# Timed I/O Automata

*It is never too late to complete your timed specification theory*

Goorden, Martijn A.; Larsen, Kim G.; Legay, Axel; Lorber, Florian; Nyman, Ulrik; Wasowski, Andrzej

*DOI (link to publication from Publisher):*
10.48550/ARXIV.2302.04529



*Publication date:*
2023

*Document Version*
Publisher's PDF, also known as Version of record

# Timed I/O Automata: It is never too late to complete your timed specification theory

Martijn A. Goorden[1*], Kim G. Larsen[1], Axel Legay[2], Florian Lorber[1], Ulrik Nyman[1] and Andrzej Wąsowski[3]

[1*]Department of Computer Science, Aalborg University, Selma Lagerlöfs Vej 300, Aalborg Öst, 9220, Danmark.
[2]Department of Computer Science Engineering, UC Louvain, Place Sainte Barbe 2, Louvain-la-Neuve, 1348, Belgium.
[3]Department of Computer Science, IT University, Langgaards Vej 7, Copenhagen S, 2300, Denmark.

*Corresponding author(s). E-mail(s): mgoorden@cs.aau.dk;
Contributing authors: kgl@cs.aau.dk; axel.legay@uclouvain.be; florber@cs.aau.dk; ulrik@cs.aau.dk; wasowski@itu.dk;

**Abstract**

A specification theory combines notions of specifications and implementations with a satisfaction relation, a refinement relation and a set of operators supporting stepwise design. We develop a complete specification framework for real-time systems using Timed I/O Automata as the specification formalism, with the semantics expressed in terms of Timed I/O Transition Systems. We provide constructs for refinement, consistency checking, logical and structural composition, and quotient of specifications – all indispensable ingredients of a compositional design methodology. The theory is backed by rigorous proofs and implemented in the open-source tool ECDAR.

**Keywords:** Specification theory, timed input-output automata, timed input-output transition systems

# 1 Introduction

Software systems are decomposed into components, often designed by independent teams, working under a common agreement on what the interface of each component should be. Consequently, *compositional reasoning* [1], the mathematical foundations of reasoning about interfaces, is an active research area. Besides supporting compositional development, it enables compositional reasoning about the system (verification) and allows well-grounded reuse.

In a logical interpretation, interfaces are specifications, while components that implement an interface are understood as models/implementations. Specification theories should support various features including (1) a *refinement* that allows to compare specifications and to replace a specification by another one in a design, (2) a *logical conjunction* that expresses combining the requirements of two or more specifications, (3) a *structural composition*, which allows to combine specifications, and (4) a *quotient operator* that, being a dual to structural composition, allows decomposing the design by groups of requirements. The latter is crucial to perform incremental design. Also, the operations have to be related by compositional reasoning theorems, guaranteeing both incremental design and independent implementability [2].

Building good specification theories is the subject of intensive studies [3, 4]. Interface automata are one such successful direction [2, 4–6]. In this framework, an interface is represented by an input/output automaton [7], i.e., an automaton whose transitions are typed with *input* and *output*. The semantics of such an automaton is given by a two-player game: the *input* player represents the environment, and the *output* player represents the component itself. Contrary to the input/output model proposed by Lynch [7], this semantic offers an optimistic treatment of composition: two interfaces can be composed if there exists at least one environment in which they can interact together in a safe way. A timed extension of the theory of interface automata has been motivated by the fact that real time can be a crucial parameter in practice, for example in embedded systems [8]. While the theory of timed interface automata focuses on structural composition, in this paper we go further and build the first game-based specification theory for timed systems with all four operators (refinement, conjunction, composition, and quotient).

*Component interface specification and consistency* We represent specifications by timed input/output transition systems [9], i.e., timed transitions systems whose sets of discrete transitions are split into input and output transitions. Contrary to [8] and [9] we distinguish between implementations and specifications by adding conditions on the models. This is done by assuming that the former have fixed timing behaviour and they can always advance either by producing an output or delaying. We also provide a game-based methodology to decide whether a specification is consistent, i.e., whether it has at least one implementation. The latter reduces to deciding existence of a strategy that despite the behaviour of the environment will avoid states that cannot possibly satisfy the implementation requirements.

*Refinement and logical conjunction* A specification $S_1$ *refines* a specification $S_2$ iff it is possible to replace $S_2$ with $S_1$ in every environment and obtain an equivalent system. In the input/output setting, checking refinement reduces to deciding an alternating timed simulation between the two specifications [4]. In our timed extension, checking such simulation can be done with a slight modification of the theory proposed in [10]. As implementations are specifications, refinement coincides with the satisfaction relation. Our refinement operator has the *model inclusion property*, i.e., $S_1$ refines $S_2$ iff the set of implementations satisfied by $S_1$ is included in the set of implementations satisfied by $S_2$. We also propose a *logical conjunction* operator between specifications. Given two specifications, the operator will compute a specification whose implementations are satisfied by both operands. The operation may introduce error states that do not satisfy the implementation requirement. Those states are pruned by synthesizing a strategy for the component to avoid reaching them. Here we assume that we want to avoid reaching error states with any possible environment, hence this pruning is called *adversarial pruning*. We also show that conjunction coincides with shared refinement, i.e., it corresponds to the greatest specification that refines both $S_1$ and $S_2$.

*Structural composition* Following [8], specifications interact by synchronizing on inputs and outputs. However, like in [7, 9], we restrict ourselves to input-enabled systems. This makes it impossible to reach an immediate *deadlock state*, where a component proposes an output that cannot be captured by the other component. Unlike in [7, 9], input-enabledness shall not be seen as a way to avoid error states. Indeed, such error states can still be designated by the designer as states which do not warrant desirable temporal properties. When composing specifications together, one would like to simplify the composition as much as possible before continuing the compositional analysis. We show that adversarial pruning does not distribute over the parallel composition operator. Therefore, we introduce the notion of *cooperative pruning*. Finally, we show that our composition operator is associative and that refinement is a precongruence with respect to it.

*Quotient* We propose a quotient operator dual to composition. Intuitively, given a global specification $T$ of a composite system as well as the specification of an already realized component $S$, the *quotient* will return the most liberal specification $X$ for the missing component, i.e., $X$ is the largest specification such that $S$ in parallel with $X$ refines $T$.

*Implementation* Our methodology is being implemented in the open-source tool ECDAR[1]. It builds on timed input/output automata, a symbolic representation for timed input/output transition systems. We show that conjunction, composition, and quotienting are simple product constructions allowing for consistency checking to be solved using the zone-based algorithms for synthesizing winning strategies in timed games [11, 12]. Finally, refinement between specifications is checked using a variant of the recent efficient game-based algorithm of [10].

[1] http://ecdar.net

**Paper extensions.** This journal paper is an extended and revised version of the conference papers [13, 14]. In this journal paper, we clarify the notion and effect of pruning by introducing adversarial pruning and cooperative pruning, we show that adversarial pruning (in [13, 14] just called pruning) does not distribute over the parallel composition so we no longer require pruning after each composition, we corrected several definitions, including the one of the quotient, we removed the notion of strictly undesirable states, and lastly all theorems are now actually proven.

**Structure of the paper.** The paper is organized as follows. Section 2 introduces the general framework of timed input/output transition systems and timed input/output automata, the notions of specification and implementation, and the concept of refinement. Section 3 continuous by introducing consistency, the conjunction operator, and adversarial pruning. Then, in Section 4 we introduce and discuss parallel composition and in Section 5 the quotient operator. Section 6 briefly mentions the current state of the implementation of the theory in ECDAR. Finally, Section 7 concludes the paper.

**Example.** Universities operate under increasing pressure and competition. One of the popular factors used in determining the level of national funding is that of societal impact, which is approximated by the number of news articles published based on research outcomes. Clearly one would expect that the number (and size) of grants given to a university has a (positive) influence on the number of news articles.

Figure 1 gives the insight as to the organisation of a very small University comprising three components Administration, Machine and Researcher. The Administration is responsible for interaction with society in terms of acquiring grants (grant) and writing news articles (news). However, the other components are necessary for news articles to be obtained. The Researcher will produce the crucial publications (pub) within given time intervals, provided timely stimuli in terms of coffee (cof) or tea (tea). Here coffee is clearly preferred over tea. The beverage is provided by a Machine, which given a coin (coin) will provide either coffee or tea within some time interval, or even the possibility of free tea after some time.

In Figure 1 the three components are specifications, each allowing for a multitude of incomparable, actual implementations differing with respect to exact timing behavior (e.g., at what time are publications actually produced by the Researcher given a coffee) and exact output produced (e.g., does the Machine offer tea or coffee given a coin).

As a first property, we may want to check that the composition of the three components comprising our University is compatible: we notice that the specification of the Researcher contains an Err state, essentially not providing any guarantees as to what behaviour to expect if tea is offered at a late stage. Now, compatibility checking amounts simply to deciding whether the user of the University (i.e., the society) has such a strategy for using it that the Researcher will avoid ever entering this error state.

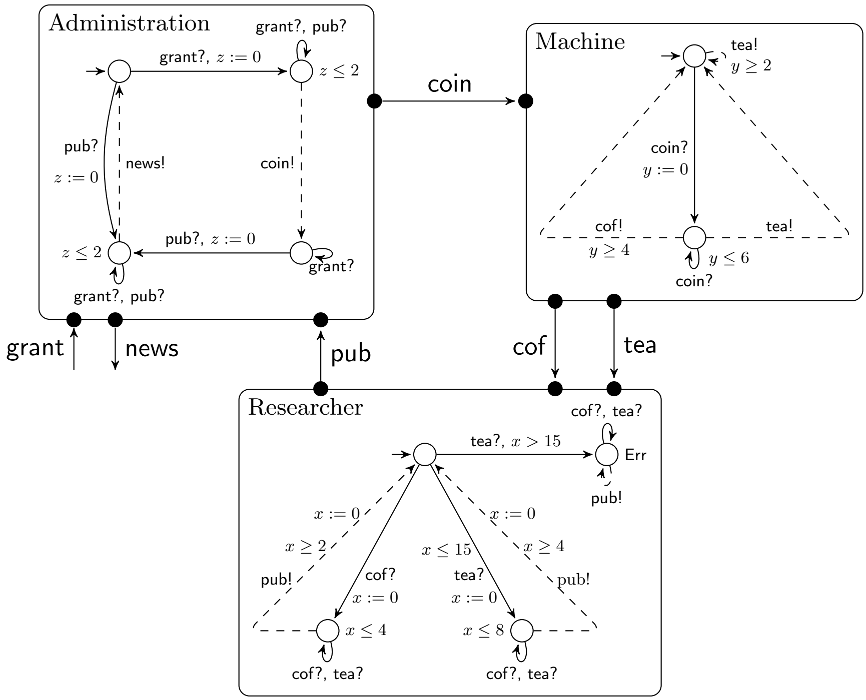



**Fig. 1**: Specifications for and interconnections between the three main components of a modern University: Administration, Machine and Researcher.

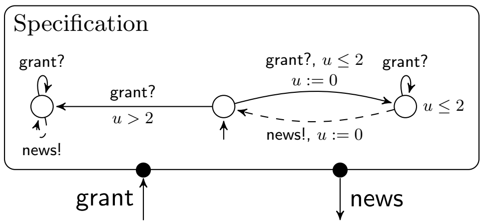



**Fig. 2**: Overall specification for a University.

As a second property, we may want to show that the composition of arbitrary implementations conforming to respective component specification is guaranteed to satisfy some overall specification. Here Figure 2 provides an overall specification (essentially saying that whenever grants are given to the University sufficiently often then news articles are also guaranteed within a certain upper time-bound). Checking this property amounts to establishing a refinement between the composition of the three component specifications and the overall specification. We leave the reader in suspense until the concluding section before we reveal whether the refinement actually holds or not!

## 2 Specifications and refinements

Throughout the presentation of our specification theory, we continuously switch the mode of discussion between the semantic and syntactic levels. In general, the formal framework is developed for the semantic objects, *Timed I/O Transition Systems* (TIOTSs in short) [15], and lifted to the syntactic constructions for *Timed I/O Automata* (TIOAs), which act as a symbolic and finite representation for TIOTSs. However, it is important to emphasize that the theory for TIOTSs does not rely in any way on the TIOAs representation – one can build TIOTSs that cannot be represented by TIOAs, and the theory remains sound for them (although we do not know how to manipulate them automatically).

**Definition 1** *A* Timed Input Output Transition System *(TIOTS) is a tuple $S = (Q^S, q_0^S, Act^S, \rightarrow^S)$, where $Q^S$ is usually an infinite set of states, $q_0 \in Q$ the initial state, $Act^S = Act_i^S \uplus Act_o^S$ a finite set of actions partitioned into inputs ($Act_i^S$) and outputs ($Act_o^S$), and $\rightarrow^S \subseteq Q^S \times (Act^S \cup \mathbb{R}_{\geq 0}) \times Q^S$ a transition relation satisfying the following conditions:*

*[time determinism] whenever $q \xrightarrow{d}^S q'$ and $q \xrightarrow{d}^S q''$, then $q' = q''$*

*[time reflexivity] $q \xrightarrow{0}^S q$ for all $q \in Q^S$*

*[time additivity] for all $q, q'' \in Q^S$ and all $d_1, d_2 \in \mathbb{R}_{\geq 0}$ we have $q \xrightarrow{d_1+d_2}^S q''$ iff $q \xrightarrow{d_1}^S q'$ and $q' \xrightarrow{d_2}^S q''$ for some $q' \in Q^S$.*

We write $q \xrightarrow{a}^S q'$ instead of $(q, a, q') \in \rightarrow^S$ and use $i?$, $o!$, and $d$ to range over inputs, outputs, and $\mathbb{R}_{\geq 0}$, respectively. When no confusion can arise, for example when only a single specification is given in a definition, we might drop the superscript for readability, like $Q$ instead of $Q^S$ if $S$ is the only given TIOTS. We write $q \xrightarrow{a}$ to indicate that there exists a $q' \in Q$ s.t. $q \xrightarrow{a} q'$, and $q \not\xrightarrow{a}$ to indicate that there does not exist $q' \in Q$ s.t. $q \xrightarrow{a} q'$. In the interest of simplicity, we work with *deterministic* TIOTSs: for all $a \in Act \cup \mathbb{R}_{\geq 0}$ whenever $q \xrightarrow{a}^S q'$ and $q \xrightarrow{a}^S q''$, we have $q' = q''$ (determinism is required not only for timed transitions but also for discrete transitions). In the rest of the paper, we often drop the adjective 'deterministic.'

For a TIOTS $S$ and a set of states $X$, we write

$$\mathrm{pred}_a^S(X) = \{q \in Q^S \mid \exists q' \in X : q \xrightarrow{a}^S q'\}$$

for the set of all $a$-predecessors of states in $X$. We write $\mathrm{ipred}^S(X)$ for the set of all input predecessors and $\mathrm{opred}^S(X)$ for all output predecessors of $X$:

$$\mathrm{ipred}^S(X) = \bigcup_{a \in Act_i^S} \mathrm{pred}_a^S(X)$$

$$\text{opred}^S(X) = \bigcup_{a \in Act_o^S} \text{pred}_a^S(X).$$

Furthermore, $\text{post}_d^S(q)$ is the set of all time successors of a state $q$ that can be reached by delays smaller than $d$:

$$\text{post}_d^S(q) = \{q' \in Q^S \mid \exists d' \in [0, d\rangle : q \xrightarrow{d'}{}^S q'\}.$$

We shall now introduce a symbolic representation for TIOTSs in terms of Timed I/O Automata (TIOAs). Let *Clk* be a finite set of *clocks*. A *clock valuation* over *Clk* is a mapping $v \in [Clk \mapsto \mathbb{R}_{\geq 0}]$. We write $v + d$ to denote a valuation such that for any clock $r$ we have $(v + d)(r) = v(r) + d$. Given $d \in \mathbb{R}_{\geq 0}$ and a set of clocks $c$, we write $v[r \mapsto 0]_{r \in c}$ for a valuation which agrees with $v$ on all values for clocks not in $c$, and returns 0 for all clocks in $c$. So this notation resets the clocks in $c$. For example, $\{x \mapsto 3, y \mapsto 4.5\}[r \mapsto 0]_{r\in\{x\}} \equiv \{x \mapsto 0, y \mapsto 4.5\}$. A guard over *Clk* is a finite Boolean formula with the usual propositional connectives where clauses are expressions of the form $x \prec n$, where $x \in Clk$, $\prec \in \{<, \leq, >, \geq, =\}$, and $n \in \mathbb{N}$. We write $\mathcal{B}(Clk)$ for the set of all guards over *Clk*. The notation $\mathbf{T}$ is used for the logical true and $\mathbf{F}$ for the logical false. The reset of a guard $q \in \mathcal{B}(Clk)$, denoted by $g[r \mapsto 0]_{r\in c}$, is again a guard where each occurrence of clock $x \in c$ is replaced by 0. For example $(x < 4 \wedge y > 2)[x \mapsto 0] \equiv 0 < 4 \wedge y > 2 \equiv y > 2$.

**Definition 2** *A* Timed Input Output Automaton *(TIOA) is a tuple* $A = (Loc, l_0, Act, Clk, E, Inv)$ *where Loc is a finite set of locations,* $l_0 \in Loc$ *the initial location,* $Act = Act_i \uplus Act_o$ *is a finite set of actions partitioned into inputs* ($Act_i$) *and outputs* ($Act_o$)*, Clk a finite set of clocks,* $E \subseteq Loc \times Act \times \mathcal{B}(Clk) \times 2^{Clk} \times Loc$ *a set of edges, and* $Inv : Loc \mapsto \mathcal{B}(Clk)$ *a location invariant function.*

If $(l, a, \varphi, c, l') \in E$ is an edge, then $l$ is a source location, $a$ is an action label, $\varphi$ is a guard over clocks that must be satisfied when the edge is executed, $c$ is a set of clocks to be reset, and $l'$ is a target location. Examples of TIOAs have been shown in the introduction.

**Definition 3** *The* semantic *of a TIOA* $A = (Loc, l_0, Act, Clk, E, Inv)$ *is the TIOTS* $[\![A]\!]_{\text{sem}} = (Loc \times [Clk \mapsto \mathbb{R}_{\geq 0}], (l_0, \mathbf{0}), Act, \rightarrow)$*, where* $\mathbf{0}$ *is a constant function mapping all clocks to zero,* $\mathbf{0} \models Inv(l_0)$*, and* $\rightarrow$ *is the largest transition relation generated by the following rules:*

- *Each* $(l, a, \varphi, c, l') \in E$ *gives rise to* $(l, v) \xrightarrow{a} (l', v')$ *for each clock valuation* $v \in [Clk \mapsto \mathbb{R}_{\geq 0}]$ *such that* $v \models \varphi$ *and* $v' = v[r \mapsto 0]_{r\in c}$ *and* $v' \models Inv(l')$.
- *Each location* $l \in Loc$ *with a valuation* $v \in [Clk \mapsto \mathbb{R}_{\geq 0}]$ *gives rise to a transition* $(l, v) \xrightarrow{d} (l, v + d)$ *for each delay* $d \in \mathbb{R}_{\geq 0}$ *such that* $v + d \models Inv(l)$ *and* $\forall d' \in \mathbb{R}_{\geq 0}, d' < d : v + d' \models Inv(l)$.

Note that the TIOTSs induced by TIOAs satisfy the axioms 1–3 of Definition 1. In order to guarantee determinism, the TIOA has to be deterministic: for each action–location pair, if more than one edge is enabled at the same time, the resets and target locations need to be the same. This is a standard check. We assume that all TIOAs below are deterministic.

Having introduced a syntactic representation for TIOTSs, we now turn back to the semantic level in order to define the basic concepts of implementation and specification.

**Definition 4** *A TIOTS S is a* specification *if each of its states $q \in Q$ is input-enabled: $\forall i? \in Act_i : \exists q' \in Q$ s.t. $q \xrightarrow{i?} q'$. A TIOA A is a* specification automaton *if its semantic $[\![A]\!]_{\mathrm{sem}}$ is a specification.*

The assumption of input-enabledness, also seen in many interface theories [16–20], reflects our belief that an input cannot be prevented from being sent to a system, but it might be unpredictable how the system behaves after receiving it. Input-enbledness encourages explicit modeling of this unpredictability, and compositional reasoning about it; for example, deciding if an unpredictable behaviour of one component induces unpredictability of the entire system.

In practice tools can interpret absent input transitions in at least two reasonable ways. First, they can be interpreted as ignored inputs, corresponding to location loops in the automaton. Second, they may be seen as unavailable ('blocking') inputs, which can be achieved by assuming implicit transitions to a designated error state.

The role of specifications in a specification theory is to abstract, or underspecify, sets of possible implementations. *Implementations* are concrete executable realizations of systems. We will assume that implementations of timed systems have fixed timing behaviour (outputs occur at predictable times) and systems can always advance either by producing an output or delaying. This is formalized using axioms of *output-urgency* and *independent-progress* below.

**Definition 5** *A specification $P = (Q, q_0, Act, \rightarrow)$ is an* implementation *if for each state $q \in Q$ we have*

*[output urgency] $\forall q', q'' \in Q$, if $q \xrightarrow{o!}^P q'$ and $q \xrightarrow{d}^P q''$ for some $o! \in Act_o$ and $d \in \mathbb{R}_{\geq 0}$, then $d = 0$.*

*[independent progress] either $\forall d \in \mathbb{R}_{\geq 0} : q \xrightarrow{d}^P$ or $\exists d \in \mathbb{R}_{\geq 0}, \exists o! \in Act_o$ s.t. $q \xrightarrow{d}^P q'$ and $q' \xrightarrow{o!}^P$.*

*A specification automaton A is an* implementation automaton *if its semantic $[\![A]\!]_{\mathrm{sem}}$ is an implementation.*

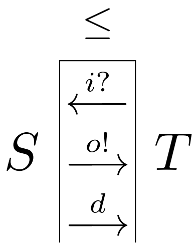



**Fig. 3**: Visual representation of the simulation relation defined by refinement.

Independent progress is one of the central properties in our theory: it states that an implementation cannot ever get stuck in a state where it is up to the environment to induce progress. So in every state there either exists an ability to delay until an output is possible or the state can delay indefinitely. An implementation cannot wait for an input from the environment without letting time pass. Unfortunately, implementations might contain zeno behavior, for example, a state having an output action as a self-loop might stop time by firing this transition infinitely often. So time should be able to diverge, see [21]. Yet, to verify whether an implementation has time divergence, we need to analyze it in the context of an environment to form a closed-system. Environments could both ensure or prevent time to diverge, so one cannot determine time divergence by analyzing the system without an environment. In this paper, we focus on specifying components as part of a system. Therefore, we ignore the problem of time divergence for now and postpone it to future work.

A notion of *refinement* allows to compare two specifications as well as to relate an implementation to a specification. Refinement should be a pre-congruence when we compose several specifications of a system together. This is formalized with Theorem 8 in Section 4.

We study these kind of properties in later sections. It is well known from the literature [2, 4, 10] that in order to give these kind of guarantees a refinement should have the flavour of *alternating (timed) simulation* [22]. Figure 3 shows a visual representation of the direction of the simulation relation captures by refinement. While it is typical to define simulation relations on transitions systems that have equal alphabet, we relaxed that in our definition of refinement below. Then it fits the main theorem of quotient in Section 5 and it matches the usage in practical examples, see for example the university example in this paper.

**Definition 6** *Given specifications* $S = (Q^S, q_0^S, Act^S, \rightarrow^S)$ *and* $T = (Q^T, q_0^T, Act^T, \rightarrow^T)$ *where* $Act_i^S \cap Act_o^T = \emptyset$, $Act_o^S \cap Act_i^T = \emptyset$, $Act_i^S \subseteq Act_i^T$, *and* $Act_o^T \subseteq Act_o^S$. $S$ refines $T$, *denoted by* $S \leq T$, *iff there exists a binary relation* $R \subseteq Q^S \times Q^T$ *such that* $(q_0^S, q_0^T) \in R$ *and for each pair of states* $(s, t) \in R$ *it holds that*

1. *Whenever* $t \xrightarrow{i?}^T t'$ *for some* $t' \in Q^T$ *and* $i? \in Act_i^T \cap Act_i^S$, *then* $s \xrightarrow{i?}^S s'$ *and* $(s', t') \in R$ *for some* $s' \in Q^S$
2. *Whenever* $t \xrightarrow{i?}^T t'$ *for some* $t' \in Q^T$ *and* $i? \in Act_i^T \setminus Act_i^S$, *then* $(s, t') \in R$
3. *Whenever* $s \xrightarrow{o!}^S s'$ *for some* $s' \in Q^S$ *and* $o! \in Act_o^S \cap Act_o^T$, *then* $t \xrightarrow{o!}^T t'$ *and* $(s', t') \in R$ *for some* $t' \in Q^T$
4. *Whenever* $s \xrightarrow{o!}^S s'$ *for some* $s' \in Q^S$ *and* $o! \in Act_o^S \setminus Act_o^T$, *then* $(s', t) \in R$
5. *Whenever* $s \xrightarrow{d}^S s'$ *for some* $s' \in Q^S$ *and* $d \in \mathbb{R}_{\geq 0}$, *then* $t \xrightarrow{d}^T t'$ *and* $(s', t') \in R$ *for some* $t' \in Q^T$

*A specification automaton* $A$ refines *another specification automaton* $B$, *denoted by* $A \leq B$, *iff* $[\![A]\!]_{\text{sem}} \leq [\![B]\!]_{\text{sem}}$.

It is easy to see that the refinement is reflexive. Refinement is only transitive under specific conditions. These conditions are captured in Lemma 1. A special case satisfying these conditions is when the action sets of all specifications are the same. Refinement can be checked for specification automata by reducing the problem to a specific refinement game, and using a symbolic representation to reason about it. We discuss details of this process in Section 6. Figure 4 shows a coffee machine that is a refinement of the one in Figure 1. It has been refined in two ways: one output transition has been completely dropped and one state invariant has been tightened.

**Lemma 1** *Given specifications* $S^i = (Q^i, q_0^i, Act^i, \rightarrow^i)$ *with* $i \in \{1, 2, 3\}$. *If* $S^1 \leq S^2$, $S^2 \leq S^3$, $Act_i^1 \cap Act_o^3 = \emptyset$, *and* $Act_o^1 \cap Act_i^3 = \emptyset$, *then* $S^1 \leq S^3$.

*Proof* (⇒) We first show that the action sets of $S^1$ and $S^3$ satisfy the conditions of refinement. From $S^1 \leq S^2$ it follows that $Act_i^1 \subseteq Act_i^2$, and $Act_o^2 \subseteq Act_o^1$; similarly, from $S^2 \leq S^3$ it follows that $Act_i^2 \subseteq Act_i^3$, and $Act_o^3 \subseteq Act_o^2$. Combining this results in $Act_i^1 \subseteq Act_i^3$, and $Act_o^3 \subseteq Act_o^1$. Together with the antecedent and Definition 6 of refinement we can conclude that action sets of $S^1$ and $S^3$ satisfy the conditions of refinement.

It remains to show that there exists a relation $R^{13}$ witnessing $S^1 \leq S^3$. Let $R^{12}$ and $R^{23}$ the relations witnessing $S^1 \leq S^2$ and $S^2 \leq S^3$, respectively. Using a standard co-inductive argument it can be shown that

$$R^{13} = \left\{(q^1, q^3) \in R^{13} \mid \exists q^2 \in Q^2 : (q^1, q^2) \in R^{12} \wedge (q^2, q^3) \in R^{23}\right\}$$

witnesses $S^1 \leq S^3$.

□

Since our implementations are a subclass of specifications, we simply use *refinement* as an implementation relation.

**Definition 7** *An implementation* $P$ *satisfies a specification* $S$, *denoted* $P \,\text{sat}\, S$, *iff* $P \leq S$. *We write* $[\![S]\!]_{\text{mod}}$ *for the set of all implementations of* $S$, *so* $[\![S]\!]_{\text{mod}} = \{P \mid P \,\text{sat}\, S\}$.

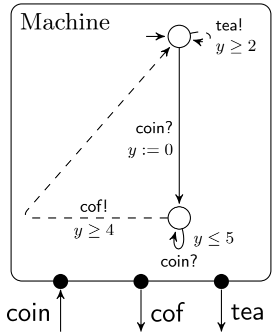



**Fig. 4**: A coffee machine specification that refines the coffee machine in Figure 1.

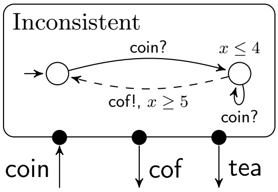



**Fig. 5**: An inconsistent specification.

From a logical perspective, specifications are like formulae, and implementations are their models. This analogy leads us to a classical notion of consistency, as existence of models.

**Definition 8** *A specification $S$ is* consistent *iff there exists an implementation $P$ such that $P \leq S$. A specification automaton $A$ is* consistent *iff its semantic $[\![A]\!]_{\mathrm{sem}}$ is consistent.*

All specification automata in Figure 1 are consistent. An example of an inconsistent specification can be found in Figure 5. Notice that the invariant in the second state ($x \leq 4$) is stronger than the guard ($x \geq 5$) on the cof edge. This location violates the independent progress property.

We also define a stricter, more syntactic, notion of consistency, which requires that all states are consistent.

**Definition 9** *A specification $S$ is* locally consistent *iff every state $s \in Q$ allows independent progress. A specification automaton $A$ is* locally consistent *iff its semantic $[\![A]\!]_{\mathrm{sem}}$ is locally consistent.*

**Theorem 1** *Every locally consistent specification is consistent in the sense of Definition 8.*

*Proof* Let us begin with defining an auxiliary function $\delta$ which chooses a delay for every state $s$ in a locally consistent specification $S$:

$$\delta(s) = \begin{cases} d & \text{the infimum } d \text{ such that } s \xrightarrow{d}^{S} s' \text{ and } \exists o! : s' \xrightarrow{o!}^{S} \\ +\infty & \text{otherwise} \end{cases}$$

Note that since $s$ allows independent progress, it always hold that $s \xrightarrow{\delta(s)}^{S}$. $\delta$ is time additive in the following sense: if $s \xrightarrow{d}^{S} s'$ and $d \leq \delta(s)$ then $\delta(s') + d = \delta(s)$, which is due to time additivity of $\rightarrow^{S}$, and local consistency of $S$.

We want to show for an arbitrary locally consistent specifications $S$ that it has an implementation. This can be shown by synthesizing an implementation $P = (Q^S, s_0, Act^S, \rightarrow^P)$, where $\rightarrow^P$ is the largest transition relation generated by the following rules:

$$s \xrightarrow{i?}^{P} s' \text{ if } s \xrightarrow{i?}^{S} s' \wedge i? \in Act_i^S$$

$$s \xrightarrow{o!}^{P} s' \text{ if } s \xrightarrow{o!}^{S} s' \wedge o! \in Act_o^S \wedge \delta(s) = 0$$

$$s \xrightarrow{d}^{P} s' \text{ if } s \xrightarrow{d}^{S} s' \wedge d \in \mathbb{R}_{\geq 0} \wedge d \leq \delta(s)$$

Since $P$ only takes a subset of transitions of $S$, the determinism of $S$ implies determinism of $P$. The transition relation of $P$ is time-additive due to time additivity of $\rightarrow^S$ and of $\delta$. It is also time-reflexive due to the last rule ($0 \leq \delta(s)$ for every state $s$ and $\rightarrow^S$ was time reflexive). So $P$ is a TIOTS.

The new transition relation is also input enabled as it inherits of input transitions from $S$, which was input enabled. So $P$ is a specification. The second rule guarantees that outputs are urgent (by construction $P$ only outputs when no further delays are possible). Moreover $P$ observes independent progress. Consider a state $s$ in $P$. Then if $\delta(s) = +\infty$ clearly $s$ can delay indefinitely. If $\delta(s)$ is finite, then by definition of $\delta$ and of $P$, the state $s$ can delay and hence produce an output. Thus $P$ is an implementation in the sense of Definition 5.

Now an unsurprising coinductive argument shows that the following relation $R \subseteq Q^S \times Q^S$ witnesses $P$ sat $S$:

$$R = \left\{ (s, s) \mid s \in Q^S \right\}.$$

□

The opposite implication in the theorem does not hold as we shall see later. Local consistency, or independent progress, can be checked for specification automata establishing local consistency for the syntactic representation. Technically it suffices to check for each location that if the supremum of all solutions of every location invariant exists then it satisfies the invariant itself and allows at least one enabled output transition.

Prior specification theories for discrete time [5] and probabilistic [23] systems reveal two main requirements for a definition of implementation. These are the same requirements that are typically imposed on a definition of a model as a special case of a logical formula. First, implementations should be consistent specifications (logically, models correspond to some consistent formulae). Second, implementations should be most specified (models cannot be refined by non-models), as opposed to proper specifications, which should be *underspecified.* For example, in propositional logics, a model is represented as a complete consistent term. Any implicant of such a term is also a model (in propositional logics, it is actually equivalent to it).

Our definition of implementation satisfies both requirements, and to the best of our knowledge, it is the first example of a proper notion of implementation for timed specifications. As the refinement is reflexive we get $P \,\mathrm{sat}\, P$ for any implementation and thus each implementation is consistent as per Definition 8. Furthermore, each implementation cannot be refined anymore by any underspecified specifications.

**Theorem 2** *Any locally consistent specification $S$ refining an implementation $P$ is an implementation as per Definition 5.*

*Proof* Observe first that $S$ is already locally consistent, so all its states warrant independent progress. We only need to argue that it satisfies output urgency. Without loss of generality, assume that $S$ only contains states which are reachable by (sequences of) discrete or timed transitions.

If $S$ only contains reachable states, every state of $S$ has to be related to some state of $P$ in a relation $R$ witnessing $S \leq P$ (output and delay transitions need to be matched in the refinement; input transitions also need to be matched as $P$ is input enabled and $S$ is deterministic). This can be argued for using a standard, though slightly lengthy argument, by formalizing reachable states as a fixpoint of a monotonic operator.

Now that we know that every state of $S$ is related to some state of $P$ consider an arbitrary $s \in Q^S$ and let $p \in Q^P$ be such that $(s, p) \in R$. Then if $s \xrightarrow{o!}{}^S s'$ for some state $s' \in Q^S$ and an output $o! \in Act_o^S$, it must be that also $p \xrightarrow{o!}{}^P p'$ for some state $p' \in Q^P$ (and $(s', p') \in R$). But since $P$ is an implementation, its outputs must be urgent, so $p \not\xrightarrow{d}{}^P$ for all $d > 0$, and consequently $s \not\xrightarrow{d}{}^S$ for all $d > 0$. We have shown that all states of $S$ have urgent outputs (if any) and thus $S$ is an implementation. □

We conclude the section with the first major theorem. Observe that every preorder $\preceq$ is intrinsically complete in the following sense: $S \preceq T$ iff for every smaller element $P \preceq S$ also $P \preceq T$. This means that a refinement of two specifications coincides with inclusion of sets of all the specifications refining each of them. However, since out of all specifications only the implementations correspond to real world objects, another completeness question is more relevant: does the refinement coincide with the inclusion of implementation sets? This property, which does not hold for any preorder in general, turns out to hold for our refinement.

**Theorem 3** *For any two locally consistent specifications $S, T$ having the same action set we have that $S \leq T$ iff $[\![S]\!]_{\mathrm{mod}} \subseteq [\![T]\!]_{\mathrm{mod}}$.*

*Proof* (⇒) Assume existence of relations $R_1$ and $R_2$ witnessing satisfaction of $S$ by the implementation $P$ and refinement of $T$ by $S$, respectively. Use a standard co-inductive argument and Lemma 1 to show that

$$R = \left\{(p,t) \in Q^P \times Q^T \mid \exists s \in Q^S : (p,s) \in R_1 \wedge (s,t) \in R_2\right\}$$

is a relation witnessing satisfaction of $T$ by $P$. Also observe that $(p_0, t_0) \in R$.

(⇐) In the following we write $p \,\mathrm{sat}\, s$ for states $p$ and $s$ meaning that there exists a relation $R'$ witnessing $P \,\mathrm{sat}\, S$ that contains $(p, s)$.

We construct a binary relation $R \subseteq Q^S \times Q^T$:

$$R = \{(s,t) \mid \forall P : p_0 \text{ sat } s \implies p_0 \text{ sat } t\},$$

where $p_0$ is the initial state of $P$. We shall argue that $R$ witnesses $S \leq T$. Consider a pair $(s,t) \in R$. There are two cases to be considered.

- Consider any input $i?$. Due to input-enabledness, there exists $t' \in Q^T$ such that $t \xrightarrow{i?}{}^T t'$. We need to show existence of a state $s' \in Q^S$ such that $s \xrightarrow{i?}{}^S s'$ and $(s',t') \in R$, so $\forall P : p_0 \text{ sat } s' \implies p_0 \text{ sat } t'$.

  Due to input-enabledness, for the same $i?$ there exists a state $s' \in Q^S$ such that $s \xrightarrow{i?}{}^S s'$. We need to show that $(s',t') \in R$. By Theorem 1 applied to $Q^S$ we have that there exists an implementation $P$ and its state $p_0 \in Q^P$ such that $p_0$ sat $s'$ (technically speaking $s$ may not be an initial state of $S$, but we can consider a version of $S$ with initial state changed to $s$ to apply Theorem 1, concluding existence of an implementation).

  Consider an arbitrary implementation $Q$ sat $S$ and its state $q_0 \in Q^Q$ such that $q_0$ sat $s'$. We need to show that also $q_0$ sat $t'$. We do this by extending $Q$ deterministically to a model of $s$, showing that this is also a model of $t$, and then arguing that the only $i?$ successor state models $t'$. Create an implementation $Q'$ by merging $Q$ and $P$ above and adding a fresh state $q$ with transition $q \xrightarrow{i?}{}^{Q'} q_0$ and transitions $q \xrightarrow{j?}{}^{Q'} p_0$ for all $j? \neq i?$, $j? \in Act_i$[2]. Now $q$ sat $s$ as $q \xrightarrow{i?}{}^{Q'} q_0$ with $q_0$ sat $s'$ and $q \xrightarrow{j?}{}^{Q'} p_0$ with $p_0$ sat $s'$ for $j? \neq i?$. By assumption, every implementation of $S$ is also an implementation of $T$, so $q \,\mathrm{sat}\, t$ and consequently $q_0 \,\mathrm{sat}\, t'$ as $q$ is deterministic on $i?$. Summarizing, for any implementation $q_0 \,\mathrm{sat}\, s'$ we are able to argue that $q_0$ sat $t'$, thus necessarily $(s',t') \in R$.

- Consider any action $a$ (which is an output or a delay) for which there exists $s'$ such that $s \xrightarrow{a}{}^S s'$. Using a construction similar to the one above it is not hard to see that one can actually construct (and thus postulate existence of) an implementation $P$ containing $p \in Q^P$ such that $p \,\mathrm{sat}\, s$ that has a transition $p \xrightarrow{a}{}^P p'$. Since also $p \mathrm{sat} t$, we have that there exists $t' \in Q^T$ such that $t \xrightarrow{a}{}^T t'$. It remains to argue that $(s',t') \in R$. This is done in the same way as with the first case, by considering any model of $s'$, then by extending it deterministically to a model of $s$, concluding that it is now a model of $t$ and the only $a$-derivative, which is $p'$, must be a model of $t'$. Consequently $(s',t') \in R$.

It follows directly from the definition of $R$ with $[\![S]\!]_{\text{sem}} \subseteq [\![T]\!]_{\text{sem}}$ that $(s_0,t_0) \in R$. □

[2] State $q$ allows independent progress if you combine the construction of $q$ with the second case for action $a$.

The restriction of the theorem to locally consistent specifications is not a serious one. As we shall see in Theorem 5, any consistent specification can be transformed into a locally consistent one preserving the set of implementations.

# 3 Consistency and conjunction

An *immediate error* occurs in a state of a specification if the specification disallows progress of time and output transitions in a given state – such a specification will break if the environment does not send an input. For a specification $S$ we define the set of immediate error states imerr as follows.

**Definition 10** *Given a specification* $S = (Q, q_0, Act, \rightarrow)$*, the set of* immediate error *states, denoted by* err*, is defined as*

$$\mathrm{imerr} = \Big\{ q \in Q \mid (\exists d \in \mathbb{R}_{\geq 0} : q \overset{d}{\not\longrightarrow}) \wedge \\ \forall d \in \mathbb{R}_{\geq 0} \forall o! \in Act_o \forall q' \in Q : q \overset{d}{\longrightarrow} q' \Rightarrow q' \overset{o!}{\not\longrightarrow} \Big\} .$$

It follows that no immediate error states can occur in implementations, or in locally consistent specifications. Error states can also be created when output actions are disabled, for example by pruning away immediate error states, see Definition 12 below. Therefore, we extend the definition of immediate error states into error states err as follows.

**Definition 11** *Given a specification* $S = (Q, q_0, Act, \rightarrow)$ *and a set of states* $X \subseteq Q$*, the set of* error *states, denoted by* err*, is defined as*

$$\mathrm{err}(X) = \Big\{ q \in Q \mid (\exists d \in \mathbb{R}_{\geq 0} : q \overset{d}{\not\longrightarrow}) \wedge \forall d \in \mathbb{R}_{\geq 0} \forall o! \in Act_o \forall q' \in Q : \\ q \overset{d}{\longrightarrow} q' \Rightarrow (q' \overset{o!}{\not\longrightarrow} \vee \forall q'' \in Q : q' \overset{o!}{\longrightarrow} q'' \Rightarrow q'' \in X) \Big\} .$$

Note that $\mathrm{err}(\emptyset) = \mathrm{imerr}$, thus for any $X$ we have that $\mathrm{imerr} \subseteq \mathrm{err}(X)$.

In general, error states in a specification do not necessarily mean that a specification cannot be implemented. Figure 6 shows a partially inconsistent specification, a version of the coffee machine that becomes inconsistent if it ever outputs tea. The inconsistency can be possibly avoided by some implementations, who would not implement delay or output transitions leading to it. More precisely an implementation will exist if there is a strategy for the output player in a safety game to avoid err. In order to be able to build on existing formalizations [12] we will consider a dual reachability game, asking for a strategy of the input player to reach err. We first define a timed predecessor operator [11, 12, 24], which gives all the states that can delay into $X$

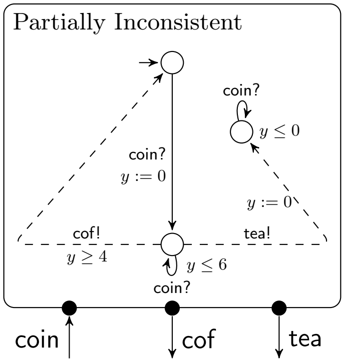



**Fig. 6**: A partially inconsistent specification.

while avoiding $Y$:

$$\text{cPred}_t^S(X,Y) = \left\{ q \in Q^S \mid \exists d \in \mathbb{R}_{\geq 0} \wedge \exists q' \in X \text{ s.t. } q \xrightarrow{d}{}^S q' \wedge \text{post}_d^S(q) \subseteq \overline{Y} \right\}.$$

Since $\text{post}_d^S(q)$ is defined on an open interval, we have that $X \cap Y \subseteq \text{cPred}_t^S(X,Y)$. This means that the input player has priority over the output player when both could do an action from a state. The controllable predecessors operator, denoted by $\pi^S(X)$, which extends the set of states that can reach an error state uncontrollably, is defined by

$$\pi^S(X) = \text{err}^S(X) \cup \text{cPred}_t^S(X \cup \text{ipred}^S(X), \text{opred}^S(\overline{X})).$$

The set of all inconsistent states $\text{incons}^S \subseteq Q^S$ of specification $S$ (i.e. the states for which the environment has a winning strategy for reaching an error state) is defined as the least fixpoint of $\pi^S$: $\text{incons}^S = \pi^S(\text{incons}^S)$, which is guaranteed to exist by monotonicity of $\pi^S$ and completeness of the powerset lattice due to the theorem of Knaster and Tarski [25]. For transitions systems enjoying finite symbolic representations, automata specifications included, the fixpoint computation converges after a finite number of iterations [12].

Now we define the set of consistent states, $\text{cons}^S$, simply as the complement of $\text{incons}^S$, i.e. $\text{cons}^S = \overline{\text{incons}^S}$. We obtain it by complementing the result of the above fixpoint computation for $\text{incons}^S$. For the purpose of proofs it is more convenient to formalize the dual operator, say $\Theta^S$, whose *greatest* fixpoint directly and equivalently characterizes $\text{cons}^S$. While least fixpoints are convenient for implementation of on-the-fly algorithms, characterizations with greatest fixpoint are useful in proofs as they allow use of coinduction. Unlike induction on the number of iterations, coinduction is a sound proof principle without assuming finite symbolic representation for the transition system (and thus finite convergence of the fixpoint computation). We define $\Theta^S$ as

$$\Theta^S(X) = \overline{\mathrm{err}^S(\overline{X})} \cap \Big\{ q \in Q^S \mid \forall d \geq 0 : [\forall q' \in Q^S : q \xrightarrow{d}{}^S q' \Rightarrow q' \in X \wedge \forall i? \in Act_i^S : \exists q'' \in X : q' \xrightarrow{i?}{}^S q''] \vee [\exists d' \leq d \wedge \exists q', q'' \in X \wedge \exists o! \in Act_o^S : q \xrightarrow{d'}{}^S q' \wedge q' \xrightarrow{o!}{}^S q'' \wedge \forall i? \in Act_i^S : \exists q''' \in X : q' \xrightarrow{i?}{}^S q'''] \Big\},$$

so the greatest fixpoint becomes $\mathrm{cons}^S = \Theta^S(\mathrm{cons}^S)$.

**Theorem 4** *A specification $S = (Q, s_0, Act, \rightarrow)$ is consistent iff $s_0 \in \mathrm{cons}$.*

*Proof* First, assume that $s_0 \in \mathrm{cons}^S$. Show that $S$ is consistent in the sense of Definition 8. In a similar fashion to the proof of Theorem 1 we first postulate existence of a function $\delta$, which chooses a delay and an output for every consistent state $s$:

$$\delta(s) = \begin{cases} d & \text{if } \exists s', s'' \in \mathrm{cons}^S : \text{ the infimum } d \text{ such that } s \xrightarrow{d}{}^S s' \\ & \text{and } \exists o! : s' \xrightarrow{o!}{}^S s'' \\ +\infty & \text{otherwise} \end{cases}$$

Note that $\delta$ is time additive in the following sense: if $s \xrightarrow{d}{}^S s'$ and $d \leq \delta(s)$ then $\delta(s') + d = \delta(s)$, which is due to time additivity of $\rightarrow^S$ and the fact that $\mathrm{cons}^S$ is a fixpoint of $\Theta^S$.

We show this by constructing an implementation $P = (Q^S, s_0, Act^S, \rightarrow^P)$ where the transition relation is the largest relation generated by the following rules:

1. $s \xrightarrow{o!}{}^P s'$ iff $s \xrightarrow{o!}{}^S s'$ and $s' \in \mathrm{cons}^S$ and $\delta_s = 0$,
2. $s \xrightarrow{i?}{}^P s'$ iff $s \xrightarrow{i?}{}^S s'$,
3. $s \xrightarrow{d}{}^P s'$ iff $s \xrightarrow{d}{}^S s'$ and $d \leq \delta_s$.

Observe that the construction of $P$ is essentially identical to the one in the proof of Theorem 1 above. It can be argued in almost the same way as in the above proof, that $P$ satisfies the axioms of TIOTSs and is an implementation. Here one has to use the definition of $\Theta^S$ in order to see that the side condition in the first rule, that is $s' \in \mathrm{cons}^S$, does not introduce a violation of independent progress.

It remains to argue that $P$ sat $S$. This is done by arguing that the following relation $R$

$$R = \Big\{ (p, s) \in Q^S \times Q^S \mid p = s \Big\}$$

witnesses the refinement of $S$ by $P$.

Consider now the other direction. Assume that $S$ is consistent and show that $s_0 \in \mathrm{cons}^S$. In the following we write that a state $s$ is consistent meaning that a specification would be consistent if $s$ was the initial state. Let $X = \{s \in Q^S \mid$

$s$ is consistent}. It suffices to show that $X$ is a post-fixed point of $\Theta^S$, thus $X \subseteq \Theta^S(X)$ (then $s_0 \in X = \mathrm{cons}^S$).

Since $s$ is consistent, let us consider an implementation $P$ and a state $p$ such that $p \,\mathrm{sat}\, s$. We will show that $s \in \Theta^S(X)$. Consider an arbitrary $d \geq 0$ and the first disjunct in the definition of $\Theta^S$. If $p \xrightarrow{d}{}^P p^d$ then also $s \xrightarrow{d}{}^S s^d$ and $p^d$ sat $s^d$, so $s^d \in X$. Consider an arbitrary input $i?$ such that $s^d \xrightarrow{i?}{}^S s'$. Then also $p^d \xrightarrow{i?}{}^P p'$ and $p'$ sat $s'$ (by satisfaction). But then $s' \in X$. So by the first disjunct of definition of $\Theta^S$ we have that $s \in \Theta^S(X)$.

If $p \not\xrightarrow{d}{}^P$ for our fixed value of $d$, then by independent progress of $p$ there exists a $d_{\max} < d$ such that $p \xrightarrow{d_{\max}}{}^P p'$ for some $p'$ and $p' \xrightarrow{o!}{}^P p''$ for some $p''$ and some output $o!$. By $p \,\mathrm{sat}\, s$ there also exist $s'$ and $s''$ such that $s \xrightarrow{d_{\max}}{}^S s'$ and $s' \xrightarrow{o!}{}^S s''$. Moreover $p''$ sat $s''$, so $s'' \in X$, which by the second disjunct in the definition of $\Theta^S$ implies that $s \in \Theta^S(X)$.

So we conclude that $X$ is a fixpoint of $\Theta^S$. Since $s_0$ is consistent by assumption, then $s_0 \in X \subseteq \mathrm{cons}^S$. □

The set of (in)consistent states can be computed for timed games, and thus for specification automata, using controller synthesis algorithms [12]. We discuss it briefly in Section 6.

The inconsistent states can be pruned from a consistent $S$ leading to a locally consistent specification. Adversarial pruning is applied in practice to decrease the size of specifications.

**Definition 12** *Given a specification $S = (Q, q_0, Act, \rightarrow)$, the result of* adversarial pruning, *denoted by $S^\Delta$, is specification* $(\mathrm{cons}, q_0, Act, \rightarrow^\Delta)$ *where* $\rightarrow^\Delta = \rightarrow \cap (\mathrm{cons} \times (Act \cup \mathbb{R}_{\geq 0}) \times \mathrm{cons})$.

For specification automata adversarial pruning is realized by applying a controller synthesis algorithm, obtaining a maximum winning strategy, which is then presented as a specification automaton itself. Theorem 5 captures the main result of adversarial pruning. It also explains the reason of the name of adversarial pruning: the pruned specification contains all winning strategies independently of an environment, including those that are adversarial. This contrasts with cooperative pruning, which we define in Section 4 later in the paper.

**Theorem 5** *For a consistent specification $S$, $S^\Delta$ is locally consistent and* $[\![S]\!]_{\mathrm{mod}} = [\![S^\Delta]\!]_{\mathrm{mod}}$.

*Proof* We first proof that $S^\Delta$ is locally consistent. From Definitions 9 and 5 of local consistency and implementation, respectively, it follows that we have to show that $\forall q \in Q^{S^\Delta}$: either $\forall d \in \mathbb{R}_{\geq 0} : q \xrightarrow{d}{}^P$ or $\exists d \in \mathbb{R}_{\geq 0}, \exists o! \in Act_o$ s.t. $q \xrightarrow{d}{}^P q'$ and $q' \xrightarrow{o!}{}^P$. From Definition 12 of adversarial pruning it follows that $Q^{S^\Delta} = \mathrm{cons}$.

Consider a state $q \in \text{cons}$. From the definition of $\Theta$, it follows that $q \in \overline{\text{err}(\overline{\text{cons}})}$ and $q \in \{q_1 \in Q \mid \forall d \geq 0 : [\forall q_2 \in Q : q_1 \xrightarrow{d} q_2 \Rightarrow q_2 \in \text{cons} \wedge \forall i? \in Act_i : \exists q_3 \in \text{cons} : q_2 \xrightarrow{i?} q_3] \vee [\exists d' \leq d \wedge \exists q_2, q_3 \in \text{cons} \wedge \exists o! \in Act_o : q_1 \xrightarrow{d'} q_2 \wedge q_2 \xrightarrow{o!} q_3 \wedge \forall i? \in Act_i : \exists q_4 \in \text{cons} : q_2 \xrightarrow{i?} q_4]\}$. In case that the condition $[\exists d' \leq d \wedge \exists q_2, q_3 \in \text{cons} \wedge \exists o! \in Act_o : q_1 \xrightarrow{d'} q_2 \wedge q_2 \xrightarrow{o!} q_3 \wedge \forall i? \in Act_i : \exists q_4 \in \text{cons} : q_2 \xrightarrow{i?} q_4]$ holds for some $d$, then it follows immediately that $q$ allows independent progress. In the other case, i.e., there does not exists a $d$ such that $[\exists d' \leq d \wedge \exists q_2, q_3 \in \text{cons} \wedge \exists o! \in Act_o : q_1 \xrightarrow{d'} q_2 \wedge q_2 \xrightarrow{o!} q_3 \wedge \forall i? \in Act_i : \exists q_4 \in \text{cons} : q_2 \xrightarrow{i?} q_4]$ holds, it follows from the fact that $q \in \overline{\text{err}(\overline{\text{cons}})}$ and Definition 11 that $\forall d \in \mathbb{R}_{\geq 0} : q \xrightarrow{d}{}^P$, thus allowing independent progress.

We now show that $[\![S]\!]_{\text{mod}} = [\![S^\Delta]\!]_{\text{mod}}$. From Definition 7 it follows that $[\![S]\!]_{\text{mod}} = [\![S^\Delta]\!]_{\text{mod}}$ iff for all implementations $P$ it holds that $P \leq S \Leftrightarrow P \leq S^\Delta$.

($P \leq S \Rightarrow P \leq S^\Delta$) Consider an implementation $P$ such that $P \leq S$. This implies from Definition 6 of refinement that there exists a relation $R \subseteq Q^P \times Q^S$ witnessing the refinement. We will arguing that for any pair $(p, s) \in R$ it holds that $s \in \text{cons}$.

For this, consider the controllable predecessor operator $\pi$ and $\pi(\text{imerr})$ to understand what it exactly calculates with respect to the definition of a consistent specification. A state $q \in \pi(\text{imerr})$ is either directly an error state or it can first delay followed by an input action to reach an error state *without* encountering an output action preventing it reaching an error state. With other words, no implementation can prevent state $q$ from reaching an error state.

