Input Output Symbolic Transition Systems Enriched by Program Calls and Contracts: a detailed example of vending machine

Imen Boudhiba, Christophe Gaston, Pascale Le Gall, Virgile Prévosto

▶ **To cite this version:**

Imen Boudhiba, Christophe Gaston, Pascale Le Gall, Virgile Prévosto. Input Output Symbolic Transition Systems Enriched by Program Calls and Contracts: a detailed example of vending machine. [Research Report] Laboratoire MAS - CentraleSupelec. 2015. hal-01191890

HAL Id: hal-01191890
https://hal.science/hal-01191890

Submitted on 4 Sep 2015

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.

Input Output Symbolic Transition Systems Enriched by Program Calls and Contracts: a detailed example of vending machine

Imen Boudhiba[1], Christophe Gaston[2] and
Pascale Le Gall[1] and Virgile Prevosto[2]

[1] Laboratoire MAS, CentraleSupelec, 92195 Châtenay-Malabry, France
email: {imen.boudhiba,pascale.legall}@centralesupelec.fr
[2] CEA LIST, Point Courrier 174, 91191, Gif-sur-Yvette, France
email: {virgile.prevosto, christophe.gaston}@cea.fr

Abstract. An Input Output Symbolic Transition System (IOSTS) specifies all expected sequences of input and output messages of a reactive system. Symbolic execution over this IOSTS then allows to generate a set of test cases that can exercise the various possible behaviors of the system it represents. In this paper, we extend the IOSTS framework with explicit program calls, possibly equipped with contracts specifying what the program is supposed to do. This approach bridges the gap between a model-based approach in which user-defined programs are abstracted away and a code-based approach in which small pieces of code are separately considered regardless of the way they are combined. First, we extend symbolic execution techniques for IOSTS with programs, in order to re-use classical test case generation algorithms. Second, we explore how constraints coming from IOSTS symbolic execution can be used to infer contracts for programs used in the IOSTS.
Keywords: Input Output Symbolic Transition Systems, Program Contracts, Model-based Testing, Symbolic Execution, Feasibility.

1 Introduction

Symbolic transition systems, such as Input Output Symbolic Transition Systems (IOSTS) [10] are a classical reference modeling framework for model-based testing of reactive systems. They provide a convenient abstraction of the behaviors of such systems by modeling system state evolution using variable assignments. The symbolic execution tree of an IOSTS characterizes the different classes of numeric executions. Each path defines a sequence of symbolic inputs and outputs, and a path condition which is a formula constraining the values exchanged (inputs or outputs) with the environment of the system. It is possible to use such paths as reference symbolic behaviors to be tested (i.e. as *test purposes*). In [10], we have proposed a framework to analyze IOSTS both to extract such test purposes and to solve the oracle problem thanks to a fully on-line algorithm. However, this kind of framework is limited by the symbolic treatment of functions. Indeed, IOSTS variables are assigned by terms built on functions. In order

to be able to reason on the symbolic values assigned to variables, the symbolic execution engine is equipped with constraint solving techniques able to analyze those functions. As long as one deals with basic arithmetic or boolean functions, it is generally tractable, but as soon as one deals with user-defined or ad-hoc functions, solving techniques may fail to scale, or even, due to undecidability results, such techniques may not exist. Analyzing such functions (later referred as "programs") may require both to deal with sophisticated data structures and to explore their (arbitrarily complex) control graph.

In this paper we propose an approach to overcome this limitation by abstracting program behaviors by means of *contracts* [17]. A contract for a program consists in a collection of couples, also called *behaviours*, formed of a pre-condition that specifies constraints that the caller must enforce at the call site, and a post-condition which is a property guaranteed at the program return. We enrich the basic IOSTS framework to deal with program calls equipped with contracts. We show how to extend symbolic execution mechanisms to reason about IOSTS equipped with program calls by analyzing those calls through their contracts. Thus, we avoid analyzing the actual behavior of the program and replace it by abstract constraints on its formal parameters. Our framework allows computing symbolic paths that can be used as test purposes. It may happen that guards and contracts are incompatible so that some symbolic paths are infeasible (*i.e.* they have no associated trace). In practice it means that there exists no program that can both satisfy its associated contracts and compute values allowing to follow the whole symbolic path. We show how to use symbolic techniques to check that a given set of symbolic paths is consistent with respect to program calls.

Moreover, since guards occurring on transitions of an IOSTS interact with contracts associated to programs, we present an approach to extract new contracts for each of the program exercised. Such contracts reflect constraints on the program that make the path feasible. As such, they represent new contracts that can be used at the unitary level, to evaluate the correctness of actual program used to implement the system under test.

The remaining of the paper is organized as follows. In Section 2, we give basic definitions about many-typed first order logic. Section 3 presents programs and their contracts. In Section 4, we introduce IOSTS with programs. Section 5 defines symbolic execution of an IOSTS with programs and the associated feasibility condition. Usage of symbolic execution for testing purposes, including contract inference for unitary testing is introduced in Section 6. In Section 7, we give a detailed example of a vending machine modelled by an IOSTS enriched by program calls: in particular, it includes a program in charge of computing the giving of change in function of coins inserted by the user and of the machine reserve.

2 Preliminaries

For two sets A and B, B^A denotes the set of mappings $f : A \to B$ from A to B and id_A is the identity mapping on A. For a mapping $f : A \to B$, $f[a_i \mapsto b_i]_{i\in 1..n}$ is the mapping associating b_i to a_i for all i in $1..n$ and $f(a)$ to a not belonging to $\{a_i \mid i \in 1..n\}$. By convention, $[a_i \mapsto b_i]_{i\in 1..n}$ stands for $id_A[a_i \mapsto b_i]_{i\in 1..n}$. For two mappings $f : A_1 \to B$ and $g : A_2 \to B$ with $A_1 \cap A_2 = \emptyset$, $f \cup g : A_1 \cup A_2 \to B$ is the mapping defined by: $\forall a \in A_1, (f \cup g)(a) = f(a)$ and $\forall a \in A_2, (f \cup g)(a) = g(a)$. A^* (resp. A^+) denotes the set of words on A provided with the concatenation operator '.' and the empty word ε (resp. deprived of the empty word ε). For an ordered list $l = (a_1, \ldots, a_n)$ of n elements of A, $\{\!\{l\}\!\}$ denotes the set $\{a_1, \ldots, a_n\}$ of elements occurring in l.

We use classical multi-typed first order logic to handle data. A *data signature* is a pair (S, F) where S is a set of so-called *types* and F is a set of *functions* provided with a profile $s_1 ... s_{n-1} \to s_n$ with each $s_i \in S$. For $V = \coprod_{s\in S} V_s$ a set of variables typed in S, the set $T_F(V) = \coprod_{s\in S} T_F(V)_s$ of so-called functional terms over V is defined as usual over (S, F). Moreover, each set V_s contains an identified subset, denoted V_s^{fro}, whose elements are called *frozen variables* and we denote $V^{fro} = \coprod_{s\in S} V_s^{fro}$ the subset of V of all frozen variables. The set $Sen_F(V)$ of *formulas* is built over Boolean constants $\top$ and $\bot$, equalities $t = t'$ for t and t' terms in $T_F(V)$ of same type and usual Boolean connectives ($\wedge$, $\vee$, $\neg$, ...). *Substitutions* over V are applications $\sigma : V \to T_F(V)$ that preserve types and are such that all elements of V^{fro} are frozen for σ (i.e. $\forall v \in V^{fro}, \sigma(v) = v$). Thus, as frozen variables cannot be substituted, they may be considered as new special constants. Substitutions can be canonically extended to $T_F(V)$. For a term t in $T_F(V)$, for a formula φ in $Sen_F(V)$, $Occ(t)$ and $Occ(\varphi)$ will denote the set of variables occurring in respectively t and φ.

A *F-model* is a set of typed variables $M = \coprod_{s\in S} M_s$ provided with a function $\overline{f} : M_{s_1} \times \cdots \times M_{s_{n-1}} \to M_{s_n}$ for each $f : s_1 \cdots s_{n-1} \to s_n$ in F. An *interpretation* is an application $\nu : M^V$ that preserves types and can be canonically extended to $T_F(V)$. The satisfaction of a formula φ in $Sen_F(V)$ by an interpretation $\nu \in M^V$, denoted $M \models_\nu \varphi$, is defined as usual by considering the meaning of the equality predicate, Boolean constants and connectives. A formula φ in $Sen_F(V)$ is valid if and only if for all interpretations $\nu : V \to M$, $M \models_\nu \varphi$. In the sequel, data signature (S, F) and F-model M are supposed given.

3 Programs and contracts

Programs. User-defined functions, called *programs*, are identifiers provided with an interface specifying their formal parameters used to store input and output data. We only consider here programs with no side effect and one output variable.

Definition 1 (Program). *Let $X = \coprod_{s\in S} X_s$ be a set of typed variables. A program over X is an identifier p provided with:*

- *a list* $InOut(p) = (x_1, \cdots, x_{n+1}) \in X^{n+1}$*, called the* interface *of* p*, with* $n \geq 1$ *and* $\forall i \neq j, x_i \neq x_j$*.* $In(p)$ *(resp.* $Out(p)$*) denotes the list* $(x_1 \cdots x_n)$ *(resp.* (x_{n+1})*) of* input (resp. output) formal parameters *of* p*.*
- *and a mapping* $Sem : M^{\{\!|In(p)|\!\}} \to M^{\{\!|InOut(p)|\!\}}$*, called the* semantics *of* p*, verifying the so-called* semantic condition*:*
  $\forall \nu \in M^{\{\!|In(p)|\!\}}, \forall x_j \in \{\!|In(p)|\!\}, Sem(\nu)(x_j) = \nu(x_j)$.

Depending on the values associated to $In(p)$ through the interpretation ν, Sem associates a value to the formal parameter x_{n+1} in $Out(p)$. The semantic condition ensures that a program call has no effect on its input formal parameters. By extrapolation, given a list $l = (x_1, \cdots, x_{n+1})$, $In(l)$ and $Out(l)$ will resp. denote $(x_1, \cdots, x_n)$ and (x_{n+1}).

