overset{\varepsilon}{\Longrightarrow} R$ in $P \otimes Q$ with $R \subseteq P' \times Q'$.*

Proof Consider $P'' \subseteq P$ and P''' with (i) $p \overset{\varepsilon}{\Longrightarrow}_P P'' = \{p_1,\ldots,p_n\}$ and $\forall i.\, p_i \overset{a}{\longrightarrow}_P P_i$ such that $P''' = \bigcup_{i=1}^n P_i$ and (ii) P' is obtained from P''' by repeated application of Def. 2(a) with $\omega = \tau$. 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 Rule (Must1). Now, according to the definition of $\overset{\varepsilon}{\Longrightarrow}$, one can replace $(p_1,q),\ldots,(p_n,q)$ in $P'' \times \{q\}$ one after the other by the elements of $P_1 \times Q',\ldots,P_n \times Q'$ such that we finally get $(p,q) \overset{\varepsilon}{\Longrightarrow} R'$ where $R' \subseteq P''' \times Q'$. Note that R' can be a proper subset of $P''' \times Q$, 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 (i) $P''' \times Q'$ and (ii) R'. In Case (i), all $(\overline{p},q')$ with $q' \in Q'$ are replaced by the elements of $\{\overline{p}\} \times Q'$. The same is done in Case (ii), provided there is some $(\overline{p},q')$; if not, no replacement occurs. These transformations preserve the inclusion, so finally $R \subseteq P' \times Q'$. □

Fig. 4 shows that, in general, $R \neq P' \times Q'$; here, $1 \overset{a!}{\Longrightarrow}_P \{2,3,4,5\}$ and $0 \overset{a?}{\Longrightarrow}_Q 0$, but not $1|0 \overset{\varepsilon}{\Longrightarrow} \{2,3,4,5\} \times \{0\}$. The sets R with maximal cardinality satisfying $1|0 \overset{\varepsilon}{\Longrightarrow} R$ are $\{2,4,5\} \times \{0\}$ and $\{3,4,5\} \times \{0\}$.

Theorem 12 (Compositionality of Parallel Composition) *Let P_1, P_2, and Q be MIAs with $p_1 \in P_1$, $p_2 \in P_2$, $q \in Q$ and $p_1 \sqsubseteq q$, as well as $A_1 \cap A_2 \subseteq A_Q \cap A_2$. Assume that Q and P_2 are composable; then:*

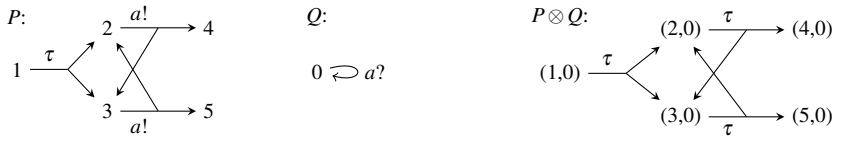

Fig. 4 Example showing that set R in Lemma 11 is not always the full set $P' \times Q'$.

(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 $p_1|p_2 \sqsubseteq_{\smile} q|p_2$.

Proof Part (a) follows from Lemma 9. Regarding Part (b), the first claim is implied by Lemma 10 above. To establish the second claim, note that the alphabet inclusion preconditions for $p_1|p_2 \sqsubseteq_{\smile} q|p_2$ follow from the respective preconditions for $p_1 \sqsubseteq_{\smile} q$. In addition, by simple set algebra and preservation of action types for P_1 and Q, we have

$$\begin{aligned} I_{P_1|P_2} \cap O_{Q|P_2} &= ((I_1 \cup I_2) \setminus (O_1 \cup O_2)) \cap ((O_Q \cup O_2) \setminus (I_Q \cup I_2)) \\ &\overset{(*)}{=} (I_1 \setminus (O_1 \cup O_2)) \cap (O_Q \setminus (I_Q \cup I_2)) \\ &\subseteq I_1 \cap O_Q \\ &= \emptyset . \end{aligned}$$

For equality $(*)$ observe that I_2 can be omitted from the left operand of $\cap$ since it is excluded in the right operand, and vice versa for O_2. We now prove that

$$\mathscr{R} =_{\text{df}} \{(p_1|p_2, q|p_2) \mid p_1 \sqsubseteq_{\smile} q,\ p_1, p_2 \text{ as well as } q, p_2 \text{ compatible}\}$$

is a MIA-refinement relation, for which we let $(p_1|p_2, q|p_2) \in \mathscr{R}$ and check the conditions of Def. 3. In the following, E_P stands for the E-set of $P_1 \otimes P_2$ and E_Q for the one of $Q \otimes P_2$, as in Lemma 10.

(i) Let $q|p_2 \xrightarrow{i} \overline{Q}$ with $\overline{Q} \cap E_Q = \emptyset$ due to either Rule (Must1) or (Must2).
  (Must1) $q \xrightarrow{i}_Q Q'$ and $\overline{Q} = Q' \times \{p_2\}$. Then, by $p_1 \sqsubseteq_{\smile} q$, there is a $P_1' \subseteq P_1$ such that $p_1 \xrightarrow{i}_{P_1} P_1'$ and $\forall p_1' \in P_1' \, \exists q' \in Q' . \, p_1' \sqsubseteq_{\smile} q'$. Now, $(p_1, p_2) \xrightarrow{i} P_1' \times \{p_2\}$ according to Rule (Must1) and as $i \notin A_2$. For $p_1' \in P_1'$, we have a suitable $q' \in Q'$; moreover, $(p_1', p_2) \notin E_P$ since $(q', p_2) \notin E_Q$ and due to Lemma 10 that is applicable by the theorem's assumptions. Thus, for the arbitrary $p_1'|p_2$, we have $(p_1'|p_2, q'|p_2) \in \mathscr{R}$.
  (Must2) $p_2 \xrightarrow{i}_{P_2} P_2'$ and $\overline{Q} = \{q\} \times P_2'$. Then, $(p_1, p_2) \xrightarrow{i} \overline{P} = \{p_1\} \times P_2'$ according to Rule (Must2) and since $i \notin A_Q \cap A_2 \supseteq A_1 \cap A_2$. For $(p_1, p_2') \in \overline{P}$, we get $(p_1, p_2') \notin E_P$ because $(q, p_2') \notin E_Q$ and due to Lemma 10. Thus, $p_1|p_2 \xrightarrow{i} \overline{P}$ and, for $p_1|p_2' \in \overline{P}$, we have $q|p_2' \in \overline{Q}$ with $(p_1|p_2', q|p_2') \in \mathscr{R}$.

(ii) Let $q|p_2 \xrightarrow{\omega} \overline{Q}$ and $\overline{Q} \cap E_Q = \emptyset$ due to either Rule (Must1), (Must2) or (Must3):
  (Must1) $q \xrightarrow{\omega}_Q Q'$ and $\overline{Q} = Q' \times \{p_2\}$. Then, by $p_1 \sqsubseteq_{\smile} q$, there exists $P_1' \subseteq P_1$ such that $p_1 \xRightarrow{\hat{\omega}}_{P_1} P_1'$ and $\forall p_1' \in P_1' \, \exists q' \in Q' . \, p_1' \sqsubseteq_{\smile} q'$. Now, $(p_1, p_2) \xRightarrow{\hat{\omega}} P_1' \times \{p_2\}$ according to Rule (Must1) 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 $q' \in Q'$ such that, for the arbitrary $p_1'|p_2$, we also have $(p_1'|p_2, q'|q_2) \in \mathscr{R}$.

(Must2) $p_2 \xrightarrow{\omega}_{P_2} P_2'$ and $\overline{Q} = \{q\} \times P_2'$. In this case we obtain that $(p_1,p_2) \xrightarrow{\omega} \overline{P} = \{p_1\} \times P_2'$ by Rule (Must2) and since $\omega \notin A_Q \cap A_2 \supseteq A_1 \cap A_2$. For $(p_1,p_2') \in \overline{P}$ we get $(p_1,p_2') \notin E_P$ since $(q,p_2') \notin E_Q$ and due to Lemma 10. Thus, $p_1|p_2 \xrightarrow{\omega} \overline{P}$ and therefore also $p_1|p_2 \stackrel{\hat{\omega}}{\Longrightarrow} \overline{P}$. Moreover, for $(p_1,p_2') \in \overline{P}$, we have $(p_1|p_2', q|p_2') \in \mathscr{R}$.

(Must3) $\omega = \tau$, and we distinguish the following cases:

- $q \xrightarrow{a}_Q Q'$ with $a \in O_Q$, $p_2 \xrightarrow{a}_{P_2} P_2'$ with $a \in I_2$, and $\overline{Q} = Q' \times P_2'$. By $p_1 \sqsubseteq q$, there exists some P_1' with $p_1 \stackrel{a}{\Longrightarrow}_{P_1} P_1'$ such that $\forall p_1' \in P_1'\, \exists q' \in Q'.\, p_1' \sqsubseteq q'$. Now, $(p_1,p_2) \stackrel{\varepsilon}{\Longrightarrow} R \subseteq P_1' \times P_2'$ by Lemma 11 and, as in Case (ii)(Must1) above, all pairs along this weak transition are compatible. Hence, for all $p_1'|p_2' \in R$, we have some $q' \in Q'$ such that $(p_1'|p_2', q'|p_2') \in \mathscr{R}$.
- $q \xrightarrow{a}_Q Q'$ with $a \in I_Q$, $p_2 \xrightarrow{a}_{P_2} P_2'$ with $a \in O_2$, and $\overline{Q} = Q' \times P_2'$. By $p_1 \sqsubseteq q$, there exists some P_1' with $p_1 \xrightarrow{a}_{P_1} P_1'$ such that $\forall p_1' \in P_1'\, \exists q' \in Q'.\, p_1' \sqsubseteq q'$. Now, $(p_1,p_2) \xrightarrow{\tau} P_1' \times P_2'$ by Rule (Must3), whence $(p_1,p_2) \stackrel{\varepsilon}{\Longrightarrow} P_1' \times P_2'$. Consider some $(p_1',p_2') \in P_1' \times P_2'$ and some $q' \in Q'$ with $p_1' \sqsubseteq q'$. Since $q'|p_2' \in \overline{Q}$ is not in E_Q, we also have $(p_1',p_2') \notin E_P$ due to Lemma 10. Thus, $(p_1'|p_2', q'|p_2') \in \mathscr{R}$ for all $p_1'|p_2' \in P_1' \times P_2'$.

(iii) Let $p_1|p_2 \stackrel{\omega}{\dashrightarrow} p_1'|p_2' \notin E_P$, which is due to one of the Rules (May1), (May2) or (May3):

(May1) $p_2' = p_2$ and $p_1 \stackrel{\omega}{\dashrightarrow}_{P_1} p_1'$. By $p_1 \sqsubseteq q$, we have $q \stackrel{\hat{\omega}}{=\!=\!\Rightarrow}_Q q'$ for some q' such that $p_1' \sqsubseteq q'$. Hence, $(q,p_2) \stackrel{\hat{\omega}}{=\!=\!\Rightarrow} (q',p_2)$ by repeated application of Rule (May1) and since $\omega \notin A_2$. If any state on this weak transition were in E_Q, then also $(q,p_2) \in E_Q$, which contradicts $(p_1|p_2, q|p_2) \in \mathscr{R}$. Thus, $q|p_2 \stackrel{\hat{\omega}}{=\!=\!\Rightarrow} q'|p_2$ with $(p_1'|p_2, q'|p_2) \in \mathscr{R}$.

(May2) $p_1' = p_1$ and $p_2 \stackrel{\omega}{\dashrightarrow}_{P_2} p_2'$. Then, $(q,p_2) \stackrel{\omega}{\dashrightarrow} (q,p_2')$ by Rule (May2) and since $I_1 \supseteq I_Q$ due to $p_1 \sqsubseteq q$. If the latter state (q,p_2') were in E_Q, then also the former state (q,p_2). Therefore, we have $q|p_2 \stackrel{\omega}{\dashrightarrow} q|p_2'$ and, moreover, $(p_1|p_2', q|p_2') \in \mathscr{R}$.

(May3) $\omega = \tau$, $p_1 \stackrel{a}{\dashrightarrow}_{P_1} p_1'$ and $p_2 \stackrel{a}{\dashrightarrow}_{P_2} p_2'$ for some action a.

