Timed I/O Automata: A Complete Specification Theory for Real-time Systems

Alexandre David
Computer Science
Aalborg University, Denmark
adavid@cs.aau.dk

Kim G. Larsen
Computer Science
Aalborg University, Denmark
kgl@cs.aau.dk

Axel Legay
INRIA/IRISA
Rennes Cedex, France
axel.legay@irisa.fr

Ulrik Nyman
Computer Science
Aalborg University, Denmark
ulrik@cs.aau.dk

Andrzej Wąsowski
IT University
Copenhagen, Denmark
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 implemented on top of an engine for timed games, UPPAAL-Tiga, and illustrated with a small case study.

Categories and Subject Descriptors
F.3.1 [Specifying and Verifying and Reasoning about Programs]

General Terms
Theory, Verification

1. INTRODUCTION
Many modern systems are big and complex assemblies of numerous components. The components are often designed by independent teams, working under a common agreement on what the interface of each component should be. Consequently, compositional reasoning [20], the mathematical foundations of reasoning about interfaces, is an active research area. It supports inferring properties of the global implementation, or designing and advisedly reusing components.

In a logical interpretation, interfaces are specifications and components that implement an interface are understood as models/implementations. Specification theories should support various features including (1) refinement, which allows to compare specifications as well as to replace a specification by another one in a larger design, (2) logical conjunction expressing the intersection of the set of requirements expressed by two or more specifications, (3) structural composition, which allows to combine specifications, and (4) last but not least, a quotient operator that is dual to structural composition. 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 [13].

Building good specification theories is the subject of intensive studies [10, 12]. One successfully promoted direction is the one of interface automata [12, 13, 22, 28]. In this framework, an interface is represented by an input/output automaton [26], 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 [26], 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. In [15], a timed extension of the theory of interface automata has been introduced, motivated by the fact that time can be a crucial parameter in practice, for example in embedded systems. While [15] focuses mostly on structural composition, in this paper we go one step further and build what we claim to be the first game-based specification theory for timed systems.

Component Interface specification and consistency. We represent specifications by timed input/output transition systems [21], i.e., timed transitions systems whose sets of discrete transitions are split into Input and Output transitions. Contrary to [15] and [21] 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
Refinement and logical conjunction. A specification $S_1$ refines a specification $S_2$ if 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 [12]. In our timed extension, checking such simulation can be done with a slight modification of the theory proposed in [6]. 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. 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 [15], specifications interact by synchronizing on inputs and outputs. However, like in [21, 26], 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 [21, 26], input-enabledness, shall not be seen as a way to avoid error states. Indeed, such error states can be designated by the designer as states which do not warrant desirable temporal properties. Here, in checking for compatibility of the composition of specifications, one tries to synthesize a strategy for the inputs to avoid the error states, i.e., an environment in which the components can be used together in a safe way. Our composition operator is associative and the 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 has been implemented as an extension of UPFAAL-TIGA [3]. 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 both consistency and compatibility checking to be solved using the zone-based algorithms for synthesizing winning strategies in timed games [27, 8]. Finally, refinement between specifications is checked using a variant of the recent efficient game-based algorithm of [6].

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 patent applications filed. Clearly one would expect that the number (and size) of grants given to a university has a (positive) influence on the amount of patents filed for.

2. SPECIFICATIONS & REFINEMENT

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) [18], and enriched with 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 TIOTs does not rely in any way on the TIOAs representation - one can build TIOTs 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 I/O Transition System (TIOTS) is a tuple $S = (S_0, S, \Sigma^0, \Sigma, s_0, Z, Z_0)$, where $S_0$ is an infinite set of states, $s_0 \in S_0$ is the initial state, $\Sigma^0 = \Sigma^0 \cup \Sigma_0^0$ is a finite set of actions partitioned into inputs ($\Sigma^I$) and outputs ($\Sigma^O$), and $Z = Z \cup \Sigma^I \times Z \cup \Sigma^O \times \Sigma^I \times Z$ is a transition relation. We write $Z(s,s') \in Z$ instead of $(s,s') \in Z$ and use $\{s\}, \{s\}$ and $d$ to range over inputs, outputs and $R \geq 0$ respectively. In addition any TIOTS satisfies the following:

- **[time determinism]** whenever $s \xrightarrow{\Sigma} s'$ and $s \xrightarrow{\Sigma} s''$ then $s' = s''$.
- **[time reflexivity]** $s \xrightarrow{\Sigma} s$ for all $s \in S$.
- **[time additivity]** for all $s, s', s'' \in S$ and all $d_1, d_2 \in R > 0$ we have $s \xrightarrow{d_1 + d_2} s''$ if $s \xrightarrow{d_1} s'$ and $s' \xrightarrow{d_2} s''$ for an $s' \in S$.