A *signature* Σ is a tuple (S, F, X, P) where (S, F) is a data signature and P is a set of programs defined over the set of typed variables X.

Let $V = \coprod_{s \in S} V$ be a set of typed variables. The set $T_\Sigma(V) = \coprod_{s \in S} T_\Sigma(V)_s$ of *typed terms* over V contains:

- all functional terms of $T_F(V)$
- all elements $p(t_1, \cdots, t_n)$ with $p \in P$ of interface $(x_1, \cdots, x_{n+1})$, $\forall 1 \leq i \leq n, x_i \in X_{s_i}$, and $t_i \in T_F(V)_{s_i}$. If $x_{n+1} \in V_s$, $p(t_1, \cdots, t_n) \in T_\Sigma(V)_s$.

Any interpretation $\nu : V \to M$ can be canonically extended on $T_\Sigma(V)$ as follows: for any program p in P defined by its interface $(x_1 \cdots x_{n+1})$ and its semantics Sem_p, let us consider $\mu^p_\nu : \{\!|In(p)|\!\} \to M$ an interpretation such that $\forall 1 \leq i \leq n,\ \mu^p_\nu(x_i) = \nu(t_i)$, we have $\nu(p(t_1, \cdots, t_n)) = Sem_p(\mu^p_\nu)(x_{n+1})$.

Contracts. Contracts specify what programs are expected to compute, as opposed to how they compute their result. They have been introduced in the pioneering work of Floyd [9] and Hoare [11], and form a key ingredient of the Eiffel programming language [17]. In short, a contract describes what a program requires from its caller (the pre-condition) and what it guarantees when it returns (the post-condition). We use here a slightly refined notion where a contract can be split in a set of behaviors [2, 4]. In this setting, pre-condition of a behavior indicates a possible case in which the program may be executed. As before, when a behavior is active, its post-condition must hold at the end of the execution.

Most of the times, pre and post conditions of a program are simply formulas in resp. $Sen_F(\{\!|In(p)|\!\})$ and $Sen_F(\{\!|InOut(p)|\!\})$. However, contracts can involve other variables representing the global state of the system. The latter will be frozen variables whose associated values are conditioned by axioms and cannot be modified. These variables will be useful for inferring contracts from symbolic execution tree, as shown in Section 6.2.

Definition 2 (Program contract). *Let* $l = (x_1, \ldots, x_{n+1})$ *be a list of variables with* $\forall i \leq n+1, x_i \in X$*. Let* W *be a subset of frozen variables verifying* $X \cap W = \emptyset$*. A program contract for* l *and* W *is a set:*

$$\{(Pre_1, Post_1), \ldots, (Pre_k, Post_k)\}$$

such that $\forall\ i \leq k$, $Pre_i \in Sen_F(\{\!|In(l)|\!\} \cup W)$ *and* $Post_i \in Sen_F(\{\!|l|\!\} \cup W)$.

A program contract is said to be:

- disjoint *if for all* $i, j \leq k$ *with* $i \neq j$, *the formula* $\neg(Pre_i \wedge Pre_j)$ *is valid.*
- complete *if the formula* $\bigvee_{i \leq k} Pre_i$ *is valid.*

Disjointness requires that at most one behavior of the contract is applicable for any considered input data, *i.e.* the pre-conditions are mutually exclusive. For simplicity purpose, we only consider disjoint contracts in this paper. Completeness indicates that for any input at least one behavior is applicable. In practice, programs are often partially defined over their input domain. We thus allow incomplete contracts, rejecting input data outside the scope of preconditions.

Example 1. Let us consider a program *Price* of interface (x_1, x_2) where x_1 is of type *Drink*, an enumerated type with two values $\{0, 1\}$ and x_2 is of type *Integer*. x_1 is the input parameter indicating the selected beverage and x_2 is the output parameter corresponding to its price. An example of contract for *Price* is $C_r = \{(Pre_1, Post_1), (Pre_2, Post_2)\}$ (both disjoint and complete), with:

- $Pre_1 :\ x_1 = 0$, $Post_1 :\ x_2 \geq 100 \wedge x_2 \leq 200$
- $Pre_2 :\ x_1 = 1$, $Post_2 :\ x_2 \geq 200 \wedge x_2 \leq 300$

Definition 3 (Contract satisfaction). *Let* $l = (x_1, \cdots, x_{n+1})$ *be an interface,* W *a set of frozen variables provided with* $Ax \subseteq Sen_F(W)$ *and* C *a contract for* l *and* W. *Let us consider an interpretation* $\nu \in M^W$ *such that* $M \models_\nu Ax$ *and a mapping* $Sem : M^{\{\!|In(l)|\!\}} \rightarrow M^{\{\!|l|\!\}}$ *satisfying the semantic condition.*

Sem satisfies C *up to* ν, *denoted* $Sem \models_\nu C$, *if and only if:*

$$\forall (Pre, Post) \in C, \forall \mu \in M^{\{\!|In(l)|\!\}}, M \models_{\nu \cup \mu} Pre \Rightarrow M \models_{\nu \cup Sem(\mu)} Post$$

$Sem_\nu(C) = \{Sem : M^{\{\!|In(l)|\!\}} \rightarrow M^{\{\!|l|\!\}} \mid Sem \models_\nu C\}$ *denotes the set of semantics satisfying* C *up to* ν.

For each interface l, we consider the trivial contract $C_{\emptyset,l} = \{\}$, simply denoted $C_\emptyset$, defined on l that does not restrict behaviors of programs, that is $p \in Sem(C_\emptyset)$ for all programs p of interface l. Similarly, we consider the contract $C_{\top,l} = \{(\top, \top)\}$, simply denoted $C_\top$, defined on l that requires that the program is defined for every well-typed input data tuple.

Given a signature $\Sigma = (S, F, X, P)$, a set of frozen variables W with its set of axioms $Ax \subseteq Sen_F(W)$, and an interpretation $\nu \in M^W$ verifying $M \models_\nu Ax$, we consider families $\mathbb{C} = (C_p)_{p \in P}$ of contracts indexed by P, in particular $\mathbb{C}_\emptyset = (C_\emptyset)_{p \in P}$ and $\mathbb{C}_\top = (C_\top)_{p \in P}$. $Mod_\nu(\mathbb{C})$ is the set of all families $\mathcal{S}em = (Sem_p)_{p \in P}$ such that $\forall p \in P, Sem_p \models_\nu C_p$. $\mathcal{S}em$ is then called a *P-model.*

4 IOSTS

Input Output Symbolic Transition Systems (IOSTS) represent behaviors of reactive systems as sequences of emissions or receptions of values through communication channels conditioned by guards expressed on some attribute values.

An *IOSTS-signature* Γ is a couple (A, Ch), where $A = \coprod_{s \in S} A_s$ is a set of types variables, called *attribute variables*, such that for all s in S, $A_s \cap X_s = \emptyset$ and where Ch is a set of *communication channel names*.

An IOSTS communicates with its environment through communication actions. The set of *symbolic actions* over Γ, denoted $Act(\Gamma)$, is $I(\Gamma) \cup O(\Gamma) \cup \{\tau\}$ where: $I(\Gamma) = \{c?x | x \in A, c \in Ch\}$ is the set of inputs, $O(\Gamma) = \{c!t | t \in T_\Sigma(A), c \in Ch\}$ is the set of outputs and τ is an internal action.

Values of attribute variables can be modified in two ways: by receiving a value from the environment or by assigning a value from some internal process.

Definition 4 (IOSTS). *An IOSTS (Q, q_0, Tr) over Σ and $\Gamma = (A, Ch)$ is a triple where Q is a set of states, $q_0 \in Q$ is the initial state and $Tr \subseteq Q \times Sen_F(A) \times Act(\Gamma) \times T_\Sigma(A)^A \times Q$ is a set of transitions tr of the form (q, ψ, act, ρ, q') where:*

- *q and q' are resp. the source ($source(tr)$) and target state ($target(tr)$) of tr,*
- *$\psi \in Sen_F(A)$ is a* guard
- *$act \in Act(\Gamma)$ is a communication action;*
- *$\rho \in T_\Sigma(A)^A$ is a substitution associating a term to attribute variables;*

Remark 1. We can always consider an IOSTS in which guards only contain conjunctions. If not, for a transition tr of guard ψ, it suffices to use a disjunctive normal form $\bigvee_{i=1}^{n} \psi_i$ equivalent to ψ and to split the transition into n transitions having the same source, target and communication action as tr and ψ_i as guard.

Example 2 (Drink vending machine). We consider a very simple drink vending machine. Its behavior is specified by the IOSTS in Fig. 4. An initialization step $(q \to q_0)$ sets the amount to zero. Then, in q_0, the machine waits for an amount (x) of *coins* introduced by the user, and updates the amount m. The user then chooses his/her beverage (0 or 1 for "Tea" or "Coffee"). The choice is stored in variable B. In the transition $q_2 \to q_3$, the program $Price$ computes the price of the chosen drink. Two cases are possible here. If the introduced amount is lower than the price $(m < p)$, then a message "Add" appears on the screen and the machine returns to q_0. Otherwise $(m \geq p)$, the drink is delivered, the amount is reinitialized to zero and the machine goes back to q_0. Note that transitions outgoing from q_3 constrain the value (p) computed by $Price$ $(p \geq 150 \wedge p \leq 200)$.

For a transition $tr = (q, \psi, act, \rho, q') \in Tr$ and a P-model $\mathcal{S}em$, the semantics of tr, denoted as $Run(tr, \mathcal{S}em) \subseteq M^A \times Act^M(\Gamma) \times M^A$, is defined as the set of triple (ν_i, act_M, ν_f) verifying:

- if act is of the form $c!t$ (*resp.* τ), then $M \models_{\nu_i} \psi$, $\nu_f = \nu_i \circ \rho$ and $act_M = c!\nu_i(t)$ (*resp.* $act_M = \tau$)
- if act is of the form $c?x$, then $M \models_{\nu_i} \psi$, there exists ν_a such that $\nu_a(z) = \nu_i(z)$ for every $z \neq x$, $\nu_f = \nu_a \circ \rho$ and $act_M = c?\nu_a(x)$,

Note that the definition of semantics of transitions is very classical and does not explicitly refers to $\mathcal{S}em$. In fact, semantics of programs are taken into account when defining ν_f from the extensions of ν_i or ν_a to $T_\Sigma(A)$ as defined in Section 3.