Now, denote $\pi^n(\text{err})$ the $n$-th iteration of the fixed-point calculation, i.e., $\pi^1(\text{imerr}) = \pi(\text{imerr})$, $\pi^2(\text{imerr}) = \pi(\pi(\text{imerr}))$, etc. Following the above reasoning about the effect of $\pi$ on the reachability of error states, we can formulate the following fixed-point invariant: for each $n$ and $q \in \pi^n(\text{err})$, there does not exists an implementation preventing $q$ from reaching an error state. Once the fixed-point $\text{incons} = \pi(\text{incons}) = \pi^N(\text{imerr})$ for some $N$ is reached, we know for all $q \in \overline{\text{incons}}$ that it cannot reach the fixed-point incons because either incons is just simply unreachable by any means or an implementation can prevent it from reaching it.

Consider a pair $(p, s) \in R$ where $s \in \text{incons}$. This means that specification $S$ cannot be prevented from reaching an error state $s'$. If we follow this path, we end up with pair $(p', s') \in R$. Now, $s'$ is an error state, which either cannot progress time indefinitely and do an output. But since $p'$ is a state from an implementation $P$, it has the independent progress property. Therefore, once the specification wants to do an output or (indefinite) delay, the second or third property from Definition 6 is violated. Therefore, we can conclude that for pair $(p, s) \in R$, $s \notin \text{incons}$, i.e., $s \in \text{cons}$. As the argument above does not rely on a specific state $s$ in $S$, it holds for all states $s \in Q^S$.

Now, we effectively have that $R \subseteq Q^P \times \text{cons}$, thus it follows from Definition 12 of adversarial pruning that $R$ is also a relation witnessing the refinement $P \leq S^\Delta$. As we considered an arbitrarily implementation $P$ refining $S$, it holds for all implementations $P$ refining $S$. Therefore, we conclude that $P \leq S \Leftarrow P \leq S^\Delta$.

($P \leq S \Leftarrow P \leq S^\Delta$) This case follows directly from the construction of $S^\Delta$ and the fact that $\text{cons} \subseteq Q^S$, i.e., for all implementations $P$ that refine $S^\Delta$, the binary relation $R \subseteq Q^P \times \text{cons}$ also witnesses the refinement of $P$ and $S$. □

Consistency guarantees realizability of a single specification. It is of further interest whether several specifications can be *simultaneously* met by the same component, without reaching error states of any of them. We formalize this notion by defining a logical conjunction for specifications.

**Definition 13** *Given two TIOTSs $S^i = (Q^i, q_0^i, Act^i, \rightarrow^i), i = 1,2$ where $Act_i^1 \cap Act_o^2 = \emptyset \wedge Act_o^1 \cap Act_i^2 = \emptyset$, the conjunction of $S^1$ and $S^2$, denoted by $S^1 \wedge S^2$, is TIOTS $(Q^1 \times Q^2, (q_0^1, q_0^2), Act, \rightarrow)$ where $Act = Act_i \uplus Act_o$ with $Act_i = Act_i^1 \cup Act_i^2$ and $Act_o = Act_o^1 \cup Act_o^2$, and $\rightarrow$ is defined as*

- $(q_1^1, q_1^2) \xrightarrow{a} (q_2^1, q_2^2)$ *if* $a \in Act^1 \cap Act^2$, $q_1^1 \xrightarrow{a}{}^1 q_2^1$, *and* $q_1^2 \xrightarrow{a}{}^2 q_2^2$
- $(q_1^1, q^2) \xrightarrow{a} (q_2^1, q^2)$ *if* $a \in Act^1 \setminus Act^2$, $q_1^1 \xrightarrow{a}{}^1 q_2^1$, *and* $q^2 \in Q^2$
- $(q^1, q_1^2) \xrightarrow{a} (q^1, q_2^2)$ *if* $a \in Act^2 \setminus Act^1$, $q_1^2 \xrightarrow{a}{}^2 q_2^2$, *and* $q^1 \in Q^1$
- $(q_1^1, q^2) \xrightarrow{d} (q_2^1, q^2)$ *if* $d \in \mathbb{R}_{\geq 0}$, $q_1^1 \xrightarrow{d}{}^1 q_2^1$, *and* $q_1^2 \xrightarrow{d}{}^2 q_2^2$

In general, a result of the conjunction may be locally inconsistent, or even inconsistent. To guarantee consistency, one could apply a consistency check to the result, checking if $(s_0, t_0) \in \text{cons}^{S \times T}$ and, possibly, adversarially pruning the inconsistent parts. Clearly conjunction is commutative and associative.

**Lemma 2** *For two specifications $S$, $T$, and their states $s$ and $t$, respectively, if there exists an implementation $P$ and its state $p$ such that simultaneously $p \,\text{sat}\, s$ and $p \,\text{sat}\, t$ then $(s,t) \in \text{cons}^{S \wedge T}$.*

*Proof* This is shown by arguing that the following set $X$ of states of $S \wedge T$ is a postfixed point of $\Theta$ (then $(s,t) \in X \subseteq \Theta(X) \subseteq \text{cons}^{S \wedge T}$):

$$X = \{(s,t) \mid \exists P : \exists p \in Q^P : p \,\text{sat}\, s \wedge p \,\text{sat}\, t\}.$$

This is done by checking that $X \subseteq \Theta(X)$. Take $(s,t) \in X$, show that $(s,t) \in \Theta(X)$. So consider an arbitrary $d_0 \geq 0$. We know that there exists state $p$ such that $p \,\text{sat}\, s$ and $p \,\text{sat}\, t$. Since $p$ is a state of an implementation it guarantees independent progress, so there exists a delay $d^p$ such that $p \xrightarrow{d^p}{}^P p'$ for some state $p'$. Now the proof is split in two cases, proceeding by coinduction.

- $d^p \leq d_0$ is used to show that $(s,t) \in \Theta(X)$ using a standard argument with the second disjunct in definition of $\Theta$ (namely that $p$ can delay and output leading to a refinement of successors of $s$ and $t$, which again will be in $X$).
- $d^p > d_0$ is used to show that $(s,t) \in \Theta(X)$ using the same kind of argument with the first disjunct in the definition of $\Theta$ (namely that then $p$ can delay $d_0$ time and by refinement for any input transition it can advanced to a state refining successors of $s$ and $t$, which are in $X$).

□

**Theorem 6** *For any locally consistent specifications $S$, $T$ and $U$ over the same alphabet:*

*1.* $S \wedge T \le S$ *and* $S \wedge T \le T$

*2.* $(U \le S)$ *and* $(U \le T)$ *implies* $U \le (S \wedge T)$

*3.* $[\![S \wedge T]\!]_{\text{mod}} = [\![S]\!]_{\text{mod}} \cap [\![T]\!]_{\text{mod}}$

*Proof* We will prove the four items separately.

1. We will prove that $S \wedge T$ refines $S$ (the other refinement is entirely symmetric). Let $S \wedge T = (Q^S \times Q^T, (s_0, t_0), Act, \rightarrow)$ constructed according to the definition of conjunction. We abbreviate the set of states of $S \wedge T$ as $Q^{S \wedge T}$. It is easy to see that the following relation on states of $S \wedge T$ and states of $T$ witnesses refinement of $S$ by $S \wedge T$:
$$R = \left\{((s_1, t), s_2) \in Q^{S \wedge T} \times Q^S \mid s_1 = s_2\right\}$$
The argument is standard, and it takes into account that $Q^{S \wedge T} = \text{cons}^{S \wedge T}$ is a fixpoint of $\Theta$. How $\Theta$ is taken into account is demonstrated in more detail in the proof for the next item.

2. Assume that $U \le S$ and $U \le T$. Then $U \le S \wedge T$. The first refinement is witnessed by some relation $R_1$, the second refinement by $R_2$. Then the third refinement is witnessed by the following relation $R \subseteq Q^U \times Q^{S \wedge T}$:
$$R = \left\{(u, (s, t)) \in Q^U \times \text{cons}^{S \wedge T} \mid (u, s) \in R_1 \wedge (u, t) \in R_2\right\}.$$
The argument that $R$ is a refinement is standard again, relying on the fact that $\text{cons}^{S \wedge T}$ is a fixed point of $\Theta$.
Consider an output case when $u \xrightarrow{o!}^U u'$ for some output $o!$ and the target state $u'$. Then $s \xrightarrow{o!}^S s'$ and $t \xrightarrow{o!}^T t'$ for some states $s'$ and $t'$ and $(u', s') \in R_1$ and $(u', t') \in R_2$. This means that $(s, t) \xrightarrow{o!}^{S \wedge T} (s', t')$. In order to finish the case we need to argue that $(s', t') \in Q^{S \wedge T} = \text{cons}^{S \wedge T}$. This follows from Lemma 2 since $U$, and thus $u'$, is locally consistent, and by transitivity any implementation satisfying $u'$ would be a common implementation of $s'$ and $t'$.
The case for delay is identical, while the case for inputs is unsurprising (since adversarial pruning in the computation of conjunction never removes input transitions from consistent to inconsistent states – there are no such transitions).

3. The 3rd statement follows from the above facts. First assume that $U$ is an implementation (and thus also a specification) such that $U \in [\![S \wedge T]\!]_{\text{mod}}$. This means that $U \le S \wedge T$. Using statement 1 and Lemma 1 we can extend this to $U \le S \wedge T \le S$. Therefore, $U \in [\![S]\!]_{\text{mod}}$. With the same argument we can also show $U \in [\![T]\!]_{\text{mod}}$, thus $U \in [\![S]\!]_{\text{mod}} \cap [\![T]\!]_{\text{mod}}$.
The reverse of the 3rd statement can be shown by assuming that $U \in [\![S]\!]_{\text{mod}} \cap [\![T]\!]_{\text{mod}}$. This implies that $U \le S$ and $U \le T$. Now, using statement 2 we have $U \le S \wedge T$, which concludes that $U \in [\![S \wedge T]\!]_{\text{mod}}$.

□

We turn our attention to syntactic representations again.

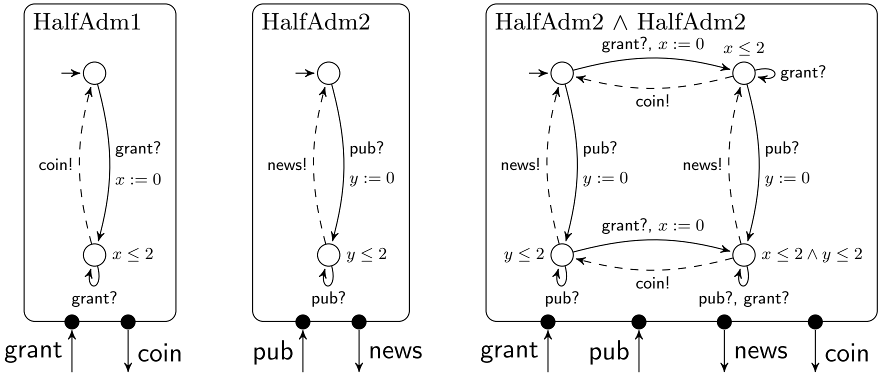



**Fig. 7**: Example of two specifications each handling one aspect of the administration and their conjunction.

**Definition 14** *Given two TIOAs* $A^i = (Loc^i, l_0^i, Act^i, Clk^i, E^i, Inv^i), i = 1, 2$ *where* $Act_i^1 \cap Act_o^2 = \emptyset \wedge Act_o^1 \cap Act_i^2 = \emptyset$[3]*, the* conjunction *of* $A^1$ *and* $A^2$*, denoted by* $A^1 \wedge A^2$*, is TIOA* $(Loc^1 \times Loc^2, (l_0^1, l_0^2), Act, Clk^1 \uplus Clk^2, E, Inv)$ *where* $Act = Act_i \uplus Act_o$ *with* $Act_i = Act_i^1 \cup Act_i^2$ *and* $Act_o = Act_o^1 \cup Act_o^2$*,* $Inv((l^1, l^2)) = Inv^1(l^1) \wedge Inv^2(l^2)$*, and* $E$ *is defined as*

- $((l_1^1, l_1^2), a, \varphi^1 \wedge \varphi^2, c^1 \cup c^2, (l_2^1, l_2^2)) \in E$ *if* $a \in Act^1 \cap Act^2$*,* $(l_1^1, a, \varphi^1, c^1, l_2^1) \in E^1$*, and* $(l_1^2, a, \varphi^2, c^2, l_2^2) \in E^2$
- $((l_1^1, l^2), a, \varphi^1, c^1, (l_2^1, l^2)) \in E$ *if* $a \in Act^1 \setminus Act^2$*,* $(l_1^1, a, \varphi^1, c^1, l_2^1) \in E^1$*, and* $l^2 \in Loc^2$
- $((l^1, l_1^2), a, \varphi^2, c^2, (l^1, l_2^2)) \in E$ *if* $a \in Act^2 \setminus Act^1$*,* $(l_1^2, a, \varphi^2, c^2, l_2^2) \in E^2$*, and* $l^1 \in Loc^1$

It might appear as if two systems can only advance on an input if both are ready to receive an input, but because of input enableness this is always the case. An example of a conjunction is shown in Figure 7. The two aspects of the administration, handing out coins and writing news articles, is split into two specifications. HalfAdm1 describes the alternation between grant? and coin!, while HalfAdm2 describes the alternation between pub? and news!. Together they form HalfAdm1 ∧ HalfAdm2. Observe that this is an alternative and slightly more loose specification of the administration than the one in Figure 1. Yet it is the case that Administration refines HalfAdm1 ∧ HalfAdm2, while the opposite is not true.

The following theorem lifts all the results from the TIOTSs level to the symbolic representation level:

**Theorem 7** *Given two TIOAs* $A^i = (Loc^i, l_0^i, Act^i, Clk^i, E^i, Inv^i), i = 1, 2$ *where* $Act_i^1 \cap Act_o^2 = \emptyset \wedge Act_o^1 \cap Act_i^2 = \emptyset$*. Then* $(\llbracket A^1 \wedge A^2 \rrbracket_{\text{sem}})^{\Delta} = (\llbracket A^1 \rrbracket_{\text{sem}} \wedge \llbracket A^2 \rrbracket_{\text{sem}})^{\Delta}$.

[3] Formulated differently, $\nexists a \in \bigcup_{i \in I} Act^i$ s.t. $a \in Act_i^i \wedge a \in Act_o^j, i, j \in I, i \neq j$ and $I = \{1, 2\}$. This is a more direct formulation of the desired property and can be extended easily for the conjunction of more than two TIOAs.

Before we can prove this theorem, we have to introduce several lemmas. The first lemma shows that the state set of $[\![A^1 \wedge A^2]\!]_{\text{sem}}$ and $[\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}}$ are the same, including the initial state.

**Lemma 3** *Given two TIOAs $A^i = (Loc^i, l_0^i, Act^i, Clk^i, E^i, Inv^i), i = 1, 2$ where $Act_i^1 \cap Act_o^2 = \emptyset \wedge Act_o^1 \cap Act_i^2 = \emptyset$. Then $Q^{[\![A^1 \wedge A^2]\!]_{\text{sem}}} = Q^{[\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}}}$ and $q_0^{[\![A^1 \wedge A^2]\!]_{\text{sem}}} = q_0^{[\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}}}$.*

*Proof* For brevity, we write $X = [\![A^1 \wedge A^2]\!]_{\text{sem}}$, $Y = [\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}}$, and $Clk = Clk^1 \uplus Clk^2$ in the rest of this proof. Following Definition 3 of semantic of a TIOA, Definition 12 of adversarial pruning, Definition 13 of the conjunction for TIOTS, and Definition 14 of the conjunction for TIOA, the set of states of $X$ is $Q^X = (Loc^1 \times Loc^2) \times [Clk \mapsto \mathbb{R}_{\geq 0}] = Loc^1 \times Loc^2 \times [Clk \mapsto \mathbb{R}_{\geq 0}]$ and the set of states of $Y$ is $Q^Y = (Loc^1 \times [Clk^1 \mapsto \mathbb{R}_{\geq 0}]) \times (Loc^2 \times [Clk^2 \mapsto \mathbb{R}_{\geq 0}]) = Loc^1 \times Loc^2 \times [Clk \mapsto \mathbb{R}_{\geq 0}]$. Therefore, $Q^X = Q^Y$. Furthermore, it now also follows immediately from the same definitions that $q_0^X = q_0^Y$, as none of these definitions alter the initial location of a TIOA or initial state of a TIOTS. □

Lemmas 4 and 5 show that $[\![A^1 \wedge A^2]\!]_{\text{sem}}$ and $[\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}}$ mimic each other with delays and shared actions.

**Lemma 4** *Given two TIOAs $A^i = (Loc^i, l_0^i, Act^i, Clk^i, E^i, Inv^i), i = 1, 2$ where $Act_i^1 \cap Act_o^2 = \emptyset \wedge Act_o^1 \cap Act_i^2 = \emptyset$. Denote $X = [\![A^1 \wedge A^2]\!]_{\text{sem}}$ and $Y = [\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}}$, and let $d \in \mathbb{R}_{\geq 0}$ and $q_1, q_2 \in Q^X \cap Q^Y$. Then $q_1 \xrightarrow{d}^X q_2$ if and only if $q_1 \xrightarrow{d}^Y q_2$.*

*Proof* First, from Lemma 3 it follows that $Q^X = Q^Y$. Consider a delay $d \in \mathbb{R}_{\geq 0}$. For brevity, in the rest of this proof we write $Clk = Clk^1 \uplus Clk^2$, and $u^1$ and $u^2$ to indicate the part of a valuation $u$ of only the clocks of $A^1$ and $A^2$, respectively.

($\Rightarrow$) Assume that $\exists q_1, q_2 \in Q^X$ such that $q_1 \xrightarrow{d}^X q_2$. From Definition 3 of the semantic of a TIOA it follows that $q_1 = (l, v)$, $q_2 = (l, v + d)$, $l \in Loc^{A^1 \wedge A^2}$, $v \in [Clk \mapsto \mathbb{R}_{\geq 0}]$, $v + d \models Inv^{A^1 \wedge A^2}(l)$, and $\forall d' \in \mathbb{R}_{\geq 0}, d' < d : v + d' \models Inv^{A^1 \wedge A^2}(l)$. From Definition 14 of the conjunction for TIOA it follows that $l = (l^1, l^2)$, $l^1 \in Loc^1$, $l^2 \in Loc^2$, and $Inv^{A^1 \wedge A^2}(l) = Inv^1(l^1) \wedge Inv^2(l^2)$. Therefore, $v + d \models Inv^1(l^1) \wedge Inv^2(l^2)$, and thus $v + d \models Inv^1(l^1)$ and $v + d \models Inv^2(l^2)$. Similarly, $v + d' \models Inv^1(l^1) \wedge Inv^2(l^2)$, and thus $v + d' \models Inv^1(l^1)$ and $v + d' \models Inv^2(l^2)$. Because $Clk^1 \cap Clk^2 = \emptyset$, it follows that $v^1 + d \models Inv^1(l^1)$, $v^2 + d \models Inv^2(l^2)$, $v^1 + d' \models Inv^1(l^1)$, and $v^2 + d' \models Inv^2(l^2)$. Now, from Definition 3 of the semantic of a TIOA, it follows that $(l^1, v^1) \xrightarrow{d}^{[\![A^1]\!]_{\text{sem}}} (l^1, v^1 + d)$ and $(l^2, v^2) \xrightarrow{d}^{[\![A^2]\!]_{\text{sem}}} (l^2, v^2 + d)$. Finally, from Definition 13 of the conjunction for TIOTS, if follows that $(l^1, v^1, l^2, v^2) \xrightarrow{d}^Y (l^1, v^1 + d, l^2, v^2 + d)$. Again by using that $Clk^1 \cap Clk^2 = \emptyset$, we can rewrite the states: $(l^1, v^1, l^2, v^2) = (l^1, l^2, v) = q_1$ and $(l^1, v^1 + d, l^2, v^2 + d) = (l^1, l^2, v + d) = q_2$. Thus $q_1 \xrightarrow{d}^Y q_2$.

($\Leftarrow$) Assume that $\exists q_1, q_2 \in Q^Y$ such that $q_1 \xrightarrow{d}^Y q_2$. From Definition 13 of the conjunction for TIOTS it follows that $q_1 = (q_1^1, q_1^2)$, $q_2 = (q_2^1, q_2^2)$, $q_1^1, q_2^1 \in Q^{[\![A^1]\!]_{\mathrm{sem}}}$, $q_1^2, q_2^2 \in Q^{[\![A^2]\!]_{\mathrm{sem}}}$, $q_1^1 \xrightarrow{d}^{[\![A^1]\!]_{\mathrm{sem}}} q_2^1$, and $q_1^2 \xrightarrow{d}^{[\![A^2]\!]_{\mathrm{sem}}} q_2^2$. From Definition 3 of the semantic of a TIOA it follows that for $i = 1, 2$: $q_1^i = (l^i, v^i)$, $q_2^i = (l^i, v^i + d)$, $l^i \in Loc^i$, $v^i \in [Clk^i \mapsto \mathbb{R}_{\geq 0}]$, $v^i + d \models Inv^i(l^i)$, and $\forall d' \in \mathbb{R}_{\geq 0}, d' < d : v + d' \models Inv^i(l^i)$. Because $Clk^1 \cap Clk^2 = \emptyset$, it follows that for $i = 1, 2$: $v + d \models Inv^i(l^i)$ and $v + d' \models Inv^i(l^i)$. Now, from Definition 14 it follows that $Inv^{A^1 \wedge A^2}(l^1, l^2) = Inv^1(l^1) \wedge Inv^2(l^2)$. Thus we know that $v + d \models Inv^{A^1 \wedge A^2}((l^1, l^2))$ and $v + d' \models Inv^{A^1 \wedge A^2}((l^1, l^2))$. Therefore, using Definition 3 of the semantic of a TIOA, it follows that $(l^1, l^2, v) \xrightarrow{d}^X (l^1, l^2, v + d)$. Again by using that $Clk^1 \cap Clk^2 = \emptyset$, we can rewrite the states: $(l^1, l^2, v) = (l^1, v^1, l^2, v^2) = q_1$ and $(l^1, l^2, v + d) = (l^1, v^1 + d, l^2, v^2 + d) = q_2$. Thus $q_1 \xrightarrow{d}^X q_2$.

As the analysis above holds for any chosen $d \in \mathbb{R}_{\geq 0}$, it holds for all $d$. This concludes the proof. □

**Lemma 5** *Given two TIOAs $A^i = (Loc^i, l_0^i, Act^i, Clk^i, E^i, Inv^i), i = 1, 2$ where $Act_i^1 \cap Act_o^2 = \emptyset \wedge Act_o^1 \cap Act_i^2 = \emptyset$. Denote $X = [\![A^1 \wedge A^2]\!]_{\mathrm{sem}}$ and $Y = [\![A^1]\!]_{\mathrm{sem}} \wedge [\![A^2]\!]_{\mathrm{sem}}$, and let $a \in Act^1 \cap Act^2$ and $q_1, q_2 \in Q^X \cap Q^Y$. Then $q_1 \xrightarrow{a}^X q_2$ if and only if $q_1 \xrightarrow{a}^Y q_2$.*

*Proof* First, from Lemma 3 it follows that $Q^X = Q^Y$. For brevity, in the rest of this proof we write $Clk = Clk^1 \uplus Clk^2$, and $v^1$ and $v^2$ to indicate the part of a valuation $v$ of only the clocks of $A^1$ and $A^2$, respectively.

($\Rightarrow$) Assume a transition $q_1^X \xrightarrow{a} q_2^X$ in $X$. Following Definition 3 of the semantic, it follows that there exists an edge $(l_1, a, \varphi, c, l_2) \in E^{A^1 \wedge A^2}$ with $q_1^X = (l_1, v_1)$, $q_2^X = (l_2, v_2)$, $l_1, l_2 \in Loc^{A^1 \wedge A^2}$, $v_1, v_2 \in [Clk \mapsto \mathbb{R}_{\geq 0}]$, $v_1 \models \varphi$, $v_2 = v_1[r \mapsto 0]_{r \in c}$, and $v_2 \models Inv(l_2)$.

From Definition 14 of the conjunction for TIOA it follows that $(l_1^1, a, \varphi^1, c^1, l_2^1)$ is an edge in $A^1$ and $(l_1^2, a, \varphi^2, c^2, l_2^2)$ in $A^2$, $l_1 = (l_1^1, l_1^2)$, $l_2 = (l_2^1, l_2^2)$, $\varphi = \varphi^1 \wedge \varphi^2$, $c = c^1 \cup c^2$. Since $v_1 \models \varphi$, it holds that $v_1 \models \varphi^1$ and $v_1 \models \varphi^2$. Because $Clk^1 \cap Clk^2 = \emptyset$, it holds that $v_1^1 \models \varphi^1$ and $v_1^2 \models \varphi^2$. Also, since $v_2 = v_1[r \mapsto 0]_{r \in c}$, it holds that $v_2^1 = v_1^1[r \mapsto 0]_{r \in c^1}$ and $v_2^2 = v_1^2[r \mapsto 0]_{r \in c^2}$. Finally, because $Inv^{A^1 \wedge A^2}(l_2) = Inv^1(l_2^1) \wedge Inv^2(l_2^2)$ (see Definition 14) and $v_2 \models Inv^{A^1 \wedge A^2}(l_2)$, it follows that $v_2 \models Inv^1(l_2^1)$ and $v_2 \models Inv^2(l_2^2)$. Since $Clk^1 \cap Clk^2 = \emptyset$, it follows that $v_2^1 \models Inv^1(l_2^1)$ and $v_2^2 \models Inv^2(l_2^2)$.

Combining all the information about $A^1$, we have that $(l_1^1, a, \varphi^1, c^1, l_2^1)$ is an edge in $A^1$, $v_1^1 \models \varphi^1$, $v_2^1 = v_1^1[r \mapsto 0]_{r \in c^1}$, and $v_2^1 \models Inv^1(l_2^1)$. Therefore, from Definition 3 it follows that $(l_1^1, v_1^1) \xrightarrow{a} (l_2^1, v_2^1)$ is a transition in $[\![A^1]\!]_{\mathrm{sem}}$. Combining all the information about $A^2$, we have that $(l_1^2, a, \varphi^2, c^2, l_2^2)$ is an edge in $A^2$, $v_1^2 \models \varphi^2$, $v_2^2 = v_1^2[r \mapsto 0]_{r \in c^2}$, and $v_2^2 \models Inv^2(l_2^2)$. Therefore, from Definition 3 it follows that $(l_1^2, v_1^2) \xrightarrow{a} (l_2^2, v_2^2)$ is a transition in $[\![A^2]\!]_{\mathrm{sem}}$.

Now, from Definition 13 of the conjunction for TIOTS it follows that $((l_1^1, v_1^1), (l_1^2, v_1^2)) \xrightarrow{a} ((l_2^1, v_2^1), (l_2^2, v_2^2))$ is a transition in $[\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}}$. Because $\mathit{Clk}^1 \cap \mathit{Clk}^2 = \emptyset$, we can rearrange the states into $((l_1^1, v_1^1), (l_1^2, v_1^2)) = ((l_1^1, l_1^2), v_1) = q_1^X$ and $((l_2^1, v_2^1), (l_2^2, v_2^2)) = ((l_2^1, l_2^2), v_2) = q_2^X$. Thus, $q_1^X \xrightarrow{a} q_2^X$ is a transition in $[\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}} = Y$.

($\Leftarrow$) Assume a transition $q_1^Y \xrightarrow{a} q_2^Y$ in $Y$. From Definition 13 of the conjunction for TIOTS it follows that $q_1^{[\![A^1]\!]_{\text{sem}}} \xrightarrow{a} q_2^{[\![A^1]\!]_{\text{sem}}}$ is a transition in $[\![A^1]\!]_{\text{sem}}$ and $q_1^{[\![A^2]\!]_{\text{sem}}} \xrightarrow{a} q_2^{[\![A^2]\!]_{\text{sem}}}$ in $[\![A^2]\!]_{\text{sem}}$, $q_1^Y = (q_1^{[\![A^1]\!]_{\text{sem}}}, q_1^{[\![A^2]\!]_{\text{sem}}})$, and $q_2^Y = (q_2^{[\![A^1]\!]_{\text{sem}}}, q_2^{[\![A^2]\!]_{\text{sem}}})$. From Definition 3 of semantic it follows that there exists an edge $(l_1^1, a, \varphi^1, c^1, l_2^1) \in E^1$ with $q_1^{[\![A^1]\!]_{\text{sem}}} = (l_1^1, v_1^1)$, $q_2^{[\![A^1]\!]_{\text{sem}}} = (l_2^1, v_2^1)$, $l_1^1, l_2^1 \in \mathit{Loc}^1$, $v_1^1, v_2^1 \in [\mathit{Clk}^1 \mapsto \mathbb{R}_{\geq 0}]$, $v_1^1 \models \varphi^1$, $v_2^1 = v_1^1[r \mapsto 0]_{r \in c^1}$, and $v_2^1 \models \mathit{Inv}^1(l_2^1)$. Similarly, it follows from the same definition that there exists an edge $(l_1^2, a, \varphi^2, c^2, l_2^2) \in E^2$ with $q_1^{[\![A^2]\!]_{\text{sem}}} = (l_1^2, v_1^2)$, $q_2^{[\![A^2]\!]_{\text{sem}}} = (l_2^2, v_2^2)$, $l_1^2, l_2^2 \in \mathit{Loc}^2$, $v_1^2, v_2^2 \in [\mathit{Clk}^2 \mapsto \mathbb{R}_{\geq 0}]$, $v_1^2 \models \varphi^2$, $v_2^2 = v_1^2[r \mapsto 0]_{r \in c^2}$, and $v_2^2 \models \mathit{Inv}^2(l_2^2)$.

Now, from Definition 14 of the conjunction for TIOA, it follows that there exists an edge $((l_1^1, l_1^2), a, \varphi^1 \wedge \varphi^2, c^1 \cup c^2, (l_2^1, l_2^2))$ in $A^1 \wedge A^2$. Let $v_i, i = 1, 2$ be the valuations that combines the one from $A^1$ with the one from $A^2$, i.e. $\forall r \in \mathit{Clk}^1 : v_i(r) = v_i^1(r)$ and $\forall r \in \mathit{Clk}^2 : v_i(r) = v_i^2(r)$. Because $\mathit{Clk}^1 \cap \mathit{Clk}^2 = \emptyset$, it holds that $v_1 \models \varphi^1$ and $v_1 \models \varphi^2$, thus $v_1 \models \varphi^1 \wedge \varphi^2$; $v_2 = v_1[r \mapsto 0]_{r \in c^1 \cup c^2}$; and $v_2 \models \mathit{Inv}^1(l_2^1)$ and $v_2 \models \mathit{Inv}^2(l_2^2)$, thus $v_2 \models \mathit{Inv}^1(l_2^1) \wedge \mathit{Inv}^2(l_2^2)$.

From Definition 3 it now follows that $((l_1^1, l_1^2), v_1) \xrightarrow{a} ((l_2^1, l_2^2), v_2)$ is a transition in $[\![A^1 \wedge A^2]\!]_{\text{sem}}$. Because $\mathit{Clk}^1 \cap \mathit{Clk}^2 = \emptyset$, we can rearrange the states into $((l_1^1, l_1^2), v_1) = ((l_1^1, v_1^1), (l_1^2, v_1^2)) = q_1^Y$ and $((l_2^1, l_2^2), v_2) = ((l_2^1, v_2^1), (l_2^2, v_2^2)) = q_2^Y$. Thus, $q_1^Y \xrightarrow{a} q_2^Y$ is a transition in $[\![A^1 \wedge A^2]\!]_{\text{sem}} = Y$. □

Lemma 6 considers transitions in $[\![A^1 \wedge A^2]\!]_{\text{sem}}$ and $[\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}}$ labeled by non-shared actions. A special case of this lemma is captured with Corollary 1. Compared to Lemma 5, we can see that we need the additional condition $v_2 \models \mathit{Inv}^2(l_2)$ in order to show that transitions can be mimicked. A simple example demonstrating the necessity of this condition is shown in Figure 8. From two TIOA $A^1$ and $A^2$, the TIOTSs $[\![A^1 \wedge A^2]\!]_{\text{sem}}$ in (c) and $[\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}}$ in (e) are calculated. As can be seen, $[\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}}$ has an additional transition $(1, 4) \xrightarrow{a!} (2, 4)$, which is not present in $[\![A^1 \wedge A^2]\!]_{\text{sem}}$. The reason for this is that the location invariant $\mathit{Inv}(4) = \mathbf{F}$ is processed by the semantic operator before $[\![A^2]\!]_{\text{sem}}$ is combined with $[\![A^1]\!]_{\text{sem}}$ by the conjunction operator. Therefore, it is suddenly possible to reach location $(2, 4)$ with $a!$ in $[\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}}$. Looking at Lemma 6, we can see that the condition $v_2 \models \mathit{Inv}^2(l_2)$ is not satisfied for $q_2 = (l_2^1, l_2^2, v_2) = (2, 4)$, as $\mathit{Inv}^2(4) = \mathbf{F}$ and no valuation $v_2$ can satisfy a false invariant. So, the additional condition in the lemma 'remembers' the original invariant in case we first go to the semantic representation before we perform the conjunction operation.

**Lemma 6** *Given two TIOAs* $A^i = (\mathit{Loc}^i, l_0^i, \mathit{Act}^i, \mathit{Clk}^i, E^i, \mathit{Inv}^i), i = 1, 2$ *where* $\mathit{Act}_i^1 \cap \mathit{Act}_o^2 = \emptyset \wedge \mathit{Act}_o^1 \cap \mathit{Act}_i^2 = \emptyset$. *Denote* $X = [\![A^1 \wedge A^2]\!]_{\text{sem}}$ *and* $Y = [\![A^1]\!]_{\text{sem}} \wedge$

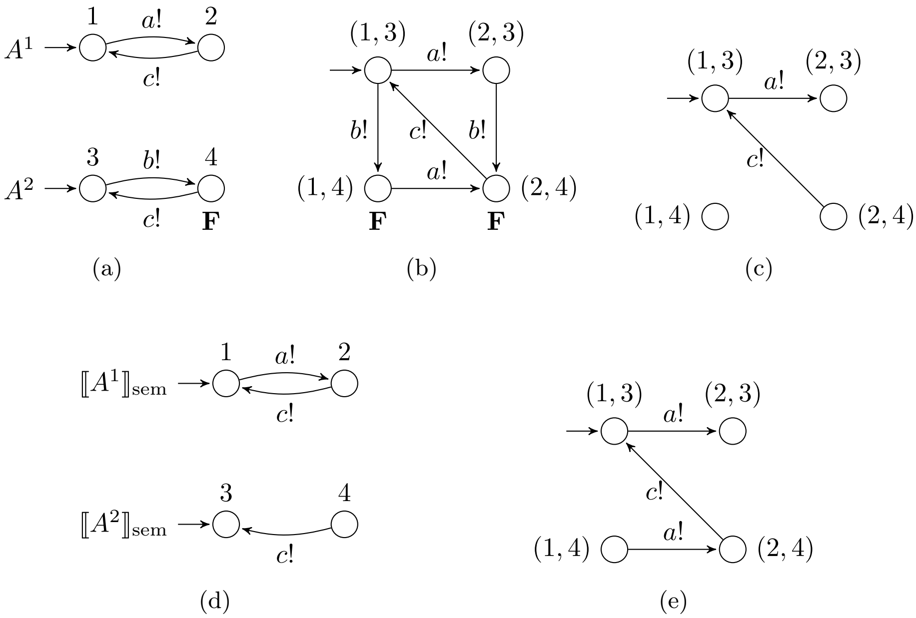



**Fig. 8**: Example demonstrating additional condition in Lemma 6. In (a) two TIOA $A^1$ and $A^2$ are shown, where location 4 has a **F** invariant. In (b) the conjunction $A^1 \wedge A^2$ is shown. In (c) the semantic representation $[\![A^1 \wedge A^2]\!]_{\text{sem}}$ is shown (ignoring the delays for simplicity). In (d) the semantic representations $[\![A^1]\!]_{\text{sem}}$ and $[\![A^2]\!]_{\text{sem}}$ are shown. And finally, in (e) the conjunction $[\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}}$ is shown.

*$[\![A^2]\!]_{\text{sem}}$, and let $a \in Act^1 \setminus Act^2$ and $q_1, q_2 \in Q^X \cap Q^Y$, where $q_2 = (l_2^1, l_2^2, v_2)$. If $v_2 \models Inv^2(l_2)$, then $q_1 \xrightarrow{a}{}^X q_2$ if and only if $q_1 \xrightarrow{a}{}^Y q_2$.*

*Proof* First, from Lemma 3 it follows that $Q^X = Q^Y$. For brevity, in the rest of this proof we write $Clk = Clk^1 \uplus Clk^2$, and $v^1$ and $v^2$ to indicate the part of a valuation $v$ of only the clocks of $A^1$ and $A^2$, respectively.

($\Rightarrow$) Assume a transition $q_1^X \xrightarrow{a} q_2^X$ in $X$. Following Definition 3 of the semantic, it follows that there exists an edge $(l_1, a, \varphi, c, l_2) \in E^{A^1 \wedge A^2}$ with $q_1^X = (l_1, v_1)$, $q_2^X = (l_2, v_2)$, $l_1, l_2 \in Loc^{A^1 \wedge A^2}$, $v_1, v_2 \in [Clk \mapsto \mathbb{R}_{\geq 0}]$, $v_1 \models \varphi$, $v_2 = v_1[r \mapsto 0]_{r \in c}$, and $v_2 \models Inv(l_2)$.

From Definition 14 of the conjunction for TIOA it follows that $(l_1^1, a, \varphi^1, c^1, l_2^1)$ is an edge in $A^1$, $l_1 = (l_1^1, l_1^2)$, $l_2 = (l_2^1, l_2^2)$, $l_1^2 = l_2^2 = l^2$, $\varphi = \varphi^1$, $c = c^1$. Since $v_1 \models \varphi$ and $Clk^1 \cap Clk^2 = \emptyset$, it holds that $v_1^1 \models \varphi^1$. Also, since $v_2 = v_1[r \mapsto 0]_{r \in c}$ and $c = c^1$, it holds that $v_2^1 = v_1^1[r \mapsto 0]_{r \in c^1}$ and $v_2^2 = v_1^2$. Finally, because $Inv^{A^1 \wedge A^2}(l_2) = Inv^1(l_2^1) \wedge Inv^2(l^2)$ (see Definition 14) and $v_2 \models Inv^{A^1 \wedge A^2}(l_2)$, it follows that $v_2 \models Inv^1(l_2^1)$ and $v_2 \models Inv^2(l^2)$[4]. Since $Clk^1 \cap Clk^2 = \emptyset$, it follows that $v_2^1 \models Inv^1(l_2^1)$ and $v_2^2 \models Inv^2(l^2)$.

Combining all the information about $A^1$, we have that $(l_1^1, a, \varphi^1, c^1, l_2^1)$ is an edge in $A^1$, $v_1^1 \models \varphi^1$, $v_2^1 = v_1^1[r \mapsto 0]_{r \in c^1}$, and $v_2^1 \models Inv^1(l_2^1)$. Therefore, from Definition 3 it follows that $(l_1^1, v_1^1) \xrightarrow{a} (l_2^1, v_2^1)$ is a transition in $[\![A^1]\!]_{\text{sem}}$. Combining all the information about $A^2$, we have that $v_1^2 = v_2^2$ and $v_2^2 \models Inv^2(l^2)$.

Now, from Definition 13 of the conjunction for TIOTS it follows that $((l_1^1, v_1^1), (l^2, v_1^2)) \xrightarrow{a} ((l_2^1, v_2^1), (l^2, v_1^2))$ is a transition in $[\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}}$. Because $Clk^1 \cap Clk^2 = \emptyset$, we can rearrange the states into $((l_1^1, v_1^1), (l^2, v_1^2)) = ((l_1^1, l^2), v_1) = q_1^X$ and $((l_2^1, v_2^1), (l^2, v_2^2)) = ((l_2^1, l^2), v_2) = q_2^X$. Thus, $q_1^X \xrightarrow{a} q_2^X$ is a transition in $[\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}} = Y$.

($\Leftarrow$) Assume a transition $q_1^Y \xrightarrow{a} q_2^Y$ in $Y$. From Definition 13 of the conjunction for TIOTS it follows that $q_1^{[\![A^1]\!]_{\text{sem}}} \xrightarrow{a} q_2^{[\![A^1]\!]_{\text{sem}}}$ is a transition in $[\![A^1]\!]_{\text{sem}}$, $q^{[\![A^2]\!]_{\text{sem}}} \in Q^{[\![A^2]\!]_{\text{sem}}}$, $q_1^Y = (q_1^{[\![A^1]\!]_{\text{sem}}}, q^{[\![A^2]\!]_{\text{sem}}})$, and $q_2^Y = (q_2^{[\![A^1]\!]_{\text{sem}}}, q^{[\![A^2]\!]_{\text{sem}}})$. From Definition 3 of semantic it follows that there exists an edge $(l_1^1, a, \varphi^1, c^1, l_2^1) \in E^1$ with $q_1^{[\![A^1]\!]_{\text{sem}}} = (l_1^1, v_1^1)$, $q_2^{[\![A^1]\!]_{\text{sem}}} = (l_2^1, v_2^1)$, $l_1^1, l_2^1 \in Loc^1$, $v_1^1, v_2^1 \in [Clk^1 \mapsto \mathbb{R}_{\geq 0}]$, $v_1^1 \models \varphi^1$, $v_2^1 = v_1^1[r \mapsto 0]_{r \in c^1}$, and $v_2^1 \models Inv^1(l_2^1)$. Similarly, it follows from the same definition that $q^{[\![A^2]\!]_{\text{sem}}} = (l^2, v^2)$, $l^2 \in Loc^2$, and $v^2 \in [Clk^2 \mapsto \mathbb{R}_{\geq 0}]$.

Now, from Definition 14 of the conjunction for TIOA, it follows that there exists an edge $((l_1^1, l^2), a, \varphi^1, c^1, (l_2^1, l^2))$ in $A^1 \wedge A^2$. Let $v_i, i = 1, 2$ be a valuation that combines the one from $A^1$ with the one from $A^2$, i.e. $\forall r \in Clk^1 : v_i(r) = v_i^1(r)$ and $\forall r \in Clk^2 : v_i(r) = v_i^2(r)$. Because $Clk^1 \cap Clk^2 = \emptyset$, it holds that $v_1 \models \varphi^1$; $v_2 = v_1[r \mapsto 0]_{r \in c^1}$ with $v_1^2 = v_2^2$; and $v_2 \models Inv^1(l_2^1)$. As the antecedent states that $v_2 \models Inv^2(l^2)$, it follows that $v^2 \models Inv(l_2^1) \wedge Inv(l^2)$.

From Definition 3 it now follows that $((l_1^1, l^2), v_1) \xrightarrow{a} ((l_2^1, l^2), v_2)$ is a transition in $[\![A^1 \wedge A^2]\!]_{\text{sem}}$. Because $Clk^1 \cap Clk^2 = \emptyset$, we can rearrange the states into $((l_1^1, l^2), v_1) = ((l_1^1, v_1^1), (l^2, v_1^2)) = q_1^Y$ and $((l_2^1, l^2), v_2) = ((l_2^1, v_2^1), (l^2, v_2^2)) = q_2^Y$. Thus, $q_1^Y \xrightarrow{a} q_2^Y$ is a transition in $[\![A^1 \wedge A^2]\!]_{\text{sem}} = Y$. □

**Corollary 1** *Given two TIOAs* $A^i = (Loc^i, l_0^i, Act^i, Clk^i, E^i, Inv^i), i = 1, 2$ *where* $Act_i^1 \cap Act_o^2 = \emptyset \wedge Act_o^1 \cap Act_i^2 = \emptyset$. *Denote* $X = [\![A^1 \wedge A^2]\!]_{\text{sem}}$ *and* $Y = [\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}}$, *and let* $a \in Act^1 \backslash Act^2$ *and* $q_1, q_2 \in Q^X \cap Q^Y$. *If* $q_1 \xrightarrow{a}^X q_2$, *then* $q_1 \xrightarrow{a}^Y q_2$.

*Proof* First, from Lemma 3 it follows that $Q^X = Q^Y$. For brevity, in the rest of this proof we write $Clk = Clk^1 \uplus Clk^2$, and $v^1$ and $v^2$ to indicate the part of a valuation $v$ of only the clocks of $A^1$ and $A^2$, respectively.

Following Definition 3 of the semantic, it follows that there exists an edge $(l_1, a, \varphi, c, l_2) \in E^{A^1 \wedge A^2}$ with $q_1^X = (l_1, v_1)$, $q_2^X = (l_2, v_2)$, $l_1, l_2 \in Loc^{A^1 \wedge A^2}$, $v_1, v_2 \in [Clk \mapsto \mathbb{R}_{\geq 0}]$, $v_1 \models \varphi$, $v_2 = v_1[r \mapsto 0]_{r \in c}$, and $v_2 \models Inv(l_2)$. From Definition 14 of the conjunction for TIOA it follows that $l_1 = (l_1^1, l_1^2)$, $l_2 = (l_2^1, l_2^2)$, $l_1^2 = l_2^2 = l^2$, and $Inv^{A^1 \wedge A^2}(l_2) = Inv^1(l_2^1) \wedge Inv^2(l^2)$. Since $v_2 \models Inv^{A^1 \wedge A^2}(l_2)$, it follows that $v_2 \models Inv^1(l_2^1)$ and $v_2 \models Inv^2(l^2)$.

It now follows directly from Lemma 6 that $q_1 \xrightarrow{a}^Y q_2$. □

[4]So the if condition in the lemma is always satisfied once we know that $q_1 \xrightarrow{a}^X q_2$ is a transition in $X$. We formalize this in Corollary 1.

The following two lemmas consider the error states and consistent states, respectively, in $[\![A^1 \wedge A^2]\!]_{\text{sem}}$ and $[\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}}$. We can show that both sets are the same for $[\![A^1 \wedge A^2]\!]_{\text{sem}}$ and $[\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}}$.

**Lemma 7** *Given two TIOAs* $A^i = (Loc^i, l_0^i, Act^i, Clk^i, E^i, Inv^i), i = 1, 2$ *where* $Act_i^1 \cap Act_o^2 = \emptyset \wedge Act_o^1 \cap Act_i^2 = \emptyset$. *Let* $Q \subseteq Loc^1 \times Loc^2 \times [(Clk^1 \cup Clk^2) \mapsto \mathbb{R}_{\geq 0}]$. *Then* $\text{err}^{[\![A^1 \wedge A^2]\!]_{\text{sem}}}(Q) = \text{err}^{[\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}}}(Q)$.

*Proof* It follows from Lemma 3 that $[\![A^1 \wedge A^2]\!]_{\text{sem}}$ and $[\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}}$ have the same state set. We will show that $\text{err}^{[\![A^1 \wedge A^2]\!]_{\text{sem}}}(Q) \subseteq \text{err}^{[\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}}}(Q)$ and $\text{err}^{[\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}}}(Q) \subseteq \text{err}^{[\![A^1 \wedge A^2]\!]_{\text{sem}}}(Q)$. For brevity, we write $X = [\![A^1 \wedge A^2]\!]_{\text{sem}}$, $Y = [\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}}$, and $Clk = Clk^1 \uplus Clk^2$ in the rest of this proof. Also, we will use $v^1$ and $v^2$ to indicate the part of a valuation $v$ of only the clocks of $A^1$ and $A^2$, respectively.

($\text{err}^X(Q) \subseteq \text{err}^Y(Q)$) Consider a state $q^X \in \text{err}^X(Q)$. From Definition 11 of error states we know that $\exists d \in \mathbb{R}_{\geq 0}$ s.t. $q^X \stackrel{d}{\not\longrightarrow}{}^X$ and $\forall d' \in \mathbb{R}_{\geq 0} \forall o! \in Act_o \forall q_2 \in Q^X : q^X \xrightarrow{d'} q_2 \Rightarrow (q_2 \stackrel{o!}{\not\longrightarrow}{}^X \vee \forall q_3 \in Q^X : q_2 \xrightarrow{o!}{}^X q_3 \Rightarrow q_3 \in Q)$. From Definition 3 of the semantic of a TIOA it follows that $q^X = (l_1, v)$ for some $l_1 \in Loc^{A^1 \wedge A^2}$ and $v \in [Clk \mapsto \mathbb{R}_{\geq 0}]$, $v + d \not\models Inv^{A^1 \wedge A^2}(l_1)$, and $v + d' \models Inv^{A^1 \wedge A^2}(l_1) \implies [\nexists (l_1, o!, \varphi, c, l_3) \in E^{A^1 \wedge A^2} \vee \forall (l_1, o!, \varphi, c, l_3) \in E^{A^1 \wedge A^2} : v + d' \not\models \varphi \vee v + d'[r \mapsto 0]_{r \in c} \not\models Inv^{A^1 \wedge A^2}(l_3) \vee (l_3, v + d'[r \mapsto 0]_{r \in c}) \in Q]$.

From Lemma 4 it follows immediately that $q^X \stackrel{d}{\not\longrightarrow}{}^X$ implies that $q^X \stackrel{d}{\not\longrightarrow}{}^Y$. So the first condition in the definition of error states holds for $q^X$ in $Y$.

Now, pick any $d'$, $q_2$, and $o!$ such that $v + d' \models Inv^{A^1 \wedge A^2}(l_1) \implies [\nexists (l_1, o!, \varphi, c, l_3) \in E^{A^1 \wedge A^2} \vee \forall (l_1, o!, \varphi, c, l_3) \in E^{A^1 \wedge A^2} : v + d' \not\models \varphi \vee v + d'[r \mapsto 0]_{r \in c} \not\models Inv^{A^1 \wedge A^2}(l_3) \vee (l_3, v + d'[r \mapsto 0]_{r \in c}) \in Q]$. The implication holds if $v + d' \not\models Inv^{A^1 \wedge A^2}(l_1)$ or $v + d' \models Inv^{A^1 \wedge A^2}(l_1) \wedge [\nexists (l_1, o!, \varphi, c, l_3) \in E^{A^1 \wedge A^2} \vee \forall (l_1, o!, \varphi, c, l_3) \in E^{A^1 \wedge A^2} : v + d' \not\models \varphi \vee v + d'[r \mapsto 0]_{r \in c} \not\models Inv^{A^1 \wedge A^2}(l_3) \vee (l_3, v + d'[r \mapsto 0]_{r \in c}) \in Q]$. The first case follows directly from Lemma 4 that shows that $q^X \stackrel{d'}{\not\longrightarrow}{}^Y$, which ensures that the second condition in the definition of error states holds for $q^X$ in $Y$. For the second case we again use Lemma 4, thus $q^X \xrightarrow{d'}{}^Y q_2$, where $q_2 = (l_1, v + d')$. Now consider the two cases in the right-hand side of the implication.

- $\nexists (l_1, o!, \varphi, c, l_3) \in E^{A^1 \wedge A^2}$. We have to consider the three cases from Definition 14 of the conjunction for TIOA.
  - $o! \in Act^1 \cap Act^2$. In this case, we know that $\nexists (l_1^1, o!, \varphi^1, c^1, l_3^1) \in E^1$ or $\nexists (l_1^2, o!, \varphi^2, c^2, l_3^2) \in E^2$ (or both). Therefore, it follows from Definition 3 of the semantic of a TIOA that $(l_1^1, v^1 + d') \stackrel{o!}{\not\longrightarrow}{}^{[\![A^1]\!]_{\text{sem}}}$ or $(l_1^2, v^2 + d') \stackrel{o!}{\not\longrightarrow}{}^{[\![A^2]\!]_{\text{sem}}}$ (or both). Now, from Definition 13 of the conjunction for TIOTS it follows that $((l_1^1, v^1 + d'), (l_1^2, v^2 + d')) \stackrel{o!}{\not\longrightarrow}{}^Y$[5].

[5]Alternatively, we could use Lemma 5 to come to the same conclusion. This also holds for the other two cases, where we have to use Corollary 1 instead.

– $o! \in \mathit{Act}^1 \setminus \mathit{Act}^2$. In this case, we know that $\nexists(l_1^1, o!, \varphi^1, c^1, l_3^1) \in E^1$. Therefore, it follows from Definition 3 of the semantic of a TIOA that $(l_1^1, v^1 + d') \overset{o!}{\not\longrightarrow}{}^{[\![A^1]\!]_{\text{sem}}}$. Now, from Definition 13 of the conjunction for TIOTS it follows that $((l_1^1, v^1 + d'), (l_1^2, v^2 + d')) \overset{o!}{\not\longrightarrow}{}^{Y}$.

– $o! \in \mathit{Act}^2 \setminus \mathit{Act}^1$. In this case, we know that $\nexists(l_1^2, o!, \varphi^2, c^2, l_3^2) \in E^2$. Therefore, it follows from Definition 3 of the semantic of a TIOA that $(l_1^2, v^2 + d') \overset{o!}{\not\longrightarrow}{}^{[\![A^2]\!]_{\text{sem}}}$. Now, from Definition 13 of the conjunction for TIOTS it follows that $((l_1^1, v^1 + d'), (l_1^2, v^2 + d')) \overset{o!}{\not\longrightarrow}{}^{Y}$.

So, in all three cases we can show that $((l_1^1, v^1 + d'), (l_1^2, v^2 + d')) \overset{o!}{\not\longrightarrow}{}^{Y}$. And note that $((l_1^1, v^1 + d'), (l_1^2, v^2 + d')) = q_2$.

