On the Schedulability of Real-Time Discrete-Event Systems*

Eleftherios Matsikoudis Christos Stergiou Edward A. Lee

Abstract

We consider end-to-end latency specifications for hard real-time embedded systems. We introduce a discrete-event programming model generalizing such specifications, and address its schedulability problem for uniprocessor systems. This turns out to be rather idiosyncratic, involving complex, time-dependent release predicates and precedence constraints, quite unlike anything we have seen in the hard real-time computing literature. We prove the optimality of the earliest-deadline-first scheduling policy, and provide an algorithmic solution, reducing the schedulability problem to a reachability problem for timed automata.

1 Introduction

One of the defining features of embedded software, and one setting it apart from general-purpose computing, is its intimate relationship with the notion of time. Embedded programs are expected to interact with an inherently timed physical world, and are thus required to embrace time as part of their semantics. This is perhaps best exemplified by computer-control systems, which are required to sense the physical world and act upon it, all in a timely manner.

A computer-control system can be typically represented as a diagram of the form depicted in Figure 1(a). A sensor is producing measurements of the environment at certain instances of time. Each measurement is processed, and in response, an action on the environment is generated, and handed to an actuator responsible for carrying it through. What is often critical is that each action be delivered to the actuator within a certain time interval beginning from the time of the corresponding measurement. This interval is often chosen based on the control algorithm in use, and the control designer will often try to enforce it by specifying a certain desired latency from a measurement at the sensor to a response to it from the actuator. The system engineer is then responsible for implementing the system in such a way that the latency requirement is met. But this is hardly rocket science. Assuming a latency specification L and a worst-case computation time W required for processing a measurement, the latency requirement can be met just as long as there are no more than $\lceil \frac{L}{W} \rceil$ measurements in any time window of size W.

It is worth noting here that the computation performed over different measurements may preserve a notion of state from one invocation to the next. Consequently, successive measurements have to be processed in the order that they are received, and cannot overlap in time.

Of course, the simple structure of Figure 1(a) may be replicated any number of times to produce systems with more than one sensor-to-actuator path, each with its own latency requirement, as depicted in Figure 1(b). The job of the engineer is a little harder now, because the computing resources of the system

* This work was supported in part by the Center for Hybrid and Embedded Software Systems (CHESS) at UC Berkeley, which receives support from the National Science Foundation (NSF awards #0720882 (CSR-EHS: PRET), #1035672 (CPS: PTIDES), and #0931843 (ActionWebs)), the U. S. Army Research Lab (ARL #W911NF-11-2-0038), the Air Force Research Lab (AFRL), the Multiscale Systems Center (MuSyC), one of six research centers funded under the Focus Center Research Program, a Semiconductor Research Corporation program, and the following companies: Bosch, National Instruments, Thales, and Toyota.

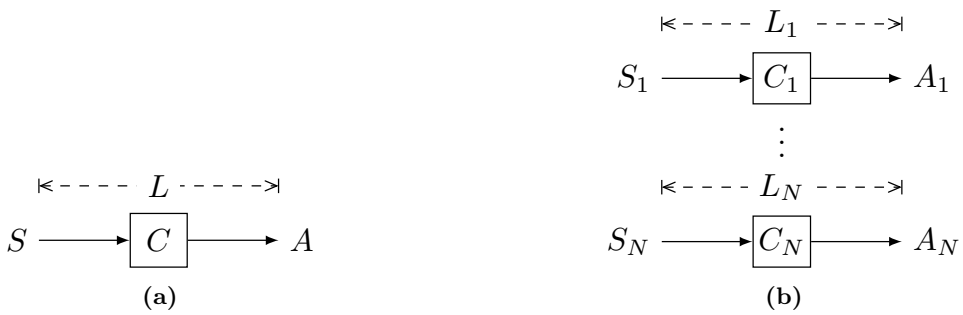

Figure 1. Simple path-latency specifications.

are now shared among the different paths, which must be scheduled in a way that ensures that all different latency requirements are satisfied. Still, this is well trodden territory. In the case of periodic or sporadic measurements, and assuming a single processing unit, one can rely on the classical hard real-time scheduling theory (e.g., see [2]), whereas for more complex input models, one may turn to more recent advances in algorithmic solutions (e.g., see [8]).

Things start to get interesting when one is considering merging paths from different sensors to a single actuator, as in Figure 2(a). If the latencies of the two paths are the same, nothing really changes; measurements at the two sensors may be thought of as jobs of the same task, and processed in the order received, with the exception of simultaneous measurements, which are to be treated as a single job. But what if one is inclined to specify different latencies for the two paths? How is the engineer supposed to execute such a specification? More importantly, what is the designer meant to specify? And is such a specification always meaningful?

Suppose that the latency specification from sensor S_1 to the actuator A is strictly larger than that from sensor S_2 to A; that is, $L_1 > L_2$. And suppose that S_1 produces a measurement m_1 at time t_1. Can m_1 be processed at t_1? If it is, and at some time t_2 between t_1 and $t_1 + (L_1 - L_2)$, S_2 produces a measurement m_2, then the actuation caused by m_1 will be performed after the actuation caused by m_2, even though m_1 was processed before m_2. But surely, this cannot be the intention of any rational designer wishing to merge the measurements of two different sensors through a common, possibly stateful processing component. In other words, the relative order of actuation times translates into a processing order on shared components. And therefore, assuming that m_2 can be produced at any time t_2 between t_1 and $t_1 + (L_1 - L_2)$, m_1 cannot be processed until it is possible to guarantee that $t_1 + L_1 \leq t_2 + L_2$, which is not until $t_1 + (L_1 - L_2)$.

But what if one tries to do the same on a more complex structure with two sensors and two actuators, arranged as in Figure 2(b)? Here, the designer might be tempted to specify four different latencies, one for each pair of sensor and actuator. However, not all possible choices make sense. For example, suppose that $L_1 > L_2$. Then, by the above reasoning, if S_1 produces m_1 at time t_1, and S_2 produces m_2 at time t_2 between t_1 and $t_1 + (L_1 - L_2)$, then m_1 must be processed after m_2. But if $t_1 + L_3 < t_2 + L_4$, then m_1 must be processed before m_2. And this is actually possible in the case that $L_3 - L_4 < L_1 - L_2$. Therefore, it must be the case that $L_3 - L_4 \geq L_1 - L_2$. But then $L_3 > L_4$, and by a symmetric argument, $L_1 - L_2 \geq L_3 - L_4$. So L_1, L_2, L_3, and L_4 must satisfy the equation $L_1 - L_2 = L_3 - L_4$ if the specification of the designer is to make any sense. What this means is that the designer is expected to come up with a real-time specification in terms of a number of dependent variables, a rather unappealing and impractical way to design systems, which is unlikely to scale well on yet more complex structures.

Luckily, there is a very natural solution to this problem. The way to go from dependent to independent variables is to forgo the notion of a path latency in favour of a notion of a link delay. For example, to return to the system in Figure 2(a), one may specify a delay D_1 on the link from S_1 to the processing

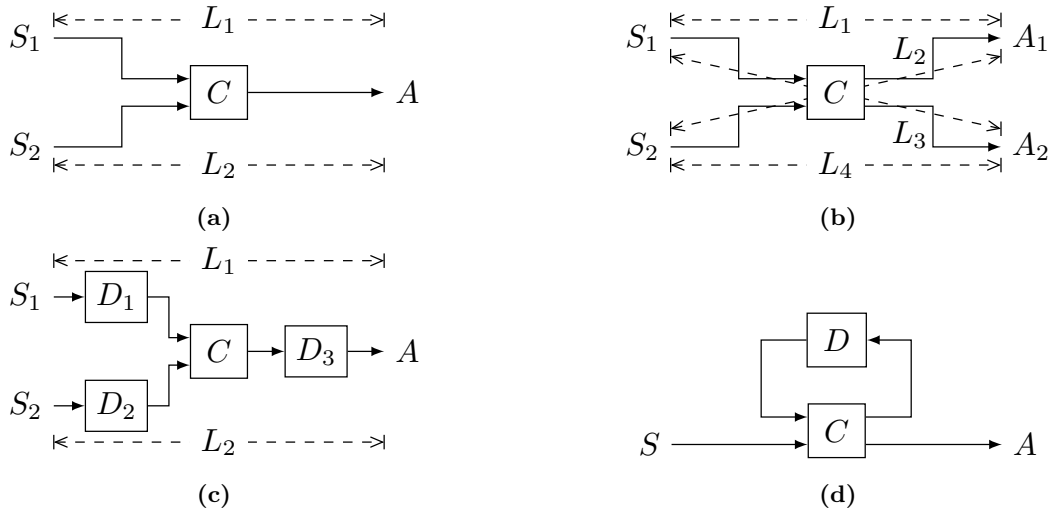

Figure 2. Delay versus latency specification examples.

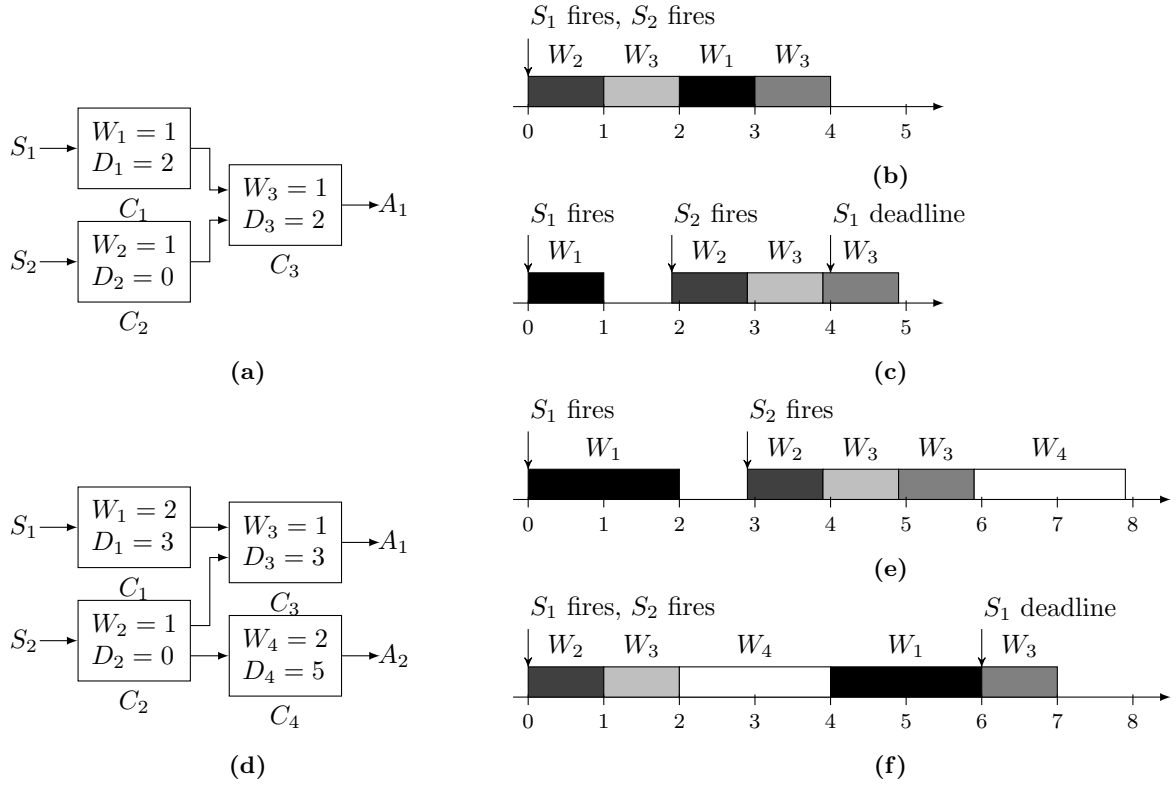

Figure 3. Maximizing processor demand (b), (f) versus waiting time (c), (e) as worst-case scenarios

component C, a delay D_2 on the link from S_2 to C, and a delay D_3 on the link from C to A, as in Figure 2(c), and by setting $D_1 = L_1 - L_2$, $D_2 = 0$, and $D_3 = L_2$, one can prescribe the same end-to-end

latencies as before. And one can populate the links of the system in Figure 2(b) with any arbitrary choice of delays without any fear of ending up with nonsensical specifications. Once liberated from the notion of path latency, the designer may even begin to think of systems with feedback loops, as in Figure 2(d), where end-to-end latency specifications are at the very least incomplete, if not ambiguous.

Interestingly, it is now possible to come up with the same latency specification in more than one way. For example, in Figure 2(c), one may specify the same end-to-end latencies as before by setting $D_1 = L_1$, $D_2 = L_2$, and $D_3 = 0$. This raises the question of what the semantics of a link-delay specification is, and whether different delay specifications corresponding to identical latency specifications should be implemented differently by the system engineer.

One way to address this question is by making use of the above observation that the relative order of actuation times translates into a processing order on shared components. Of course, in order to resolve processing decisions at shared components deep inside the system, one would need to keep track of the paths traversed by the arriving tokens. And especially in the case of loops, this can become quite messy. But there is an equivalent, and we believe, more natural interpretation.

We may think of processing as a logical operation that takes no time, and transmission over a link as an operation that takes time equal to the delay associated with that link. For example, in the system of Figure 2(c), and according to the last delay specification above, a measurement at S_1 at time t is not available for processing at C until $t + L_1$, at which time it can be safely processed, along with any measurement arriving at that time through the link from S_2. This leads naturally to a programming model according to which programs are represented as block diagrams, and blocks correspond to components, or so-called "actors", consuming and producing time-stamped tokens, or so-called "events", conceptually ordered according to their time stamps. What we end up with is a discrete-event model of computation that is not used for modelling and simulation (e.g., see [6]), but for real-time programming (e.g., see [7]). Semantically then, different delay specifications correspond to different programs. However, the notion of time imparted by the time stamps is not a physical one, but a logical one. And while the designer is free to think of this as a timed programming model, and think of the components of the control algorithm and the physical world as living in the same space, and sharing the same temporal semantics, this is not required for the engineer. A measurement is initially time-stamped by the sensor with the actual time at which it was taken. It is then communicated between actors, which may increase the time stamp by some arbitrary but fixed amount before forwarding to the next actor, until it reaches an actuator, where the time stamp is interpreted as the actual time when actuation is to occur. It does not really matter when events are processed, as long as they are processed in time-stamp order. And the job of the engineer is to make sure that every event reaching an actuator is delivered before the time corresponding to its time stamp.

This amounts to a rather complex schedulability problem that has not been considered before in the hard real-time computing literature. A typical approach to schedulability problems is to reduce the problem of scheduling every possible scenario to the problem of scheduling a single "worst-case" scenario. And that "worst-case" scenario typically corresponds in one way or another to a job-arrival pattern that maximizes processor demand over a certain time window. But in our case, there is another factor that may contribute to a bad scenario. And the two pull in opposite directions (see also [1]).

For example, consider the system in Figure 3(a), where each actor is annotated with a worst-case execution time and a delay added to the time stamps of processed events. Suppose that both sensors produce events at time 0, as in Figure 3(b). This is a scenario that maximizes processor demand, and yet is perfectly schedulable. Now, suppose that, instead, S_1 produces an event e_1 at time 0, whereas S_2 produces an event e_2 at time $2 - \epsilon$ for some small ϵ, as in Figure 3(c). Then C_1 will begin processing e_1 at time 0, and having a worst-case execution time $W = 1$ and a delay $D = 2$, will produce an event e_1' at time 1 with time stamp 2. But since C_2 has a delay 0, e_1' cannot be processed by C_3 until real time reaches the time stamp of that event, namely 2, lest there be another event produced by S_2 at some time t between 1 and 2, and thus, another one by C_2 with time stamp t. Thus, the system remains idle for almost a unit of time, in order to make sure that events are safely processed in time stamp order. And after C_2 produces e_2' in response to

e_2, C_3 will have to process e'_2 before e'_1, since e'_2 has a time stamp of $2 - \epsilon$ whereas e'_1 a time stamp of 2. This causes the deadline of e'_1 to be missed. The reverse situation is exhibited by the system of Figure 3(d), where instead, trying to maximize the time wasted waiting for events to become safe to process does not yield the worst-case scenario.

Another source of complexity is the expressiveness of the proposed programming model. The ability to design systems with feedback loops comes with a cost, namely the possibility of unbounded accumulation of events circulating in these feedback loops, and thus, it is not immediately obvious that the schedulability problem is even decidable.

The purpose of this work is to address this schedulability problem for a uniprocessor system. Because of the above complications, it is unlikely that an analytical solution exists. Here, we consider an algorithmic solution. We introduce a detailed formalization of the programming model, prove that the earliest-deadline-first scheduling policy is optimal, and show that the schedulability problem can be reduced to a finite-state reachability problem. Finally, we describe how to carry out this reduction using timed automata. The formalism of timed automata is not intrinsic to our solution, but rather a convenient tool to seamlessly integrate system abstraction with different, and complex, input-event arrival models.

2 Events and signals

We fix $\mathbb{T}$ to be the set $\mathbb{R}_{\geq 0}$ of all non-negative real numbers, and use it to represent our time domain. In order to formalize our notion of event, we further postulate an infinite set C of *channels*, and an infinite set V of values.

Definition 2.1. A *sort* is a non-empty finite subset of C.

Sorts will serve to represent the interfaces of actors, and facilitate their composition into programs.

Definition 2.2. A *program event* of sort C is an ordered triple $\langle c, t^{\text{prog}}, v\rangle \in C \times \mathbb{T} \times \text{V}$.

We write $\text{E}^{\text{prog}}(C)$ for the set of all program events of sort C.

Assume a program event $e^{\text{prog}} = \langle c, t^{\text{prog}}, v\rangle$.

We write e^{prog} for c, $\mathsf{time}^{\text{prog}}\, e^{\text{prog}}$ for t^{prog}, and $\mathsf{val}\, e^{\text{prog}}$ for v.

Definition 2.3. A *program signal* of sort C is a single-valued[1] subset of $\text{E}^{\text{prog}}(C)$.

We write $\text{S}^{\text{prog}}(C)$ for the set of all program signals of sort C, and $\text{S}^{\text{prog}}_{\text{fin}}(C)$ for the set of all finite program signals of sort C.

We will use signals to represent inputs and outputs of programs, as well as store the events circulating inside programs, much like calendar queues in typical discrete-event simulation implementations.

Notice that the empty set is vacuously single-valued, and hence, by Definition 2.3, a program signal of every sort.

Assume $s^{\text{prog}} \in \text{S}^{\text{prog}}(C)$.

We say that s^{prog} is *discrete-event* if and only if there is an order-embedding from $\langle \{\mathsf{time}^{\text{prog}}\, e^{\text{prog}} \mid e^{\text{prog}} \in s^{\text{prog}}\}, \preceq\rangle$ to $\langle \mathbb{N}, \leq\rangle$.

[1] For every set A and B, and every $S \subseteq A \times B$, S is *single-valued* if and only if for any $\langle a_1, b_1\rangle, \langle a_2, b_2\rangle \in S$, if $a_1 = a_2$, then $b_1 = b_2$.

We write $\mathrm{S}_{\mathrm{DE}}^{\mathrm{prog}}(C)$ for the set of all discrete-event program signals of sort C.

Here, we will be interested only in discrete-event signals, admittedly the only practicable type of signals.

Notice that $\mathrm{S}_{\mathrm{fin}}^{\mathrm{prog}} \subseteq \mathrm{S}_{\mathrm{DE}}^{\mathrm{prog}} \subseteq \mathrm{S}^{\mathrm{prog}}$.

3 Actors

Actors are the basic blocks of computation in our programs. An actor is a stateful, in general, component that interfaces with its environment through a set of input and a set of output channels, what we call its input and output sort respectively. Each time it fires, it consumes a set of events from its input sort, and produces a set of events at its output sort, possibly updating its state in the process.

Definition 3.1. An *input action* of sort C is a non-empty single-valued subset α of $\mathrm{E}^{\mathrm{prog}}(C)$ such that for every $e_1^{\mathrm{prog}}, e_2^{\mathrm{prog}} \in \alpha$,

$$\mathsf{time}^{\mathrm{prog}}\, e_1^{\mathrm{prog}} = \mathsf{time}^{\mathrm{prog}}\, e_2^{\mathrm{prog}}.$$

We write $\mathrm{IA}(C)$ for the set of all input actions of sort C.

Assume $\alpha \in \mathrm{IA}(C)$.

We write $\mathsf{chan}\,\alpha$ for $\{\mathsf{chan}\, e^{\mathrm{prog}} \mid e^{\mathrm{prog}} \in \alpha\}$, and $\mathsf{time}^{\mathrm{prog}}\,\alpha$ for the unique $t^{\mathrm{prog}} \in \mathbb{T}$ such that for every $e^{\mathrm{prog}} \in \alpha$,

$$\mathsf{time}^{\mathrm{prog}}\, e^{\mathrm{prog}} = t^{\mathrm{prog}}.$$

Input actions restrict the possible input behaviours of actors, and are central to our perception of a time stamp as a logical time instant: an actor is perceived to fire at the unique logical time instant associated with the corresponding input action.

Definition 3.2. An *output action* of sort C is a single-valued subset α of $\mathrm{E}^{\mathrm{prog}}(C)$ such that for any $e_1^{\mathrm{prog}}, e_2^{\mathrm{prog}} \in \alpha$ such that $\mathsf{chan}\, e_1^{\mathrm{prog}} = \mathsf{chan}\, e_2^{\mathrm{prog}}$,

$$\mathsf{time}^{\mathrm{prog}}\, e_1^{\mathrm{prog}} = \mathsf{time}^{\mathrm{prog}}\, e_2^{\mathrm{prog}}.$$

We write $\mathrm{OA}(C)$ for the set of all output actions of sort C.

Unlike input actions, the events of an output action need not share the same time stamp. This is not inconsistent with our perception of time stamps as logical time instants. Output actions can be understood operationally: they schedule events in logical time according to their time stamps. What might seem strange, then, is why output actions are constrained to carry no more than one event per channel. This is a technical constraint that will simplify our analysis, without sacrificing any expressiveness, as can be easily shown.

Definition 3.3. An *actor* is an ordered sextuple $\langle S, s_{\mathrm{init}}, C_{\mathrm{in}}, C_{\mathrm{out}}, f, u\rangle$ such that the following are true:

1. S is a non-empty set;
2. $s_{\mathrm{init}} \in S$;
3. C_{in} is a sort;
4. C_{out} is a sort;

5. f is a function from $S \times \mathrm{IA}(C_{\mathrm{in}})$ to $\mathrm{OA}(C_{\mathrm{out}})$;
6. u is a function from $S \times \mathrm{IA}(C_{\mathrm{in}})$ to S.

Assume an actor $A = \langle S, s_{\mathrm{init}}, C_{\mathrm{in}}, C_{\mathrm{out}}, f, u \rangle$.

We write S^A for S, $\mathrm{s}^A_{\mathrm{init}}$ for s_{init}, $\mathrm{C}^A_{\mathrm{in}}$ for C_{in}, $\mathrm{C}^A_{\mathrm{out}}$ for C_{out}, f^A for f, and u^A for u.

We now identify the class of actors that we will consider in this work.

We say that A is *output-homogeneous* if and only if for every $\langle s, \alpha \rangle \in \mathrm{S}^A \times \mathrm{IA}(\mathrm{C}^A_{\mathrm{in}})$,

$$\{\mathsf{chan}\, e^{\mathrm{prog}} \mid e^{\mathrm{prog}} \in \mathrm{f}^A(\langle s, \alpha \rangle)\} = \mathrm{C}^A_{\mathrm{out}}.$$

An output-homogeneous actor is simply an actor that, when fired, produces a single event at each channel in its output sort. This is of course consistent with the way we described the programming model in the introduction but as it will be apparent later on, it is also a necessary condition in order to be able to statically determine event deadlines.

Assume an output-homogeneous actor A.

We say that A is *constant-delay* if and only if for every $c \in \mathrm{C}^A_{\mathrm{out}}$, there is $\delta \in \mathbb{Q}_{\geq 0}$ such that for every $\langle s, \alpha \rangle \in \mathrm{S}^A \times \mathrm{IA}(\mathrm{C}^A_{\mathrm{in}})$, and every $e^{\mathrm{prog}} \in \mathrm{f}^A(\langle s, \alpha \rangle)$ such that $\mathsf{chan}\, e^{\mathrm{prog}} = c$,

$$\mathsf{time}^{\mathrm{prog}}\, e^{\mathrm{prog}} = \mathsf{time}^{\mathrm{prog}}\, \alpha + \delta.$$

Constant-delay output-homogeneous actors are *causal* actors that produce events at fixed, non-negative logical time distances from the logical time instance associated with the events consumed.

Assume a constant-delay output-homogeneous actor A.

