



HAL
open science

Symbolic Path-guided Test Cases for Models with Data and Time

Boutheina Bannour, Arnault Lapitre, Pascale Le Gall, Thang Nguyen

► **To cite this version:**

Boutheina Bannour, Arnault Lapitre, Pascale Le Gall, Thang Nguyen. Symbolic Path-guided Test Cases for Models with Data and Time. Formal Aspects of Component Software (FACS), Oct 2023, Paris (en ligne), France. hal-04486318

HAL Id: hal-04486318

<https://hal.science/hal-04486318>

Submitted on 1 Mar 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Symbolic Path-guided Test Cases for Models with Data and Time

Boutheina Bannour¹, Arnault Lapitre¹, Pascale Le Gall², and
Thang Nguyen²

¹ Université Paris-Saclay, CEA, List, F-91120, Palaiseau, France

² Université Paris-Saclay, CentraleSupélec, MICS, F-91192, Gif-sur-Yvette, France

Abstract. This paper focuses on generating test cases from timed symbolic transition systems. At the heart of the generation process are symbolic execution techniques on data and time. Test cases look like finite symbolic trees with verdicts on their leaves and are based on a user-specified finite symbolic path playing the role of a test purpose. Generated test cases handle data involved in time constraints and uninitialized parameters, leveraging the advantages of symbolic execution techniques.

Keywords: model-based testing · timed input/output symbolic transition systems · symbolic execution · tioco conformance relation · test purpose · test case generation · uninitialized parameters

1 Introduction

Context. Symbolic execution [19,14,12,6] explores programs or models' behaviors using formal parameters instead of concrete values and computes a logical constraint on them, the so-called path condition. Interpretations of these parameters satisfying the constraint yield inputs that trigger executions along the desired path. Symbolic execution's primary application is test case generation, where considering test cases guided by different symbolic paths facilitates achieving high coverage across diverse behaviors. Symbolic execution has been defined first for programs [19] and extended later to models [14,12,3,26,4,7] in particular to symbolic transition systems where formal parameters abstract values of uninitialized data variables [14,4], values of received data from the system's environment [14,12,26,3,4,7,1], and durations stored in clock variables [26,4].

Contribution. In this paper, we investigate test case generation from models given as symbolic transition systems that incorporate both data and time. Time is modeled with explicit clock variables, which are treated as a particular case of data variables that occur in guards and constrain the transitions' firing. Our approach allows for general logical reasoning that mixes data and time through symbolic execution, typically compared to Timed Automata [2], which are models dedicated to time and use tailored zone-based abstraction techniques to handle time. Test cases are built based on a test purpose, defined as a selected symbolic path of the model. We require that test purposes

are deterministic in that any system behavior given as a trace cannot be executed both on the test purpose and on another symbolic path. By leveraging this determinism property and symbolic execution techniques, we define test cases as tree-like structures [18,23], presenting the following advantages: (i) data and time benefit from comparable property languages, seamlessly handled with the same symbolic execution techniques; (ii) input communication channels are partitioned into controllable input channels enabling the test case to stimulate the system under test, and uncontrollable input channels enabling observation of data from third parties; (iii) state variables do not need to be initialized, and finally (iv), test cases can be easily executed on systems under test, typically achieved through behavioral composition techniques, such as employing TTCN-3 [25], or by maintaining a test case state at runtime using on-the-fly test case execution [11,14,7]. In either case, our test cases are to be coupled with constraint solving to assess the satisfiability of test cases' progress or verdict conditions. We provide a soundness result of our test case execution on the system under test in the framework of the timed conformance relation tioco [20] issued from the well-established relation ioco [27]. Finally, we implement our test case generation in the symbolic execution platform Diversity [8].

Paper plan. We devote Sec.2 to present timed symbolic transition systems mixing data and time, and in Sec.3, we define their symbolic execution serving as the foundation for our test case generation. In Sec.4, we give the main elements of the testing framework: the conformance relation tioco and test purposes. In Sec.5, we detail the construction of symbolic path-guided test cases. In Sec.6, we provide some links to related work. In Sec.7, we provide concluding words.

2 Timed Input/Output Symbolic Transition Systems

Preliminaries on data types. For two sets A and B , we denote B^A , the set of applications from A to B . We denote $\coprod_{i \in \{1, \dots, n\}} A_i$ the disjoint union of sets A_1, \dots , and A_n . For a set A , A^* (resp. A^+) denotes the set of all (resp. non-empty) finite sequences of elements of A , with ε being the empty sequence. For any two sequences $w, w' \in A^*$, we denote $w.w' \in A^*$ their concatenation.

A data signature is a pair $\Omega = (S, Op)$ where S is a set of type names and Op is a set of operation names provided with a profile in S^+ . We denote $V = \coprod_{s \in S} V_s$ the set of typed variables in S with $\text{type} : V \rightarrow S$ the function that associates variables with their type. The set $\mathcal{T}_\Omega(V) = \coprod_{s \in S} \mathcal{T}_\Omega(V)_s$ of Ω -terms in V is inductively defined over V and operations Op of Ω as usual and the function type is extended to $\mathcal{T}_\Omega(V)$ as usual. The set $\mathcal{F}_\Omega(V)$ of typed equational Ω -formulas over V is inductively defined over the classical equality and inequality predicates $t \bowtie t'$ with $\bowtie \in \{<, \leq, =, \geq, >\}$ for any $t, t' \in \mathcal{T}_\Omega(V)_s$ and over usual Boolean constants and connectives $True, False, \neg, \vee, \wedge$ and quantifiers $\forall x, \exists x$ with x a variable of V . We may use the syntax $\exists\{x_1, \dots, x_n\}$ for the expression $\exists x_1 \dots \exists x_n$. A substitution over V is a type-preserving application $\rho : V \rightarrow \mathcal{T}_\Omega(V)$. The identity substitution over V is denoted id_V and substitutions are canonically extended on terms and formulas.

An Ω -model $M = (\coprod_{s \in S} M_s, (f_M)_{f \in Op})$ provides a set of values M_s for each type s in S and a concrete operation $f_M : M_{s_1} \times \cdots \times M_{s_n} \rightarrow M_s$ for each operation name $f : s_1 \dots s_n \rightarrow s$ in Op . An interpretation $\nu : V \rightarrow M$ associates a value in M with each variable $v \in V$, and is canonically extended to $\mathcal{T}_\Omega(V)$ and $\mathcal{F}_\Omega(V)$ as usual. For ν an interpretation in M^V , x a variable in V and v a value in M , $\nu[x \mapsto v]$ is the interpretation $\nu' \in M^V$ which sends x on the value v and coincides with ν for all other variables in V . For $\nu \in M^V$ and $\varphi \in \mathcal{F}_\Omega(V)$, the satisfaction of φ by ν is denoted $M \models_\nu \varphi$ and is inductively defined w.r.t. the structure of φ as usual. We say a formula $\varphi \in \mathcal{F}_\Omega(V)$ is satisfiable, denoted $Sat(\varphi)$, if there exists $\nu \in M^V$ such that $M \models_\nu \varphi$.

In the sequel, we consider a data signature $\Omega = (S, Op)$ with $time \in S$ to represent durations and Op containing the usual operations $< : time.time \rightarrow Bool$ and $+ : time.time \rightarrow time, \dots$. An Ω -model M being given, M_{time} is denoted D and is isomorphic to the set of non-negative real numbers. $< : time.time \rightarrow Bool$ and $+ : time.time \rightarrow time$ are mapped to their usual meanings.

Timed Input/Output Symbolic Transition Systems (TIOSTS) are automata handling data and time, and defined over a *signature* $\Sigma = (A, K, C)$, where:

- $A = \coprod_{s \in S} A_s$ and K are pairwise disjoint sets of variables representing respectively *data variables* and *clock variables* of type *time*
- and $C = \coprod_{s \in S} C_s$ is a set of *communication channels* with the convention $type(c) = s$ for any $c \in C_s$. Moreover, channels of type $s \in S$ are partitioned into input and output channels, i.e., $C_s = C_s^{in} \amalg C_s^{out}$.

We denote $C^{in} = \coprod_{s \in S} C_s^{in}$, resp. $C^{out} = \coprod_{s \in S} C_s^{out}$, the set of all input, resp. output, channels, regardless of their type.

Interactions of TIOSTS with the environment are expressed in terms of communication actions. The *set of communication actions* over Σ is $Act(\Sigma) = I(\Sigma) \cup O(\Sigma)$ where:

- $I(\Sigma) = \{c?x \mid c \in C^{in}, x \in A_{type(c)}\}$ is the set of input actions, and
- $O(\Sigma) = \{c!t \mid c \in C^{out}, t \in \mathcal{T}_\Omega(A \cup K)_{type(c)}\}$ is the set of output actions.

$c?x$ denotes the reception of a value to be stored in x through channel c . $c!t$ denotes the emission of the value corresponding to the current interpretation of term t through channel c . The *set of concrete communication actions* over C is $Act(C) = I(C) \cup O(C)$ where:

$$I(C) = \{c?v \mid c \in C^{in}, v \in M_{type(c)}\} \text{ and } O(C) = \{c!v \mid c \in C^{out}, v \in M_{type(c)}\}$$

Notations. For $a \in Act(\Sigma)$ (resp. $a \in Act(C)$) of the form $c?y$ or $c!y$, $chan(a)$ and $val(a)$ denote c and y respectively. For expressiveness concerns, we also use extensions of those actions: either carrying n pieces of data, i.e. $c!(t_1, \dots, t_n)$ or $c?(x_1, \dots, x_n)$, and simple signals $c!$ or $c?$ which are actions carrying no-data.