- $\forall (l_1, o!, \varphi, c, l_3) \in E^{A^1 \wedge A^2} : v + d' \not\models \varphi \vee v + d'[r \mapsto 0]_{r \in c} \not\models \mathit{Inv}^{A^1 \wedge A^2}(l_3) \vee (l_3, v + d'[r \mapsto 0]_{r \in c}) \in Q$. For each edge $(l_1, o!, \varphi, c, l_3) \in E^{A^1 \wedge A^2}$, we have to consider the three cases from Definition 14 of the conjunction for TIOA.
  – $o! \in \mathit{Act}^1 \cap \mathit{Act}^2$. In this case, we know that $(l_1^1, o!, \varphi^1, c^1, l_3^1) \in E^1$, $(l_1^2, o!, \varphi^2, c^2, l_3^2) \in E^2$, $\varphi = \varphi^1 \wedge \varphi^2$, and $c = c^1 \cup c^2$. Now consider the three cases that should hold for each edge $(l_1, o!, \varphi, c, l_3) \in E^{A^1 \wedge A^2}$.
    * $v + d' \not\models \varphi$. In this case, we know that $v + d' \not\models \varphi$ implies that $v + d' \not\models \varphi^1$ or $v + d' \not\models \varphi^2$ (or both). Because $\mathit{Clk}^1 \cap \mathit{Clk}^2 = \emptyset$, it holds that $v^1 + d' \not\models \varphi^1$ or $v^2 + d' \not\models \varphi^2$ (or both). Therefore, it follows from Definition 3 of the semantic of a TIOA that $(l_1^1, v^1 + d') \overset{o!}{\not\longrightarrow}{}^{[\![A^1]\!]_{\text{sem}}}$ or $(l_1^2, v^2 + d') \overset{o!}{\not\longrightarrow}{}^{[\![A^2]\!]_{\text{sem}}}$ (or both). Now, from Definition 13 of the conjunction for TIOTS it follows that $((l_1^1, v^1 + d'), (l_1^2, v^2 + d')) \overset{o!}{\not\longrightarrow}{}^{Y}$.
    * $v + d'[r \mapsto 0]_{r \in c} \not\models \mathit{Inv}^{A^1 \wedge A^2}(l_3)$. In this case, we know that $v + d'[r \mapsto 0]_{r \in c} \not\models \mathit{Inv}^{A^1 \wedge A^2}(l_3)$ implies that $v + d'[r \mapsto 0]_{r \in c} \not\models \mathit{Inv}^1(l_3^1)$ or $v + d'[r \mapsto 0]_{r \in c} \not\models \mathit{Inv}^2(l_3^2)$ (or both). Because $\mathit{Clk}^1 \cap \mathit{Clk}^2 = \emptyset$, it holds that $v^1 + d'[r \mapsto 0]_{r \in c^1} \not\models \mathit{Inv}^1(l_3^1)$ or $v^2 + d'[r \mapsto 0]_{r \in c^2} \not\models \mathit{Inv}^2(l_3^2)$ (or both). Therefore, it follows from Definition 3 of the semantic of a TIOA that $(l_1^1, v^1 + d') \overset{o!}{\not\longrightarrow}{}^{[\![A^1]\!]_{\text{sem}}}$ or $(l_1^2, v^2 + d') \overset{o!}{\not\longrightarrow}{}^{[\![A^2]\!]_{\text{sem}}}$ (or both). Now, from Definition 13 of the conjunction for TIOTS it follows that $((l_1^1, v^1 + d'), (l_1^2, v^2 + d')) \overset{o!}{\not\longrightarrow}{}^{Y}$.
    * $(l_3, v + d'[r \mapsto 0]_{r \in c}) \in Q$. In this case, assume that $v + d' \models \varphi$ and $v + d[r \mapsto 0]_{r \in c} \models \mathit{Inv}^{A^1 \wedge A^2}(l_3)$ (otherwise, one of the above cases can be used instead). Because $\mathit{Clk}^1 \cap \mathit{Clk}^2 = \emptyset$, it follows that $v^1 + d' \models \varphi^1$, $v^2 + d' \models \varphi^2$, $v^1 + d'[r \mapsto 0]_{r \in c^1} \models \mathit{Inv}^1(l_3^1)$, and $v^2 + d'[r \mapsto 0]_{r \in c^2} \models \mathit{Inv}^2(l_3^2)$. Therefore, it follows from Definition 3 of the semantic of a TIOA that $(l_1^1, v^1 + d') \xrightarrow{o!}{}^{[\![A^1]\!]_{\text{sem}}} (l_3^1, v^1 + d'[r \mapsto 0]_{r \in c^1})$ and $(l_1^2, v^2 + d') \xrightarrow{o!}{}^{[\![A^2]\!]_{\text{sem}}} (l_3^2, v^2 + d'[r \mapsto 0]_{r \in c^2})$. Now, from Definition 13 of the conjunction for TIOTS it follows that $((l_1^1, v^1 + d'), (l_1^2, v^2 + d')) \xrightarrow{o!}{}^{Y} ((l_3^1, v^1 + d'[r \mapsto 0]_{r \in c^1}), (l_3^2, v^2 + d'[r \mapsto 0]_{r \in c^2}))$. And note that $((l_3^1, v^1 + d'[r \mapsto 0]_{r \in c^1}), (l_3^2, v^2 + d'[r \mapsto 0]_{r \in c^2})) = (l_3^1, l_3^2, v + d'[r \mapsto 0]_{r \in c}) = (l_3, v + d'[r \mapsto 0]_{r \in c})$.

So, in the first two cases we have shown that $((l_1^1, v^1+d'), (l_1^2, v^2+d')) \overset{o!}{\not\longrightarrow}_Y$ [6] and in the third case that $((l_1^1, v^1+d'), (l_1^2, v^2+d')) \xrightarrow{o!}^Y (l_3, v+d'[r \mapsto 0]_{r\in c})$.

- $o! \in Act^1 \setminus Act^2$. In this case, we know that $(l_1^1, o!, \varphi^1, c^1, l_3^1) \in E^1$, $\varphi = \varphi^1$, and $c = c^1$. Now consider the three cases that should hold for each edge $(l_1, o!, \varphi, c, l_3) \in E^{A^1 \wedge A^2}$.
  * $v + d' \not\models \varphi$. In this case, we know that $v + d' \not\models \varphi$ implies that $v + d' \not\models \varphi^1$. Because $Clk^1 \cap Clk^2 = \emptyset$, it holds that $v^1 + d' \not\models \varphi^1$. Therefore, it follows from Definition 3 of the semantic of a TIOA that $(l_1^1, v^1+d') \overset{o!}{\not\longrightarrow}{}^{[\![A^1]\!]_{\text{sem}}}$. Now, from Definition 13 of the conjunction for TIOTS it follows that $((l_1^1, v^1+d'), (l_1^2, v^2+d')) \overset{o!}{\not\longrightarrow}{}^Y$.
  * $v + d[r \mapsto 0]_{r\in c} \not\models Inv^{A^1 \wedge A^2}(l_3)$. In this case, we know that $v + d[r \mapsto 0]_{r\in c} \not\models Inv^{A^1 \wedge A^2}(l_3)$ implies that $v + d[r \mapsto 0]_{r\in c} \not\models Inv^1(l_3^1)$. Because $Clk^1 \cap Clk^2 = \emptyset$, it holds that $v^1 + d[r \mapsto 0]_{r\in c^1} \not\models Inv^1(l_3^1)$. Therefore, it follows from Definition 3 of the semantic of a TIOA that $(l_1^1, v^1+d') \overset{o!}{\not\longrightarrow}{}^{[\![A^1]\!]_{\text{sem}}}$. Now, from Definition 13 of the conjunction for TIOTS it follows that $((l_1^1, v^1+d'), (l_1^2, v^2+d')) \overset{o!}{\not\longrightarrow}{}^Y$.
  * $(l_3, v + d'[r \mapsto 0]_{r\in c}) \in Q$. In this case, assume that $v + d' \models \varphi$ and $v + d[r \mapsto 0]_{r\in c} \models Inv^{A^1 \wedge A^2}(l_3)$ (otherwise, one of the above cases can be used instead). Because $Clk^1 \cap Clk^2 = \emptyset$, it follows that $v^1 + d' \models \varphi^1$ and $v^1 + d'[r \mapsto 0]_{r\in c^1} \models Inv^1(l_3^1)$. Therefore, it follows from Definition 3 of the semantic of a TIOA that $(l_1^1, v^1+d') \xrightarrow{o!}{}^{[\![A^1]\!]_{\text{sem}}} (l_3^1, v^1 + d'[r \mapsto 0]_{r\in c^1})$. Now, from Definition 13 of the conjunction for TIOTS it follows that $((l_1^1, v^1+d'), (l_1^2, v^2+d')) \xrightarrow{o!}{}^Y ((l_3^1, v^1+d'[r \mapsto 0]_{r\in c^1}), (l_1^2, v^2+d'))$. And note that $((l_3^1, v^1+d'[r \mapsto 0]_{r\in c^1}), (l_1^2, v^2+d')) = (l_3^1, l_1^2, v+d'[r \mapsto 0]_{r\in c}) = (l_3, v+d'[r \mapsto 0]_{r\in c})$.

  So, in the first two cases we have shown that $((l_1^1, v^1+d'), (l_1^2, v^2+d')) \overset{o!}{\not\longrightarrow}{}^Y$ and in the third case that $((l_1^1, v^1+d'), (l_1^2, v^2+d')) \xrightarrow{o!}{}^Y (l_3, v+d'[r \mapsto 0]_{r\in c})$.
- $o! \in Act^2 \setminus Act^1$. In this case, we know that $(l_1^2, o!, \varphi^2, c^2, l_3^2) \in E^2$, $\varphi = \varphi^2$, and $c = c^2$. Now consider the three cases that should hold for each edge $(l_1, o!, \varphi, c, l_3) \in E^{A^1 \wedge A^2}$.
  * $v + d' \not\models \varphi$. In this case, we know that $v + d \not\models \varphi$ implies that $v + d' \not\models \varphi^2$. Because $Clk^1 \cap Clk^2 = \emptyset$, it holds that $v^2 + d' \not\models \varphi^2$. Therefore, it follows from Definition 3 of the semantic of a TIOA that $(l_1^2, v^2+d') \overset{o!}{\not\longrightarrow}{}^{[\![A^2]\!]_{\text{sem}}}$. Now, from Definition 13 of the conjunction for TIOTS it follows that $((l_1^1, v^1+d'), (l_1^2, v^2+d')) \overset{o!}{\not\longrightarrow}{}^Y$.
  * $v + d[r \mapsto 0]_{r\in c} \not\models Inv^{A^1 \wedge A^2}(l_3)$. In this case, we know that $v + d[r \mapsto 0]_{r\in c} \not\models Inv^{A^1 \wedge A^2}(l_3)$ implies that $v + d[r \mapsto 0]_{r\in c} \not\models Inv^2(l_3^2)$. Because $Clk^1 \cap Clk^2 = \emptyset$, it holds that $v^2 + d[r \mapsto 0]_{r\in c^2} \not\models Inv^2(l_3^2)$. Therefore, it follows from Definition 3 of the semantic of a TIOA that

[6] Alternatively, we could use Lemma 5 to come to the same conclusion. This also holds for the other two cases, where we have to use Corollary 1 instead.

$(l_1^2, v^2 + d') \overset{o!}{\not\longrightarrow}{}_{[\![A^2]\!]_{\mathrm{sem}}}$. Now, from Definition 13 of the conjunction for TIOTS it follows that $((l_1^1, v^1 + d'), (l_1^2, v^2 + d')) \overset{o!}{\not\longrightarrow}{}^{Y}$.

* $(l_3, v + d'[r \mapsto 0]_{r \in c}) \in Q$. In this case, assume that $v + d' \models \varphi$ and $v + d[r \mapsto 0]_{r \in c} \models \mathit{Inv}^{A^1 \wedge A^2}(l_3)$ (otherwise, one of the above cases can be used instead). Because $\mathit{Clk}^1 \cap \mathit{Clk}^2 = \emptyset$, it follows that $v^2 + d' \models \varphi^2$ and $v^2 + d'[r \mapsto 0]_{r \in c^2} \models \mathit{Inv}^2(l_3^2)$. Therefore, it follows from Definition 3 of the semantic of a TIOA that $(l_1^2, v^2 + d') \overset{o!}{\longrightarrow}{}_{[\![A^2]\!]_{\mathrm{sem}}} (l_3^2, v^2 + d'[r \mapsto 0]_{r \in c^2})$. Now, from Definition 13 of the conjunction for TIOTS it follows that $((l_1^1, v^1 + d'), (l_1^2, v^2 + d')) \overset{o!}{\longrightarrow}{}^{Y} ((l_1^1, v^1 + d'[r \mapsto 0]_{r \in c^1}), (l_3^2, v^2 + d'[r \mapsto 0]_{r \in c^2}))$. And note that $((l_1^1, v^1 + d'), (l_3^2, v^2 + d'[r \mapsto 0]_{r \in c^2})) = (l_1^1, l_3^2, v + d'[r \mapsto 0]_{r \in c}) = (l_3, v + d'[r \mapsto 0]_{r \in c})$.

So, in the first two cases we have shown that $((l_1^1, v^1 + d'), (l_1^2, v^2 + d')) \overset{o!}{\not\longrightarrow}{}^{Y}$ and in the third case that $((l_1^1, v^1 + d'), (l_1^2, v^2 + d')) \overset{o!}{\longrightarrow}{}^{Y} (l_3, v + d'[r \mapsto 0]_{r \in c})$.

So, in all three cases we have shown that $((l_1^1, v^1 + d'), (l_1^2, v^2 + d')) \overset{o!}{\not\longrightarrow}{}^{Y}$ or $((l_1^1, v^1 + d'), (l_1^2, v^2 + d')) \overset{o!}{\longrightarrow}{}^{Y} (l_3, v + d'[r \mapsto 0]_{r \in c})$. And note that $((l_1^1, v^1 + d'), (l_1^2, v^2 + d')) = q_2$ and $(l_3, v + d'[r \mapsto 0]_{r \in c}) = q_3$.

So we have shown that $((l_1^1, v^1 + d'), (l_1^2, v^2 + d')) \overset{o!}{\not\longrightarrow}{}^{Y}$ or $((l_1^1, v^1 + d'), (l_1^2, v^2 + d')) \overset{o!}{\longrightarrow}{}^{Y} (l_3, v + d'[r \mapsto 0]_{r \in c})$ with $(l_3, v + d'[r \mapsto 0]_{r \in c}) \in Q$. We can rewrite this into $q^X \overset{d'}{\longrightarrow}{}^{Y} q_2 \overset{o!}{\not\longrightarrow}{}^{Y}$ or $q^X \overset{d'}{\longrightarrow}{}^{Y} q_2 \overset{o!}{\longrightarrow}{}^{Y} q_3$. Since we have chosen $d'$, $q_2$, $q_3$, and $o!$ arbitrarily, the conclusion holds for all $d'$, $q_2$, $q_3$, and $o!$. Therefore, the second condition in the definition of error states hold for $q^X$.

Now, since both conditions in the definition of the error states hold for $q^X$, we know that $q^X \in \mathrm{err}^Y(Q)$. Since we have chosen $q^X$ arbitrarily from $\mathrm{err}^X(Q)$, it holds for all $q^X \in \mathrm{err}^X(Q)$. Therefore, it holds that $\mathrm{err}^X(Q) \subseteq \mathrm{err}^Y(Q)$.

($\mathrm{err}^Y \subseteq \mathrm{err}^X$) Consider a state $q^Y \in \mathrm{err}^Y$. From Definition 11 of error states we know that $\exists d \in \mathbb{R}_{\geq 0}$ s.t. $q^Y \overset{d'}{\not\longrightarrow}{}^{Y}$ and $\forall d' \in \mathbb{R}_{\geq 0} \forall o! \in \mathit{Act}_o \forall q_2 \in Q^Y : q^Y \overset{d}{\longrightarrow} q_2 \Rightarrow (q_2 \overset{o!}{\not\longrightarrow}{}^{Y} \vee \forall q_3 \in Q^Y : q_2 \overset{o!}{\longrightarrow}{}^{Y} q_3 \Rightarrow q_3 \in Q)$. From Definition 13 of the conjunction for TIOTS it follows that $q^Y = (q^{[\![A^1]\!]_{\mathrm{sem}}}, q^{[\![A^2]\!]_{\mathrm{sem}}})$ and $q_2 = (q_2^{[\![A^1]\!]_{\mathrm{sem}}}, q_2^{[\![A^2]\!]_{\mathrm{sem}}})$.

First, consider the first condition in the definition of error states. From Lemma 4 it follows immediately that $q^Y \overset{d}{\not\longrightarrow}{}^{Y}$ implies that $q^Y \overset{d}{\not\longrightarrow}{}^{X}$. So the first condition in the definition of error states holds for $q^Y$ in $X$.

Now, consider the second condition in the definition of error states. Pick any $d'$, $q_2$, and $o!$ such that $q^Y \overset{d'}{\longrightarrow} q_2 \Rightarrow (q_2 \overset{o!}{\not\longrightarrow}{}^{Y} \vee \forall q_3 \in Q^Y : q_2 \overset{o!}{\longrightarrow}{}^{Y} q_3 \Rightarrow q_3 \in Q)$. The implication holds if $q^Y \overset{d'}{\not\longrightarrow}{}^{Y}$ or $q^Y \overset{d'}{\longrightarrow} q_2 \wedge (q_2 \overset{o!}{\not\longrightarrow}{}^{Y} \vee \forall q_3 \in Q^Y : q_2 \overset{o!}{\longrightarrow}{}^{Y} q_3 \Rightarrow q_3 \in Q)$. The first case follows directly from Lemma 4 that shows that $q^Y \overset{d}{\not\longrightarrow}{}^{Y}$ implies that $q^Y \overset{d}{\not\longrightarrow}{}^{X}$, which ensures that the second condition in the definition of error states holds for $q^Y$ in $X$. For the second case we again use Lemma 4, thus $q^Y \overset{d'}{\longrightarrow}{}^{X} q_2$, where $q^Y = (l_1^1, l_1^2, v)$ and $q_2 = (l_1^1, l_1^2, v + d)$.

It remains to be shown that $q_2 \overset{o!}{\not\longrightarrow}^Y \vee \forall q_3 \in Q^Y : q_2 \overset{o!}{\longrightarrow}^Y q_3 \Rightarrow q_3 \in Q$ in $Y$ implies that $q_2 \overset{o!}{\not\longrightarrow}^X \vee \forall q_3 \in Q^X : q_2 \overset{o!}{\longrightarrow}^X q_3 \Rightarrow q_3 \in Q$ in $X$. We have to consider the three cases from Definition 13 of the conjunction for TIOTS.

- $o! \in Act^1 \cap Act^2$. It follows directly from Lemma 5 that $q_2 \overset{o!}{\not\longrightarrow}^X \vee \forall q_3 \in Q^X : q_2 \overset{o!}{\longrightarrow}^X q_3 \Rightarrow q_3 \in Q$.
- $o! \in Act^1 \backslash Act^2$. Using Definition 3 of the semantic of a TIOA, we now know that $\nexists (l_1^1, o!, \varphi^1, c^1, l_3^1) \in E^1$ or $\forall (l_1^1, o!, \varphi^1, c^1, l_3^1) \in E^1 : v^1 + d' \not\models \varphi^1 \vee v^1 + d'[r \mapsto 0]_{r \in c^1} \not\models Inv^1(l_3^1) \vee (l_3^1, l_1^2, v + d'[r \mapsto 0]_{r \in c^1}) \in Q$.
In case that $\nexists (l_1^1, o!, \varphi^1, c^1, l_3^1) \in E^1$, it follows directly from Definition 14 of the conjunction for TIOA that $\nexists ((l_1^1, l_1^2), o!, \varphi^1, c^1, (l_3^1, l_3^2)) \in E^{A^1 \wedge A^2}$. Then, with Definition 3 of the semantic of a TIOA, it follows that $(l_1^1, l_1^2, v + d') \overset{o!}{\not\longrightarrow}^X$.
In case that $\forall (l_1^1, o!, \varphi^1, c^1, l_3^1) \in E^1 : v^1 + d' \not\models \varphi^1 \vee v^1 + d'[r \mapsto 0]_{r \in c^1} \not\models Inv^1(l_3^1)$, it follows from Definition 14 that for each edge $(l_1^1, o!, \varphi^1, c^1, l_3^1) \in E^1$, $\exists ((l_1^1, l_1^2), o!, \varphi^1, c^1, (l_3^1, l_3^2)) \in E^{A^1 \wedge A^2}$. Because $Clk^1 \cap Clk^2 = \emptyset$, it holds that $v + d' \not\models \varphi^1 \vee v + d'[r \mapsto 0]_{r \in c} \not\models Inv^1(l_3^1)$. Therefore, it also holds that $v + d' \not\models \varphi^1 \vee v + d'[r \mapsto 0]_{r \in c} \not\models Inv^1(l_3^1) \wedge Inv^2(l_1^2)$. Note that from Definition 14 we know that $Inv^{A^1 \wedge A^2}((l_3^1, l_1^2)) = Inv^1(l_3^1) \wedge Inv^2(l_1^2)$. As we have shown that $v + d' \not\models \varphi^1 \vee v + d'[r \mapsto 0]_{r \in c} \not\models Inv^1(l_3^1) \wedge Inv^2(l_1^2)$ for all edges labeled with $o!$ from $(l_1^1, l_1^2)$, it follows from Definition 3 of the semantic of a TIOA that $(l_1^1, l_1^2, v + d') \overset{o!}{\not\longrightarrow}^X$.
In case that $\forall (l_1^1, o!, \varphi^1, c^1, l_3^1) \in E^1 : (l_3^1, l_1^2, v + d'[r \mapsto 0]_{r \in c^1}) \in Q$, it follows from Definition 14 that for each edge $(l_1^1, o!, \varphi^1, c^1, l_3^1) \in E^1$, $\exists ((l_1^1, l_1^2), o!, \varphi^1, c^1, (l_3^1, l_3^2)) \in E^{A^1 \wedge A^2}$. Because $Clk^1 \cap Clk^2 = \emptyset$, it holds that $v + d' \models \varphi^1 \wedge v + d'[r \mapsto 0]_{r \in c} \models Inv^1(l_3^1)$ (in case one of them does not hold, we can use the argument above). Therefore, it also holds that $v + d' \models \varphi^1 \wedge v + d'[r \mapsto 0]_{r \in c} \models Inv^1(l_3^1) \wedge Inv^2(l_1^2)$. Note that from Definition 14 we know that $Inv^{A^1 \wedge A^2}((l_3^1, l_1^2)) = Inv^1(l_3^1) \wedge Inv^2(l_1^2)$. As we have shown that $v + d' \models \varphi^1 \wedge v + d'[r \mapsto 0]_{r \in c} \models Inv^1(l_3^1) \wedge Inv^2(l_1^2)$ for all edges labeled with $o!$ from $(l_1^1, l_1^2)$, it follows from Definition 3 of the semantic of a TIOA that $(l_1^1, l_1^2, v + d') \overset{o!}{\longrightarrow}^X (l_3^1, l_1^2, v + d'[r \mapsto 0]_{r \in c})$. Now notice that $(l_3^1, l_1^2, v + d'[r \mapsto 0]_{r \in c}) \in Q$.
- $o! \in Act^2 \backslash Act^1$. Using Definition 3 of the semantic of a TIOA, we now know that $\nexists (l_1^2, o!, \varphi^2, c^2, l_3^2) \in E^2$ or $\forall (l_1^2, o!, \varphi^2, c^2, l_3^2) \in E^2 : v^2 + d' \not\models \varphi^2 \vee v^2 + d'[r \mapsto 0]_{r \in c^2} \not\models Inv^2(l_3^2) \vee (l_1^1, l_3^2, v + d'[r \mapsto 0]_{r \in c^1}) \in Q$.
In case that $\nexists (l_1^2, o!, \varphi^2, c^2, l_3^2) \in E^2$, it follows directly from Definition 14 of the conjunction for TIOA that $\nexists ((l_1^1, l_1^2), o!, \varphi^2, c^2, (l_3^1, l_3^2)) \in E^{A^1 \wedge A^2}$. Then, with Definition 3 of the semantic of a TIOA, it follows that $(l_1^1, l_1^2, v + d') \overset{o!}{\not\longrightarrow}^X$.
In case that $\forall (l_1^2, o!, \varphi^2, c^2, l_3^2) \in E^2 : v^2 + d' \not\models \varphi^2 \vee v^2 + d'[r \mapsto 0]_{r \in c^2} \not\models Inv^2(l_3^2)$, it follows from Definition 14 that for each edge $(l_1^2, o!, \varphi^2, c^2, l_3^2) \in E^2$, $\exists ((l_1^1, l_1^2), o!, \varphi^2, c^2, (l_3^1, l_3^2)) \in E^{A^1 \wedge A^2}$. Because $Clk^1 \cap Clk^2 = \emptyset$, it holds that $v + d' \not\models \varphi^2 \vee v + d'[r \mapsto 0]_{r \in c} \not\models Inv^2(l_3^2)$. Therefore, it also holds that $v + d' \not\models \varphi^2 \vee v + d'[r \mapsto 0]_{r \in c} \not\models Inv^2(l_3^2) \wedge Inv^2(l_3^2)$. Note that from Definition 14 we know that $Inv^{A^1 \wedge A^2}((l_3^1, l_1^2)) = Inv^1(l_3^1) \wedge Inv^2(l_1^2)$. As we have shown that $v + d' \not\models \varphi^2 \vee v + d'[r \mapsto 0]_{r \in c} \not\models Inv^1(l_1^1) \wedge Inv^2(l_3^2)$ for all edges labeled with

$o!$ from $(l_1^1, l_1^2)$, it follows from Definition 3 of the semantic of a TIOA that $(l_1^1, l_1^2, v + d') \overset{o!}{\not\longrightarrow}{}^X$.

In case that $\forall (l_1^2, o!, \varphi^2, c^2, l_3^2) \in E^2 : (l_1^1, l_3^2, v + d'[r \mapsto 0]_{r \in c^2}) \in Q$, it follows from Definition 14 that for each edge $(l_1^2, o!, \varphi^2, c^2, l_3^2) \in E^2$, $\exists ((l_1^1, l_1^2), o!, \varphi^2, c^2, (l_3^1, l_2^2)) \in E^{A^1 \wedge A^2}$. Because $Clk^1 \cap Clk^2 = \emptyset$, it holds that $v + d' \models \varphi^2 \wedge v + d'[r \mapsto 0]_{r \in c} \models Inv^2(l_3^2)$ (in case one of them does not hold, we can use the argument above). Therefore, it also holds that $v + d' \models \varphi^2 \wedge v + d'[r \mapsto 0]_{r \in c} \models Inv^1(l_1^1) \wedge Inv^2(l_3^2)$. Note that from Definition 14 we know that $Inv^{A^1 \wedge A^2}((l_1^1, l_3^2)) = Inv^1(l_1^1) \wedge Inv^2(l_3^2)$. As we have shown that $v + d' \models \varphi^2 \wedge v + d'[r \mapsto 0]_{r \in c} \models Inv^1(l_1^1) \wedge Inv^2(l_3^2)$ for all edges labeled with $o!$ from $(l_1^1, l_1^2)$, it follows from Definition 3 of the semantic of a TIOA that $(l_1^1, l_1^2, v + d') \xrightarrow{o!}{}^X (l_1^1, l_3^2, v + d'[r \mapsto 0]_{r \in c})$. Now notice that $(l_1^1, l_3^2, v + d'[r \mapsto 0]_{r \in c}) \in Q$.

So, in all three cases, we have shown that $(l_1^1, l_1^2, v+d') \overset{o!}{\not\longrightarrow}{}^X$ or $((l_1^1, v^1+d'), (l_1^2, v^2+d')) \xrightarrow{o!}{}^X (l_3, v + d'[r \mapsto 0]_{r \in c})$ with $(l_3, v + d'[r \mapsto 0]_{r \in c}) \in Q$. We can rewrite this into $q^Y \xrightarrow{d'}{}^X q_2 \overset{o!}{\not\longrightarrow}{}^X$ or $q^X \xrightarrow{d'}{}^Y q_2 \xrightarrow{o!}{}^Y q_3$. Since we have chosen $d'$, $q_2$, $q)3$, and $o!$ arbitrarily, the conclusion holds for all $d'$, $q_2$, $q_3$, and $o!$. Therefore, the second condition in the definition of error states hold for $q^Y$.

Now, since both conditions in the definition of the error states hold for $q^Y$, we know that $q^Y \in \mathrm{err}^X$. Since we have chosen $q^Y$ arbitrarily, it holds for all $q^Y \in \mathrm{err}^Y$. Therefore, it holds that $\mathrm{err}^Y \subseteq \mathrm{err}^X$. □

**Lemma 8** *Given two TIOAs* $A^i = (Loc^i, l_0^i, Act^i, Clk^i, E^i, Inv^i), i = 1, 2$ *where* $Act_i^1 \cap Act_o^2 = \emptyset \wedge Act_o^1 \cap Act_i^2 = \emptyset$. *Then* $\mathrm{cons}^{[\![A^1 \wedge A^2]\!]_{\mathrm{sem}}} = \mathrm{cons}^{[\![A^1]\!]_{\mathrm{sem}} \wedge [\![A^2]\!]_{\mathrm{sem}}}$.

*Proof* We will proof this by using the $\Theta$ operator. It follows from Lemma 3 that $[\![A^1 \wedge A^2]\!]_{\mathrm{sem}}$ and $[\![A^1]\!]_{\mathrm{sem}} \wedge [\![A^2]\!]_{\mathrm{sem}}$ have the same state set. Also, observe that the semantic of a TIOA, conjunction, and adversarial pruning do not alter the action set. Therefore, it follows that $[\![A^1 \wedge A^2]\!]_{\mathrm{sem}}$ and $[\![A^1]\!]_{\mathrm{sem}} \wedge [\![A^2]\!]_{\mathrm{sem}}$ have the same action set and partitioning into input and output actions. We will show for any postfixed point $P$ of $\Theta$ that $\Theta^{[\![A^1 \wedge A^2]\!]_{\mathrm{sem}}}(P) \subseteq \Theta^{[\![A^1]\!]_{\mathrm{sem}} \wedge [\![A^2]\!]_{\mathrm{sem}}}(P)$ and $\Theta^{[\![A^1]\!]_{\mathrm{sem}} \wedge [\![A^2]\!]_{\mathrm{sem}}}(P) \subseteq \Theta^{[\![A^1 \wedge A^2]\!]_{\mathrm{sem}}}(P)$. For brevity, we write $X = [\![A^1 \wedge A^2]\!]_{\mathrm{sem}}$, $Y = [\![A^1]\!]_{\mathrm{sem}} \wedge [\![A^2]\!]_{\mathrm{sem}}$, and $Clk = Clk^1 \uplus Clk^2$ in the rest of this proof. Also, we will use $v^1$ and $v^2$ to indicate the part of a valuation $v$ of only the clocks of $A^1$ and $A^2$, respectively.

($\Theta^X(P) \subseteq \Theta^Y(P)$) Consider a state $q^X \in P$. Because $P$ is a postfixed point of $\Theta^X$, it follows that $q^X \in \Theta^X(P)$. From the definition of $\Theta$, it follows that $q^X \in \overline{\mathrm{err}^X(\overline{P})}$ and $q^X \in \{q_1 \in Q^X \mid \forall d \geq 0 : [\forall q_2 \in Q^X : q_1 \xrightarrow{d}{}^X q_2 \Rightarrow q_2 \in P \wedge \forall i? \in Act_i^X : \exists q_3 \in P : q_2 \xrightarrow{i?}{}^X q_3] \vee [\exists d' \leq d \wedge \exists q_2, q_3 \in P \wedge \exists o! \in Act_o^X : q_1 \xrightarrow{d'}{}^X q_2 \wedge q_2 \xrightarrow{o!}{}^X q_3 \wedge \forall i? \in Act_i^X : \exists q_4 \in P : q_2 \xrightarrow{i?}{}^X q_4]\}$. From Lemma 7 it follows directly that $q^X \in \overline{\mathrm{err}^Y(\overline{P})}$. Now we only focus on the second part of the definition of $\Theta$.

Consider a $d \in \mathbb{R}_{\geq 0}$. Then the left-hand side or the right-hand side of the disjunction is true (or both).

- Assume the left-hand side is true, i.e., $\forall q_2 \in Q^X : q^X \xrightarrow{d}{}^X q_2 \Rightarrow q_2 \in P \wedge \forall i? \in Act_i^X : \exists q_3 \in P : q_2 \xrightarrow{i?}{}^X q_3$. Pick a $q_2 \in Q^X$. The implication is true when $q^X \not\xrightarrow{d}{}^X q_2$ or $q^X \xrightarrow{d}{}^X q_2 \wedge q_2 \in P \wedge \forall i? \in Act_i^X : \exists q_3 \in P : q_2 \xrightarrow{i?}{}^X q_3$.
  - Consider the first case. From Lemma 4 it follows that $q^X \not\xrightarrow{d}{}^Y$. Note that $q^X = (l_1^1, v_1^1, l_1^2, v_1^2)$. Thus the implication also holds for $q_2$ in $Y$.
  - Consider the second case. From Lemma 4, we have that $q^X \xrightarrow{d}{}^X q_2$ implies that $q^X \xrightarrow{d}{}^Y q_2$, and from Definition 3 of the semantic of a TIOA it follows that $v_1 + d \models Inv^{A^1 \wedge A^2}(l_1)$ for $q^X = (l_1, v_1)$, $q_2 = (l_1, v_1 + d)$, $l_1 \in Loc^{A^1 \wedge A^2}$, and $v_1 \in [Clk \mapsto \mathbb{R}_{\geq 0}]$. Now, pick $i? \in Act_i^X$ and $q_3 \in Q^X$ such that $q_2 \xrightarrow{i?}{}^X q_3$ and $q_3 \in P$. From Definition 3 of the semantic of a TIOA it follows that $(l_1, i?, \varphi, c, l_3) \in E^{A^1 \wedge A^2}$, $q_3 = (l_3, v_3)$, $v_1 + d \models \varphi$, $v_3 = v_1 + d[r \mapsto 0]_{r \in c}$, and $v_3 \models Inv^{A^1 \wedge A^2}(l_3)$. From Definition 14 of the conjunction of TIOA it follows that $l_1 = (l_1^1, l_1^2)$, $l_3 = (l_3^1, l_3^2)$, $Inv^{A^1 \wedge A^2}(l_1) = Inv^1(l_1^1) \wedge Inv^2(l_1^2)$, and $Inv^{A^1 \wedge A^2}(l_3) = Inv^1(l_3^1) \wedge Inv^2(l_3^2)$. We have to consider the three cases of Definition 14 in relation to $i?$.
    * $i? \in Act_i^1 \cap Act_i^2$. It follows directly from Lemma 5 that $q_2 \xrightarrow{i?} q_3$ is a transition in $Y$.
    * $i? \in Act_i^1 \setminus Act_i^2$. It follows directly from Corollary 1 that $q_2 \xrightarrow{i?} q_3$ is a transition in $Y$.
    * $i? \in Act_i^2 \setminus Act_i^1$. It follows directly from Corollary 1 (where we switched $A^1$ and $A^2$) that $q_2 \xrightarrow{i?} q_3$ is a transition in $Y$.

    So, in all three cases we have that $q_2 \xrightarrow{i?} q_3$ is a transition in $Y$. As the analysis above is independent of the particular $i?$, $q_2 \xrightarrow{i?} q_3$ is a transition in $Y$ for all $i?$. Because both $q_2, q_3 \in P$ and $q^X \xrightarrow{d}{}^Y q_2$, we have that the implication also holds for $q_2 \in Y$.

  So, in both cases we have that for $q^X \xrightarrow{d}{}^Y q_2 \Rightarrow q_2 \in P \wedge \forall i? \in Act_i^Y : \exists q_3 \in P : q_2 \xrightarrow{i?}{}^Y q_3$. As $q_2$ is chosen arbitrarily, it holds for all $q_2 \in Q^X = Q^Y$. Therefore, the left-hand side is true.
- Assume the right-hand side is true, i.e., $\exists d' \leq d \wedge \exists q_2, q_3 \in P \wedge \exists o! \in Act_o^X : q^X \xrightarrow{d'}{}^X q_2 \wedge q_2 \xrightarrow{o!}{}^X q_3 \wedge \forall i? \in Act_i^X : \exists q_4 \in P : q_2 \xrightarrow{i?}{}^X q_4$.
  First, following Definition 3 of the semantic of a TIOA, we have that $q^X = (l_1, v_1)$, $q_2 = (l_1, v_1 + d')$, $q_3 = (l_3, v_3)$, $q_4 = (l_4, v_4)$, $l_1, l_3, l_4 \in Loc^{A^1 \wedge A^2}$, $v_1, v_3, v_4 \in [Clk \mapsto \mathbb{R}_{\geq 0}]$, $v_1 + d' \models Inv^{A^1 \wedge A^2}(l_1)$, $\exists (l_1, o!, \varphi, c, l_3) \in E^{A^1 \wedge A^2}$, $v_1 + d' \models \varphi$, $v_3 = v_1 + d'[r \mapsto 0]_{r \in c}$, and $v_3 \models Inv^{A^1 \wedge A^2}(l_3)$. First, focus on the delay transition. From Lemma 4 it follows that $q^X \xrightarrow{d'}{}^Y q_2$ in $Y$, with $q^X = (l_1^1, v_1^1, l_1^2, v_1^2) = (l_1^1, l_1^2, v_1)$ and $q_2 = (l_1^1, v_1^1 + d', l_1^2, v_1^2 + d') = (l_1^1, l_1^2, v_1 + d')$. Now consider the output transition labeled with $o!$. We have to consider the three cases from Definition 14.
  - $o! \in Act_o^1 \cap Act_o^2$. It follows directly from Lemma 5 that $q_2 \xrightarrow{o!} q_3$ is a transition in $Y$.
  - $o! \in Act_o^1 \setminus Act_o^2$. It follows directly from Corollary 1 that $q_2 \xrightarrow{o!} q_3$ is a transition in $Y$.

- $o! \in Act_o^2 \setminus Act_o^1$. It follows directly from Corollary 1 (where we switched $A^1$ and $A^2$) that $q_2 \xrightarrow{o!} q_3$ is a transition in $Y$.

Thus, in all three cases we have that $q_2 \xrightarrow{o!} q_3$ is a transition in $Y$. Therefore, we can conclude that $q^X \xrightarrow{d'}{}^Y q_2 \wedge q_2 \xrightarrow{o!}{}^Y q_3$ with $q_2, q_3 \in P$.
Finally, consider the input transitions labeled with $i?$. Using the same argument as before, we can show that $q_2 \xrightarrow{i?} q_4$ in $X$ is also a transition in $Y$, and $q_4 \in P$. Therefore, we can conclude that $q^X \xrightarrow{d'}{}^Y q_2 \wedge q_2 \xrightarrow{o!}{}^Y q_3 \wedge \forall i? \in Act_i^Y : \exists q_4 \in P : q_2 \xrightarrow{i?}{}^Y q_4$ with $q_2, q_3, q_4 \in P$. Thus, the right-hand side is true.

Thus, we have shown that when the left-hand side is true for $q^X$ in $X$, it is also true for $q^X$ in $Y$; and that when the right-hand side is true for $q^X$ in $X$, it is also true for $q^X$ in $Y$. Thus, $q^X \in \Theta^Y(P)$. Since $q^X \in P$ was chosen arbitrarily, it holds for all states in $P$. Once we choose $P$ to be the fixed-point of $\Theta^X$, we have that $\Theta^X(P) \subseteq \Theta^Y(P)$.

($\Theta^Y(P) \subseteq \Theta^X(P)$) Consider a state $q^Y \in P$. Because $P$ is a postfixed point of $\Theta^Y$, it follows that $p \in \Theta^X(Y)$. From the definition of $\Theta$, it follows that $q^Y \in \overline{\text{err}^Y(\overline{P})}$ and $q^Y \in \{q \in Q^Y \mid \forall d \geq 0 : [\forall q_2 \in Q^Y : q \xrightarrow{d}{}^Y q_2 \Rightarrow q_2 \in P \wedge \forall i? \in Act_i^Y : \exists q_3 \in P : q_2 \xrightarrow{i?}{}^Y q_3] \vee [\exists d' \leq d \wedge \exists q_2, q_3 \in P \wedge \exists o! \in Act_o^Y : q \xrightarrow{d'}{}^Y q_2 \wedge q_2 \xrightarrow{o!}{}^Y q_3 \wedge \forall i? \in Act_i : \exists q_4 \in P : q_2 \xrightarrow{i?}{}^Y q_4]\}$. From Lemma 7 it follows directly that $q^X \in \overline{\text{err}^X(\overline{P})}$. Now we only focus on the second part of the definition of $\Theta$.

Consider a $d \in \mathbb{R}_{\geq 0}$. Then the left-hand side or the right-hand side of the disjunction is true (or both).

- Assume the left-hand side is true, i.e., $\forall q_2 \in Q^Y : q^Y \xrightarrow{d}{}^Y q_2 \Rightarrow q_2 \in P \wedge \forall i? \in Act_i^Y : \exists q_3 \in P : q_2 \xrightarrow{i?}{}^Y q_3$. Pick a $q_2 \in Q^Y$. The implication is true when $q^Y \not\xrightarrow{d}{}^Y q_2$ or $q^Y \xrightarrow{d}{}^Y q_2 \wedge q_2 \in P \wedge \forall i? \in Act_i^Y : \exists q_3 \in P : q_2 \xrightarrow{i?}{}^Y q_3$.
  - Consider the first case. From Lemma 4 it follows that $q^Y \not\xrightarrow{d}{}^X$. Note that $q^Y = (l^1, v^1, l^2, v^2)$. Thus the implication also holds for $q_2$ in $X$.
  - Consider the second case. From Lemma 4 we have that $q^Y \xrightarrow{d}{}^Y q_2$ implies that $q^Y \xrightarrow{d}{}^X q_2$, and from Definition 13 of the conjunction for TIOTS that $q^Y = (q_1^1, q_1^2)$ and $q_2 = (q_2^1, q_2^2)$. Also, using Definition 3 of the semantic of a TIOA it follows for $i = 1, 2$ that $q_1^i = (l_1^i, v_1^i)$, $q_2^i = (l_1^i, v_1^i + d)$, $l_1^i \in Loc^i$, and $v_1^i \in [Clk^i \mapsto \mathbb{R}_{\geq 0}]$. Now, pick an $i? \in Act_i^Y$ with its corresponding $q_3$ according to the implication. We have to consider the three cases from Definition 13.
    * $i? \in Act_i^1 \cap Act_i^2$. It follows directly from Lemma 5 that $q_2 \xrightarrow{i?}{}^X q_3$.
    * $i? \in Act_i^1 \setminus Act_i^2$. From the fact that $q^Y \xrightarrow{d}{}^X q_2$[7], it follows from Definitions 3 and 13 that $v_1^2 + d \models Inv^2(l_1^2)$ (see also proof of Lemma 4). Observe that $v_1^2 + d[r \mapsto 0]_{r \in c^1} = v_1^2 + d$, so $v_3 \models Inv^2(l_1^2)$. Now it follows directly from Lemma 6 that $q_2 \xrightarrow{i?}{}^X q_3$.
    * $i? \in Act_i^2 \setminus Act_i^1$. From the fact that $q^Y \xrightarrow{d}{}^X q_2$, it follows from Definitions 3 and 13 that $v_1^1 + d \models Inv^1(l_1^1)$ (see also proof of Lemma 4).

---

[7]This fact is key for finalizing the proof of Theorem 7: without adversarial pruning in that theorem, you cannot assume this, and you get stuck in proving that $v_3 \models Inv^2(l_1^2)$ and thus $v_3 \models Inv^{A^1 \wedge A^2}((l_3^1, l_1^2))$, i.e., you cannot prove that.

Observe that $v_1^1 + d[r \mapsto 0]_{r \in c^2} = v_1^1 + d$, so $v_3 \models Inv^1(l_1^1)$. Now it follows directly from Lemma 6 (where we switched $A^2$ and $A^2$) that $q_2 \xrightarrow{i?}{}^X q_3$.

Thus, in all three cases we can show that $q_2 \xrightarrow{i?}{}^Y q_3$ implies $q_2 \xrightarrow{i?}{}^X q_3$. Since we have chosen an arbitrarily $i? \in Act_i^Y$, it holds for all $i? \in Act_i^Y$. Thus the implication also holds for $q_2$ in $X$.

Thus, in both cases the implication holds. Therefore, we can conclude that $q^Y \xrightarrow{d}{}^X q_2 \Rightarrow q_2 \in P \wedge \forall i? \in Act_i^X : \exists q_3 \in P : q_2 \xrightarrow{i?}{}^X q_3$. As $q_2$ is chosen arbitrarily, it holds for all $q_2 \in Q^X = Q^Y$. Therefore, the left-hand side is true.

- Assume the right-hand side is true, i.e., $\exists d' \leq d \wedge \exists q_2, q_3 \in P \wedge \exists o! \in Act_o^Y : q \xrightarrow{d'}{}^Y q_2 \wedge q_2 \xrightarrow{o!}{}^Y q_3 \wedge \forall i? \in Act_i : \exists q_4 \in P : q_2 \xrightarrow{i?}{}^Y q_4$. First, focus on the delay. From Lemma 4 it follows that $q \xrightarrow{d'}{}^Y q_2$ implies $q \xrightarrow{d'}{}^X q_2$, and from Definition 13 of the conjunction for TIOTS that $q^Y = (q_1^1, q_1^2)$ and $q_2 = (q_2^1, q_2^2)$. Also, using Definition 3 of the semantic of a TIOA it follows for $i = 1, 2$ that $q_1^i = (l_1^i, v_1^i)$, $q_2^i = (l_1^i, v_1^i + d')$, $l_1^i \in Loc^i$, and $v_1^i \in [Clk^i \mapsto \mathbb{R}_{\geq 0}]$. Now, consider the output transition labeled with $o!$. We have to consider the three cases from Definition 13 of the conjunction for TIOTS.
  - $o! \in Act_o^1 \cap Act_o^2$. It follows directly from Lemma 5 that $q_2 \xrightarrow{o!}{}^X q_3$.
  - $o! \in Act_o^1 \subset Act_o^2$. From the fact that $q^Y \xrightarrow{d'}{}^X q_2$, it follows from Definitions 3 and 13 that $v_1^2 + d' \models Inv^2(l_1^2)$ (see also proof of Lemma 4). Observe that $v_1^2 + d'[r \mapsto 0]_{r \in c^1} = v_1^2 + d'$, so $v_3 \models Inv^2(l_1^2)$. Now it follows directly from Lemma 6 that $q_2 \xrightarrow{o!}{}^X q_3$.
  - $o! \in Act_o^2 \subset Act_o^1$. From the fact that $q^Y \xrightarrow{d'}{}^X q_2$, it follows from Definitions 3 and 13 that $v_1^i + d' \models Inv^1(l_1^1)$ (see also proof of Lemma 4). Observe that $v_1^1 + d'[r \mapsto 0]_{r \in c^2} = v_1^1 + d'$, so $v_3 \models Inv^1(l_1^1)$. Now it follows directly from Lemma 6 (where we switched $A^2$ and $A^2$) that $q_2 \xrightarrow{o!}{}^X q_3$.

  Thus, in all three cases we have that $q_2 \xrightarrow{o!}{}^X q_3$ is a transition in $X$. Therefore, we can conclude that $q^Y \xrightarrow{d'}{}^X q_2 \wedge q_2 \xrightarrow{o!}{}^X q_3$ with $q_2, q_3 \in P$. Thus, the right-hand side is true.

  Finally, consider the input transitions labeled with $i?$. Using the same argument as before, we can show that $q_2 \xrightarrow{i?} q_4$ in $Y$ is also a transition in $X$, and $q_4 \in P$. Therefore, we can conclude that $q^Y \xrightarrow{d'}{}^X q_2 \wedge q_2 \xrightarrow{o!}{}^X q_3 \wedge \forall i? \in Act_i^X : \exists q_4 \in P : q_2 \xrightarrow{i?}{}^X q_4$ with $q_2, q_3, q_4 \in P$. Thus, the right-hand side is true.

Thus, we have shown that when the left-hand side is true for $q^Y$ in $Y$, it is also true for $q^Y$ in $X$; and that when the right-hand side is true for $q^Y$ in $Y$, it is also true for $q^Y$ in $X$. Thus, $q^Y \in \Theta^X(P)$. Since $q^Y \in P$ was chosen arbitrarily, it holds for all states in $P$. Once we choose $P$ to be the fixed-point of $\Theta^Y$, we have that $\Theta^Y(P) \subseteq \Theta^X(P)$. □

Finally, we are ready to proof Theorem 7. The reason why adversarial pruning is needed becomes apparent in the second half of the proof where we consider non-shared events. To further illustrate this, consider again the example in Figure 8, where we show that $[\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}}$ has an additional transition $(1, 4) \xrightarrow{a!} (2, 4)$, which is not present in $[\![A^1 \wedge A^2]\!]_{\text{sem}}$. We can 'remove' this transition with adversarial pruning by realizing that the target state $(2,4)$ is an inconsistent state (you can see this by noticing that no time delay, including a zero time delay, is possible).

*Proof of Theorem 7* We will prove this theorem by showing that $(\llbracket A^1 \wedge A^2 \rrbracket_{\mathrm{sem}})^\Delta$ and $(\llbracket A^1 \rrbracket_{\mathrm{sem}} \wedge \llbracket A^2 \rrbracket_{\mathrm{sem}})^\Delta$ have the same set of states, same initial state, same set of actions, and same transition relation.

It follows from Lemma 3 that $\llbracket A^1 \wedge A^2 \rrbracket_{\mathrm{sem}}$ and $\llbracket A^1 \rrbracket_{\mathrm{sem}} \wedge \llbracket A^2 \rrbracket_{\mathrm{sem}}$ have the same state set and initial state. As $\mathrm{cons}^{\llbracket A^1 \wedge A^2 \rrbracket_{\mathrm{sem}}} = \mathrm{cons}^{\llbracket A^1 \rrbracket_{\mathrm{sem}} \wedge \llbracket A^2 \rrbracket_{\mathrm{sem}}} = \mathrm{cons}$ from Lemma 8, it follows that $(\llbracket A^1 \wedge A^2 \rrbracket_{\mathrm{sem}})^\Delta$ and $(\llbracket A^1 \rrbracket_{\mathrm{sem}} \wedge \llbracket A^2 \rrbracket_{\mathrm{sem}})^\Delta$ have the same state set and initial state. Also, observe that the semantic of a TIOA and adversarial pruning do not alter the action set. Therefore, it follows directly that $(\llbracket A^1 \wedge A^2 \rrbracket_{\mathrm{sem}})^\Delta$ and $(\llbracket A^1 \rrbracket_{\mathrm{sem}} \wedge \llbracket A^2 \rrbracket_{\mathrm{sem}})^\Delta$ have the same action set and partitioning into input and output actions.

It remains to show that $(\llbracket A^1 \wedge A^2 \rrbracket_{\mathrm{sem}})^\Delta$ and $(\llbracket A^1 \rrbracket_{\mathrm{sem}} \wedge \llbracket A^2 \rrbracket_{\mathrm{sem}})^\Delta$ have the same transition relation. In the remainder of the proof, we will use $v^1$ and $v^2$ to indicate the part of a valuation $v$ of only the clocks of $A^1$ and $A^2$, respectively. Also, for brevity we write $X = (\llbracket A^1 \wedge A^2 \rrbracket_{\mathrm{sem}})^\Delta$, $Y = (\llbracket A^1 \rrbracket_{\mathrm{sem}} \wedge \llbracket A^2 \rrbracket_{\mathrm{sem}})^\Delta$, and $\mathit{Clk} = \mathit{Clk}^1 \uplus \mathit{Clk}^2$ in the rest of this proof.

($\Rightarrow$) Assume a transition $q_1^X \xrightarrow{a} q_2^X$ in $X$. From Definition 12 it follows that $q_1^X \xrightarrow{a} q_2^X$ in $\llbracket A^1 \wedge A^2 \rrbracket_{\mathrm{sem}}$ and $q_2^X \in \mathrm{cons}$. Following Definition 3 of the semantic, it follows that there exists an edge $(l_1, a, \varphi, c, l_2) \in E^{A^1 \wedge A^2}$ with $q_1^X = (l_1, v_1)$, $q_2^X = (l_2, v_2)$, $l_1, l_2 \in \mathit{Loc}^{A^1 \wedge A^2}$, $v_1, v_2 \in [\mathit{Clk} \mapsto \mathbb{R}_{\geq 0}]$, $v_1 \models \varphi$, $v_2 = v_1[r \mapsto 0]_{r \in c}$, and $v_2 \models \mathit{Inv}(l_2)$. Now we consider the three cases of Definition 14 of the conjunction for TIOA.

- $a \in \mathit{Act}^1 \cap \mathit{Act}^2$. It follows directly from Lemma 5 that $q_1^X \xrightarrow{a} q_2^X$ is a transition in $\llbracket A^1 \rrbracket_{\mathrm{sem}} \wedge \llbracket A^2 \rrbracket_{\mathrm{sem}}$. Since $q_2^X \in \mathrm{cons}$, it holds that $q_1^X \xrightarrow{a} q_2^X$ is a transition in $Y$.
- $a \in \mathit{Act}^1 \setminus \mathit{Act}^2$. It follows directly from Corollary 1 that $q_1^X \xrightarrow{a} q_2^X$ is a transition in $\llbracket A^1 \rrbracket_{\mathrm{sem}} \wedge \llbracket A^2 \rrbracket_{\mathrm{sem}}$. Since $q_2^X \in \mathrm{cons}$, it holds that $q_1^X \xrightarrow{a} q_2^X$ is a transition in $Y$.
- $a \in \mathit{Act}^2 \setminus \mathit{Act}^1$. It follows directly from Corollary 1 (where we switched $A^1$ and $A^2$) that $q_1^X \xrightarrow{a} q_2^X$ is a transition in $\llbracket A^1 \rrbracket_{\mathrm{sem}} \wedge \llbracket A^2 \rrbracket_{\mathrm{sem}}$. Since $q_2^X \in \mathrm{cons}$, it holds that $q_1^X \xrightarrow{a} q_2^X$ is a transition in $Y$.

Now consider that $a$ is a delay $d$. It follows directly from Lemma 4 that $q_1^X \xrightarrow{d} q_2^X$ is a transition in $\llbracket A^1 \rrbracket_{\mathrm{sem}} \wedge \llbracket A^2 \rrbracket_{\mathrm{sem}}$. Since $q_2^X \in \mathrm{cons}$, it holds that $q_1^X \xrightarrow{d} q_2^X$ is a transition in $Y$.

We have shown that when $q_1^X \xrightarrow{a} q_2^X$ is a transition in $X = (\llbracket A^1 \wedge A^2 \rrbracket_{\mathrm{sem}})^\Delta$, it holds that $q_1^X \xrightarrow{a} q_2^X$ is a transition in $Y = (\llbracket A^1 \rrbracket_{\mathrm{sem}} \wedge \llbracket A^2 \rrbracket_{\mathrm{sem}})^\Delta$. Since the transition is arbitrarily chosen, it holds for all transitions in $X$.

($\Leftarrow$) Assume a transition $q_1^Y \xrightarrow{a} q_2^Y$ in $Y$. From Definition 12 it follows that $q_1^Y \xrightarrow{a} q_2^Y$ in $\llbracket A^1 \rrbracket_{\mathrm{sem}} \wedge \llbracket A^2 \rrbracket_{\mathrm{sem}}$ and $q_2^Y \in \mathrm{cons}$. Now we consider the three cases of Definition 13 of the conjunction for TIOTS.