We write $\mathsf{delay}\, A$ for a function from $\mathrm{C}^A_{\mathrm{out}}$ to $\mathbb{Q}_{\geq 0}$ such that for every $c \in \mathrm{C}^A_{\mathrm{out}}$, every $\langle s, \alpha \rangle \in \mathrm{S}^A \times \mathrm{IA}(\mathrm{C}^A_{\mathrm{in}})$, and every $e^{\mathrm{prog}} \in \mathrm{f}^A(\langle s, \alpha \rangle)$ such that $\mathsf{chan}\, e^{\mathrm{prog}} = c$,

$$\mathsf{time}^{\mathrm{prog}}\, e^{\mathrm{prog}} = \mathsf{time}^{\mathrm{prog}}\, \alpha + (\mathsf{delay}\, A)(c).$$

4 Programs

For every actor A_1 and A_2, we say that A_1 and A_2 are *compatible* if and only if $\mathrm{C}^{A_1}_{\mathrm{in}} \cap \mathrm{C}^{A_2}_{\mathrm{in}} = \emptyset$ and $\mathrm{C}^{A_1}_{\mathrm{out}} \cap \mathrm{C}^{A_2}_{\mathrm{out}} = \emptyset$.

Definition 4.1. A *program* is a non-empty finite set of pairwise compatible constant-delay output-homogeneous actors.

Assume a program P.

We write $\mathsf{chan}\, P$ for $\bigcup \{\mathrm{C}^A_{\mathrm{in}}, \mathrm{C}^A_{\mathrm{out}} \mid A \in P\}$,$\mathrm{C}^P_{\mathrm{in}}$ for $\bigcup \{\mathrm{C}^A_{\mathrm{in}} \mid A \in P\} \setminus \bigcup \{\mathrm{C}^A_{\mathrm{out}} \mid A \in P\}$,and $\mathrm{C}^P_{\mathrm{out}}$ for $\bigcup \{\mathrm{C}^A_{\mathrm{out}} \mid A \in P\} \setminus \bigcup \{\mathrm{C}^A_{\mathrm{in}} \mid A \in P\}$.

$\mathsf{chan}\, P$ is the set of all channels appearing in a program, whereas $\mathrm{C}^P_{\mathrm{in}}$ and $\mathrm{C}^P_{\mathrm{out}}$ are the sets of all unconnected input and output actor channels respectively.

We use a labelled transition system to formalize all possible executions of P.

Definition 4.2. A *state* of P is an ordered triple $\langle Q, \iota, \varepsilon \rangle$ such that the following are true:

$$\text{input}\ \frac{l \in \mathsf{lab}_{\text{in}}\, P}{\langle Q, \iota, \varepsilon\rangle \xrightarrow{l}_P \langle Q \cup \{l\}, \iota, \varepsilon\rangle} \qquad \text{start}\ \frac{\langle A, \langle s, \alpha\rangle\rangle \in \mathsf{lab}_{\text{start}}\, P \quad \alpha \subseteq Q \quad \iota(A) = s}{\langle Q, \iota, \varepsilon\rangle \xrightarrow{\langle A, \langle s, \alpha\rangle\rangle}_P \langle Q \setminus \alpha, \iota \setminus \{\langle A, s\rangle\}, \varepsilon \cup \{\langle A, \langle s, \alpha\rangle\rangle\}\rangle}$$

$$\text{output}\ \frac{l \in \mathsf{lab}_{\text{out}}\, P \quad l \in Q}{\langle Q, \iota, \varepsilon\rangle \xrightarrow{l}_P \langle Q \setminus \{l\}, \iota, \varepsilon\rangle} \qquad \text{finish}\ \frac{\langle A, \alpha, s\rangle \in \mathsf{lab}_{\text{finish}}\, P \quad \mathrm{f}^A(\varepsilon(A)) = \alpha \quad \mathrm{u}^A(\varepsilon(A)) = s}{\langle Q, \iota, \varepsilon\rangle \xrightarrow{\langle A, \alpha, s\rangle}_P \langle Q \cup \alpha, \iota \cup \{\langle A, s\rangle\}, \varepsilon \setminus \{\langle A, \varepsilon(A)\rangle\}\rangle}$$

Figure 4. Program transition rules.

1. $Q \in \mathrm{S}^{\text{prog}}_{\text{fin}}(\mathsf{chan}\, P)$;
2. there is a partition $\{P_{\text{idle}}, P_{\text{exec}}\}$ of P such that the following are true:
   (a) ι is a function from P_{idle} such that for any $A \in P_{\text{idle}}$, $\iota(A) \in \mathrm{S}^A$;
   (b) ε is a function from P_{exec} such that for any $A \in P_{\text{exec}}$, $\varepsilon(A) \in \mathrm{S}^A \times \mathrm{IA}(\mathrm{C}^A_{\text{in}})$.

We write $\mathsf{state}\, P$ for the set of all states of P.

A state $\langle Q, \iota, \varepsilon\rangle$ of P captures the composite state of P at some particular time instant during its execution: Q represents the set of all events circulating inside the program, ι the set of all idle actors, along with their state, and ε the set of all executing actors, along with their state and input events processed.

We write $\mathsf{state}_{\text{init}}\, P$ for a state $\langle Q, \iota, \varepsilon\rangle$ of P such that the following are true:

1. Q is the empty program signal;
2. ι is a function from P such that for every $A \in P$,
$$\iota(A) = \mathrm{s}^A_{\text{init}};$$
3. ε is the empty function.

The labels of the transition system that we will associate with P represent the possible actions of P. P can either receive an event from its environment, have an idle actor start processing an input action, have a processing actor finish its execution and produce an output action, or send an event to its environment.

We write $\mathsf{lab}_{\text{in}}\, P$ for $\mathrm{E}^{\text{prog}}(\mathrm{C}^P_{\text{in}})$, $\mathsf{lab}_{\text{start}}\, P$ for

$$\{\langle A, \langle s, \alpha\rangle\rangle \mid A \in P,\ s \in \mathrm{S}^A, \text{ and } \alpha \in \mathrm{IA}(\mathrm{C}^A_{\text{in}})\},$$

$\mathsf{lab}_{\text{finish}}\, P$ for

$$\{\langle A, \alpha, s\rangle \mid A \in P,\ \alpha \in \mathrm{OA}(\mathrm{C}^A_{\text{out}}), \text{ and } s \in \mathrm{S}^A\},$$

$\mathsf{lab}_{\text{out}}\, P$ for $\mathrm{E}^{\text{prog}}(\mathrm{C}^P_{\text{out}})$, and $\mathsf{lab}\, P$ for

$$\mathsf{lab}_{\text{in}}\, P \cup \mathsf{lab}_{\text{start}}\, P \cup \mathsf{lab}_{\text{finish}}\, P \cup \mathsf{lab}_{\text{out}}\, P.$$

We write $\longrightarrow_P$ for a ternary relation between $\mathsf{state}\, P$, $\mathsf{lab}\, P$, and $\mathsf{state}\, P$ defined by the rules in Figure 4.

We write $\langle Q_1, \iota_1, \varepsilon_1\rangle \xrightarrow{l}_P \langle Q_2, \iota_2, \varepsilon_2\rangle$ if and only if $\longrightarrow_P(\langle Q_1, \iota_1, \varepsilon_1\rangle, l, \langle Q_2, \iota_2, \varepsilon_2\rangle)$.

We write $\langle Q_1, \iota_1, \varepsilon_1\rangle \xrightarrow{l}^{\text{in}}_P \langle Q_2, \iota_2, \varepsilon_2\rangle$ if and only if $\langle Q_1, \iota_1, \varepsilon_1\rangle \xrightarrow{l}_P \langle Q_2, \iota_2, \varepsilon_2\rangle$ and $l \in \mathsf{lab}_{\text{in}}\, P$.

We write $\langle Q_1, \iota_1, \varepsilon_1\rangle \xrightarrow{l}^{\text{start}}_P \langle Q_2, \iota_2, \varepsilon_2\rangle$ if and only if $\langle Q_1, \iota_1, \varepsilon_1\rangle \xrightarrow{l}_P \langle Q_2, \iota_2, \varepsilon_2\rangle$ and $l \in \mathsf{lab}_{\text{start}}\, P$.

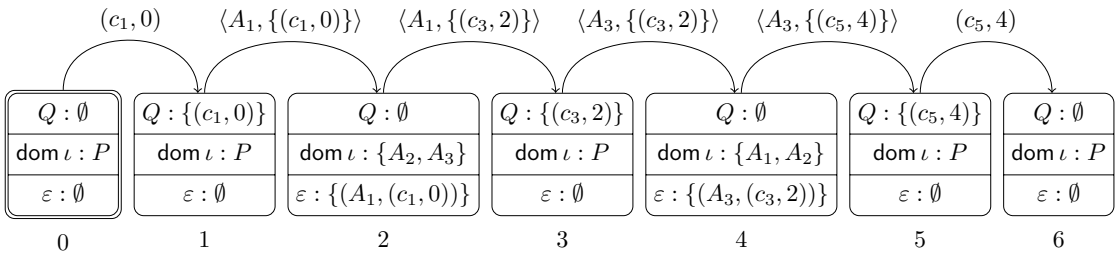

Figure 5. An example of a finite execution of the program of Figure 3(a), where event values and actor states have been omitted.

We write $\langle Q_1, \iota_1, \varepsilon_1\rangle \xrightarrow{l}{}^{\text{finish}}_{P} \langle Q_2, \iota_2, \varepsilon_2\rangle$ if and only if $\langle Q_1, \iota_1, \varepsilon_1\rangle \xrightarrow{l}_P \langle Q_2, \iota_2, \varepsilon_2\rangle$ and $l \in \mathsf{lab}_{\text{finish}}\, P$.

We write $\langle Q_1, \iota_1, \varepsilon_1\rangle \xrightarrow{l}{}^{\text{out}}_{P} \langle Q_2, \iota_2, \varepsilon_2\rangle$ if and only if $\langle Q_1, \iota_1, \varepsilon_1\rangle \xrightarrow{l}_P \langle Q_2, \iota_2, \varepsilon_2\rangle$ and $l \in \mathsf{lab}_{\text{out}}\, P$.

Definition 4.3. An *execution* of P is a non-empty sequence E^{prog} such that the following are true:

1. $E^{\text{prog}}(0) = \mathsf{state}_{\text{init}}\, P$;
2. one of the following is true:
   (a) E^{prog} is finite, and the following are true:
      i. for any $n < (|E^{\text{prog}}| - 1)/2$, $E^{\text{prog}}_{2n} \xrightarrow{E^{\text{prog}}_{2n+1}}_P E^{\text{prog}}_{2n+2}$;
      ii. for every l and $\langle Q, \iota, \varepsilon\rangle$, if $E^{\text{prog}}(|E^{\text{prog}}| - 1) \xrightarrow{l}_P \langle Q, \iota, \varepsilon\rangle$, then $l \in \mathsf{lab}_{\text{in}}\, P$;
   (b) E^{prog} is infinite, and for every $n \in \mathbb{N}$, $E^{\text{prog}}_{2n} \xrightarrow{E^{\text{prog}}_{2n+1}}_P E^{\text{prog}}_{2n+2}$.

Figure 5 displays an example of a finite execution of the program of Figure 3(a), where event values and actor states have been omitted.

Assume an execution E^{prog} of P.

Assume $L \subseteq \mathsf{lab}\, P$.

We write $L\text{-}\mathsf{trace}\, E^{\text{prog}}$ for a sequence over L such that for every $n \in \mathbb{N}$,

$$(L\text{-}\mathsf{trace}\, E^{\text{prog}})(n) \simeq E^{\text{prog}}(\min\{n' \mid n < |\{n'' \mid n'' \leq n' \text{ and } E^{\text{prog}}(n'') \in L\}|\}).$$

We write $\mathsf{trace}_{\text{in}}\, E^{\text{prog}}$ for $(\mathsf{lab}_{\text{in}}\, P)\text{-}\mathsf{trace}\, E^{\text{prog}}$.

For every $A \in P$, we write $\mathsf{trace}^A_{\text{start}}\, E^{\text{prog}}$ for $\{\langle A, \langle s, \alpha\rangle\rangle \mid s \in \mathrm{S}^A \text{ and } \alpha \in \mathrm{IA}(\mathrm{C}^A_{\text{in}})\}\text{-}\mathsf{trace}\, E^{\text{prog}}$.

For every $A \in P$, we write $\mathsf{trace}_{\text{finish}\, A}\, E^{\text{prog}}$ for $\{\langle A, \alpha, s\rangle \mid \alpha \in \mathrm{OA}(\mathrm{C}^A_{\text{out}}) \text{ and } s \in \mathrm{S}^A\}\text{-}\mathsf{trace}\, E^{\text{prog}}$.

For every $c \in \mathrm{C}^P_{\text{out}}$, we write $\mathsf{trace}_{\text{out}\, c}\, E^{\text{prog}}$ for $\mathrm{E}^{\text{prog}}(\{c\})\text{-}\mathsf{trace}\, E^{\text{prog}}$.

We write $\mathsf{in}\, E^{\text{prog}}$ for $\{E^{\text{prog}}_{2n+1} \mid n \in \mathbb{N} \text{ and } E^{\text{prog}}_{2n+1} \in \mathsf{lab}_{\text{in}}\, P\}$.

We write $\mathsf{out}\, E^{\text{prog}}$ for $\{E^{\text{prog}}_{2n+1} \mid n \in \mathbb{N} \text{ and } E^{\text{prog}}_{2n+1} \in \mathsf{lab}_{\text{out}}\, P\}$.

Notice that $\mathsf{in}\, E^{\text{prog}} \in \mathrm{S}^{\text{prog}}(\mathrm{C}^P_{\text{in}})$ and $\mathsf{out}\, E^{\text{prog}} \in \mathrm{S}^{\text{prog}}(\mathrm{C}^P_{\text{out}})$.

Clearly, our definition of execution is too liberal. In particular, it allows for executions where an actor processes its inputs out of time-stamp order, what is at odds with the intended role of time stamps as a logical notion of time.

We say that E^{prog} is *actor-safe* if and only if for every $A \in P$, and any n_1, $\langle Q_1, \iota_1, \varepsilon_1 \rangle$, and $\langle s_1, \alpha_1 \rangle$ such that

$$E^{\text{prog}}_{2n_1} = \langle Q_1, \iota_1, \varepsilon_1 \rangle$$

and

$$\varepsilon_1(A) = \langle s_1, \alpha_1 \rangle,$$

and any n_2, $\langle Q_2, \iota_2, \varepsilon_2 \rangle$, and $\langle s_2, \alpha_2 \rangle$ such that

$$E^{\text{prog}}_{2n_2} = \langle Q_2, \iota_2, \varepsilon_2 \rangle$$

and

$$\varepsilon_2(A) = \langle s_2, \alpha_2 \rangle,$$

if $n_1 < n_2$, then $\mathsf{time}^{\text{prog}}\, \alpha_1 < \mathsf{time}^{\text{prog}}\, \alpha_2$.

We say that E^{prog} is *output-safe* if and only if for every $c \in \mathrm{C}^P_{\text{out}}$, and any n_1 and n_2 such that $E^{\text{prog}}_{2n_1+1} \in \mathrm{E}^{\text{prog}}(\{c\})$ and $E^{\text{prog}}_{2n_2+1} \in \mathrm{E}^{\text{prog}}(\{c\})$, if $n_1 < n_2$, then $\mathsf{time}^{\text{prog}}\, E^{\text{prog}}_{2n_1+1} < \mathsf{time}^{\text{prog}}\, E^{\text{prog}}_{2n_2+1}$.

We say that E^{prog} is *safe* if and only if E^{prog} is actor-safe and output-safe.

Informally, an execution is safe just as long as every actor processes its input events in time-stamp order. Notice that safety does not constrain a program to process every single event in time-stamp order, only that each actor does so.

Another worrisome type of execution allowed by our definition is that of one where either an event in the program remains unprocessed indefinitely, or an actor is not given the opportunity to finish processing, or an output event of the program is never sent to the environment.

We say that E^{prog} is *actor-fair* if and only if for every $A \in P$, the following are true:

1. for any n and $\langle Q, \iota, \varepsilon \rangle$ such that

   $$E^{\text{prog}}_{2n} = \langle Q, \iota, \varepsilon \rangle,$$

   if $A \in \mathsf{dom}\, \iota$, and there is $e^{\text{prog}} \in Q$ such that $\mathsf{chan}\, e^{\text{prog}} \in \mathrm{C}^A_{\text{in}}$, then there is n', $\langle Q', \iota', \varepsilon' \rangle$, s', and α' such that $n < n'$,

   $$E^{\text{prog}}_{2n'} = \langle Q', \iota', \varepsilon' \rangle,$$

   $A \in \mathsf{dom}\, \varepsilon'$,

   $$\varepsilon'(A) = \langle s', \alpha' \rangle,$$

   and $e^{\text{prog}} \in \alpha'$;

2. for any n and $\langle Q, \iota, \varepsilon \rangle$ such that

   $$E^{\text{prog}}_{2n} = \langle Q, \iota, \varepsilon \rangle,$$

   if $A \in \mathsf{dom}\, \varepsilon$, then there is n' and $\langle Q', \iota', \varepsilon' \rangle$ such that $n < n'$,

   $$E^{\text{prog}}_{2n'} = \langle Q', \iota', \varepsilon' \rangle,$$

   and $A \in \mathsf{dom}\, \iota'$.

We say that E^{prog} is *output-fair* if and only if for every $c \in \mathrm{C}_{\text{out}}^P$, and any n and $\langle Q, \iota, \varepsilon \rangle$ such that

$$E_{2n}^{\text{prog}} = \langle Q, \iota, \varepsilon \rangle,$$

if there is $e^{\text{prog}} \in Q$ such that

$$\mathsf{chan}\, e^{\text{prog}} = c,$$

then there is n' such that $n \leq n'$ and

$$E_{2n'+1}^{\text{prog}} = e^{\text{prog}}.$$

We say that E^{prog} is *fair* if and only if E^{prog} is actor-fair and output-fair.

We say that E^{prog} is *correct* if and only if E^{prog} is safe and fair.

Correct executions of a program constitute a semantic specification of valid implementations of that program.

Theorem 4.4. *For every correct execution E_1^{prog} and E_2^{prog} of P, if*

$$\mathsf{in}\, E_1^{\text{prog}} = \mathsf{in}\, E_2^{\text{prog}},$$

then the following are true:

1. *for every $A \in P$, the following are true:*
   (a) $\mathsf{trace}_{\text{start}}^A\, E_1^{\text{prog}} = \mathsf{trace}_{\text{start}}^A\, E_2^{\text{prog}}$;
   (b) $\mathsf{trace}_{\text{finish}\, A}\, E_1^{\text{prog}} = \mathsf{trace}_{\text{finish}\, A}\, E_2^{\text{prog}}$;
2. *for every $c \in \mathrm{C}_{\text{out}}^P$,*

$$\mathsf{trace}_{\text{out}\, c}\, E_1^{\text{prog}} = \mathsf{trace}_{\text{out}\, c}\, E_2^{\text{prog}}.$$

Proof. We will show that for every $A \in P$, $\mathsf{trace}_{\text{start}}^A\, E_1^{\text{prog}} = \mathsf{trace}_{\text{start}}^A\, E_2^{\text{prog}}$. The other statements follow easily.

We write $\alpha_i^{A,j}$ for the input action of the j^{th} start transition of actor A in execution E_i.

We write $s_i^{A,j}$ for the state of actor A at the j^{th} start transition of A in execution E_i.

Let n be the largest n such that for all $A \in P$:

$$\langle (\mathsf{trace}_{\text{start}}^A\, E_1^{\text{prog}})(0), \ldots, (\mathsf{trace}_{\text{start}}^A\, E_1^{\text{prog}})(n-1) \rangle = \langle (\mathsf{trace}_{\text{start}}^A\, E_2^{\text{prog}})(0), \ldots, (\mathsf{trace}_{\text{start}}^A\, E_2^{\text{prog}})(n-1) \rangle$$

This implies that there is $A \in P$ such that either $(\mathsf{trace}_{\text{start}}^A\, E_1^{\text{prog}}(n) \neq (\mathsf{trace}_{\text{start}}^A\, E_2^{\text{prog}}(n)$ or without loss of generality $|(\mathsf{trace}_{\text{start}}^A\, E_1^{\text{prog}}| > n$ and $|(\mathsf{trace}_{\text{start}}^A\, E_2^{\text{prog}}| = n$.

We examine those cases separately, first assume that $(\mathsf{trace}_{\text{start}}^A\, E_1^{\text{prog}})(n)$ exists but $(\mathsf{trace}_{\text{start}}^A\, E_2^{\text{prog}})(n)$ does not.

For any $e^{\text{prog}} \in \alpha_1^{A,n}$, if $\mathsf{chan}\, e^{\text{prog}} \in \mathrm{C}_{\text{in}}^P$ or there is $i < n$ and A' such that e^{prog} is produced by $(\mathsf{trace}_{\text{finish}}^{A'}\, E_1^{\text{prog}})(i)$ then e^{prog} is produced in E_2^{prog} as well, and by fairness $(\mathsf{trace}_{\text{start}}^A\, E_1^{\text{prog}})(n)$ exists.

Therefore for every $e^{\text{prog}} \in \alpha_1^{A,n}$, there is A' such that $\mathsf{chan}\, e^{\text{prog}} \in \mathrm{C}_{\text{out}}^{A'}$, $(\mathsf{trace}_{\text{start}}^{A'}\, E_1^{\text{prog}})(n)$ precedes $(\mathsf{trace}_{\text{start}}^A\, E_1^{\text{prog}})(n)$ in E_1^{prog}, and $|(\mathsf{trace}_{\text{start}}^{A'}\, E_2^{\text{prog}})| < n$.

If we apply the same reasoning as we did for A in the case of A' and so on, we will either find actor A'' such that $\mathrm{C}_{\text{in}}^{A''} \subseteq \mathrm{C}_{\text{in}}^P$ or reach actor A again. In the first case, since the input signals of A'' are the same in

E_1^{prog} and E_2^{prog}, the start transitions cannot differ. In the second case, we will have concluded that the n^{th} start transition of A precedes the n^{th} start transition of A which is also a contradiction.

Therefore it must be $|(\mathsf{trace}_{\text{start}}\, E_2^{\text{prog}})| > n$ and $(\mathsf{trace}^A_{\text{start}}\, E_1^{\text{prog}})(n) \neq (\mathsf{trace}^A_{\text{start}}\, E_2^{\text{prog}})(n)$.

Note that the value of $s_i^{A,n}$ depends on $\langle(\mathsf{trace}^A_{\text{start}}\, E_1^{\text{prog}})(0), \ldots, (\mathsf{trace}^A_{\text{start}}\, E_1^{\text{prog}})(n-1)\rangle$ therefore $s_1^{A,n} = s_2^{A,n}$, and it has to be that $\alpha_1^{A,n} \neq \alpha_2^{A,n}$.

One of the following is true:

1. $\mathsf{time}^{\text{prog}}\, \alpha_1^{A,n} > \mathsf{time}^{\text{prog}}\, \alpha_2^{A,n}$:

   Note that because E_1^{prog} is actor-safe, there cannot be any start transitions in E_1^{prog} that process the events in $\alpha_2^{A,n}$. Furthermore, because E_1^{prog} is actor-fair, we conclude that the events $\alpha_2^{A,n}$ are never produced in E_1^{prog}.

   Let e^{prog} be an event in $\alpha_2^{A,n}$, and A' the actor such that $\mathsf{chan}\, e^{\text{prog}} \in \mathrm{C}^{A'}_{\text{out}}$. Such an actor exists since if $\mathsf{chan}\, e^{\text{prog}} \in \mathrm{C}^{P}_{\text{in}}$ it would also exist in E_1^{prog}.

   Since E_2^{prog} is actor-safe and constant-delay, A' produces events in timestamp order. Furthermore, the first n start and finish transitions of A' are the same in E_1^{prog} and E_2^{prog}.

   Hence, we conclude that $(\mathsf{trace}^{A'}_{\text{start}}\, E_1^{\text{prog}})(n) \neq (\mathsf{trace}^{A'}_{\text{start}}\, E_2^{\text{prog}})(n)$, $\mathsf{time}^{\text{prog}}\, \alpha_1^{A',n} > \mathsf{time}^{\text{prog}}\, \alpha_2^{A',n}$, and $(\mathsf{trace}^{A'}_{\text{start}}\, E_2^{\text{prog}})(n)$ precedes $(\mathsf{trace}^{A}_{\text{start}}\, E_2^{\text{prog}})(n)$ in E_2^{prog}.