Definition 1 (TIOSTS). A *TIOSTS* over $\Sigma = (A, K, C)$ is a triple $\mathbb{G} = (Q, q_0, Tr)$, where

- Q is the set of states,
- $q_0 \in Q$ is the initial state,

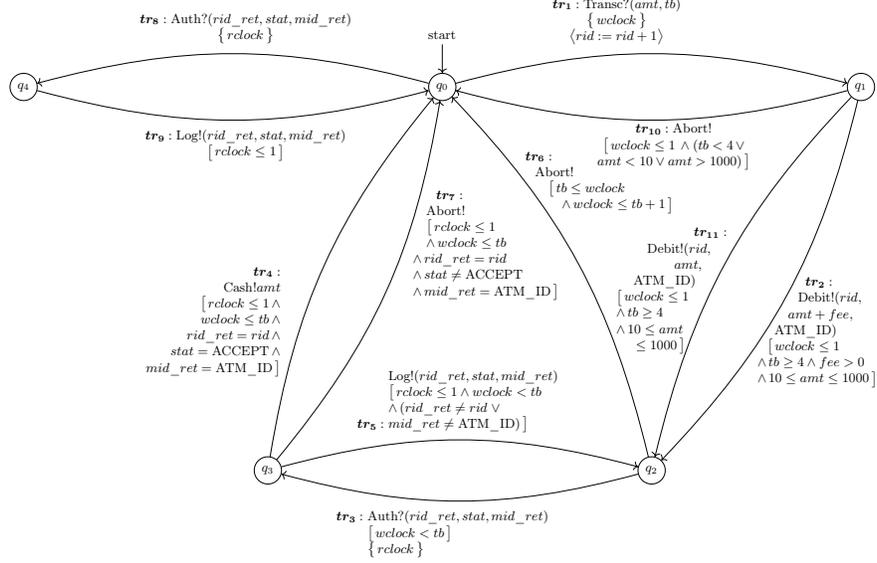


Fig. 1: Example TIOSTS of an ATM

- Tr is the set of transitions of the form $(q, act, \phi, \mathbb{K}, \rho, q')$ with $q, q' \in Q$, $act \in Act(\Sigma)$, $\phi \in \mathcal{F}_\Omega(A \cup K)$, $\mathbb{K} \subseteq K$ and $\rho : A \rightarrow \mathcal{T}_\Omega(A \cup K)$ is a type-preserving function.

In the sequel, given a transition tr of the form $(q, act, \phi, \mathbb{K}, \rho, q')$, we will access its components by their name, for example, $act(tr)$ for its communication action. We comment on the ingredients of a TIOSTS through the TIOSTS given in Ex. 1.

Example 1. The TIOSTS $\mathbb{G} = (Q, q_0, Tr)$ in Fig. 1 represents a simple Automatic Teller Machine (ATM) with $Q = \{q_0, \dots, q_4\}$ and $Tr = \{tr_1, \dots, tr_{11}\}$. Its signature introduces two clocks ($wclock$, $rclock$), 7 data variables (rid , amt , tb , fee , rid_ret , $stat$, mid_ret) and 6 channels including 2 input channels (Transc, Auth) and 4 output channels (Debit, Abort, Cash and Log).

Transition $tr_1 : q_0 \xrightarrow{\text{Transc?}(amt, tb), [True], \{wclock\}, (rid := rid + 1)} q_1$ represents a reception on channel Transc of a client withdrawal request for a given amount stored in variable amt and the corresponding bound on processing time stored in variable tb , which can vary due to bank security checks. tr_1 is unconditionally fired (due to the guard $True$), resets clocks in $\mathbb{K} = \{wclock\}$ and updates variable rid with $rid + 1$. tr_1 abstracts client interaction and bank processing time retrieval.

Transition $tr_2 : q_1 \xrightarrow{\text{Debit!}(rid, amt + fee, ATM_ID), [wclock \leq 1 \wedge tb \geq 4 \wedge fee > 0 \wedge 10 \leq amt \leq 1000], \{\}, \{\}} q_2$ represents an emission of (bank) debit request on channel Debit of the value of rid , the value of the term $amt + fee$, and the value of the constant ATM_ID . tr_2 can be fired if and only if the duration since $wclock$ reset is less than or equal 1, the processing time bound is greater than or equal 4, the ATM fee is strictly positive, and the withdrawal amount in some range (between 10 and 1000).

Other transitions represent debit authorization reception (tr_3), cash return (tr_4), logging non-involved debit authorization (tr_5 and tr_9), cancellation upon

timeout (tr_6) or debit refusal (tr_7), cancellation due to amount out of range or inappropriate processing time bound (tr_{10}), reception of non-involved debit authorization (tr_8), and feeless debit request (tr_{11}).

3 Symbolic execution of TIOSTS

We use symbolic execution techniques for defining the semantics of TIOSTS: transitions are executed not for concrete values but rather using fresh variables and computing constraints on them. Given an TIOSTS $\mathbb{G} = (Q, q_0, Tr)$ over $\Sigma = (A, K, C)$, we consider a set F of fresh variables disjoint from TIOSTS variables, i.e. $F \cap (A \cup K) = \emptyset$, and partitioned with the following subsets:

- F^{ini} a set of variables dedicated to initialize variables of \mathbb{G} ;
- $F^{in} = (F_c^{in})_{c \in C^{in}}$ verifying that variables in F_c^{in} are of type $type(c)$;
- $F^{out} = (F_c^{out})_{c \in C^{out}}$ verifying that variables in F_c^{out} are of type $type(c)$;
- F^{dur} a set of variables of type *time*.

For the signature $\Sigma_F = (F, \emptyset, C)$, the set $Evt(\Sigma_F)$ of *symbolic events* over Σ_F is $F_{time} \times (Act(\Sigma_F) \cup \{_ \})$ with $_$ for indicating the absence of an action. For $ev = (z, act)$ in $Evt(\Sigma_F)$, $delay(ev)$ and $act(ev)$ denote resp. z and act . Intuitively, z is the duration elapsed between the action preceding act and act .

An Execution Context (EC) ec is a data structure of the form $(q, \pi, \lambda, ev, pec)$ composed of pieces of information about symbolic execution:

- $q \in Q$, a state (control point) of the TIOSTS reached so far,
- $\pi \in \mathcal{F}_\Omega(F)$, a constraint on variables in F , the so-called *path condition*, to be satisfiable by the symbolic execution to reach ec ,
- $\lambda : A \cup K \rightarrow \mathcal{T}_\Omega(F)$, a substitution,
- $ev \in Evt(\Sigma_F)$, a symbolic event that has been executed to reach ec ,
- pec a predecessor of ec useful to build a symbolic tree in which nodes are ECs and edges connect predecessor ECs to ECs themselves.

For any execution context ec , we note $q(ec), \pi(ec), \lambda(ec), ev(ec)$ and $pec(ec)$ to denote the corresponding elements in ec . In the same line, we also note $act(ec), delay(ec)$ and $chan(ec)$ for resp. $act(ev(ec)), delay(ev(ec))$ and $chan(act(ev(ec)))$. For convenience, $Sat(\pi(ec))$ will be denoted $Sat(ec)$.

Initial ECs are of the form $ec_0 = (q_0, True, \lambda_0, _, self)$ with: λ_0 associating to every variable of A a distinct fresh variable of F^{ini} , and to variables of K the constant 0; " $_$ " an identifier indicating the absence of an action to start the system; and $self$ an identifier indicating that, the predecessor of an initial EC is the initial context itself. $\mathbb{EC}(\mathbb{G})$ denotes the set of all ECs of a TIOSTS \mathbb{G} .

For a non-initial execution context ec , we use the notation $pec(ec) \xrightarrow{ev(ec)} ec$ or $pec(ec) \xrightarrow{ev(ec)} ec \in \mathbb{EC}$ if ec and its predecessor are both in a subset \mathbb{EC} of $\mathbb{EC}(\mathbb{G})$.

Transitions are executed symbolically from an EC. An example execution on the TIOSTS of Fig. 1 is provided before presenting the general definition.

Example 2. In Fig.2, the symbolic execution of transition tr_2 (Ex.1) is depicted from the execution context ec_1 , where variables fee , rid , rid_ret , $stat$, and mid_ret are evaluated with fresh initial parameters. This execution creates a successor context ec_2 , where the clock $wclock$ is associated with a new duration \mathbf{z}_1 in F^{dur} , representing the time passed since the preceding event. The emission event $(\mathbf{z}_1, \text{Debit}!(\mathbf{y}_{D_1}^1, \mathbf{y}_{D_2}^1, \mathbf{y}_{D_3}^1))$ with $\mathbf{y}_{D_1}^1, \mathbf{y}_{D_2}^1, \mathbf{y}_{D_3}^1$ variables resp. in $F_{\text{Debit},1}^{out}, F_{\text{Debit},2}^{out}, F_{\text{Debit},3}^{out}$ corresponds to the symbolic evaluation of the action $act(tr_2) = \text{Debit}!(rid, amt + fee, \text{ATM_ID})$.

The evaluation of the transition guard $\phi(tr_2) = wclock \leq 1 \wedge tb \geq 4 \wedge fee > 0 \wedge 10 \leq amt \leq 1000$ yields formula $\mathbf{z}_1 \leq 1 \wedge \mathbf{tb}_1 \geq 4 \wedge \mathbf{fee}_0 > 0 \wedge 10 \leq \mathbf{amt}_1 \leq 1000$ which together with identification conditions $\mathbf{y}_{D_1}^1 = \mathbf{rid}_0 + 1, \mathbf{y}_{D_2}^1 = \mathbf{amt}_1 + \mathbf{fee}_0, \mathbf{y}_{D_3}^1 = \text{ATM_ID}$ constitutes the path condition of ec_2 . Identification conditions result from the transition action evaluation.