- $a \in \mathit{Act}^1 \cap \mathit{Act}^2$. It follows directly from Lemma 5 that $q_1^Y \xrightarrow{a} q_2^Y$ is a transition in $\llbracket A^1 \wedge A^2 \rrbracket_{\mathrm{sem}}$. Since $q_2^Y \in \mathrm{cons}$, it holds that $q_1^Y \xrightarrow{a} q_2^Y$ is a transition in $X$.

- $a \in Act^1 \setminus Act^2$. From time reflexivity of Definition 1 we have that $q_2^Y \xrightarrow{d}$ with $d = 0$. From Definitions 12 and 13 it follows that $q_2^{[\![A^1]\!]_{\text{sem}}} \xrightarrow{d}$ and $q^{[\![A^2]\!]_{\text{sem}}} \xrightarrow{d}$. Now, from Definition 3 it follows that $v^2 + d \models Inv^2(l^2)$, i.e., $v^2 \models Inv^2(l^2)$. It now follows directly from Lemma 6 that $q_1^Y \xrightarrow{a} q_2^Y$ is a transition in $[\![A^1 \wedge A^2]\!]_{\text{sem}}$. Since $q_2^Y \in \text{cons}$, it holds that $q_1^Y \xrightarrow{a} q_2^Y$ is a transition in $X$.
- $a \in Act^2 \setminus Act^1$. From time reflexivity of Definition 1 we have that $q_2^Y \xrightarrow{d}$ with $d = 0$. From Definitions 12 and 13 it follows that $q^{[\![A^1]\!]_{\text{sem}}} \xrightarrow{d}$ and $q_2^{[\![A^2]\!]_{\text{sem}}} \xrightarrow{d}$. Now, from Definition 3 it follows that $v^1 + d \models Inv^1(l^1)$, i.e., $v^1 \models Inv^1(l^1)$. It now follows directly from Lemma 6 (where we switched $A^1$ and $A^2$) that $q_1^Y \xrightarrow{a} q_2^Y$ is a transition in $[\![A^1 \wedge A^2]\!]_{\text{sem}}$. Since $q_2^Y \in \text{cons}$, it holds that $q_1^Y \xrightarrow{a} q_2^Y$ is a transition in $X$.

Now consider that $a$ is a delay $d$. It follows directly from Lemma 4 that $q_1^Y \xrightarrow{d} q_2^Y$ is a transition in $[\![A^1 \wedge A^2]\!]_{\text{sem}}$. Since $q_2^Y \in \text{cons}$, it holds that $q_1^Y \xrightarrow{d} q_2^Y$ is a transition in $X$.

We have shown that when $q_1^Y \xrightarrow{a} q_2^Y$ is a transition in $Y = ([\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}})^{\Delta}$, it holds that $q_1^Y \xrightarrow{a} q_2^Y$ is a transition in $X = ([\![A^1 \wedge A^2]\!]_{\text{sem}})^{\Delta}$. Since the transition is arbitrarily chosen, it holds for all transitions in $Y$. □

**Corollary 2** *Given two TIOAs* $A^i = (Loc^i, l_0^i, Act^i, Clk^i, E^i, Inv^i), i = 1, 2$ *where* $Act_i^1 = Act_i^2 \wedge Act_o^1 = Act_o^2$. *Then* $[\![A^1 \wedge A^2]\!]_{\text{sem}} = [\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}}$.

*Proof* This corollary follows directly as a special case from the proof of Theorem 7. The special case only depends on Lemmas 3 and 5, which do not require adversarial pruning to be applied. □

# 4 Parallel composition

We shall now define *structural composition*, also called *parallel composition*, between specifications. We follow the optimistic approach of [8], i.e., *two specifications can be composed if there exists at least one environment in which they can work together*. Before going further, we would like to contrast the structural and logical composition.

The main use case for parallel composition is in fact dual to the one for conjunction. Indeed, as observed in the previous section, conjunction is used to reason about internal properties of an implementation set, so if a local inconsistency arises in conjunction we limit the implementation set to avoid it in implementations. A pruned specification can be given to a designer, who chooses a particular implementation satisfying conjoined requirements. A conjunction is consistent if the output player can avoid inconsistencies, and its main theorem states that its set of implementation coincides with the intersection of implementation sets of the conjuncts.

In contrast, parallel composition is used to reason about external use of two (or more) components. We assume an independent implementation scenario, where the two composed components are implemented by independent designers. The designer of any of the components can only assume that the other composed implementations will adhere to the original specifications being composed. Consequently if an error occurs in parallel composition of the two specifications, the independent designers receive additional information on how to restrict their specifications to avoid reaching the error states in the composed system.

We now propose our formal definition for parallel composition, which roughly corresponds to the one defined on timed input/output automata [9]. We consider two TIOTSs $S = (Q^S, q_0^S, Act^S, \rightarrow^S)$ and $T = (Q^T, q_0^T, Act^T, \rightarrow^T)$ and we say that they are *composable* iff their output alphabets are disjoint $Act_o^S \cap Act_o^T = \emptyset$.

**Definition 15** *Given two specifications $S^i = (Q^i, q_0^i, Act^i, \rightarrow^i), i = 1, 2$ where $Act_o^1 \cap Act_o^2 = \emptyset$, the* parallel composition *of $S^1$ and $S^2$, denoted by $S^1 \parallel S^2$, is TIOTS $(Q^1 \times Q^2, (q_0^1, q_0^2), Act, \rightarrow)$ where $Act = Act^1 \cup Act^2 = Act_i \uplus Act_o$ with $Act_i = (Act_i^1 \setminus Act_o^2) \cup (Act_i^2 \setminus Act_o^1)$ and $Act_o = Act_o^1 \cup Act_o^2$, and $\rightarrow$ is defined as*

- $(q_1^1, q_1^2) \xrightarrow{a} (q_2^1, q_2^2)$ *if* $a \in Act^1 \cap Act^2$, $q_1^1 \xrightarrow{a}{}^1 q_2^1$, *and* $q_1^2 \xrightarrow{a}{}^2 q_2^2$
- $(q_1^1, q^2) \xrightarrow{a} (q_2^1, q^2)$ *if* $a \in Act^1 \setminus Act^2$, $q_1^1 \xrightarrow{a}{}^1 q_2^1$, *and* $q^2 \in Q^2$
- $(q^1, q_1^2) \xrightarrow{a} (q^1, q_2^2)$ *if* $a \in Act^2 \setminus Act^1$, $q_1^2 \xrightarrow{a}{}^2 q_2^2$, *and* $q^1 \in Q^1$
- $(q_1^1, q_1^2) \xrightarrow{d} (q_2^1, q_2^2)$ *if* $d \in \mathbb{R}_{\geq 0}$, $q_1^1 \xrightarrow{d}{}^1 q_2^1$, *and* $q_1^2 \xrightarrow{d}{}^2 q_2^2$

Observe that if we compose two locally specifications using the above product rules, then the resulting product is also locally consistent. This is formalized in Lemma 9. Furthermore, observe that parallel composition is commutative, and that two specifications composed give rise to well-formed specifications. It is also associative in the following sense:

$$[\![(S \parallel T) \parallel U]\!]_{\text{mod}} = [\![S \parallel (T \parallel U)]\!]_{\text{mod}}$$

**Lemma 9** *Given two locally consistent specifications $S^i = (Q^i, q_0^i, Act^i, \rightarrow^i), i = 1, 2$ where $Act_o^1 \cap Act_o^2 = \emptyset$. Then $S^1 \parallel S^2$ is locally consistent.*

*Proof* Since, $S^1$ and $S^2$ are locally consistent, the only reason why $S^1 \parallel S^2$ could be inconsistent is when a new error state is created by the parallel composition. We show by contradiction that this is not possible.

Assume that state $q_1 \in S^1 \parallel S^2$ is an error state. From Definition 11 of the error state it follows that $\exists d_1 \in \mathbb{R}_{\geq 0} : q_1 \stackrel{d_1}{\not\longrightarrow} \wedge \forall d_2 \in \mathbb{R}_{\geq 0} \forall o! \in Act_o \forall q_2 \in Q : q_1 \xrightarrow{d_2} q_2 \Rightarrow q_2 \stackrel{o!}{\not\longrightarrow}$. From Definition 15 of the parallel composition for TIOTS it follows that (1) $q_1 = (q_1^1, q_1^2)$ with $q_1^1 \in Q^1$ and $q_1^2 \in Q^2$, and that either $q^1 \stackrel{d_1}{\not\longrightarrow}{}^1$ or $q^2 \stackrel{d_2}{\not\longrightarrow}{}^2$

(or both); (2) that $q_2 = (q_2^1, q_2^2)$ with $q_2^1 \in Q^1$ and $q_2^2 \in Q^2$, and that $q_1^1 \xrightarrow{d_2}{}^1 q_2^1$ and $q_1^2 \xrightarrow{d_2}{}^2 q_2^2$; and (3) that $o! \in Act_o^1$ and possibly $o? \in Act_i^2$, or $o! \in Act_o^2$ and possibly $o? \in Act_i^1$. In the next step we assume that $o! \in Act_o^1$ and possibly $o? \in Act_i^2$, as the other case is symmetrical. Consider two cases and Definition 15:

- $o? \in Act_i^2$. As $S^2$ is a specification, it is input-enabled. Therefore, $q_1 \xrightarrow{d_2} q_2 \Rightarrow q_2 \overset{o!}{\not\longrightarrow}$ implies that $q_1^1 \xrightarrow{d_2} q_2^1 \Rightarrow q_2^1 \overset{o!}{\not\longrightarrow}$.
- $o? \notin Act_i^2$. This directly results in that $q_1 \xrightarrow{d_2} q_2 \Rightarrow q_2 \overset{o!}{\not\longrightarrow}$ implies that $q_1^1 \xrightarrow{d_2} q_2^1 \Rightarrow q_2^1 \overset{o!}{\not\longrightarrow}$.

Applying the above reasoning for all output actions and knowing that $Act_o = Act_o^1 \cup Act_o^2$ from Definition 15, it follows that $\forall o! \in Act_o^1 : q_1^1 \xrightarrow{d_2}{}^1 q_2^1 \implies q_2^1 \overset{o!}{\not\longrightarrow}$ and $\forall o! \in Act_o^2 : q_1^2 \xrightarrow{d_2}{}^2 q_2^2 \implies q_2^2 \overset{o!}{\not\longrightarrow}$. As this is independent of the actual value of $d_2$, it holds for all $d_2$.

Finally, since either $q^1 \overset{d_1}{\not\longrightarrow}{}^1$ or $q^2 \overset{d_2}{\not\longrightarrow}{}^2$ (or both), it follows that either $\exists d_1 \in \mathbb{R}_{\geq 0} : q_1^1 \overset{d_1}{\not\longrightarrow}{}^1 \land \forall d_2 \in \mathbb{R}_{\geq 0} \forall o! \in Act_o^1 \forall q_2^1 \in Q^1 : q_1^1 \xrightarrow{d_2}{}^1 q_2^1 \Rightarrow q_2^1 \overset{o!}{\not\longrightarrow}{}^1$ or $\exists d_1 \in \mathbb{R}_{\geq 0} : q_1^2 \overset{d_1}{\not\longrightarrow}{}^2 \land \forall d_2 \in \mathbb{R}_{\geq 0} \forall o! \in Act_o^2 \forall q_2^2 \in Q^1 : q_1^2 \xrightarrow{d_2}{}^2 q_2^2 \Rightarrow q_2^2 \overset{o!}{\not\longrightarrow}{}^2$ (or both). Therefore, either $q_1^1$ or $q_1^2$ (or both) is an error state, which contradicts with the antecedent stating that $S^1$ and $S^2$ are consistent. □

**Theorem 8** *Refinement is a pre-congruence with respect to parallel composition: for any specifications $S^1$, $S^2$, and $T$ such that $S^1 \leq S^2$ and $S^1$ is composable with $T$, we have that $S^2$ is composable with $T$ and $S^1 \parallel T \leq S^2 \parallel T$.*

*Proof* $S^1 \leq S^2$ implies that $Act_o^{S^2} \subseteq Act_o^{S^2}$ (see Definition 6), and $S^1$ is composable with $T$ implies that $Act_o^{S^1} \cap Act_o^T = \emptyset$. Combining this results immediately in that $Act_o^{S^2} \cap Act_o^T = \emptyset$, thus $S^2$ is composable with $T$. Furthermore, since $S^1 \leq S^2$, there exists a relation $R \in Q^1 \times Q^2$ with the properties given in Definition 6 of the refinement. Construct relation $R' = \{((q^1, q^T), (q^2, q^T)) \in Q^{S^1 \parallel T} \times Q^{S^2 \parallel T} \mid (q^1, q^2) \in R\}$. We show that $R'$ witnesses $S^1 \parallel T \leq S^2 \parallel T$. Consider the five cases of refinement for a state pair $((q_1^1, q_1^T), (q_1^2, q_1^T)) \in R'$.

1. $(q_1^2, q_1^T) \xrightarrow{i?}{}^{S^2 \parallel T} (q_2^2, q_2^T)$ for some $(q_2^2, q_2^T) \in Q^{S^2 \parallel T}$ and $i? \in Act_i^{S^2 \parallel T} \cap Act_i^{S^1 \parallel T}$. Consider the five feasible combinations for input action $i?$ using Definition 15 such that $i? \in Act_i^{S^2 \parallel T} \cap Act_i^{S^1 \parallel T}$.
   - $i? \in Act_i^{S^1}$, $i? \in Act_i^{S^2}$, and $i? \in Act_i^T$. In this case, it follows from Definition 15 that $q_1^2 \xrightarrow{i?}{}^{S^2} q_2^2$ and $q_1^T \xrightarrow{i?}{}^T q_2^T$. Now, using $R$ and Definition 6, it follows that $q_1^1 \xrightarrow{i?}{}^{S^1} q_2^1$ and $(q_2^1, q_2^2) \in R$. Thus, following Definition 15 again, we have that $(q_1^1, q_1^T) \xrightarrow{i?}{}^{S^1 \parallel T} (q_2^1, q_2^T)$. From the construction of $R'$ we confirm that $((q_2^1, q_2^T), (q_2^2, q_2^T)) \in R'$.
   - $i? \in Act_i^{S^1}$, $i? \in Act_i^{S^2}$, and $i? \notin Act^T$. In this case, it follows from Definition 15 that $q_1^2 \xrightarrow{i?}{}^{S^2} q_2^2$ and $q_1^T = q_2^T$. Now, using $R$ and Definition 6,

it follows that $q_1^1 \xrightarrow{i?}{}^{S^1} q_2^1$ and $(q_2^1, q_2^2) \in R$. Thus, following Definition 15 again, we have that $(q_1^1, q_1^T) \xrightarrow{i?}{}^{S^1 \| T} (q_2^1, q_2^T)$ with $q_1^T = q_2^T$. From the construction of $R'$ we confirm that $((q_2^1, q_2^T), (q_2^2, q_2^T)) \in R'$.

- $i? \in Act_i^{S^1}$, $i \notin Act^{S^2}$, and $i? \in Act_i^T$. This case is infeasible, as Definition 6 of refinement requires that $Act_i^{S^1} \subseteq Act_i^{S^2}$.
- $i? \notin Act^{S^1}$, $i? \in Act_i^{S^2}$, and $i? \in Act_i^T$. In this case, it follows from Definition 15 that $q_1^2 \xrightarrow{i?}{}^{S^2} q_2^2$ and $q_1^T \xrightarrow{i?}{}^T q_2^T$. Now, using $R$ and Definition 6, it follows that $(q_2^1, q_2^2) \in R$ and $q_1^1 = q_2^1$. Thus, following Definition 15 again, we have that $(q_1^1, q_1^T) \xrightarrow{i?}{}^{S^1 \| T} (q_2^1, q_2^T)$ and $q_1^1 = q_2^1$. From the construction of $R'$ we confirm that $((q_2^1, q_2^T), (q_2^2, q_2^T)) \in R'$.
- $i? \notin Act^{S^1}$, $i? \notin Act^{S^2}$, and $i? \in Act_i^T$. In this case, it follows from Definition 15 that $q_1^T \xrightarrow{i?}{}^T q_2^T$ and $q_1^2 = q_2^2$. Following Definition 15 again, we have that $(q_1^1, q_1^T) \xrightarrow{i?}{}^{S^1 \| T} (q_2^1, q_2^T)$ and $q_1^1 = q_2^1$. From the construction of $R'$ we confirm that $((q_2^1, q_2^T), (q_2^2, q_2^T)) \in R'$.

So, in all feasible cases we can show that $(q_1^1, q_1^T) \xrightarrow{i?}{}^{S^1 \| T} (q_2^1, q_2^T)$ and $((q_2^1, q_2^T), (q_2^2, q_2^T)) \in R'$.

2. $(q_1^2, q_1^T) \xrightarrow{i?}{}^{S^2 \| T} (q_2^2, q_2^T)$ for some $(q_2^2, q_2^T) \in Q^{S^2 \| T}$ and $i? \in Act_i^{S^2 \| T} \setminus Act_i^{S^1 \| T}$. In this case it follows from Definition 6 and 15 that $i? \in Act_i^{S^2}$, $i? \notin Act_i^{S^1}$, and $i? \notin Act_i^T$. Therefore, from the same definitions, we have that $q_1^2 \xrightarrow{i?}{}^{S^2} q_2^2$ and $q_1^T = q_2^T$. Now, using $R$ and Definition 6, it follows that $(q_2^1, q_2^2) \in R$ and $q_1^1 = q_2^1$. From the construction of $R'$ we confirm that $((q_2^1, q_2^T), (q_2^2, q_2^T)) \in R'$.
3. $(q_1^1, q_1^T) \xrightarrow{o!}{}^{S^1 \| T} (q_2^1, q_2^T)$ for some $(q_2^1, q_2^T) \in Q^{S^1 \| T}$ and $o! \in Act_o^{S^1 \| T} \cap Act_o^{S^2 \| T}$. Consider the eight feasible combinations for output action $o!$ using Definition 15 such that $o! \in Act_o^{S^2 \| T} \cap Act_o^{S^1 \| T}$, already taking into account that if $o \in Act^{S^1}$ and $o \in Act^{S^2}$ then $o! \in Act_o^{S^1}$ and $o! \in Act_o^{S^2}$ or $o? \in Act_i^{S^1}$ and $o? \in Act_i^{S^2}$ (see Definition 6).
   - $o! \in Act_o^{S^1}$, $o! \in Act_o^{S^2}$, and $o \in Act^T$[8]. In this case, it follows from Definition 15 that $q_1^1 \xrightarrow{o!}{}^{S^1} q_2^1$ and $q_1^T \xrightarrow{o}{}^T q_2^T$. Now, using $R$ and Definition 6, it follows that $q_1^2 \xrightarrow{o!}{}^{S^2} q_2^2$ and $(q_2^1, q_2^2) \in R$. Thus, following Definition 15 again, we have that $(q_1^2, q_1^T) \xrightarrow{o!}{}^{S^2 \| T} (q_2^2, q_2^T)$. From the construction of $R'$ we confirm that $((q_2^1, q_2^T), (q_2^2, q_2^T)) \in R'$.
   - $o? \in Act_i^{S^1}$, $o? \in Act_i^{S^2}$, and $o! \in Act_o^T$. In this case, it follows from Definition 15 that $q_1^1 \xrightarrow{o?}{}^{S^1} q_2^1$ and $q_1^T \xrightarrow{o!}{}^T q_2^T$. As $S^2$ is input-enabled, it follows that $q_1^2 \xrightarrow{o?}{}^{S^2} q_2^2$ for some $q_2^2 \in Q^2$. Now, using $R$ and Definition 6, it follows that $(q_2^1, q_2^2) \in R$. Thus, following Definition 15 again, we have that $(q_1^2, q_1^T) \xrightarrow{o!}{}^{S^2 \| T} (q_2^2, q_2^T)$. From the construction of $R'$ we confirm that $((q_2^1, q_2^T), (q_2^2, q_2^T)) \in R'$.
   - $o! \in Act_o^{S^1}$, $o! \in Act_o^{S^2}$, and $o! \notin Act^T$. In this case, it follows from Definition 15 that $q_1^1 \xrightarrow{o!}{}^{S^1} q_2^1$ and $q_1^T = q_2^T$. Now, using $R$ and Definition 6,

[8] With this notation, we indicate that it does not matter whether $o! \in Act_o^T$ or $o? \in Act_i^T$.

it follows that $q_1^2 \xrightarrow{o!}{}^{S^2} q_2^2$ and $(q_2^1, q_2^2) \in R$. Thus, following Definition 15 again, we have that $(q_1^2, q_1^T) \xrightarrow{o!}{}^{S^2\|T} (q_2^2, q_2^T)$ with $q_1^T = q_2^T$. From the construction of $R'$ we confirm that $((q_2^1, q_2^T), (q_2^2, q_2^T)) \in R'$.

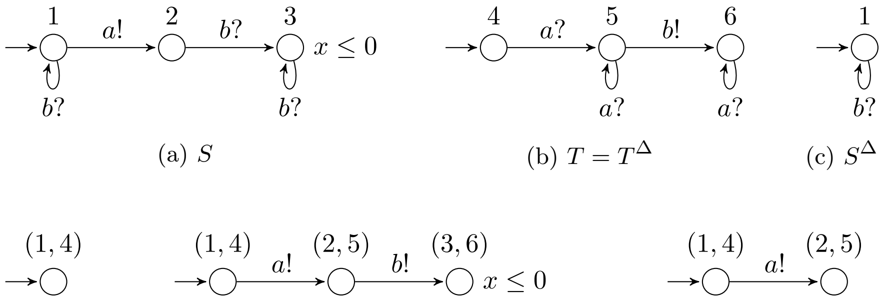
- $o! \in Act_o^{S^1}$, $o! \notin Act^{S^2}$, and $o! \in Act_o^T$. In this case, it follows from Definition 15 that $q_1^1 \xrightarrow{o!}{}^{S^1} q_2^1$ and $q_1^T \xrightarrow{o!}{}^{T} q_2^T$. Now, using $R$ and Definition 6, it follows that $(q_2^1, q_2^2) \in R$ and $q_1^2 = q_2^2$. Thus, following Definition 15 again, we have that $(q_1^2, q_1^T) \xrightarrow{o!}{}^{S^2\|T} (q_2^2, q_2^T)$ and $q_1^2 = q_2^2$. From the construction of $R'$ we confirm that $((q_2^1, q_2^T), (q_2^2, q_2^T)) \in R'$.
- $o? \in Act_i^{S^1}$, $o! \notin Act^{S^2}$, and $o! \in Act_o^T$. This case is infeasible, as Definition 6 of refinement requires that $Act_i^{S^1} \subseteq Act_i^{S^2}$.
- $o! \notin Act^{S^1}$, $o! \in Act_o^{S^2}$, and $o! \in Act_o^T$. This case is infeasible, as Definition 6 of refinement requires that $Act_o^{S^2} \subseteq Act_o^{S^1}$.
- $o! \notin Act^{S^1}$, $o? \in Act_i^{S^2}$, and $o! \in Act_o^T$. In this case, it follows from Definition 15 that $q_1^T \xrightarrow{o!}{}^{T} q_2^T$ and $q_1^1 = q_2^1$. As $S^2$ is input-enabled, it follows that $q_1^2 \xrightarrow{o?}{}^{S^2} q_2^2$ for some $q_2^2 \in Q^2$. Now, using $R$ and Definition 6, it follows that $(q_2^1, q_2^2) \in R$. Thus, following Definition 15 again, we have that $(q_1^2, q_1^T) \xrightarrow{o!}{}^{S^2\|T} (q_2^2, q_2^T)$. From the construction of $R'$ we confirm that $((q_2^1, q_2^T), (q_2^2, q_2^T)) \in R'$.
- $o! \notin Act^{S^1}$, $o! \notin Act^{S^2}$, and $o! \in Act_i^T$. In this case, it follows from Definition 15 that $q_1^T \xrightarrow{o!}{}^{T} q_2^T$ and $q_1^1 = q_2^1$. Following Definition 15 again, we have that $(q_1^2, q_1^T) \xrightarrow{o!}{}^{S^2\|T} (q_2^2, q_2^T)$ and $q_1^2 = q_2^2$. From the construction of $R'$ we confirm that $((q_2^1, q_2^T), (q_2^2, q_2^T)) \in R'$.

So, in all feasible cases we can show that $(q_1^2, q_1^T) \xrightarrow{o!}{}^{S^2\|T} (q_2^2, q_2^T)$ and $((q_2^1, q_2^T), (q_2^2, q_2^T)) \in R'$.

4. $(q_1^1, q_1^T) \xrightarrow{o!}{}^{S^1\|T} (q_2^1, q_2^T)$ for some $(q_2^1, q_2^T) \in Q^{S^1\|T}$ and $o! \in Act_o^{S^1\|T} \setminus Act_o^{S^2\|T}$. In this case it follows from Definitions 6 and 15 that $o! \in Act_o^{S^1}$, $o \notin Act^{S^2}$, and $o \notin Act^T$. Therefore, from the same definitions, we have that $q_1^1 \xrightarrow{o!}{}^{S^1} q_2^1$ and $q_1^T = q_2^T$. Now, using $R$ and Definition 6, it follows that $(q_2^1, q_2^2) \in R$ and $q_1^2 = q_2^2$. From the construction of $R'$ we confirm that $((q_2^1, q_2^T), (q_2^2, q_2^T)) \in R'$.
5. $(q_1^1, q_1^T) \xrightarrow{d}{}^{S^1\|T} (q_2^1, q_2^T)$ for some $(q_2^1, q_2^T) \in Q^{S^1\|T}$ and $d \in \mathbb{R}_{\geq 0}$. In this case, it follows from Definition 15 that $q_1^2 \xrightarrow{d}{}^{S^1} q_2^2$ and $q_1^T \xrightarrow{d}{}^{T} q_2^T$. Now, using $R$ and Definition 6, it follows that $q_1^2 \xrightarrow{d}{}^{S^2} q_2^2$ and $(q_2^1, q_2^2) \in R$. Thus, following Definition 15 again, we have that $(q_1^2, q_1^T) \xrightarrow{d}{}^{S^2\|T} (q_2^2, q_2^T)$. From the construction of $R'$ we confirm that $((q_2^1, q_2^T), (q_2^2, q_2^T)) \in R'$.

□

Adversarial pruning does not distribute over the parallel composition operator. Consider two composable specifications $S$ and $T$: $S^\Delta \parallel T^\Delta \neq (S \parallel T)^\Delta$. An example is shown in Figure 9. Observe that $S^\Delta \parallel T^\Delta$ (Figure 9d) does not allow any behavior from the initial state, while $(S \parallel T)^\Delta$ (Figure 9f) still allows action $a$ to be performed. If we want specification $S$ to never reach the




(a) $S$ (b) $T = T^{\Delta}$ (c) $S^{\Delta}$ (d) $S^{\Delta} \parallel T^{\Delta}$ (e) $S \parallel T$ (f) $(S \parallel T)^{\Delta}$

**Fig. 9**: Example showing that adversarial pruning does not distribute over the parallel composition operator. Observe that the result in (d) differs from the one in (f).

error state for *all* possible environments, we have to disable output action $a!$ from location 1. Yet, in the example we are composing $S$ with the specific environment $T$, which can help $S$ in avoiding the error state. Therefore, as long as we are composing components of a system together, we should not apply adversarial pruning on intermediate specifications.

We still would like to simplify intermediate specifications as much as possible before and after performing parallel composition without any loss of possible implementations. This is captured in the following definition of cooperative pruning.

**Definition 16** *Given a specification $S = (Q, s_0, Act, \rightarrow)$, the result of* cooperative pruning *of $S$, denoted by $S^{\forall}$, is a subspecification $S^{\forall} = (Q^{\forall}, s_0, Act, \rightarrow^{\forall})$ with $S^{\forall} \subseteq S$ and $\rightarrow^{\forall} \subseteq \rightarrow$ such that for all specifications $T$ composable with $S$ it holds that $[\![S \parallel T]\!]_{\mathrm{mod}} = [\![S^{\forall} \parallel T]\!]_{\mathrm{mod}}$*

Unfortunately, the best we can do, in the sense of removing states, transitions, or both, is to remove nothing, i.e., cooperative pruning is the identity transformation. We prove this with the following lemma.

**Lemma 10** *Given a specification $S = (Q^S, s_0, Act^S, \rightarrow^S)$ and its cooperatively pruned subspecification $S^{\forall}$. It holds that $S = S^{\forall}$.*

*Proof* The idea of pruning is to remove error states and related transitions from a specification that violate the independent progress property, as all states of any implementation of that specification need to have independent progress, see Definition 5. So, for a state $q_{\text{imerr}} \in \text{imerr}^S$ of $S$ (see Definition 10), it holds that $(\exists d \in \mathbb{R}_{\geq 0} : q_{\text{imerr}} \stackrel{d}{\not\longrightarrow}) \wedge \forall d \in \mathbb{R}_{\geq 0} \forall o! \in Act_o^S \forall q' \in Q^S : q_{\text{imerr}} \xrightarrow{d} q' \Rightarrow q' \stackrel{o!}{\not\longrightarrow}$.

Now, consider a specification $T = (t, t, Act^T, \rightarrow^T)$ with a single state $t$, $Act^T = Act_o^T = Act_i^S \cup \{\tau\}$ with $\tau \notin Act^S$, and $\rightarrow^T = \{(t, a, t) \mid a \in Act^T\} \cup \{(t, d, t) \mid d \in \mathbb{R}_{\geq 0}\}$. The unique event $\tau$ is present to ensure that the following argument holds in case $S$ does not have any input actions. In the composition $S \parallel T$, it still holds that $(q_{\text{imerr}}, t) \xrightarrow{d} (q', t)$ (see Definition 15). Since a specification is input enabled, Definition 4, we know that in the composition $S \parallel T$ there exist an output action $o! \in Act^T$ such that $(q', t) \xrightarrow{o!}$. Thus, in the composition $S \parallel T$, the state $(q_{\text{imerr}}, t)$ is no longer an immediate error state. As this holds for all $q_{\text{imerr}} \in \text{imerr}^S$, we have that $\text{imerr}^{S\parallel T} = \emptyset$. And once $\text{imerr}^{S\parallel T} = \emptyset$, we have that $\text{err}^{S\parallel T}(\emptyset) = \emptyset$ and therefore $\text{incons}^{S\parallel T} = \emptyset$ (using the fixed-point operator $\pi$). Thus for this $T$ we need to keep all states of $S$ in $S^\forall$ to ensure that $[\![S \parallel T]\!]_{\text{mod}} = [\![S^\forall \parallel T]\!]_{\text{mod}}$. □

We now switch to the symbolic representation. Parallel composition of two TIOA is defined in the following way.

**Definition 17** *Given two specification automata* $A^i = (Loc^i, q_0^i, Act^i, Clk^i, E^i, Inv^i), i = 1, 2$ *where* $Act_o^1 \cap Act_o^2 = \emptyset$*, the* parallel composition *of* $A^1$ *and* $A^2$*, denoted by* $A^1 \parallel A^2$*, is TIOA* $(Loc^1 \times Loc^2, (q_0^1, q_0^2), Act, Clk^1 \uplus Clk^2, E, Inv)$ *where* $Act = Act_i \uplus Act_o$ *with* $Act_i = (Act_i^1 \setminus Act_o^2) \cup (Act_i^2 \setminus Act_o^1)$ *and* $Act_o = Act_o^1 \cup Act_o^2$*,* $Inv((q^1, q^2)) = Inv(q^1) \wedge Inv(q^2)$*, and* $E$ *is defined as*

- $((q_1^1, q_1^2), a, \varphi^1 \wedge \varphi^2, c^1 \cup c^2, (q_2^1, q_2^2)) \in E$ *if* $a \in Act^1 \cap Act^2$*,* $(q_1^1, a, \varphi^1, c^1, q_2^1) \in E^1$*, and* $(q_1^1, a, \varphi^2, c^2, q_2^1) \in E^1$
- $((q_1^1, q^2), a, \varphi^1, c^1, (q_2^1, q^2)) \in E$ *if* $a \in Act^1 \setminus Act^2$*,* $(q_1^1, a, \varphi^1, c^1, q_2^1) \in E^1$*, and* $q^2 \in Loc^2$
- $((q^1, q_1^2), a, \varphi^2, c^2, (q^1, q_2^2)) \in E$ *if* $a \in Act^2 \setminus Act^1$*,* $(q_1^2, a, \varphi^2, c^2, q_2^2) \in E^2$*, and* $q^1 \in Loc^1$

Figure 10 shows the parallel composition Machine‖Researcher where Machine and Researcher are from Figure 1. As typical for composing automata, the parallel composition of Machine and Researcher looks much more complicated that the two individual specifications. Furthermore, the actions cof and tea, which were outputs in Machine and inputs in Researcher, have become outputs in the combined specification.

Finally, the following theorem lifts all the results from timed input/output transition systems to the symbolic representation level. Similarly to Theorem 7, we need to take the special case from Figure 8 into account (but now consider action $c$ to be an input for $A^2$). The transition in Figure 8 (e) from $(1, 4) \xrightarrow{a!} (2, 4)$ can be 'removed' with adversarial pruning by realizing that the target state $(2, 4)$ is an inconsistent state (you can see this by noticing that no time delay, including a zero time delay, is possible).

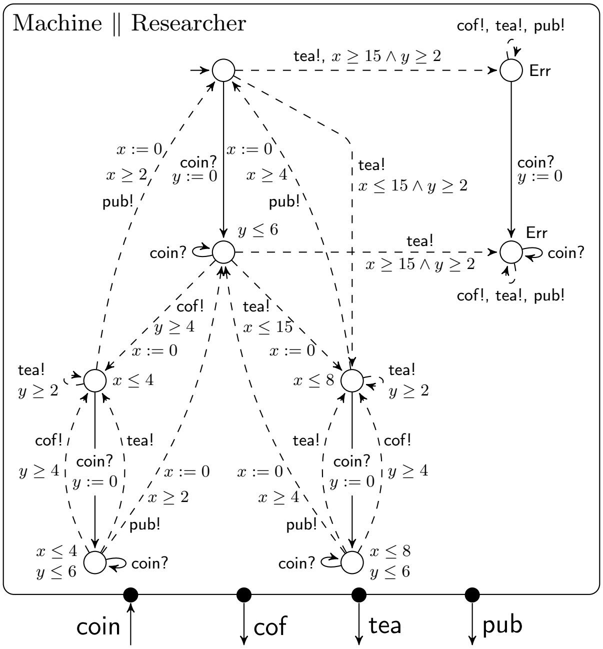



**Fig. 10**: The parallel composition of the Machine and Researcher from Figure 1.

**Theorem 9** *Given two specification automata* $A^i = (Loc^i, l_0^i, Act^i, Clk^i, E^i, Inv^i), i = 1, 2$ *where* $Act_o^1 \cap Act_o^2 = \emptyset$. *Then* $(\llbracket A^1 \parallel A^2 \rrbracket_{\text{sem}})^\Delta = (\llbracket A^1 \rrbracket_{\text{sem}} \parallel \llbracket A^2 \rrbracket_{\text{sem}})^\Delta$.

Before we can prove this theorem, we have to introduce several lemmas. These lemmas are almost identical to the ones in Section 3 for the conjunction. Therefore, we have omitted the proof.

**Lemma 11** *Given two TIOAs* $A^i = (Loc^i, l_0^i, Act^i, Clk^i, E^i, Inv^i), i = 1, 2$ *where* $Act_o^1 \cap Act_o^2 = \emptyset$. *Then* $Q^{\llbracket A^1 \parallel A^2 \rrbracket_{\text{sem}}} = Q^{\llbracket A^1 \rrbracket_{\text{sem}} \parallel \llbracket A^2 \rrbracket_{\text{sem}}}$ *and* $q_0^{\llbracket A^1 \parallel A^2 \rrbracket_{\text{sem}}} = q_0^{\llbracket A^1 \rrbracket_{\text{sem}} \parallel \llbracket A^2 \rrbracket_{\text{sem}}}$.

*Proof* The proof is exactly the same as the proof of Lemma 3 except replacing conjunction by parallel composition. □

**Lemma 12** *Given two TIOAs* $A^i = (Loc^i, l_0^i, Act^i, Clk^i, E^i, Inv^i), i = 1, 2$ *where* $Act_o^1 \cap Act_o^2 = \emptyset$. *Denote* $X = \llbracket A^1 \parallel A^2 \rrbracket_{\text{sem}}$ *and* $Y = \llbracket A^1 \rrbracket_{\text{sem}} \parallel \llbracket A^2 \rrbracket_{\text{sem}}$, *and let* $d \in \mathbb{R}_{\geq 0}$ *and* $q_1, q_2 \in Q^X \cap Q^Y$. *Then* $q_1 \xrightarrow{d}^X q_2$ *if and only if* $q_1 \xrightarrow{d}^Y q_2$.

*Proof* The proof is exactly the same as the proof of Lemma 4 except replacing conjunction by parallel composition. □

**Lemma 13** *Given two TIOAs* $A^i = (Loc^i, l_0^i, Act^i, Clk^i, E^i, Inv^i), i = 1, 2$ *where* $Act_o^1 \cap Act_o^2 = \emptyset$*. Denote* $X = [\![A^1 \parallel A^2]\!]_{\mathrm{sem}}$ *and* $Y = [\![A^1]\!]_{\mathrm{sem}} \parallel [\![A^2]\!]_{\mathrm{sem}}$*, and let* $a \in Act^1 \cap Act^2$ *and* $q_1, q_2 \in Q^X \cap Q^Y$*. Then* $q_1 \xrightarrow{a}^X q_2$ *if and only if* $q_1 \xrightarrow{a}^Y q_2$*.*

*Proof* The proof is exactly the same as the proof of Lemma 5 except replacing conjunction by parallel composition. □

**Lemma 14** *Given two TIOAs* $A^i = (Loc^i, l_0^i, Act^i, Clk^i, E^i, Inv^i), i = 1, 2$ *where* $Act_o^1 \cap Act_o^2 = \emptyset$*. Denote* $X = [\![A^1 \parallel A^2]\!]_{\mathrm{sem}}$ *and* $Y = [\![A^1]\!]_{\mathrm{sem}} \parallel [\![A^2]\!]_{\mathrm{sem}}$*, and let* $a \in Act^1 \setminus Act^2$ *and* $q_1, q_2 \in Q^X \cap Q^Y$*, where* $q_2 = (l_2^1, l_2^2, v_2)$*. If* $v_2 \models Inv^2(l_2)$*, then* $q_1 \xrightarrow{a}^X q_2$ *if and only if* $q_1 \xrightarrow{a}^Y q_2$*.*

*Proof* The proof is exactly the same as the proof of Lemma 6 except replacing conjunction by parallel composition. □

**Corollary 3** *Given two TIOAs* $A^i = (Loc^i, l_0^i, Act^i, Clk^i, E^i, Inv^i), i = 1, 2$ *where* $Act_o^1 \cap Act_o^2 = \emptyset$*. Denote* $X = [\![A^1 \parallel A^2]\!]_{\mathrm{sem}}$ *and* $Y = [\![A^1]\!]_{\mathrm{sem}} \parallel [\![A^2]\!]_{\mathrm{sem}}$*, and let* $a \in Act^1 \setminus Act^2$ *and* $q_1, q_2 \in Q^X \cap Q^Y$*. If* $q_1 \xrightarrow{a}^X q_2$*, then* $q_1 \xrightarrow{a}^Y q_2$*.*

*Proof* The proof is exactly the same as the proof of Corollary 1 except replacing conjunction by parallel composition. □

The following two lemmas consider the error states and consistent states, respectively, in $[\![A^1 \parallel A^2]\!]_{\mathrm{sem}}$ and $[\![A^1]\!]_{\mathrm{sem}} \parallel [\![A^2]\!]_{\mathrm{sem}}$. We can show that both sets are the same for $[\![A^1 \parallel A^2]\!]_{\mathrm{sem}}$ and $[\![A^1]\!]_{\mathrm{sem}} \parallel [\![A^2]\!]_{\mathrm{sem}}$.

**Lemma 15** *Given two TIOAs* $A^i = (Loc^i, l_0^i, Act^i, Clk^i, E^i, Inv^i), i = 1, 2$ *where* $Act_o^1 \cap Act_o^2 = \emptyset$*. Let* $Q \subseteq Loc^1 \times Loc^2 \times [(Clk^1 \cup Clk^2) \mapsto \mathbb{R}_{\geq 0}]$*. Then* $\mathrm{err}^{[\![A^1 \parallel A^2]\!]_{\mathrm{sem}}}(Q) = \mathrm{err}^{[\![A^1]\!]_{\mathrm{sem}} \parallel [\![A^2]\!]_{\mathrm{sem}}}(Q)$*.*

*Proof* The proof is exactly the same as the proof of Lemma 7 except replacing conjunction by parallel composition. □

**Lemma 16** *Given two TIOAs* $A^i = (Loc^i, l_0^i, Act^i, Clk^i, E^i, Inv^i), i = 1, 2$ *where* $Act_o^1 \cap Act_o^2 = \emptyset$*. Then* $\mathrm{cons}^{[\![A^1 \| A^2]\!]_{\mathrm{sem}}} = \mathrm{cons}^{[\![A^1]\!]_{\mathrm{sem}} \| [\![A^2]\!]_{\mathrm{sem}}}$*.*

*Proof* The proof is exactly the same as the proof of Lemma 8 except replacing conjunction by parallel composition. □

Finally, we are ready to proof Theorem 9.

*Proof of Theorem 9* We will prove this theorem by showing that $([\![A^1 \parallel A^2]\!]_{\mathrm{sem}})^{\Delta}$ and $([\![A^1]\!]_{\mathrm{sem}} \parallel [\![A^2]\!]_{\mathrm{sem}})^{\Delta}$ have the same set of states, same initial state, same set of actions, and same transition relation.

It follows from Lemma 11 that $[\![A^1 \parallel A^2]\!]_{\mathrm{sem}}$ and $[\![A^1]\!]_{\mathrm{sem}} \parallel [\![A^2]\!]_{\mathrm{sem}}$ have the same state set and initial state. As $\mathrm{cons}^{[\![A^1 \| A^2]\!]_{\mathrm{sem}}} = \mathrm{cons}^{[\![A^1]\!]_{\mathrm{sem}} \| [\![A^2]\!]_{\mathrm{sem}}} = \mathrm{cons}$ from Lemma 16, it follows that $([\![A^1 \parallel A^2]\!]_{\mathrm{sem}})^{\Delta}$ and $([\![A^1]\!]_{\mathrm{sem}} \parallel [\![A^2]\!]_{\mathrm{sem}})^{\Delta}$ have the same state set and initial state. Also, observe that the semantic of a TIOA and adversarial pruning do not alter the action set. Therefore, it follows directly that $([\![A^1 \parallel A^2]\!]_{\mathrm{sem}})^{\Delta}$ and $([\![A^1]\!]_{\mathrm{sem}} \parallel [\![A^2]\!]_{\mathrm{sem}})^{\Delta}$ have the same action set and partitioning into input and output actions.

It remains to show that $([\![A^1 \parallel A^2]\!]_{\mathrm{sem}})^{\Delta}$ and $([\![A^1]\!]_{\mathrm{sem}} \parallel [\![A^2]\!]_{\mathrm{sem}})^{\Delta}$ have the same transition relation. In the remainder of the proof, we will use $v^1$ and $v^2$ to indicate the part of a valuation $v$ of only the clocks of $A^1$ and $A^2$, respectively. Also, for brevity we write $X = ([\![A^1 \parallel A^2]\!]_{\mathrm{sem}})^{\Delta}$, $Y = ([\![A^1]\!]_{\mathrm{sem}} \parallel [\![A^2]\!]_{\mathrm{sem}})^{\Delta}$, and $Clk = Clk^1 \uplus Clk^2$ in the rest of this proof.

($\Rightarrow$) Assume a transition $q_1^X \xrightarrow{a} q_2^X$ in $X$. From Definition 12 it follows that $q_1^X \xrightarrow{a} q_2^X$ in $[\![A^1 \parallel A^2]\!]_{\mathrm{sem}}$ and $q_2^X \in \mathrm{cons}$. Following Definition 3 of the semantic, it follows that there exists an edge $(l_1, a, \varphi, c, l_2) \in E^{A^1 \| A^2}$ with $q_1^X = (l_1, v_1)$, $q_2^X = (l_2, v_2)$, $l_1, l_2 \in Loc^{A^1 \| A^2}$, $v_1, v_2 \in [Clk \mapsto \mathbb{R}_{\geq 0}]$, $v_1 \models \varphi$, $v_2 = v_1[r \mapsto 0]_{r \in c}$, and $v_2 \models Inv(l_2)$. Now we consider the three cases of Definition 17 of the parallel composition for TIOA.

- $a \in Act^1 \cap Act^2$. It follows directly from Lemma 13 that $q_1^X \xrightarrow{a} q_2^X$ is a transition in $[\![A^1]\!]_{\mathrm{sem}} \parallel [\![A^2]\!]_{\mathrm{sem}}$. Since $q_2^X \in \mathrm{cons}$, it holds that $q_1^X \xrightarrow{a} q_2^X$ is a transition in $Y$.
- $a \in Act^1 \setminus Act^2$. It follows directly from Corollary 3 that $q_1^X \xrightarrow{a} q_2^X$ is a transition in $[\![A^1]\!]_{\mathrm{sem}} \parallel [\![A^2]\!]_{\mathrm{sem}}$. Since $q_2^X \in \mathrm{cons}$, it holds that $q_1^X \xrightarrow{a} q_2^X$ is a transition in $Y$.
- $a \in Act^2 \setminus Act^1$. It follows directly from Corollary 3 (where we switched $A^1$ and $A^2$) that $q_1^X \xrightarrow{a} q_2^X$ is a transition in $[\![A^1]\!]_{\mathrm{sem}} \parallel [\![A^2]\!]_{\mathrm{sem}}$. Since $q_2^X \in \mathrm{cons}$, it holds that $q_1^X \xrightarrow{a} q_2^X$ is a transition in $Y$.

Now consider that $a$ is a delay $d$. It follows directly from Lemma 12 that $q_1^X \xrightarrow{d} q_2^X$ is a transition in $[\![A^1]\!]_{\mathrm{sem}} \parallel [\![A^2]\!]_{\mathrm{sem}}$. Since $q_2^X \in \mathrm{cons}$, it holds that $q_1^X \xrightarrow{d} q_2^X$ is a transition in $Y$.

We have shown that when $q_1^X \xrightarrow{a} q_2^X$ is a transition in $X = ([\![A^1 \parallel A^2]\!]_{\mathrm{sem}})^{\Delta}$, it holds that $q_1^X \xrightarrow{a} q_2^X$ is a transition in $Y = ([\![A^1]\!]_{\mathrm{sem}} \parallel [\![A^2]\!]_{\mathrm{sem}})^{\Delta}$. Since the transition is arbitrarily chosen, it holds for all transitions in $X$.

($\Leftarrow$) Assume a transition $q_1^Y \xrightarrow{a} q_2^Y$ in $Y$. From Definition 12 it follows that $q_1^Y \xrightarrow{a} q_2^Y$ in $[\![A^1]\!]_{\text{sem}} \wedge [\![A^2]\!]_{\text{sem}}$ and $q_2^Y \in \text{cons}$. Now we consider the three cases of Definition 15 of the parallel composition for TIOTS.

- $a \in Act^1 \cap Act^2$. It follows directly from Lemma 13 that $q_1^Y \xrightarrow{a} q_2^Y$ is a transition in $[\![A^1 \parallel A^2]\!]_{\text{sem}}$. Since $q_2^Y \in \text{cons}$, it holds that $q_1^Y \xrightarrow{a} q_2^Y$ is a transition in $X$.
- $a \in Act^1 \setminus Act^2$. From time reflexivity of Definition 1 we have that $q_2^Y \xrightarrow{d}$ with $d = 0$. From Definitions 12 and 15 it follows that $q_2^{[\![A^1]\!]_{\text{sem}}} \xrightarrow{d}$ and $q^{[\![A^2]\!]_{\text{sem}}} \xrightarrow{d}$. Now, from Definition 3 it follows that $v^2 + d \models Inv^2(l^2)$, i.e., $v^2 \models Inv^2(l^2)$. It now follows directly from Lemma 14 that $q_1^Y \xrightarrow{a} q_2^Y$ is a transition in $[\![A^1 \parallel A^2]\!]_{\text{sem}}$. Since $q_2^Y \in \text{cons}$, it holds that $q_1^Y \xrightarrow{a} q_2^Y$ is a transition in $X$.
- $a \in Act^2 \setminus Act^1$. From time reflexivity of Definition 1 we have that $q_2^Y \xrightarrow{d}$ with $d = 0$. From Definitions 12 and 15 it follows that $q^{[\![A^1]\!]_{\text{sem}}} \xrightarrow{d}$ and $q_2^{[\![A^2]\!]_{\text{sem}}} \xrightarrow{d}$. Now, from Definition 3 it follows that $v^1 + d \models Inv^1(l^1)$, i.e., $v^1 \models Inv^1(l^1)$. It now follows directly from Lemma 14 (where we switched $A^1$ and $A^2$) that $q_1^Y \xrightarrow{a} q_2^Y$ is a transition in $[\![A^1 \parallel A^2]\!]_{\text{sem}}$. Since $q_2^Y \in \text{cons}$, it holds that $q_1^Y \xrightarrow{a} q_2^Y$ is a transition in $X$.

Now consider that $a$ is a delay $d$. It follows directly from Lemma 12 that $q_1^Y \xrightarrow{d} q_2^Y$ is a transition in $[\![A^1 \parallel A^2]\!]_{\text{sem}}$. Since $q_2^Y \in \text{cons}$, it holds that $q_1^Y \xrightarrow{d} q_2^Y$ is a transition in $X$.

We have shown that when $q_1^Y \xrightarrow{a} q_2^Y$ is a transition in $Y = [\![A^1]\!]_{\text{sem}} \parallel [\![A^2]\!]_{\text{sem}}$, it holds that $q_1^Y \xrightarrow{a} q_2^Y$ is a transition in $X = [\![A^1 \parallel A^2]\!]_{\text{sem}}$. Since the transition is arbitrarily chosen, it holds for all transitions in $Y$. □

**Corollary 4** *Given two specification automata* $A^i = (Loc^i, l_0^i, Act^i, Clk^i, E^i, Inv^i), i = 1,2$ *where* $Act_o^1 \cap Act_o^2 = \emptyset$ *and* $Act^1 = Act^2$*. Then* $[\![A^1 \parallel A^2]\!]_{\text{sem}} = [\![A^1]\!]_{\text{sem}} \parallel [\![A^2]\!]_{\text{sem}}$*.*

*Proof* This corollary follows directly as a special case from the proof of Theorem 9. The special case only depends on Lemmas 11 and 13, which do not require adversarial pruning to be applied. □

# 5 Quotient

An essential operator in a complete specification theory is the one of *quotienting*. It allows for factoring out behavior from a larger component. If one has a large component specification $T$ and a small one $S$ then $T \backslash\backslash S$ is the specification of exactly those components that when composed with $S$ refine $T$. In other words, $T \backslash\backslash S$ specifies the work that still needs to be done, given availability of an implementation of $S$, in order to provide an implementation of $T$.

We proceed like for structural and logical compositions and start with a quotient that may introduce error states. Those errors can then pruned.

**Definition 18** *Given specifications* $S = (Q^S, q_0^S, Act^S, \rightarrow^S)$ *and* $T = (Q^T, q_0^T, Act^T, \rightarrow^T)$ *where* $Act_o^S \cap Act_i^T = \emptyset$. *The* quotient of $T$ and $S$, *denoted by* $T \backslash\backslash S$, *is a specification* $(Q^T \times Q^S \cup \{u, e\}, (q_0^T, q_0^S), Act, \rightarrow)$ *where* $u$ *is the universal state,* $e$ *the inconsistent state,* $Act = Act_i \uplus Act_o$ *with* $Act_i = Act_i^T \cup Act_o^S$ *and* $Act_o = Act_o^T \setminus Act_o^S \cup Act_i^S \setminus Act_i^T$, *and* $\rightarrow$ *is defined as*

1. $(q_1^T, q_1^S) \xrightarrow{a} (q_2^T, q_2^S)$ *if* $a \in Act^S \cap Act^T$, $q_1^T \xrightarrow{a}^T q_2^T$, *and* $q_1^S \xrightarrow{a}^S q_2^S$
2. $(q^T, q_1^S) \xrightarrow{a} (q^T, q_2^S)$ *if* $a \in Act^S \setminus Act^T$, $q^T \in Q^T$, *and* $q_1^S \xrightarrow{a}^S q_2^S$
3. $(q_1^T, q^S) \xrightarrow{a} (q_2^T, q^S)$ *if* $a \in Act^T \setminus Act^S$, $q^S \in Q^S$, *and* $q_1^T \xrightarrow{a}^T q_2^T$
4. $(q_1^T, q_1^S) \xrightarrow{d} (q_2^T, q_2^S)$ *if* $d \in \mathbb{R}_{\geq 0}$, $q_1^T \xrightarrow{d}^T q_2^T$, *and* $q_1^S \xrightarrow{d}^S q_2^S$
5. $(q^T, q^S) \xrightarrow{a} u$ *if* $a \in Act_o^S$, $q^T \in Q^T$, *and* $q^S \not\xrightarrow{a}^S$
6. $(q^T, q^S) \xrightarrow{d} u$ *if* $d \in \mathbb{R}_{\geq 0}$, $q^T \in Q^T$, *and* $q^S \not\xrightarrow{d}^S$
7. $(q^T, q^S) \xrightarrow{a} e$ *if* $a \in Act_o^S \cap Act_o^T$, $q^T \not\xrightarrow{a}^T$, *and* $q^S \xrightarrow{a}^S$
8. $(q^T, q^S) \xrightarrow{a} (q^T, q^S)$ *if* $a \in Act_o^S \cap Act_o^T$, $q^T \not\xrightarrow{a}^T$, *and* $q^S \not\xrightarrow{a}^S$[9]
9. $u \xrightarrow{a} u$ *if* $a \in Act \cup \mathbb{R}_{\geq 0}$
10. $e \xrightarrow{a} e$ *if* $a \in Act_i$

In this definition, $u$ and $e$ are fresh states such that $u$ is universal (allows arbitrary behaviour) and $e$ is inconsistent (no output-controllable behaviour can satisfy it). State $e$ disallows progress of time and has no output transitions. The universal state guarantees nothing about the behaviour of its implementations (thus any refinement with a suitable alphabet is possible), and dually the inconsistent state allows no implementations.