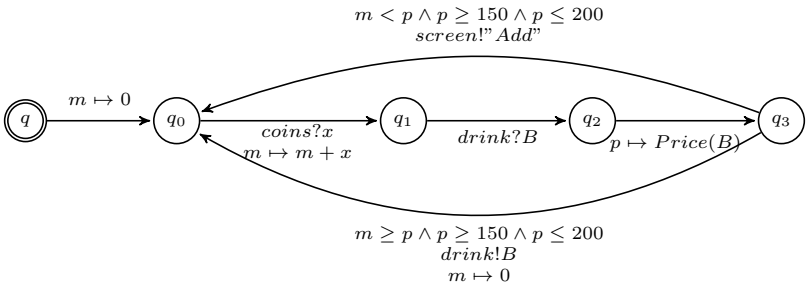

Fig. 1: IOSTS of the drink vending machine.

For a run $r = (\nu_i, act_M, \nu_f)$, we note $source(r)$, $act(r)$ and $target(r)$ resp. for ν_i, act_M and ν_f. ν_i and ν_f are the interpretation of attribute variables resp. before and after executing the transition. Let us observe that, given a transition tr and an interpretation ν_i, the set $Run(tr, \mathcal{S}em)$ does not necessarily contain a run of the form (ν_i, act_M, ν_f) due to the fact that ν_i may not satisfy ψ.

The set of paths of an IOSTS $\mathbb{G} = (Q, q_0, Tr)$, denoted $Path(\mathbb{G})$, are all finite sequences $tr_1.\cdots.tr_n$ of transitions with $source(tr_1) = q_0$ and $\forall i, 1 \leq i < n$, $target(tr_i) = source(tr_{i+1})$. The set of runs of a path $pa = tr_1.\cdots.tr_n$ in $Path(\mathbb{G})$, denoted as $Run(pa, \mathcal{S}em)$, are sequences $r_1.\cdots.r_n$ such that $\forall i \leq n$, $r_i \in Run(tr_i, \mathcal{S}em)$ and $\forall i < n$, $target(r_i) = source(r_{i+1})$. Similarly, the set of traces $Traces(pa, \mathcal{S}em)$ of pa is the set of sequences $act(r_1).\cdots.act(r_n)$ for all $r_1.\cdots.r_n \in Run(pa, \mathcal{S}em)$, $act(r)$ being equal to ε if $act(r) = \tau$.

In general, it is not guaranteed that there exists at least a run for a given path pa, as it depends on the semantics associated to programs involved in pa.

Definition 5 (Path feasibility condition). *Let $\mathbb{G} = (Q, q_0, Tr)$ be an IOSTS over $\Gamma = (A, Ch)$ and pa a path of $\mathbb{G}$. pa is a* feasible path *if and only if:*

$$\exists\ \mathcal{S}em \in Mod(\mathbb{C}_\emptyset), Traces(pa, \mathcal{S}em) \neq \emptyset$$

Let W be a set of frozen variables provided with $Ax \subseteq Sen_F(W)$ and $\nu \in M^W$ an interpretation satisfying $M \models_\nu Ax$. Let us consider $\mathbb{C} = (C_p)_{p \in P}$ a family of contracts indexed by P. pa is a feasible path *up to $(\nu, \mathbb{C})$ if and only if:*

$$\exists \mathcal{S}em \in Mod_\nu(\mathbb{C}), Traces(pa, \mathcal{S}em) \neq \emptyset$$

5 Symbolic Execution and path feasibility condition

Symbolic execution consists in executing an IOSTS for symbolic values (taken from a dedicated set of frozen variables $Fr = \coprod_{s \in S} Fr_s$) rather than numerical

ones, and computing constraints on those values for all possible IOSTS executions. The main novelties with respect to [10] are twofold: substitutions occurring in transitions may include program calls and a renaming mechanism ensures that a given frozen variable can not appear in two distinct paths.

To store information concerning an execution, we use structures called symbolic states. A *symbolic state* is a tuple of the form $(q, \pi, \lambda, \kappa)$ where $q \in Q$, $\pi \in Sen_F(Fr)$, $\lambda : A \to T_F(Fr)$ is an application preserving types and $\kappa \subset P \times T_F(Fr)^* \times Fr$. For a symbolic state $\eta = (q, \pi, \lambda, \kappa)$, q (or $q(\eta)$) denotes the state reached after an execution leading to η, π (or $\pi(\eta)$) is a constraint on variables in Fr called *path condition* that should be satisfied for the execution to reach η, λ (or $\lambda(\eta)$) denotes terms over variables in Fr that are assigned to variables of A and κ (or $\kappa(\eta)$) denotes the set of tuples of the form $(p, (t_1, \cdots, t_n), x)$ indicating that a program call has been performed for the program p with the arguments $(t_1, \cdots, t_n)$ and that its result is stored in the variable x in Fr.

In our approach we do not have the code of programs. Instead, we reason on their contracts. Since the input formal parameters associated to a call are represented symbolically by functional terms $t_1, \cdots, t_n$, different pre-conditions may hold depending on the way those terms will be interpreted. At the symbolic execution level, we thus consider a sub-case for each of those pre-conditions. More precisely, the symbolic execution of a transition tr from a given symbolic state η will consist in a set of symbolic transitions, one for each possible combination of pre-conditions for all program calls occurring in tr. We now introduce some notations aiming at tracing program calls: for a substitution $\rho : A \to T_\Sigma(A)$ and for $p \in P$, $Res(p, \rho)$ is the set of variables $y \in A$ such that $\rho(y)$ is of the form $p(t_1, \cdots, t_n)$ and for such an y, $Arg(y, \rho)$ is then $(t_1, \cdots, t_n)$ and $Prog(y, \rho) = p$. We also denote $Res(\rho)$ for $\bigcup_{p \in P} Res(p, \rho)$.

Definition 6 (Symbolic execution of transitions). *Let $\mathbb{G} = (Q, q_0, Tr)$ be an IOSTS over Σ and $\Gamma = (A, Ch)$, $tr = (q, \psi, act, \rho, q') \in Tr$ be a transition and $\eta = (q, \pi, \lambda, \kappa)$ be a symbolic state over $\mathbb{G}$.*

If act is of the form $c?x$, $\lambda_i = \lambda[x \mapsto f]$, f fresh in Fr. Otherwise, $\lambda_i = \lambda$.

λ' is the substitution such that for all $y \in Res(\rho)$, $\lambda'(y)$ is a fresh variable of Fr and for all $y \in A \setminus Res(\rho)$, $\lambda'(y) = \lambda_i \circ \rho(y)$.

The symbolic execution *$SE(tr, \eta)$ of tr from η is the set defined as follows:*

- *if $Res(\rho) = \emptyset$ then $SE(tr, \eta) = \{(\eta, \lambda_i(act), \eta')\}$ with $\eta' = (q', \pi \wedge \lambda(\psi), \lambda', \kappa)$.*
- *if $Res(\rho) \neq \emptyset$, for any mapping $Beh : Res(\rho) \to \bigcup_{p \in P} C_p$ such that for $y \in Res(p, \rho)$, $Beh(y) = (Pre_y, Post_y) \in C_p$.*
  For $y \in Res(p, \rho)$ with $InOut(p) = (x_1, \cdots, x_n, x_{n+1})$ and $Arg(y, \rho) = (t_1, \cdots, t_n)$, we have $(\eta, \lambda_i(act), \eta') \in SE(tr, \eta)$ with
  - *η' the symbolic state $(q', \pi \wedge \lambda(\psi) \wedge \bigwedge_{y \in Res(\rho)} \Delta(y), \lambda', \kappa')$*
  - *$\Delta(y) = (Pre_y \wedge Post_y)[x_1 \mapsto \lambda_i(t_1) \cdots x_n \mapsto \lambda_i(t_n), x_{n+1} \mapsto \lambda'(x)]$*
  - *κ' the set $\kappa \cup \bigcup_{y \in Res(\rho)} \{(Prog(y, \rho), (\lambda_i(t_1), \cdots, \lambda_i(t_n)), \lambda'(y))\}$*

Elements of $SE(tr, \eta)$ are called symbolic transitions. *We denote $Fr(\eta')$ the set of all fresh variables of Fr occurring in its definition.*

Example 3. In order to illustrate Definition 6, let us consider a transition tr of the form $(q, \psi, c?x, \rho, q')$ with $\rho = [y \mapsto p_1(t_1, t_2), z \mapsto t'_1 + t'_2]$ with p_1 a program and t_1, t_2, t'_1, t'_2 functional terms. Let us observe that $Res(p_1, \rho) = \{y\}$, $Arg(y, p_1) = (t_1, t_2)$, $Prog(y, \rho) = p_1$ and $Res(\rho) = \{y\}$.

Let $\eta = (q, \pi, \lambda, \kappa)$ be a symbolic state. Let us suppose that the program p_1 is provided with an interface (x_1, x_2, x_3) and with a behavior $(Pre_1, Post_1)$. Then $SE(tr, \eta)$ contains the symbolic transition $(\eta, c?f_1, \eta')$ with f_1 a fresh variable of Fr and η' the symbolic state defined as:

$$
\begin{array}{l}
(\ q',\\
\quad \pi \wedge \lambda(\psi) \wedge (Pre_1 \wedge Post_1)[x_1 \mapsto \lambda[x \mapsto f_1](t_1), x_2 \mapsto \lambda[x \mapsto f_1](t_2), x_3 \mapsto f_2]\\
\quad [x \mapsto f_1, y \mapsto f_2, z \mapsto \lambda[x \mapsto f_1](t'_1 + t'_2)],\\
\quad \kappa \cup \{(p_1, (\lambda[x \mapsto f_1](t_1), \lambda[x \mapsto f_1](t_2)), f_2\})
\end{array}
$$

$Fr(\eta')$ is then $\{f_1, f_2\}$.