2. $\mathsf{time}^{\text{prog}}\, \alpha_1^{A,n} = \mathsf{time}^{\text{prog}}\, \alpha_2^{A,n}$:

   One of the following is true:

   - $\mathsf{chan}\, \alpha_1^{A,n} = \mathsf{chan}\, \alpha_2^{A,n}$: there is an upstream actor A' such that $(\mathsf{trace}^{A'}_{\text{start}}\, E_1^{\text{prog}})(n) \neq (\mathsf{trace}^{A'}_{\text{start}}\, E_2^{\text{prog}})(n)$, $(\mathsf{trace}^{A'}_{\text{start}}\, E_1^{\text{prog}})(n)$ precedes $(\mathsf{trace}^{A}_{\text{start}}\, E_1^{\text{prog}})(n)$ in E_1^{prog}, $(\mathsf{trace}^{A'}_{\text{start}}\, E_2^{\text{prog}})(n)$ precedes $(\mathsf{trace}^{A}_{\text{start}}\, E_2^{\text{prog}})(n)$ in E_2^{prog}, and $\mathsf{time}^{\text{prog}}\, \alpha_1^{A',n} = \mathsf{time}^{\text{prog}}\, \alpha_2^{A',n}$.
   - $\mathsf{chan}\, \alpha_1^{A,n} \neq \mathsf{chan}\, \alpha_2^{A,n}$: without loss of generality there is $e^{\text{prog}} \in \alpha_1^{A,n}$ such that $\mathsf{chan}\, e^{\text{prog}} \notin \mathsf{chan}\, \alpha_2^{A,n}$ and with the same reasoning as in case 1, we can conclude that there is A' such that $(\mathsf{trace}^{A'}_{\text{start}}\, E_1^{\text{prog}})(n) \neq (\mathsf{trace}^{A'}_{\text{start}}\, E_2^{\text{prog}})(n)$, $\mathsf{time}^{\text{prog}}\, \alpha_1^{A',n} < \mathsf{time}^{\text{prog}}\, \alpha_2^{A',n}$, $(\mathsf{trace}^{A'}_{\text{start}}\, E_1^{\text{prog}})(n)$ precedes $(\mathsf{trace}^{A}_{\text{start}}\, E_1^{\text{prog}})(n)$ in E_1^{prog}, and $(\mathsf{trace}^{A'}_{\text{start}}\, E_2^{\text{prog}})(n)$ precedes $(\mathsf{trace}^{A}_{\text{start}}\, E_2^{\text{prog}})(n)$.

In all cases, we can repeat the process for the upstream actor A' in the same way as when it was showed that both $(\mathsf{trace}^{A}_{\text{start}}\, E_1^{\text{prog}})(n)$ and $(\mathsf{trace}^{A}_{\text{start}}\, E_2^{\text{prog}})(n)$ must exist, and reach a contradiction.

□

The following is immediate:

Corollary 4.5. *For every correct execution E_1^{prog} and E_2^{prog} of P, if*

$$\mathsf{in}\, E_1^{\text{prog}} = \mathsf{in}\, E_2^{\text{prog}},$$

then

$$\mathsf{out}\, E_1^{\text{prog}} = \mathsf{out}\, E_2^{\text{prog}}.$$

Corollary 4.5 formally characterizes the determinacy of discrete-event programs. It asserts that as long as the logical notion of time in a program is not violated, in the rather loose sense of the safety property, and

each party involved is given the opportunity to make progress, the behaviour of the program is determinate with respect to input and output signals.

The question remains whether a program has correct executions at all, that is, other than the trivial one. Clearly, a program that contains cycles of zero logical-time delay cannot possibly have an execution where an event enters the cycle without violating either safety or fairness. Here, we exclude such ill-behaved programs from consideration.

We say that P is *well defined* if and only if for every non-empty $X \subseteq P$, there is $A \in X$ such that for every $A' \in X$,

$$(\mathsf{delay}\, A')^{-1}(0) \cap (\mathrm{C}_{\mathrm{in}}^{A}) = \emptyset.$$[2]

Assume a well defined program P.

Theorem 4.6. *For any non-Zeno* $s^{\mathrm{prog}} \in \mathrm{S}_{\mathrm{DE}}^{\mathrm{prog}}(\mathrm{C}_{\mathrm{in}}^{P})$*, there is a correct execution* E^{prog} *of* P *such that*

$$\mathsf{in}\, E^{\mathrm{prog}} = s^{\mathrm{prog}}.$$

Proof. We describe how to construct given a program P and an input signal s^{prog} a correct program execution E^{prog} such that $\mathsf{in}\, E^{\mathrm{prog}} = s^{\mathrm{prog}}$.

In every step, we describe how to extend a prefix of the program execution, in a way that guarantees that the execution is safe and fair. The prefix is extended with either an input transition, a start transition followed by the corresponding finish transition, or an output transition.

The initial prefix of the program execution is

$$E^{\mathrm{prog}}(0) = \mathsf{state}_{\mathrm{init}}\, P.$$

At the beginning of each iteration, we calculate the next event to be processed.

In the following we assume that the last state of the prefix is $\langle Q, \iota, \varepsilon \rangle$ and the remaining input signal is s^{prog}.

The source of the next event might be the input signal s^{prog}, or the program signal Q.

We define a function $(\mathsf{min\text{-}time}^{\mathrm{prog}} P)$ from $\mathrm{S}^{\mathrm{prog}}(\mathsf{chan}\, P)$ to $\mathbb{T}$ such that for every $s^{\mathrm{prog}\prime} \in \mathrm{S}^{\mathrm{prog}}(\mathsf{chan}\, P)$ $(\mathsf{min\text{-}time}^{\mathrm{prog}} P)(s^{\mathrm{prog}\prime}) = \min\{\mathsf{time}^{\mathrm{prog}}\, e^{\mathrm{prog}} \mid e^{\mathrm{prog}} \in s^{\mathrm{prog}\prime}\}$.

If we choose the event that has the smallest timestamp, then the resulting execution is guaranteed to be safe.

Let $\tau_i = (\mathsf{min\text{-}time}^{\mathrm{prog}} P)(s^{\mathrm{prog}})$ and $\tau_q = (\mathsf{min\text{-}time}^{\mathrm{prog}} P)(Q)$.

If $\tau_i \leq \tau_q$, let e_i^{prog} be an event in $\{e^{\mathrm{prog}} \mid e^{\mathrm{prog}} \in s^{\mathrm{prog}} \text{ and } \mathsf{time}^{\mathrm{prog}}\, e^{\mathrm{prog}} = \tau_i\}$ and $s^{\mathrm{prog}\prime} = s^{\mathrm{prog}} \setminus \{e_i^{\mathrm{prog}}\}$. We extend the program execution prefix with an input transition with label e_i^{prog} and the new state $\langle Q \cup \{e_i^{\mathrm{prog}}\}, \iota, \varepsilon \rangle$

If $\tau_i > \tau_q$, we will append a start and a finish transition, or an output transition.

Let $S = \{e^{\mathrm{prog}} \in Q \mid \mathsf{time}^{\mathrm{prog}}\, e^{\mathrm{prog}} = \tau_q\}$

We define an order between channels in $\mathsf{chan}\, P$ in the following way: $c_1 \prec c_2$ if and only if there is a sequence of actors $A_1, \ldots, A_N$ such that $c_1 \in \mathrm{C}_{\mathrm{in}}^{A_1}$, $c_2 \in \mathrm{C}_{\mathrm{in}}^{A_N}$, and for every i such that $1 \leq i < N$, $(\mathsf{delay}\, A_i)^{-1}(0) \cap \mathrm{C}_{\mathrm{in}}^{A_{i+1}} \neq \emptyset$.

[2]

We lift that order to program events and say that $e_1^{\text{prog}} \prec e_2^{\text{prog}}$ if and only if $\mathsf{chan}\, e_1^{\text{prog}} \prec \mathsf{chan}\, e_2^{\text{prog}}$.

Let S' be the set of events that are minimal elements of S according to $\prec$.

We prove now that S' cannot non-empty because P is well-defined.

By definition of τ_q, S is not empty. S' is empty if and only if S has no $\prec$-minimal elements. Note that S is finite since Q is single-valued and thus for every $c \in \mathsf{chan}\, P$, $|\{e^{\text{prog}} \in S \mid \mathsf{chan}\, e^{\text{prog}} = c\}| \leq 1$. Assume that S' is empty. The absence of a $\prec$-minimal element implies that there is a sequence $e_1, \ldots, e_N$ such that for every i such that $1 \leq i < N$, $e_i \prec e_{i+1}$, and $e_1 = e_N$. By the definition of $\prec$, given cycle $e_1 \prec \ldots \prec e_{N-1} \prec e_1$, we can construct a set of actors $X \subseteq P$ such that for every $A \in X$, there is $A' \in X$ such that $(\mathsf{delay}\, A')^{-1}(0) \cap \mathrm{C}_{\text{in}}^A \neq \emptyset$. That implies that P is not well-defined, therefore S' cannot be empty.

If the set $\{A \in P \mid \text{there is } e^{\text{prog}} \in S' \text{ such that } \mathsf{chan}\, e^{\text{prog}} \in \mathrm{C}_{\text{in}}^A\}$ is empty, then it must be the case that for every $e^{\text{prog}} \in S'$, $\mathsf{chan}\, e^{\text{prog}} \in \mathrm{C}_{\text{out}}^P$. In that case we pick an event e^{prog} from S' and add an output transition with label e^{prog}, and a state $\langle Q \setminus \{e^{\text{prog}}\}, \iota, \varepsilon \rangle$.

If the set is not empty, then let B be an actor in $\{A \in P \mid \text{there is } e^{\text{prog}} \in S' \text{ such that } \mathsf{chan}\, e^{\text{prog}} \in \mathrm{C}_{\text{in}}^A\}$, and $\alpha_{\text{input}} \in \mathrm{IA}(B)$ such that $\alpha_{\text{input}} = \{e^{\text{prog}} \in S' \mid \mathsf{chan}\, e^{\text{prog}} \in \mathrm{C}_{\text{in}}^B\}$.

We extend the current program execution prefix with a start transition for actor B with label l_{start} and input action α_{input}, a state $\langle Q', \iota', \varepsilon' \rangle$, a finish transition for actor B with label l_{finish}, and a final state $\langle Q'', \iota'', \varepsilon'' \rangle$.

Let s_B be the state of actor B at the beginning of the iteration, or $s_B = \iota(A_B)$, s_B'' the state of B after the finish transition, or $s_B'' = \mathrm{u}^B(\langle s_B, \alpha_{\text{input}} \rangle)$, and α_{output} the output action of the finish transition, or $\alpha_{\text{output}} = \mathrm{f}^B(\langle s_B, \alpha_{\text{input}} \rangle)$.

The label of the start transition will then be

$$l_{\text{start}} = \langle B, \langle s_B, \alpha_{\text{input}} \rangle \rangle,$$

the intermediate state

$$\langle Q', \iota', \varepsilon' \rangle = \langle Q \setminus \alpha_{\text{input}}, \iota \setminus \{\langle B, s_B \rangle\}, \varepsilon \cup \{l_{\text{start}}\} \rangle,$$

the label of the finish transition

$$l_{\text{finish}} = \langle B, \alpha_{\text{output}}, s_B'' \rangle,$$

and the final state

$$\langle Q'', \iota'', \varepsilon'' \rangle = \langle Q' \cup \alpha_{\text{output}}, \iota' \cup \{\langle B, s_B'' \rangle\}, \varepsilon' \setminus \{l_{\text{start}}\} \rangle.$$

The resulting execution is safe.

We know argue about its fairness.

First, the second part of the actor-fairness definition is satisfied because we explicitly accompany each start transition with the corresponding finish transition.

Second, for both the first part of actor-fairness and output-fairness we argue that in the resulting execution E^{prog} if there is n, $\langle Q, \iota, \varepsilon \rangle$, and e^{prog} such that $E^{\text{prog}}(n) = \langle Q, \iota, \varepsilon \rangle$, and $e^{\text{prog}} \in Q$, then there is n' and $\langle Q', \iota', \varepsilon' \rangle$ such that $(\mathsf{min\text{-}time}^{\text{prog}} P)(Q') > \mathsf{time}^{\text{prog}}\, e^{\text{prog}}$.

Let s^{prog} be the unprocessed input signal when $E^{\text{prog}}(n)$ was added in the program execution. At that point it could either be the case that $(\mathsf{min\text{-}time}^{\text{prog}} P)(s^{\text{prog}}) \leq (\mathsf{min\text{-}time}^{\text{prog}} P)(Q)$ or not. In the former case, because s^{prog} in non-Zeno, after a finite number of steps that add input transitions, the latter case will hold. W.l.o.g. we assume that it holds when the input is s^{prog} and $E^{\text{prog}}(n)$ is added.

The process described above will then add a pair of a start and a finish transition such that the program time of the input action is $(\mathsf{min\text{-}time}^{\mathrm{prog}}\, P)(Q)$ and the program time of the events in the output action is $\geq (\mathsf{min\text{-}time}^{\mathrm{prog}}\, P)(Q)$. Such start and finish transition pairs with an input action of program time equal to $(\mathsf{min\text{-}time}^{\mathrm{prog}}\, P)(Q)$ will continue to be added as long as there are events in the program with program time equal to $(\mathsf{min\text{-}time}^{\mathrm{prog}}\, P)(Q)$. Because P is well-defined, in a bounded number of transitions, the state of the program will be $\langle Q', \iota', \varepsilon' \rangle$ where $(\mathsf{min\text{-}time}^{\mathrm{prog}}\, P)(Q') \geq (\mathsf{min\text{-}time}^{\mathrm{prog}}\, P)(Q) + \delta$ and $\delta \geq \min\{(\mathsf{delay}\, A)(c) \mid A \in P,\ c \in \mathrm{C}^A_{\mathrm{out}}, \text{ and } (\mathsf{delay}\, A)(c) > 0\}$.

The program time of the input action of the next start transition will not be greater or equal than $(\mathsf{min\text{-}time}^{\mathrm{prog}}\, P)(Q) + \delta$ if the next input event has program time smaller than that. Note, however, that because the number of input events with program time between $(\mathsf{min\text{-}time}^{\mathrm{prog}}\, P)(Q)$ and $(\mathsf{min\text{-}time}^{\mathrm{prog}}\, P)(Q) + \delta$ is finite, since the input signal is non-Zeno, it is still guaranteed that in a finite number of steps there will be a start transition with input action with program time larger than or equal to $(\mathsf{min\text{-}time}^{\mathrm{prog}}\, P)(Q) + \delta$.

We can now repeat the reasoning above $\left\lceil \frac{\mathsf{time}^{\mathrm{prog}}\, e^{\mathrm{prog}} - (\mathsf{min\text{-}time}^{\mathrm{prog}}\, P)(Q)}{\delta} \right\rceil$ number of times.

□

Theorem 4.6 guarantees that any program free of zero logical-time delay cycles will have a correct execution for every possible discrete-event and non-Zeno input signal it is presented with.

We write $\mathsf{delay}\, P$ for a function from $\mathsf{chan}\, P \times \mathsf{chan}\, P$ to $\mathbb{Q}_{\geq 0} \cup \{\infty\}$ such that for every $c_1, c_2 \in \mathsf{chan}\, P$,

$$(\mathsf{delay}\, P)(c_1, c_2) = \begin{cases} 0 & \text{if } c_1 = c_2; \\ \infty & \text{if } c_1 \neq c_2 \text{ and } c_1 \in \mathrm{C}^P_{\mathrm{out}}; \\ \min\{(\mathsf{delay}\, A)(c) + (\mathsf{delay}\, P)(c, c_2) \mid A \in P, \ c_1 \in \mathrm{C}^A_{\mathrm{in}}, \text{ and } c \in \mathrm{C}^A_{\mathrm{out}}\} & \text{otherwise.} \end{cases}$$

5 Systems

Programs deal exclusively in logical time. There is nothing in their semantics that bears any relevance to physical time at all. But if we are to use them as executable real-time specifications, we need to determine how exactly these two different notions of time relate to one another.

Definition 5.1. A *system* is an ordered pair $\langle P, R \rangle$ such that the following are true:

1. P is a well-defined program;
2. R is a function from P to $\mathscr{P}_{\geq 1}\, \mathbb{T}$,[3] such that for every $A \in P$, $0 < \inf R(A) \leq \sup R(A)$ and $\sup R(A) \in \mathbb{Q}_{\geq 0}$.

Assume a system $\langle P, R \rangle$.

$\langle P, R \rangle$ is understood as a program P running on a given uniprocessor platform. The function R captures the computation-time requirements of each actor in P on that platform. We use a timed labelled transition system to formalize all possible executions of $\langle P, R \rangle$.

Definition 5.2. A *state* of $\langle P, R \rangle$ is an ordered sextuple $\langle Q, \iota, \varepsilon, \rho, \pi, t^{\mathrm{sys}} \rangle$ such that the following are true:

[3] For every set A, we write $\mathscr{P}_{\geq 1}\, A$ for the set of all non-empty subsets of A.

1. $\langle Q, \iota, \varepsilon \rangle \in \mathsf{state}\, P$;
2. ρ is a function from $\mathsf{dom}\, \varepsilon$ to $\mathbb{T}$ such that for any $A \in \mathsf{dom}\, \varepsilon$, there is $r \in R(A)$ such that

$$\rho(A) \leq r;$$

3. $\pi \in \{\texttt{NULL}\} \cup \{A \mid A \in \mathsf{dom}\, \varepsilon \text{ and } 0 < \rho(A)\}$;
4. $t^{\mathrm{sys}} \in \mathbb{T}$.

A state $\langle Q, \iota, \varepsilon, \rho, \pi, t^{\mathrm{sys}} \rangle$ of $\langle P, R \rangle$ augments the state of P with information on the actual state of the platform at some particular time instant during the execution of P. Specifically, ρ captures the remaining computation time of any processing actor, π represents the actor running on the processor at that time instant, and t^{sys} stands for that time instant.

We write $\mathsf{state}\, \langle P, R \rangle$ for the set of all states of $\langle P, R \rangle$.

We write $\mathsf{state}_{\mathrm{init}}\, \langle P, R \rangle$ for a state $\langle Q, \iota, \varepsilon, \rho, \pi, t^{\mathrm{sys}} \rangle$ of $\langle P, R \rangle$ such that the following are true:

1. $\langle Q, \iota, \varepsilon \rangle = \mathsf{state}_{\mathrm{init}}\, P$;
2. ρ is the empty function;
3. $\pi = \texttt{NULL}$;
4. $t^{\mathrm{sys}} = 0$.

Assume $\langle Q, \iota, \varepsilon, \rho, \pi, t^{\mathrm{sys}} \rangle \in \mathsf{state}\, \langle P, R \rangle$.

We write $\mathsf{prog}\, \langle Q, \iota, \varepsilon, \rho, \pi, t^{\mathrm{sys}} \rangle$ for $\langle Q, \iota, \varepsilon \rangle$.

We write $\mathsf{time}^{\mathrm{sys}}\, \langle Q, \iota, \varepsilon, \rho, \pi, t^{\mathrm{sys}} \rangle$ for t^{sys}.

We write $\mathsf{lab}_{\mathrm{in}}\, \langle P, R \rangle$ for $\mathsf{lab}_{\mathrm{in}}\, P$.

We write $\mathsf{lab}_{\mathrm{start}}\, \langle P, R \rangle$ for $\{\langle \langle A, \langle s, \alpha \rangle \rangle, r \rangle \mid \langle A, \langle s, \alpha \rangle \rangle \in \mathsf{lab}_{\mathrm{start}}\, P \text{ and } r \in R(A)\}$.

We write $\mathsf{lab}_{\mathrm{finish}}\, \langle P, R \rangle$ for $\mathsf{lab}_{\mathrm{finish}}\, P$.

We write $\mathsf{lab}_{\mathrm{out}}\, \langle P, R \rangle$ for $\mathsf{lab}_{\mathrm{out}}\, P$.

We write $\mathsf{lab}_{\mathrm{prog}}\, \langle P, R \rangle$ for $\mathsf{lab}_{\mathrm{in}}\, \langle P, R \rangle \cup \mathsf{lab}_{\mathrm{start}}\, \langle P, R \rangle \cup \mathsf{lab}_{\mathrm{finish}}\, \langle P, R \rangle \cup \mathsf{lab}_{\mathrm{out}}\, \langle P, R \rangle$.

For every $l \in \mathsf{lab}_{\mathrm{prog}}\, \langle P, R \rangle$, we write $\mathsf{prog}\, l$ for $\begin{cases} \langle A, \langle s, \alpha \rangle \rangle & \text{if } l \in \mathsf{lab}_{\mathrm{start}}\, \langle P, R \rangle, \text{ and there is } r \text{ such that } l = \langle \langle A, \langle s, \alpha \rangle \rangle, r \rangle; \\ l & \text{otherwise.} \end{cases}$

We write $\mathsf{lab}_{\mathrm{sch}}\, \langle P, R \rangle$ for $\{\texttt{NULL}\} \cup P$.

We write $\mathsf{lab}\, \langle P, R \rangle$ for $\mathsf{lab}_{\mathrm{prog}}\, \langle P, R \rangle \cup \mathsf{lab}_{\mathrm{sch}}\, \langle P, R \rangle$.

Notice that the labels related to an actor starting to process an input action are augmented with a rational number representing the amount of computation time that will be required for processing that input action.

We write $\longrightarrow_{\langle P, R \rangle}$ for a ternary relation between $\mathsf{state}\, \langle P, R \rangle$, $\mathsf{lab}\, \langle P, R \rangle$, and $\mathsf{state}\, \langle P, R \rangle$ defined by the rules in Figure 6.

There are a few observations that need to be made here.

First, input and output actions of a system bind program time to system time and system time to program time respectively. One may think of an input channel of a program as connected to an ideal sensor that will time-stamp its measurements with the exact physical time at which they were made, and

$$\text{input}\ \frac{\langle Q_1, \iota_1, \varepsilon_1\rangle \xrightarrow{l}{}^{\text{in}}_{P} \langle Q_2, \iota_2, \varepsilon_2\rangle \qquad \mathsf{time}^{\text{prog}}\, l = t^{\text{sys}}}{\langle Q_1, \iota_1, \varepsilon_1, \rho, \pi, t^{\text{sys}}\rangle \xrightarrow{l}_{\langle P,R\rangle} \langle Q_2, \iota_2, \varepsilon_2, \rho, \pi, t^{\text{sys}}\rangle}$$

$$\text{output}\ \frac{\langle Q_1, \iota_1, \varepsilon_1\rangle \xrightarrow{l}{}^{\text{out}}_{P} \langle Q_2, \iota_2, \varepsilon_2\rangle \qquad \mathsf{time}^{\text{prog}}\, l = t^{\text{sys}}}{\langle Q_1, \iota_1, \varepsilon_1, \rho, \pi, t^{\text{sys}}\rangle \xrightarrow{l}_{\langle P,R\rangle} \langle Q_2, \iota_2, \varepsilon_2, \rho, \pi, t^{\text{sys}}\rangle}$$

$$\text{start}\ \frac{\langle Q_1, \iota_1, \varepsilon_1\rangle \xrightarrow{\langle A,\langle s,\alpha\rangle\rangle}{}^{\text{start}}_{P} \langle Q_2, \iota_2, \varepsilon_2\rangle \qquad r \in R(A) \qquad \rho_2 = \rho_1 \cup \{\langle A, r\rangle\}}{\langle Q_1, \iota_1, \varepsilon_1, \rho_1, \pi, t^{\text{sys}}\rangle \xrightarrow{\langle\langle A,\langle s,\alpha\rangle\rangle, r\rangle}_{\langle P,R\rangle} \langle Q_2, \iota_2, \varepsilon_2, \rho_2, \pi, t^{\text{sys}}\rangle}$$

$$\text{finish}\ \frac{\langle Q_1, \iota_1, \varepsilon_1\rangle \xrightarrow{\langle A,\alpha,s\rangle}{}^{\text{finish}}_{P} \langle Q_2, \iota_2, \varepsilon_2\rangle \qquad \rho_1(A) = 0 \qquad \rho_2 = \rho_1 \setminus \{\langle A, 0\rangle\}}{\langle Q_1, \iota_1, \varepsilon_1, \rho_1, A, t^{\text{sys}}\rangle \xrightarrow{\langle A,\alpha,s\rangle}_{\langle P,R\rangle} \langle Q_2, \iota_2, \varepsilon_2, \rho_2, \mathtt{NULL}, t^{\text{sys}}\rangle}$$

$$\text{context-switch}\ \frac{l \in \{\mathtt{NULL}\} \cup \mathsf{dom}\, \varepsilon}{\langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}}\rangle \xrightarrow{l}_{\langle P,R\rangle} \langle Q, \iota, \varepsilon, \rho, l, t^{\text{sys}}\rangle}$$

Figure 6. System transition rules.

$$\text{idle}\ \frac{\pi = \mathtt{NULL}}{\langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}}\rangle \xrightarrow{d}_{\langle P,R\rangle} \langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}} + d\rangle}$$

$$\text{busy}\ \frac{\pi \neq \mathtt{NULL} \qquad d \leq \rho_1(\pi) \qquad \rho_2(A) = \begin{cases} \rho_1(A) - d & \text{if } A = \pi; \\ \rho_1(A) & \text{otherwise;} \end{cases}}{\langle Q, \iota, \varepsilon, \rho_1, \pi, t^{\text{sys}}\rangle \xrightarrow{d}_{\langle P,R\rangle} \langle Q, \iota, \varepsilon, \rho_2, \pi, t^{\text{sys}} + d\rangle}$$

Figure 7. System time transition rules.

instantaneously deliver them to the program, and an output channel as connected to an ideal actuator that will actuate the environment instantaneously at the exact physical time dictated by the time stamp of the corresponding output event.

