Department of Computer Science

An Algebraic Theory of Interface Automata

Chris Chilton, Bengt Jonsson, and Marta Kwiatkowska

CS-RR-13-02

Department of Computer Science, University of Oxford
Wolfson Building, Parks Road, Oxford, OX1 3QD

An Algebraic Theory of Interface Automata

Chris Chilton[a], Bengt Jonsson[b], Marta Kwiatkowska[a]

[a]*Department of Computer Science, University of Oxford, UK*
[b]*Department of Information Technology, Uppsala University, Sweden*

Abstract

We formulate a compositional specification theory for interface automata, where a component model specifies the allowed sequences of input and output interactions with the environment. A trace-based linear-time refinement is provided, which is the weakest preorder preserving substitutivity of components, and is weaker than the classical alternating simulation defined on interface automata. Since our refinement allows a component to be refined by refusing to produce any output, we also define a refinement relation that guarantees safety and progress. The theory includes the operations of parallel composition to support the structural composition of components, logical conjunction and disjunction for independent development, hiding to support abstraction of interfaces, and quotient for incremental synthesis of components. Our component formulation highlights the algebraic properties of the specification theory for both refinement preorders, and is shown to be fully abstract with respect to observation of communication mismatches. Examples of independent and incremental component development are provided.

Keywords: component-based design, interfaces, specification theory, compositionality, refinement, substitutivity, synthesis

1. Introduction

Interface automata (de Alfaro and Henzinger, 2001) are an influential formalism for modelling the interactions between components and their environment. Components are assumed to communicate by synchronisation of input and output (I/O) actions, with the understanding that outputs are non-blocking. If an output is issued when a component is unwilling to receive it, a communication mismatch is said to occur. This allows one to reason about the allowed behaviours of the environment, which is crucial for, e.g., assume-guarantee reasoning.

An important paradigm for developing complex reactive systems is component-based design, which should be supported by a specification theory. A specification captures the requirements for a component to function in the intended system context, while operators and refinement relations allow for the composing and comparing of specifications in analogy with how components are composed and refined towards the overall system design. Substitutive refinement is essential for dynamic systems of components, as it allows for the replacing of components without introducing errors into the system.

The original theory of interface automata defines a substitutive refinement in terms of alternating simulation (Alur et al., 1998), along with a parallel composition operator for observing component interaction. In subsequent papers, variants of the framework have also been extended with additional operators, including conjunction (defined for synchronous automata by Doyen et al. (2008)) and quotient for supporting incremental development (defined for deterministic automata by Bhaduri and Ramesh (2008)).

In this article, we formulate a theory for components that is conceptually similar to interface automata, but is based on a linear-time notion of substitutive refinement involving trace containment. We define a specification theory for component behaviours, which includes the operations of: *parallel composition* for structural composition of components; *conjunction* for supporting independent development, by constructing a component that will work in any environment compatible with at least one of its arguments; *disjunction* for constructing a component that has an environment compatible for both of its operands; *hiding* to support abstraction in hierarchical development; and *quotient* for incrementally synthesising new components to satisfy partial requirements. We prove compositionality for all the operations and show that the specification theory enjoys strong algebraic properties.

Our formalism addresses the following shortcomings of the interface automata theory as formulated by de Alfaro and Henzinger (2001):

- Alternating simulation is conceptually more complex than refinement based on trace containment, which is standard in widely used theories such as CSP (Brookes et al., 1984) and I/O automata (Lynch and Tuttle, 1989; Jonsson, 1994). Further, alternating simulation is overly strong in comparison to our refinement based on traces, which is the weakest preorder preserving compatibility with the environment.

- It is not clear how to extend a refinement relation based on alternating simulation so that it also preserves liveness properties. This should be

contrasted with the conceptually simple handling of liveness properties in formalisms such as I/O automata, which use trace inclusion. In the case of our refinement, we are able to extend it with the notion of quiescence to guarantee observational progress, in addition to substitutivity. We prove that compositionality results for all the operations continue to hold for this enhanced refinement.

The contribution of this article is therefore a compositional, linear-time specification theory for interface automata based on fully abstract substitutive and progress-preserving refinement. Our framework includes all desirable operations on components known from the literature, and satisfies strong algebraic properties, including characterisation of conjunction and disjunction, respectively, as the meet and join of the refinement preorder. The theory naturally supports a component-based design process that starts from some initial design considerations and applies the operations of the theory compositionally and in a stepwise fashion, relying on substitutivity to guarantee that no errors will be introduced even if components are refined at runtime.

A preliminary version of this article appeared as (Chen et al., 2012), where we introduced the operations of parallel, conjunction and quotient, but did not consider an extension with quiescence. To demonstrate the applicability of the theory in component-based design, the quotient operation was used to synthesise mediator components in (Inverardi and Tivoli, 2013). The flexibility and expressiveness of our specification theory has been shown through a compositional assume-guarantee reasoning framework (Chilton et al., 2013) and a real-time extension (Chilton et al., 2012).

1.1. Related Work

Interface automata. These are essentially finite state automata with I/O distinction on actions (de Alfaro and Henzinger, 2001). The models in this article are conceptually similar, except that our refinement preorder is a linear-time alternative to the alternating simulation of Alur et al. (1998) defined on interface automata. Both refinements are substitutive, but alternating simulation is overly strong due to the conflict between non-determinism in the automaton and the selection of a matching transition to complete the simulation. We essentially work with the same notion of parallel composition as on interface automata, except that we encode inconsistency due to communication mismatches explicitly in the model. To the best of our knowledge, conjunction and disjunction have not been defined on interface automata, although Doyen et al. (2008) define conjunction (called shared refinement) on

a synchronous component model. A definition of quotient has been provided for deterministic interface automata by Bhaduri and Ramesh (2008), which mirrors the method developed by Verhoeff (1994).

I/O automata. Due to Lynch and Tuttle (1989); Jonsson (1994), I/O automata are conceptually similar to interface automata, except that each state is required to be input-enabled. This input receptiveness means that communication mismatches cannot arise between a component and its environment. Consequently, substitutive refinement can be cast in terms of trace containment (Jonsson, 1994). The operation of parallel composition is defined in the same way as for interface automata, except that consideration need not be given to inconsistencies. Conjunction can be defined as a synchronous product, meaning that its set of traces is the intersection of its operands' traces. Disjunction can be defined similarly. Hiding is already defined on outputs (Jonsson, 1994) and quotient can be defined in a straightforward manner (Drissi and v. Bochmann, 1999).

We mention a process-algebraic characterisation of I/O automata due to de Nicola and Segala (1995), which is also applicable to interface automata, since a process exhibits chaotic behaviour on receiving a non-enabled input. Refinement is defined by trace inclusion, but this does not extend to inconsistent trace containment. Consequently, the theory is not able to distinguish a non-enabled input from one that is enabled and can subsequently behave chaotically. Furthermore, high-level operations such as conjunction and quotient are not defined. Note that CCS (Milner, 1980) merely has a syntactic distinction of inputs from outputs, so we give it no further attention.

Logic LTSs. These are labelled transition system (LTS) models, without I/O distinction, augmented by an inconsistency predicate on states (Lüttgen and Vogler, 2007). A number of compositional operators are considered (parallel composition, conjunction, disjunction, external choice, and hiding (Lüttgen and Vogler, 2010)), and refinement is given by ready-simulation, a branching time relation that requires the refining component not to introduce any new inconsistency and equality of offered actions at each state in the simulation chain. This formulation of refinement differs from our intuition behind substitutivity, meaning that their operations, such as conjunction, are incomparable to ours. Taking inspiration from Lüttgen and Vogler (2007), in Section 4 we formulate an operational model of components that are I/O automata augmented by an inconsistency predicate for indicating communication mismatches (and, consequently, non-enabled inputs), making our

formalism achieve similar goals as interface automata, but with notation and semantics derived from I/O automata and Logic LTSs.

Circuit trace structures. Dill (1988) presents a trace-based theory for modelling circuits, with I/O distinction, which conceptually uses the same basic semantic model as in our framework. A circuit can be characterised by prefix closed sets of traces, which corresponds exactly with our component model in Section 2. Dill's conformance is also similar to our substitutive refinement, except that we generalise this to allow non-identical (static) interfaces, but his liveness extension is based on infinite traces, rather than finite traces and quiescence. Further, compared to Dill (1988), we formulate a richer collection of compositional operators.

Receptive process theory. Josephs et al. (1989) formulate an I/O extension of CSP (Hoare, 1985) for modelling asynchronous circuits. The work differs from ours in that processes must communicate through unbounded buffers, which eliminates the possibility of communication errors arising through non-enabledness of inputs. Avoiding this, Josephs (1992) formulates a theory of receptive processes, where components must communicate directly with one another. This has connections to our liveness framework, since a receptive process is modelled by means of its failures (communication mismatches and divergences) and quiescent traces (violations of liveness). Consequently, the refinement relation is similar to our progress-sensitive refinement, except that we give an explicit treatment of divergence. Josephs' work does not consider conjunction and quotient (the latter is defined on the restricted class of delay-insensitive networks (Josephs and Kapoor, 2007), where it is referred to as factorisation; however, this does not match our setting).

Modal interfaces. A modal specification characterises sequences of (non I/O) interactions between a component and its environment, along with modalities on the interactions, indicating whether an interaction may or must be possible. Raclet et al. (2009a,b, 2011) introduce a specification theory for modal specifications that considers a substitutive refinement relation, along with the operations of parallel composition, conjunction and quotient (Raclet, 2008). Their notion of liveness and progress is based on must-modalities, and thus differs from our trace-based formulation. The theory is extended in Raclet et al. (2009b, 2011) to modal interfaces (modal specifications with I/O distinction), where a mapping is given from deterministic interface automata without hidden actions to modal interfaces. This is similar to the

theory of Larsen et al. (2007), except that: a number of technical issues are resolved, relating to compatibility and parallel composition; refinement is based on trace-containment, rather than being game-based; and additional compositional operators are defined.

A weakness of Raclet et al. (2009b, 2011) is that the compositionality results for the different operators must be given with respect to either strong or weak refinement relations (the former for parallel and quotient, the latter for conjunction) when the components to be composed have dissimilar alphabets. This has repercussions for parallel composition, which is an asynchronous operator on interface automata, but is treated synchronously on modal interfaces by a lifting on alphabets. This lifting is essentially equivalent to requiring that a refining component is enabled in every state on each input that is not in the interface of the original component. Consequently, there are also differences between the quotient operators of the two frameworks, since they should be the adjoint of their respective parallel operations.

Ioco-testing theory. Our work is related to the ioco theory for model based testing (Tretmans, 2011), which only considers the operators of parallel composition, hiding and choice. Aarts and Vaandrager (2010) show the similarities between interface automata and the ioco theory. A key result of that paper relates quiescence-extended alternating simulation refinement on interface automata with the ioco relation, under determinism of models. In comparison with our framework, this implies that the ioco relation coincides with our progress-sensitive refinement for components free of divergence.

1.2. Outline

Section 2 begins by introducing a trace-based theory of interface automata, and defines substitutive refinement, along with the collection of compositional operators. In Section 3, we extend the trace-based theory by formulating a refinement preorder guaranteeing substitutivity along with preservation of progress, for which we generalise the compositional operators. An operational theory of components is presented in Section 4, for both the substitutive and progress-sensitive frameworks. A detailed comparison of our work with interface automata is given in Section 5, while Section 6 concludes. Proofs for our claims can be found in the appendix.

2. A Trace-Based Theory of Substitutable Components

In this section, we introduce a trace-based representation for components modelled as interface automata. The formulation captures the essential information relating to whether a component can work in an arbitrary environment without introducing communication mismatches, which is vital for checking substitutability of components. Based on this representation, we introduce a weakest refinement relation preserving safe substitutivity of components and provide definitions of compositional operators for our theory.

Definition 1 (Component). *A* component $\mathcal{P}$ *is a tuple* $\langle \mathcal{A}^I_\mathcal{P}, \mathcal{A}^O_\mathcal{P}, T_\mathcal{P}, F_\mathcal{P} \rangle$ *in which* $\mathcal{A}^I_\mathcal{P}$ *and* $\mathcal{A}^O_\mathcal{P}$ *are disjoint sets referred to as the inputs and outputs respectively (the union of which is denoted by* $\mathcal{A}_\mathcal{P}$*),* $T_\mathcal{P} \subseteq \mathcal{A}^*_\mathcal{P}$ *is a set of observable traces, and* $F_\mathcal{P} \subseteq \mathcal{A}^*_\mathcal{P}$ *is a set of inconsistent traces. The trace sets must satisfy the constraints:*

1. $F_\mathcal{P} \subseteq T_\mathcal{P}$
2. $T_\mathcal{P}$ *is prefix closed*
3. *If* $t \in T_\mathcal{P}$ *and* $t' \in (\mathcal{A}^I_\mathcal{P})^*$*, then* $tt' \in T_\mathcal{P}$
4. *If* $t \in F_\mathcal{P}$ *and* $t' \in \mathcal{A}^*_\mathcal{P}$*, then* $tt' \in F_\mathcal{P}$*.*

If $\epsilon \notin T_\mathcal{P}$*, we say that* $\mathcal{P}$ *is unrealisable, and is realisable contrariwise.*

The sets $\mathcal{A}^I_\mathcal{P}$ and $\mathcal{A}^O_\mathcal{P}$ make up the *interface* of $\mathcal{P}$, i.e., the interaction primitives that the component is willing to observe, while the trace sets encode the possible interaction sequences over the component's interface. $T_\mathcal{P}$ consists of all *observable* traces of interactions that can arise between the component and the environment. As inputs are controlled by the environment, any trace in $T_\mathcal{P}$ is extendable by a sequence of inputs, since the component cannot prevent these inputs from being issued. Traces contained in $F_\mathcal{P}$ are deemed to be *inconsistent*, which can encode, e.g., run-time errors and communication mismatches. As interface automata are not required to be input receptive, we use $F_\mathcal{P}$ to record the traces in $T_\mathcal{P}$ that involve non-enabled inputs. Under this treatment of inputs, we say that our theory is *not* input enabled, even though $T_\mathcal{P}$ is closed under input extensions. Once an inconsistency has arisen, the resulting behaviour is unspecified, so we assume that subsequent observations of the component are chaotic.

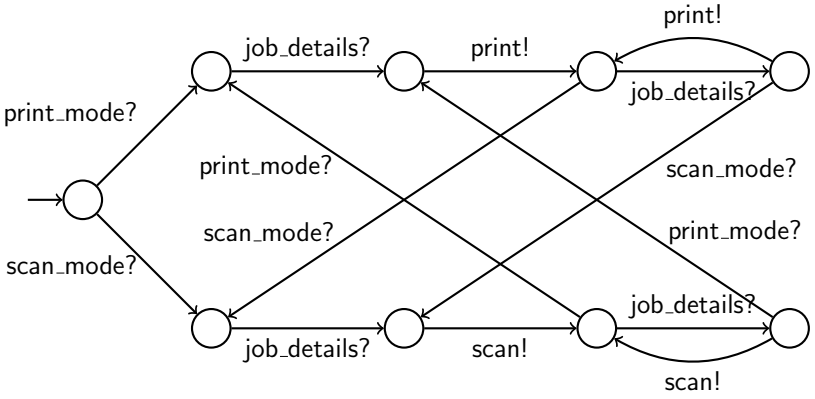

Figure 1: Multi-function Device.

Example 1. *Throughout this article, we use the following running example to demonstrate the suitability of our framework for component-based design. A multi-function device capable of printing and scanning is modelled as a component* Device *in Figure 1. The device can be placed in* print_mode *or* scan_mode*, can receive* job_details*, and can* print *and* scan*. From the perspective of the device, actions* print *and* scan *should be treated as outputs (indicated by* !*), while all other actions are inputs (indicated by* ?*).*

Concerning the diagrammatic representation, the interface of a component is given by the actions labelling transitions in the figure (note that, in general, the interface may contain actions that do not occur in a component's behaviour). For compactness, we avoid giving an explicit representation for input transitions immediately leading to an inconsistent state, since they can be inferred due to the requirement of components being receptive.

From hereon let $\mathcal{P}$, $\mathcal{Q}$ and $\mathcal{R}$ be components with signatures $\langle \mathcal{A}^I_{\mathcal{P}}, \mathcal{A}^O_{\mathcal{P}}, T_{\mathcal{P}}, F_{\mathcal{P}} \rangle$, $\langle \mathcal{A}^I_{\mathcal{Q}}, \mathcal{A}^O_{\mathcal{Q}}, T_{\mathcal{Q}}, F_{\mathcal{Q}} \rangle$ and $\langle \mathcal{A}^I_{\mathcal{R}}, \mathcal{A}^O_{\mathcal{R}}, T_{\mathcal{R}}, F_{\mathcal{R}} \rangle$ respectively.

Notation. Let $\mathcal{A}$ and $\mathcal{B}$ be sets of actions. For a trace t, write $t \restriction \mathcal{A}$ for the projection of t onto $\mathcal{A}$. Now for $T \subseteq \mathcal{A}^*$, write $T \restriction \mathcal{B}$ for $\{t \restriction \mathcal{B} : t \in T\}$, $T \Uparrow \mathcal{B}$ for $\{t \in \mathcal{B}^* : t \restriction \mathcal{A} \in T\}$ and $T \uparrow \mathcal{B}$ for $T(\mathcal{B} \setminus \mathcal{A})(\mathcal{A} \cup \mathcal{B})^*$.

2.1. Refinement

The refinement relation on components should support safe substitutivity, meaning that, for $\mathcal{Q}$ to be used in place of $\mathcal{P}$, we require that $\mathcal{Q}$ exists safely in *every* environment that is safe for $\mathcal{P}$. Whether an environment is safe

or not for a component depends on the interaction sequences between the two. The affirmative holds if the environment can prevent the component from performing an inconsistent trace. As outputs are controlled by the component, it follows that a safe environment must refuse to issue an input on any trace from which there is a sequence of output actions that allow the trace to become inconsistent.

Given a component $\mathcal{P}$, we can formulate the most general safe component $\mathcal{E}(\mathcal{P})$, containing all of $\mathcal{P}$'s observable and inconsistent traces, but satisfying the additional property: if $t \in T_{\mathcal{P}}$ and there exists $t' \in (\mathcal{A}^O_{\mathcal{P}})^*$ such that $tt' \in F_{\mathcal{P}}$, then $t \in F_{\mathcal{E}(\mathcal{P})}$. This has the effect of making the component immediately inconsistent whenever it has the potential to become inconsistent under its own control. If the environment respects this safe component, by not issuing any input that results in an inconsistent trace, then the component can never encounter an inconsistent trace. Note that if $\epsilon \in F_{\mathcal{E}(\mathcal{P})}$ then there is no environment that can prevent $\mathcal{P}$ from performing an inconsistent trace. However, for uniformity we still refer to $\mathcal{E}(\mathcal{P})$ as the safe component of $\mathcal{P}$.

Definition 2. *The* safe component *for* $\mathcal{P}$ *is defined as* $\mathcal{E}(\mathcal{P}) = \langle \mathcal{A}^I_{\mathcal{P}}, \mathcal{A}^O_{\mathcal{P}}, T_{\mathcal{P}} \cup F_{\mathcal{E}(\mathcal{P})}, F_{\mathcal{E}(\mathcal{P})} \rangle$*, where* $F_{\mathcal{E}(\mathcal{P})} = \{t \in T_{\mathcal{P}} : \exists t' \in (\mathcal{A}^O_{\mathcal{P}})^* \cdot tt' \in F_{\mathcal{P}}\} \cdot \mathcal{A}^*_{\mathcal{P}}$.

Based on safe components, we can now give the formal definition of substitutive refinement.

Definition 3 (Refinement). $\mathcal{Q}$ *is said to be a* refinement *of* $\mathcal{P}$*, written* $\mathcal{Q} \sqsubseteq_{imp} \mathcal{P}$*, iff:*

I1. $\mathcal{A}^I_{\mathcal{P}} \subseteq \mathcal{A}^I_{\mathcal{Q}}$

I2. $\mathcal{A}^O_{\mathcal{Q}} \subseteq \mathcal{A}^O_{\mathcal{P}}$

I3. $\mathcal{A}^I_{\mathcal{Q}} \cap \mathcal{A}^O_{\mathcal{P}} = \emptyset$

I4. $T_{\mathcal{E}(\mathcal{Q})} \subseteq T_{\mathcal{E}(\mathcal{P})} \cup (T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{Q}})$

I5. $F_{\mathcal{E}(\mathcal{Q})} \subseteq F_{\mathcal{E}(\mathcal{P})} \cup (T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{Q}})$.

For $\mathcal{Q}$ to be a refinement of $\mathcal{P}$, the interface of $\mathcal{Q}$ must be substitutable for the interface of $\mathcal{P}$, meaning that $\mathcal{Q}$ must be willing to accept all of $\mathcal{P}$'s inputs, while it must produce only a subset of $\mathcal{P}$'s outputs, as witnessed by I1 and I2. Condition I3 ensures that $\mathcal{P}$ and $\mathcal{Q}$ are *compatible*, that is, they are

not allowed to mix action types. In Chen et al. (2012) we did not impose this constraint, as it is not necessary to guarantee substitutivity. However, in this article we choose to include the constraint for three reasons: (i) it is not necessarily meaningful to convert outputs into inputs during refinement; (ii) compositionality of hiding does not hold without this constraint; and (iii) mixing of action types is problematic for assume-guarantee reasoning, which deals with the behaviour of the environment.

Condition I4 ensures that the observable behaviour of $\mathcal{Q}$ is contained within the behaviour of $\mathcal{P}$, except for when an input in $\mathcal{A}_{\mathcal{Q}}^I \setminus \mathcal{A}_{\mathcal{P}}^I$ is encountered. The lifting $T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}_{\mathcal{Q}}^I$ represents the extension of $\mathcal{P}$'s interface to include all inputs in $\mathcal{A}_{\mathcal{Q}}^I \setminus \mathcal{A}_{\mathcal{P}}^I$. As these inputs are not accepted by $\mathcal{P}$, they are treated as bad inputs, hence the suffix closure with arbitrary (chaotic) behaviour. Finally, condition I5 ensures that $\mathcal{Q}$ cannot introduce any new errors that are not in $\mathcal{P}$'s behaviour. Note that checking $F_{\mathcal{Q}} \subseteq F_{\mathcal{P}} \cup (T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}_{\mathcal{Q}}^I)$ would be too strong to use for the last clause, as we are only interested in trace containment up to the point where an environment can issue a bad input, from which the component can become inconsistent autonomously.

Definition 4. *$\mathcal{P}$ and $\mathcal{Q}$ are said to be* equivalent*, written $\mathcal{P} \equiv_{imp} \mathcal{Q}$, iff $\mathcal{P} \sqsubseteq_{imp} \mathcal{Q}$ and $\mathcal{Q} \sqsubseteq_{imp} \mathcal{P}$.*

Lemma 1. *Refinement is reflexive, and is transitive subject to preservation of action types: $\mathcal{R} \sqsubseteq_{imp} \mathcal{Q}$, $\mathcal{Q} \sqsubseteq_{imp} \mathcal{P}$ and $\mathcal{A}_{\mathcal{R}}^I \cap \mathcal{A}_{\mathcal{P}}^O = \emptyset$ implies $\mathcal{R} \sqsubseteq_{imp} \mathcal{P}$.*

We are now in a position to define the compositional operators of our theory. In general, the compositional operators are only partially defined, specifically on components that are said to be *composable*. This is a syntactic check on the interfaces of the components to be composed, which ensures that their composition is meaningful. For each operator, we state the required composability constraints.

2.2. Parallel Composition

The parallel composition of two components yields a component representing the combined effect of its operands running asynchronously. The composition is obtained by synchronising on common actions and interleaving on independent actions. This makes sense even in the presence of non-blocking outputs, because communication mismatches arising through non-enabledness of inputs automatically appear as inconsistent traces in the

composition, on account of our component formulation. To support broadcasting, we make the assumption that inputs and outputs synchronise to produce outputs. As the outputs of a component are controlled locally, we also assume that the output actions of the components to be composed are disjoint, in which case we say that the components are *composable*. In practice, components that are not composable can be made so by employing renaming.

Definition 5. *Let $\mathcal{P}$ and $\mathcal{Q}$ be composable for parallel, i.e., $\mathcal{A}^O_\mathcal{P} \cap \mathcal{A}^O_\mathcal{Q} = \emptyset$. Then $\mathcal{P} \,||\, \mathcal{Q}$ is the component $\langle \mathcal{A}^I_{\mathcal{P}||\mathcal{Q}}, \mathcal{A}^O_{\mathcal{P}||\mathcal{Q}}, T_{\mathcal{P}||\mathcal{Q}}, F_{\mathcal{P}||\mathcal{Q}} \rangle$, where:*

- $\mathcal{A}^I_{\mathcal{P}||\mathcal{Q}} = (\mathcal{A}^I_\mathcal{P} \cup \mathcal{A}^I_\mathcal{Q}) \setminus (\mathcal{A}^O_\mathcal{P} \cup \mathcal{A}^O_\mathcal{Q})$
- $\mathcal{A}^O_{\mathcal{P}||\mathcal{Q}} = \mathcal{A}^O_\mathcal{P} \cup \mathcal{A}^O_\mathcal{Q}$
- $T_{\mathcal{P}||\mathcal{Q}} = [(T_\mathcal{P} \Uparrow \mathcal{A}_{\mathcal{P}||\mathcal{Q}}) \cap (T_\mathcal{Q} \Uparrow \mathcal{A}_{\mathcal{P}||\mathcal{Q}})] \cup F_{\mathcal{P}||\mathcal{Q}}$
- $F_{\mathcal{P}||\mathcal{Q}} = [(T_\mathcal{P} \Uparrow \mathcal{A}_{\mathcal{P}||\mathcal{Q}}) \cap (F_\mathcal{Q} \Uparrow \mathcal{A}_{\mathcal{P}||\mathcal{Q}})]\mathcal{A}^*_{\mathcal{P}||\mathcal{Q}} \cup$
  $[(F_\mathcal{P} \Uparrow \mathcal{A}_{\mathcal{P}||\mathcal{Q}}) \cap (T_\mathcal{Q} \Uparrow \mathcal{A}_{\mathcal{P}||\mathcal{Q}})]\mathcal{A}^*_{\mathcal{P}||\mathcal{Q}}$.

In words, the observable traces of the composition are simply those traces that are inconsistent, plus any trace whose projection onto $\mathcal{A}_\mathcal{P}$ is a trace of $\mathcal{P}$ and whose projection onto $\mathcal{A}_\mathcal{Q}$ is a trace of $\mathcal{Q}$. A trace is inconsistent if it has a prefix whose projection onto the alphabet of one of the components is inconsistent and the projection onto the alphabet of the other component is an observable trace of that component.

The definition of parallel composition for interface automata (de Alfaro and Henzinger, 2001) also includes backward propagation of inconsistencies. In our framework, this is not necessary, since backward propagation of inconsistencies is implicitly performed in our definition of refinement.

Lemma 2. *Parallel composition is associative and commutative.*

The following result shows that parallel composition is monotonic on refinement, subject to restrictions on the interfaces to be composed and composability. A corollary of this result is that mutual refinement is a congruence for parallel, subject (only) to composability.

Theorem 1. *Let $\mathcal{P}$, $\mathcal{Q}$, $\mathcal{P}'$ and $\mathcal{Q}'$ be components such that $\mathcal{P}$ and $\mathcal{Q}$ are composable, $\mathcal{A}_{\mathcal{P}'} \cap \mathcal{A}_{\mathcal{Q}'} \cap \mathcal{A}_{\mathcal{P}||\mathcal{Q}} \subseteq \mathcal{A}_\mathcal{P} \cap \mathcal{A}_\mathcal{Q}$ and $\mathcal{A}^O_{\mathcal{P}||\mathcal{Q}} \cap \mathcal{A}^I_{\mathcal{P}'||\mathcal{Q}'} = \emptyset$. If $\mathcal{P}' \sqsubseteq_{imp} \mathcal{P}$ and $\mathcal{Q}' \sqsubseteq_{imp} \mathcal{Q}$, then $\mathcal{P}' \,||\, \mathcal{Q}' \sqsubseteq_{imp} \mathcal{P} \,||\, \mathcal{Q}$.*

Note that, in Raclet et al. (2011), parallel composition is claimed to be monotonic for modal interfaces without any conditions on the interfaces (except for composability). This is due to the fact that they use strong refinement, based on a strong lifting, which is more restrictive than $\sqsubseteq_{imp}$.