Definition 7 (IOSTS symbolic execution). *Given an IOSTS $\mathbb{G}$, the symbolic execution $SE(\mathbb{G}) = (Init, ST)$ of $\mathbb{G}$ is minimally defined by:*

- *$Init = (q_0, Ax, \lambda_0)$ with $\forall x \in A, \lambda_0(x) \in Fr$ and $\forall x \neq y \in A, \lambda_0(x) \neq \lambda_0(y)$,*
- *for $tr \in Tr$ and η symbolic state with $source(tr) = q(\eta)$, $SE(tr, \eta) \subseteq ST$.*
- *for any distinct $SE(tr_1, \eta_1)$ $SE(tr_2, \eta_2)$ that are defined, $Fr(SE(tr_1, \eta_1)) \cap Fr(SE(tr_2, \eta_2)) = \emptyset$.*

Definition 8 (Paths and distinguished paths). *The set $Paths(SE(\mathbb{G}))$ of* paths *of $SE(\mathbb{G})$ is the set of all sequences $tr_1 \cdots tr_n$ with $\forall i \in 1..n, tr_i \in ST$ such that $source(tr_1) = Init$ and for any $j < n$, $q(target(tr_j)) = q(source(tr_{j+1}))$.*

For a non-empty sequence $\delta = tr_1 \cdots tr_n$, we note $End(\delta) = target(tr_n)$ and $Fr(\delta) = \cup_{i \in 1..n} Fr(target(tr_i))$. By convention, $End(\varepsilon) = Init$ and $Fr(\varepsilon) = \emptyset$.

Given a finite subset Δ of $Paths(SE(\mathbb{G}))$, $DPaths(\Delta)$ is a set of paths δ^* such that there exists an unique path δ in Δ such that δ and δ^* are isomorphic up to a renaming of variables of Fr and such that for two distinct paths δ_1^* and δ_2^* in $DPaths(\Delta)$, $Fr(\delta_1^*) \cap Fr(\delta_2^*) = \emptyset$.

We say that $DPaths(\Delta)$ is a set of distinguished *paths issued from $SE(\mathbb{G})$.*

Generally speaking, a set Δ of $Paths(SE(\mathbb{G}))$ represents a tree whose transitions issued from the root $Init$ can be shared by several paths of Δ while $DPaths(\Delta)$ consists in applying a variable renaming mechanism in order to duplicate shared transitions to completely separate paths. Distinguished paths can still share common variables, namely those in W.

Example 4. The drink vending machine of Fig. 4 has two possible paths from q to q_0 with exactly one cycle on q_0. They share a transition with a call to program *Price* defined by its contract C_r as seen in Ex. 1. We thus get 4 distinguished paths shown in Fig. 5. Associated path conditions are the following:

$$
\begin{array}{l}
pc_1 : B_1 = 0 \wedge p_1 \geq 100 \wedge p_1 \leq 200 \wedge v_1 < p_1 \wedge p_1 \geq 150 \wedge p_1 \leq 200\\
pc_2 : B_2 = 0 \wedge p_2 \geq 100 \wedge p_2 \leq 200 \wedge v_2 \geq p_2 \wedge p_2 \geq 150 \wedge p_2 \leq 200\\
pc_3 : B_3 = 1 \wedge p_3 \geq 200 \wedge p_3 \leq 300 \wedge v_3 < p_3 \wedge p_3 \geq 150 \wedge p_3 \leq 200\\
pc_4 : B_4 = 1 \wedge p_4 \geq 200 \wedge p_4 \leq 300 \wedge v_4 \geq p_4 \wedge p_4 \geq 150 \wedge p_4 \leq 200
\end{array}
$$

$Init_1$	$Init_2$	$Init_3$	$Init_4$
$\downarrow \tau$	$\downarrow \tau$	$\downarrow \tau$	$\downarrow \tau$
η_1^1	η_1^2	η_1^3	η_1^4
$\downarrow coins?v_1$	$\downarrow coins?v_2$	$\downarrow coins?v_3$	$\downarrow coins?v_4$
η_2^1	η_2^2	η_2^3	η_2^4
$\downarrow drink?B_1$	$\downarrow drink?B_2$	$\downarrow drink?B_3$	$\downarrow drink?B_4$
η_3^1	η_3^2	η_3^3	η_3^4
$\downarrow \tau$	$\downarrow \tau$	$\downarrow \tau$	$\downarrow \tau$
η_4^1	η_4^2	η_4^3	η_4^4
$\downarrow screen!"Add"$	$\downarrow drink!B_2$	$\downarrow screen!"Add"$	$\downarrow drink!B_4$
η_5^1	η_5^2	η_5^3	η_5^4

Fig. 2: Symbolic paths.

A path condition is a formula over the frozen variables built by accumulating constraints from the guards of the IOSTS transitions and from constraints of called programs contracts. The path is infeasible if its path condition is not satisfiable. In addition, this feasibility depends on the fact that if a program is called twice with the same arguments, it returns the same value (semantic condition of Definition 1). Since this is not enforced by the path condition alone, we consider another set of constraints accounting for this condition:

Definition 9 (Feasibility of a set of paths). *Let $\mathbb{G}$ be an IOSTS over $\Gamma = (A, Ch)$ and let Δ^* be a set of distinguished paths issued from $SE(\mathbb{G})$.*

For any program p of interface $(x_1, \cdots, x_n, x_{n+1})$, for $(p, (t_1, \cdots, t_n), f)$ and $(p, (t'_1, \cdots, t'_n), f')$ two distinct elements of $\cup_{\delta^* \in \Delta^*} \kappa(End(\delta^*))$ we introduce the deterministic program condition *relating to these two program calls as the formula $\phi_{\{f,f'\}}$ defined by $\bigwedge_{i=1}^{n} t_i = t'_i \Rightarrow f = f'$.*

The deterministic program condition *related to Δ^* is then $\Phi_p = \bigwedge \phi_{\{f,f'\}}$, for all f and f' appearing as return variable of a call of p in Δ^*.*

Finally, the feasibility condition of Δ^* *is*

$$\bigwedge_{\delta^* \in \Delta^*} \pi(End(\delta^*)) \wedge \bigwedge_{p \in P} \Phi_p$$

If this feasibility condition holds, it is possible to implement the programs occurring in the IOSTS so that all paths of Δ^* will complete successfully. Note that the contracts of the programs are taken into account in the path condition, and have thus an impact on the paths that are feasible or not.

Example 5. In the context of the drink vending machine, we now want to check the feasibility condition of the distinguished paths associated to the paths described in Ex. 4 according to two distinct contracts for *Price*, denoted resp. C_w and C_r (in Example 1). Both C_w and C_r include two behaviors resulting in 4 distinguished paths. Path conditions are given in Tab. 2.

- With the contract C_w, no distinguished path is feasible because of contradictions between guards of the IOSTS transitions and post-conditions of C_w.
- With the contract C_r, all distinguished paths are feasible. *Price* can return anything between 150 and 200 for an argument equal to 0 and must return 200 for an argument equal to 1.

$C_w : \{(x_1 = 0, x_2 \geq 0 \wedge x_2 \leq 100), (x_1 = 1, x_2 \geq 250)\}$	$C_r : \{(x_1 = 0, x_2 \geq 100 \wedge x_2 \leq 200), (x_1 = 1, x_2 \geq 200 \wedge x_2 \leq 300)\}$
$pc_1 : B_1 = 0 \wedge p_1 \geq 0 \wedge p_1 \leq 100 \wedge v_1 < p_1 \wedge p_1 \geq 150 \wedge p_1 \leq 200$	$pc_1 : B_1 = 0 \wedge p_1 \geq 100 \wedge p_1 \leq 200 \wedge v_1 < p_1 \wedge p_1 \geq 150 \wedge p_1 \leq 200$
$pc_2 : B_2 = 0 \wedge p_2 \geq 0 \wedge p_2 \leq 100 \wedge v_2 \geq p_2 \wedge p_2 \geq 150 \wedge p_2 \leq 200$	$pc_2 : B_2 = 0 \wedge p_2 \geq 100 \wedge p_2 \leq 200 \wedge v_2 \geq p_2 \wedge p_2 \geq 150 \wedge p_2 \leq 200$
$pc_3 : B_3 = 1 \wedge p_3 \geq 250 \wedge v_3 < p_3 \wedge p_3 \geq 150 \wedge p_3 \leq 200$	$pc_3 : B_3 = 1 \wedge p_3 \geq 200 \wedge p_3 \leq 300 \wedge v_3 < p_3 \wedge p_3 \geq 150 \wedge p_3 \leq 200$
$pc_4 : B_4 = 1 \wedge p_4 \geq 250 \wedge v_4 \geq p_4 \wedge p_4 \geq 150 \wedge p_4 \leq 200$	$pc_4 : B_4 = 1 \wedge p_4 \geq 200 \wedge p_4 \leq 300 \wedge v_4 \geq p_4 \wedge p_4 \geq 150 \wedge p_4 \leq 200$
$\phi_{\{p_1,p_2\}} : B_1 = B_2 \Rightarrow p_1 = p_2$	$\phi_{\{p_1,p_2\}} : B_1 = B_2 \Rightarrow p_1 = p_2$
$\phi_{\{p_1,p_3\}} : B_1 = B_3 \Rightarrow p_1 = p_3$	$\phi_{\{p_1,p_3\}} : B_1 = B_3 \Rightarrow p_1 = p_3$
$\phi_{\{p_1,p_4\}} : B_1 = B_4 \Rightarrow p_1 = p_4$	$\phi_{\{p_1,p_4\}} : B_1 = B_4 \Rightarrow p_1 = p_4$
$\phi_{\{p_2,p_3\}} : B_2 = B_3 \Rightarrow p_2 = p_3$	$\phi_{\{p_2,p_3\}} : B_2 = B_3 \Rightarrow p_2 = p_3$
$\phi_{\{p_2,p_4\}} : B_2 = B_4 \Rightarrow p_2 = p_4$	$\phi_{\{p_2,p_4\}} : B_2 = B_4 \Rightarrow p_2 = p_4$
$\phi_{\{p_3,p_4\}} : B_3 = B_4 \Rightarrow p_3 = p_4$	$\phi_{\{p_3,p_4\}} : B_3 = B_4 \Rightarrow p_3 = p_4$
Feasibility: No	Feasibility: Yes

Table 1: Feasibility according to different contracts

6 Testing

6.1 Model-based testing of IOSTS with program calls and contracts

In a previous work [10], we have proposed an online testing algorithm to test Systems Under Test (SUT) with respect to a basic IOSTS (without program calls). The algorithm is based on the *ioco* conformance relation [20] and on the use of test purposes (TP) to select some behaviors to be tested. A TP is a finite sub-tree of the symbolic execution structure (SES) derived from the IOSTS of reference so that any execution trace constructed by interacting with SUT and leading to a leaf of TP will be considered as covering TP. The testing process is implemented as a simultaneous traversal of both SES and TP. Verdicts depend on whether the observed execution trace does or does not belong to TP and SES: $WeakPASS$ when the execution trace covers TP and belongs to at least one path of SES which does not end at a leaf of TP, $PASS$ when the execution trace covers TP and does not belong to another path of SES, $INCONC$ (for inconclusive) when the execution trace belongs to SES but does not cover TP, $FAIL$ when the execution trace does not cover TP and goes outside SES.