In the interest of simplicity, we work with deterministic TIOTSs: for all $a \in \Sigma \cup R > 0$ whenever $s \xrightarrow{\Sigma} s'$ and $s \xrightarrow{\Sigma} s''$, we have $s' = s''$ (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 $X$, write

\[
\text{pred}^0_S(X) = \{s \in S \mid \exists s' \in X, s \xrightarrow{\Sigma} s'\}
\]

for the set of all $a$-predecessors of states in $X$. We write $\text{ipred}^0_S(X)$ for the set of all input predecessors, and $\text{opred}^0_S(X)$ for all the output predecessors of $X$:

\[
\text{ipred}^0_S(X) = \bigcup_{a \in \Sigma^I} \text{pred}^0_S(X)
\]

\[
\text{opred}^0_S(X) = \bigcup_{a \in \Sigma^O} \text{pred}^0_S(X).
\]

Also $\text{post}^0_{S,d_0}(s)$ is the set of all time successors of a state $s$ that can be reached by delays smaller than $d_0$:

\[
\text{post}^0_{S,d_0}(s) = \{s' \in S \mid \exists d \in [0, d_0], s \xrightarrow{d} s'\}
\]

We shall now introduce a finite symbolic representation for TIOTSs in terms of Timed I/O Automata (TIOAs). Let $\text{Clk}$ be a finite set of clocks. A clock valuation over $\text{Clk}$ is a mapping $u \in [\text{Clk} \mapsto R_{\geq 0}]$. We write $u + d$ to denote a valuation such that for any clock $r$ we have $(u + d)(r) = x + d$ iff $u(r) = x$. Given $d \in R_{\geq 0}$, we write $u[r \mapsto 0]_{\leq d}$ for a valuation which agrees with $u$ on all values for clocks not in $c$, and returns 0 for all clocks in $c$. Let $\text{op}$ be the set of relational operators: $\text{op} = \{\lt, \leq, \geq\}$. A guard over $\text{Clk}$ is a finite conjunction of expressions of the form $x < n$, where $x$ is a relational operator and $n \in N$. We write $B(\text{Clk})$ for the set of guards over $\text{Clk}$ using operators in the set $\text{op}$. We also write $\mathcal{P}(X)$ for the power set of a set $X$.

**Definition 2.** A Timed I/O Automaton (TIOA) is a tuple $A = (\text{Loc}, q_0, \text{Clk}, E, \text{Act}, \text{Inv})$ where $\text{Loc}$ is a finite set of locations, $q_0 \in \text{Loc}$ is the initial location, $\text{Clk}$ is a finite set of clocks, $\text{E} \subseteq \text{Loc} \times \text{Act} \times B(\text{Clk}) \times \mathcal{P}(\text{Clk}) \times \text{Loc}$ is a set of edges, $\text{Act} = \text{Act}_I \cup \text{Act}_O$, is a finite set of actions, partitioned into inputs and outputs respectively, and $\text{Inv} : \text{Loc} \mapsto \mathcal{P}(\text{Clk})$ is a set of location invariants.

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

We define the semantic of a TIOA $A = (\text{Loc}, q_0, \text{Clk}, E, \text{Act}, \text{Inv})$ to be a TIOTS $A_{sem} = (\text{Loc} \times (\text{Clk} \mapsto R_{\geq 0}), (q_0, 0), \text{Act}, \text{Inv})$, where 0 is a constant function mapping all clocks to zero, and $\text{Inv}$ is the largest transition relation generated by the following rules:

- Each $(q, a, \varphi, c, q') \in E$ gives rise to $(q, u) \xrightarrow{d}(q', u')$ for each clock valuation $u \in [\text{Clk} \mapsto R_{\geq 0}]$ such that $u \models \varphi$ and $u' = u[r \mapsto 0]_{\leq c}$ and $u' \models \text{Inv}(q')$.
- Each location $q \in \text{Loc}$ with a valuation $u \in [\text{Clk} \mapsto R_{\geq 0}]$ gives rise to a transition $(q, u) \xrightarrow{d}(q, u + d)$ for each delay $d \in R_{\geq 0}$ such that $u + d \models \text{Inv}(q)$.

The TIOAs 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 only one transition can be enabled at the same time. This is a standard check. We assume that all TIOAs below are deterministic.

Having introduced a syntactic representation for TIOTs, we now turn back to the semantic level in order to define the basic concepts of implementation and specification:
Definition 3. A TIOTS $S$ is a specification if each of its states $s \in St^S$ is input-enabled: $\forall t \in T^S_s \exists s' \in St^S_s, s \xrightarrow{t} s'$. The assumption of input-enabledness, also seen in many interface theories [25, 17, 30, 33, 29], 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-enabledness 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.