The first four rules are part of the standard rules of parallel composition, see Definition 15. Rules 5 and 6 capture the situation where $S$ does not allow a particular output action or delay, respectively, so the parallel composition of $S$ and the quotient also does not allow this to happen. Therefore, it technically does not matter what the quotient does after performing these transitions, hence they go to the universal state $u$. Rule 7 captures the situation that an output shared between $S$ and $T$ as causes a problem in the refinement $S \leq T$ as $T$ is blocking the output. Thus the quotient, representing the missing component put into parallel composition with $S$, needs to block $S$ from performing this output action. But the output action has become an input action in the quotient, so we redirect this output to the error state to 'memorize' this problem. Rule 8 complements rule 7 in the sense that it ensures that the quotient is actually input enabled by construction. Finally, rules 9 and 10 simply express what we mean by universal and error state, respectively.

Theorem 10 states that the proposed quotient operator has exactly the property that it is dual of structural composition with regards to refinement.

[9] This ensures that the quotient is input enabled.

**Lemma 17** *For any two specifications $S$ and $T$ such that the quotient $T\backslash\backslash S$ is defined, and for any implementation $X$ over the same alphabet as $T\backslash\backslash S$, we have that $S \parallel X$ is defined, $Act_i^{S\parallel X} = Act_i^T$ and $Act_0^{S\parallel X} = Act_o^S \cup Act_o^T \cup Act_i^S \setminus Act_i^T$.*

*Proof* We will first show that $S \parallel X$ is defined. This boils down to show that $S$ and $X$ are composable., i.e., $Act_o^S \cap Act_o^X = \emptyset$. From Definition 18 and the assumption that $X$ has the same alphabet as $T\backslash\backslash S$, it follows that $Act_o^X = Act_o^T \setminus Act_o^S \cup Act_i^S \setminus Act_i^T$. Thus it holds that $Act_o^S \cap Act_o^X = \emptyset$.

To show that $Act_i^{S\parallel X} = Act_i^T$, we follow Definition 15 of the parallel composition and Definition 18 of the quotient and use careful rewriting to get to this conclusion.

$$\begin{aligned}
Act_i^{S\parallel X} &= Act_i^S \setminus Act_o^X \cup Act_i^X \setminus Act_o^S \\
&= Act_i^S \setminus (Act_o^T \setminus Act_o^S \cup Act_i^S \setminus Act_i^T) \cup (Act_i^T \cup Act_o^S) \setminus Act_o^S \\
&= Act_i^S \setminus (Act_o^T \setminus Act_o^S \cup Act_i^S \setminus Act_i^T) \cup Act_i^T \setminus Act_o^S \cup Act_o^S \setminus Act_o^S \\
&= Act_i^S \setminus (Act_o^T \setminus Act_o^S \cup Act_i^S \setminus Act_i^T) \cup Act_i^T \\
&= \Big(Act_i^S \setminus (Act_o^T \setminus Act_o^S) \cap Act_i^S \setminus (Act_i^S \setminus Act_i^T)\Big) \cup Act_i^T \\
&= \Big(Act_i^S \setminus (Act_o^T \setminus Act_o^S) \cap Act_i^S \cap Act_i^T\Big) \cup Act_i^T \\
&= \Big(\big((Act_i^S \cap Act_o^S) \cup (Act_i^S \setminus Act_o^T)\big) \cap Act_i^S \cap Act_i^T\Big) \cup Act_i^T \\
&= \Big(Act_i^S \setminus Act_o^T \cap Act_i^S \cap Act_i^T\Big) \cup Act_i^T \\
&= \Big(Act_i^S \cap Act_i^S \cap Act_i^T\Big) \setminus Act_o^T \cup Act_i^T \\
&= \Big(Act_i^S \cap Act_i^T\Big) \setminus Act_o^T \cup Act_i^T \\
&= \Big(Act_i^S \cap (Act_i^T \setminus Act_o^T)\Big) \cup Act_i^T \\
&= \Big(Act_i^S \cap Act_i^T\Big) \cup Act_i^T \\
&= Act_i^T
\end{aligned}$$

To show that $Act_0^{S\parallel X} = Act_o^S \cup Act_o^T \cup Act_i^S \setminus Act_i^T$, we follow again Definition 15 of the parallel composition and Definition 18 of the quotient and use careful rewriting to get to this conclusion.

$$\begin{aligned}
Act_0^{S\parallel X} &= Act_o^S \cup Act_o^X \\
&= Act_o^S \cup (Act_o^T \setminus Act_o^S \cup Act_i^S \setminus Act^T) \\
&= Act_o^S \cup Act_o^T \cup Act_i^S \setminus Act_i^T
\end{aligned}$$

□

**Theorem 10** *For any two specifications $S$ and $T$ such that the quotient $T\backslash\backslash S$ is defined, and for any implementation $X$ over the same alphabet as $T\backslash\backslash S$, we have that $S \parallel X$ is defined and $S \parallel X \leq T$ iff $X \leq T\backslash\backslash S$.*

*Proof* It is shown in Lemma 17 that $S \parallel X$ is defined. The alphabet pre-condition of Definition 6 is satisfied for $X \leq T\backslash\backslash S$ by definition of $X$; using Lemma 17 we can see that this is also the case for $S \parallel X \leq T$. So we only have to show that $S \parallel X \leq T$ iff $X \leq T\backslash\backslash S$.

($S \parallel X \leq T \Rightarrow X \leq T\backslash\backslash S$) Since $S \parallel X \leq T$, it follows from Definition 6 of refinement that there exists a relation $R \in Q^{S\parallel X} \times Q^T$ that witness the refinement. Note that $Q^{S\parallel X} = Q^S \times Q^X$ according to Definition 15. Construct relation $R' = \{(q_1^X, (q_1^T, q_1^S)) \in Q^X \times Q^{T\backslash\backslash S} \mid ((q_1^S, q_1^X), q_1^T) \in R\} \cup \{(q_1^X, u) \in Q^X \times Q^{T\backslash\backslash S} \mid q_1^X \in Q^X\}$. We will show that $R'$ witnesses $X \leq T\backslash\backslash S$. First consider the five cases of Definition 6 for a state pair $(q_1^X, (q_1^T, q_1^S)) \in R'$.

1. $(q_1^T, q_1^S) \xrightarrow{i?}{}^{T\backslash\backslash S} (q_2^T, q_2^S)$ for some $(q_2^T, q_2^S) \in Q^{T\backslash\backslash S}$ and $i? \in Act_i^{T\backslash\backslash S} \cap Act_i^X$. By definition of $X$ it follows that $Act_i^{T\backslash\backslash S} = Act_i^X$. Consider the following five possible cases from Definition 18 of the quotient that might result in $i? \in Act_i^{T\backslash\backslash S} (= Act_i^T \cup Act_o^S)$.
    - $i? \in Act_i^T$ and $i! \in Act_o^S$. This case is actually not feasible, since Definition 18 also requires that $Act_o^S \cap Act_i^T = \emptyset$.
    - $i? \in Act_i^T$ and $i? \in Act_i^S$. In this case, it follows from Definition 18 that $q_1^T \xrightarrow{i?}{}^T q_2^T$ and $q_1^S \xrightarrow{i?}{}^S q_2^S$. Now, using $R$, the first case of Definition 6 of refinement, and the fact that $Act_i^{S\parallel X} = Act_i^T$ (Lemma 17) it follows that $(q_1^S, q_1^X) \xrightarrow{i?}{}^{S\parallel X} (q_2^S, q_2^X)$ and $((q_2^S, q_2^X), q_2^T) \in R$. From Definition 15 of parallel composition it follows that $q_1^X \xrightarrow{i?}{}^X q_2^X$. From the construction of $R'$ we confirm that $(q_2^X, (q_2^T, q_2^S)) \in R'$.
    - $i? \in Act_i^T$ and $i? \notin Act^S$. In this case, it follows from Definition 18 that $q_1^T \xrightarrow{i?}{}^T q_2^T$ and $q_1^S = q_2^S$. Now, using $R$, the first case of Definition 6 of refinement, and the fact that $Act_i^{S\parallel X} = Act_i^T$ (Lemma 17) it follows that $(q_1^S, q_1^X) \xrightarrow{i?}{}^{S\parallel X} (q_2^S, q_2^X)$ and $((q_2^S, q_2^X), q_2^T) \in R$. From Definition 15 of parallel composition it follows that $q_1^X \xrightarrow{i?}{}^X q_2^X$. From the construction of $R'$ we confirm that $(q_2^X, (q_2^T, q_2^S)) \in R'$.
    - $i! \in Act_o^T$ and $i! \in Act_o^S$. In this case, it follows from Definition 18 that $q_1^T \xrightarrow{i!}{}^T q_2^T$ and $q_1^S \xrightarrow{i!}{}^S q_2^S$. Since $X$ is an implementation and $i? \in Act_i^X$, it follows that $q_1^X \xrightarrow{i?}{}^X q_2^X$ for some $q_2^X \in Q^X$ (any implementation is a specification, see Definition 5, which is input-enabled, see Definition 4). Now, using Definition 15 of parallel composition it follows that $(q_1^S, q_1^X) \xrightarrow{i!}{}^{S\parallel X} (q_2^S, q_2^X)$. Using $R$ and the third case of Definition 6 of refinement, it follows that $((q_2^S, q_2^X), q_2^T) \in R$. Thus from the construction of $R'$ we confirm that $(q_2^X, (q_2^T, q_2^S)) \in R'$.
    - $i! \notin Act^T$ and $i! \in Act_o^S$. In this case, it follows from Definition 18 that $q_1^S \xrightarrow{i!}{}^S q_2^S$ and $q_1^T = q_2^T$. Since $X$ is an implementation and $i? \in Act_i^X$, it follows that $q_1^X \xrightarrow{i?}{}^X q_2^X$ for some $q_2^X \in Q^X$ (any implementation is a specification, see Definition 5, which is input-enabled, see Definition 4). Now, using Definition 15 of parallel composition it follows that $(q_1^S, q_1^X) \xrightarrow{i!}{}^{S\parallel X} (q_2^S, q_2^X)$. Using $R$ and the forth case of Definition 6 of refinement, it follows that $((q_2^S, q_2^X), q_2^T) \in R$. Thus from the construction of $R'$ we confirm that $(q_2^X, (q_2^T, q_2^S)) \in R'$.

So, in all feasible cases we can show that $q_1^X \xrightarrow{i?}{}^X q_2^X$ and $(q_2^X, (q_2^T, q_2^S)) \in R'$.

2. $(q_1^T, q_1^S) \xrightarrow{i?}{}^{T\backslash\backslash S} (q_2^T, q_2^S)$ for some $(q_2^T, q_2^S) \in Q^{T\backslash\backslash S}$ and $i? \in Act_i^{T\backslash\backslash S} \setminus Act_i^X$. By definition of $X$ it follows that $Act_i^{T\backslash\backslash S} \setminus Act_i^X = \emptyset$, so this case can be ignored.

3. $q_1^X \xrightarrow{o!}{}^X q_2^X$ for some $q_2^X \in Q^X$ and $o! \in Act_o^X \cap Act_o^{T\backslash\backslash S}$. By definition of $X$ it follows that $Act_o^X = Act_o^{T\backslash\backslash S}$. Consider the following five possible cases from Definition 18 of the quotient that might result in $o! \in Act_o^{T\backslash\backslash S} (= Act_o^T \setminus Act_o^S \cup Act_i^S \setminus Act_i^T)$.
   - $o! \in Act_o^T \setminus Act_o^S$ and $o? \in Act_i^S \setminus Act_i^T$. It follows from Definition 4 of a specification that $S$ is input-enabled. Therefore, there is a transition $q_1^S \xrightarrow{o?}{}^S q_2^S$ for some $q_2^S \in Q^S$. Now, from Definition 15 of parallel composition it follows that there is a transition $(q_1^S, q_1^X) \xrightarrow{o!}{}^{S\|X} (q_2^S, q_2^X)$. Using $R$ and the third case of Definition 6 of refinement, it follows that $q_1^T \xrightarrow{o!}{}^T q_2^T$ and $((q_2^S, q_2^X), q_2^T) \in R$. Now, using Definition 18 of the quotient, it follows that $(q_1^T, q_1^S) \xrightarrow{o!}{}^{T\backslash\backslash S} (q_2^T, q_2^S)$. And from the construction of $R'$ we confirm that $(q_2^X, (q_2^T, q_2^S)) \in R'$.
   - $o! \in Act_o^T \setminus Act_o^S$ and $o? \in Act_i^S \cap Act_i^T$. This case is not feasible, as an action cannot be both an output and input in $T$.
   - $o! \in Act_o^T \setminus Act_o^S$ and $o? \notin Act_i^S$. In this case, it follows that $o \notin Act^S$ at all. Then from Definition 15 it follows that there is a transition $(q_1^S, q_1^X) \xrightarrow{i?}{}^{S\|X} (q_2^S, q_2^X)$ and $q_1^S = q_2^S$. Using $R$ and the third case of Definition 6 of refinement, it follows that $q_1^T \xrightarrow{o!}{}^T q_2^T$ and $((q_2^S, q_2^X), q_2^T) \in R$. Now, using Definition 18 of the quotient, it follows that $(q_1^T, q_1^S) \xrightarrow{o!}{}^{T\backslash\backslash S} (q_2^T, q_2^S)$. And from the construction of $R'$ we confirm that $(q_2^X, (q_2^T, q_2^S)) \in R'$.
   - $o! \in Act_o^T \cap Act_o^S$ and $o? \in Act_i^S \setminus Act_i^T$. This case is not feasible, as an action cannot be both an output and input in $S$.
   - $o! \notin Act_o^T$ and $o? \in Act_i^S \setminus Act_i^T$. It follows from Definition 4 of a specification that $S$ is input-enabled. Therefore, there is a transition $q_1^S \xrightarrow{o?}{}^S q_2^S$ for some $q_2^S \in Q^S$. Now, from Definition 15 of parallel composition it follows that there is a transition $(q_1^S, q_1^X) \xrightarrow{i?}{}^{S\|X} (q_2^S, q_2^X)$. Using $R$ and the forth case of Definition 6 of refinement, it follows that $q_1^T = q_2^T$ and $((q_2^S, q_2^X), q_2^T) \in R$. Now, using Definition 18 of the quotient, it follows that $(q_1^T, q_1^S) \xrightarrow{o!}{}^{T\backslash\backslash S} (q_2^T, q_2^S)$. And from the construction of $R'$ we confirm that $(q_2^X, (q_2^T, q_2^S)) \in R'$.

   So, in all feasible cases we can show that $(q_1^T, q_1^S) \xrightarrow{o!}{}^{T\backslash\backslash S} (q_2^T, q_2^S)$ and $(q_2^X, (q_2^T, q_2^S)) \in R'$.

4. $q_1^X \xrightarrow{o!}{}^X q_2^X$ for some $q_2^X \in Q^X$ and $o! \in Act_o^X \setminus Act_o^{T\backslash\backslash S}$. By definition of $X$ it follows that $Act_o^X \setminus Act_o^{T\backslash\backslash S} = \emptyset$, so this case can be ignored.

5. $q_1^X \xrightarrow{d}{}^X q_2^X$ for some $q_2^X \in Q^X$ and $d \in \mathbb{R}_{\geq 0}$. Consider two cases in $S$.
   - $q_1^S \xrightarrow{d}{}^S$. In this case, there exists some $q_2^S \in Q^S$ such that $q_1^S \xrightarrow{d}{}^S q_2^S$. Now, from Definition 15 of parallel composition it follows that there is a transition $(q_1^S, q_1^X) \xrightarrow{d}{}^{S\|X} (q_2^S, q_2^X)$. Using $R$ and the fifth

case of Definition 6 of refinement, it follows that $q_1^T \xrightarrow{d}{}^T q_2^T$ and $((q_2^S, q_2^X), q_2^T) \in R$. Now, using Definition 18 of the quotient, it follows that $(q_1^T, q_1^S) \xrightarrow{d}{}^{T\backslash\backslash S} (q_2^T, q_2^S)$. And from the construction of $R'$ we confirm that $(q_2^X, (q_2^T, q_2^S)) \in R'$.

- $q_1^S \not\xrightarrow{d}{}^S$. In this case, it follows from Definition 15 of parallel composition that there is no transition in $S \parallel X$, i.e., $(q_1^S, q_1^X) \not\xrightarrow{d}{}^{S\parallel X}$. Furthermore, from Definition 18 it follows that $(q_1^T, q_1^S) \xrightarrow{d}{}^{T\backslash\backslash S} u$. And from the construction of $R'$ we confirm that $(q_2^X, u) \in R'$.

So, in both cases we can show that $(q_1^T, q_1^S) \xrightarrow{d}{}^{T\backslash\backslash S} (q_2^X, q^{T\backslash\backslash S})$ and $(q_2^X, q^{T\backslash\backslash S}) \in R'$ with $q^{T\backslash\backslash S} = (q_2^T, q_2^S)$ or $q^{T\backslash\backslash S} = u$.

So for all state pairs $(q_1^X, (q_1^T, q_1^S)) \in R'$ we have shown that $R'$ witnesses the refinement $X \leq T\backslash\backslash S$. Now consider the five cases of Definition 6 for a state pair $(q_1^X, u) \in R'$.

1. $u \xrightarrow{i?}{}^{T\backslash\backslash S} u$ for some $i? \in Act_i^{T\backslash\backslash S} \cap Act_i^X$. By definition of $X$ it follows that $Act_i^{T\backslash\backslash S} = Act_i^X$. Since $X$ is an implementation and $i? \in Act_i^X$, it follows that $q_1^X \xrightarrow{i?}{}^X q_2^X$ for some $q_2^X \in Q^X$ (any implementation is a specification, see Definition 5, which is input-enabled, see Definition 4). By construction of $R'$ it follows that $(q_2^X, u) \in R'$.
2. $u \xrightarrow{i?}{}^{T\backslash\backslash S} u$ for some $i? \in Act_i^{T\backslash\backslash S} \setminus Act_i^X$. By definition of $X$ it follows that $Act_i^{T\backslash\backslash S} \setminus Act_i^X = \emptyset$, so this case can be ignored.
3. $q_1^X \xrightarrow{o!}{}^X q_2^X$ for some $q_2^X \in Q^X$ and $o! \in Act_o^X \cap Act_o^{T\backslash\backslash S}$. By definition of $X$ it follows that $Act_o^X = Act_o^{T\backslash\backslash S}$. From Definition 18 of the quotient it follows that $u \xrightarrow{o!}{}^{T\backslash\backslash S} u$. By construction of $R'$ it also follows that $(q_2^X, u) \in R'$.
4. $q_1^X \xrightarrow{o!}{}^X q_2^X$ for some $q_2^X \in Q^X$ and $o! \in Act_o^X \setminus Act_o^{T\backslash\backslash S}$. By definition of $X$ it follows that $Act_o^X \setminus Act_o^{T\backslash\backslash S} = \emptyset$, so this case can be ignored.
5. $q_1^X \xrightarrow{d}{}^X q_2^X$ for some $q_2^X \in Q^X$ and $d \in \mathbb{R}_{\geq 0}$. From Definition 18 of the quotient it follows that $u \xrightarrow{d}{}^{T\backslash\backslash S} u$. By construction of $R'$ it also follows that $(q_2^X, u) \in R'$.

So for all state pairs $(q_1^X, u) \in R'$ we have shown that $R'$ witnesses the refinement $X \leq T\backslash\backslash S$. Finally, since $R$ witnesses $S \parallel X \leq T$ it holds that $((q_0^S, q_o^X), q_0^T) \in R$ (see Definition 6). Thus by construction of $R'$ it holds that $(q_0^X, (q_0^T, q_0^S)) \in R'$. Therefore, we can now conclude that $R'$ witnesses $X \leq T\backslash\backslash X$.

($S \parallel X \leq T \Leftarrow X \leq T\backslash\backslash S$) Since $X \leq T\backslash\backslash S$, it follows from Definition 6 of refinement that there exists a relation $R \in Q^X \times Q^{T\backslash\backslash S}$ that witness the refinement. Note that $Q^{S\parallel X} = Q^S \times Q^X$ according to Definition 15. Construct relation $R' = \{((q_1^S, q_1^X), q_1^T) \in Q^X \times Q^{T\backslash\backslash S} \mid (q_1^X, (q_1^T, q_1^S)) \in R\}$. We will show that $R'$ witnesses $S \parallel X \leq T$. First consider the five cases of Definition 6 for a state pair $((q_1^S, q_1^X), q_1^T) \in R'$.

1. $q_1^T \xrightarrow{i?}{}^T q_2^T$ for some $q_2^T \in Q^T$ and $i? \in Act_i^T \cap Act_i^{S\parallel X}$. From Lemma 17 it follows that $Act_i^T = Act_i^{S\parallel X}$. Consider the following five possible cases from Definition 15 of the parallel composition that might result in $i? \in Act_i^{S\parallel X} (= Act_i^S \setminus Act_o^X \cup Act_i^X \setminus Act_o^S)$.

- $i? \in Act_i^S \setminus Act_o^X$ and $i? \in Act_i^X \setminus Act_o^S$. Since $S$ and $X$ are specifications and $i? \in Act_i^S \cap Act_i^X$, it follows that $q_1^S \xrightarrow{i?}{}^S q_2^S$ for some $q_2^S \in Q^S$ and $q_1^X \xrightarrow{i?}{}^X q_2^X$ for some $q_2^X \in Q^X$ (any specification is input-enabled, see Definition 4). Therefore, using Definition 15 of parallel composition, it follows that $(q_1^S, q_1^X) \xrightarrow{i?}{}^{S\|X} (q_2^S, q_2^X)$. Also, using Definition 18 of the quotient it follows that $(q_1^T, q_1^S) \xrightarrow{i?}{}^{T\backslash\backslash S} (q_2^T, q_2^S)$. Now, using $R$, the first case of Definition 6 of refinement, and $Act^X = Act^{T\backslash\backslash S}$ by construction, it follows that $(q_2^X, (q_2^T, q_2^S)) \in R$. And from the construction of $R'$ we confirm that $((q_2^S, q_2^X), q_2^T) \in R'$.
- $i? \in Act_i^S \setminus Act_o^X$ and $i? \in Act_i^X \cap Act_o^S$. This case is infeasible, as an action cannot be both an output and input in $S$.
- $i? \in Act_i^S \setminus Act_o^X$ and $i? \notin Act_i^X$. This case is infeasible, as $i? \in Act_i^S \setminus Act_o^X$ and $i? \notin Act_i^X$ implies that $i \notin Act^X$, but from Definition 18 of the quotient it follows that $i? \in Act_i^S$ implies that $i \in Act^{T\backslash\backslash S} (= Act^X)$.
- $i? \in Act_i^S \cap Act_o^X$ and $i? \in Act_i^X \setminus Act_o^S$. This case is infeasible, as an action cannot be both an output and input in $X$.
- $i? \notin Act_i^S$ and $i? \in Act_i^X \setminus Act_o^S$. Since $i? \in Act_i^X \setminus Act_o^S$ implies that $i! \notin Act_o^S$, it follows that $i \notin Act^S$. From Definition 18 of quotient if follows that $(q_1^T, q_1^S) \xrightarrow{i?}{}^{T\backslash\backslash S} (q_2^T, q_2^S)$ and $q_1^S = q_2^S$. Now, using $R$, the first case of Definition 6 of refinement, and $Act^X = Act^{T\backslash\backslash S}$ by construction, it follows that $q_1^X \xrightarrow{i?}{}^X q_2^X$ and $(q_2^X, (q_2^T, q_2^S)) \in R$. Using Definition 15 of the parallel composition, it follows that $(q_1^S, q_1^X) \xrightarrow{i?}{}^{S\|X} (q_2^S, q_2^X)$. And from the construction of $R'$ we confirm that $((q_2^S, q_2^X), q_2^T) \in R'$.

So, in all feasible cases we can show that $(q_1^S, q_1^X) \xrightarrow{i?}{}^{S\|X} (q_2^S, q_2^X)$ and $((q_2^S, q_2^X), q_2^T) \in R'$.

2. $q_1^T \xrightarrow{i?}{}^T q_2^T$ for some $q_2^T \in Q^T$ and $i? \in Act_i^T \setminus Act_i^{S\|X}$. From Lemma 17 it follows that $Act_i^T \setminus Act_i^{S\|X} = \emptyset$, so this case can be ignored.

3. $(q_1^S, q_1^X) \xrightarrow{o!}{}^{S\|X} (q_2^S, q_2^X)$ for some $(q_2^S, q_2^X) \in Q^{S\|X}$ and $o! \in Act_o^{S\|X} \cap Act_o^T$. From Lemma 17 we have that $Act_o^{S\|X} = Act_o^S \cup Act_o^T \cup Act_i^S \setminus Act_i^T$. Consider the following three cases that might result in $o! \in Act_o^{S\|X}$ and $o! \in Act_o^T$.
   - $o! \in Act_o^S$ and $o! \in Act_o^T$. In this case we have that $o? \in Act_i^{T\backslash\backslash S}$ by Definition 18, and thus by construction of $X$ that $o? \in Act_i^X$. Now, using Definition 15 of the parallel composition, it follows that $q_1^S \xrightarrow{o!}{}^S q_2^S$ and $q_1^X \xrightarrow{o?}{}^X q_2^X$. Consider the following two cases for $T$.
     - $q_1^T \xrightarrow{o!}{}^T q_2^T$. In this case it follows that from Definition 18 of the quotient that $(q_1^T, q_1^S) \xrightarrow{o?}{}^{T\backslash\backslash S} (q_2^T, q_2^S)$. Using $R$, the first case of Definition 6 of refinement, and $Act^X = Act^{T\backslash\backslash S}$ by construction, it follows that $(q_2^X, (q_2^T, q_2^S)) \in R$. And from the construction of $R'$ we confirm that $((q_2^S, q_2^X), q_2^T) \in R'$.
     - $q_1^T \not\xrightarrow{o!}{}^T$. In this case it follows from Definition 18 of the quotient that $(q_1^T, q_1^S) \xrightarrow{o?}{}^{T\backslash\backslash S} e$. By construction of $e$, it does not allow independent progress. But, since $X$ is an implementation, all states in $X$

allow independent progress, see Definition 5[10]. Therefore, either $X$ can delay indefinitely from state $q_2^X$ or there exists a delay after which $X$ can perform an output action. Neither of these options can be simulated by $T\backslash\backslash S$ when in state $e$. Thus $(q_2^X, e) \notin R$, i.e., $X \not\leq T\backslash\backslash S$. This contradicts with the assumption, thus this is not a feasible case.

- $o? \in Act_i^S$ and $o! \in Act_o^T$. In this case we have that $o! \in Act_o^{T\backslash\backslash S}$ by Definition 18, and thus by construction of $X$ that $o! \in Act_o^X$. Now, using Definition 15 of the parallel composition, it follows that $q_1^S \xrightarrow{o?}{}^S q_2^S$ and $q_1^X \xrightarrow{o!}{}^X q_2^X$. Using $R$, the third case of Definition 6 of refinement, and $Act^X = Act^{T\backslash\backslash S}$ by construction, it follows that $(q_1^T, q_1^S) \xrightarrow{o!}{}^{T\backslash\backslash S} (q_2^T, q_2^S)$ and $(q_2^X, (q_2^T, q_2^S)) \in R$. Now, using Definition 18 of quotient again, it follows that $q_1^T \xrightarrow{o!}{}^T q_2^T$. And from the construction of $R'$ we confirm that $((q_2^S, q_2^X), q_2^T) \in R'$.
- $o \notin Act^S$ and $o! \in Act_o^T$. In this case we have that $o! \in Act_o^{T\backslash\backslash S}$ by Definition 18, and thus by construction of $X$ that $o! \in Act_o^X$. Now, using Definition 15 of the parallel composition, it follows that $q_1^X \xrightarrow{o!}{}^X q_2^X$ and $q_1^S = q_2^S$. Using $R$, the third case of Definition 6 of refinement, and $Act^X = Act^{T\backslash\backslash S}$ by construction, it follows that $(q_1^T, q_1^S) \xrightarrow{o!}{}^{T\backslash\backslash S} (q_2^T, q_2^S)$ and $(q_2^X, (q_2^T, q_2^S)) \in R$. Now, using Definition 18 of quotient again, it follows that $q_1^T \xrightarrow{o!}{}^T q_2^T$. And from the construction of $R'$ we confirm that $((q_2^S, q_2^X), q_2^T) \in R'$.

So, in all feasible cases we can show that $q_1^T \xrightarrow{o!}{}^T q_2^T$ and $((q_2^S, q_2^X), q_2^T) \in R'$.

4. $(q_1^S, q_1^X) \xrightarrow{o!}{}^{S\|X} (q_2^S, q_2^X)$ for some $(q_2^S, q_2^X) \in Q^{S\|X}$ and $o! \in Act_o^{S\|X} \setminus Act_o^T$. From Lemma 17 we have that $Act_o^{S\|X} = Act_o^S \cup Act_o^T \cup Act_i^S \setminus Act_i^T$. So $Act_o^{S\|X} \setminus Act_o^T = (Act_o^S \cup Act_i^S \setminus Act_i^T) \setminus Act_o^T = Act_o^S \setminus Act_o^T \cup (Act_i^S \setminus Act_i^T) \setminus Act_o^T = Act_o^S \setminus Act_o^T \cup Act_i^S \setminus Act^T$. Consider the following five cases that might result in $o! \in Act_o^{S\|X} \setminus Act_o^T$.
   - $o! \in Act_o^S \setminus Act_o^T$ and $o? \in Act_i^S \setminus Act^T$. This case is infeasible, as an action cannot be both an output and input in $S$.
   - $o! \in Act_o^S \setminus Act_o^T$ and $o? \in Act_i^S \cap Act^T$. This case is infeasible, as an action cannot be both an output and input in $S$.
   - $o! \in Act_o^S \setminus Act_o^T$ and $o? \notin Act_i^S$. In this case, we have that $o? \in Act_i^{T\backslash\backslash S}$ from Definition 18 of the quotient. Therefore, $o? \in Act_i^X$ by construction of $X$. Now, using Definition 15 of the parallel composition, it follows that $q_1^S \xrightarrow{o!}{}^S q_2^S$ and $q_1^X \xrightarrow{o?}{}^X q_2^X$. Since Definition 18 also requires that $Act_o^S \cap Act_i^T = \emptyset$, it follows that in this case $o \notin Act^T$. Thus, from Definition 18 it follows that $(q_1^T, q_1^S) \xrightarrow{o?}{}^{T\backslash\backslash S} (q_2^T, q_2^S)$ and $q_1^T = q_2^T$. Using $R$, the first case of Definition 6 of refinement, and $Act^X = Act^{T\backslash\backslash S}$ by construction, it follows that $(q_2^X, (q_2^T, q_2^S)) \in R$. And from the construction of $R'$ we confirm that $((q_2^S, q_2^X), q_2^T) \in R'$.
   - $o! \in Act_o^S \cap Act_o^T$ and $o? \in Act_i^S \setminus Act^T$. This case is infeasible, as an action cannot be both an output and input in $S$.

[10]This is the reason why $X$ is assumed to be an implementation and not just a specification.

- $o! \notin Act_o^S$ and $o? \in Act_i^S \setminus Act^T$. In this case, we have that $o! \in Act_o^{T \backslash\backslash S}$ from Definition 18 of the quotient. Therefore, $o! \in Act_o^X$ by construction of $X$. Now, using Definition 15 of the parallel composition, it follows that $q_1^S \xrightarrow{o!}{}^S q_2^S$ and $q_1^X \xrightarrow{o?}{}^X q_2^X$. Using $R$, the fourth case of Definition 6 of refinement, $Act^X = Act^{T\backslash\backslash S}$ by construction, and $o \notin Act^T$, it follows that $(q_2^X, (q_2^T, q_2^S)) \in R$ and $q_1^T = q_2^T$. And from the construction of $R'$ we confirm that $((q_2^S, q_2^X), q_2^T) \in R'$.

So, in all feasible cases we can show that $o \notin Act^T$, $q_1^T = q_2^T$, and $((q_2^S, q_2^X), q_2^T) \in R'$.

5. $(q_1^S, q_1^X) \xrightarrow{d}{}^{S\|X} (q_2^S, q_2^X)$ for some $(q_2^S, q_2^X) \in Q^{S\|X}$ and $d \in \mathbb{R}_{\geq 0}$. It follows from Definition 15 of the parallel composition that $q_1^S \xrightarrow{d}{}^S q_2^S$ and $q_1^X \xrightarrow{d}{}^X q_2^X$. Using $R$ and the fifth case of Definition 6 of refinement it follows that $(q_1^T, q_1^S) \xrightarrow{d}{}^{T\backslash\backslash S} q_2$ for some $q_2^{T\backslash\backslash S} \in Q^{T\backslash\backslash S}$ and $(q_2^X, q_2^{T\backslash\backslash S})) \in R$. Now, by Definition 18 of the quotient it follows that $q_1^T \xrightarrow{d}{}^T q_2^T$ (and $q_1^S \xrightarrow{d}{}^S q_2^S$). And from the construction of $R'$ we confirm that $((q_2^S, q_2^X), q_2^T) \in R'$.

So for all state pairs $((q_1^S, q_1^X), q_1^T) \in R'$ we have shown that $R'$ witnesses the refinement $S \parallel X \leq T$. Finally, since $R$ witnesses $X \leq T\backslash\backslash S$ it holds that $(q_0^X, (q_0^T, q_0^S)) \in R$ (see Definition 6). Thus by construction of $R'$ it holds that $((q_0^S, q_o^X), q_0^T) \in R'$. Therefore, we can now conclude that $R'$ witnesses $S \parallel X \leq T$. □

Quotienting for TIOA is defined in the following way.

**Definition 19** *Given specification automata* $S = (Loc^S, l_0^S, Act^S, Clk^S, E^S, Inv^S)$ *and* $T = (Loc^T, l_0^T, Act^T, Clk^T, E^T, Inv^T)$ *where* $Act_o^S \cap Act_i^T = \emptyset$. *The quotient of* $T$ *and* $S$, *denoted by* $T\backslash\backslash S$, *is a specification automaton* $(Loc^T \times Loc^S \cup \{l_u, l_e\}, (l_0^T, l_0^S), Act, Clk^T \uplus Clk^S \uplus \{x_{new}\}, E, Inv)$ *where* $l_u$ *is the universal state,* $l_e$ *the inconsistent state,* $Act = Act_i \uplus Act_o$ *with* $Act_i = Act_i^T \cup Act_o^S \cup \{i_{new}\}$ *and* $Act_o = Act_o^T \setminus Act_o^S \cup Act_i^S \setminus Act_i^T$, $Inv((l^T, l^S)) = Inv(l_u) = \mathbf{T}$, $Inv(l_e) = x_{new} \leq 0$ *and* $E$ *is defined as*

1. $((l_1^T, l_1^S), a, \varphi^T \wedge Inv(l_2^T)[r \mapsto 0]_{r \in c^T} \wedge \varphi^S \wedge Inv(l_1^S) \wedge Inv(l_2^S)[r \mapsto 0]_{r \in c^S}, c^T \cup c^S, (l_2^T, l_2^S)) \in E$ *if* $a \in Act^S \cap Act^T$, $(l_1^T, a, \varphi^T, c^T, l_2^T) \in E^T$, *and* $(l_1^S, a, \varphi^S, c^S, l_2^S) \in E^S$[11]
2. $((l^T, l_1^S), a, \varphi^S \wedge Inv(l_1^S) \wedge Inv(l_2^S)[r \mapsto 0]_{r \in c^S}, c^S, (l^T, l_2^S)) \in E$ *if* $a \in Act^S \setminus Act^T$, $l^T \in Loc^T$, *and* $(l_1^S, a, \varphi^S, c^S, l_2^S) \in E^S$
3. $((l^T, l_1^S), a, \neg G_S, \emptyset, l_u) \in E$ *if* $a \in Act_o^S$, $l^T \in Loc^T$ *and* $G_S = \bigvee\{\varphi^S \wedge Inv(l_2^S)[r \mapsto 0]_{r \in c^S} \mid (l_1^S, a, \varphi^S, c^S, l_2^S) \in E^S\}$
4. $((l^T, l^S), a, \neg Inv(l^S), \emptyset, l_u) \in E$ *if* $a \in Act$, $l^T \in Loc^T$, *and* $l^S \in Loc^S$
5. $((l_1^T, l_1^S), a, \varphi^S \wedge Inv(l_2^S)[r \mapsto 0]_{r \in c^S} \wedge \neg G_T, \{x_{new}\}, l_e) \in E$ *if* $a \in Act_o^S \cap Act_o^T$, $(l^S, a, \varphi^S, c^S, l_2^S) \in E^S$, *and* $G_T = \bigvee\{\varphi^T \wedge Inv(l_2^T)[r \mapsto 0]_{r \in c^T} \mid (l_1^T, a, \varphi^T, c^T, l_2^T) \in E^T\}$

[11] Only the target invariant of $T$ matters. $Inv(l_1^S)$ is used to force the complementary edge to the universal state (which depends on $S$, see rules 5 and 6 in Definition 18 of quotient for TIOTS), $Inv(l_2^S)[r \mapsto 0]_{r \in c^S}$ is used to ensure the transition only appears in feasible states in the semantic representation as the location invariants are removed.

6. $((l^T_!, l^S_1), a, \neg G_S \wedge \neg G_T, \emptyset, (l^T_1, l^S_1)) \in E$ *if* $a \in Act^S_o \cap Act^T_o$, $G_S = \bigvee\{\varphi^S \wedge Inv(l^S_2)[r \mapsto 0]_{r\in c^S} \mid (l^S_1, a, \varphi^S, c^S, l^S_2) \in E^S\}$, *and* $G_T = \bigvee\{\varphi^T \wedge Inv(l^T_2)[r \mapsto 0]_{r\in c^T} \mid (l^T_1, a, \varphi^T, c^T, l^T_2) \in E^T\}$
7. $((l^T, l^S), i_{new}, \neg Inv(l^T) \wedge Inv(l^S), \{x_{new}\}, l_e) \in E$ *if* $l^T \in Loc^T$ *and* $l^S \in Loc^S$
8. $((l^T, l^S), i_{new}, Inv(l^T) \vee \neg Inv(l^S), \emptyset, (l^T, l^S)) \in E$ *if* $l^T \in Loc^T$ *and* $l^S \in Loc^S$
9. $((l^T_1, l^S), a, \varphi^T \wedge Inv(l^T_2)[r \mapsto 0]_{r\in c^T} \wedge Inv(l^S), c^T, (l^T_2, l^S)) \in E$ *if* $a \in Act^T \setminus Act^S$, $l^S \in Loc^S$, *and* $(l^T_1, a, \varphi^T, c^T, l^T_2) \in E^T$[12]
10. $(l_u, a, \mathbf{T}, \emptyset, l_u) \in E$ *if* $a \in Act$
11. $(l_e, a, x_{new} = 0, \emptyset, l_e) \in E$ *if* $a \in Act_i$

*and the conjunction of an empty set equals false* ($\bigvee \emptyset = \mathbf{F}$).

**Definition 20** *Given specifications* $S = (Q^S, q^S_0, Act^S, \rightarrow^S)$ *and* $T = (Q^T, q^T_0, Act^T, \rightarrow^T)$. *S and T are* bisimular, *denoted by* $S \simeq T$, *iff there exists a bisimulation relation* $R \subseteq Q^S \times Q^T$ *containing* $(q^S_0, q^T_0)$ *such that for each pair of states* $(s,t) \in R$ *it holds that*

1. *whenever* $s \xrightarrow{a}{}^S s'$ *for some* $s' \in Q^S$ *and* $a \in Act^S \cap Act^T$, *then* $t \xrightarrow{a}{}^T t'$ *and* $(s', t') \in R$ *for some* $t' \in Q^T$
2. *whenever* $s \xrightarrow{a}{}^S s'$ *for some* $s' \in Q^S$ *and* $a \in Act^S \setminus Act^T$, *then* $(s', t) \in R$
3. *whenever* $t \xrightarrow{a}{}^T t'$ *for some* $t' \in Q^T$ *and* $a \in Act^T \cap Act^S$, *then* $s \xrightarrow{a}{}^S s'$ *and* $(s', t') \in R$ *for some* $s' \in Q^S$
4. *whenever* $t \xrightarrow{a}{}^T t'$ *for some* $t' \in Q^T$ *and* $a \in Act^T \setminus Act^S$, *then* $(s, t') \in R$
5. *whenever* $s \xrightarrow{d}{}^S s'$ *for some* $s' \in Q^S$ *and* $d \in \mathbb{R}_{\geq 0}$, *then* $t \xrightarrow{d}{}^T t'$ *and* $(s', t') \in R$ *for some* $t' \in Q^T$
6. *whenever* $t \xrightarrow{d}{}^T t'$ *for some* $t' \in Q^T$ *and* $d \in \mathbb{R}_{\geq 0}$, *then* $s \xrightarrow{d}{}^S s'$ *and* $(s', t') \in R$ *for some* $s' \in Q^S$

*Two specification automata A and B are bisimular, denoted by* $A \simeq B$, *iff* $[\![A]\!]_{\text{sem}} \simeq [\![B]\!]_{\text{sem}}$.

Finally, the following theorem lifts all the results from timed input/output transition systems to the symbolic representation level.

**Theorem 11** *Given specification automata* $S = (Loc^S, l^S_0, Act^S, Clk^S, E^S, Inv^S)$ *and* $T = (Loc^T, l^T_0, Act^T, Clk^T, E^T, Inv^T)$ *where* $Act^S_o \cap Act^T_i = \emptyset$. *Then* $([\![T \backslash\backslash S]\!]_{\text{sem}})^\Delta \simeq ([\![T]\!]_{\text{sem}} \backslash\backslash [\![S]\!]_{\text{sem}})^\Delta$.

First observe that $[\![T \backslash\backslash S]\!]_{\text{sem}}$ and $[\![T]\!]_{\text{sem}} \backslash\backslash [\![S]\!]_{\text{sem}}$ have different state and action sets. For example, $[\![T \backslash\backslash S]\!]_{\text{sem}}$ has a set of error states $\{(l_e, v) \mid v \in$

[12] Location invariant $\neg Inv(l^S)$ is added to this transition to avoid nondeterminism caused by rule 4. This problem is not present in Definition 18 of the quotient for TIOTS, as there we can directly refer to the delay action $d$ in rule 5.

$[Clk^{T\backslash\backslash S} \mapsto \mathbb{R}_{\geq 0}]\}$, while $[\![T]\!]_{\text{sem}} \backslash\backslash [\![S]\!]_{\text{sem}}$ only has a single error state $e$. Or $[\![T\backslash\backslash S]\!]_{\text{sem}}$ contains the input action $i_{new}$ which $[\![T]\!]_{\text{sem}} \backslash\backslash [\![S]\!]_{\text{sem}}$ lacks. This makes the proof of Theorem 11 much more tedious that those of theorems in previous sections. Therefore, we first introduce several definitions and lemmas to show that, when considering bisimulation, we can simplify $[\![T\backslash\backslash S]\!]_{\text{sem}}$ until we have a bijective mapping of the states between the simplified $[\![T\backslash\backslash S]\!]_{\text{sem}}$ and $[\![T]\!]_{\text{sem}} \backslash\backslash [\![S]\!]_{\text{sem}}$.

**Definition 21** *Given a TIOTS* $S = (Q, q_0, Act, \rightarrow)$ *and equivalence relation* $\sim$ *on the set of states* $Q$*. The* $\sim$-quotient $S$*, denoted by* $S/\sim$*, is a specification* $([Q]_\sim, [q_0]_\sim, Act, \rightarrow/\sim)$ *where* $[Q]_\sim$ *is the set of all equivalence classes of* $Q$[13] *and* $\rightarrow/\sim$ *being defined as* $([q_1], a, [q_2]) \in \rightarrow/\sim$ *if* $(q_1, a, q_2) \in\rightarrow$ *for some* $q_1 \in [q_1]$ *and* $q_2 \in [q_2]$*.*

**Lemma 18** *Given specification automata* $S = (Loc^S, l_0^S, Act^S, Clk^S, E^S, Inv^S)$ *and* $T = (Loc^T, l_0^T, Act^T, Clk^T, E^T, Inv^T)$ *where* $Act_o^S \cap Act_i^T = \emptyset$*. Let* $V_0 = \{v \in [Clk^{T\backslash\backslash S} \mapsto \mathbb{R}_{\geq 0}] \mid v(x_{new}) = 0\}$*,* $V_{>0} = [Clk^{T\backslash\backslash S} \mapsto \mathbb{R}_{\geq 0}] \setminus V_0$*, and* $\sim = \{(q_1, q_2) \mid q_1, q_2 \in \{l_e\} \times V_0\} \cup \{(q, q) \mid q \in \{l_e\} \times V_{>0}\} \cup \{(q_1, q_2) \mid q_1, q_2 \in \{l_u\} \times [Clk^{T\backslash\backslash S} \mapsto \mathbb{R}_{\geq 0}]\} \cup \{((l, v_1), (l, v_2)) \mid l \in Loc^{T\backslash\backslash S} \setminus \{l_e, l_u\}, v_1, v_2 \in [Clk^{T\backslash\backslash S} \mapsto \mathbb{R}_{\geq 0}], \forall c \in Clk^{T\backslash\backslash S} \setminus \{x_{new}\}, v_1(c) = v_2(c)\}$*. Then* $[\![T\backslash\backslash S]\!]_{\text{sem}} \simeq [\![T\backslash\backslash S]\!]_{\text{sem}}/\sim$*.*

*Proof* It follows directly from the definition of $\sim$ that it is reflexive, symmetric, and transitive, thus it is an equivalence relation. Now, observe from Definition 21 that an equivalence quotient of a TIOTS does not alter the action set, i.e., $Act^{[\![T\backslash\backslash S]\!]_{\text{sem}}} = Act^{[\![T\backslash\backslash S]\!]_{\text{sem}}/\sim}$. Let $R = \{(q, [q]_\sim) \mid q \in Q^{[\![T\backslash\backslash S]\!]_{\text{sem}}}\}$. We will show that $R$ is a bisimulation relation. First, observe that $(q_0, [q_0]_\sim) \in R$. Consider a state pair $(q_1, [r_1]_\sim) \in R$. We have to check whether the six cases from Definition 20 of bisimulation hold.

1. $q_1 \xrightarrow{a}{}^{[\![T\backslash\backslash S]\!]_{\text{sem}}} q_2$, $q_2 \in Q^{[\![T\backslash\backslash S]\!]_{\text{sem}}}$, and $a \in Act^{[\![T\backslash\backslash S]\!]_{\text{sem}}} \cap Act^{[\![T\backslash\backslash S]\!]_{\text{sem}}/\sim}$. By the definition of an equivalence class and Definition 21 it follows immediately that $[q_1]_\sim \xrightarrow{a}{}^{[\![T\backslash\backslash S]\!]_{\text{sem}}/\sim} [q_2]_\sim$. By construction of $R$ it follows that $(q_2, [q_2]_\sim) \in R$.
2. $q_1 \xrightarrow{a}{}^{[\![T\backslash\backslash S]\!]_{\text{sem}}} q_2$, $q_2 \in Q^{[\![T\backslash\backslash S]\!]_{\text{sem}}}$, and $a \in Act^{[\![T\backslash\backslash S]\!]_{\text{sem}}} \setminus Act^{[\![T\backslash\backslash S]\!]_{\text{sem}}/\sim}$. This case is infeasible, since $Act^{[\![T\backslash\backslash S]\!]_{\text{sem}}} = Act^{[\![T\backslash\backslash S]\!]_{\text{sem}}/\sim}$.
3. $[r_1]_\sim \xrightarrow{a}{}^{[\![T\backslash\backslash S]\!]_{\text{sem}}/\sim} [r_2]_\sim$, $[r_2]_\sim \in Q^{[\![T\backslash\backslash S]\!]_{\text{sem}}/\sim}$, and $a \in Act^{[\![T\backslash\backslash S]\!]_{\text{sem}}/\sim} \cap Act^{[\![T\backslash\backslash S]\!]_{\text{sem}}}$. By construction of $R$, we have to show that $\forall q_1 \in [r_1]_\sim \exists q_2 \in Q^{[\![T\backslash\backslash S]\!]_{\text{sem}}} : q_1 \xrightarrow{a}{}^{[\![T\backslash\backslash S]\!]_{\text{sem}}} q_2$, $q_2 \in [r_2]_\sim$, and $(q_2, [r_2]_\sim) \in R$. Consider the following four cases based on the construction of $\sim$:
   - $[r_1]_\sim = \{q \mid q \in \{l_e\} \times V_0\}$. In this case, let $q_1 = (l_e, v_1) \in [r_1]_\sim$ for some $v_1 \in V_0$. From Definition 3 of the semantic of a TIOA it follows that $[\![T\backslash\backslash S]\!]_{\text{sem}}$ is in location $l_e$. From Definition 19 of the quotient it follows that the only possible transition in $T\backslash\backslash S$ is $(l_e, a, x_{new} = 0, \emptyset, l_e)$. Furthermore, since $[r_1]_\sim \xrightarrow{a}{}^{[\![T\backslash\backslash S]\!]_{\text{sem}}/\sim} [r_2]_\sim$, it holds that $\exists r_1, r_2 \in Q^{[\![T\backslash\backslash S]\!]_{\text{sem}}} : r_1 \xrightarrow{a}$

[13] Recall that an equivalent class is defined as $[q]_\sim = \{r \in Q \mid q \sim r\}$.

$[\![T\backslash\backslash S]\!]_{\text{sem}} r_2$. Following Definition 3 and the above observation, it holds that $r_1 = (l_e, v_1')$ and $r_2 = (l_e, v_2')$ for some $v_1', v_2' \in [Clk^{T\backslash\backslash S} \mapsto \mathbb{R}_{\geq 0}]$, $v_1' \models x_{new} = 0$, and $v_1' = v_2'$. From $v_1' \models x_{new} = 0$ it follows that $v_1'(x_{new}) = 0$ and $v_1', v_2' \in V_0$, and from $v_1' = v_2'$ that $[r_2]_\sim = [r_1]_\sim$. Thus we can conclude that $q_1 \xrightarrow{a} {}_{[\![T\backslash\backslash S]\!]_{\text{sem}}} q_2$ with $q_2 \in [r_2]_\sim$. By construction of $R$ it follows that $(q_2, [r_2]_\sim) \in R$.

- $[r_1]_\sim = \{q \mid q \in \{l_e\} \times V_{>0}\}$. This case is trivial, since $[r_1]_\sim = \{r_1\} = \{q_1\}$. Therefore, if $[r_1]_\sim \xrightarrow{a} {}_{[\![T\backslash\backslash S]\!]_{\text{sem}}/\sim} [r_2]_\sim$, $\exists q_2 \in [r_2]_\sim$ such that $q_1 \xrightarrow{a} {}_{[\![T\backslash\backslash S]\!]_{\text{sem}}} q_2$.
- $[r_1]_\sim = \{q \mid q \in \{l_u\} \times [Clk^{T\backslash\backslash S} \mapsto \mathbb{R}_{\geq 0}]\}$. In this case, let $q_1 = (l_u, v_1) \in [r_1]_\sim$ for some $v_1 \in [Clk^{T\backslash\backslash S} \mapsto \mathbb{R}_{\geq 0}]$. From Definition 3 of the semantic of a TIOA it follows that $[\![T\backslash\backslash S]\!]_{\text{sem}}$ is in location $l_u$. From Definition 19 of the quotient it follows that the only possible transition in $T\backslash\backslash S$ is $(l_u, a, \mathbf{T}, \emptyset, l_u)$. Furthermore, since $[r_1]_\sim \xrightarrow{a} {}_{[\![T\backslash\backslash S]\!]_{\text{sem}}/\sim} [r_2]_\sim$, it holds that $\exists r_1, r_2 \in Q^{[\![T\backslash\backslash S]\!]_{\text{sem}}} : r_1 \xrightarrow{a} {}_{[\![T\backslash\backslash S]\!]_{\text{sem}}} r_2$. Following Definition 3 and the above observation, it holds that $r_1 = (l_u, v_1')$ and $r_2 = (l_u, v_2')$ for some $v_1', v_2' \in [Clk^{T\backslash\backslash S} \mapsto \mathbb{R}_{\geq 0}]$, $v_1' \models \mathbf{T}$, and $v_1' = v_2'$. From $v_1' = v_2'$ it follows that $[r_2]_\sim = [r_1]_\sim$. Thus we can conclude that $q_1 \xrightarrow{a} {}_{[\![T\backslash\backslash S]\!]_{\text{sem}}} q_2$ with $q_2 \in [r_2]_\sim$. By construction of $R$ it follows that $(q_2, [r_2]_\sim) \in R$.
- In this case, since $[r_1]_\sim \xrightarrow{a} {}_{[\![T\backslash\backslash S]\!]_{\text{sem}}/\sim} [r_2]_\sim$, it holds that $\exists r_1, r_2 \in Q^{[\![T\backslash\backslash S]\!]_{\text{sem}}} : r_1 \xrightarrow{a} {}_{[\![T\backslash\backslash S]\!]_{\text{sem}}} r_2$. Following Definition 3 of the semantic of a TIOA, it holds that $(l_1, a, \varphi, c, l_2) \in E^{T\backslash\backslash S}$, $r_1 = (l_1, v_1)$, $r_2 = (l_2, v_2)$, $l_1, l_2 \in Loc^{T\backslash\backslash S}$, $v_1, v_2 \in [Clk^{T\backslash\backslash S} \mapsto \mathbb{R}_{\geq 0}]$, $v_1 \models \varphi$, $v_2 = v_1[r \mapsto 0]_{r \in c}$, and $v_2 \models Inv(l_2)$. From the construction of $\sim$, it follows that for any state $(l_1', v_1') \in [r_1]_\sim$ it holds that $l_1' = l_1$, $l_1 \neq l_e$, and $\forall c \in Clk^{T\backslash\backslash S} \setminus \{x_{new}\} : v_1'(c) = v_1(c)$. Since $x_{new} \notin Clk^T \cup Clk^S$ and none of the possible rules for this location from Definition 19 of the quotient for TIOA use $x_{new}$ in its guard, it follows that $v_1' \models \varphi$. Furthermore, no matter whether $x_{new} \in c$ or not, we have for $v_2' = v_1'[r \mapsto 0]_{r \in c}$ that $\forall c \in Clk^{T\backslash\backslash S} \setminus \{x_{new}\} : v_2'(c) = v_2(c)$. Now consider the following three options for the target location $l_2$.
  - If $l_2 = (l^T, l^S)$ with $l^T \in Loc^T$ and $l^S \in Loc^S$, then $Inv(l_2) = \mathbf{T}$. Thus $v_2' \models Inv(l_2)$.
  - If $l_2 = l_u$, then $Inv(l_2) = \mathbf{T}$. Thus $v_2' \models Inv(l_2)$.
  - If $l_2 = l_e$, then $Inv(l_2) = x_{new} = 0$. Also, $c = \{x_{new}\}$, thus $v_2(x_{new}) = v_2'(x_{new}) = 0$. Thus $v_2' \models Inv(l_2)$.