In Section 5, we have associated to any IOSTS with contracts a symbolic tree structure in order to be able to use it both as the SES input of the algorithm given in [10] and as a carrier to extract a finite sub-tree to play the role of TP. We can use the work described in [10] with the following slight modifications:

– Unlike [10], we allow unobservable τ transitions. Under the assumption that there does not exist a cycle of τ transitions, we can replace any sequence of consecutive τ transitions by a transition carrying the input/output action just located at the end of the τ sequence. Furthermore, in [10], quiescence

conditions are expressed by enriching the reference IOSTS with transitions carrying the special label δ denoting the intended absence of reaction. Because the presence of τ transitions makes such a direct enrichment tricky, it becomes more appropriate to perform this enrichment at the level of the τ-reduced symbolic execution itself. Once the operations of τ-reduction and δ-enrichment are applied to the symbolic execution of the IOSTS with contracts, we can then apply the algorithm of [10] for free.
- In [10], path conditions for paths that are part of test purposes are satisfiable by construction. In our setting, we have to take into account the notion of feasibility, i.e, the existence or not of programs that meet their associated contracts and that are compatible with considered paths. Indeed, if the considered set of distinguished paths constituting the test purpose is unfeasible, then the application of algorithm is meaningless. In other words, the feasibility of the targeted set of paths plays the role of a testing hypothesis.

6.2 Contracts Inference

As we have seen in Section 5, the feasibility condition checks whether a given program contract preserves the feasibility of a symbolic path or not. In this section, we focus on the inference of contracts based on path conditions. Such contracts can then be used to define unit tests for the programs. More precisely, we start with an IOSTS $\mathbb{G}$ calling programs without associated contract. We then show that we can infer contracts such that feasible paths of $\mathbb{G}$ are guaranteed to verify the feasibility condition of the IOSTS augmented with contracts. The generated contract for a program p contains one behavior per call to p in $SE(\mathbb{G})$. For that, we use the parts of the final condition of the path on which the call occurs that are related to the return variable and to the arguments.

Given a formula F, we define inductively the set $Rel_F(X)$ of variables related to a set X of variables, as the smallest set satisfying the following conditions

- $X \subset Rel_F(X)$
- $Occ(t_1 = t_2) \cap Rel_{t_1=t_2}(X) \neq \emptyset \Rightarrow Occ(t_1 = t_2) \subset Rel_{t_1=t_2}(X)$
- $Rel_{F_1}(X) \cup Rel_{F_2}(X) = Rel_{F_1 \wedge F_2}(X) = Rel_{F_1 \vee F_2}(X)$
- $Rel_F(X) = Rel_{\neg F}(X)$

Similarly, for a formula F and a set of variables X, $Clean_X(F)$ is defined as follows. As noted in remark 1, we can assume that the path condition only has conjunctions, and is in negation-normal form.

- $Clean_X(\top) = \top$
- $Clean_X(\bot) = \bot$
- $Clean_X(t_1 = t_2) = t_1 = t_2$ if $Occ(t_1 = t_2) \cap X \neq \emptyset$
- $Clean_X(t_1 = t_2) = \top$ if $Occ(t_1 = t_2) \cap X = \emptyset$
- $Clean_X(\neg t_1 = t_2) = \neg t_1 = t_2$ if $Occ(t_1 = t_2) \cap X \neq \emptyset$
- $Clean_X(\neg t_1 = t_2) = \top$ if $Occ(t_1 = t_2) \cap X = \emptyset$
- $Clean_X(F_1 \wedge F_2) = Clean_X(F_1) \wedge Clean_X(F_2)$

Remark 2. If F is satisfiable, then $Clean_X(F)$ is also satisfiable, as we only remove atomic propositions from the conjunction.

Definition 10 (Contract inference). *Let $\mathbb{G}$ be an IOSTS , Δ^* a set of distinguished paths from $SE(\mathbb{G})$. We note $\kappa(\Delta^*) = \cup_{\delta^* \in \Delta^*} \kappa(End(\delta^*))$.*

For any f such that $(p, (t_1, \cdots, t_n), f) \in \kappa(\Delta^*)$, with $In(p) = (x_1, ..., x_n)$ and $Out(p) = x_{n+1}$, we define a behavior $(Pre_f, Post_f)$ for p, as well as a set of frozen variables G_f and axioms Ax_f.

We pose $\phi = \pi(End(\delta^*))$ the final condition for the path containing the call and $Y = Occ(t_1, \cdots, t_n) \cup \{f\}$ the variables occurring in the call. Then

- *G_f is $Rel_\phi(Y)$*
- *Ax_f is $Clean_{Rel_\phi(Y)}(\phi)$*
- *Pre_f is $\bigwedge_{i=1}^{n} x_i = t_i$*
- *$Post_f$ is $x_{n+1} = f$*

Finally, the inferred contracts for Δ^* are defined as follows.

- *G is $\bigcup_{(p,(t_1,\cdots,t_n),f) \in \kappa(\Delta^*)} G_f$*
- *Ax is $\bigwedge_{(p,(t_1,\cdots,t_n),f) \in \kappa(\Delta^*)} Ax_f$*
- *$\forall p \in P, C_p = ((Pre_f, Post_f))_{(p,(t_1,\cdots,t_n),f) \in \kappa(\Delta^*)}$*

Example 6. Let us consider here a symbolic path δ^* of our drink vending machine's specification (Figure 6) that calls twice the program *Price* of interface (x_1, x_2). The first call leads to the appearance of a message "Add" on the screen and the second call permits the drink delivery, such that:
$\pi(End(\delta^*)) : v_1 < p_1 \wedge p_1 \geq 150 \wedge p_1 \leq 200 \wedge (v_1 + v_2) \geq p_2 \wedge p_2 \geq 150 \wedge p_2 \leq 200$

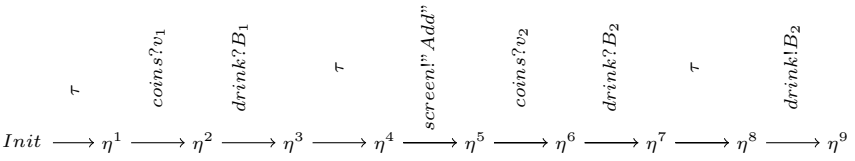

Fig. 3: Symbolic path.

From the path condition $\phi = \pi(End(\delta^*))$, two behaviors will be generated according to Def. 10. For p_1 the result of the first call $(Price, (B_1), p_1)$ we have:

$$
\begin{aligned}
Y &: \{B_1, p_1\} \\
G_{p_1} &: \{B_1, p_1, v_1, p_2, v_2\} \\
Ax_{p_1} &: v_1 < p_1 \wedge p_1 \geq 150 \wedge p_1 \leq 200 \wedge (v_1 + v_2) \geq p_2 \wedge p_2 \geq 150 \wedge p_2 \leq 200 \\
Pre_{p_1} &: x_1 = B_1 \\
Post_{p_1} &: x_2 = p_1
\end{aligned}
$$

For p_2 the result of the second call $(Price, (B_2), p_2)$ we have:

$$\begin{aligned} Y &: \{B_2, p_2\} \\ G_{p_2} &: \{B_2, p_2, v_1, p_1, v_2\} \\ Ax_{p_2} &: v_1 < p_1 \wedge p_1 \geq 150 \wedge p_1 \leq 200 \wedge (v_1 + v_2) \geq p_2 \wedge p_2 \geq 150 \wedge p_2 \leq 200 \\ Pre_{p_2} &: x_1 = B_2 \\ Post_{p_2} &: x_2 = p_2 \end{aligned}$$

Finally, the inferred contract for our program $Price$ in δ^* is:

- $G = G_{p_1} \cup G_{p_2}$
- $Ax = Ax_{p_1} \wedge Ax_{p_2}$
- $C = ((Pre_{p_1}, Post_{p_1}), (Pre_{p_2}, Post_{p_2}))$

We can now define the IOSTS $\mathbb{G}'$ with the same signature and transitions than $\mathbb{G}$ and equipped with the inferred contracts for the programs in P. Then, for every path δ^* in Δ^* that is feasible, there exist paths $\underline{\delta^*}$ in $\mathbb{G}'$ similar to δ^* except that the path conditions π are augmented with axioms and behaviors. For each $(p, (t_1, ..., t_n), f) \in \kappa(End(\delta^*))$, Ax_f is satisfiable by remark 2 and the behavior $(Pre_f, Post_f)$ becomes trivially true: one of the behaviors of p makes the corresponding transition feasible. Since this is true for any call in δ^*, there exists thus a path in $\underline{\delta^*}$ that is feasible. This leads to the following theorem.

Theorem 1 (Feasibility preservation). *Let $\mathbb{G}$ be an IOSTS, Δ^* a set of feasible distinguished symbolic paths of $\mathbb{G}$. $\mathbb{G}'$ is the IOSTS obtained by adding to G the inferred contracts of Definition 10. For any path δ^* in Δ^*, there exists a symbolic path $\delta^{*\prime}$ for $\mathbb{G}'$ having the same transitions as δ^* and which is feasible.*

7 A detailed example of a vending machine with a program call for giving the change

In this section, we consider a more realistic drink vending machine example in order to introduce a rather complex user-defined program. The program call will help us to calculate the giving of change according to the coins inserted by the user and to the machine reserve.