Def. 2 will make precise the EC successors' computation from TIOSTS transitions. While in Ex. 2, we have illustrated the symbolic execution of a unique transition (tr_2), we will define symbolic execution by simultaneously executing all the outgoing transitions from a given EC. In this way, we can introduce the same symbolic variables for all outgoing transitions as far as they have the same role. Generically, given an execution context ec in $\mathbb{EC}(\mathbb{G})$, we will access the symbolic variables introduced by the executions from ec with the following notations: $f_c^{in}(ec)$ for $c \in C^{in}$, $f_c^{out}(ec)$ for $c \in C^{out}$, and $f^{dur}(ec)$. For convenience, all such fresh variables are available by default with every execution context ec , even if there is no outgoing transition from $q(ec)$ carrying on a given channel c . For $\alpha \in \{in, out\}$, $f^\alpha(ec) = \{f_c^\alpha(ec) \mid c \in C^\alpha\}$. In Def 2, to make it easier to read, $f_c^{in}(ec)$, $f_c^{out}(ec)$ and $f^{dur}(ec)$ are respectively denoted as x_c , y_c and z .

Definition 2 (Symbolic Execution of a TIOSTS). Let $\mathbb{G} = (Q, q_0, Tr)$ be a TIOSTS, $ec = (q, \pi, \lambda, ev, pec)$ be an execution context in $\mathbb{EC}(\mathbb{G})$, and x_c be a fresh variable in F_c^{in} for any $c \in C^{in}$, y_c be a fresh variable in F_c^{out} for any $c \in C^{out}$ and let z be a fresh variable in F^{dur} .

The successors of ec are all execution contexts of the form $(q', \pi', \lambda', ev', ec)$ verifying that there exists a transition $tr = (q, act, \phi, \mathbb{K}, \rho, q')$ in Tr and constituents λ', ev' and π' of ec' are defined as follows:

– the substitution $\lambda' : A \cup K \rightarrow \mathcal{T}_\Omega(F)$:

$$\lambda'(w) = \begin{cases} \lambda'_0(\rho(w)) & \text{if } w \in A \\ 0 & \text{if } w \in \mathbb{K} \\ \lambda'_0(w) & \text{else i.e. if } w \in K \setminus \mathbb{K} \end{cases} \quad (1)$$

$q(ec_1) : q_1$ $\pi(ec_1) : True$ $\lambda(ec_1) : rid \mapsto \mathbf{rid}_0 + 1, amt \mapsto \mathbf{amt}_1,$ $fee \mapsto \mathbf{fee}_0, rid_ret \mapsto \mathbf{rid_reto},$ $stat \mapsto \mathbf{stato},$ $mid_ret \mapsto \mathbf{mid_reto},$ $tb \mapsto \mathbf{tb}_1, wclock \mapsto 0, rclock \mapsto \mathbf{z}_0$ $ev(ec_1) : (\mathbf{z}_0, \text{Transc}?(amt_1, tb_1))$ $pec(ec_1) : ec_0$
$(\mathbf{z}_1, \text{Debit}!(\mathbf{y}_{D_1}^1, \mathbf{y}_{D_2}^1, \mathbf{y}_{D_3}^1))$ $ec_1 \xrightarrow{\quad} ec_2$
$q(ec_2) : q_2$ $\pi(ec_2) : (\mathbf{z}_1 \leq 1) \wedge (\mathbf{tb}_1 \geq 4)$ $\wedge (\mathbf{fee}_0 > 0)$ $\wedge (10 \leq \mathbf{amt}_1 \leq 1000)$ $\wedge (\mathbf{y}_{D_1}^1 = \mathbf{rid}_0 + 1)$ $\wedge (\mathbf{y}_{D_2}^1 = \mathbf{amt}_1 + \mathbf{fee}_0)$ $\wedge (\mathbf{y}_{D_3}^1 = \text{ATM_ID})$ $\lambda(ec_2) : rid \mapsto \mathbf{rid}_0 + 1, amt \mapsto \mathbf{amt}_1,$ $fee \mapsto \mathbf{fee}_0, rid_ret \mapsto \mathbf{rid_reto},$ $stat \mapsto \mathbf{stato}, tb \mapsto \mathbf{tb}_1,$ $mid_ret \mapsto \mathbf{mid_reto},$ $wclock \mapsto \mathbf{z}_1, rclock \mapsto \mathbf{z}_0 + \mathbf{z}_1$ $ev(ec_2) : (\mathbf{z}_1, \text{Debit}!(\mathbf{y}_{D_1}^1, \mathbf{y}_{D_2}^1, \mathbf{y}_{D_3}^1))$ $pec(ec_2) : ec_1$

Fig. 2: Symbolic execution of a TIOSTS transition

where $\lambda'_0 : A \cup K \rightarrow \mathcal{T}_\Omega(F)$ is the auxiliary function defined as:

$$\lambda'_0(w) = \begin{cases} x_c & \text{if } act = c?w \\ \lambda(w) + z & \text{if } w \in K \\ \lambda(w) & \text{else} \end{cases} \quad (2)$$

- ev' is $(z, c?x_c)$ if $act = c?w$ and is $(z, c!y_c)$ if $act = c!t$ for a given channel c
- π' is the formula $\pi \wedge \lambda'_0(\phi)$ if $act = c?w$ and is $\pi \wedge \lambda'_0(\phi) \wedge (y_c = \lambda'_0(t))$ if $act = c!t$ for a given channel c .

The symbolic execution $SE(\mathbb{G})$ of \mathbb{G} is a couple (ec_0, \mathbb{EC}) where: ec_0 is an arbitrary initial EC, and \mathbb{EC} is the smallest set of execution contexts containing ec_0 and all successors of its elements.

The computation of the successors of an execution context translates the standard execution of a transition from that context: λ'_0 is an intermediate substitution that advances all clocks by the same fresh duration z to indicate time passing, assigns to a data variable w a fresh variable x_c if w is the variable of a reception ($c?w$) and leaves the other data variables unchanged. Then, λ' is defined, for the data variables, by applying λ'_0 on the terms defined by the substitution ρ introduced by tr and, for the clock variables, by resetting the variables of \mathbb{K} to zero and advancing the other clocks using λ'_0 . The event action is either $c?x_c$ (case of a reception $c?w$) or $c!y_c$ (case of an emission $c!t$). The path condition π' is obtained by the accumulation of the condition π of the predecessor context ec and of the guard ϕ of the transition evaluated using λ'_0 . Moreover, in case of an emission, π' keeps track of the identification condition matching y_c with the evaluation $\lambda'_0(t)$ of the emitted term t .

In the sequel, we will denote $tr(ec)$ the transition that allows building the execution context ec . By convention, $tr(ec)$ is undefined for initial contexts.

Example 3. Fig. 3 illustrates parts of the symbolic execution of the ATM example TIOSTS given in Fig. 1.

So far, we have defined the symbolic execution of a TIOSTS without any adjustments related to our testing concerns from TIOSTS. In the following, we will complete the symbolic execution with quiescent configurations, i.e., identifying situations where the system can remain silent. The system is usually expected to react by sending messages when it receives a message from its environment. However, sometimes, it cannot emit an output from any given state [27,24,14,4,17]. In such a case, the inability of the system to react becomes a piece of information. To make this fact clear we enrich symbolic execution by adding a special output action $\delta!$ to denote the absence of output in those specific deadlock situations.

Definition 3 (Quiescence enrichment). *The quiescence enrichment $SE(\mathbb{G})^\delta$ of $SE(\mathbb{G}) = (ec_0, \mathbb{EC})$ is $(ec_0, \mathbb{EC}^\delta)$ where \mathbb{EC}^δ is the set \mathbb{EC} enriched by new execution contexts ec^δ . For each context $ec = (q, \pi, \lambda, ev, pec)$ in \mathbb{EC} , a new context $ec^\delta = (q, \pi \wedge \pi^\delta, \lambda, (f^{dur}(ec), \delta!), ec)$ is considered where³:*

³ with the convention that \bigwedge quantified over empty conditions is the formula *True*

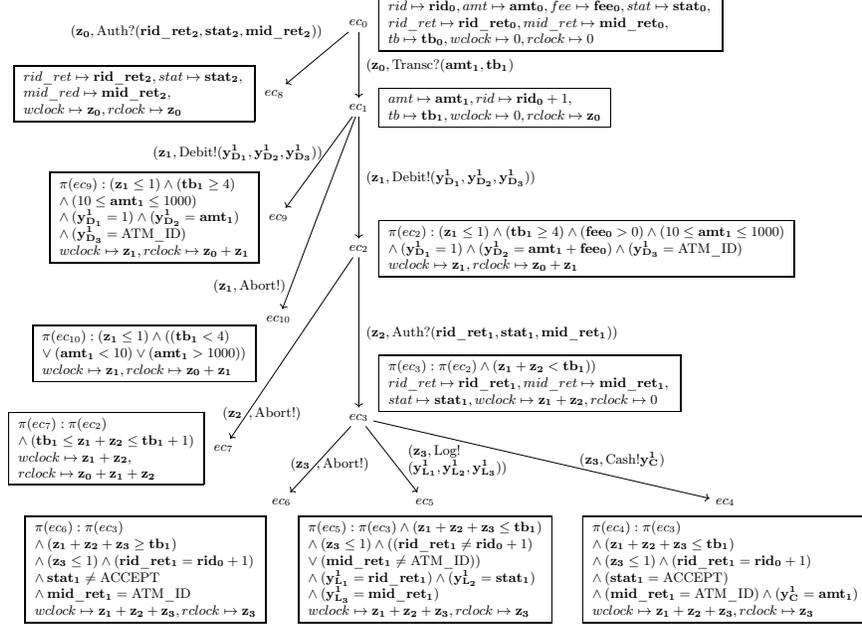


Fig. 3: Symbolic execution of the ATM TIOSTS of Fig. 1

$$\pi^\delta = \bigwedge_{\substack{pec(ec')=ec \\ chan(ec') \in C^{out}}} (\forall f^{dur}(ec). \forall f_{chan}^{out}(ec'). \neg \pi(ec'))$$

Let us emphasize that π^δ is satisfiable only for contexts ec where there is no choice of values for the variables for triggering from ec a transition carrying an emission. The context could not be considered quiescent if such a choice were possible, i.e. if there would exist an output transition towards an execution context ec' , for which there is an instantiation of variables $f^{dur}(ec)$ and $f_{chan}^{out}(ec')$ making the condition $\pi(ec')$ true.

