Compositional Liveness-Preserving Conformance Testing of Timed I/O Automata - Technical Report

Lars Luthmann*
Real-Time Systems Lab
TU Darmstadt, Germany
lars.luthmann@es.tu-darmstadt.de

Hendrik Göttmann
Real-Time Systems Lab
TU Darmstadt, Germany
h.goettmann@stud.tu-darmstadt.de

Malte Lochau*
Real-Time Systems Lab
TU Darmstadt, Germany
malte.lochau@es.tu-darmstadt.de

I/O conformance testing theories (e.g., $ioco$) are concerned with formally defining when observable output behaviors of an implementation conform to those permitted by a specification. Thereupon, several real-time extensions of $ioco$, usually called $tioco$, have been proposed, further taking into account permitted delays between actions. In this paper, we propose an improved version of $tioco$, called live timed $ioco$ ($ltioco$), tackling various weaknesses of existing definitions. Here, a reasonable adaptation of quiescence (i.e., observable absence of any outputs) to real-time behaviors has to be done with care: $ltioco$ therefore distinguishes safe outputs being allowed to happen, from live outputs being enforced to happen within a certain time period thus inducing two different facets of quiescence. Furthermore, $tioco$ is frequently defined on Timed I/O Labeled Transition Systems (TIOLTS), a semantic model of Timed I/O Automata (TIOA) which is infinitely branching and thus infeasible for practical testing tools. Instead, we extend the theory of zone graphs to enable $ltioco$ testing on a finite semantic model of TIOA. Finally, we investigate compositionality of $ltioco$ with respect to parallel composition including a proper treatment of silent transitions.

1 Introduction

Model-based testing constitutes a practically emerging, yet theoretically founded technique for automated quality assurance of software systems [16]. In particular, input/output conformance testing theories formalize notions of observable conformance between an implementation under test and a specification, where the $ioco$ theory [41] constitutes one of the most prominent examples. The $ioco$ relation requires both the input/output-behaviors of the specification and the implementation to be represented as input/output labeled transition systems (IOLTS), where the IOLTS of the implementation is unknown (black-box assumption) [11]. For an implementation to satisfy $ioco$, all its possible output behaviors must be permitted by the specification. To rule out trivial implementations never showing any output, $ioco$ employs the notion of quiescence to explicitly permit starvation. In order to ensure proper test-execution semantics, $ioco$ requires input-enabled implementations, never blocking any (test-)inputs. Hence, $ioco$ is concerned with the correct ordering of (or causality among) input/output (re-)actions, whereas quantified time delays between action occurrences are not considered. However, reasoning about real-time behaviors becomes more and more crucial and various real-time extensions of $ioco$, so-called $tioco$, have been recently proposed [38, 14, 24, 26, 27]. Based on timed extensions of IOLTS (so-called TIOLTS), a system run progresses by either actively performing discrete, instantaneous actions or by inactively letting

---

*This work was funded by the Hessian LOEWE initiative within the Software-Factory 4.0 project.

© L. Luthmann, H. Göttmann, and M. Lochau
This work is licensed under the Creative Commons Attribution License.
a quantified amount of time pass. Nevertheless, existing definitions of \textit{tioco} suffer from several weaknesses which we tackle in this paper by proposing an improved version called \textit{live timed ioco (ltioco)}. Our contributions can be summarized as follows.

- Recent adoptions of quiescence in a timed setting also show several weaknesses: most recent versions of \textit{tioco} either do not incorporate any notion of quiescence at all \cite{38,24,26,28}, or define quiescence in terms of (either infinite or bounded) time intervals without observable output actions \cite{14,38}. Both fail to distinguish the \textit{enabling} of output actions (i.e., an output is allowed to occur in a time interval to constitute \textit{safe} behavior) from \textit{enforced} output actions (i.e., an output must occur in a certain time interval to meet \textit{liveness} requirements). To this end, \textit{ltioco} distinguishes safe outputs from live outputs thus explicitly incorporating the two different facets of timed quiescence. We prove correctness of \textit{ltioco} with respect to TIOLTS semantics and we show that \textit{ltioco} is strictly more discriminating than most recent versions of \textit{tioco}.

- We investigate compositionality properties of \textit{ltioco} with respect to (synchronous) parallel composition.

- Finally, all recent versions of \textit{tioco} are defined on TIOLTS, constituting a semantic model of Timed I/O Automata (TIOA) which is infinitely branching and thus infeasible for practical testing tools. Instead, we extend the notion of \textit{zone} graphs to effectively check \textit{ltioco} on a finite semantic model of TIOA using so-called \textit{span traces}. Thereupon, we developed a tool for online testing using \textit{tioco} (see \url{https://www.es.tu-darmstadt.de/ltioco}).

The remainder of this paper is structured as follows. We first give an formal introduction into TIOA and parallel composition of TIOA in Sect. 2. Then, we discuss existing notions of \textit{tioco} and point out their weaknesses in Sect. 3 which we address in the subsequent Sect. 4. Furthermore, we give an intuition on how to apply \textit{zone} graphs for an efficient implementation of our approach in Sect. 5 and we summarize related work in Sect. 6.

2 Timed Input/Output Automata

We first recall foundations of \textit{Timed Automata (TA)} \cite{2,3}, extension of TA by input/output labels \cite{34,35,17} and their composition involving silent transitions \cite{10}.

TA are labeled finite state-transition graphs with states being called \textit{locations} and transitions being called \textit{switches}. A TA is further defined with respect to a finite set \( \mathcal{C} \) of \textit{clocks} over a numerical \textit{clock domain} \( \mathbb{T} \) (e.g., \( \mathbb{T} = \mathbb{N}_0 \) for \textit{discrete time} and \( \mathbb{T} = \mathbb{R}_+ \), with \( \mathbb{R}_+ := \{ r \mid r \in \mathbb{R} \wedge r \geq 0 \} \) for \textit{dense time}). Clocks constitute constantly and synchronously increasing, yet independently resettable variables over \( \mathbb{T} \) for measuring and restricting time intervals (durations/delays) between action occurrences. Note that we consider \( \mathbb{T} = \mathbb{N}_0 \) in all examples for the sake of readability. In particular, we consider \textit{Timed Safety Automata} \cite{23} in which time-critical behaviors are expressed by \textit{clock constraints} as \textit{guards} for switches and \textit{invariants} for locations. Guards restrict time intervals in which a switch is enabled while residing in its source location, whereas invariants restrict time intervals in which a TA run is permitted to reside in a location. Alternative TA definitions may incorporate distinguished \textit{acceptance locations} thus employing Büchi acceptance semantics on \textit{infinite runs} \cite{2,23} which is out of the scope of this paper as model-based testing is inherently limited to \textit{finite} test runs.

\textit{Timed Input/Output-labeled Automata (TIOA)} extend TA for timed interface specifications (e.g., for model-based conformance testing of time-critical components or systems \cite{34,35}). The \textit{label alphabet} \( \Sigma = \Sigma_I \cup \Sigma_O \) of a TIOA consists of two disjoint subsets of (externally controllable, internally observable)
Definition 1 (TIOA). A TIOA $\mathcal{A}$ is a tuple $(L, \ell_0, \Sigma_I, \Sigma_O, \rightarrow)$, where

- $L$ is a finite set of locations with initial location $\ell_0 \in L$,
- $\Sigma_I$ and $\Sigma_O$ are sets of input actions and output actions with $\Sigma_I \cap \Sigma_O = \emptyset$,
- $\rightarrow \subseteq L \times \mathcal{B}(\mathcal{C}) \times \Sigma_I \times 2^\ell \times L$ is a relation defining switches, with a set $\mathcal{B}(\mathcal{C})$ of clock constraints $\varphi$ inductively defined as

$$\varphi := x \sim r \mid x - y \sim r \mid \neg \varphi \mid \varphi \land \varphi \mid \text{true},$$

where $x, y \in \mathcal{C}$, $r \in \mathbb{Q}^+$, and $\sim \in \{<, \leq, =, \geq, >\}$, and
- $I : L \rightarrow \mathcal{B}(\mathcal{C})$ is a function assigning location invariants.

We write $\ell \xrightarrow{\ell, g, \sigma, R} \ell'$ to denote switches from location $\ell$ to $\ell'$ with guard $g$, action $\sigma$ and set $R \subseteq \mathcal{C}$ of clocks being reset. Without loss of generality, we assume each location invariant being unequal to true to be downward-closed (i.e., with clauses $x \leq r$ or $x < r$) [8]. The operational semantics of TIOA may be defined as Timed Input/Output Labeled Transition System (TIOLTS) [22]. A TIOLTS state $\langle \ell, u \rangle$ is a pair consisting of a location $\ell \in L$ and a clock valuation $u \in \mathcal{C} \rightarrow \mathbb{T}$. A TIOLTS defines two kinds of transitions: (1) passage of time while inactively residing in a location, and (2) instantaneous switches between locations due to action occurrences (including $\tau$). Given a clock valuation $u, u + d$ denotes the clock valuation mapping each clock $c \in \mathcal{C}$ to the updated clock value $u(c) + d$ with $d \in \mathbb{T}$. For a subset $R \subseteq \mathcal{C}$ of clocks, $[R \rightarrow 0]u$ denotes the clock valuation mapping every clock in $R$ to 0 while preserving the values of all other clocks in $\mathcal{C} \setminus R$. Finally, $u \in g$ denotes that clock valuation $u$ satisfies clock constraint $g \in \mathcal{B}(\mathcal{C})$. We further distinguish between strong and weak transitions, depending on whether silent transitions are visible or not.

Definition 2 (TIOLTS). The TIOLTS of TIOA $(L, \ell_0, \Sigma_I, \Sigma_O, \rightarrow)$ is a tuple $(S, s_0, \Sigma_I, \Sigma_O, \rightarrow)$, where

- $S = L \times (\mathcal{C} \rightarrow \mathbb{T})$ is a set of states with initial state $s_0 = \langle \ell_0, [\mathcal{C} \rightarrow 0]u_0 \rangle \in S$,
- $\hat{\Sigma}_\tau = \Sigma_I \cup \Sigma_O \cup \{\tau\} \cup \Delta$ is a set of labels with $\Delta = \mathbb{T}$, $\Sigma_\tau \cap \Delta = \emptyset$, and
- $\rightarrow \subseteq S \times \hat{\Sigma}_\tau \times S$ is a set of (strong) transitions being the least relation satisfying the rules:

- $(\ell, u) \xrightarrow{d} (\ell, u + d)$ if $u \in I(\ell)$ and $(u + d) \in I(\ell)$ for $d \in \mathbb{T}$, and
- $(\ell, u) \xrightarrow{\sigma, R} (\ell', u')$ if $\ell \xrightarrow{\ell, g, \sigma, R} \ell'$, $u \in g$, $u' = [R \rightarrow 0]u$, $u' \in I(\ell')$, $\sigma \in \Sigma_\tau$. 

By $\rightarrow \subseteq S \times \hat{\Sigma}_\tau \times S$ we further denote a set of (weak) transitions being the least relation satisfying the rules:

- $s_0 \xrightarrow{\sigma} s$ if $\exists s_1, \ldots, s_{n-1} \in S : s_0 \xrightarrow{\sigma} s_1 \xrightarrow{\sigma} \ldots \xrightarrow{\sigma} s_n \text{ with } n \in \mathbb{N}_0$,
- $s \xrightarrow{\sigma} s'$ if $\exists s_1, s_2 \in S : s \xrightarrow{\sigma} s_1 \xrightarrow{\sigma} s_2 \xrightarrow{\sigma} s'$ with $n, m \in \mathbb{N}_0$,
- $s \xrightarrow{0} s'$ if $s \xrightarrow{\sigma} s'$,
- $s \xrightarrow{0} s'$ if $s \xrightarrow{\sigma} s'$ with $n \in \mathbb{N}_0$,
- $s_0 \xrightarrow{\sigma_1 \cdots \sigma_n} s$ if $\exists s_1, \ldots, s_n \in S : s_0 \xrightarrow{\sigma_1} s_1 \xrightarrow{\sigma_2} \ldots \xrightarrow{\sigma_n} s_n \text{ with } n \in \mathbb{N}_0$ and
- $s \xrightarrow{d + R} s'$ if $\exists s'' \in S : s \xrightarrow{d} s''$ and $s'' \xrightarrow{R} s'$.
We only consider strongly convergent TIOA (i.e., having TIOLTS without infinite \( \tau \)-sequences). By \( \llbracket \mathcal{A} \rrbracket^w_x, x \in \{w, s\} \), we refer to the (either weak or strong) TIOLTS semantics of TIOA \( \mathcal{A} \), where we omit parameter \( x \) if not relevant. The weak semantics is obtained by replacing all occurrences of \( \rightarrow \) by \( \Rightarrow \) in all definitions. We recall three essential properties for strong TIOLTS semantics of any given TIOA \([17,1]\).