The machine allows the user to order a coffee or a tea and returns money. The machine accepts only three different types of coins: €0.20, €0.50 and €1.

A counter (variable m) is used for calculating the total amount inserted by the user in the machine. According to the drink chosen by the user, as for Example 2, the price of the selected drink is given by the program $Price$ of interface (x_1, x_2) where x_1 is of type $Drink$, an enumerated type with two values $\{0, 1\}$ and x_2 is of type $Integer$. x_1 is the input parameter indicating the selected beverage and x_2 is the output parameter corresponding to its price. An example of contract for $Price$ is $C_r = \{(Pre_1, Post_1), (Pre_2, Post_2)\}$ (two behaviors both disjoint and complete), with:

- $Pre_1 : \ x_1 = 0$, $Post_1 : \ x_2 \geq 100 \wedge x_2 \leq 200$

– $Pre_2 : \ x_1 = 1$, $Post_2 : \ x_2 \geq 200 \wedge x_2 \leq 300$

When the desired amount is inserted, the selected beverage will be delivered to the user. If the inserted amount is more than the beverage's cost and if the reserve contains enough change, the drink will be delivered to the user and the extra change will be returned to him. If the reserve does not contain enough change, the inserted coins will be returned to the user and he/she will be asked to top up the amount. The inserted money is specified as an array C (has three cases $C[0]$, $C[1]$ and $C[2]$) that contains respectively the number of €0.20, €0.50 and €1 coins. More precisely, we consider four such arrays, C for storing the cumulated amount inserted by the user, X for storing the current inserted amount (that the user is likefy to top up if the amount is not sufficient for covering the beverage price), E for storing the giving of change and R for storing the machine reserve.

If the cumulated inserted amount $20{*}C[0]{+}50{*}C[1]{+}100{*}C[2]$ is greater than the cost and the reserve has enough change, then a program *Return* calculates the extra change to be returned to the user as an array (E). The program *Return* of interface (x'_1, x'_2, x'_3, x'_4) where

– x'_1 represents the beverage price (positive integer),
– x'_2 represents the amount (positive integer) ,
– x'_3 represents the reserve (as an array storing separately the number of €0.20, €0.50 and €1 coins),
– and x'_4 is the program output variable (an array that contains the number of different coins to be returned to the user)

We associate with the *Return* program a contract: $(Pre, Post)$ such that:

– Pre: $x'_1 > 0 \wedge x'_2 \geq x'_1$
– Post: $(((x'_4[0]{*}20{+}x'_4[1]{*}50{+}x'_4[2]{*}100) = x'_2{-}x'_1){\wedge}x'_4[0] \leq x'_3[0]{\wedge}x'_4[1] \leq x'_3[1] \wedge x'_4[2] \leq x'_3[2])$.

The contract specifies that under the conditions that the beverage price (x'_1) is strictly positive and that the cumulated inserted amount (x'_2) is greater that the beverage price (x'_1), then the amount $(x'_4[0] * 20 + x'_4[1] * 50 + x'_4[2] * 100)$ represented by the output variable (x'_4) is equal to the difference $(x'_2{-}x'_1)$ and the array variable (x'_4) is less than or equal to the reserve, component by component.

Let us notice than the considered contract cannot be achieved in any situation: in particular, if the difference is equal to 20 and if $x'_3[0]$ is equal to 0, there is no way to give back an array x'_4 making the postcondition true.

The machine's behavior is specified by the IOSTS in Figure 4. An initialization step $(q \to q_0)$ sets C cases and the amount m to zero. Then, in state q_0, the machine waits for coins (X) introduced by the user, updates C and the amount m. The user then chooses his/her beverage (0 or 1 for "Tea" or "Coffee"). The choice is stored in the variable B. In the transition $q_2 \to q_3$, the program *Price* of interface (x_1, x_2) computes the price of the chosen drink. Four cases are possible here:

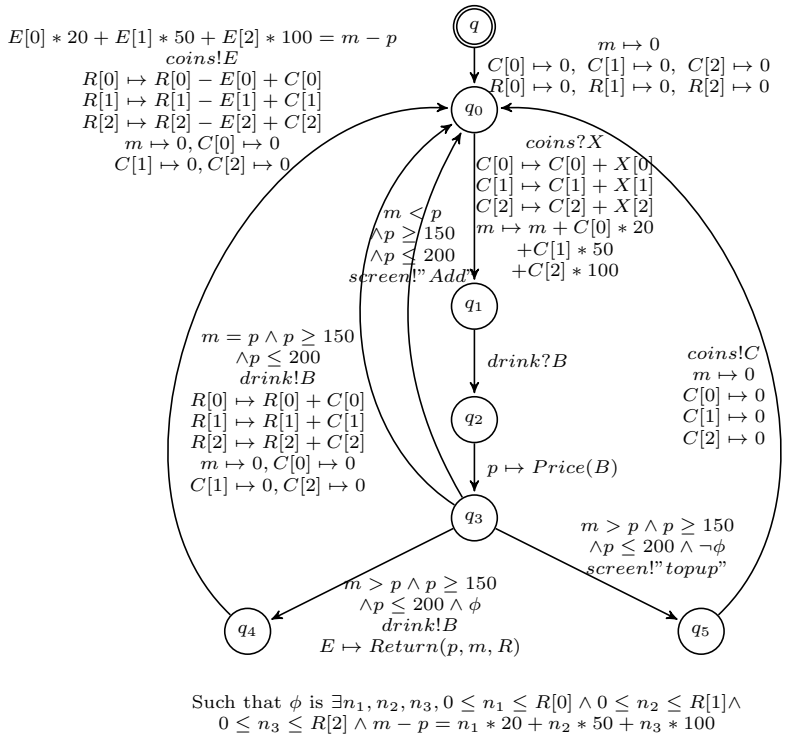

Fig. 4: IOSTS of the drink vending machine.

- If the introduced amount is lower than the price ($m < p$), then a message "Add" appears on the screen and the machine returns to q_0;
- if the user has introduced exactly an amount equal to the price ($m = p$), the drink is delivered, the reserve is updated, the amount and C cases are reinitialized to zero and the machine goes back to q_0;
- if the user has introduced an amount strictly greater than the beverage price and if the reserve has enough change ($m > p \wedge \phi$), then the program *Return* calculates the extra change to be returned to the user and the machine goes to the state q_4 in order to return extra coins, set up the reserve and initialize m and C. The formula ϕ defined as:

$$\exists n_1, n_2, n_3, 0 \leq n_1 \leq R[0] \wedge 0 \leq n_2 \leq R[1] \wedge 0 \leq n_3 \leq R[2] \wedge$$

$$m - p = n_1 * 20 + n_2 * 50 + n_3 * 100$$

specifies that with the current reserve (R), there is at least a possibility of giving the expected change ($m - p$).

– otherwise (the user has introduced an amount strictly greater than the beverage price and the reserve does not permit to return back the extra to the user ($m > p \wedge \neg\phi$)), the user is asked to refill the machine (if possible, with the exact amount) and from the state q_5, the introduced coins are returned to the user.

Note that to be triggered, guards on transitions outgoing from q_3 to q_4 and q_5 contain the ϕ formula that checks the reserve's availability. The ϕ formula expresses that there is at least a combination of coins among the coin reserve that permits to give back to the user a correct change. Note also that the ϕ formula is stronger than the postcondition *Post* previously associated to the program *Return*: in particular, ϕ makes explicit that giving change is possible, without explaining how it is calculated.

7.1 Symbolic execution: distinguished paths

The drink vending machine of Figure 4 has 4 possible paths from the state q to state q_0 with exactly one cycle on q_0, with a common transition ($q_0 \rightarrow q_1$) including a call to the program *Price* defined by its contract C_r that has two behaviors (coffee or tea). The symbolic execution of the *IOSTS* gives rise to a set of 8 distinguished paths. They are shown in Figure 5, taken into account the renaming mechanism ensuring that fresh variables occurring in two distinct paths are distinct.

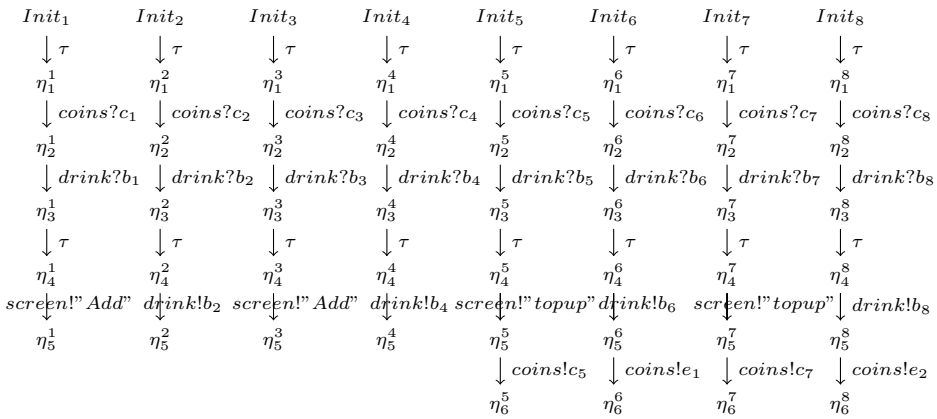

Fig. 5: Symbolic paths.

