

# Timed Systems through the Lens of Logic

**S. Akshay**

Department of CSE, IIT Bombay, India  
akshayss@cse.iitb.ac.in

**Paul Gastin**

LSV, ENS Paris-Saclay & CNRS, Université Paris-Saclay  
paul.gastin@ens-paris-saclay.fr

**Vincent Jugué**

LIGM, Université Paris-Est Marne-la-Vallée, CNRS  
vincent.juge@u-pem.fr

**Shankara Narayanan Krishna**

Department of CSE, IIT Bombay, India  
krishnas@cse.iitb.ac.in

---

## Abstract

In this paper, we analyze timed systems with data structures, using a rich interplay of logic and properties of graphs. We start by describing behaviors of timed systems using graphs with timing constraints. Such a graph is called realizable if we can assign time-stamps to nodes or events so that they are consistent with the timing constraints. The logical definability of several graph properties [17, 9] has been a challenging problem, and we show, using a highly non-trivial argument, that the realizability property for collections of graphs with strict timing constraints is logically definable in a class of propositional dynamic logic (EQ-ICPDL), which is strictly contained in MSO. Using this result, we propose a novel, algorithmically efficient and uniform proof technique for the analysis of timed systems enriched with auxiliary data structures, like stacks and queues. Our technique unravels new results (for emptiness checking as well as model checking) for timed systems with richer features than considered so far, while also recovering existing results.

**2012 ACM Subject Classification** Theory of computation → Quantitative automata; Theory of computation → Logic and verification; Theory of computation → Timed and hybrid models

**Keywords and phrases** Timed systems, propositional dynamic logic, Logical definability, Efficient algorithms, graphs

**Funding** Partly supported by UMI ReLaX and DST/INRIA CEFIPRA project EQuaVe.

## 1 Introduction

The modeling and analysis of complex real-time systems is a challenging and important area, both from theoretical and practical points of view. Indeed, the challenge often stems from the fact that such models have different sources of infinite behaviors, which makes them highly expressive but difficult to analyze. On one hand, the timing features engender complex constraints between events, which allow (or disallow) infinite sets of timed behaviors (over real numbers) satisfying these constraints. On the other hand, the auxiliary data structures such as multiple stacks allow a rich expressive power often leading to undecidable verification problems, even in the absence of time. Thus, each choice of combining these components of real-time and specific data structures leads to rich models whose analysis is complicated and often intractable.

The analysis of timed systems without any additional data structures has often been done using well-accepted models like timed automata [7], where clocks are real-valued variables that are reset and checked at guards. The classical approach to analyze such timed automata is by abstracting the real-timed system using the so-called region abstraction into a finite-state

automaton preserving emptiness. Several variants and extensions of this basic model have been considered over the years, for instance using event-clocks [8] or diagonal constraints, or even by allowing (non-) deterministic updates of clocks. Subsequently, there has been a growing body of work [2, 1, 5, 6, 12, 13, 14, 15] towards adding auxiliary data structures like stacks [23, 4, 3] or queues [3] to such timed automata. In all these, the analyses required to solve the emptiness problem were specific to the choice of the data structure, and the exact kind of constraints and updates that are allowed. As an example, [2] allows checking time constraints on the messages stored in the stack, carefully “lifting” the classical region construction to obtain decidable emptiness. [13] showed that the model considered in [2] is expressively equivalent to a weaker model where the stack did not pass clocks. In general, it is not easy to see whether a particular feature can be toned down preserving expressiveness, or whether a specific proof technique extends to handle richer timing constraints.

Our goal in this paper is to introduce a novel and uniform approach for reasoning about such timed systems which allow rich timing features along with several types of auxiliary data structures at the same time. This technique captures the behaviors of the underlying model as graphs and examines the logical definability of certain properties of interest over these graphs. More precisely, we start with graphs whose edges are decorated with the time constraints that must be respected between two events. These graphs, in turn, give rise to weighted graphs, and the realizability of these constraints implies the existence of a feasible run in the system. *Realizability* in a weighted graph amounts to assigning non-decreasing time-stamps to all the events such that they satisfy all the constraints.

A timed system generates an infinite collection of such graphs, which collectively form the set of behaviors of the system. In other words, to check if the system has a timed run, we need to check for the realizability of some graph from an entire family of graphs which are obtained from the given system. Thus, we begin by investigating the logical definability of realizability over this family of graphs. We use a light-weight propositional dynamic logic called EQ-ICPDL for the logical definability. Writing formulae for our systems in EQ-ICPDL is rather intuitive and improves readability in several cases compared to the classical MSO. On a technical note, it is known that EQ-ICPDL is a strict fragment of MSO, and gives us a more tractable complexity than MSO (avoiding a non-elementary blowup).

Our first contribution is that, for collections of weighted graphs with a linear order, realizability is definable in EQ-ICPDL (and hence in MSO). All sequential timed systems, such as timed (multi-pushdown/channel) automata, generate such graphs. Our logical characterization is easier when the underlying system only has closed guards, but we go beyond this and prove that realizability is also definable in EQ-ICPDL in the presence of both open and closed guards. On the other hand, we show that, for an arbitrary family of weighted graphs (without the linear order), realizability is not definable in MSO. In fact, we show that this already holds for graphs with a partial order that has width (i.e., the size of the largest anti-chain) 2, thus proving a tight characterization.

Our second contribution is a result showing that emptiness of a large class of sequential timed systems with data structures can be reduced to checking satisfiability of a formula in EQ-ICPDL over graphs describing the behaviors of the system. This reduction is based on the critical insight that the timing features that we consider engender relations between vertices of a weighted graph, which can be interpreted (in the logic EQ-ICPDL) in graphs describing the behavior of the system. Thus, we can take the formulae for realizability over weighted graphs, and backward translate them into formulae over the behavior graphs of the timed system. Using this, we finally build a single EQ-ICPDL formula that is satisfiable iff the timed system has a non-empty set of timed behaviors.

Our third contribution is to show how the two results above can be combined with *existing* techniques to give an effective algorithm for checking emptiness of several classes of timed systems. First, observe that the above two contributions do not immediately imply that checking emptiness of the system is decidable, as satisfiability of EQ-ICPDL formulae over arbitrary collections of graphs is undecidable. This is unsurprising, since even in the untimed case, having a single queue or two stacks as data structures leads to undecidability of emptiness. However, we can now consider under-approximations, as classically done for untimed systems. One such under-approximation is to consider collections of graphs that have a fixed bound on the tree-width. Such graph behaviors can now be interpreted into trees and we can use the fact that checking satisfiability for EQ-ICPDL (with bounded intersection width) over trees is decidable in EXPTIME. This gives us a matching EXPTIME algorithm for checking emptiness of timed systems which describe graph behaviors that have a bounded tree-width. Note that showing MSO definability would not give us a EXPTIME algorithm, but only a non-elementary algorithm. Thanks to the above, we have a powerful logical framework that is uniformly applicable to any timed system, provided that (1) the realizability of the underlying weighted graphs are definable in EQ-ICPDL, and (2) the behavioral graphs corresponding to the system have a bounded tree-width. Using this approach, we are able to retrieve many known results on timed systems with data structures and, more importantly, to obtain new results for timed systems with complex inter-dependencies between data structures (see figure 8). More precisely, we are able to capture an intricate flow and exchange of information between data structures and clocks, without any additional difficulties. Yet another significant novelty and milestone of this technique is the capability of model checking on timed systems, an interesting class of timed properties.

**Related work** Our technique is orthogonal to the theory of timed systems via the region construction as well as to other related existing approaches discussed below. In the untimed setting, the closest work to ours is in [23, 4], where generic approaches for decidability via logic and tree-width have been developed for automata with data structures in the untimed setting. However, the questions that we focus on, namely, the problem of realizability and of defining timing features, do not even arise there. There have been several papers on the decidability of timed systems with a single stack; [11, 2] deal with specific timing constraints, while [13, 14] use the language of timed atoms to specify and analyze an orthogonal but powerful extension to timed registers. In [15], a NEXPTIME bound is shown in this setting by reduction to one-dimensional branching vector addition systems. However, all these works are restricted to a single stack, while we tackle several data structures including multiple stacks, queues. Our work is also related to [5, 6], where the behaviors of timed systems with stacks are modeled as graphs with a bounded tree-width. However, these are designed only for stacks (single or multiple with restrictions), and directly build a tree automaton instead of going via the logic. This requires separate proofs of tree-width for each specific system and limits the timing constraints (e.g., the implementation [6] is only for closed guards) and data structures that can be modeled.

The logic we use builds on Propositional Dynamic Logic, a classical logic to reason about programs [20]. The extension with loop, intersection and converse was explored in [21], where complexity bounds were shown for satisfiability and model checking. However, to the best of our knowledge, this is the first time this logic has been used in the analysis of timed systems, and we inherit the complexity bounds from the above papers. Even with MSO logic (a strictly more powerful and well-known logic), the characterization of realizability in MSO

over graphs of timed systems was open, as mentioned in [5]: we settle this problem in the first result of this paper.

## 2 Preliminaries

**Node- and edge-labeled graphs** Let  $\Sigma$  and  $\Gamma$  be two alphabets. Nodes will be labeled with  $\Sigma$  and edges with  $\Gamma$ . A  $(\Sigma, \Gamma)$ -labeled graph is a tuple  $G = (V, E, \lambda)$  where  $V$  is a finite set of vertices,  $\lambda: V \rightarrow 2^\Sigma$  labels vertices with (sets of) letters from  $\Sigma$  and  $E \subseteq V \times \Gamma \times V$  is the set of labeled edges. A vertex may have 0, 1 or several labels from  $\Sigma$ . For  $\gamma \in \Gamma$ , we let  $E_\gamma = \{(u, v) : (u, \gamma, v) \in E\}$  be the set of edges labeled  $\gamma$ .  $\mathcal{G}(\Sigma, \Gamma)$  denotes the set of  $(\Sigma, \Gamma)$ -labeled graphs.

In this paper, graphs model behaviors of sequential systems. Hence, we have a special symbol  $\text{succ}$  in  $\Gamma$  to define the successor relation  $E_{\text{succ}}$  of a total order on  $V$ . We simply write  $u \prec v$  instead of  $(u, v) \in E_{\text{succ}}$ . We call these graphs *linear*; we let  $\preceq = \prec^*$  be the linear order induced by  $\prec$  and we note  $\prec = \prec^+$  the strict order. The other edges  $E_\gamma$ , with  $\gamma \in \Gamma \setminus \{\text{succ}\}$ , are used to model other useful relations in the graph, for instance the matching push-pop relation if we are interested in pushdown systems.

**Propositional dynamic logic over labeled graphs** We define now the logic that we will use to specify properties of graphs. We use a variant of the propositional dynamic logic [20]. This logic is sufficiently expressive for our purposes and enjoys good complexity for the satisfiability problem, rather than the more expressive monadic second order logic (MSO) which has a much higher complexity. The logic ICPDL( $\Sigma, \Gamma$ ) is defined over  $\Sigma$  (often seen as propositional variables), and  $\Gamma$  (often seen as atomic programs).

**Syntax** We have the following, with  $p \in \Sigma$  and  $\gamma \in \Gamma$ :

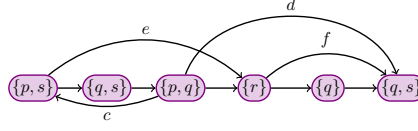
$$\begin{aligned} \Phi &::= E\sigma : \neg\Phi : \Phi \vee \Phi \\ \sigma &::= \top : p : \sigma \vee \sigma : \neg\sigma : \langle\pi\rangle\sigma : \text{loop}(\pi) \\ \pi &::= \xrightarrow{\gamma} : \text{test}\{\sigma\} : \pi + \pi : \pi \cdot \pi : \pi^* : \pi^{-1} : \pi \cap \pi \end{aligned}$$

In ICPDL,  $C$  stands for converse ( $\pi^{-1}$ ) and  $I$  for intersection ( $\pi \cap \pi$ ). We also consider LCPDL which is the fragment with loop but without intersection, since it has better complexity, as stated in Theorem 2. We also write CPDL or PDL with the obvious meaning. In the syntax above,  $\Phi$  are sentences and  $E$  is the existential node quantifier. The universal node quantifier  $A\sigma$  is written  $\neg E\neg\sigma$ . Formulae  $\sigma$  are called *node* or *state* formulae and have one implicit free first-order variable, while formulae  $\pi$  are called *path* or *program* formulae and have two implicit free first-order variables, the endpoints of the path.

**Semantics** Given a  $(\Sigma, \Gamma)$ -labeled graph  $G = (V, E, \lambda)$ , we can write the semantics of the formulae. The semantics of a *state formula*  $\sigma$  is a set  $\llbracket \sigma \rrbracket_G \subseteq V$ , while the semantics of a *path formula*  $\pi$  is a binary relation  $\llbracket \pi \rrbracket_G \subseteq V^2$ . Their definitions are mutually inductive. If the graph  $G$  is clear from the context, we omit subscripts and simply write  $\llbracket \sigma \rrbracket$  and  $\llbracket \pi \rrbracket$ .

The base cases for path formulae are  $\llbracket \xrightarrow{\gamma} \rrbracket = E_\gamma$  and  $\llbracket \text{test}\{\sigma\} \rrbracket = \{(v, v) : v \in \llbracket \sigma \rrbracket\}$ . The operations  $+$ ,  $\cap$ ,  $\cdot$ ,  $*$  correspond to rational expression notations, interpreted respectively as union, intersection, concatenation and Kleene star of the respective relations. Finally, the converse is defined by  $\llbracket \pi^{-1} \rrbracket = \{(u, v) : (v, u) \in \llbracket \pi \rrbracket\}$ .

The base cases for state formulae are  $\llbracket \top \rrbracket = V$  and  $\llbracket p \rrbracket = \{v \in V : p \in \lambda(v)\}$ , where  $p \in \Sigma$ . Disjunction and negation correspond to union and complement. We let  $\llbracket \text{loop}(\pi) \rrbracket$



■ **Figure 1** A node- and edge-labeled graph.

consist of the vertices  $v \in E$  from which there is a loop following path  $\pi$ , i.e., such that  $(v, v) \in \llbracket \pi \rrbracket$ . Similarly, we let  $\llbracket \langle \pi \rangle \sigma \rrbracket$  consist of the vertices  $u \in E$  from which it is possible to follow the path  $\pi$  and reach a vertex satisfying  $\sigma$ , i.e.,  $(u, v) \in \llbracket \pi \rrbracket$  for some  $v \in \llbracket \sigma \rrbracket$ . We often write  $\langle \pi \rangle$  instead of  $\langle \pi \rangle \top$ . A sentence  $E \sigma$  states that there exists a vertex of  $G$  satisfying  $\sigma$ , i.e.,  $G \models E \sigma$  if  $\llbracket \sigma \rrbracket_G \neq \emptyset$ . Disjunction and negation of sentences are as usual.

While ICPDL allows intersection, loop and converse, we also look at EQ-ICPDL where we allow existential quantification over new propositional variables in a similar spirit as in [22]. Thus, formulae of EQ-ICPDL( $\Sigma, \Gamma$ ) have the form  $\Psi = \exists p_1, \dots, p_n \Phi$  where  $\text{AP} = \{p_1, \dots, p_n\}$  is disjoint from  $\Sigma$  and  $\Phi \in \text{ICPDL}(\Sigma \uplus \text{AP}, \Gamma)$ . The semantics is defined by  $G = (V, E, \lambda) \models \exists p_1, \dots, p_n \Phi$  if there exists  $\lambda' : V \rightarrow 2^{\text{AP}}$  such that  $(G, \lambda') = (V, E, \lambda \cup \lambda') \models \Phi$ . For formulae  $\Psi$  in ICPDL( $\Sigma, \Gamma$ ) or EQ-ICPDL( $\Sigma, \Gamma$ ), we let  $L(\Psi) = \{G \in \mathcal{G}(\Sigma, \Gamma) : G \models \Psi\}$ .