**Proposition 1.** Let \( (S, s_0, \Sigma_I, \Sigma_O, \rightarrow) \) be a TIOLTS of a TIOA.

- (Time Add) \( \forall s_1, s_3 \in S, \forall d_1, d_2 \in \Delta : s_1 \xrightarrow{d_1 + d_2} s_3 \iff \exists s_2 : s_1 \xrightarrow{d_1} s_2 \xrightarrow{d_2} s_3 \)
- (Time Reflex) \( \forall s_1, s_2 \in S : s_1 \xrightarrow{0} s_2 \Rightarrow s_1 = s_2 \)
- (Time Determ) \( \forall s_1, s_2, s_3 \in S : s_1 \xrightarrow{\Delta} s_2 \text{ and } s_1 \xrightarrow{\Delta} s_3 \text{ then } s_2 = s_3 \)

In contrast, the weak semantics obviously obstructs all three properties.

Furthermore, by \( \text{traces}(s_0) = \{ \omega | s_0 \xrightarrow{\omega} \} \) we denote the set of all traces \( \omega = \alpha_1 \alpha_2 \cdots \alpha_k \in (\Sigma \cup \Delta)^* \) corresponding to some path \( s_0 \xrightarrow{\alpha_1} s_1 \xrightarrow{\alpha_2} \cdots \xrightarrow{\alpha_k} s_k \) of TIOLTS \( s \). Given a TIOA \( \mathcal{A} \), the TIOLTS \( \llbracket \mathcal{A} \rrbracket^s \) defines all possible (timed) runs \( s_0 = (\ell_0, u_0) \xrightarrow{d_1} \alpha_1 \xrightarrow{\ell_1, u_1} d_2 \xrightarrow{\sigma_2} \cdots \alpha_k \) of \( \mathcal{A} \) in terms of sequences of (timed) steps \( s \xrightarrow{\delta} s' \) denoting \( \exists s' \in S : s \xrightarrow{\delta} s' \xrightarrow{\mathcal{A}} s'' \) \([38]\). We refer to the set of weak/strong traces of state \( s \) by \( \text{traces}(s)^x, x \in \{w, s\} \), respectively.

**Example 1.** Figure \([4,8]\) shows a (simplified) TIOA \( \mathcal{A}^1 \) of a vending machine with two clocks, \( x \) and \( y \), and Fig. \([17]\) depicts an extract from its TIOLTS. Switches are labeled with actions (prefixes “?” for inputs and “!” for outputs), guards (e.g., \( x \leq 20 \)), and (possibly empty) clock resets. We label locations by their names (e.g., initial location idle) and their location invariants. Clock constraints being equal to true are omitted. Each (timed) run of the machine starts in initial location idle, where a user may press a button to switch to location add sugar. If no button is pressed for 20 time units (e.g., seconds), the machine is turned off via a silent switch and may be switched to idle, again, by pressing a button. In location add sugar, sugar may be repeatedly selected, where at least 10 seconds must pass between two consecutive requests and the machine proceeds to location preparing coffee at most 20 second after input press. Here, coffee is dispensed for at most 20 seconds and the machine finally returns to idle. The machine either produces small coffees (finishing after less than 15 seconds) or large coffees (requiring more than 15 seconds). This example illustrates the semantic differences between guards and invariants: guards restrict time intervals in which a switch is allowed to be taken, whereas invariants define time intervals after which a location is enforced to be left (e.g., it is allowed to perform !proceed to leave location add sugar while \( y \leq 20 \) holds, whereas it is enforced to leave location preparing coffee in case of \( y = 20 \)). Hence, guards express safety conditions, whereas invariants express liveness conditions of timed runs.
A TIOA is supposed to specify one particular part of an arbitrary complex system composed of several concurrently interacting components. We define CCS-like parallel composition of TIOA with synchronous communication via shared input/output actions, becoming internal τ-actions [17]. As a prerequisite for composing two TIOA $\mathcal{A}_1$ and $\mathcal{A}_2$, denoted as $\mathcal{A}_1 \parallel \mathcal{A}_2$, we require both to be composable (i.e., all shared actions have opposed directions).

**Definition 3 (TIOA Composition).** Let $(L_j, \ell_0, \Sigma_j, \Sigma, \sigma_j, \rightarrow_j, I_j)$ with $j \in \{1, 2\}$ be TIOA with $\Sigma_1 \cap \Sigma_2 = \emptyset, \Sigma_1 \cap \Sigma_2 = \emptyset$ and $\ell_1 \cap \ell_2 = \emptyset$. Their parallel composition is a TIOA $(L_1 \times L_2, (\ell_0, \ell_0), \Sigma_{1|2}, \Sigma_{1|2}, \rightarrow_{1|2}, I_{1|2})$ over $\ell_{1|2} = \ell_1 \cup \ell_2$ with $\Sigma_{1|2} = (\Sigma_1 \cup \Sigma_2) \setminus (\Sigma_1 \cap \Sigma_2), \Sigma_{1|2} = (\Sigma_1 \cup \Sigma_2) \setminus (\Sigma_1 \cap \Sigma_2), I_{1|2}(\ell_1, \ell_2) = I_1(\ell_1) \wedge I_2(\ell_2)$, and $\rightarrow_{1|2}$ is the least relation satisfying the rules:

1. $(\ell_1, \ell_2) \xrightarrow{g_1, \sigma, R_1} \ell'_{1|2} (\ell'_1, \ell'_2)$ if $\ell_1 \xrightarrow{g_1, \sigma, R_1} \ell'_1$ and $\sigma \in (\Sigma_1 \setminus \Sigma_2) \cup \{\tau\}$
2. $(\ell_1, \ell_2) \xrightarrow{g_2, \sigma, R_2} \ell'_{1|2} (\ell'_1, \ell'_2)$ if $\ell_2 \xrightarrow{g_2, \sigma, R_2} \ell'_2$ and $\sigma \in (\Sigma_2 \setminus \Sigma_1) \cup \{\tau\}$
3. $(\ell_1, \ell_2) \xrightarrow{g_1, g_2, \sigma, R_1, R_2} \ell'_{1|2} (\ell'_1, \ell'_2)$ if $\ell_1 \xrightarrow{g_1, \sigma, R_1} \ell'_1, \ell'_1 R_1 \xrightarrow{g_2, \sigma, R_2} \ell'_2$ and $\sigma \in (\Sigma_1 \cap \Sigma_2) \setminus \{\tau\}$

**Example 2.** Consider TIOA $\mathcal{A}_1, \mathcal{A}_2$ and their parallel composition $\mathcal{A}_1 \parallel \mathcal{A}_2$ (cf. Figs. 1a, 2a, and 2b).

A customer $\mathcal{A}_2$ may press a button, add sugar and wait for coffee. In $\mathcal{A}_1 \parallel \mathcal{A}_2$, shared actions are performed synchronously only if being enabled in both $\mathcal{A}_1$ and $\mathcal{A}_2$, thus resulting in a τ-step. For instance, the synchronized switch from idle to add sugar is labeled with τ and clocks x, y (from $\mathcal{A}_1$ and z (from $\mathcal{A}_2$) being reset. Similarly, the sugar loop also becomes a τ-step, while clock resets are unified and guards are conjugated. In contrast, switch proceed does not become internal as this output is not observed by $\mathcal{A}_2$ (but instead transmitted to some administration component). Location preparing coffee has two switches labeled with τ as both coffee switches of $\mathcal{A}_1$ are synchronized with the coffee switch of $\mathcal{A}_2$. Location off has a τ-step to add sugar’ as the switch of $\mathcal{A}_1$ from off to idle may also be synchronized with the switch of $\mathcal{A}_2$ from idle to add sugar. Here, add sugar’ does not have any outgoing transitions as add sugar (of $\mathcal{A}_2$) has no actions shared with idle (of $\mathcal{A}_1$). The sugar loop and the switch from preparing coffee to done guarded by $y > 15 \land z \leq 10$ are semantically incompatible as their guards are unsatisfiable in all runs.

### 3 Timed Input/Output Conformance

TIOLTS have been considered as a formal basis for conformance testing theories of time-critical input/output behaviors [38]. Timed conformance relations are usually defined in the flavor of loco testing.
as initially proposed on input/output labeled transition systems (IOLTS) for untimed behaviors \[41\].

Intuitively, IOLTS \(im\) representing an implementation under test input/output-conforms to IOLTS \(sp\) representing a specification, denoted \(im \text{ioco} sp\), if for all input behaviors specified in \(sp\), the observable output behaviors of \(im\) for those input behaviors are permitted by \(sp\). Input behaviors may be only partially specified (i.e., only for relevant/intended environmental input sequences, the expected output behaviors are explicitly captured in \(sp\)), whereas implementation \(im\) is supposed to be input-enabled (i.e., to never block any input action). Timed adaptations of \(ioco\), so-called \(tioco\), consider both \(im\) and \(sp\) to be represented as TIOATS as checking timed input/output conformance directly on TIOA is unfeasible due to non-observability of clock resets in timed runs. For instance, in the example in Fig. 1a it is unknown if it is allowed to wait for 20 time units in \(idle\) if we reach this location from \(done\) as resets of \(x\) and \(y\) are not observable. Similar to the untimed case, TIOATS \(im\) is supposed to be input-enabled (i.e., \(im\) must always—at any time—be able to instantaneously accept all possible inputs). In addition, for \(im\) to specify realistic behaviors, we further impose the independent-progress property: In each state, \(im\) is able to either wait for an infinite amount of time or to eventually perform an output action thus preventing forced inputs \[17, 38\].

**Definition 4.** Let \((S, S_0, \Sigma_I, \Sigma_O, \rightarrow)\) be a TIOATS.

- *(Input-Enabledness)* State \(s \in S\) is weak input-enabled iff \(\forall i \in \Sigma_I : s \xrightarrow{\cdot} {\cdot}\).  
- *(Independent Progress)* State \(s \in S\) of a TIOATS enables weak independent progress iff \(\forall d \in \Delta : s \xrightarrow{d} {\cdot}\) or \(\exists d \in \Delta, \exists o \in \Sigma_O : s \xrightarrow{d} o\).

A TIOATS is (weak) input-enabled iff all states are (weak) input-enabled and it enables (weak) independent progress if all states do (for the strong versions of both properties, we replace \(\rightarrow\) by \(\rightarrow\)). Similarly to \(ioco\), we assume weak input-enabledness and independent progress for all implementations under test, whereas specifications may be underspecified. This is required for practical testing where an implementation should always at least accept (and then potentially ignore) every input. Conversely, the environment (i.e., a tester) should not be enforced by the implementation to provide a particular input in order to guarantee any progress. For instance, consider Fig. 1a location \(off\) is not input-enabled as there is no switch for input sugar. However, if there would be such a switch, then also location \(idle\) would be weak input-enabled as output \(off\) may be reached by a \(\tau\)-step. In contrast, all locations in Fig. 1a enable (weak) independent progress.

We now revisit two major definitions of \(tioco\) from recent literature. We first consider the (notationally slightly adapted) definition of Krichen and Tripakis \[26\] which we will refer to as \(tioco_\Delta\). It is based on the assumption that, in addition to timed traces consisting of sequences of timed steps \((d, o)\) including output actions \(o \in \Sigma_O\), also all possible delays \(d \in \Delta\) permitted to elapse in states \(s \in S\) are observable in isolation.

**Definition 5 (\(tioco_\Delta\)).** Let \(im, sp\) be a TIOATS over \(\Sigma = \Sigma_I \cup \Sigma_O, s \in S, S' \subseteq S\), and \(\xi \in (\Delta \times \Sigma)^*\).

- \(s \text{ after } \xi := \{s' | s \xrightarrow{\xi} s'\}\),
- \(\text{out}_\Delta(s) := \{o | o \in \Sigma_O, s \xrightarrow{o}\} \cup \{d | d \in \Delta, s \xrightarrow{d}\}\),
- \(\text{out}_\Delta(S') := \bigcup_{s \in S'} \text{out}_\Delta(s)\),
- \(\text{ttraces}(s) := \{\xi | s \xrightarrow{\xi}\},\) and
- \(im \text{ tioco}_\Delta sp \iff \forall \xi \in \text{ttraces}(sp) : \text{out}_\Delta(im \text{ after } \xi) \subseteq \text{out}_\Delta(sp \text{ after } \xi)\).
We may use the name of the whole TIO LTS and the name of its initial state interchangeably as frequently done in ioco-based theories (e.g., by im after ξ we refer to the set of states being reachable by ξ from the initial state of im). The second version of ioco, which we will denote as tioco₅, does not rely on observability of arbitrary delays, but instead incorporates a notion of timed quiescence \[38\]. Quiescence constitutes another fundamental concept of (untimed) ioco: IOLTS state \(s\) is quiescent, denoted \(δ(s)\), if no output or internal action is enabled in \(s\) thus requiring an input to proceed a (suspended) run reaching \(s\). By making quiescence observable by a special output \(δ\), ioco rejects trivial implementations im never showing any outputs as this must be explicitly permitted by the specification. In the timed case, state \(s\) of a TIO LTS may be considered quiescent if no output action is ever (or, at least not until some fixed maximum delay \(M\) \[14\]) enabled in \(s\). To this end, the notion of timed suspension traces (tstraces) extends traces of TIO LTS by timed observable quiescence. The most common definition of tioco₅ may be given as follows.