- $a \in O_1 \cap I_2$: Due to $p_1 \sqsubseteq q$, we get $q \stackrel{\varepsilon}{=\!=\!\Rightarrow}_Q q'' \stackrel{a}{\dashrightarrow}_Q q''' \stackrel{\varepsilon}{=\!=\!\Rightarrow} q'$ for q', q'', q''' such that $p_1' \sqsubseteq q'$. Now, we obtain $(q,p_2) \stackrel{\varepsilon}{=\!=\!\Rightarrow} (q'',p_2) \stackrel{\tau}{\dashrightarrow} (q''',p_2') \stackrel{\varepsilon}{=\!=\!\Rightarrow} (q',p_2')$ by Rules (May1) and (May3). As in Case (May1) above, $q|p_2 \stackrel{\varepsilon}{=\!=\!\Rightarrow} q'|p_2'$ and $(p_1'|p_2', q'|p_2') \in \mathscr{R}$.
- $a \in I_1 \cap O_2$: Note that $a \in I_Q$ since $I_1 \cap O_2 = I_Q \cap O_2$ by Lemma 9. If $q \not\xrightarrow{a}_Q$, then (q,p_2) would be an error state, which is a contradiction. Therefore, $q \stackrel{a}{\dashrightarrow}_Q$ and, by Def. 1(b), there exist unique $p_1 \xrightarrow{a}_{P_1} P_1'$ and $q \xrightarrow{a}_Q Q'$ by input-determinism and syntactic consistency. We have $p_1' \in P_1'$ and $\exists q' \in Q'.\, p_1' \sqsubseteq q'$ since $p_1 \sqsubseteq q$. Hence, $(q,p_2) \stackrel{\tau}{\dashrightarrow} (q',p_2')$ by Rule (May3), and (q',p_2') cannot be in E_Q by reasoning as above. Thus, $q|p_2 \stackrel{\tau}{\dashrightarrow} q'|p_2'$ with $(p_1'|p_2', q'|p_2') \in \mathscr{R}$. □

2.2 Conjunction & Disjunction

Conjunction will be defined for MIAs with potentially different alphabets; naturally, we demand that an input of one MIA cannot be in the output alphabet of the other. We proceed in two stages, similarly to parallel composition. State pairs can be logically inconsistent due to unsatisfiable must-transitions (cf. Def. 14 (F1) and (F2)) and are then removed incrementally

in the second stage. The following definition coincides with the one of our previous version of MIA [16], but now considers τ-must-transitions (cf. Rules (OMust1) and (OMust2)) and allows conjuncts with different alphabets.

Definition 13 (Conjunctive Product) Let $(P, I_P, O_P, \longrightarrow_P, \dashrightarrow_P)$, $(Q, I_Q, O_Q, \longrightarrow_Q, \dashrightarrow_Q)$ be MIAs with $(I_P \cap O_Q) = \emptyset = (O_P \cap I_Q)$ and disjoint state sets. The conjunctive product $P\&Q =_{\mathrm{df}} ((P \times Q) \cup P \cup Q, I, O, \longrightarrow, \dashrightarrow)$, where $I = I_P \cup I_Q$ and $O = O_P \cap O_Q$, inherits the transitions of P and Q and has additional transitions as follows:

(OMust1)	$(p,q) \xrightarrow{\omega} \{(p',q') \mid p' \in P', q \overset{\hat{\omega}}{=\!=\!\!\twoheadrightarrow}_Q q'\}$	if $p \xrightarrow{\omega}_P P'$ and $q \overset{\hat{\omega}}{=\!=\!\!\twoheadrightarrow}_Q$
(OMust2)	$(p,q) \xrightarrow{\omega} \{(p',q') \mid p \overset{\hat{\omega}}{=\!=\!\!\twoheadrightarrow}_P p', q' \in Q'\}$	if $p \overset{\hat{\omega}}{=\!=\!\!\twoheadrightarrow}_P$ and $q \xrightarrow{\omega}_Q Q'$
(IMust1)	$(p,q) \xrightarrow{i} P'$	if $p \xrightarrow{i}_P P'$ and $q \not\xrightarrow{i}_Q$
(IMust2)	$(p,q) \xrightarrow{i} Q'$	if $p \not\xrightarrow{i}_P$ and $q \xrightarrow{i}_Q Q'$
(IMust3)	$(p,q) \xrightarrow{i} P' \times Q'$	if $p \xrightarrow{i}_P P'$ and $q \xrightarrow{i}_Q Q'$
(May1)	$(p,q) \overset{\tau}{\dashrightarrow} (p',q)$	if $p \overset{\tau}{=\!=\!\!\twoheadrightarrow}_P p'$
(May2)	$(p,q) \overset{\tau}{\dashrightarrow} (p,q')$	if $q \overset{\tau}{=\!=\!\!\twoheadrightarrow}_Q q'$
(May3)	$(p,q) \overset{\omega}{\dashrightarrow} (p',q')$	if $p \overset{\omega}{=\!=\!\!\twoheadrightarrow}_P p'$ and $q \overset{\omega}{=\!=\!\!\twoheadrightarrow}_Q q'$
(IMay1)	$(p,q) \overset{i}{\dashrightarrow} p'$	if $p \overset{i}{\dashrightarrow}_P p'$ and $q \not\overset{j}{\dashrightarrow}_Q$
(IMay2)	$(p,q) \overset{i}{\dashrightarrow} q'$	if $p \not\overset{j}{\dashrightarrow}_P$ and $q \overset{i}{\dashrightarrow}_Q q'$
(IMay3)	$(p,q) \overset{i}{\dashrightarrow} (p',q')$	if $p \overset{i}{\dashrightarrow}_P p'$ and $q \overset{i}{\dashrightarrow}_Q q'$

Observe that the conjunctive product is inherently different from the parallel product, as can be seen from some 'unusual' rules that define single transitions on the basis of weak transitions (Rules (OMust) and (May)) and synchronize on τ-transitions (Rule (May3)). These will be justified by Thm. 15 below; see also [16] for examples demonstrating that the above rules cannot be simplified. Regarding Rules (IMust1) and (IMust2), observe that inputs are always implicitly allowed in MIA; for example, in Rule (IMust1), q does not impose any restrictions on the behaviour after input i and is therefore dropped from the target state. Finally, Rules (May3) to (IMay3) guarantee syntactic consistency.

As an aside, note that in the (OMust) rules and in similar cases below the target set of the defined transition is finite (cf. Def. 1). If one wishes to deal with infinite target sets in MIA, one has to modify the definition of $\overset{\varepsilon}{\Longrightarrow}$ by allowing the simultaneous replacement of several p' by suitable P' in Def. 2(a); this would make the latter definition more complicated and Lemma 11 superfluous.

Definition 14 (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:

(F1)	$\exists. o \in O_P.\ p \xrightarrow{o}_P$ and $q \not\overset{\rho}{=\!=\!\!\twoheadrightarrow}_Q$	implies	$(p,q) \in F$
(F2)	$\exists. o \in O_Q.\ p \not\overset{\rho}{=\!=\!\!\twoheadrightarrow}_P$ and $q \xrightarrow{o}_Q$	implies	$(p,q) \in F$
(F3)	$(p,q) \xrightarrow{\alpha} R'$ and $R' \subseteq F$	implies	$(p,q) \in F$

The conjunction $P \wedge Q$ of MIAs P and Q with $(I_P \cap O_Q) = \emptyset = (O_P \cap I_Q)$ 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.

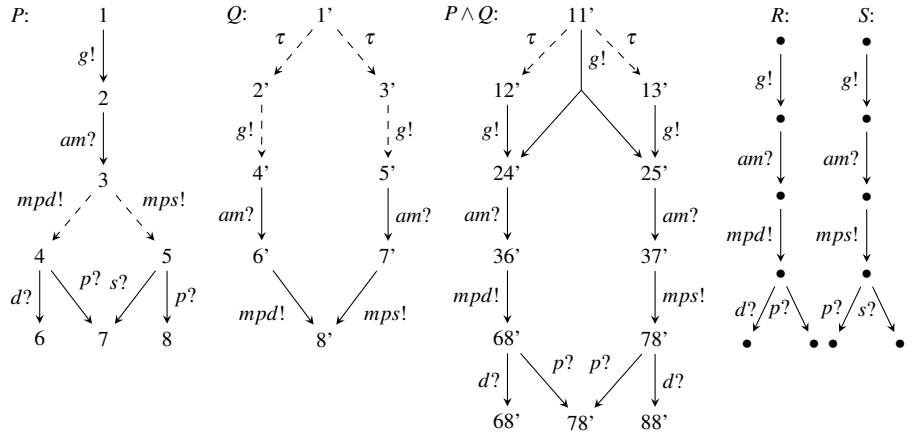

Fig. 5 Disjunctive must-transitions are needed for conjunction (adapted from Fig. 7 in [16] and Fig. 5 in [5]).

Note that conjunction is well-defined; in particular, $I \cap O = \emptyset$ and target sets are never empty: if R' becomes empty for some $(p,q) \xrightarrow{\alpha} R'$, then also (p,q) is deleted when constructing $P \wedge Q$ from $P\&Q$ according to (F3). Conjunction is also commutative and associative.

Figure 5 shows an example of conjunction: we specify the behaviour of a waiter in a restaurant from two perspectives. The desired overall specification will then be the conjunctive composition of both perspectives. The first perspective, P, requires the waiter to greet ($g!$) the customer and to accept that the customer then asks for the menu ($am?$). Then, the waiter may hand out a menu with pizzas and desserts on it ($mpd!$) or a menu with pizzas and salads on it ($mps!$); afterwards, an order of a pizza ($p?$) and an order of a dessert ($d?$) or, resp., an order of a pizza ($p?$) and an order of a salad ($s?$) must be accepted. The second perspective, Q, allows one to enquire in the kitchen whether desserts or salads will be on offer today (internal action τ) and to greet the customer. After being asked for a menu, the respective menu must be handed out. The overall specification $P \wedge Q$ and two common refinements R and S of P and Q are also shown.

That the conjunction of two MTSs cannot always be expressed as an MTS has been shown in [12,5,16] for three different refinement notions somewhat related to MIA-refinement and in [8] for a range of refinement notions. We adapt these proofs to our example and argue that no MIA without disjunctive must-transitions can serve as a conjunction, i.e., is equivalent to $P \wedge Q$. By contradiction, consider a MIA C where $c \in C$ is equivalent to $1 \wedge 1'$. Cleary, we have $c \xrightarrow{g} \xrightarrow{am}$, but neither $c \xrightarrow{g} \xrightarrow{am} \xrightarrow{mps}$ (cf. R) nor $c \xrightarrow{g} \xrightarrow{am} \xrightarrow{mpd}$ (cf. S). Hence, for any c' with $c \xrightarrow{g} \xrightarrow{am} c'$, we have neither $c' \xrightarrow{mps}$ nor $c' \xrightarrow{mpd}$. Hence, C is not a refinement of Q, which is impossible.

Operator $\wedge$ indeed defines conjunction on MIA, i.e., $\wedge$ is the greatest lower bound wrt. $\sqsubseteq$:

Theorem 15 ($\wedge$ is And) *Let P and Q be MIAs with $(I_P \cap O_Q) = \emptyset = (O_P \cap I_Q)$ and disjoint state sets. We have (i) $(\exists$ MIA R and $r \in R.\, r \sqsubseteq p$ and $r \sqsubseteq q)$ iff $p \wedge q$ is defined. Further, in case $p \wedge q$ is defined and for any MIA R and $r \in R$: (ii) $r \sqsubseteq p$ and $r \sqsubseteq q$ iff $r \sqsubseteq p \wedge q$.*

The theorem's first part reflects the intuition that specifications p and q are logically inconsistent if they do not have a common implementation; formally, $p \wedge q$ is undefined in this case. Its proof demands us to reason about inconsistent states, for which we resort to a notion

of witness, in analogy to [16] but now also considering τ-must-transitions (see Cond. (W3) below):

Definition 16 (Witness) A *witness* W of $P\&Q$ is a subset of $(P\times Q)\cup P\cup Q$ such that the following conditions hold for all $(p,q)\in W$:

(W1) $p \xrightarrow{o}_P$ implies $q \overset{o}{=\!=\!\!\rightarrow}_Q$
(W2) $q \xrightarrow{o}_Q$ implies $p \overset{o}{=\!=\!\!\rightarrow}_P$
(W3) $(p,q) \xrightarrow{\alpha} R'$ implies $R'\cap W\neq\emptyset$

Lemma 17 (Concrete Witness) *Let $P\&Q$ be a conjunctive product of MIAs. Then, for any witness W of $P\&Q$, we have (i) $F\cap W=\emptyset$. Also, (ii) the set $W=_{df}\{(p,q)\in P\times Q \mid \exists MIA\, R$ and $r\in R.\, r\subseteq p$ and $r\subseteq q\}\cup P\cup Q$ is a witness of $P\&Q$.*

Proof Since Part (i) is obvious, we directly proceed to proving Part (ii), for which it suffices to consider the elements of $\{(p,q)\in P\times Q \mid \exists \text{MIA}\, R$ and $r\in R.\, r\subseteq p$ and $r\subseteq q\}$; thus, let $(p,q)\in W$ due to MIA R and $r\in R$:

(W1) $p \xrightarrow{o}_P P'$ implies $r \overset{o}{\Longrightarrow}_R R'$ by $r\subseteq p$. Choose some $r'\in R'$. Then, $r \overset{o}{=\!=\!\!\rightarrow}_R r'$ by syntactic consistency, and $q \overset{o}{=\!=\!\!\rightarrow}_Q$ by $r\subseteq q$.
(W2) Analogous to (W1).
(W3) According to the operational rules for conjunction, we distinguish the following cases for a must-transition of (p,q):
(OMust1) Then, $(p,q) \xrightarrow{\omega} S'$, i.e., $p \xrightarrow{\omega}_P P'$ and $S'=\{(p',q') \mid p'\in P',\ q \overset{\hat{\omega}}{=\!=\!\!\rightarrow}_Q q'\}$. By $r\subseteq p$ we obtain some $R'\subseteq R$ such that $r \overset{\hat{\omega}}{\Longrightarrow}_R R'$ and $\forall r'\in R'\ \exists p'\in P'.\, r'\subseteq p'$. Choose $r'\in R'$ and the resp. $p'\in P'$; now, $r \overset{\hat{\omega}}{=\!=\!\!\rightarrow}_R r'$ due to syntactic consistency, and $q \overset{\hat{\omega}}{=\!=\!\!\rightarrow}_Q q'$ with $r'\subseteq q'$ for some q' by $r\subseteq q$. Thus, we have $p'\in P'$ and q' such that $(p',q')\in W\cap S'$ due to R and r'. Case (OMust2) is analogous.
(IMust1) Then, $(p,q) \xrightarrow{i} P'$, and we are done. Case (IMust2) is analogous.
(IMust3) Then, $(p,q) \xrightarrow{i} P'\times Q'$ due to $p \xrightarrow{i}_P P'$ and $q \xrightarrow{i}_Q Q'$. By $r\subseteq p$, $r\subseteq q$ and input-determinism, we have some R' and $r'\in R'$ with $r \xrightarrow{i}_R R'$, $\exists p'\in P'.\, r'\subseteq p'$ and $\exists q'\in Q'.\, r'\subseteq q'$. Thus, $(p',q')\in W\cap(P'\times Q')$ due to r'. □

Statement (ii) of this lemma is now the key for proving Thm. 15:

Proof (of Thm. 15) (i)"$\Longrightarrow$": This follows directly from Lemma 17 above.