It is easy to check if a TIOA induces an input-enabled TIOTS. Thus we define Timed Input/Output Specification Automata (Specification Automata in short) to be TIOSs, whose semantic TIOTS is a specification. In practice tools can interpret absent input transitions in at least two reasonable ways. First, they can be interpreted as ignored inputs, whose semantic TIOTS is a specification. In practice tools

Implementations are concrete executable ralizations 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 4. An implementation $P = (St^P, p_0, \Sigma^P, \rightarrow^P)$ is a specification such that for each state $p \in St^P$ we have:

(output urgency) $\forall p', p'' \in St^P$ if $p \rightarrow^P p'$ and $p \rightarrow^P p''$ then $d = 0$ (and consequently, due to determinism $p = p''$)

[independent progress] either ($\forall d \geq 0, p \rightarrow^P p'$) or

$\exists d \in R_{\geq 0}, \exists d' \in \Sigma^P, p \rightarrow^P d'$ and $p' \rightarrow^P d'.

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 is either an output transition (which is controlled by the implementation) or an ability to delay until an output is possible. Otherwise a state can delay indefinitely. An implementation cannot wait for an input from the environment without letting time pass.

A notion of refinement allows to compare two specifications as well as to relate an implementation to a specification. Refinement should satisfy the following substitutability condition. If $P$ refines $Q$, then it should be possible to replace $Q$ with $P$ in every environment and obtain an equivalent system.

We study these kind of properties in later sections. It is well known from the literature [12, 13, 6] that in order to give these kind of guarantees a refinement should have the flavour of alternating (timed) simulation [2].

Definition 5. A specification $S = (St^S, s_0, \Sigma, \rightarrow_S)$ refines a specification $T = (St^T, t_0, \Sigma, \rightarrow_T)$, written $S \preceq T$, iff there exists a binary relation $R \subseteq St^S \times St^T$ containing $(s_0, t_0)$ such that for each pair of states $(s, t) \in R$ we have:

1. whenever $t \xrightarrow{\Sigma} t'$ for some $t' \in St^T$ then $s \xrightarrow{\Sigma} S s'$ and $(s', t') \in R$ for some $s' \in St^S$.
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 [22] and probabilistic [7] 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, is the first example of a proper notion of implementation for timed specifications. As the refinement is reflexive we get $P \text{ sat } P$ for any implementation and thus each implementation is consistent as per Definition 7. 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 Def. 4.*

Just like the specifications, we represent implementations syntactically using Timed I/O Automata. A TIOA $P$ is an implementation automaton if its underlying TIOTS $[P]_{sem}$ is an implementation. To decide whether a specification automaton is an implementation automaton, one checks for output urgency and independent progress.

We conclude the section with the first major theorem. Observe that every preorder $\leq$ 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 $S, T$ we have that $S \preceq T$ iff $[S]_{mod} \subseteq [T]_{mod}$.*

The restriction of the theorem to locally consistent specifications is not a serious one. As we shall see, 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 $\text{err}^S \subseteq S^{\text{st}}$ as:

$$\text{err}^S = \{ s \mid (3d, s, \nabla \geq 0) \text{ and } \forall d \forall s', s, \nabla, s' \text{ implies } s'/\nabla \geq 0 \}$$

It follows that no immediate error states can occur in implementations, or in locally consistent specifications.

In general, immediate error states in a specification do not necessarily mean that a specification cannot be implemented. Fig. 5 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 $\text{err}^S$. In order to be able to build on existing formalizations [8] we will consider a dual reachability game, asking for a strategy of the input player to reach $\text{err}^S$. We first define a timed predecessor operator [14, 27, 8], which gives all the states that can delay into $X$ while avoiding $Y$:

$$\text{cPred}^S(Y, X) = \{ s \in S^{\text{st}} \mid 3d_h \in R_{\geq 0}, 3s' \in X, s, d_h, s', \nabla \text{ and } \text{post}^S(s, d_h(s)) \subseteq \overline{Y} \}$$

where $X$ and $Y$ are specifications.

Now the controllable predecessors operator is:

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

and the set of all inconsistent states $\text{cons}^S$ (i.e. the states for which the environment has a winning strategy) is defined as the least fixpoint of $\pi$: $\text{cons}^S = \pi(\text{cons}^S)$, which is guaranteed to exist by monotonicity of $\pi$ and completeness of the powerset lattice due to the theorem of Knaster and Tarski [31]. For transitions systems enjoying finite symbolic representations, automata specifications included, the fixpoint computation converges after a finite number of iterations [8].

Now we define the set of consistent states, $\text{cons}^\text{c}$, simply as the complement of $\text{cons}^S$. We obtain it by complementing the result of the above fixpoint computation for $\text{cons}^S$. 

---

**Figure 4:** An inconsistent specification.

**Figure 5:** A partially inconsistent specification.
For the purpose of proofs it is more convenient to formalize the dual operator, say \( \theta \), whose greatest fixpoint directly and equivalently characterizes \( \text{cons}^\Delta \). 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 avoid discussing \( \theta \) in details here, since it is a mere technicality.