**Definition 6 (tioco₅).** Let im, sp be a TIO LTS over \(Σ = Σ_I ∪ Σ_O\), \(s, s′ ∈ S, S′ ⊆ S\) and \(ξ ∈ (Δ × (Σ ∪ \{δ\}))^∗\).

- \(s\) is quiescent, denoted by \(δ(s)\), iff ∀μ ∈ Σ₀, ∀d ∈ Δ : \(s \xrightarrow{(d,μ)} s\).
- \(s\text{ after }ξ := \{s' \mid s \xrightarrow{ξ} s'\}\).
- \(\text{out}(s) := \{(d, o) \mid o ∈ Σ_O, d ∈ Δ, s \xrightarrow{(d,o)} \} ∪ \{δ \mid δ(s)\}\).
- \(\text{out}(S') := \bigcup_{s ∈ S} \text{out}(s)\).
- \(\text{tstraces}(s) := \{ξ \mid s \xrightarrow{ξ}\), where \(s' \xrightarrow{s' \text{ after } ξ} \) iff \(δ(s')\), and
- \(\text{im } tioco₅ \text{ sp } \Leftrightarrow ∀ξ ∈ \text{tstraces}(sp) : \text{out}(\text{im after } ξ) ⊆ \text{out}(\text{sp after } ξ)\).

**Example 3.** Figure 3 provides a collection of small examples illustrating tioco₅. In Fig. 3a it holds that \([A_0]_S tioco₅ [A_1]_S\) as the required inclusion relation holds for all possible out sets, for instance, \(\text{out}( [A_0]_S \text{ after } ε) = \{(1, o),(2, o)\} ⊆ \text{out}( [A_1]_S \text{ after } ε) = \{(1, o),(2, o),(3, o)\}\). Note, that this is also true for output behaviors enabled after 3 time units as \([A_0]_S\) does not permit to wait for 3 time units, such that the respective out set is empty. Hence, tioco permits implementations to show less output behavior than the specification allows. Figure 3b depicts a further implementation where \([A_2]_S tioco₅ [A_3]_S\) does not hold as \(\text{out}( [A_2]_S \text{ after } ε) = \{δ\} \notin \text{out}( [A_3]_S \text{ after } ε) = \{(1, o),(2, o),...\}\) (i.e., implementation \([A_2]_S\) is quiescent but specification \([A_3]_S\) is not). The TIO LTS in Fig. 3c illustrates how non-determinism is handled by tioco₅. For specification \([A_3]_S\), it holds that \(\text{out}( [A_3]_S \text{ after } (0, o)) = \{(0, o),(1, o),(2, o),(2, o')\}\) and, the same holds for \(\text{out}( [A_4]_S \text{ after } (0, o))\) and, particularly, (2, o) and (2, o'). This is due
to the fact that in $\text{tioco}_8$ only outputs of those states are considered being reachable via some trace of the specification, but not necessarily of any state of the respective TIOA. Therefore, it holds that $[A_1]_S \text{tioco}_8 [A_5]_S$.

Next, we apply $\text{tioco}_8$ to our running example to illustrate the differences to $\text{tioco}_\Delta$.

**Example 4.** Consider TIOA $\mathcal{A}_1'$ depicted in Fig. 4 to be a candidate implementation of TIOA $\mathcal{A}_1$ in Fig. 1a. First, the guard $y \leq 20$ of the switch labeled with proceed is not contained in $\mathcal{A}_1'$, and instead, location add sugar has an invariant $y \leq 15$. Considering only this difference, we have $[\mathcal{A}_1']_S \text{tioco}_8 [\mathcal{A}_1]_S$ as well as $[\mathcal{A}_1']_S \text{tioco}_\Delta [\mathcal{A}_1]_S$ as we forbid output proceed for $15 < y \leq 20$ and waiting in add sugar for an arbitrary amount of time. In contrast, omitting the switch labeled 'proceed in $\mathcal{A}_1'$ would lead to a violation of $\text{tioco}_8$ as location add sugar would become quiescent (whereas $\text{tioco}_\Delta$ still holds as it does not check for quiescence). Second, the invariant $x \leq 20$ of location idle in $\mathcal{A}_1$ is not contained in $\mathcal{A}_1'$ but, instead, becomes a guard to the switch labeled with ?press. As a result, $[\mathcal{A}_1']_S \text{tioco}_8 [\mathcal{A}_1]_S$ still holds as delays in timed runs are only observable by $\text{tioco}_8$ if paired with a subsequent output action. In contrast, $[\mathcal{A}_1']_S \text{tioco}_\Delta [\mathcal{A}_1]_S$ does not hold as in $\text{tioco}_\Delta$ delays of any possible duration are observable, even if no subsequent outputs will ever occur.

**Weaknesses of Existing Definitions of Timed Input/Output Conformance.** As a result, $\text{tioco}_\Delta$ and $\text{tioco}_8$ are incomparable. In addition, observability capabilities required for effectively checking $\text{tioco}_\Delta$ are unrealistic and therefore only of theoretical interest, but infeasible in practice. In contrast, $\text{tioco}_8$ is more realistic but fails to guarantee liveness requirements as the notion of quiescence does not properly reflect the differences between allowed and enforced outputs in TIOA specifications. To further illustrate this problem, consider the five TIOA, $\mathcal{A}_1$ to $\mathcal{A}_5$, and their TIOLTS in Fig. 5. According to Def. 6 location $\ell_1$ of $\mathcal{A}_1$ is quiescent, whereas none of the locations $\ell_2$ to $\ell_5$ of $\mathcal{A}_2$ to $\mathcal{A}_5$ are quiescent as output $o$ is eventually enabled. The table in Fig. 5 shows all possible comparisons of all five TIOA under $\text{tioco}_8$. Here, the fact that $[\mathcal{A}_5]_S \text{tioco}_8 [\mathcal{A}_5]_S$ and $[\mathcal{A}_5]_S \text{tioco}_8 [\mathcal{A}_5]_S$ hold is particularly undesirable (as highlighted in the table): $\mathcal{A}_5$ may either produce output $o$ within interval $0 \leq x < k$, or it may behave quiescent, whereas $\mathcal{A}_4$ and $\mathcal{A}_5$ must produce output $o$ within interval $0 \leq x < k$ and therefore must not be quiescent. In contrast, $\mathcal{A}_2$ and $\mathcal{A}_3$ are allowed to be quiescent, by residing for unlimited durations in $\ell_2$ and $\ell_3$.

We summarize the most important weaknesses of existing versions of $\text{tioco}$.

- **(Live Timed Behaviors)** $\text{tioco}$ either relies on a (unrealistically) strong notion of observability including arbitrary delays, or on a (unnecessarily) weak notion of quiescence not distinguishing
allowed from enforced outputs.

- **(Compositionality)** To the best of our knowledge, there only exists one work investigating compositionality properties of tioco so far which does not take any notion of quiescence into account [3].
- **(Infinite TIOA)** tioco is defined on TIOA, an infinitely-branching state-transition graph being intractable for realistic testing practices and tools. However, a sound characterization of tioco directly on TIOA is also not feasible as timed (suspension) traces are not directly derivable from TIOA.

We next propose an improved version of tioco to tackle these weaknesses.

## 4 Improved Timed Input/Output Conformance

In this section, we tackle the weaknesses of existing versions of tioco as described in the previous section.

### 4.1 Safe vs. Enforced Quiescence

Existing definitions of tioco either do not have any notion of quiescence at all [26], or quiescence includes both (1) states that, if no input is provided, will delay forever with no output and (2) states that may eventually produce an output (cf. Fig. 5) [38]. We instead consider two different facets of quiescence: state $s$ is *enforced quiescent* if each run *must* wait in this state for an input for an arbitrary duration to proceed. This coincides with quiescence of tioco$_S$. In contrast, state $s$ is *safe quiescent* if a run *may* wait in this state for an input for an arbitrary duration, but *may* also proceed by eventually producing an output. Consequently, state $s$ is *not quiescent*, if a run *must* eventually proceed from this state by producing an output. Hence, $s$ is *live* if it is neither safe quiescent nor enforced quiescent.

**Definition 7** (Safe/Enforced Quiescence). Let $(S, s_0, \Sigma_I, \Sigma_O, \rightarrow)$ be a TIOA.

- $s \in S$ is safe-quiescent, denoted $\delta_S(s)$, iff $\forall d \in \Delta : s \xrightarrow{d} s'$.
- $s \in S$ is enforced-quiescent, denoted $\delta_E(s)$, iff $\forall \mu \in \Sigma_O, \forall d \in \Delta : s \xrightarrow{(d, \mu)} s'$.
Intuitively, we may assume enforced-quiescent states to be also safe-quiescent. However, as a counter-example, assume a TIOLTS with one state \( (\ell, x = 0) \) (corresponding to a TIOA with one location \( \ell \) and \( I(\ell) = x \leq 0 \)): here, no outputs are possible and no delays are allowed thus obstructing the intuition.

**Lemma 1.** Let \( (S, s_0, \Sigma_I, \Sigma_O, \rightarrow) \) be a TIOLTS. If \( s \in S \) enables independent progress, then \( \delta_E(s) \Rightarrow \delta_S(s) \).

**Proof.** We prove Lemma 1 by contradiction. Let \( (S, s_0, \Sigma_I, \Sigma_O, \rightarrow) \) be a TIOLTS. If \( s \in S \) enables independent progress, then \( \forall d \in \Delta : s \xrightarrow{d} o \) or \( \exists d \in \Delta, \exists o \in \Sigma_O : s \xrightarrow{d} o \) (cf. Definition 4). Assume that it holds that \( \delta_E(s) \) but not \( \delta_S(s) \). Then, \( \forall o \in \Sigma_O, \forall d \in \Delta : s \xrightarrow{d(o)} \) and \( \exists d \in \Delta : s \xrightarrow{d \not\in o} \). However, this contradicts the assumption that \( s \) enables independent progress. Hence, it holds that \( \delta_E(s) \Rightarrow \delta_S(s) \) if \( s \) enables independent progress. \( \square \)

We add \( \delta_S \) and \( \delta_E \) to \( \textit{out} \) to distinguish both types of quiescence and adjust \( \textit{tstraces} \), accordingly. This allows us to define \textit{live timed ioco} (\textit{ltioco}S) by extending \textit{tico}S with outputs \( \delta_S \) and \( \delta_E \). Hence, \textit{ltioco}S not only guarantees output behaviors of implementation \( \textit{im} \) to be \textit{safe} (i.e., allowed to occur within the observed time interval as specified in \( \textit{sp} \)), but also requires \( \textit{im} \) to be \textit{live} (i.e., to progress with an output within a time interval if enforced by \( \textit{sp} \)).

**Definition 8.** Let \( \textit{im}, \textit{sp} \) be TIOLTS over \( \Sigma = \Sigma_I \cup \Sigma_O \), \( s, s' \in S \), \( S' \subseteq S \), \( \xi \in (\Delta \times (\Sigma \cup \{\delta_I\})) \).

- \( s \textit{ after } \xi := \{s' \mid s \xrightarrow{\xi} s'\} \)
- \( \textit{out}_S(s) := \{(d, o) \mid d \in \Delta, o \in \Sigma_O, s \xrightarrow{d(o)} \} \cup \{\delta_I \mid \delta_S(s)\} \)
- \( \textit{out}_S(S') := \bigcup_{s \in S} \textit{out}_S(s) \)
- \( \textit{tstraces}_L(s) := \{\xi \mid s \xrightarrow{\xi} s' \text{ iff } \delta_S(s')\} \)
- \( \textit{im} \textit{ltioco}_S \textit{sp} := \forall \xi \in \textit{tstraces}_L(s) : \textit{out}_S(\textit{im after } \xi) \subseteq \textit{out}_S(\textit{sp after } \xi) \)

Obviously, using two different quiescence symbols does not increase complexity of conformance checking as compared to \textit{tico}S in Def. 6.