► **Example 1.** We illustrate the semantics of ICPDL( $\Sigma, \Gamma$ ) using Figure 1. We have a node- and edge-labeled graph, with node labels  $\Sigma = \{p, q, r, s\}$  and edge labels  $\Gamma = \{d, e, f, \text{succ}\}$ . In path formulae, we simply write  $\rightarrow$  instead of  $\xrightarrow{\text{succ}}$ . The formula  $E \langle (\text{test}\{p \vee q\} \cdot \rightarrow)^* \rangle r$  evaluates to true on the given graph: the leftmost node is a witness. Likewise, the formula  $\neg E \langle \rightarrow \rangle (p \wedge s)$  is also true, since there are no nodes in the graph whose successors are labeled both  $p$  and  $s$ . Let  $\Delta = \Gamma \setminus \{\text{succ}\}$ . The formula  $E \bigvee_{(d, d') \in \Delta^2, d \neq d'} \text{loop}(\xrightarrow{d} \cdot \xrightarrow{d'}^{-1})$  is not true since all the non-successor edges are labeled by a unique symbol. Finally, the formula  $E \langle \text{test}\{s\} \cdot \xrightarrow{e} \cdot \text{test}\{r\} \cdot \xrightarrow{f} \cdot \text{test}\{s\} \cdot \xrightarrow{d}^{-1} \cdot \xrightarrow{c} \rangle p$  is true, while  $E \langle \text{test}\{p\} \cdot \xrightarrow{d} \rangle r$  is not.

**Satisfiability of propositional dynamic logic** The following definitions and results will be used in Section 4.3. Over arbitrary graphs, the satisfiability problem for PDL is undecidable. On the other hand, when we restrict to graphs of bounded tree-width, then the satisfiability problem becomes decidable with elementary complexity. We explain this now. Tree-width is a well-known measure for graphs [24]. We say that a labeled graph  $G = (V, E, \lambda)$  has tree-width  $k$  if the underlying unlabeled graph has tree-width  $k$ . We will not need the formal definition of tree-width in this paper, so it is omitted. We denote by  $\mathcal{G}^k(\Sigma, \Gamma)$  the graphs in  $\mathcal{G}(\Sigma, \Gamma)$  having tree-width at most  $k$ .

Below is one of the main theorems that we use in this paper. It refers to the intersection width of an EQ-ICPDL formula, which is the maximum of the intersection widths of its path subformulae: the intersection width of path formulae is defined inductively by  $\text{iw}(\xrightarrow{\gamma}) = \text{iw}(\text{test}\{\sigma\}) = 1$ ,  $\text{iw}(\pi_1 + \pi_2) = \text{iw}(\pi_1 \cdot \pi_2) = \max(\text{iw}(\pi_1), \text{iw}(\pi_2))$ ,  $\text{iw}(\pi^{-1}) = \text{iw}(\pi^*) = \text{iw}(\pi)$ , and  $\text{iw}(\pi_1 \cap \pi_2) = \text{iw}(\pi_1) + \text{iw}(\pi_2)$ . Hence, a formula in LCPDL has intersection width 1.

► **Theorem 2 (Satisfiability).** *Given  $k \geq 1$  in unary and a formula  $\Psi$  in EQ-ICPDL( $\Sigma, \Gamma$ ) of intersection width bounded by a constant, checking whether  $G \models \Psi$  for some  $G \in \mathcal{G}^k(\Sigma, \Gamma)$  can be solved in EXPTIME.*

This is a consequence of a similar result over trees due to Göller, Lohrey and Lutz [21, Theorem 3.8]. Indeed, graphs of tree-width at most  $k$  can be represented by binary trees which are called  $k$ -terms. Moreover, for each formula  $\Psi \in \text{ICPDL}(\Sigma, \Gamma)$  we can construct an

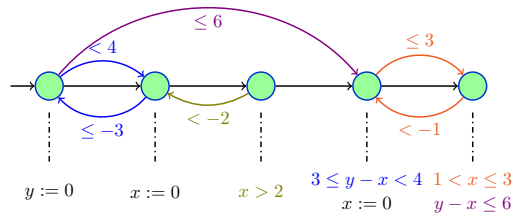
ICPDL formula  $\bar{\Psi}^k$  of size  $\mathcal{O}(k^2|\Psi|)$  over  $k$ -terms such that, for all  $k$ -terms  $\tau$ , we have  $\tau \models \bar{\Psi}^k$  iff  $\llbracket \tau \rrbracket \models \Psi$ , where  $\llbracket \tau \rrbracket$  is the graph denoted by the  $k$ -term  $\tau$  [10]. Hence, satisfiability of  $\Psi$  over  $\mathcal{G}^k(\Sigma, \Gamma)$  is reduced to satisfiability of  $\bar{\Psi}^k$  over  $k$ -terms.

**Graph interpretation and backward translation** [18, 10] The following definitions and results will be used in Section 4.2. We consider two signatures  $(\Sigma, \Gamma)$  and  $(\Sigma', \Gamma')$ . Intuitively, a graph  $G' \in \mathcal{G}(\Sigma', \Gamma')$  is interpreted in a graph  $G \in \mathcal{G}(\Sigma, \Gamma)$  if we have formulae over the signature  $(\Sigma, \Gamma)$  which, when evaluated on  $G$ , express nodes, labels and edges of  $G'$ . In this paper, we use CPDL interpretations, which means that the formulae for the interpretation are in CPDL $(\Sigma, \Gamma)$ . Also, we only need interpretation when the graphs  $G$  and  $G'$  have the same set of nodes. In this simple case, an interpretation  $\mathcal{I}$  is given by a tuple of state formulae  $(\sigma_p)_{p \in \Sigma'}$  and a tuple of path formulae  $(\pi_\gamma)_{\gamma \in \Gamma'}$ , all in CPDL $(\Sigma, \Gamma)$ . Now, we say that a graph  $G' = (V, E', \lambda') \in \mathcal{G}(\Sigma', \Gamma')$  is  $\mathcal{I}$ -interpreted in the graph  $G = (V, E, \lambda) \in \mathcal{G}(\Sigma, \Gamma)$  if, for all  $u, v \in V$ , all  $p \in \Sigma'$  and all  $\gamma \in \Gamma'$ , we have  $p \in \lambda'(u)$  iff  $G, u \models \sigma_p$  and  $(u, \gamma, v) \in E'$  iff  $G, u, v \models \pi_\gamma$ . In this case, we write  $G' = \mathcal{I}(G)$ .

Interpretations allow for a *backward translation* theorem: for each formula  $\Psi' \in \text{EQ-ICPDL}(\Sigma', \Gamma')$ , we can construct a formula  $\Psi \in \text{EQ-ICPDL}(\Sigma, \Gamma)$  such that, for all graphs  $G \in \mathcal{G}(\Sigma, \Gamma)$ , we have  $\mathcal{I}(G) \models \Psi'$  iff  $G \models \Psi$ . The formula  $\Psi$  is obtained from  $\Psi'$  by replacing the atomic state formulae  $p$  with  $\sigma_p$  (for  $p \in \Sigma'$ ) and the atomic path formulae  $\xrightarrow{\gamma}$  with  $\pi_\gamma$  (for  $\gamma \in \Gamma'$ ). Hence,  $\Psi$  and  $\Psi'$  have same intersection width and  $|\Psi| \leq |\Psi'| \cdot \max\{|\sigma_p|, |\pi_\gamma| : p \in \Sigma', \gamma \in \Gamma'\}$ .

### 3 Logical definability of realizability

**Weighted graphs** We consider linear weighted graphs where node labels are irrelevant, i.e.,  $\Sigma = \emptyset$ , and edges are labeled with constraints of the form  $< \alpha$  or  $\leq \alpha$ , where  $\alpha \in \mathbb{Z}$ , i.e.,  $\Gamma = \{\text{succ}\} \cup (\{<, \leq\} \times \mathbb{Z})$ . Since node labels are irrelevant, a linear weighted graph is simply denoted  $G = (V, E)$ . Often we use a maximal constant  $M \in \mathbb{N}$  and let  $\Gamma_M = \{\text{succ}\} \cup (\{<, \leq\} \times \{-(M-1), \dots, 0, \dots, M-1\})$ . A graph  $G \in \mathcal{G}(\emptyset, \Gamma_M)$  is called *M weight-bounded*. If we only compare using  $\leq$ , i.e., if there are no edges of the form  $(u, <, \alpha, v)$ , then we say that the graph is *closed* or a graph with closed constraints. Otherwise, we call it a *mixed* weighted graph or a graph with mixed constraints.



■ **Figure 2** A realizable linear weighted graph obtained from a sequence of instructions of a timed system.  $x, y$  are real-valued variables called *clocks*.  $x := 0$  ( $y := 0$ ) denotes reset instructions. Changing the last instruction to  $x - y \leq 5$  gives a non-realizable weighted graph. The non-realizability follows from (i) there is a time elapse more than 5 between the first and third nodes, (ii) the time elapse is at most 5 between the first and fourth nodes, and (iii) time is monotone, hence there is at least zero time elapse between the third and fourth nodes. This gives a negative cycle between the first and fourth nodes.

**Realizability** One important property of interest, which is the focus of this paper, is *realizability*. The property of realizability asks whether the constraints defined by the weights can be satisfied in a manner that is consistent with the order.

► **Definition 3.** A weighted graph  $G$  is *realizable* if there exists a time-stamp map  $\text{ts} : V \rightarrow \mathbb{R}$  such that (i) all constraints are satisfied:  $\forall (u, \triangleleft, \alpha, v) \in E$ ,  $\text{ts}(v) - \text{ts}(u) \triangleleft \alpha$ , and (ii)  $\text{ts}$  is monotone w.r.t. the linear order:  $\forall u, v \in V$ , if  $u \preceq v$ , then  $\text{ts}(u) \leq \text{ts}(v)$ .

If  $G$  is realizable via a map  $\text{ts}$ , then we say that  $\text{ts}$  is a *realization* of  $G$ . Note that the monotonicity could have been enforced by adding more constraint edges: when  $u \prec v$  we could have added an edge  $(v, \leq, 0, u)$ . With these extra constraints, realizability corresponds to checking the feasibility of the difference constraints. This is a classical problem on graphs which amounts to checking the absence of a negative cycle (see [16] for more details). There are many algorithms to solve this problem, e.g., the Bellman-Ford shortest path algorithm. Finally, as a quick aside, note that if we have reflexive edges  $(u, \triangleleft, \alpha, u) \in E$ , checking realizability for these constraints is always vacuously true or false for all possible time-stamps, and is easy. A realizable linear weighted graph obtained from a sequence of instructions of a timed system is depicted in Figure 2.

### 3.1 The first main result: logical definability of realizability

We are interested in properties of (possibly infinite) collections of such graphs, presented in a finite fashion. In particular, we wish to view graphs as being generated by an automaton, i.e., as behaviors of a system, and we wish to reason about this set of graphs. From this automata-theoretic viewpoint, a natural question to ask is whether the properties that we wish to reason about are definable in a certain logic. We focus on the specific property of realizability in weighted graphs and study its definability in EQ-ICPDL in our first main result below. In the next section, we will explain far-reaching consequences of our logical characterization, and in particular its application for checking emptiness of timed systems.

► **Theorem 4.** *Realizability is EQ-ICPDL definable on the set of graphs  $\mathcal{G}(\emptyset, \Gamma_M)$ . The size of the formula is polynomial in  $M$  and its intersection width is 2.*

We prove the above theorem in two steps: in Subsection 3.1.1, we consider closed graphs and show that the logical definition is rather easy for them. Then, in Subsection 3.1.2, we consider graphs with mixed constraints.

Throughout the proof, given a linear weighted graph  $G = (V, E)$  with  $|V| = n$ , we let  $V = \{u_1, \dots, u_n\}$  with  $u_1 \prec u_2 \prec \dots \prec u_n$ . We start with a simple observation regarding the time-stamps witnessing realizability in weighted graphs. Given an  $M$  weight-bounded graph  $G = (V, E)$ , a mapping  $\text{ts} : V \rightarrow \mathbb{R}$  is said to be *slowly monotone* if  $0 \leq \lfloor \text{ts}(v) \rfloor - \lfloor \text{ts}(u) \rfloor \leq M - 1$  for all  $u \rightarrow v$ . If a realization of a graph  $G$  is not slowly monotone, then there must exist two consecutive points whose time-stamps are separated by more than  $M - 1$ . But in this case there can be no forward edge (i.e., upper bound) that crosses this point, and hence the time difference between them can be reduced to any value larger than  $M - 1$  without affecting realizability. Formally,

► **Lemma 5.** *A graph  $G = (V, E)$  in  $\mathcal{G}(\emptyset, \Gamma_M)$  is realizable iff there is a slowly monotone map  $\text{ts} : V \rightarrow \mathbb{R}$  that realizes  $G$ .*

**Proof.** Let  $G = (V, E) \in \mathcal{G}(\emptyset, \Gamma_M)$  be realizable. Then there exists a map  $\text{ts}' : V \rightarrow \mathbb{R}$  such that all constraints are satisfied and  $\text{ts}'$  is monotone w.r.t.  $\preceq$ .



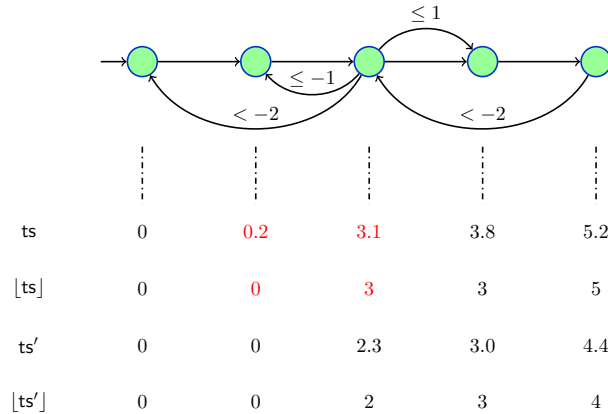
A *large gap* in  $\mathbf{ts}'$  is an integer  $i < n$  such that  $\lfloor \mathbf{ts}'(u_{i+1}) \rfloor - \lfloor \mathbf{ts}'(u_i) \rfloor \geq M$ . First, if  $\mathbf{ts}'$  has no large gap, then  $\mathbf{ts}'$  is slowly monotone and we are done. Henceforth, we assume that  $\mathbf{ts}'$  has at least one large gap, and we prove Lemma 5 by backward induction on the smallest large gap of  $\mathbf{ts}'$ .

Let  $i$  be the smallest large gap of  $\mathbf{ts}'$ . Notice that  $\mathbf{ts}'(u_{i+1}) - \mathbf{ts}'(u_i) > M - 1$ . Since  $\mathbf{ts}'$  is a realization of  $G$ , there cannot exist a forward edge  $(u, \triangleleft, \alpha, v) \in E$  crossing  $(u_i, u_{i+1})$ , i.e., such that  $u \preceq u_i \prec u_{i+1} \preceq v$ , since  $\alpha \leq M - 1$  contradicts the satisfaction of constraints. The back edges  $(u, \triangleleft, \alpha, v) \in E$  crossing over  $(u_i, u_{i+1})$ , i.e.,  $v \preceq u_i \prec u_{i+1} \preceq u$  are all satisfied since  $\mathbf{ts}'(v) - \mathbf{ts}'(u) \leq \mathbf{ts}'(u_i) - \mathbf{ts}'(u_{i+1}) < 1 - M \leq \alpha$ . Now, if we reduce the difference  $\mathbf{ts}'(u_{i+1}) - \mathbf{ts}'(u_i)$  to any value larger than  $M - 1$ , then the constraint on back edges are still satisfied. Hence, we choose  $t > \mathbf{ts}'(u_i) + M - 1$  such that  $\lfloor t \rfloor = \lfloor \mathbf{ts}'(u_i) \rfloor + M - 1$  and we define

$$\mathbf{ts}''(w) = \begin{cases} \mathbf{ts}'(w) & \text{if } w \preceq u_i \\ t + \mathbf{ts}'(w) - \mathbf{ts}'(u_{i+1}) & \text{otherwise.} \end{cases}$$

We can check that  $\mathbf{ts}''$  is a monotone time-stamping satisfying all constraints of  $G$ . Moreover, all large gaps of  $\mathbf{ts}''$ , if any, are greater than  $i$ . By backward induction, we conclude that there exists a monotone time-stamping  $\mathbf{ts}$  satisfying all constraints of  $G$  and having no large gap. Note indeed that the  $\mathbf{ts}$  values themselves can be unboundedly large, but the difference between integral parts of consecutive points is at most  $M - 1$ .  $\blacktriangleleft$

Let us see the above Lemma in action on an example. Consider the weighted graph in Figure 3 with map  $\mathbf{ts}: V \rightarrow \mathbb{R}$  which has a single large gap. We will apply Lemma 5 to show that we can replace  $\mathbf{ts}$  with a slowly monotone map  $\mathbf{ts}'$ . For the example, we have  $M = 3$ . The large gap is between time-stamps 0.2 and 3.1.  $\alpha$  is chosen as any value  $> 0.2 + 2 = 2.2$ . Let  $\alpha = 2.3$ . We then replace the time-stamp 3.1 by 2.3. Indeed, this new time-stamp satisfies the constraint  $\leq -1$  of the gap ( $2.3 - 0.2 \geq 1$ ). Had we tried any other time-stamp satisfying the constraint  $\leq -1$ , for instance 1.3 instead of 2.3, we might fail to satisfy the constraint  $< -2$  between the first and third time-stamps. Thus, reducing the time difference to be just more than  $M - 1$  is a safe choice whenever we have a large gap. We propagate the reduction by 0.8 ( $3.1 \mapsto 2.3$ ) to the subsequent time-stamps as well, so that the relative time differences are not affected. This gives us the slowly monotone map  $\mathbf{ts}'$ .