**Theorem 4.** A specification \( S = (S^\Sigma, s_0^S, \Sigma^S, \omega^S) \) is consistent iff \( s_0 \in \text{cons}^\Sigma \).

The set of (in)consistent states can be computed for timed games, and thus for specification automata, using controller synthesis algorithms \([8]\). We discuss it briefly in Section 6.

The inconsistent states can be pruned from a consistent \( S \) leading to a locally consistent specification. Pruning is applied in practice to decrease the size of specifications.

**Theorem 5.** For a consistent specification \( S = (S^\Sigma, s_0^S, \Sigma^S, \omega^S) \) and \( S' = (\text{cons}^\Sigma, s_0^S, \Sigma^S, \omega^S) \), where \( \Delta = \Sigma^S \cap (\text{cons}^\Sigma \times (\Sigma^S \cup R \geq 0)) \), \( S' \Delta \) is locally consistent and \([S']_{\text{mod}} = [S^\Sigma]_{\text{mod}}\).

For specification automata pruning is realized by applying a controller synthesis algorithm, obtaining a maximum winning strategy, which is then presented as a specification automaton itself.

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.

We define a product first. Let \( S = (S^\Sigma, s_0^S, \Sigma^S, \omega^S) \) and \( T = (S^\Sigma, s_0^T, \Sigma^T, \omega^T) \) be two specifications. A product of \( S \) and \( T \), written \( S \times T \), is defined to be a specification \( (S^\Sigma \times S^\Sigma, (s_0^S, s_0^T), \Sigma^S \times \Sigma^T, \omega^S \times \omega^T) \), where the transition relation \( \to \) is the largest relation generated by the following rule:

\[
\frac{s, a \in S^\Sigma \quad s', t \in S^\Sigma \times T^\Sigma}{(s, t) \to (s', t')} \quad a \in \Sigma \cup R \geq 0
\]

In general, a result of the product may be locally inconsistent, or even inconsistent. To guarantee consistency we have to avoid it in implementations. A pruned specification can be given to a designer, who chooses a particular implementation satisfying conjoint 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 environment components can only assume that the composed implementations will adhere to original specifications being composed. Consequently if an error occurs in parallel composition of the two specifications, the environment is the only entity that is possibly in power to avoid it. Thus, following \([12]\), we say that a composition is useful, and composed components are compatible, if the input player has a strategy in the safety game to avoid error states in the composition. The main theorem will state that if an environment is compatible with a useful specification, it is also compatible with any of its refinements, including implementations.

We turn our attention to syntactic representations again. Consider two TIOA \( A_1 = (\text{Loc}_1, q_0^1, \text{Clk}_1, E_1, \text{Act}_1, \text{Inv}_1) \) and \( A_2 = (\text{Loc}_2, q_0^2, \text{Clk}_2, E_2, \text{Act}_2, \text{Inv}_2) \) with \( \text{Act}_1^\Sigma = \text{Act}_2^\Sigma \) and \( \text{Act}_1^C = \text{Act}_2^C \). Their conjunction, denoted \( A_1 \land A_2 \), is the TIOA \( A = (\text{Loc}, q_0, \text{Clk}, E, \text{Act}, \text{Inv}) \) given by: \( \text{Loc} = \text{Loc}_1 \times \text{Loc}_2 \), \( q_0 = (q_0^1, q_0^2) \), \( \text{Clk} = \text{Clk}_1 \cup \text{Clk}_2 \), \( \text{Inv}(q_1, q_2) = \text{Inv}(q_1) \cap \text{Inv}(q_2) \).

The set of edges \( E \) is defined by the following rule:

- If \( (q_1, a, \varphi_1, c_1, q_1') \in E_1 \) and \( (q_2, a, \varphi_2, c_2, q_2') \in E_2 \) this gives rise to \( ((q_1, q_2), a, \varphi_1 \land \varphi_2, c_1 \cup c_2, (q_1', q_2')) \in E \)

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 enabledness this is always the case.

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

**Theorem 7.** Let \( A_1 \) and \( A_2 \) be two specification automata, we have \([A_1]_{\text{sem}} \land [A_2]_{\text{sem}} = [A_1 \land A_2]_{\text{sem}}\).

### 4. Compatibility & Composition

We shall now define structural composition, also called parallel composition, between specifications. We follow the optimistic approach of \([15]\), i.e., two specifications can be composed if there exists at least one environment in which they can work together. Parallel composition is made of three main steps. First, we compute the classical product between timed specifications \([21]\), where components synchronize on common inputs/outputs. The second step is to identify incompatible states in the product, i.e., states in which the two components cannot work together. The last step is to compatible states in the product, i.e., states in which the two components cannot work together.