Example 2. *The most liberal* User *that can interact with the* Device *(shown in Figure 1) is a component obtained from* Device *by interchanging inputs and outputs (given that we do not explicitly represent traces making the component receptive). The definition of parallel composition guarantees that the composition of the* Device *along with the resultant* User *is free of inconsistencies (i.e., communication mismatches), and is a transition system equal to that of the* Device *and the* User*, but with all actions converted to outputs.*

Note that, if a user wished to perform the trace print_mode! scan_mode!*, then this would also be a trace in the parallel composition, since* print_mode? scan_mode? *is a trace of* Device*, albeit an inconsistent one, which is why it is not explicitly represented in Figure 1. Consequently, the trace would also be inconsistent in the parallel composition.*

2.3. Conjunction

The conjunction operator on components can be thought of as supporting independent development, in the sense that it yields the coarsest component that will work in any environment safe for at least one of its operands. Consequently, the conjunction of components is the coarsest component that is a refinement of its operands (i.e. is the meet operator), which is why it is frequently referred to as the *shared refinement* operator (Doyen et al., 2008; Raclet et al., 2009b).

In a number of frameworks, including (Lüttgen and Vogler, 2007), conjunction represents synchronous parallel composition, formed as the intersection of the good behaviours of the components to be composed. In contrast, our conjunction is a *substitutive refinement* of each component. Therefore, an input must be accepted in the conjunction if at least one of the components accepts it, while an input should be accepted in the synchronous parallel only if all of the appropriately alphabetised components accept it.

Conjunction is only defined on composable components, where $\mathcal{P}$ and $\mathcal{Q}$ are composable for conjunction if the sets $\mathcal{A}^I_\mathcal{P} \cup \mathcal{A}^I_\mathcal{Q}$ and $\mathcal{A}^O_\mathcal{P} \cup \mathcal{A}^O_\mathcal{Q}$ are disjoint.

Definition 6. *Let $\mathcal{P}$ and $\mathcal{Q}$ be components composable for conjunction, i.e., such that the sets $\mathcal{A}^I_\mathcal{P} \cup \mathcal{A}^I_\mathcal{Q}$ and $\mathcal{A}^O_\mathcal{P} \cup \mathcal{A}^O_\mathcal{Q}$ are disjoint. Then $\mathcal{P} \wedge \mathcal{Q}$ is the component $\langle \mathcal{A}^I_{\mathcal{P}\wedge\mathcal{Q}}, \mathcal{A}^O_{\mathcal{P}\wedge\mathcal{Q}}, T_{\mathcal{P}\wedge\mathcal{Q}}, F_{\mathcal{P}\wedge\mathcal{Q}} \rangle$, where:*

- $\mathcal{A}^I_{\mathcal{P}\wedge\mathcal{Q}} = \mathcal{A}^I_{\mathcal{P}} \cup \mathcal{A}^I_{\mathcal{Q}}$
- $\mathcal{A}^O_{\mathcal{P}\wedge\mathcal{Q}} = \mathcal{A}^O_{\mathcal{P}} \cap \mathcal{A}^O_{\mathcal{Q}}$
- $T_{\mathcal{P}\wedge\mathcal{Q}} = (T_{\mathcal{P}} \cup (T_{\mathcal{P}} \uparrow \mathcal{A}^I_{\mathcal{Q}})) \cap (T_{\mathcal{Q}} \cup (T_{\mathcal{Q}} \uparrow \mathcal{A}^I_{\mathcal{P}}))$
- $F_{\mathcal{P}\wedge\mathcal{Q}} = (F_{\mathcal{P}} \cup (T_{\mathcal{P}} \uparrow \mathcal{A}^I_{\mathcal{Q}})) \cap (F_{\mathcal{Q}} \cup (T_{\mathcal{Q}} \uparrow \mathcal{A}^I_{\mathcal{P}}))$.

The T and F sets are defined such that any trace in the conjunction is a trace of both $\mathcal{P}$ and $\mathcal{Q}$, unless if there is an input along the trace that does not belong in the alphabet of one of the components (say $\mathcal{Q}$). On encountering such an input, the remainder of the trace would be in $T_{\mathcal{Q}} \uparrow \mathcal{A}^I_{\mathcal{P}}$, which has the effect of leaving the behaviour of $\mathcal{P}$ unconstrained.

Lemma 3. *Conjunction is associative, commutative and idempotent.*

The following theorem demonstrates that conjunction really does correspond to the meet operator, and that it is monotonic under refinement, subject to composability.

Theorem 2. *Let $\mathcal{P}$ and $\mathcal{Q}$, and $\mathcal{P}'$ and $\mathcal{Q}'$, be components composable for conjunction. Then:*

- $\mathcal{P} \wedge \mathcal{Q} \sqsubseteq_{imp} \mathcal{P}$ *and* $\mathcal{P} \wedge \mathcal{Q} \sqsubseteq_{imp} \mathcal{Q}$
- $\mathcal{R} \sqsubseteq_{imp} \mathcal{P}$ *and* $\mathcal{R} \sqsubseteq_{imp} \mathcal{Q}$ *implies* $\mathcal{R} \sqsubseteq_{imp} \mathcal{P} \wedge \mathcal{Q}$
- $\mathcal{P}' \sqsubseteq_{imp} \mathcal{P}$ *and* $\mathcal{Q}' \sqsubseteq_{imp} \mathcal{Q}$ *implies* $\mathcal{P}' \wedge \mathcal{Q}' \sqsubseteq_{imp} \mathcal{P} \wedge \mathcal{Q}$.

Example 3. *To demonstrate conjunction, we consider a device that is capable of printing and faxing documents. The behaviour of this device is shown in Figure 2. Note how this device is capable of* print*ing multiple documents after having received* job_details *(indicated by the self-loop labelled with* print*).*

The conjunction of the original multi-function device (capable of printing and scanning, shown in Figure 1) along with this new printing/faxing device is shown in Figure 3. The resulting device is responsive to the inputs that can be issued for each of the separate devices, but is only willing to perform functions that can be executed by both. Therefore, the resulting device is unable to scan *or* fax *documents, even though it can be placed in these modes. Moreover, the device is only able to* print *a single document after having received*

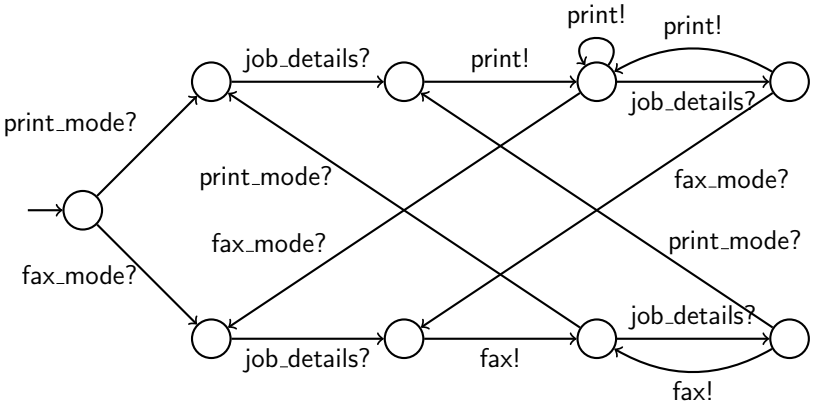

Figure 2: A printing and faxing device.

job_details. *Such behaviour may seem unnecessarily restrictive and undesirable; however, the resulting device is the most general that can be used safely in place of the original printing/scanning device and the printing/faxing device. Consequently, the resulting device can only introduce communication mismatches that both of the original devices can introduce.*

One reason why the conjunction in Figure 3 is so restrictive is that it cannot perform any output action that is not in the interface of both conjuncts. If we improve on this situation by extending the set of actions of the device in Figure 1 with fax_mode *and* fax*, and extending the set of actions of the device in Figure 2 with* scan_mode *and* scan*, so that the components to be conjoined have identical interfaces, then the conjunction is a component as shown in Figure 4. This device is capable of* scan*ning and* fax*ing documents, but cannot be placed in* scan_mode *after it has been placed in* fax_mode *and vice versa, although it can still be switched into* print_mode *and back.*

We remark that if, instead, we used conjunction defined as the intersection of behaviours (i.e. synchronous parallel, as in e.g. Lüttgen and Vogler (2007)), this would yield a device that cannot be used safely in place of either. The problem is that the behaviour would be unspecified when the device is placed in either scan_mode *or* fax_mode*, which means it will not work in any environment compatible with the printing/scanning device, nor the printing/faxing device.*

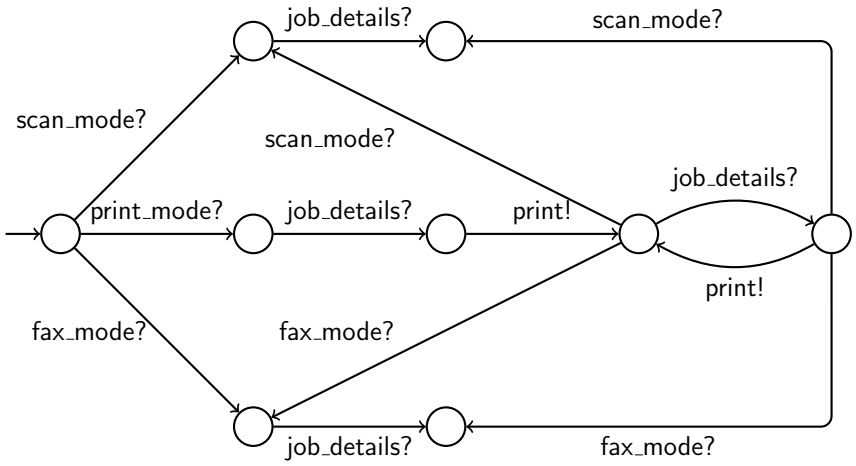

Figure 3: The conjunction of the printing/scanning and printing/faxing devices.

2.4. Disjunction

Disjunction is the dual of conjunction, so corresponds to the join operator on the refinement preorder. Therefore, the disjunction of a collection of components is the finest component that they each refine, meaning that the disjunction will work in environments safe for both of its operands. Composability of components under disjunction is the same as for conjunction.

Definition 7. *Let $\mathcal{P}$ and $\mathcal{Q}$ be components composable for disjunction, i.e., such that the sets $\mathcal{A}^I_\mathcal{P} \cup \mathcal{A}^I_\mathcal{Q}$ and $\mathcal{A}^O_\mathcal{P} \cup \mathcal{A}^O_\mathcal{Q}$ are disjoint. Then $\mathcal{P} \vee \mathcal{Q}$ is the component $\langle \mathcal{A}^I_{\mathcal{P}\vee\mathcal{Q}}, \mathcal{A}^O_{\mathcal{P}\vee\mathcal{Q}}, T_{\mathcal{P}\vee\mathcal{Q}}, F_{\mathcal{P}\vee\mathcal{Q}} \rangle$, where:*

- $\mathcal{A}^I_{\mathcal{P}\vee\mathcal{Q}} = \mathcal{A}^I_\mathcal{P} \cap \mathcal{A}^I_\mathcal{Q}$
- $\mathcal{A}^O_{\mathcal{P}\vee\mathcal{Q}} = \mathcal{A}^O_\mathcal{P} \cup \mathcal{A}^O_\mathcal{Q}$
- $T_{\mathcal{P}\vee\mathcal{Q}} = (T_\mathcal{P} \cup T_\mathcal{Q}) \cap \mathcal{A}^*_{\mathcal{P}\vee\mathcal{Q}}$
- $F_{\mathcal{P}\vee\mathcal{Q}} = (F_\mathcal{P} \cup F_\mathcal{Q}) \cap \mathcal{A}^*_{\mathcal{P}\vee\mathcal{Q}}$.

Essentially, as the disjunction should be refined by its arguments, the behaviours of $\mathcal{P}$ and $\mathcal{Q}$ should be contained within the behaviour of $\mathcal{P} \vee \mathcal{Q}$. Similarly, if a trace is inconsistent in one of $\mathcal{P}$ or $\mathcal{Q}$, then it must also be inconsistent within the disjunction.

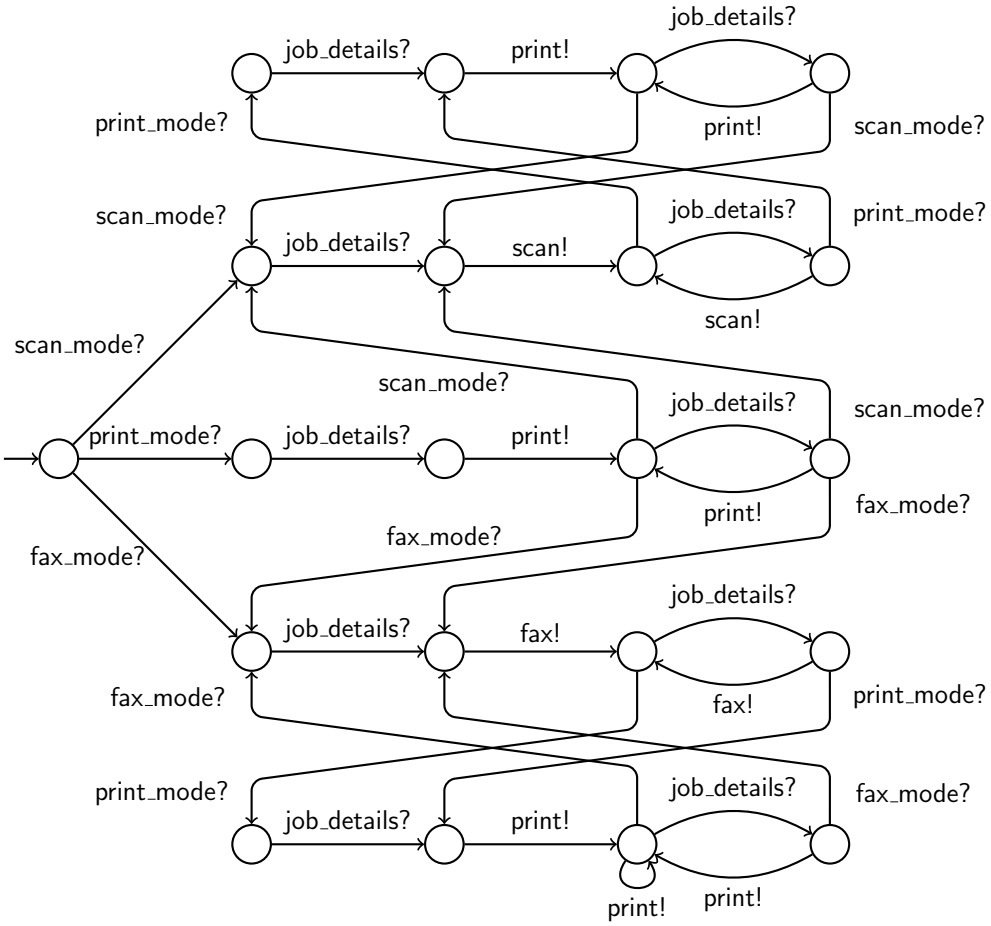

Figure 4: The conjunction of the printing/scanning and printing/faxing devices when the components have identical interfaces incorporating all actions.

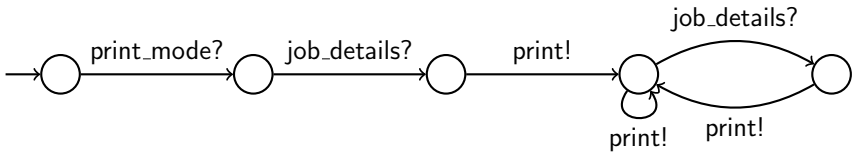

Figure 5: The disjunction of the printing/scanning and printing/faxing devices.

Lemma 4. *Disjunction is associative, commutative and idempotent.*

As for conjunction, disjunction has an analogous set of algebraic properties, obtained by reversing the direction of refinement.

Theorem 3. *Let $\mathcal{P}$ and $\mathcal{Q}$, and $\mathcal{P}'$ and $\mathcal{Q}'$, be components composable for disjunction. Then:*

- $\mathcal{P} \sqsubseteq_{imp} \mathcal{P} \vee \mathcal{Q}$ *and* $\mathcal{Q} \sqsubseteq_{imp} \mathcal{P} \vee \mathcal{Q}$
- $\mathcal{P} \sqsubseteq_{imp} \mathcal{R}$ *and* $\mathcal{Q} \sqsubseteq_{imp} \mathcal{R}$ *implies* $\mathcal{P} \vee \mathcal{Q} \sqsubseteq_{imp} \mathcal{R}$
- $\mathcal{P}' \sqsubseteq_{imp} \mathcal{P}$ *and* $\mathcal{Q}' \sqsubseteq_{imp} \mathcal{Q}$ *implies* $\mathcal{P}' \vee \mathcal{Q}' \sqsubseteq_{imp} \mathcal{P} \vee \mathcal{Q}$.

Example 4. *A user wishing to use a multi-function device is non-deterministically allocated the printing/scanning device (Figure 1) or the printing/faxing device (Figure 2). The most general behaviour allowed by the user (such that communication mismatches are not introduced) is obtained by inverting the inputs and outputs on the disjunction of the two devices. The disjunction is shown in Figure 5.*

2.5. Hiding

We introduce hiding to support abstraction for hierarchical development. Hiding is a unary operator on components that has the effect of contracting the interface by removing an action. Taking intuition from a simple analogy in which inputs correspond to buttons and outputs correspond to lights, the resulting behaviour of a component under hiding of action b is as follows:

- If b is an input, then the b-button will never be pressed. This means that no behaviour is observable beyond a b on a trace, so all traces should be pruned on encountering a b.

- If b is an output, then hiding suppresses the visibility of the b-light. The component should thus silently skip over b, which corresponds to projecting out b from all traces.

From this, we give the formal definition, which is dependent on the type of action to be hidden.

Definition 8. *Let $\mathcal{P}$ be a component and let b be an action. The hiding of b in $\mathcal{P}$ is a component $\mathcal{P}/b = \langle \mathcal{A}^I_{\mathcal{P}/b}, \mathcal{A}^O_{\mathcal{P}/b}, T_{\mathcal{P}/b}, F_{\mathcal{P}/b} \rangle$, where:*

- $\mathcal{A}^I_{\mathcal{P}/b} = \mathcal{A}^I_{\mathcal{P}} \setminus \{b\}$
- $\mathcal{A}^O_{\mathcal{P}/b} = \mathcal{A}^O_{\mathcal{P}} \setminus \{b\}$
- $T_{\mathcal{P}/b} = \begin{cases} T_{\mathcal{P}} \upharpoonright \mathcal{A}_{\mathcal{P}/b} & \text{if } b \in \mathcal{A}^O_{\mathcal{P}} \\ T_{\mathcal{P}} \cap \mathcal{A}^*_{\mathcal{P}/b} & \text{otherwise} \end{cases}$
- $F_{\mathcal{P}/b} = \begin{cases} F_{\mathcal{P}} \upharpoonright \mathcal{A}_{\mathcal{P}/b} & \text{if } b \in \mathcal{A}^O_{\mathcal{P}} \\ F_{\mathcal{P}} \cap \mathcal{A}^*_{\mathcal{P}/b} & \text{otherwise.} \end{cases}$

The soundness of this definition requires careful consideration when b is an output. For a trace $tb \in T_{\mathcal{P}}$ and input $a \in \mathcal{A}^I_{\mathcal{P}}$, observe that ta is a safe trace of $\mathcal{P}/b$ (i.e., $ta \in T_{\mathcal{P}/b} \setminus F_{\mathcal{P}/b}$) iff both ta and tba are safe traces of $\mathcal{P}$. Taking intuition from b being a hidden light, this behaviour is correct since it cannot be known precisely when the light will illuminate, so it is only safe for the environment to issue the input a after t if the component is willing to accept a both before and after the light has been silently illuminated.

Theorem 4. *Let $\mathcal{P}$ and $\mathcal{Q}$ be components and let b an action. If $\mathcal{Q} \sqsubseteq_{imp} \mathcal{P}$, then $\mathcal{Q}/b \sqsubseteq_{imp} \mathcal{P}/b$.*

Example 5. *Disaster strikes and the* Device *becomes broken such that it will no longer* scan *documents (depicted as* BrokenDevice *in Figure 6). As a result, the* BrokenDevice *should not be placed in* scan_mode*. The updated behaviour of the device is given by* BrokenDevice / scan_mode*, as shown in Figure 7. The resulting component model contracts the interface of the* BrokenDevice *by being indifferent to* scan_mode *requests.*

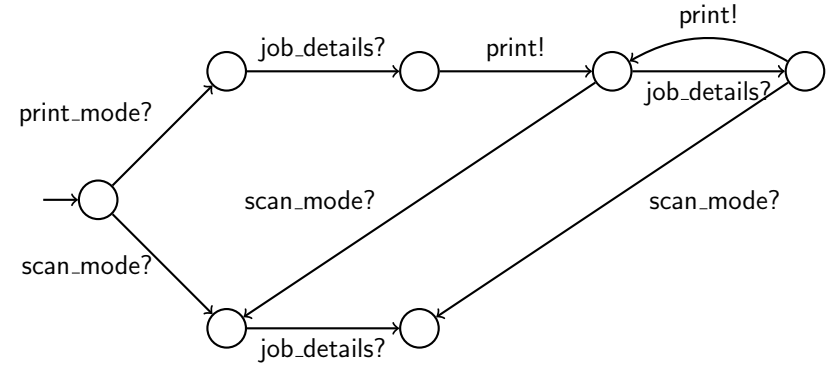

Figure 6: BrokenDevice without the ability to scan.

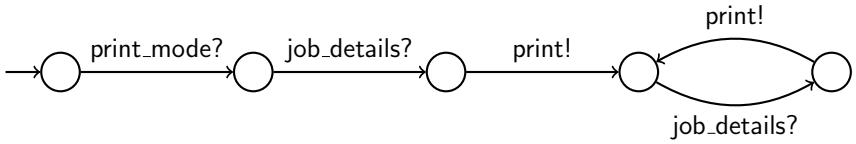

Figure 7: BrokenDevice after hiding the scan_mode functionality.

2.6. Quotient

The final operation that we consider is that of quotient, which provides functionality to synthesise components from a global specification and partial implementation. Given a component representing a system $\mathcal{R}$, together with an implementation of one component $\mathcal{P}$ in the system $\mathcal{R}$, the quotient yields the coarsest component for the remaining part of $\mathcal{R}$ to be implemented. Thus, the parallel composition of the quotient with $\mathcal{P}$ should be a refinement of $\mathcal{R}$. Therefore, quotient can be thought of as the adjoint of parallel composition.

A necessary condition for the existence of the quotient is that $\mathcal{A}^O_{\mathcal{P}} \subseteq \mathcal{A}^O_{\mathcal{R}}$, otherwise refinement will fail on the alphabet containment checks.

Definition 9. *Let $\mathcal{P}$ and $\mathcal{R}$ be components such that $\mathcal{A}^O_{\mathcal{P}} \subseteq \mathcal{A}^O_{\mathcal{R}}$. The quotient of $\mathcal{P}$ from $\mathcal{R}$ is the component $\mathcal{R}/\mathcal{P}$ with signature $\langle \mathcal{A}^I_{\mathcal{R}/\mathcal{P}}, \mathcal{A}^O_{\mathcal{R}/\mathcal{P}}, T_{\mathcal{R}/\mathcal{P}}, F_{\mathcal{R}/\mathcal{P}} \rangle$, where:*

- $\mathcal{A}^I_{\mathcal{R}/\mathcal{P}} = \mathcal{A}^I_{\mathcal{R}} \setminus \mathcal{A}^I_{\mathcal{P}}$
- $\mathcal{A}^O_{\mathcal{R}/\mathcal{P}} = \mathcal{A}^O_{\mathcal{R}} \setminus \mathcal{A}^O_{\mathcal{P}}$

- $T_{\mathcal{R}/\mathcal{P}} = X \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}}$, *where* X *is the largest prefix closed set satisfying* $X(\mathcal{A}_{\mathcal{R}} \setminus \mathcal{A}_{\mathcal{R}/\mathcal{P}})^* \subseteq \{t \in \mathcal{A}_{\mathcal{R}}^* : \forall t' \text{ a prefix of } t \cdot L(t') \text{ and } \forall t'' \in (\mathcal{A}_{\mathcal{R}} \setminus \mathcal{A}_{\mathcal{R}/\mathcal{P}}^O)^* \cdot L(tt'')\}$
- $F_{\mathcal{R}/\mathcal{P}} = \{t \in \mathcal{A}_{\mathcal{R}}^* : (t \upharpoonright \mathcal{A}_{\mathcal{P}} \in T_{\mathcal{P}} \implies t \in F_{\mathcal{E}(\mathcal{R})}) \text{ and } \forall t' \text{ a prefix of } t \cdot L(t')\} \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}}$
- $L(t) = (t \upharpoonright \mathcal{A}_{\mathcal{P}} \in F_{\mathcal{P}} \implies t \in F_{\mathcal{E}(\mathcal{R})})$ *and* $(t \upharpoonright \mathcal{A}_{\mathcal{P}} \in T_{\mathcal{P}} \implies t \in T_{\mathcal{E}(\mathcal{R})})$.

Explaining the intuition behind the definition, whenever $\mathcal{R}$ is inconsistent, the parallel composition of $\mathcal{P}$ and the quotient can be inconsistent, so the quotient itself can be inconsistent. Similarly, if a trace is not in $\mathcal{P}$, then it will not be encountered in the composition $\mathcal{P} \mid\mid \mathcal{R}/\mathcal{P}$, hence it should be inconsistent in the quotient (so that we obtain the least refined solution). These two conditions correlate with $t \upharpoonright \mathcal{A}_{\mathcal{P}} \in T_{\mathcal{P}} \implies t \in F_{\mathcal{E}(\mathcal{R})}$ in the definition of $F_{\mathcal{R}/\mathcal{P}}$. If $\mathcal{P}$ is inconsistent on a trace t when $\mathcal{R}$ is not inconsistent, then the parallel composition of $\mathcal{P}$ and the quotient would be inconsistent if t is in the quotient. This is problematic, as then the composition of $\mathcal{P}$ and the quotient would not be a refinement of $\mathcal{R}$. Consequently, the quotient must suppress the last output on its behaviour of this trace, so that the composition can never encounter the inconsistency that $\mathcal{P}$ will introduce. In our definition, this correlates with $L(t)$ not holding.

Although $\mathcal{R}/\mathcal{P}$ is always defined when $\mathcal{A}_{\mathcal{P}}^O \subseteq \mathcal{A}_{\mathcal{R}}^O$, it may not be a realisable component, even if both $\mathcal{R}$ and $\mathcal{P}$ are realisable. Unfortunately, there is no syntactic check on the interfaces of $\mathcal{R}$ and $\mathcal{P}$ that can determine whether $\mathcal{R}/\mathcal{P}$ is realisable or not. This can only be inferred by examining the behaviours of $\mathcal{R}$ and $\mathcal{P}$.

Theorem 5. *Let* $\mathcal{P}$, $\mathcal{Q}$ *and* $\mathcal{R}$ *be components. Then there exists* $\mathcal{Q}$ *such that* $\mathcal{P} \mid\mid \mathcal{Q} \sqsubseteq_{imp} \mathcal{R}$ *iff:*

- $\mathcal{R}/\mathcal{P}$ *is defined (i.e.,* $\mathcal{A}_{\mathcal{P}}^O \subseteq \mathcal{A}_{\mathcal{R}}^O$*)*
- $\mathcal{P} \mid\mid (\mathcal{R}/\mathcal{P}) \sqsubseteq_{imp} \mathcal{R}$
- $\mathcal{A}_{\mathcal{Q}}^I = \mathcal{A}_{\mathcal{R}/\mathcal{P}}^I$ *implies* $\mathcal{Q} \sqsubseteq_{imp} \mathcal{R}/\mathcal{P}$.

This definition of quotient generalises that supplied in Chen et al. (2012) and Bhaduri and Ramesh (2008), both of which require that the interface of $\mathcal{R}/\mathcal{P}$ synchronises with all actions of $\mathcal{P}$. Although in this article we take $\mathcal{A}^I_{\mathcal{R}/\mathcal{P}} = \mathcal{A}^I_{\mathcal{R}} \setminus \mathcal{A}^I_{\mathcal{P}}$, our definition works for any set such that $\mathcal{A}^I_{\mathcal{R}} \setminus \mathcal{A}^I_{\mathcal{P}} \subseteq \mathcal{A}^I_{\mathcal{R}/\mathcal{P}} \subseteq \mathcal{A}_{\mathcal{R}}$, with the results of Theorem 5 continuing to hold. In other words, the quotient operation can be parameterised on the set $\mathcal{A}^I_{\mathcal{R}/\mathcal{P}}$ of input actions of $\mathcal{R}/\mathcal{P}$. For any such choice of $\mathcal{A}^I_{\mathcal{R}/\mathcal{P}}$, the construction of $T_{\mathcal{R}/\mathcal{P}}$ and $F_{\mathcal{R}/\mathcal{P}}$ for this extended set of inputs remains unchanged from Definition 9 (having redefined $\mathcal{A}^I_{\mathcal{R}/\mathcal{P}}$). Consequently, we can take $\mathcal{A}^I_{\mathcal{R}/\mathcal{P}} = \mathcal{A}^I_{\mathcal{R}} \cup \mathcal{A}^O_{\mathcal{P}}$, which allows the interface of the quotient to observe all actions of $\mathcal{P}$ and hence capture more specific behaviours. In general, it is not possible to start with the original quotient $\mathcal{R}/\mathcal{P}$ (having inputs $\mathcal{A}^I_{\mathcal{R}} \setminus \mathcal{A}^I_{\mathcal{P}}$) and refine it to a component $\mathcal{Q}$ over the extended set of inputs such that $\mathcal{P} \parallel \mathcal{Q} \sqsubseteq_{imp} \mathcal{R}$ can be inferred, since parallel composition has interface restrictions for monotonicity to hold (cf Theorem 1).