(ii)"$\Longleftarrow$": Let R be a MIA. We now show that $\mathscr{R}=_{\text{df}}\{(r,p)\in R\times P \mid \exists q\in Q.\, r\subseteq p\wedge q\}\cup\subseteq$ is a MIA-refinement relation, by checking the three conditions of Def. 3 for some $(r,p)\in\mathscr{R}$ due to q:

– Let $p \xrightarrow{i}_P P'$. This can lead to a transition of $p\wedge q$ in two ways:
(IMust1) $q \not\xrightarrow{i}_Q$, whence $p\wedge q \xrightarrow{i} P'$. By $r\subseteq p\wedge q$, there is some R' such that $r \xrightarrow{i}_R R'$ and $\forall r'\in R'\ \exists p'\in P'.\, r'\subseteq p'$.
(IMust3) $q \xrightarrow{i}_Q Q'$, whence $p\wedge q \xrightarrow{i} (P'\times Q')\setminus F$. By $r\subseteq p\wedge q$, there is some R' such that $r \xrightarrow{i}_R R'$ and $\forall r'\in R'\exists p'\wedge q'\in P'\times Q'.\, r'\subseteq p'\wedge q'$ and, thus, $(r',p')\in\mathscr{R}$ due to q'.

– Let $p \xrightarrow{\omega}_P P'$. Then, $q \overset{\hat{\omega}}{=\!=\!\!\rightarrow}_Q$ since, otherwise, $p \wedge q$ would not be defined due to (F1). Thus, by Rule (OMust1), $p \wedge q \xrightarrow{\omega} \{p' \wedge q' \mid p' \in P',\ q \overset{\hat{\omega}}{=\!=\!\!\rightarrow}_Q q',\ p' \wedge q' \text{ defined}\}$. By $r \subseteq\!\!\!\cdot\ p \wedge q$, we get some $R' \subseteq R$ such that $r \overset{\hat{\omega}}{\Longrightarrow}_R R'$ and $\forall r' \in R'\ \exists p' \wedge q'.\ p' \in P',\ q \overset{\hat{\omega}}{=\!=\!\!\rightarrow}_Q q'$ and $r' \subseteq\!\!\!\cdot\ p' \wedge q'$. Hence, $\forall r' \in R'\ \exists p' \in P'.\ (r', p') \in \mathscr{R}$ due to q'.
– $r \overset{\omega}{\dashrightarrow}_R r'$ implies $\exists p' \wedge q'.\ p \wedge q \overset{\hat{\omega}}{=\!=\!\!\rightarrow} p' \wedge q'$ and $r' \subseteq\!\!\!\cdot\ p' \wedge q'$. The contribution of p in this weak transition gives $p \overset{\hat{\omega}}{=\!=\!\!\rightarrow}_P p'$, and we have $(r', p') \in \mathscr{R}$ due to q'.

(i)"$\Longleftarrow$": This follows from (ii)"$\Longleftarrow$" by choosing $R = P \wedge Q$ and $r = p \wedge q$.

(ii)"$\Longrightarrow$": Let R be a MIA. We show that $\mathscr{R} =_{\text{df}} \{(r, p \wedge q) \mid r \in R,\ r \subseteq\!\!\!\cdot\ p \text{ and } r \subseteq\!\!\!\cdot\ q\} \cup \subseteq\!\!\!\cdot$ is a MIA-refinement relation. By Part (i), $p \wedge q$ is defined whenever $r \subseteq\!\!\!\cdot\ p$ and $r \subseteq\!\!\!\cdot\ q$. We verify the conditions of Def. 3 for $(r, p \wedge q) \in \mathscr{R}$:

– $p \wedge q \xrightarrow{i} P'$. This is w.l.o.g. due to Rule (IMust1), i.e., $p \xrightarrow{i}_P P'$ and $q \not\xrightarrow{i}_Q$. By $r \subseteq\!\!\!\cdot\ p$, we have some R' such that $r \xrightarrow{i}_R R'$ and $\forall r' \in R'\ \exists p' \in P'.\ r' \subseteq\!\!\!\cdot\ p'$, whence $(r', p') \in \mathscr{R}$.
– Let $p \wedge q \xrightarrow{i} (P' \times Q') \setminus F$. This is due to Rule (IMust3), i.e., $p \xrightarrow{i}_P P'$ and $q \xrightarrow{i}_Q Q'$. By $r \subseteq\!\!\!\cdot\ p$ and $r \subseteq\!\!\!\cdot\ q$, we get a unique $r \xrightarrow{i}_R R'$ because of input-determinism such that $\forall r' \in R'\ \exists p' \in P', q' \in Q'.\ r' \subseteq\!\!\!\cdot\ p'$ and $r' \subseteq\!\!\!\cdot\ q'$; thus, $(r', p' \wedge q') \in \mathscr{R}$.
– Let $p \wedge q \xrightarrow{\omega} S'$. This is w.l.o.g. due to $p \xrightarrow{\omega}_P P'$ and $S' = \{p' \wedge q' \mid p' \in P', q \overset{\hat{\omega}}{=\!=\!\!\rightarrow}_Q q',$ $p' \wedge q' \text{ defined}\}$ (cf. Rule (OMust1)). By $r \subseteq\!\!\!\cdot\ p$, we have some $R' \subseteq R$ such that $r \overset{\hat{\omega}}{\Longrightarrow}_R R'$ and $\forall r' \in R'\ \exists p' \in P'.\ r' \subseteq\!\!\!\cdot\ p'$. Consider some arbitrary $r' \in R'$ and the resp. $p' \in P'$. Then, we have $r \overset{\hat{\omega}}{=\!=\!\!\rightarrow}_R r'$ by syntactic consistency and, due to $r \subseteq\!\!\!\cdot\ q$, some q' with $q \overset{\hat{\omega}}{=\!=\!\!\rightarrow}_Q q'$ and $r' \subseteq\!\!\!\cdot\ q'$. Thus, $p' \wedge q' \in S'$ and $(r', p' \wedge q') \in \mathscr{R}$.
– Let $r \overset{\omega}{\dashrightarrow}_R r'$. Consider $p \overset{\hat{\omega}}{=\!=\!\!\rightarrow}_P p'$, $q \overset{\hat{\omega}}{=\!=\!\!\rightarrow}_Q q'$ satisfying $r' \subseteq\!\!\!\cdot\ p'$ and $r' \subseteq\!\!\!\cdot\ q'$. Therefore, $(r', p' \wedge q') \in \mathscr{R}$. Further, if $\omega \neq \tau$, we have $p \wedge q \overset{\omega}{\dashrightarrow} p' \wedge q'$ by Rule (May3). Otherwise, either $p \overset{\tau}{=\!=\!\!\rightarrow}_P p'$ and $q \overset{\tau}{=\!=\!\!\rightarrow}_Q q'$ and we are done by Rule (May3), or w.l.o.g. $p \overset{\tau}{=\!=\!\!\rightarrow}_P p'$ and $q{=}q'$ and we are done by Rule (May1), or $p = p'$ and $q = q'$. □

As a corollary to this theorem, one obtains compositionality of MIA-refinement wrt. conjunction:

Corollary 18 *If $p \subseteq\!\!\!\cdot\ q$ and $p \wedge r$ is defined, then $q \wedge r$ is defined and $p \wedge r \subseteq\!\!\!\cdot\ q \wedge r$.*

Proof Assume $p \subseteq\!\!\!\cdot\ q$. Then, (always) $p \wedge r \subseteq\!\!\!\cdot\ p \wedge r \iff$ (by Thm. 15(ii)) $p \wedge r \subseteq\!\!\!\cdot\ p$ and $p \wedge r \subseteq\!\!\!\cdot\ r \implies$ (by assumption and transitivity) $p \wedge r \subseteq\!\!\!\cdot\ q$ and $p \wedge r \subseteq\!\!\!\cdot\ r \iff$ (by Thm. 15(i) and (ii)) $p \wedge r \subseteq\!\!\!\cdot\ q \wedge r$. □

Note that one cannot expect that definedness of $q \wedge r$ implies that of $p \wedge r$, because specializing q to p might introduce an inconsistency.

We now turn our attention to defining the dual disjunction operator $\vee$ on MIA, which expresses the least upper bound property wrt. $\subseteq\!\!\!\cdot$. The definition of disjunction may make use of the disjunctive must-transitions relation also for inputs and the internal action τ:

Definition 19 (Disjunction) Let $(P, I_P, O_P, \longrightarrow_P, \dashrightarrow_P)$ and $(Q, I_Q, O_Q, \longrightarrow_Q, \dashrightarrow_Q)$ be two MIAs with $I_P \cap O_Q = \emptyset = O_P \cap I_Q$ and disjoint state sets. The disjunction $P \vee Q$ is defined by $(\{p \vee q \mid p{\in}P, q{\in}Q\} \cup P \cup Q, I, O, \longrightarrow, \dashrightarrow)$, where $I =_{\text{df}} I_P \cap I_Q$, $O =_{\text{df}} O_P \cup O_Q$, and

$\longrightarrow$ 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) $p \vee q \xrightarrow{\tau} \{p,q\}$

(IMust) $p \vee q \xrightarrow{i} P' \cup Q'$ if $p \xrightarrow{i}_P P'$ and $q \xrightarrow{i}_Q Q'$

(May) $p \vee q \dashrightarrow p$, $p \vee q \dashrightarrow q$

(May1) $p \vee q \dashrightarrow p'$ if $p \dashrightarrow_P p'$ and $\exists q'.\, q \dashrightarrow_Q q'$

(May2) $p \vee q \dashrightarrow q'$ if $q \dashrightarrow_Q q'$ and $\exists p'.\, p \dashrightarrow_P p'$

It is not difficult to see that $\vee$ is commutative and associative. The idea behind the operational reading of $\vee$ is very intuitive since $p \vee q \xrightarrow{\tau} \{p,q\}$ naturally describes disjunctive behaviour. The only subtle point is that must-inputs must be matched directly, which justifies Rule (IMust) above. We now have the following desired theorem and corollary:

Theorem 20 **($\vee$ is Or)** *Let P, Q and R be MIAs with $I_P \cap O_Q = \emptyset = O_P \cap I_Q$ and disjoint state sets and states p, q, r, resp. Then, $p \vee q \sqsubseteq r$ iff $p \sqsubseteq r$ and $q \sqsubseteq r$.*

Proof "$\Longrightarrow$": We establish that $\mathscr{R} =_{\mathrm{df}} \{(p,r) \mid \exists q.\, p \vee q \sqsubseteq r\} \cup \sqsubseteq$ is a MIA-refinement relation. To do so, we let $(p,r) \in \mathscr{R}$ due to q and check the conditions of Def. 3:

(i) Let $r \xrightarrow{i}_R R'$. By $p \vee q \sqsubseteq r$ and the only applicable Rule (IMust), $p \vee q \xrightarrow{i} P' \cup Q'$ due to $p \xrightarrow{i}_P P'$ and $q \xrightarrow{i}_Q Q'$ such that $\forall p' \in P' \cup Q'\, \exists r' \in R'.\, p' \sqsubseteq r'$. Therefore, $\forall p' \in P' \exists r' \in R'.\, p' \sqsubseteq r'$ and, hence, $(p',r') \in \mathscr{R}$.