Parallel composition is made of three main steps. First, we compute the classical product between timed specifications \([21]\), where components synchronize on common inputs/outputs. The second step is to identify incompatible states in the product, i.e., states in which the two components cannot work together. The last step is to compatible states in the product, i.e., states in which the two components cannot work together.
We now propose our formal definition for parallel composition. We consider two specifications $S = (S^S, s_0^S, \Sigma^S, \omega^S)$ and $T = (S^T, s_0^T, \Sigma^T, \omega^T)$ and we say that they are composable iff their output alphabets are disjoint, $\Sigma^S \cap \Sigma^T = \emptyset$.

As we did for conjunction, before defining the parallel composition we first introduce a suitable notion of product. The parallel product of $S$ and $T$, which roughly corresponds to the one defined on timed input/output automata [21], is the specification $S \otimes T = (S^S \otimes S^T, s_0^S \otimes s_0^T, \Sigma^S \otimes \Sigma^T, \omega^S \sqcup \omega^T)$, where the alphabet $\Sigma^S \otimes T = \Sigma^S \cup \Sigma^T$ is partitioned in inputs and outputs in the following way: $\Sigma^S_{\setminus \Sigma^T} = (\Sigma^S \setminus \Sigma^T) \cup (\Sigma^T \setminus \Sigma^S)$.

The transition relation of the product is the largest relation generated by the following rules:

\[
\begin{align*}
(s, t) &\xrightarrow{a \in \Sigma^S \setminus \Sigma^T} (s', t) \quad \text{(indep-l)} \\
(s, t) &\xrightarrow{a \in \Sigma^T \setminus \Sigma^S} (s', t) \quad \text{(indep-r)} \\
(s, t) &\xrightarrow{a \in \Sigma^S \cap \Sigma^T} (s', t) \quad \text{(sync-in)} \\
(s, t) &\xrightarrow{d \in \mathbb{R}_{\geq 0}} (s', t) \quad \text{(delay)} \\
(s, t) &\xrightarrow{a \in (\Sigma^S \otimes \Sigma^T)} (s', t') \quad \text{(sync-io)}
\end{align*}
\]

Observe that if we compose to locally-consistent specifications using the above product rules, then the resulting product is also locally consistent. Since we normally work with consistent specifications in a development process, immediate errors as defined for conjunction are not applicable to parallel composition. Moreover, unlike [15], our specifications are input-enabled, and there is no way to define an error state in which a component can issue an output that cannot be captured by the other component.

The absence of “model-related” error states allows us to define more elaborated errors, specified by the designer. Those cannot easily be considered in [15]. Now give more details. When reasoning about parallel composition we use model specific error states, i.e., error states indicated by the designer. These error states could arise in several ways. First, a specification may contain an error state in order to model unavailable inputs in presence of input-enabledness (transitions under inputs that the system is not ready to receive, should target such an incompatible state). Typically universal states are used for the purpose, to signal unpredicatability of the behaviour after receiving an unanticipated input). Second, a temporal property written in some logic such as TCTL [1] can be interpreted over our specification, which when analyzed by a model checker, will result in partitioning of the states into good ones (say satisfying the property) and bad ones (violating the property). Third, an incompatibility in a composition can be propagated from incompatibilities in the composed components. It should always be the case that a state in a product $(s, t)$ is an incompatible state if $s$ is an incompatible state in $S$, or $t$ is an incompatible state in $T$.

Formally we will model all these sources of incompatibility as a set of error states. We will call this set of states, strictly undesirable states and refer to it as undesirable$^S$. In the rest of the section, to simplify the presentation, we will include the set of strictly undesirable states as a part of specification definition.

We will say that a specification is useful if there exists an environment $E$ that can avoid reaching a strictly undesirable state whatever the specification will do. The environment $E$ is said to be compatible with $S$. We are now ready to define structural composition.

We now propose to compute the set of useful states of $S$ using a fixpoint characterisation. We consider a variant of controllable time predecessor operator, where the roles of the inputs and outputs are reversed:

\[
\omega(X) = \text{undesirable}^S \cup \text{cPred}_S(X \sqcup \text{ipred}(X), \text{opred}(\overline{X}))
\] (8)

Now the set of useless states useful$^S$ can be characterized as the least fixpoint of $\omega$, so $\text{useful}^S \supseteq \omega(\text{useful}^S)$. Again existence and uniqueness of this fixpoint is guaranteed by monotonicity of $\omega$. The set of useful states is defined as the complement: useful$^S = \overline{\text{useful}^S}$.

Theorem 8. For a consistent specification $S$, $S$ is useful iff $s_0 \in \text{useful}^S$.

The following theorem shows that pruning the specification does not change the set of compatible environment.

Theorem 9. If $S$ such that $s_0 \in \text{useful}^S$ and $S^g = (\text{useful}^S \cup \{ u \}, s_0, \Sigma^S, \rightarrow, \{ u \})$. Then $E$ is compatible with $S$ iff $E$ compatible with $S^g$.