Second, every time an actor starts processing, a requirement for computation-time necessary to perform its processing is chosen nondeterministically, and the actor becomes available for execution. But it is not executed until the system decides to allocate the platform's processor to it. Once it starts executing, it can be preempted and resumed arbitrarily according to the scheduling decisions of the system.

And third, a processing actor finishes exactly when it has been allocated processor time equal to its corresponding computation-time requirement, at which point it is taken off the processor.

System-time progress is modeled using a different type of transition labelled with the amount of physical time elapsed.

We write $\langle Q_1, \iota_1, \varepsilon_1, \rho_1, \pi_1, t_1^{\text{sys}}\rangle \xrightarrow{l}_{\langle P,R\rangle} \langle Q_2, \iota_2, \varepsilon_2, \rho_2, \pi_2, t_2^{\text{sys}}\rangle$ if and only if $\longrightarrow_{\langle P,R\rangle}(\langle Q_1, \iota_1, \varepsilon_1, \rho_1, \pi_1, t_1^{\text{sys}}\rangle, l, \langle Q_2, \iota_2, \varepsilon_2, \rho_2, \pi_2, t_2^{\text{sys}}\rangle)$.

We write $\dashrightarrow_{\langle P,R\rangle}$ for a ternary relation between $\mathsf{state}\,\langle P, R\rangle$, $\mathbb{T}$, and $\mathsf{state}\,\langle P, R\rangle$ defined by the rules in Figure 7.

We write $\langle Q_1, \iota_1, \varepsilon_1, \rho_1, \pi_1, t_1^{\text{sys}}\rangle \xrightarrow{d}_{\langle P,R\rangle} \langle Q_2, \iota_2, \varepsilon_2, \rho_2, \pi_2, t_2^{\text{sys}}\rangle$ if and only if $\dashrightarrow_{\langle P,R\rangle}(\langle Q_1, \iota_1, \varepsilon_1, \rho_1, \pi_1, t_1^{\text{sys}}\rangle, d, \langle Q_2, \iota_2, \varepsilon_2, \rho_2, \pi_2, t_2^{\text{sys}}\rangle)$.

When the processor of the platform is free, there is no actor executing, and unless there is an actor

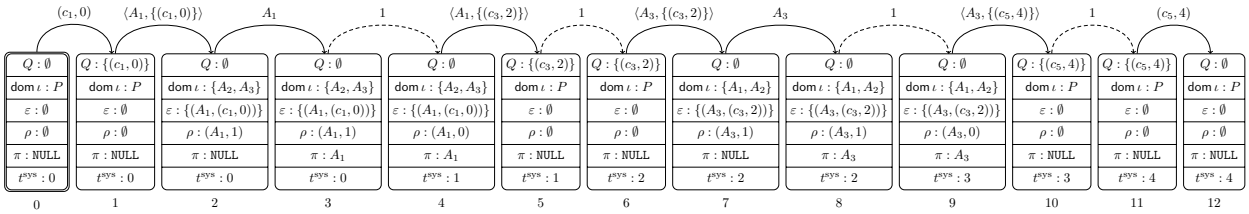

Figure 8. A prefix of an execution of the system of Figure 3(a) corresponding to the program execution of Figure 5, where event values and actor states have been omitted.

available for processing that the system decides to execute, system time may progress arbitrarily. But when the processor is allocated to a processing actor, system time cannot progress more than the remaining computation time of that actor, for at that point, a discrete transition corresponding to that actor finishing must occur.

Definition 5.3. An *execution* of $\langle P, R\rangle$ is an infinite sequence E^{sys} such that the following are true:

1. $E^{\text{sys}}(0) = \mathsf{state}_{\text{init}}\,\langle P, R\rangle$;
2. for every $n \in \mathbb{N}$, one of the following is true:
   (a) $E^{\text{sys}}_{2n} \xrightarrow{E^{\text{sys}}_{2n+1}}_{\langle P,R\rangle} E^{\text{sys}}_{2n+2}$;
   (b) $E^{\text{sys}}_{2n} \overset{E^{\text{sys}}_{2n+1}}{\dashrightarrow}_{\langle P,R\rangle} E^{\text{sys}}_{2n+2}$;
3. for every $t^{\text{sys}} \in \mathbb{T}$, there is n such that $t^{\text{sys}} \leq \mathsf{time}^{\text{sys}}\, E^{\text{sys}}_{2n}$.
4. for any n such that

$$\mathsf{time}^{\text{sys}}\, E^{\text{sys}}_{2n} = \mathsf{time}^{\text{sys}}\, E^{\text{sys}}_{2n+2},$$

   if $E^{\text{sys}}_{2n+3} \in \mathsf{lab}_{\text{in}}\,\langle P, R\rangle$, then $E^{\text{sys}}_{2n+1} \in \mathsf{lab}_{\text{in}}\,\langle P, R\rangle$;

A system execution is always infinite, for even if the environment ceases to produce input stimuli, system time will continue to progress, and in fact, diverge, as required by the fourth clause of the definition. What the fourth clause amounts to is giving input transitions a higher priority, and is necessitated by the idealization choices of our formalization, as will soon become clear.

Assume an execution E^{sys} of $\langle P, R\rangle$.

We write $\mathsf{prog}\, E^{\text{sys}}$ for a sequence over $\mathsf{state}\, P \cup \mathsf{lab}\, P$ such that for every $n \in \mathbb{N}$,

$$(\mathsf{prog}\, E^{\text{sys}})(2 \cdot n) \simeq \mathsf{prog}\, E^{\text{sys}}(\min\{n' \mid n < |\{n'' \mid n'' \leq n' \text{ and } E^{\text{sys}}(n''+1) \in \mathsf{lab}_{\text{prog}}\,\langle P, R\rangle\}|\})$$

and

$$(\mathsf{prog}\, E^{\text{sys}})(2 \cdot n + 1) \simeq \mathsf{prog}\, E^{\text{sys}}(\min\{n' \mid n < |\{n'' \mid n'' \leq n' \text{ and } E^{\text{sys}}(n'') \in \mathsf{lab}_{\text{prog}}\,\langle P, R\rangle\}|\}).$$

Proposition 5.4. $\mathsf{prog}\, E^{\text{sys}}$ *is an execution of* P.

Figure 8 shows a prefix of an execution of the system of Figure 3(a), whose underlying program execution is that of Figure 5, where, again, event values and actor states have been omitted.

Just as was the case with program executions, system executions are too general. What we want is that the logical-time specification of our programs prescribe the physical-time behaviour of our systems. And for

that to be the case, we need to make sure that program time, as expressed through time stamps of events, maintains its role as a logical notion of time. To do so we have to limit ourselves to system executions whose underlying program executions are safe. But here we must further guarantee that the resulting system specification will exclude non-causal implementations that clairvoyantly execute actors without ever violating program safety, correctly guessing the environment's future behaviour. And having bound program time to system time at the input edges of a program, we can use the structure and state of the program to determine at any given time, whether it is safe for an actor to process an input event or not.

We say that A is *ready* in $\langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}} \rangle$ if and only if $A \in \mathsf{dom}\, \iota$, there is $\alpha \in \text{IA}(\text{C}_{\text{in}}^A)$ such that $\alpha \subseteq Q$, and the following are true:

1. $t^{\text{sys}} \geq \mathsf{time}^{\text{prog}}\, \alpha - (\mathsf{delay}\, P)(\text{C}_{\text{in}}^P, \text{C}_{\text{in}}^A)$;
2. for any $e^{\text{prog}} \in Q \setminus \alpha$,

   $$\mathsf{time}^{\text{prog}}\, e^{\text{prog}} > \mathsf{time}^{\text{prog}}\, \alpha - (\mathsf{delay}\, P)(\mathsf{chan}\, e^{\text{prog}}, \text{C}_{\text{in}}^A);$$

3. for any A' and $\langle s', \alpha' \rangle$ such that $\varepsilon(A') = \langle s', \alpha' \rangle$,

   $$\mathsf{time}^{\text{prog}}\, \alpha' > \mathsf{time}^{\text{prog}}\, \alpha - (\mathsf{delay}\, P)(\text{C}_{\text{in}}^{A'}, \text{C}_{\text{in}}^A).$$

Informally, an actor is ready just as long as there is an event to process, it is impossible for a new event arriving at a sensor to eventually cause an event of smaller or equal time stamp as the event to be processed, and the same is true for any other event already circulating or being processed inside the program. Notice that the inequality in the first clause is non-strict, as opposed to those in the second and third one. This reflects our idealization that allows a system to instantaneously make a scheduling decision that takes into account the input status at that same time instant, and is the reason for giving input transitions a higher priority in system executions.

We say that E^{sys} is *actor-safe* if and only if for every $A \in P$, and any n, $\langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}} \rangle$, $\langle s, \alpha \rangle$, and r such that

$$E_{2n}^{\text{sys}} = \langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}} \rangle$$

and

$$E_{2n+1}^{\text{sys}} = \langle \langle A, \langle s, \alpha \rangle \rangle, r \rangle,$$

A is ready in E_{2n}^{sys}.

Of course, we are interested in system executions that meet the physical-time constraints implied by the logical-time specification of our programs.

We say that E^{sys} is *output-safe* if and only if for any $c \in \text{C}_{\text{out}}^P$, and every n and $\langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}} \rangle$ such that

$$E_{2n}^{\text{sys}} = \langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}} \rangle,$$

if there is e^{prog} in Q such that

$$\mathsf{chan}\, e^{\text{prog}} = c,$$

then

$$t^{\text{sys}} \leq \mathsf{time}^{\text{prog}}\, e^{\text{prog}}.$$

If we think of time stamps of events reaching the output channels of a program as actuator deadlines, then a system execution is output-safe just as long as no actuator deadline is ever missed.

We say that E^{sys} is *safe* if and only if E^{sys} is actor-safe and output-safe.

We say that e^{prog} *immediately produces* $e^{\text{prog}\prime}$ in E^{sys} if and only if there is A, n, $\langle\langle A, \langle s, \alpha\rangle\rangle, r\rangle$, n', and $\langle A, s', \alpha'\rangle$ such that the following are true:

1. $E^{\text{sys}}_{2n+1} = \langle\langle A, \langle s, \alpha\rangle\rangle, r\rangle$;
2. $e^{\text{prog}} \in \alpha$;
3. $E^{\text{sys}}_{2n'+1} = \langle A, s', \alpha'\rangle$;
4. $e^{\text{prog}\prime} \in \alpha'$;
5. $n < n'$;
6. for every n'' such that $n < n'' < n'$, if there is $\langle A', s'', \alpha''\rangle$ such that $E^{\text{sys}}_{2n''+1} = \langle A', s'', \alpha''\rangle$, then $A' \neq A$.

We say that e^{prog} *causally produces* $e^{\text{prog}\prime}$ in E^{sys} if and only if there is $e^{\text{prog}}_1, \ldots, e^{\text{prog}}_N$ such that $e^{\text{prog}}_1 = e^{\text{prog}}$, $e^{\text{prog}}_N = e^{\text{prog}\prime}$, and for every i such that $1 \leq i < N$, e^{prog}_i immediately produces e^{prog}_{i+1} in E^{sys}.

Notice that if e^{prog} causally produces $e^{\text{prog}\prime}$, then

$$\mathsf{time}^{\text{prog}}\, e^{\text{prog}\prime} > \mathsf{time}^{\text{prog}}\, e^{\text{prog}} + (\mathsf{delay}\, P)(\mathsf{chan}\, e^{\text{prog}}, \mathsf{chan}\, e^{\text{prog}\prime}).$$

Theorem 5.5. *If E^{sys} is safe, then* $\mathsf{prog}\, E^{\text{sys}}$ *is safe.*

Proof. We examine two consecutive start transitions of an actor A in E^{sys}, and show that the program time of the corresponding input actions strictly increases.

There are n_1, n_2, $\langle\langle A, \langle s_1, \alpha_1\rangle\rangle, r_1\rangle$, $\langle\langle A, \langle s_2, \alpha_2\rangle\rangle, r_2\rangle$, $\langle Q_1, \iota_1, \varepsilon_1, \rho_1, \pi_1, t^{\text{sys}}_1\rangle$, $\langle Q_2, \iota_2, \varepsilon_2, \rho_2, \pi_2, t^{\text{sys}}_2\rangle$ such that the following are true:

1. $n_1 < n_2$;
2. $E^{\text{sys}}_{2n_1} = \langle Q_1, \iota_1, \varepsilon_1, \rho_1, \pi_1, t^{\text{sys}}_1\rangle$;
3. $E^{\text{sys}}_{2n_2} = \langle Q_2, \iota_2, \varepsilon_2, \rho_2, \pi_2, t^{\text{sys}}_2\rangle$;
4. $E^{\text{sys}}_{2n_1+1} = \langle\langle A, \langle s_1, \alpha_1\rangle\rangle, r_1\rangle$;
5. $E^{\text{sys}}_{2n_2+1} = \langle\langle A, \langle s_2, \alpha_2\rangle\rangle, r_2\rangle$;
6. for every n such that $n_1 < n < n_2$, if there is $\langle\langle A', \langle s', \alpha'\rangle\rangle, r'\rangle$ such that $E^{\text{sys}}(2 \cdot n + 1) = \langle\langle A, \langle s', \alpha'\rangle\rangle, r'\rangle$, then $A' \neq A$.

$E^{\text{sys}}_{2n_1+1}$ and $E^{\text{sys}}_{2n_2+1}$ are the two consecutive start transitions of A in E^{sys}.

We will show that $\mathsf{time}^{\text{prog}}\, \alpha_1 < \mathsf{time}^{\text{prog}}\, \alpha_2$.

For every event e^{prog} in α_2, either e^{prog} is in Q_1 or it is not.

If it is not in Q_1, since e^{prog} is in Q_2, we will trace its source, i.e. the finish transition of an actor, an event that causally produces it, or an input transition, in the states and transitions that preceed $E^{\text{sys}}_{2n_2}$.

Note that for every $e^{\text{prog}} \in \alpha_2$, $\mathsf{time}^{\text{prog}}\, e^{\text{prog}} = \mathsf{time}^{\text{prog}}\, \alpha_2$, so it is sufficient to show that $\mathsf{time}^{\text{prog}}\, e^{\text{prog}} > \mathsf{time}^{\text{prog}}\, \alpha_1$.

For every $e^{\text{prog}} \in \alpha_2$ one of the following is true:

1. $e^{\text{prog}} \in Q_1$ and by condition 2 of the definition of ready 5 for A for start transition $E^{\text{sys}}_{2n_1+1}$,

$$\mathsf{time}^{\text{prog}}\, e^{\text{prog}} > \mathsf{time}^{\text{prog}}\, \alpha_1 - (\mathsf{delay}\, P)(\mathsf{chan}\, e^{\text{prog}}, \mathrm{C}^A_{\text{in}}) = \mathsf{time}^{\text{prog}}\, \alpha_1;$$

2. $e^{\text{prog}} \notin Q_1$ and one of the following is true:

   (a) there exists $e^{\text{prog}\prime} \in Q_1$ that causally produces e^{prog}, so $\mathsf{time}^{\text{prog}}\, e^{\text{prog}\prime} \leq \mathsf{time}^{\text{prog}}\, e^{\text{prog}}$, and by condition 2 of the definition of ready 5 for A for start transition $E^{\text{sys}}_{2n_1+1}$,

   $$\mathsf{time}^{\text{prog}}\, e^{\text{prog}\prime} > \mathsf{time}^{\text{prog}}\, \alpha_1 - (\mathsf{delay}\, P)(\mathsf{chan}\, e^{\text{prog}\prime}, \mathrm{C}^A_{\text{in}});$$

   (b) there exists A', $e^{\text{prog}\prime}$, and $\langle s', \alpha' \rangle$ such that the following are true:

      i. $\varepsilon_1(A') = \langle s', \alpha' \rangle$;

      ii. $e^{\text{prog}\prime} \in \alpha'$, $e^{\text{prog}\prime}$ causally produces e^{prog}, and $\mathsf{time}^{\text{prog}}\, e^{\text{prog}\prime} \leq \mathsf{time}^{\text{prog}}\, e^{\text{prog}}$;

      iii. by condition 3 of the definition of ready 5 for A for start transition $E^{\text{sys}}_{2n_1+1}$,

      $$\mathsf{time}^{\text{prog}}\, \alpha' > \mathsf{time}^{\text{prog}}\, \alpha_1 - (\mathsf{delay}\, P)(\mathrm{C}^{A'}_{\text{in}}, \mathrm{C}^A_{\text{in}});$$

   (c) there exists n', and $e^{\text{prog}\prime} \in \mathsf{lab}_{\text{in}}\, \langle P, R \rangle$ such that the following are true:

      i. $E^{\text{sys}}_{2n'+1} = e^{\text{prog}\prime}$;

      ii. $e^{\text{prog}\prime}$ causally produces e^{prog};

      iii. $n' > n_1$ implying that $\mathsf{time}^{\text{prog}}\, e^{\text{prog}\prime} > t^{\text{sys}}_1$ by the input-first property of executions;

      iv. by condition 1 of the definition of ready 5 for A for start transition $E^{\text{sys}}_{2n_1+1}$,

      $$t^{\text{sys}}_1 \geq \mathsf{time}^{\text{prog}}\, \alpha_1 - (\mathsf{delay}\, P)(\mathrm{C}^P_{\text{in}}, \mathrm{C}^A_{\text{in}}).$$

□

We say that E^{sys} is *fair* if and only if $\mathsf{prog}\, E^{\text{sys}}$ is actor-fair.

We say that E^{sys} is *correct* if and only if E^{sys} is safe and fair.

Theorem 5.6. *If E^{sys} is correct, then $\mathsf{prog}\, E^{\text{sys}}$ is correct.*

Proof. By definition if E^{sys} is correct then E^{sys} is safe and fair, or $\mathsf{prog}\, E^{\text{sys}}$ is safe and $\mathsf{prog}\, E^{\text{sys}}$ is actor-fair.

Therefore it remains to be shown that $\mathsf{prog}\, E^{\text{sys}}$ is output-fair.

Let n, $\langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}} \rangle$, and e^{prog} be such that

$$E^{\text{sys}}_{2n} = \langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}} \rangle,$$

$$e^{\text{prog}} \in Q,$$

and

$$\mathsf{chan}\, e^{\text{prog}} = c.$$

We will show that there is n' such that $n \leq n'$ and

$$E^{\text{sys}}_{2n'+1} = e^{\text{prog}}.$$

Since E^{sys} is output-safe, $t^{\text{sys}} \leq \mathsf{time}^{\text{prog}}\, e^{\text{prog}}$.

By definition of an execution, there is n'', $\langle Q'', \iota'', \varepsilon'', \rho'', \pi'', t^{\mathrm{sys}\prime\prime}\rangle$, and $\epsilon > 0$ such that $\mathsf{time}^{\mathrm{prog}} + \epsilon \leq t^{\mathrm{sys}\prime\prime}$.

$e^{\mathrm{prog}} \notin Q''$ because $t^{\mathrm{sys}\prime\prime} > \mathsf{time}^{\mathrm{prog}}\, e^{\mathrm{prog}}$ and E^{sys} is output-safe.

$t^{\mathrm{sys}\prime\prime} > t^{\mathrm{sys}}$ therefore $n'' > n$.

Since e^{prog} is in Q, e^{prog} is not in Q'', and $\mathsf{chan}\, e^{\mathrm{prog}} \in \mathrm{C}^P_{\mathrm{out}}$, there is n' such that $n \leq n' < n''$ and $E^{\mathrm{sys}}_{2n'+1} = e^{\mathrm{prog}}$.

□

6 Schedulability

By Theorem 4.6, every well defined program will be able to execute correctly when presented with any discrete-event input signal. For a system, this is clearly not the case. The problem is to decide whether a given system will be able to execute correctly when presented with any discrete-event input signal from some given class of such signals.

First we need to address a technical issue. Since computation-time requirements of actors are chosen nondeterministically, we need to be able to quantify system executions of the same underlying program executions over all possible computation-time-requirement choices made.

For every $A \in P$, we write $\mathsf{trace}^A_{\mathrm{start}}\, E^{\mathrm{prog}}$ for $(\mathsf{filter}\,\{\langle \mathrm{A}, \langle \mathrm{s}, \alpha\rangle\rangle \mid \langle A, \langle s, \alpha\rangle\rangle \in \mathsf{lab}_{\mathrm{start}}\, P\})\, E^{\mathrm{prog}}$.

For every $A \in P$, we write $\mathsf{trace}^{\mathrm{A}}_{\mathrm{start}}\, E^{\mathrm{sys}}$ for $(\mathsf{filter}\,\{\langle\langle \mathrm{A}, \langle \mathrm{s}, \alpha\rangle\rangle, \mathrm{r}\rangle \mid \langle\langle A, \langle s, \alpha\rangle\rangle, r\rangle \in \mathsf{lab}_{\mathrm{start}}\, \langle P, R\rangle\})\, E^{\mathrm{sys}}$.

Proposition 6.1. *For every $A \in P$, there is $O \in \mathscr{S}\, R(A)$ such that*

$$\mathsf{trace}^A_{\mathrm{start}}\, E^{\mathrm{sys}} = \mathsf{zip}\,\langle \mathsf{trace}^A_{\mathrm{start}}\, \mathsf{prog}\, E^{\mathrm{sys}}, O\rangle.$$

Proof. We define $O' \in \mathscr{S}\, R(A)$ such that for every i, if there is $\langle\langle A, \langle s, \alpha\rangle\rangle, r\rangle$ such that $(\mathsf{trace}^A_{\mathrm{start}}\, E^{\mathrm{sys}})(i) = \langle\langle A, \langle s, \alpha\rangle\rangle, r\rangle$ then $O'(i) = r$.

By definiton of $\mathsf{prog}\, E^{\mathrm{sys}}$, for every i, there is $r \in R(A)$ and $\langle A, \langle s, \alpha\rangle\rangle$ such that

$$(\mathsf{trace}^A_{\mathrm{start}}\, E^{\mathrm{sys}})(i) = \langle\langle A, \langle s, \alpha\rangle\rangle, r\rangle$$

and

$$(\mathsf{trace}^A_{\mathrm{start}}\, \mathsf{prog}\, E^{\mathrm{sys}})(i) = \langle A, \langle s, \alpha\rangle\rangle.$$

Therefore,

$$(\mathsf{trace}^A_{\mathrm{start}}\, E^{\mathrm{sys}})(i) = \langle (\mathsf{trace}^A_{\mathrm{start}}\, \mathsf{prog}\, E^{\mathrm{sys}})(i), O'(i)\rangle,$$

or

$$\mathsf{trace}^A_{\mathrm{start}}\, E^{\mathrm{sys}} = \mathsf{zip}\,\langle \mathsf{trace}^A_{\mathrm{start}}\, \mathsf{prog}\, E^{\mathrm{sys}}, O'\rangle.$$

□

We write $(\mathrm{RO}\,\langle P, R\rangle)(E^{\mathrm{prog}})$ for a set such that for every $O \in (\mathrm{RO}\,\langle P, R\rangle)(E^{\mathrm{prog}})$, O is a function from P such that for every $A \in P$, $O(A) \in \mathscr{S}_{|\mathsf{trace}^A_{\mathrm{start}}\, E^{\mathrm{prog}}|}\, R(A)$.

We think of every member of $(\mathrm{RO}\,\langle P, R\rangle)(E^{\mathrm{prog}})$ as an oracle, capturing the nondeterministic choices of computation-time requirements for each actor over a given system realization of the program execution E^{prog}.

Definition 6.2. A *model* is an ordered pair $\langle\langle P, R\rangle, I\rangle$ such that the following are true:

1. $\langle P, R\rangle$ is a well defined system;
2. $I \subseteq \mathrm{S}^{\mathrm{prog}}(\mathrm{C}^P_{\mathrm{in}})$.

Assume a model $\langle\langle P, R\rangle, I\rangle$.