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

(iii) Let $p \dashrightarrow_P p'$. Then, $p \vee q \dashrightarrow p$ and, due to $p \vee q \sqsubseteq r$, we apply Def. 3(iii) twice to obtain some r' with $r \stackrel{\hat{\omega}}{=\!=\!\Rightarrow}_R r'$ and $p' \sqsubseteq r'$.

"$\Longleftarrow$": Let $p \sqsubseteq r$ and $q \sqsubseteq r$. We prove that $\mathscr{R} =_{\mathrm{df}} \{(p \vee q, r)\} \cup \sqsubseteq$ is an MIA-refinement relation by considering the following cases for $(p \vee q, r)$:

(i) Let $r \xrightarrow{i}_R R'$. By $p \sqsubseteq r$ and $q \sqsubseteq r$ we have P' and Q' satisfying $p \xrightarrow{i}_P P'$, $q \xrightarrow{i}_Q Q'$ 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, $p \vee q \xrightarrow{i} P' \cup Q'$ using Rule (IMust) and we are done.

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

(iii) Let $p \vee q \dashrightarrow^{\omega}$. Hence, $\omega = \tau$, and w.l.o.g. we must only consider $p \vee q \dashrightarrow p$. This transition is matched with $r \stackrel{\varepsilon}{=\!=\!\Rightarrow}_R r$ since $p \sqsubseteq r$. □

Corollary 21 *MIA-refinement is compositional wrt. disjunction.*

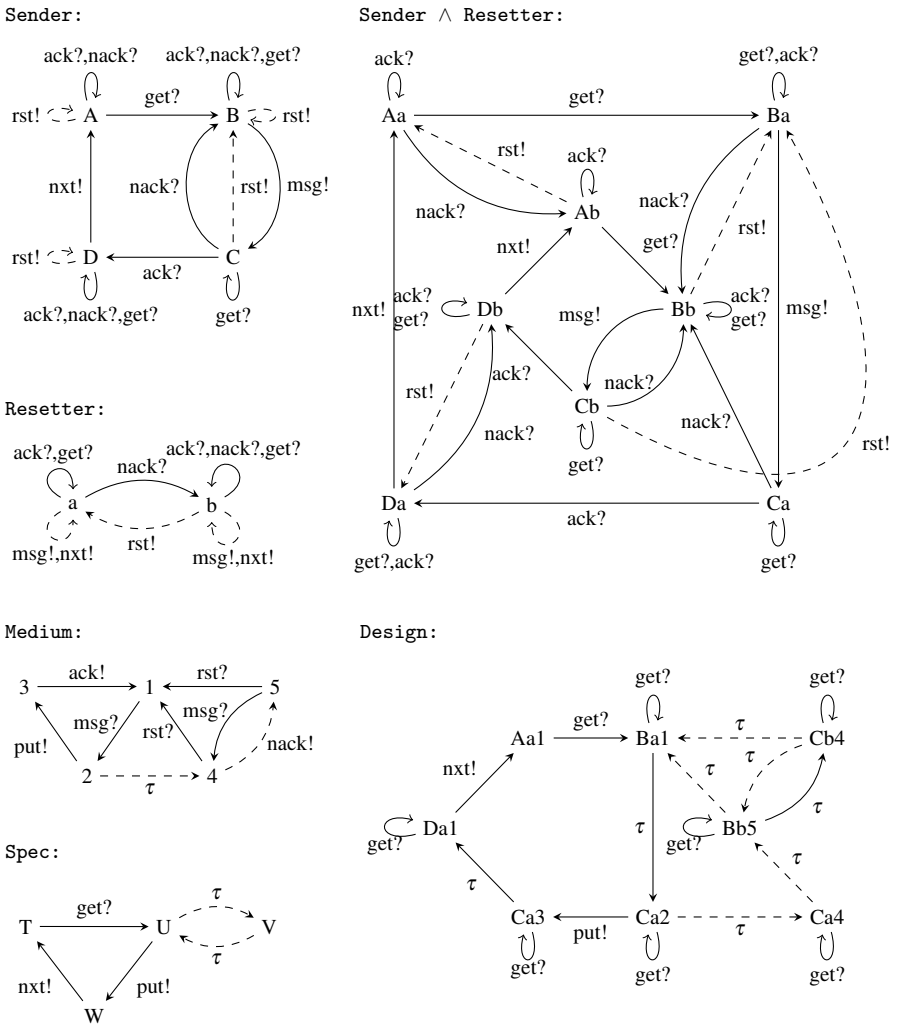

Fig. 6 Example in the optimistic MIA setting: `Design` = (`Sender` ∧ `Resetter`) | `Medium` and `Spec`.

2.3 Example

We illustrate the utility of our interface theory by a small example that models parts of a communication protocol (see Fig. 6) and is inspired by an example in [19]. The protocol's abstract specification is given by MIA `Spec`. It receives a message from its environment (action `get`), delivers it (`put`) and signals to its environment its willingness to handle the next message (`nxt`). The two τ-may-transitions making up the τ-loop model that the message's transmission may fail and that this failure may possibly be repaired.

The design of our protocol contains a generic component `Sender`, which receives a message for delivery (`get`). It sends this message (`msg`) to the `Medium` and waits for an according acknowledgment (`ack`). In case a negative acknowledgment arrives (`nack`), the message is re-sent. `Sender` is specialized by conjoining it with component `Resetter`, which

can suggest a reset (rst) after a negative acknowledgment. Both Sender and Resetter have input must-loops in certain states (actions ack, nack and get) in order to make the protocol robust against unexpected messages, which are simply dropped.

MIA $\texttt{Sender} \wedge \texttt{Resetter}$ is the result of formally applying our conjunction operator to Sender and Resetter. No inconsistency arises in our example. However, if one would refine Sender and Resetter by removing the rst-loop at state D and making the rst-transition from b to a a must-transition instead of a may-transition, then state Db (or, more precisely, $\texttt{D} \wedge \texttt{b}$) would be inconsistent.

MIA Medium specifies a communication medium with potential failure, which receives a message (msg) and may either deliver it to the environment (put) or – via the τ-may-transition – may lose it. In the former case, Medium returns to its initial state by sending an acknowledgment (ack); in the latter case, it may return a negative acknowledgment (nack), which may either be followed by a re-sent of the message (msg) or by the medium being reset (rst).

The parallel composition $\texttt{Design} =_{\mathrm{df}} (\texttt{Sender} \wedge \texttt{Resetter}) \,|\, \texttt{Medium}$ is also shown in Fig. 6. Using our MIA-refinement preorder, it is now easy to check that $\texttt{Design} \sqsubseteq \texttt{Spec}$ since $\mathscr{R} =_{\mathrm{df}} \{(\texttt{Aa1},\texttt{T}),(\mathrm{Ba1},\texttt{U}),(\texttt{Ca2},\texttt{U}),(\mathrm{Ca4},\texttt{V}),(\texttt{Bb5},\texttt{V}),(\mathrm{Cb4},\texttt{V}),(\texttt{Ca3},\texttt{W}),(\mathrm{Da1},\texttt{W})\}$ is a MIA-refinement relation. Note that the put-must-transition originating in state U is matched by the weak must-transition $\texttt{Ba1} \stackrel{\texttt{put}}{\Longrightarrow} \texttt{Ca3}$, i.e., the ability to abstract from internal computation is indeed required in practice. In addition, observe that the get-loop in state Ba1 does not need to be matched.

2.4 Perspective-Based Specification: Alphabet Extension

In perspective-based specification as employed in software engineering, one wishes to specify a component from multiple separate perspectives. Each perspective should be specifiable independently of the other perspectives and consider only those actions that are relevant for the current perspective, i.e., each component has its own alphabet; these alphabets may be identical, disjoint or overlapping. The specification of the overall component should then arise as the conjunction of all perspective specifications. We will show in this section that our theory – as presented so far – is not really suited for perspective-based specification, and that various approaches of addressing this issue that appear to be intuitive at first sight, are not appropriate solutions.

As an example of perspective-based specification, recall MIAs Sender and Resetter, which are specifications of two perspectives of the component $\texttt{Sender} \wedge \texttt{Resetter}$. Observe that Resetter has only loops for ack and get, and therefore it does not really know these actions. They are, basically, actions of the Sender perspective but not of the Resetter perspective. In the spirit of perspective-based specification, we wish to specify Resetter without the ack- and get-loops, and not even mention these two actions in the alphabet of Resetter; these actions are then not known to Resetter. In general, such 'unknown' actions may not only be inputs but also outputs.

Unknown inputs. The main source of problems is due to Rules (IMust1) and (IMust2) in Def. 13. For example, if conjunct P specifies a transition $p \xrightarrow{i} P'$ where input i is unknown to Q, then $p \wedge q \xrightarrow{i} P'$ for any $q \in Q$, thereby losing the behavioural requirements expressed by conjunct Q. This is usually undesired in perspective-based specification.

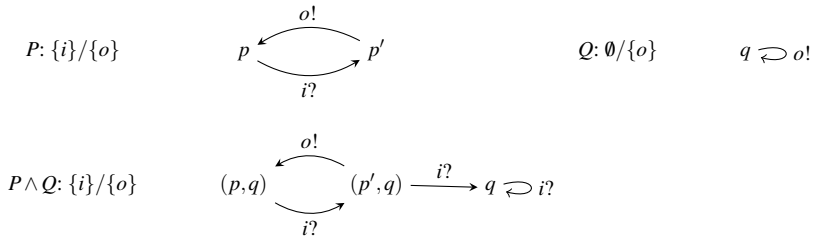

Fig. 7 Extending Q with an i-loop.

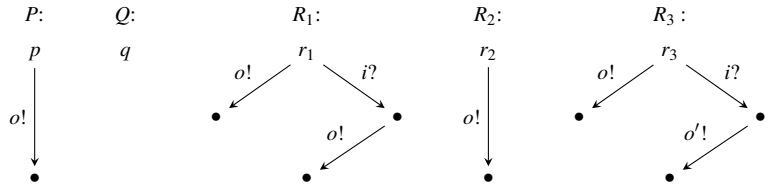

Fig. 8 Alphabet extension and conjunction in the optimistic setting.

To keep conjunct Q, one could add an i-must-loop to each state $q \in Q$ such that then $p \wedge q \xrightarrow{i} \{p' \wedge q \,|\, p' \in P'\}$, expressing the neutrality of Q wrt. i in each of its states. But now the problem is at those states $p' \in P$ with $p' \not\xrightarrow{i}_P$, i.e., p' stipulates on the environment not to produce i, because $p' \wedge q \xrightarrow{i} q$ is also undesirable (cf. Fig. 7). For this reason, we made both `Sender` and `Resetter` input-enabled by employing input must-loops. However, as said above, we would rather prefer not to mention, e.g., inputs `ack` and `get` in `Resetter`. Furthermore, `Sender`'s specifier really requires that a well-behaved environment will not produce `get` when `Sender` is, e.g., in state `B`; this cannot be expressed anymore when using conjunction, although expressing such requirements is an essential feature of interface theories based on IA [1].

A potential way out would be input may-loops. However, input may-transitions without accompanying must-transitions are not allowed in MIA; see the *input must* condition of Def. 1 and the discussion of its necessity in Fig. 3. However, such may-transitions would not help solving the problem. To see this, consider the MIAs P and Q depicted in Fig. 8 with input/output alphabets $\emptyset/\{o,o'\}$ and resp. $\{i\}/\emptyset$, as well as MIAs R_1, R_2 and R_3 with alphabets $\{i\}/\{o,o'\}$. Intuitively, r_1 and r_2 should refine $p \wedge q$, while r_3 should not. This is because (i) p morally has an i-may-loop and q allows input i, and (ii) p enforces one output o and prohibits o' independently of any i. However, there is no MIA R with alphabets $\{i\}/\{o,o'\}$ and $r \in R$ which has these properties of $p \wedge q$, because, if r_2 refines r, then so does r_3.

Unknown outputs. We now consider the case that conjunct P specifies a transition $p \xrightarrow{o}_P P'$, where output o is unknown to conjunct Q. Then, o is not in the alphabet of $P \wedge Q$, i.e., whatever P specifies wrt. o is ignored; this most likely contradicts what the specifier wants. Even worse, $p \wedge q$ is inconsistent for any $q \in Q$. This can be avoided by inserting o-may-loops for all $q \in Q$, which is what we have done wrt. outputs `msg` and `nxt` of `Resetter` in Fig. 6. The loops express that Q is neutral wrt. o, and this time without further undesirable con-

sequences. Rather than explicitly adding such loops, this can be done more elegantly and implicitly by modifying the refinement preorder, as we will do in Sec. 3.

In passing we note that adding an o-must-loop to each $q \in Q$ instead, makes $p' \wedge q$ inconsistent if $p' \not\xrightarrow{o}_P$. This is certainly inadequate since Q has no knowledge of o.