The next theorem shows that quotient is well-behaved with respect to refinement.

Theorem 6. *Let $\mathcal{P}$, $\mathcal{Q}$ and $\mathcal{R}$ be components such that $\mathcal{Q} \sqsubseteq_{imp} \mathcal{P}$.*

- *If $\mathcal{Q}/\mathcal{R}$ is defined and $\mathcal{A}^I_{\mathcal{R}} \cap \mathcal{A}^O_{\mathcal{P}} = \emptyset$, then $\mathcal{Q}/\mathcal{R} \sqsubseteq_{imp} \mathcal{P}/\mathcal{R}$.*
- *If $\mathcal{R}/\mathcal{P}$ is defined and $(\mathcal{A}^I_{\mathcal{Q}} \setminus \mathcal{A}^I_{\mathcal{P}}) \cap \mathcal{A}_{\mathcal{R}} = \emptyset$, then $\mathcal{R}/\mathcal{Q} \sqsupseteq_{imp} \mathcal{R}/\mathcal{P}$.*

Example 6. *To demonstrate quotient, we assume that the action* job_details *can encode two types of behaviour, depending on the mode of the device. When* Device *is in* print_mode*, the* job_details *should encode information pertaining to printing, such as the document to be printed. Conversely, when* Device *is in* scan_mode*, the* job_details *should contain information indicative of scanning functionality, such as the resolution at which scanning must be performed. This essentially means that, after the* job_details *have been sent to* Device*, the device mode may not be changed until the current job has been* print*ed or* scan*ned. This constraint is represented by the component* Constraint *in Figure 8. The* Constraint *component is an observer that generates errors when bad sequences of actions are seen, which is why all actions are treated as inputs. The behaviour of the constrained device is given by* Device || Constraint.

The most general behaviour of a user that interacts with the constrained device is given by the quotient User2 = ErrorFree/(Device || Constraint) *(as*

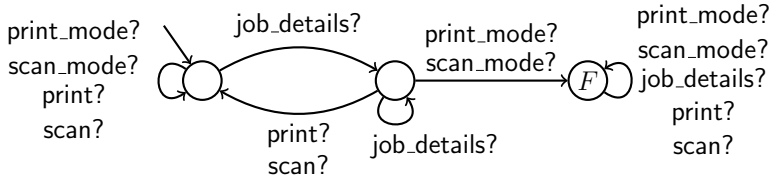

Figure 8: Constraint on job_details.

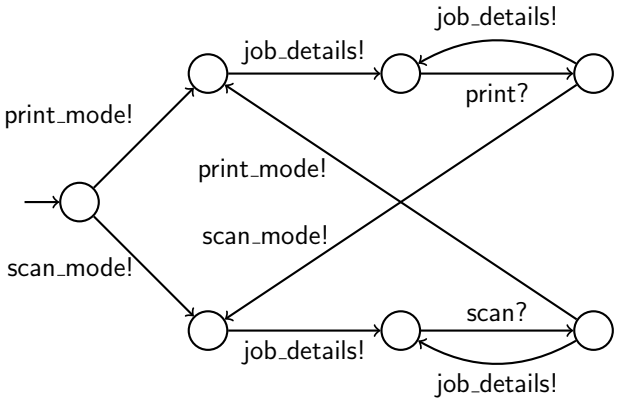

Figure 9: Component representing User2.

depicted in Figure 9). ErrorFree *is the component having a single state with a self-loop for each action (treated as an output). As* ErrorFree *does not possess any inconsistent states, the quotient operation guarantees that* User2 || Device || Constraint *is free of inconsistencies, hence* User2 || Device *conforms to the behaviour of* Constraint.

An application of quotient to mediator synthesis was demonstrated by Inverardi and Tivoli (2013).

2.7. Full Abstraction

In this section, we demonstrate that our refinement relation precisely characterises safe substitutivity of components, by means of a testing framework that places components in parallel with an arbitrary environment and checks for inconsistency. Based on this testing scenario, we show that $\equiv_{imp}$ is fully abstract for the full collection of operators in the specification theory.

Definition 10. *Let $\mathcal{P}$ and $\mathcal{Q}$ be components. Then $\mathcal{Q}$ is inconsistency substitutable for $\mathcal{P}$, denoted by $\mathcal{Q} \sqsubseteq^{F}_{imp} \mathcal{P}$, iff $\epsilon \in F_{\mathcal{E}(\mathcal{Q})}$ implies $\epsilon \in F_{\mathcal{E}(\mathcal{P})}$.*

From this definition, we can show that $\sqsubseteq_{imp}$ is the weakest preorder representing safe-substitutivity.

Theorem 7. *Let $\mathcal{P}$ and $\mathcal{Q}$ be components such that $\mathcal{A}^I_\mathcal{P} \subseteq \mathcal{A}^I_\mathcal{Q}$, $\mathcal{A}^O_\mathcal{Q} \subseteq \mathcal{A}^O_\mathcal{P}$ and $\mathcal{A}^I_\mathcal{Q} \cap \mathcal{A}^O_\mathcal{P} = \emptyset$. Then:*

$$\mathcal{Q} \sqsubseteq_{imp} \mathcal{P} \text{ iff } \forall \mathcal{R} \cdot \mathcal{A}^O_\mathcal{R} = \mathcal{A}^I_\mathcal{P} \text{ and } \mathcal{A}^I_\mathcal{R} = \mathcal{A}^O_\mathcal{Q} \implies \mathcal{Q} \parallel \mathcal{R} \sqsubseteq^F_{imp} \mathcal{P} \parallel \mathcal{R}.$$

The conditions on the interfaces of $\mathcal{P}$ and $\mathcal{Q}$ are required for Theorem 7 to hold, since $\mathcal{Q} \parallel \mathcal{R} \sqsubseteq_{imp} \mathcal{P} \parallel \mathcal{R}$ does not imply that $\mathcal{A}^I_\mathcal{P} \subseteq \mathcal{A}^I_\mathcal{Q}$, $\mathcal{A}^O_\mathcal{Q} \subseteq \mathcal{A}^O_\mathcal{P}$ and $\mathcal{A}^I_\mathcal{Q} \cap \mathcal{A}^O_\mathcal{P} = \emptyset$.

From this characterisation of $\sqsubseteq_{imp}$, we obtain a full abstraction result for $\equiv_{imp}$ on the specification theory, with respect to checking of inconsistency equivalence $\equiv^F_{imp}$ (i.e., $\sqsubseteq^F_{imp} \cap \sqsupseteq^F_{imp}$). Our definition of full abstraction is taken from van Glabbeek (1994) (Definition 16), which means that $\equiv_{imp}$ is the coarsest congruence for the operators of our specification theory with respect to simple inconsistency equivalence.

Corollary 1. *Substitutive equivalence $\equiv_{imp}$ is fully abstract for parallel composition, conjunction, disjunction, hiding and quotient with respect to observational equivalence of inconsistency.*

We do not obtain full abstraction for $\sqsubseteq_{imp}$, since the compositional operators do not form a pre-congruence under $\sqsubseteq_{imp}$, due to the compatibility constraints. The constraints are, however, automatically satisfied for $\equiv_{imp}$.

3. Extending the Component Theory: Preservation of Progress

A perceived shortcoming of interface automata (and hence our theory in Section 2) is that the principle of substitutivity requires a refining component to be no more expressive on the output it can produce, in comparison to the behaviour of the original. In fact, the most refined component will have an interface that is unwilling to produce any external stimuli whatsoever. Refinement resulting in absence of external behaviour is frequently seen in the literature, one such example being the trace semantics of CSP (Hoare, 1985), in which every process can be refined by the deadlocked process STOP. Such refinements preserve safety, but they do not require any meaningful computation to be performed. To resolve this issue, the refinement relation should be adapted by instilling a notion of liveness/progress.

In this section, we adapt the substitutive refinement relation of Section 2.1 by forcing a refining component to make progress whenever the original can. Our choice of progress is based on the notion of *quiescence*; a trace is said to be quiescent just if it cannot be extended by an output. Quiescence differs from deadlock in that a deadlocked component is unwilling to accept any input (or produce any output), whereas a quiescent component may be able to accept input. The updated refinement relation requires substitutability, as in Section 2.1, but also that any non-quiescent trace of the original component is non-quiescent in the refining component. Our choice of quiescence, in place of fairness sets (Segala, 1997; Romijn and Vaandrager, 1996), is motivated by the desire to utilise only finite-length traces, as in Section 2. In addition to quiescence, a component should not be allowed to make progress by performing an unbounded amount of internal computation. As a result, our refinement relation must also take into account the divergence of a component. Note that, in contrast to CSP (Hoare, 1985), we do *not* require divergent traces to be extension closed.

The remainder of this section presents an updated component formulation, together with the formal definition of the substitutive and progress-sensitive refinement relation. Revised definitions for the compositional operators are presented, and the algebraic results are re-established.

Definition 11. *A* progress-sensitive component $\mathcal{P}$ *(henceforth referred to as a component) is a tuple* $\langle \mathcal{A}^I_\mathcal{P}, \mathcal{A}^O_\mathcal{P}, T_\mathcal{P}, F_\mathcal{P}, D_\mathcal{P}, K_\mathcal{P} \rangle$ *in which* $\langle \mathcal{A}^I_\mathcal{P}, \mathcal{A}^O_\mathcal{P}, T_\mathcal{P}, F_\mathcal{P} \rangle$ *is a component as in Definition 3, and:*

- $D_\mathcal{P}$ *is a set of extended divergent traces such that* $F_\mathcal{P} \subseteq D_\mathcal{P} \subseteq T_\mathcal{P}$
- $K_\mathcal{P}$ *is a set of extended quiescent traces such that* $\{t \in T_\mathcal{P} : \nexists o \in \mathcal{A}^O_\mathcal{P} \cdot to \in T_\mathcal{P}\} \cup D_\mathcal{P} \subseteq K_\mathcal{P} \subseteq T_\mathcal{P}$.

The set $D_\mathcal{P}$ consists of all divergent and inconsistent traces of $\mathcal{P}$, while $K_\mathcal{P}$ also contains the quiescent traces of $\mathcal{P}$. Note that, due to the possibility of internal computation (which introduces non-deterministic behaviour), the quiescent traces of a component are not completely determined by $T_\mathcal{P}$ and $F_\mathcal{P}$. In our framework, a separate treatment of divergence is given in order to guarantee that a refining component makes observable progress. This is in contrast to, e.g., the receptive process theory (Josephs, 1992) and the work of Jonsson (1991).

We now redefine $\mathcal{P}$, $\mathcal{Q}$ and $\mathcal{R}$ to be components with signatures $\langle \mathcal{A}^I_{\mathcal{P}}, \mathcal{A}^O_{\mathcal{P}}, T_{\mathcal{P}}, F_{\mathcal{P}}, D_{\mathcal{P}}, K_{\mathcal{P}} \rangle$, $\langle \mathcal{A}^I_{\mathcal{Q}}, \mathcal{A}^O_{\mathcal{Q}}, T_{\mathcal{Q}}, F_{\mathcal{Q}}, D_{\mathcal{Q}}, K_{\mathcal{Q}} \rangle$ and $\langle \mathcal{A}^I_{\mathcal{R}}, \mathcal{A}^O_{\mathcal{R}}, T_{\mathcal{R}}, F_{\mathcal{R}}, D_{\mathcal{R}}, K_{\mathcal{R}} \rangle$ respectively.

3.1. Refinement

As in Section 2.1, refinement of component $\mathcal{Q}$ by component $\mathcal{P}$ needs to talk about the most general safe representations $\mathcal{E}(\mathcal{P})$ and $\mathcal{E}(\mathcal{Q})$. This carries across to the new setting effortlessly, by taking $D_{\mathcal{E}(\mathcal{P})} = D_{\mathcal{P}} \cup F_{\mathcal{E}(\mathcal{P})}$ and $K_{\mathcal{E}(\mathcal{P})} = K_{\mathcal{P}} \cup F_{\mathcal{E}(\mathcal{P})}$. Based on this, we give the formal definition of refinement.

Definition 12. *$\mathcal{Q}$ is said to be a* progress-sensitive refinement *of $\mathcal{P}$, written $\mathcal{Q} \sqsubseteq^l_{imp} \mathcal{P}$, iff $\mathcal{Q} \sqsubseteq_{imp} \mathcal{P}$, $D_{\mathcal{E}(\mathcal{Q})} \subseteq D_{\mathcal{E}(\mathcal{P})} \cup (T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{Q}})$ and $K_{\mathcal{E}(\mathcal{Q})} \subseteq K_{\mathcal{E}(\mathcal{P})} \cup (T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{Q}})$.*

By $\mathcal{Q} \sqsubseteq_{imp} \mathcal{P}$ we mean refinement as in Definition 3 after having projected out $D_{\mathcal{P}}$, $K_{\mathcal{P}}$, $D_{\mathcal{Q}}$ and $K_{\mathcal{Q}}$ from $\mathcal{P}$ and $\mathcal{Q}$; this condition guarantees that $\mathcal{Q}$ is substitutable for $\mathcal{P}$. The additional constraints $D_{\mathcal{E}(\mathcal{Q})} \subseteq D_{\mathcal{E}(\mathcal{P})} \cup (T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{Q}})$ and $K_{\mathcal{E}(\mathcal{Q})} \subseteq K_{\mathcal{E}(\mathcal{P})} \cup (T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{Q}})$ ensure that $\mathcal{Q}$ is only allowed to diverge when $\mathcal{P}$ can diverge, and can only be quiescent when $\mathcal{P}$ is quiescent. It is these final clauses that force a refining component to make observable progress whenever the original can.

Equivalence of components, indicated using $\equiv^l_{imp}$, can easily be defined by means of mutual refinement, i.e., is equal to $\sqsubseteq^l_{imp} \cap (\sqsubseteq^l_{imp})^{-1}$.

Lemma 5. *Progress-sensitive refinement is reflexive, and transitive subject to preservation of action types.*

3.2. Parallel Composition

As parallel composition is not related to refinement, the definition remains largely unchanged, excepting the sets of extended divergent and quiescent traces. To compute these sets, it is straightforward to observe that a trace is divergent in the parallel composition if its projection onto the alphabet of at least one of the components is a divergent trace, and is quiescent if its projections onto the alphabets of both components are quiescent.

Definition 13. *Let $\mathcal{P}$ and $\mathcal{Q}$ be composable for parallel. Then $\mathcal{P} \,||_l\, \mathcal{Q}$ is the component $\langle \mathcal{A}^I_{\mathcal{P}||\mathcal{Q}}, \mathcal{A}^O_{\mathcal{P}||\mathcal{Q}}, T_{\mathcal{P}||\mathcal{Q}}, F_{\mathcal{P}||\mathcal{Q}}, D_{\mathcal{P}||\mathcal{Q}}, K_{\mathcal{P}||\mathcal{Q}} \rangle$, where:*

- $D_{\mathcal{P}||\mathcal{Q}} = [(D_{\mathcal{P}} \Uparrow \mathcal{A}_{\mathcal{P}||\mathcal{Q}}) \cap (T_{\mathcal{Q}} \Uparrow \mathcal{A}_{\mathcal{P}||\mathcal{Q}})] \cup$
  $[(T_{\mathcal{P}} \Uparrow \mathcal{A}_{\mathcal{P}||\mathcal{Q}}) \cap (D_{\mathcal{Q}} \Uparrow \mathcal{A}_{\mathcal{P}||\mathcal{Q}})] \cup F_{\mathcal{P}||\mathcal{Q}}$
- $K_{\mathcal{P}||\mathcal{Q}} = [(K_{\mathcal{P}} \Uparrow \mathcal{A}_{\mathcal{P}||\mathcal{Q}}) \cap (K_{\mathcal{Q}} \Uparrow \mathcal{A}_{\mathcal{P}||\mathcal{Q}})] \cup D_{\mathcal{P}||\mathcal{Q}}$.

Given the effect of divergence and quiescence on parallel composition, it is not surprising that the monotonicity result is unchanged.

Theorem 8. *Let $\mathcal{P}$, $\mathcal{P}'$, $\mathcal{Q}$ and $\mathcal{Q}'$ be components such that $\mathcal{P}$ and $\mathcal{Q}$ are composable, $\mathcal{A}_{\mathcal{P}'} \cap \mathcal{A}_{\mathcal{Q}'} \cap \mathcal{A}_{\mathcal{P}||\mathcal{Q}} \subseteq \mathcal{A}_{\mathcal{P}} \cap \mathcal{A}_{\mathcal{Q}}$ and $\mathcal{A}^I_{\mathcal{P}'||\mathcal{Q}'} \cap \mathcal{A}^O_{\mathcal{P}||\mathcal{Q}} = \emptyset$. If $\mathcal{P}' \sqsubseteq^l_{imp} \mathcal{P}$ and $\mathcal{Q}' \sqsubseteq^l_{imp} \mathcal{Q}$, then $\mathcal{P}' \,||_l\, \mathcal{Q}' \sqsubseteq^l_{imp} \mathcal{P} \,||_l\, \mathcal{Q}$.*

3.3. Conjunction

As conjunction corresponds to the meet operator on the refinement preorder, its definition in the progress-sensitive setting is substantially altered. In particular, we require that a trace in the conjunction can only be quiescent if it is permitted to be quiescent in both of the components to be conjoined. For substitutability, it is necessary to synchronise on outputs, which means that the conjunction can introduce new undesirable quiescence. Hence, it is necessary to perform a backward pruning, which removes an output at an earlier stage to avoid violating the constraints on quiescence later on. Of course, removing outputs at an earlier stage can introduce more quiescence, so a fixed point pruning must be applied.

Definition 14. *Let $\mathcal{P}$ and $\mathcal{Q}$ be composable for conjunction. Then $\mathcal{P} \wedge_l \mathcal{Q}$ is the component $\langle \mathcal{A}^I_{\mathcal{P}\wedge\mathcal{Q}}, \mathcal{A}^O_{\mathcal{P}\wedge\mathcal{Q}}, T_{\mathcal{P}\wedge\mathcal{Q}} \setminus Err, F_{\mathcal{P}\wedge\mathcal{Q}} \setminus Err, D_{\mathcal{P}\wedge\mathcal{Q}} \setminus Err, K_{\mathcal{P}\wedge\mathcal{Q}} \setminus Err \rangle$, where:*

- $D_{\mathcal{P}\wedge\mathcal{Q}} = (D_{\mathcal{P}} \cup (T_{\mathcal{P}} \uparrow \mathcal{A}^I_{\mathcal{Q}})) \cap (D_{\mathcal{Q}} \cup (T_{\mathcal{Q}} \uparrow \mathcal{A}^I_{\mathcal{P}}))$
- $K_{\mathcal{P}\wedge\mathcal{Q}} = (K_{\mathcal{P}} \cup (T_{\mathcal{P}} \uparrow \mathcal{A}^I_{\mathcal{Q}})) \cap (K_{\mathcal{Q}} \cup (T_{\mathcal{Q}} \uparrow \mathcal{A}^I_{\mathcal{P}}))$
- *Err is the smallest set containing $\{t \in T_{\mathcal{P}\wedge\mathcal{Q}} : \exists t' \in (\mathcal{A}^I_{\mathcal{P}\wedge\mathcal{Q}})^* \cdot$ $tt' \notin K_{\mathcal{P}\wedge\mathcal{Q}}$ and $\forall o \in \mathcal{A}^O_{\mathcal{P}\wedge\mathcal{Q}} \cdot tt'o \notin T_{\mathcal{P}\wedge\mathcal{Q}} \setminus Err\}$.*

Err captures the quiescent traces in $\mathcal{P} \wedge \mathcal{Q}$ that are not quiescent in both $\mathcal{P}$ and $\mathcal{Q}$. These traces correspond to a clash of requirements between safety and progress, so are subsequently removed from the behaviour of $\mathcal{P} \wedge_l \mathcal{Q}$. In removing these traces, we can introduce further quiescence, which is why Err is defined as a least fixed point. Note that, unlike in the original definition, the conjunction of two realisable components may not be realisable.

Theorem 9. *Let $\mathcal{P}$ and $\mathcal{Q}$, and $\mathcal{P}'$ and $\mathcal{Q}'$ be components composable for conjunction. Then:*

- $\mathcal{P} \wedge_l \mathcal{Q} \sqsubseteq^l_{imp} \mathcal{P}$ *and* $\mathcal{P} \wedge_l \mathcal{Q} \sqsubseteq^l_{imp} \mathcal{Q}$
- $\mathcal{R} \sqsubseteq^l_{imp} \mathcal{P}$ *and* $\mathcal{R} \sqsubseteq^l_{imp} \mathcal{Q}$ *implies* $\mathcal{R} \sqsubseteq^l_{imp} \mathcal{P} \wedge_l \mathcal{Q}$
- $\mathcal{P}' \sqsubseteq^l_{imp} \mathcal{P}$ *and* $\mathcal{Q}' \sqsubseteq^l_{imp} \mathcal{Q}$ *implies* $\mathcal{P}' \wedge_l \mathcal{Q}' \sqsubseteq^l_{imp} \mathcal{P} \wedge_l \mathcal{Q}$.

3.4. Disjunction

Recall that the definition of conjunction is complicated by the fact that, after a common trace, one of the components may be quiescent while the other is not. It is this behaviour that forces us to prune the traces contained in Err, which are subject to the conflicts of requirements between progress and safety. Being the dual of conjunction, the disjunctive operator does not share a similar fate, since the disjunction can always avoid conflicts by including the undesirable behaviours of the components to be composed.

Definition 15. *Let $\mathcal{P}$ and $\mathcal{Q}$ be composable for disjunction. Then $\mathcal{P} \vee_l \mathcal{Q}$ is the component $\langle \mathcal{A}^I_{\mathcal{P}\vee\mathcal{Q}}, \mathcal{A}^O_{\mathcal{P}\vee\mathcal{Q}}, T_{\mathcal{P}\vee\mathcal{Q}}, F_{\mathcal{P}\vee\mathcal{Q}}, D_{\mathcal{P}\vee\mathcal{Q}}, K_{\mathcal{P}\vee\mathcal{Q}} \rangle$, where:*

- $D_{\mathcal{P}\vee\mathcal{Q}} = (D_{\mathcal{P}} \cup D_{\mathcal{Q}}) \cap \mathcal{A}^*_{\mathcal{P}\vee\mathcal{Q}}$
- $K_{\mathcal{P}\vee\mathcal{Q}} = (K_{\mathcal{P}} \cup K_{\mathcal{Q}}) \cap \mathcal{A}^*_{\mathcal{P}\vee\mathcal{Q}}$.

Under progress-sensitive refinement, the algebraic properties of disjunction continue to hold.

Theorem 10. *Let $\mathcal{P}$ and $\mathcal{Q}$, and $\mathcal{P}'$ and $\mathcal{Q}'$ be components composable for disjunction. Then:*

- $\mathcal{P} \sqsubseteq^l_{imp} \mathcal{P} \vee_l \mathcal{Q}$ *and* $\mathcal{Q} \sqsubseteq^l_{imp} \mathcal{P} \vee_l \mathcal{Q}$
- $\mathcal{P} \sqsubseteq^l_{imp} \mathcal{R}$ *and* $\mathcal{Q} \sqsubseteq^l_{imp} \mathcal{R}$ *implies* $\mathcal{P} \vee_l \mathcal{Q} \sqsubseteq^l_{imp} \mathcal{R}$
- $\mathcal{P}' \sqsubseteq^l_{imp} \mathcal{P}$ *and* $\mathcal{Q}' \sqsubseteq^l_{imp} \mathcal{Q}$ *implies* $\mathcal{P}' \vee_l \mathcal{Q}' \sqsubseteq^l_{imp} \mathcal{P} \vee_l \mathcal{Q}$.

3.5. Hiding

The removal of inputs from a component's interface can have no effect on the quiescence or divergence of traces. This is not true for outputs in our setting, although there are a number of ways to handle quiescence. Therefore, the reasoning needs careful attention, once we have considered the definition.

Definition 16. *Let $\mathcal{P}$ be a component and let b be an action. The hiding of b in $\mathcal{P}$ is a component $\mathcal{P} /_l b = \langle \mathcal{A}^I_{\mathcal{P}/b}, \mathcal{A}^O_{\mathcal{P}/b}, T_{\mathcal{P}/b}, F_{\mathcal{P}/b}, D_{\mathcal{P}/b}, K_{\mathcal{P}/b} \rangle$, where:*

- $\mathcal{A}^I_{\mathcal{P}/b} = \mathcal{A}^I_{\mathcal{P}} \setminus \{b\}$
- $\mathcal{A}^O_{\mathcal{P}/b} = \mathcal{A}^O_{\mathcal{P}} \setminus \{b\}$
- $D_{\mathcal{P}/b} = \begin{cases} D_{\mathcal{P}} \upharpoonright \mathcal{A}_{\mathcal{P}/b} \cup \mathsf{div} & \text{if } b \in \mathcal{A}^O_{\mathcal{P}} \\ D_{\mathcal{P}} \cap \mathcal{A}^*_{\mathcal{P}/b} & \text{otherwise} \end{cases}$
- $K_{\mathcal{P}/b} = \begin{cases} K_{\mathcal{P}} \upharpoonright \mathcal{A}_{\mathcal{P}/b} \cup \mathsf{div} & \text{if } b \in \mathcal{A}^O_{\mathcal{P}} \\ K_{\mathcal{P}} \cap \mathcal{A}^*_{\mathcal{P}/b} & \text{otherwise} \end{cases}$
- $\mathsf{div} = \{t \upharpoonright \mathcal{A}_{\mathcal{P}/b} : t \in T_{\mathcal{P}} \text{ and } \forall i \in \mathbb{N} \cdot tb^i \in T_{\mathcal{P}}\}$.

According to our definition, in the case that b is an output, divergence can be introduced after a trace t under two circumstances. The first is when there is a sequence of b actions leading to a divergent trace, while the second corresponds to the introduction of divergence outright, whereby t can be extended by an arbitrary number of b actions. This makes sense, and is common to a number of formulations of hiding (e.g., CSP (Hoare, 1985)).

In the case of quiescence, a trace t is quiescent if t can diverge, or if there is a sequence of b actions leading to a quiescent state. This means that, if a component can only produce the single output b and cannot diverge after the trace t, then it is not necessarily the case that the component becomes quiescent on t after hiding b. This formulation of quiescence is justified since, immediately after the trace t, the component can perform internal computation, which can affect the subsequently offered outputs. This can be seen clearly in the operational setting (see Section 4.5), and corresponds to the notion that quiescence should only be considered in stable states. Moreover, this interpretation ensures that hiding is compositional under refinement.

Theorem 11. *Let $\mathcal{P}$ and $\mathcal{Q}$ be components and let b be an action. If $\mathcal{Q} \sqsubseteq_{imp} \mathcal{P}$, then $\mathcal{Q} /_l b \sqsubseteq_{imp} \mathcal{P} /_l b$.*

3.6. Quotient

The definition of quotient remains largely unchanged from the substitutive case, except for the need to remove two types of trace:

QC1. Quiescent (resp. divergent) traces in the parallel composition of $\mathcal{P}$ and $\mathcal{R}/\mathcal{P}$ that are non-quiescent (resp. non-divergent) in $\mathcal{R}$. As we are unable to alter the traces of $\mathcal{P}$, it is necessary to prune all behaviour from (and including) the last available output in $\mathcal{A}^O_{\mathcal{R}/\mathcal{P}}$ on the projection of these traces onto $\mathcal{A}_{\mathcal{R}/\mathcal{P}}$, in order to avoid reaching such conflicts.

QC2. Traces of $\mathcal{R}/\mathcal{P}$ that introduce new quiescence conflicts, after having repeatedly removed traces satisfying this or the previous condition.