  Therefore, we can conclude that $(l_1', v_1') \xrightarrow{a} {}_{[\![T\backslash\backslash S]\!]_{\text{sem}}} (l_2, v_2')$, $(l_2, v_2') \in [r_2]_\sim$, and by construction of $R$ that $((l_2, v_2'), [r_2]_\sim) \in R$. Since we picked any state $(l_1', v_1') \in [r_1]_\sim$, the conclusion holds for all states $q_1 \in [r_1]_\sim$.

4. $[r_1]_\sim \xrightarrow{a} {}_{[\![T\backslash\backslash S]\!]_{\text{sem}}/\sim} [r_2]_\sim$, $[r_2]_\sim \in Q^{[\![T\backslash\backslash S]\!]_{\text{sem}}/\sim}$, and $a \in Act^{[\![T\backslash\backslash S]\!]_{\text{sem}}/\sim} \setminus Act^{[\![T\backslash\backslash S]\!]_{\text{sem}}}$. This case is infeasible, since $Act^{[\![T\backslash\backslash S]\!]_{\text{sem}}} = Act^{[\![T\backslash\backslash S]\!]_{\text{sem}}/\sim}$.

5. $q_1 \xrightarrow{d} {}_{[\![T\backslash\backslash S]\!]_{\text{sem}}} q_2$, $q_2 \in Q^{[\![T\backslash\backslash S]\!]_{\text{sem}}}$, and $d \in \mathbb{R}_{\geq 0}$. By the definition of an equivalence class and Definition 21 it follows immediately that $[q_1]_\sim \xrightarrow{a} {}_{[\![T\backslash\backslash S]\!]_{\text{sem}}/\sim} [q_2]_\sim$. By construction of $R$ it follows that $(q_2, [q_2]_\sim) \in R$.

6. $[r_1]_\sim \xrightarrow{d} {}_{[\![T\backslash\backslash S]\!]_{\text{sem}}/\sim} [r_2]_\sim$, $[r_2]_\sim \in Q^{[\![T\backslash\backslash S]\!]_{\text{sem}}/\sim}$, and $d \in \mathbb{R}_{\geq 0}$. By construction of $R$, we have to show that $\forall q_1 \in [r_1]_\sim \exists q_2 \in Q^{[\![T\backslash\backslash S]\!]_{\text{sem}}} : q_1 \xrightarrow{a}$

$\llbracket T \backslash\backslash S \rrbracket_{\text{sem}} q_2$, $q_2 \in [r_2]_\sim$, and $(q_2, [r_2]_\sim) \in R$. Consider the following three cases based on the construction of $\sim$:

- $[r_1]_\sim = \{q \mid q \in \{l_e\} \times V_0\}$. In this case, let $q_1 = (l_e, v_1) \in [r_1]_\sim$ for some $v_1 \in V_0$. From Definition 3 of the semantic of a TIOA it follows that $\llbracket T \backslash\backslash S \rrbracket_{\text{sem}}$ is in location $l_e$. From Definition 19 of the quotient it follows that $\mathit{Inv}(l_e) = x_{new} = 0$. Furthermore, since $[r_1]_\sim \xrightarrow{d}_{\llbracket T \backslash\backslash S \rrbracket_{\text{sem}}/\sim} [r_2]_\sim$, it holds that $\exists r_1, r_2 \in Q^{\llbracket T \backslash\backslash S \rrbracket_{\text{sem}}} : r_1 \xrightarrow{d}_{\llbracket T \backslash\backslash S \rrbracket_{\text{sem}}} r_2$. Following Definition 3 and the above observation, it holds that $r_1 = (l_e, v_1')$ and $r_2 = (l_e, v_2')$ for some $v_1', v_2' \in [\mathit{Clk}^{T \backslash\backslash S} \mapsto \mathbb{R}_{\geq 0}]$, $v_2' = v_1' + d$ and $v_2' \models \mathit{Inv}(l_e)$. From $v_2' \models \mathit{Inv}(l_e)$ it follows that $v_2'(x_{new}) = 0$, thus $d = 0$, $v_1' = v_2'$, $v_1', v_2' \in V_0$, and $[r_2]_\sim = [r_1]_\sim$. Thus we can conclude that $q_1 \xrightarrow{d}_{\llbracket T \backslash\backslash S \rrbracket_{\text{sem}}} q_2$ with $q_2 \in [r_2]_\sim$. By construction of $R$ it follows that $(q_2, [r_2]_\sim) \in R$.
- $[r_1]_\sim = \{q \mid q \in \{l_e\} \times V_{>0}\}$. This case is trivial, since $[r_1]_\sim = \{r_1\} = \{q_1\}$. Therefore, if $[r_1]_\sim \xrightarrow{d}_{\llbracket T \backslash\backslash S \rrbracket_{\text{sem}}/\sim} [r_2]_\sim$, $\exists q_2 \in [r_2]_\sim$ such that $q_1 \xrightarrow{d}_{\llbracket T \backslash\backslash S \rrbracket_{\text{sem}}} q_2$.
- $[r_1]_\sim = \{q \mid q \in \{l_u\} \times [\mathit{Clk}^{T \backslash\backslash S} \mapsto \mathbb{R}_{\geq 0}]\}$. In this case, let $q_1 = (l_u, v_1) \in [r_1]_\sim$ for some $v_1 \in V_0$. From Definition 3 of the semantic of a TIOA it follows that $\llbracket T \backslash\backslash S \rrbracket_{\text{sem}}$ is in location $l_u$. From Definition 19 of the quotient it follows that $\mathit{Inv}(l_u) = \mathbf{T}$. Furthermore, since $[r_1]_\sim \xrightarrow{d}_{\llbracket T \backslash\backslash S \rrbracket_{\text{sem}}/\sim} [r_2]_\sim$, it holds that $\exists r_1, r_2 \in Q^{\llbracket T \backslash\backslash S \rrbracket_{\text{sem}}} : r_1 \xrightarrow{d}_{\llbracket T \backslash\backslash S \rrbracket_{\text{sem}}} r_2$. Following Definition 3 and the above observation, it holds that $r_1 = (l_u, v_1')$ and $r_2 = (l_u, v_2')$ for some $v_1', v_2' \in [\mathit{Clk}^{T \backslash\backslash S} \mapsto \mathbb{R}_{\geq 0}]$, $v_2' = v_1' + d$ and $v_2' \models \mathit{Inv}(l_u)$. Now it follows that $(l_u, v_2') \in [r_1]_\sim$, thus $[r_2]_\sim = [r_1]_\sim$. Therefore, we can conclude that $q_1 \xrightarrow{d}_{\llbracket T \backslash\backslash S \rrbracket_{\text{sem}}} q_2$ with $q_2 \in [r_2]_\sim$ and by construction of $R$ it follows that $(q_2, [r_2]_\sim) \in R$.
- In this case, since $[r_1]_\sim \xrightarrow{d}_{\llbracket T \backslash\backslash S \rrbracket_{\text{sem}}/\sim} [r_2]_\sim$, it holds that $\exists r_1, r_2 \in Q^{\llbracket T \backslash\backslash S \rrbracket_{\text{sem}}} : r_1 \xrightarrow{d}_{\llbracket T \backslash\backslash S \rrbracket_{\text{sem}}} r_2$. Following Definition 3 of the semantic of a TIOA, it holds that $r_1 = (l, v_1)$, $r_2 = (l, v_2)$, $l \in \mathit{Loc}^{T \backslash\backslash S}$, $v_1, v_2 \in [\mathit{Clk}^{T \backslash\backslash S} \mapsto \mathbb{R}_{\geq 0}]$, $v_2 = v_1 + d$, $v_2 \models \mathit{Inv}(l)$, and $\forall d' \in \mathbb{R}_{\geq 0}, d' < d : v_1 + d' \models \mathit{Inv}(l)$. From the construction of $\sim$, it follows that for any state $(l_1', v_1') \in [r_1]_\sim$ it holds that $l_1' = l_1$, $l_1 \neq l_e$, and $\forall c \in \mathit{Clk}^{T \backslash\backslash S} \setminus \{x_{new}\} : v_1'(c) = v_1(c)$. Therefore, we have for $v_2' = v_1' + d$ that $\forall c \in \mathit{Clk}^{T \backslash\backslash S} \setminus \{x_{new}\} : v_2'(c) = v_2(c)$; similarly, for $v_1' + d'$ we have that $\forall c \in \mathit{Clk}^{T \backslash\backslash S} \setminus \{x_{new}\} : v_1' + d'(c) = v_1 + d'(c)$. From Definition 19 of the quotient for TIOA it follows that $\mathit{Inv}(l) = \mathit{Inv}(l') = \mathbf{T}$. Thus $v_2' \models \mathit{Inv}(l')$ and $v_1' + d' \models \mathit{Inv}(l')$. Therefore, from Definition 3 again we have that $(l_1', v_1') \xrightarrow{d}_{\llbracket T \backslash\backslash S \rrbracket_{\text{sem}}} (l_1', v_2')$, $(l_2, v_2') \in [r_2]_\sim$, and by construction of $R$ that $((l_2, v_2'), [r_2]_\sim) \in R$. Since we picked any state $(l_1', v_1') \in [r_1]_\sim$, the conclusion holds for all states $q_1 \in [r_1]_\sim$.

□

The following definition defines the TIOTS of the $\sim$-quotient of $\llbracket T \backslash\backslash S \rrbracket_{\text{sem}}$ where all states consisting of the error location and a valuation where $u(x_{new}) > 0$ are removed, as these states are never reachable.

**Definition 22** *Given specification automata* $S = (Loc^S, l_0^S, Act^S, Clk^S, E^S, Inv^S)$ *and* $T = (Loc^T, l_0^T, Act^T, Clk^T, E^T, Inv^T)$ *where* $Act_o^S \cap Act_i^T = \emptyset$. *Let* $V_0 = \{u \in [Clk^{T\backslash\backslash S} \mapsto \mathbb{R}_{\geq 0}] \mid u(x_{new}) = 0\}$, $V_{>0} = [Clk^{T\backslash\backslash S} \mapsto \mathbb{R}_{\geq 0}] \setminus V_0$, *and* $\sim = \{(q_1, q_2) \mid q_1, q_2 \in \{l_e\} \times V_0\} \cup \{(q, q) \mid q \in \{l_e\} \times V_{>0}\} \cup \{(q_1, q_2) \mid q_1, q_2 \in \{l_u\} \times [Clk^{T\backslash\backslash S} \mapsto \mathbb{R}_{\geq 0}]\} \cup \{((l, v_1), (l, v_2)) \mid l \in Loc^{T\backslash\backslash S} \setminus \{l_e, l_u\}, v_1, v_2 \in [Clk^{T\backslash\backslash S} \mapsto \mathbb{R}_{\geq 0}], \forall c \in Clk^{T\backslash\backslash S} \setminus \{x_{new}\}, v_1(c) = v_2(c)\}$. *The* reduced $\sim$-quotient of $[\![T\backslash\backslash S]\!]_{\text{sem}}$, *denoted by* $[\![T\backslash\backslash S]\!]_{\text{sem}}^{\rho}$, *is defined as TIOTS* $(Q^\rho, q_0^\rho, Act^{T\backslash\backslash S}, \rightarrow^\rho)$ *where* $Q^\rho = Q^{[\![T\backslash\backslash S]\!]_{\text{sem}}/\sim} \setminus \{[q] \mid q \in \{l_e\} \times V_{>0}\}$, $q_0^\rho = q_0^{[\![T\backslash\backslash S]\!]_{\text{sem}}/\sim}$, *and* $\rightarrow^\rho = \rightarrow^{[\![T\backslash\backslash S]\!]_{\text{sem}}/\sim} \cap \{(q_1, a, q_2) \mid q_1, q_2 \in Q, a \in Act^{T\backslash\backslash S}\}$.

**Lemma 19** *Given specification automata* $S = (Loc^S, l_0^S, Act^S, Clk^S, E^S, Inv^S)$ *and* $T = (Loc^T, l_0^T, Act^T, Clk^T, E^T, Inv^T)$ *where* $Act_o^S \cap Act_i^T = \emptyset$. *Then* $[\![T\backslash\backslash S]\!]_{\text{sem}} \simeq [\![T\backslash\backslash S]\!]_{\text{sem}}^{\rho}$.

*Proof* Since bisimulation relation is an equivalence relation, it follows from Lemma 18 that it suffice to show that $[\![T\backslash\backslash S]\!]_{\text{sem}}/\sim \; \simeq [\![T\backslash\backslash S]\!]_{\text{sem}}^{\rho}$. Let $R = \{(q, q) \mid q \in Q^{[\![T\backslash\backslash S]\!]_{\text{sem}}^{\rho}}\}$. We will show that $R$ is a bisimulation relation. First, observe that $(q_0, q_0) \in R$ by definition of $[\![T\backslash\backslash S]\!]_{\text{sem}}^{\rho}$. Instead of checking all six cases of bisimulation (Definition 20), we will show that $q_1 \overset{a}{\not\rightarrow}^{[\![T\backslash\backslash S]\!]_{\text{sem}}/\sim} q_2$ for any $a \in Act^{T\backslash\backslash S} \cup \mathbb{R}_{\geq 0}$ where $q_1 \in Q^{[\![T\backslash\backslash S]\!]_{\text{sem}}^{\rho}}$ and $q_2 \in \{l_e\} \times V_{>0}$ (i.e., $q_2 \notin Q^{[\![T\backslash\backslash S]\!]_{\text{sem}}^{\rho}}$). Only rules 5, 7, and 11 of Definition 19 of the quotient for TIOA have target location $l_e$, and thus could become $q_2$ in the semantic of it. But notice that all three cases have clock reset $c = \{x_{new}\}$. Therefore, any state $(l_e, u)$ reached after taking a transition matching one of these three rules has a valuation $u(x_{new}) = 0$. Thus $(l_e, u) \notin \{l_e\} \times V_{>0}$ and $q_1 \overset{a}{\not\rightarrow}^{[\![T\backslash\backslash S]\!]_{\text{sem}}/\sim} q_2$. Therefore, all reachable state pairs by bisimulation remains within $R$. □

**Lemma 20** *Given specification automata* $S = (Loc^S, l_0^S, Act^S, Clk^S, E^S, Inv^S)$ *and* $T = (Loc^T, l_0^T, Act^T, Clk^T, E^T, Inv^T)$ *where* $Act_o^S \cap Act_i^T = \emptyset$. *Let* $f : Q^{[\![T\backslash\backslash S]\!]_{\text{sem}}^{\rho}} \rightarrow Q^{[\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}}$ *be defined as*

- $f([((l^T, l^S), v)]_\sim) = ((l^T, v^T), (l^S, v^S))$ *for any* $v \in (Clk^{[\![T\backslash\backslash S]\!]_{\text{sem}}} \times \mathbb{R}_{\geq 0})$, $l^T \in Loc^T$, $v^T \in (Clk^T \times \mathbb{R}_{\geq 0})$, $l^S \in Loc^S$, *and* $v^S \in (Clk^S \times \mathbb{R}_{\geq 0})$ *such that* $\forall x \in Clk^T : v(x) = v^T(x)$ *and* $\forall x \in Clk^S : v(x) = v^S(x)$.
- $f([(l_u, v)]_\sim) = u$ *for any* $v \in (Clk^{[\![T\backslash\backslash S]\!]_{\text{sem}}} \times \mathbb{R}_{\geq 0})$.
- $f([(l_e, v)]_\sim) = e$ *for any* $v \in V_0$.

*Then* $f$ *is a bijective function.*

*Proof* It follows directly from the definition that $f$ is injective. We only have to show that $f$ is surjective, where the last two cases are again trivial by definition of $f$. Thus we only have to show that any state $((l^T, v^T), (l^S, v^S))$ maps to only a single state $[((l^T, l^S), v)]_\sim$ in $[\![T\backslash\backslash S]\!]_{\text{sem}}^{\rho}$. For this, note that $\sim$ in Definition 22 contains $\{((l, v_1), (l, v_2)) \mid l \in Loc^{T\backslash\backslash S} \setminus \{l_e, l_u\}, v_1, v_2 \in [Clk^{T\backslash\backslash S} \mapsto \mathbb{R}_{\geq 0}], \forall c \in$

$Clk^{T\backslash\backslash S} \setminus \{x_{new}\}, v_1(c) = v_2(c)\}$. Now we will show that state $((l^T, v^T), (l^S, v^S))$ maps to only a single state $[((l^T, l^S), v)]_\sim$ using contradiction. Assume that state $((l^T, v^T), (l^S, v^S))$ maps to two (or more) states $[((l_1^T, l_1^S), v_1)]_\sim$ and $[((l_2^T, l_2^S), v_1)]_\sim$. From $\sim$ it follows that either $l_1^T \neq l_2^T$, $l_1^S \neq l_2^S$, or $\exists c \in Clk^{T\backslash\backslash S} \setminus \{x_{new}\} : v_1(c) \neq v_2(c)$. But since we only consider a single state $((l^T, v^T), (l^S, v^S))$, none of these options can hold. Thus our assumption does not hold, which concludes the proof. □

Since we now have a bijective function $f$ relating states in $[\![T\backslash\backslash S]\!]^\rho_{\text{sem}}$ and $[\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}$ together, we can effectively relabel the states in $[\![T\backslash\backslash S]\!]^\rho_{\text{sem}}$ from $[((l^T, l^S), v)]_\sim$ to $((l^T, l^S), v^{T,S})$ in all proofs below, where $v^{T,S} \in [Clk^T \cup Clk^S \mapsto \mathbb{R}_{\geq 0}]$ with $\forall c \in Clk^T \cup Clk^S : v^{T,S}(c) = v(c)$. Notice that we remove the clock $x_{new}$ from the state label, as this clock is not present in the state labels in $[\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}$. Thus $Q^{[\![T\backslash\backslash S]\!]^\rho_{\text{sem}}} = \{((l^T, l^S), v) \mid l^T \in Loc^T, l^S \in Loc^S, v \in [Clk^T \cup Clk^S \mapsto \mathbb{R}_{\geq 0}]\} \cup \{u, e\}$.

**Lemma 21** *Given specification automata* $S = (Loc^S, l_0^S, Act^S, Clk^S, E^S, Inv^S)$ *and* $T = (Loc^T, l_0^T, Act^T, Clk^T, E^T, Inv^T)$ *where* $Act_o^S \cap Act_i^T = \emptyset$. *Then* $\forall [q] \in Q^{[\![T\backslash\backslash S]\!]^\rho_{\text{sem}}}, \forall q \in [q]_\sim$*:* $q \in \text{cons}^{[\![T\backslash\backslash S]\!]_{\text{sem}}}$ *iff* $[q] \in \text{cons}^{[\![T\backslash\backslash S]\!]^\rho_{\text{sem}}}$.

*Proof* From Lemmas 18 and 19 it follows that $[\![T\backslash\backslash S]\!]_{\text{sem}} \simeq [\![T\backslash\backslash S]\!]^\rho_{\text{sem}}$. With $R_1 = \{(q, [q]_\sim) \mid q \in Q^{[\![T\backslash\backslash S]\!]_{\text{sem}}}\}$ being the bisimulation relation for $[\![T\backslash\backslash S]\!]_{\text{sem}} \simeq [\![T\backslash\backslash S]\!]_{\text{sem}}/\!\sim$ and $R_2 = \{(q, q) \mid q \in Q^{[\![T\backslash\backslash S]\!]^\rho_{\text{sem}}}\}$ the bisimulation relation for $[\![T\backslash\backslash S]\!]_{\text{sem}}/\!\sim\, \simeq [\![T\backslash\backslash S]\!]^\rho_{\text{sem}}$, we have that $R = \{(q, [q]_\sim) \mid [q]_\sim \in Q^{[\![T\backslash\backslash S]\!]^\rho_{\text{sem}}}\}$ is a bisimulation relation for $[\![T\backslash\backslash S]\!]_{\text{sem}} \simeq [\![T\backslash\backslash S]\!]^\rho_{\text{sem}}$. Using this bisimulation relation, we can easily see that $q$ is an error state iff $[q]_\sim$ is an error state.

We will now proof $q \in \text{cons}^{[\![T\backslash\backslash S]\!]_{\text{sem}}}$ iff $[q] \in \text{cons}^{[\![T\backslash\backslash S]\!]^\rho_{\text{sem}}}$ by contradiction. First, assume that $[q] \in \text{cons}^{[\![T\backslash\backslash S]\!]^\rho_{\text{sem}}}$, but $\exists q' \in [q]_\sim$ such that $q' \notin \text{cons}^{[\![T\backslash\backslash S]\!]_{\text{sem}}}$. That means that there exists a path from $q'$ to an error state $q''$. But since $[\![T\backslash\backslash S]\!]_{\text{sem}} \simeq [\![T\backslash\backslash S]\!]^\rho_{\text{sem}}$, it follows that $[\![T\backslash\backslash S]\!]^\rho_{\text{sem}}$ can simulate the same path from $[q]_\sim$, and using $R$ we have that $[\![T\backslash\backslash S]\!]^\rho_{\text{sem}}$ reaches state $[q'']_\sim$. But since we assume that $[q] \in \text{cons}^{[\![T\backslash\backslash S]\!]^\rho_{\text{sem}}}$, it must hold that $[q'']_\sim$ is not an error state. But this contradicts with the previous observation on error states. Showing the contradiction the other way around follows the same argument. Therefore, we can conclude that $q \in \text{cons}^{[\![T\backslash\backslash S]\!]_{\text{sem}}}$ iff $[q] \in \text{cons}^{[\![T\backslash\backslash S]\!]^\rho_{\text{sem}}}$. □

**Lemma 22** *Given specification automata* $S = (Loc^S, l_0^S, Act^S, Clk^S, E^S, Inv^S)$ *and* $T = (Loc^T, l_0^T, Act^T, Clk^T, E^T, Inv^T)$ *where* $Act_o^S \cap Act_i^T = \emptyset$. *Then* $([\![T\backslash\backslash S]\!]_{\text{sem}})^\Delta \simeq ([\![T\backslash\backslash S]\!]^\rho_{\text{sem}})^\Delta$.

*Proof* First, observe from Definition 12 that adversarial pruning does not alter the action set. Therefore, together with Definition 22 of the reduced quotient it follows that $([\![T\backslash\backslash S]\!]_{\text{sem}})^\Delta$ and $([\![T\backslash\backslash S]\!]^\rho_{\text{sem}})^\Delta$ have the same action set. From the proof of Lemma 21 it follows that $R = \{(q, [q]_\sim) \mid q \in Q^{([\![T\backslash\backslash S]\!]_{\text{sem}})^\Delta}\}$ is a bisimulation relation showing $[\![T\backslash\backslash S]\!]_{\text{sem}} \simeq [\![T\backslash\backslash S]\!]^{\rho}_{\text{sem}}$. Finally, using the result of Lemma 21 that $\forall [q] \in Q^{[\![T\backslash\backslash S]\!]^{\rho}_{\text{sem}}}, \forall q \in [q]_{\sim}$: $q \in \text{cons}^{[\![T\backslash\backslash S]\!]_{\text{sem}}}$ iff $[q] \in \text{cons}^{[\![T\backslash\backslash S]\!]^{\rho}_{\text{sem}}}$ together with Definition 12, we can immediately conclude that $R = \{(q, [q]_{\sim}) \mid q \in Q^{([\![T\backslash\backslash S]\!]_{\text{sem}})^{\Delta}}\}$ is also a bisimulation relation showing $([\![T\backslash\backslash S]\!]_{\text{sem}})^{\Delta} \simeq ([\![T\backslash\backslash S]\!]^{\rho}_{\text{sem}})^{\Delta}$. □

**Lemma 23** *Given specification automata* $S = (Loc^S, l_0^S, Act^S, Clk^S, E^S, Inv^S)$ *and* $T = (Loc^T, l_0^T, Act^T, Clk^T, E^T, Inv^T)$ *where* $Act_o^S \cap Act_i^T = \emptyset$. *Then* $\text{imerr}^{[\![T\backslash\backslash S]\!]^{\rho}_{\text{sem}}} \subseteq \text{imerr}^{[\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}}$ *and* $\text{imerr}^{[\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}} \subseteq \text{incons}^{[\![T\backslash\backslash S]\!]^{\rho}_{\text{sem}}}$.

*Proof* First, observe that the semantic of a TIOA and the reduced quotient do not alter the action set. Therefore, it follows directly that $[\![T\backslash\backslash S]\!]^{\rho}_{\text{sem}}$ and $[\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}$ have the same action set and partitioning into input and output actions, except that $[\![T\backslash\backslash S]\!]^{\rho}_{\text{sem}}$ has an additional input event $i_{new}$, i.e., $Act^{[\![T\backslash\backslash S]\!]^{\rho}_{\text{sem}}} \cup \{i_{new}\} = Act^{[\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}}$.

It follows from Lemma 20 that there is a bijective function $f$ relating states from $[\![T\backslash\backslash S]\!]^{\rho}_{\text{sem}}$ and $[\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}$ together. Therefore, we can effectively say that they have the same state set (up to relabeling), i.e., $Q^{[\![T\backslash\backslash S]\!]^{\rho}_{\text{sem}}} = Q^{[\![T\backslash\backslash S]\!]_{\text{sem}}}$. For brevity, in the rest of this proof we write we write $X = [\![T\backslash\backslash S]\!]^{\rho}_{\text{sem}}$, $Y = [\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}$, $Clk = Clk^T \uplus Clk^S$, and $v^S$ and $v^T$ to indicate the part of a valuation $v$ of only the clocks of $S$ and $T$, respectively. Note that $x_{new} \notin Clk$, but $x_{new} \in Clk^X$.

$\text{imerr}^{[\![T\backslash\backslash S]\!]^{\rho}_{\text{sem}}} \subseteq \text{imerr}^{[\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}}$. From Definition 19 of the quotient for TIOA and Definition 22 of the reduced $\sim$-quotient of $[\![T\backslash\backslash S]\!]_{\text{sem}}$, it follows that states in $\{(l_e, v) \in Q^{[\![T\backslash\backslash S]\!]^{\rho}_{\text{sem}}} \mid v(x_{new}) = 0\} = \text{imerr}^{[\![T\backslash\backslash S]\!]^{\rho}_{\text{sem}}}$ are immediate error states, as only states with location $l_e$ have an invariant other than $\mathbf{T}$. From Lemma 20, we have that $\forall q \in f(q) = e$ with $e \in Q^{[\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}}$. From Definition 18 of the quotient for TIOTS, it follows immediately that $e$ is an error state, since only $d = 0$ time delay is possible without any transition labeled with output actions. Thus $e \in \text{imerr}^{[\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}}$. This shows that $\text{imerr}^{[\![T\backslash\backslash S]\!]^{\rho}_{\text{sem}}} \subseteq \text{imerr}^{[\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}}$.

$\text{imerr}^{[\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}} \subseteq \text{incons}^{[\![T\backslash\backslash S]\!]^{\rho}_{\text{sem}}}$. From Definition 18 of the quotient for TIOTS, it follows that state $e$ is an immediate error state and that states in $\{(q^T, q^S) \in Q^{[\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}} \mid q^T \xrightarrow{d}\!\!\!\!\!\!/\;\, [\![T]\!]_{\text{sem}} \wedge q^S \xrightarrow{d} [\![S]\!]_{\text{sem}}\}$ are potentially error states, as these states have no outgoing delay transition, i.e., $(q^T, q^S) \xrightarrow{d}\!\!\!\!\!\!/\;\, [\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}$. Some states of this set are actual immediate error states if $\not\exists o! \in Act_o^{[\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}}$ s.t. $(q^T, q^S) \xrightarrow{o!}\!\!\!\!\!\!/\;\, [\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}$. By Definition 18 we have that $Act_o^{[\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}} = Act_o^T \setminus Act_o^S \cup Act_i^S \setminus Act_i^T$. Consider the following two cases.

- $o! \in Act_o^T \setminus Act_o^S$. Assume that $(q^T, q^S) \xrightarrow{o!}\!\!\!\!\!\!/\;\, [\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}$, such that $(q^T, q^S)$ is actually an error state. It follows from Definition 3 of the semantic that $q^{[\![T]\!]_{\text{sem}}} = (l^T, v^T)$ and $v^T + d \not\models Inv(l^T)$; similarly we have that $q^{[\![S]\!]_{\text{sem}}} = (l^S, v^S)$ and $v^S + d \models Inv(l^S)$. Since TIOTSs are time additive, see Definition 1, we can assume that for $\forall d' < d : v^T + d' \not\models Inv(l^T)$[14]. Thus $v^T + 0 \not\models Inv(l^T)$, which simplifies to $v^T \not\models Inv(l^T)$. Again, using time additivity of TIOTS and $v^S + d \models Inv(l^S)$, we have that $v^S + 0 \models Inv(l^S)$. Combining this information, we have that $v \models \neg Inv(l^T) \wedge Inv(l^S)$, where we used the fact that $Clk^T \cap Clk^S =$

[14]In case there would be a $d' < d$ such that $v^T + d' \models Inv(l^T)$, we can first delay $d'$ in $[\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}$ such that the reached state can no longer delay.

$\emptyset$. Now, using Definition 19 of the quotient for TIOA and Definition 3 of the semantics, we have that $(l^T, l^S, v) \xrightarrow{i_{new}}{}^{[\![T\backslash\backslash S]\!]_{\text{sem}}} (l_e, v)$. Since the target state $(l_e, v)$ is an immediate error state and $i_{new}$ is an input action, it follows the controllable predecessor operator that $(l^T, l^S, v) \in \text{incons}^{[\![T\backslash\backslash S]\!]^{\rho}_{\text{sem}}}$.

- $o? \in Act_i^S \setminus Act_i^T$. Since $S$ is a specification, it is input-enabled, see Definition 4. Therefore, $q^S \xrightarrow{o?}{}^{[\![S]\!]_{\text{sem}}}$. From the second rule of Definition 18 of the quotient for TIOTS, it follows that $(q^T, q^S) \xrightarrow{o!}{}^{[\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}}$. Therefore, in this case state $(q^T, q^S)$ is not an error state in $[\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}$.

□

**Lemma 24** *Given specification automata $S = (Loc^S, l_0^S, Act^S, Clk^S, E^S, Inv^S)$ and $T = (Loc^T, l_0^T, Act^T, Clk^T, E^T, Inv^T)$ where $Act_o^S \cap Act_i^T = \emptyset$. Denote $X = [\![T\backslash\backslash S]\!]^{\rho}_{\text{sem}}$ and $Y = [\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}$, and let $d \in \mathbb{R}_{\geq 0}$ and $q_1, q_2 \in Q^X \cap Q^Y$ with $q_1 = (l^T, l^S, v)$ for some $v \in (Clk^T \uplus Clk^S \to \mathbb{R}_{\geq 0})$. If $v \not\models \neg Inv(l^T) \land Inv(l^S)$, then $q_1 \xrightarrow{d}{}^X q_2$ if and only if $q_1 \xrightarrow{d}{}^Y q_2$.*

*Proof* It follows from Lemma 20 that there is a bijective function $f$ relating states from $[\![T\backslash\backslash S]\!]^{\rho}_{\text{sem}}$ and $[\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}$ together. Therefore, we can effectively say that they have the same state set (up to relabeling), i.e., $Q^{[\![T\backslash\backslash S]\!]^{\rho}_{\text{sem}}} = Q^{[\![T\backslash\backslash S]\!]_{\text{sem}}}$. For brevity, in the rest of this proof we write we write $Clk = Clk^T \uplus Clk^S$, and $v^S$ and $v^T$ to indicate the part of a valuation $v$ of only the clocks of $S$ and $T$, respectively. Note that $x_{new} \notin Clk$, but $x_{new} \in Clk^X$.

From Definition 19 of the quotient for TIOA it follows that $Inv((l^T, l^S)) = \mathbf{T}$. Therefore, with Definition 3 of the semantic and Definition 22 of the $\sim$-reduced quotient of $[\![T\backslash\backslash S]\!]_{\text{sem}}$ it follows that $q_1 \xrightarrow{d}{}^X q_2$ is possible for any $d \in \mathbb{R}_{\geq 0}$ and any valuation $v$. Thus $q_1 \xrightarrow{d}{}^Y q_2$ implies $q_1 \xrightarrow{d}{}^X q_2$.

It remains to show the other way around. Observe from Definition 18 of the quotient for TIOTS that there are two cases involving a delay (actually three, but we do not consider the universal location in this lemma). So a delay is only possible from $q_1$ if either $q_1^{[\![T]\!]_{\text{sem}}} \xrightarrow{d}{}^{[\![T]\!]_{\text{sem}}} q_2^{[\![T]\!]_{\text{sem}}} \land q_1^{[\![S]\!]_{\text{sem}}} \xrightarrow{d}{}^{[\![S]\!]_{\text{sem}}} q_2^{[\![S]\!]_{\text{sem}}}$ or $q_1^{[\![S]\!]_{\text{sem}}} \not\xrightarrow{d}{}^{[\![S]\!]_{\text{sem}}}$. So a delay is *not* possible if $q_1^{[\![T]\!]_{\text{sem}}} \not\xrightarrow{d}{}^{[\![T]\!]_{\text{sem}}} \land q_1^{[\![S]\!]_{\text{sem}}} \xrightarrow{d}{}^{[\![S]\!]_{\text{sem}}} q_2^{[\![S]\!]_{\text{sem}}}$. It follows from Definition 3 of the semantic that $q_1^{[\![T]\!]_{\text{sem}}} = (l^T, v^T)$ and $v^T + d \not\models Inv(l^T)$ or $\exists d' \in \mathbb{R}_{\geq 0}, d' < d : v^T + d' \not\models Inv(l^T)$; similarly we have that $q_1^{[\![S]\!]_{\text{sem}}} = (l^S, v^S)$, $v^S + d \models Inv(l^S)$, and $\forall d' \in \mathbb{R}_{\geq 0}, d' < d : v^S + d' \models Inv(l^S)$. Without loss of generality, we can state that $d' = 0$[15], so $v^T + 0 \not\models Inv(l^T)$, which simplifies to $v^T \not\models Inv(l^T)$. We have also that $v^S + 0 \models Inv(l^S)$. Combining this information, we have that $v \models \neg Inv(l^T) \land Inv(l^S)$, where we used the fact that $Clk^T \cap Clk^S = \emptyset$. But this contradicts with the assumption in the lemma. Thus we can conclude that if $v \not\models \neg Inv(l^T) \land Inv(l^S)$, then $q_1 \xrightarrow{d}{}^X q_2$ implies $q_1 \xrightarrow{d}{}^Y q_2$. □

[15]In case there would be a $d' > 0$ such that $v^T + d' \models Inv(l^T)$, we can first delay $d'$ in $[\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}$ such that the reached state can no longer delay.

**Lemma 25** *Given specification automata $S = (Loc^S, l_0^S, Act^S, Clk^S, E^S, Inv^S)$ and $T = (Loc^T, l_0^T, Act^T, Clk^T, E^T, Inv^T)$ where $Act_o^S \cap Act_i^T = \emptyset$. Then* $\mathrm{cons}^{[\![T \backslash\backslash S]\!]_{\mathrm{sem}}^{\rho}} = \mathrm{cons}^{[\![T]\!]_{\mathrm{sem}} \backslash\backslash [\![S]\!]_{\mathrm{sem}}}$.

*Proof* We will proof this by using the $\Theta$ operator. First, observe that the semantic of a TIOA and the reduced quotient do not alter the action set. Therefore, it follows directly that $[\![T \backslash\backslash S]\!]_{\mathrm{sem}}^{\rho}$ and $[\![T]\!]_{\mathrm{sem}} \backslash\backslash [\![S]\!]_{\mathrm{sem}}$ have the same action set and partitioning into input and output actions, except that $[\![T \backslash\backslash S]\!]_{\mathrm{sem}}^{\rho}$ has an additional input event $i_{new}$, i.e., $Act^{[\![T \backslash\backslash S]\!]_{\mathrm{sem}}^{\rho}} \cup \{i_{new}\} = Act^{[\![T]\!]_{\mathrm{sem}} \backslash\backslash [\![S]\!]_{\mathrm{sem}}}$.

It follows from Lemma 20 that there is a bijective function $f$ relating states from $[\![T \backslash\backslash S]\!]_{\mathrm{sem}}^{\rho}$ and $[\![T]\!]_{\mathrm{sem}} \backslash\backslash [\![S]\!]_{\mathrm{sem}}$ together. Therefore, we can effectively say that they have the same state set (up to relabeling), i.e., $Q^{[\![T \backslash\backslash S]\!]_{\mathrm{sem}}^{\rho}} = Q^{[\![T \backslash\backslash S]\!]_{\mathrm{sem}}}$. For brevity, in the rest of this proof we write we write $X = [\![T \backslash\backslash S]\!]_{\mathrm{sem}}^{\rho}$, $Y = [\![T]\!]_{\mathrm{sem}} \backslash\backslash [\![S]\!]_{\mathrm{sem}}$, $Clk = Clk^T \uplus Clk^S$, and $v^S$ and $v^T$ to indicate the part of a valuation $v$ of only the clocks of $S$ and $T$, respectively. Note that $x_{new} \notin Clk$, but $x_{new} \in Clk^X$.

We will show for any postfixed point $P$ of $\Theta$ that $\Theta^{[\![T \backslash\backslash S]\!]_{\mathrm{sem}}^{\rho}}(P) \subseteq \Theta^{[\![T]\!]_{\mathrm{sem}} \backslash\backslash [\![S]\!]_{\mathrm{sem}}}(P)$ and $\Theta^{[\![T]\!]_{\mathrm{sem}} \backslash\backslash [\![S]\!]_{\mathrm{sem}}}(P) \subseteq \Theta^{[\![T \backslash\backslash S]\!]_{\mathrm{sem}}^{\rho}}(P)$.

($\Theta^X(P) \subseteq \Theta^Y(P)$) Consider a state $q^X \in P$. Because $P$ is a postfixed point of $\Theta^X$, it follows that $q^X \in \Theta^X(P)$. From the definition of $\Theta$, it follows that $q^X \in \overline{\mathrm{err}^X(\overline{P})}$ and $q^X \in \{q_1 \in Q^X \mid \forall d \geq 0 : [\forall q_2 \in Q^X : q_1 \xrightarrow{d}{}^X q_2 \Rightarrow q_2 \in P \wedge \forall i? \in Act_i^X : \exists q_3 \in P : q_2 \xrightarrow{i?}{}^X q_3] \vee [\exists d' \leq d \wedge \exists q_2, q_3 \in P \wedge \exists o! \in Act_o^X : q_1 \xrightarrow{d'}{}^X q_2 \wedge q_2 \xrightarrow{o!}{}^X q_3 \wedge \forall i? \in Act_i^X : \exists q_4 \in P : q_2 \xrightarrow{i?}{}^X q_4]\}$. We will focus on the second part of the definition of $\Theta$.

Consider a $d \in \mathbb{R}_{\geq 0}$. Then the left-hand side or the right-hand side of the disjunction is true (or both).

- Assume the left-hand side is true, i.e., $\forall q_2 \in Q^X : q^X \xrightarrow{d}{}^X q_2 \Rightarrow q_2 \in P \wedge \forall i? \in Act_i^X : \exists q_3 \in P : q_2 \xrightarrow{i?}{}^X q_3$. Pick a $q_2 \in Q^X$. The implication is true when $q^X \not\xrightarrow{d}{}^X q_2$ or $q^X \xrightarrow{d}{}^X q_2 \wedge q_2 \in P \wedge \forall i? \in Act_i^X : \exists q_3 \in P : q_2 \xrightarrow{i?}{}^X q_3$.
  - Consider the first case. This case is only applicable if $q^X = (l_e, v)$, since in Definition 19 of the quotient for TIOA only location $l_e$ has an invariant other than $\mathbf{T}$. But then $q^X \in \mathrm{imerr}^X$. This contradicts with the fact that $q^X \in \Theta(P)$ implies that $q^X \in \overline{\mathrm{err}^X(\overline{P})}$. Thus this case is infeasible.
  - Consider the second case. From Definition 3 of the semantic of a TIOA and Definition 22 of the $\sim$-reduced quotient of $[\![T \backslash\backslash S]\!]_{\mathrm{sem}}$ it follows that $v_1 + d \models Inv^{T \backslash\backslash S}(l_1)$ for $q^X = (l_1, v_1)$, $q_2 = (l_1, v_1 + d)$, $l_1 \in Loc^{T \backslash\backslash S}$, and $v_1 \in [Clk \mapsto \mathbb{R}_{\geq 0}]$. Since $q^X \in \overline{\mathrm{err}^X(\overline{P})}$, we have that $l_1 \neq l_e$, thus $Inv^{T \backslash\backslash S}(l_1) = \mathbf{T}$. Now, pick $i? \in Act_i^X$ and $q_3 \in Q^X$ such that $q_2 \xrightarrow{i?}{}^X q_3$ and $q_3 \in P$. From Definition 3 of the semantic of a TIOA it follows that $(l_1, i?, \varphi, c, l_3) \in E^{T \backslash\backslash S}$, $q_3 = (l_3, v_3)$, $v_1 + d \models \varphi$, $v_3 = v_1 + d[r \mapsto 0]_{r \in c}$, and $v_3 \models Inv^{T \backslash\backslash S}(l_3)$.

    From Lemma 24 it follows that $q^X \xrightarrow{d}{}^Y q_2$ if $v \not\models \neg Inv(l^T) \wedge Inv(l^S)$. In case that $v \models \neg Inv(l^T) \wedge Inv(l^S)$, we have from Definitions 19, 3, and 22 that $q^X \xrightarrow{i_{new}}{}^X e$. But since $e \in \mathrm{err}^X(\overline{P})$, it follows that $e \notin P$. Therefore, this case is infeasible. Thus we have that $q^X \xrightarrow{d}{}^Y q_2$ in $Y$.

Now, consider the eleven cases from Definition 19 of quotient of TIOAs. Remember that $Act_i^X = Act_i^{T \backslash\backslash S} = Act_i^T \cup Act_o^S \cup \{i_{new}\}$.

1. $i? \in Act^S \cap Act^T$, $l_1 = (l_1^T, l_1^S)$, $l_3 = (l_3^T, l_3^S)$, $\varphi = \varphi^T \wedge Inv(l_3^T)[r \mapsto 0]_{r \in c^T} \wedge \varphi^S \wedge Inv(l_1^S) \wedge Inv(l_3^S)[r \mapsto 0]_{r \in c^S}$, $c = c^T \cup c^S$, $(l_1^T, i, \varphi^T, c^T, l_3^T) \in E^T$, and $(l_1^S, i, \varphi^S, c^S, l_3^S) \in E^S$. Since $v_1 + d \models \varphi$, it holds that $v_1 + d \models \varphi^T$, $v_1 + d \models Inv(l_3^T)[r \mapsto 0]_{r \in c^T}$, $v_1 + d \models \varphi^S$, $v_1 + d \models Inv(l_1^S)$, and $v_1 + d \models Inv(l_3^S)[r \mapsto 0]_{r \in c^S}$. Because $Clk^S \cap Clk^T = \emptyset$, it holds that $v_1^T + d \models \varphi^T$, $v_1^T + d \models Inv(l_3^T)[r \mapsto 0]_{r \in c^T}$, $v_1^S + d \models \varphi^S$, $v_1^S + d \models Inv(l_1^S)$, and $v_1^S + d \models Inv(l_3^S)[r \mapsto 0]_{r \in c^S}$. Since $v_3 = v_1 + d[r \mapsto 0]_{r \in c}$, it holds that $v_3^T = v_1^T + d[r \mapsto 0]_{r \in c^T}$ and $v_3^S = v_1^S + d[r \mapsto 0]_{r \in c^S}$. Therefore, $v_3^T + d \models Inv(l_3^T)$ and $v_3^S + d \models Inv(l_3^S)$.

   Combining all information about $T$, we have that $(l_1^T, i, \varphi^T, c^T, l_2^T) \in E^T$, $v_1^T + d \models \varphi^T$, $v_3^T = v_1^T + d[r \mapsto 0]_{r \in c^T}$, and $v_3^T \models Inv(l_3^T)$. Therefore, from Definition 3 it follows that $(l_1^T, v_1^T + d) \xrightarrow{i} (l_3^T, v_3^T)$ in $[\![T]\!]_{\text{sem}}$. Combining all information about $S$, we have that $(l_1^S, i, \varphi^S, c^S, l_2^S) \in E^S$, $v_1^S + d \models \varphi^S$, $v_3^S = v_1^S + d[r \mapsto 0]_{r \in c^S}$, and $v_3^S \models Inv(l_3^S)$. Therefore, from Definition 3 it follows that $(l_1^S, v_1^S + d) \xrightarrow{i} (l_3^S, v_3^S)$ in $[\![S]\!]_{\text{sem}}$.

   Now, from Definition 18 it follows that $((l_1^T, v_1^T + d), (l_1^S, v_1^S + d)) = (l_1^T, l_1^S, v_1 + d) = q_2^Y \xrightarrow{i?}{}^Y ((l_3^T, v_3^T), (l_3^S, v_3^S)) = (l_3^T, l_3^S, v_3) = q_3^Y$ in $Y$. Thus, we can simulate a transition in $Y$. Also, observe now that $q_2 = q_2^Y$ and $q_3 = q_3^Y$.
2. $i? \in Act^S \setminus Act^T$, $l_1 = (l^T, l_1^S)$, $l_3 = (l^T, l_3^S)$, $\varphi = \varphi^S \wedge Inv(l_1^S) \wedge Inv(l_3^S)[r \mapsto 0]_{r \in c^S}$, $c = c^S$, $l^T \in Loc^T$, and $(l_1^S, i!, \varphi^S, c^S, l_3^S) \in E^S$. Since $v_1 + d \models \varphi$ and $Clk^S \cap Clk^T = \emptyset$, it holds that $v_1^S + d \models \varphi^S$, $v_1^S + d \models Inv(l_1^S)$, and $v_1^S + d \models Inv(l_3^S)[r \mapsto 0]_{r \in c^S}$. Since $v_3 = v_1 + d[r \mapsto 0]_{r \in c}$ and $c = c^S$, it holds that $v_3^S = v_1^S + d[r \mapsto 0]_{r \in c^S}$, $v_3^T = v_1^T + d$, and $v_3^S \models Inv(l_3^S)$. Combining all information above about $S$, it follows from Definition 3 that $(l_1^S, v_1^S + d) \xrightarrow{i!} (l_3^S, v_3^S)$ in $[\![S]\!]_{\text{sem}}$. From Definition 3 it also follows that $(l^T, v_1^T + d) \in Q^{[\![T]\!]_{\text{sem}}}$. Therefore, following Definition 18 it follows that $((l^T, v_1^T + d), (l_1^S, v_1^S + d)) = (l^T, l_1^S, v_1 + d) = q_2^Y \xrightarrow{i!}{}^Y ((l^T, v_1^T + d), (l_3^S, v_3^S)) = (l^T, l_3^S, v_3) = q_3^Y$ in $Y$. Thus, we can simulate a transition in $Y$. Also, observe now that $q_2 = q_2^Y$ and $q_3 = q_3^Y$.
3. $i! \in Act_o^S$, $l_1 = (l^T, l_1^S)$, $l_3 = l_u$, $\varphi = \neg G_S$, $c = \emptyset$, $l^T \in Loc^T$ and $G_S = \bigvee\{\varphi^S \wedge Inv(l_3^S)[r \mapsto 0]_{r \in c^S} \mid (l_1^S, a, \varphi^S, c^S, l_3^S) \in E^S\}$. Since $v_1 + d \models \varphi$ and $Clk^S \cap Clk^T = \emptyset$, it holds that $v_1^S + d \models \neg G_S$. Therefore, $v_1^S + d \not\models G_S$, which indicates that $\forall (l_1^S, a, \varphi^S, c^S, l_3^S) \in E^S$: $v_1^S + d \not\models \varphi^S \wedge Inv(l_3^S)[r \mapsto 0]_{r \in c^S}$. This means that $v_1^S + d \not\models \varphi^S$ or $v_1^S + d \not\models Inv(l_3^S)[r \mapsto 0]_{r \in c^S}$ or both, where the second option is equivalent to $v_1^S + d[r \mapsto 0]_{r \in c^S} \not\models Inv(l_3^S)$. Following Definition 3, we can conclude that $(l_1^S, v_1^S + d) \not\xrightarrow{a}$ in $[\![S]\!]_{\text{sem}}$. From Definition 3 it also follows that $(l^T, v_1^T + d) \in Q^{[\![T]\!]_{\text{sem}}}$. Now, following Definition 18, we have transition $((l^T, v_1^T + d), (l_1^S, v_1^S + d)) = (l^T, l_1^S, v_1 + d) = q_2^Y \xrightarrow{a}$

$^{Y} u = q_3^Y$ in $Y$. Thus we can simulate a transition in $Y$. Also, observe now that $q_2 = q_2^Y$ and $q_3 = q_3^Y$ (where $(l_u, v_3)$ is mapped into $u$ by $f$ from Lemma 20).

4. $i? \in Act^S \cup Act^T$, $l_1 = (l^T, l^S)$, $l_3 = l_u$, $\varphi = \neg Inv(l^S)$, $c = \emptyset$, $l^T \in Loc^T$, and $l^S \in Loc^S$.(If $i? = i_{new}$, this case is trivial, see item 8 and 10 below.) Since $v_1 + d \models \varphi$ and $Clk^S \cap Clk^T = \emptyset$, it holds that $v_1^S + d \models \neg Inv(l^S)$. Therefore, $v_1^S + d \not\models Inv(l^S)$. Since we delayed into state $q_2^Y$, it must hold that the delay was according to rule 6 of Definition 18 of the quotient for TIOTS. Therefore, $q_2^Y = u \in P$. From Definition 18 it also follows that $u = q_2^Y \xrightarrow{i?}{}^Y u = q_3^Y$ in $Y$. Thus we can simulate a transition in $Y$. Also, observe now that $q_3 = q_3^Y$ (where $(l_u, v_3)$ is mapped into $u$ by $f$ from Lemma 20).
5. $i! \in Act_o^S \cap Act_o^T$, $l_1 = (l_1^T, l_1^S)$, $l_3 = l_e$, $\varphi = \varphi^S \wedge Inv(l_3^S)[r \mapsto 0]_{r \in c^S} \wedge \neg G_T$, $c = \{x_{new}\}$, $(l_1^S, a, \varphi^S, c^S, l_3^S) \in E^S$, and $G_T = \bigvee\{\varphi^T \wedge Inv(l_3^T)[r \mapsto 0]_{r \in c^T} \mid (l_1^T, a, \varphi^T, c^T, l_3^T) \in E^T\}$. Since the target location is the error location, it holds that $q_3 \notin P$. Thus this case is not feasible.
6. $i! \in Act_o^S \cap Act_o^T$, $l_1 = l_3 = (l_1^T, l_1^S)$, $\varphi = \neg G_S \wedge \neg G_T$, $c = \emptyset$, $G_S = \bigvee\{\varphi^S \wedge Inv(l_3^S)[r \mapsto 0]_{r \in c^S} \mid (l_1^S, a, \varphi^S, c^S, l_3^S) \in E^S\}$, and $G_T = \bigvee\{\varphi^T \wedge Inv(l_3^T)[r \mapsto 0]_{r \in c^T} \mid (l_1^T, a, \varphi^T, c^T, l_3^T) \in E^T\}$. Since $v_1 + d \models \varphi$, it holds that $v_1 + d \models \neg G_S$ and $v_1 + d \models \neg G_T$. Because $Clk^S \cap Clk^T = \emptyset$, it holds that $v_1^S + d \models \neg G_S$ and $v_1^T + d \models \neg G_T$. This indicates that $v_1^S + d \not\models G_S$ and $v_1^T + d \not\models G_T$, which implies that $\forall (l_1^S, a, \varphi^S, c^S, l_3^S) \in E^S$: $v_1^S + d \not\models \varphi^S \wedge Inv(l_3^S)[r \mapsto 0]_{r \in c^S}$ and $\forall (l_1^T, a, \varphi^T, c^T, l_3^T) \in E^T$: $v_1^T + d \not\models \varphi^T \wedge Inv(l_3^T)[r \mapsto 0]_{r \in c^T}$. This means that $v_1^S + d \not\models \varphi^S$ or $v_1^S + d \not\models Inv(l_3^S)[r \mapsto 0]_{r \in c^S}$ or both for $S$, and $v_1^T + d \not\models \varphi^T$ or $v_1^T + d \not\models Inv(l_3^T)[r \mapsto 0]_{r \in c^T}$ or both for $T$, where the second option for both $S$ and $T$ is equivalent to $v_1^S + d[r \mapsto 0]_{r \in c^S} \not\models Inv(l_3^S)$ and $v_1^T + d[r \mapsto 0]_{r \in c^T} \not\models Inv(l_3^T)$, respectively. It follows from Definition 3 that $(l_1^S, v_1^S + d) \overset{i!}{\not\longrightarrow}$ in $[\![S]\!]_{\text{sem}}$ and $(l_1^T, v_1^T + d) \overset{i!}{\not\longrightarrow}$ in $[\![T]\!]_{\text{sem}}$. Now, following Definition 18, we have transition $((l_1^T, v_1^T + d), (l_1^S, v_1^S + d)) = (l_1^T, l_1^S, v_1 + d) = q_2^Y \xrightarrow{i?}{}^Y (l_1^T, l_1^S, v_1 + d) = q_3^Y$ in $Y$. Thus we can simulate a transition in $Y$. Also, observe now that $q_2 = q_2^Y$ and $q_3 = q_3^Y$.
7. $a = i_{new}$, $l_1 = (l^T, l^S)$, $l_3 = l_e$, $\varphi = \neg Inv(l^T) \wedge Inv(l^S)$, $c = \{x_{new}\}$, $l^T \in Loc^T$, and $q^S \in Loc^S$. Since the target location is the error location, it holds that $q_3 \notin P$. Thus this case is not feasible.
8. $a = i_{new}$, $l_1 = l_3 = (l_1^T, l_1^S)$, $\varphi = Inv(l^T) \vee \neg Inv(l^S)$ and $c = \emptyset$. First note that $i_{new} \notin Act^Y$. Now, since $c = \emptyset$, it follows that $v_3 = v_1 + d$. Therefore, $q_2 = q_3$. Since $q_3 \in P$, it follows $q_2 \in P$. Since $q_2 = q_2^Y$, it follows that $q_2^Y \in P$.
9. $i? \in Act^T \setminus Act^S$, $l_1 = (l_1^T, l^S)$, $l_3 = (l_3^T, l^S)$, $\varphi = \varphi^T \wedge Inv(l_3^T)[r \mapsto 0]_{r \in c^T} \wedge Inv(l^S)$, $c = c^T$, $l^S \in Loc^S$, and $(l_1^T, i?, \varphi^T, c^T, l_3^T) \in E^T$. Since $v_1 + d \models \varphi$ and $Clk^S \cap Clk^T = \emptyset$, it holds that $v_1^T + d \models \varphi^T$ and $v_1^T + d \models Inv(l_3^T)[r \mapsto 0]_{r \in c^T}$. Since $v_3 = v_1 + d[r \mapsto 0]_{r \in c}$ and $c = c^T$, it holds that $v_3^T = v_1^T + d[r \mapsto 0]_{r \in c^T}$, $v_3^S = v_1^S + d$, and $v_3^T \models Inv(l_3^T)$. Combining all information above about $T$, it follows

from Definition 3 that $(l_1^T, v_1^T + d) \xrightarrow{i?} (l_3^T, v_3^T)$ in $[\![T]\!]_{\text{sem}}$. From Definition 3 it also follows that $(l^S, v_1^S + d) \in Q^{[\![S]\!]_{\text{sem}}}$. Therefore, following Definition 18 it follows that $((l_1^T, v_1^T + d), (l^S, v_1^S + d)) = (l_1^T, l^S, v_1 + d) = q_2^Y \xrightarrow{i?}{}^Y ((l_3^T, v_3^T), (l^S, v_1^S + d)) = (l_3^T, l^S, v_3) = q_3^Y$ in $Y$. Thus, we can simulate a transition in $Y$. Also, observe now that $q_2 = q_2^Y$ and $q_3 = q_3^Y$.