Conclusion. The use of loops for dealing with alphabet extensions has already been studied by Raclet et al. in [19] for their *Modal Interfaces* (MI); they refer to the addition of may- and must-loops as *weak* and *strong* extension, resp. As our interface theory does, MI combines MTS and IA, but unlike MIA in a purely deterministic setting without disjunctive transitions. Raclet et al. employ weak extensions when dealing with conjunction, and strong extensions for parallel composition. In effect, they end up with two different refinement relations when showing precongruence for conjunction and parallel composition, resp. As a consequence, MI is an incoherent theory.

In summary, conjunction, or refinement, for perspective-based specification is still an open problem in the optimistic setting. Next, we will investigate this problem again, but for the *pessimistic* approach to interface theories [4], and show how it can be solved there.

3 The Pessimistic Setting

Orthogonal to the 'optimistic' school on interface theories, comprising IA [1], IOMTS [15] and the above MIA, is the school of Bauer et al. who has adopted a *pessimistic* view of compatibility in the presence of errors; see, e.g., [4]. Their interface theory, called MIO, also roots in Larsen's modal transition systems [14] and allows may-inputs, but it defines parallel composition for much fewer interfaces when compared to optimistic approaches.

In our opinion, intuition for the pessimistic setting is weak since it distinguishes a state p where an input i is absent, from the situation where an i-transition leads to an error state; in both cases, an error is reached if and only if the environment provides input i. However, the pessimistic setting has technical advantages as we will see below. We will therefore redevelop our MIA theory for such a *pessimistic* setting, to which we will primarily contribute conjunction and disjunction operators and also *disjunctive* must-transitions. For completeness note that conjunction was defined by Bauer for a pessimistic interface theory in [2]; however, he considered deterministic interfaces only and no internal actions.

Definition 22 (Relaxed MIA) A *Relaxed Modal Interface Automaton* (Relaxed MIA) is a tuple $(P, I, O, \longrightarrow, \dashrightarrow)$ as in Def. 1, but which must only satisfy *syntactic consistency*.

In the context of the pessimistic setting, it turns out that *input determinism* and *input must* (Conds. (a) and (b) of Def. 1) are not necessary. We thus eliminate these conditions from MIA and call the resulting automata *Relaxed MIAs*. In analogy to Def. 2 we now define weak transitions for Relaxed MIA and, for convenience, overload the transition symbols:

Definition 23 (Relaxed Weak Transition Relations) The *relaxed weak must-transition relation* $\Longrightarrow$ and *relaxed weak may-transition relation* $\dashrightarrow\!\!\!\!\!\Rightarrow$ are defined identically to the weak must- and may-transition relations in Def. 2, but replacing ω by α, $\hat{\omega}$ by $\hat{\alpha}$, and o by a. For input actions, we additionally define a restricted weak must-transition that only allows trailing τ-actions as follows:

(e) $p \xrightarrow{i} P'$ implies $p \overset{i}{\Longrightarrow} P'$,

(f) $p \overset{i}{\Longrightarrow} P'$, $p' \in P'$ and $p' \xrightarrow{\tau} P''$ implies $p \overset{i}{\Longrightarrow} (P' \setminus \{p'\}) \cup P''$,

Observe that $p \overset{i}{\Longrightarrow\!\!\!\!\to} P'$ implies $p \overset{i}{\Longrightarrow} P'$, which will be used in the sequel.

Since may-inputs are available in the pessimistic setting, extending the alphabets of interfaces can be defined via an according operation, as we will see below (Def. 33). Therefore, we first consider refinement and operators for Relaxed MIAs with the same input and output alphabets. The corresponding notions for Relaxed MIAs with dissimilar alphabets will then be defined on the basis of the existing ones and the alphabet extension operator.

Definition 24 (Modal Refinement on Relaxed MIA) Let P, Q be Relaxed MIAs with the same input/output alphabets. $\mathscr{R} \subseteq P \times Q$ is a *modal refinement relation* if for all $(p,q) \in \mathscr{R}$:

(i) $q \overset{i}{\longrightarrow} Q'$ implies $\exists P'.\, p \overset{i}{\Longrightarrow\!\!\!\!\to} P'$ and $\forall p' {\in} P'\, \exists q' {\in} Q'.\, (p',q') \in \mathscr{R}$,

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

(iii) $p \overset{\alpha}{\dashrightarrow} p'$ implies $\exists q'.\, q \overset{\hat{\alpha}}{\dashrightarrow} q'$ and $(p',q') \in \mathscr{R}$.

We write $p \sqsubseteq_{\frown} q$ and say that p *modal-refines* q if there exists a modal refinement relation $\mathscr{R}$ such that $(p,q) \in \mathscr{R}$. Moreover, we denote the kernel of $\sqsubseteq_{\frown}$ by $\sqsubseteq\!\sqsupseteq_{\frown\frown}$.

Using the same line of argumentation as in the optimistic case, one can establish that $\sqsubseteq_{\frown}$ is a preorder and the largest modal refinement relation.

3.1 Parallel Composition

The definitions of composability, parallel product and error state for Relaxed MIAs are as in Def. 7 for MIAs. However, the pessimistic setting is distinguished from the optimistic one by the following definition of *compatibility*, which is much stricter than the notion of compatibility introduced in Def. 7:

Definition 25 (Compatibility on Relaxed MIA) Given Relaxed MIAs P_1 and P_2, states $p_1 \in P_1$ and $p_2 \in P_2$ are called *incompatible* if an error state is reachable from (p_1, p_2) in $P_1 \otimes P_2$. Here, *reachable* means reachable via any kind of may-transition, in particular also via input may-transitions. We write $p_1 \otimes p_2$ for (p_1, p_2), if p_1 and p_2 are compatible.

It is important to point out that, due to the strict notion of compatibility, parallel composition is undefined much more often than in the optimistic approach. This view ignores that errors can be masked by suitable environments; in this sense, the pessimistic approach does not capture a truly *open systems* view.

Note that Lemma 11 is still valid in the pessimistic setting. We now obtain the analogue of Thm. 12:

Theorem 26 (Compositionality of Parallel Composition) *Let P_1, P_2, Q be Relaxed MIAs with $p_1 \in P_1$, $p_2 \in P_2$, $q \in Q$ and $p_1 \sqsubseteq_{\frown} q$. Assume that Q and P_2 are composable; 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 $p_1 \otimes p_2 \sqsubseteq_{\frown} q \otimes p_2$.

Proof Part (a) follows immediately since Relaxed MIA Q has the same input and output alphabets as MIA P_1, due to $p_1 \sqsubseteq_{\frown} q$. Regarding Part (b), we first show that

$$\mathscr{R} =_{\mathrm{df}} \{((p_1,p_2),(q,p_2)) \mid p_1 \sqsubseteq_{\frown} q\}$$

is a modal refinement relation; observe that this relation does not mention compatibility. We check the conditions of Def. 24 for some $((p_1,p_2),(q,p_2)) \in \mathscr{R}$:

(i) Let $(q,p_2) \xrightarrow{i} \overline{Q}$ due to either Rule (Must1) or (Must2).

(Must1) $q \xrightarrow{i}_Q Q'$ and $\overline{Q} = Q' \times \{p_2\}$. By $p_1 \sqsubseteq_{\frown} q$, there is $P_1' \subseteq P_1$ such that $p_1 \overset{i}{\Longrightarrow} P_1'$ and $\forall p_1' \in P_1' \, \exists q' \in Q' . \, p_1' \sqsubseteq_{\frown} q'$. Now, we obtain $(p_1,p_2) \overset{i}{\Longrightarrow} P_1' \times \{p_2\}$ by repeated application of Rule (Must1) and $i \notin A_2$. For each $(p_1',p_2) \in P_1' \times \{p_2\}$, there is a suitable q' such that $((p_1',p_2),(q',p_2)) \in \mathscr{R}$.

(Must2) $p_2 \xrightarrow{i}_P P_2'$ and $\overline{Q} = \{q\} \times P_2'$. Then, $(p_1,p_2) \xrightarrow{i} \{p_1\} \times P_2'$ by Rule (Must2), since p_1 and q have the same alphabets by $p_1 \sqsubseteq_{\frown} q$. Because $((p_1,p_2'),(q,p_2')) \in \mathscr{R}$ for each $p_2' \in P_2$, we are done.

(ii) Let $(q,p_2) \xrightarrow{\omega} \overline{Q}$ due to either Rule (Must1), (Must2) or (Must3). The cases (Must1) and (Must2) are as in Case (i) with $\xrightarrow{\omega}$ in place of $\xrightarrow{i}$ and $\overset{\hat{\omega}}{\Longrightarrow}$ in place of $\overset{i}{\Longrightarrow}$. In Case (Must3), we have $\omega = \tau$ and distinguish the following sub-cases:

- $q \xrightarrow{a}_Q Q'$ with $a \in O_Q$, $p_2 \xrightarrow{a}_{P_2} P_2'$ with $a \in I_2$, and $\overline{Q} = Q' \times P_2'$. As $p_1 \sqsubseteq_{\frown} q$, there exists some P_1' with $p_1 \overset{a}{\Longrightarrow}_{P_1} P_1'$ such that $\forall p_1' \in P_1' \, \exists q' \in Q' . \, p_1' \sqsubseteq_{\frown} q'$. Now, $(p_1,p_2) \overset{\varepsilon}{\Longrightarrow} R$ for some $R \subseteq P_1' \times P_2'$ by Lemma 11. Hence, for each $(p_1',p_2') \in R$ we have a $q' \in Q'$ with $((p_1',p_2'),(q',p_2')) \in \mathscr{R}$.
- The case for $a \in I_Q \cap O_2$ is analogous, writing $\overset{a}{\Longrightarrow}_{P_1}$ for $\overset{a}{\Longrightarrow}_{P_1}$.

(iii) This condition, where $(p_1,p_2) \overset{\alpha}{\dashrightarrow} (p_1',p_2')$ due to either Rule (May1), (May2) or (May3), is similar but much simpler to establish than Conds. (i) (in case $\alpha \in I_Q$) and (ii) (in case $\alpha \in O_Q \cup \{\tau\}$) above.

We now conclude the proof of Part (b) by reasoning that compatibility of q and p_2 implies compatibility of p_1 and p_2. To do so, assume p_1 and p_2 are incompatible; then, the sequence of may-transitions leading from (p_1,p_2) to an error state (p_1',p_2') can be matched according to the above modal refinement relation $\mathscr{R}$ and Def. 24(iii) via a transition sequence leading from (q,p_2) to (q',p_2') with $p_1' \sqsubseteq_{\frown} q'$. If there is an action $a \in O_1 \cap I_2$ with $p_1' \overset{a}{\dashrightarrow}_{P_1}$ and $p_2' \not\xrightarrow{a}_{P_2}$, then $q' \overset{\varepsilon}{=\!=\!\Rightarrow}_Q q'' \overset{a}{\dashrightarrow}_Q$ and $(q',p_2') \overset{\varepsilon}{=\!=\!\Rightarrow} (q'',p_2')$, where the latter is an error state. If there is an action $a \in I_1 \cap O_2$ with $p_1' \not\xrightarrow{a}$ and $p_2' \overset{a}{\dashrightarrow}$, then $q' \xrightarrow{a}$ would contradict Cond. (i) of Def. 24 and the definition of $\overset{i}{\Longrightarrow}$; thus, (q',p_2') is an error state. In any case, (q,p_2) would reach an error state. Hence, compatibility of q and p_2 implies compatibility of p_1 and p_2.

Now we can restrict $\mathscr{R}$ to pairs where p_1 and p_2 as well as q and p_2 are compatible. This relation is a modal refinement relation, too: the strong and weak transitions considered above use only pairs of compatible states since these can be reached from $p_1 \otimes p_2$ or $q \otimes p_2$. Thus, the restricted relation proves $p_1 \otimes p_2 \sqsubseteq_{\frown} q \otimes p_2$. □

In contrast to the optimistic setting, the matching of input may-transitions in the refinement preorder does not preclude compositionality. This is because for $p_1 \sqsubseteq_{\frown} q$, there exist much fewer p_2 such that q and p_2 are compatible. Hence, for establishing the precongruence property for parallel composition $\otimes$, there are much fewer results $p_1 \otimes p_2 \sqsubseteq_{\frown} q \otimes p_2$ to prove.