Definition 17. *Let $\mathcal{P}$ and $\mathcal{R}$ be components such that $\mathcal{A}^O_{\mathcal{P}} \subseteq \mathcal{A}^O_{\mathcal{R}}$. The quotient of $\mathcal{P}$ from $\mathcal{R}$ is the component $\mathcal{R} /_l \mathcal{P}$ with signature $\langle \mathcal{A}^I_{\mathcal{R}/\mathcal{P}}, \mathcal{A}^O_{\mathcal{R}/\mathcal{P}}, T_{\mathcal{R}/\mathcal{P}} \setminus Err, F_{\mathcal{R}/\mathcal{P}} \setminus Err, D_{\mathcal{R}/\mathcal{P}} \setminus Err, K_{\mathcal{R}/\mathcal{P}} \setminus Err \rangle$, where:*

- $D_{\mathcal{R}/\mathcal{P}} = [T_{\mathcal{R}/\mathcal{P}} \cap (X \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}})] \cup F_{\mathcal{R}/\mathcal{P}}$, *where X is the largest subset of $\{\epsilon\} \cup \mathcal{A}^*_{\mathcal{R}}\mathcal{A}_{\mathcal{R}/\mathcal{P}}$ such that $X(\mathcal{A}_{\mathcal{R}} \setminus \mathcal{A}_{\mathcal{R}/\mathcal{P}})^* \cap T_{\mathcal{E}(\mathcal{R})} \subseteq D_{\mathcal{E}(\mathcal{R})}$*
- $K_{\mathcal{R}/\mathcal{P}} = \{t \in T_{\mathcal{R}/\mathcal{P}} : \nexists o \in \mathcal{A}^O_{\mathcal{R}/\mathcal{P}} \cdot to \in T_{\mathcal{R}/\mathcal{P}} \setminus Err\} \cup F_{\mathcal{R}/\mathcal{P}}$
- $Err = Y \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}}$, *where Y is the smallest set containing*
  $\{t \in \mathcal{A}^*_{\mathcal{R}} : \exists t' \in (\mathcal{A}_{\mathcal{R}} \setminus \mathcal{A}^O_{\mathcal{R}/\mathcal{P}})^* \cdot tt' \in \overline{D_{\mathcal{E}(\mathcal{R})}} \cap (D_{\mathcal{P}} \Uparrow \mathcal{A}_{\mathcal{R}})$ *or*
  $(tt' \in \overline{K_{\mathcal{E}(\mathcal{R})}} \cap (K_{\mathcal{P}} \Uparrow \mathcal{A}_{\mathcal{R}})$ *and* $\nexists o \in \mathcal{A}^O_{\mathcal{R}/\mathcal{P}} \cdot tt'o \in (T_{\mathcal{R}/\mathcal{P}} \Uparrow \mathcal{A}_{\mathcal{R}}) \setminus Y)\}$.

From $D_{\mathcal{R}/\mathcal{P}}$ we see that the quotient is only divergent when $\mathcal{R}$ becomes divergent on a trace ending with an action of $\mathcal{A}_{\mathcal{R}/\mathcal{P}}$, otherwise the quotient would become divergent prematurely. On the other hand, $K_{\mathcal{R}/\mathcal{P}}$ captures the traces of the quotient that are certainly quiescent. Err records all traces of the quotient violating conditions QC1 and QC2. Accordingly, the first line of the set contained in Y captures violations of divergence in QC1, while the second line captures quiescence violations in QC1 and the propagation condition QC2.

As for conjunction, the quotient of two realisable components may not be realisable, and this can only be determined by examining the behaviours of $\mathcal{P}$ and $\mathcal{R}$. However, the quotient is always defined when $\mathcal{A}^O_{\mathcal{P}} \subseteq \mathcal{A}^O_{\mathcal{R}}$.

Theorem 12. *Let $\mathcal{P}$, $\mathcal{Q}$ and $\mathcal{R}$ be components. Then $\mathcal{P} ||_l \mathcal{Q} \sqsubseteq^l_{imp} \mathcal{R}$ iff:*

- $\mathcal{R} /_l \mathcal{P}$ *is defined (i.e.,* $\mathcal{A}^O_{\mathcal{P}} \subseteq \mathcal{A}^O_{\mathcal{R}}$*)*
- $\mathcal{P} \,||_l\, (\mathcal{R} /_l \mathcal{P}) \sqsubseteq^l_{imp} \mathcal{R}$
- $\mathcal{A}^I_{\mathcal{Q}} = \mathcal{A}^I_{\mathcal{R}/\mathcal{P}}$ *implies* $\mathcal{Q} \sqsubseteq^l_{imp} \mathcal{R} /_l \mathcal{P}$.

Theorem 13. *Let* $\mathcal{P}$*,* $\mathcal{Q}$ *and* $\mathcal{R}$ *be components such that* $\mathcal{Q} \sqsubseteq^l_{imp} \mathcal{P}$*.*

- *If* $\mathcal{Q} /_l \mathcal{R}$ *is defined and* $\mathcal{A}^I_{\mathcal{R}} \cap \mathcal{A}^O_{\mathcal{P}} = \emptyset$*, then* $\mathcal{Q} /_l \mathcal{R} \sqsubseteq^l_{imp} \mathcal{P} /_l \mathcal{R}$*.*
- *If* $\mathcal{R} /_l \mathcal{P}$ *is defined and* $(\mathcal{A}^I_{\mathcal{Q}} \setminus \mathcal{A}^I_{\mathcal{P}}) \cap \mathcal{A}_{\mathcal{R}} = \emptyset$*, then* $\mathcal{R} /_l \mathcal{Q} \sqsupseteq^l_{imp} \mathcal{R} /_l \mathcal{P}$*.*

Example 7. *To demonstrate quotient in the quiescent framework, suppose that a user wishes to interact with* BrokenDevice *(Figure 6), but without ever reaching a deadlocked (quiescent) state, i.e., a point from which the system as a whole is blocked waiting for input. Note that* User2 *(as shown in Figure 9) is not a suitable candidate, since, after placing* BrokenDevice *in* scan_mode *and sending* job_details*, the system becomes blocked due to* BrokenDevice *never offering to* scan*. We generate a satisfying user as* User3 = ErrorFree $/_l$ BrokenDevice*, the result of which is shown in Figure 10.* ErrorFree *is the previously mentioned component having chaotic behaviour over all actions, which we treat as outputs. As* ErrorFree *does not have inconsistencies, and moreover is non-quiescent, it follows that* User3 $||_l$ BrokenDevice *is both inconsistency free and does not deadlock.*

The quotient is computed in two phases: first the computation of the T*,* F*,* D *and* G *sets is performed, after which traces in* Err *are removed. The first phase generates a component equal to* User2*. In the second phase, we see that the trace* scan_mode job_details *becomes quiescent in* User2 $||_l$ BrokenDevice*, which we consider to be problematic, since this is a non-quiescent trace of* ErrorFree*. We therefore remove the trace* scan_mode job_details *from the* T*,* F*,* D *and* K *sets. But now the trace* scan_mode *becomes quiescent, so we must also remove this trace. The empty trace* ϵ *is not quiescent, since* print_mode *can be performed. Consequently, the behaviour of* User3 *is obtained from* User2 *by never placing the device in* scan_mode*, since any trace exhibiting* scan_mode *is contained within* Err*.*

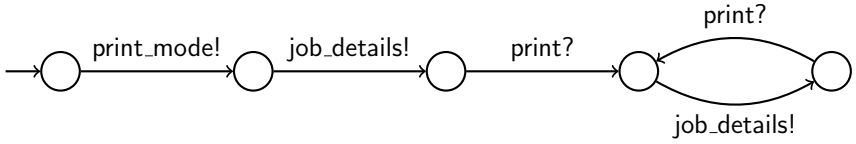

Figure 10: Component representing User3.

4. Operational Theory of Components

In this section, we outline an operational representation for components, and demonstrate the relationship between these operational models and the trace-based models of Sections 2 and 3. From this, we supply operational definitions for the compositional operators of our theory.

Definition 18. *An* operational component P *is a tuple* $\langle \mathcal{A}^I_{\mathsf{P}}, \mathcal{A}^O_{\mathsf{P}}, S_{\mathsf{P}}, \longrightarrow_{\mathsf{P}}, s^0_{\mathsf{P}}, \bot_{\mathsf{P}} \rangle$*, where:*

- $\mathcal{A}^I_{\mathsf{P}}$ *is a finite set of input actions*
- $\mathcal{A}^O_{\mathsf{P}}$ *is a finite set of output actions, disjoint from* $\mathcal{A}^I_{\mathsf{P}}$
- S_{P} *is a finite set of states*
- $\longrightarrow_{\mathsf{P}} \subseteq S_{\mathsf{P}} \times (\mathcal{A}_{\mathsf{P}} \cup \{\tau\}) \times S_{\mathsf{P}}$ *is the transition relation*
- $s^0_{\mathsf{P}} \in S_{\mathsf{P}}$ *is the designated initial state*
- $\bot_{\mathsf{P}} \in S_{\mathsf{P}}$ *is the designated inconsistent state.*

The transition relation satisfies the properties that: (i) $\bot_{\mathsf{P}} \xrightarrow{a}_{\mathsf{P}} \bot_{\mathsf{P}}$ *for each* $a \in \mathcal{A}_{\mathsf{P}} \cup \{\tau\}$*; and (ii) for each* $s \in S_{\mathsf{P}}$ *and* $a \in \mathcal{A}^I_{\mathsf{P}}$ *there exists* $s' \in S_{\mathsf{P}}$ *such that* $s \xrightarrow{a}_{\mathsf{P}} s'$*. These conditions ensure that all states are input-receptive, and that the inconsistent state is chaotic.*

It is important that the set of states S_{P} is finite, so that divergence of a state can be determined in finite time. This allows us to decide which inputs are safe, and which outputs may eventually be issued, for a particular state.

Notation. For a compositional operator $\oplus$, and sets A and B, we write $A \oplus B$ for the set $\{a \oplus b : a \in A \text{ and } b \in B\}$. A relation $\stackrel{\epsilon}{\Longrightarrow}_{\mathsf{P}} \subseteq S_{\mathsf{P}} \times S_{\mathsf{P}}$ is defined by $p \stackrel{\epsilon}{\Longrightarrow}_{\mathsf{P}} p'$ iff $p(\stackrel{\tau}{\longrightarrow}_{\mathsf{P}})^* p'$. Generalising $\stackrel{\epsilon}{\Longrightarrow}_{\mathsf{P}}$ for visible actions $a \in \mathcal{A}$, we obtain $p \stackrel{a}{\Longrightarrow|}_{\mathsf{P}} p'$ iff there exists p_a such that $p \stackrel{\epsilon}{\Longrightarrow}_{\mathsf{P}} p_a \stackrel{a}{\longrightarrow}_{\mathsf{P}} p'$, and $p \stackrel{a}{\Longrightarrow}_{\mathsf{P}} p'$ iff there exists p_a such that $p \stackrel{a}{\Longrightarrow|}_{\mathsf{P}} p_a \stackrel{\epsilon}{\Longrightarrow}_{\mathsf{P}} p'$. The extension to words $w = a_1 \ldots a_n$ is defined in the natural way by $p \stackrel{w}{\Longrightarrow}_{\mathsf{P}} p'$ iff $p \stackrel{a_1}{\Longrightarrow}_{\mathsf{P}} \ldots \stackrel{a_n}{\Longrightarrow}_{\mathsf{P}} p'$.

Henceforth, let P, Q and R be operational components with signatures $\langle \mathcal{A}^I_{\mathsf{P}}, \mathcal{A}^O_{\mathsf{P}}, S_{\mathsf{P}}, \longrightarrow_{\mathsf{P}}, s^0_{\mathsf{P}}, \bot_{\mathsf{P}} \rangle$, $\langle \mathcal{A}^I_{\mathsf{Q}}, \mathcal{A}^O_{\mathsf{Q}}, S_{\mathsf{Q}}, \longrightarrow_{\mathsf{Q}}, s^0_{\mathsf{Q}}, \bot_{\mathsf{Q}} \rangle$ and $\langle \mathcal{A}^I_{\mathsf{R}}, \mathcal{A}^O_{\mathsf{R}}, S_{\mathsf{R}}, \longrightarrow_{\mathsf{R}}, s^0_{\mathsf{R}}, \bot_{\mathsf{R}} \rangle$ respectively.

4.1. Refinement

We now give semantic mappings from operational models to trace-based models that preserve both substitutive and progress-sensitive behaviour.

Definition 19. *Let P be an operational component. Then $[\![\mathsf{P}]\!]$ is the trace-based component $\langle \mathcal{A}^I_{\mathsf{P}}, \mathcal{A}^O_{\mathsf{P}}, T_{[\![\mathsf{P}]\!]}, F_{[\![\mathsf{P}]\!]} \rangle$, where $T_{[\![\mathsf{P}]\!]} = \{t : s^0_{\mathsf{P}} \stackrel{t}{\Longrightarrow}_{\mathsf{P}}\}$ and $F_{[\![\mathsf{P}]\!]} = \{t : s^0_{\mathsf{P}} \stackrel{t}{\Longrightarrow}_{\mathsf{P}} \bot_{\mathsf{P}}\}$.*

The trace-based representation of an operational model simply records the component's interface, and its sets of observable and inconsistent traces.

Definition 20. *Let P be an operational component. Then $[\![\mathsf{P}]\!]^l$ is the progress-sensitive trace-based component $\langle \mathcal{A}^I_{\mathsf{P}}, \mathcal{A}^O_{\mathsf{P}}, T_{[\![\mathsf{P}]\!]}, F_{[\![\mathsf{P}]\!]}, D_{[\![\mathsf{P}]\!]^l}, K_{[\![\mathsf{P}]\!]^l} \rangle$, where:*

- $D_{[\![\mathsf{P}]\!]^l} = \{t : \exists s' \cdot s^0_{\mathsf{P}} \stackrel{t}{\Longrightarrow}_{\mathsf{P}} s'$ *and s' can diverge*$\}$
- $K_{[\![\mathsf{P}]\!]^l} = \{t : \exists s' \cdot s^0_{\mathsf{P}} \stackrel{t}{\Longrightarrow}_{\mathsf{P}} s'$ *and* $\nexists o \in \mathcal{A}^O_{\mathsf{P}} \cup \{\tau\} \cdot s' \stackrel{o}{\longrightarrow}_{\mathsf{P}}\} \cup D_{[\![\mathsf{P}]\!]^l}$.

The progress-sensitive trace-based representation of an operational model includes the constituents of a standard trace-based component, together with a set of extended divergent traces and a set of extended quiescent traces. The inclusion of inconsistent traces within the divergent and quiescent trace sets is a condition of being a progress-sensitive component (cf Definition 11). Note that $D_{[\![\mathsf{P}]\!]^l}$ includes all inconsistent traces, since $\bot_{\mathsf{P}}$ is divergent. Moreover, only stable states (without outgoing τ transitions) are able to be quiescent (although the extended quiescent trace set includes divergences). This has similarities with the stable-failures and failures-divergences models of CSP (Hoare, 1985).

Based on these mappings to trace-based models, we can formulate definitions of refinement on operational models.

Definition 21. *Let* P *and* Q *be operational components. Then* Q *is a substitutable refinement of* P*, written* $\mathsf{Q} \sqsubseteq_{op} \mathsf{P}$*, iff* $[\![\mathsf{Q}]\!] \sqsubseteq_{imp} [\![\mathsf{P}]\!]$*. Similarly,* Q *is a substitutable and progress-sensitive refinement of* P*, written* $\mathsf{Q} \sqsubseteq^{l}_{op} \mathsf{P}$*, iff* $[\![\mathsf{Q}]\!]^l \sqsubseteq^{l}_{imp} [\![\mathsf{P}]\!]^l$*.*

Justification of these mappings is presented in Section 4.7. But first, we present operational definitions for all of the operators considered in the trace-based section with respect to both the substitutive and progress-sensitive refinement preorders. For each operator, we make explicit the relationship with the trace-based definition. This allows the compositionality results from the trace-based sections to carry across to this operational setting.

4.2. Parallel Composition

We give a single operational definition of parallel composition applicable to both the substitutive and progress-sensitive refinements.

Definition 22. *Let* P *and* Q *be components composable for parallel. Then the parallel composition of* P *and* Q *is the component* $\mathsf{P} \mid\mid \mathsf{Q} = \mathsf{P} \mid\mid_l \mathsf{Q} = \langle \mathcal{A}^I, \mathcal{A}^O, S, \longrightarrow, s_0, \bot \rangle$*, where:*

- $\mathcal{A}^I = (\mathcal{A}^I_{\mathsf{P}} \cup \mathcal{A}^I_{\mathsf{Q}}) \setminus (\mathcal{A}^O_{\mathsf{P}} \cup \mathcal{A}^O_{\mathsf{Q}})$
- $\mathcal{A}^O = \mathcal{A}^O_{\mathsf{P}} \cup \mathcal{A}^O_{\mathsf{Q}}$
- $S = S_{\mathsf{P}} \mid\mid S_{\mathsf{Q}}$
- $\longrightarrow$ *is the smallest relation satisfying the following rules:*

  P1. If $p \xrightarrow{a}_{\mathsf{P}} p'$ *with* $a \in \mathcal{A}_{\mathsf{P}} \setminus \mathcal{A}_{\mathsf{Q}} \cup \{\tau\}$*, then* $p \mid\mid q \xrightarrow{a} p' \mid\mid q$

  P2. If $q \xrightarrow{a}_{\mathsf{Q}} q'$ *with* $a \in \mathcal{A}_{\mathsf{Q}} \setminus \mathcal{A}_{\mathsf{P}} \cup \{\tau\}$*, then* $p \mid\mid q \xrightarrow{a} p \mid\mid q'$

  P3. If $p \xrightarrow{a}_{\mathsf{P}} p'$ *and* $q \xrightarrow{a}_{\mathsf{Q}} q'$ *with* $a \in \mathcal{A}_{\mathsf{P}} \cap \mathcal{A}_{\mathsf{Q}}$*, then* $p \mid\mid q \xrightarrow{a} p' \mid\mid q'$*.*

- $s_0 = s^0_{\mathsf{P}} \mid\mid s^0_{\mathsf{Q}}$
- $\{\bot\} = (S_{\mathsf{P}} \mid\mid \{\bot_{\mathsf{Q}}\}) \cup (\{\bot_{\mathsf{P}}\} \mid\mid S_{\mathsf{Q}})$.

Conditions P1 to P3 ensure that the parallel composition of components interleaves on independent actions and synchronises on common actions. For P3, given the parallel composability constraint, synchronisation can take place between an output and an input, or two inputs.

The following theorem shows the relationship between parallel composition on operational and trace-based components. Consequently, the monotonicity results from the trace-based sections are applicable here.

Theorem 14. *Let* P *and* Q *be components composable for parallel composition. Then* $[\![\mathsf{P} \mid\mid \mathsf{Q}]\!] = [\![\mathsf{P}]\!] \mid\mid [\![\mathsf{Q}]\!]$ *and* $[\![\mathsf{P} \mid\mid_l \mathsf{Q}]\!]^l = [\![\mathsf{P}]\!]^l \mid\mid_l [\![\mathsf{Q}]\!]^l$.

4.3. Conjunction

We now formulate an operational definition of conjunction. As this operator corresponds to the meet of the refinement preorder, its definition depends on the refinement type we are considering. For substitutive refinement, we have a straightforward definition that considers the enabled actions in any pair of states. When considering the progress-sensitive refinement, we first apply the substitutive definition, but then have to prune bad states that violate progress. These bad states are defined inductively.

Definition 23. *Let* P *and* Q *be components composable for conjunction. Then the substitutive conjunction of* P *and* Q *is a component* $\mathsf{P} \wedge \mathsf{Q} = \langle \mathcal{A}^I_{\mathsf{P}} \cup \mathcal{A}^I_{\mathsf{Q}}, \mathcal{A}^O_{\mathsf{P}} \cap \mathcal{A}^O_{\mathsf{Q}}, S, \longrightarrow, s_0, \bot \rangle$*, where:*

- $S = S_{\mathsf{P}} \wedge S_{\mathsf{Q}}$
- $\longrightarrow$ *is the smallest relation satisfying the following rules:*

  C1. If $a \in \mathcal{A}_{\mathsf{P}} \cap \mathcal{A}_{\mathsf{Q}}$, $p \stackrel{a}{\Longrightarrow\!\!|}_{\mathsf{P}} p'$ *and* $q \stackrel{a}{\Longrightarrow\!\!|}_{\mathsf{Q}} q'$, *then* $p \wedge q \stackrel{a}{\longrightarrow} p' \wedge q'$

  C2. If $a \in \mathcal{A}^I_{\mathsf{P}} \setminus \mathcal{A}^I_{\mathsf{Q}}$ *and* $p \stackrel{a}{\Longrightarrow\!\!|}_{\mathsf{P}} p'$, *then* $p \wedge q \stackrel{a}{\longrightarrow} p' \wedge \bot_{\mathsf{Q}}$

  C3. If $a \in \mathcal{A}^I_{\mathsf{Q}} \setminus \mathcal{A}^I_{\mathsf{P}}$ *and* $q \stackrel{a}{\Longrightarrow\!\!|}_{\mathsf{Q}} q'$, *then* $p \wedge q \stackrel{a}{\longrightarrow} \bot_{\mathsf{P}} \wedge q'$

  C4. If p *does not diverge and* $p \stackrel{\tau}{\longrightarrow}_{\mathsf{P}} p'$, *then* $p \wedge q \stackrel{\tau}{\longrightarrow} p' \wedge q$

  C5. If q *does not diverge and* $q \stackrel{\tau}{\longrightarrow}_{\mathsf{Q}} q'$, *then* $p \wedge q \stackrel{\tau}{\longrightarrow} p \wedge q'$

  C6. If p *diverges and* q *diverges, then* $p \wedge q \stackrel{\tau}{\longrightarrow} p \wedge q$.

- $s_0 = s^0_{\mathsf{P}} \wedge s^0_{\mathsf{Q}}$
- $\bot = \bot_{\mathsf{P}} \wedge \bot_{\mathsf{Q}}$.

In contrast to the definition in Chen et al. (2012), here we give a more elaborate handling of τ transitions in order to use the same base definition for conjunction under substitutivity and progress. The original definition permitted τ transitions to proceed independently, which allows the conjunction to diverge if at least one of the components can diverge. However, this is not acceptable under our progress-sensitive refinement preorder. Instead, we must only allow the conjunction to diverge on occasions when both components are willing to diverge. This is achieved by condition C6 and the fact that the remaining conditions work on the τ-closure of the components.

We now inductively define the pruned conjunction of two components, which is used for defining conjunction under the progress-sensitive preorder.

Definition 24. *Let* P *and* Q *be components composable for conjunction. The progress-sensitive conjunction of* P *and* Q*, denoted* $\mathsf{P} \wedge_l \mathsf{Q}$*, is obtained from* $\mathsf{P} \wedge \mathsf{Q}$ *by pruning all states in* F*, the smallest set defined inductively by:*

- *If* p *is stable,* $p \xrightarrow{o}_{\mathsf{P}}$ *for some* $o \in \mathcal{A}^O_{\mathsf{P}}$*, and* $\nexists a \in \mathcal{A}^O_{\mathsf{P}\wedge\mathsf{Q}} \cdot p \wedge q \xrightarrow{a} p' \wedge q'$ *with* $p' \wedge q' \notin F$*, then* $p \wedge q \in F$
- *If* q *is stable,* $q \xrightarrow{o}_{\mathsf{Q}}$ *for some* $o \in \mathcal{A}^O_{\mathsf{Q}}$*, and* $\nexists a \in \mathcal{A}^O_{\mathsf{P}\wedge\mathsf{Q}} \cdot p \wedge q \xrightarrow{a} p' \wedge q'$ *with* $p' \wedge q' \notin F$*, then* $p \wedge q \in F$
- *If* $p \wedge q \xrightarrow{a} p' \wedge q'$ *for* $a \in \mathcal{A}^I_{\mathcal{P}\wedge\mathcal{Q}}$ **implies** $p' \wedge q' \in F$*, then* $p \wedge q \in F$*.*

Note that $\mathsf{P} \wedge_l \mathsf{Q}$ may prune the initial state in $\mathsf{P} \wedge \mathsf{Q}$, in which case we say that $\mathsf{P} \wedge_l \mathsf{Q}$ is unrealisable. As for parallel, there is a correspondence between conjunction at the operational and trace-based levels.

Theorem 15. *Let* P *and* Q *be operational components composable for conjunction. Then* $[\![\mathsf{P} \wedge \mathsf{Q}]\!] = [\![\mathsf{P}]\!] \wedge [\![\mathsf{Q}]\!]$ *and* $[\![\mathsf{P} \wedge_l \mathsf{Q}]\!]^l = [\![\mathsf{P}]\!]^l \wedge_l [\![\mathsf{Q}]\!]^l$*.*

4.4. Disjunction

As the trace-based definition of disjunction does not need to prune error traces, the operational definition of disjunction is applicable to both the substitutive and progress-sensitive refinements.

Definition 25. *Let* P *and* Q *be components composable for disjunction. Then the disjunction of* P *and* Q *is the component* $\mathsf{P} \vee \mathsf{Q} = \mathsf{P} \vee_l \mathsf{Q} = \langle \mathcal{A}^I_{\mathsf{P}} \cap \mathcal{A}^I_{\mathsf{Q}}, \mathcal{A}^O_{\mathsf{P}} \cup \mathcal{A}^O_{\mathsf{Q}}, S, \longrightarrow, s_0, \bot \rangle$*, where:*

- $S = \{s_0\} \cup S_{\mathsf{P}} \cup S_{\mathsf{Q}}$, *for* $s_0 \notin S_{\mathsf{P}}, S_{\mathsf{Q}}$
- $\longrightarrow$ *is the smallest relation containing* $\longrightarrow_{\mathsf{P}}$ *and* $\longrightarrow_{\mathsf{Q}}$ *restricted to* $\mathcal{A}_{\mathsf{P}\vee\mathsf{Q}}$, *and the transitions* $s_0 \xrightarrow{\tau} s^0_{\mathsf{P}}$ *and* $s_0 \xrightarrow{\tau} s^0_{\mathsf{Q}}$
- $\{\bot\} = \{\bot_{\mathsf{P}}, \bot_{\mathsf{Q}}\}$.

A correspondence can be shown between the two forms of operational disjunction and the trace-based versions.

Theorem 16. *Let* P *and* Q *be components composable for disjunction. Then* $[\![\mathsf{P} \vee \mathsf{Q}]\!] = [\![\mathsf{P}]\!] \vee [\![\mathsf{Q}]\!]$ *and* $[\![\mathsf{P} \vee_l \mathsf{Q}]\!]^l = [\![\mathsf{P}]\!]^l \vee_l [\![\mathsf{Q}]\!]^l$.

4.5. Hiding

Since hiding is not concerned with the refinement preorder, it has a common definition for both the substitutive and progress frameworks.

Definition 26. *Let* P *be a component and let* b *be an action. The hiding of* b *from* P *is the component* $\mathsf{P}/b = \mathsf{P} /_l b = \langle \mathcal{A}^I_{\mathsf{P}} \setminus \{b\}, \mathcal{A}^O_{\mathsf{P}} \setminus \{b\}, S_{\mathsf{P}}, \longrightarrow, s^0_{\mathsf{P}}, \bot_{\mathsf{P}} \rangle$, *where:*

H1. If $p \xrightarrow{a}_{\mathsf{P}} p'$ *and* $a \neq b$, *then* $p \xrightarrow{a} p'$

H2. If $p \xrightarrow{b}_{\mathsf{P}} p'$ *and* $b \in \mathcal{A}^O_{\mathsf{P}}$, *then* $p \xrightarrow{\tau} p'$.

As for all of the previously considered operators, there is a natural correspondence between hiding on operational and trace-based models.

Theorem 17. *Let* P *be a component, and let* b *be an arbitrary action. Then* $[\![\mathsf{P}/b]\!] = [\![\mathsf{P}]\!]/b$ *and* $[\![\mathsf{P} /_l b]\!]^l = [\![\mathsf{P}]\!]^l /_l b$.

4.6. Quotient

The operational definition of quotient needs to consider all resolutions of non-determinism in the components to be composed. For simplicity, we therefore restrict to deterministic components without τ-transitions. We begin by giving an operational definition of quotient for which we must prune a number of states that violate inconsistency containment on the substitutive refinement preorder. We then extend the pruning so that it removes violations of the quiescence containment on the progress-sensitive refinement relation. To improve the clarity of our definition, we further assume that the quotient can observe all of R's actions.