■ **Figure 3** Replacing large gaps.



Next, we have a crucial definition on general weighted graphs. Given an  $M$  weight-bounded linear graph  $G = (V, E)$ , a *time-stamping modulo  $M$*  is a map  $\text{tsm}: V \rightarrow \mathbb{Z}_M = \{0, \dots, M-1\}$ . For all  $u, v \in V$ , we set  $\text{d}_{\text{tsm}}(u, v) = \text{tsm}(v) - \text{tsm}(u) \bmod M$ . Further,  $(u, v)$  is said to be *tsm-big* if there exist  $w_1, w_2 \in V$  such that  $u \preceq w_1 \prec w_2 \preceq v$  and  $\text{d}_{\text{tsm}}(u, w_1) + \text{d}_{\text{tsm}}(w_1, w_2) \geq M$ . Observe that, if  $v \preceq u$ , then  $(u, v)$  cannot be tsm-big.

► **Definition 6.** A time-stamping modulo  $M$   $\text{tsm}$  is said to weakly satisfy  $G = (V, E)$  if for all  $e = (u, \triangleleft, \alpha, v) \in E$ ,

- (a) if  $u \preceq v$ , then  $(u, v)$  is not tsm-big and  $\text{d}_{\text{tsm}}(u, v) \leq \alpha$ ;
- (b) if  $v \prec u$  then  $(v, u)$  is tsm-big or  $\text{d}_{\text{tsm}}(v, u) \geq -\alpha$ .

Lemma 9 below shows that for linear weighted graphs, existence of such a map is a necessary condition for realizability. But first, we establish some useful facts. Recall that  $V = \{u_1, \dots, u_n\}$  with  $u_1 \prec u_2 \prec \dots \prec u_n$ . For  $i \leq j$ , we also define  $\text{d}_{\text{tsm}}^+(u_i, u_j) = \min\{M, \text{d}_{\text{tsm}}(u_i, u_{i+1}) + \dots + \text{d}_{\text{tsm}}(u_{j-1}, u_j)\}$  and  $\text{d}_{\text{tsm}}^+(u_j, u_i) = -\text{d}_{\text{tsm}}^+(u_i, u_j)$ . Notice that we have  $\text{d}_{\text{tsm}}^+(u_i, u_i) = 0$ .

▷ **Claim 7.** Let  $G = (V, E) \in \mathcal{G}(\emptyset, \Gamma_M)$  and let  $\text{ts}: V \rightarrow \mathbb{R}$  be a slowly monotone map (which need not satisfy the constraints of  $G$ ). Define  $\text{tsm}: V \rightarrow \mathbb{Z}_M$  by  $\text{tsm}(v) = \lfloor \text{ts}(v) \rfloor \bmod M$  for all  $v \in V$ . Then, for all  $u, v \in V$  such that  $u \preceq v$ , we have  $\text{d}_{\text{tsm}}^+(u, v) = \min\{\lfloor \text{ts}(v) \rfloor - \lfloor \text{ts}(u) \rfloor, M\}$ . Furthermore, we have  $\text{d}_{\text{tsm}}^+(u, v) = M$  if  $(u, v)$  is tsm-big, and  $\text{d}_{\text{tsm}}^+(u, v) = \text{d}_{\text{tsm}}(u, v)$  otherwise.

**Proof.** First,  $\text{d}_{\text{tsm}}(u_i, u_j) = (\lfloor \text{ts}(u_j) \rfloor - \lfloor \text{ts}(u_i) \rfloor \bmod M) \leq \lfloor \text{ts}(u_j) \rfloor - \lfloor \text{ts}(u_i) \rfloor$  for all  $i \leq j$ . Since  $\text{ts}$  is slowly monotone, we know that  $\lfloor \text{ts}(u_{i+1}) \rfloor - \lfloor \text{ts}(u_i) \rfloor < M$  for all  $i < n$ . We deduce that  $\text{d}_{\text{tsm}}(u_i, u_{i+1}) = \lfloor \text{ts}(u_{i+1}) \rfloor - \lfloor \text{ts}(u_i) \rfloor$ . Hence, from the definition of  $\text{d}_{\text{tsm}}^+$ , we have  $\text{d}_{\text{tsm}}^+(u_i, u_j) = \min\{M, \lfloor \text{ts}(u_j) \rfloor - \lfloor \text{ts}(u_i) \rfloor\}$  for  $i \leq j$ , and  $\text{d}_{\text{tsm}}(u_i, u_j) = \text{d}_{\text{tsm}}^+(u_i, u_j)$  if and only if  $\text{d}_{\text{tsm}}^+(u_i, u_j) < M$ . Moreover, if  $(u_i, u_j)$  is tsm-big, there exist integers  $k$  and  $\ell$  such that  $i \leq k < \ell \leq j$  and  $\text{d}_{\text{tsm}}(u_i, u_k) + \text{d}_{\text{tsm}}(u_k, u_\ell) \geq M$ . Hence  $\lfloor \text{ts}(u_j) \rfloor \geq \lfloor \text{ts}(u_\ell) \rfloor \geq \lfloor \text{ts}(u_k) \rfloor + \text{d}_{\text{tsm}}(u_k, u_\ell) \geq \lfloor \text{ts}(u_i) \rfloor + \text{d}_{\text{tsm}}(u_i, u_\ell) + \text{d}_{\text{tsm}}(u_k, u_\ell) \geq \lfloor \text{ts}(u_i) \rfloor + M$ , and thus we have  $\text{d}_{\text{tsm}}^+(u_i, u_j) = M$ .

Conversely, if  $\text{d}_{\text{tsm}}^+(u_i, u_j) = M$ , then  $\lfloor \text{ts}(u_j) \rfloor \geq \lfloor \text{ts}(u_i) \rfloor + M$ . Then, let  $k$  be the smallest integer such that  $k \geq i$  and  $\lfloor \text{ts}(u_k) \rfloor \geq \lfloor \text{ts}(u_i) \rfloor + M$ . We must have  $k > i$ . It follows that  $\lfloor \text{ts}(u_{k-1}) \rfloor < \lfloor \text{ts}(u_i) \rfloor + M$ , and therefore that  $\lfloor \text{ts}(u_{k-1}) \rfloor - \lfloor \text{ts}(u_i) \rfloor = \text{d}_{\text{tsm}}(u_i, u_{k-1})$ . Since  $\text{ts}$  is slowly monotone, we also have  $\lfloor \text{ts}(u_k) \rfloor < \lfloor \text{ts}(u_{k-1}) \rfloor + M$ , and therefore  $\lfloor \text{ts}(u_k) \rfloor - \lfloor \text{ts}(u_{k-1}) \rfloor = \text{d}_{\text{tsm}}(u_{k-1}, u_k)$ . This shows that  $\text{d}_{\text{tsm}}(u_i, u_{k-1}) + \text{d}_{\text{tsm}}(u_{k-1}, u_k) = \lfloor \text{ts}(u_k) \rfloor - \lfloor \text{ts}(u_i) \rfloor \geq M$ , and thus that  $(u_i, u_j)$  is tsm-big, which completes the proof. ◀

Given that  $|\alpha| < M$  for all edges  $e = (u, \triangleleft, \alpha, v) \in E$ , Claim 7 provides us with the following, alternative characterization of weak satisfiability.

► **Lemma 8.** A time-stamping modulo  $M$   $\text{tsm}$  weakly satisfies the graph  $G = (V, E)$  if and only if  $\text{d}_{\text{tsm}}^+(u, v) \leq \alpha$  for all  $(u, \triangleleft, \alpha, v) \in E$ .

**Proof.** Let  $(u, \triangleleft, \alpha, v) \in E$  with  $u \preceq v$ . If  $(u, v)$  is not  $\text{d}_{\text{tsm}}$ -big and  $\text{d}_{\text{tsm}}(u, v) \leq \alpha$ , then  $\text{d}_{\text{tsm}}^+(u, v) = \text{d}_{\text{tsm}}(u, v) \leq \alpha$ . Conversely, if  $\text{d}_{\text{tsm}}^+(u, v) \leq \alpha$ , since  $\alpha < M$  we deduce that  $(u, v)$  is not  $\text{d}_{\text{tsm}}$ -big and  $\text{d}_{\text{tsm}}(u, v) = \text{d}_{\text{tsm}}^+(u, v) \leq \alpha$ .

Then, let  $(u, \triangleleft, \alpha, v) \in E$  with  $v \prec u$ . If  $(v, u)$  is  $\text{d}_{\text{tsm}}$ -big, then  $\text{d}_{\text{tsm}}^+(u, v) = -\text{d}_{\text{tsm}}^+(v, u) = -M < \alpha$ . Likewise, if  $(v, u)$  is not  $\text{d}_{\text{tsm}}$ -big and  $\text{d}_{\text{tsm}}(v, u) \geq -\alpha$ , then  $\text{d}_{\text{tsm}}^+(u, v) = -\text{d}_{\text{tsm}}^+(v, u) = -\text{d}_{\text{tsm}}(v, u) \leq \alpha$ . Conversely, if  $\text{d}_{\text{tsm}}^+(u, v) \leq \alpha$ , then either  $\text{d}_{\text{tsm}}^+(u, v) = -M$  and  $(v, u)$  is  $\text{d}_{\text{tsm}}$ -big, or else  $(v, u)$  is not  $\text{d}_{\text{tsm}}$ -big and  $\text{d}_{\text{tsm}}(v, u) = \text{d}_{\text{tsm}}^+(v, u) = -\text{d}_{\text{tsm}}^+(u, v) \geq -\alpha$ . ◀

Now, we obtain one direction of the characterization, which works both for closed and open constraints.

► **Lemma 9.** *If  $G \in \mathcal{G}(\emptyset, \Gamma_M)$  is realizable, then there exists a time-stamping modulo  $M$  that weakly satisfies  $G$ .*

**Proof.** Lemma 5 proves that there exists a slowly monotone time-stamping  $\text{ts}$  that satisfies the constraints  $G$ . We define  $\text{tsm}: V \rightarrow \mathbb{Z}_M$  by  $\text{tsm}(v) = \lfloor \text{ts}(v) \rfloor \bmod M$ , and we show below that  $\text{tsm}$  weakly satisfies  $G$ .

Let  $(u, \triangleleft, \alpha, v) \in E$ . By Lemma 8, it is enough to show that  $d_{\text{tsm}}^+(u, v) \leq \alpha$ . According to Claim 7, distinguishing the cases  $u \preceq v$  and  $v \prec u$ , we show easily that  $d_{\text{tsm}}^+(u, v) \leq \lfloor \text{ts}(v) \rfloor - \lfloor \text{ts}(u) \rfloor$  or  $d_{\text{tsm}}^+(u, v) = -M$ . In the first case, it follows that  $d_{\text{tsm}}^+(u, v) \leq \lfloor \text{ts}(v) \rfloor - \lfloor \text{ts}(u) \rfloor \leq \text{ts}(v) - \text{ts}(u) < \text{ts}(v) - \text{ts}(u) + 1 \leq \alpha + 1$ , and in the second case, we also have  $d_{\text{tsm}}^+(u, v) = -M < \alpha + 1$ . Hence, in both cases, we have  $d_{\text{tsm}}^+(u, v) < \alpha + 1$ . Observing that  $d_{\text{tsm}}^+(u, v)$  and  $\alpha$  are integers proves that  $d_{\text{tsm}}^+(u, v) \leq \alpha$ . ◀

The converse of the above lemma does not hold with mixed guards and this will be handled in the next subsection. However, for closed guards it yields the following characterization.

### 3.1.1 Characterizing realizability in closed graphs

► **Lemma 10.** *A closed graph  $G = (V, E)$  in  $\mathcal{G}(\emptyset, \Gamma_M)$  is realizable iff there exists a time-stamping modulo  $M$  that weakly satisfies  $G$ .*

**Proof.** One direction is Lemma 9. Conversely, suppose that  $\text{tsm}: V \rightarrow \mathbb{Z}_M$  is a time-stamping modulo  $M$  that weakly satisfies  $G$ . Then, the map  $\text{ts}: V \rightarrow \mathbb{N}$  defined inductively by  $\text{ts}(u_1) = 0$  and  $\text{ts}(u_{i+1}) = \text{ts}(u_i) + d_{\text{tsm}}(u_i, u_{i+1})$  is a slowly monotone map.

Let  $(u, \triangleleft, \alpha, v) \in E$ . By Claim 7, distinguishing the cases  $u \preceq v$  and  $v \prec u$ , we show easily that  $d_{\text{tsm}}^+(u, v) \geq \lfloor \text{ts}(v) \rfloor - \lfloor \text{ts}(u) \rfloor$  or  $d_{\text{tsm}}^+(u, v) = M$ . Since  $\text{tsm}$  weakly satisfies  $G$  (i.e.,  $d_{\text{tsm}}^+(u, v) \leq \alpha$ ) and  $M > \alpha$ , the second case is impossible. It follows that  $\text{ts}(v) - \text{ts}(u) = \lfloor \text{ts}(v) \rfloor - \lfloor \text{ts}(u) \rfloor \leq d_{\text{tsm}}^+(u, v) \leq \alpha$ , which shows that  $\text{ts}$  satisfies the constraints of  $G$ . ◀

It remains to encode the characterization of Lemma 10 in EQ-ICPDL to obtain the logical definability of realizability for linear weighted graphs.

**EQ-LCPDL characterization** We use existential quantification over atomic propositions  $p_0, \dots, p_{M-1}$  to guess the time-stamping modulo  $M$ . Intuitively, a node satisfies  $p_i$  iff its  $\text{tsm}$  value is  $i$ . So we define the formula  $\exists p_0, \dots, p_{M-1} \text{ Partition} \wedge \text{Forward} \wedge \text{Backward}$  where the auxiliary formulae are defined in Table 1. The formula **Partition** states that every vertex satisfies exactly one  $p_i$  ( $0 \leq i < M$ ).

For  $0 \leq i, j < M$ , let  $\delta_M(i, j) = (j - i) \bmod M$ . We use a path formula to characterize pairs of vertices that are **tsm-big**: a pair  $(u, v)$  is **tsm-big** iff we can go from node  $u$  to node  $v$  following the path formula **BigPath**.

Since negation is not allowed at the level of path formulae, we provide another formula, **SmallPath**, to express that a pair  $(u, v)$  of vertices is not **tsm-big**. There are two cases, depending on whether  $\text{tsm}(u) \leq \text{tsm}(v)$  or not. In both cases,  $(u, v) \models \text{SmallPath}_{i,j}$  iff  $u \preceq v$ ,  $(u, v)$  is not **tsm-big**,  $i = \text{tsm}(u)$  and  $j = \text{tsm}(v)$ .