Example 4. We discuss some examples from Fig. 3. The execution context ec_0 does not have successors with outputs (π^δ is *True*) which denotes that the ATM is awaiting withdrawal requests or non-involved debit authorizations. This quiescent situation is captured by adding the context $ec_0^\delta = (q_1, \text{True}, \lambda(ec_0), (z_1, \delta!), ec_0)$. The execution context ec_1 has three successors with outputs, ec_2 , ec_9 and ec_{10} . Then, π^δ is:

$$\bigwedge_{j \in \{2, 9, 10\}} \forall f^{dur}(ec_1). \forall f_{chan}^{out}(ec_j)(ec_1). \neg \pi(ec_j)$$

which is not satisfiable. Thus, there is no need to add a quiescent transition from ec_1 . The same applies to ec_2 and ec_3 .

A symbolic path of $SE(\mathbb{G})^\delta = (ec_0, \mathbb{E}C^\delta)$ is a sequence $p = ec_0.ec_1 \dots ec_n$ where ec_0 is the initial context, for $i \in [1, n]$, $ec_i \in \mathbb{E}C^\delta$, and $pec(ec_i) = ec_{i-1}$. $Paths(SE(\mathbb{G})^\delta)$ denotes the set of all such paths. We will use the notation $tgt(p)$

to refer to ec_n , the last context of p . We define the set of traces of a symbolic path p in $Paths(SE(\mathbb{G})^\delta)$ by:

$$Traces(p) = \bigcup_{\nu \in M^F} \{ \nu(p) \mid M \models_\nu \exists F^{ini}. \pi(tgt(p)) \}$$

where ν applies to a path p of the form $p'.ec$ as $\nu(p) = \nu(p').\nu(ev(ec))$ with the convention $\nu(ev(ec_0)) = \epsilon$ and $\nu(ev(ec)) = (\nu(z), c?\nu(x))$ (resp. $(\nu(z), c!\nu(y))$ or $(\nu(z), \delta!)$) if $ev(ec)$ is of the form $(z, c?x)$ (resp. $(z, c!y)$ or $(z, \delta!)$).

By solving the path condition of a given path, we can evaluate all symbolic events occurring in the path and extract the corresponding trace. The set of traces of \mathbb{G} is defined as :

$$Traces(\mathbb{G}) = \bigcup_{p \in Paths(SE(\mathbb{G})^\delta)} Traces(p)$$

4 Conformance testing

Conformance testing aims to check that a system under test behaves correctly w.r.t a reference model, a TIOSTS \mathbb{G} in our case. The test case stimulates the system with inputs and observes the system's outputs, their temporalities, and the quiescent situations to compare them to those specified by \mathbb{G} . For generality, we propose test cases that control some inputs of the system under test while leaving other inputs driven by systems in its environment. We assume that the test case selects inputs and observes outputs on some channels while it can only observe inputs and outputs on other channels of the system under test. Illustrating with the ATM, a test case provides the ATM with withdrawal requests, and observes withdrawal authorizations received from the bank.

We characterize a *Localized System Under Test (LUT)* (terminology from [13,5]) tested in a context where some inputs are not controllable. For this, we partition $C^{in} = CC^{in} \amalg UC^{in}$ where:

- CC^{in} is the set of controllable input channels and
- UC^{in} is the set of uncontrollable input channels.

For a set of channels C , we denote $Evt(C) = D \times Act(C)$ the set of all concrete events that can occur in a trace: an event (d, act) indicates that the occurrence of action act happens d units of time after the previous event. In model-based testing, a LUT is a black box and as such, is abstracted by a set of traces $LUT \subseteq Evt(C_\delta)^*$ with $C_\delta = C \cup \{\delta\}$ satisfying additional hypotheses, denoted as \mathcal{H} , ensuring its consistency. Hypotheses \mathcal{H} gather the following 3 properties, where for σ_1, σ_2 in $Evt(C)^*$, d in D and $ev \in Evt(C)$ we have:

- *stable by prefix*: $\sigma_1.\sigma_2 \in LUT \Rightarrow \sigma_1 \in LUT$
- *quiescence*: for any $d < delay(ev)$, $\sigma_1.ev \in LUT \Rightarrow \sigma_1.(d, \delta!) \in LUT$
- *input complete*: for any $d < delay(ev)$, $c \in CC^{in}$, $v \in M$,
 $\sigma_1.ev \in LUT \Rightarrow \sigma_1.(d, c?v) \in LUT$

The first hypothesis simply states that every prefix of a system trace is also a system trace. The hypothesis on quiescence states that if an event ev whose action is in $act(C)$ occurs in LUT , then LUT can remain quiescent for any

duration strictly less than the delay of the event. The hypothesis on input completeness enables LUT to receive any input on a controllable channel, i.e., an input received from the test case, during the delay of any ev in the LUT .

The semantics of a TIOSTS \mathbb{G} , denoted by $Sem(\mathbb{G})$, will include traces with the admissible temporary observation of quiescence: if an event $ev = (d, act)$ is specified in \mathbb{G} then quiescence can be observed for any duration $d' < d$. $Sem(\mathbb{G})$ is then defined as the smallest set containing $Traces(\mathbb{G})$ and such that for any $\sigma \in Evt(C)^*$, $ev \in Evt(C)$, for any $d < delay(ev)$:

$$\sigma.ev \in Traces(\mathbb{G}) \Rightarrow \sigma.(d, \delta!) \in Sem(\mathbb{G})$$

As other previous works [22,28] have already done to suit their needs, we are now slightly adapting the conformance relation of [20]:

Definition 4 (tioco). *Let C be a set of channels. Let \mathbb{G} and LUT be resp. a TIOSTS defined on C and a subset of $Evt(C_\delta)^*$ satisfying \mathcal{H} .*

LUT tioco \mathbb{G} iff for all $\sigma \in Sem(\mathbb{G})$, for any $ev \in Evt(C^{out} \cup \{\delta\})$, we have:

$$\sigma.ev \in LUT \Rightarrow \sigma.ev \in Sem(\mathbb{G})$$

The relation *tioco* states that LUT is in conformance with \mathbb{G} , if and only if after a specified sequence σ observed on LUT , any event produced by LUT as an output or a delay of quiescence, leads to a sequence $\sigma.ev$ of $sem(\mathbb{G})$.

Test case generation is often based on the selection of a test purpose which permits to choose a particular behavior in \mathbb{G} to be tested [14,16,4,7]. As symbolic execution plays a key role both for the semantics of TIOSTS and for testing issues in general, whether it is for the test case generation or the verdict computation, our test purposes will be paths $tp \in Paths(SE(\mathbb{G})_\delta)$ with satisfiable path conditions, i.e. verifying $Sat(tgt(tp))$. As outputs are involved in the *tioco* relation, we require tp to end with an output event, i.e., $chan(tgt(tp)) \in C^{out}$.

Contrary to [14], our test purposes are simple paths and not (finite) subtrees, simplifying the construction of test cases. We will not need to consider the case where the observed behavior on LUT corresponds to several symbolic paths simultaneously. By taking it a step further, to avoid such tricky situations completely, we restrict ourselves to symbolic paths that do not induce non-determinism. In line with [3,18], we forbid there are two outgoing transitions of an execution context concerning the same channel which can be covered by the same trace. Unlike [3,18] which impose determinism conditions at the state level, we deal with uninitialized variables at the path level:

Definition 5 (Test purpose). *Let $tp \in Paths(SE(\mathbb{G})_\delta)$ be a symbolic path verifying $Sat(tgt(tp))$ and $chan(tgt(tp)) \in C^{out}$. Let $\mathbb{EC}(tp)$ be its set of execution contexts.*

tp is a test purpose for \mathbb{G} if tp satisfies the so-called trace-determinism property: for ec in $\mathbb{EC}(tp)$ and ec' in $\mathbb{EC}(\mathbb{G})$ s.t. $Sat(ec')$, $pec(ec) = pec(ec')$, $tr(ec) \neq tr(ec')$, and $chan(ec) = chan(ec')$, the following formula is unsatisfiable:

$$(\exists F^{ini}.\pi(ec)) \bigwedge (\exists F^{ini}.\pi(ec'))$$

The trace-determinism property simply expresses that from any intermediate execution context of tp , it is impossible to deviate in \mathbb{G} with a common trace, independently of the initial conditions.