We say that $\langle\langle P, R\rangle, I\rangle$ is *schedulable* if and only if for any $s^{\mathrm{prog}} \in I$, every correct execution E^{prog} of P such that

$$\mathsf{in}\, E^{\mathrm{prog}} = s^{\mathrm{prog}},$$

and every $O \in (\mathrm{RO}\,\langle P, R\rangle)(E^{\mathrm{prog}})$, there is a correct execution E^{sys} of $\langle P, R\rangle$ such that

$$\mathsf{in}\,\mathsf{prog}\, E^{\mathrm{sys}} = s^{\mathrm{prog}},$$

and for every $A \in P$,

$$\mathsf{trace}^A_{\mathrm{start}}\, E^{\mathrm{sys}} = \mathsf{zip}\,\langle \mathsf{trace}^A_{\mathrm{start}}\, E^{\mathrm{prog}}, O(A)\rangle.$$

A convenient tool in approaching schedulability problems is the identification of a particular scheduling strategy that is optimal, in the sense that if a system is schedulable, then it is also schedulable under that particular strategy. For uniprocessor platforms, the earliest-deadline-first (EDF) strategy has been proven optimal over a variety of different schedulability problems. To make it applicable here, we first need to formalize a notion of deadline for the events circulating inside the program of a system.

We write $\mathsf{deadline}\, P$ for a function from $\bigcup\{\mathrm{IA}(\mathrm{C}^A_{\mathrm{in}}) \mid A \in P\}$ to $\mathbb{T}$ such that for every $\alpha \in \bigcup\{\mathrm{IA}(\mathrm{C}^A_{\mathrm{in}}) \mid A \in P\}$,

$$(\mathsf{deadline}\, P)(\alpha) = \mathsf{time}^{\mathrm{prog}}\,\alpha + (\mathsf{delay}\, P)(\mathsf{chan}\,\alpha, \mathrm{C}^P_{\mathrm{out}}).$$

In other words, an event's deadline is the earliest time stamp of any event eventually caused by the former that reaches an actuator.

We say that E^{sys} is *eager* if and only if for every $A \in P$, the following are true:

1. for any n and $\langle Q, \iota, \varepsilon, \rho, \pi, t^{\mathrm{sys}}\rangle$ such that

   $$E^{\mathrm{sys}}_{2n} = \langle Q, \iota, \varepsilon, \rho, \pi, t^{\mathrm{sys}}\rangle,$$

   and any d such that A is ready in $\langle Q, \iota, \varepsilon, \rho, \pi, t^{\mathrm{sys}} + d\rangle$, if $E^{\mathrm{sys}}_{2n+1} \in \mathbb{T}$, then

   $$E^{\mathrm{sys}}_{2n+1} \leq d;$$

2. for any n, $\langle Q, \iota, \varepsilon, \rho, \pi, t^{\mathrm{sys}}\rangle$, such that

   $$E^{\mathrm{sys}}_{2n} = \langle Q, \iota, \varepsilon, \rho, \pi, t^{\mathrm{sys}}\rangle,$$

   $$\mathsf{dom}\,\varepsilon \neq \emptyset,$$

   and

   $$\pi = \texttt{NULL},$$

   if $E^{\mathrm{sys}}_{2n+1} \in \mathbb{T}$, then

   $$E^{\mathrm{sys}}_{2n+1} = 0;$$

3. for any n and $\langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}} \rangle$ such that

$$E^{\text{sys}}_{2n} = \langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}} \rangle,$$

$A \in \mathsf{dom}\, \varepsilon$, and

$$\rho(A) = 0,$$

if $E^{\text{sys}}_{2n+1} \in \mathbb{T}$, then

$$E^{\text{sys}}_{2n+1} = 0.$$

We say that E^{sys} is *earliest-deadline-first* if and only if E^{sys} is eager and for any n, $\langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}} \rangle$, and $\langle s, \alpha \rangle$ such that

$$E^{\text{sys}}_{2n} = \langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}} \rangle,$$

and

$$\pi \notin \{A \mid \text{there is } A \text{ such that } \varepsilon(A) = \langle s, \alpha \rangle, \text{ and for every } A' \text{ and } \langle s', \alpha' \rangle \text{ such that } \varepsilon(A') = \langle s', \alpha' \rangle, (\mathsf{deadline}\, P)(\alpha) \leq (\mathsf{deadline}\, P)(\alpha')\},$$

if $E^{\text{sys}}_{2n+1} \in \mathbb{T}$, then

$$E^{\text{sys}}_{2n+1} = 0.$$

In other words, a system execution is earliest-deadline-first just as long as it is eager with respect to start and finish transitions, and at each time instant, allocates the processor to the actor processing the events with the smallest deadline.

Proposition 6.3. *If E^{sys} is earliest-deadline-first, then E^{sys} is fair.*

Proof. We first show that if there is n, $\langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}} \rangle$, A, and $\langle s, \alpha \rangle$ such that $E^{\text{sys}}_{2n} = \langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}} \rangle$, $\varepsilon(A) = \langle s, \alpha \rangle$, then there is n' and $\langle Q', \iota', \varepsilon', \rho', \pi', t^{\text{sys}\prime} \rangle$ such that $n < n'$, $E^{\text{sys}}_{2n'} = \langle Q', \iota', \varepsilon', \rho', \pi', t^{\text{sys}\prime} \rangle$, and $A \in \mathsf{dom}\, \iota'$.

By the definition of a system execution there is n'' and $\langle Q'', \iota'', \varepsilon'', \rho'', \pi'', t^{\text{sys}\prime\prime} \rangle$ such that $n'' > n$, $E^{\text{sys}}_{2n''} = \langle Q'', \iota'', \varepsilon'', \rho'', \pi'', t^{\text{sys}\prime\prime} \rangle$ and $t^{\text{sys}\prime\prime} > \mathsf{time}^{\text{prog}}\, \varepsilon(A)$.

If $\varepsilon''(A) \neq \langle s, \alpha \rangle$ then n' exists and is between n and n''.

If $\varepsilon''(A) = \langle s, \alpha \rangle$ then the following are true:

- all new events that arrive through input transitions will have a greater deadline than α,
- if there is event $e^{\text{prog}} \in Q''$ with $\mathsf{deadline}(\{e^{\text{prog}}\}) < \mathsf{deadline}(\alpha)$ then there is A' and $\langle s', \alpha' \rangle$ such that $\varepsilon''(A') = \langle s', \alpha' \rangle$ and $\mathsf{deadline}(\alpha') \leq \mathsf{deadline}(\{e^{\text{prog}}\})$,

Using the same as in the proof of 4.6, within a finite number of steps, the set of events and input actions with deadline smaller than $\mathsf{deadline}(\alpha)$ will be exhausted and thus A will eventually occupy the processor for $\rho(A)$ time units and the system will execute a finish transition for A.

We now show that if there is n, $\langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}} \rangle$, A, and e^{prog} such that $E^{\text{sys}}_{2n} = \langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}} \rangle$, $A \in \mathsf{dom}\, \iota$, $e^{\text{prog}} \in Q$, and $\mathsf{chan}\, e^{\text{prog}} \in \mathrm{C}^A_{\text{in}}$, then there is n', $\langle Q', \iota', \varepsilon', \rho', \pi', t^{\text{sys}\prime} \rangle$, s', and α' such that $n < n'$, $E^{\text{sys}}_{2n'} = \langle Q', \iota', \varepsilon', \rho', \pi', t^{\text{sys}\prime} \rangle$, $A \in \mathsf{dom}\, \varepsilon'$, $\varepsilon'(A) = \langle s', \alpha' \rangle$ and $e^{\text{prog}} \in \alpha'$.

We use the same reasoning as the previous case: by the definition of a system execution there is n'' and $\langle Q'', \iota'', \varepsilon'', \rho'', \pi'', t^{\text{sys}\prime\prime} \rangle$ such that $n'' > n$, $E^{\text{sys}}_{2n''} = \langle Q'', \iota'', \varepsilon'', \rho'', \pi'', t^{\text{sys}\prime\prime} \rangle$ and $t^{\text{sys}\prime\prime} > \mathsf{time}^{\text{prog}}\, \varepsilon(A)$.

If $e^{\text{prog}} \notin Q''$ then n' exists and is between n and n''.

If $e^{\text{prog}} \in Q''$ then the following are true:

- all new events that arrive through input transitions will have a greater deadline than e^{prog},
- for any event $e^{\text{prog}\prime} \in Q \setminus \{e^{\text{prog}}\}$ such that $\mathsf{time}^{\text{prog}}\, e^{\text{prog}\prime} \leq \mathsf{time}^{\text{prog}}\, e^{\text{prog}} - (\mathsf{delay}\, P)(\mathsf{chan}\, e^{\text{prog}}, \mathrm{C}^A_{\text{in}})$, $(\mathsf{deadline}\, P)(\{e^{\text{prog}\prime}\}) \leq (\mathsf{deadline}\, P)(\{e^{\text{prog}}\})$;
- for any A' and $\langle s', \alpha' \rangle$ such that $\varepsilon(A') = \langle s', \alpha' \rangle$, and $\mathsf{time}^{\text{prog}}\, \alpha' \leq \mathsf{time}^{\text{prog}}\, e^{\text{prog}} - (\mathsf{delay}\, P)(\mathrm{C}^{A'}_{\text{in}}, \mathrm{C}^A_{\text{in}})$, $(\mathsf{deadline}\, P)(\alpha') \leq (\mathsf{deadline}\, P)(\{e^{\text{prog}}\})$;

As before, eventually, there will be no events or input actions that would make actor A not be ready and A will execute a start transition with an input action that includes e^{prog}.

□

The following is immediate from Proposition 6.3:

Theorem 6.4. *If E^{sys} is earliest-deadline-first, then E^{sys} is correct if and only if E^{sys} is safe.*

Lemma 6.5. *For any $s^{\text{prog}} \in I$, every execution E^{prog} of P such that*

$$\mathsf{in}\, E^{\text{prog}} = s^{\text{prog}},$$

and every $O \in (\mathrm{RO}\, \langle P, R \rangle)(E^{\text{prog}})$, if there is a correct execution E^{sys} of $\langle P, R \rangle$ such that

$$\mathsf{in}\, \mathsf{prog}\, E^{\text{sys}} = s^{\text{prog}},$$

and for every $A \in P$,

$$\mathsf{trace}^A_{\text{start}}\, E^{\text{sys}} = \mathsf{zip}\, \langle \mathsf{trace}^A_{\text{start}}\, E^{\text{prog}}, O(A) \rangle,$$

then there is a correct eager execution $E^{\text{sys}}_{\text{eager}}$ of $\langle P, R \rangle$ such that

$$\mathsf{in}\, \mathsf{prog}\, E^{\text{sys}}_{\text{eager}} = s^{\text{prog}},$$

and for every $A \in P$,

$$\mathsf{trace}^A_{\text{start}}\, E^{\text{sys}}_{\text{eager}} = \mathsf{zip}\, \langle \mathsf{trace}^A_{\text{start}}\, E^{\text{prog}}, O(A) \rangle.$$

Proof. Assume there is s^{prog}, E^{prog}, $O \in (\mathrm{RO}\, \langle P, R \rangle)(E^{\text{prog}})$, and E^{sys} such that $\mathsf{in}\, E^{\text{prog}} = s^{\text{prog}}$, E^{sys} is a correct execution, $\mathsf{in}\, \mathsf{prog}\, E^{\text{sys}} = s^{\text{prog}}$, and for every $A \in P$, $\mathsf{trace}^A_{\text{start}}\, E^{\text{sys}} = \mathsf{zip}\, \langle \mathsf{trace}^A_{\text{start}}\, E^{\text{prog}}, O(A) \rangle$.

We will describe how to transform E^{sys} into an execution $E^{\text{sys}\prime}$ such that $E^{\text{sys}\prime}$ is eager, $E^{\text{sys}\prime}$ is correct, $\mathsf{in}\, \mathsf{prog}\, E^{\text{sys}\prime} = s^{\text{prog}}$, and for every $A \in P$, $\mathsf{trace}^A_{\text{start}}\, E^{\text{sys}\prime} = \mathsf{trace}^A_{\text{start}}\, E^{\text{sys}}$.

Let n be the smallest index such that $E^{\text{sys}}(2 \cdot n + 1) = d_t$ where $d_t \in \mathbb{T}$ and $d_t > 0$.

We write s for state $E^{\text{sys}}(2 \cdot n)$.

We write $E^{\text{sys}}(s \ldots)$ for $\langle E^{\text{sys}}(2 \cdot n + 1), E^{\text{sys}}(2 \cdot n + 2), \ldots \rangle$.

Let $\langle Q, \varepsilon, \iota, \rho, \pi, t^{\text{sys}} \rangle$ be such that $E^{\text{sys}}(2 \cdot n) = \langle Q, \varepsilon, \iota, \rho, \pi, t^{\text{sys}} \rangle$.

First, if there is an actor $A \in \mathsf{dom}\, \rho$ such that $\rho(A) = 0$, then because E^{sys} is fair, there is $n' > n$ such that $E^{\text{sys}}(2 \cdot n' + 1)$ is the corresponding finish transition that removes A from $\mathsf{dom}\, \rho$. In order for the new execution to satisfy the eagerness constraints $E^{\text{sys}}(2 \cdot n' + 1)$ has to be moved at the beginning of $E^{\text{sys}}(s \ldots)$.

We write s' for the state of the new execution that follows all finish transitions for actors A with $\rho(A) = 0$.

Next, for any actor A that is ready in s', we move the corresponding start transition from $E^{\text{sys}}(s\ldots)$ after state s'. Let s'' be the state that follows the start transitions. Let $\langle Q'', \iota'', \varepsilon'', \rho'', \pi'', t^{\text{sys}\prime\prime}\rangle$ be such that $s'' = \langle Q'', \iota'', \varepsilon'', \rho'', \pi'', t^{\text{sys}\prime\prime}\rangle$.

Next, let $d_{\min}$ be the smallest delay in $\mathbb{T}$ such that there is an actor A that is ready in $\langle Q'', \iota'', \varepsilon'', \rho'', \pi'', t^{\text{sys}\prime\prime} + d_{\min}\rangle$.

If $d_{\min} < d_t$ then we split the time transition that follows s'' to two time transition with delays $d_{\min}$ and $d_t - d_{\min}$. Let t' be the time transition that follows s'' and d'_t its delay.

If $\mathsf{dom}\,\varepsilon''$ is not empty and $\pi'' = \texttt{NULL}$ then we choose a time transition in $E^{\text{sys}}(s''\ldots)$ during which an actor A from $\mathsf{dom}\,\varepsilon''$ is executing. Let d_A be the delay of that time transition.

If d_A is smaller than $d_{t'}$ then we replace the t' time transition with t_A followed by a time transition with duration $d_A - d_{t'}$ during which $\pi = \texttt{NULL}$.

If d_A is larger than $d_{t'}$ then we split t_A into two transitions: one with duration $d_A - d_{t'}$ executing A and one with duration $d_{t'}$ executing `NULL`, and make the t' execute A.

At this point the new execution including time transition t' is eager therefore we can restart the process outlined above in the target state of t'.

□

Theorem 6.6. *For any $s^{\text{prog}} \in I$, every execution E^{prog} of P such that*

$$\mathsf{in}\, E^{\text{prog}} = s^{\text{prog}},$$

and every $O \in (\text{RO}\,\langle P, R\rangle)(E^{\text{prog}})$, if there is a correct execution E^{sys} of $\langle P, R\rangle$ such that

$$\mathsf{in\ prog}\, E^{\text{sys}} = s^{\text{prog}},$$

and for every $A \in P$,

$$\mathsf{trace}^A_{\text{start}}\, E^{\text{sys}} = \mathsf{zip}\,\langle \mathsf{trace}^A_{\text{start}}\, E^{\text{prog}}, O(A)\rangle,$$

then there is a correct earliest-deadline-first execution $E^{\text{sys}}_{\text{EDF}}$ of $\langle P, R\rangle$ such that

$$\mathsf{in\ prog}\, E^{\text{sys}}_{\text{EDF}} = s^{\text{prog}},$$

and for every $A \in P$,

$$\mathsf{trace}^A_{\text{start}}\, E^{\text{sys}}_{\text{EDF}} = \mathsf{zip}\,\langle \mathsf{trace}^A_{\text{start}}\, E^{\text{prog}}, O(A)\rangle.$$

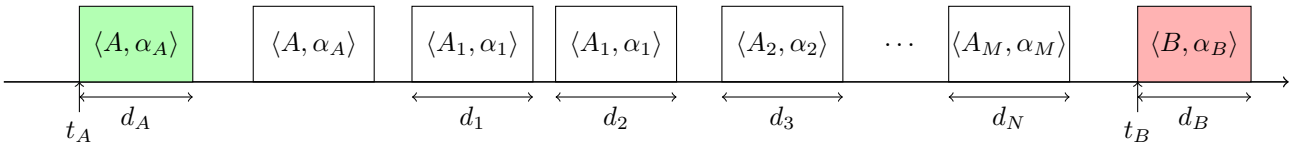

Figure 9. Execution that violates EDF properties

Proof. Given a correct execution E^{sys} of $\langle P, R\rangle$ as described in the theorem, from lemma 6.5 we can construct an eager execution $E^{\text{sys}}_{\text{eager}}$ such that

$$\mathsf{in\ prog}\, E^{\text{sys}}_{\text{eager}} = s^{\text{prog}},$$

and for every $A \in P$,

$$\mathsf{trace}^{A}_{\mathrm{start}}\, E^{\mathrm{sys}}_{\mathrm{eager}} = \mathsf{zip}\,\langle \mathsf{trace}^{A}_{\mathrm{start}}\, E^{\mathrm{prog}}, O(A)\rangle.$$

We will show how we can convert $E^{\mathrm{sys}}_{\mathrm{eager}}$ into an EDF execution $E^{\mathrm{sys}}_{\mathrm{EDF}}$. The conversion consists of the following steps: identify the earliest point at which $E^{\mathrm{sys}}_{\mathrm{eager}}$ violates the EDF property; fix the violation; produce an intermediate correct execution which is EDF up to and including the initial violation point; convert the intermediate correct execution into an eager execution; repeat the process on the rest of the execution.

Assume that figure 9 depicts a violation of the EDF property in $E^{\mathrm{sys}}_{\mathrm{eager}}$. The axis represents system time and each rectangle labeled $\langle A, \alpha\rangle$ represents the uninterrupted execution of input action α by actor A on the processor.

For the execution to violate EDF we assume that $(\mathsf{deadline}\, P)(\alpha_A) > (\mathsf{deadline}\, P)(\alpha_B)$ and B is safe to process α_B when A starts processing α_A. Furthermore, assume that α_B has the smallest deadline among all input actions that are safe to process at time t_A and that t_B is the first time after t_A that α_B starts processing.

While the execution should process α_B at time t_A, it instead processes α_A. In order to produce an EDF execution, α_B has to be processed at time t_A. We will place as much as possible of the d_B processing time of α_B at time t_A and shift the processing of α_A to the future as appropriate.

The input actions $\alpha_1, \ldots, \alpha_M$ correspond to input actions that are "caused" by the processing of α_A. In other words, $\alpha_1, \ldots, \alpha_M$ are the input actions that contain events that causally depend on the events of α_A. In the rearrangement of $E^{\mathrm{sys}}_{\mathrm{eager}}$ into an EDF execution, that causal ordering has to be respected. In effect this requires the processing of α_A to pushed into the processing of $\alpha_1, \ldots, \alpha_M$ and finally into the region where α_B was previously executing.

Shifting the processing of α_A will change the times at which the processing of α_A and $\alpha_1, \ldots, \alpha_M$ terminate. Therefore, the start transitions of $\alpha_1, \ldots, \alpha_M$ and the finish transitions of α_A and $\alpha_1, \ldots, \alpha_M$ will have to be shifted as well.

The intermediate shifted execution is correct. Notice that the shift does not change the program time of any of the actions. If α_i was safe to process at time t_i then α_i is guaranteed to be safe to process at any time greater than t_i. Furthermore, remember that $(\mathsf{deadline}\, P)(\alpha_A) > (\mathsf{deadline}\, P)(\alpha_B)$ and note that for every i such that $1 \leq i \leq M$, $(\mathsf{deadline}\, P)(\alpha_A) \leq (\mathsf{deadline}\, P)(\alpha_i)$. In the intermediate execution, the processing of α_A and all α_is terminate either at the same time as in the original execution or before B terminates.

The intermediate execution might not eagerly execute start transitions. We can tranform it into an eager one using the process described in lemma 6.5.

□

7 Decidability

In the previous section we showed that in order to decide if a model is schedulable we can narrow our search in the EDF executions of the system. Furthermore, since the properties of actor-safe and EDF system executions are local properties, we can construct a transition system whose traces are prefixes of actor-safe EDF system executions. The question of whether a non output-safe, actor-safe, and EDF execution exists, is equivalent to whether a state in which an event misses its deadline is reachable. Is the reachability of a deadline miss state decidable? At first the answer seems negative since the state space of a

system is infinite. However, since we are only interested in the schedulability of the system we can abstract away part of its state.

First, we abstract all states that contain any events that have missed their deadline under a new state called `error`.

Note that we have constrained the actors in a program to be output homogeneous and constant delay. Effectively this means that the timing properties of the executions of a system, and thus its schedulability, do not depend on the actor states or on the event values, and thus, those can also be abstracted away.

Next, intuitively it should be the case that in correct executions the number of events in any state of the program could not grow unboundedly. Events are associated with an execution time requirement and a deadline, and thus the accumulation of too many execution requirements should conclusively lead the system to a deadline miss. One complication that arises in our programs is the fact that the deadline of an event in a channel does not only depend on that channel but also on the path that the event has followed to reach that channel. Specifically, the deadline of an event is a function of its timestamp which in principle could grow unboundedly (e.g. if the event circles around a program loop). However, what is really of interest in order to bound the number of events, is the relative deadline which does not only depend on the timestamp but rather on the difference between the timestamp and the current system time. That difference can be shown to be bounded in all correct executions for all events in every channel of the program. The lower bound naturally follows the definition of deadline. The upper bound, which claims that the timestamp of an event in a channel cannot grow too much relatively to system time, is a consequence of safety and the requirement that actors are ready.

Theorem 7.1. *For every correct execution E^{sys} of $\langle P, R\rangle$, every n and $\langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}}\rangle$ such that*

$$E^{\text{sys}}_{2n} = \langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}}\rangle,$$

and any $e^{\text{prog}} \in Q$,

$$-(\mathsf{delay}\, P)(\mathsf{chan}\, e^{\text{prog}}, \mathrm{C}^P_{\text{out}}) \leq \mathsf{time}^{\text{prog}}\, e^{\text{prog}} - t^{\text{sys}} \leq (\mathsf{delay}\, P)(\mathrm{C}^P_{\text{in}}, \mathsf{chan}\, e^{\text{prog}}).$$

Proof. Assume that there exists correct execution E^{sys} of $\langle P, R\rangle$, n, $\langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}}\rangle$, and e^{prog} such that

$$E^{\text{sys}}_{2n} = \langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}}\rangle,$$

$$e^{\text{prog}} \in Q,$$

and

$$\mathsf{time}^{\text{prog}}\, e^{\text{prog}} - t^{\text{sys}} > (\mathsf{delay}\, P)(\mathrm{C}^P_{\text{in}}, \mathsf{chan}\, e^{\text{prog}}).$$

If $\mathsf{chan}\, e^{\text{prog}} \in \mathrm{C}^P_{\text{in}}$ then $(\mathsf{delay}\, P)(\mathrm{C}^P_{\text{in}}, \mathsf{chan}\, e^{\text{prog}}) = 0$, $t^{\text{sys}} = \mathsf{time}^{\text{prog}}\, e^{\text{prog}}$ at the time of the input transition that produces e^{prog} and $t^{\text{sys}} \geq \mathsf{time}^{\text{prog}}\, e^{\text{prog}}$ thereafter.

Therefore, it cannot be the case that $\mathsf{chan}\, e^{\text{prog}} \in \mathrm{C}^P_{\text{in}}$, or there is actor A such that $\mathsf{chan}\, e^{\text{prog}} \in \mathrm{C}^A_{\text{out}}$.