**Example 5.** State \( (\ell_1, x = 0) \) in Fig. 5 is quiescent, whereas \( (\ell_2, x = 0) \) and \( (\ell_3, x = 0) \) are not. With our improved definition, \( (\ell_1, x = 0) \) is enforced-quiescent, whereas \( (\ell_2, x = 0) \) and \( (\ell_3, x = 0) \) are safe-quiescent. States \( (\ell_4, x = 0) \) and \( (\ell_5, x = 0) \) are neither safe-quiescent nor enforced-quiescent due to the invariants of \( \ell_4 \) and \( \ell_5 \). Hence, \textit{ltioco}S is now able to reject \( \ell_3 \) as incorrect implementation of \( \ell_4 \) and \( \ell_5 \) as both \( \ell_4 \) and \( \ell_5 \) are not quiescent, whereas \( \ell_3 \) is safe-quiescent. For all other cases, \textit{ltioco}S yields the same results as listed in Fig. 5.

**Lemma 2.** \textit{ltioco}S is a preorder on the set of input-enabled TIOLTS.

**Proof.** Let \( p, q, r \) be input-enabled TIOLTS being derived from TIOA, and \( p \textit{ltioco}_S q \) and \( q \textit{ltioco}_S r \). It holds by Definition 8 that \( p \textit{ltioco}_S q \) i.e., \( \textit{ltioco}S \) is reflexive.

It remains to be shown that \( p \textit{ltioco}_S r \), i.e., \( \forall \xi \in \textit{tstraces}_L(r) : \textit{out}_S(p \textit{after } \xi) \subseteq \textit{out}_S(r \textit{after } \xi) \). Let \( \xi \in \textit{tstraces}_L(r) \). If \( \xi \in \textit{tstraces}_L(q) \), then \( \forall \xi \in \textit{tstraces}_L(q) : \textit{out}_S(p \textit{after } \xi) \subseteq \textit{out}_S(r \textit{after } \xi) \) follows from transitivity of \( \subseteq \).

The case of \( \xi \notin \textit{tstraces}_L(q) \) remains, i.e., the case where behaviors are not present in \( q \) such that \( \xi \in \textit{tstraces}_L(p) \), \( \xi \notin \textit{tstraces}_L(q) \), and \( \xi \in \textit{tstraces}_L(r) \). We prove this part by contradiction. Suppose, \( \forall \xi \in \textit{tstraces}_L(r) : \textit{out}_S(p \textit{after } \xi) \subseteq \textit{out}_S(r \textit{after } \xi) \) fails for a \( \xi \in \textit{tstraces}_L(r) \setminus \textit{tstraces}_L(q) \), i.e., such
Proof. Let \( \xi \) decomposes into \( \xi_1 \cdot (d, a) \cdot \xi_2 \) where \( \xi_1 \in \text{tstraces}_L(q) \) but \( \xi_1 \cdot (d, a) \notin \text{tstraces}_L(q) \). Since \( \text{outs}(p \text{ after } \xi_1) \subseteq \text{outs}(q \text{ after } \xi_1) \), \( a \notin \Sigma_D \cup \{ \delta_s, \delta_E \} \). Additionally, \( a \in \Sigma_I \) contradicts input-enabledness of \( q \). Thus, \( \xi \in \text{tstraces}_L(q) \) and \( \text{tioco} \) is transitive.

From reflexivity and transitivity of \( \text{tioco} \) it follows that \( \text{tioco} \) is indeed a preorder on input-enabled TIO LTS.

Furthermore, we can prove that \( \text{tioco} \) is sound (i.e., strictly more discriminating) with respect to \( \text{tioco} \) in the sense that \( \text{im tioco} sp \Rightarrow \text{im tioco} sp \) (but not vice versa).

**Theorem 1** (Correctness of \( \text{tioco} \)). Let \( im \) and \( sp \) be TIO LTS with \( im \) being input-enabled and enabling independent progress.

- \( \text{im tioco} sp \Rightarrow \text{im tioco} sp \)
- \( \text{im tioco} sp \Rightarrow \text{im tioco} \delta sp \)
- \( \text{im tioco} \delta sp \Rightarrow \text{im tioco} sp \) does, in general, not hold.

Additionally, let \( sp \) also be input-enabled.

- \( \text{im tioco} sp \Rightarrow \text{traces}^{w}(im) \subseteq \text{traces}^{w}(sp) \)

**Proof.** Let \( im \) and \( sp \) be TIO LTS with \( im \) being input-enabled and enabling independent progress.

First, we prove \( \text{im tioco} sp \Rightarrow \text{im tioco} \delta sp \). The only difference between \( \text{tioco} \) and \( \text{tioco} \) is \( \delta \) because \( \delta_E((\ell, u)) \leftrightarrow \delta((\ell, u)) \), i.e., enforced quiescence, coincides with classical quiescence. When we remove the output symbol \( \delta \) from the \( \text{outs} \) sets it holds that \( \text{outs}(\text{im after } \xi) \subseteq \text{outs}(\text{sp after } \xi) \Rightarrow \text{outs}(\text{im after } \xi) \setminus \{ \delta \} \subseteq \text{outs}(\text{sp after } \xi) \setminus \{ \delta \} \). Hence, \( \text{im tioco} sp \Rightarrow \text{im tioco} \delta sp \).

Next, we prove \( \text{im tioco} sp \Rightarrow \text{im tioco} \delta sp \). The difference between \( \text{tioco} \) and \( \text{tioco} \) is the output-set, containing output and delays for \( \text{tioco} \) and pairs of outputs and delays and quiescence \( \delta_E \) and \( \delta_S \) for \( \text{tioco} \). Note, that we do not have to consider the differences in the \( \text{tstraces} \) and \( \text{tstraces}_L \), respectively, as these differences are already captured by the out-sets.

When only considering delays, \( \text{im tioco} \delta sp \) holds if \( im \) does not allow more delays than \( sp \). This behavior is captured by \( \text{tioco} \) as \( im \) may only introduce an invariant, resulting in \( im \) not having output symbol \( \delta \), preserving the subset relation. Making the invariant stricter is already captured as outputs are always pairs of delays and actions. Furthermore, \( \text{im tioco} \delta sp \) if \( im \) allows for more delays than \( sp \). This is also captured by \( \text{tioco} \) as allowing more delays means removing the invariant of the corresponding location, thus introducing output symbol \( \delta \). Only changing the invariant to a greater value either violates independent progress (if no output action or \( \tau \) is possible after this delay) or also allows outputs after these greater delays (which is covered through outputs in \( \text{tioco} \) being pairs of delays and actions).

Next, we show that \( \text{im tioco} \delta sp \Rightarrow \text{im tioco} sp \) does, in general, not hold. Figure 5 provides an example. Here, \( \llbracket \phi \rrbracket_{\text{tioco}} \llbracket \phi \rrbracket_{\text{tioco}} \) holds, but \( \llbracket \phi \rrbracket_{\text{tioco}} \llbracket \phi \rrbracket_{\text{tioco}} \) does not hold.

Now, let \( im \) and \( sp \) be TIO LTS with \( im \) and \( sp \) being input-enabled and \( im \) enabling independent progress. Finally, we prove that \( \text{im tioco} sp \Rightarrow \text{traces}^{w}(im) \subseteq \text{traces}^{w}(sp) \). From \( \text{im tioco} sp \) it follows by definition that \( \forall \xi \in \text{tstraces}_L(sp) : \text{outs}(im \text{ after } \xi) \subseteq \text{outs}(sp \text{ after } \xi) \), resulting in trace inclusion for \( \text{tstraces}_L \). For \( \text{im tioco} sp \Rightarrow \text{traces}^{w}(im) \subseteq \text{traces}^{w}(sp) \), we have to show that removing quiescence symbols \( \delta_E \) and \( \delta_S \) from all \( \text{tstraces}_L \) (resulting in \( \text{traces}^{w} \)) preserves the subset relation. In \( \text{tstraces}_L \), \( \delta_E \) and \( \delta_S \) are added with self-loops to the respective TIO LTS states. Therefore, we remove all \( \xi \in \text{tstraces}_L(sp) \) and \( \xi \in \text{tstraces}_L(im) \) containing \( \delta_E \) and/or \( \delta_S \). By \( \Xi_{sp}^{\delta} \) and \( \Xi_{im}^{\delta} \) we denote the sets of traces containing \( \delta_E \) and \( \delta_S \). Due to \( \text{im tioco} sp \) it holds that \( \Xi_{im}^{\delta} \subseteq \Xi_{sp}^{\delta} \). Hence, removing all
\(\xi \in \mathbb{Z}_m^\delta\) from \(t\text{traces}_L(sp)\) and \(t\text{traces}_L(im)\) does not effect the subset relation. Furthermore removing all \(\xi \in \mathbb{Z}_m^\delta \setminus \mathbb{Z}_m^\delta\) also does not effect the subset relation as \(\forall \xi \in \mathbb{Z}_m^\delta \setminus \mathbb{Z}_m^\delta : (\xi \in t\text{traces}_L(sp) \wedge \xi \notin t\text{traces}_L(im))\). Finally, we have to require input-enabledness for \(sp\) such that \(\text{ltioco}_S\) is a preorder (cf. Lemma 2). We have this requirement as \(\text{traces}^w(im) \subseteq \text{traces}^w(sp)\) also is a preorder. Therefore, \(im \text{ltioco}_S sp \Rightarrow \text{traces}^w(im) \subseteq \text{traces}^w(sp)\).

Note, that \(im \text{ltioco}_\Delta sp \Rightarrow im \text{ltioco}_S sp\) does not hold as \(\text{ltioco}_\Delta\) has no notion of quiescence, and \(im \text{ltioco}_S sp \Rightarrow \text{traces}^s(im) \subseteq \text{traces}^s(sp)\) does not hold as \(\text{ltioco}_S\) is limited to observable (weak) steps of timed (suspension) traces.

4.2 Compositionality

For investigating compositionality of \(\text{ltioco}_S\), we first define parallel composition of TIOA also at the level of TIOATS.

**Definition 9** (TIOATS Composition). Let \((S_j,s_0,j,\Sigma_i,\Sigma_{O_j},\rightarrow_j)\) with \(j \in \{1,2\}\) be TIOATS of composable TIOA. The parallel product is a TIOATS \((S_1 \times S_2,(s_0 \times s_0),\Sigma_{O_1 \times \Sigma_{O_2}},\rightarrow_{1 \parallel 2})\), where \(\Sigma_{O_1 \parallel 2}\) and \(\Sigma_{O_1 \parallel 2}\) are defined according to Def. 3 and \(\rightarrow_{1 \parallel 2}\) is the least relation satisfying the rules:

1. \((s_1,s_2) \sim_{1 \parallel 2} (s'_1,s'_2)\) if \(s_1 \sim_1 s'_1, \sigma \in (\Sigma_1 \setminus \Sigma_2) \cup \{\tau\}\),
2. \((s_1,s_2) \sim_{1 \parallel 2} (s'_1,s'_2)\) if \(s_1 \sim_2 s'_2, \sigma \in (\Sigma_2 \setminus \Sigma_1) \cup \{\tau\}\),
3. \((s_1,s_2) \sim_{1 \parallel 2} (s'_1,s'_2)\) if \(s_1 \sim_1 s'_1, s'_2 \sim_2 s'_2\) and \(\sigma \in (\Sigma_1 \cap \Sigma_2)\), and
4. \((s_1,s_2) \sim_{1 \parallel 2} (s'_1,s'_2)\) if \(s_1 \sim_1 s'_1, s'_2 \sim_2 s'_2\) and \(d \in \Delta\).

Rules (1) and (2) preserve transitions of non-shared (i.e., unsynchronized) actions from both TIOATS, whereas rule (3) introduces silent transitions for input/output action pairs synchronized between both TIOATS. Rule (4) preserves (synchronous) delay steps of length \(\Delta\) enabled by both TIOATS. Rule (5) handles inputs leading to the failure state in one of the components, where our notion of composable TIOA ensures that those actions leading to the failure state are not shared. We conclude the following properties.

**Lemma 3.** Let \(\mathcal{A}_1\) and \(\mathcal{A}_2\) be composable TIOA.

1. \(\text{traces}(\llbracket \mathcal{A}_1 \parallel \mathcal{A}_2 \rrbracket)_S = \text{traces}(\llbracket \mathcal{A}_1 \rrbracket_S \parallel \llbracket \mathcal{A}_2 \rrbracket_S)\), and
2. if \(\mathcal{A}_1\) and \(\mathcal{A}_2\) are input-enabled and enable independent progress, then this also holds for \(\mathcal{A}_1 \parallel \mathcal{A}_2\).