Example 5. The test purpose $tp = ec_0.ec_1 \dots ec_4$ given in Fig. 3 satisfies trace-determinism. To support our comments, let us consider a simpler TIOSTS with three transitions (tr_1 , tr_2 and tr_3), with two of them, tr_2 and tr_3 , creating a non-deterministic situation:

$$tr_1 : q_0 \xrightarrow{\text{Transc?amt}} q_1, tr_2 : q_1 \xrightarrow{\text{Debit!amt}} q_2 \text{ and } tr_3 : q_1 \xrightarrow{[\text{fee} > 0], \text{Debit!amt+fee}} q_3$$

The TIOSTS symbolic execution for some initial execution context ec_0 ($F^{ini} = \{\mathbf{amt}_0, \mathbf{fee}_0\}$) can reach execution contexts ec_1 ($tr(ec_1) = tr_1$, $pec(ec_1) = ec_0$), ec_2 ($tr(ec_2) = tr_2$, $pec(ec_2) = ec_1$), and ec_3 ($tr(ec_3) = tr_3$, $pec(ec_3) = ec_1$), building 2 symbolic paths $ec_0.ec_1.ec_2$ and $ec_0.ec_1.ec_3$. Respective path conditions are $\pi(ec_2) = (\mathbf{y}_D^1 = \mathbf{amt}_1)$ and $\pi(ec_3) = (\mathbf{fee}_0 > 0) \wedge (\mathbf{y}_D^1 = \mathbf{amt}_1 + \mathbf{fee}_0)$ where \mathbf{amt}_1 binds the value received on the channel Transc ($f_{\text{Transc}}^{in}(ec_0) = \mathbf{amt}_1$) and \mathbf{y}_D^1 binds the value emitted on the channel Debit ($f_{\text{Debit}}^{out}(ec_1) = \mathbf{y}_D^1$).

Given $tp = ec_0.ec_1.ec_2$, execution contexts ec_2 and ec_3 share the same output channel Debit and the same predecessor context ec_1 . tp satisfies the trace-determinism property. Indeed, the formula:

$$(\exists \{\mathbf{fee}_0, \mathbf{amt}_0\}. (\mathbf{y}_D^1 = \mathbf{amt}_1)) \wedge (\exists \{\mathbf{fee}_0, \mathbf{amt}_0\}. (\mathbf{fee}_0 > 0) \wedge (\mathbf{y}_D^1 = \mathbf{amt}_1 + \mathbf{fee}_0))$$

is not satisfiable because $\mathbf{amt}_1 < \mathbf{amt}_1 + \mathbf{fee}_0$ holds as we have $\mathbf{fee}_0 > 0$. A trace cannot belong to distinct paths: if the debit value is the same as what is requested for withdrawal then trace covers ec_2 , else ec_3 is covered.

5 Path-guided test cases

Roughly speaking, a test case $\mathbb{T}\mathbb{C}$ will be a mirror TIOSTS of a TIOSTS \mathbb{G} , restricted by tp , a test purpose of \mathbb{G} , intended to interact with a LUT that we wish to check its conformance to \mathbb{G} up to tp . $\mathbb{T}\mathbb{C}$ will be a tree-like TIOSTS with tp of \mathbb{G} as a backbone, incorporating the following specific characteristics:

- execution contexts in $\mathbb{E}\mathbb{C}(tp)$ constitute the main branch,
- sink states or leaves are assimilated with a test verdict. Notably, the last execution context $tgt(tp)$ of tp will be assimilated with the PASS verdict,
- from each ec in $\mathbb{E}\mathbb{C}(tp)$ other than $tgt(tp)$, the outgoing arcs outside tp decline all ways to deviate from tp and directly lead to a verdict state, either an inconclusive verdict or a failure verdict.

In Def.6, we define $\mathbb{T}\mathbb{C}$ by enumerating the different cases of transitions to be built according to channel type and tp membership. We now give a few indications for enhancing the definition readability. Channel roles are reversed: channels in CC^{in} as well as channel δ (resp. $C^{out} \cup UC^{in}$) become output (resp. input) channels. Variables of $\mathbb{T}\mathbb{C}$ will be symbolic variables involved in tp and will be used to store successive concrete events observed on LUT . Any observation on LUT will be encoded as an input transition in $\mathbb{T}\mathbb{C}$, whether it is an emission from a channel of C^{out} , a reception on a channel of UC^{in} or a time-out observation. On the latter, it is conventional to consider that a system that does not react before a certain delay, chosen to be long enough, is in a state of quiescence. The only notable exception is when input transitions of tp give rise to output transitions for $\mathbb{T}\mathbb{C}$, modeling a situation in which $\mathbb{T}\mathbb{C}$ stimulates LUT by sending it data.

The choice of the data to send is conditioned by two constraints: (i) taking into account the information collected so far and stored in the variables of \mathbb{TC} in the first steps, and (ii) the guarantee of being able to reach the last EC of tp , i.e. the verdict PASS. This will be done by ensuring the satisfiability of the path condition of tp , leaving aside the variables already binded.

We will refer to variables of a symbolic path as follows: for⁴ $\alpha \in \{in, out\}$, $f^\alpha(p) = \bigcup_{i \in [1, n]} f^\alpha(ec_i)$ will denote all introduced fresh variables in F^α used to compute a symbolic path $p = ec_0.ec_1 \dots ec_n$. Similarly, $f^{dur}(p) = \{f^{dur}(ec_i) \mid i \in [1, n]\}$. Moreover, for a target execution context $ec_n = tgt(p)$, we denote $\bar{f}^\alpha(ec_n)$ and $\bar{f}(ec_n)$ resp. for $f^\alpha(p)$ and $f(p)$.

Definition 6 (Path-guided test case). *Let tp be a test purpose for a TIOSTS \mathbb{G} . Let us consider the signature $\widehat{\Sigma} = (\widehat{A}, \widehat{K}, \widehat{C})$ where:*

- $\widehat{A} = f^{in}(tp) \cup f^{out}(tp)$,
- $\widehat{K} = f^{dur}(tp)$,
- $\widehat{C} = C_\delta$ such that $\widehat{C}^{in} = C^{out} \cup UC^{in}$ and $\widehat{C}^{out} = CC^{in} \cup \{\delta\}$

A test case guided by tp is a TIOSTS $\mathbb{TC} = (\widehat{Q}, \widehat{q}_0, \widehat{Tr})$ over $\widehat{\Sigma}$ where:

- $\widehat{Q} = (\mathbb{EC}(tp) \setminus \{tgt(tp)\}) \cup \mathbb{V}$ where:
 $\mathbb{V} = \{ \text{PASS}, \text{FAIL}^{out}, \text{FAIL}^{dur}, \text{INC}^{out}, \text{INC}^{dur}, \text{INC}_{spec}^{ucIn}, \text{INC}_{uspec}^{ucIn} \}$,
- $\widehat{q}_0 = ec_0$,
- \widehat{Tr} is defined by a set \mathcal{R} of 10 rules of the form $\frac{H}{tr \in \widehat{Tr}} \text{ LABEL}$ for $i \in [1, 10]$.
 Such a rule reads as follows: the transition tr can be added due to rule Ri to \widehat{Tr} provided that hypothesis H holds and $\text{Sat}(\phi(tr))$.

In writing the rules of \mathcal{R} , we will use the following formulas

$$\begin{aligned} \phi_{stim} &: \exists F^{ini} \cup \bar{f}(tgt(tp)) \setminus \bar{f}(ec'). \pi(tp) \\ \phi_{spec}^{obs} &: f^{dur}(ec) < \text{TM} \wedge (\exists F^{ini}. \pi(ec')) \\ \phi_{uspec}^{obs} &: f^{dur}(ec) < \text{TM} \wedge \bigwedge_{\substack{pec(ec')=ec \\ chan(ec')=c}} (\forall F^{ini}. \neg \pi(ec')) \\ \phi_{spec}^\delta &: f^{dur}(ec) \geq \text{TM} \wedge \bigvee_{\substack{pec(ec')=ec \\ chan(ec') \in C^{out} \cup UC^{in} \cup \{\delta\}}} (\exists F^{ini}. \pi(ec')) \\ \phi_{uspec}^\delta &: f^{dur}(ec) \geq \text{TM} \wedge \bigwedge_{\substack{pec(ec')=ec \\ chan(ec') \in C^{out} \cup UC^{in} \cup \{\delta\}}} (\forall F^{ini}. \neg \pi(ec')) \end{aligned}$$

where the constant TM (*Time-out*) sets the maximum waiting-time for observing outputs or uncontrollable inputs.

$$\frac{ec \xrightarrow{(z, c?x)} ec' \in \mathbb{EC}(tp) \quad c \in CC^{in}}{(ec, c!x, \phi_{stim}, \{f^{dur}(ec)\}, id_{\widehat{A}}, ec') \in \widehat{Tr}} \text{SKIP} \quad (R1)$$

$$\frac{\frac{ec \xrightarrow{(z, c!y)} ec' \in \mathbb{EC}(tp) \quad ec' \neq tgt(tp) \quad c \in C^{out}}{(ec, c?y, \phi_{spec}^{obs}, \{f^{dur}(ec')\}, id_{\widehat{A}}, ec') \in \widehat{Tr}} \text{SKIP} \quad (R2) \quad \frac{ec \xrightarrow{(z, c!y)} ec' \in \mathbb{EC}(tp) \quad ec' = tgt(tp) \quad c \in C^{out}}{(ec, c?y, \phi_{spec}^{obs}, \emptyset, id_{\widehat{A}}, \text{PASS}) \in \widehat{Tr}} \text{PASS} \quad (R3)}$$

⁴ For i and j in \mathbb{N} verifying $i < j$, $[i, j]$ contains the integers from i to $j - 1$ included.