The associated path conditions are the following:

$pc_1 : b_1 = 0 \wedge p_1 \geq 100 \wedge p_1 \leq 200 \wedge m_1 < p_1 \wedge p_1 \geq 150 \wedge p_1 \leq 200$
$pc_2 : b_2 = 0 \wedge p_2 \geq 100 \wedge p_2 \leq 200 \wedge m_2 = p_2 \wedge p_2 \geq 150 \wedge p_2 \leq 200$
$pc_3 : b_3 = 1 \wedge p_3 \geq 200 \wedge p_3 \leq 300 \wedge m_3 < p_3 \wedge p_3 \geq 150 \wedge p_3 \leq 200$
$pc_4 : b_4 = 1 \wedge p_4 \geq 200 \wedge p_4 \leq 300 \wedge m_4 = p_4 \wedge p_4 \geq 150 \wedge p_4 \leq 200$
$pc_5 : b_5 = 0 \wedge p_5 \geq 100 \wedge p_5 \leq 200 \wedge m_5 > p_5 \wedge \neg(\exists n_1, n_2, n_3 / \ 0 \leq n_1 \leq r_5[0]$
$\wedge 0 \leq n_2 \leq r_5[1] \wedge 0 \leq n_3 \leq r_5[2] \wedge m_5 - p_5 = n_1 * 20 + n_2 * 50 + n_3 * 100)$
$\wedge p_5 \geq 150 \wedge p_5 \leq 200$
$pc_6 : b_6 = 0 \wedge p_6 \geq 100 \wedge p_6 \leq 200 \wedge m_6 > p_6 \wedge \exists n_1, n_2, n_3 / \ 0 \leq n_1 \leq r_6[0]$
$\wedge 0 \leq n_2 \leq r_6[1] \wedge 0 \leq n_3 \leq r_6[2] \wedge m_6 - p_6 = n_1 * 20 + n_2 * 50 + n_3 * 100$
$\wedge p_6 > 0 \wedge m_6 > p_6 \wedge ((e_1[0] * 20 + e_1[1] * 50 + e_1[2] * 100) = m_6 - p_6)$
$\wedge e_1[0] \geq r_6[0] \wedge e_1[1] \geq r_6[1] \wedge e_1[2] \geq r_6[2] \wedge p_6 \geq 150 \wedge p_6 \leq 200$
$pc_7 : b_7 = 1 \wedge p_7 \geq 200 \wedge p_7 \leq 300 \wedge m_7 > p_7 \wedge \neg(\exists n_1, n_2, n_3 / \ 0 \leq n_1 \leq r_7[0]$
$\wedge 0 \leq n_2 \leq r_7[1] \wedge 0 \leq n_3 \leq r_7[2] \wedge m_7 - p_7 = n_1 * 20 + n_2 * 50 + n_3 * 100)$
$\wedge p_7 \geq 150 \wedge p_7 \leq 200$
$pc_8 : b_8 = 1 \wedge p_8 \geq 200 \wedge p_8 \leq 300 \wedge m_8 > p_8 \wedge \exists n_1, n_2, n_3 / \ 0 \leq n_1 \leq r_8[0]$
$\wedge 0 \leq n_2 \leq r_8[1] \wedge 0 \leq n_3 \leq r_8[2] \wedge m_8 - p_8 = n_1 * 20 + n_2 * 50 + n_3 * 100$
$\wedge p_8 > 0 \wedge m_8 > p_8 \wedge ((e_2[0] * 20 + e_2[1] * 50 + e_2[2] * 100) = m_8 - p_8)$
$\wedge e_2[0] \geq r_8[0] \wedge e_2[1] \geq r_8[1] \wedge e_2[2] \geq r_8[2] \wedge p_8 \geq 150 \wedge p_8 \leq 200$

The four path conditions (from pc_1 to pc_4) are associated with paths when the inserted amount is lower than the price and when the introduced amount equal to the price (for different choices of drink: coffee or tea). pc_5 and pc_7 are associated with symbolic paths issued from the numeric path where the reserve is not enough to return change. pc_6 and pc_8 are resulted from the symbolic execution of the path that contain the program *Return*

7.2 Feasibility

In the context of the drink vending machine, we now want to check the feasibility condition of a set of distinguished paths Δ^* having $\{pc_1, pc_2, pc_3, pc_4\}$ as path conditions, the first four paths described in Figure 5, according to two distinct contracts for *Price*, denoted respectively C_w and C_r and already discussed in Example 5 . Both C_w and C_r include two behaviors resulting in 4 distinguished paths. Path conditions and the feasibility decision are given in Tab. 2.

- With the contract C_w, no distinguished path of Δ^* is feasible because of contradictions between guards of the IOSTS transitions and post-conditions of C_w.
- With the contract C_r, all distinguished paths are feasible. *Price* can return anything between 150 and 200 for an argument equal to 0 and must return 200 for an argument equal to 1.

7.3 Contract Inference

Let us consider here a symbolic path δ^* of our drink vending machine's specification (Figure 6) that calls twice the program *Price* of interface (x_1, x_2) and the program *Return* of interface (x'_1, x'_2, x'_3, x'_4) without associating contracts with programs. The first call of *Price* leads to the appearance of a message "Add" on the screen and the second call permits the drink delivery and the return of the extra, such that:

$C_w : \{(x_1 = 0, x_2 \geq 0 \wedge x_2 \leq 100), (x_1 = 1, x_2 \geq 250)\}$
$pc_1 : b_1 = 0 \wedge p_1 \geq 0 \wedge p_1 \leq 100 \wedge m_1 < p_1 \wedge p_1 \geq 150 \wedge p_1 \leq 200$
$pc_2 : b_2 = 0 \wedge p_2 \geq 0 \wedge p_2 \leq 100 \wedge m_2 = p_2 \wedge p_2 \geq 150 \wedge p_2 \leq 200$
$pc_3 : b_3 = 1 \wedge p_3 \geq 250 \wedge m_3 < p_3 \wedge p_3 \geq 150 \wedge p_3 \leq 200$
$pc_4 : b_4 = 1 \wedge p_4 \geq 250 \wedge m_4 = p_4 \wedge p_4 \geq 150 \wedge p_4 \leq 200$
$\phi_{\{p_1,p_2\}} : b_1 = b_2 \Rightarrow p_1 = p_2$
$\phi_{\{p_1,p_3\}} : b_1 = b_3 \Rightarrow p_1 = p_3$
$\phi_{\{p_1,p_4\}} : b_1 = b_4 \Rightarrow p_1 = p_4$
$\phi_{\{p_2,p_3\}} : b_2 = b_3 \Rightarrow p_2 = p_3$
$\phi_{\{p_2,p_4\}} : b_2 = b_4 \Rightarrow p_2 = p_4$
$\phi_{\{p_3,p_4\}} : b_3 = b_4 \Rightarrow p_3 = p_4$
Feasibility: No

$C_r : \{(x_1 = 0, x_2 \geq 100 \wedge x_2 \leq 200), (x_1 = 1, x_2 \geq 200 \wedge x_2 \leq 300)\}$
$pc_1 : b_1 = 0 \wedge p_1 \geq 100 \wedge p_1 \leq 200 \wedge m_1 < p_1 \wedge p_1 \geq 150 \wedge p_1 \leq 200$
$pc_2 : b_2 = 0 \wedge p_2 \geq 100 \wedge p_2 \leq 200 \wedge m_2 = p_2 \wedge p_2 \geq 150 \wedge p_2 \leq 200$
$pc_3 : b_3 = 1 \wedge p_3 \geq 200 \wedge p_3 \leq 300 \wedge m_3 < p_3 \wedge p_3 \geq 150 \wedge p_3 \leq 200$
$pc_4 : b_4 = 1 \wedge p_4 \geq 200 \wedge p_4 \leq 300 \wedge m_4 = p_4 \wedge p_4 \geq 150 \wedge p_4 \leq 200$
$\phi_{\{p_1,p_3\}} : b_1 = b_3 \Rightarrow p_1 = p_3$
$\phi_{\{p_1,p_4\}} : b_1 = b_4 \Rightarrow p_1 = p_4$
$\phi_{\{p_2,p_3\}} : b_2 = b_3 \Rightarrow p_2 = p_3$
$\phi_{\{p_2,p_4\}} : b_2 = b_4 \Rightarrow p_2 = p_4$
$\phi_{\{p_3,p_4\}} : b_3 = b_4 \Rightarrow p_3 = p_4$
Feasibility: Yes

Table 2: Feasibility according to different contracts

$\pi(End(\delta^*)) : m_1 < p_1 \wedge p_1 \geq 150 \wedge p_1 \leq 200 \wedge (m_1 + m_2) > p_2 \wedge p_2 \geq 150 \wedge p_2 \leq 200 \wedge \exists n_1, n_2, n_3 / \ 0 \leq n_1 \leq r[0] \wedge 0 \leq n_2 \leq r[1] \wedge 0 \leq n_3 \leq r[2] \wedge (m_1 + m_2) - p_2 = n_1 * 20 + n_2 * 50 + n_3 * 100 \wedge ((e_1[0] * 20 + e_1[1] * 50 + e_1[2] * 100) = (m_1 + m_2) - p_2)$

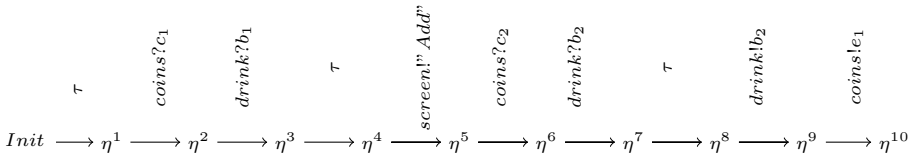

Fig. 6: Symbolic path.

From the path condition $\phi = \pi(End(\delta^*))$, we will generate a contract for the *Return* program and *Price* program according to[3] Definition 10. For e_1 the result of

[3] In fact, Definition 10, and in particular the function *Clean*, should be adapted to take into account the case of quantifier in formulas.

the program call $(Return, (p_2, m_1 + m_2, r), e_1)$ we have:

$$
\begin{array}{ll}
Y & : \{p_2, m_1 + m_2, r, e_1\} \\
G_{e_1} & : \{e_1, m_1, m_2, p_2, r, p_1\} \\
Ax_{e_1} & : m_1 < p_1 \wedge p_1 \geq 150 \wedge p_1 \leq 200 \wedge (m_1 + m_2) > p_2 \wedge p_2 \geq 150 \wedge p_2 \leq 200 \\
 & \wedge \exists n_1, n_2, n_3, 0 \leq n_1 \leq r[0] \wedge 0 \leq n_2 \leq r[1] \wedge 0 \leq n_3 \leq r[2] \\
 & \wedge (m_1 + m_2) - p_2 = n_1 * 20 + n_2 * 50 + n_3 * 100 \wedge ((e_1[0] * 20 + e_1[1] * 50 \\
 & + e_1[2] * 100) = (m_1 + m_2) - p_2) \\
Pre_{e_1} & : x'_1 = p_2 \wedge x'_2 = m_1 + m_2 \wedge x'_3 = r \\
Post_{e_1} & : x'_4 = e_1
\end{array}
$$

The inferred contract for our program *Return* in δ^* is $C = (Pre_{e_1}, Post_{e_1})$.