Formulae **Forward** and **Backward** respectively state the two conditions in Definition 6. The constraint on  $\preceq$ -forward edges is stated using the loop operator of LCPDL. By excluding the existence of a loop following the path  $\text{BigPath} \cdot \xrightarrow{\leq_\alpha}^{-1}$  we make sure that forward edges  $(u, v) \in E_{\leq_\alpha}$  are not **tsm-big**. Now, to ensure that forward edges  $(u, \triangleleft, \alpha, v)$  satisfy

$$\begin{aligned}
\text{Partition} &= A \bigvee_{0 \leq i < M} [p_i \wedge \bigwedge_{j \neq i} \neg p_j] \\
\text{BigPath} &= \sum_{\substack{0 \leq i, j, k < M \\ \delta_M(i, j) + \delta_M(j, k) \geq M}} \text{test}\{p_i\} \cdot \rightarrow^+ \cdot \text{test}\{p_j\} \cdot \rightarrow^+ \cdot \text{test}\{p_k\} \cdot \rightarrow^* \\
\text{SmallPath}_{i,j} &= \text{test}\{p_i\} \cdot \left( \sum_{i \leq k \leq \ell \leq j} \text{test}\{p_k\} \cdot \rightarrow \cdot \text{test}\{p_\ell\} \right)^* \cdot \text{test}\{p_j\} \text{ if } i \leq j \\
\text{SmallPath}_{i,j} &= \sum_{0 \leq \ell \leq j < i \leq k < M} \text{SmallPath}_{i,k} \cdot \rightarrow \cdot \text{SmallPath}_{\ell,j} \quad \text{if } j < i \\
\text{Forward} &= \neg E \bigvee_{-M < \alpha < M} \text{loop}(\text{BigPath} \cdot \xrightarrow{\leq \alpha}^{-1}) \\
&\quad \wedge \neg E \bigvee_{\substack{0 \leq i, j < M \\ \delta_M(i, j) > \alpha}} \text{loop}(\text{test}\{p_i\} \cdot \xrightarrow{\leq \alpha} \cdot \text{test}\{p_j\} \cdot (\rightarrow^{-1})^+) \\
\text{Backward} &= \neg E \bigvee_{\substack{-M < \alpha < M \\ 0 \leq i, j < M \\ \delta_M(i, j) < -\alpha}} \text{loop}(\text{SmallPath}_{i,j} \cdot \xrightarrow{\leq \alpha})
\end{aligned}$$

■ **Table 1** LCPDL for realizability of linear closed graphs

$d_{\text{tsm}}(u, v) \leq \alpha$ , we exclude the existence of a path violating this property, i.e., a loop following  $\text{test}\{p_i\} \cdot \xrightarrow{\leq \alpha} \cdot \text{test}\{p_j\} \cdot (\rightarrow^{-1})^+$  with  $\delta_M(i, j) > \alpha$ .

### 3.1.2 A characterization with mixed guards

The characterization above is not sufficient when some of the constraints are strict, i.e.,  $E$  contains edges of the form  $(u, <, \alpha, v)$ . It turns out that we need an additional condition to make sure that the fractional parts do not violate the realizability.

► **Definition 11.** Given a graph  $G = (V, E)$  and a time-stamping  $\text{tsm} : V \rightarrow \mathbb{Z}_M$  modulo  $M$ , we define two binary relations  $\text{geq}_{\text{Fr}}$  and  $\text{gt}_{\text{Fr}}$  on  $V$ :

■  $(u, v) \in \text{geq}_{\text{Fr}}$  iff one of the following conditions hold:

1.  $u \prec v$ ,  $(u, v)$  is not tsm-big and  $d_{\text{tsm}}(u, v) = \alpha$  for some edge  $(u, \triangleleft, \alpha, v) \in E$ ;
2.  $v \prec u$ ,  $(v, u)$  is not tsm-big and  $d_{\text{tsm}}(v, u) = -\alpha$  for some edge  $(u, \triangleleft, \alpha, v) \in E$ ;
3.  $v \prec u$  and  $d_{\text{tsm}}(u, v) = 0$ .

■  $(u, v) \in \text{gt}_{\text{Fr}}$  iff one of the following conditions hold:

1.  $u \prec v$ ,  $(u, v)$  is not tsm-big and  $d_{\text{tsm}}(u, v) = \alpha$  for some edge  $(u, <, \alpha, v) \in E$ ;
2.  $v \prec u$ ,  $(v, u)$  is not tsm-big and  $d_{\text{tsm}}(v, u) = -\alpha$  for some edge  $(u, <, \alpha, v) \in E$ .

Notice that  $\text{gt}_{\text{Fr}} \subseteq \text{geq}_{\text{Fr}}$ . The idea is that these relations give the ordering between the fractional parts. Thus,  $(u, v) \in \text{geq}_{\text{Fr}}$  (resp.  $\text{gt}_{\text{Fr}}$ ) means that the fractional part of  $\text{ts}(u)$  must be at least (resp. strictly greater than) the fractional part of  $\text{ts}(v)$ . Once again, since  $|\alpha| < M$  for all edges  $(u, \triangleleft, \alpha, v) \in E$ , Claim 7 provides an alternative characterization of the relations  $\text{geq}_{\text{Fr}}$  and  $\text{gt}_{\text{Fr}}$ .

► **Lemma 12.** Consider graph  $G = (V, E)$ ,  $\text{tsm} : V \rightarrow \mathbb{Z}_M$  modulo  $M$  and a pair  $(u, v)$  of vertices of  $G$ . Then,

- $(u, v) \in \text{geq}_{\text{Fr}}$  iff there exists an edge  $(u, \triangleleft, \alpha, v) \in E$  such that  $d_{\text{tsm}}^+(u, v) = \alpha$ , or if  $v \prec u$  and  $d_{\text{tsm}}^+(u, v) = 0$ ;
- $(u, v) \in \text{gt}_{\text{Fr}}$  iff there exists an edge  $(u, <, \alpha, v) \in E$  such that  $d_{\text{tsm}}^+(u, v) = \alpha$ .

► **Lemma 13.** Let  $G = (V, E)$  be an  $M$  weight-bounded graph with a linear order and mixed constraints.  $G$  is realizable iff there exists a time-stamping modulo  $M$   $\text{tsm}$  such that (i)  $\text{tsm}$  weakly satisfies  $G$  and (ii) there do not exist  $u, v \in V$  such that  $(u, v) \in \text{gt}_{\text{Fr}}$  and  $(v, u) \in \text{geq}_{\text{Fr}}^*$ , where  $\text{geq}_{\text{Fr}}^*$  is the reflexive transitive closure of  $\text{geq}_{\text{Fr}}$ .

**Proof.** In the forward direction, let  $G$  be realizable. Let  $\text{ts}: V \rightarrow \mathbb{R}$  be a slowly monotone map that realizes  $G$ , and let  $\text{tsm}$  be the time-stamping modulo  $M$  defined by  $\text{tsm}: v \rightarrow \lfloor \text{ts}(v) \rfloor \bmod M$ . Lemma 9 proves that  $\text{tsm}$  weakly realizes  $G$ . We further claim that, if  $(u, v) \in \text{geq}_{\text{Fr}}$ , then  $\{\text{ts}(u)\} \geq \{\text{ts}(v)\}$ , and that, if  $(u, v) \in \text{gt}_{\text{Fr}}$ , then  $\{\text{ts}(u)\} > \{\text{ts}(v)\}$ . The proof is as follows.

- If  $(u, v) \in \text{geq}_{\text{Fr}}$  because  $v \prec u$  and  $d_{\text{tsm}}^+(u, v) = 0$ , then  $\text{ts}(v) \leq \text{ts}(u)$  and  $0 = d_{\text{tsm}}^+(u, v) = \min\{\lfloor \text{ts}(v) \rfloor - \lfloor \text{ts}(u) \rfloor, -M\}$ . Hence,  $\lfloor \text{ts}(u) \rfloor = \lfloor \text{ts}(v) \rfloor$ , and therefore  $\{\text{ts}(v)\} \leq \{\text{ts}(u)\}$ .
- If  $(u, v) \in \text{geq}_{\text{Fr}}$  because there exists an edge  $(u, \triangleleft, \alpha, v) \in E$  such that  $d_{\text{tsm}}^+(u, v) = \alpha$ , then  $-M < \alpha = d_{\text{tsm}}^+(u, v) < M$ , and Claim 7 proves that  $\alpha = d_{\text{tsm}}^+(u, v) = \lfloor \text{ts}(v) \rfloor - \lfloor \text{ts}(u) \rfloor$ . It follows that  $\{\text{ts}(v)\} = \text{ts}(v) - \lfloor \text{ts}(v) \rfloor \leq \text{ts}(u) + \alpha - \lfloor \text{ts}(v) \rfloor = \text{ts}(u) - \lfloor \text{ts}(u) \rfloor = \{\text{ts}(u)\}$ .
- If  $(u, v) \in \text{gt}_{\text{Fr}}$ , then the same argument proves that  $\alpha = d_{\text{tsm}}^+(u, v) = \lfloor \text{ts}(v) \rfloor - \lfloor \text{ts}(u) \rfloor$ , and it follows that  $\{\text{ts}(v)\} = \text{ts}(v) - \lfloor \text{ts}(v) \rfloor < \text{ts}(u) + \alpha - \lfloor \text{ts}(v) \rfloor = \text{ts}(u) - \lfloor \text{ts}(u) \rfloor = \{\text{ts}(u)\}$ .

In the reverse direction, let  $\text{tsm}: V \rightarrow \mathbb{Z}_M$  be a time-stamping modulo  $M$  that weakly satisfies  $G$  and such that (ii) holds. As a direct consequence of (ii), every path in the graph  $G_{\text{geq}_{\text{Fr}}} = (V, \text{geq}_{\text{Fr}})$  contains at most  $|V|$  edges in  $\text{gt}_{\text{Fr}}$ . Indeed, otherwise two such edges would start from the same vertex, so that one edge would belong to a cycle of  $G_{\text{geq}_{\text{Fr}}}$ . Hence, for every vertex  $v \in V$ , we define the integer  $\text{ts}_1(v)$  as the largest number of edges in  $\text{gt}_{\text{Fr}}$  that may be used by a path in  $G_{\text{geq}_{\text{Fr}}}$  starting from  $v$ : observe that  $0 \leq \text{ts}_1(v) \leq |V|$ .

By construction, for every pair  $(u, v)$  in  $\text{geq}_{\text{Fr}}$ , we have  $\text{ts}_1(u) \geq \text{ts}_1(v)$ , and we even have  $\text{ts}_1(u) > \text{ts}_1(v)$  if  $(u, v) \in \text{gt}_{\text{Fr}}$ . Then, consider the map  $\text{ts}_0: V \rightarrow \mathbb{N}$  defined inductively by  $\text{ts}_0(u_1) = 0$  and  $\text{ts}_0(u_{i+1}) = \text{ts}_0(u_i) + d_{\text{tsm}}(u_i, u_{i+1})$ . The proof of Lemma 10 shows that  $\text{ts}_0$  is a slowly monotone map and that  $\text{ts}_0(v) - \text{ts}_0(u) \leq \alpha$  for all edges  $(u, \triangleleft, \alpha, v) \in E$ .

We prove now that the map  $\text{ts}: V \rightarrow \mathbb{R}$  defined by  $\text{ts}(v) = \text{ts}_0(v) + \text{ts}_1(v)/(|V| + 1)$  is monotone. For all pairs  $(u, v)$ ,

- if  $u \prec v$  and  $(v, u) \in \text{geq}_{\text{Fr}}$ , then  $\text{ts}(v) = \text{ts}_0(v) + \text{ts}_1(v)/(|V| + 1) \geq \text{ts}_1(u) + \text{ts}_1(u)/(|V| + 1) \geq \text{ts}(u)$ , because  $\text{ts}_0(v) \geq \text{ts}_0(u)$  and  $\text{ts}_1(v) \geq \text{ts}_1(u)$ ;
- if  $u \prec v$  and  $(v, u) \notin \text{geq}_{\text{Fr}}$ , then  $d_{\text{tsm}}^+(v, u) \neq 0$ , and therefore  $d_{\text{tsm}}^+(u, v) \geq 1$ , which proves that  $\text{ts}(v) \geq \text{ts}_0(v) = \text{ts}_0(u) + d_{\text{tsm}}^+(u, v) \geq \text{ts}_0(u) + 1 > \text{ts}_0(u) + \text{ts}_1(u)/(|V| + 1) = \text{ts}(u)$ .

Then, we prove that  $\text{ts}$  satisfies the constraints of  $G$ . Indeed, for every edge  $(u, \triangleleft, \alpha, v) \in E$ ,

- if  $d_{\text{tsm}}^+(u, v) = \alpha$ , then  $(u, v) \in \text{geq}_{\text{Fr}}$ , and therefore  $\text{ts}_1(v) \leq \text{ts}_1(u)$ ; it follows that  $\text{ts}(v) = \text{ts}_0(v) + \text{ts}_1(v)/(|V| + 1) \leq \text{ts}_0(u) + \alpha + \text{ts}_1(u)/(|V| + 1) = \text{ts}(u) + \alpha$ ;
- if  $d_{\text{tsm}}^+(u, v) = \alpha$  and, furthermore,  $\triangleleft = <$ , then  $(u, v) \in \text{gt}_{\text{Fr}}$ , hence  $\text{ts}_1(v) < \text{ts}_1(u)$ ; it follows that  $\text{ts}(v) = \text{ts}_0(v) + \text{ts}_1(v)/(|V| + 1) < \text{ts}_0(u) + \alpha + \text{ts}_1(u)/(|V| + 1) = \text{ts}(u) + \alpha$ ;
- if  $d_{\text{tsm}}^+(u, v) \neq \alpha$ , then  $d_{\text{tsm}}^+(u, v) \leq \alpha - 1$ , since  $\text{tsm}$  weakly satisfies  $G$ ; it follows that  $\text{ts}(v) = \text{ts}_0(v) + \text{ts}_1(v)/(|V| + 1) < \text{ts}_0(v) + 1 \leq \text{ts}_0(u) + (\alpha - 1) + 1 \leq \text{ts}(u) + \alpha$ .

Consequently, in all cases, we have  $\text{ts}(v) - \text{ts}(u) \triangleleft \alpha$ , which completes the proof. ◀

$$\begin{aligned}
\text{geq}_{\text{Fr}} &= (\xrightarrow{\leq \alpha} + \xrightarrow{< \alpha}) \cap \left( \sum_{\substack{0 \leq i, j < M \\ \delta_M(i, j) = \alpha}} \text{SmallPath}_{i, j} + \sum_{\substack{0 \leq i, j < M \\ \delta_M(j, i) = -\alpha}} \text{SmallPath}_{j, i}^{-1} \right) \\
&\quad + \sum_{i < M} \text{test}\{p_i\} \cdot \rightarrow^{-1} \cdot \text{test}\{p_i\} \\
\text{gt}_{\text{Fr}} &= \xrightarrow{< \alpha} \cap \left( \sum_{\substack{0 \leq i, j < M \\ \delta_M(i, j) = \alpha}} \text{SmallPath}_{i, j} + \sum_{\substack{0 \leq i, j < M \\ \delta_M(j, i) = -\alpha}} \text{SmallPath}_{j, i}^{-1} \right)
\end{aligned}$$

■ **Table 2** ICPDL formulae for capturing strict guards

**EQ-ICPDL characterization** As before, we use existentially quantified propositional variables  $p_0, \dots, p_{M-1}$  to guess the **tsm** values. To state weak-realizability, we use the formula  $\text{WRealizable} = \text{Partition} \wedge \text{Forward} \wedge \text{Backward}$  where the subformulae have been defined in Table 1. In addition, we have to check the absence of a cycle among the fractional parts, which contains at least one strict inequality and other, possibly non-strict, inequalities. By Lemma 13, this suffices to ensure realizability. To capture the ordering among the fractional parts, we use two EQ-ICPDL formulae,  $\text{gt}_{\text{Fr}}$  and  $\text{geq}_{\text{Fr}}$  respectively for the strict and non-strict parts, formally defined in Table 2. The EQ-ICPDL formula **Realizable** is then:

$$\exists p_0, \dots, p_{M-1} \text{ WRealizable} \wedge \neg \text{E loop}(\text{gt}_{\text{Fr}} \cdot \text{geq}_{\text{Fr}}^*)$$

The intersection width of  $\text{gt}_{\text{Fr}}$  and  $\text{geq}_{\text{Fr}}$  is 2. Hence, the intersection width of **Realizable** is also 2. This completes the proof of Theorem 4.