$$\begin{array}{c}
\frac{ec \xrightarrow{(z,c?y)} ec' \quad ec \in \mathbb{E}C(tp) \setminus \{tgt(tp)\}}{ec' \notin \mathbb{E}C(tp) \quad c \in C^{out}} \quad (R4) \quad \frac{ec \in \mathbb{E}C(tp) \quad c \in C^{out}}{(ec, c?f_c^{out}(ec), \phi_{uspec}^{obs}, \emptyset, id_{\hat{A}}, FAIL^{out}) \in \widehat{Tr}} \quad (R5) \\
\frac{ec \xrightarrow{(z,c?x)} ec' \in \mathbb{E}C(tp)}{c \in UC^{in}} \quad (R6) \quad \frac{ec \xrightarrow{(z,c?x)} ec' \quad ec \in \mathbb{E}C(tp) \setminus \{tgt(tp)\}}{ec' \notin \mathbb{E}C(tp) \quad c \in UC^{in}} \quad (R7) \\
\frac{}{(ec, c?x, \phi_{spec}^{obs}, \{f^{dur}(ec')\}, id_{\hat{A}}, ec') \in \widehat{Tr}} \quad SKIP \quad \frac{}{(ec, c?x, \phi_{spec}^{obs}, \emptyset, id_{\hat{A}}, INC_{spec}^{ucIn}) \in \widehat{Tr}} \quad INC_{spec}^{ucIn} \\
\frac{ec \in \mathbb{E}C(tp) \quad c \in UC^{in}}{(ec, c?f_c^{in}(ec), \phi_{uspec}^{obs}, \emptyset, id_{\hat{A}}, INC_{uspec}^{ucIn}) \in \widehat{Tr}} \quad (R8) \quad INC_{uspec}^{ucIn} \\
\frac{ec \in \mathbb{E}C(tp)}{(ec, \delta!, \phi_{spec}^{\delta}, \emptyset, id_{\hat{A}}, INC^{dur}) \in \widehat{Tr}} \quad (R9) \quad INC^{dur} \quad \frac{ec \in \mathbb{E}C(tp)}{(ec, \delta!, \phi_{uspec}^{\delta}, \emptyset, id_{\hat{A}}, FAIL^{dur}) \in \widehat{Tr}} \quad (R10) \quad FAIL^{dur}
\end{array}$$

A verdict PASS is reached when tp is covered, verdicts INC_n^m are reached when traces deviate from tp while remaining in \mathbb{G} , and verdicts $FAIL^m$ denote traces outside \mathbb{G} . The annotations n and m provide additional information on the cause of the verdict. Rules $R1$, $R2$ and $R6$, grouped together under the label SKIP, allow advancing along tp , resp. by stimulating LUT with the sending of data, observing an emission on C^{out} and observing a reception on UC^{in} . Rule $R3$ indicates that the last EC of tp , thus the PASS verdict, has been reached. Rules $R4$, $R7$, $R8$ and $R9$, each with a label INC_n^m indicate that the observed event causes LUT to leave tp , without leaving \mathbb{G} , resp. by observing an output, an input specified in \mathbb{G} , an input not specified in \mathbb{G} and a time-out observation. Lastly, rules $R5$ and $R10$, resp. labeled by $FAIL^{out}$ and $FAIL^{dur}$, raise a FAIL verdict, for resp. an unauthorized output and an exceeded time-out.

Example 6. In Fig. 4, the test case for $tp = ec_0ec_1 \dots ec_4$ (see Ex. 5) is depicted. Certain verdict states are repeated for readability, and defining rules annotate the transitions. The test case utilizes the Transc channel as a controllable input channel for stimulation while observing all other channels. For space considerations, we comment only on some rules.

Rule $R1$ defines a stimulation action $Transc!(\mathbf{amt}_1, \mathbf{tb}_1)$ (transition from ec_0 to ec_1) constrained by $\pi(tp)$ to select an appropriate value for \mathbf{amt}_1 and \mathbf{tb}_1 together with a time of stimulation \mathbf{z}_0 that allows to follow the test purpose. Within $\pi(tp)$, \mathbf{amt}_1 is limited to some range ($10 \leq \mathbf{amt}_1 \leq 1000$), \mathbf{tb}_1 is greater than or equal 4, while \mathbf{z}_0 is unconstrained (a duration measured with clock \mathbf{z}_0). Non-revealed variables, i.e., other than \mathbf{z}_0 , \mathbf{amt}_1 and \mathbf{tb}_1 appearing in $\pi(tp)$ are bound by the existential quantifier due to their unknown values at this execution point. The clock \mathbf{z}_1 is reset to enable reasoning on subsequent actions' duration (measured on \mathbf{z}_1). Rule $R2$ defines an observation action $Debit?(\mathbf{y}_{D_1}^1, \mathbf{y}_{D_2}^1, \mathbf{y}_{D_3}^1)$ constrained by $(\mathbf{z}_1 < TM) \wedge \exists \mathbf{fee}_0. \pi(ec_2)$ (transition from ec_1 to ec_2) while rule $R5$ defines the same observation constrained by $(\mathbf{z}_1 < TM) \wedge \forall \mathbf{fee}_0. \neg \pi(ec_2) \wedge \forall \{\mathbf{fee}_0\}. \neg \pi(ec_9)$ (transition from ec_1 to $FAIL^{out}$). Both situations are possible: Trace $(0, Transc!(50, 4)).(0, Debit?(1, 51, ATM_ID))$ reaches ec_2 whereas $FAIL_{out}$ is reached by traces $(0, Transc!(50, 4)).(0, Debit?(1, 0, ATM_ID))$ and

Definition 7 (Relation execution $\rightsquigarrow_{\text{TC}}$). Let \mathbb{G} be a TIOSTS and tp a test purpose for \mathbb{G} with $\text{TC} = (\widehat{Q}, \widehat{q}_0, \widehat{Tr})$ the test case guided by tp .

The execution relation $\rightsquigarrow_{\text{TC}} \subseteq (\text{Evt}(C_\delta)^* \times \widehat{Q} \times M^F)^2$ is defined by:

for $ev.\sigma \in \text{Evt}(C_\delta)^*$, $q, q' \in \widehat{Q}$ and for $\nu, \nu' \in M^F$, $(ev.\sigma, q, \nu) \rightsquigarrow_{\text{TC}} (\sigma, q', \nu')$ holds iff there exists $tr \in \widehat{Tr}$ s.t. $\text{src}(tr) = q$, $\text{tgt}(tr) = q'$, $\nu'(\text{act}(tr)) = \text{act}(ev)$ and $M \models_{\nu'} \phi(tr)$ with ν' defined as:

- if $ev = (d, c?v)$ and $\text{chan}(tr) = c$ then $\nu' = \nu[f^{dur}(q) \mapsto d][f_c^{in}(q) \mapsto v]$;
- if $ev = (d, c!v)$ and $\text{chan}(tr) = c$ then $\nu' = \nu[f^{dur}(q) \mapsto d][f_c^{out}(q) \mapsto v]$;
- else, i.e., $ev = (d, \delta!)$ and $\text{chan}(tr) = \delta$, $\nu' = \nu[f^{dur}(q) \mapsto d]$.

Intuitively, a step $(ev.\sigma, q, \nu) \rightsquigarrow_{\text{TC}} (\sigma, q', \nu')$ consists in:

- reading the first element ev of a trace from a test case state q and an interpretation ν synthesizing the known information about the variables in F ;
- finding a transition tr in \widehat{Tr} whose action matches the mirror action of ev ;
- building a new triple with σ the trace remaining to be read, q' a successor state of q in \widehat{Q} , and ν' the updated interpretation of the variables F .

The execution relation simulates a parallel composition between timed input output systems, synchronizing inputs and outputs. Our formulation deviates from the one in [21] for two essential reasons: the symbolic nature of the test case requires the intermediate interpretations of variables to be memorized, and uncontrollable channels require to adapt the synchronization [10]. Let LUT be a subset of $\text{Evt}(C_\delta)^*$ satisfying \mathcal{H} and $\rightsquigarrow_{\text{TC}}^*$ be the reflexive and transitive closure of $\rightsquigarrow_{\text{TC}}$. Given a LUT trace σ_0 , we apply the execution relation iteratively from an initial triplet consisting of σ_0 a trace, ec_0 an initial EC and ν_0 an arbitrary interpretation, to obtain the corresponding test verdict for tp , so that the verdict set obtained from the execution of TC on LUT is defined by:

$$\text{vdt}(LUT, \text{TC}) = \{V \mid \exists \sigma_0 \in LUT, \nu_0 \in M^F, (\sigma_0, q_{0\text{TC}}, \nu_0) \rightsquigarrow_{\text{TC}}^* (\sigma, V, \nu)\}.$$

Th. 1 states the soundness of the test case execution for detecting errors through the FAIL^{out} and FAIL^{dur} verdicts. A proof can be found in Appendix A. Comparable results can be formulated for the other verdicts. Still, those relating to FAIL verdicts are the only ones to guarantee that any discarded system under test does not satisfy the tioco conformance relation.

Theorem 1. Let C be a set of channels. Let \mathbb{G} and LUT be resp. a TIOSTS defined on C and a subset of $\text{Evt}(C_\delta)^*$ satisfying \mathcal{H} .

If LUT tioco \mathbb{G} then for any test purpose tp for \mathbb{G} with TC as test case guided by tp , we have $\text{FAIL}^{out} \notin \text{vdt}(LUT, \text{TC})$ and $\text{FAIL}^{dur} \notin \text{vdt}(LUT, \text{TC})$.

The test case generation is implemented as module in the Diversity symbolic execution platform [8]. Resulting test cases are expressed in Diversity's entry language, allowing their exploration through symbolic execution with the SMT-solver Z3 [9]. For easier execution, we export the test cases from Diversity in JSON format, with transition guards expressed in the SMT-LIB input format for SMT-solvers. Our experiments involved applying this test case generation

to the ATM example on an Intel Core i7 processor. Varying the size of the test purposes up to 100 transitions, we observed successful trace-determinism verification for all test purposes. We noted a noticeable increase in generation duration as the test purpose size grew, while still remaining feasible. Generating the TIOSTS test case (513 transitions) for the test purpose of 100 transitions took more than 40s, in contrast to only 500ms for the test purpose of size 4 in Ex. 6 (31 transitions) resp. 8s for the test purpose of size 50 (138 transitions).