**Proof.** Let \(\mathcal{A}_1\) and \(\mathcal{A}_2\) be composable TIOA. We prove (1) and (2) separately.

1. Let \(P = (S_P,s_0^P,\Sigma_I^P,\Sigma_O^P,\rightarrow_P) = [\llbracket \mathcal{A}_1 \parallel \mathcal{A}_2 \rrbracket]_S\) and \(Q = (S_Q,s_0^Q,\Sigma_I^Q,\Sigma_O^Q,\rightarrow_Q) = [\llbracket \mathcal{A}_1 \rrbracket]_S \parallel [\llbracket \mathcal{A}_2]_S\). In order to prove \(\text{traces}(\llbracket \mathcal{A}_1 \parallel \mathcal{A}_2 \rrbracket)_S = \text{traces}(\llbracket \mathcal{A}_1 \rrbracket_S \parallel \llbracket \mathcal{A}_2 \rrbracket_S)\), we show the following:
   - \(S_P = S_Q\). When deriving a TIOATS from a TIOA, the set of states can only be reduced by location invariants. When composing two locations, their invariants are, by definition, conjugated. Therefore, the set of states of \(\llbracket \mathcal{A}_1 \parallel \mathcal{A}_2 \rrbracket\) is determined by conjunction of location invariants of both \(\mathcal{A}_1\) and \(\mathcal{A}_2\). Furthermore, delay transitions only remain after composition if both \(\llbracket \mathcal{A}_1 \rrbracket\) and \(\llbracket \mathcal{A}_2 \rrbracket\) are able to perform a delay (cf. Rule (4) of Definition 9). As these delay transitions are a result of location invariants, it holds that \(S_P = S_Q\).
   - \(\Sigma_I^P = \Sigma_I^Q\) and \(\Sigma_O^P = \Sigma_O^Q\). These equalities hold by definition (cf. Definitions 3 and 9).
\[ \rightarrow p = \rightarrow q \]. Similar to \( S_p = S_q \), TIOLOTS transitions are dependent on on clock constraints, and additionally they depend on TIOA switches. As with \( S_p = S_q \), clock constraints are, by definition, conjugated. Hence, the set of transitions of \([A_1 \parallel A_2]_S\) is determined by conjunction of clock constraints of both \( A_1 \) and \( A_2 \), and, as with \( S_p = S_q \), it holds that \( \rightarrow p = \rightarrow q \).

Hence, it holds that traces(\([A_1 \parallel A_2]_S\)) = traces(\([A_1]_S \parallel [A_2]_S\)) as the sets of states, actions, and transitions are equal.

(2) Let \( \Sigma_1^j \) be the inputs of \( A_1 \), \( \Sigma_2^j \) be the inputs of \( A_2 \), and \( \Sigma_1^{1,2} = (\Sigma_1^j \cup \Sigma_2^j) \setminus (\Sigma_1^{1} \cup \Sigma_2^{1}) \) be the inputs of \([A_1]_S\). Rules (1) and (2) of TIOA composition ensure that inputs \( \Sigma_1^j \setminus (\Sigma_1^{1} \cup \Sigma_2^{1}) \) and \( \Sigma_2^j \setminus (\Sigma_1^{1} \cup \Sigma_2^{1}) \) are preserved, respectively. As \( \Sigma_1^j \cap \Sigma_2^j = \emptyset \), \( \Sigma_1^{1,2} \) does not contain further inputs. Therefore, input-enabledness is preserved under TIOA composition. Furthermore, assume that TIOA composition does not preserve independent progress. Hence, there is a restriction in \( A_2 \) such that it holds for a state \( s \) of \([A_1]_S\) (or vice versa) that \( \exists d \in \Delta : s \xrightarrow{d} s' \) or \( \exists d \in \Delta : s \xrightarrow{d} s'' \) for an \( o \in \Sigma_1^{1} \). However, if such a restriction would exist, then the corresponding state in \([A_2]_S\) would enable independent progress as \( A_2 \) enables independent progress. Futhermore, output \( o \in \Sigma_2^{1} \) (or \( \Sigma_2^{2} \), respectively) does not obstruct independent progress if \( o \in \Sigma_1^j \cap \Sigma_2^{2} \) or \( o \in \Sigma_2^j \cap \Sigma_1^{3} \) is a common action as the matching input is always available due to input-enabledness. The result is an internal action \( \tau \) not obstructing independent progress. Hence, TIOA composition preserves independent progress. □

Property (1) ensures parallel composition on TIOA and TIOLOTS to commute with respect to timed-traces semantics such that a composed specification can be effectively built from the (finite) TIOA representations of its components. Property (2) ensures that input-enabled and independent-progress enabling TIOA are closed under parallel composition. We now prove compositionality of ltioco.

**Theorem 2.** Let \( im_1 \), \( im_2 \), \( sp_1 \), and \( sp_2 \) be input-enabled and independent progress enabling TIOLOTS of composable TIOA. Then it holds that

\[
(im_1 \ ltioco_S sp_1) \wedge (im_2 \ ltioco_S sp_2) \Rightarrow (im_1 \parallel im_2) \ ltioco_S (sp_1 \parallel sp_2).
\]

**Proof.** Let \( im_1 \) and \( im_2 \) as well as \( sp_1 \) and \( sp_2 \) be input-enabled and independent progress enabling TIOLOTS of composable TIOA. Additionally, it holds that \( im_1 \ ltioco_S sp_1 \) and \( im_2 \ ltioco_S sp_2 \). In order to prove \( im_1 \parallel im_2 \ ltioco_S sp_1 \parallel sp_2 \), we have to prove that \( \forall \xi \in \text{tstraces}_S(sp_1 \parallel sp_2) : \text{outs}_S(im_1 \parallel im_2 \text{after } \xi) \subseteq \text{outs}_S(sp_1 \parallel sp_2 \text{after } \xi) \). To prove this we first assume that Rule (3) of TIOLOTS composition (cf. Definition 9) results in becoming the respective output action instead of an internal action \( \tau \) and prove \( im_1 \parallel im_2 \ ltioco_S sp_1 \parallel sp_2 \) for this adjusted composition operator. Afterwards, we hide the output actions being generated by adjusted Rule (3) by replacing them with internal actions \( \tau \) such that we prove Theorem 2 for TIOLOTS composition as defined in Definition 9.

Let \( \mu \in \text{outs}_S(im_1 \parallel im_2 \text{after } \xi) \) such that, w.l.o.g., \( \mu \in \text{outs}_S(im_1 \text{after } \xi) \) with \( \text{outs}_S(im_1 \parallel im_2 \text{after } \xi) \subseteq \Sigma_0 \). Then, \( \mu \in \text{outs}_S(sp_1 \parallel sp_2 \text{after } \xi) \) as otherwise \( im_1 \) would have more output behavior than \( sp_1 \) such that \( im_1 \ ltioco_S sp_1 \) would not hold. Next, assume that \( \delta \in \text{outs}_S(im_1 \text{after } \xi) \). Then, it also holds that \( \delta \in \text{outs}_S(sp_1 \parallel sp_2 \text{after } \xi) \) if \( \exists \mu \in \Sigma_0 : \mu \in \text{outs}_S(im_2 \text{after } \xi) \). Otherwise, it also holds that \( \delta \not\in \text{outs}_S(im_2 \text{after } \xi) \) such that \( \delta \not\in \text{outs}_S(sp_1 \parallel sp_2 \text{after } \xi) \). The reasoning for \( \delta \) is analogous. Hence, \( im_1 \parallel im_2 \ ltioco_S sp_1 \parallel sp_2 \) with the adjusted Rule (3) as described above.

Next, we replace the adjusted Rule (3) by the original one to prove Theorem 2. Here, \( im' \) and \( sp' \) describe the adjusted variants of \( im_1 \parallel im_2 \) and \( sp_1 \parallel sp_2 \) where outputs of Rule (3) are hidden, i.e., replaced by \( \tau \). Additionally, let \( \xi' \in \text{tstraces}_S(sp') \) denote the ttrace corresponding to \( \xi \in \text{tstraces}_S(sp_1 \parallel sp_2) \). Assume, Theorem 2 does not hold. Then, there exists a \( \mu \neq \tau \) such that \( \mu \in \text{outs}_S(im_1 \parallel im_2 \text{after } \xi) \),
However, in order to lift \( k \)-bounded constraint by a difference greater than \( k \), we dictate how \( k \)-bounded actions related to TIOA switches (including \( \tau \)) implement every input \( i \in \Sigma_I \) for every state \( s \in S \) such that \( s_{sp_1} \stackrel{\ell}{\to} s_{sp_2} \Rightarrow s_{im_1} \stackrel{\ell}{\to} s_{im_2} \). This means, we dictate how \( im_1 \parallel im_2 \) should behave after \( \xi' \). Therefore, \( im' \) cannot have any additional output behaviors after \( \xi' \) not being in \( (sp' \after \xi') \). Hence, \( im_1 \parallel im_2 \text{lioco}_S sp_1 \parallel sp_2 \) and Theorem 2 is correct.

## 4.3 Symbolic Live Timed Input/Output Conformance Testing

Concerning the practical intractability of infinitely branching TIO LTS, zone graphs have been proposed as finite representation of TA semantics [18]. A zone graph \( (Z, \sim) \) of TIOA \( A \) consists of a transition relation \( \sim \) on a set \( Z \) of symbolic states by means of pairs \( (\ell, \varphi) \) of locations \( \ell \in L \) and zones \( \varphi \in B(C) \). A zone represents a (potentially infinite) maximum set \( D \) of clock valuations satisfying clock constraint \( \varphi \), where we assume zones in canonical form by requiring \( D \) to be closed under entailment (i.e., \( \varphi \) cannot be strengthened without changing \( D \)). We may write \( D \) as a synonym for \( \varphi \) and use the notations \( D^+ = \{ u + d \mid u \in D, d \in \mathbb{T} \} \) and \( R(D) = \{ [R \rightarrow 0]u \mid u \in D \} \). Although zone graphs \( (Z, \sim) \) are, again, not necessarily finite, an equivalent, finite zone graph \( (Z', \sim') \) can be obtained with \( \sim' \subseteq \sim \) by constructing an equivalent diagonal-free TA only containing atomic clock constraints of the form \( x \sim r \) [10], and (2) by constructing for this TA a \( k \)-bounded zone graph with all zones being bound by a maximum global clock ceiling \( k \) using \( k \)-normalization [37, 36]. Here, the basic idea of \( k \)-normalization is to set the value of \( k \) to the greatest constant appearing in any clock constraint in the TA. Then, we replace each difference constraint by a difference greater than \( k \) (i.e., a difference constraint stating that the difference is greater than \( k \)).

As zone-graph constructions from TA ignore switch labels, they are likewise applicable to TIOA. However, in order to lift \text{lioco}_5 to zone graphs of specifications \( \mathcal{A}_p \) and implementations \( \mathcal{A}_i \) given as TIOA, actions related to TIOA switches (including \( \tau \)) must be also included as labels for the respective transitions between the corresponding symbolic states. In contrast, symbolic transitions not corresponding to switches of the TIOA are labeled with the special void symbol \( \varepsilon \notin \Sigma \). We define input/output-labeled zone graph (IOLZG) representations of TIOA as follows.

**Definition 10 (IOLZG).** An IOLZG of TIOA \( A = (L, \ell_0, \Sigma_I, \Sigma_O, \rightarrow, I) \) is a tuple \( (Z', z_0, \Sigma_I, \Sigma_O, \sim) \), where

- \( Z' = L \times B(C) \) is a set of symbolic states with initial state \( z_0 = (\ell_0, D_0) \in Z' \).
- \( \Sigma_\tau = \Sigma_I \cup \Sigma_O \cup \{ \tau \} \) is a set of labels, and
- \( \sim \subseteq Z' \times (\Sigma_\tau \cup \{ \varepsilon \}) \times Z' \) is a symbolic transition relation being the least relation satisfying the following rules:

\[
(\ell, D) \xRightarrow{\delta} (\ell, D^+ \land I(\ell)) \quad \text{and} \quad (\ell, D) \xRightarrow{\delta} (\ell', R(D \land g) \land I(\ell')) \quad \text{if} \; \ell \xrightarrow{\delta, g, R} \ell'.
\]

Let \( (\ell, D) \in Z' \) be a symbolic state. We further use the following notations.