3.2 Conjunction & Disjunction

The definition of conjunction $\wedge$ on Relaxed MIA gets by with five instead of eleven rules. This is because it allows one to merge the corresponding rules for outputs and inputs, due to the use of weak input must-transitions in Def. 24:

Definition 27 (Conjunctive Product on Relaxed MIA) Let $(P,I,O,\longrightarrow_P,\ \dashrightarrow_P)$ as well as $(Q,I,O,\longrightarrow_Q,\dashrightarrow_Q)$ be Relaxed MIAs with common alphabets. The conjunctive product $P\&Q =_{\text{df}} (P\times Q,I,O,\longrightarrow,\dashrightarrow)$ is defined by the following operational transition rules:

(Must1)	$(p,q)\xrightarrow{\alpha}\{(p',q')\mid p'\in P', q\overset{\hat\alpha}{=\!=\!\!\twoheadrightarrow}_Q q'\}$	if	$p\xrightarrow{\alpha}_P P'$ and $q\overset{\hat\alpha}{=\!=\!\!\twoheadrightarrow}_Q$
(Must2)	$(p,q)\xrightarrow{\alpha}\{(p',q')\mid p\overset{\hat\alpha}{=\!=\!\!\twoheadrightarrow}_P p', q'\in Q'\}$	if	$p\overset{\hat\alpha}{=\!=\!\!\twoheadrightarrow}_P$ and $q\xrightarrow{\alpha}_Q Q'$
(May1)	$(p,q)\overset{\tau}{\dashrightarrow}(p',q)$	if	$p\overset{\tau}{=\!=\!\!\twoheadrightarrow}_P p'$
(May2)	$(p,q)\overset{\tau}{\dashrightarrow}(p,q')$	if	$q\overset{\tau}{=\!=\!\!\twoheadrightarrow}_Q q'$
(May3)	$(p,q)\overset{\alpha}{\dashrightarrow}(p',q')$	if	$p\overset{\alpha}{=\!=\!\!\twoheadrightarrow}_P p'$ and $q\overset{\alpha}{=\!=\!\!\twoheadrightarrow}_Q q'$

Conjunction on Relaxed MIAs with the same alphabets – including the set F of inconsistent states – is now defined identically to these notions on MIA (Def. 14), but replacing $o\in O$ with $a\in A$; the same applies to the notion of witness (Def. 16). In analogy to Lemma 17, we obtain the following concrete witness lemma for our pessimistic setting:

Lemma 28 (Concrete Witness for Relaxed MIAs) *Let P, Q and R be Relaxed MIAs with common alphabets.*

(i) For any witness W of $P\&Q$, we have $F\cap W=\emptyset$.
(ii) The set $\{(p,q)\in P\times Q\mid \exists r\in R.\, r\mathrel{\underset{\frown}{\sqsubseteq}} p$ and $r\mathrel{\underset{\frown}{\sqsubseteq}} q\}$ is a witness of $P\&Q$.

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

(W1) $p\xrightarrow{a}_P P'$ implies $r\overset{a}{\Longrightarrow}_R R'$ by $r\mathrel{\underset{\frown}{\sqsubseteq}} p$. Choose some $r'\in R'$. Then, $r\overset{a}{=\!=\!\!\twoheadrightarrow}_R r'$ by syntactic consistency and $q\overset{a}{=\!=\!\!\twoheadrightarrow}_Q$ by $r\mathrel{\underset{\frown}{\sqsubseteq}} q$.
(W2) Analogous to (W1).
(W3) Consider $(p,q)\in W$ due to r, with $(p,q)\xrightarrow{\alpha} S'$ because of $p\xrightarrow{\alpha}_P P'$ and $S'=\{(p',q')\mid p'\in P', q\overset{\hat\alpha}{=\!=\!\!\twoheadrightarrow}_Q q'\}$ by Rule (Must1). By $r\mathrel{\underset{\frown}{\sqsubseteq}} p$ we get some $R'\subseteq R$ such that $r\overset{\hat\alpha}{\Longrightarrow}_R R'$ (recall that $r\overset{i}{\Longrightarrow}_R R'$ implies $r\overset{i}{\Longrightarrow}_R R'$) and $\forall r'\in R'\,\exists p'\in P'.\, r'\mathrel{\underset{\frown}{\sqsubseteq}} p'$. Choose $r'\in R'$; now, $r\overset{\hat\alpha}{=\!=\!\!\twoheadrightarrow}_R r'$ due to syntactic consistency, and $q\overset{\hat\alpha}{=\!=\!\!\twoheadrightarrow}_Q q'$ with $r'\mathrel{\underset{\frown}{\sqsubseteq}} q'$ by $r\mathrel{\underset{\frown}{\sqsubseteq}} q$. Thus, we have $p'\in P'$ and q' such that $(p',q')\in W\cap S'$ due to r'. □

On the basis of this lemma we can now establish the desired greatest lower bound result for $\wedge$, which implies the compositionality of $\mathrel{\underset{\frown}{\sqsubseteq}}$ wrt. $\wedge$:

Theorem 29 ($\wedge$ is And) *Let P and Q be Relaxed MIAs with common alphabets. Then, (i) ($\exists R$ and $r\in R$. $r\mathrel{\underset{\frown}{\sqsubseteq}} p$ and $r\mathrel{\underset{\frown}{\sqsubseteq}} q$) iff $p\wedge q$ is defined. Further, in case $p\wedge q$ is defined and for any R and $r\in R$: (ii) $r\mathrel{\underset{\frown}{\sqsubseteq}} p$ and $r\mathrel{\underset{\frown}{\sqsubseteq}} q$ iff $r\mathrel{\underset{\frown}{\sqsubseteq}} p\wedge q$.*

Note that R is implicitly required to have the same alphabets as P and Q by our definition of $\mathrel{\underset{\frown}{\sqsubseteq}}$.

Proof (i)"$\Longrightarrow$": This follows from Lemma 28.

(i), (ii)"$\Longleftarrow$": It suffices to show that $\mathscr{R}=_{\text{df}}\{(r,p)\mid \exists q.\, r\mathrel{\underset{\frown}{\sqsubseteq}} p\wedge q\}$ is a modal refinement relation. Then, in particular, (i)"$\Longleftarrow$" follows by choosing $r=p\wedge q$. We check the conditions of Def. 24:

– Let $p \xrightarrow{\alpha}_P P'$; then $q \overset{\hat{\alpha}}{=\!=\!\twoheadrightarrow}_Q$, since otherwise $\alpha \neq \tau$, and $p \wedge q$ would not be defined due to (F1). Hence, by Rule (Must1), $p \wedge q \xrightarrow{\alpha} \{p' \wedge q' \mid p' \in P', q \overset{\hat{\alpha}}{=\!=\!\twoheadrightarrow}_Q q', p' \wedge q' \text{ defined}\}$. By $r \mathrel{\widehat{\sqsubseteq}} p \wedge q$, we get $r \overset{\hat{\alpha}}{\Longrightarrow}_R R'$ such that $\forall r' \in R' \, \exists p' \wedge q' . \, p' \in P', q \overset{\hat{\alpha}}{=\!=\!\twoheadrightarrow}_Q q'$ and $r' \mathrel{\widehat{\sqsubseteq}} p' \wedge q'$. Hence, $\forall r' \in R' \exists p' \in P' . (r', p') \in \mathscr{R}$.
– $r \overset{\alpha}{\dashrightarrow}_R r'$ implies $\exists p' \wedge q' . \, p \wedge q \overset{\hat{\alpha}}{=\!=\!\twoheadrightarrow} p' \wedge q'$ and $r' \mathrel{\widehat{\sqsubseteq}} p' \wedge q'$. The contribution of p in this weak transition sequence gives $p \overset{\hat{\alpha}}{=\!=\!\twoheadrightarrow}_P p'$, and we have $(r', p') \in \mathscr{R}$ due to q'.

(ii)"$\Longrightarrow$": Here, we show that $\mathscr{R} =_{\text{df}} \{(r, p \wedge q) \mid r \mathrel{\widehat{\sqsubseteq}} p \text{ and } r \mathrel{\widehat{\sqsubseteq}} q\}$ is a modal refinement relation. By Part (i), $p \wedge q$ is defined and $(r, p \wedge q) \in \mathscr{R}$ whenever $r \mathrel{\widehat{\sqsubseteq}} p$ and $r \mathrel{\widehat{\sqsubseteq}} q$. We now verify the conditions of Def. 24:

– Let $p \wedge q \xrightarrow{\alpha} S'$, w.l.o.g. this is due to $p \xrightarrow{\alpha}_P P'$ and $S' = \{p' \wedge q' \mid p' \in P', q \overset{\hat{\alpha}}{=\!=\!\twoheadrightarrow}_Q q', p' \wedge q' \text{ defined}\}$. Because of $r \mathrel{\widehat{\sqsubseteq}} p$, we have $r \overset{\hat{\alpha}}{\Longrightarrow}_R R'$ so that $\forall r' \in R' \, \exists p' \in P' . \, r' \mathrel{\widehat{\sqsubseteq}} p'$. Consider some arbitrary $r' \in R'$ and the resp. $p' \in P'$. Then, $r \overset{\hat{\alpha}}{=\!=\!\twoheadrightarrow}_R r'$ by syntactic consistency and, due to $r \mathrel{\widehat{\sqsubseteq}} q$, there exists some q' with $q \overset{\hat{\alpha}}{=\!=\!\twoheadrightarrow}_Q q'$ and $r' \mathrel{\widehat{\sqsubseteq}} q'$. Thus, $p' \wedge q' \in S'$ and $(r', p' \wedge q') \in \mathscr{R}$.
– Let $r \overset{\alpha}{\dashrightarrow}_R r'$ and consider $p \overset{\hat{\alpha}}{=\!=\!\twoheadrightarrow}_P p'$ and $q \overset{\hat{\alpha}}{=\!=\!\twoheadrightarrow}_Q q'$ satisfying $r' \mathrel{\widehat{\sqsubseteq}} p'$ and $r' \mathrel{\widehat{\sqsubseteq}} q'$. Thus, $(r', p' \wedge q') \in \mathscr{R}$. Further, if $\alpha \neq \tau$, we have $p \wedge q \overset{\alpha}{\dashrightarrow} p' \wedge q'$ by Rule (May3). Otherwise, either $p \overset{\tau}{=\!=\!\twoheadrightarrow}_P p'$ and $q \overset{\tau}{=\!=\!\twoheadrightarrow}_Q q'$ and we are done by Rule (May3) again, or w.l.o.g. $p \overset{\tau}{=\!=\!\twoheadrightarrow}_P p'$ and $q = q'$ and we are done by Rule (May1), or $p = p'$ and $q = q'$. □

Corollary 30 *Modal-refinement is compositional wrt. conjunction.*

We now turn our attention to disjunction $\vee$ on Relaxed MIAs with the same alphabets, which is defined as in Def. 19 for MIA and for which we obtain, in analogy to Thm. 20 and Cor. 30:

Theorem 31 **($\vee$ is Or)** *Let P, Q and R be Relaxed MIAs with common alphabets, disjoint state sets and states p, q and r, resp. Then, $p \vee q \mathrel{\widehat{\sqsubseteq}} r$ iff $p \mathrel{\widehat{\sqsubseteq}} r$ and $q \mathrel{\widehat{\sqsubseteq}} r$.*

Proof "$\Longrightarrow$": We establish that $\mathscr{R} =_{\text{df}} \{(p, r) \mid \exists q . \, p \vee q \mathrel{\widehat{\sqsubseteq}} r\} \cup \mathrel{\widehat{\sqsubseteq}}$ is a modal-refinement relation. To do so, we let $(p, r) \in \mathscr{R}$ due to q and check the conditions of Def. 3:

(i) Let $r \xrightarrow{i}_R R'$. Because of $p \vee q \mathrel{\widehat{\sqsubseteq}} r$ and by the only initially applicable Rule (IMust), $p \vee q \overset{i}{\Longrightarrow\!\!\!\!\twoheadrightarrow} P' \cup Q'$ due to $p \overset{i}{\Longrightarrow\!\!\!\!\twoheadrightarrow}_P P'$, $q \overset{i}{\Longrightarrow\!\!\!\!\twoheadrightarrow}_Q Q'$ such that $\forall p' \in P' \cup Q' \, \exists r' \in R' . \, p' \mathrel{\widehat{\sqsubseteq}} r'$; recall $P \cap Q = \emptyset$. Hence, $\forall p' \in P' \exists r' \in R' . \, p' \mathrel{\widehat{\sqsubseteq}} r'$ and, thus, $(p', r') \in \mathscr{R}$.
(ii) Let $r \xrightarrow{\omega}_R R'$. The proof in this case is identical to the corresponding case in the proof of Thm. 20.
(iii) Let $p \overset{\alpha}{\dashrightarrow}_P p'$. Then, $p \vee q \overset{\tau}{\dashrightarrow} p$ and, due to $p \vee q \mathrel{\widehat{\sqsubseteq}} r$, we apply Def. 3(iii) twice to obtain some r' with $r \overset{\hat{\alpha}}{=\!=\!\twoheadrightarrow}_R r'$ and $p' \mathrel{\widehat{\sqsubseteq}} r'$.

"$\Longleftarrow$": We prove that $\mathscr{R} =_{\text{df}} \{(p \vee q, r) \mid p \mathrel{\widehat{\sqsubseteq}} r \text{ and } q \mathrel{\widehat{\sqsubseteq}} r\} \cup \mathrel{\widehat{\sqsubseteq}}$ is a modal-refinement relation. Let $(p \vee q, r) \in \mathscr{R}$ and consider the following cases:

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

(ii) Let $r \xrightarrow{\omega}_R R'$. The proof in this case is identical to the corresponding case in the proof of Thm. 20.