6 Related work

Existing works for (t)ioco conformance test cases from symbolic models employs two main generation methods: online and offline. Online generation [11,14,7] involves dynamically generating test cases while exploring the model during execution on the system under test. In contrast, offline generation [15,3,4] focuses on deriving test cases from the model before executing them on the system under test. Some works [11,14,7] propose online test case generation using symbolic execution. Yet, these works did not consider time constraints, and in particular, work [7] did not consider quiescence. In [7], a test purpose is a finite path, while in [14], it is a finite symbolic subtree. Both works require maintaining a set of reached symbolic states during test case execution to avoid inconsistent verdicts in case of non-determinism, at the expense of computational resources for tracking the symbolic states and solving their path conditions. Work [4] proposes offline test case generation using a path to compute a timed stimulation sequence for the system under test. The recorded timed output sequence is then analyzed for conformance. This approach lacks control over the value and timing of the next stimulation relative to the observed system behavior, potentially resulting in greater deviations from the test purpose. In [15], objective-centered testers for timed automata are built using game theory. Works [18,3] propose offline test case generation as tree-like symbolic transition systems and thus restricted to determinism as we do. The test case generation in [18] relies on abstract interpretation to reinforce test case guards on data to keep chances of staying in the test purpose and does not consider time. In [3], symbolic execution techniques are used for data handling, while zone-based abstraction techniques are employed for time. This separation results in less expressive and flexible models, as it cannot extend to incorporate data parameters in the time constraints.

7 Conclusion

This paper presents an offline approach to conformance test case generation from models of timed symbolic transition systems using symbolic execution to handle data and time. Our test purpose is a symbolic path in the model which fulfills a determinism condition to enable the generation of sound tree-like test cases. By distinguishing between controllable inputs (from the test case) and uncontrollable inputs (from other systems), our approach enhances the usability of test cases when the system interacts with other systems (remote in general). It should be noted that our test cases include configurations where the resolution time exceeds the stimulation time or overlaps the arrival of an observation.

References

1. Aichernig, B.K., Tappler, M.: Symbolic input-output conformance checking for model-based mutation testing. In: USE@FM 2015. Elsevier (2015). <https://doi.org/10.1016/j.entcs.2016.01.002>, <https://doi.org/10.1016/j.entcs.2016.01.002>
2. Alur, R., Dill, D.L.: A theory of timed automata. *Theor. Comput. Sci.* (1994). [https://doi.org/10.1016/0304-3975\(94\)90010-8](https://doi.org/10.1016/0304-3975(94)90010-8)
3. Andrade, W.L., Machado, P.D.L., Jérón, T., Marchand, H.: Abstracting time and data for conformance testing of real-time systems. In: ICST Workshops (2011). <https://doi.org/10.1109/ICSTW.2011.82>
4. Bannour, B., Escobedo, J.P., Gaston, C., Le Gall, P.: Off-line test case generation for timed symbolic model-based conformance testing. In: ICTSS (2012). https://doi.org/10.1007/978-3-642-34691-0_10
5. Benharrat, N., Gaston, C., Hierons, R.M., Lapitre, A., Le Gall, P.: Constraint-based oracles for timed distributed systems. In: ICTSS. Springer (2017). https://doi.org/10.1007/978-3-319-67549-7_17
6. de Boer, F.S., Bonsangue, M.M.: On the nature of symbolic execution. In: ter Beek, M.H., McIver, A., Oliveira, J.N. (eds.) FM. Springer (2019). https://doi.org/10.1007/978-3-030-30942-8_6
7. van den Bos, P., Tretmans, J.: Coverage-based testing with symbolic transition systems. In: Beyer, D., Keller, C. (eds.) TAP. Springer (2019). https://doi.org/10.1007/978-3-030-31157-5_5
8. CEA: Diversity, Eclipse Formal Modeling Project. <https://projects.eclipse.org/proposals/eclipse-formal-modeling-project> (2023)
9. De Moura, L., Bjørner, N.: Z3: An efficient smt solver. In: TACAS. Springer (2008). https://doi.org/10.1007/978-3-540-78800-3_24
10. Escobedo, J.P., Gaston, C., Gall, P.L., Cavalli, A.R.: Testing web service orchestrators in context: A symbolic approach. In: SEFM. pp. 257–267. IEEE Computer Society (2010)
11. Frantzen, L., Tretmans, J., Willemse, T.A.C.: Test generation based on symbolic specifications. In: FATES (2004). https://doi.org/10.1007/978-3-540-31848-4_1
12. Frantzen, L., Tretmans, J., Willemse, T.A.C.: A symbolic framework for model-based testing. In: FATES and RV 2006 Workshops. Springer (2006). https://doi.org/10.1007/11940197_3
13. Gaston, C., Hierons, R.M., Le Gall, P.: An implementation relation and test framework for timed distributed systems. In: ICTSS (2013). https://doi.org/10.1007/978-3-642-41707-8_6
14. Gaston, C., Le Gall, P., Rapin, N., Touil, A.: Symbolic execution techniques for test purpose definition. In: TestCom (2006). https://doi.org/10.1007/11754008_1
15. Henry, L., Jérón, T., Markey, N.: Control strategies for off-line testing of timed systems. *Formal Methods Syst. Des.* (2022). <https://doi.org/https://doi.org/10.1007/s10703-022-00403-w>
16. Hessel, A., Larsen, K.G., Mikucionis, M., Nielsen, B., Petterson, P., Skou, A.: Testing real-time systems using UPPAAL. In: FORTEST (2008). https://doi.org/10.1007/978-3-540-78917-8_3
17. Janssen, R., Tretmans, J.: Matching implementations to specifications: the corner cases of ioco. In: Hung, C., Papadopoulos, G.A. (eds.) SAC. ACM (2019). <https://doi.org/10.1145/3297280.3297496>

18. Jéron, T.: Symbolic model-based test selection. In: Machado, P.D.L. (ed.) SBMF. Elsevier (2008). <https://doi.org/10.1016/j.entcs.2009.05.051>
19. King, J.C.: Symbolic execution and program testing. Commun. ACM **19**(7), 385–394 (1976). <https://doi.org/10.1145/360248.360252>
20. Krichen, M., Tripakis, S.: Black-box conformance testing for real-time systems. In: SPIN Workshop. Springer (2004). https://doi.org/10.1007/978-3-540-24732-6_8
21. Krichen, M., Tripakis, S.: Interesting properties of the real-time conformance relation. In: ICTAC. Lecture Notes in Computer Science, vol. 4281, pp. 317–331. Springer (2006)
22. Luthmann, L., Göttmann, H., Lochau, M.: Compositional liveness-preserving conformance testing of timed I/O automata. In: FACS. Springer (2019). https://doi.org/10.1007/978-3-030-40914-2_8
23. Marsso, L., Mateescu, R., Serwe, W.: TESTOR: A modular tool for on-the-fly conformance test case generation. In: Beyer, D., Huisman, M. (eds.) TACAS. Springer (2018). https://doi.org/10.1007/978-3-319-89963-3_13
24. Rusu, V., Marchand, H., Jéron, T.: Automatic verification and conformance testing for validating safety properties of reactive systems. In: FM. Springer (2005). https://doi.org/10.1007/11526841_14
25. Standard, E.: Methods for Testing and Specification (MTS); The Testing and Test Control Notation version 3; Part 1: TTCN-3 core language (2005)
26. von Styp, S., Bohnenkamp, H.C., Schmaltz, J.: A conformance testing relation for symbolic timed automata. In: Chatterjee, K., Henzinger, T.A. (eds.) FORMATS. Springer (2010). https://doi.org/10.1007/978-3-642-15297-9_19
27. Tretmans, J.: Test generation with inputs, outputs, and quiescence. In: Margaria, T., Steffen, B. (eds.) TACAS. Springer (1996). https://doi.org/10.1007/3-540-61042-1_42
28. Tretmans, J., Janssen, R.: Goodbye ioco. In: A Journey from Process Algebra via Timed Automata to Model Learning. Springer (2022). https://doi.org/10.1007/978-3-031-15629-8_26

A Proof of Th. 1

We carry out the proof by contraposition, i.e. we prove that if there exists a test objective tp for \mathbb{G} and a test case \mathbb{TC} guided by tp s.t. FAIL^{out} or FAIL^{dur} are in $vdt(LUT, \mathbb{TC})$ then $\neg(LUT \text{ tioco } \mathbb{G})$. According to the definition of tioco, this amounts to proving that there exists $\sigma \in \text{Sem}(\mathbb{G}) \cap LUT$, and an $ev \in \text{Evt}(C^{out} \cup \{\delta\})$ s.t. $\sigma.ev \in LUT$ and $\sigma.ev \notin \text{Sem}(\mathbb{G})$. Prop.1 states this claim.