Definition 27. *Let* P *and* R *be deterministic components such that* $\mathcal{A}^O_\mathsf{P} \subseteq \mathcal{A}^O_\mathsf{R}$*. Then the quotient is the component* $\mathsf{R}/\mathsf{P} = \langle \mathcal{A}^I_{\mathsf{R}/\mathsf{P}}, \mathcal{A}^O_{\mathsf{R}/\mathsf{P}}, S_{\mathsf{R}/\mathsf{P}}, \longrightarrow, s_0, \bot_{\mathsf{R}/\mathsf{P}} \rangle$*, where:*

- $\mathcal{A}^I_{\mathsf{R}/\mathsf{P}} = \mathcal{A}^I_\mathsf{R} \cup \mathcal{A}^O_\mathsf{P}$
- $\mathcal{A}^O_{\mathsf{R}/\mathsf{P}} = \mathcal{A}^O_\mathsf{R} \setminus \mathcal{A}^O_\mathsf{P}$
- $S_{\mathsf{R}/\mathsf{P}} = (S_\mathsf{R}/S_\mathsf{P}) \setminus F$
- $\longrightarrow$ *is the smallest relation satisfying the following rules:*

  Q1. *If* $a \in \mathcal{A}_{\mathsf{R}/\mathsf{P}} \setminus \mathcal{A}_\mathsf{P}$ *and* $r \xrightarrow{a}_\mathsf{R} r'$*, then* $r/p \xrightarrow{a} r'/p$

  Q2. *If* $a \in \mathcal{A}_{\mathsf{R}/\mathsf{P}} \cap \mathcal{A}_\mathsf{P}$*,* $r \xrightarrow{a}_\mathsf{R} r'$ *and* $p \xrightarrow{a}_\mathsf{P} p'$*, then* $r/p \xrightarrow{a} r'/p'$

  Q3. *If* $a \in \mathcal{A}_{\mathsf{R}/\mathsf{P}} \cap \mathcal{A}_\mathsf{P}$ *and* $p \not\xrightarrow{a}_\mathsf{P}$*, then* $r/p \xrightarrow{a} \bot_{\mathsf{R}/\mathsf{P}}$

- $s_0 = \begin{cases} s^0_\mathsf{R}/s^0_\mathsf{P} & \text{both } s^0_\mathsf{R} \text{ and } s^0_\mathsf{P} \text{ are defined} \\ \bot_{\mathsf{R}/\mathsf{P}} & s^0_\mathsf{P} \text{ undefined} \\ \text{undefined} & s^0_\mathsf{R} \text{ undefined and } s^0_\mathsf{P} \text{ defined} \end{cases}$
- $\{\bot_{\mathsf{R}/\mathsf{P}}\} = \{\bot_{\mathcal{E}(\mathsf{R})}\}/S_\mathsf{P}$
- $F \subseteq S_\mathsf{R}/S_\mathsf{P}$ *is the smallest set satisfying:*

  F1. *If* $r \neq \bot_\mathsf{R}$ *and* $p = \bot_\mathsf{P}$*, then* $r/p \in F$

  F2. *If* $a \in \mathcal{A}^O_\mathsf{R} \cap \mathcal{A}^O_\mathsf{P}$*,* $r \not\xrightarrow{a}_\mathsf{R}$ *and* $p \xrightarrow{a}_\mathsf{P}$*, then* $r/p \in F$

  F3. *If* $r/p \xrightarrow{a} r'/p'$*,* $a \in \mathcal{A}_\mathsf{R} \setminus \mathcal{A}^O_{\mathsf{R}/\mathsf{P}}$ *and* $r'/p' \in F$*, then* $r/p \in F$*.*

  These F*-states must be removed from the quotient (and the transition relation must consequently be pruned), so that* $\mathsf{P} \parallel (\mathsf{R}/\mathsf{P}) \sqsubseteq_{op} \mathsf{R}$*.*

Conditions Q1 and Q2 essentially correspond to the parallel composition of P and R, whereby the two components synchronise on common actions, and interleave on the independent actions of R. Independent actions of P must be inputs, so they are irrelevant to the quotient, since an environment safe for R will never issue them. Condition Q3 states that the quotient can become inconsistent on an input that is never issued by P (meaning the action is an output of P). Conditions F1 and F2 capture situations where substitutivity

would be violated, while F3 propagates the violation backwards to a point where the quotient can avoid it, by not producing an output from which the environment can, under its own control, reach the violation.

As quotient is the adjoint of parallel composition under the refinement relation, we must give an alternative characterisation for the progress-sensitive framework. We do this by removing states that introduce quiescence errors in the definition above.

Definition 28. *Let* P *and* R *be deterministic components such that* $\mathcal{A}^O_{\mathsf{P}} \subseteq \mathcal{A}^O_{\mathsf{R}}$*. Then the progress-sensitive quotient is the component* $\mathsf{R} \mathbin{/_l} \mathsf{P}$ *obtained from* R/P *by removing states contained within the smallest* F*-set defined by:*

- *If* $\exists o \in \mathcal{A}^O_{\mathsf{R}} \cdot r \xrightarrow{o}_{\mathsf{R}}$, $\nexists a \in \mathcal{A}^O_{\mathsf{P}} \cdot p \xrightarrow{a}_{\mathsf{P}}$ *and* $\nexists b \in \mathcal{A}^O_{\mathsf{R}/\mathsf{P}} \cdot r/p \xrightarrow{b}_{\mathsf{R}/\mathsf{P}} r'/p'$ *with* $r'/p' \notin F$*, then* $r/p \in F$
- *If* $r/p \xrightarrow{a} r'/p'$*,* $a \in \mathcal{A}_{\mathsf{R}} \setminus \mathcal{A}^O_{\mathsf{R}/\mathsf{P}}$ *and* $r'/p' \in F$*, then* $r/p \in F$*.*

As usual, the operational definitions are closely related to the trace-based definitions.

Theorem 18. *Let* P *and* R *be deterministic components such that* $\mathcal{A}^O_{\mathsf{P}} \subseteq \mathcal{A}^O_{\mathsf{R}}$*. Then* $[\![\mathsf{R}/\mathsf{P}]\!] = [\![\mathsf{R}]\!]/[\![\mathsf{P}]\!]$ *and* $[\![\mathsf{R} \mathbin{/_l} \mathsf{P}]\!]^l = [\![\mathsf{R}]\!]^l \mathbin{/_l} [\![\mathsf{P}]\!]^l$*.*

4.7. Full Abstraction

The close correspondence between the operational and trace-based models allows us to present a full abstraction result for the operational framework. This relies on showing that operational refinement $\sqsubseteq_{op}$ given in terms of trace containment can be equated with contextual checking of inconsistency in the operational models.

Definition 29. *Let* P *and* Q *be operational components. Then* Q *is said to be inconsistency substitutable for* P*, denoted by* $\mathsf{Q} \sqsubseteq^F_{op} \mathsf{P}$*, iff* $\bot_{\mathsf{Q}}$ *is reachable from* s^0_{Q} *by hidden and output actions implies* $\bot_{\mathsf{P}}$ *is reachable from* s^0_{P} *by hidden and output actions.*

From this, $\mathsf{Q} \sqsubseteq_{op} \mathsf{P}$ can be characterised by $\sqsubseteq^F_{op}$ when considering the environments that Q and P can interact with. This shows that $\sqsubseteq_{op}$ is the weakest preorder preserving substitutivity.

Theorem 19. *Let* P *and* Q *be operational components such that* $\mathcal{A}^I_\mathsf{P} \subseteq \mathcal{A}^I_\mathsf{Q}$, $\mathcal{A}^O_\mathsf{Q} \subseteq \mathcal{A}^O_\mathsf{P}$ *and* $\mathcal{A}^I_\mathsf{Q} \cap \mathcal{A}^O_\mathsf{P} = \emptyset$. *Then:*

$$\mathsf{Q} \sqsubseteq_{op} \mathsf{P} \text{ iff } \forall \mathsf{R} \cdot \mathcal{A}^O_\mathsf{R} = \mathcal{A}^I_\mathsf{P} \text{ and } \mathcal{A}^I_\mathsf{R} = \mathcal{A}^O_\mathsf{Q} \implies \mathsf{Q} \parallel \mathsf{R} \sqsubseteq^F_{op} \mathsf{P} \parallel \mathsf{R}.$$

Based on this result, it is straightforward to show full abstraction.

Corollary 2. *Operational equivalence* $\equiv_{op}$ *is fully abstract for parallel composition, conjunction, disjunction, hiding and quotient with respect to observational equivalence of inconsistency.*

5. On the Relationship with Interface Automata

In this section, we relate our operational theory of components to the interface automata of de Alfaro and Henzinger (2001). We show that the theory of interface automata can be embedded within our framework, and demonstrate that the alternating refinement relation is stronger than our substitutive preorder.

5.1. Interface Automata

We recall a general definition of interface automata (de Alfaro and Henzinger, 2001), which, unlike the restrictions imposed in (de Alfaro and Henzinger, 2005), permits hidden transitions and does not insist on determinism of inputs. Thus, an interface automaton can be thought of as a finite-state machine with transitions labelled by input, output or τ, and does not require input enabledness in each state.

Definition 30. *An* interface automaton P *is a tuple* $\langle S_\mathsf{P}, \mathcal{A}^I_\mathsf{P}, \mathcal{A}^O_\mathsf{P}, \longrightarrow_\mathsf{P}, s^0_\mathsf{P} \rangle$, *where:*

- S_P *is a finite set of states*
- $\mathcal{A}^I_\mathsf{P}$ *is a finite set of input actions*
- $\mathcal{A}^O_\mathsf{P}$ *is a finite set of output actions, disjoint from* $\mathcal{A}^I_\mathsf{P}$
- $\longrightarrow_\mathsf{P} \subseteq S_\mathsf{P} \times (\mathcal{A}_\mathsf{P} \cup \{\tau\}) \times S_\mathsf{P}$ *is the transition relation*
- $s^0_\mathsf{P} \in S_\mathsf{P}$ *is the designated initial state.*

Substitutive refinement of interface automata is given by means of alternating simulation, with a covariant inclusion on inputs and contravariant inclusion on outputs. Again, we reproduce the general definition from (de Alfaro and Henzinger, 2001), which is free of unnecessary restrictions. First, we introduce two shorthands for simplifying the definition:

- $Act^I_{\mathsf{P}}(p) \triangleq \{a \in \mathcal{A}^I_{\mathsf{P}} : p \stackrel{\epsilon}{\Longrightarrow}_{\mathsf{P}} p' \text{ implies } p' \stackrel{a}{\longrightarrow}_{\mathsf{P}}\}$
- $Act^O_{\mathsf{P}}(p) \triangleq \{a \in \mathcal{A}^O_{\mathsf{P}} : p \stackrel{\epsilon}{\Longrightarrow}_{\mathsf{P}} \stackrel{a}{\longrightarrow}_{\mathsf{P}}\}$.

The set $Act^I_{\mathsf{P}}(p)$ denotes the input actions that may safely be issued when P is in state p. Any action in $Act^I_{\mathsf{P}}(p)$ must therefore be enabled in any state reachable from p by hidden transitions. On the other hand, $Act^O_{\mathsf{P}}(p)$ represents the output actions of P that the environment must be willing to accept. Thus, this set is the collection of outputs enabled in any state reachable from p by hidden transitions. We now give the formal definition of alternating refinement.

Definition 31. *Interface automaton* Q *is said to be an* alternating refinement *of* P*, written* $\mathsf{Q} \sqsubseteq_{IA} \mathsf{P}$*, just if* $\mathcal{A}^I_{\mathsf{P}} \subseteq \mathcal{A}^I_{\mathsf{Q}}$*,* $\mathcal{A}^O_{\mathsf{Q}} \subseteq \mathcal{A}^O_{\mathsf{P}}$*, and* $s^0_{\mathsf{Q}}\ R\ s^0_{\mathsf{P}}$*, where* $R \subseteq S_{\mathsf{Q}} \times S_{\mathsf{P}}$ *is an alternating simulation satisfying the property: if* $q\ R\ p$*, then:*

AS1. $Act^I_{\mathsf{P}}(p) \subseteq Act^I_{\mathsf{Q}}(q)$

AS2. $Act^O_{\mathsf{Q}}(q) \subseteq Act^O_{\mathsf{P}}(p)$

AS3. For each $a \in Act^I_{\mathsf{P}}(p) \cup Act^O_{\mathsf{Q}}(q)$ *and for each* $q \stackrel{a}{\Longrightarrow}\!|_{\mathsf{Q}}\ q'$*, there exists* $p \stackrel{a}{\Longrightarrow}\!|_{\mathsf{P}}\ p'$ *such that* $q'\ R\ p'$*.*

Conditions AS1 and AS2 require that q can safely accept any input that p is willing to accept, while q will only produce a subset of outputs that p can produce. Condition AS3 propagates this constraint on to the common successor states.

5.1.1. Relation with Operational Components

We now indicate how to map interface automata to the operational components as defined in Section 4. The mapping must add additional transitions for the non-enabled inputs to the special inconsistent state $\perp$.

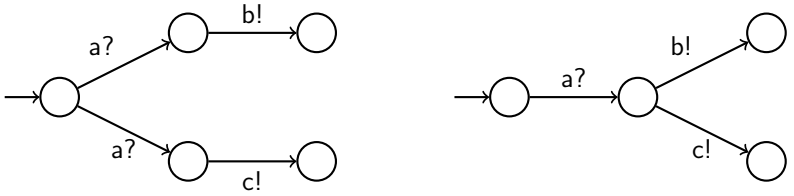

Figure 11: Interface automata distinguishing alternating simulation and $\sqsubseteq_{imp}$.

Definition 32. *Let* P *be an interface automaton. Then the corresponding operational component is* $[\![\mathsf{P}]\!]^{IA} = \langle S_{\mathsf{P}} \cup \{\bot\}, \mathcal{A}^I_{\mathsf{P}}, \mathcal{A}^O_{\mathsf{P}}, \longrightarrow, s^0_{\mathsf{P}}, \bot\rangle$*, where:*

$$\longrightarrow = \longrightarrow_{\mathsf{P}} \cup \{(s, a, \bot) : s \in S_{\mathsf{P}},\ a \in \mathcal{A}^I_{\mathsf{P}} \text{ and } \nexists s' \cdot s \xrightarrow{a}_{\mathsf{P}} s'\}$$
$$\cup \{(\bot, a, \bot) : a \in \{\tau\} \cup \mathcal{A}_{\mathsf{P}}\}.$$

Given this definition, it should be straightforward to see that interface automata are a subclass of our operational components, in particular, the components that can only become inconsistent by seeing a bad input, and that are not permitted to be inconsistent up front.

The following theorem shows the relationship between alternating refinement and the substitutive preorder of our modelling framework.

Theorem 20. *Let* P *and* Q *be interface automata. Then* $\mathsf{Q} \sqsubseteq_{IA} \mathsf{P}$ *implies* $[\![\mathsf{Q}]\!]^{IA} \sqsubseteq_{op} [\![\mathsf{P}]\!]^{IA}$.

Being a branching-time relation, alternating refinement is too strong for substitutivity. This is demonstrated by the interface automata in Figure 11. The automaton on the left is an alternating refinement of the one on the right, but not vice-versa, whereas the component representations of the automata are substitutively equivalent in our framework under $\equiv_{op}$. Consequently, it is not the case in Theorem 20 that $[\![\mathsf{Q}]\!]^{IA} \sqsubseteq_{op} [\![\mathsf{P}]\!]^{IA}$ implies $\mathsf{Q} \sqsubseteq_{IA} \mathsf{P}$.

The existence of a matching transition in condition AS3 is the cause of this asymmetry in the expressive power of alternating refinement and our substitutive preorder. If we restrict to deterministic interface automata, the choice of successor is determined, and so the two refinements coincide.

Theorem 21. *Let* P *and* Q *be deterministic interface automata. Then* $\mathsf{Q} \sqsubseteq_{IA} \mathsf{P}$ *iff* $[\![\mathsf{Q}]\!]^{IA} \sqsubseteq_{op} [\![\mathsf{P}]\!]^{IA}$.

It is worth pointing out that the definition of alternating refinement by de Alfaro and Henzinger (2005), which applies only to input-deterministic

interface automata, is also too strong for substitutivity, since the original definition of alternating refinement relates more input-deterministic models than the later definition.

5.1.2. Compositional Operators

In this section, we briefly remark on the relation between the composition operators for interface automata and our operational framework.

Parallel composition of interface automata P and Q can be defined as $[\![\mathsf{P}]\!]^{IA} \mid\mid [\![\mathsf{Q}]\!]^{IA}$, after propagating inconsistencies backwards over output and τ transitions, and removing the resultant inconsistent states. The obtained model is an interface automaton only if the initial state remains. This also provides a characterisation of *compatibility* for interface automata: P and Q are compatible only if, after performing the parallel composition as just defined, the initial state remains.

Conjunction is more problematic to define, because of the discrepancies between alternating simulation and our substitutive refinement. If we consider only deterministic interface automata, for which the refinements coincide, conjunction of interface automata P and Q can be defined as $[\![\mathsf{P}]\!]^{IA} \wedge [\![\mathsf{Q}]\!]^{IA}$, after having pruned all inconsistent states. Disjunction can be defined similarly.

Hiding is also straightforward, in that removal of b from interface automaton P is given by $[\![\mathsf{P}]\!]^{IA}/b$, once all inconsistent states have been removed.

As quotient for interface automata is only defined on deterministic models (Bhaduri and Ramesh, 2008), alternating refinement and our substitutive refinement coincide. Therefore, the quotient of interface automaton P from R is given by the removal of inconsistent states from $[\![\mathsf{R}]\!]^{IA}/[\![\mathsf{P}]\!]^{IA}$, but is only defined when $[\![\mathsf{R}]\!]^{IA}/[\![\mathsf{P}]\!]^{IA}$ is realisable, the latter meaning that an initial state exists.

6. Conclusion and Future Work

We have developed a compositional specification theory for components that may be modelled operationally, closely mirroring actual implementations, or in an abstract manner by means of trace structures. Both frameworks admit linear-time refinement relations, defined in terms of traces, which correspond to substitutivity and progress-sensitive substitutivity respectively. We define the operations of parallel composition, conjunction, disjunction, hiding and quotient, and prove that the induced equivalence is

a congruence for these operations, allowing us to provide full abstraction results. The simplicity of our formalism facilitates compositional reasoning about the temporal ordering of interactions needed for assume-guarantee inference, both for safety (Chilton et al., 2013) and (progress-sensitive) liveness properties.

Acknowledgments. The authors are supported by EU FP7 project CONNECT and ERC Advanced Grant VERIWARE. We would also like to thank the anonymous reviewers for their insightful comments.

References

Aarts, F., Vaandrager, F., 2010. Learning I/O Automata, in: Gastin, P., Laroussinie, F. (Eds.), CONCUR 2010 - Concurrency Theory. Springer. volume 6269 of *Lecture Notes in Computer Science*, pp. 71–85.

de Alfaro, L., Henzinger, T.A., 2001. Interface automata. SIGSOFT Softw. Eng. Notes 26, 109–120.

de Alfaro, L., Henzinger, T.A., 2005. Interface-based design, in: Broy, M., Grünbauer, J., Harel, D., Hoare, T. (Eds.), Engineering Theories of Software Intensive Systems. Springer. volume 195 of *NATO Science Series II: Mathematics, Physics and Chemistry*, pp. 83–104.

Alur, R., Henzinger, T.A., Kupferman, O., Vardi, M.Y., 1998. Alternating refinement relations, in: Sangiorgi, D., de Simone, R. (Eds.), CONCUR '98: Concurrency Theory. Springer. volume 1466 of *Lecture Notes in Computer Science*, pp. 163–178.

Bhaduri, P., Ramesh, S., 2008. Interface synthesis and protocol conversion. Form. Asp. Comput. 20, 205–224.

Brookes, S.D., Hoare, C.A.R., Roscoe, A.W., 1984. A theory of communicating sequential processes. J. ACM 31, 560–599.

Chen, T., Chilton, C., Jonsson, B., Kwiatkowska, M., 2012. A Compositional Specification Theory for Component Behaviours, in: Seidl, H. (Ed.), Programming Languages and Systems, Proc. 21st European Symposium on Programming (ESOP'12), Springer-Verlag. pp. 148–168.

Chilton, C., Jonsson, B., Kwiatkowska, M., 2013. Assume-guarantee reasoning for safe component behaviours, in: Pasareanu, C., Salaün, G. (Eds.), Proc. 9th International Symposium on Formal Aspects of Component Software (FACS'12), Springer. pp. 92–109.

Chilton, C., Kwiatkowska, M., Wang, X., 2012. Revisiting timed specification theories: A linear-time perspective, in: Jurdzinski, M., Nickovic, D. (Eds.), Proc. 10th International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS'12), Springer. pp. 75–90.

Dill, D.L., 1988. Trace theory for automatic hierarchical verification of speed-independent circuits. Ph.D. thesis. Carnegie Mellon University.

Doyen, L., Henzinger, T.A., Jobstmann, B., Petrov, T., 2008. Interface theories with component reuse, in: Proc. 8th ACM international conference on Embedded software, ACM. pp. 79–88.

Drissi, J., v. Bochmann, G., 1999. Submodule construction for systems of I/O automata. Technical Report. M.B. JOSEPHS, H.K. KAPOOR / CONTROLLABLE DELAY-INSENSITIVE PROCESSES.

van Glabbeek, R.J., 1994. Full abstraction in structural operational semantics (extended abstract), in: Proceedings of the Third International Conference on Methodology and Software Technology: Algebraic Methodology and Software Technology, Springer-Verlag. pp. 75–82.

Hoare, C.A.R., 1985. Communicating Sequential Processes. Prentice Hall.

Inverardi, P., Tivoli, M., 2013. Automatic Synthesis of Modular Connectors via Composition of Protocol Mediation Patterns, in: To appear in International Conference on Software Engineering.

Jonsson, B., 1991. A Hierarchy of Compositional Models of I/O Automata. Technical Report SICS:R91:04. Swedish Institute of Computer Science.

Jonsson, B., 1994. Compositional specification and verification of distributed systems. ACM Trans. on Programming Languages and Systems 16, 259–303.

Josephs, M., Hoare, C., Jifeng, H., 1989. A Theory of Asynchronous Processes. Technical Report PRG-TR-6-89. Oxford University Computing Laboratory.

Josephs, M.B., 1992. Receptive process theory. Acta Inf. 29, 17–31.

Josephs, M.B., Kapoor, H.K., 2007. Controllable delay-insensitive processes. Fundam. Inf. 78, 101–130.

Larsen, K.G., Nyman, U., Wasowski, A., 2007. Modal I/O automata for interface and product line theories, in: Nicola, R.D. (Ed.), ESOP, Springer. pp. 64–79.

Lüttgen, G., Vogler, W., 2007. Conjunction on processes: Full abstraction via ready-tree semantics. Theor. Comput. Sci. 373, 19–40.

Lüttgen, G., Vogler, W., 2010. Ready simulation for concurrency: It's logical! Inf. Comput. 208, 845–867.

Lynch, N.A., Tuttle, M.R., 1989. An introduction to input/output automata. CWI Quarterly 2, 219–246.

Milner, R., 1980. A Calculus of Communicating Systems. volume 92 of *Lecture Notes in Computer Science*. Springer.

de Nicola, R., Segala, R., 1995. A process algebraic view of input/output automata. Theor. Comput. Sci. 138, 391–423.

Raclet, J.B., 2008. Residual for component specifications. Electr. Notes Theor. Comput. Sci. 215, 93–110.

Raclet, J.B., Badouel, E., Benveniste, A., Caillaud, B., Legay, A., Passerone, R., 2009a. Modal Interfaces: Unifying Interface Automata and Modal Specifications, in: Proc. 7th International Conference on Embedded Software, ACM. pp. 87–96.

Raclet, J.B., Badouel, E., Benveniste, A., Caillaud, B., Legay, A., Passerone, R., 2011. A modal interface theory for component-based design. Fundam. Inform. 108, 119–149.

Raclet, J.B., Badouel, E., Benveniste, A., Caillaud, B., Passerone, R., 2009b. Why are modalities good for Interface Theories?, in: Proc. 9th International Conference on Application of Concurrency to System Design, IEEE Computer Society. pp. 119–127.

Romijn, J., Vaandrager, F., 1996. A note on fairness in i/o automata. Information Processing Letters 59, 245 – 250.

Segala, R., 1997. Quiescence, fairness, testing, and the notion of implementation. Inf. Comput. 138, 194–210.

Tretmans, J., 2011. Model-based testing and some steps towards test-based modelling, in: Bernardo, M., Issarny, V. (Eds.), SFM, Springer. pp. 297–326.

Verhoeff, T., 1994. A Theory of Delay-Insensitive Systems. PhD thesis. Dept. of Math. and C.S., Eindhoven Univ. of Technology.

Appendix A. Proofs of Results

Proof of Lemma 1

Reflexivity is trivial. Transitivity follows by transitivity of subset inclusion, given $T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{Q}} \subseteq T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{R}}$, and $T_{\mathcal{E}(\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{R}} \subseteq T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{R}}$.

Proof of Lemma 2

Follows immediately from the associativity and commutativity of the set and lifting operations.

Proof of Theorem 1

It is easy to show that the conditions on alphabets are satisfied. To show $t \in F_{\mathcal{E}(\mathcal{P}'||\mathcal{Q}')}$ implies $t \in F_{\mathcal{E}(\mathcal{P}||\mathcal{Q})} \cup (T_{\mathcal{E}(\mathcal{P}||\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{P}'||\mathcal{Q}'})$, proceed by induction on the length of the trace t.

- For $t \equiv \epsilon$, there exists $t' \in (\mathcal{A}^O_{\mathcal{P}'||\mathcal{Q}'})^*$ such that, without loss of generality, $t' \upharpoonright \mathcal{A}_{\mathcal{P}'} \in F_{\mathcal{P}'}$ and $t' \upharpoonright \mathcal{A}_{\mathcal{Q}'} \in T_{\mathcal{Q}'}$. Note that $t' \upharpoonright \mathcal{A}_{\mathcal{P}} = t' \upharpoonright \mathcal{A}_{\mathcal{P}'}$ and $t' \upharpoonright \mathcal{A}_{\mathcal{Q}} = t' \upharpoonright \mathcal{A}_{\mathcal{Q}'}$. To see this, first suppose there is an action on t' in $\mathcal{A}_{\mathcal{P}'} \setminus \mathcal{A}_{\mathcal{P}}$. Then this action is in $\mathcal{A}^I_{\mathcal{P}'} \cap \mathcal{A}^O_{\mathcal{Q}'}$, implying it is also in $\mathcal{A}^I_{\mathcal{P}'} \cap \mathcal{A}^O_{\mathcal{Q}'}$ by the constraints on parallel composition, which is contradictory. It is also contradictory if the action is in $\mathcal{A}_{\mathcal{P}} \setminus \mathcal{A}_{\mathcal{P}'}$, since it must also be in $\mathcal{A}^O_{\mathcal{P}'||\mathcal{Q}'}$. By refinement on the individual components, it thus holds that $t' \upharpoonright \mathcal{A}_{\mathcal{P}} \in F_{\mathcal{E}(\mathcal{P})} \cup (T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{P}'})$ and $t' \upharpoonright \mathcal{A}_{\mathcal{Q}} \in T_{\mathcal{E}(\mathcal{Q})} \cup (T_{\mathcal{E}(\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{Q}'})$. But, in fact, $t' \upharpoonright \mathcal{A}_{\mathcal{P}} \in F_{\mathcal{E}(\mathcal{P})}$ and $t' \upharpoonright \mathcal{A}_{\mathcal{Q}} \in T_{\mathcal{E}(\mathcal{Q})}$ since $t' \upharpoonright \mathcal{A}_{\mathcal{P}} = t' \upharpoonright \mathcal{A}_{\mathcal{P}'}$ and $t' \upharpoonright \mathcal{A}_{\mathcal{Q}} = t' \upharpoonright \mathcal{A}_{\mathcal{Q}'}$. Hence, $t' \in F_{\mathcal{E}(\mathcal{P}||\mathcal{Q})}$, implying $\epsilon \in F_{\mathcal{E}(\mathcal{P}||\mathcal{Q})}$.

- For $t \equiv t'a$ with $a \in \mathcal{A}^O_{\mathcal{P}'||\mathcal{Q}'} \cap \mathcal{A}^O_{\mathcal{P}'}$, it is known that $t' \in F_{\mathcal{E}(\mathcal{P}'||\mathcal{Q}')}$, so by the induction hypothesis it follows that $t' \in F_{\mathcal{E}(\mathcal{P}||\mathcal{Q})} \cup (T_{\mathcal{E}(\mathcal{P}||\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{P}'||\mathcal{Q}'})$. As $a \in \mathcal{A}^O_{\mathcal{P}||\mathcal{Q}}$, we thus have $t'a \in F_{\mathcal{E}(\mathcal{P}||\mathcal{Q})} \cup (T_{\mathcal{E}(\mathcal{P}||\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{P}'||\mathcal{Q}'})$ as required.