Having introduced the general notion of usefulnes of components and specifications, we are now ready to define compatibility of specifications and parallel composition. We propose the following definition, which is in the spirit of [12].

Definition 10. Two composable specifications $S$ and $T$ are compatible iff the initial state of $S \otimes T$ is useful.

Definition 11. For two compatible specifications $S$ and $T$ define their parallel composition $S[T = (S \otimes T)^g$, and undesirable$^{S[T]} = \{(s, t) \mid s \in \text{undesirable}^S \cup t \in \text{undesirable}^T\}$. As we have discussed above, the set of strictly undesirable states, undesirable$^{S[T]}$, can be increased by designer as needed, for example by adding state for which desirable temporal properties about the interplay of $S$ and $T$ do not hold.

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:

\[
[(S[T])U]_{mod} = [(S[T(U)])_{mod}]
\] (9)

Theorem 10. 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 $S_1$ composable with $T$, we have that $S_2$ composable with $T$ and $S_1[T \leq S_2[T]$. Moreover if $S_2$ compatible with $T$ then $S_1$ compatible with $T$.

We now switch to the symbolic representation. Parallel composition of two TIOA can be defined in the following way. Consider two TIOA $A_1 = (Loc_1, q_0^1, C_{loc_1}, E_1, Act_1, Inv_1)$ and $A_2 = (Loc_2, q_0^2, C_{loc_2}, E_2, Act_2, Inv_2)$ with $Act_1 \cap Act_2^c = \emptyset$.
Their parallel composition which is denoted $A_1 | A_2$ is the TIOA $A = \langle \text{Loc}, q_0, \text{Cnk}, E, \text{Act}, \text{Inv} \rangle$ given by: $\text{Loc} = \text{Loc}_1 \times \text{Loc}_2, q_0 = (q_0, q_0')$, $\text{Cnk} = \text{Cnk}_1 \vee \text{Cnk}_2, \text{Inv}(q_1, q_2) = \text{Inv}(q_1') \wedge \text{Inv}(q_2')$ and the set of actions $\text{Act} = \text{Act}_1 \cup \text{Act}_2$ is given by $\text{Act}_1 = \text{Act}_1^1 \setminus \text{Act}_2^1 \cup \text{Act}_1^2$, and $\text{Act}_2 = \text{Act}_2^1 \cup \text{Act}_2^2$. The set of edges $E$ is defined by the following rules:

- If $(q_1, a, \varphi_1, c_1, \varphi_1', q_1') \in E_1$ with $a \in \text{Act}_1 \setminus \text{Act}_2$ then for each $q_2 \in \text{Loc}_2$ this gives $((q_2, q_2'), a, \varphi_1, c_1, (q_1, q_1')) \in E$
- If $(q_2, a, \varphi_2, c_2, q_2') \in E_2$ with $a \in \text{Act}_2 \setminus \text{Act}_1$, then for each $q_1 \in \text{Loc}_1$ this gives $((q_1, q_1'), a, \varphi_1, c_1, (q_1, q_1')) \in E$
- If $(q_1, a, \varphi_1, c_1, q_1') \in E_1$ and $(q_2, a, \varphi_2, c_2, q_2') \in E_2$ with $a \in \text{Act}_1 \cap \text{Act}_2$ this gives rise to $((q_1, q_1'), a, \varphi_1 \lor \varphi_2, c_1 \lor c_2, (q_1, q_1')) \in E$

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

**Theorem 11.** Let $A_1$ and $A_2$ be two specification automata, we have $[A_1]_{\text{sem}} \times [A_2]_{\text{sem}} = [A_1 | A_2]_{\text{sem}}$.

### 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 $T\backslash S$ is the specification of exactly those components that when composed with $S$ refine $T$. In other words, $T\backslash S$ 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 have the following requirements on the sets of inputs and outputs of the dividend $T$ and the divisor $S$ when applying quotienting: $\Sigma^S \subseteq \Sigma^T$ and $\Sigma^o_1 \subseteq \Sigma^o_2$.

We proceed like for structural and logical compositions and start with a pre-quotient that may introduce error states. Those errors are then pruned to obtain the quotient.

Given two specifications $S = (S^I, S^o, \Sigma^I, \Sigma^o)$ and $T = (T^I, T^o, \Sigma^I, \Sigma^o)$ the pre-quotient is a specification $T \backslash S = (S\backslash (S^I \times S^T) \cup \{u\} \in \Sigma^I \times \Sigma^o, \Sigma^o)$ where $S\backslash S^I \times S^T$ and $\Sigma^o$ 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 $S$ 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.