- \( (\ell, D) \xrightarrow{\delta} (\ell', R(D \land g) \land I(\ell')) \) if \( \exists u \in D : u \in g \land ([R \rightarrow 0](u + d)) \in R(D \land g) \land I(\ell') \),

- \( (\ell, D) \xrightarrow{(\delta, g, R)} (\ell', D') \) if \( \exists \ell', D' \in Z' : (\ell, D) \xrightarrow{\delta} (\ell', D') \),

- \( (\ell, D) \xrightarrow{(\delta_1, \delta_2, \ldots, \delta_n)} (\ell, D_n) \) if \( \exists (\ell_1, D_1), \ldots, (\ell_n, D_n) \in Z' : (\ell, D) \xrightarrow{(\delta_1, \delta_2, \ldots, \delta_n)} (\ell_n, D_n) \) with \( n \in \mathbb{N}_0 \).
\begin{itemize}
\item $\langle \ell, D \rangle$ is input-enabled iff $\forall i \in \Sigma_I, \forall d \in D : \exists \langle \ell', D' \rangle \in \mathcal{Z} : \langle \ell, D \rangle \xrightarrow{(d,i)} \langle \ell', D' \rangle \land d \in D$, and
\item $\langle \ell, D \rangle$ enables independent progress iff $\langle \forall d \in \Delta : \langle \ell, D \rangle \xrightarrow{d} \rangle$ or $\exists d, e \in \Sigma_0 : \langle \ell, D \rangle \xrightarrow{d \cdot e} $.
\end{itemize}

An IOLZG is input-enabled and enables independent progress if all its state do. Again, we obtain weak steps by replacing $\rightsquigarrow$ by $\Rightarrow$, where in both relations, $\epsilon$-steps are treated as unobservable. By $[\mathcal{A}]_x$, $x \in \{w,s\}$, we refer to the weak/strong IOLZG of TIOA $\mathcal{A}$, again, by possibly omitting $x$. In fact, $k$-normalization also applies to IOLZG, where switch labels may cause duplications of transitions but, however, do not affect the set of symbolic states. Hence, the correctness claim for zone graphs of TA (cf. [8]) also holds for IOLZG of TIOA.

**Theorem 3.** Let $s_0 = \langle \ell_0, u_0 \rangle$ be the initial state of TIOLTS $[\mathcal{A}]_S$ of TIOA $\mathcal{A}$ and $\langle \ell, \{u_0\} \rangle$ be the initial state of IOLZG $[\mathcal{A}]_x$.

- (Soundness) $\langle \ell_0, \{u_0\} \rangle \xrightarrow{k} \langle \ell, D \rangle$ implies $\langle \ell_0, u_0 \rangle \xrightarrow{\Delta} \langle \ell, u \rangle$ for all $u \in D$.
- (Completeness) $\langle \ell_0, u_0 \rangle \xrightarrow{\Delta} \langle \ell, u \rangle$ implies $\langle \ell_0, \{u_0\} \rangle \xrightarrow{k} \langle \ell, D \rangle$ such that $u \in D$.

**Proof.** The correctness of this proof directly follows from correctness of $k$-normalization [8] and the fact that labeled zone graphs connect the same symbolic states through transitions as zone graphs with the only difference being the labels of the labeled zone graphs (cf. [8] and Definition [10]). Furthermore, adding labels $\epsilon$ to transitions not corresponding to TIOA switches does not obstruct this result as these transitions are only use to apply operation $D^\uparrow$.

**Example 6.** Figure 6 shows an extract from the (k-normalized) IOLZG of the TIOA in Fig. 1a. Here, $k = 20$ is the largest constant appearing in all clock constraints such that every value of clocks $x$ larger than 20 falls into zone $x > 20$. The initial zone restricts all clock values to 0. Symbolic state $\langle idle, x \leq 20, x = y \rangle$ comprises all TIOLTS states being in location idle as long as $x \leq 20$ holds, and, similarly, for the symbolic states with location off. On reaching location as (add sugar), all clocks are reset. Symbolic state $\langle as, x \leq 10, y \leq 20, y - x \geq 10 \rangle$ thus aggregates all clock constraints of related TIOLTS runs.

As all TIOLTS states comprised in a symbolic state share the same visible behaviors (up to different clock valuations), IOLZG can be used as a basis for checking $\texttt{ltioco}_S$ between respective TIOA. In particular, if a zone of a symbolic state is downward-closed, outputs of that state are enforced as runs may not starve in that state. Correspondingly, we can lift all auxiliary definitions of $\texttt{ltioco}_S$ from TIOLTS to IOLZG (marked by index $\mathcal{Z}$). For $\texttt{out}_x$, we have to check for a given symbolic state reached by some $tstrace$ whether it is possible to extend the $tstrace$ by an output of that symbolic state such that the resulting extended $tstrace$ is still a valid $tstrace$. For instance, assume a simple IOLZG with $\langle \ell_0, x \geq 5 \rangle \xrightarrow{o} \langle \ell_1, x < 3 \rangle$: state $\langle \ell_0, x \geq 5 \rangle$ has output $o$ which is only enabled as long as $x < 3$ holds as the state reached...
by that output is \((\ell_1, x < 3)\). As the set of all valid extensions of \(traces\) by means of pairs of delays and subsequently enabled output actions of one symbolic state is, in general, infinite, they do not provide a reasonable basis for effectively checking \(ltioco_3\) on zone-graph representations of TIOA. However, a symbolic solution (i.e., comparing the timing constraints for output-action occurrences of symbolic states) is also not feasible for checking \(ltioco_4\) due to the (generally) unrelated names of locations and clocks of the two different TIOA under consideration. To solve this problem, we instead employ the notion of \(spans\) \([20]\): the span of clock \(c\) in zone \(D\) denotes the minimum time interval containing the minimum and maximum valuations of \(c\) enabled in \(D\). We use \(\infty\) to denote upward-open intervals (i.e., \(d < \infty\) for all \(d \in \mathbb{T}\)).

**Definition 11** (Span). Let \(D\) be a zone and \(c \in C\).

- \(span(c, D) = (lo, up) \in \mathbb{T} \times (\mathbb{T} \cup \{\infty\})\) is the minimal interval s.t. \(\forall u \in D : u(c) \geq lo \land u(c) \leq up\).
- \((lo, up) \preceq (lo', up') \iff lo \geq lo' \land up \leq up'\).
- \(span(D) = (lo, up) \iff \forall c \in C : (lo, up) \subseteq span(c, D) \land \exists c' : span(c', D) = (lo, up'), span(c'', D) = (lo', up')\).

Given a span \(sp = (lo, up)\), we write \(d \in sp\) for short if \(d \geq lo\) and \(d \leq up\) hold. Based on the notion of spans, we are able define span traces \((sp_1, \sigma_1), \ldots, (sp_n, \sigma_n)\) as sequences of pairs of spans and action occurrences denoting (maximum) sets of all valid timed traces \((d_1, \sigma_1), \ldots, (d_n, \sigma_n)\) of a given TIOA with equal untimed traces \(\sigma_1, \ldots, \sigma_n\) and \(d_i \in sp_i\) for \(1 \leq i \leq n\).

**Example 7.** A span trace of the TIOA in Fig.1\(\text{[d]}\) is, for instance, given as \(spt = ((20, \infty), ?press), ((0, 20), ?press), ((10, \infty), ?sugar)\). This span trace comprises all timed traces that first perform the invisible \(\tau\)-switch leading to location off after exactly 20 time units. The first visible step, performing output action ?press, then corresponds to the switch leading from location off back to location idle after at least 20 time units (due to the constraint of the \(\tau\)-switch). The second occurrence of output action ?press corresponding to the switch leading from location idle to location add sugar has to be performed at least 0 and at most 20 time units after the previous step. Afterwards, for the self-switch of location add sugar labeled ?sugar to be enabled, at least 10 time units must elapse.

Please note that the set of valid timed traces of a given untimed trace may not be representable by a single span trace (e.g., in case of non-deterministic TIOA). The minimal, yet complete set of span traces comprising all valid timed traces of a given TIOA \(\mathcal{A}\) can be defined with respect to the corresponding IOLZG representation of \(\mathcal{A}\) as follows.

**Definition 12** (Span Trace). Let \(\mathcal{A} = (L, \ell_0, \Sigma_l, \Sigma_O, \rightarrow, I)\) be a TIOA with IOLZG \((\mathcal{X}, z_0, \Sigma_l, \Sigma_O, \rightsquigarrow)\). By \(\Psi_\mathcal{X}\) we denote the set of span traces of \(\mathcal{A}\) being the least set such that \((sp_1, \sigma_1), \ldots, (sp_n, \sigma_n) \in \Psi_\mathcal{X} \iff z_0 \Rightarrow (d_1, \sigma_1) \ldots (d_i, \sigma_i)\), where \(d_i \in sp_i, 1 \leq i \leq n\).

We can show that the set of span traces derived from the IOLZG representation of a TIOA exactly comprises the set of timed traces of the respective TIOLTS representation of the TIOA.

**Lemma 4.** Let \(\mathcal{A} = (L, \ell_0, \Sigma_l, \Sigma_O, \rightarrow, I)\) be a TIOA with TIOLTS \((S, s_0, \Sigma_l, \Sigma_O, \rightsquigarrow)\). Then it holds that \((sp_1, \sigma_1), \ldots, (sp_n, \sigma_n) \in \Psi_\mathcal{X} \iff s_0 \xrightarrow{\ell_0} \sigma_1 \ldots \xrightarrow{\ell_n} \sigma_n\), where \(d_i \in sp_i, 1 \leq i \leq n\).

**Proof.** Let \(\mathcal{A} = (L, \ell_0, \Sigma_l, \Sigma_O, \rightarrow, I)\) be a TIOA with TIOLTS \((S, s_0, \Sigma_l, \Sigma_O, \rightsquigarrow)\) and IOLZG \((\mathcal{X}, z_0, \Sigma_l, \Sigma_O, \rightsquigarrow)\). In order to prove \((sp_1, \sigma_1), \ldots, (sp_n, \sigma_n) \in \Psi_\mathcal{X} \Rightarrow s_0 \xrightarrow{\ell_0} \sigma_1 \ldots \xrightarrow{\ell_n} \sigma_n\) with \(d_i \in sp_i, 1 \leq i \leq n\), we prove (1) \((sp_1, \sigma_1), \ldots, (sp_n, \sigma_n) \in \Psi_\mathcal{X} \Rightarrow s_0 \xrightarrow{\ell_0} \sigma_1 \ldots \xrightarrow{\ell_n} \sigma_n\) and (2) \(s_0 \xrightarrow{\ell_0} \sigma_1 \ldots \xrightarrow{\ell_n} \sigma_n\) with \(d_i \in sp_i, 1 \leq i \leq n\) ⇒ \((sp_1, \sigma_1), \ldots, (sp_n, \sigma_n) \in \Psi_\mathcal{X}\) separately.
(1) It holds by Def. 12 that \((sp_1, \sigma_1), \ldots, (sp_n, \sigma_n) \in \Psi_\mathcal{Z} \iff z_0 \xrightarrow{(d_i, \sigma_i)-(d_i, \sigma_i)} \) with \(d_i \in sp_i, 1 \leq i \leq n\). Furthermore, \(\langle \ell, D \rangle \xrightarrow{d} \langle \ell', R(D \land g) \land I(\ell') \rangle\) if \(\exists u \in D : u \in g \land (\langle R \Rightarrow 0 \rangle(u + d)) \in R(D \land g) \land I(\ell')\) and \(\langle \ell, D \rangle \xrightarrow{d} \) if \(\exists \langle \ell', D' \rangle \in \mathcal{Z} : \langle \ell, D \rangle \xrightarrow{d} \langle \ell', D' \rangle \) by Def. 10. Here, it directly follows that \((sp_1, \sigma_1), \ldots, (sp_n, \sigma_n) \in \Psi_\mathcal{Z} \Rightarrow s_0 \xrightarrow{d_1, \sigma_1} \ldots \xrightarrow{d_n, \sigma_n}\).