In the same way, from $\phi = \pi(End(\delta^*))$, two behaviors (a behavior par call) will be generated for the *Price* program according to our inference Definition. For p_1 the result of the first call $(Price, (b_1), p_1)$ we have:

$$
\begin{array}{ll}
Y & : \{b_1, p_1\} \\
G_{p_1} & : \{b_1, p_1, m_1, p_2, m_2, r, e_1\} \\
Ax_{p_1} & : m_1 < p_1 \wedge p_1 \geq 150 \wedge p_1 \leq 200 \wedge (m_1 + m_2) > p_2 \wedge p_2 \geq 150 \wedge p_2 \leq 200 \\
 & \wedge \exists n_1, n_2, n_3, 0 \leq n_1 \leq r[0] \wedge 0 \leq n_2 \leq r[1] \wedge 0 \leq n_3 \leq r[2] \\
 & \wedge (m_1 + m_2) - p_2 = n_1 * 20 + n_2 * 50 + n_3 * 100 \wedge ((e_1[0] * 20 + e_1[1] * 50 \\
 & + e_1[2] * 100) = (m_1 + m_2) - p_2) \\
Pre_{p_1} & : x_1 = b_1 \\
Post_{p_1} & : x_2 = p_1
\end{array}
$$

For p_2 the result of the second call $(Price, (b_2), p_2)$ we have:

$$
\begin{array}{ll}
Y & : \{b_2, p_2\} \\
G_{p_2} & : \{b_2, p_2, m_1, p_1, m_2, r, e_1\} \\
Ax_{p_2} & : m_1 < p_1 \wedge p_1 \geq 150 \wedge p_1 \leq 200 \wedge (m_1 + m_2) > p_2 \wedge p_2 \geq 150 \wedge p_2 \leq 200 \\
 & \wedge \exists n_1, n_2, n_3, 0 \leq n_1 \leq r[0] \wedge 0 \leq n_2 \leq r[1] \wedge 0 \leq n_3 \leq r[2] \\
 & \wedge (m_1 + m_2) - p_2 = n_1 * 20 + n_2 * 50 + n_3 * 100 \wedge ((e_1[0] * 20 + e_1[1] * 50 \\
 & + e_1[2] * 100) = (m_1 + m_2) - p_2) \\
Pre_{p_2} & : x_1 = b_2 \\
Post_{p_2} & : x_2 = p_2
\end{array}
$$

Finally, the inferred contract for our program *Price* in δ^* is:

- $G = G_{p_1} \cup G_{p_2}$
- $Ax = Ax_{p_1} \wedge Ax_{p_2}$
- $C = ((Pre_{p_1}, Post_{p_1}), (Pre_{p_2}, Post_{p_2}))$

8 Related Work

In the context of reactive systems verification, IOSTS and symbolic execution have been used in many works [1,10,13] for different purposes. They use IOSTS with atomic actions and substitutions whereas, in our case, we enrich IOSTS with programs specified by contracts. Our purpose is to define an integration framework and analyze in one hand the impact of programs contracts on a whole system and in the other hand elicit accurate contracts for our programs.

Our work is quite close to [12], that augments a SOA's BPEL business model with pre- and post-condition contracts defining essential component traits, and derive a suite of feasible test cases, taking into account contracts that are provided for some of the opaque components of their system. On the other hand, they do not infer contracts from the constraints expressed directly in the BPEL model as is done in section 6.2.

The use of symbolic execution and path feasibility analysis are studied in [3,21] but this is limited to the analysis of programs themselves and does not take in consideration as we do the impact of the program calls on the feasibility of the system as a whole. Similarly, symbolic execution techniques over the code have been used to infer program annotations. More specifically, such approaches concentrate on generating invariants. This is for instance the case in the KeY verification framework [19], for the DySy tool [6], or for the iDiscovery tool [23]. Those invariants are meant to help the formal verification of the code against its specification, while we are aiming at generating a specification that the programs must meet in order to be usable in the context of the system under test.

The problem of inferring contracts for programs has been studied differently in other works that do not rely on symbolic execution. In particular, [5] derives pre-conditions from assertions already present in the code using abstract interpretation. [22] uses dynamic analysis to augment simple programmer-written contracts with candidate post-conditions that describes precisely what the code is doing, building upon techniques developed initially in the Daikon tool [8] for proposing likely invariants. This kind of inference is dual to ours, in the sense that we infer contracts in a top-down approach, in order to express what conditions individual components should fulfill inside a broader system, while the works mentioned above are bottom-up, encapsulating the behavior of actual code in contracts in order to check whether callers can use this particular implementation. The same can be said of works that aim at generating transition systems modeling the behavior of programs, either as message sequence charts as in [15], or as scenarios expressed under the form of live sequence charts, as in [16].

9 Conclusion

In this work, we extended the IOSTS framework with programs which are specified with contracts and we adapted symbolic execution techniques to deal with them. This gives rise to two main results. First, we study how contracts impact path conditions and describe the feasibility condition of the entire symbolic execution tree. Second, we show that path conditions can be used to infer contracts for programs in order to specify what these programs should do in the context of the system under test. Such contracts can then be used for unitary testing purposes, while feasibility preservation theorem gives some guarantees that program calls will not get in the way during integration testing. Implementation of the technique presented in this paper is currently under development in the Diversity [7] symbolic execution tool and the Frama-C [14] C code analysis framework using the ACSL specification language [2] as target for contract inference.

Future work include in particular integrating programs and contracts into various IOSTS extensions. From an implementation point of view, UML Sequence Diagrams [18], a widely used formalism for describing transition systems, would be a good input language from a practical point of view. Sequence diagrams are already supported by Diversity, but program calls and contracts need to be added to the UML

subset supported by Diversity. On a more theoretical level, we have so far examined program and contracts in one single component. IOSTS are nevertheless meant to model whole systems consisting in various components interacting with each other through communication actions. Path conditions can then be projected on the internal state of a single component to define constraints on this component. It would be interesting to examine how to compose such projections with contract inference.

References

1. B. Bannour. *Symbolic analysis of scenario based timed models for component-based systems: Compositionality results for testing.* PhD thesis, Ecole Centrale Paris, CEA, 2012.
2. P. Baudin, J.-C. Filliâtre, T. Hubert, C. Marché, B. Monate, Y. Moy, and V. Prevosto. *ACSL: ANSI/ISO C Specification Language, v1.9*, March 2015.
3. N. Bjørner, N. Tillmann, and A. Voronkov. Path feasibility analysis for string-manipulating programs. In *15th Int. Conf., TACAS*, volume 5505 of *Lecture Notes in Computer Science*. Springer, 2009.
4. P. Chalin, J. R. Kiniry, G. T. Leavens, and E. Poll. Beyond assertions: Advanced specification and verification with JML and esc/java2. In *4th Int. Symposium, FMCO*, volume 4111 of *Lecture Notes in Computer Science*. Springer, 2006.
5. P. Cousot, R. Cousot, and F. Logozzo. Precondition Inference from Intermittent Assertions and Application to Contracts on Collections. In *Proc. VMCAI*, 2011.
6. C. Csallner, N. Tillmann, and Y. Smaragdakis. Dysy: Dynamic symbolic execution for invariant inference. In *Proceedings of ICSE*, 2008.
7. J. Deltour, A. Faivre, E. Gaudin, and A. Lapitre. Model-based testing: An approach with SDL/RTDS and DIVERSITY. In *8th Int. Conference, SAM 2014*, volume 8769 of *Lecture Notes in Computer Science*. Springer, 2014.
8. M. D. Ernst, J. Cockrell, W. G. Griswold, and D. Notkin. Dynamically discovering likely program invariants to support program evolution. *Trans. Soft. Eng.*, 27, 2001.
9. R. W. Floyd. Assigning meanings to programs. *Proc. AMS Symp. on Applied Mathematics*, 19, 1967.
10. C. Gaston, P. Le Gall, N. Rapin, and A. Touil. Symbolic execution techniques for test purpose definition. In *Testing of Communicating Systems, Int. Conference, TestCom*, volume 3964 of *Lecture Notes in Computer Science*. Springer, 2006.
11. C. A. R. Hoare. An axiomatic basis for computer programming. *Communications of the ACM*, 12(10), 1969.
12. S. Jehan, I. Pill, and F. Wotawa. Functional SOA Testing Based on Constraints. In *Automation of Software Test*, 2013.
13. J. C. King. Symbolic Execution and Program Testing. *Comm. ACM*, 17, 1976.
14. F. Kirchner, N. Kosmatov, V. Prevosto, J. Signoles, and B. Yakobowski. Frama-C, A Software Analysis Perspective. *Formal Aspects of Computing*, 27, 2015.
15. S. Kumar, S.-C. Khoo, A. Roychoudhury, and D. Lo. Inferring class level specifications for distributed systems. In *Proc. ICSE*, 2012.
16. D. Lo and S. Maoz. Scenario-based and value-based specification mining: better together. *Autom. Softw. Eng.*, 19, 2012.
17. B. Meyer. Applying "design by contract". *IEEE Computer*, 25(10), 1992.
18. Object Management Group. *OMG Unified Modeling Language^{TM} (OMG UML)*, version 2.5 edition, 2013.
19. P. H. Schmitt and B. Weiß. Inferring invariants by symbolic execution. In *VERIFY Workshop*, volume 259 of *CEUR Workshop Proceedings*, 2007.

20. J. Tretmans. Conformance Testing with Labelled Transition Systems: Implementation Relations and Test Generation. *Computer Networks and ISDN Systems*, 1996.
21. Y. Wang, Y. Xing, and X. Zhang. A Method of Path Feasibility Judgment Based on Symbolic Execution and Range Analysis. *International Journal of Future Generation Communication and Networking*, 2014.
22. Y. Wei, C. A. Furia, N. Kazmin, and B. Meyer. Inferring better contracts. In *Proc. ICSE*, 2011.
23. L. Zhang, G. Yang, N. Rungta, S. Person, and S. Khurshid. Invariant discovery guided by symbolic execution. In *The Java PathFinder Workshop*, 2013.