Proposition 1. *Let $\sigma.ev.\sigma'$ be a trace of LUT with σ and σ' traces in $\text{Evt}(C_\delta)^*$ and ev a concrete event in $\text{Evt}(C_\delta)$. If there exists a test purpose tp for \mathbb{G} and a test case \mathbb{TC} guided by tp s.t. $(\sigma.ev.\sigma', ec_0, \nu_0) \overset{*}{\sim}_{\mathbb{TC}} (\sigma', V, \nu')$ with $V \in \{\text{FAIL}^{out}, \text{FAIL}^{dur}\}$ then:*

- (1) $ev \in \text{Evt}(C^{out} \cup \{\delta\})$
- (2) $\sigma \in \text{Sem}(\mathbb{G})$
- (3) $\sigma.ev \notin \text{Sem}(\mathbb{G})$

Let us suppose $(\sigma.ev.\sigma', ec_0, \nu_0) \overset{*}{\sim}_{\mathbb{TC}} (\sigma', V, \nu')$ with $V \in \{\text{FAIL}^{out}, \text{FAIL}^{dur}\}$. There exists an execution sequence $(\sigma.ev.\sigma', ec_0, \nu_0) \overset{*}{\sim}_{\mathbb{TC}} (ev.\sigma', ec, \nu) \rightsquigarrow_{\mathbb{TC}} (\sigma', V, \nu')$ s.t. ev is executed with a Test-Case transition (TC-transition) tr built with either rule $R5 \text{ FAIL}^{out}$ or rule $R10 \text{ FAIL}^{dur}$.

Proof of (1) As $\text{chan}(tr) = \text{chan}(ev)$, by $R5 \text{ FAIL}^{out}$ (resp. $R10 \text{ FAIL}^{dur}$), $\text{chan}(tr) \in C^{out}$ (resp. $\text{chan}(tr) = \delta$). Hence $ev \in \text{Evt}(C^{out} \cup \{\delta\})$.

Proof of (2) Based on the execution steps and corresponding TC-transitions, the events in σ can only be of the form $(d, c!v)$ or $(d, c?v)$, excluding the form $(d, \delta!)$. Indeed, no TC transitions on the channel δ lead to an execution context. The only TC-transitions involving channel δ are from rules $R9 \text{ INC}^{dur}$ and $R10 \text{ FAIL}^{dur}$, and their target state is a verdict.

Let ec an execution context of tp distinct from $\text{tgt}(tp)$. Following its predecessor contexts, it defines a unique path p_{ec} of \mathbb{G} leading to ec defining a non-empty set of traces. Let ν in M^F an interpretation verifying $M \models_\nu \exists F^{ini}.\pi(\text{tgt}(p_{ec}))$ and let σ_ν be the trace of p_{ec} built using ν .

Let us now consider $(ev.\sigma, ec, \nu) \rightsquigarrow_{\mathbb{TC}} (\sigma, ec', \nu')$ with $ec \notin V$. Let us denote tr the transition of $\widehat{T}r$ underlying the execution step $(ev.\sigma, ec, \nu) \rightsquigarrow_{\mathbb{TC}} (\sigma, ec', \nu')$. We have $\text{tgt}(tr) = ec'$ and $\text{src}(tr) = ec$. As $ec \notin V$, the rule involved in building the transition tr is one of the $R1$, $R2$ and $R6$ rules.

- In case $ev = (d, c!v)$, tr comes from the use of rule $R2 \text{ SKIP}$. $ev(ec') = (z, c!y)$ with $z = f^{dur}(ec')$ and $y = f_c^{out}(ec')$; and $\phi(tr) = (z < \text{TM}) \wedge (\exists F^{ini}.\pi(ec'))$. On the other hand $M \models_{\nu'} \phi(tr)$ where $\nu' = \nu[z \mapsto d][y \mapsto v]$ (Def.7 of $\rightsquigarrow_{\mathbb{TC}}$) then $M \models_{\nu'} \exists F^{ini}.\pi(ec)$ (ν' satisfies the right-side of the conjunction of $\phi(tr)$). We can thus extend the trace σ_ν of p_{ec} with the concrete event $(d, c!v) = \nu'(ev(ec'))$ to constitute a trace of $p_{ec}.ec'$. Then $\sigma_\nu.(d, c!v) \in \text{Sem}(\mathbb{G})$.
- In case $ev = (d, c?v)$ with $c \in UC^{in}$, tr comes from the use of rule $R6 \text{ SKIP}$. Similar reasoning as for case $ev = (d, c!v)$ ($R2 \text{ SKIP}$) applies.

- In case $ev = (d, c?v)$ with $c \in CC^{in}$, tr comes from the use of rule $R1$ SKIP. We have $tgt(tr) = ec'$; $ev(ec') = (z, c?x)$ with $z = f^{dur}(ec)$ and $x = f_c^{in}(ec)$ and $\phi(tr) = \exists F^{ini} \cup \bar{f}(tgt(tp)) \setminus \bar{f}(ec').\pi(tp)$. On the other hand $M \models_{\nu'} \phi(tr)$ where $\nu' = \nu[z \mapsto d][x \mapsto v]$. As ec' belongs to $\mathbb{E}C(tp)$, path condition $\pi(ec')$ occurs in the conjunction defining formula $\pi(tp)$, then $M \models_{\nu'} \exists F^{ini} \cup \bar{f}(tgt(tp)) \setminus \bar{f}(ec').\pi(ec')$. Also ν' satisfies $\pi(ec')$ for the values d and v associated with $f^{dur}(ec)$ and $f_c^{in}(ec)$ because these variables are excluded from the variables which are bound by the existential quantifier in $\phi(tr)$. The rest of variables of $\bar{f}(tgt(tp))$ are irrelevant as they do not occur in $\pi(ec')$, then $M \models_{\nu'} \exists F^{ini}.\pi(ec')$. We can thus extend the trace σ_ν of p_{ec} with the concrete event $(d, c?v)$ so that $\sigma_\nu.(d, c?v) \in Sem(\mathbb{G})$.

Thus, moving along tp without reaching the $tgt(tp)$ provides traces of \mathbb{G} .

Proof of (3) Given the execution $(\sigma.ev.\sigma', ec_0, \nu_0) \xrightarrow{*}_{\text{TC}} (\sigma', V, \nu')$ with $V \in \{\text{FAIL}^{out}, \text{FAIL}^{dur}\}$, we prove that $\sigma.ev \notin Sem(\mathbb{G})$.

Let us remark that the path p leading to ec ($tgt(p) = ec$) admits traces $\sigma = \nu(p)$ for interpretations verifying $\nu \models \exists F^{ini}.\pi(ec)$. Moreover, given such a trace σ , by Prop.1 (2), $\sigma \in Sem(\mathbb{G})$ and trace-determinism makes such a corresponding path p unique.

- Case FAIL^{out} (rule $R5$ FAIL^{out}): by Prop.1 (1), ev is of the form $(d, c!v)$. For the TC-transition tr that allows the execution of ev , $chan(tr) = chan(ev)$, $src(tr) = ec$, $tgt(tr) = \text{FAIL}^{out}$ and $\phi(tr) = (f^{dur}(ec) < \text{TM}) \wedge \bigwedge_{\substack{pec(ec')=ec \\ chan(ec')=c}} (\forall F^{ini}.\neg\pi(ec'))$

On the other hand $\nu' \models \phi(tr)$ with $\nu' = \nu[f^{dur}(ec) \mapsto d][f_c^{out}(ec) \mapsto v]$ thus $\nu' \models \forall F^{ini}.\neg\pi(ec')$ for any successor ec' of ec such that $chan(ec') = c$. That is, for any such successor ec' , $\nu' \not\models \exists F^{ini}.\pi(ec')$. Thus, there is no ec' which extends p into a path $p.ec'$ carrying $\sigma.ev$ through ν' , i.e., such that $\nu' \models \exists F^{ini}.\pi(ec')$ and $\nu'(p.ec') = \sigma.ev$. Then $\sigma.ev \notin Traces(\mathbb{G})$.

- Case FAIL^{dur} (rule $R10$ FAIL^{dur}): by Prop.1 (1), ev is of the form $(d, \delta!)$. For the the TC-transition tr that allows the execution of ev , $chan(tr) = chan(ev)$, $src(tr) = ec$, $tgt(tr) = \text{FAIL}^{dur}$ and $\phi(tr) = f^{dur}(ec) \geq \text{TM} \wedge \bigwedge_{\substack{pec(ec')=ec \\ chan(ec') \in C^{out} \cup UC^{in} \cup \{\delta\}}} \forall F^{ini}.\neg\pi(ec')$

On the other hand, $\nu' \models \phi(tr)$ with $\nu' = \nu[f^{dur}(ec) \mapsto d]$ thus $\nu' \models \forall F^{ini}.\neg\pi(ec')$ for any successor ec' of ec (i.e. verifying $pec(ec') = ec$) such that $chan(ec') \in C^{out} \cup UC^{in} \cup \{\delta\}$. If $chan(ec') = \delta$, there is at most one of such successor ec' by the quiescence enrichment. Yet as $\nu' \not\models \exists F^{ini}.\pi(ec')$, we cannot extend p into a path $p.ec'$ carrying $\sigma.ev$ through ν' , i.e., such that $\nu' \models \exists F^{ini}.\pi(ec')$ and $\nu'(p.ec') = \sigma.ev$. Then $\sigma.ev \notin Traces(\mathbb{G})$. If $chan(ec') \in C^{out} \cup UC^{in}$, those successors ec' can result in traces ending with quiescence events in $Sem(\mathbb{G})$. Such quiescent traces are of the form $\sigma.(d', \delta!)$ with $d' < d$ and are computed for $p.ec'$ through ν' , i.e., such that $\nu' \models \exists F^{ini}.\pi(ec')$ and $\nu'(p.ec') = \sigma.(d, c!v)$ or $\nu'(p.ec') = \sigma.(d, c?v)$ with $c = chan(ec')$. Yet as $\nu' \not\models \exists F^{ini}.\pi(ec')$, we cannot infer such traces in $Sem(\mathbb{G})$. Then, $\sigma.ev \notin Sem(\mathbb{G})$. \square