10. $i? \in Act^S \cup Act^T$, $l_1 = l_u$, $l_3 = l_u$, $\varphi = \mathbf{T}$, $c = \emptyset$. Since $q^X = q^Y$, it follows from Definition 18 of the quotient for TIOTS that $Y$ delayed within state $u$ as well, i.e., $q_2^X = q_2^Y$. Therefore, using Definition 18 again, we have that there exists a transition $q_2^Y = u \xrightarrow{i?}{}^Y u = q_3^Y$ in $Y$. Thus, we can simulate a transition in $Y$. Also, observe now that $q_2 = q_2^Y$ and $q_3 = q_3^Y$.
11. $a \in Act_i^S \cup Act_i^T$, $l_1 = l_e$, $l_3 = l_e$, $\varphi = x_{new} = 0$, $c = \emptyset$. Since the target location is the error location, it holds that $q_3^X \notin P$. Thus this case is not feasible.

So, in all feasible cases we have that $q_2^Y \xrightarrow{i?} q_3^Y$ is a transition in $Y$ if $i? \neq i_{new}$. When $i? = i_{new}$, we have shown explicitly that $q_2^Y \in P$. As the analysis above is independent of the particular $i?$, $q_2^Y \xrightarrow{i?} q_3^Y$ is a transition in $Y$ for all $i? \in Act_i^Y$. Furthermore, all feasible cases show that $q_2^Y, q_3^Y \in P$ directly, or because $q_2^Y = q_2$ or $q_3^Y = q_3$.

So, in both cases we have that for $q^X \xrightarrow{d}{}^Y q_2^Y \Rightarrow q_2^Y \in P \wedge \forall i? \in Act_i^Y : \exists q_3^Y \in P : q_2^Y \xrightarrow{i?}{}^Y q_3^Y$. As $q_2$ is chosen arbitrarily, it holds for all $q_2 \in Q^X = Q^Y$. Therefore, the left-hand side is true.

- Assume the right-hand side is true, i.e., $\exists d' \leq d \wedge \exists q_2, q_3 \in P \wedge \exists o! \in Act_o^X$ : $q^X \xrightarrow{d'}{}^X q_2 \wedge q_2 \xrightarrow{o!}{}^X q_3 \wedge \forall i? \in Act_i^X : \exists q_4 \in P : q_2 \xrightarrow{i?}{}^X q_4$.

  Following Definition 3 of the semantic of a TIOA and Definition 22 of the $\sim$-reduced quotient of $[\![T\backslash\backslash S]\!]_{\text{sem}}$, we have that $q^X = (l_1, v_1)$, $q_2 = (l_1, v_1 + d')$, $q_3 = (l_3, v_3)$, $q_4 = (l_4, v_4)$, $l_1, l_3, l_4 \in Loc^{T\backslash\backslash S}$, $v_1, v_3, v_4 \in [Clk \mapsto \mathbb{R}_{\geq 0}]$, $v_1 + d' \models Inv^{T\backslash\backslash S}(l_1)$, $\exists (l_1, o!, \varphi, c, l_3) \in E^{T\backslash\backslash S}$, $v_1 + d' \models \varphi$, $v_3 = v_1 + d'[r \mapsto 0]_{r \in c}$, and $v_3 \models Inv^{T\backslash\backslash S}(l_3)$. First, focus on the delay transition.

  From Lemma 24 it follows that $q^X \xrightarrow{d}{}^Y q_2$ if $v \not\models \neg Inv(l^T) \wedge Inv(l^S)$. In case that $v \models \neg Inv(l^T) \wedge Inv(l^S)$, we have from Definitions 19, 3, and 22 that $q^X \xrightarrow{i_{new}}{}^X e$. But since $e \in \text{err}^X(\overline{P})$, it follows that $e \notin P$. Since $i_{new}$ is an input action, it must hold that $q_2 \notin P$ (see analysis above in the proof). Therefore, this case is infeasible. Thus we have that $q^X \xrightarrow{d}{}^Y q_2$ in $Y$.

  Now consider the output transition labeled with $o!$. Remember that $Act_o^{T\backslash\backslash S} = Act_o^T \setminus Act_o^S \cup Act_i^S \setminus Act_i^T$. We have to consider the eleven cases from Definition 19 of the quotient for TIOA. We can use the exact same argument as before (where now rules 3, 5, and 6 have become infeasible) to show that $q_2 \xrightarrow{o!} q_3$ is a transition in $Y$ for all feasible cases. As the analysis is independent of the particular $o!$, we can conclude that $q^X \xrightarrow{d'}{}^Y q_2 \wedge q_2 \xrightarrow{o!}{}^Y q_3$ with $q_2, q_3 \in P$.

  Finally, consider the input transitions labeled with $i?$. Using the same argument as before, we can show that $q_2 \xrightarrow{i?} q_4$ in $X$ is also a transition in $Y$, and $q_4 \in P$.

Therefore, we can conclude that $q^X \xrightarrow{d'}{}^Y q_2 \wedge q_2 \xrightarrow{o!}{}^Y q_3 \wedge \forall i? \in Act_i^Y : \exists q_4 \in P : q_2 \xrightarrow{i?}{}^Y q_4$ with $q_2, q_3, q_4 \in P$. Thus, the right-hand side is true.

Thus, we have shown that when the left-hand side is true for $q^X$ in $X$, it is also true for $q^X$ in $Y$; and that when the right-hand side is true for $q^X$ in $X$, it is also true for $q^X$ in $Y$. Thus, $q^X \in \Theta^Y(P)$. Since $q^X \in P$ was chosen arbitrarily, it holds for all states in $P$. Once we choose $P$ to be the fixed-point of $\Theta^X$, we have that $\Theta^X(P) \subseteq \Theta^Y(P)$.

($\Theta^Y(P) \subseteq \Theta^X(P)$) Consider a state $q^Y \in P$. Because $P$ is a postfixed point of $\Theta^Y$, it follows that $p \in \Theta^X(Y)$. From the definition of $\Theta$, it follows that $q^Y \in \mathrm{err}^Y(\overline{P})$ and $q^Y \in \{q \in Q^Y \mid \forall d \geq 0 : [\forall q_2 \in Q^Y : q \xrightarrow{d}{}^Y q_2 \Rightarrow q_2 \in P \wedge \forall i? \in Act_i^Y : \exists q_3 \in P : q_2 \xrightarrow{i?}{}^Y q_3] \vee [\exists d' \leq d \wedge \exists q_2, q_3 \in P \wedge \exists o! \in Act_o^Y : q \xrightarrow{d'}{}^Y q_2 \wedge q_2 \xrightarrow{o!}{}^Y q_3 \wedge \forall i? \in Act_i^Y : \exists q_4 \in P : q_2 \xrightarrow{i?}{}^Y q_4]\}$. Now we focus on the second part of the definition of $\Theta$.

Consider a $d \in \mathbb{R}_{\geq 0}$. Then the left-hand side or the right-hand side of the disjunction is true (or both).

- Assume the left-hand side is true, i.e., $\forall q_2 \in Q^Y : q^Y \xrightarrow{d}{}^Y q_2 \Rightarrow q_2 \in P \wedge \forall i? \in Act_i^Y : \exists q_3 \in P : q_2 \xrightarrow{i?}{}^Y q_3$. Pick a $q_2 \in Q^Y$. The implication is true when $q^Y \not\xrightarrow{d}{}^Y q_2$ or $q^Y \xrightarrow{d}{}^Y q_2 \wedge q_2 \in P \wedge \forall i? \in Act_i^Y : \exists q_3 \in P : q_2 \xrightarrow{i?}{}^Y q_3$.
  - Consider the first case. From Lemma 24 it follows that $q^Y \not\xrightarrow{d}{}^Y$ if $v \models \neg Inv(l^T) \wedge Inv(l^S)$ with $q^Y = (l_1, v_1)$. Now we have from Definitions 19, 3, and 22 that $q^Y \xrightarrow{i_{new}}{}^X e$. But since $e \in \mathrm{err}^Y(\overline{P})$, it follows that $e \notin P$. Since $i_{new}$ is an input action, it must hold that $(l_1, v) \notin P$ for any valuation $v$ (see analysis above in the proof). Therefore, $q^Y \not\xrightarrow{d}{}^X$. Thus the implication also holds for $q_2$ in $X$.
  - Consider the second case. From Definition 19 of the quotient for TIOA it follows that $Inv((l^T, l^S)) = \mathbf{T}$. Therefore, with Definition 3 of the semantic and Definition 22 of the $\sim$-reduced quotient of $[\![T \backslash\backslash S]\!]_{\mathrm{sem}}$ it follows that $q^Y \xrightarrow{d}{}^X q_2$. Now, pick an $i? \in Act_i^Y$ with its corresponding $q_3$ according to the implication. Remember that $Act_i^Y = Act_i^T \cup Act_o^S$. We have to consider the ten cases from Definition 18.
    1. $i? \in Act^S \cap Act^T$, $q_2^Y = (q_2^{[\![T]\!]_{\mathrm{sem}}}, q_2^{[\![S]\!]_{\mathrm{sem}}})$, $q_3^Y = (q_3^{[\![T]\!]_{\mathrm{sem}}}, q_3^{[\![S]\!]_{\mathrm{sem}}})$, $q_2^{[\![T]\!]_{\mathrm{sem}}} \xrightarrow{i}{}^{[\![T]\!]_{\mathrm{sem}}} q_3^{[\![T]\!]_{\mathrm{sem}}}$, and $q_2^{[\![S]\!]_{\mathrm{sem}}} \xrightarrow{i}{}^{[\![S]\!]_{\mathrm{sem}}} q_3^{[\![S]\!]_{\mathrm{sem}}}$. From Definition 3 of semantic it follows that there exists an edge $(l_2^T, i, \varphi^T, c^T, l_3^T) \in E^T$ with $q_2^{[\![T]\!]_{\mathrm{sem}}} = (l_2^T, v_2^T)$, $q_3^{[\![T]\!]_{\mathrm{sem}}} = (l_3^T, v_3^T)$, $l_2^T, l_3^T \in Loc^T$, $v_2^T, v_3^T \in [Clk^T \mapsto \mathbb{R}_{\geq 0}]$, $v_2^T \models \varphi^T$, $v_3^T = v_2^T[r \mapsto 0]_{r \in c^T}$, and $v_3^T \models Inv^T(l_3^T)$. Similarly, it follows from the same definition that there exists an edge $(l_2^S, i, \varphi^S, c^S, l_3^S) \in E^S$ with $q_2^{[\![S]\!]_{\mathrm{sem}}} = (l_2^S, v_2^S)$, $q_3^{[\![S]\!]_{\mathrm{sem}}} = (l_3^S, v_3^S)$, $l_2^S, l_3^S \in Loc^S$, $v_2^S, v_3^S \in [Clk^S \mapsto \mathbb{R}_{\geq 0}]$, $v_2^S \models \varphi^S$, $v_3^S = v_2^S[r \mapsto 0]_{r \in c^S}$, and $v_3^S \models Inv^S(l_3^S)$. Based on Definition 19 of the quotient for TIOA, we need to consider the following two cases.
       * $v_2^S \models Inv(l_2^S)$. In this case, there exists an edge $((l_2^T, l_2^S), i, \varphi^T \wedge Inv(l_3^T)[r \mapsto 0]_{r \in c^T} \wedge \varphi^S \wedge Inv(l_2^S) \wedge Inv(l_3^S)[r \mapsto 0]_{r \in c^S}, c^T \cup$

$c^S, (l_3^T, l_3^S))$ in $T \backslash\backslash S$. Let $v_i, i = 1, 2$ be the valuations that combines the one from $T$ with the one from $S$, i.e. $\forall r \in Clk^T : v_i(r) = v_i^T(r)$ and $\forall r \in Clk^S : v_i(r) = v_i^S(r)$. Because $Clk^T \cap Clk^S = \emptyset$, it holds that $v_2 \models \varphi^T$, $v_2 \models \varphi^S$, and $v_2^S \models Inv(l_2^S)$, thus $v_2 \models \varphi^T \wedge \varphi^S \wedge Inv(l_2^S)$; $v_3 = v_2[r \mapsto 0]_{r \in c^T \cup c^S}$; and $v_3 \models Inv^T(l_3^T)$ and $v_3 \models Inv^S(l_3^S)$, thus $v_3 \models Inv^T(l_3^T) \wedge Inv^S(l_3^S)$.

From Definition 3 it now follows that $((l_2^T, l_2^S), v_2) \xrightarrow{i} ((l_3^T, l_3^S), v_3)$ is a transition in $[\![T \backslash\backslash S]\!]_{\text{sem}}$. Because $Clk^T \cap Clk^S = \emptyset$, we can rearrange the states into $((l_2^T, l_2^S), v_2) = ((l_2^T, v_2^S), (l_2^T, v_2^S)) = q_2^Y$ and $((l_3^T, l_3^S), v_3) = ((l_3^T, v_3^T), (l_3^S, v_3^S)) = q_3^Y$. Thus, $q_2^Y \xrightarrow{a} q_3^Y$ is a transition in $[\![T \backslash\backslash S]\!]_{\text{sem}} = Y$. Also, observe now that $q_2^X = q_2^Y$ and $q_3^X = q_3^Y$.

- $v_2^S \not\models Inv(l_2^S)$. In this case, state $q_2 = (l_2^T, v_2^T, l_2^S, v_2^S)$ cannot be reached by delaying into it, since $v_2^S \not\models Inv(l_2^S)$ implies with Definition 3 of the semantic that $\forall q^{[\![S]\!]_{\text{sem}}} \in Q^{[\![S]\!]_{\text{sem}}}$ we have $q^{[\![S]\!]_{\text{sem}}} \overset{d}{\not\longrightarrow}{}^{[\![S]\!]_{\text{sem}}} q_2^{[\![S]\!]_{\text{sem}}}$. From Definition 18 we have that in this case $q^Y \xrightarrow{d}{}^Y u$, and $q_2^Y \neq u$. Thus this case is infeasible.

2. $i! \in Act^S \setminus Act^T$, $q_2^Y = (q^{[\![T]\!]_{\text{sem}}}, q_2^{[\![S]\!]_{\text{sem}}})$, $q_3^Y = (q^{[\![T]\!]_{\text{sem}}}, q_3^{[\![S]\!]_{\text{sem}}})$, $q^{[\![T]\!]_{\text{sem}}} \in Q^{[\![T]\!]_{\text{sem}}}$, and $q_2^{[\![S]\!]_{\text{sem}}} \xrightarrow{i!}{}^{[\![S]\!]_{\text{sem}}} q_3^{[\![S]\!]_{\text{sem}}}$. From Definition 3 of semantic it follows that there exists an edge $(l_2^S, i!, \varphi^S, c^S, l_3^S) \in E^S$ with $q_2^{[\![S]\!]_{\text{sem}}} = (l_2^S, v_2^S)$, $q_3^{[\![S]\!]_{\text{sem}}} = (l_3^S, v_3^S)$, $l_2^S, l_3^S \in Loc^S$, $v_2^S, v_3^S \in [Clk^S \mapsto \mathbb{R}_{\geq 0}]$, $v_2^S \models \varphi^S$, $v_3^S = v_2^S[r \mapsto 0]_{r \in c^S}$, and $v_3^S \models Inv^S(l_3^S)$. From the same definition, it follows that $q^{[\![T]\!]_{\text{sem}}} = (l^T, v^T)$ for some $l^T \in Loc^T$ and $v^T \in [Clk^T \mapsto \mathbb{R}_{\geq 0}]$. Based on Definition 19 of the quotient for TIOA, we need to consider the following two cases.
   - $v_2^S \models Inv(l_2^S)$. In this case, there exists an edge $((l^T, l_2^S), a, \varphi^S \wedge Inv(l_2^S) \wedge Inv(l_3^S)[r \mapsto 0]_{r \in c^S}, c^S, (l^T, l_3^S))$ in $T \backslash\backslash S$. Let $v_i, i = 1, 2$ be the valuations that combines the one from $T$ with the one from $S$, i.e. $\forall r \in Clk^T : v_i(r) = v_i^T(r)$ and $\forall r \in Clk^S : v_i(r) = v_i^S(r)$. Because $Clk^T \cap Clk^S = \emptyset$, it holds that $v_2 \models \varphi^S$, and $v_2 \models Inv(l_2^S)$, thus $v_2 \models \varphi^S \wedge Inv(l_2^S)$; $v_3 = v_2[r \mapsto 0]_{r \in c^S}$; and $v_3 \models Inv^S(l_3^S)$.

     Since $Inv((l^T, l_3^S)) = \mathbf{T}$ by definition $T \backslash\backslash S$, we have that $v_3 \models Inv((l^T, l_3^S))$. From Definition 3 it now follows that $((l^T, l_2^S), v_2) \xrightarrow{i?} ((l^T, l_3^S), v_3)$ is a transition in $[\![T \backslash\backslash S]\!]_{\text{sem}}$. Using Definition 22 of the reduced $\sim$-quotient of $[\![T \backslash\backslash S]\!]_{\text{sem}}$ and Lemma 20, we can rearrange the states into $((l^T, l_2^S), v_2) = ((l^T, v_2^T), (l_2^S, v_2^S)) = q_2^Y$ and $((l^T, l_3^S), v_3) = ((l^T, v_3^T), (l_3^S, v_3^S)) = q_3^Y$, and we can show that $q_2^Y \xrightarrow{i?} q_3^Y$ is a transition in $[\![T \backslash\backslash S]\!]^{\rho}_{\text{sem}} = X$. Also, observe now that $q_2^X = q_2^Y$ and $q_3^X = q_3^Y$.
   - $v_2^S \not\models Inv(l_2^S)$. In this case, state $q_2 = (l_2^T, v_2^T, l_2^S, v_2^S)$ cannot be reached by delaying into it, since $v_2^S \not\models Inv(l_2^S)$ implies with Definition 3 of the semantic that $\forall q^{[\![S]\!]_{\text{sem}}} \in Q^{[\![S]\!]_{\text{sem}}}$ we have $q^{[\![S]\!]_{\text{sem}}} \overset{d}{\not\longrightarrow}{}^{[\![S]\!]_{\text{sem}}} q_2^{[\![S]\!]_{\text{sem}}}$. From Definition 18 we have that in this case $q^Y \xrightarrow{d}{}^Y u$, and $q_2^Y \neq u$. Thus this case is infeasible.

3. $i? \in Act^T \setminus Act^S$, $q_2^Y = (q_2^{[\![T]\!]_{\text{sem}}}, q^{[\![S]\!]_{\text{sem}}})$, $q_3^Y = (q_3^{[\![T]\!]_{\text{sem}}}, q^{[\![S]\!]_{\text{sem}}})$, $q^{[\![S]\!]_{\text{sem}}} \in Q^{[\![S]\!]_{\text{sem}}}$, and $q_2^{[\![T]\!]_{\text{sem}}} \xrightarrow{i?}{}^{[\![T]\!]_{\text{sem}}} q_3^{[\![T]\!]_{\text{sem}}}$. From Definition 3 of semantic it follows that there exists an edge $(l_2^T, i?, \varphi^T, c^T, l_3^T) \in E^T$ with $q_2^{[\![T]\!]_{\text{sem}}} = (l_2^T, v_2^T)$, $q_3^{[\![T]\!]_{\text{sem}}} = (l_3^T, v_3^T)$, $l_2^T, l_3^T \in Loc^T$, $v_2^T, v_3^T \in [Clk^T \mapsto \mathbb{R}_{\geq 0}]$, $v_2^T \models \varphi^T$, $v_3^T = v_2^T[r \mapsto 0]_{r \in c^T}$, and $v_3^T \models Inv^T(l_3^T)$. From the same definition, it follows that $q^{[\![S]\!]_{\text{sem}}} = (l^S, v^S)$ for some $l^S \in Loc^S$ and $v^S \in [Clk^S \mapsto \mathbb{R}_{\geq 0}]$. Based on Definition 19 of the quotient for TIOA, we need to consider the following two cases.
   * $v_2^S \models Inv(l_2^S)$. In this case, there exists an edge $((l_2^T, l^S), i?, \varphi^T \wedge Inv(l_3^T)[r \mapsto 0]_{r \in c^T} \wedge Inv(l^S), c^T, (l_3^T, l^S))$ in $T \backslash\backslash S$. Let $v_i, i = 1, 2$ be the valuations that combines the one from $T$ with the one from $S$, i.e. $\forall r \in Clk^T : v_i(r) = v_i^T(r)$ and $\forall r \in Clk^S : v_i(r) = v_i^S(r)$. Because $Clk^T \cap Clk^S = \emptyset$, it holds that $v_2 \models \varphi^T$, and $v_2 \models Inv(l^S)$, thus $v_2 \models \varphi^T \wedge Inv(l^S)$; $v_3 = v_2[r \mapsto 0]_{r \in c^T}$; and $v_3 \models Inv^T(l_3^T)$.

     Since $Inv((l_3^T, l^S)) = \mathbf{T}$ by definition $T \backslash\backslash S$, we have that $v_3 \models Inv((l_3^T, l^S))$. From Definition 3 it now follows that $((l_2^T, l^S), v_2) \xrightarrow{i?} ((l_3^T, l^S), v_3)$ is a transition in $[\![T \backslash\backslash S]\!]_{\text{sem}}$. Using Definition 22 of the reduced $\sim$-quotient of $[\![T \backslash\backslash S]\!]_{\text{sem}}$ and Lemma 20, we can rearrange the states into $((l_2^T, l^S), v_2) = ((l_2^T, v_2^T), (l^S, v_2^S)) = q_2^Y$ and $((l_3^T, l^S), v_3) = ((l_3^T, v_3^T), (l^S, v_3^S)) = q_3^Y$, and we can show that $q_2^Y \xrightarrow{i?} q_3^Y$ is a transition in $[\![T \backslash\backslash S]\!]_{\text{sem}}^{\rho} = X$. Also, observe now that $q_2^X = q_2^Y$ and $q_3^X = q_3^Y$.
   * $v_2^S \not\models Inv(l_2^S)$. In this case, state $q_2 = (l_2^T, v_2^T, l_2^S, v_2^S)$ cannot be reached by delaying into it, since $v_2^S \not\models Inv(l_2^S)$ implies with Definition 3 of the semantic that $\forall q^{[\![S]\!]_{\text{sem}}} \in Q^{[\![S]\!]_{\text{sem}}}$ we have $q^{[\![S]\!]_{\text{sem}}} \not\xrightarrow{d}{}^{[\![S]\!]_{\text{sem}}} q_2^{[\![S]\!]_{\text{sem}}}$. From Definition 18 we have that in this case $q^Y \xrightarrow{d}{}^Y u$, and $q_2^Y \neq u$. Thus this case is infeasible.
4. $d \in \mathbb{R}_{\geq 0}$, $q_2^Y = (q_2^{[\![T]\!]_{\text{sem}}}, q_2^{[\![S]\!]_{\text{sem}}})$, $q_3^Y = (q_3^{[\![T]\!]_{\text{sem}}}, q_3^{[\![S]\!]_{\text{sem}}})$, $q_2^{[\![T]\!]_{\text{sem}}} \xrightarrow{d}{}^{[\![T]\!]_{\text{sem}}} q_3^{[\![T]\!]_{\text{sem}}}$, and $q_2^{[\![S]\!]_{\text{sem}}} \xrightarrow{d}{}^{[\![S]\!]_{\text{sem}}} q_3^{[\![S]\!]_{\text{sem}}}$. This case is infeasible, since $i? \neq d$.
5. $i! \in Act_o^S$, $q_2^Y = (q^{[\![T]\!]_{\text{sem}}}, q^{[\![S]\!]_{\text{sem}}})$, $q_3^Y = u$, $q^{[\![T]\!]_{\text{sem}}} \in Q^{[\![T]\!]_{\text{sem}}}$, and $q^{[\![S]\!]_{\text{sem}}} \not\xrightarrow{i!}{}^{[\![S]\!]_{\text{sem}}}$. From Definition 3 of semantic it follows that $q^{[\![T]\!]_{\text{sem}}} = (l^T, v^T)$ and $q^{[\![S]\!]_{\text{sem}}} = (l^S, v^S)$. There are two reasons why $q^{[\![S]\!]_{\text{sem}}} \not\xrightarrow{i!}{}^{[\![S]\!]_{\text{sem}}}$: there might be no edge in $E^S$ labeled with action $i!$ from location $l^S$ or none of the edges labeled with $i!$ from $l^S$ are enabled. An edge $(l^S, i!, \varphi, c, l^{S\prime}) \in E^S$ is not enabled if $v^S \not\models \varphi$ or $v^S[r \mapsto 0]_{r \in c} \not\models Inv(l^{S\prime})$ (or both), which can also be written as $v^S \not\models \varphi \wedge Inv(l^{S\prime})[r \mapsto 0]_{r \in c}$. Looking at the third rule in Definition 19 of the quotient for TIOA, we have that $((l^T, l^S), i?, \neg G_S, \emptyset, l_u) \in E^{T \backslash\backslash S}$ and $v^S \not\models G_S$, or $v^S \models \neg G_S$. Because $Clk^T \cap Clk^S = \emptyset$, it holds that $v \models \neg G_S$.

   Now, since $Inv(l_u) = \mathbf{T}$ and no clocks are reset, it holds that $v[r \mapsto 0]_{r \in \emptyset} = v \models Inv(l_u)$. From Definition 3 it now follows that $((l^T, l^S), v) \xrightarrow{i?} (l_u, v_3)$ is a transition in $[\![T \backslash\backslash S]\!]_{\text{sem}}$. From the state label renaming function $f$ from Lemma 20 we have that $q_3^X = f((l_u, v_3)) = u = q_3^Y$ and $q_2^X = q_2^Y$. And from Definition 22 of the reduced $\sim$-quotient of $[\![T \backslash\backslash S]\!]_{\text{sem}}$ we have that $q_2^Y \xrightarrow{i?} q_3^Y$ is a transition in $[\![T \backslash\backslash S]\!]_{\text{sem}}^{\rho} = X$.

6. $d \in \mathbb{R}_{\geq 0}$, $q_2^Y = (q^{[\![T]\!]_{\text{sem}}}, q^{[\![S]\!]_{\text{sem}}})$, $q_3^Y = u$, $q^{[\![T]\!]_{\text{sem}}} \in Q^{[\![T]\!]_{\text{sem}}}$, and $q^{[\![S]\!]_{\text{sem}}} \xrightarrow{d}\!\!\!\!\!\!/\;^{[\![S]\!]_{\text{sem}}}$. This case is infeasible, since $i? \neq d$.
7. $i! \in Act_o^S \cap Act_o^T$, $q_2^Y = (q^{[\![T]\!]_{\text{sem}}}, q^{[\![S]\!]_{\text{sem}}})$, $q_3^Y = e$, $q^{[\![T]\!]_{\text{sem}}} \xrightarrow{a}\!\!\!\!\!\!/\;^{[\![T]\!]_{\text{sem}}}$, and $q^{[\![S]\!]_{\text{sem}}} \xrightarrow{a}{}^{[\![S]\!]_{\text{sem}}}$. Since the target location is the error location, it holds that $q_3 \notin P$. Thus this case is not feasible.
8. $i! \in Act_o^S \cap Act_o^T$, $q_2^Y = (q^{[\![T]\!]_{\text{sem}}}, q^{[\![S]\!]_{\text{sem}}})$, $q_3^Y = (q^{[\![T]\!]_{\text{sem}}}, q^{[\![S]\!]_{\text{sem}}})$, $q^{[\![T]\!]_{\text{sem}}} \xrightarrow{i!}\!\!\!\!\!\!/\;^{[\![T]\!]_{\text{sem}}}$, and $q^{[\![S]\!]_{\text{sem}}} \xrightarrow{i!}\!\!\!\!\!\!/\;^{[\![S]\!]_{\text{sem}}}$. From Definition 3 of semantic it follows that $q^{[\![T]\!]_{\text{sem}}} = (l^T, v^T)$ and $q^{[\![S]\!]_{\text{sem}}} = (l^S, v^S)$. There are two reasons why $q^{[\![T]\!]_{\text{sem}}} \xrightarrow{i!}\!\!\!\!\!\!/\;^{[\![T]\!]_{\text{sem}}}$: there might be no edge in $E^T$ labeled with action $i!$ from location $l^T$ or none of the edges labeled with $i!$ from $l^T$ are enabled. An edge $(l^T, i!, \varphi, c, l^{T\prime}) \in E^T$ is not enabled if $v^T \not\models \varphi$ or $v^T[r \mapsto 0]_{r \in c} \not\models Inv(l^{T\prime})$ (or both), which can also be written as $v^T \not\models \varphi \wedge Inv(l^{T\prime})[r \mapsto 0]_{r \in c}$. We have the exact same reasoning explaining $q^{[\![S]\!]_{\text{sem}}} \xrightarrow{i!}\!\!\!\!\!\!/\;^{[\![S]\!]_{\text{sem}}}$. Looking at the sixth rule in Definition 19 of the quotient for TIOA, we have that $((l^T, l^S), i?, \neg G_T \wedge \neg G_S, \emptyset, (l^T, l^S)) \in E^{T \backslash\backslash S}$, $v^T \models \neg G_T$, $v^S \models \neg G_S$, and $v[r \mapsto 0]_{r \in \emptyset} = v$. Because $Clk^T \cap Clk^S = \emptyset$, it holds that $v \models \neg G_T \wedge \neg G_S$.

   Since $Inv((l^T, l^S)) = \mathbf{T}$ by definition of $T \backslash\backslash S$, we have that $v \models Inv((l^T, l^S))$. From Definition 3 it now follows that $((l^T, l^S), v) \xrightarrow{i?} ((l^T, l^S), v)$ is a transition in $[\![T \backslash\backslash S]\!]_{\text{sem}}$. Using Definition 22 of the reduced $\sim$-quotient of $[\![T \backslash\backslash S]\!]_{\text{sem}}$ and Lemma 20, we can rearrange the states into $((l^T, l^S), v) = ((l^T, v^T), (l^S, v^S)) = q_2^Y = q_3^Y$, and we can show that $q_2^Y \xrightarrow{i?} q_3^Y$ is a transition in $[\![T \backslash\backslash S]\!]_{\text{sem}}^{\rho} = X$. Also, observe now that $q_2^X = q_2^Y$ and $q_3^X = q_3^Y$.
9. $i \in Act^T \cup Act^S \cup \mathbb{R}_{\geq 0}$, $q_2^Y = u$, $q_3^Y = u$. There are two cases how $q_2^Y = u$ could have been reached by a delay.
   * $q^Y = u$. In this case, it follows directly from Definition 19 that $(l_u, i?, \mathbf{T}, \emptyset, l_u) \in E^{T \backslash\backslash S}$. Since any valuation satisfies a true guard and by definition of $T \backslash\backslash S$ that $Inv(l_u) = \mathbf{T}$, we have with Definition 3 of semantic that $(l_u, v) \xrightarrow{i?} (l_u, v)$ is a transition in $[\![T \backslash\backslash S]\!]_{\text{sem}}$. From the state label renaming function $f$ from Lemma 20 we have that $q_2^X = q_2^Y$ and $q_3^X = f((l_u, v)) = u = q_3^Y$. And from Definition 22 of the reduced $\sim$-quotient of $[\![T \backslash\backslash S]\!]_{\text{sem}}$ we have that $q_2^Y \xrightarrow{i?} q_3^Y$ is a transition in $[\![T \backslash\backslash S]\!]_{\text{sem}}^{\rho} = X$.
   * $q^Y = (l^T, v^T, l^S, v^S) \in Q^Y$ with $v^S + d \not\models Inv(l^S)$. In this case, it follows from Definitions 19, 3, and 22 that $q^Y \xrightarrow{d} (l^T, l^S, v + d)$ in $X$. Furthermore, it follows directly from Definition 19 that $((l^T, l^S), i?, \neg Inv(l^S), \emptyset, l_u) \in E^{T \backslash\backslash S}$. Since $v^S + d \not\models Inv(l^S)$, we have $v^S + d \models \neg Inv(l^S)$. By definition of $T \backslash\backslash S$ we have that $Inv(l_u) = \mathbf{T}$, thus $v + d[r \mapsto 0]_{r \in \emptyset} = v + d \models Inv(l_u)$. Now, with Definition 3 of semantic we it follows that $(l_u, v +$

$d) \xrightarrow{i?} (l_u, v+d)$ is a transition in $[\![T\backslash\backslash S]\!]_{\text{sem}}$. From the state label renaming function $f$ from Lemma 20 we have that $q_3^X = f((l_u, v+d)) = u = q_3^Y$. And from Definition 22 of the reduced $\sim$-quotient of $[\![T\backslash\backslash S]\!]_{\text{sem}}$ we have that $q_2^Y \xrightarrow{i?} q_3^Y$ is a transition in $[\![T\backslash\backslash S]\!]^{\rho}_{\text{sem}} = X$.

10. $a \in Act_i^T \cup Act_o^S$, $q_2^Y = e$, $q_3^Y = e$. Since the target location is the error location, it holds that $q_3 \notin P$. Thus this case is not feasible.

Thus, in all feasible cases we can show that $q_2 \xrightarrow{i?}{}^Y q_3$ implies $q_2 \xrightarrow{i?}{}^X q_3$. Since we have chosen an arbitrarily $i? \in Act_i^Y$, it holds for all $i? \in Act_i^Y$.

It remains to be shown that $q_2 \xrightarrow{i_{new}}{}^X q_3$ and $q_3 \in P$, since $i_{new} \notin Act_i^Y$. We only have to consider five cases from Definition 19 that involve $i_{new}$ (rule 4, 7, 8, 10, and 11). Using the same arguments as in these cases when we were considering $\Theta^X(P) \subseteq \Theta^Y(P)$ we can conclude that $q_3 \in P$ in all feasible cases for $i_{new}$. Thus the implication also holds for $q_2$ in $X$.

Thus, in both cases the implication holds. Therefore, we can conclude that $q^Y \xrightarrow{d}{}^X q_2 \Rightarrow q_2 \in P \wedge \forall i? \in Act_i^X : \exists q_3 \in P : q_2 \xrightarrow{i?}{}^X q_3$. As $q_2$ is chosen arbitrarily, it holds for all $q_2 \in Q^X = Q^Y$. Therefore, the left-hand side is true.

- Assume the right-hand side is true, i.e., $\exists d' \leq d \wedge \exists q_2, q_3 \in P \wedge \exists o! \in Act_o^Y : q \xrightarrow{d'}{}^Y q_2 \wedge q_2 \xrightarrow{o!}{}^Y q_3 \wedge \forall i? \in Act_i^Y : \exists q_4 \in P : q_2 \xrightarrow{i?}{}^Y q_4$. First, focus on the delay. From Definition 19 of the quotient for TIOA it follows that $Inv((l^T, l^S)) = \mathbf{T}$. Therefore, with Definition 3 of the semantic and Definition 22 of the $\sim$-reduced quotient of $[\![T\backslash\backslash S]\!]_{\text{sem}}$ it follows that $q^Y \xrightarrow{d}{}^X q_2$.
  Now, consider the output transition labeled with $o!$. Remember that $Act_o^Y = Act_o^X = Act_o^T \setminus Act_o^S \cup Act_i^S \setminus Act_i^T$. We have to consider the ten cases from Definition 18. We can use the exact same argument as before (where now rules 5, 7, and 8 have become infeasible) to show that $q_2 \xrightarrow{o!}{}^X q_3$ is a transition in $X$ for all feasible cases. Since we have chosen an arbitrarily $o! \in Act_o^Y$, it holds for all $o! \in Act_o^Y$. Therefore, we can conclude that $q^Y \xrightarrow{d'}{}^X q_2 \wedge q_2 \xrightarrow{o!}{}^X q_3$ with $q_2, q_3 \in P$.
  Finally, consider the input transitions labeled with $i?$. Using the same argument as before, we can show that $q_2 \xrightarrow{i?} q_4$ in $Y$ is also a transition in $X$, and $q_4 \in P$. Therefore, we can conclude that $q^Y \xrightarrow{d'}{}^X q_2 \wedge q_2 \xrightarrow{o!}{}^X q_3 \wedge \forall i? \in Act_i^X : \exists q_4 \in P : q_2 \xrightarrow{i?}{}^X q_4$ with $q_2, q_3, q_4 \in P$. Thus, the right-hand side is true.

Thus, we have shown that when the left-hand side is true for $q^Y$ in $Y$, it is also true for $q^Y$ in $X$; and that when the right-hand side is true for $q^Y$ in $Y$, it is also true for $q^Y$ in $X$. Thus, $q^Y \in \Theta^X(P)$. Since $q^Y \in P$ was chosen arbitrarily, it holds for all states in $P$. Once we choose $P$ to be the fixed-point of $\Theta^Y$, we have that $\Theta^Y(P) \subseteq \Theta^X(P)$. □

Finally, we are ready to proof Theorem 11.

*Proof of Theorem 11* First, observe that the semantic of a TIOA and adversarial pruning do not alter the action set. Therefore, it follows directly that $([\![T\backslash\backslash S]\!]_{\text{sem}})^{\Delta}$ and $([\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}})^{\Delta}$ have the same action set and partitioning into input and output actions, except that $([\![T\backslash\backslash S]\!]_{\text{sem}})^{\Delta}$ has an additional input event $i_{new}$, i.e., $Act^{[\![T\backslash\backslash S]\!]_{\text{sem}}} \cup \{i_{new}\} = Act^{[\![T]\!]_{\text{sem}}\backslash\backslash[\![S]\!]_{\text{sem}}}$.

Now, it follows from Lemma 22 that it suffice to show that $(\llbracket T\backslash\backslash S\rrbracket^{\rho}_{\text{sem}})^{\Delta} \simeq (\llbracket T\rrbracket_{\text{sem}}\backslash\backslash\llbracket S\rrbracket_{\text{sem}})^{\Delta}$. It follows from Lemma 20 that there is a bijective function $f$ relating states from $\llbracket T\backslash\backslash S\rrbracket^{\rho}_{\text{sem}}$ and $\llbracket T\rrbracket_{\text{sem}}\backslash\backslash\llbracket S\rrbracket_{\text{sem}}$ together. Therefore, we can effectively say that they have the same state set (up to relabeling), i.e., $Q^{\llbracket T\backslash\backslash S\rrbracket^{\rho}_{\text{sem}}} = Q^{\llbracket T\backslash\backslash S\rrbracket_{\text{sem}}}$. For brevity, in the rest of this proof we write we write $X = \llbracket T\backslash\backslash S\rrbracket^{\rho}_{\text{sem}}$, $Y = \llbracket T\rrbracket_{\text{sem}}\backslash\backslash\llbracket S\rrbracket_{\text{sem}}$, $\mathit{Clk} = \mathit{Clk}^T \uplus \mathit{Clk}^S$, and $v^S$ and $v^T$ to indicate the part of a valuation $v$ of only the clocks of $S$ and $T$, respectively. Note that $x_{new} \notin \mathit{Clk}$, but $x_{new} \in \mathit{Clk}^X$.

Let $A = \{q \in Q^{X^{\Delta}} \mid q = ((l^T, l^S), v), v \not\models \mathit{Inv}(l^S)\}$. Let $R \subseteq Q^{X^{\Delta}} \times Q^{Y^{\Delta}}$ such that $R = \{(q, u) \mid q \in A\} \cup \{(q^X, q^Y) \in Q^{X^{\Delta}} \setminus A \times Q^{Y^{\Delta}} \mid q^X = q^Y\}$. We will show that $R$ is a bisimulation relation. First, observe that $(q_0, q_0) \in R$. Consider a state pair $(q_1^X, q_1^Y) \in R$. We have to check whether the six cases from Definition 20 of bisimulation hold.

- $q_1^X \xrightarrow{a}{}^{X^{\Delta}} q_2^X$, $q_2^X \in Q^X$, and $a \in \mathit{Act}^X \cap \mathit{Act}^Y$. Combining Definitions 12, 18 and 19 it follows that $a \in \mathit{Act}^S \cup \mathit{Act}^T$. From Definition 12 of adversarial pruning we have that $q_1^X \xrightarrow{a}{}^X q_2^X$ and $q_1^X, q_2^X \in \text{cons}^X$. Following Definition 3 of the semantic and Definition 22 of the reduced $\sim$-quotient of $\llbracket T\backslash\backslash S\rrbracket_{\text{sem}}$, it follows that there exists an edge $(l_1, a, \varphi, c, l_2) \in E^{T\backslash\backslash S}$ with $q_1^X = (l_1, v_1)$, $q_2^X = (l_2, v_2)$, $l_1, l_2 \in \mathit{Loc}^{T\backslash\backslash S}$, $v_1, v_2 \in [\mathit{Clk} \mapsto \mathbb{R}_{\geq 0}]$, $v_1 \models \varphi$, $v_2 = v_1[r \mapsto 0]_{r\in c}$, and $v_2 \models \mathit{Inv}(l_2)$. Now, consider the eleven cases from Definition 19 of quotient of TIOAs. We have to show for feasible each case that we can simulate a transition in $Y$, that the involved states in $Y$ are consistent, and that the resulting state pair is again in the bisimulation relation $R$.
    1. $a \in \mathit{Act}^S \cap \mathit{Act}^T$, $l_1 = (l_1^T, l_1^S)$, $l_2 = (l_2^T, l_2^S)$, $\varphi = \varphi^T \wedge \mathit{Inv}(l_2^T)[r \mapsto 0]_{r\in c^T} \wedge \varphi^S \wedge \mathit{Inv}(l_1^S) \wedge \mathit{Inv}(l_2^S)[r \mapsto 0]_{r\in c^S}$, $c = c^T \cup c^S$, $(l_1^T, a, \varphi^T, c^T, l_2^T) \in E^T$, and $(l_1^S, a, \varphi^S, c^S, l_2^S) \in E^S$. Since $v_1 \models \varphi$, it holds that $v_1 \models \varphi^T$, $v_1 \models \mathit{Inv}(l_2^T)[r \mapsto 0]_{r\in c^T}$, $v_1 \models \varphi^S$, $v_1 \models \mathit{Inv}(l_1^S)$, and $v_1 \models \mathit{Inv}(l_2^S)[r \mapsto 0]_{r\in c^S}$. Because $\mathit{Clk}^S \cap \mathit{Clk}^T = \emptyset$, it holds that $v_1^T \models \varphi^T$, $v_1^T \models \mathit{Inv}(l_2^T)[r \mapsto 0]_{r\in c^T}$, $v_1^S \models \varphi^S$, $v_1^S \models \mathit{Inv}(l_1^S)$, and $v_1^S \models \mathit{Inv}(l_2^S)[r \mapsto 0]_{r\in c^S}$. Since $v_2 = v_1[r \mapsto 0]_{r\in c}$, it holds that $v_2^T = v_1^T[r \mapsto 0]_{r\in c^T}$ and $v_2^S = v_1^S[r \mapsto 0]_{r\in c^S}$. Therefore, $v_2^T \models \mathit{Inv}(l_2^T)$ and $v_2^S \models \mathit{Inv}(l_2^S)$.
       Combining all information about $T$, we have that $(l_1^T, a, \varphi^T, c^T, l_2^T) \in E^T$, $v_1^T \models \varphi^T$, $v_2^T = v_1^T[r \mapsto 0]_{r\in c^T}$, and $v_2^T \models \mathit{Inv}(l_2^T)$. Therefore, from Definition 3 it follows that $(l_1^T, v_1^T) \xrightarrow{a} (l_2^T, v_2^T)$ in $\llbracket T\rrbracket_{\text{sem}}$. Combining all information about $S$, we have that $(l_1^S, a, \varphi^S, c^S, l_2^S) \in E^S$, $v_1^S \models \varphi^S$, $v_2^S = v_1^S[r \mapsto 0]_{r\in c^S}$, and $v_2^S \models \mathit{Inv}(l_2^S)$. Therefore, from Definition 3 it follows that $(l_1^S, v_1^S) \xrightarrow{a} (l_2^S, v_2^S)$ in $\llbracket S\rrbracket_{\text{sem}}$.
       Now, from Definition 18 it follows that $((l_1^T, v_1^T), (l_1^S, v_1^S)) = (l_1^T, l_1^S, v_1) = q_1^Y \xrightarrow{a}{}^Y ((l_2^T, v_2^T), (l_2^S, v_2^S)) = (l_2^T, l_2^S, v_2) = q_2^Y$ in $Y$. Thus, we can simulate a transition in $Y$. Also, observe now that $q_1^X = q_1^Y$ and $q_2^X = q_2^Y$.
    2. $a \in \mathit{Act}^S \setminus \mathit{Act}^T$, $l_1 = (l^T, l_1^S)$, $l_2 = (l^T, l_2^S)$, $\varphi = \varphi^S \wedge \mathit{Inv}(l_1^S) \wedge \mathit{Inv}(l_2^S)[r \mapsto 0]_{r\in c^S}$, $c = c^S$, $l^T \in \mathit{Loc}^T$, and $(l_1^S, a, \varphi^S, c^S, l_2^S) \in E^S$. Since $v_1 \models \varphi$ and $\mathit{Clk}^S \cap \mathit{Clk}^T = \emptyset$, it holds that $v_1^S \models \varphi^S$, $v_1^S \models \mathit{Inv}(l_1^S)$, and $v_1^S \models \mathit{Inv}(l_2^S)[r \mapsto 0]_{r\in c^S}$. Since $v_2 = v_1[r \mapsto 0]_{r\in c}$ and $c = c^S$, it holds that $v_2^S = v_1^S[r \mapsto 0]_{r\in c^S}$, $v_2^T = v_1^T$, and $v_2^S \models \mathit{Inv}(l_2^S)$. Combining all information above about $S$, it follows from Definition 3 that $(l_1^S, v_1^S) \xrightarrow{a} (l_2^S, v_2^S)$ in

$[\![S]\!]_{\text{sem}}$. From Definition 3 it also follows that $(l^T, v_1^T) \in Q^{[\![T]\!]_{\text{sem}}}$. Therefore, following Definition 18 it follows that $((l^T, v_1^T), (l_1^S, v_1^S)) = (l^T, l_1^S, v_1) = q_1^Y \xrightarrow{a}^Y ((l^T, v_1^T), (l_2^S, v_2^S)) = (l^T, l_2^S, v_2) = q_2^Y$ in $Y$. Thus, we can simulate a transition in $Y$. Also, observe now that $q_1^X = q_1^Y$ and $q_2^X = q_2^Y$.

3. $a \in Act_o^S$, $l_1 = (l^T, l_1^S)$, $l_2 = l_u$, $\varphi = \neg G_S$, $c = \emptyset$, $l^T \in Loc^T$ and $G_S = \bigvee\{\varphi^S \wedge Inv(l_2^S)[r \mapsto 0]_{r \in c^S} \mid (l_1^S, a, \varphi^S, c^S, l_2^S) \in E^S\}$. Since $v_1 \models \varphi$ and $Clk^S \cap Clk^T = \emptyset$, it holds that $v_1^S \models \neg G_S$. Therefore, $v_1^S \not\models G_S$, which indicates that $\forall (l_1^S, a, \varphi^S, c^S, l_2^S) \in E^S$: $v_1^S \not\models \varphi^S \wedge Inv(l_2^S)[r \mapsto 0]_{r \in c^S}$. This means that $v_1^S \not\models \varphi^S$ or $v_1^S \not\models Inv(l_2^S)[r \mapsto 0]_{r \in c^S}$ or both, where the second option is equivalent to $v_1^S[r \mapsto 0]_{r \in c^S} \not\models Inv(l_2^S)$. Following Definition 3, we can conclude that $(l_1^S, v_1^S) \not\xrightarrow{a}$ in $[\![S]\!]_{\text{sem}}$. From Definition 3 it also follows that $(l^T, v_1^T) \in Q^{[\![T]\!]_{\text{sem}}}$. Now, following Definition 18, we have transition $((l^T, v_1^T), (l_1^S, v_1^S)) = (l^T, l_1^S, v_1) = q_1^Y \xrightarrow{a}^Y u = q_2^Y$ in $Y$. Thus we can simulate a transition in $Y$. Also, observe now that $q_1^X = q_1^Y$ and $q_2^X = q_2^Y$ (where $(l_u, v_2)$ is mapped into $u$ by $f$ from Lemma 20).
4. $a \in Act^S \cup Act^T$, $l_1 = (l^T, l^S)$, $l_2 = l_u$, $\varphi = \neg Inv(l^S)$, $c = \emptyset$, $l^T \in Loc^T$, and $l^S \in Loc^S$. Since $v_1 \models \varphi$ and $Clk^S \cap Clk^T = \emptyset$, it holds that $v_1^S \models \neg Inv(l^S)$. Therefore, $v_1^S \not\models Inv(l^S)$. Since $(q_1^X, q_1^Y) \in R$ and $v_1^S \not\models Inv(l^S)$, it follows that $q_1^Y = u$. From Definition 18 it follows that $u = q_1^Y \xrightarrow{a}^Y u = q_2^Y$ in $Y$. Thus we can simulate a transition in $Y$. Also, observe now that $q_2^X = q_2^Y$ (where $(l_u, v_2)$ is mapped into $u$ by $f$ from Lemma 20).
5. $a \in Act_o^S \cap Act_o^T$, $l_1 = (l_1^T, l_1^S)$, $l_2 = l_e$, $\varphi = \varphi^S \wedge Inv(l_2^S)[r \mapsto 0]_{r \in c^S} \wedge \neg G_T$, $c = \{x_{new}\}$, $(l_1^S, a, \varphi^S, c^S, l_2^S) \in E^S$, and $G_T = \bigvee\{\varphi^T \wedge Inv(l_2^T)[r \mapsto 0]_{r \in c^T} \mid (l_1^T, a, \varphi^T, c^T, l_2^T) \in E^T\}$. Since the target location is the error location, it holds that $q_2^X \notin \text{cons}^X$. Thus this case is not feasible.
6. $a \in Act_o^S \cap Act_o^T$, $l_1 = l_2 = (l_1^T, l_1^S)$, $\varphi = \neg G_S \wedge \neg G_T$, $c = \emptyset$, $G_S = \bigvee\{\varphi^S \wedge Inv(l_2^S)[r \mapsto 0]_{r \in c^S} \mid (l_1^S, a, \varphi^S, c^S, l_2^S) \in E^S\}$, and $G_T = \bigvee\{\varphi^T \wedge Inv(l_2^T)[r \mapsto 0]_{r \in c^T} \mid (l_1^T, a, \varphi^T, c^T, l_2^T) \in E^T\}$. Since $v_1 \models \varphi$, it holds that $v_1 \models \neg G_S$ and $v_1 \models \neg G_T$. Because $Clk^S \cap Clk^T = \emptyset$, it holds that $v_1^S \models \neg G_S$ and $v_1^T \models \neg G_T$. This indicates that $v_1^S \not\models G_S$ and $v_1^T \not\models G_T$, which implies that $\forall (l_1^S, a, \varphi^S, c^S, l_2^S) \in E^S$: $v_1^S \not\models \varphi^S \wedge Inv(l_2^S)[r \mapsto 0]_{r \in c^S}$ and $\forall (l_1^T, a, \varphi^T, c^T, l_2^T) \in E^T$: $v_1^T \not\models \varphi^T \wedge Inv(l_2^T)[r \mapsto 0]_{r \in c^T}$. This means that $v_1^S \not\models \varphi^S$ or $v_1^S \not\models Inv(l_2^S)[r \mapsto 0]_{r \in c^S}$ or both for $S$, and $v_1^T \not\models \varphi^T$ or $v_1^T \not\models Inv(l_2^T)[r \mapsto 0]_{r \in c^T}$ or both for $T$, where the second option for both $S$ and $T$ is equivalent to $v_1^S[r \mapsto 0]_{r \in c^S} \not\models Inv(l_2^S)$ and $v_1^T[r \mapsto 0]_{r \in c^T} \not\models Inv(l_2^T)$, respectively. It follows from Definition 3 that $(l_1^S, v_1^S) \not\xrightarrow{a}$ in $[\![S]\!]_{\text{sem}}$ and $(l_1^T, v_1^T) \not\xrightarrow{a}$ in $[\![T]\!]_{\text{sem}}$. Now, following Definition 18, we have transition $((l_1^T, v_1^T), (l_1^S, v_1^S)) = (l_1^T, l_1^S, v_1) = q_1^Y \xrightarrow{a}^Y (l_1^T, l_1^S, v_1) = q_2^Y$ in $Y$. Thus we can simulate a transition in $Y$.
7. $a = i_{new}$, $l_1 = (l^T, l^S)$, $l_2 = l_e$, $\varphi = \neg Inv(l^T) \wedge Inv(l^S)$, $c = \{x_{new}\}$, $l^T \in Loc^T$, and $q^S \in Loc^S$. This case is infeasible, since $i_{new} \notin Act^Y$, thus $i_{new} \notin Act^X \cap Act^Y$.
8. $a = i_{new}$, $l_1 = l_2 = (l_1^T, l_1^S)$, $\varphi = Inv(l^T) \vee \neg Inv(l^S)$ and $c = \emptyset$. This case is infeasible, since $i_{new} \notin Act^Y$, thus $i_{new} \notin Act^X \cap Act^Y$.
9. $a \in Act^T \setminus Act^S$, $l_1 = (l_1^T, l^S)$, $l_2 = (l_2^T, l^S)$, $\varphi = \varphi^T \wedge Inv(l_2^T)[r \mapsto 0]_{r \in c^T} \wedge Inv(l^S)$, $c = c^T$, $l^S \in Loc^S$, and $(l_1^T, a, \varphi^T, c^T, l_2^T) \in E^T$. Since $v_1 \models \varphi$ and $Clk^S \cap Clk^T = \emptyset$, it holds that $v_1^T \models \varphi^T$ and $v_1^T \models Inv(l_2^T)[r \mapsto 0]_{r \in c^T}$.