- For $t \equiv t'a$ with $a \in \mathcal{A}^I_{\mathcal{P}'||\mathcal{Q}'} \cap \mathcal{A}^I_{\mathcal{P}'}$, it holds by the induction hypothesis that $t' \in T_{\mathcal{E}(\mathcal{P}||\mathcal{Q})} \cup (T_{\mathcal{E}(\mathcal{P}||\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{P}'||\mathcal{Q}'})$. Suppose for a contradiction that $t'a \notin F_{\mathcal{E}(\mathcal{P}||\mathcal{Q})} \cup (T_{\mathcal{E}(\mathcal{P}||\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{P}'||\mathcal{Q}'})$. Then it follows that $t'a \in T_{\mathcal{P}||\mathcal{Q}}$. It can now be shown that $t'a \in F_{\mathcal{E}(\mathcal{P}||\mathcal{Q})}$ by using the same reasoning as when $t \equiv \epsilon$.

Now proceed by induction on the length of the trace t to show that $t \in T_{\mathcal{E}(\mathcal{P}'||\mathcal{Q}')}$ implies $t \in T_{\mathcal{E}(\mathcal{P}||\mathcal{Q})} \cup (T_{\mathcal{E}(\mathcal{P}||\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{P}'||\mathcal{Q}'})$.

- For $t \equiv \epsilon$, note that $\epsilon \in T_{\mathcal{E}(\mathcal{P}'||\mathcal{Q}')}$ implies $\epsilon \in T_{\mathcal{P}'}$ and $\epsilon \in T_{\mathcal{Q}'}$, which by refinement on components gives $\epsilon \in T_{\mathcal{P}} \cap T_{\mathcal{Q}}$, meaning $\epsilon \in T_{\mathcal{E}(\mathcal{P}||\mathcal{Q})}$.

- For $t \equiv t'a$ with $a \in \mathcal{A}^O_{\mathcal{P}'||\mathcal{Q}'} \cap \mathcal{A}^O_{\mathcal{P}'}$, note that in the difficult case $t'a \in T_{\mathcal{P}'||\mathcal{Q}'}$ and $t' \in T_{\mathcal{P}||\mathcal{Q}}$. Consequently, $t' \upharpoonright \mathcal{A}_{\mathcal{P}} = t' \upharpoonright \mathcal{A}_{\mathcal{P}'}$ and $t' \upharpoonright \mathcal{A}_{\mathcal{Q}} = t' \upharpoonright \mathcal{A}_{\mathcal{Q}'}$ by the alphabet constraints. Therefore, as $t'a \upharpoonright \mathcal{A}_{\mathcal{P}'} \in T_{\mathcal{P}'}$ it holds by refinement that $t'a \upharpoonright \mathcal{A}_{\mathcal{P}} \in T_{\mathcal{P}}$. Similarly, as $t'a \upharpoonright \mathcal{A}_{\mathcal{Q}'} \in T_{\mathcal{Q}'}$ it follows by the alphabet constraints that $a \in \mathcal{A}^I_{\mathcal{Q}}$ iff $a \in \mathcal{A}^I_{\mathcal{Q}'}$, hence $t'a \upharpoonright \mathcal{A}_{\mathcal{Q}} \in T_{\mathcal{Q}}$. Thus, $t'a \in T_{\mathcal{P}||\mathcal{Q}}$ as required.

- For $t \equiv t'a$ with $a \in \mathcal{A}^I_{\mathcal{P}'||\mathcal{Q}'}$, the result holds trivially by the induction hypothesis and input receptiveness of observable traces.

Proof of Lemma 3

Obvious, given the algebraic properties of the set operations.

Proof of Theorem 2

For the first claim, we consider just inconsistent trace containment (the proof for observable traces being similar). Let $t \in F_{\mathcal{E}(\mathcal{P}\wedge\mathcal{Q})}$, then there exists t' a prefix of t and $t'' \in (\mathcal{A}^O_{\mathcal{P}\wedge\mathcal{Q}})^*$ such that $t't'' \in F_{\mathcal{P}\wedge\mathcal{Q}}$. By the definition of conjunction, we have $t't'' \in F_{\mathcal{E}(\mathcal{P})} \cup (T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{Q}})$ and $t't'' \in F_{\mathcal{E}(\mathcal{Q})} \cup (T_{\mathcal{E}(\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{P}})$. By the properties of lifting, we see that $t't'' \in F_{\mathcal{E}(\mathcal{P})} \cup (T_{\mathcal{E}(\mathcal{P})} \uparrow (\mathcal{A}^I_{\mathcal{P}} \cup \mathcal{A}^I_{\mathcal{Q}}))$ and $t't'' \in F_{\mathcal{E}(\mathcal{Q})} \cup (T_{\mathcal{E}(\mathcal{Q})} \uparrow (\mathcal{A}^I_{\mathcal{P}} \cup \mathcal{A}^I_{\mathcal{Q}}))$. The result then follows from noting that $\mathcal{A}^I_{\mathcal{P}} \cup \mathcal{A}^I_{\mathcal{Q}} = \mathcal{A}^I_{\mathcal{P}\wedge\mathcal{Q}}$, $t'' \in (\mathcal{A}^O_{\mathcal{P}} \cap \mathcal{A}^O_{\mathcal{Q}})^*$, and extension closure of $F_{\mathcal{E}(\mathcal{P})} \cup (T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{P}\wedge\mathcal{Q}})$ and $F_{\mathcal{E}(\mathcal{Q})} \cup (T_{\mathcal{E}(\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{P}\wedge\mathcal{Q}})$.

For the second claim, we again show the containment on inconsistent traces, as the proof for the observable traces is near identical. Let $t \in F_{\mathcal{E}(\mathcal{R})}$. Then from $\mathcal{R} \sqsubseteq_{imp} \mathcal{P}$ and $\mathcal{R} \sqsubseteq_{imp} \mathcal{Q}$ we obtain $t \in F_{\mathcal{E}(\mathcal{P})} \cup (T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{R}})$ and $t \in F_{\mathcal{E}(\mathcal{Q})} \cup (T_{\mathcal{E}(\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{R}})$. Thus $t \in F_{\mathcal{E}(\mathcal{P})} \cap F_{\mathcal{E}(\mathcal{Q})}$ or $t \in F_{\mathcal{E}(\mathcal{P})} \cap (T_{\mathcal{E}(\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{R}})$ or $t \in F_{\mathcal{E}(\mathcal{Q})} \cap (T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{R}})$ or $t \in (T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{R}}) \cap (T_{\mathcal{E}(\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{R}})$. The first implies $t \in F_{\mathcal{E}(\mathcal{P}) \wedge \mathcal{E}(\mathcal{Q})}$, while the remaining three imply $t \in F_{\mathcal{E}(\mathcal{P}) \wedge \mathcal{E}(\mathcal{Q})} \cup (T_{\mathcal{E}(\mathcal{P}) \wedge \mathcal{E}(\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{R}})$. Hence $t \in F_{\mathcal{E}(\mathcal{P} \wedge \mathcal{Q})} \cup (T_{\mathcal{E}(\mathcal{P} \wedge \mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{R}})$ as required.

Finally, for the third claim, note that composability of $\mathcal{P}$ and $\mathcal{Q}$, and $\mathcal{P}'$ and $\mathcal{Q}'$ implies $\mathcal{A}^I_{\mathcal{P}' \wedge \mathcal{Q}'} \cap \mathcal{A}^O_{\mathcal{P} \wedge \mathcal{Q}} = \emptyset$. Hence the interfaces work out. So suppose $t \in F_{\mathcal{E}(\mathcal{P}' \wedge \mathcal{Q}')}$. Then there exists a prefix t' of t and $t'' \in (\mathcal{A}^O_{\mathcal{P} \wedge \mathcal{Q}})^*$ such that $t't'' \in F_{\mathcal{P}' \wedge \mathcal{Q}'}$. Consequently, $t't'' \in (F_{\mathcal{P}'} \cup (T_{\mathcal{P}'} \uparrow \mathcal{A}^I_{\mathcal{Q}'})) \cap (F_{\mathcal{Q}'} \cup (T_{\mathcal{Q}'} \uparrow \mathcal{A}^I_{\mathcal{P}'}))$. From $\mathcal{P}' \sqsubseteq_{imp} \mathcal{P}$ and $\mathcal{Q}' \sqsubseteq_{imp} \mathcal{Q}$, it follows that $t't'' \in F_{\mathcal{E}(\mathcal{P})} \cup (T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{P}'}) \cup (T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{Q}'}) \cup ((T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{P}'}) \uparrow \mathcal{A}^I_{\mathcal{Q}'})$ and $t't'' \in F_{\mathcal{E}(\mathcal{Q})} \cup (T_{\mathcal{E}(\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{Q}'}) \cup (T_{\mathcal{E}(\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{P}'}) \cup ((T_{\mathcal{E}(\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{Q}'}) \uparrow \mathcal{A}^I_{\mathcal{P}'})$. Rearranging, and distributing $\cup$ over $\cap$ we obtain $t't'' \in (F_{\mathcal{E}(\mathcal{P})} \cup (T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{Q}'})) \cap (F_{\mathcal{E}(\mathcal{Q})} \cup (T_{\mathcal{E}(\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{P}'}))$ or $t't'' \in (F_{\mathcal{E}(\mathcal{P})} \cup (T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{Q}'})) \cap ((T_{\mathcal{E}(\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{Q}'}) \cup ((T_{\mathcal{E}(\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{Q}'}) \uparrow \mathcal{A}^I_{\mathcal{P}'}))$ or $t't'' \in (F_{\mathcal{E}(\mathcal{Q})} \cup (T_{\mathcal{E}(\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{P}'})) \cap ((T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{P}'}) \cup ((T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{P}'}) \uparrow \mathcal{A}^I_{\mathcal{Q}'}))$ or $t't'' \in ((T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{P}'}) \cup ((T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{P}'}) \uparrow \mathcal{A}^I_{\mathcal{Q}'})) \cap ((T_{\mathcal{E}(\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{Q}'}) \cup ((T_{\mathcal{E}(\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{Q}'}) \uparrow \mathcal{A}^I_{\mathcal{P}'}))$. The first of these implies $t't'' \in F_{\mathcal{E}(\mathcal{P}) \wedge \mathcal{E}(\mathcal{Q})} \cup (T_{\mathcal{E}(\mathcal{P}) \wedge \mathcal{E}(\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{P}' \wedge \mathcal{Q}'})$, while the remaining three imply $t't'' \in T_{\mathcal{E}(\mathcal{P}) \wedge \mathcal{E}(\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{P}' \wedge \mathcal{Q}'}$. Therefore, $t't'' \in F_{\mathcal{E}(\mathcal{P}) \wedge \mathcal{E}(\mathcal{Q})} \cup (T_{\mathcal{E}(\mathcal{P}) \wedge \mathcal{E}(\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{P}' \wedge \mathcal{Q}'})$, which is equivalent to having $t't'' \in F_{\mathcal{E}(\mathcal{P} \wedge \mathcal{Q})} \cup (T_{\mathcal{E}(\mathcal{P} \wedge \mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{P}' \wedge \mathcal{Q}'})$, from which it easily follows that $t \in F_{\mathcal{E}(\mathcal{P} \wedge \mathcal{Q})} \cup (T_{\mathcal{E}(\mathcal{P} \wedge \mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{P}' \wedge \mathcal{Q}'})$ as required. Observable trace containment is similar.

Proof of Lemma 4

Evident from the definition.

Proof of Theorem 3

For the first claim, suppose $t \in F_{\mathcal{E}(\mathcal{P})}$. Then there exists a prefix t' of t and a trace $t'' \in (\mathcal{A}^O_{\mathcal{P}})^*$ such that $t't'' \in F_{\mathcal{P}}$. Now either $t't'' \in \mathcal{A}^*_{\mathcal{P} \vee \mathcal{Q}}$, implying $t't'' \in F_{\mathcal{P} \vee \mathcal{Q}}$ and so $t \in F_{\mathcal{E}(\mathcal{P} \vee \mathcal{Q})}$, or there exists a prefix $t_1 i$ of t' with $t_1 \in \mathcal{A}^*_{\mathcal{P} \vee \mathcal{Q}}$ and $i \in \mathcal{A}^I_{\mathcal{P}} \setminus \mathcal{A}^I_{\mathcal{Q}}$. Consequently, $t_1 \in T_{\mathcal{P} \vee \mathcal{Q}}$ and $t_1 i \in T_{\mathcal{P} \vee \mathcal{Q}} \uparrow \mathcal{A}^I_{\mathcal{P}}$. Hence $t \in T_{\mathcal{P} \vee \mathcal{Q}} \uparrow \mathcal{A}^I_{\mathcal{P}}$ as required. For observable trace containment, suppose $t \in T_{\mathcal{P}}$ Then either $t \in T_{\mathcal{P}} \cap \mathcal{A}^*_{\mathcal{P} \vee \mathcal{Q}}$ or $t \in (T_{\mathcal{P}} \cap \mathcal{A}^*_{\mathcal{P} \vee \mathcal{Q}}) \uparrow \mathcal{A}^I_{\mathcal{P}}$. This means that $t \in T_{\mathcal{P} \vee \mathcal{Q}} \cup (T_{\mathcal{P} \vee \mathcal{Q}} \uparrow \mathcal{A}^I_{\mathcal{P}})$ as required. Hence $\mathcal{P} \sqsubseteq_{imp} \mathcal{P} \vee \mathcal{Q}$. Showing $\mathcal{Q} \sqsubseteq_{imp} \mathcal{P} \vee \mathcal{Q}$ is similar.

For the second claim, suppose $t \in F_{\mathcal{E}(\mathcal{P}\vee\mathcal{Q})}$. Then there exists t' a prefix of t and $t'' \in (\mathcal{A}^O_{\mathcal{P}\vee\mathcal{Q}})^*$ such that $t't'' \in F_{\mathcal{P}\vee\mathcal{Q}}$. Consequently, without loss of generality, $t't'' \in F_{\mathcal{P}} \cap \mathcal{A}^*_{\mathcal{P}\vee\mathcal{Q}}$. From $\mathcal{P} \sqsubseteq_{imp} \mathcal{R}$, it follows that $t't'' \in (F_{\mathcal{E}(\mathcal{R})} \cup (T_{\mathcal{E}(\mathcal{R})} \uparrow \mathcal{A}^I_{\mathcal{P}})) \cap \mathcal{A}^*_{\mathcal{P}\vee\mathcal{Q}}$. Hence $t't'' \in F_{\mathcal{E}(\mathcal{R})} \cup (T_{\mathcal{E}(\mathcal{R})} \uparrow \mathcal{A}^I_{\mathcal{P}\vee\mathcal{Q}})$, meaning $t' \in F_{\mathcal{E}(\mathcal{R})} \cup (T_{\mathcal{E}(\mathcal{R})} \uparrow \mathcal{A}^I_{\mathcal{P}\vee\mathcal{Q}})$ and so $t \in F_{\mathcal{E}(\mathcal{R})} \cup (T_{\mathcal{E}(\mathcal{R})} \uparrow \mathcal{A}^I_{\mathcal{P}\vee\mathcal{Q}})$. For the observable trace $t \in T_{\mathcal{P}\vee\mathcal{Q}}$, it holds without loss of generality that $t \in T_{\mathcal{P}} \cap \mathcal{A}^*_{\mathcal{P}\vee\mathcal{Q}}$. From $\mathcal{P} \sqsubseteq_{imp} \mathcal{R}$ it follows that $t \in (T_{\mathcal{E}(\mathcal{R})} \cup (T_{\mathcal{E}(\mathcal{R})} \uparrow \mathcal{A}^I_{\mathcal{P}})) \cap \mathcal{A}^*_{\mathcal{P}\vee\mathcal{Q}}$, and so $t \in T_{\mathcal{E}(\mathcal{R})} \cup (T_{\mathcal{E}(\mathcal{R})} \uparrow \mathcal{A}^I_{\mathcal{P}\vee\mathcal{Q}})$ as required.

For the third claim, suppose $t \in F_{\mathcal{E}(\mathcal{P}'\vee\mathcal{Q}')}$. Then there exists t' a prefix of t and $t'' \in (\mathcal{A}^O_{\mathcal{P}'\vee\mathcal{Q}'})^*$ such that $t't'' \in F_{\mathcal{P}'\vee\mathcal{Q}'}$. Thus, without loss of generality, $t't'' \in F_{\mathcal{P}'} \cap \mathcal{A}^*_{\mathcal{P}'\vee\mathcal{Q}'}$. From $\mathcal{P}' \sqsubseteq_{imp} \mathcal{P}$, it follows that $t't'' \in (F_{\mathcal{E}(\mathcal{P})} \cup (T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{P}'})) \cap \mathcal{A}^*_{\mathcal{P}'\vee\mathcal{Q}'}$. If $t't'' \in \mathcal{A}^*_{\mathcal{P}\vee\mathcal{Q}}$, then it follows that $t't'' \in F_{\mathcal{E}(\mathcal{P})\vee\mathcal{E}(\mathcal{Q})}$. Consequently, $t't'' \in F_{\mathcal{E}(\mathcal{P}\vee\mathcal{Q})}$, from which it can easily be shown that $t \in F_{\mathcal{E}(\mathcal{P}\vee\mathcal{Q})}$. Instead, if $t't'' \notin \mathcal{A}^*_{\mathcal{P}\vee\mathcal{Q}}$, then there exists a prefix t_1a of t' such that $t_1 \in \mathcal{A}^*_{\mathcal{P}\vee\mathcal{Q}}$ and $a \in \mathcal{A}^I_{\mathcal{P}'\vee\mathcal{Q}'} \setminus \mathcal{A}^I_{\mathcal{P}\vee\mathcal{Q}}$. By the induction hypothesis, $t_1 \in T_{\mathcal{E}(\mathcal{P}\vee\mathcal{Q})}$, and so $t_1a \in T_{\mathcal{E}(\mathcal{P}\vee\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{P}'\vee\mathcal{Q}'}$. From this, it can be seen that $t \in T_{\mathcal{E}(\mathcal{P}\vee\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{P}'\vee\mathcal{Q}'}$. For the observable trace containment, suppose $t \in T_{\mathcal{P}'\vee\mathcal{Q}'}$. Then without loss of generality, we have $t \in T_{\mathcal{P}'} \cap \mathcal{A}^*_{\mathcal{P}'\vee\mathcal{Q}'}$. From $\mathcal{P}' \sqsubseteq_{imp} \mathcal{P}$, it follows that $t \in (T_{\mathcal{E}(\mathcal{P})} \cup (T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{P}'})) \cap \mathcal{A}^*_{\mathcal{P}'\vee\mathcal{Q}'}$. If $t \in \mathcal{A}^*_{\mathcal{P}\vee\mathcal{Q}}$, then $t \in T_{\mathcal{E}(\mathcal{P})\vee\mathcal{E}(\mathcal{Q})}$, giving $t \in T_{\mathcal{E}(\mathcal{P}\vee\mathcal{Q})}$ as required. Instead, if $t \notin \mathcal{A}^*_{\mathcal{P}\vee\mathcal{Q}}$, then there exists a prefix t_1a of t such that $t_1 \in \mathcal{A}^*_{\mathcal{P}\vee\mathcal{Q}}$ and $a \in \mathcal{A}^I_{\mathcal{P}'\vee\mathcal{Q}'} \setminus \mathcal{A}^I_{\mathcal{P}\vee\mathcal{Q}}$. By the induction hypothesis we obtain $t_1 \in T_{\mathcal{E}(\mathcal{P}\vee\mathcal{Q})}$ from which we can deduce $t_1a \in T_{\mathcal{E}(\mathcal{P}\vee\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{P}'\vee\mathcal{Q}'}$, itself implying $t \in T_{\mathcal{E}(\mathcal{P}\vee\mathcal{Q})} \uparrow \mathcal{A}^I_{\mathcal{P}'\vee\mathcal{Q}'}$.

Proof of Theorem 4

First consider the case when $b \in \mathcal{A}^I_{\mathcal{Q}}$. Let $t \in T_{\mathcal{Q}/b}$. Then $t \in T_{\mathcal{Q}} \cap \mathcal{A}^*_{\mathcal{Q}/b}$. By the refinement relation, we have $t \in (T_{\mathcal{P}} \cup (T_{\mathcal{P}} \uparrow \mathcal{A}^I_{\mathcal{Q}})) \cap \mathcal{A}^*_{\mathcal{Q}/b}$. This means $t \in (T_{\mathcal{P}} \cap \mathcal{A}^*_{\mathcal{P}/b}) \cup (T_{\mathcal{P}} \cap \mathcal{A}^*_{\mathcal{P}/b})(\mathcal{A}^I_{\mathcal{Q}/b})(\mathcal{A}_{\mathcal{P}/b} \cup \mathcal{A}^I_{\mathcal{Q}/b})^*$, implying $t \in T_{\mathcal{P}/b} \cup (T_{\mathcal{P}/b} \uparrow \mathcal{A}^I_{\mathcal{Q}/b})$. The inconsistent trace containment can be shown similarly. Note that this case also applies when $b \notin \mathcal{A}_{\mathcal{P}} \cup \mathcal{A}_{\mathcal{Q}}$.

For the case when $b \in \mathcal{A}^O_{\mathcal{P}}$, first show $t \in F_{\mathcal{E}(\mathcal{Q}/b)}$ implies $t \in F_{\mathcal{E}(\mathcal{P}/b)} \cup (T_{\mathcal{E}(\mathcal{P}/b)} \uparrow \mathcal{A}^I_{\mathcal{Q}/b})$. For $t \equiv \epsilon$, note that $\epsilon \in F_{\mathcal{E}(\mathcal{Q}/b)}$ implies $\epsilon \in F_{\mathcal{E}(\mathcal{Q})}$, which by $\mathcal{Q} \sqsubseteq_{imp} \mathcal{P}$ means $\epsilon \in F_{\mathcal{E}(\mathcal{P})}$, and so $\epsilon \in F_{\mathcal{E}(\mathcal{P}/b)}$ as required. The case of $t \equiv t'o$ with $o \in \mathcal{A}^O_{\mathcal{Q}}$ holds by the induction hypothesis and upwards closure of inconsistent traces, given it must hold that $t' \in F_{\mathcal{E}(\mathcal{Q}/b)}$. For $t \equiv t'i$ with $i \in \mathcal{A}^I_{\mathcal{Q}}$, there exists $t'' \in (\mathcal{A}^O_{\mathcal{Q}/b})^*$ such that $t'it'' \in F_{\mathcal{Q}/b}$. Therefore, there exists $t''' \in \mathcal{A}^*_{\mathcal{Q}}$ such that $t'it'' = t''' \upharpoonright \mathcal{A}_{\mathcal{Q}/b}$ with $t''' \in F_{\mathcal{Q}}$. Now

define t_1 such that $t_1 t'' \equiv t'''$. Then $t_1 \in F_{\mathcal{E}(\mathcal{Q})}$, which by $\mathcal{Q} \sqsubseteq_{imp} \mathcal{P}$ implies $t_1 \in F_{\mathcal{E}(\mathcal{P})} \cup (T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{Q}})$. Consequently $t'i \in F_{\mathcal{E}(\mathcal{P}/b)} \cup (T_{\mathcal{E}(\mathcal{P}/b)} \uparrow \mathcal{A}^I_{\mathcal{Q}/b})$, given $t'i \equiv t_1 \upharpoonright \mathcal{A}_{\mathcal{Q}/b}$.

Now to show that $t \in T_{\mathcal{E}(\mathcal{Q}/b)}$ implies $t \in T_{\mathcal{E}(\mathcal{P}/b)} \cup (T_{\mathcal{E}(\mathcal{P}/b)} \uparrow \mathcal{A}^I_{\mathcal{Q}/b})$, it is necessary to just consider $t \in T_{\mathcal{Q}/b}$. If $t \equiv \epsilon$, then $\epsilon \in T_{\mathcal{Q}/b}$ implies $\epsilon \in T_{\mathcal{Q}}$, which by $\mathcal{Q} \sqsubseteq_{imp} \mathcal{P}$ gives $\epsilon \in T_{\mathcal{P}}$, and so $\epsilon \in T_{\mathcal{P}/b}$ as required. For $t \equiv t'i$ with $i \in \mathcal{A}^I_{\mathcal{Q}}$, by the induction hypothesis we have $t' \in T_{\mathcal{E}(\mathcal{P}/b)} \cup (T_{\mathcal{E}(\mathcal{P}/b)} \uparrow \mathcal{A}^I_{\mathcal{Q}/b})$, which by receptiveness of inputs yields $t'i \in T_{\mathcal{E}(\mathcal{P}/b)} \cup (T_{\mathcal{E}(\mathcal{P}/b)} \uparrow \mathcal{A}^I_{\mathcal{Q}/b})$. For $t \equiv t'o$ with $o \in \mathcal{A}^O_{\mathcal{Q}}$, in the difficult case we have $t'o \in T_{\mathcal{Q}/b}$. Consequently, there exists $t''o \in \mathcal{A}^*_{\mathcal{Q}}$ such that $t'o = t''o \upharpoonright \mathcal{A}_{\mathcal{Q}/b}$ and $t''o \in T_{\mathcal{Q}}$. From $\mathcal{Q} \sqsubseteq_{imp} \mathcal{P}$ it follows that $t''o \in T_{\mathcal{E}(\mathcal{P})} \cup (T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{Q}/b})$. If $t''o \in T_{\mathcal{E}(\mathcal{P})}$, then $t''o \in (\mathcal{A}_{\mathcal{P}} \cap \mathcal{A}_{\mathcal{Q}})^*$, meaning $t''o \upharpoonright \mathcal{A}_{\mathcal{Q}/b} = t''o \upharpoonright \mathcal{A}_{\mathcal{P}/b}$. Thus $t'o \in T_{\mathcal{E}(\mathcal{P})/b}$, yielding $t'o \in T_{\mathcal{E}(\mathcal{P}/b)}$. Instead, if $t''o \in T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{Q}/b}$, then a prefix t_1 can be considered up to the first symbol in $\mathcal{A}^I_{\mathcal{Q}/b} \setminus \mathcal{A}^I_{\mathcal{P}}$, such that $t_1 \in T_{\mathcal{E}(\mathcal{P})}$. It then follows that $t_1 \upharpoonright \mathcal{A}_{\mathcal{P}/b} \in T_{\mathcal{E}(\mathcal{P}/b)}$. As the next action is contained in $\mathcal{A}^I_{\mathcal{Q}/b} \setminus \mathcal{A}^I_{\mathcal{P}}$, we have that $t'o \in T_{\mathcal{E}(\mathcal{P}/b)} \uparrow \mathcal{A}^I_{\mathcal{Q}/b}$.

Proof of Theorem 5

For the first claim, if $\mathcal{P} \parallel \mathcal{Q} \sqsubseteq_{imp} \mathcal{R}$, then $\mathcal{A}^O_{\mathcal{P}\parallel\mathcal{Q}} \subseteq \mathcal{A}^O_{\mathcal{R}}$. As $\mathcal{A}^O_{\mathcal{P}\parallel\mathcal{Q}} = \mathcal{A}^O_{\mathcal{P}} \cup \mathcal{A}^O_{\mathcal{Q}}$, it follows that $\mathcal{A}^O_{\mathcal{P}} \subseteq \mathcal{A}^O_{\mathcal{R}}$ i.e., the quotient is defined. Instead, if $\mathcal{R}/\mathcal{P}$ is defined, then $\mathcal{A}^O_{\mathcal{P}} \subseteq \mathcal{A}^O_{\mathcal{R}}$. Taking $\mathcal{Q} = \langle \mathcal{A}^I_{\mathsf{R}}, \emptyset, \emptyset, \emptyset \rangle$ gives $\mathcal{P} \parallel \mathcal{Q} \sqsubseteq_{imp} \mathcal{R}$.

For the second claim, show that a trace $t \in F_{\mathcal{E}(\mathcal{P}\parallel(\mathcal{R}/\mathcal{P}))}$ implies $t \in F_{\mathcal{E}(\mathcal{R})} \cup (T_{\mathcal{E}(\mathcal{R})} \uparrow \mathcal{A}^I_{\mathcal{P}\parallel(\mathcal{R}/\mathcal{P})})$ by induction on the length of the trace t.