### 3.2 Realizability is beyond logical definability in general

Above, we have seen the EQ-ICPDL definability of realizability for linear weighted graphs. In the absence of a linear order, we now show that this is no longer true, even if one uses the strictly more expressive MSO logic (an easy example is the property of connectivity which separates EQ-ICPDL from MSO).

We start by defining MSO interpretations, which will be used to formalize the arguments below.

► **Definition 14.** An MSO interpretation [18] is a partial function that constructs for a given family of input structures, a new family of output structures as specified by a number of MSO formulae. The universe of the output structure is determined in terms of the universe of the input structure as specified by some MSO formula. Each predicate  $R(x_1, \dots, x_k)$  in the output structure is determined using an MSO formula  $\psi^R(x_1, \dots, x_k)$  over the input structure. More precisely, a deterministic MSO interpretation  $\tau: \mathcal{S} \rightarrow \mathcal{T}$  is given by (i) an MSO sentence  $\varphi_{\text{dom}}$  which determines which input structures  $S \in \mathcal{S}$  are in the domain of  $\tau$ , (ii) an MSO formula  $\varphi(x)$  over the signature of  $S$ , with one free variable  $x$ , which determines the universe of  $\tau(S)$  for each  $S \in \text{dom}(\tau)$ , (iii) for each predicate  $R$  of arity  $k$  of the output signature, a formula  $\psi^R(x_1, \dots, x_k)$  over the signature of  $S$ , with  $k$  free first order variables  $x_1, \dots, x_k$ , which determines  $R$  in  $\tau(S)$  as the set of tuples  $(x_1, \dots, x_k)$  from the universe of  $\tau(S)$  which satisfy  $\psi^R$ .

For ease of understanding, we give here an example that illustrates MSO interpretations.

► **Example 15.** Consider as input the family of word structures over alphabet  $\{a, b\}$  and binary relation  $S$  (successor) that satisfy the formula  $\varphi_{\text{dom}} = \text{is\_word} \wedge \psi$ , where  $\text{is\_word}$

is an MSO sentence stating that  $S$  is the successor relation of a total order and that each vertex is labeled either  $a$  ( $\text{lab}_a$ ) or  $b$  ( $\text{lab}_b$ ). The formula  $\psi$  is given by

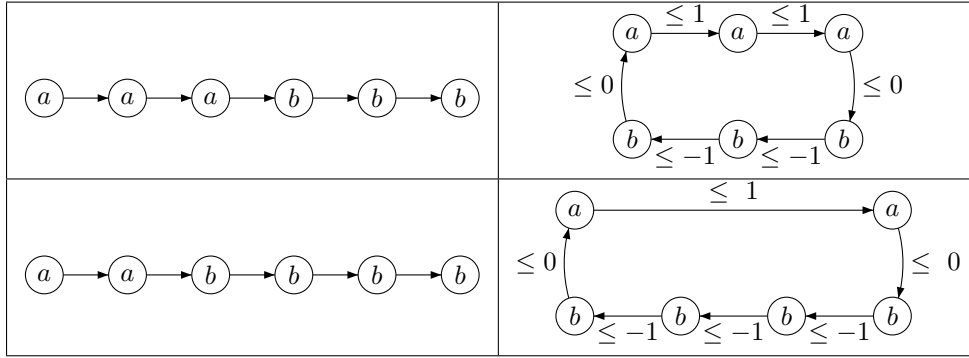
$$\exists x. [\text{first}(x) \wedge \text{lab}_a(x)] \wedge \exists x. [\text{last}(x) \wedge \text{lab}_b(x)] \wedge \forall x \forall y [\text{lab}_b(x) \wedge S(x, y) \Rightarrow \text{lab}_b(y)]$$

where  $\text{first}(x) = \neg \exists z S(z, x)$  and  $\text{last}(x) = \neg \exists z S(x, z)$ .

Clearly, the input consists of words in  $a^+b^+$ . Consider the MSO interpretation having formulae  $\varphi(u) = \text{true}$ , which asserts that the universe is unchanged, formulae  $\psi^{\text{lab}_a}(u) = \text{lab}_a(u)$  and  $\psi^{\text{lab}_b}(u) = \text{lab}_b(u)$ , which preserve the labeling of positions as they were in the input word, and formulae  $\psi^S(u, v) = S(v, u)$ , which revert the successor edges. Thus, an input word  $a^k b^j$  will result in  $b^j a^k$  after interpretation.

Next, we recall the backwards translation theorem [18], which is used in the proof of Theorem 17.

► **Theorem 16** (Backwards Translation Theorem, [18]). *Let  $L \subseteq \mathcal{G}_2$  be definable in MSO and let  $\theta: \mathcal{G}_1 \rightarrow \mathcal{G}_2$  be an MSO interpretation. Then the set  $\theta^{-1}(L) = \{G \in \mathcal{G}_1 : \theta(G) \cap L \neq \emptyset\}$  is definable in MSO.*



■ **Figure 4** The MSO interpretation that interprets words  $a^n b^m$  as realizable weighted graphs iff  $n \geq m$ .

► **Theorem 17.** *The property of realizability is not definable in MSO for weighted graphs without the linear order.*

**Proof.** We prove the result by contradiction using MSO interpretations. Let us consider word structures defined by the formula  $\varphi_{\text{dom}}$  in Example 15. We define the MSO interpretation  $\theta$  that takes as input the above family of word structures. We construct a family of weighted graph structures as our output. The following MSO formulae complete the interpretation. The predicates  $E_{\bowtie \beta}$  in the output structure are determined by formulae  $\psi^{E_{\bowtie \beta}}$  over the signature of the input word structure.

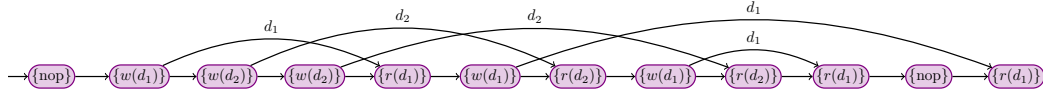
1.  $\varphi(u) = \text{true}$ . This ensures that all nodes of the input word are also part of the output graph.
2.  $\psi^{E_{\leq 1}}(u, v) = S(u, v) \wedge \text{lab}_a(u) \wedge \text{lab}_a(v)$
3.  $\psi^{E_{\leq -1}}(u, v) = S(u, v) \wedge \text{lab}_b(u) \wedge \text{lab}_b(v)$
4.  $\psi^{E_{\leq 0}}(u, v) = [S(u, v) \wedge \text{lab}_a(u) \wedge \text{lab}_b(v)] \vee [\text{last}(u) \wedge \text{first}(v)]$ ,
5.  $\varphi^{\prec}(u, v) = [S(u, v) \wedge \text{lab}_a(u) \wedge \text{lab}_a(v)] \vee [S(v, u) \wedge \text{lab}_b(u) \wedge \text{lab}_b(v)]$

Figure 4 illustrates this interpretation by giving two input words and the respective weighted graphs obtained. It can be seen that if one starts from words of the form  $a^n b^m$  where  $n \geq m$ , then the resulting graph is realizable, and otherwise, it is not since there is a negative cycle. If we consider  $L \subseteq \mathcal{G}$  to be the set of realizable graphs, and assume that  $L$  is definable in MSO, then by the Backwards translation theorem, we obtain  $\theta^{-1}(L) = \{a^n b^m : n \geq m\}$  to be a language definable in MSO, which we know is not the case. Hence, realizability is not an MSO-definable property of weighted graphs. Notice that, by the formula  $\varphi^{\prec}(u, v)$ , the weighted graphs constructed are not linear but are covered by two chains. ◀

## 4 Analyzing timed systems with data structures

In this section, we develop a generic technique to analyze timed systems with auxiliary data structures. We start with untimed systems with data structures.

### 4.1 Capturing data structure operations as graphs



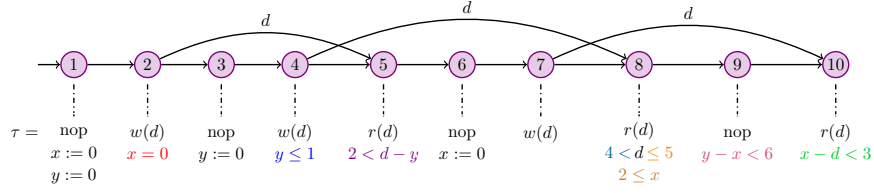
**Figure 5** A valid sequence  $\sigma = \text{nop } w(d_1) w(d_2) w(d_2) r(d_1) w(d_1) r(d_2) w(d_1) r(d_2) r(d_1) \text{nop } r(d_1)$  of operations from a system having two data structures (a stack  $d_1$  and a queue  $d_2$ ), with its graph  $G_\sigma$ .

Let us fix a finite set of data structures  $\text{DS}$ . Each data structure  $d \in \text{DS}$  can be operated via two instructions, either a *write* that writes to the data structure, denoted  $w(d)$ , or a *read* instruction that reads from the data structure, denoted  $r(d)$ . The set of instructions from  $\text{DS}$  is denoted  $\Sigma^{\text{DS}} = \{r(d), w(d) : d \in \text{DS}\} \cup \{\text{nop}\}$ , where  $\text{nop}$  is a special operation that does not access the data-structures. For simplicity and ease of exposition, we restrict each  $d \in \text{DS}$  to be a stack or a queue. However, the approach described here can be adapted to other structures (such as bags) with minor modifications. When  $d \in \text{DS}$  is a stack,  $r(d)$  is the **pop** operation and  $w(d)$  is the **push** operation on stack  $d$ . Similarly, if  $d$  is a queue,  $r(d)$  is the dequeue operation, while  $w(d)$  is the enqueue operation on queue  $d$ .

A sequence of operations from  $\Sigma^{\text{DS}}$  abstracts a run of a system with these data structures. We can then define the system as a generator of (possibly infinitely many) sequences of operations. The mechanism for generating this sequence of operations can be some machine (an automaton), or can be specified by regular expressions. We do not dwell on this detail here, and instead define a *system  $\mathcal{S}$  with data structures* as a regular language of sequences of operations over  $\Sigma^{\text{DS}}$ . Without loss of generality, we assume that all sequences will start with  $\text{nop}$ . It is easy to see that standard models such as (multi)pushdown automata, (multi)queue automata, multiset automata and so on generate regular languages of sequences of such operations.

A sequence  $\sigma$  of operations over  $\Sigma^{\text{DS}}$  is said to be *valid* if, for every prefix  $\sigma'$  of  $\sigma$  and for every data structure  $d \in \text{DS}$ , the number of reads  $r(d)$  in  $\sigma'$  is at most the number of writes  $w(d)$  in  $\sigma'$ , and the number of reads and writes in  $\sigma$  are equal. For a system  $\mathcal{S}$ , we are only interested in *valid* sequences generated by  $\mathcal{S}$ , and we denote this set by  $L(\mathcal{S})$ . For instance, a valid behavior of a pushdown system cannot read/pop from a stack before writing/pushing to it. Let  $\Gamma^{\text{DS}} = \text{DS} \cup \{\text{succ}\}$ . We associate, to any valid sequence  $\sigma$  of operations over  $\Sigma^{\text{DS}}$ , a  $(\Sigma^{\text{DS}}, \Gamma^{\text{DS}})$  linear graph  $G_\sigma$ .





■ **Figure 6** A labeled linear graph  $G_\tau$  obtained from a sequence of instructions  $\tau$  from  $\Sigma_{\text{Clocks}}^{\text{DS}}$ . For readability, the nodes are numbered and their instruction labels are written below them.

► **Definition 18.** Let  $\sigma = \sigma_1 \dots \sigma_n$  be a valid sequence of operations over  $\Sigma^{\text{DS}}$ . We define its  $(\Sigma^{\text{DS}}, \Gamma^{\text{DS}})$ -graph as  $G_\sigma = (V, E, \lambda)$ , where  $V = \{1, \dots, n\}$  and

1. for  $1 \leq i \leq n$ ,  $\lambda(i) = \{\sigma_i\}$ , and, for  $1 \leq i < n$ ,  $i \xrightarrow{\text{succ}} i + 1$ ,
2.  $\sigma_i = w(d)$  ( $r(d)$ ) iff there is an outgoing (incoming) edge in  $E$  labeled  $d$  from (to)  $i$ .
3. for each stack (queue)  $d$ , edges labeled  $d$  satisfy the LIFO (FIFO) property.

As an example, let  $\sigma$  be a sequence of operations from  $\text{DS} = \{d_1, d_2\}$ , where  $d_1$  is a stack and  $d_2$  is a queue. The graph  $G_\sigma$  corresponding to  $\sigma$  is depicted in Figure 5, where the node labels are exactly the singleton sets of operations  $w(d)$  and  $r(d)$ , for  $d \in \{d_1, d_2\}$ . We remark that this graph depends crucially on the interpretation of the data structure, as a stack or a queue. Notice that the edges labeled  $d_1$  respect the stack discipline (well-nesting), while the edges labeled  $d_2$  respect FIFO. For a fixed  $\text{DS}$ , we assume the interpretation of each data structure to be fixed and simply write  $G_\sigma$ .

Given a  $(\Sigma, \Gamma^{\text{DS}})$ -graph  $G = (V, E, \lambda)$ , we define its projection  $\pi(G)$  as the  $(\emptyset, \Gamma^{\text{DS}})$ -graph obtained by removing the node labels:  $\pi(G) = (V, E)$ .

► **Theorem 19** ([10]). Let  $\mathcal{S}$  be a system with data structures from  $\text{DS}$ . We can construct an EQ-LCPDL( $\emptyset, \Gamma^{\text{DS}}$ ) formula  $\psi_{\mathcal{S}}$  such that, for all  $(\emptyset, \Gamma^{\text{DS}})$ -graphs  $G$ ,  $G \models \psi_{\mathcal{S}}$  iff  $G = \pi(G_\sigma)$  for some  $\sigma \in L(\mathcal{S})$ .

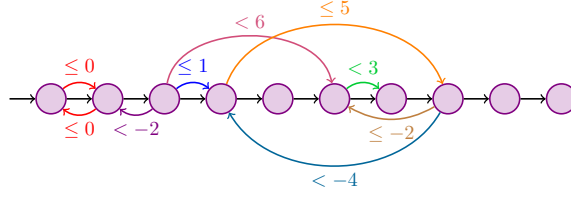
The classical *non-emptiness problem* for a system  $\mathcal{S}$  with data structures can be formulated as whether  $L(\mathcal{S}) \neq \emptyset$ .

► **Corollary 20.** For system  $\mathcal{S}$ ,  $\psi_{\mathcal{S}}$  is satisfiable iff  $L(\mathcal{S}) \neq \emptyset$ .

This corollary, along with Theorem 2, and using known bounds on tree-width, provides a “uniform” proof for the decidability of checking non-emptiness for a variety of untimed systems including (multi)pushdown and (multi)queue systems with bounded contexts, scope, or phases in a sequential setting. In many cases, the complexity obtained matches the best known bounds. We extend this approach uniformly to timed systems, using the realizability proof of Section 3.

## 4.2 Combining timing and data structures

While combining time constraints and data structures, we cannot directly rely on the formula for realizability from Section 3 in the approach outlined above. The vocabulary of graphs obtained from systems having time constraints and data structures might differ from the (weighted)  $(\emptyset, \Gamma^M)$ -graphs of Section 3 and the (unweighted)  $(\Sigma, \Gamma^{\text{DS}})$ -graphs above, where  $\Sigma = \emptyset$  or  $\Sigma = \Sigma^{\text{DS}}$ . The crucial observation is that, for a large class of timing constraints and data structures that we are interested in, it turns out that the former weighted graphs can be interpreted in the latter unweighted graphs, paving the way to extend the approach for systems having both time constraints and data structures. We now detail this intuition.