Furthermore, there is n', $\langle Q', \iota', \varepsilon', \rho', \pi', t^{\text{sys}\prime}\rangle$, s, α, and r such that

$$n' < n,$$

$$E^{\text{sys}}_{2n'} = \langle Q', \iota', \varepsilon', \rho', \pi', t^{\text{sys}\prime}\rangle,$$
$$E^{\text{sys}}_{2n'+1} = \langle\langle A, \langle s, \alpha\rangle\rangle, r\rangle,$$

and

$$\mathsf{time}^{\text{prog}}\, e^{\text{prog}} = \mathsf{time}^{\text{prog}}\, \alpha + (\mathsf{delay}\, A)(\mathsf{chan}\, e^{\text{prog}}).$$

Since E^{sys} is a correct execution, A has to be ready in $E^{\text{sys}}_{2n'}$. However,

$$\begin{aligned}
&\mathsf{time}^{\text{prog}}\,\alpha - (\mathsf{delay}\,P)(\mathrm{C}^P_{\text{in}}, \mathrm{C}^A_{\text{in}}) = \\
&(\mathsf{time}^{\text{prog}}\,e^{\text{prog}} - (\mathsf{delay}\,A)(\mathsf{chan}\,e^{\text{prog}})) - ((\mathsf{delay}\,P)(\mathrm{C}^P_{\text{in}}, \mathsf{chan}\,e^{\text{prog}}) - (\mathsf{delay}\,A)(\mathsf{chan}\,e^{\text{prog}})) = \\
&\mathsf{time}^{\text{prog}}\,e^{\text{prog}} - (\mathsf{delay}\,P)(\mathrm{C}^P_{\text{in}}, \mathsf{chan}\,e^{\text{prog}}) > t^{\text{sys}} \geq t^{\text{sys}\prime}
\end{aligned}$$

The last two inequalities are by assumption and since $n' < n$, respectively. Hence, our initial assumption lead to the conclusion that there exists a start transition of actor A from a state in which A is not ready, or that E^{sys} is not a correct execution, which is a contradiction.

Assume there exists correct execution E^{sys} of $\langle P, R\rangle$, n, $\langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}}\rangle$, and e^{prog} such that

$$E^{\text{sys}}_{2n} = \langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}}\rangle,$$

$$e^{\text{prog}} \in Q,$$

and

$$\mathsf{time}^{\text{prog}}\,e^{\text{prog}} - t^{\text{sys}} < -(\mathsf{delay}\,P)(\mathsf{chan}\,e^{\text{prog}}, \mathrm{C}^P_{\text{out}}).$$

If $\mathsf{chan}\,e^{\text{prog}} \in \mathrm{C}^P_{\text{out}}$, the inequality becomes

$$\mathsf{time}^{\text{prog}}\,e^{\text{prog}} > t^{\text{sys}}$$

which would imply that E^{sys} is not output-safe. Therefore, there is A such that $\mathsf{chan}\,e^{\text{prog}} \in \mathrm{C}^A_{\text{in}}$. Furthermore, because we have constrained actors to be output homogeneous, and by definition of $(\mathsf{delay}\,P)$ there exists a path from $\mathsf{chan}\,e^{\text{prog}}$ to $\mathrm{C}^P_{\text{out}}$ with delay equal to $(\mathsf{delay}\,P)(\mathsf{chan}\,e^{\text{prog}}, \mathrm{C}^P_{\text{out}})$, it is easy to see that after e^{prog} and its descendants are processed, an event with timestamp $\mathsf{time}^{\text{prog}}\,e^{\text{prog}} + (\mathsf{delay}\,P)(\mathsf{chan}\,e^{\text{prog}}, \mathrm{C}^P_{\text{out}})$ will appear at one of the programs output channels. Hence, there is n', $\langle Q', \iota', \varepsilon', \rho', \pi', t^{\text{sys}\prime}\rangle$, and $e^{\text{prog}\prime}$ such that

$$\begin{aligned}
&n' > n, \\
&E^{\text{sys}}_{2n'} = \langle Q', \iota', \varepsilon', \rho', \pi', t^{\text{sys}\prime}\rangle, \\
&e^{\text{prog}\prime} \in Q', \\
&\mathsf{chan}\,e^{\text{prog}\prime} \in \mathrm{C}^P_{\text{out}},
\end{aligned}$$

and

$$\mathsf{time}^{\text{prog}}\,e^{\text{prog}\prime} = \mathsf{time}^{\text{prog}}\,e^{\text{prog}} + (\mathsf{delay}\,P)(\mathsf{chan}\,e^{\text{prog}}, \mathrm{C}^P_{\text{out}}).$$

Furthermore, since $n' > n$,

$$t^{\text{sys}\prime} \geq t^{\text{sys}} > \mathsf{time}^{\text{prog}}\,e^{\text{prog}} + (\mathsf{delay}\,P)(\mathsf{chan}\,e^{\text{prog}}, \mathrm{C}^P_{\text{out}}) = \mathsf{time}^{\text{prog}}\,e^{\text{prog}\prime}$$

or

$$t^{\text{sys}\prime} > \mathsf{time}^{\text{prog}}\,e^{\text{prog}\prime}$$

which implies that E^{sys} is not output safe, therefore we again reached a contradiction.

□

Theorem 7.2. *For every correct execution E^{sys} of $\langle P, R\rangle$, every n and $\langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}}\rangle$ such that*

$$E^{\text{sys}}_{2n} = \langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}}\rangle,$$

and every $A \in P$, the following are true:

1. *for every $c \in \mathrm{C}^A_{\text{in}}$,*

$$|\{e^{\text{prog}} \mid e^{\text{prog}} \in Q \text{ and } \mathsf{chan}\, e^{\text{prog}} = c\}| \leq \frac{(\mathsf{delay}\, P)(\mathrm{C}^P_{\text{in}}, c) + (\mathsf{delay}\, P)(c, \mathrm{C}^P_{\text{out}})}{\inf R(A)};$$

2. *for every $c \in \mathrm{C}^A_{\text{out}}$,*

$$|\{e^{\text{prog}} \mid e^{\text{prog}} \in Q \text{ and } \mathsf{chan}\, e^{\text{prog}} = c\}| \leq \frac{(\mathsf{delay}\, P)(\mathrm{C}^P_{\text{in}}, c) + (\mathsf{delay}\, P)(c, \mathrm{C}^P_{\text{out}})}{\inf R(A)} + 1.$$

Proof. Assume A, c, n, $\langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}}\rangle$, e^{prog}, and N such that

$$A \in P,$$

$$c \in \mathrm{C}^A_{\text{in}},$$

$$E^{\text{sys}}_{2n} = \langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}}\rangle,$$

$$e^{\text{prog}} \in Q,$$

$$\mathsf{chan}\, e^{\text{prog}} = c,$$

$$\mathsf{time}^{\text{prog}}\, e^{\text{prog}} = \max\{\mathsf{time}^{\text{prog}}\, e^{\text{prog}\prime} \mid e^{\text{prog}\prime} \in Q \text{ and } \mathsf{chan}\, e^{\text{prog}\prime} = c\},$$

and

$$N = |\{e^{\text{prog}} \mid e^{\text{prog}} \in Q \text{ and } \mathsf{chan}\, e^{\text{prog}} = c\}|.$$

The deadline of e^{prog} is $\mathsf{time}^{\text{prog}}\, e^{\text{prog}} + (\mathsf{delay}\, P)(\mathsf{chan}\, e^{\text{prog}}, \mathrm{C}^P_{\text{out}})$.

Note that system time cannot grow larger than $\mathsf{time}^{\text{prog}}\, e^{\text{prog}} + (\mathsf{delay}\, P)(\mathsf{chan}\, e^{\text{prog}}, \mathrm{C}^P_{\text{out}})$ before e^{prog} reaches an actuator channel, otherwise e^{prog} would miss its deadline and E^{sys} would not be output-safe.

Let $t^{\text{sys}\prime}$ be the system time that A finishes processing e^{prog}. Since E^{sys} is output-safe, it has to at least be the case that $t^{\text{sys}\prime} \leq \mathsf{time}^{\text{prog}}\, e^{\text{prog}} + (\mathsf{delay}\, P)(\mathsf{chan}\, e^{\text{prog}}, \mathrm{C}^P_{\text{out}})$

Because e^{prog} has the largest timestamp between the events in channel c, t^{sys} and $t^{\text{sys}\prime}$ are separated by at least N executions of actor A, or

$$t^{\text{sys}\prime} - t^{\text{sys}} \geq N \cdot \inf R(A).$$

Hence, since e^{prog} cannot miss its deadline in E^{sys}, it is necessary that

$$N \cdot \inf R(A) + t^{\text{sys}} \leq \mathsf{time}^{\text{prog}}\, e^{\text{prog}} + (\mathsf{delay}\, P)(\mathsf{chan}\, e^{\text{prog}}, \mathrm{C}^P_{\text{out}})$$

$$N \leq \frac{\mathsf{time}^{\text{prog}}\, e^{\text{prog}} - t^{\text{sys}} + (\mathsf{delay}\, P)(\mathsf{chan}\, e^{\text{prog}}, \mathrm{C}^P_{\text{out}})}{\inf R(A)}$$

Using the bound from 7.1 for the difference between $\mathsf{time}^{\text{prog}}\, e^{\text{prog}} - t^{\text{sys}}$,

$$N \leq \frac{(\mathsf{delay}\, P)(\mathrm{C}^P_{\text{in}}, \mathsf{chan}\, e^{\text{prog}}) + (\mathsf{delay}\, P)(\mathsf{chan}\, e^{\text{prog}}, \mathrm{C}^P_{\text{out}})}{\inf R(A)}$$

Assume A, c, n, $\langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}} \rangle$, e^{prog}, and N such that

$$A \in P,$$

$$c \in \mathrm{C}_{\text{out}}^{A},$$

$$E_{2n}^{\text{sys}} = \langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}} \rangle,$$

$$e^{\text{prog}} \in Q,$$

$$\mathsf{chan}\, e^{\text{prog}} = c,$$

$$\mathsf{time}^{\text{prog}}\, e^{\text{prog}} = \min \{ \mathsf{time}^{\text{prog}}\, e^{\text{prog}\prime} \mid e^{\text{prog}\prime} \in Q \text{ and } \mathsf{chan}\, e^{\text{prog}\prime} = c \},$$

and

$$N = |\{ e^{\text{prog}} \mid e^{\text{prog}} \in Q \text{ and } \mathsf{chan}\, e^{\text{prog}} = c \}|.$$

Let $t^{\text{sys}\prime}$ be the time of the finish transition of A that produced e^{prog}.

Because e^{prog} does not to miss its deadline in E^{sys}, it has to be:

$$t^{\text{sys}} \leq \mathsf{time}^{\text{prog}}\, e^{\text{prog}} + (\mathsf{delay}\, P)(c, \mathrm{C}_{\text{out}}^{P})$$

By choosing e^{prog} to have the smallest timestamp between events in c, it can be inferred that since $t^{\text{sys}\prime}$, A has been executed $N - 1$ times, therefore

$$t^{\text{sys}} - t^{\text{sys}\prime} \geq N \cdot \inf R(A).$$

Combining the two inequalities:

$$\begin{aligned} (N-1) \cdot \inf R(A) + t^{\text{sys}\prime} &\leq \mathsf{time}^{\text{prog}}\, e^{\text{prog}} + (\mathsf{delay}\, P)(c, \mathrm{C}_{\text{out}}^{P}) \\ N &\leq \frac{\mathsf{time}^{\text{prog}}\, e^{\text{prog}} - t^{\text{sys}\prime} + (\mathsf{delay}\, P)(c, \mathrm{C}_{\text{out}}^{P})}{\inf R(A)} + 1 \end{aligned}$$

Again using 7.1:

$$N \leq \frac{(\mathsf{delay}\, P)(\mathrm{C}_{\text{in}}^{P}, c) + (\mathsf{delay}\, P)(c, \mathrm{C}_{\text{out}}^{P})}{\inf R(A)} + 1.$$

□

Theorem 7.2 allows to further abstract under the `error` state all those system states that have channels with more events than the specified bound.

Furthermore, note that both system time and event logical times can grow unboundedly. However, it is possible instead of using system time to timestamp new events at the input transitions, to track the relative time that an event is in the program. This alternative involves associating a *timer* and a *delay* with each event. At input transitions, the timer and the delay are set to zero. At time transitions, all the events's timers are increased by the time elapsed. At every finish transition, the delay of each event in the output action is set equal to the sum of the delay of the input action and the delay of the corresponding output channel of the actor. It is easy to see that the difference between the delay and the timer is always equal to the difference between the logical time of the event and system time. Since all operations of the EDF transition system only involve differences between logical time and system time, this alternative scheme, which tracks the relative time an event is in the program, can replace system time and event

logical times. Moreover, because of Theorem 7.1, it is possible to keep timers and delays of events bounded. Since their difference is bounded, we can set a limit for the value of a timer, and exactly when the timer crosses the limit, reset it and subtract the value of the limit from the corresponding delay so that their difference stays the same.

So far, we have argued that the part of the EDF transition system that handles events has a bounded discrete state and uses timers that are linearly compared and reset. Therefore, that can be implemented with a timed automaton. What remains is to see whether the part of the system that deals with actor execution can also be implemented using finite state and "clocks".

We write $\mathsf{worst}\, R$ for a function from P to $\mathscr{P}_{\geq 1}\, \mathbb{T}$ such that for every $A \in P$,

$$(\mathsf{worst}\, R)(A) = \{\sup R(A)\}.$$

Theorem 7.3. *$\langle\langle P, R\rangle, I\rangle$ is schedulable if and only if $\langle\langle P, \mathsf{worst}\, R\rangle, I\rangle$ is schedulable.*

Proof. In order that to see that if $\langle\langle P, R\rangle, I\rangle$ is schedulable then $\langle\langle P, \mathsf{worst}\, R\rangle, I\rangle$ is schedulable, note that, by definition, $\mathsf{worst}\, R \subseteq R$ and therefore for a program execution E^{prog} of P and $A \in P$,

$$\mathscr{S}_{|\mathsf{trace}^A_{\text{start}}\, E^{\text{prog}}|}(\mathsf{worst}\, R)(A) \subseteq \mathscr{S}_{|\mathsf{trace}^A_{\text{start}}\, E^{\text{prog}}|}\, R(A)$$

and

$$(\text{RO}\, \langle P, \mathsf{worst}\, R\rangle)(E^{\text{prog}}) \subseteq (\text{RO}\, \langle P, R\rangle)(E^{\text{prog}}).$$

We can thus replace the statement $O \in (\text{RO}\, \langle P, R\rangle)$ with $O \in (\text{RO}\, \langle P, \mathsf{worst}\, R\rangle)$ in the schedulability statement of $\langle\langle P, R\rangle, I\rangle$ and infer the schedulability of $\langle\langle P, \mathsf{worst}\, R\rangle, I\rangle$.

We next prove that if $\langle\langle P, \mathsf{worst}\, R\rangle, I\rangle$ is schedulable then $\langle\langle P, R\rangle, I\rangle$ is schedulable.

It is easy to see that for any s^{prog}, if there is a correct execution E^{sys} of $\langle P, R\rangle$, $A \in P$, i, s, α, r, such that $\mathsf{in\ prog}\, E^{\text{sys}} = s^{\text{prog}}$, and $(\mathsf{trace}^A_{\text{start}}\, E^{\text{sys}})(i) = \langle\langle A, \langle s, \alpha\rangle\rangle, r\rangle$, then for any r' such that $r' \leq r$, we can construct a correct execution $E^{\text{sys}\prime}$ such that $\mathsf{in\ prog}\, E^{\text{sys}\prime} = s^{\text{prog}}$, $(\mathsf{trace}^A_{\text{start}}\, E^{\text{sys}\prime})(i) = \langle\langle A, \langle s, \alpha\rangle\rangle, r'\rangle$, and will all other start transitions the same as E^{sys}.

We construct $E^{\text{sys}\prime}$ starting from E^{sys} in the following way:

We change the corresponding start transition by replacing the execution time r with r'.

There is n, d, ρ_1, and ρ_2 such that $E^{\text{sys}}_{2n+1} = d$, the value of $\rho(A)$ in E^{sys}_{2n} is ρ_1, the value of $\rho(A)$ in E^{sys}_{2n+2} is ρ_2, $\rho_2 \leq r - r'$, $n > i$, and n is the smallest such n.

We replace the time transition E^{sys}_{2n+1} with a time transition of $\rho_1 - (r - r')$ and a following scheduler transition of `NULL`.

We subtract $r - r'$ from the value of $\rho(A)$ from all states between i and n, and in the states and transitions that follow n up to the first finish transition of A we set $\rho(A)$ to zero, and replace all scheduler transitions of A with `NULL`.

We can perform the same transformation for multiple start transitions of A, as well as for multiple actors, without violating safety or fairness in the resulting executions. Therefore we can infer that $\langle\langle P, R\rangle, I\rangle$ is schedulable from the fact that $\langle\langle P, \mathsf{worst}\, R\rangle, I\rangle$ is schedulable.

□

The following is immediate:

Corollary 7.4. *For every correct execution* E^{sys} *of* $\langle P, \mathsf{worst}\, R\rangle$*, every* n *and* $\langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}}\rangle$ *such that*

$$E^{\text{sys}}_{2n} = \langle Q, \iota, \varepsilon, \rho, \pi, t^{\text{sys}}\rangle,$$

and every $A \in P$*, the following are true:*

1. *for every* $c \in \mathrm{C}^A_{\text{in}}$,

$$|\{e^{\text{prog}} \mid e^{\text{prog}} \in Q \text{ and } \mathsf{chan}\, e^{\text{prog}} = c\}| \leq \frac{(\mathsf{delay}\, P)(\mathrm{C}^P_{\text{in}}, c) + (\mathsf{delay}\, P)(c, \mathrm{C}^P_{\text{out}})}{\sup R(A)};$$

2. *for every* $c \in \mathrm{C}^A_{\text{out}}$,

$$|\{e^{\text{prog}} \mid e^{\text{prog}} \in Q \text{ and } \mathsf{chan}\, e^{\text{prog}} = c\}| \leq \frac{(\mathsf{delay}\, P)(\mathrm{C}^P_{\text{in}}, c) + (\mathsf{delay}\, P)(c, \mathrm{C}^P_{\text{out}})}{\sup R(A)} + 1.$$

In the EDF transition system, actor execution is tracked using the ρ function. At the start transition of an actor A, $\rho(A)$ is set equal to a value in $R(A)$, which from Theorem 7.3 can be fixed to $\sup R(A)$, and the ρ value of the actor that is executing decreases as time elapses at time transitions. An actor completes its execution when its ρ value is equal to zero. Note that this is equivalent to setting $\rho(A)$ to zero initially and increase it until it reaches $\sup R(A)$. To show that this functionality can be implemented with clocks that do not freeze when an actor is not executing, we add in the state a value that tracks the total preemption time of an actor. When an actor A is first assigned the processor, $\rho(A)$ is set to zero, and at time transitions all ρ values are increased by the elapsed time. When an actor A is preempted by another actor B, $\sup R(B)$ is added to the preemption time of A. An actor A finishes executing when its ρ value is equal to the sum of $\sup R(A)$ and its preemption time. The scheme above is correct since, in EDF, when B preempts A, B will finish executing before A executes again. Lastly, note that an actor is added to ρ's domain when the actor is first allocated the processor and not at the start transition. This is because any delay that follows the allocation time can be accounted for precisely, whereas the interval between start time and allocation time cannot.

With actor execution, all parts of the system have been shown to require finite discrete state and continuous variables that behave like clocks. Hence, the EDF transition system can be implemented as a timed automaton. We use timed automata with deadlines and priorities, as introduced in [5], because we found them to simplify modeling. We write $\mathsf{TADP}\,\langle\langle P, R\rangle, b\rangle$ for the resulting timed automaton with deadlines and priorities that simulates safe EDF executions for system $\langle P, R\rangle$, where b is the chosen limit of the event timers.

Of course, in a timed automaton implementation of the system, the inputs also have to be described using a timed automaton. An *input model* of sort C is a timelock-free TADP (see [4]) such that the label set of the automaton is a subset of $L \subseteq C \cup \{\tau\}$, and in any run of the automaton, for each time instant, and every $c \in C$, there can only be one transition with label c.

We postulate a non-empty class $\mathbb{X}$ of *clock symbols*.

Assume a non-empty subset X of $\mathbb{X}$.

Definition 7.5. An X-valuation is a function from X to $\mathbb{T}$.

We write $\mathrm{V}(X)$ for the set of all X-valuations.

Definition 7.6. An X-constraint is a member of the smallest set of formulas Γ such that the following are true:

1. for every $x \in X$ and $r \in \mathbb{Q}$, the following are true:

   (a) $x \leq r \in \Gamma$;
   (b) $r \leq x \in \Gamma$;
2. for every $x_1, x_2 \in X$ and $r \in \mathbb{Q}$, the following are true:
   (a) $x_1 - x_2 \leq r \in \Gamma$;
   (b) $r \leq x_1 - x_2 \in \Gamma$;
3. for every $\gamma \in \Gamma$, $\neg\gamma \in \Gamma$;
4. for every $\gamma_1, \gamma_2 \in \Gamma$, $\gamma_1 \wedge \gamma_2 \in \Gamma$.

We write $\Gamma(X)$ for the set of all X-constraints.

For every X-valuation v and every X-constraint γ, we say that v *satisfies* γ, and write $\models \gamma(v)$, if and only if one of the following is true:

1. there is $x \in X$ and $r \in \mathbb{Q}$ such that one of the following is true:
   (a) $\gamma = x \leq r$ and $v(x) \leq r$;
   (b) $\gamma = x \geq r$ and $r \leq v(x)$;
2. there is $x_1, x_2 \in X$ and $r \in \mathbb{Q}$ such that one of the following is true:
   (a) $\gamma = x_1 - x_2 \leq r$ and $v(x_1) - v(x_2) \leq r$;
   (b) $\gamma = r \geq x_1 - x_2$ and $r \leq v(x_1) - v(x_2)$;
3. there is γ' such that $\gamma = \neg\gamma'$, and v does not satisfy γ';
4. there is γ_1 and γ_2 such that $\gamma = \gamma_1 \wedge \gamma_2$, and v satisfies γ_1 and γ_2.

Definition 7.7. A *timed automaton with deadlines and priorities* (*TADP*) is an ordered sextuple $\langle S, s_{\text{init}}, L, X, T, \preceq \rangle$ such that the following are true:

1. S is a finite set;
2. $s_{\text{init}} \in S$;
3. L is a finite set;
4. X is a subset of $\mathbb{X}$;
5. T is a subset of $S \times \Gamma(X) \times \Gamma(X) \times L \times \mathscr{P} X \times S$ such that for every $\langle s_1, \gamma, \delta, l, U s_2 \rangle \in T$ and every $v \in \mathrm{V}(X)$, if $\models \delta(v)$, then $\models \gamma(v)$;
6. $\preceq$ is an order on L.

Assume a TADP $\langle S, s_{\text{init}}, L, X, T, \preceq \rangle$.

We write $\longrightarrow_{\langle S, s_{\text{init}}, L, X, T, \preceq \rangle}$ for a ternary relation between $S \times \mathrm{V}(X)$, L, and $S \times \mathrm{V}(X)$ such that for every $\langle s_1, v_1 \rangle \in S \times \mathrm{V}(X)$, $l \in L$, and $\langle s_2, v_2 \rangle \in S \times \mathrm{V}(X)$,

$$\longrightarrow_{\langle S, s_{\text{init}}, L, X, T, \preceq \rangle} (\langle s_1, v_1 \rangle, l, \langle s_2, v_2 \rangle)$$

if and only if there is γ, δ, and U such that the following are true:

1. $\langle s_1, \gamma, \delta, l, U, s_2 \rangle \in T$ and $\models \gamma(v_1)$, and for every γ', δ', l', U', and s_2' such that $\langle s_1, \gamma', \delta', l', U', s_2' \rangle \in T$ and $\models \gamma'(v_1)$, $l' \preceq l$;

2. for every $x \in X$,

$$v_2(x) = \begin{cases} 0 & \text{if } x \in U; \\ v_1(x) & \text{otherwise.} \end{cases}$$

We write $\langle s_1, v_1 \rangle \xrightarrow{l}_{\langle S, s_{\text{init}}, L, X, T, \preceq \rangle} \langle s_2, v_2 \rangle$ if and only if $\longrightarrow_{\langle S, s_{\text{init}}, L, X, T, \preceq \rangle} (\langle s_1, v_1 \rangle, l, \langle s_2, v_2 \rangle)$.

We write $\dashrightarrow_{\langle S, s_{\text{init}}, L, X, T, \preceq \rangle}$ for a ternary relation between $S \times \mathrm{V}(X)$, $\mathbb{T}$, and $S \times \mathrm{V}(X)$ such that for every $\langle s_1, v_1 \rangle \in S \times \mathrm{V}(X)$, $d \in \mathbb{T}$, and $\langle s_2, v_2 \rangle \in S \times \mathrm{V}(X)$,

$$\dashrightarrow_{\langle S, s_{\text{init}}, L, X, T, \preceq \rangle} (\langle s_1, v_1 \rangle, d, \langle s_2, v_2 \rangle)$$

if and only if the following are true:

1. $s_1 = s_2$, and for every γ, δ, l, U, and s_2' such that $\langle s_1, \gamma, \delta, l, U, s_2' \rangle \in T$, and every $d' < d$, $\not\models \delta(v_1')$, where v_1' is an X-valuation such that for every $x \in X$,

$$v_1'(x) = v_1(x) + d'.$$

2. for every $x \in X$,

$$v_2(x) = v_1(x) + d.$$

We write $\langle s_1, v_1 \rangle \xrightarrow{d}_{\langle S, s_{\text{init}}, L, X, T, \preceq \rangle} \langle s_2, v_2 \rangle$ if and only if $\dashrightarrow_{\langle S, s_{\text{init}}, L, X, T, \preceq \rangle} (\langle s_1, v_1 \rangle, d, \langle s_2, v_2 \rangle)$.