- $t \equiv \epsilon$. Then there exists $t' \in (\mathcal{A}^O_{\mathcal{P}\parallel(\mathcal{R}/\mathcal{P})})^* = (\mathcal{A}^O_{\mathcal{R}})^*$, such that $t' \upharpoonright \mathcal{A}_{\mathcal{P}} \in F_{\mathcal{P}}$ and $t' \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}} \in T_{\mathcal{R}/\mathcal{P}}$, or $t' \upharpoonright \mathcal{A}_{\mathcal{P}} \in T_{\mathcal{P}}$ and $t' \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}} \in F_{\mathcal{R}/\mathcal{P}}$. For the former, by definition of $T_{\mathcal{R}/\mathcal{P}}$, it follows that $L(t')$ holds, hence $t' \in F_{\mathcal{E}(\mathcal{R})}$, implying $\epsilon \in F_{\mathcal{E}(\mathcal{R})}$. For the latter, by definition of $F_{\mathcal{R}/\mathcal{P}}$ it follows that $t' \in F_{\mathcal{E}(\mathcal{R})}$, hence $\epsilon \in F_{\mathcal{E}(\mathcal{R})}$.

- $t \equiv t'o$ with $o \in \mathcal{A}^O_{\mathcal{P}\parallel(\mathcal{R}/\mathcal{P})}$. Follows immediately by the induction hypothesis, given that $t' \in F_{\mathcal{E}(\mathcal{P}\parallel(\mathcal{R}/\mathcal{P}))}$.

- $t \equiv t'i$ with $i \in \mathcal{A}^I_{\mathcal{P}\parallel(\mathcal{R}/\mathcal{P})} \cap \mathcal{A}^I_{\mathcal{R}}$. It follows that there exists $t'' \in (\mathcal{A}^O_{\mathcal{R}})^*$ such that $t'it'' \upharpoonright \mathcal{A}_{\mathcal{P}} \in F_{\mathcal{P}}$ and $t'it'' \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}} \in T_{\mathcal{R}/\mathcal{P}}$, or $t'it'' \upharpoonright \mathcal{A}_{\mathcal{P}} \in T_{\mathcal{P}}$ and $t'it'' \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}} \in F_{\mathcal{R}/\mathcal{P}}$. In the case of the former, by the definition of $T_{\mathcal{R}/\mathcal{P}}$, it follows that $L(t'it'')$ holds, so $t'it'' \in F_{\mathcal{E}(\mathcal{R})}$, itself implying $t'i \in F_{\mathcal{E}(\mathcal{R})}$. For the latter case, by the definition of $F_{\mathcal{R}/\mathcal{P}}$ it follows that

$t'it'' \in F_{\mathcal{E}(\mathcal{R})}$, hence $t'i \in F_{\mathcal{E}(\mathcal{R})}$. When $i \in \mathcal{A}^I_{\mathcal{P}||(\mathcal{R}/\mathcal{P})} \setminus \mathcal{A}^I_{\mathcal{R}}$, it must be the case that $i \in \mathcal{A}^I_{\mathcal{P}}$. We therefore obtain by the induction hypothesis on t' that $t'i \in T_{\mathcal{E}(\mathcal{R})} \uparrow \mathcal{A}^I_{\mathcal{P}||(\mathcal{R}/\mathcal{P})}$.

For the second claim, we must also show that $t \in T_{\mathcal{P}||(\mathcal{R}/\mathcal{P})}$ implies $t \in T_{\mathcal{E}(\mathcal{R})} \cup (T_{\mathcal{E}(\mathcal{R})} \uparrow \mathcal{A}^I_{\mathcal{P}||(\mathcal{R}/\mathcal{P})})$ by induction on the length of the trace t.

- $t \equiv \epsilon$. Then $\epsilon \in T_{\mathcal{P}}$ and $\epsilon \in T_{\mathcal{R}/\mathcal{P}}$. By the definition of $T_{\mathcal{R}/\mathcal{P}}$, it follows that $L(\epsilon)$ holds, and so $\epsilon \in T_{\mathcal{E}(\mathcal{R})}$ as required.

- $t \equiv t'o$ with $o \in \mathcal{A}^O_{\mathcal{P}||(\mathcal{R}/\mathcal{P})}$. Then $t'o \in T_{\mathcal{P}||(\mathcal{R}/\mathcal{P})}$ implies $t'o \upharpoonright \mathcal{A}_{\mathcal{P}} \in T_{\mathcal{P}}$ and $t'o \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}} \in T_{\mathcal{R}/\mathcal{P}}$. By the induction hypothesis in the difficult case, we have $t' \in T_{\mathcal{R}}$, and so $t'o \in (\mathcal{A}^O_{\mathcal{R}})^*$. Consequently, from $t'o \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}} \in T_{\mathcal{R}/\mathcal{P}}$, it follows that $L(t'o)$. Now, as $t'o \upharpoonright \mathcal{A}_{\mathcal{P}} \in T_{\mathcal{P}}$, we obtain $t'o \in T_{\mathcal{E}(\mathcal{R})}$ as required.

- $t \equiv t'i$ with $i \in \mathcal{A}^I_{\mathcal{P}||(\mathcal{R}/\mathcal{P})}$. Then by the induction hypothesis on t' and receptiveness of $\mathcal{R}$ the result holds trivially.

For the third claim, we show that $t \in F_{\mathcal{E}(\mathcal{Q})}$ implies $t \in F_{\mathcal{E}(\mathcal{R}/\mathcal{P})}$ by induction on the length of the trace t.

- $t \equiv \epsilon$. Then there exists $t' \in (\mathcal{A}^O_{\mathcal{Q}})^*$ such that $t' \in F_{\mathcal{Q}}$. Consequently, either $\epsilon \notin T_{\mathcal{P}}$, or $t' \upharpoonright \mathcal{A}_{\mathcal{P}} \in T_{\mathcal{P}}$ implying $\epsilon \in F_{\mathcal{E}(\mathcal{P}||\mathcal{Q})}$. For the former, we obtain $\epsilon \in F_{\mathcal{R}/\mathcal{P}}$ as required, while for the latter it must hold that $\epsilon \in F_{\mathcal{E}(\mathcal{R})}$ (since $\mathcal{P} \mid\mid \mathcal{Q} \sqsubseteq_{imp} \mathcal{R}$), which also yields $\epsilon \in F_{\mathcal{R}/\mathcal{P}}$.

- $t \equiv t'o$ with $o \in \mathcal{A}^O_{\mathcal{Q}}$. It follows by the induction hypothesis on t' that $t' \in F_{\mathcal{E}(\mathcal{R}/\mathcal{P})}$. Hence $t'o \in F_{\mathcal{E}(\mathcal{R}/\mathcal{P})}$ as required.

- $t \equiv t'i$ with $i \in \mathcal{A}^I_{\mathcal{Q}}$. It follows by the induction hypothesis in the difficult case that $t'i \in T_{\mathcal{R}/\mathcal{P}}$, but $t'i \notin F_{\mathcal{R}/\mathcal{P}}$. Consequently, there exists $t''i \in \mathcal{A}^*_{\mathcal{R}}$ such that $t''i \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}} = t'i$, for which $L(t''i)$ holds (according to the definition of $T_{\mathcal{R}/\mathcal{P}}$), while $t''i \upharpoonright \mathcal{A}_{\mathcal{P}} \in T_{\mathcal{P}}$ and $t''i \notin F_{\mathcal{E}(\mathcal{R})}$ (since $t'i \notin F_{\mathcal{R}/\mathcal{P}}$). Consequently, $t''i \in F_{\mathcal{E}(\mathcal{P}||\mathcal{Q})}$, but this contradicts $\mathcal{P} \mid\mid \mathcal{Q} \sqsubseteq_{imp} \mathcal{R}$, since $t''i \notin F_{\mathcal{E}(\mathcal{R})}$.

For the third claim we also show that $t \in T_{\mathcal{Q}}$ implies $t \in T_{\mathcal{E}(\mathcal{R}/\mathcal{P})}$ by induction on the length of the trace t.

- $t \equiv \epsilon$. Then if $\epsilon \notin T_{\mathcal{P}}$, we have $\epsilon \in T_{\mathcal{R}/\mathcal{P}}$ by default. Instead, if $\epsilon \in T_{\mathcal{P}}$ and $\epsilon \notin T_{\mathcal{E}(\mathcal{R}/\mathcal{P})}$, then we know $\epsilon \notin T_{\mathcal{R}/\mathcal{P}}$, so there exists $t' \in (\mathcal{A}_{\mathcal{R}} \setminus \mathcal{A}_{\mathcal{R}/\mathcal{P}})^*$ and $t'' \in (\mathcal{A}_{\mathcal{R}} \setminus \mathcal{A}^O_{\mathcal{R}/\mathcal{P}})^*$ such that (i) $t't'' \upharpoonright \mathcal{A}_{\mathcal{P}} \in F_{\mathcal{P}}$ and $t't'' \notin F_{\mathcal{E}(\mathcal{R})}$, or (ii) $t't'' \upharpoonright \mathcal{A}_{\mathcal{P}} \in T_{\mathcal{P}}$ and $t't'' \notin T_{\mathcal{E}(\mathcal{R})}$. Note that $t' \upharpoonright \mathcal{A}_{\mathcal{Q}} \in (\mathcal{A}^I_{\mathcal{Q}})^*$ and $t'' \upharpoonright \mathcal{A}_{\mathcal{Q}} \in (\mathcal{A}^I_{\mathcal{Q}})^*$. Hence $t't'' \upharpoonright \mathcal{A}_{\mathcal{Q}} \in T_{\mathcal{Q}}$, given $\epsilon \in T_{\mathcal{Q}}$. If (i) holds, then we have $t't'' \in F_{\mathcal{P}||\mathcal{Q}}$, but $t't'' \notin F_{\mathcal{E}(\mathcal{R})}$, which contradicts $\mathcal{P} \mid\mid \mathcal{Q} \sqsubseteq_{imp} \mathcal{R}$ (given $t't'' \in \mathcal{A}^*_{\mathcal{R}}$). Instead, if (ii) holds, we have $t't'' \in T_{\mathcal{P}||\mathcal{Q}}$, but $t't'' \notin T_{\mathcal{E}(\mathcal{R})}$, which again contradicts $\mathcal{P} \mid\mid \mathcal{Q} \sqsubseteq_{imp} \mathcal{R}$.

- $t \equiv t_1 o$ with $o \in \mathcal{A}^O_{\mathcal{Q}}$. Suppose $t_1 o \notin T_{\mathcal{R}/\mathcal{P}}$. By the induction hypothesis it holds that $t_1 \in T_{\mathcal{R}/\mathcal{P}}$. Take a trace $t_2 o \in \mathcal{A}^*_{\mathcal{R}}$ such that $t_2 o \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}} = t_1 o$, and traces $t' \in (\mathcal{A}_{\mathcal{R}} \setminus \mathcal{A}_{\mathcal{R}/\mathcal{P}})^*$ and $t'' \upharpoonright (\mathcal{A}_{\mathcal{R}} \setminus \mathcal{A}^O_{\mathcal{R}/\mathcal{P}})^*$ such that $L(t_2 o t' t'')$ does not hold. By the fact that $\mathcal{A}^I_{\mathcal{Q}} = \mathcal{A}^I_{\mathcal{R}/\mathcal{P}}$, we know that $t_2 o \upharpoonright \mathcal{A}_{\mathcal{Q}} = t_1 o$. As $t't'' \upharpoonright \mathcal{A}_{\mathcal{Q}} \in (\mathcal{A}^I_{\mathcal{Q}})^*$, by the same reasoning as in the previous case we derive $\mathcal{P} \mid\mid \mathcal{Q} \not\sqsubseteq_{imp} \mathcal{R}$ when $t_1 o \notin T_{\mathcal{R}/\mathcal{P}}$.

- $t \equiv t' i$ with $i \in \mathcal{A}^I_{\mathcal{Q}}$. The result holds trivially by the induction hypothesis on t' and receptiveness of components.

Proof of Theorem 6

For the first property, note that definedness of $\mathcal{Q}/\mathcal{R}$ implies definedness of $\mathcal{P}/\mathcal{R}$. Consequently, $\mathcal{R} \mid\mid (\mathcal{Q}/\mathcal{R}) \sqsubseteq_{imp} \mathcal{Q} \sqsubseteq_{imp} \mathcal{P}$. The constraint $\mathcal{A}^I_{\mathcal{R}} \cap \mathcal{A}^O_{\mathcal{P}} = \emptyset$ ensures that transitivity holds, from which we derive $\mathcal{R} \mid\mid (\mathcal{Q}/\mathcal{R}) \sqsubseteq_{imp} \mathcal{P}$. Hence $\mathcal{Q}/\mathcal{R} \sqsubseteq_{imp} \mathcal{P}/\mathcal{R}$ by Theorem 5.

For the second property, definedness of $\mathcal{R}/\mathcal{P}$ implies definedness of $\mathcal{R}/\mathcal{Q}$. From $\mathcal{Q} \sqsubseteq_{imp} \mathcal{P}$, we obtain $\mathcal{Q} \mid\mid (\mathcal{R}/\mathcal{P}) \sqsubseteq_{imp} \mathcal{P} \mid\mid (\mathcal{R}/\mathcal{P})$ by Theorem 1 (the conditions of which are satisfied by $(\mathcal{A}^I_{\mathcal{Q}} \setminus \mathcal{A}^I_{\mathcal{P}}) \cap \mathcal{A}_{\mathcal{R}} = \emptyset$). By Theorem 5 we know $\mathcal{P} \mid\mid (\mathcal{R}/\mathcal{P}) \sqsubseteq_{imp} \mathcal{R}$, and so we obtain $\mathcal{Q} \mid\mid (\mathcal{R}/\mathcal{P}) \sqsubseteq_{imp} \mathcal{R}$ by transitivity (Lemma 1), given that $(\mathcal{A}^I_{\mathcal{Q}} \setminus \mathcal{A}^I_{\mathcal{P}}) \cap \mathcal{A}_{\mathcal{R}} = \emptyset$ ensures that action types are not mixed. Finally, by Theorem 5, it follows that $\mathcal{R}/\mathcal{Q}$ is the minimal solution to $\mathcal{Q} \mid\mid X \sqsubseteq_{imp} \mathcal{R}$, and so $\mathcal{R}/\mathcal{P} \sqsubseteq_{imp} \mathcal{R}/\mathcal{Q}$.

Proof of Theorem 7

First suppose $\mathcal{Q} \sqsubseteq_{imp} \mathcal{P}$. Then, from the constraint on the interface for $\mathcal{R}$, we have that $\mathcal{Q} \mid\mid \mathcal{R} \sqsubseteq_{imp} \mathcal{P} \mid\mid \mathcal{R}$ by Theorem 1, since the constraints for that Theorem are satisfied. Hence $\mathcal{Q} \mid\mid \mathcal{R} \sqsubseteq^F_{imp} \mathcal{P} \mid\mid \mathcal{R}$ as required.

For the other direction, suppose that $\mathcal{Q} \not\sqsubseteq_{imp} \mathcal{P}$. Then there exists a smallest t such that $t \in F_{\mathcal{E}(\mathcal{Q})}$ and $t \notin F_{\mathcal{E}(\mathcal{P})} \cup (T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{Q}})$, or $t \in T_{\mathcal{E}(\mathcal{Q})}$ and $t \notin T_{\mathcal{E}(\mathcal{P})} \cup (T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{Q}})$.

In the case of the former, it follows (by the minimality of t) that $t \in F_{\mathcal{Q}}$. By the constraints on the alphabets, it follows that there is a maximal prefix t' of t such that $t' \in \mathcal{A}^*_{\mathcal{R}}$, and, moreover, this is the same maximal prefix such that $t' \in \mathcal{A}^*_{\mathcal{P}}$. If t' is a strict prefix of t, then by minimality of t we have $t' \in T_{\mathcal{E}(\mathcal{P})}$ and $t \in T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{Q}}$, since the next action after t' must be in $\mathcal{A}^I_{\mathcal{Q}} \setminus \mathcal{A}_{\mathcal{P}}$, but this is contradictory. Therefore, $t' = t$, which means we can construct an $\mathcal{R}$ such that $F_{\mathcal{R}} = \emptyset$ and $T_{\mathcal{R}}$ is the smallest set containing t that makes $\mathcal{R}$ a component. Now $t \in T_{\mathcal{R}}$ implies $t \in F_{\mathcal{Q}||\mathcal{R}}$, and so $\epsilon \in F_{\mathcal{E}(\mathcal{Q}||\mathcal{R})}$ given $t \in (\mathcal{A}^O_{\mathcal{Q}||\mathcal{R}})^*$. However, as $t \notin F_{\mathcal{E}(\mathcal{P})}$, it follows that $t \notin F_{\mathcal{E}(\mathcal{P}||\mathcal{R})}$, hence $\epsilon \notin F_{\mathcal{E}(\mathcal{P}||\mathcal{R})}$, which means $\mathcal{Q} \,||\, \mathcal{R} \not\sqsubseteq^F_{imp} \mathcal{P} \,||\, \mathcal{R}$ as required.

In the case of the latter, it is sufficient to consider $t \in T_{\mathcal{Q}}$. Again, there is a maximal prefix t' of t such that $t' \in \mathcal{A}^*_{\mathcal{R}}$, and, moreover, this is the same maximal prefix contained in $\mathcal{A}^*_{\mathcal{P}}$. If t' is a strict prefix, then the next symbol after t' is an element of $\mathcal{A}^I_{\mathcal{Q}} \setminus \mathcal{A}_{\mathcal{P}}$. Hence, by minimality of t, it follows that $t \in T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{Q}}$, but this is contradictory. Therefore, we know $t' = t$, so we construct an $\mathcal{R}$ such that $F_{\mathcal{R}} = \{t'' \in \mathcal{A}^*_{\mathcal{R}} : t \text{ is a prefix of } t''\}$ and $T_{\mathcal{R}}$ is the least set making $\mathcal{R}$ a component. Therefore $t \in F_{\mathcal{Q}||\mathcal{R}}$, which yields $\epsilon \in F_{\mathcal{E}(\mathcal{Q}||\mathcal{R})}$ given $t \in (\mathcal{A}^O_{\mathcal{Q}||\mathcal{R}})^*$. However, as $t \notin T_{\mathcal{E}(\mathcal{P})}$, it follows that $t \notin T_{\mathcal{E}(\mathcal{P}||\mathcal{R})}$, hence $\epsilon \notin T_{\mathcal{E}(\mathcal{P}||\mathcal{R})}$. From this we obtain $\epsilon \notin F_{\mathcal{E}(\mathcal{P}||\mathcal{R})}$, so $\mathcal{Q} \,||\, \mathcal{R} \not\sqsubseteq^F_{imp} \mathcal{P} \,||\, \mathcal{R}$ as required.

Proof of Corollary 1

Note that, under $\equiv_{imp}$, none of the alphabet constraints (other than those for composability) are required for the compositionality results to hold in Theorems 1, 2, 3, 4 and 6. Consequently, $\equiv_{imp}$ is a congruence for all of the compositional operators. Taking this along with Theorem 7 shows that $\equiv_{imp}$ is the coarsest such equivalence with respect to observational equivalence of inconsistency.

Proof of Lemma 5

Follows by the exact same reasoning as in Lemma 1.

Proof of Theorem 8

By Theorem 1, we know that the T and F-set containments hold. In the difficult case, suppose $t \in D_{\mathcal{P}'||\mathcal{Q}'} \setminus F_{\mathcal{E}(\mathcal{P}'||\mathcal{Q}')}$. Then, without loss of

generality, we know $t \upharpoonright \mathcal{A}_{\mathcal{P}'} \in D_{\mathcal{P}'}$ and $t \upharpoonright \mathcal{A}_{\mathcal{Q}'} \in T_{\mathcal{Q}'}$. By the alphabet constraints (as elaborated in Theorem 1) it follows that $t \upharpoonright \mathcal{A}_{\mathcal{P}'} = t \upharpoonright \mathcal{A}_{\mathcal{P}}$ and $t \upharpoonright \mathcal{A}_{\mathcal{Q}'} = t \upharpoonright \mathcal{A}_{\mathcal{Q}}$. Hence, from $\mathcal{P}' \sqsubseteq^l_{imp} \mathcal{P}$ and $\mathcal{Q}' \sqsubseteq^l_{imp} \mathcal{Q}$, it follows that $t \upharpoonright \mathcal{A}_{\mathcal{P}} \in D_{\mathcal{E}(\mathcal{P})}$ and $t \upharpoonright \mathcal{A}_{\mathcal{Q}} \in T_{\mathcal{E}(\mathcal{Q})}$, yielding $t \in D_{\mathcal{E}(\mathcal{P}||\mathcal{Q})}$ as required. The quiescent trace containment is similar.

Proof of Theorem 9

For the first claim, we just need to show divergent and quiescent trace containment, which is a straightforward modification to Theorem 2. The proof for observable and inconsistent trace containment remains unchanged.

For the second claim, under the assumption that $T_{\mathcal{E}(\mathcal{R})} \cap Err = \emptyset$, the observable and inconsistent trace containments remain as in Theorem 2, and the divergent and inconsistent trace containments are a straightforward extension. We therefore need to show that $T_{\mathcal{E}(\mathcal{R})} \cap Err = \emptyset$, by proving that $T_{\mathcal{E}(\mathcal{R})} \cap X_i = \emptyset$ for each $i \in \mathbb{N}$, where X_i is the i-th approximation of Err defined as a fixed point. Clearly the result holds for $i = 0$ (since $X_0 = \emptyset$), so show that it holds for $i = k + 1$ given that it holds for $i = k$. Suppose $t \in T_{\mathcal{E}(\mathcal{R})} \cap X_{k+1}$. Then by Theorem 2 we know $t \in T_{\mathcal{E}(\mathcal{P}\wedge\mathcal{Q})} \cap X_{k+1}$ (since $Err \subseteq \mathcal{A}^*_{\mathcal{P}\wedge\mathcal{Q}}$), which means that there exists $t' \in (\mathcal{A}^I_{\mathcal{P}\wedge\mathcal{Q}})^*$ such that $tt' \notin K_{\mathcal{E}(\mathcal{P}\wedge\mathcal{Q})}$ and $\forall o \in \mathcal{A}^O_{\mathcal{P}\wedge\mathcal{Q}} \cdot tt'o \notin T_{\mathcal{E}(\mathcal{P}\wedge\mathcal{Q})} \setminus X_k$. From $tt' \in T_{\mathcal{E}(\mathcal{P}\wedge\mathcal{Q})} \cap \overline{K_{\mathcal{E}(\mathcal{P}\wedge\mathcal{Q})}}$, we know that $tt' \in T_{\mathcal{E}(\mathcal{R})} \cap \overline{K_{\mathcal{E}(\mathcal{R})}}$. Thus, there exists $o' \in \mathcal{A}^O_{\mathcal{R}}$ such that $tt'o' \in T_{\mathcal{E}(\mathcal{R})}$, which means that $tt'o' \in T_{\mathcal{E}(\mathcal{P}\wedge\mathcal{Q})}$. Hence $tt'o' \in X_k$, but this implies $tt'o' \notin T_{\mathcal{E}(\mathcal{R})}$, which is contradictory.

For the third claim, under the assumption that $(T_{\mathcal{E}(\mathcal{P}'\wedge\mathcal{Q}')} \setminus Err_{\mathcal{P}'\wedge\mathcal{Q}'}) \cap Err_{\mathcal{P}\wedge\mathcal{Q}} = \emptyset$, the observable and inconsistent trace containments follow as before in Theorem 2, and the divergent and quiescent containments can be shown similarly. To show that $(T_{\mathcal{E}(\mathcal{P}'\wedge\mathcal{Q}')} \setminus Err_{\mathcal{P}'\wedge\mathcal{Q}'}) \cap Err_{\mathcal{P}\wedge\mathcal{Q}} = \emptyset$, $Err_{\mathcal{P}\wedge\mathcal{Q}}$ can be approximated as for the previous claim. The proof is then a straightforward modification, having noted that $t \in T_{\mathcal{E}(\mathcal{P}'\wedge\mathcal{Q}')} \setminus Err_{\mathcal{P}'\wedge\mathcal{Q}'}$ and $t' \in (\mathcal{A}^I_{\mathcal{P}\wedge\mathcal{Q}})^*$ implies $tt' \in T_{\mathcal{E}(\mathcal{P}'\wedge\mathcal{Q}')} \setminus Err_{\mathcal{P}'\wedge\mathcal{Q}'}$.

Proof of Theorem 10

A straightforward extension of Theorem 3.

Proof of Theorem 11

The divergent and quiescent trace containments follow by the same reasoning as in Theorem 4 when $b \in \mathcal{A}^I_{\mathcal{Q}}$ or $b \notin \mathcal{A}_{\mathcal{P}} \cup \mathcal{A}_{\mathcal{Q}}$, and the observable and inconsistent containments are entirely unchanged.

When $b \in \mathcal{A}^O_{\mathcal{P}}$, suppose that $t \in D_{\mathcal{Q}/b}$. Then there exists $t' \in T_{\mathcal{Q}}$ such that $t' \upharpoonright \mathcal{A}_{\mathcal{Q}/b} = t$ and $t' \in D_{\mathcal{Q}}$ or $\forall i \in \mathbb{N} \cdot t'b^i \in T_{\mathcal{Q}}$. In the case of the former, it follows that $t' \in D_{\mathcal{E}(\mathcal{P})} \cup (T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{Q}})$. Hence $t \in D_{\mathcal{E}(\mathcal{P}/b)} \cup (T_{\mathcal{E}(\mathcal{P}/b)} \uparrow \mathcal{A}^I_{\mathcal{Q}})$ as required. In the case of the latter, $t' \in T_{\mathcal{Q}}$ implies $t' \in T_{\mathcal{E}(\mathcal{P})} \cup (T_{\mathcal{E}(\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{Q}})$. The difficult case is when $t' \in T_{\mathcal{E}(\mathcal{P})}$, from which we can deduce $t'b^i \in T_{\mathcal{E}(\mathcal{P})}$ for each $i \in \mathbb{N}$. Hence $t \in D_{\mathcal{E}(\mathcal{P}/b)}$. Quiescent trace containment is similar.

Proof of Theorem 12

The reasoning for the first claim is identical to that in Theorem 5. For the second claim, inconsistent trace and observable trace containment follows by Theorem 5, having replaced $F_{\mathcal{R}/\mathcal{P}}$ with $F_{\mathcal{R}/\mathcal{P}} \setminus Err$ and $T_{\mathcal{R}/\mathcal{P}}$ with $T_{\mathcal{R}/\mathcal{P}} \setminus Err$. For the divergent traces, let $t \in D_{\mathcal{P}||_l(\mathcal{R}/\mathcal{P})}$. Then either $t \upharpoonright \mathcal{A}_{\mathcal{P}} \in D_{\mathcal{P}}$ and $t \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}} \in T_{\mathcal{R}/\mathcal{P}} \setminus Err$, or $t \upharpoonright \mathcal{A}_{\mathcal{P}} \in T_{\mathcal{P}}$ and $t \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}} \in D_{\mathcal{R}/\mathcal{P}} \setminus Err$. Supposing the former, if $t \notin \mathcal{A}^*_{\mathcal{R}}$, then there is a prefix of t contained within $T_{\mathcal{E}(\mathcal{R})} \uparrow \mathcal{A}^I_{\mathcal{P}}$, which is extension closed. Instead, if $t \in \mathcal{A}^*_{\mathcal{R}}$, then $t \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}} \notin Err$ implies $t \notin Y$. Consequently, $t \notin \overline{D_{\mathcal{E}(\mathcal{R})}} \cap (D_{\mathcal{P}} \Uparrow \mathcal{A}_{\mathcal{R}})$, which implies $t \in D_{\mathcal{R}}$ as required. Now, for the latter case, suppose $t \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}} \in D_{\mathcal{R}/\mathcal{P}} \setminus Err$, then by the definition of $D_{\mathcal{R}/\mathcal{P}}$ it follows that if $t \in \mathcal{A}^*_{\mathcal{R}}$, then $t \in D_{\mathcal{E}(\mathcal{R})}$ as required. If $t \notin \mathcal{A}^*_{\mathcal{R}}$, then it follows $t \in T_{\mathcal{E}(\mathcal{R})} \uparrow \mathcal{A}^I_{\mathcal{P}}$. To show quiescent trace containment, suppose $t \in K_{\mathcal{P}||_l(\mathcal{R}/_l\mathcal{P})}$. Then $t \upharpoonright \mathcal{A}_{\mathcal{P}} \in K_{\mathcal{P}}$ and $t \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}} \in K_{\mathcal{R}/\mathcal{P}} \setminus Err$. In the difficult case, suppose $t \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}} \notin F_{\mathcal{R}/\mathcal{P}}$, then $t \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}} \in T_{\mathcal{R}/\mathcal{P}}$ and $\nexists o \in \mathcal{A}^O_{\mathcal{R}/\mathcal{P}} \cdot to \in T_{\mathcal{R}/\mathcal{P}} \setminus Err$. Consequently, as $t \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}} \notin Err$, it follows that $t \notin Y$. Hence it must be the case that $t \in K_{\mathcal{E}(\mathcal{R})}$ as required when $t \in \mathcal{A}^*_{\mathcal{R}}$. If $t \notin \mathcal{A}^*_{\mathcal{R}}$, then it is easy to show $t \in T_{\mathcal{E}(\mathcal{R})} \uparrow \mathcal{A}^I_{\mathcal{P}}$.