Moreover we require that $\Sigma = \Sigma^I \cup \Sigma^T$ and $\Sigma_o = \Sigma_o^I \setminus \Sigma_o^T$. Finally the transition relation $\rightarrow_{T^I \times S^I}$ is the largest relation generated by the following rules:

$$
\begin{align*}
&\frac{t \in T^I, t' \in S^I \quad s \in S^o \cup R_{\geq 0}}{(t, s) \rightarrow_{T^I \times S^I} (t', s')} & \text{[all]} \\
&\frac{s \not\in S^o} {(t, s) \rightarrow_{T^I \times S^I} u} & \text{[unreachable]} \\
&\frac{t \not\in T^I \quad s \in S^o \cup R_{\geq 0}} {t \rightarrow_{T^I} s} & \text{[unsafe]} \\
&\frac{t \in T^I \quad s \in S^o \cup R_{\geq 0}} {t \rightarrow_{T^I} s} & \text{[dividend]} \\
&\frac{a \in S^o} {u \rightarrow_{T^I \times S^I} u} & \text{[universal]} \\
&\frac{a \in S^o} {e \rightarrow_{T^I \times S^I} e} & \text{[inconsistent]}
\end{align*}
$$

Theorem 12 states that the proposed pre-quotient operator has exactly the property that it is dual of structural composition with regards to refinement.

**Theorem 12.** For any two specifications $S$ and $T$ such that the pre-quotient $T \backslash S$ is defined, and for any implementation $X$ over the same alphabet as $T \times S$ we have that $T \times S \mid X$ is defined and $(T \times S) \mid X \leq T \times S$.

Finally, the actual quotient, denoted $T \backslash \{S\}$, is defined if $T \times S$ is consistent. It is obtained by pruning the states of the prequotient $T \times S$ from where the implementation has no strategy to avoid immediate errors states $e \rightarrow_{T \times S} u$ using the same game characterization like in Section 3. Effectively we define the quotient to be $T \backslash \{S\} = (T \times S) \mid X$. It follows from Theorem 5 that Theorem 12 also holds for the actual quotient operator $\mid \{\}$ (as opposed to the prequotient).

Quotienting for TIOA is defined in the following way. Consider two TIOA $A_T = (\text{Loc}_T, q_0^T, \text{Cnk}_T, \text{Act}_T, \text{Inv}_T)$ and $A_S = (\text{Loc}_S, q_0^S, \text{Cnk}_S, \text{Act}_S, \text{Inv}_S)$ with $\text{Act}_T \subseteq \text{Act}_S$ and $\text{Act}_S \subseteq \text{Act}_T$. The quotient, which is denoted $A_T \backslash \{A\}$ is the TIOA given by: $\text{Loc} = \text{Loc}_T \times \text{Loc}_S \cup \{l_0, l_0\}$, $q_0 = (q_0^T, q_0^S)$, $\text{Cnk} = \text{Cnk}_T \vee \text{Cnk}_S \cup \{\text{new}\}$, $\text{Inv}(q, q') = \text{Inv}(l_0) = \text{true}$ and $\text{Inv}(l_0) \subseteq \{\text{new} \leq 0\}$. The two new states $l_0$ and $l_0$ are respectively universal and inconsistent. The set of actions are $\text{Act} = \text{Act}_S \cup \text{Act}_T \cup \{\text{new}\}$ and $\text{Act} = \text{Act}_T \cup \text{Act}_S$. The set of edges $E$ is defined by the following rules:

- For each $q_T \in \text{Loc}_T, q_S \in \text{Loc}_S$ and $a \in \text{Act}$ this gives $((q_T, q_S), a, \text{Inv}_T(q_T) \wedge \text{Inv}_S(q_S), \{\text{new}\}, l_0) \in E$.
- For each $q_T \in \text{Loc}_T, q_S \in \text{Loc}_S$ this gives $((q_T, q_S), \text{new}, \text{Inv}_T(q_T) \wedge \text{Inv}_S(q_S), \{\text{new}\}, l_0) \in E$.
- For each $(q_T, a, \varphi_T, c_T, q_T') \in \text{Act}_T$ and $(q_S, a, \varphi_S, c_S, q_S') \in \text{Act}_S$ this gives $((q_T, q_S), a, \varphi_T \lor \varphi_S, c_T \lor c_S, (q_T', q_S')) \in E$.
- For each $(q_T, a, \varphi_T, c_T, q_T') \in \text{Act}_T$ this gives $((q_T, q_S), a, \varphi_T \lor \varphi_S, \text{new}, (q_T', q_S')) \in E$.
- For each $(q_T, a, \varphi_T, c_T, q_T') \in \text{Act}_T$ this gives $((q_T, q_S), a, \varphi_T \lor \varphi_S, \text{new}, (q_T', q_S')) \in E$.

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

**Theorem 13.** Let $A_1$ and $A_2$ be two specification automata, we have $([A_1]_{\text{sem}} \times [A_2]_{\text{sem}}) = ([A_1 \times A_2]_{\text{sem}})$.}

### 6. TOOL IMPLEMENTATION

Our specification theory has been implemented using the verification engine for timed games UPPAAL-TIGA.