Since $v_2 = v_1[r \mapsto 0]_{r \in c}$ and $c = c^T$, it holds that $v_2^T = v_1^T[r \mapsto 0]_{r \in c^T}$, $v_2^S = v_1^S$, and $v_2^T \models Inv(l_2^T)$. Combining all information above about $T$, it follows from Definition 3 that $(l_1^T, v_1^T) \xrightarrow{a} (l_2^T, v_2^T)$ in $[\![T]\!]_{\text{sem}}$. From Definition 3 it also follows that $(l^S, v_1^S) \in Q^{[\![S]\!]_{\text{sem}}}$. Therefore, following Definition 18 it follows that $((l_1^T, v_1^T), (l^S, v_1^S)) = (l_1^T, l^S, v_1) = q_1^Y \xrightarrow{a}{}^Y ((l_2^T, v_2^T), (l^S, v_1^S)) = (l_2^T, l^S, v_2) = q_2^Y$ in $Y$. Thus, we can simulate a transition in $Y$. Also, observe now that $q_1^X = q_1^Y$ and $q_2^X = q_2^Y$.

10. $a \in Act^S \cup Act^T$, $l_1 = l_u$, $l_2 = l_u$, $\varphi = \mathbf{T}$, $c = \emptyset$. From the construction of the bisimulation relation $R$, we know that if $q_1^X = f((l_u, v_1)) = u$ for some valuation $v_1$, then $q_1^Y = u$. From Definition 18 it follows directly that there exists a transition $q_1^Y = u \xrightarrow{a}{}^Y u = q_2^Y$ in $Y$. Thus, we can simulate a transition in $Y$. Also, observe now that $q_1^X = q_1^Y$ and $q_2^X = q_2^Y$.
11. $a \in Act_i^S \cup Act_i^T$, $l_1 = l_e$, $l_2 = l_e$, $\varphi = x_{new} = 0$, $c = \emptyset$. Since the source and target locations are the error location, it holds that $q_1^X, q_2^X \notin \text{cons}^X$. Thus this case is not feasible.

In all feasible cases we can show that $q_1^Y = q_1^X$ or $q_1^Y = u$ and $q_2^Y = q_2^X$. Since $q_1^X, q_2^X \in \text{cons}^X$ and $u \in \text{cons}^Y$ by construction of $u$, it follows from Lemma 25 that $q_1^Y, q_2^Y \in \text{cons}^Y$. Therefore, we can conclude that $q_1^Y \xrightarrow{a}{}^{Y^\Delta} q_2^Y$. And from the construction of the bisimulation relation $R$ it follows that $(q_2^X, q_2^Y) \in R$.

- $q_1^X \xrightarrow{a}{}^{X^\Delta} q_2^X$, $q_2^X \in Q^X$, and $a = i_{new}$. From Definition 12 of adversarial pruning we have that $q_1^X \xrightarrow{a}{}^X q_2^X$ and $q_1^X, q_2^X \in \text{cons}^X$. Following Definition 3 of the semantic, it follows that there exists an edge $(l_1, a, \varphi, c, l_2) \in E^{T \backslash\backslash S}$ with $q_1^X = (l_1, v_1)$, $q_2^X = (l_2, v_2)$, $l_1, l_2 \in Loc^{T \backslash\backslash S}$, $v_1, v_2 \in [Clk \mapsto \mathbb{R}_{\geq 0}]$, $v_1 \models \varphi$, $v_2 = v_1[r \mapsto 0]_{r \in c}$, and $v_2 \models Inv(l_2)$. There are three cases from Definition 19 of the quotient for TIOA that apply here.
  - $l_1 = (l^T, l^S)$, $l_2 = l_e$, $\varphi = \neg Inv(l^T) \wedge Inv(l^S)$, $c = \{x_{new}\}$, $l^T \in Loc^T$, and $q^S \in Loc^S$. Since the target location is the error location, it holds that $q_2^X \notin \text{cons}^X$. Thus this case is not feasible.
  - $l_1 = l_2 = (l_1^T, l_1^S)$, $\varphi = Inv(l^T) \vee \neg Inv(l^S)$ and $c = \emptyset$. Since $c = \emptyset$, it follows that $v_2 = v_1$. Therefore, $q_1^X = q_2^X$. Following the second case of Definition 20 and knowing that $(q_1^X, q_1^Y) \in R$, if follows immediately that $(q_2^X, q_1^Y) \in R$. Since $q_1^X \in \text{cons}^X$, it follows from the construction of $R$ and Lemma 25 that $q_1^y = q_1^X$ and thus $q_1^Y \in \text{cons}^Y$.
  - $l_1 = l_2$, $l_2 = l_e$, $\varphi = x_{new}$, and $c = \emptyset$. Since the source and target locations are the error location, it holds that $q_1^X, q_2^X \notin \text{cons}^X$. Thus this case is not feasible.
- $q_1^Y \xrightarrow{a}{}^{Y^\Delta} q_2^Y$, $q_2^Y \in Q^Y$, and $a \in Act^Y \cap Act^X$. Combining Definitions 12, 18 and 19 it follows that $a \in Act^S \cup Act^T$. From Definition 12 of adversarial pruning we have that $q_1^Y \xrightarrow{a}{}^Y q_2^Y$ and $q_1^Y, q_2^Y \in \text{cons}^Y$. Now, consider the ten cases from Definition 18 of the quotient of TIOTS. We have to show for each feasible case that we can simulate a transition in $X$, that the involved states in $X$ are consistent, and that the resulting state pair is again in the bisimulation relation $R$.
  1. $a \in Act^S \cap Act^T$, $q_1^Y = (q_1^{[\![T]\!]_{\text{sem}}}, q_1^{[\![S]\!]_{\text{sem}}})$, $q_2^Y = (q_2^{[\![T]\!]_{\text{sem}}}, q_2^{[\![S]\!]_{\text{sem}}})$, $q_1^{[\![T]\!]_{\text{sem}}} \xrightarrow{a}{}^{[\![T]\!]_{\text{sem}}} q_2^{[\![T]\!]_{\text{sem}}}$, and $q_1^{[\![S]\!]_{\text{sem}}} \xrightarrow{a}{}^{[\![S]\!]_{\text{sem}}} q_2^{[\![S]\!]_{\text{sem}}}$. From Definition 3 of semantic it follows that there exists an edge $(l_1^T, a, \varphi^T, c^T, l_2^T) \in E^T$ with $q_1^{[\![T]\!]_{\text{sem}}} = (l_1^T, v_1^T)$, $q_2^{[\![T]\!]_{\text{sem}}} = (l_2^T, v_2^T)$, $l_1^T, l_2^T \in Loc^T$, $v_1^T, v_2^T \in$

$[Clk^T \mapsto \mathbb{R}_{\geq 0}]$, $v_1^T \models \varphi^T$, $v_2^T = v_1^T[r \mapsto 0]_{r \in c^T}$, and $v_2^T \models Inv^T(l_2^T)$. Similarly, it follows from the same definition that there exists an edge $(l_1^S, a, \varphi^S, c^S, l_2^S) \in E^S$ with $q_1^{[\![S]\!]_{\text{sem}}} = (l_1^S, v_1^S)$, $q_2^{[\![S]\!]_{\text{sem}}} = (l_2^S, v_2^S)$, $l_1^S, l_2^S \in Loc^S$, $v_1^S, v_2^S \in [Clk^S \mapsto \mathbb{R}_{\geq 0}]$, $v_1^S \models \varphi^S$, $v_2^S = v_1^S[r \mapsto 0]_{r \in c^S}$, and $v_2^S \models Inv^S(l_2^S)$. Based on Definition 19 of the quotient for TIOA, we need to consider the following two cases.

- $v_1^S \models Inv(l_1^S)$. In this case, there exists an edge $((l_1^T, l_1^S), a, \varphi^T \wedge Inv(l_2^T)[r \mapsto 0]_{r \in c^T} \wedge \varphi^S \wedge Inv(l_1^S) \wedge Inv(l_2^S)[r \mapsto 0]_{r \in c^S}, c^T \cup c^S, (l_2^T, l_2^S))$ in $T \backslash\backslash S$. Let $v_i, i = 1, 2$ be the valuations that combines the one from $T$ with the one from $S$, i.e. $\forall r \in Clk^T : v_i(r) = v_i^T(r)$ and $\forall r \in Clk^S : v_i(r) = v_i^S(r)$. Because $Clk^T \cap Clk^S = \emptyset$, it holds that $v_1 \models \varphi^T$, $v_1 \models \varphi^S$, and $v_1^S \models Inv(l_1^S)$, thus $v_1 \models \varphi^T \wedge \varphi^S \wedge Inv(l_1^S)$; $v_2 = v_1[r \mapsto 0]_{r \in c^T \cup c^S}$; and $v_2 \models Inv^T(l_2^T)$ and $v_2 \models Inv^S(l_2^S)$, thus $v_2 \models Inv^T(l_2^T) \wedge Inv^S(l_2^S)$.

  From Definition 3 it now follows that $((l_1^T, l_1^S), v_1) \xrightarrow{a} ((l_2^T, l_2^S), v_2)$ is a transition in $[\![T \backslash\backslash S]\!]_{\text{sem}}$. Because $Clk^T \cap Clk^S = \emptyset$, we can rearrange the states into $((l_1^T, l_1^S), v_1) = ((l_1^T, v_1^S), (l_1^T, v_1^S)) = q_1^Y$ and $((l_2^T, l_2^S), v_2) = ((l_2^T, v_2^T), (l_2^S, v_2^S)) = q_2^Y$. Thus, $q_1^Y \xrightarrow{a} q_2^Y$ is a transition in $[\![T \backslash\backslash S]\!]_{\text{sem}} = Y$. Also, observe now that $q_1^X = q_1^Y$ and $q_2^X = q_2^Y$.
- $v_1^S \not\models Inv(l_1^S)$. From the construction of $R$, it follows that $((l_1^T, l_1^S, v_1), u) \in R$, i.e. $q_1^Y = u$. This contradicts with the start of this case that $q_2^Y = (q_2^{[\![T]\!]_{\text{sem}}}, q_2^{[\![S]\!]_{\text{sem}}})$. Thus this case is infeasible.

2. $a \in Act^S \setminus Act^T$, $q_1^Y = (q^{[\![T]\!]_{\text{sem}}}, q_1^{[\![S]\!]_{\text{sem}}})$, $q_2^Y = (q^{[\![T]\!]_{\text{sem}}}, q_2^{[\![S]\!]_{\text{sem}}})$, $q^{[\![T]\!]_{\text{sem}}} \in Q^{[\![T]\!]_{\text{sem}}}$, and $q_1^{[\![S]\!]_{\text{sem}}} \xrightarrow{a}{}^{[\![S]\!]_{\text{sem}}} q_2^{[\![S]\!]_{\text{sem}}}$. From Definition 3 of semantic it follows that there exists an edge $(l_1^S, a, \varphi^S, c^S, l_2^S) \in E^S$ with $q_1^{[\![S]\!]_{\text{sem}}} = (l_1^S, v_1^S)$, $q_2^{[\![S]\!]_{\text{sem}}} = (l_2^S, v_2^S)$, $l_1^S, l_2^S \in Loc^S$, $v_1^S, v_2^S \in [Clk^S \mapsto \mathbb{R}_{\geq 0}]$, $v_1^S \models \varphi^S$, $v_2^S = v_1^S[r \mapsto 0]_{r \in c^S}$, and $v_2^S \models Inv^S(l_2^S)$. From the same definition, it follows that $q^{[\![T]\!]_{\text{sem}}} = (l^T, v^T)$ for some $l^T \in Loc^T$ and $v^T \in [Clk^T \mapsto \mathbb{R}_{\geq 0}]$. Based on Definition 19 of the quotient for TIOA, we need to consider the following two cases.
   - $v_1^S \models Inv(l_1^S)$. In this case, there exists an edge $((l^T, l_1^S), a, \varphi^S \wedge Inv(l_1^S) \wedge Inv(l_2^S)[r \mapsto 0]_{r \in c^S}, c^S, (l^T, l_2^S))$ in $T \backslash\backslash S$. Let $v_i, i = 1, 2$ be the valuations that combines the one from $T$ with the one from $S$, i.e. $\forall r \in Clk^T : v_i(r) = v_i^T(r)$ and $\forall r \in Clk^S : v_i(r) = v_i^S(r)$. Because $Clk^T \cap Clk^S = \emptyset$, it holds that $v_1 \models \varphi^S$, and $v_1 \models Inv(l_1^S)$, thus $v_1 \models \varphi^S \wedge Inv(l_1^S)$; $v_2 = v_1[r \mapsto 0]_{r \in c^S}$; and $v_2 \models Inv^S(l_2^S)$.

     Since $Inv((l^T, l_2^S)) = \mathbf{T}$ by definition $T \backslash\backslash S$, we have that $v_2 \models Inv((l^T, l_2^S))$. From Definition 3 it now follows that $((l^T, l_1^S), v_1) \xrightarrow{a} ((l^T, l_2^S), v_2)$ is a transition in $[\![T \backslash\backslash S]\!]_{\text{sem}}$. Using Definition 22 of the reduced $\sim$-quotient of $[\![T \backslash\backslash S]\!]_{\text{sem}}$ and Lemma 20, we can rearrange the states into $((l^T, l_1^S), v_1) = ((l^T, v_1^T), (l_1^S, v_1^S)) = q_1^Y$ and $((l^T, l_2^S), v_2) = ((l^T, v_2^T), (l_2^S, v_2^S)) = q_2^Y$, and we can show that $q_1^Y \xrightarrow{a} q_2^Y$ is a transition in $[\![T \backslash\backslash S]\!]_{\text{sem}}^{\rho} = X$. Also, observe now that $q_1^X = q_1^Y$ and $q_2^X = q_2^Y$.

 - $v_1^S \not\models Inv(l_1^S)$. From the construction of $R$, it follows that $((l_1^T, l_1^S, v_1), u) \in R$, i.e. $q_1^Y = u$. This contradicts with the start of this case that $q_2^Y = (q_2^{[\![T]\!]_{\text{sem}}}, q_2^{[\![S]\!]_{\text{sem}}})$. Thus this case is infeasible.

3. $a \in Act^T \setminus Act^S$, $q_1^Y = (q_1^{[\![T]\!]_{\text{sem}}}, q^{[\![S]\!]_{\text{sem}}})$, $q_2^Y = (q_2^{[\![T]\!]_{\text{sem}}}, q^{[\![S]\!]_{\text{sem}}})$, $q^{[\![S]\!]_{\text{sem}}} \in Q^{[\![S]\!]_{\text{sem}}}$, and $q_1^{[\![T]\!]_{\text{sem}}} \xrightarrow{a}{}_{[\![T]\!]_{\text{sem}}} q_2^{[\![T]\!]_{\text{sem}}}$. From Definition 3 of semantic it follows that there exists an edge $(l_1^T, a, \varphi^T, c^T, l_2^T) \in E^T$ with $q_1^{[\![T]\!]_{\text{sem}}} = (l_1^T, v_1^T)$, $q_2^{[\![T]\!]_{\text{sem}}} = (l_2^T, v_2^T)$, $l_1^T, l_2^T \in Loc^T$, $v_1^T, v_2^T \in [Clk^T \mapsto \mathbb{R}_{\geq 0}]$, $v_1^T \models \varphi^T$, $v_2^T = v_1^T[r \mapsto 0]_{r \in c^T}$, and $v_2^T \models Inv^T(l_2^T)$. From the same definition, it follows that $q^{[\![S]\!]_{\text{sem}}} = (l^S, v^S)$ for some $l^S \in Loc^S$ and $v^S \in [Clk^S \mapsto \mathbb{R}_{\geq 0}]$. Based on Definition 19 of the quotient for TIOA, we need to consider the following two cases.
 - $v_1^S \models Inv(l_1^S)$. In this case, there exists an edge $((l_1^T, l^S), a, \varphi^T \wedge Inv(l_2^T)[r \mapsto 0]_{r \in c^T} \wedge Inv(l^S), c^T, (l_2^T, l^S))$ in $T \backslash\backslash S$. Let $v_i, i = 1, 2$ be the valuations that combines the one from $T$ with the one from $S$, i.e. $\forall r \in Clk^T : v_i(r) = v_i^T(r)$ and $\forall r \in Clk^S : v_i(r) = v_i^S(r)$. Because $Clk^T \cap Clk^S = \emptyset$, it holds that $v_1 \models \varphi^T$, and $v_1 \models Inv(l^S)$, thus $v_1 \models \varphi^T \wedge Inv(l^S)$; $v_2 = v_1[r \mapsto 0]_{r \in c^T}$; and $v_2 \models Inv^T(l_2^T)$.

   Since $Inv((l_2^T, l^S)) = \mathbf{T}$ by definition $T \backslash\backslash S$, we have that $v_2 \models Inv((l_2^T, l^S))$. From Definition 3 it now follows that $((l_1^T, l^S), v_1) \xrightarrow{a} ((l_2^T, l^S), v_2)$ is a transition in $[\![T \backslash\backslash S]\!]_{\text{sem}}$. Using Definition 22 of the reduced $\sim$-quotient of $[\![T \backslash\backslash S]\!]_{\text{sem}}$ and Lemma 20, we can rearrange the states into $((l_1^T, l^S), v_1) = ((l_1^T, v_1^T), (l^S, v_1^S)) = q_1^Y$ and $((l_2^T, l^S), v_2) = ((l_2^T, v_2^T), (l^S, v_2^S)) = q_2^Y$, and we can show that $q_1^Y \xrightarrow{a} q_2^Y$ is a transition in $[\![T \backslash\backslash S]\!]_{\text{sem}}^{\rho} = X$. Also, observe now that $q_1^X = q_1^Y$ and $q_2^X = q_2^Y$.
 - $v_1^S \not\models Inv(l_1^S)$. From the construction of $R$, it follows that $((l_1^T, l^S, v_1), u) \in R$, i.e. $q_1^Y = u$. This contradicts with the start of this case that $q_2^Y = (q_2^{[\![T]\!]_{\text{sem}}}, q_2^{[\![S]\!]_{\text{sem}}})$. Thus this case is infeasible.

4. $d \in \mathbb{R}_{\geq 0}$, $q_1^Y = (q_1^{[\![T]\!]_{\text{sem}}}, q_1^{[\![S]\!]_{\text{sem}}})$, $q_2^Y = (q_2^{[\![T]\!]_{\text{sem}}}, q_2^{[\![S]\!]_{\text{sem}}})$, $q_1^{[\![T]\!]_{\text{sem}}} \xrightarrow{d}{}_{[\![T]\!]_{\text{sem}}} q_2^{[\![T]\!]_{\text{sem}}}$, and $q_1^{[\![S]\!]_{\text{sem}}} \xrightarrow{d}{}_{[\![S]\!]_{\text{sem}}} q_2^{[\![S]\!]_{\text{sem}}}$. This case is infeasible, since $a \neq d$ (delays will be treated later in the proof).

5. $a \in Act_o^S$, $q_1^Y = (q^{[\![T]\!]_{\text{sem}}}, q^{[\![S]\!]_{\text{sem}}})$, $q_2^Y = u$, $q^{[\![T]\!]_{\text{sem}}} \in Q^{[\![T]\!]_{\text{sem}}}$, and $q^{[\![S]\!]_{\text{sem}}} \not\xrightarrow{a}{}_{[\![S]\!]_{\text{sem}}}$. From Definition 3 of semantic it follows that $q^{[\![T]\!]_{\text{sem}}} = (l^T, v^T)$ and $q^{[\![S]\!]_{\text{sem}}} = (l^S, v^S)$. There are two reasons why $q^{[\![S]\!]_{\text{sem}}} \not\xrightarrow{a}{}_{[\![S]\!]_{\text{sem}}}$: there might be no edge in $E^S$ labeled with action $a$ from location $l^S$ or none of the edges labeled with $a$ from $l^S$ are enabled. An edge $(l^S, a, \varphi, c, l^{S\prime}) \in E^S$ is not enabled if $v^S \not\models \varphi$ or $v^S[r \mapsto 0]_{r \in c} \not\models Inv(l^{S\prime})$ (or both), which can also be written as $v^S \not\models \varphi \wedge Inv(l^{S\prime})[r \mapsto 0]_{r \in c}$. Looking at the third rule in Definition 19 of the quotient for TIOA, we have that $((l^T, l^S), a, \neg G_S, \emptyset, l_u) \in E^{T \backslash\backslash S}$ and $v^S \not\models G_S$, or $v^S \models \neg G_S$. Because $Clk^T \cap Clk^S = \emptyset$, it holds that $v \models \neg G_S$.

   Now, since $Inv(l_u) = \mathbf{T}$ and no clocks are reset, it holds that $v[r \mapsto 0]_{r \in \emptyset} = v \models Inv(l_u)$. From Definition 3 it now follows that $((l^T, l^S), v) \xrightarrow{a} (l_u, v_2)$ is a transition in $[\![T \backslash\backslash S]\!]_{\text{sem}}$. From the state label renaming function $f$ from Lemma 20 we have that $q_2^X = f((l_u, v_2)) = u = q_2^Y$ and $q_1^X = q_1^Y$.

And from Definition 22 of the reduced $\sim$-quotient of $[\![T\backslash\backslash S]\!]_{\text{sem}}$ we have that $q_1^Y \xrightarrow{a} q_2^Y$ is a transition in $[\![T\backslash\backslash S]\!]_{\text{sem}}^{\rho} = X$.

6. $d \in \mathbb{R}_{\geq 0}$, $q_1^Y = (q^{[\![T]\!]_{\text{sem}}}, q^{[\![S]\!]_{\text{sem}}})$, $q_2^Y = u$, $q^{[\![T]\!]_{\text{sem}}} \in Q^{[\![T]\!]_{\text{sem}}}$, and $q^{[\![S]\!]_{\text{sem}}} \not\xrightarrow{d}^{[\![S]\!]_{\text{sem}}}$. This case is infeasible, since $a \neq d$ (delays will be treated later in the proof).
7. $a \in Act_o^S \cap Act_o^T$, $q_1^Y = (q^{[\![T]\!]_{\text{sem}}}, q^{[\![S]\!]_{\text{sem}}})$, $q_2^Y = e$, $q^{[\![T]\!]_{\text{sem}}} \not\xrightarrow{a}^{[\![T]\!]_{\text{sem}}}$, and $q^{[\![S]\!]_{\text{sem}}} \xrightarrow{a}^{[\![S]\!]_{\text{sem}}}$. Since the target state is the error state, it holds that $q_2^Y \notin \text{cons}^Y$. Thus this case is not feasible.
8. $a \in Act_o^S \cap Act_o^T$, $q_1^Y = (q^{[\![T]\!]_{\text{sem}}}, q^{[\![S]\!]_{\text{sem}}})$, $q_2^Y = (q^{[\![T]\!]_{\text{sem}}}, q^{[\![S]\!]_{\text{sem}}})$, $q^{[\![T]\!]_{\text{sem}}} \not\xrightarrow{a}^{[\![T]\!]_{\text{sem}}}$, and $q^{[\![S]\!]_{\text{sem}}} \not\xrightarrow{a}^{[\![S]\!]_{\text{sem}}}$. From Definition 3 of semantic it follows that $q^{[\![T]\!]_{\text{sem}}} = (l^T, v^T)$ and $q^{[\![S]\!]_{\text{sem}}} = (l^S, v^S)$. There are two reasons why $q^{[\![T]\!]_{\text{sem}}} \not\xrightarrow{a}^{[\![T]\!]_{\text{sem}}}$: there might be no edge in $E^T$ labeled with action $a$ from location $l^T$ or none of the edges labeled with $a$ from $l^T$ are enabled. An edge $(l^T, a, \varphi, c, l^{T\prime}) \in E^T$ is not enabled if $v^T \not\models \varphi$ or $v^T[r \mapsto 0]_{r\in c} \not\models Inv(l^{T\prime})$ (or both), which can also be written as $v^T \not\models \varphi \wedge Inv(l^{T\prime})[r \mapsto 0]_{r\in c}$. We have the exact same reasoning explaining $q^{[\![S]\!]_{\text{sem}}} \not\xrightarrow{a}^{[\![S]\!]_{\text{sem}}}$. Looking at the sixth rule in Definition 19 of the quotient for TIOA, we have that $((l^T, l^S), a, \neg G_T \wedge \neg G_S, \emptyset, (l^T, l^S)) \in E^{T\backslash\backslash S}$, $v^T \models \neg G_T$, $v^S \models \neg G_S$, and $v[r \mapsto 0]_{r\in\emptyset} = v$. Because $Clk^T \cap Clk^S = \emptyset$, it holds that $v \models \neg G_T \wedge \neg G_S$.

   Since $Inv((l^T, l^S)) = \mathbf{T}$ by definition of $T\backslash\backslash S$, we have that $v \models Inv((l^T, l^S))$. From Definition 3 it now follows that $((l^T, l^S), v) \xrightarrow{a} ((l^T, l^S), v)$ is a transition in $[\![T\backslash\backslash S]\!]_{\text{sem}}$. Using Definition 22 of the reduced $\sim$-quotient of $[\![T\backslash\backslash S]\!]_{\text{sem}}$ and Lemma 20, we can rearrange the states into $((l^T, l^S), v) = ((l^T, v^T), (l^S, v^S)) = q_1^Y = q_2^Y$, and we can show that $q_1^Y \xrightarrow{a} q_2^Y$ is a transition in $[\![T\backslash\backslash S]\!]_{\text{sem}}^{\rho} = X$. Also, observe now that $q_1^X = q_1^Y$ and $q_2^X = q_2^Y$.
9. $a \in Act^T \cup Act^S \cup \mathbb{R}_{\geq 0}$, $q_1^Y = u$, $q_2^Y = u$. From the construction of $R$ it follows that there are two options for $q_1^X$ for the pair $(q_1^X, u) \in R$.
   - $q_1^X = u$ $(= (l_u, v))$. In this case, it follows directly from Definition 19 that $(l_u, a, \mathbf{T}, \emptyset, l_u) \in E^{T\backslash\backslash S}$. Since any valuation satisfies a true guard and by definition of $T\backslash\backslash S$ that $Inv(l_u) = \mathbf{T}$, we have with Definition 3 of semantic that $(l_u, v) \xrightarrow{a} (l_u, v)$ is a transition in $[\![T\backslash\backslash S]\!]_{\text{sem}}$. From the state label renaming function $f$ from Lemma 20 we have that $q_1^X = q_1^Y$ and $q_2^X = f((l_u, v)) = u = q_2^Y$. And from Definition 22 of the reduced $\sim$-quotient of $[\![T\backslash\backslash S]\!]_{\text{sem}}$ we have that $q_1^Y \xrightarrow{a} q_2^Y$ is a transition in $[\![T\backslash\backslash S]\!]_{\text{sem}}^{\rho} = X$.
   - $q_1^X = ((l^T, l^S), v) \in Q^{X^\Delta}$ with $v \not\models Inv(l^S)$. In this case, it follows directly from Definition 19 that $((l^T, l^S), a, \neg Inv(l^S), \emptyset, l_u) \in E^{T\backslash\backslash S}$. Since $v \not\models Inv(l^S)$, we have $v \models \neg Inv(l^S)$. By definition of $T\backslash\backslash S$ we have that $Inv(l_u) = \mathbf{T}$, thus $v[r \mapsto 0]_{r\in\emptyset} = v \models Inv(l_u)$. Now, with Definition 3 of semantic we it follows that $(l_u, v) \xrightarrow{a} (l_u, v)$ is a transition in $[\![T\backslash\backslash S]\!]_{\text{sem}}$. From the state label renaming function $f$ from Lemma 20 we have that $q_2^X = f((l_u, v)) = u = q_2^Y$. And from Definition 22 of the reduced $\sim$-quotient of $[\![T\backslash\backslash S]\!]_{\text{sem}}$ we have that $q_1^Y \xrightarrow{a} q_2^Y$ is a transition in $[\![T\backslash\backslash S]\!]_{\text{sem}}^{\rho} = X$.

10. $a \in Act_i^T \cup Act_o^S$, $q_1^Y = e$, $q_2^Y = e$. Since the source and target states are the error state, it holds that $q_1^Y, q_2^Y \notin \text{cons}^Y$. Thus this case is not feasible.

In all feasible cases we can show that $q_1^X = q_1^Y$ or $q_1^X = ((l^T, l^S), v)$ with $v \not\models Inv(l^S)$ and $q_2^X = q_2^Y$. Since $q_1^Y, q_2^Y \in \text{cons}^Y$ and $((l^T, l^S), v) \in Q^{X^\Delta}$ by construction of $R$, it follows from Lemma 25 that $q_1^X, q_2^X \in \text{cons}^X$. Therefore, we can conclude that $q_1^X \xrightarrow{a}{}^{X^\Delta} q_2^X$. And from the construction of the bisimulation relation $R$ it follows that $(q_2^X, q_2^Y) \in R$.

- $q_1^Y \xrightarrow{a}{}^{Y^\Delta} q_2^Y$, $q_2^Y \in Q^Y$, and $a \in Act^Y \setminus Act^X$. This case is infeasible, as $Act^X = Act^Y \cup \{i_{new}\}$.
- $q_1^X \xrightarrow{d}{}^{X^\Delta} q_2^X$, $q_2^X \in Q^X$, and $d \in \mathbb{R}_{\geq 0}$. From Definition 12 of adversarial pruning we have that $q_1^X \xrightarrow{d}{}^X q_2^X$ and $q_1^X, q_2^X \in \text{cons}^X$. Following Definition 3 of the semantic and Definition 22 of the reduced $\sim$-quotient of $[\![T \backslash\backslash S]\!]_{\text{sem}}$, it follows that $q_1^X = (l_1, v_1)$ and $q_2^X = (l_1, v_1 + d)$ with $l_1 \in Loc^{T\backslash\backslash S}$, $v_1 \in [Clk \mapsto \mathbb{R}_{\geq 0}]$, $v_1 + d \models Inv(l_1)$, and $\forall d' \in \mathbb{R}_{\geq 0}, d' < d : v_1 + d' \models Inv(l_1)$. Since $q_1^X \in \text{cons}^X$, it follows that $l_1 = (l_1^T, l_1^S)$ or $l_1 = l_u$. Therefore, from Definition 19 of the quotient for TIOA, we have that and $Inv(l_1) = \mathbf{T}$. Note that we do not directly get information about whether the valuation $v_1 + d$ satisfy the location invariant in $T$ or $S$.

  Now consider first the simple case where $l_1 = l_u$. From Definition 18 of the quotient for TIOTS, it follows directly that $u \xrightarrow{d}{}^Y u$. And note with Lemma 20 that $q_2^X = f((l_u, v_1 + d)) = u = q_2^Y$ and thus $(q_2^X, q_2^Y) \in R$.

  Now consider the case where $l_1 = (l_1^T, l_1^S)$. We have to consider whether delays are possible in $[\![T]\!]_{\text{sem}}$ and $[\![S]\!]_{\text{sem}}$ in order to show that $Y$ can follow the delay and that the resulting state pair is in the bisimulation relation $R$.

  - $q_1^{[\![T]\!]_{\text{sem}}} \xrightarrow{d}{}^{[\![T]\!]_{\text{sem}}} q_2^{[\![T]\!]_{\text{sem}}}$ and $q_1^{[\![S]\!]_{\text{sem}}} \xrightarrow{d}{}^{[\![S]\!]_{\text{sem}}} q_2^{[\![S]\!]_{\text{sem}}}$. In this case, it follows from Definition 3 of the semantic that $q_1^{[\![T]\!]_{\text{sem}}} = (l_1^T, v_1^T)$, $\forall c \in Clk^T : v_1^T(c) = v_1(c)$, $q_2^{[\![T]\!]_{\text{sem}}} = (l_1^T, v_1^T + d)$, $v_1^T + d \models Inv(l_1^T)$, and $\forall d' \in \mathbb{R}_{\geq 0}, d' < d : v_1^T + d' \models Inv(l_1^T)$; similarly we have that $q_1^{[\![S]\!]_{\text{sem}}} = (l_1^S, v_1^S)$, $\forall c \in Clk^S : v_1^S(c) = v_1(c)$, $q_2^{[\![S]\!]_{\text{sem}}} = (l_1^S, v_1^S + d)$, $v_1^S + d \models Inv(l_1^S)$, and $\forall d' \in \mathbb{R}_{\geq 0}, d' < d : v_1^S + d' \models Inv(l_1^S)$. From Definition 18 of the quotient for TIOTS it follows that $(q_1^T, q_1^S) \xrightarrow{d}{}^Y (q_2^T, q_2^S)$. Observe with Lemma 20 that $q_1^Y = (q_1^{[\![T]\!]_{\text{sem}}}, q_1^{[\![S]\!]_{\text{sem}}}) = (l_1^T, l_1^S, v_1) = q_1^X$ and $q_2^Y = (q_2^{[\![T]\!]_{\text{sem}}}, q_2^{[\![S]\!]_{\text{sem}}}) = (l_1^T, l_1^S, v_2) = q_2^X$. Thus $(q_2^X, q_2^Y) \in R$.
  - $q_1^{[\![T]\!]_{\text{sem}}} \xrightarrow{d}{}^{[\![T]\!]_{\text{sem}}} q_2^{[\![T]\!]_{\text{sem}}}$ and $q_1^{[\![S]\!]_{\text{sem}}} \not\xrightarrow{d}{}^{[\![S]\!]_{\text{sem}}}$. In this case, it follows from Definition 3 of the semantic that $q_1^{[\![T]\!]_{\text{sem}}} = (l_1^T, v_1^T)$, $\forall c \in Clk^T : v_1^T(c) = v_1(c)$, $q_2^{[\![T]\!]_{\text{sem}}} = (l_1^T, v_1^T + d)$, $v_1^T + d \models Inv(l_1^T)$, and $\forall d' \in \mathbb{R}_{\geq 0}, d' < d : v_1^T + d' \models Inv(l_1^T)$; similarly we have that $q_1^{[\![S]\!]_{\text{sem}}} = (l_1^S, v_1^S)$, $\forall c \in Clk^S : v_1^S(c) = v_1(c)$, and $\exists d' \in \mathbb{R}_{\geq 0}, d' \leq d : v_1^S + d' \not\models Inv(l_1^S)$. We have to consider two cases.
    * $v_1^S \models Inv(l_1^S)$. Since $Clk^T \cap Clk^S = \emptyset$, $v_1 \models Inv(l_1^S)$. Since $(q_1^X, q_1^Y) \in R$ and $v_1^S \models Inv(l_1^S)$, we have that $q_1^Y = q_1^X$. From Definition 18 of the quotient for TIOTS, it follows that $q_1^Y = ((l_1^T, v_1^T), (l_1^S, v_1^S)) \xrightarrow{d}$

${}^{Y} u = q_2^Y$. From the construction of $R$ we have that $q_2^X \in A$, thus we can confirm that $(q_2^T, q_2^Y) \in R$.

* $v_1^S \not\models \mathit{Inv}(l_1^S)$. Again, since $\mathit{Clk}^T \cap \mathit{Clk}^S = \emptyset$, $v_1 \not\models \mathit{Inv}(l_1^S)$. Since $(q_1^X, q_1^Y) \in R$ and $v_1^S \not\models \mathit{Inv}(l_1^S)$, we have that $q_1^X \in A$, thus $q_1^Y = u$. From Definition 18 of the quotient for TIOTS, it follows that $u \xrightarrow{d}{}^{Y} u$. And by construction of $R$ it follows that $(q_2^X, q_2^Y) \in R$.

- $q_1^{[\![T]\!]_{\text{sem}}} \stackrel{d}{\not\longrightarrow}{}^{[\![T]\!]_{\text{sem}}} q_2^{[\![T]\!]_{\text{sem}}}$ and $q_1^{[\![S]\!]_{\text{sem}}} \stackrel{d}{\not\longrightarrow}{}^{[\![S]\!]_{\text{sem}}}$. This case follows the exact same reasoning as the one above, since Definition 18 of the quotient for TIOTS does not care whether a delay $d$ is possible in $[\![T]\!]_{\text{sem}}$ once it is not possible in $[\![S]\!]_{\text{sem}}$.
- $q_1^{[\![T]\!]_{\text{sem}}} \stackrel{d}{\not\longrightarrow}{}^{[\![T]\!]_{\text{sem}}} q_2^{[\![T]\!]_{\text{sem}}}$ and $q_1^{[\![S]\!]_{\text{sem}}} \xrightarrow{d}{}^{[\![S]\!]_{\text{sem}}} q_2^{[\![S]\!]_{\text{sem}}}$. In this case, it follows directly from Definition 18 of the quotient for TIOTS that there is no delay possible in $Y$, i.e., $(q_1^{[\![T]\!]_{\text{sem}}}, q_1^{[\![S]\!]_{\text{sem}}}) \stackrel{d}{\not\longrightarrow}{}^{[\![T]\!]_{\text{sem}} \backslash\backslash [\![S]\!]_{\text{sem}}}$. It follows from Definition 3 of the semantic that $q_1^{[\![T]\!]_{\text{sem}}} = (l_1^T, v_1^T)$, $\forall c \in \mathit{Clk}^T : v_1^T(c) = v_1(c)$, and $\exists d' \in \mathbb{R}_{\geq 0}, d' \leq d : v_1^T + d' \not\models \mathit{Inv}(l_1^T)$; similarly we have that $q_1^{[\![S]\!]_{\text{sem}}} = (l_1^S, v_1^S)$, $\forall c \in \mathit{Clk}^S : v_1^S(c) = v_1(c)$, $q_2^{[\![S]\!]_{\text{sem}}} = (l_1^S, v_1^S + d)$, $v_1^S + d \models \mathit{Inv}(l_1^S)$, and $\forall d' \in \mathbb{R}_{\geq 0}, d' < d : v_1^S + d' \models \mathit{Inv}(l_1^S)$. Without loss of generality, we can assume that $v_1^T + 0 \not\models \mathit{Inv}(l_1^T)$[16], which simplifies to $v_1^T \not\models \mathit{Inv}(l_1^T)$. Combining this information, we have that $v_1 \models \neg \mathit{Inv}(l_1^T) \wedge \mathit{Inv}(l_1^S)$, where we used the fact that $\mathit{Clk}^T \cap \mathit{Clk}^S = \emptyset$. Now, using Definition 19 of the quotient for TIOA and Definition 3 of the semantics, we have that $(l_1^T, l_1^S, v_1) \xrightarrow{i_{new}}{}^{[\![T \backslash\backslash S]\!]_{\text{sem}}} (l_e, v_1)$. Since $(l_e, v_1) \notin \text{cons}^X$ and $i_{new}$ is an input, it follows that $(l_1^T, l_1^S, v_1) = q_1^X \notin \text{cons}^X$. This contradicts with our assumption that $q_1^X \in \text{cons}^X$. Therefore, this case is infeasible.

In all feasible cases we can show that $(q_2^X, q_2^Y) \in R$. Since $q_1^X, q_2^X \in \text{cons}^X$ and $A \subseteq Q^{X^\Delta}$ by construction of $R$, it follows from Lemma 25 that $q_1^Y, q_2^Y \in \text{cons}^Y$. Therefore, we can conclude that $q_1^Y \xrightarrow{d}{}^{Y^\Delta} q_2^Y$.

- $q_1^Y \xrightarrow{d}{}^{Y^\Delta} q_2^Y$, $q_2^Y \in Q^Y$, and $d \in \mathbb{R}_{\geq 0}$. From Definition 12 of adversarial pruning we have that $q_1^Y \xrightarrow{d}{}^{Y} q_2^Y$ and $q_1^Y, q_2^Y \in \text{cons}^Y$. Consider the following three cases from Definition 18 of the quotient for TIOTS.
  - $q_1^Y = (q_1^{[\![T]\!]_{\text{sem}}}, q_1^{[\![S]\!]_{\text{sem}}})$, $q_2^Y = (q_2^{[\![T]\!]_{\text{sem}}}, q_2^{[\![S]\!]_{\text{sem}}})$, $q_1^{[\![T]\!]_{\text{sem}}} \xrightarrow{d}{}^{[\![T]\!]_{\text{sem}}} q_2^{[\![T]\!]_{\text{sem}}}$, and $q_1^{[\![S]\!]_{\text{sem}}} \xrightarrow{d}{}^{[\![S]\!]_{\text{sem}}} q_2^{[\![S]\!]_{\text{sem}}}$. From Definition 3 of the semantic it follows that $q_1^{[\![T]\!]_{\text{sem}}} = (l_1^T, v_1^T)$, $q_2^{[\![T]\!]_{\text{sem}}} = (l_1^T, v_1^T + d)$, $v_1^T + d \models \mathit{Inv}(l_1^T)$, $\forall d' \in \mathbb{R}_{\geq 0}, d' < d : v_1^T + d' \models \mathit{Inv}(l_1^T)$, $q_1^{[\![S]\!]_{\text{sem}}} = (l_1^S, v_1^S)$, $q_2^{[\![S]\!]_{\text{sem}}} = (l_1^S, v_1^S + d)$, $v_1^S + d \models \mathit{Inv}(l_1^S)$, and $\forall d' \in \mathbb{R}_{\geq 0}, d' < d : v_1^S + d' \models \mathit{Inv}(l_1^S)$. Now, from Definition 19 of the quotient for TIOA we have that $\mathit{Inv}((l_1^S, l_1^T)) = \mathbf{T}$ in $T \backslash\backslash S$, thus using Definitions 3 and 22 we have $q_1^X = (l_1^S, l_1^T, v_1) \xrightarrow{d}{}^{X} (l_1^S, l_1^T, v_1 + d) = q_2^X$. Observe that $q_1^X = q_1^Y$ and $q_2^X = q_2^Y$, thus $q_2^X, q_2^Y \in R$.
  - $q_1^Y = (q_1^{[\![T]\!]_{\text{sem}}}, q_1^{[\![S]\!]_{\text{sem}}})$, $q_2^Y = u$, and $q_1^{[\![S]\!]_{\text{sem}}} \stackrel{d}{\not\longrightarrow}{}^{[\![S]\!]_{\text{sem}}} q_2^{[\![S]\!]_{\text{sem}}}$. From Definition 3 of the semantic it follows that $q_1^{[\![T]\!]_{\text{sem}}} = (l_1^T, v_1^T)$, $q_1^{[\![S]\!]_{\text{sem}}} =$

[16] In case there would be a $d' < d$ such that $v_1^T + d' \models \mathit{Inv}(l_1^T)$, we can use the first case to simulate the delay $d'$ in$Y$.

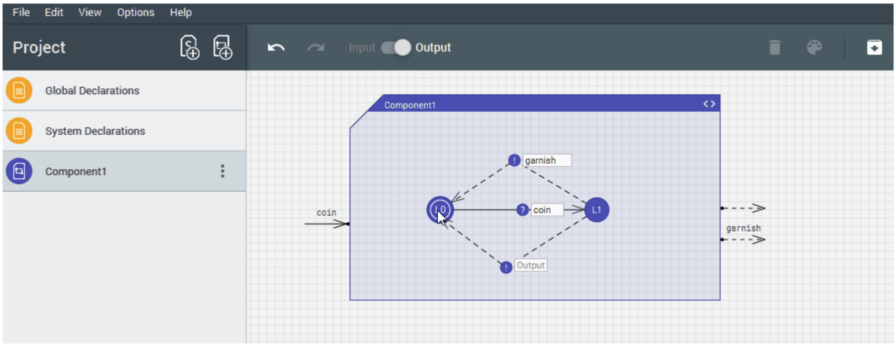



**Fig. 11**: Screenshot of the GUI of Ecdar 2.4

$(l_1^S, v_1^S)$, and $\exists d' \in \mathbb{R}_{\geq 0}, d' \leq d : v_1^S + d' \not\models \mathit{Inv}(l_1^S)$. Now, from Definition 19 of the quotient for TIOA we have that $\mathit{Inv}((l_1^S, l_1^T)) = \mathbf{T}$ in $T \backslash\backslash S$, thus using Definitions 3 and 22 we have $q_1^X = (l_1^S, l_1^T, v_1) \xrightarrow{d}{}^X (l_1^S, l_1^T, v_1 + d) = q_2^X$. We have to consider two cases to show that $(q_2^X, q_2^Y) \in R$.

 * $v_1^S \models \mathit{Inv}(l_1^S)$. In this case $q_1^X \notin A$ and $q_2^X \in A$. Therefore, $(q_2^X, q_2^Y) \in R$.
 * $v_1^S \not\models \mathit{Inv}(l_1^S)$. In this case $q_1^X, q_2^X \in A$. From the construction of $R$ it follows that any state from $A$ can only be related to state $u$ in $Y$, but $q_1^Y = (q_1^{[\![T]\!]_{\text{sem}}}, q_1^{[\![S]\!]_{\text{sem}}})$. This contradiction renders this case infeasible.

– $q_1^Y = u$ and $q_2^Y = u$. From Definition 19 of the quotient for TIOA, it follows directly that $(l_u, v) \xrightarrow{d}{}^X (l_u, v)$ for any $v \in [\mathit{Clk} \mapsto \mathbb{R}_{\geq 0}]$. And note with Lemma 20 that $q_1^X = q_2^X = f((l_u, v)) = u = q_1^Y = q_2^Y$ and thus $(q_2^X, q_2^Y) \in R$.

In all feasible cases we can show that $(q_2^X, q_2^Y) \in R$. Since $q_1^Y, q_2^Y \in \text{cons}^Y$ and $A \subseteq Q^{X^\Delta}$ by construction of $R$, it follows from Lemma 25 that $q_1^X, q_2^X \in \text{cons}^X$. Therefore, we can conclude that $q_1^X \xrightarrow{d}{}^{X^\Delta} q_2^X$.

We have show for state pair $(q_1^X, q_1^Y) \in R$ that all the six cases of bisimulation hold. Since we have chosen an arbitrary state pair from $R$, it holds for all state pairs in $R$. This concludes the proof. □

# 6 Tool implementation

In parallel with writing this paper and proving all the theorems in it we are also implementing the theory in an updated tool. This process also helps with an extra layer of sanity check for the theory.

The tool consists of two major parts: the GUI and the verification engine jEcdar. Figure 11 shows a screenshot of the GUI for Ecdar version 2.4. The verification engine developed along with the GUI is written in Java and is called jEcdar and can be used both from the GUI and through a command line interface. The tool can be found at http://ecdar.net.

## 7 Conclusion

We have proposed a complete game-based specification theory for timed systems, in which we distinguish between a component and the environment in which it is used. To the best of our knowledge, our contribution is the first game-based approach to support both refinement, consistency checking, logical and structural composition, and quotient. Our results have been implemented in the ECDAR toolset.

One could also investigate whether our approach can be used to perform scheduling of timed systems (see [1, 26, 27] for examples). For example, the quotient operation could perhaps be used to synthesize a scheduler for such problem.

## References

[1] Henzinger, T.A., Sifakis, J.: The embedded systems design challenge. In: International Symposium on Formal Methods. Lecture Notes in Computer Science, vol. 4085, pp. 1–15. Springer, Berlin, Heidelberg (2006). https://doi.org/10.1007/11813040_1

[2] de Alfaro, L., Henzinger, T.A.: Interface-based design. In: Engineering Theories of Software Intensive Systems. NATO Science Series, vol. 195, pp. 83–104. Springer, Dordrecht (2005). https://doi.org/10.1007/1-4020-3532-2_3

[3] Chakabarti, A., de Alfaro, L., Henzinger, T.A., Stoelinga, M.I.A.: Resource interfaces. In: Proceedings of the International Workshop on Embedded Software. Lecture Notes in Computer Science, vol. 2855, pp. 117–133. Springer, Berlin, Heidelberg (2003). https://doi.org/10.1007/978-3-540-45212-6_9

[4] de Alfaro, L., Henzinger, T.A.: Interface automata. In: Proceedings of the Annual Symposium on Foundations of Software Engineering, pp. 109–120. ACM Press, New York, NY (2001). https://doi.org/10.1145/503209.503226

[5] Larsen, K.G.: Modal specifications. In: Automatic Verification Methods for Finite State Systems. Lecture Notes in Computer Science, vol. 407, pp. 232–246. Springer, Berlin, Heidelberg (1989). https://doi.org/10.1007/3-540-52148-8_19

[6] Milner, R.: Communication and Concurrency. Prentice Hall, USA (1989)

[7] Lynch, N.A., Tuttle, M.R.: An introduction to input/output automata. Technical Report MIT/LCS/TM-373, The MIT Press (1988)

[8] de Alfaro, L., Henzinger, T.A., Stoelinga, M.I.A.: Timed interfaces. In:

Proceedings of the International Workshop on Embedded Software. Lecture Notes in Computer Science, vol. 2491, pp. 108–122. Springer, Berlin, Heidelberg (2002). https://doi.org/10.1007/3-540-45828-X_9

[9] Kaynar, D.K., Lynch, N.A., Segala, R., Vaandrager, F.W.: Timed i/o automata: A mathematical framework for modeling and analyzing real-time systems. In: Proceedings of the IEEE Real-Time Systems Symposium, pp. 166–177 (2003). https://doi.org/10.1109/REAL.2003.1253264

[10] Bulychev, P., Chatain, T., David, A., Larsen, K.G.: Efficient on-the-fly algorithm for checking alternating timed simulation. In: Proceedings of the International Conference on Formal Modeling and Analysis of Timed Systems. Lecture Notes in Computer Science, vol. 5813, pp. 73–87. Springer, Berlin, Heidelberg (2009). https://doi.org/10.1007/978-3-642-04368-0_8

[11] Maler, O., Pnueli, A., Sifakis, J.: On the synthesis of discrete controllers for timed systems (an extended abstract). In: Proceedings of the Annual Symposium on Theoretical Aspects of Computer Science. Lecture Notes in Computer Science, vol. 900, pp. 229–242. Springer, Berlin, Heidelberg (1995). https://doi.org/10.1007/3-540-59042-0_76

[12] Cassez, F., David, A., Fleury, E., Larsen, K.G., Lime, D.: Efficient on-the-fly algorithms for the analysis of timed games. In: Proceedings of the International Conference on Concurrency Theory. Lecture Notes in Computer Science, vol. 3653, pp. 66–80. Springer, Berlin, Heidelberg (2005). https://doi.org/10.1007/11539452_9

[13] David, A., Larsen, K.G., Legay, A., Nyman, U., Wasowski, A.: Timed i/o automata: a complete specification theory for real-time systems. In: Proceedings of the 13th ACM International Conference on Hybrid Systems: Computation and Control. HSCC '10, pp. 91–100. Association for Computing Machinery. https://doi.org/10.1145/1755952.1755967

[14] David, A., Larsen, K.G., Legay, A., Nyman, U., Wąsowski, A.: Methodologies for specification of real-time systems using timed i/o automata. In: de Boer, F.S., Bonsangue, M.M., Hallerstede, S., Leuschel, M. (eds.) Formal Methods for Components and Objects. Lecture Notes in Computer Science, pp. 290–310. Springer. https://doi.org/10.1007/978-3-642-17071-3_15

[15] Henzinger, T.A., Manna, Z., Pnueli, A.: Timed transition systems. In: REX Workshop. Lecture Notes in Computer Science, vol. 600, pp. 226–251. Springer, Berlin, Heidelberg (1991). https://doi.org/10.1007/BFb0031995

[16] Lynch, N.: I/O automata: A model for discrete event systems. In: Annual

Conference on Information Sciences and Systems, Princeton University, Princeton, N.J., pp. 29–38 (1988)

[17] Garland, S.J., Lynch, N.A.: The IOA language and toolset: Support for designing, analyzing, and building distributed systems. Technical report, Massachusetts Institute of Technology, Cambridge, MA (1998)

[18] Stark, E.W., Cleavland, R., Smolka, S.A.: A process-algebraic language for probabilistic I/O automata. In: Proceedings of the International Conference on Concurrency Theory. Lecture Notes in Computer Science, vol. 2761, pp. 193–207. Springer, Berlin, Heidelberg (2003). https://doi.org/10.1007/978-3-540-45187-7_13

[19] Vaandrager, F.W.: On the relationship between process algebra and input/output automata. In: Proceedings Annual IEEE Symposium on Logic in Computer Science, pp. 387–398 (1991). https://doi.org/10.1109/LICS.1991.151662

[20] Nicola, R.D., Segala, R.: A process algebraic view of input/output automata. Theoretical Computer Science **138**(2), 391–423 (1995). https://doi.org/10.1016/0304-3975(95)92307-J

[21] de Alfaro, L., Faella, M., Henzinger, T.A., Majumdar, R., Stoelinga, M.: The element of surprise in timed games. In: Amadio, R., Lugiez, D. (eds.) CONCUR 2003 - Concurrency Theory. Lecture Notes in Computer Science, pp. 144–158. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-45187-7_9

[22] Alur, R., Henzinger, T.A., Kupferman, O., Vardi, M.: Alternating refinement relations. In: Proceedings of the International Conference on Concurrency Theory. Lecture Notes in Computer Science, vol. 1466, pp. 163–178. Springer, Berlin, Heidelberg (1998). https://doi.org/10.1007/BFb0055622

[23] Caillaud, B., Delahaye, B., Larsen, K.G., Legay, A., Peddersen, M., Wasowski, A.: Compositional design methodology with constraint markov chains. Technical report, Hal-INRIA (2009)

[24] de Alfaro, L., Henzinger, T.A., Majumdar, R.: Symbolic algorithms for infinite-state games. In: Proceedings of the International Conference on Concurrency Theory. Lecture Notes in Computer Science, vol. 2154, pp. 536–550. Springer, Berlin, Heidelberg (2001). https://doi.org/10.1007/3-540-44685-0_36

[25] Tarski, A.: A lattice-theoretical fixpoint theorem and its applications. Pacific Journal of Mathematics **5**, 285–309 (1955)

[26] de Alfaro, L., Faella, M.: An accelerated algorithm for 3-color parity games with an application to timed games. In: Proceedings of the International Conference on Computer Aided Verification. Lecture Notes in Computer Science, vol. 4590, pp. 108–120. Springer, ??? (2007). https://doi.org/10.1007/978-3-540-73368-3_13

[27] Deng, Z., Liu, J.W.-s.: Scheduling real-time applications in an open environment. In: Proceedings of the IEEE Real-Time Systems Symposium, pp. 308–319 (1997). https://doi.org/10.1109/REAL.1997.641292