Definition 7.8. A *run* of $\langle S, s_{\text{init}}, L, X, T, \preceq \rangle$ is an infinite sequence R such that the following are true:

1. there is $v_{\text{init}} \in \mathrm{V}(X)$ such that for every $x \in X$, $v_{\text{init}}(x) = 0$, and $R(0) = \langle s_{\text{init}}, v_{\text{init}} \rangle$;
2. for every $n \in \mathbb{N}$, one of the following is true:
   (a) $R(2 \cdot n) \xrightarrow{R(2 \cdot n+1)}_{\langle S, s_{\text{init}}, L, X, T, \preceq \rangle} R(2 \cdot n + 2)$;
   (b) $R(2 \cdot n) \dashrightarrow^{R(2 \cdot n+1)}_{\langle S, s_{\text{init}}, L, X, T, \preceq \rangle} R(2 \cdot n + 2)$;

We say that s is *reachable* in $\langle S, s_{\text{init}}, L, X, T, \preceq \rangle$ if and only if there is a run R of $\langle S, s_{\text{init}}, L, X, T, \preceq \rangle$, n, and $v \in V(X)$ such that $R(n) = \langle s, v \rangle$.

Assume a run R of $\langle S, s_{\text{init}}, L, X, T, \preceq \rangle$.

We write $\mathsf{lapse}\, R$ for a function from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{T}$ such that for every $n_1, n_2 \in \mathbb{N}$,

$$(\mathsf{lapse}\, R)(n_1, n_2) = \sum \{R(2 \cdot n + 1) \mid n_1 \leq n < n_2 \text{ and } R(2 \cdot n' + 1) \in \mathbb{T}\}.$$

We say that R is *divergent* if and only if for every $t \in \mathbb{T}$, there is $n \in \mathbb{N}$ such that

$$t \leq (\mathsf{lapse}\, R)(0, n).$$

We say that $\langle S, s_{\text{init}}, L, X, T, \preceq \rangle$ is *timelock-free* if and only if for every run R of $\langle S, s_{\text{init}}, L, X, T, \preceq \rangle$, and every $n \in \mathbb{N}$, there is a divergent run R' of $\langle S, s_{\text{init}}, L, X, T, \preceq \rangle$ such that for any $n' < n$,

$$R'(2 \cdot n') = R(2 \cdot n')$$

and

$$R'(2 \cdot n' + 1) = R(2 \cdot n' + 1).$$

Previously we described how the difference of event program and system time is sufficient to determine if an execution is safe and EDF. In a timed automaton, it is possible to simulate that difference using for each event a timer clock and an accumulated delay value. When a new event arrives in the system, it is associated with a new clock that is reset and an accumulated delay value set to zero. For new events that are generated when an actor finishes executing, the same clock as the actor input is used and the new accumulated delay values are adjusted according to the actor delay values. Since the accumulated delay and clock difference is bounded, and the clock grows continuously, we can keep both bounded by resetting the clock exactly when it crosses a specific limit and adjusting at the same time the accumulated value so that their difference stays the same.

We express the clock limit value as a multiple of the greatest common divisor of the actor delays, thereby restricting the delay accumulator values to a finite domain, as described next.

Assume $b \in \mathbb{N}$.

We write $\mathrm{R}_{\mathrm{AD}}(b)$ for a function from $\mathsf{chan}\, P$ to $\mathscr{P}_{\mathrm{fin}}\, \mathbb{Q}$ such that for every $c \in \mathsf{chan}\, P$,

$$\mathrm{R}_{\mathrm{AD}}(b)(c) = \{i \cdot g \mid i \in \mathbb{Z} \qquad \text{and } -(\mathsf{delay}\, P)(c, \mathrm{C}^P_{\mathrm{out}}) \leq i \cdot g \leq (\mathsf{delay}\, P)(\mathrm{C}^P_{\mathrm{in}}, c) + b \cdot g\},$$

where $g = \mathrm{GCD}(\{(\mathsf{delay}\, A)(c) \mid A \in P \text{ and } c \in \mathrm{C}^A_{\mathrm{out}}\})$.

We write $\mathrm{b}_{\mathrm{queue}}$ for a function from $\mathsf{chan}\, P$ to $\mathbb{N}$ such that for every $c \in \mathsf{chan}\, P$ and every $A \in P$,

$$\mathrm{b}_{\mathrm{queue}}(c) = \begin{cases} \left\lfloor \frac{(\mathsf{delay}\, P)(\mathrm{C}^P_{\mathrm{in}}, c) + (\mathsf{delay}\, P)(c, \mathrm{C}^P_{\mathrm{out}})}{(\sup R)(A)} \right\rfloor & \text{if } c \in \mathrm{C}^A_{\mathrm{in}}; \\ \left\lfloor \frac{(\mathsf{delay}\, P)(\mathrm{C}^P_{\mathrm{in}}, c) + (\mathsf{delay}\, P)(c, \mathrm{C}^P_{\mathrm{out}})}{(\sup R)(A)} \right\rfloor + 1 & \text{if } c \in \mathrm{C}^A_{\mathrm{out}} \cap \mathrm{C}^P_{\mathrm{out}}. \end{cases}$$

In order to track the execution of actors, we associate a clock with each actor. The clock is reset every time an actor starts executing in the processor. The execution is complete when the clock value turns equal to the actor's execution time, if the actor is not preempted. If it is preempted, since its clock cannot freeze during the preemption time, detecting completion becomes more difficult. We circumvent the problem by maintaining in the state a map from actors to preemption delays. When an actor is preempted by another actor, the execution time of the latter is added to the map value for the former. When the preempted actor resumes we compare its clock to the sum of its execution time and the map value. The method is correct since if actor A preempts B, then A will not resume until B completes.

Furthermore, since relative deadlines were shown to be bounded, if an actor is preempted too many times the events processing will lose their deadline. Observe that when an actor A is preempted k times by an actor B, we know that at least $(k-1) \cdot (\sup R(B))$ time units have passed since A started executing. Therefore a combination of other actor execution times is a possible preemption delay for an actor as long as it does not imply that more time than the actor's maximum relative deadline has gone by.

We write R_{PD} for a function from P to $\mathscr{P}_{\mathrm{fin}}\, \mathbb{Q}$ such that for every $A \in P$ and every $r \in \mathbb{Q}$, $r \in \mathrm{R}_{\mathrm{PD}}(A)$ if and only if there is a subset P' of $P \setminus \{A\}$, and a function f from P' to $\mathbb{N}$ such that

$$\sum \{f(A') \cdot (\sup R)(A') \mid A' \in P'\} \leq (\mathsf{delay}\, P)(\mathrm{C}^P_{\mathrm{in}}, \mathrm{C}^A_{\mathrm{in}}) + (\mathsf{delay}\, P)(\mathrm{C}^A_{\mathrm{in}}, \mathrm{C}^P_{\mathrm{out}})$$

and

$$r = \sum \{(f(A') + 1) \cdot (\sup R)(A') \mid A' \in P'\}.$$

For every $n \in \mathbb{N}$, we fix a distinct clock symbol $\mathtt{x}_n$, and for every actor A, a distinct clock symbol $\mathtt{x}_A$.

We write $\mathsf{TADP}\, \langle \langle P, R \rangle, b \rangle$ for a TADP $\langle S, s_{\mathrm{init}}, L, X, T, \preceq \rangle$ such that the following are true:

1. S is the set of all s such that one of the following is true:

(a) s is a ordered quadruple $\langle Q, \varepsilon, \rho, \pi \rangle$ such that the following are true:

i. Q is a function from $\mathsf{chan}\, P$ such that for every $c \in \mathsf{chan}\, P$, $Q(c) \in \mathscr{S}_{\leq \mathrm{b}_{\mathrm{queue}}(c)}(X \times \mathrm{R}_{\mathrm{AD}}(b)(c))$;

ii. there is a subset P_{exec} of P such that ε is a function from P_{exec} such that for any $A \in P_{\mathrm{exec}}$,

$$\varepsilon(A) \in X \times \bigcup \{\mathrm{R}_{\mathrm{AD}}(b)(c) \mid c \in \mathrm{C}_{\mathrm{in}}^{A}\};$$

iii. there is a subset P_{run} of $\mathsf{dom}\, \varepsilon$ such that ρ is a function from P_{run} such that for any $A \in P_{\mathrm{run}}$,

$$\rho(A) \in \mathrm{R}_{\mathrm{PD}}(A);$$

iv. $\pi \in \{\mathtt{NULL}\} \cup P$;

(b) $s = \mathtt{error}$;

2. s_{init} is an ordered quadruple $\langle Q_{\mathrm{init}}, \varepsilon_{\mathrm{init}}, \rho_{\mathrm{init}}, \pi_{\mathrm{init}} \rangle$ such that the following are true:

(a) Q_{init} is a function from $\mathsf{chan}\, P$ such that for every $c \in \mathsf{chan}\, P$,

$$Q_{\mathrm{init}}(c) = \langle\ \rangle;$$

(b) $\varepsilon_{\mathrm{init}}$ is the empty function;

(c) ρ_{init} is the empty function;

(d) $\pi_{\mathrm{init}} = \mathtt{NULL}$;

3. $L = (\mathrm{C}_{\mathrm{in}}^{P}) \cup \{\mathtt{start}\text{-}A, \mathtt{finish}\text{-}A \mid A \in P\} \cup P \cup (\mathrm{C}_{\mathrm{out}}^{P}) \cup \{\mathtt{bound}\} \cup \{\mathtt{miss}\}$;

4. $X = \{\mathtt{x}_n \mid n \in \mathbb{N} \text{ and } n < \sum \{\mathrm{b}_{\mathrm{queue}}(c) \mid c \in \mathsf{chan}\, P\}\} \cup \{\mathtt{x}_A \mid A \in P\}$;

5. T is a subset of $S \times \Gamma(X) \times \Gamma(X) \times L \times \mathscr{P}\, X \times S$ such that one of the following is true:

(a) for every $\langle Q_1, \varepsilon_1, \rho_1, \pi_1 \rangle \in S$, every $\gamma \in \Gamma(X)$, every $\delta \in \Gamma(X)$, every $l \in L$, every $U \in \mathscr{P}\, X$, and every $\langle Q_2, \varepsilon_2, \rho_2, \pi_2 \rangle \in S$,

$$\langle \langle Q_1, \varepsilon_1, \rho_1, \pi_1 \rangle, \gamma, \delta, l, U, \langle Q_2, \varepsilon_2, \rho_2, \pi_2 \rangle \rangle \in T$$

if and only if one of the following is true:

i. there is $c \in \mathrm{C}_{\mathrm{in}}^{P}$ and i such that the following are true:

A. $|Q_1(c)| < \mathrm{b}_{\mathrm{queue}}(c)$;

B. $i = \min\{j \mid$ for every $c' \in \mathsf{chan}\, P$, every δ, and any $n < |Q_1(c')|$, $Q_1(c')(n) \neq \langle \mathtt{x}_j, \delta \rangle$, and for any $A \in \mathsf{dom}\, \varepsilon_1$ and every δ, $\varepsilon_1(A) \neq \langle \mathtt{x}_j, \delta \rangle\}$;

C. $\gamma = \mathtt{true}$;

D. $\delta = \mathtt{false}$;

E. $l = c$;

F. $U = \{\mathtt{x}_i\}$;

G. for every $c' \in \mathsf{chan}\, P$,

$$Q_2(c') = \begin{cases} Q_1(c') \cdot \langle\langle \mathtt{x}_i, 0 \rangle\rangle & \text{if } c' = c; \\ Q_1(c') & \text{otherwise;} \end{cases}$$

H. $\varepsilon_2 = \varepsilon_1$;

I. $\rho_2 = \rho_1$;

J. $\pi_2 = \pi_1$;

ii. there is A, $I \subseteq \mathrm{C}_{\mathrm{in}}^A$, $c \in I$, and $\langle x, d \rangle$ such that the following are true:

A. for every $c' \in I$, $|Q_1(c')| > 0$, and $\mathsf{head}\, Q_1(c) = \langle x, d \rangle$;

B. $A \notin \mathsf{dom}\, \varepsilon_1$;

C. $\gamma = \gamma_{\text{action}} \wedge \gamma_{\text{safe-to-processs}}$, where the following are true:

(1) $\gamma_{\text{action}} = \bigwedge \{d' - x' = d - x \mid \text{there is } c' \in I \text{ such that } \mathsf{head}\, Q_1(c') = \langle x', d' \rangle\}$;

(2) $\gamma_{\text{safe-to-process}} = \gamma_1 \wedge \gamma_2 \wedge \gamma_3$, where the following are true:

a. $\gamma_1 = x \geq d - (\mathsf{delay}\, P)(\mathrm{C}_{\mathrm{in}}^P, \mathrm{C}_{\mathrm{in}}^A)$;

b. $\gamma_2 = \bigwedge \{d' - x' + (\mathsf{delay}\, P)(c', \mathrm{C}_{\mathrm{in}}^A) > d - x \mid c' \notin I \text{ and } \mathsf{head}\, Q(c') = \langle x', d' \rangle\}$;

c. $\gamma_3 = \bigwedge \{d' - x' + (\mathsf{delay}\, P)(\mathrm{C}_{\mathrm{in}}^{A'}, \mathrm{C}_{\mathrm{in}}^A) > d - x \mid \varepsilon_1(A') = \langle x', d' \rangle\}$;

D. $\delta = \gamma$;

E. $l = \mathtt{start}\text{-}A$;

F. $U = \emptyset$;

G. for every $c' \in \mathsf{chan}\, P$,

$$Q_2(c') = \begin{cases} \mathsf{tail}\, Q_1(c') & \text{if } c' \in I; \\ Q_1(c') & \text{otherwise;} \end{cases}$$

H. $\varepsilon_2 = \varepsilon_1 \cup \{\langle A, \langle x, d \rangle\rangle\}$;

I. $\rho_2 = \rho_1$;

J. $\pi_2 = \pi_1$;

iii. there is $\langle x, d \rangle$ such that the following are true:

A. for any $c \in (\mathrm{C}_{\mathrm{out}}^{\pi_1} \setminus \mathrm{C}_{\mathrm{out}}^P)$, $|Q_1(c)| < \mathrm{b}_{\mathrm{queue}}(c)$;

B. $\varepsilon_1(\pi_1) = \langle x, d \rangle$;

C. $\gamma = \mathtt{x}_{\pi_1} = (\sup R)(\pi_1) + \rho_1(\pi_1)$;

D. $\delta = \gamma$;

E. $l = \mathtt{finish}\text{-}\pi_1$;

F. $U = \emptyset$;

G. for every $c \in \mathsf{chan}\, P$,

$$Q_2(c) = \begin{cases} Q_1(c) \cdot \langle\langle x, d + (\mathsf{delay}\, \pi_1)(c)\rangle\rangle & \text{if } c \in \mathrm{C}^{\pi_1}_{\mathrm{out}}; \\ Q_1(c) & \text{otherwise;} \end{cases}$$

H. $\varepsilon_2 = \varepsilon_1 \setminus \{\langle A, \varepsilon_1(A)\rangle\}$;

I. $\rho_2 = \rho_1 \setminus \{\langle A, \rho_1(A)\rangle\}$;

J. $\pi_2 = \mathtt{NULL}$;

iv. there is $c \in \mathrm{C}^P_{\mathrm{out}}$ and $\langle x, d\rangle$ such that the following are true:

A. $\mathsf{head}\, Q_1(c) = \langle x, d\rangle$;

B. $\gamma = x = d$;

C. $\delta = \gamma$;

D. $l = c$;

E. $U = \emptyset$;

F. for every $c' \in \mathsf{chan}\, P$,

$$Q_2(c') = \begin{cases} \mathsf{tail}\, Q_1(c') & \text{if } c' = c; \\ Q_1(c') & \text{otherwise;} \end{cases}$$

G. $\varepsilon_2 = \varepsilon_1$;

H. $\rho_2 = \rho_1$;

I. $\pi_2 = \pi_1$;

v. there is A and $\langle x, d\rangle$ such that the following are true:

A. $\varepsilon_1(A) = \langle x, d\rangle$;

B. $A \notin \mathsf{dom}\, \rho_1$;

C. $\pi_1 = \mathtt{NULL}$;

D. $\gamma = \bigwedge\{(\mathsf{deadline}\, P)(A, \langle x, d\rangle) \leq (\mathsf{deadline}\, P)(A', \langle x', d'\rangle) \mid \varepsilon_1(A') = \langle x', d'\rangle\}$, where

$$(\mathsf{deadline}\, P)(A, \langle x, d\rangle) = d - x + (\mathsf{delay}\, P)(\mathrm{C}^A_{\mathrm{in}}, \mathrm{C}^P_{\mathrm{out}});$$

E. $\delta = \gamma$;

F. $l = A$;

G. $U = \{\mathtt{x}_A\}$;

H. $Q_2 = Q_1$;

I. $\varepsilon_2 = \varepsilon_1$;

J. ρ_2 is a function from $\mathsf{dom}\, \rho_1 \cup \{A\}$ such that for every $A' \in \mathsf{dom}\, \rho_1 \cup \{A\}$,

$$\rho_2(A') = \begin{cases} 0 & \text{if } A' = A; \\ \rho_1(A') + (\sup R)(A) & \text{otherwise;} \end{cases}$$

K. $\pi_2 = A$;

vi. there is A and $\langle x, d\rangle$ such that the following are true:

A. $\varepsilon_1(A) = \langle x, d\rangle$;

B. $A \notin \mathsf{dom}\,\rho_1$;

C. $\pi_1 \neq \texttt{NULL}$;

D. $\gamma = (\mathsf{deadline}\,P)(A, \langle x, d\rangle) < (\mathsf{deadline}\,P)(\pi_1, \varepsilon_1(\pi_1)) \wedge$
$\bigwedge\{(\mathsf{deadline}\,P)(A, \langle x, d\rangle) \leq (\mathsf{deadline}\,P)(A', \langle x', d'\rangle) \mid \varepsilon_1(A') = \langle x', d'\rangle\}$ where

$$(\mathsf{deadline}\,P)(A, \langle x, d\rangle) = d - x + (\mathsf{delay}\,P)(\mathrm{C}^A_{\mathrm{in}}, \mathrm{C}^P_{\mathrm{out}});$$

E. $\delta = \gamma$;

F. $l = A$;

G. $U = \{\mathtt{x}_A\}$;

H. $Q_2 = Q_1$;

I. $\varepsilon_2 = \varepsilon_1$;

J. ρ_2 is a function from $\mathsf{dom}\,\rho_1 \cup \{A\}$ such that for every $A' \in \mathsf{dom}\,\rho_1 \cup \{A\}$,

$$\rho_2(A') = \begin{cases} 0 & \text{if } A' = A; \\ \rho_1(A') + (\sup R)(A) & \text{otherwise;} \end{cases}$$

K. $\pi_2 = A$;

vii. there is A and $\langle x, d\rangle$ such that the following are true:

A. $\varepsilon_1(A) = \langle x, d\rangle$;

B. $A \in \mathsf{dom}\,\rho_1$;

C. $\pi_1 = \texttt{NULL}$;

D. $\gamma = \bigwedge\{(\mathsf{deadline}\,P)(A, \langle x, d\rangle) \leq (\mathsf{deadline}\,P)(A, \langle x', d'\rangle) \mid \varepsilon_1(A') = \langle x', d'\rangle\}$, where

$$(\mathsf{deadline}\,P)(A, \langle x, d\rangle) = d - x + (\mathsf{delay}\,P)(\mathrm{C}^A_{\mathrm{in}}, \mathrm{C}^P_{\mathrm{out}});$$

E. $\delta = \gamma$;

F. $l = A$;

G. $U = \emptyset$;

H. $Q_2 = Q_1$;

I. $\varepsilon_2 = \varepsilon_1$;

J. $\rho_2 = \rho_1$;

K. $\pi_2 = A$;

viii. there is x and $g = \mathrm{GCD}(\{(\mathsf{delay}\,A)(c) \mid A \in P \text{ and } c \in \mathrm{C}^A_{\mathrm{out}}\})$ such that the following is true:

A. $\gamma = x = b \cdot g$;

B. $\delta = \gamma$;

C. $l = \texttt{bound}$;

D. $U = \{x\}$;

E. for every $c \in \mathsf{chan}\, P$, any $n < |Q_1(c)|$, and every d,

$$Q_2(c)(n) = \begin{cases} \langle x, d - b \cdot g \rangle & \text{if } Q_1(c)(n) = \langle x, d \rangle; \\ Q_1(c)(n) & \text{otherwise;} \end{cases}$$

F. for any $A \in \mathsf{dom}\, \varepsilon_1$ and every d,

$$\varepsilon_2(A) = \begin{cases} \langle x, d - b \cdot g \rangle & \text{if } \varepsilon_1(A) = \langle x, d \rangle; \\ \varepsilon_1(A) & \text{otherwise;} \end{cases}$$

G. $\rho_2 = \rho_1$;

H. $\pi_2 = \pi_1$;

(b) for every $\langle Q, \varepsilon, \rho, \pi \rangle \in S$, every $\gamma \in \Gamma(X)$, every $\delta \in \Gamma(X)$, every $l \in L$, and every $U \in \mathscr{P}\, X$,

$$\langle \langle Q, \varepsilon, \rho, \pi \rangle, \gamma, \delta, l, U, \texttt{error} \rangle \in T$$

if and only if one of the following is true:

i. there is $c \in \mathrm{C}_{\mathrm{in}}^P$ such that the following are true:

A. $|Q(c)| = \mathrm{b}_{\mathrm{queue}}(c)$;

B. $\gamma = \texttt{true}$;

C. $\delta = \gamma$;

D. $l = c$;

E. $U = \emptyset$;

ii. there is $c \in (\mathrm{C}_{\mathrm{out}}^{\pi} \setminus \mathrm{C}_{\mathrm{out}}^P)$ such that the following are true:

A. $|Q(c)| = \mathrm{b}_{\mathrm{queue}}(c)$;

B. $\gamma = \mathtt{x}_\pi = (\sup R)(\pi) + \rho(\pi)$;

C. $\delta = \gamma$;

D. $l = \texttt{finish-}\pi$;

E. $U = \emptyset$;

iii. there is c and $\langle x, d \rangle$ such that the following are true:

A. there is n such that $Q(c)(n) = \langle x, d \rangle$;

B. $\gamma = x \geq d + (\mathsf{delay}\, P)(c, \mathrm{C}_{\mathrm{out}}^P)$

C. $\delta = \gamma$;

D. $l = \texttt{miss}$;

E. $U = \emptyset$;

iv. there is A and $\langle x, d \rangle$ such that the following are true:

A. $\varepsilon(A) = \langle x, d \rangle$;

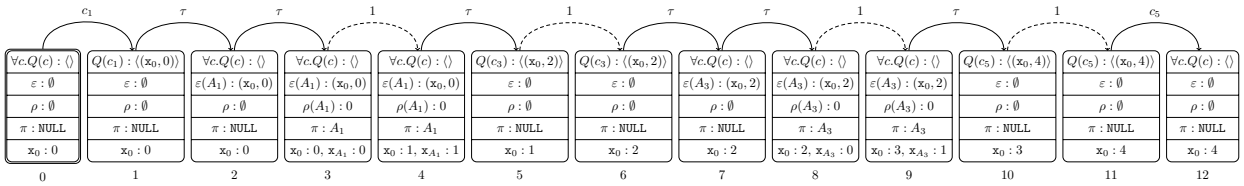

Figure 10. A prefix of a run of the TADP of the system of Figure 3(a) corresponding to the system execution of Figure 8.

B. $\gamma = x \geq d + (\mathsf{delay}\, P)(\mathrm{C}^A_{\mathrm{in}}, \mathrm{C}^P_{\mathrm{out}})$

C. $\delta = \gamma$;

D. $l = \mathtt{miss}$;

E. $U = \emptyset$;

6. $\preceq$ is the least order on L such that the following are true:
   (a) for every $c \in \mathrm{C}^P_{\mathrm{in}}$, $\tau \preceq c$;
   (b) for every $c \in \mathrm{C}^P_{\mathrm{out}}$, $c \preceq \tau$;
   (c) for every $c \in \mathrm{C}^P_{\mathrm{out}}$, $\mathtt{miss} \preceq c$.

Definition 7.9. An *input model* of sort C is a timelock-free TADP $\langle S, s_{\mathrm{init}}, L, X, T, \preceq \rangle$ such that the following are true:

1. $L \subseteq C \cup \{\tau\}$;
2. for every $c \in C$, every run R of $\langle S, s_{\mathrm{init}}, L, X, T, \preceq \rangle$, and every n_1 and n_2 such that $R(n_1) = c$ and $R(n_2) = c$,

$$0 < (\mathsf{lapse}\, R)(n_1, n_2).$$

Assume an input model IM of sort C.