Application of The Engine. The engine of UPPAAL-TIGA supports the computation of winning strategies for timed
games with respect to a large class of TCTL winning objectives. The basic algorithm applied is that of \cite{8} being an on-the-fly algorithm performing forward exploration or reachable states and back-propagation of (so-far) computed winning states in an interleaved manner.

Crucial to the algorithm of \cite{8} is the symbolic representation and efficient manipulation of state-sets using zones, i.e., sets of clock valuations characterized by constraints on individual clocks and clock-differences. In particular the operators $cPred$, $ipred$ and $opred$ used in the fixpoint characterization of consistent and compatible states may be effectively computed using federations (unions of zones).

The operations of conjunction and quotienting may produce specification with inconsistent states, which needs to be determined and subsequently pruned away. For this, we apply the algorithm of Uppaal-Tiga to a timed reachability game, where input transitions are controllable, output transitions uncontrollable, and where states that do not have any outputs nor allow time to elapse are target states. The additional effort in implementing this algorithm required an on-the-fly detection of such states (instead of using ordinary state predicates) and back-propagating these according to the algorithm of Uppaal-Tiga.

Dually, for the composition of component specifications with designated error-states, we want to check for compatibility. For this we apply Uppaal-Tiga to a timed safety game, where input transitions are controllable, output transitions uncontrollable, and where error states in any of the two (or more) components should be avoided.

Finally, the problem of checking the refinement $S \preceq T$ is solved as a turn-based game between two players. The first player, or attacker, plays outputs on $S$ and inputs on $T$, whereas the second player, or defender, plays inputs on $S$ and inputs on $T$. The product of $S$ and $T$ according to these rules is then constructed on-the-fly, which is the forward exploration step. We detect error states on-the-fly and we back-propagate them. There are two kinds of error states: 1) Either the attacker may delay and violates invariants on $T$, which is, the defender cannot match a delay, or 2) the defender has to play a given action and cannot do so, i.e., a deadlock. In this implementation we can specialize our algorithm to simplify the operator $cPred$, analogously to \cite{6} with inverted rules with respect to controllable and uncontrollable transitions. This has been implemented and the tool has been extended to handle open systems.

Using the Tool. Returning to the example of the University of Figure 2, we may apply the extended version of Uppaal-Tiga for checking the desired properties of compatibility and consistency. Checking for compatibility simply amounts to checking for controllability of the following safety property:

control: $\not\forall$ not Researcher. ERR

Checking for refinement between the University and the stated overall specification Specification is checked using the following new type of refinement property:

refinement: $\left\{\text{Administration}, \text{Machine}, \text{Researcher}\right\} \setminus \{\text{coin, tea, cof, pub}\} \preceq \{\text{Spec}\}$

We are now able to reveal that, unexpectedly, this refinement does not hold! In fact the Administration’s ability to take in publications and produce patents without a preceding grant, combined with the Machine’s ability to produce tea without any coin, violates the overall Specification’s requirement that patents can only be produced given a preceding grant. In Figure 6 a screen-shot of the extension of Uppaal-Tiga playing the counter-strategy against a (disbelieving but to be convinced) user is shown.

7. CONCLUDING REMARKS

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 Uppaal toolset \cite{3}.

There have been several other attempts to propose an interface theory for timed systems (see \cite{15, 11, 5, 4, 9, 32, 16, 24} for some examples). Our model shall definitely be viewed as an extension of the timed input/output automaton model proposed by Lynch et al. \cite{21}. The majors differences are in the game-based treatment of interactions and the addition of quotient and conjunction operators.

In \cite{15}, de Alfaro et al. suggested timed interfaces, a model that is similar to the one of TIO Ts. Our definition of composition builds on the one proposed in there. However, the work in \cite{15} is incomplete. Indeed there is no notion of implementation and refinement. Moreover, conjunction and quotient are not studied. Finally, the theory has only been implemented in a prototype tool \cite{11} which does not handle continuous time, while our contribution takes advantages of the powerful game engine of Uppaal-Tiga.

In \cite{22} Larsen proposes modal automata, which are deterministic automata equipped with transitions of the following two types: may and must. The components that implement such interfaces are simple labeled transition systems. Roughly, a must transition is available in every component that implements the modal specification, while a may transition need not be. Recently \cite{5, 4} a timed extension of modal automata was proposed, which embeds all the operations presented in the present paper. However, modalities are orthogonal to inputs and outputs, and it is well-known \cite{23} that, contrary to the game-semantic approach, they cannot be used to distinguish between the behaviors of the component and those of the environment.

One could also investigate whether our approach can be
used to perform scheduling of timed systems (see [11, 19, 16] for examples). For example, the quotient operation could perhaps be used to synthesize a scheduler for such problem.

8. REFERENCES