(2) From Def. 10 and Theorem 8 it follows that for all \(s_0 \xrightarrow{d_1, \sigma_1} \ldots \xrightarrow{d_n, \sigma_n}\) there exists a \(z_0 \xrightarrow{(d_i, \sigma_i)-(d_i, \sigma_i)}\). Additionally, it holds by Def. 12 that \((sp_1, \sigma_1), \ldots, (sp_n, \sigma_n) \in \Psi_\mathcal{Z} \iff z_0 \xrightarrow{(d_i, \sigma_i)-(d_i, \sigma_i)} \) with \(d_i \in sp_i, 1 \leq i \leq n\). Here, it directly follows that \(s_0 \xrightarrow{d_1, \sigma_1} \ldots \xrightarrow{d_n, \sigma_n}\) with \(d_i \in sp_i, 1 \leq i \leq n\). Hence, it holds that \((sp_1, \sigma_1), \ldots, (sp_n, \sigma_n) \in \Psi_\mathcal{Z} \iff s_0 \xrightarrow{d_1, \sigma_1} \ldots \xrightarrow{d_n, \sigma_n}\) with \(d_i \in sp_i, 1 \leq i \leq n\). □

Based on this result, we are able to lift \(ltioco\) from TIO LTS (see Def. 8) to the level of IOLZG and span traces. First, defining the two different notions of quiescence on symbolic states of IOLZG is straightforward. In contrast, the \(after_\mathcal{Z}\) set has now to be redefined in a recursive manner to consecutively traverse span traces \(\xi\) instead of timed traces. In particular, the set of symbolic states \(\langle \ell, D \rangle\) reachable after \(\xi\) is given as the set of symbolic states reachable by all possible sequences of timed steps comprised in \(\xi\). In a similar way, the set of \(s\) reachable \(lsp\) traces \(\langle \ell, D \rangle\) can be defined for a symbolic state \(\langle \ell, D \rangle\) of an IOLZG as the least set of span traces comprising all possible timed traces. Those traces are additionally equipped by special quiescence output symbols \(\delta_E\) and \(\delta_I\) to mark occurrences of (enforced or safe) suspension. Thereupon, the \(out_\mathcal{Z}\) set can be defined as the set of all output behaviors (i.e., pairs \((sp, a)\) of spans \(sp\) and output actions \(a\) including quiescence) being enabled in all symbolic states reachable from state \(\langle \ell, D \rangle\) via span trace \(\xi\) such that \(\xi \cdot (sp, a)\), again, forms a valid span trace. We further define the set \(out_\mathcal{Z}(\mathcal{Z}', \xi)\) to contain the \(out_\mathcal{Z}\) sets reachable from sets \(\mathcal{Z}'\) of symbolic states via span trace \(\xi\). In case of multiple output behaviors (e.g., \((sp, a)\) and \((sp', a')\)) with equal output actions \(a\), but different spans \(sp, sp'\), we implicitly unify overlapping spans by requiring the set \(out_\mathcal{Z}(\mathcal{Z}', \xi)\) to be minimal. Finally, we are able to define \(ltioco_\mathcal{Z}\) almost in the usual way, where \(\subseteq\) is used instead of \(\subseteq\) to state that all output behaviors (i.e., sets \(spa\) of pairs \((sp, a)\) of spans and output actions) of the implementation are subsumed by those of the specification.

**Definition 13.** Let \(sp, im\) be IOLZG over \(S = \Sigma I \cup \Sigma O, \gamma \in \{S, E\}, \langle \ell, D \rangle \in \mathcal{Z}, \mathcal{Z}' \subseteq \mathcal{Z}, \text{ and } \xi \in (\mathcal{T}_C \times (\mathcal{T}_C \cup \{\infty\})) \times (\Sigma \cup \{\delta_T\})\):

- \(\langle \ell, D \rangle\) is safe-quiescent, denoted by \(\delta_S(\langle \ell, D \rangle)\), iff \(\forall d \in D : \langle \ell, D \rangle \xrightarrow{d}\).
- \(\langle \ell, D \rangle\) is enforced-quiescent, denoted by \(\delta_E(\langle \ell, D \rangle)\), iff \(\forall \mu \in \Sigma O, \forall d \in D : \langle \ell, D \rangle \xrightarrow{(d, \mu)}\).
- \(\langle \ell, D \rangle\) after_\mathcal{Z} is the greatest set satisfying the following rules:
  - \(\langle \ell, D \rangle \in (\langle \ell, D \rangle\) after_\mathcal{Z}\) and
  - \(\langle \ell, D \rangle \in (\langle \ell', D' \rangle after_\mathcal{Z}(sp, a) \cdot \xi''\rangle\) if \(\exists d \in D : \langle \ell', D' \rangle \xrightarrow{(d, a)} \langle \ell'', D'' \rangle \land \langle \ell, D \rangle \in (\langle \ell'', D'' \rangle after_\mathcal{Z} \cdot \xi''\rangle),\)
- \(spraces(\langle \ell, D \rangle)\) is the least set s.t. \((sp_1, \sigma_1), \ldots, (sp_n, \sigma_n) \in spraces(\langle \ell, D \rangle) \iff (\ell, D) \xrightarrow{d} \) where \(d_i \in sp_i, 1 \leq i \leq n, \text{ and } \forall \langle \ell', D' \rangle \in \mathcal{Z} : \langle \ell', D' \rangle \xrightarrow{d} \langle \ell', D' \rangle \iff \delta_T(\langle \ell', D' \rangle)\),
- \(out_\mathcal{Z}(\langle \ell, D \rangle, \xi) \subseteq (\mathcal{T}_C \times (\mathcal{T}_C \cup \{\infty\})) \times (\Sigma I \cup \Sigma O \cup \{\delta_T\})\) is the greatest set s.t. \((sp, o) \in out_\mathcal{Z}(\langle \ell, D \rangle, \xi)\) if \(\langle \ell, D \rangle \xrightarrow{\delta_T} \land \xi \cdot (sp, o) \in spraces(z_0) \land o \in \Sigma O \cup \{\delta_T\}\).
• \( \overline{\text{out}}_x(2', \xi) \) is the least set s.t. \( \forall (sp, o) \in \bigcup_{x \subseteq \mathcal{L}} \text{out}_x(z, \xi) : (sp', o) \in \overline{\text{out}}_x(2', \xi) : sp \preceq sp' \), 

• \( \text{im}_\mathcal{L} \text{tioco}_x sp : \iff \forall \xi \in \text{sptraces}(sp) : \overline{\text{out}}_x(\text{im}_\mathcal{L} \text{after}_x sp, \xi, \xi) \subseteq \overline{\text{out}}_x(sp \text{after}_x sp, \xi, \xi) \), where \( \text{spa} \subseteq \text{spa}' \iff \forall (sp, o) \in \text{spa} : \exists (sp', o) \in \text{spa}' : sp \preceq sp' \).

Example 8. Considering the running example in Figs. 1a and 2b, we observe that \( [\mathcal{L}1] \text{tioco}_x [\mathcal{L}2] \) does not hold. Let \( \xi = ((20, \infty), \text{press}), (0, 20), \text{press}) \). Then \( ((0, \infty), \delta_S) \in \overline{\text{out}}_x([\mathcal{L}1] \text{after}_x sp, \xi, \xi) \) and \( ((0, \infty), \delta_S) \notin \overline{\text{out}}_x([\mathcal{L}1] \text{after}_x sp, \xi, \xi) \) as it is not safe to wait in add sugar of \( \mathcal{L}_2 \) due to the invariant \( y \leq 15 \).

Finally, we prove that for any two TIOA \( \mathcal{A}_{\text{im}} \) and \( \mathcal{A}_{sp} \), checking \text{tioco}_x on IOLZG is equivalent to checking \text{lioco}_S on TIO LTS.

Theorem 4 (Correctness of \text{tioco}_x). Let \( \mathcal{A}_{\text{im}} \) and \( \mathcal{A}_{sp} \) be TIOA.

\[
[\mathcal{A}_{\text{im}}] \text{tioco}_x [\mathcal{A}_{sp}] : \iff [\mathcal{A}_{\text{im}}] \text{lioco}_S [\mathcal{A}_{sp}]
\]

Proof. Let \( \mathcal{A}_{\text{im}} \) and \( \mathcal{A}_{sp} \) be TIOA. Lemma 4 shows that \( (sp_1, \sigma_1), \ldots, (sp_n, \sigma_n) \in \Psi_x \iff s_0 \downarrow \sigma_1 \ldots \downarrow \sigma_n \), with \( d_i \in sp_i, 1 \leq i \leq n \). Hence, \( (sp_1, \sigma_1), \ldots, (sp_n, \sigma_n) \in \text{sptraces}([\mathcal{A}_{sp}]_x) \iff (d_1, a_1), \ldots, (d_n, a_n) \in tstraces_L([\mathcal{A}_{sp}]_x) \) with \( d_i \in sp_i, 1 \leq i \leq n \) as applying symbols \( \delta_S \) and \( \delta_R \) to the sets of tstraces\(_L\) and sptraces is done in the same manner (cf. Defs. 8 and 13). It remains to be shown that \( (d, o) \in \text{out}_S([\mathcal{A}_{sp}]_x) \) \( \text{after}(d_1, a_1), \ldots, (d_n, a_n) \) \( (sp, o) \in \text{out}_x([\mathcal{A}_{sp}]_x) \text{after}_x (sp_1, a_1), \ldots, (sp_n, a_n) \) \( \) with \( d \in sp \) and \( d_i \in sp_i, 1 \leq i \leq n \). This directly follows from the first part of this proof as, by definition, \( (d, o) \in \text{out}_S([\mathcal{A}_{sp}]_x) \text{after}(d_1, a_1), \ldots, (d_n, a_n) \iff (d_1, a_1), \ldots, (d_n, a_n) \in tstraces_L \). Hence, it holds that \( [\mathcal{A}_{\text{im}}] \text{tioco}_x [\mathcal{A}_{sp}]_x \iff [\mathcal{A}_{\text{im}}] \text{lioco}_S [\mathcal{A}_{sp}]_x \).

From Theorems 1 and 4 it also follows that \text{lioco}_x is sound with respect to \text{lioco}_S and from Theorems 2 and 4 it follows that \text{lioco}_x is a preorder on input-enabled IOLZG. Finally, we can likewise conclude compositionality of \text{lioco}_x.

Corollary 1. Let \( \text{im}_1 \) and \( \text{im}_2 \) as well as \( sp_1 \) and \( sp_2 \) be input-enabled and composable TIOA enabling independent progress. Then \( ([\text{im}_1]_x \text{tioco}_x [sp_1]_x) \land ([\text{im}_2]_x \text{tioco}_x [sp_2]_x) \Rightarrow [\text{im}_1]_x \parallel [\text{im}_2]_x \text{tioco}_x [sp_1]_x \parallel [sp_2]_x \).

5 Tool Support

To show practical feasibility of our technique, we implemented a tool based on the concepts of the JTorX tool [6, 42], originally being developed for (untimed) \text{ioco} testing. Similar to JTorX, our tool supports online white-box testing: a running implementation is investigated on-the-fly whether it is conforming to a specification both given as TIOA. Our tool supports a generic interface enabling it to be used for checking any kind of implementation (in the current version, the interface is implemented to accept TIOA models as implementation). To check conformance of a given implementation to a specification, the tool checks \text{lioco}_x on the labeled zone-graph representations of both TIOA models. As input TIOA models, our tools supports the exchange format of UPPAAL [29] (a mature model checker for timed systems).

Internally, our tool uses Difference Bound Matrices (DBM) being an efficient representation of zones [7, 18, 8]. In particular, DBM-based representations of zones provide comparison operators \( \sim \in \{<, \leq, =, \geq, >\} \). For a consistent representation, a fresh clock \( 0_C \) (with constant value zero) is introduced resulting in the set of clocks \( \mathcal{C}_0 = \mathcal{C} \cup \{0_C\} \) in which each clock is aligned to \( 0_C \). Based
on this construction, atomic clock constraints of the form \( x \sim r \) can be represented as \( x - y \leq r \) with \( \leq \in \{<,\leq\} \). Hence, every zone \( D \in \mathcal{C}_0 \) can be represented with a maximum of \( |\mathcal{C}_0|^2 \) atomic clock constraints, and therefore, each zone may be described as a matrix of size \( |\mathcal{C}_0| \times |\mathcal{C}_0| \) [8]. Each entry \( D_{i,j} \) (row \( i \), column \( j \)) thus refers to the atomic clock constraint \( x_i - x_j \leq r_{i,j} \). Hence, entries of the matrix are pairs of difference values \( r_{i,j} \) and comparison operators in \( \leq \), being derived as follows. For every entry \( D_{i,j} \), we set the value \( r_{i,j} \) such that \( x_i - x_j \leq r_{i,j} \) holds. If a difference is unbounded (i.e., \( x_i \) and \( x_j \) are not related by any constraint), we set the value to \( r_{i,j} = \infty \). Additionally, we have to require clocks to have non-negative values (i.e., \( 0 \leq x \)).

Example 9. 

Figure 7 depicts the DBM for the zone \( \langle 1 \leq x \leq 2, y \leq 2 \rangle \). For instance, \( D_{x,y} = D_{y,x} = \infty \) as \( x \) and \( y \) are not related by a comparison. Additionally, \( D_{0,C,x} = (-1, \leq) \) as \( 1 \leq x \leq 2 \) such that \( 0 - x \leq -1 \). Furthermore, \( D_{x,0,C} = 2 \) due to \( x \leq 2 \).

The tool is available online at [https://www.es.tu-darmstadt.de/ltioco](https://www.es.tu-darmstadt.de/ltioco).