We write $\mathsf{sig}^{\mathrm{prog}}\, IM$ for a subset of $\mathrm{S}^{\mathrm{prog}}(C)$ such that for every $s^{\mathrm{prog}} \in \mathrm{S}^{\mathrm{prog}}(C)$, $s^{\mathrm{prog}} \in \mathsf{sig}^{\mathrm{prog}}\, IM$ if and only if there is a run R of IM such that

$$\{\langle c, t^{\mathrm{prog}} \rangle \mid \text{there is } v \text{ such that } \langle c, t^{\mathrm{prog}}, v \rangle \in s^{\mathrm{prog}}\} = \{\langle R(2 \cdot n + 1), (\mathsf{lapse}\, R)(0, n) \rangle \mid n \in \omega \text{ and } R(2 \cdot n + 1) \in C\}.$$

Figure 10 shows a prefix of a run of the TADP that corresponds to the system of Figure 3(a),

Remark about priority of input transitions: The correctness of TADP $\langle \langle P, R \rangle, b \rangle \mid\mid IM$ depends on correctly implementing the input priority property described earlier in Definition 5.3(4). Specifically, in order to guarantee that start transitions are restricted to actors that are ready, it is necessary that, for every time instant, any input transition happens before other transitions of the timed automaton. We focus on a specific channel $c \in \mathrm{C}^P_{\mathrm{in}}$, and distinguish between two cases: the input model of c can be described with a deterministic timed automaton or not. In the former case, the transitions of IM with label c will be eager, and a higher priority, $\tau \preceq c$, is sufficient to guarantee the input priority property. In the latter case, the IM will include a transition with label c that is delayable or lazy, i.e. it is not necessarily taken as soon as its guard becomes true. Assigning priority $\tau \preceq c$ will block every transition τ as soon as and for as long as that guard is true. Therefore, the implementation of the input priority property that uses $\preceq$ for inputs that correspond to non-deterministic transitions of the IM, is incorrect. Notice that a per time instant instead

of global priority is required. That notion of priority can be implemented with the help of an extra clock x_p. The clock is reset in every transition with label τ, and the guard $x_p > 0$ is conjucted to the guards of all IM transitions with label c. This combination guarantees that for each time instant, a τ transition cannot be followed by an input transition c.

We say that $\mathsf{TADP}\,\langle\langle P, R\rangle, b\rangle \mid\mid IM$ is *safe* if and only if for every s, $\langle \texttt{error}, s\rangle$ is not reachable in $\mathsf{TADP}\,\langle\langle P, R\rangle, b\rangle \mid\mid IM$.

Theorem 7.10. *The following are equivalent:*

1. *for every* $s^{\mathrm{prog}} \in \mathsf{sig}^{\mathrm{prog}}\, IM$*, there is a safe earliest-deadline-first execution* $E^{\mathrm{sys}}_{\mathrm{EDF}}$ *of* $\langle P, \mathsf{worst}\, R\rangle$ *such that* $\mathsf{in}\, E^{\mathrm{sys}}_{\mathrm{EDF}} = s^{\mathrm{prog}}$*;*
2. *for every* $b > 0$*,* $\mathsf{TADP}\,\langle\langle P, R\rangle, b\rangle \mid\mid IM$ *is safe.*

Proof. First, note that statement 1 is not equivalent to the following:

For every $s^{\mathrm{prog}} \in \mathsf{sig}^{\mathrm{prog}}\, IM$, for every earliest-deadline-first execution $E^{\mathrm{sys}}_{\mathrm{EDF}}$ of $\langle P, \mathsf{worst}\, R\rangle$ such that $\mathsf{in}\, E^{\mathrm{sys}}_{\mathrm{EDF}} = s^{\mathrm{prog}}$, $E^{\mathrm{sys}}_{\mathrm{EDF}}$ is safe.

The two statements are not equivalent since there is nothing in the definition of earliest-deadline-first execution that forces it to produce outputs when system time is equal to timestamps of events in the output channels of the program.

However, the following is true: if there is a non-safe earliest-deadline-first system execution on an input signal s^{prog} such that there is an output transition for every event that arrives at an output channel at a system time less than or equal to the timestamp of the event, then there is no safe earliest-deadline-first system execution on that input signal.

We assume that the scheduler transitions of a $\mathsf{TADP}\,\langle\langle P, R\rangle, b\rangle$, i.e. execute v., preempt vi., and resume vii. transitions, or transitions that change the value of π to some actor $A \neq \texttt{NULL}$ have smaller priority than the other transitions. This allows us to assume that at every time instant in a run of a $\mathsf{TADP}\,\langle\langle P, R\rangle, b\rangle \mid\mid IM$ there is at most one scheduler transition, and further that for every two actors $A, A' \in \mathsf{dom}\,\rho$, $\mathtt{x}_A \neq \mathtt{x}_{A'}$ since no two such clocks can be reset at the same time instant (scheduler transitions are the only transitions that reset actor clocks). This transition priority assumption is not necessary for the theorem to be true; it is only made in order to simplify the proof.

If $\mathsf{TADP}\,\langle\langle P, R\rangle, b\rangle = \langle S, s_{\mathrm{init}}, L, X, T, \preceq\rangle$, we define a relation $\mathcal{R} \subseteq \mathsf{state}\,\langle P, R\rangle \times (S \times V(X))$ between states of the system $\langle P, R\rangle$ and states of the timed automaton $\mathsf{TADP}\,\langle\langle P, R\rangle, b\rangle$ such that for every $\langle Q_e, \iota_e, \varepsilon_e, \rho_e, \pi_e, t^{\mathrm{sys}}_e\rangle \in \mathsf{state}\,\langle P, R\rangle$ and every $\langle\langle Q_t, \varepsilon_t, \rho_t, \pi_t\rangle, v_t\rangle \in S \times V(X)$, $\langle\langle Q_e, \iota_e, \varepsilon_e, \rho_e, \pi_e, t^{\mathrm{sys}}_e\rangle, \langle\langle Q_t, \varepsilon_t, \rho_t, \pi_t\rangle, v_t\rangle\rangle \in \mathcal{R}$ if and only if the following true:

1. for every $c \in \mathsf{chan}\, P$, $|\{e^{\mathrm{prog}} \in Q_e \mid \mathsf{chan}\, e^{\mathrm{prog}} = c\}| = |Q_t(c)|$ and for every i and $\langle x, d\rangle$ such that $Q_t(c)(i) = \langle x, d\rangle$, there is $e \in Q_e$ such that $\mathsf{chan}\, e = c$ and $t^{\mathrm{sys}}_e - \mathsf{time}^{\mathrm{prog}}\, e = v_t(x) + d$;
2. $\mathsf{dom}\,\varepsilon_e = \mathsf{dom}\,\varepsilon_t$ and for every $A \in \mathsf{dom}\,\varepsilon_e$ there is s, α, and $\langle x, d\rangle$ such that $\varepsilon_e(A) = \langle s, \alpha\rangle$, $\varepsilon_t(A) = \langle x, d\rangle$, and $\mathsf{time}^{\mathrm{prog}}\,\alpha = t^{\mathrm{sys}}_e + d - v_t(x)$;
3. $\mathsf{dom}\,\rho_e = \mathsf{dom}\,\varepsilon_t$ and for every $A \in \mathsf{dom}\,\varepsilon_t$ one of the following is true:
   (a) $A \notin \mathsf{dom}\,\rho_t$ and $\rho_e(A) = (\mathsf{worst}\, R)(A)$;
   (b) $A \in \mathsf{dom}\,\rho_t$ and one of the following is true:
      i. for every $A' \in \mathsf{dom}\,\rho_t$, $v(\mathtt{x}_{A'}) > v(\mathtt{x}_A)$ and $\rho_e(A) = (\mathsf{worst}\, R)(A) - v_t(\mathtt{x}_A) + \rho_t(A)$
      ii. the set $S = \{v(\mathtt{x}_C) \mid C \in \mathsf{dom}\,\rho_t \text{ and } v(\mathtt{x}_C) < v(\mathtt{x}_A)\}$ is non-empty, and there is $B \in \mathsf{dom}\,\rho_t$ such that $v(\mathtt{x}_B) = \max S$, and $\rho_e(A) = (\mathsf{worst}\, R)(A) - v_t(\mathtt{x}_A) + \rho_t(A) - ((\mathsf{worst}\, R)(B) - v_t(\mathtt{x}_B) + \rho_t(B))$;

4. $\pi_e = \pi_t$.

The intuition behind constraint 3 is the following:

At any point in a run of the $\mathsf{TADP}\,\langle\langle P, R\rangle, b\rangle$, if $A, B \in \mathsf{dom}\,\rho_t$ and $v_t(\mathtt{x}_A) > v_t(\mathtt{x}_B)$, then B started executing on the processor after A did, since actor clocks are only reset when an actor is first executed and never again during its execution. The relation $v_t(\mathtt{x}_A) > v_t(\mathtt{x}_B)$ therefore implies the following: (i) B has a smaller deadline than A, and (ii) B will be fully executed before A gets to run again.

From the observation above, we conclude that out of all the actors $A' \in \mathsf{dom}\,\rho_t$ with $v_t(\mathtt{x}_A) > v_t(\mathtt{x}_{A'})$, the one with the largest clock value is the one that immediately preempted actor A. Let this be actor C. If $\rho_t(A) = 0$ when C preempts A then the amount of time that A has executed for is given by $v_t(\mathtt{x}_A) - v_t(\mathtt{x}_C)$. If $\rho_t(A) \neq 0$, then A was preempted by other actors that completed their execution before C preempted A, and thus the amount of time that A has executed for has to be adjusted to be $v_t(\mathtt{x}_A) - v_t(\mathtt{x}_C) - (\rho_t(A) - \rho_t(C) - (\mathsf{worst}\,R)(C))$.

We now continue with the proof of the theorem and show that 1 implies 2 and vice versa.

$1 \Rightarrow 2$ We prove the contrapositive $\neg 2 \Rightarrow \neg 1$:

Assuming that there is b such that $\mathsf{TADP}\,\langle\langle P, R\rangle, b\rangle \mid\mid IM$ is not safe, we show that there exists $s^{\text{prog}} \in \mathsf{sig}^{\text{prog}}\,IM$ and earliest-deadline-first execution $E^{\text{sys}}_{\text{EDF}}$ of $\langle P, \mathsf{worst}\,R\rangle$ such that $\mathsf{in}\,E^{\text{sys}}_{\text{EDF}} = s^{\text{prog}}$ and $E^{\text{sys}}_{\text{EDF}}$ is not safe. Together with the observation we made about statement 1 in the beginning of the proof this is sufficient to show that statement 1 is not true.

Since $\mathsf{TADP}\,\langle\langle P, R\rangle, b\rangle \mid\mid IM$ is not safe, there exists s such that $\langle \mathtt{error}, s\rangle$ is reachable in $\mathsf{TADP}\,\langle\langle P, R\rangle, b\rangle \mid\mid IM$, or there exists a run R of $\mathsf{TADP}\,\langle\langle P, R\rangle, b\rangle \mid\mid IM$ and n such that $R(n) = \langle \mathtt{error}, s\rangle$.

Let s^{prog} be a signal such that:

$$\{\langle c, t^{\text{prog}}\rangle \mid \text{there is } v \text{ such that } \langle c, t^{\text{prog}}, v\rangle \in s^{\text{prog}}\} = \{\langle R(2\cdot n+1), (\mathsf{lapse}\,R)(0, n)\rangle \mid n \in \omega \text{ and } R(2\cdot n+1) \in C\}.$$

Then $s^{\text{prog}} \in \mathsf{sig}^{\text{prog}}\,IM$.

From run R, we construct an earliest-deadline-first execution $E^{\text{sys}}_{\text{EDF}}$ of $\langle P, \mathsf{worst}\,R\rangle$ such that $\mathsf{in\,prog}\,E^{\text{sys}}_{\text{EDF}} = s^{\text{prog}}$ and $E^{\text{sys}}_{\text{EDF}}$ is not safe.

There is s_{init}, s^{IM}_{init}, and v_{init} such that $R(0) = \langle\langle s_{\text{init}}, s^{IM}_{\text{init}}\rangle, v_{\text{init}}\rangle$

Note that $\langle \mathsf{state}_{\text{init}}\,\langle P, R\rangle, \langle s_{\text{init}}, v_{\text{init}}\rangle\rangle \in \mathcal{R}$.

For each transition of $\mathsf{TADP}\,\langle\langle P, R\rangle, b\rangle$ in run R we add the corresponding transition of the system $\langle P, \mathsf{worst}\,R\rangle$, until we hit the `error` state in R. From that point on, the resulting system execution is guaranteed not to be safe in any way that it gets extended.

We describe a correspondence between transitions of $\mathsf{TADP}\,\langle\langle P, R\rangle, b\rangle$ in a run R and system execution transitions such that the following is true: for every $n \leq \lfloor |R|/2 \rfloor$, there is s, s^{IM}, and v such that $R(2\cdot n) = \langle\langle s, s^{IM}\rangle, v\rangle$, and for every s^{sys} such that $s^{\text{sys}} \in \mathsf{state}\,\langle P, R\rangle$ and $\langle\langle s, v\rangle, s^{\text{sys}}\rangle \in \mathcal{R}$, the system execution transition that corresponds to $R(2\cdot n+1)$ is enabled in s^{sys} and if...

We can show that if there is $s^{\text{sys}} \in \mathsf{state}\,\langle P, \mathsf{worst}\,R\rangle$, n, s^{TADP}_1, s^{IM}_1, and v_1 such that $R(2\cdot n) = \langle\langle s^{\mathsf{TADP}}_1, s^{IM}_1\rangle, v_1\rangle$, $\langle s^{\text{sys}}, \langle s^{\mathsf{TADP}}, v\rangle\rangle \in \mathcal{R}$, and $R(2\cdot n+2) = \langle\langle s^{\mathsf{TADP}}_2, s^{IM}_2\rangle, v_2\rangle$ then the following are true:

- if $s^{\mathsf{TADP}}_2 \neq \mathtt{error}$ and there is $c \in \mathrm{C}^P_{\text{in}}$ such that $R(2\cdot n+1) = c$, then there is $s^{\text{sys}\prime}$ such that $s^{\text{sys}} \xrightarrow{c} s^{\text{sys}\prime}$ and $\langle s^{\text{sys}\prime}, \langle s^{\mathsf{TADP}}_2, v_2\rangle\rangle \in \mathcal{R}$;

- if there is $c \in \mathrm{C}^P_{\text{out}}$ such that $R(2 \cdot n + 1) = c$ then there is $s^{\text{sys}\prime}$ such that $s^{\text{sys}} \xrightarrow{c} s^{\text{sys}\prime}$ and $\langle s^{\text{sys}\prime}, \langle s_2^{\mathsf{TADP}}, v_2 \rangle\rangle \in \mathcal{R}$;
- if there is $A \in P$ such that $R(2 \cdot n + 1) = \texttt{start-}A$, then there is $s \in \mathrm{S}^A$, $\alpha \in \mathrm{IA}(\mathrm{C}^A_{\text{in}})$, and $s^{\text{sys}\prime}$ such that $s^{\text{sys}} \xrightarrow{\langle A, \langle s, \alpha\rangle\rangle} s^{\text{sys}\prime}$ and $\langle s^{\text{sys}\prime}, \langle s_2^{\mathsf{TADP}}, v_2 \rangle\rangle \in \mathcal{R}$;
- if $s_2^{\mathsf{TADP}} \neq \texttt{error}$ and there is $A \in P$ such that $R(2 \cdot n + 1) = \texttt{finish-}A$ then there is $s \in \mathrm{S}^A$, $\alpha \in \mathrm{OA}(\mathrm{C}^A_{\text{out}})$, and $s^{\text{sys}\prime}$ such that $s^{\text{sys}} \xrightarrow{\langle A, \alpha, s\rangle} s^{\text{sys}\prime}$ and $\langle s^{\text{sys}\prime}, \langle s_2^{\mathsf{TADP}}, v_2 \rangle\rangle \in \mathcal{R}$;
- if there is $A \in P$ such that $R(2 \cdot n + 1) = A$ then there is $s^{\text{sys}\prime}$ such that $s^{\text{sys}} \xrightarrow{A} s^{\text{sys}\prime}$ and $\langle s^{\text{sys}\prime}, \langle s_2^{\mathsf{TADP}}, v_2 \rangle\rangle \in \mathcal{R}$;
- if $R(2 \cdot n + 1) = \texttt{bound}$ then $\langle s^{\text{sys}}, \langle s_2^{\mathsf{TADP}}, v_2 \rangle\rangle \in \mathcal{R}$;
- if there is $d \in \mathbb{T}$ such that $R(2 \cdot n + 1) = d$ then there is $s^{\text{sys}\prime}$ such that $s^{\text{sys}} \xrightarrow{d} s^{\text{sys}\prime}$ and $\langle s^{\text{sys}\prime}, \langle s_2^{\mathsf{TADP}}, v_2 \rangle\rangle \in \mathcal{R}$.

Let n be the smallest n such that there is s^{IM} and v such that $R(2 \cdot n) = \langle\langle \texttt{error}, s^{IM}\rangle, v\rangle$ and let s^{TADP} be such that $R(2 \cdot n - 2) = \langle\langle s^{\mathsf{TADP}}, s^{IM}\rangle, v\rangle$ (note that error transitions do not change the state of the input model TADP).

Using the previous observation we can indeed construct a prefix of a system execution E^{sys} of length n such that $\langle sE(n-1), s^{\mathsf{TADP}}\rangle \in \mathcal{R}$, which implies that E^{sys} is not safe.

Furthermore, because start and finish transitions of the TADP are urgent, and the action with the smallest deadline is chosen to execute at each point it can be shown that the constructed prefix satisfies the earliest-deadline-first conditions.

$2 \Rightarrow 1$ Again we prove the contrapositive $\neg 1 \Rightarrow \neg 2$.

Assume $s^{\text{prog}} \in \mathsf{sig}^{\text{prog}}\, IM$ such that for every earliest-deadline-first execution $E^{\text{sys}}_{\text{EDF}}$ of $\langle P, \mathsf{worst}\, R\rangle$ such that $\mathsf{in\,prog}\, E^{\text{sys}}_{\text{EDF}} = s^{\text{prog}}$, $E^{\text{sys}}_{\text{EDF}}$ is not safe.

We will show that for every $b > 0$ $\mathsf{TADP}\, \langle\langle P, R\rangle, b\rangle \mid\mid IM$ is not safe.

Let E^{sys} be such an earliest-deadline-first execution such that $\mathsf{in\,prog}\, E^{\text{sys}} = s^{\text{prog}}$, E^{sys} is actor-safe but E^{sys} is not safe. Note that we can always produce an actor-safe earliest-deadline-first execution. Furthermore we assume that at every time instant the transitions in E^{sys} follow the order input, finish, start, and then context-switch.

By assumption and the definition of safety, E^{sys} cannot be output-safe. We transform E^{sys} so that all output transitions that can be made in time are indeed made in time. There exist output transitions for which that is not possible, since otherwise there would exist a safe earliest-deadline-first execution and that goes against the assumption. Let $E^{\text{sys}}_{\text{EDF}}$ be the resulting execution.

We construct a correspondence between system execution transitions and TADP transitions, in a symmetrical way to the way we did it in the first part of the proof. Thus in the same way we can show how to construct a run R of $\mathsf{TADP}\, \langle\langle P, R\rangle, b\rangle$ for which there is n such that $R(n) = \texttt{error}$.

Let t_{miss} be the system time when the first deadline miss occurs in $E^{\text{sys}}_{\text{EDF}}$. We set b to be equal to t_{miss}. This guarantees that no clock bound transitions are necessary in R.

For any given choice of b we can transform R to a run of $\mathsf{TADP}\, \langle\langle P, R\rangle, b\rangle$ by splitting time transitions using clock bound transitions whenever an event clock grows beyond the specified bound at the old target state.

Let R^{TADP} be the resulting run.

Let R^{IM} be a run of IM such that

$$\{\langle c, t^{\text{prog}}\rangle \mid \text{there is } v \text{ such that } \langle c, t^{\text{prog}}, v\rangle \in s^{\text{prog}}\} = \{\langle R^{IM}(2\cdot n+1), (\mathsf{lapse}\, R^{IM})(0,n)\rangle \mid n \in \omega \text{ and } R^{IM}(2\cdot n+1) \in C\}.$$

R^{IM} exists because $s^{\text{prog}} \in \mathsf{sig}^{\text{prog}}\, IM$.

Given R^{TADP} and R^{IM} we construct a run R of $\mathsf{TADP}\,\langle\langle P, R\rangle, b\rangle \mid\mid IM$ by interleaving the two runs appropriately.

□

Theorem 7.10, along with Theorem 6.4 and 6.6, establishes the decidability of the schedulability problem for our systems.

8 Related work

The programming model described in the paper has been implemented in a framework called Ptides [7]. Ptides also employs clock synchronization algorithms and network delay bounds in order to uniformly support the same discrete-event semantics across distributed embedded platforms.

Synchronous languages (see [3]) have also been used for programming real-time systems. However, their approach is different than the one presented here, in that latencies arise from the implementation instead of being part of the programming abstraction.

Our programming model belongs in the family of logically execution time based models which was pioneered by Giotto [10]. A significant difference between Giotto and our case is the fact that the former is time-triggered. That distinction is moderated with xGiotto [9], which is an event-triggered extension of Giotto that, however, does not allow for the specification of relative deadlines on events.

Furthermore, timed automata have been used before for testing schedulability of real-time systems. [8] presents a real-time system model, called task automata, where asynchronous processes are bound to timed automata locations, thereby allowing for considerable expressiveness in the task arrival and dependency patterns. Our work is inspired by the work on task automata. Schedulability there is checked algorithmically via reduction to a decidable subclass of suspension automata. In contrast, because of our encoding of preemption times in the discrete state, we can use regular timed automata.

Lastly, on the topic of schedulability of real-time systems, recent advances in pseudo-polynomial schedulability algorithms, culminating in the digraph model [11], are pushing the boundary of the expressiveness of such techniques with the ability to model different job types, conditional execution, and looping structures. However, all these models rely on the task independence assumption (see [1]) in order to offer tractability. Specifically, they cannot accurately model systems where the execution of different tasks depend on each other, which is the case in our programming model.

References

[1] Sanjoy Baruah, Deji Chen, Sergey Gorinsky, and Aloysius Mok. Generalized multiframe tasks. *Real-Time Systems*, 17:5–22, 1999. 10.1023/A:1008030427220.

[2] Sanjoy K. Baruah, Aloysius K. Mok, and Louis E. Rosier. Preemptively scheduling hard-real-time sporadic tasks on one processor. In *RTSS 11th*, December 1990.

[3] A. Benveniste and G. Berry. The synchronous approach to reactive and real-time systems. *Proceedings of the IEEE*, 79(9):1270–1282, 1991.

[4] Sébastien Bornot, Gregor Gössler, and Joseph Sifakis. On the construction of live timed systems. In Susanne Graf and Michael Schwartzbach, editors, *TACAS*, volume 1785 of *Lecture Notes in Computer Science*, pages 109–126. Springer Berlin / Heidelberg, 2000.

[5] Sébastien Bornot, Joseph Sifakis, and Stavros Tripakis. Modeling urgency in timed systems. In Willem-Paul de Roever, Hans Langmaack, and Amir Pnueli, editors, *Compositionality: The Significant Difference*, volume 1536 of *Lecture Notes in Computer Science*, pages 103–129. Springer Berlin / Heidelberg, 1998.

[6] C.G. Cassandras and S. Lafortune. *Introduction to discrete event systems*, volume 11. Kluwer academic publishers, 1999.

[7] John Eidson, Edward A. Lee, Slobodan Matic, Sanjit A. Seshia, and Jia Zou. Distributed real-time software for cyber-physical systems. *Proceedings of the IEEE (special issue on CPS)*, 100(1):45 – 59, January 2012.

[8] Elena Fersman, Pavel Krcal, Paul Pettersson, and Wang Yi. Task automata: Schedulability, decidability and undecidability. *Information and Computation*, 205(8):1149 – 1172, 2007.

[9] Arkadeb Ghosal, Thomas A Henzinger, Christoph M Kirsch, and Marco A A Sanvido. Event-driven programming with logical execution times. In *HSCC*. Springer, 2004.

[10] Thomas A. Henzinger, Benjamin Horowitz, and Christoph Meyer Kirsch. Giotto: A time-triggered language for embedded programming. In *EMSOFT'01*. Springer-Verlag, 2001.

[11] M Stigge, P Ekberg, Nan Guan, and Wang Yi. The Digraph Real-Time Task Model. In *RTAS*, 2011.