(iii) Let $p \vee q \overset{\alpha}{\dashrightarrow}$. If $\alpha = \tau$, then w.l.o.g. we must only consider $p \vee q \overset{\tau}{\dashrightarrow} p$. This transition is matched with $r \overset{\varepsilon}{=\!=\!\!\!\rightarrow}_R r$ since $p \mathrel{\sqsubseteq\!\!\!\frown} r$. If $\alpha \neq \tau$, then w.l.o.g. we must only consider $p \vee q \overset{\alpha}{\dashrightarrow} p'$ due to $p \overset{\alpha}{\dashrightarrow}_P p'$ and $q \overset{\alpha}{\dashrightarrow}_Q$. Then, $r \overset{\alpha}{=\!=\!\!\!\rightarrow}_R r'$ for some r' satisfying $p' \mathrel{\sqsubseteq\!\!\!\frown} r'$, due to $p \mathrel{\sqsubseteq\!\!\!\frown} r$. □

Corollary 32 *Modal-refinement is compositional wrt. disjunction.*

3.3 Alphabet Extension

As motivated in Sec. 2.4, we introduce alphabet extension as an operation on Relaxed MIA and employ this to lift modal-refinement to Relaxed MIAs with dissimilar alphabets. In contrast to MIA-refinement, we are now interested in extending input *and* output alphabets in a refinement step.

Definition 33 (Alphabet Extension and Refinement) Given a Relaxed MIA $(P, I, O, \longrightarrow, \dashrightarrow)$ and disjoint action sets I' and O' satisfying $I' \cap A = \emptyset = O' \cap A$, where $A =_{\text{df}} I \cup O$. The *alphabet extension of P by I' and O'* is given by $[P]_{I',O'} =_{\text{df}} (P, I \cup I', O \cup O', \longrightarrow, \dashrightarrow')$ for $\dashrightarrow' =_{\text{df}} \dashrightarrow \cup \{(p,a,p) \mid p \in P,\ a \in I' \cup O'\}$. We often write $[p]_{I',O'}$ – or conveniently $[p]$ in case I', O' are understood from the context – for p as state of $[P]_{I',O'}$.

For Relaxed MIAs P, Q with $p \in P$, $q \in Q$, $I_P \supseteq I_Q$ and $O_P \supseteq O_Q$, we define $p \mathrel{\sqsubseteq\!\!\!\frown}' q$ if $p \mathrel{\sqsubseteq\!\!\!\frown} [q]_{I_P \setminus I_Q, O_P \setminus O_Q}$. Since $\mathrel{\sqsubseteq\!\!\!\frown}'$ extends $\mathrel{\sqsubseteq\!\!\!\frown}$ to Relaxed MIAs with different alphabets, we write $\mathrel{\sqsubseteq\!\!\!\frown}$ for $\mathrel{\sqsubseteq\!\!\!\frown}'$. We also abbreviate $[q]_{I_P \setminus I_Q, O_P \setminus O_Q}$ by $[q]_P$.

Our compositionality result regarding parallel composition of Thm. 26 immediately carries over to the alphabet extension situation, if we require that alphabet extension does not yield new communications:

Theorem 34 (Compositionality of Parallel Composition) *Let P_1, P_2, Q be Relaxed MIAs as well as $p_1 \in P_1$, $p_2 \in P_2$, $q \in Q$ such that, for $I' =_{df} I_1 \setminus I_Q$ and $O' =_{df} O_1 \setminus O_Q$, we have $(I' \cup O') \cap A_2 = \emptyset$. Assume further that Q and P_2 are composable and $p_1 \mathrel{\sqsubseteq\!\!\!\frown} q$. 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 $p_1 \otimes p_2 \mathrel{\sqsubseteq\!\!\!\frown} q \otimes p_2$.

Note that the requirement $(I' \cup O') \cap A_2 = \emptyset$ above is equivalent to $(A_1 \cap A_2) = (A_Q \cap A_2)$ (cf. Thm. 12).

Proof It is easy to see that $[Q]_{I',O'}$ and P_2 are composable and that $[Q]_{I',O'} \otimes P_2$ is isomorphic to $[Q \otimes P_2]_{I',O'}$ via mapping $[q] \otimes p_2 \mapsto [q \otimes p_2]$. This follows from Rule (May1) in the definition of $\otimes$ since we only add "fresh" may-transitions to each $q \in Q$. The mapping also respects error states; in particular, new may-transitions with label $o \in O'$ cannot create new errors since $o \notin I_2$. Thus, $[q]$ and p_2 are compatible if q and p_2 are; moreover, $p_1 \mathrel{\sqsubseteq\!\!\!\frown} [q]$. Now, the result follows from Thm. 26. □

The conjunction operator in the presence of alphabet extension can now be lifted from Sec. 3.2 in a straightforward manner:

Definition 35 (Conjunction Operator) Let P, Q be Relaxed MIAs, $p \in P$ and $q \in Q$ such that $I_P \cap O_Q = \emptyset = I_Q \cap O_P$. Then, $p \wedge' q =_{\mathrm{df}} [p]_Q \wedge [q]_P$. Again, we simply write $p \wedge q$ for $p \wedge' q$.

To be able to lift our main result, Thm. 29, we only need to establish that the alphabet extension operation is a homomorphism for conjunction:

Lemma 36 *Let P with $p \in P$ and Q with $q \in Q$ be Relaxed 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, $[p \wedge q] \mathrel{\overset{\frown}{\sqsubseteq}\overset{\frown}{\sqsupseteq}} [p] \wedge [q]$.

Proof For proving Part (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) or (F2) iff $([p],[q]) \in F_{[P]\&[Q]}$ due to $a \in A$ and (F1) or (F2). Observe that (F1) and (F2) never apply to $([p],[q])$ and $a \in I' \cup O'$, because there are no must-transitions labelled a. For the same reason, Rules (Must1) and (Must2) are never applicable for a and, thus, β is an isomorphism regarding must-transitions; hence, (F3) is applicable exactly in the corresponding cases according to β. Therefore, β is also a bijection between $F_{P\&Q}$ and $F_{[P]\&[Q]}$.

Concerning Part (b), we can regard β also as a bijection between $[P \wedge Q]$ and $[P] \wedge [Q]$, and establish each direction of $\mathrel{\overset{\frown}{\sqsubseteq}\overset{\frown}{\sqsupseteq}}$ separately:

- *"$\mathrel{\overset{\frown}{\sqsubseteq}}$":* We show that β is a modal refinement relation, for which we consider $[p \wedge q]$ and $[p] \wedge [q]$. Conds. (i) and (ii) of Def. 24 are clear, because β is still an isomorphism on must-transitions. Regarding Cond. (iii), we only have to consider Rule (May3) for $\alpha \in I' \cup O'$, where $[p \wedge q] \overset{\alpha}{\dashrightarrow} r$ iff $r = [p \wedge q]$. This transition can be matched by the transition $[p] \wedge [q] \overset{\alpha}{\dashrightarrow} [p] \wedge [q]$, which exists by Rule (May3).
- *"$\mathrel{\overset{\frown}{\sqsupseteq}}$":* We show that also β^{-1} is a modal refinement relation. Take $[p] \wedge [q]$ and $[p \wedge q]$; again, Conds. (i) and (ii) are clear. Thus, we only have to consider $\alpha \in I' \cup O'$ for establishing Cond. (iii), so that $[p] \wedge [q] \overset{\alpha}{\dashrightarrow} r$ iff $r = [p'] \wedge [q']$ for $p \overset{\varepsilon}{\Longrightarrow} p'$ and $q \overset{\varepsilon}{\Longrightarrow} q'$. This 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 either Rule (May1), (May2) or (May3), or because $p = p'$ and $q = q'$. □

Theorem 37 ($\wedge$ is And) *Let P with $p \in P$, Q with $q \in Q$, and R with $r \in R$ be Relaxed 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 and $r \in R$ with $r \mathrel{\overset{\frown}{\sqsubseteq}} p$ and $r \mathrel{\overset{\frown}{\sqsubseteq}} q$ iff $p \wedge q$ is defined. Further, in case $p \wedge q$ is defined: (ii) $r \mathrel{\overset{\frown}{\sqsubseteq}} p$ and $r \mathrel{\overset{\frown}{\sqsubseteq}} q$ iff $r \mathrel{\overset{\frown}{\sqsubseteq}} p \wedge q$.*

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, $[[p]_Q]_R = [p]_R$ and $[[q]_P]_R = [q]_R$.

(i) If $r \mathrel{\overset{\frown}{\sqsubseteq}} [p]_R$ and $r \mathrel{\overset{\frown}{\sqsubseteq}} [q]_R$, then $[p]_R \wedge [q]_R$ is defined by Thm. 29. The latter conjunction equals $[[p]_Q]_R \wedge [[q]_P]_R$; hence, $[p]_Q \wedge [q]_P$ is defined by Lemma 36, and this conjunction is $p \wedge q$ by definition. If $[p]_Q \wedge [q]_P$ is defined, there exists R with the common alphabets of $[P]_Q$ and $[Q]_P$ as well as $r \in R$ with $r \mathrel{\overset{\frown}{\sqsubseteq}} [p]_Q$ and $r \mathrel{\overset{\frown}{\sqsubseteq}} [q]_P$ by Thm. 29. For this R, we have $[p]_Q = [p]_R$ and $[q]_P = [q]_R$; thus, $r \mathrel{\overset{\frown}{\sqsubseteq}} p$ and $r \mathrel{\overset{\frown}{\sqsubseteq}} q$ by definition.

(ii) Let $p \wedge q$ be defined. We reason as follows:

$$\begin{array}{lll} & r \mathrel{\widehat{\sqsubseteq}} p \text{ and } r \mathrel{\widehat{\sqsubseteq}} q & \\ \text{iff} & r \mathrel{\widehat{\sqsubseteq}} [p]_R \text{ and } r \mathrel{\widehat{\sqsubseteq}} [q]_R & \text{(by definition)} \\ \text{iff} & r \mathrel{\widehat{\sqsubseteq}} [p]_R \wedge [q]_R & \text{(by Thm. 29)} \\ \text{iff} & r \mathrel{\widehat{\sqsubseteq}} [[p]_Q \wedge [q]_P]_R & \text{(by Lemma 36 and note above)} \\ \text{iff} & r \mathrel{\widehat{\sqsubseteq}} p \wedge q & \text{(by Defs. 33 and 35)} \qquad \square \end{array}$$

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

Definition 38 (Disjunction Operator) Let P, Q be Relaxed MIAs with disjoint state sets, $p \in P$ and $q \in Q$ such that $I_P \cap O_Q = \emptyset = I_Q \cap O_P$. Then, $p \vee' q =_{\mathrm{df}} [p]_Q \vee [q]_P$. Once again, we simply write $p \vee q$ for $p \vee' q$.

Lemma 39 *Let P with $p \in P$ and R with $r \in R$ be Relaxed MIAs having the same alphabets, as well as I' and O' be suitable action sets for extending them. Then, $p \mathrel{\widehat{\sqsubseteq}} r$ iff $[p] \mathrel{\widehat{\sqsubseteq}} [r]$.*

Proof Since we only add may-loops with a fresh label a for the extension, it suffices to observe for Direction "$\Longrightarrow$" and $p \mathrel{\widehat{\sqsubseteq}} r$ that each may-transition $[p] \xrightarrow{a} [p]$ can be matched by $[r] \xrightarrow{a} [r]$. $\square$

Theorem 40 ($\vee$ is Or) *Let P with $p \in P$, Q with $q \in Q$, and R with $r \in R$ be Relaxed MIAs with disjoint state sets 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, $p \vee q \mathrel{\widehat{\sqsubseteq}} r$ iff $p \mathrel{\widehat{\sqsubseteq}} r$ and $q \mathrel{\widehat{\sqsubseteq}} r$.*

Proof The proof proceeds along the following chain of equivalences:

$$\begin{array}{lll} & p \vee q \mathrel{\widehat{\sqsubseteq}} r & \\ \text{iff} & [p]_Q \vee [q]_P \mathrel{\widehat{\sqsubseteq}} [[r]_P]_Q & \text{(by definition)} \\ \text{iff} & [p]_Q \mathrel{\widehat{\sqsubseteq}} [[r]_P]_Q \text{ and } [q]_P \mathrel{\widehat{\sqsubseteq}} [[r]_P]_Q & \text{(by Thm. 31)} \\ \text{iff} & p \mathrel{\widehat{\sqsubseteq}} [r]_P \text{ and } q \mathrel{\widehat{\sqsubseteq}} [r]_Q & \text{(by Lemma 39)} \\ \text{iff} & p \mathrel{\widehat{\sqsubseteq}} r \text{ and } q \mathrel{\widehat{\sqsubseteq}} r & \text{(by definition)} \qquad \square \end{array}$$

3.4 Example

We now return to our example of Fig. 6 and cast this into the pessimistic MIA setting as shown in Fig. 9. The major difference to the optimistic version is that we can now specify component `Sender` $\wedge$ `Resetter` perspective-based, i.e., we do not need the must-loops for inputs `ack`, `nack` and `get` in the conjuncts. This directly reflects that `Resetter` is not concerned with `ack` and `get` at all. Similarly, we do not need the may-loops for outputs `msg` and `nxt` since in Relaxed MIA we may extend output alphabets. The conjunction operator of Relaxed MIA now takes care of unknown actions; for example, the `get`-transition leaving state `Aa` in the conjunction results from the implicit `get`-may-loop at state `a` in `Resetter`.