For the third claim, under the assumption that $T_{\mathcal{E}(\mathcal{Q})} \cap Err = \emptyset$, inconsistent and observable trace containment is as presented in Theorem 5, while divergent and quiescent trace containment is very similar. To show that $T_{\mathcal{E}(\mathcal{Q})} \cap Err = \emptyset$, we show $T_{\mathcal{E}(\mathcal{Q})} \cap (Y_i \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}}) = \emptyset$ for each $i \in \mathbb{N}$, where Y_i is the i-th iteration of finding the fixed point defining Y. When $i = 0$, $Y_i = \emptyset$, so the result trivially holds. Now suppose $i = k + 1$, and assume that the result holds for $i = k$. If $t \in T_{\mathcal{E}(\mathcal{Q})} \cap (Y_{k+1} \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}})$, then we know $t \in T_{\mathcal{E}(\mathcal{R}/\mathcal{P})} \cap (Y_{k+1} \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}})$, since $t \in Y_{k+1} \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}}$ implies $t \in \mathcal{A}^*_{\mathcal{R}/\mathcal{P}}$ and $T_{\mathcal{E}(\mathcal{Q})} \subseteq T_{\mathcal{E}(\mathcal{R}/\mathcal{P})} \cup T_{\mathcal{E}(\mathcal{R}/\mathcal{P})} \uparrow \mathcal{A}^I_{\mathcal{Q}}$. Consequently, there exists $t' \in \mathcal{A}^*_{\mathcal{R}}$ such that (i) $t' \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}} = t$ and $t'' \in (\mathcal{A}_{\mathcal{R}} \setminus \mathcal{A}^O_{\mathcal{R}/\mathcal{P}})^*$ such that $t't'' \in \overline{D_{\mathcal{E}(\mathcal{R})}} \cap (D_{\mathcal{P}} \Uparrow \mathcal{A}_{\mathcal{R}})$, or (ii) $t't'' \in \overline{K_{\mathcal{E}(\mathcal{R})}} \cap (K_{\mathcal{P}} \Uparrow \mathcal{A}_{\mathcal{R}})$ such that $\nexists o \in \mathcal{A}^O_{\mathcal{R}/\mathcal{P}} \cdot t't''o \in (T_{\mathcal{R}/\mathcal{P}} \Uparrow \mathcal{A}_{\mathcal{R}}) \setminus Y_k$. Note that $t't'' \upharpoonright \mathcal{A}_{\mathcal{Q}} = t't'' \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}} \in T_{\mathcal{E}(\mathcal{Q})}$. If (i) holds, then it follows $t't'' \in D_{\mathcal{E}(\mathcal{P}||_l\mathcal{Q})}$, hence $\mathcal{P} \,||_l\, \mathcal{Q} \not\sqsubseteq^l_{imp} \mathcal{R}$, which is contradictory. If instead (ii)

holds, then, from knowing $t't'' \in T_{\mathcal{E}(\mathcal{Q})}$ and $\mathcal{P} \mid\mid_l \mathcal{Q} \sqsubseteq^l_{imp} \mathcal{R}$, it follows that $t't'' \notin K_{\mathcal{E}(\mathcal{Q})}$. Hence, there exists $o' \in \mathcal{A}^O_{\mathcal{Q}}$ such that $t't''o' \in T_{\mathcal{E}(\mathcal{Q})}$, which implies $t't''o' \in T_{\mathcal{E}(\mathcal{R}/\mathcal{P})}$. It therefore follows that $t't''o' \in Y_k$ so that $t't''o' \in T_{\mathcal{R}/\mathcal{P}} \setminus Y_k$ holds. But by the induction hypothesis, this allows us to conclude that $t't''o' \notin T_{\mathcal{E}(\mathcal{Q})}$, which is contradictory. Thus $T_{\mathcal{E}(\mathcal{Q})} \cap (Y_{k+1} \upharpoonright \mathcal{A}_{\mathcal{R}/\mathcal{P}}) = \emptyset$ and so $T_{\mathcal{E}(\mathcal{Q})} \cap Err = \emptyset$.

Proof of Theorem 13

The proof is the same as in Theorem 6 when using Theorems 8 and 12 in place of Theorems 1 and 5, and Lemma 5 in place of Lemma 1.

Proof of Theorem 14

Trivial, as the trace-based definition of parallel composition interleaves on independent actions and synchronises on common actions. This is precisely captured by the operational definition.

Proof of Theorem 15

Showing $[\![\mathsf{P} \wedge \mathsf{Q}]\!] = [\![\mathsf{P}]\!] \wedge [\![\mathsf{Q}]\!]$ is trivial, since if $t \in T_{[\![\mathsf{P}\wedge\mathsf{Q}]\!]}$, then $s^0_{\mathsf{P}} \wedge s^0_{\mathsf{Q}} \stackrel{t}{\Longrightarrow}_{\mathsf{P}\wedge\mathsf{Q}} p \wedge q$. If $s^0_{\mathsf{P}} \stackrel{t}{\Longrightarrow}_{\mathsf{P}} p$, then $t \in T_{[\![\mathsf{P}]\!]}$, while if $s^0_{\mathsf{P}} \stackrel{t}{\not\Longrightarrow}_{\mathsf{P}} p$, then $t \in T_{[\![\mathsf{P}]\!]} \uparrow \mathcal{A}^I_{\mathsf{Q}}$. Similarly for Q. Either way, $t \in T_{[\![\mathsf{P}]\!]\wedge[\![\mathsf{Q}]\!]}$. The other direction is similar, as is the inconsistent trace containment.

To show that $[\![\mathsf{P} \wedge_l \mathsf{Q}]\!]^l = [\![\mathsf{P}]\!]^l \wedge_l [\![\mathsf{Q}]\!]^l$, it is sufficient to prove that $t \in T_{[\![\mathsf{P}\wedge\mathsf{Q}]\!]}$ implies: $t \in Err$ iff $s^0_{\mathsf{P}} \wedge s^0_{\mathsf{Q}} \stackrel{t}{\Longrightarrow}_{\mathsf{P}\wedge\mathsf{Q}} p \wedge q$ implies $p \wedge q \in F$. This can be demonstrated in a straightforward manner using an inductive argument by approximating Err and F, which are both obtained as fixed points.

Proof of Theorem 16

Obvious given the definition of disjunction in both the substitutive and progress-sensitive trace-based frameworks.

Proof of Theorem 17

Trivial given the trace-based definition of hiding.

Proof of Theorem 18

First show that $t \in T_{[\![\mathsf{R}/\mathsf{P}]\!]} \iff t \in T_{[\![\mathsf{R}]\!]/[\![\mathsf{P}]\!]}$ and $t \in F_{[\![\mathsf{R}/\mathsf{P}]\!]} \iff t \in F_{[\![\mathsf{R}]\!]/[\![\mathsf{P}]\!]}$ by induction on the length of the trace t.

Case $t \equiv \epsilon$. Suppose that $\epsilon \in F_{[\![\mathsf{R}]\!]/[\![\mathsf{P}]\!]}$. Then by Definition 9, $\epsilon \in F_{\mathcal{E}([\![\mathsf{R}]\!])}$ or $\epsilon \notin T_{[\![\mathsf{P}]\!]}$. If the former holds, then $s^0_{\mathsf{R}} = \bot_{\mathcal{E}(\mathsf{R})}$, hence $s^0_{\mathsf{R}}/s^0_{\mathsf{P}} = \bot_{\mathsf{R}/\mathsf{P}}$, meaning $\epsilon \in F_{[\![\mathsf{R}/\mathsf{P}]\!]}$. If instead $\epsilon \notin T_{[\![\mathsf{P}]\!]}$, then s^0_{P} is not defined, so $s^0_{\mathsf{R}/\mathsf{P}} = \bot_{\mathsf{R}/\mathsf{P}}$, meaning $\epsilon \in F_{[\![\mathsf{R}/\mathsf{P}]\!]}$.

Now suppose that $\epsilon \in F_{[\![\mathsf{R}/\mathsf{P}]\!]}$. Then $s^0_{\mathsf{R}/\mathsf{P}} = \bot_{\mathsf{R}/\mathsf{P}}$, so P is unrealisable or $s^0_{\mathsf{R}} = \bot_{\mathcal{E}(\mathsf{R})}$. If the former holds, then $\epsilon \notin T_{[\![\mathsf{P}]\!]}$, hence $\epsilon \in F_{[\![\mathsf{R}]\!]/[\![\mathsf{P}]\!]}$. If instead $s^0_{\mathsf{R}} = \bot_{\mathcal{E}(\mathsf{R})}$, then $\epsilon \in F_{\mathcal{E}([\![\mathsf{R}]\!])}$, hence $\epsilon \in F_{[\![\mathsf{R}]\!]/[\![\mathsf{P}]\!]}$.

Suppose that $\epsilon \in T_{[\![\mathsf{R}]\!]/[\![\mathsf{P}]\!]}$. Then for all $t' \in (\mathcal{A}_{\mathsf{R}} \setminus \mathcal{A}^O_{\mathsf{R}/\mathsf{P}})^*$, $L(t')$ holds. So $s^0_{\mathsf{R}/\mathsf{P}}$ is defined and $s^0_{\mathsf{R}/\mathsf{P}} \stackrel{t'}{\Longrightarrow}_{\mathsf{R}/\mathsf{P}} s_{\mathsf{R}}/s_{\mathsf{P}}$ implies $s_{\mathsf{R}}/s_{\mathsf{P}} \notin F$. Hence $\epsilon \in T_{[\![\mathsf{R}/\mathsf{P}]\!]}$.

Now suppose that $\epsilon \in T_{[\![\mathsf{R}/\mathsf{P}]\!]}$. Then for all $t' \in (\mathcal{A}_{\mathsf{R}} \backslash \mathcal{A}^O_{\mathsf{R}/\mathsf{P}})^*$, if $s^0_{\mathsf{R}}/s^0_{\mathsf{P}} \stackrel{t'}{\Longrightarrow}_{\mathsf{R}/\mathsf{P}} s_{\mathsf{R}}/s_{\mathsf{P}}$, then $s_{\mathsf{R}}/s_{\mathsf{P}} \notin F$. Hence $t' \upharpoonright \mathcal{A}_{\mathsf{P}} \notin F_{[\![\mathsf{P}]\!]}$ or $t' \in F_{\mathcal{E}(\mathsf{R})}$ since $s_{\mathsf{R}}/s_{\mathsf{P}} \notin F$, and moreover, $t' \in T_{\mathcal{E}(\mathsf{R})}$ as $s^0_{\mathsf{R}} \stackrel{t'}{\Longrightarrow}_{\mathsf{R}} s_{\mathsf{R}}$. Hence $L(t')$ holds. If $s^0_{\mathsf{R}}/s^0_{\mathsf{P}} \stackrel{t'}{\not\Longrightarrow}_{\mathsf{R}/\mathsf{P}}$, then it follows that $s^0_{\mathsf{P}} \stackrel{t'\downarrow\mathcal{A}_{\mathsf{P}}}{\not\Longrightarrow}_{\mathsf{P}} s_{\mathsf{P}}$, since if $s^0_{\mathsf{P}} \stackrel{t'\upharpoonright\mathcal{A}_{\mathsf{P}}}{\Longrightarrow}_{\mathsf{P}} s_{\mathsf{P}}$ and $s^0_{\mathsf{R}} \stackrel{t'}{\not\Longrightarrow}_{\mathsf{R}} s_{\mathsf{R}}$ then it must be because P makes an output move that R cannot match. But then the previous composite state would be in F, which is contradictory. Hence $\epsilon \in T_{[\![\mathsf{R}]\!]/[\![\mathsf{P}]\!]}$.

Case $t \equiv t'o$ with $o \in \mathcal{A}^O_{\mathsf{R}/\mathsf{P}}$. Suppose that $t'o \in F_{[\![\mathsf{R}]\!]/[\![\mathsf{P}]\!]}$. Then $t' \in F_{[\![\mathsf{R}]\!]/[\![\mathsf{P}]\!]}$, so by the induction hypothesis we derive $t' \in F_{[\![\mathsf{R}/\mathsf{P}]\!]}$. Therefore, $s^0_{\mathsf{R}/\mathsf{P}} \stackrel{t'}{\Longrightarrow}_{\mathsf{R}/\mathsf{P}} \bot_{\mathsf{R}/\mathsf{P}}$ and so $s^0_{\mathsf{R}/\mathsf{P}} \stackrel{t'o}{\Longrightarrow}_{\mathsf{R}/\mathsf{P}} \bot_{\mathsf{R}/\mathsf{P}}$. Thus, $t'o \in F_{[\![\mathsf{R}/\mathsf{P}]\!]}$.

Now suppose that $t'o \in F_{[\![\mathsf{R}/\mathsf{P}]\!]}$. Then $s^0_{\mathsf{R}/\mathsf{P}} \stackrel{t'o}{\Longrightarrow}_{\mathsf{R}/\mathsf{P}} \bot_{\mathsf{R}/\mathsf{P}}$. By the definition of $\bot_{\mathsf{R}/\mathsf{P}}$ (defined in terms of $\bot_{\mathcal{E}(\mathsf{R})}$), it follows that $s^0_{\mathsf{R}/\mathsf{P}} \stackrel{t'}{\Longrightarrow}_{\mathsf{R}/\mathsf{P}} \bot_{\mathsf{R}/\mathsf{P}}$, and so $t' \in F_{[\![\mathsf{R}/\mathsf{P}]\!]}$. By the induction hypothesis, it follows that $t' \in F_{[\![\mathsf{R}]\!]/[\![\mathsf{P}]\!]}$. Hence, $t'o \in F_{[\![\mathsf{R}]\!]/[\![\mathsf{P}]\!]}$.

Now suppose that $t'o \in T_{[\![\mathsf{R}]\!]/[\![\mathsf{P}]\!]}$. Then by the induction hypothesis we know that $t' \in T_{[\![\mathsf{R}/\mathsf{P}]\!]}$. Moreover, for all $t'' \in (\mathcal{A}_{\mathsf{R}} \setminus \mathcal{A}^O_{\mathsf{R}/\mathsf{P}})^*$ it follows that $L(t'ot'')$ holds. So, if $s^0_{\mathsf{R}}/s^0_{\mathsf{P}} \stackrel{t'ot''}{\Longrightarrow}_{\mathsf{R}/\mathsf{P}} s_{\mathsf{R}}/s_{\mathsf{P}}$, then certainly $s_{\mathsf{R}}/s_{\mathsf{P}} \notin F$. Furthermore, $s^0_{\mathsf{R}}/s^0_{\mathsf{P}} \stackrel{t'o}{\Longrightarrow}_{\mathsf{R}/\mathsf{P}} s'_{\mathsf{R}}/s'_{\mathsf{P}}$ for some $s'_{\mathsf{R}}/s'_{\mathsf{P}}$, since $s^0_{\mathsf{P}} \stackrel{t'}{\Longrightarrow}_{\mathsf{P}} s''_{\mathsf{P}}$ for some s''_{P} as $o \notin \mathcal{A}_{\mathsf{P}}$ or $o \in \mathcal{A}^I_{\mathsf{P}}$.

Finally, suppose that $t'o \in T_{[\![\mathsf{R}/\mathsf{P}]\!]}$. Then by the induction hypothesis, we know that $t' \in T_{[\![\mathsf{R}]\!]/[\![\mathsf{P}]\!]}$. As $s^0_{\mathsf{R}}/s^0_{\mathsf{P}} \stackrel{t'o}{\Longrightarrow}_{\mathsf{R}/\mathsf{P}} s_{\mathsf{R}}/s_{\mathsf{P}}$ for some state $s_{\mathsf{R}}/s_{\mathsf{P}}$, it follows that $s_{\mathsf{R}}/s_{\mathsf{P}} \notin F$. Therefore, for any state $s'_{\mathsf{R}}/s'_{\mathsf{P}}$ such that $s^0_{\mathsf{R}}/s^0_{\mathsf{P}} \stackrel{t'ot''}{\Longrightarrow}_{\mathsf{R}/\mathsf{P}} s'_{\mathsf{R}}/s'_{\mathsf{P}}$ with $t'' \in (\mathcal{A}_{\mathsf{R}} \setminus \mathcal{A}^O_{\mathsf{R}/\mathsf{P}})^*$ we know that $s'_{\mathsf{R}}/s'_{\mathsf{P}} \notin F$. Consequently, if $t'ot'' \upharpoonright \mathcal{A}_{\mathsf{P}} \in F_{\mathsf{P}}$ then $t'ot'' \in F_{\mathcal{E}(\mathsf{R})}$, and if $t'ot'' \upharpoonright \mathcal{A}_{\mathsf{P}} \in T_{\mathsf{P}}$, then $t'ot'' \in T_{\mathcal{E}(\mathsf{R})}$. This means that $L(t'ot'')$ holds, and so we derive $t'o \in T_{[\![\mathsf{R}]\!]/[\![\mathsf{P}]\!]}$.

Case $t \equiv t'i$ with $i \in \mathcal{A}^I_{\mathsf{R}/\mathsf{P}}$. Suppose that $t'i \in F_{[\![\mathsf{R}]\!]/[\![\mathsf{P}]\!]}$. Then $t'i \upharpoonright \mathcal{A}_{\mathsf{P}} \notin T_{\mathsf{P}}$ or $t'i \in F_{\mathcal{E}(\mathsf{R})}$. By the induction hypothesis we know that $t' \in T_{[\![\mathsf{R}/\mathsf{P}]\!]}$, which by input receptiveness of components, implies that $t'i \in T_{[\![\mathsf{R}/\mathsf{P}]\!]}$. Now, if $t'i \upharpoonright \mathcal{A}_{\mathsf{P}} \notin T_{\mathsf{P}}$, then $t' \upharpoonright \mathcal{A}_{\mathsf{P}} \notin T_{\mathsf{P}}$ when $a \notin \mathcal{A}^O_{\mathsf{P}}$. Hence $t' \in F_{[\![\mathsf{R}]\!]/[\![\mathsf{P}]\!]}$, which by the induction hypothesis gives $t' \in F_{[\![\mathsf{R}/\mathsf{P}]\!]}$, and so $t'i \in F_{[\![\mathsf{R}/\mathsf{P}]\!]}$. When $a \in \mathcal{A}^O_{\mathsf{P}}$, condition Q3 ensures that $t'i \in F_{[\![\mathsf{R}/\mathsf{P}]\!]}$. If instead $t'i \in F_{\mathcal{E}(\mathsf{R})}$, then as $t'i \in T_{[\![\mathsf{R}/\mathsf{P}]\!]}$, we know $s^0_{\mathsf{R}}/s^0_{\mathsf{P}} \stackrel{t'i}{\Longrightarrow}_{\mathsf{R}/\mathsf{P}} s_{\mathsf{R}}/s_{\mathsf{P}}$. But $t'i \in F_{\mathcal{E}(\mathsf{R})}$ implies $s_{\mathsf{R}} = \bot_{\mathcal{E}(\mathsf{R})}$, hence $s_{\mathsf{R}}/s_{\mathsf{P}} = \bot_{\mathsf{R}/\mathsf{P}}$, meaning $t'i \in F_{[\![\mathsf{R}/\mathsf{P}]\!]}$.

Now suppose that $t'i \in F_{[\![\mathsf{R}/\mathsf{P}]\!]}$. By the induction hypothesis and input receptiveness of components it follows that $t'i \in T_{[\![\mathsf{R}]\!]/[\![\mathsf{P}]\!]}$. As $t'i \in F_{[\![\mathsf{R}/\mathsf{P}]\!]}$, it follows that $s^0_{\mathsf{R}}/s^0_{\mathsf{P}} \stackrel{t'i}{\Longrightarrow}_{\mathsf{R}/\mathsf{P}} \bot_{\mathsf{R}/\mathsf{P}}$. But $\bot_{\mathsf{R}/\mathsf{P}} = \bot_{\mathcal{E}(\mathsf{R})}/s_{\mathsf{P}}$ for some s_{P}. Hence, $t'i \in F_{\mathcal{E}(\mathsf{R})}$, which implies $t'i \in F_{[\![\mathsf{R}]\!]/[\![\mathsf{P}]\!]}$.

Showing that $t'i \in T_{[\![\mathsf{R}]\!]/[\![\mathsf{P}]\!]}$ iff $t'i \in T_{[\![\mathsf{R}/\mathsf{P}]\!]}$ follows by the induction hypothesis and input receptiveness of components.

For the liveness equivalence, it is sufficient to show that $t \in Err_{[\![\mathsf{R}]\!]/[\![\mathsf{P}]\!]}$ iff $t \in F_{\mathsf{R}/\mathsf{P}}$. This can be demonstrated in a straightforward manner using an inductive argument on the approximations of $Err_{[\![\mathsf{R}]\!]/[\![\mathsf{P}]\!]}$ and $F_{\mathsf{R}/\mathsf{P}}$. Note that the definition of $Err_{[\![\mathsf{R}]\!]/[\![\mathsf{P}]\!]}$ can be greatly simplified, as we assume $\mathcal{A}_{\mathsf{R}} = \mathcal{A}_{\mathsf{R}/\mathsf{P}}$ along with determinism, the latter of which implies divergence freedom.

Proof of Theorem 19

A straightforward modification to Theorem 7.

Proof of Corollary 2

Same reasoning as in Corollary 1 (with updated references).

Proof of Theorem 20

Begin by supposing $\mathsf{Q} \sqsubseteq_{IA} \mathsf{P}$ and let t be the smallest trace such that $t \in F_{\mathcal{E}([\![\mathsf{Q}]\!]^{IA})}$ and $t \notin F_{\mathcal{E}([\![\mathsf{P}]\!]^{IA})} \cup (T_{\mathcal{E}([\![\mathsf{P}]\!]^{IA})} \uparrow \mathcal{A}^I_{\mathsf{Q}})$. By definition of interface

automata, it follows that $t \in F_{[\![\mathsf{Q}]\!]^{IA}}$ and $t \notin F_{[\![\mathsf{P}]\!]^{IA}} \cup (T_{[\![\mathsf{P}]\!]^{IA}} \uparrow \mathcal{A}^I_{\mathsf{Q}})$ as the automata can only be inconsistent on seeing a bad input. Moreover, as the automata cannot be inconsistent up front, it follows that $t \equiv t'a$ with $a \in \mathcal{A}^I_{\mathsf{P}}$. By minimality of t, we know $t' \in T_{[\![\mathsf{P}]\!]^{IA}} \setminus F_{[\![\mathsf{P}]\!]^{IA}}$ and also that $t' \in T_{[\![\mathsf{Q}]\!]^{IA}} \setminus F_{[\![\mathsf{Q}]\!]^{IA}}$. Consequently, for each state q' such that $s^0_{\mathsf{Q}} \stackrel{t'}{\Longrightarrow}_{\mathsf{Q}} q'$, it follows that there exists p' such that $s^0_{\mathsf{P}} \stackrel{t'}{\Longrightarrow}_{\mathsf{P}} p'$, where at each intermediate state AS1 and AS2 hold, and $q'\ R\ p'$ for an alternating simulation R. For at least one of these q', it follows that $q' \stackrel{\epsilon}{\Longrightarrow}_{\mathsf{Q}} \not\stackrel{a}{\longrightarrow}_{\mathsf{Q}}$ (given $t'a \in F_{[\![\mathsf{Q}]\!]^{IA}}$). However, as $t'a \in T_{[\![\mathsf{P}]\!]^{IA}} \setminus F_{[\![\mathsf{P}]\!]^{IA}}$ it follows that $Act^I_{\mathsf{P}}(p')$ holds. Hence AS1 is violated, meaning $q'\ \not R\ p'$, which is contradictory. Therefore, $F_{[\![\mathsf{Q}]\!]^{IA}} \subseteq F_{[\![\mathsf{P}]\!]^{IA}} \cup (T_{[\![\mathsf{P}]\!]^{IA}} \uparrow \mathcal{A}^I_{\mathsf{Q}})$ as required.

Now suppose that $\mathsf{Q} \sqsubseteq_{IA} \mathsf{P}$ and let t be the smallest trace such that $t \in T_{[\![\mathsf{Q}]\!]^{IA}} \setminus F_{[\![\mathsf{Q}]\!]^{IA}}$ and $t \notin T_{[\![\mathsf{P}]\!]^{IA}} \cup (T_{[\![\mathsf{P}]\!]^{IA}} \uparrow \mathcal{A}^I_{\mathsf{Q}})$. It therefore follows that $t = t'a$ with $a \in \mathcal{A}^O_{\mathsf{Q}}$, and $t \in (\mathcal{A}_{\mathsf{P}} \cap \mathcal{A}_{\mathsf{Q}})^*$. Consequently, for each state q' such that $s^0_{\mathsf{Q}} \stackrel{t'}{\Longrightarrow}_{\mathsf{Q}} q'$, it follows that there exists p' such that $s^0_{\mathsf{P}} \stackrel{t'}{\Longrightarrow}_{\mathsf{P}} p'$, where at each intermediate state AS1 and AS2 hold, and $q'\ R\ p'$ for an alternating simulation R. For at least one of these q', it follows that $q' \stackrel{\epsilon}{\Longrightarrow}_{\mathsf{Q}} \stackrel{a}{\longrightarrow}_{\mathsf{Q}}$, hence $a \in Act^O_{\mathsf{Q}}(q')$. However, as $t'a \notin T_{[\![\mathsf{P}]\!]^{IA}}$ it follows that $a \notin Act^O_{\mathsf{P}}(p')$ for any p' reachable under t'. Hence AS2 is violated, meaning $q'\ \not R\ p'$, which again is contradictory. As a result, $T_{[\![\mathsf{Q}]\!]^{IA}} \subseteq T_{[\![\mathsf{P}]\!]^{IA}} \cup (T_{[\![\mathsf{P}]\!]^{IA}} \uparrow \mathcal{A}^I_{\mathsf{Q}})$.

Proof of Theorem 21

Based on Theorem 20, alternating simulation implies our trace-based refinement. So suppose $\mathsf{Q} \not\sqsubseteq_{IA} \mathsf{P}$. Then there exists a smallest trace t such that $s^0_{\mathsf{Q}} \stackrel{t}{\Longrightarrow}_{\mathsf{Q}} q'$, but no state p' such that $s^0_{\mathsf{P}} \stackrel{t}{\Longrightarrow}_{\mathsf{P}} p'$ and $q'\ R\ p'$. Note that by determinism q' is uniquely defined, as is p' if it exists. If p' exists, then $q'\ \not R\ p'$ meaning either AS1 or AS2 is violated. If AS1 is violated, then $q' \not\stackrel{a}{\longrightarrow}_{\mathsf{Q}}$ while $p' \stackrel{a}{\longrightarrow}_{\mathsf{P}}$ for some $a \in \mathcal{A}^I_{\mathsf{P}}$. Hence $ta \in F_{[\![\mathsf{Q}]\!]^{IA}}$ while $ta \notin F_{[\![\mathsf{P}]\!]^{IA}}$, which implies $[\![\mathsf{Q}]\!]^{IA} \not\sqsubseteq_{op} [\![\mathsf{P}]\!]^{IA}$. Instead, if AS2 is violated, then $q' \stackrel{a}{\longrightarrow}_{\mathsf{Q}}$ while $p' \not\stackrel{a}{\longrightarrow}_{\mathsf{P}}$ for some $a \in \mathcal{A}^O_{\mathsf{Q}}$. Hence $ta \in T_{[\![\mathsf{Q}]\!]^{IA}}$ while $ta \notin T_{[\![\mathsf{P}]\!]^{IA}}$, which also implies $[\![\mathsf{Q}]\!]^{IA} \not\sqsubseteq_{op} [\![\mathsf{P}]\!]^{IA}$. The final possibility is that p' does not exist, in which case $t \equiv t'a$, and $s^0_{\mathsf{P}} \stackrel{t'}{\Longrightarrow}_{\mathsf{P}}$ while $s^0_{\mathsf{P}} \not\stackrel{t}{\Longrightarrow}_{\mathsf{P}}$. As $\mathsf{Q} \not\sqsubseteq_{IA} \mathsf{P}$, it follows that $a \in \mathcal{A}^O_{\mathsf{Q}}$, but there is no matching transition in P. Consequently, $t \in T_{[\![\mathsf{Q}]\!]^{IA}}$, but $t \notin T_{[\![\mathsf{P}]\!]^{IA}}$, which yields $[\![\mathsf{Q}]\!]^{IA} \not\sqsubseteq_{op} [\![\mathsf{P}]\!]^{IA}$ as required.