■ **Figure 7** The weighted graph  $G_\tau$  corresponding to the sequence of instructions  $\tau$  (from Figure 6).

#### 4.2.1 Timing instructions

In a timed system with data structures, the sequence of instructions generated by the system includes (i) checking time constraints on clocks (encoded as operations on clocks), (ii) checking time constraints on data structures, and (iii) mixing operations on clocks and data structures. Recall that we already have a fixed set of data structures  $\text{DS}$  consisting of stacks and queues. To be concrete, we also fix a representative set of timing features.

We fix a finite set  $\text{Clocks}$  of real-valued “clock” variables and a maximal constant  $M \in \mathbb{N}$ . We also fix notations  $\bowtie \in \{\leq, <, =, >, \geq\}$ ,  $\beta \in [0, M) \cap \mathbb{N}$  and use letters  $x, y, x_1, \dots$  for clock variables. Atomic timing instructions are as follows:

1. for  $x \in \text{Clocks}$ ,  $x:=0$  represents *clock resets*, while  $x \bowtie \beta$  represent *guards* or *clock constraints*;
2. for  $d \in \text{DS}$ ,  $d \bowtie \beta$  represents an *age constraint* checking the “age” of the message read;
3. for  $d \in \text{DS}$  and  $x, y \in \text{Clocks}$ ,  $(x - y) \bowtie \beta$ ,  $(d - x) \bowtie \beta$  and  $(x - d) \bowtie \beta$  represent *diagonal constraints*. The latter two capture mixing clock variables and data structures.

Thus, we define a set of instructions  $\Sigma_{\text{Clocks}}^{\text{DS}}$  which contains  $\Sigma^{\text{DS}}$  with the atomic timing instructions described above. Without loss of generality, we only consider sequences of instruction sets (also called *sequences of instructions* for simplicity) from  $\Sigma_{\text{Clocks}}^{\text{DS}}$  starting with the set  $\{\text{nop}\} \cup \{x:=0 : x \in \text{Clocks}\}$ , i.e., which resets all clocks at start-up. A sequence  $\tau$  of such instructions is shown in Figure 6. We associate to every such sequence  $\tau$  a sequence of untimed instructions  $\sigma_\tau$ , obtained by ignoring the atomic timing instructions. Now we say  $\tau$  is valid if  $\sigma_\tau$  is valid. Then, for every valid  $\tau$ , we can immediately associate a  $(\Sigma_{\text{Clocks}}^{\text{DS}}, \Gamma^{\text{DS}})$ -labeled linear graph  $G_\tau$  by considering  $G_{\sigma_\tau}$  and enriching its node labels with the timing instructions.

We define a timed system with data structures  $\mathcal{T}$  as a regular language of sequences of instructions over  $\Sigma_{\text{Clocks}}^{\text{DS}}$ . It is easy to see that classical models, such as timed automata, (multi-stack) timed pushdown automata or timed automata with gap order constraints, can be modeled in this formalism. The set of valid sequences generated by  $\mathcal{T}$  is denoted  $L(\mathcal{T})$ . Now, a valid sequence of instructions  $\tau = \tau_1 \dots \tau_n$  over  $\Sigma_{\text{Clocks}}^{\text{DS}}$  is said to be *timed feasible* or just *feasible* if there exists a time-stamping  $\text{ts} : \{1, \dots, n\} \rightarrow \mathbb{R}^{\geq 0}$  such that all timing constraints engendered by the timing instructions are satisfied. That is, for  $\bowtie \in \{\leq, <, =, >, \geq\}$  and  $\beta \in \mathbb{N}$ :

- (C<sub>1</sub>) For every guard of the form  $x \bowtie \beta$  at position  $i$ , if the last reset instruction of the clock  $x$  in  $\tau$  before  $i$  was at position  $j$ , then  $\text{ts}(i) - \text{ts}(j) \bowtie \beta$ .
- (C<sub>2</sub>) For every age constraint of the form  $d \bowtie \beta$  at position  $i$ , we have an edge  $j \xrightarrow{d} i$  in  $G_\tau$  (which implies  $w(d) \in \lambda(j)$  and  $r(d) \in \lambda(i)$ ), and  $\text{ts}(i) - \text{ts}(j) \bowtie \beta$ .
- (C<sub>3</sub>) For every diagonal constraint of the form  $x - y \bowtie \beta$  at position  $i$ , if  $j$  and  $k$  are the last resets of clocks  $x$  and  $y$  respectively, then  $\text{ts}(j) - \text{ts}(k) \bowtie \beta$ .

(C<sub>4</sub>) We can similarly define diagonal constraints between clocks and data structures.

Thus, the *non-emptiness problem* for the timed system  $\mathcal{T}$  is to check whether there exists a feasible  $\tau \in L(\mathcal{T})$ .

#### 4.2.2 From timing instructions to weighted graphs

We reduce checking non-emptiness of  $\mathcal{T}$  to checking satisfiability of an EQ-ICPDL formula over  $(\Sigma_{\text{Clocks}}^{\text{DS}}, \Gamma^{\text{DS}})$ -graphs. Towards this, we first define the weighted graph  $\mathcal{G}_\tau$  corresponding to a valid sequence of instructions  $\tau$  of  $\mathcal{T}$  in a natural manner. We extend from Section 3, where all timing instructions were simply clock constraints and resets of clocks i.e., corresponding to (C<sub>1</sub>) and (C<sub>3</sub>) above. In Figure 6, the check of  $x = 0$  on node 2 gives two bidirectional weighted edges in the weighted graph  $\mathcal{G}_\tau$  depicted in Figure 7, between the last reset point of  $x$  and node 2. Similarly, instruction  $y \leq 1$  at node 4 gives rise to the forward edge labeled  $\leq 1$  between last reset of  $y$  and node 4. For diagonal constraints (C<sub>3</sub>), the edge obtained is between the last reset points. E.g.,  $y - x < 6$  at node 9 yields the weighted edge from node 3 to node 6 (last resets of clocks  $y$  and  $x$ ).

This construction easily lifts to (C<sub>2</sub>) and (C<sub>4</sub>) as well. For (C<sub>2</sub>), we just observe that each age constraint engenders edges between the source write and target read of that data structure edge. E.g., in Figure 6, the age constraint  $4 < d \leq 5$  at node 8 yields two weighted edges (in Figure 7) between the source of the data structure edge, i.e., node 4 and target, node 8. The upper bound is captured by the forward edge while the lower bound by the backward edge. Similarly the constraint  $2 < d - y$  at node 5 yields the backward edge from node 3 (the last reset of clock  $y$ ) to node 2 (the source of the data structure edge reaching node 5) labeled  $< -2$  (as it is a lower bound constraint).

The main property about the weighted graph is that it captures feasibility of a sequence of instructions as realizability.

► **Lemma 21.** *A valid sequence of instructions  $\tau$  over  $\Sigma_{\text{Clocks}}^{\text{DS}}$  is feasible iff  $\mathcal{G}_\tau$  is realizable.*

#### 4.2.3 Interpreting weighted graphs in unweighted graphs

From the above discussion, given a timed system  $\mathcal{T}$ , for each valid  $\tau$  of  $\mathcal{T}$ , we have a weighted graph  $\mathcal{G}_\tau$ . A significant contribution of this paper, of possible independent interest, is the following proposition which relates these weighted graphs with unweighted  $(\Sigma_{\text{Clocks}}^{\text{DS}}, \Gamma^{\text{DS}})$ -graphs obtained from  $\tau$ .

► **Proposition 22.** *Let  $\tau$  be a valid sequence of instructions over  $\Sigma_{\text{Clocks}}^{\text{DS}}$ . Then the weighted graph  $\mathcal{G}_\tau$  can be CPDL-interpreted in the  $(\Sigma_{\text{Clocks}}^{\text{DS}}, \Gamma^{\text{DS}})$ -graph  $G_\tau$ .*

**Proof.** Given a valid sequence of instructions  $\tau$  over  $\Sigma_{\text{Clocks}}^{\text{DS}}$ , let  $M$  be the maximal constant appearing in these instructions. We saw in the previous subsection that the weighted graph  $\mathcal{G}_\tau = (V, E)$  has successor edges, and weighted edges arising from constraints of type (C<sub>1</sub>–C<sub>4</sub>). First, we observe that successor edges in  $\mathcal{G}_\tau$  are already present as successor edges in  $G_\tau$ . For weighted edges, let  $\triangleleft \in \{<, \leq\}$ , and  $c \in [0, M) \cap \mathbb{N}$ . We assume that equality constraints such as  $x = c$  have been replaced by the conjunction of  $x \leq c$  and  $c \leq x$ . For a clock  $x \in \text{Clocks}$ , we define the path formula

$$\text{Reset}_x = \rightarrow^{-1} \cdot (\text{test}\{\neg(x := 0)\} \cdot \rightarrow^{-1})^* \cdot \text{test}\{(x := 0)\}$$

which moves backwards along successor edges up to the last reset of clock  $x$ . Then, towards

the interpretation of forward edges weighted with  $\triangleleft c$ , we define the path formula  $\Pi_{\triangleleft c}$  as

$$\sum_{x \in \text{Clocks}} \text{Reset}_x^{-1} \cdot \text{test}\{x \triangleleft c\} \quad (\text{C}_1)$$

$$+ \sum_{d \in \text{DS}} \xrightarrow{d} \cdot \text{test}\{d \triangleleft c\} \quad (\text{C}_2)$$

$$+ \sum_{x, y \in \text{Clocks}} \text{Reset}_x^{-1} \cdot \text{test}\{x - y \triangleleft c\} \cdot \text{Reset}_y \quad (\text{C}_3)$$

$$+ \sum_{\substack{x \in \text{Clocks} \\ d \in \text{DS}}} \text{Reset}_x^{-1} \cdot \text{test}\{x - d \triangleleft c\} \cdot \xrightarrow{d}^{-1} \quad (\text{C}_4)$$

$$+ \xrightarrow{d} \cdot \text{test}\{d - x \triangleleft c\} \cdot \text{Reset}_x$$

Then, for all  $u, v \in V$  and  $c > 0$  (we will discuss the case  $c = 0$  below), we have  $(u, \triangleleft, c, v) \in E$  iff  $(G_\tau, u, v) \models \Pi_{\triangleleft c}$ . The four types of *upper* constraints defined in (C<sub>1</sub>–C<sub>4</sub>) are described by the respective path formulae (C<sub>1</sub>–C<sub>4</sub>) in  $\Pi_{\triangleleft c}$ . As an example, if we refer to the  $i^{\text{th}}$  node of  $G_\tau$  as  $u_i$  in Figure 6 and  $\mathcal{G}_\tau$  in Figure 7, we have the edge  $(u_3, \triangleleft, 6, u_6)$  in  $\mathcal{G}_\tau$  because  $(G_\tau, u_3, u_6) \models \text{Reset}_y^{-1} \cdot \text{test}\{y - x \triangleleft 6\} \cdot \text{Reset}_x$ . Similarly, the edge  $(u_6, \triangleleft, 3, u_7)$  is present in  $\mathcal{G}_\tau$  since  $(G_\tau, u_6, u_7) \models \text{Reset}_x^{-1} \cdot \text{test}\{x - d \triangleleft 3\} \cdot \xrightarrow{d}^{-1}$ . Notice that in  $\text{Reset}_x$ , we walk backward to the *first* node labeled  $x := 0$ , while, in C<sub>2</sub> and C<sub>4</sub>, for checking the age of a data structure, it is sufficient to check the existence of a data structure backward edge from the point where the age is checked.

Similarly, towards the interpretation of backward edges weighted with  $\triangleleft -c$ , we define the path formula  $\Pi_{\triangleleft -c}$  as

$$\sum_{x \in \text{Clocks}} \text{test}\{c \triangleleft x\} \cdot \text{Reset}_x \quad (\text{C}_1)$$

$$+ \sum_{d \in \text{DS}} \text{test}\{c \triangleleft d\} \cdot \xrightarrow{d}^{-1} \quad (\text{C}_2)$$

$$+ \sum_{x, y \in \text{Clocks}} \text{Reset}_y^{-1} \cdot \text{test}\{c \triangleleft x - y\} \cdot \text{Reset}_x \quad (\text{C}_3)$$

$$+ \sum_{\substack{x \in \text{Clocks} \\ d \in \text{DS}}} \text{Reset}_x^{-1} \cdot \text{test}\{c \triangleleft d - x\} \cdot \xrightarrow{d}^{-1} \quad (\text{C}_4)$$

$$+ \xrightarrow{d} \cdot \text{test}\{c \triangleleft x - d\} \cdot \text{Reset}_x$$

Then, for all  $u, v \in V$  and  $c > 0$ , we have  $(u, \triangleleft, -c, v) \in E$  iff  $(G_\tau, u, v) \models \Pi_{\triangleleft -c}$ . Again, the four types of *lower* constraints defined in (C<sub>1</sub>–C<sub>4</sub>) are described by the respective path formulae (C<sub>1</sub>–C<sub>4</sub>) in  $\Pi_{\triangleleft -c}$ .

Now, when  $c = 0$ , an edge weighted  $\triangleleft 0$  may arise from an upper constraint such as  $x \triangleleft 0$  or a lower constraint such as  $0 \triangleleft x$ . Therefore, for all  $u, v \in V$ , we have  $(u, \triangleleft, 0, v) \in E$  iff  $(G_\tau, u, v) \models \Pi_{\triangleleft 0} + \Pi_{\triangleleft -0}$ .

The size of  $\Pi_{\triangleleft c}$  is  $\mathcal{O}(|\text{Clocks}|^2 + |\text{DS}| + |\text{Clocks}||\text{DS}|)$ .

Thus we have described how each edge of the weighted graph  $\mathcal{G}_\tau$  can be interpreted in the  $(\Sigma_{\text{Clocks}}^{\text{DS}}, \Gamma^{\text{DS}})$ -graph  $G_\tau$  by an CPDL-formula, of size  $\mathcal{O}(|\text{Clocks}|^2 + |\text{DS}| + |\text{Clocks}||\text{DS}|)$ , which completes the proof of this proposition.  $\blacktriangleleft$

Thus, any formula over weighted graphs can be translated into an “*equivalent*” formula over  $(\Sigma_{\text{Clocks}}^{\text{DS}}, \Gamma^{\text{DS}})$ -graphs:

► **Corollary 23.** *Given a formula  $\psi \in \text{EQ-ICPDL}(\emptyset, \Gamma_M)$ , we can construct  $\psi' \in \text{EQ-ICPDL}(\Sigma_{\text{Clocks}}^{\text{DS}}, \Gamma^{\text{DS}})$  such that, for all valid sequences of instructions  $\tau$  over  $\Sigma_{\text{Clocks}}^{\text{DS}}$ , we have  $\mathcal{G}_\tau \models \psi$  iff  $G_\tau \models \psi'$ .*

The size of  $\psi'$  is  $\mathcal{O}((|\text{Clocks}|^2 + |\text{DS}| + |\text{Clocks}||\text{DS}|)|\psi|)$  and its intersection width is same as  $\psi$ .

#### 4.2.4 Reducing emptiness of $\mathcal{T}$ to satisfiability of EQ-ICPDL

From Theorem 4, we know that there exists a formula capturing realizability on weighted graphs, with signature  $(\emptyset, \Gamma_M)$ . Combining with Corollary 23 gives us the second main theorem of the paper regarding logical characterization of emptiness checking in timed systems with data structures.