In Fig. 9 we have also changed the two `nack`-labelled must-transitions of `Resetter` to just may-transitions. Hence, an implementation of `Resetter` may decide, e.g., to initiate a reset after exactly n negative acknowledgments, showing the utility of may-inputs for specification and the modal-refinement preorder. Moreover, we are now able to signal failure in state `4` of `Medium` explicitly via an output must-loop labelled `failed`; this is, again, because Relaxed MIA permits adding outputs in a refinement step. Concretely, `Design` $= (\texttt{Sender} \wedge \texttt{Resetter}) \,|\, \texttt{Medium} \mathrel{\widehat{\sqsubseteq}} \texttt{Spec}$ with the same relation $\mathscr{R}$ as in Sec. 2.3. In particular, observe that, for $(\texttt{Ca4}, \texttt{V}) \in \mathscr{R}$, the `failed`-loop of Ca4 is matched by V due to our implicit alphabet extension in modal-refinement (cf. $\mathrel{\widehat{\sqsubseteq}}'$ of Def. 33).

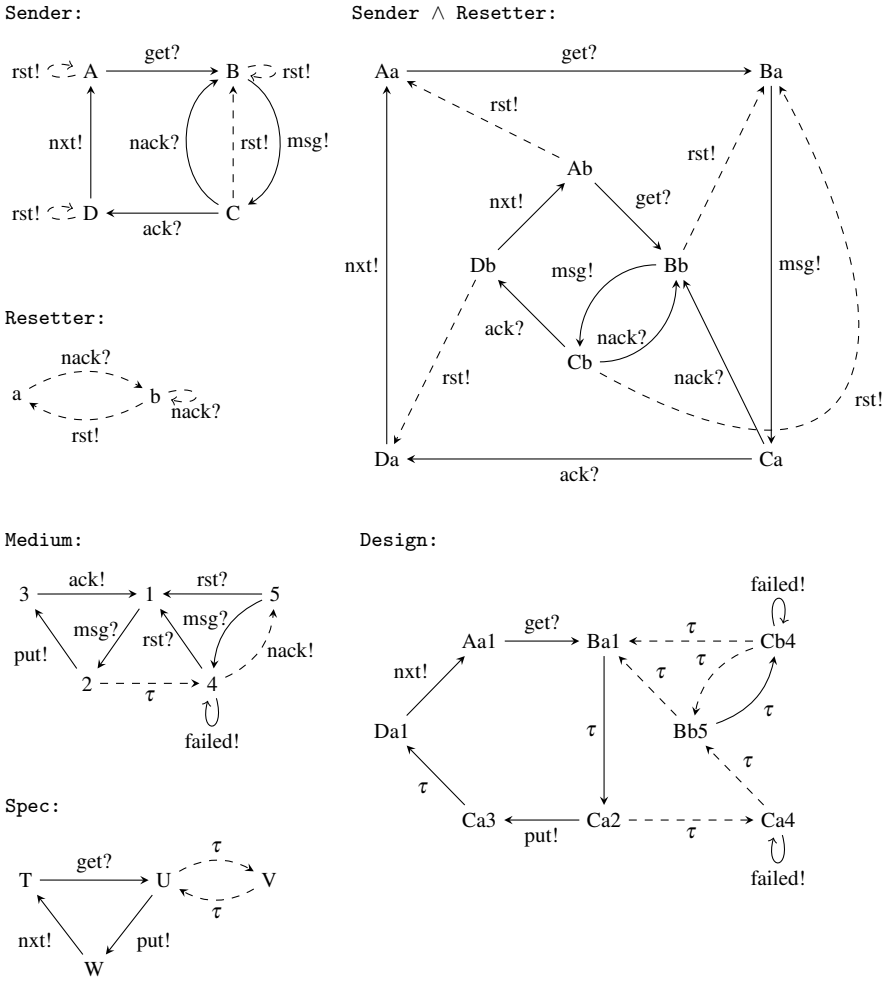

Fig. 9 Example in the pessimistic MIA setting: $\texttt{Design} = (\texttt{Sender} \wedge \texttt{Resetter}) \,|\, \texttt{Medium}$ and $\texttt{Spec}$.

4 Conclusions & Future Work

Interface theories are an important tool for reasoning about component-based systems. This article advanced the state-of-the-art of both the optimistic school [6,9,10,1,15,16,19] and the pessimistic school [3,4] on interface theories:

Regarding the optimistic school, we repaired a shortcoming of the refinement preorder introduced in [15], which ignored internal must-transitions, thereby leading to unintuitive refinements. For the first time in the literature on modal transition systems, we dealt with weak transitions in the presence of disjunctive τ-must-transitions. We also extended our MIA framework [16] so as to handle alphabet modification during refinement along the lines of de Alfaro and Henzinger [1] and of Chilton et al. [9]. This is non-trivial since changing the refinement preorder has direct consequences for the definition of conjunction.

Regarding the pessimistic school, we showed how its approach may be extended by conjunction and disjunction operators; conjunction is a key operator in any component-based setting, which enables engineers to express that some component is required to satisfy several interfaces. In comparison to the optimistic setting, conjunction in the pessimistic setting is better suited for perspective-based specification.

Regarding future work, we wish to investigate whether there are suitable interface theories in-between the optimistic and pessimistic approaches. This might fix their current limitations, namely by allowing may-inputs as in the pessimistic approach while maintaining the truly *open systems* view of the optimistic approach.

We also wish to add a quotienting operator to MIA. In the literature, quotienting has so far only been studied for deterministic interfaces [19,9,10] or nondeterministic systems without internal transitions and input/output-distinction [20,11]. Extending quotienting to our MIA setting will likely be technically challenging. We have done a first step towards this in [7], but for the multicast parallel operator of [19] rather than MIA's handshake parallel composition and for quotients where the divisor – but not the dividend – is still required to be deterministic.

References

1. de Alfaro, L., Henzinger, T.: Interface-based design. In: Engineering Theories of Software-Intensive Systems, *NATO Science Series*, vol. 195. Springer (2005)
2. Bauer, S.: Modal specification theories for component-based design. Ph.D. thesis, Faculty of Mathematics, Informatics and Statistics, LMU Munich, Germany (2012)
3. Bauer, S., David, A., Hennicker, R., Larsen, K., Legay, A., Nyman, U., Wasowski, A.: Moving from specifications to contracts in component-based design. In: FASE, *LNCS*, vol. 7212, pp. 43–58. Springer (2012)
4. Bauer, S., Mayer, P., Schroeder, A., Hennicker, R.: On weak modal compatibility, refinement, and the MIO Workbench. In: TACAS, *LNCS*, vol. 6015, pp. 175–189. Springer (2010)
5. Beneš, N., Cerná, I., Křetínský, J.: Modal transition systems: Composition and LTL model checking. In: T. Bultan, P.A. Hsiung (eds.) ATVA, *LNCS*, vol. 6996, pp. 228–242. Springer (2011)
6. Beyer, D., Chakrabarti, A., Henzinger, T., Seshia, S.: An application of web-service interfaces. In: ICWS, pp. 831–838. IEEE (2007)
7. Bujtor, F., Fendrich, S., Lüttgen, G., Vogler, W.: Nondeterministic modal interfaces. In: Software Seminar (SOFSEM) (2015)
8. Bujtor, F., Vogler, W.: Failure semantics for modal transition systems. In: Application of Concurrency to Systems Design (ACSD) (2014)
9. Chen, T., Chilton, C., Jonsson, B., Kwiatkowska, M.: A compositional specification theory for component behaviours. In: ESOP, *LNCS*, vol. 7211, pp. 148–168. Springer (2012)
10. Chilton, C.: An algebraic theory of componentised interaction. Ph.D. thesis, Department of Computer Science, University of Oxford, UK (2013)
11. Fahrenberg, U., Jan Křetínský, A.L., Traonouez, L.M.: Compositionality for quantitative specifications. In: Formal Aspects of Component Software, LNCS. Springer (2014)
12. Fischbein, D., Uchitel, S.: On correct and complete strong merging of partial behaviour models. In: Foundations of Software Engineering (SIGSOFT FSE), pp. 297–307 (2008)
13. Hatcliff, J., Leavens, G.T., Leino, K.R.M., Müller, P., Parkinson, M.: Behavioral interface specification languages. ACM Comput. Surv. **44**(3), 16:1–16:58 (2012)
14. Larsen, K.: Modal specifications. In: Automatic Verification Methods for Finite State Systems, *LNCS*, vol. 407, pp. 232–246. Springer (1990)
15. Larsen, K., Nyman, U., Wasowski, A.: Modal I/O automata for interface and product line theories. In: ESOP, *LNCS*, vol. 4421, pp. 64–79. Springer (2007)
16. Lüttgen, G., Vogler, W.: Modal interface automata. Logical Methods in Computer Science **9**(3:4) (2013)
17. Meyer, B.: Applying design by contract. IEEE Computer **25**(10), 40–51 (1992)
18. Milner, R.: Communication and Concurrency. Prentice Hall (1989)
19. Raclet, J., Badouel, E., Benveniste, A., Caillaud, B., Legay, A., Passerone, R.: A modal interface theory for component-based design. Fund. Inform. **107**, 1–32 (2011)

20. Raclet, J.B.: Residual for component specifications. ENTCS **215**, 93–110 (2008)
21. Schäfer, M., Vogler, W.: Component refinement and CSC-solving for STG decomposition. Theoret. Comp. Sc. **388**(1-3), 243–266 (2007)

A Proof of Lemma 4(b)–(e)

Proof of Part (b). We show by induction on k that there exists a $\overline{P}_k$ such that $p \stackrel{\hat{\omega}}{\Longrightarrow} \overline{P}_k \subseteq (P' \setminus \{p_1,\ldots,p_k\}) \cup \bigcup_{i=1}^{k} P_i$. 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 $\overline{P}_{k+1} = \overline{P}_k \subseteq (P' \setminus \{p_1,\ldots,p_{k+1}) \cup \bigcup_{i=1}^{k+1} P_i$. Otherwise, $p \stackrel{\hat{\omega}}{\Longrightarrow} \overline{P}_{k+1} \subseteq (\overline{P}_k \setminus \{p_{k+1}\}) \cup P_{k+1}$ by Part (a). Hence, $\overline{P}_{k+1} \subseteq (((P' \setminus \{p_1,\ldots,p_k\}) \cup \bigcup_{i=1}^{k} P_i) \setminus \{p_{k+1}\}) \cup P_{k+1} \subseteq (P' \setminus \{p_1,\ldots,p_{k+1}) \cup \bigcup_{i=1}^{k+1} P_i$. □

Proof of Part (c). The proof proceeds by induction on the overall number of applications of Def. 2(a'). If this is 0, then $\overline{P} =_{\mathrm{df}} \bigcup_{i=1}^{n} P_i$. 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 $p \stackrel{\hat{\omega}}{\Longrightarrow} \hat{P} \subseteq P_1'' \cup \bigcup_{i=2}^{n} P_i'$. If $p_1 \notin \hat{P}$, then $\hat{P} \subseteq \bigcup_{i=1}^{n} P_i'$ and we are done. Otherwise, $p \stackrel{\hat{\omega}}{\Longrightarrow} \overline{P} =_{\mathrm{df}} (\hat{P} \setminus \{p_1\}) \cup P''$. 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 $\overline{P} \subseteq \bigcup_{i=1}^{n} P_i'$. □

Proof of Part (d). The proof is by induction on the derivation of $P \stackrel{\varepsilon}{\Longrightarrow} P'$. For $P = P'$, choose $\overline{P} =_{\mathrm{df}} P''$. 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, $\overline{P} =_{\mathrm{df}} (\overline{P}' \setminus \{p\}) \cup \hat{P}' \subseteq P'$. □

Proof of Part (e). For $1 \leq i \leq n$, we have $p_i \stackrel{\varepsilon}{\Longrightarrow} P_i' = \{p_1^i,\ldots,p_{k_i}^i\}$ such that $p_j^i \stackrel{o}{\longrightarrow} P_j^i$ for $1 \leq j \leq k_i$, and can derive $p_i \stackrel{o}{\Longrightarrow} P_i$ from $p_i \stackrel{o}{\Longrightarrow} \bigcup_{j=1}^{k_i} P_j^i$ by repeated application of Def. 2(a), 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(b) we get $p \stackrel{o}{\Longrightarrow} U$, 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 $p \stackrel{o}{\Longrightarrow} \overline{P}$ such that $\overline{P}$ is contained in the union of the resp. $P_j^{\prime i}$ and, thus, in $\bigcup_{i=1}^{n} P_i$. □