### 6 Related Work

Several versions of \texttt{tioco} have recently been proposed [38 14 24 26 27], whereas \texttt{ltioco} is, to the best of our knowledge, the first approach working on the symbolic thus finite zone-graph representation of TIOA instead of infinitely branching TIOLTS. The only other existing symbolic variant of \texttt{tioco} is based on symbolic timed automata with data variables, but does neither include quiescence nor ensure finiteness of the state space [40]. In addition, our novel notions of timed quiescence are different from any existing approach, where absence of outputs is either considered only up to a fixed bound \( M \) [14 24], or for all possible delays [38 27]. Recent tools implementing variants of \texttt{tioco} [28 12 26] also mostly differ in their interpretation of quiescence which can all be simulated in our framework, but not vice versa. Moreover, neither of these approaches distinguishes safe from enforced quiescence as done in our approach.

In addition, compositionality properties have only been considered in [5] so far, where again no notion of quiescence is considered. Furthermore, there are techniques for test-generation from TIOA models. In order to handle infinitely branching state spaces, En-Nouaary and Dssouli [19] derive test cases only for a particular subset of TIOA behaviors, whereas, similar to our approach, Brandán Briones and Röhl [15] use a zone-based representation. However, the latter approach is limited to deterministic TA, which are strictly less expressive than our TIOA. Springintveld et al. [39] propose an algorithm for exhaustive black-box test generation for timed systems, but no notions of quiescence are taken into account.

Besides adopting \texttt{ioco}-like conformance notions to timed systems as done by the different variants of \texttt{tioco}, the only other timed implementation-relation theory we are aware of uses a refinement-based implementation relation [17]. Moreover, Bornot et al. [13] investigate requirements for ensuring liveness-by-construction of timed systems using trace-based composition operators for TIOLTS, whereas conformance theories are out of scope.
Finally, there are several other \textit{ioco}-based testing theories. Among others, \textit{mioco} \cite{33, 32, 31} (i.e., \textit{ioco} for modality-based systems) distinguishes optional transition (which may be implemented) from mandatory transitions (which must be implemented). Furthermore, \textit{featured-ioco} \cite{9} is based on so-called featured transition systems, incorporating feature constraints to to restrict which (pairs of) transitions may be part of the same variant. However, none of these approaches considers real-time constraints.

7 Conclusion

We presented an improved version of a timed input/output conformance testing relation, called \textit{ltioco}, to ensure not only safe but also \textit{live} behaviors of implementations with time-critical behaviors modeled as TIOA. Additionally, we investigated compositionality properties of \textit{ltioco} and we extended the construction of zone graphs to check \textit{ltioco} on a finite semantic representation of TIOA. As a future work, we plan to enrich our framework by further operators including quotienting and conjunction as well as refinement \cite{refinement} and to extend our tool implementation by automated test-generation and test-execution capabilities. Furthermore, we plan to evaluate our approach by applying our tool to a number of well-known case studies (e.g., \cite{25, 21, 30}).

References

[1] Luca Aceto, Augusto Burgueño & Kim G. Larsen (1998): \textit{Model Checking via Reachability Testing for Timed Automata}, pp. 263–280. Springer Berlin Heidelberg, doi:10.1007/3-540-14531-2_12

[2] Rajeev Alur & David L. Dill (1990): \textit{Automata for Modeling Real-Time Systems}. In Michael S. Paterson, editor: \textit{ICALP’90}. Springer Berlin Heidelberg, pp. 322–335, doi:10.1007/3-540-93661-9_25

[3] Rajeev Alur & David L. Dill (1994): \textit{A theory of timed automata}. \textit{Theoretical Computer Science} 126(2), pp. 183–235, doi:10.1016/0304-3975(94)90010-8

[4] Étienne André (2016): \textit{What’s decidable about parametric timed automata?}. In Cyril Artho & Peter Csaba Ölveczky, editors: \textit{FTSCS’16}, Springer International Publishing, pp. 52–68, doi:10.1007/978-3-319-29510-7_3

[5] Boutheina Bannour, Christophe Gaston, Marc Aiguier & Arnault Lapitre (2013): \textit{Results for Compositional Timed Testing}. In: \textit{APSEC’13}, IEEE, pp. 559–564, doi:10.1109/APSEC.2013.81

[6] Axel Belinfante (2010): \textit{JToX: A Tool for On-Line Model-Driven Test Derivation and Execution}, pp. 266–270. Springer Berlin Heidelberg, doi:10.1007/978-3-642-12002-2_21

[7] Richard Bellman (1957): \textit{Dynamic Programming}. Princeton University Press.

[8] Johan Bengtsson & Wang Yi (2004): \textit{Timed Automata: Semantics, Algorithms and Tools}, pp. 87–124. Springer Berlin Heidelberg, doi:10.1007/0-387-22900-6_4

[9] Harsh Beohar & Mohammad Reza Mousavi (2016): \textit{Input–output conformance testing for software product lines}. \textit{Journal of Logical and Algebraic Methods in Programming} 85(6), pp. 1131–1153, doi:10.1016/j.jlamp.2016.09.007

[10] Béatrice Bérard, Antoine Petit, Volker Diekert & Paul Gastin (1998): \textit{Characterization of the expressive power of silent transitions in timed automata}. \textit{Fundamenta Informaticae} 36(2,3), pp. 145–182, doi:10.3233/FI-1998-36233

[11] Gilles Bernot (1991): \textit{Testing against formal specifications: A theoretical view}, pp. 99–119. Springer Berlin Heidelberg, doi:10.1007/3-540-539816_63
[12] Henrik Bohnenkamp & Axel Belinfante (2005): *Timed Testing with TorX*, pp. 173–188. Springer Berlin Heidelberg, doi:10.1007/11526841_13

[13] Sébastien Bornot, Gregor Gößler & Joseph Sifakis (2000): *On the Construction of Live Timed Systems*, pp. 109–126. Springer Berlin Heidelberg, doi:10.1007/3-540-46419-0_9

[14] Laura Brandán Briones & Ed Brinksma (2004): *A Test Generation Framework for quiescent Real-Time Systems*. In: *FATES, LNCS 3395*, Springer Berlin Heidelberg, pp. 64–78, doi:10.1007/978-3-540-31848-4_5

[15] Laura Brandán Briones & Mathias Röhl (2005): *Test Derivation from Timed Automata*, pp. 201–231. Springer Berlin Heidelberg, doi:10.1007/11498490_10

[16] Manfred Broy, Bengt Jonsson, Joost-Pieter Katoen, Martin Leucker & Alexander Pretschner (2005): *Model-Based Testing of Reactive Systems: Advanced Lectures*. LNCS 3472, Springer Berlin Heidelberg.

[17] Alexandre David, Kim G. Larsen, Axel Legay, Ulrik Nyman & Andrzej Wasowski (2010): *Timed I/O Automata: A Complete Specification Theory for Real-time Systems*. In: *HSCC’10*, ACM, pp. 91–100, doi:10.1145/1755952.1755967

[18] David L. Dill (1990): *Timing Assumptions and Verification of Finite-State Concurrent Systems*. In Joseph Sifakis, editor: *International Workshop on Automatic Verification Methods for Finite State Systems*, Springer Berlin Heidelberg, pp. 197–212, doi:10.1007/3-540-52148-8_17

[19] Abdeslam En-Nouaary & Rachida Dssouli (2003): *A Guided Method for Testing Timed Input Output Automata*. In Dieter Hogrefe & Anthony Wiles, editors: *ICTSS’03*, Springer Berlin Heidelberg, pp. 211–225, doi:10.1007/3-540-44830-6_16

[20] Shibashis Guha, Chinmay Narayan & S. Arun-Kumar (2012): *On Decidability of Prebisimulation for Timed Automata*. In: *CAV’12, LNCS 7358*, Springer, pp. 444–461, doi:10.1007/978-3-642-31424-7_33

[21] Thomas A. Henzinger, Zohar Manna & Amir Pnueli (1991): *Temporal Proof Methodologies for Real-time Systems*. In: Proceedings of the 18th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL’91, ACM, pp. 353–366, doi:10.1145/99583.99629

[22] Thomas A. Henzinger, Xavier Nicollin, Joseph Sifakis & Sergio Yovine (1994): *Symbolic Model Checking for Real-Time Systems*. *Information and Computation* 111(2), pp. 193–244, doi:10.1006/inco.1994.1045

[23] Anders Hessel, Kim G. Larsen, Marius Mikucionis, Brian Nielsen, Paul Pettersson & Arne Skou (2008): *Testing Real-Time Systems Using UPPAAL*, pp. 77–117. Springer Berlin Heidelberg, doi:10.1007/978-3-540-78917-8_3

[24] Kim G. Larsen, Marius Mikucionis, Brian Nielsen & Arne Skou (1997): *UPPAAL in a nutshell*. *International Journal on Software Tools for Technology Transfer* 1(1), pp. 109–126, doi:10.1007/1086228.108623

[25] Henrik Ejersbo Jensen, Kim G. Larsen & Arne Skou (1996): *Modelling and Analysis of a Collision Avoidance Protocol using SPIN and UPPAAL*. In: DIMACS’96.

[26] Moez Krichen & Stavros Tripakis (2004): *Black-box conformance testing for real-time systems*. In: *SPIN’04*, Springer Berlin Heidelberg, pp. 79–94, doi:10.1007/978-3-540-31848-4_6

[27] Kim G. Larsen, Marius Mikucionis & Brian Nielsen (2005): *Testing Real-time Embedded Software Using UPPAAL-TRON: An Industrial Case Study*. In: *EMSOFT’05*, ACM, pp. 299–306, doi:10.1145/1086228.1086283

[28] Kim G. Larsen, Paul Pettersson & Wang Yi (1997): *UPPAAL in a nutshell*. *International Journal on Software Tools for Technology Transfer* 1(1), pp. 134–152, doi:10.1007/s100090050010

[29] Magnus Lindahl, Paul Pettersson & Wang Yi (2001): *Formal design and analysis of a gear controller*. *STTT* 3(3), pp. 353–368, doi:10.1007/BFb0054178

[30] Lars Luthmann, Stephan Mennicke & Malte Lochau (2015): *Towards an I/O Conformance Testing Theory for Software Product Lines based on Modal Interface Automata*. In: *FMSPL’15*, EPTCS 182, arXiv, pp. 1–13, doi:10.4204/EPTCS.182.1
[32] Lars Luthmann, Stephan Mennicke & Malte Lochau (2016): *Compositionality, Decompositionality and Refinement in Input/Output Conformance Testing*, pp. 54–72. Springer International Publishing, doi:10.1007/978-3-319-57666-4_5

[33] Lars Luthmann, Stephan Mennicke & Malte Lochau (2019): *Unifying modal interface theories and compositional input/output conformance testing*. *Science of Computer Programming* 172, pp. 27–47, doi:10.1016/j.scico.2018.09.008.

[34] Nancy A. Lynch & Hagit Attiya (1992): *Using mappings to prove timing properties*. *Distributed Computing* 6(2), pp. 121–139, doi:10.1007/BF02252683.

[35] Michael Merritt, Francesmary Modugno & Mark R. Tuttle (1991): *Time-constrained automata*. In Jos C. M. Baeten & Jan F. Groote, editors: *International Conference on Concurrency Theory*, Springer, pp. 408–423, doi:10.1007/3-540-54430-5_103.

[36] Paul Pettersson (1999): *Modelling and Verification of Real-Time Systems Using Timed Automata: Theory and Practice*. Ph.D. thesis.

[37] Tomas G. Rokicki (1994): *Representing and Modeling Digital Circuits*. Ph.D. thesis.

[38] Julien Schmaltz & Jan Tretmans (2008): *On Conformance Testing for Timed Systems*. *Formal Modeling and Analysis of Timed Systems*, pp. 250–264, doi:10.1007/978-3-540-85778-5_18

[39] Jan Springintveld, Frits W. Vaandrager & Pedro R. D’Argenio (2001): *Testing timed automata*. *Theoretical Computer Science* 254(1), pp. 225–257, doi:10.1016/S0304-3975(99)00134-6

[40] Sabrina von Styp, Henrik Bohnenkamp & Julien Schmaltz (2010): *A Conformance Testing Relation for Symbolic Timed Automata*. In Krishnendu Chatterjee & Thomas A. Henzinger, editors: *FORMATS’10*, Springer Berlin Heidelberg, pp. 243–255.

[41] Jan Tretmans (1996): *Test Generation with Inputs, Outputs and Repetitive Quiescence*. Available at http://doc.utwente.nl/65463.

[42] Jan Tretmans & Ed Brinksma (2003): *TORX: Automated Model-Based Testing*, pp. 31–43.