► **Theorem 24** (Logical characterization of a timed system). *Given a timed system with data structures  $\mathcal{T}$ , we can construct a formula  $\Psi_{\mathcal{T}} \in \text{EQ-ICPDL}(\emptyset, \Gamma^{\text{DS}})$  such that for all  $(\emptyset, \Gamma^{\text{DS}})$  linear graphs  $G$ , we have  $G \models \Psi_{\mathcal{T}}$  iff  $G = \pi(G_{\tau})$  for some feasible  $\tau \in L(\mathcal{T})$ . The size of  $\Psi_{\mathcal{T}}$  is polynomial in the size of  $\mathcal{T}$  and its intersection width is 2.*

**Proof.** By Theorem 4, we can construct a formula **Realizable** in  $\text{EQ-ICPDL}(\emptyset, \Gamma_M)$  that captures realizability over weighted graphs  $\mathcal{G}(\emptyset, \Gamma_M)$ . By Corollary 23, we obtain a formula  $\psi_{\text{real}} \in \text{EQ-ICPDL}(\emptyset, \Gamma^{\text{DS}})$  such that, for all  $\tau \in L(\mathcal{T})$ ,  $G_{\tau} \models \psi_{\text{real}}$  iff  $G_{\tau} \models \text{Realizable}$ . In fact,  $\psi_{\text{real}}$  is simply obtained from **Realizable** by replacing every reference to a weighted edge in the formula by its logical interpretation in  $G_{\tau}$ . Now, by definition of EQ-ICPDL, we have  $\psi_{\text{real}} = \exists p_1 \dots p_r \psi'$  for some  $\psi' \in \text{ICPDL}(\{p_1, \dots, p_r\}, \Gamma^{\text{DS}})$ .

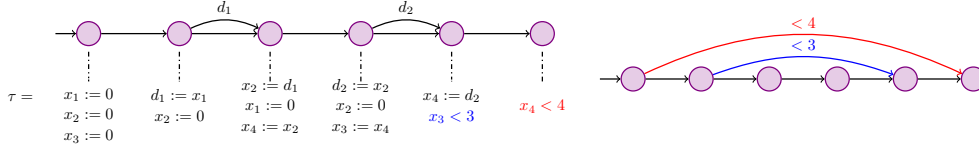
Next, recall that a timed system  $\mathcal{T}$  is a regular language of sequences of timed instructions. We consider the automaton that describes this regular collection, denoted by  $\mathcal{A} = (Q, i, F, \Delta)$  with  $Q$  the set of states,  $i$  the initial state and  $F$  the final states and  $\Delta$  the transition function. Then, the accepted sequences of instructions can be captured in EQ-LCPDL, by guessing the states visited along an accepting run, and by checking that consecutive states have a transition between them and start from initial and end at final state. Though similar in spirit to Theorem 19, for the sake of completeness and to obtain the precise complexity, we detail the construction in Appendix A.

Set  $\Sigma = \Sigma_{\text{Clocks}}^{\text{DS}} \cup Q = \{q_1, \dots, q_n\}$ . There exists a formula  $\xi = \exists q_1 \dots q_n \xi'$ , with  $\xi' \in \text{LCPDL}(\Sigma, \Gamma^{\text{DS}})$ , such that, for all  $(\emptyset, \Gamma^{\text{DS}})$ -graphs  $G$ , we have  $G \models \xi$  iff  $G = \pi(G_{\tau})$  for some sequence  $\tau \in L(\mathcal{T})$ . Combining this with the formula above, and define  $\psi_{\mathcal{T}} = \exists p_1 \dots p_r, q_1, \dots, q_n (\xi' \wedge \psi')$ . Then we have for any  $(\emptyset, \Gamma^{\text{DS}})$ -graph  $G$ ,  $G \models \psi_{\mathcal{T}}$  iff  $G = \pi(G_{\tau})$  for some  $\tau \in L(\mathcal{T})$  and  $\tau$  is feasible, which completes the proof. ◀

### 4.3 Application: deciding emptiness

While we have reduced checking emptiness of timed systems to checking satisfiability of a formula in EQ-ICPDL, this does not immediately give decidability results. This is obvious since systems with multiple data structures (such as stacks or even single queue) are all Turing powerful, even without any timing features. To obtain decidability, one often considers under-approximations, for which we essentially restrict the class of graphs that are considered as behaviors. As mentioned in the preliminaries, graphs of bounded tree-width form a large family of graphs where we regain decidability thanks to Theorem 2. Recall that  $\mathcal{G}^k$  denotes graphs of tree-width at most  $k$ . Combining Theorems 2 and 24, we have the following corollary about decidability in timed systems.

► **Corollary 25** (Underapproximations.). *Let  $k \in \mathbb{N}$ . Let  $\mathcal{S}$  be a timed system with data structures that uses clocks from  $\text{Clocks}$  and has maximum constant  $M \in \mathbb{N}$ . We can check whether there exists a feasible  $\tau \in L(\mathcal{S})$  such that  $G_{\tau} \in \mathcal{G}^k(\emptyset, \Gamma^{\text{DS}})$  in time  $2^{\text{poly}(k, M, |\text{Clocks}|, |\text{DS}|)} \times |\mathcal{S}|^{\text{poly}(k, |\text{DS}|)}$ .*



■ **Figure 8** Intricate flow of information in complex updates.

Thus, if the set  $\{G_\tau : \tau \in L(\mathcal{S})\}$  has a bounded tree-width, we obtain the same complexity bounds for checking emptiness of  $\mathcal{S}$ . As concrete applications, the following models of timed systems all fall in this category of having bounded tree-width, hence we obtain decidability (and efficient algorithms) for checking emptiness: timed automata [7], dense-timed pushdown automata with a single stack [2], multi-stack dense-timed pushdown automata with bounded rounds [5]. In fact, the complexity obtained for dense-timed pushdown automata with a single stack is even optimal. In addition, by this technique, we also have the following (new, to the best of our knowledge) results on the decidability of the emptiness problem for multi-stack dense-timed pushdown automata with (i) bounded contexts (the tree-width of graphs in the case of  $p$ -bounded context systems is  $\leq p + 1$  [23]), (ii) bounded phase (the tree-width of graphs in the case of  $p$ -bounded phase systems is  $\leq 2^{p+1}$  [19]), and (iii) bounded scope (the tree-width of graphs in the case of  $p$ -bounded scope is  $\leq 2(p + 2)$  [19]). Further, if one considers timed automata with  $b$ -bounded channels (a  $b$ -bounded channel is one where the number of unread messages is bounded by  $b \in \mathbb{N}$  at any point of time), then the  $(\emptyset, \Gamma^{\text{DS}})$ -graphs have a tree-width  $\leq b + 2$  [10]. We expect that many other data structures and various novel combinations (e.g., any combination of the above with multiple stacks and queues) can be handled using our technique, and leave these as routine exercises. In the next section, we consider more substantial extensions.

## 5 Extensions

We consider two extensions: first, adding new timing features without much change to the theory above, and second, extending from checking emptiness to model checking.

### 5.1 Extending time features - a generic template

We develop a two-step template to add new timing features to our approach above. Step 1 consists in expressing the edges engendered by the new feature in the weighted graph and Step 2 consists in writing a formula in LCPDL to capture this new edge relation. If we can accomplish these steps, then our theorems lift to the setting with these new timing features.

#### 5.1.1 Event clocks

Let us illustrate this template in action, via the example of event predicting clocks [8]. We fix a set  $\text{AP}$  of atomic propositions (events) arising from the system. An event-predicting timing instruction  $\text{next}_a \bowtie \alpha$ , for  $a \in \text{AP}$ ,  $\bowtie \in \{\leq, <, >, \geq\}$  and  $\alpha \in [0, M) \cap \mathbb{N}$ , entails a constraint between the current point (call it  $u$ ) and the point at which node label  $a$  occurs next (call it  $v$ ). Consistently with the notations on timing constraints  $C_1$ - $C_4$ , in section 4.2.1, we call this constraint  $C_5$ . Now, Step 1 is that this can be expressed in the weighted graph as an edge between these two vertices  $u$  and  $v$ . For Step 2, it is easy to write the PDL formula that

allows to interpret these edges of the weighted graph as edges in the  $\Gamma^{\text{DS}}$ -graph. Specifically, we just have to add to the path formula  $\Pi_{\triangleleft \alpha}$  in proof of Proposition 22 the following term:

$$\sum_{a \in \text{AP}} \text{test}\{(\text{next}_a \triangleleft \alpha)\} \cdot \rightarrow \cdot (\text{test}\{\neg a\} \cdot \rightarrow)^* \cdot \text{test}\{a\} \quad (\text{C}_5)$$

We proceed similarly for the path formula  $\Pi_{\triangleleft -\alpha}$ . It is not difficult to see that we can define similar formulae to capture event recording clocks as well.

### 5.1.2 Clock updates via tracking of clock names

While event clocks are relatively straightforward, for some other timing features, it is not easy to figure out, from the timing instruction, what edges in the weighted graph must be added. This happens for instance in clock updates: if we assign to  $x$  the value of clock  $y$  and then check it later with  $x \leq \alpha$ , the edge to be added is from the last reset of  $y$  to the point of checking the constraint. This is the case even if  $y$  has been reset in between after the assignment. Figure 8 illustrates this.

We consider a generic class of (deterministic) clock updates in timed systems. Clock updates are again a classical notion in timed automata but have not been studied much for timed systems with single or multiple data structures such as stacks and queues. We divide the updates we consider into 4 classes:

- (i) the usual reset of a clock  $x$  to 0 ( $x := 0$ ),
- (ii) assigning to clock  $x$  the value of clock  $x'$  ( $x := x'$ ),
- (iii) assigning to clock  $x$  the value associated to data structure  $d \in \text{DS}$ , while reading from  $d$  ( $x := d$ ),
- (iv) writing to  $d \in \text{DS}$  the value of clock  $x$  ( $d := x$ ).

Note that updates (iii) and (iv), combined with the age and diagonal constraints on data structures, give us a very rich and expressive class of timed systems. This allows us to consider timed systems where we can write to some  $d_1 \in \text{DS}$  the value of a clock  $x_1$ , then read from  $d_1$  this value (which changes with passage of time) into a clock  $x_2$ , write this value of  $x_2$  to some  $d_2 \in \text{DS}$ , and retrieve the value (after some time elapse) into a clock  $x_4$ . This value in  $x_4$  can then be checked with the value read from some  $d_4 \in \text{DS}$ , or with a clock  $x_5$ , or with a constant  $\alpha$ . In such a sequence, the clock  $x_1$  has come a long way at this time of checking, and we need to track it, to ensure that the time elapse we are looking at happens from the last reset of  $x_1$  before it was written to  $d_1$ . See Figure 8, where the value of clock  $x_1$  flows through  $d_1, x_2, d_2$  and finally  $x_4$ , from where it is checked. Likewise, the value of clock  $x_2$  flows through clocks  $x_4, x_3$ , and is checked at  $x_3$ . Now,  $x_2$  is reset after it flows into  $x_4$ ; however, when checking  $x_3$ , we use the reset of  $x_2$  before  $x_2$  flowed inside  $x_4$ .

Many recent papers [14, 12, 1] consider complex constraints between data structures and clocks; however, this intricate flow of information across clocks and data structures has not been looked at, to the best of our knowledge. Inferring such constraints requires us to follow and track the clock reset back to the original event. Rather than writing a formula in CPDL, we find it easier to describe an automaton which “walks” in the graph and performs this tracking. This enables us to express the weighted edges engendered by the constraints using the accepting paths of the automaton. This essentially handles the Step 1 we mentioned earlier. To handle Step 2, which is the logical definability, we write CPDL formulae whose paths  $\pi$  use this automaton. This allows us to interpret the weighted edges.

Formally, we construct an automaton  $\mathcal{A}$  with set of states  $Q = \{q_x : x \in \text{Clocks}\}$ . A run of  $\mathcal{A}$  starting from some state  $q_x$  will track the name of the clock whose value originates



from  $x$ . Without loss of generality, we assume that each transition of the timed system  $\mathcal{T}$  contains exactly one update for each clock, which could be of the form  $x := 0$  (reset),  $x := x'$  (deterministic clock update, we use  $x := x$  if the clock is unchanged),  $x := d$  ( $x$  is updated with the value read from  $d \in \text{DS}$ ), or  $d := x$ . There are two types of transitions:

- (clock update): if there is an update  $x' := x$  then we have a transition  $q_x \xrightarrow{\text{test}\{x' := x\} \cdot \rightarrow} q_{x'}$ ,
- (DS update): if there is an update  $x' := d$  for some  $d \in \text{DS}$ , then for all clocks  $x$ , we have a transition  $q_x \xrightarrow{\text{test}\{d := x\} \cdot \xrightarrow{d} \cdot \text{test}\{x' := d\}} q_{x'}$ . This corresponds to writing the value of clock  $x$  to some  $d \in \text{DS}$ , and, at the time of reading from  $d \in \text{DS}$ , assign this value to a clock  $x'$ .

Consider a run  $\rho = q_{x_0} \xrightarrow{\pi_1} q_{x_1} \xrightarrow{\pi_2} q_{x_2} \cdots \xrightarrow{\pi_n} q_{x_n}$  in  $\mathcal{A}$ . Let  $\tau \in L(\mathcal{T})$  be a valid sequence of instructions from the timed system  $\mathcal{T}$ . Let  $G_\tau$  be the associated  $(\Sigma_{\text{Clocks}}^{\text{DS}}, \Gamma^{\text{DS}})$ -graph and let  $u, v$  be vertices in  $G_\tau$ . Then,  $G_\tau, u, v \models \text{label}(\rho) = \pi_1 \cdot \pi_2 \cdots \pi_n$  iff the value of clock  $x_n$  at  $v$  originates from clock  $x_0$  at  $u$ . We write  $G_\tau, u, v \models \mathcal{A}_{x,x'}$  if there is a run  $\rho$  of  $\mathcal{A}$  from  $q_x$  to  $q_{x'}$  such that  $G_\tau, u, v \models \text{label}(\rho)$ .

Now, we can revisit and generalize the timing constraints above in  $(C_1-C_4)$  using  $\mathcal{A}$  instead of the paths tracking the last reset of a clock. For instance, the subformulae  $(C_1-C_3)$  of  $\Pi_{\leq \alpha}$  in the proof of Proposition 22 should be replaced with

$$\sum_{x, x' \in \text{Clocks}} \text{test}\{(x := 0)\} \cdot \mathcal{A}_{x, x'} \cdot \text{test}\{x' \triangleleft \alpha\} \quad (C_1)$$

$$+ \sum_{\substack{x, x' \in \text{Clocks} \\ d \in \text{DS}}} \text{test}\{(x := 0)\} \cdot \mathcal{A}_{x, x'} \cdot \text{test}\{d := x'\} \cdot \xrightarrow{d} \cdot \text{test}\{d \triangleleft \alpha\} \quad (C_2)$$

$$+ \sum_{x, x', y, y' \in \text{Clocks}} \text{test}\{(x := 0)\} \cdot \mathcal{A}_{x, x'} \cdot \text{test}\{x' - y' \triangleleft \alpha\} \cdot (\mathcal{A}_{y, y'})^{-1} \cdot \text{test}\{(y := 0)\} \quad (C_3)$$

This completes Steps 1 and 2 of our template. Hence, timed systems with data structures whose timing features include updates can be analyzed by our approach, with a complexity blow-up that is polynomial in the size of the input.

## 5.2 Extending to other problems: Model checking

Here, we would like to check whether a system satisfies a specification. As usual, we assume a finite set  $\text{AP}$  of atomic propositions which are used to link the system and the specification, and thus we will write specifications in the logic  $\text{LCPDL}(\text{AP}, \Gamma^{\text{DS}})$ . For instance, if  $\text{req}, \text{grant} \in \text{AP}$ , the formula  $\text{A}(\text{req} \implies \langle \rightarrow^+ \rangle \text{grant})$  says that every request should eventually be granted. As another example, the formula  $\text{A}((a \wedge \langle \rightarrow \cdot \xrightarrow{d} \rangle) \implies \langle \rightarrow \cdot \xrightarrow{d} \cdot \rightarrow \rangle a)$  says that, if some property  $a \in \text{AP}$  holds before a message is sent over data structure  $d$ , then  $a$  still holds after the message is received.

Specifications are evaluated over  $(\text{AP}, \Gamma^{\text{DS}})$ -graphs. Such graphs are generated by runs of the timed system. Again, we consider valid sequences  $\tau = \tau_1 \cdots \tau_n$  of instructions over  $\text{AP} \cup \Sigma_{\text{Clocks}}^{\text{DS}}$ . An instruction  $\tau_i \subseteq \text{AP} \cup \Sigma_{\text{Clocks}}^{\text{DS}}$  defines the atomic propositions  $\tau_i \cap \text{AP}$  which hold on the  $i^{\text{th}}$  event, together with the set of operations  $\tau_i \cap \Sigma_{\text{Clocks}}^{\text{DS}}$  which are executed at the  $i^{\text{th}}$  event. Let  $G_\tau = (V, E, \lambda)$  be the  $(\text{AP} \cup \Sigma_{\text{Clocks}}^{\text{DS}}, \Gamma^{\text{DS}})$ -graph associated with  $\tau$ . When  $\Sigma' \subseteq \Sigma$ , we note  $\pi_{\Sigma'}$  the projection on  $\Sigma'$ : if  $G = (V, E, \lambda)$  is a  $(\Sigma, \Gamma)$ -graph, then  $\pi_{\Sigma'}(G) = (V, E, \lambda')$ , where  $\lambda'(u) = \lambda(u) \cap \Sigma'$  for all  $u \in V$ .

Let  $\mathcal{T}$  be a timed system with data structures  $\text{DS}$  and let  $\Phi \in \text{LCPDL}(\text{AP}, \Gamma^{\text{DS}})$  be a specification. Recall that, in Theorem 24, we define the formula  $\Psi_{\mathcal{T}} = \exists p_1, \dots, p_n \Psi'_{\mathcal{T}}$ .

Consider  $\Psi = \exists p_1, \dots, p_n (\Psi'_\tau \wedge \neg\Phi)$ . Let  $G = (V, E)$  be an  $(\emptyset, \Gamma^{\text{DS}})$ -graph. By Theorem 24, if  $G \models \Psi$  then  $G_\tau \models \Psi$  and there exists a feasible  $\tau \in L(\mathcal{T})$  such that  $G = \pi_\emptyset(G_\tau)$ . Then  $G_\tau \models \neg\Phi$ , and since the specification uses AP only, we deduce that  $\pi_{\text{AP}}(G_\tau) \models \neg\Phi$ . Thus, as a corollary of Theorem 24, we can construct a formula  $\Psi \in \text{EQ-ICPDL}(\emptyset, \Gamma^{\text{DS}})$  which is satisfiable over  $(\emptyset, \Gamma^{\text{DS}})$ -linear graphs iff there is a run of the system which violates the specification  $\Phi$ .

► **Corollary 26.** *Let  $\mathcal{T}$  be a timed system with data structures DS and let  $\Phi \in \text{LCPDL}(\text{AP}, \Gamma^{\text{DS}})$  be a specification. For all  $(\emptyset, \Gamma^{\text{DS}})$ -linear graphs  $G$ , we can construct a formula  $\Psi$  such that  $G \models \Psi$  iff there exists a feasible  $\tau \in L(\mathcal{T})$  such that  $G = \pi_\emptyset(G_\tau)$  and  $\pi_{\text{AP}}(G_\tau) \not\models \Phi$ . The size of  $\Psi$  is polynomial in the size of  $\mathcal{T}$  and  $\Phi$ , and its intersection width is 2.*

## 6 Conclusion

We studied timed systems via their behaviors depicted as graphs and reasoned about these graphs via logic EQ-ICPDL. This gave rise to a problem of independent and basic interest: logical definability of realizability of weighted graphs. We showed that realizability is definable in EQ-ICPDL over sequential graphs but not definable, even in MSO, over non-sequential graphs. We developed a new logic based technique to analyze and model-check timed systems having a complex interplay of time and data structures. Potential future work is in generalizing this approach to handle a larger class of timed systems. In light of the negative result for non-sequential systems, an intriguing question is to come up with classes of concurrent systems that can be analyzed. Finally, it is worthwhile to explore if this technique can be applied in practice, in building tools for timed systems.

---

## References

- 1 P. Abdulla, M. F. Atig, and S. Krishna. Perfect timed communication is hard. In *FORMATS Proceedings*, pages 91–107, 2018.
- 2 P. Abdulla, M. F. Atig, and J. Stenman. Dense-timed pushdown automata. In *LICS Proceedings*, pages 35–44, 2012.
- 3 C. Aiswarya and P. Gastin. Reasoning about distributed systems: WYSIWYG (invited talk). In *FSTTCS Proceedings*, pages 11–30, 2014.
- 4 C. Aiswarya, P. Gastin, and K. Narayan Kumar. Verifying communicating multi-pushdown systems via split-width. In *ATVA Proceedings*, pages 1–17, 2014.
- 5 S. Akshay, P. Gastin, and S. Krishna. Analyzing timed systems using tree automata. In *CONCUR Proceedings*, 2016.
- 6 S. Akshay, P. Gastin, S. Krishna, and I. Sarkar. Towards an efficient tree automata based technique for timed systems. In *CONCUR Proceedings*, pages 39:1–39:15, 2017.
- 7 R. Alur and D. Dill. A theory of timed automata. *Theoretical Computer Science*, 126(2):183–235, 1994.
- 8 R. Alur, L. Fix, and T. A. Henzinger. Event-clock automata: A determinizable class of timed automata. *Theoretical Computer Science*, 211(1-2):253–273, 1999.
- 9 A. Blumensath and B. Courcelle. Monadic second-order definable graph orderings. *Logical Methods in Computer Science*, 10(1), 2014.
- 10 B. Bollig and P. Gastin. Non-sequential theory of distributed systems. <http://www.lsv.fr/~bollig/MPRI/non-sequential.pdf>, 2017.
- 11 A. Bouajjani, R. Echahed, and R. Robbana. On the automatic verification of systems with continuous variables and unbounded discrete data structures. In *Hybrid Systems II*, pages 64–85, 1994.
- 12 L. Clemente. Decidability of timed communicating automata. *CoRR*, abs/1804.07815, 2018.

- 13 L. Clemente and S. Lasota. Timed pushdown automata revisited. In *LICS Proceedings*, pages 738–749, 2015.
- 14 L. Clemente and S. Lasota. Binary reachability of timed pushdown automata via quantifier elimination and cyclic order atoms. In *ICALP Proceedings*, pages 118:1–118:14, 2018.
- 15 L. Clemente, S. Lasota, R. Lazic, and F. Mazowiecki. Timed pushdown automata and branching vector addition systems. In *LICS Proceedings*, pages 1–12, 2017.
- 16 T. H. Cormen, C. Stein, R. L. Rivest, and C. E. Leiserson. *Introduction to Algorithms*. McGraw-Hill Higher Education, 2nd edition, 2001.
- 17 B. Courcelle. Regularity equals monadic second-order definability for quasi-trees. In *Fields of Logic and Computation II - Essays Dedicated to Yuri Gurevich on the Occasion of His 75th Birthday*, volume 9300 of *Lecture Notes in Computer Science*, pages 129–141. Springer, 2015.
- 18 B. Courcelle and J. Engelfriet. *Graph Structure and Monadic Second-Order Logic - A Language-Theoretic Approach*, volume 138 of *Encyclopedia of mathematics and its applications*. CUP, 2012.
- 19 A. Cyriac, P. Gastin, and K. Narayan Kumar. MSO decidability of multi-pushdown systems via split-width. In *CONCUR Proceedings*, pages 547–561, 2012.
- 20 M. J. Fischer and R. E. Ladner. Propositional dynamic logic of regular programs. *Journal of Computer and System Sciences*, 18(2):194–211, 1979.
- 21 S. Göller, M. Lohrey, and C. Lutz. PDL with intersection and converse: satisfiability and infinite-state model checking. *Journal of Symbolic Logic*, 74(1):279–314, 2009.
- 22 F. Laroussinie and N. Markey. Quantified CTL: expressiveness and complexity. *Logical Methods in Computer Science*, 10(4), 2014.
- 23 P. Madhusudan and G. Parlato. The tree width of auxiliary storage. In *POPL Proceedings*, pages 283–294, 2011.
- 24 Neil Robertson and Paul D. Seymour. Graph minors. III. planar tree-width. *J. Comb. Theory, Ser. B*, 36(1):49–64, 1984.

## A

 Details in proof of Theorem 24

In this appendix, we present Lemma 27, which completes the proof of Theorem 24. Though this is similar in spirit to Theorem 19, for the sake of completeness and to obtain the precise complexity, we detail the construction below.

► **Lemma 27.** *Let  $\mathcal{T}$  be a timed system with data structures whose regular language of sequences of timed instructions is defined by the automaton  $\mathcal{A} = (Q, \iota, F, \Delta)$ . Let  $\Sigma = \Sigma_{\text{Clocks}}^{\text{DS}} \cup Q = \{q_1, \dots, q_n\}$ . We can construct a formula  $\xi = \exists q_1 \dots q_n \xi'$ , with  $\xi' \in \text{LCPDL}(\Sigma, \Gamma^{\text{DS}})$ , such that, for all  $(\emptyset, \Gamma^{\text{DS}})$  linear graphs  $G$ ,  $G \models \xi$  iff  $G = \pi(G_\tau)$  for some sequence  $\tau \in L(\mathcal{T})$ . Formula  $\xi$  is polynomial in the size of  $\mathcal{T}$ .*

**Proof.** Let  $\mathcal{A} = (Q, \iota, F, \Delta)$  with  $Q$  the set of states,  $\iota$  the initial state,  $F$  the set of final states, and  $\Delta \subseteq Q \times 2^{\Sigma_{\text{Clocks}}^{\text{DS}}} \times Q$  the transition relation. We denote a transtion  $\delta \in \Delta$  by  $\delta = (\text{src}(\delta), \text{lab}(\delta), \text{tgt}(\delta))$ , where  $\text{src}$ ,  $\text{tgt}$  are source and target states and  $\text{lab}(\delta)$  is the set of timed instructions labeling a transition. For simplicity, we assume that the data structure value (e.g., messages, stack symbols, etc) is a singleton set. Later we indicate how this can also be extended to a finite alphabet of data structure values.

Now, we write a formula  $\xi$  to capture the accepted sequences of sets of instructions in EQ-LCPDL. We start by guessing the states and instructions visited along an accepting run, i.e., we write

$$\xi = \exists q_1 \dots q_n \xi'$$

where  $\xi'$  is built as a conjunction of the following subformulae which check the conditions of being an accepting run. Let us describe each subformula along with the property that it is expected to capture.

- *States.* Every position in the run is labeled by a unique state.

$$\Psi_{\text{state}} = \mathbf{A} \bigvee_{q \in Q} \left( q \wedge \bigwedge_{q' \in Q \setminus \{q\}} \neg q' \right)$$

- *Transitions.* Every forward edge must have a corresponding transition either from the previous source state to a next target state, or from an initial state to the target state. Further, all node labels (instructions) are those mentioned in the transitions associated with the nodes.

$$\begin{aligned} \Psi_{\text{trans}} &= \mathbf{A} \langle \rightarrow^{-1} \rangle \implies \bigvee_{\delta \in \Delta} \text{tgt}(\delta) \wedge \langle \rightarrow^{-1} \rangle \text{src}(\delta) \wedge \bigwedge_{r \in \text{lab}(\delta)} r \wedge \bigwedge_{r \in \Sigma_{\text{Clocks}}^{\text{DS}} \setminus \text{lab}(\delta)} \neg r \\ &\quad \wedge \mathbf{A} \neg \langle \rightarrow^{-1} \rangle \implies \bigvee_{\delta \in \Delta \mid \text{src}(\delta) = \iota} \text{tgt}(\delta) \wedge \bigwedge_{r \in \text{lab}(\delta)} r \wedge \bigwedge_{r \in \Sigma_{\text{Clocks}}^{\text{DS}} \setminus \text{lab}(\delta)} \neg r \\ &\quad \wedge \mathbf{A} \neg \langle \rightarrow \rangle \implies \bigvee_{q \in F} q \end{aligned}$$

- *Data structures.* All data structure policies must be followed accurately. Let **Stacks** be the set of LIFO-Stacks and **Queues** be the set of FIFO-queues in DS. Then we need to check the following properties: (i) every stack is LIFO; (ii) every queue is FIFO; (iii) data structure edges must go forward with respect to the linear order; (iv) at any transition labeled “write” (i.e., every node labeled  $w(d)$ ), there is a unique outgoing data structure edge, and at every read transition (i.e., every node labeled  $r(d)$ ), there is a

unique incoming data structure edge. We now write the formula to capture all of these as a conjunct of formulae, each capturing the above properties.

$$\begin{aligned}
\Psi_{DS} = & \bigwedge_{d \in \text{Stacks}} A(w(d) \Rightarrow \text{loop}(\rightarrow \cdot \langle \xrightarrow{d} \cdot \rightarrow + \text{test}\{\neg(w(d) \vee r(d))\} \cdot \rightarrow)^* \cdot \xrightarrow{d}^{-1})) \\
& \wedge \bigwedge_{d \in \text{Queues}} \neg E \text{loop}(\rightarrow^+ \cdot \xrightarrow{d} \cdot \rightarrow^+ \cdot \xrightarrow{d}^{-1}) \\
& \wedge \bigwedge_{d \in \text{DS}} \neg E \text{loop}((\rightarrow^+ \cdot \xrightarrow{d}) + (\rightarrow^+ \cdot \xrightarrow{d}^{-1} \cdot \xrightarrow{d}) + (\rightarrow^+ \cdot \xrightarrow{d} \cdot \xrightarrow{d}^{-1})) \\
& \wedge \bigwedge_{d \in \text{DS}} A(w(d) \Leftrightarrow \langle \xrightarrow{d} \rangle) \wedge A(r(d) \Leftrightarrow \langle \xrightarrow{d}^{-1} \rangle).
\end{aligned}$$

For simplicity, we also make some assumptions about the data structure access – in particular, at any node (event), only one data structure access operation is performed. Hence we cannot have a push and pop at the same time, etc. These can easily be captured as a conjunction of the below formula with  $\Psi_{DS}$ .

$$\Psi'_{DS} = \bigwedge_{d \in \text{DS}} \neg E(w(d) \wedge r(d)) \wedge \bigwedge_{d' \in \text{DS} \setminus \{d\}} \neg E((w(d) \vee r(d)) \wedge (w(d') \vee r(d'))).$$

Define  $\xi' = \Psi_{state} \wedge \Psi_{trans} \wedge \Psi_{DS} \wedge \Psi'_{DS}$ . The correctness of the above formula, in encoding an accepting run, can be argued as follows: for any  $(\emptyset, \gamma^{DS})$ -labeled linear graph  $G$  with  $n$  nodes,  $G \models \xi$  iff there exists a sequence of transitions  $\delta_1, \dots, \delta_n$  such that  $\text{src}(\delta_1) = \iota$  is the initial state,  $\text{tgt}(\delta_n)$  is a final state,  $\text{tgt}(\delta_j) = \text{src}(\delta_{j+1})$  for all  $1 \leq j < n$ , all data structure policies are followed, and the labels along this accepting run define a sequence  $\tau \in L(\mathcal{T})$  such that  $G = G_\tau$ . We observe at this point that in the above formula we did not check whether the graph produced by the system was a linear graph. Indeed, this is not possible in EQ-ICPDL. However, our statement is only about linear graphs, in other words, we assume that all graphs generated by our system are linear (which is of course true for any sequential system) and hence our proof is complete.

To handle data structures over an arbitrary message alphabet, we simply enhance our propositions with the alphabet of messages  $\text{Msg}$ . Then we can write formulae to check that each read or write is associated with a single message and the message at a read event is the message that was written at the matching write event.

$$\begin{aligned}
\Psi_{\text{msg}} = & \bigwedge_{d \in \text{DS}} A(w(d) \Rightarrow \bigvee_{m \in \text{Msg}} m \wedge \langle \rightarrow \rangle m) \\
& \wedge \bigwedge_{m \in \text{Msg}} A(m \Rightarrow \bigwedge_{m' \in \text{Msg} \setminus \{m\}} \neg m' \wedge \bigvee_{d \in \text{DS}} w(d) \vee r(d))
\end{aligned}$$

This concludes the proof. ◀