Trace Specifications of Non-deterministic Multi-object Modules

Michal Iglewski[a], Marcin Kubica[b], Jan Madey[b]

a. Département d'informatique, Université du Québec à Hull, Hull, Québec, Canada J8X 3X7
E-mail: iglewski@uqah.uquebec.ca
b. Institute of Informatics, Warsaw University, Banacha 2, 02-097 Warsaw, Poland
E-mail: kubica@mimuw.edu.pl, madey@mimuw.edu.pl,

Abstract

The *trace assertion method* (in short: TAM) is a formal method for abstract specification of interfaces of software modules being designed according to the "information hiding" principle. A trace specification is a "black-box" specification, i.e., it describes only those features of a module that are *externally observable*. The method was introduced by W. Bartussek and D.L. Parnas some 15 years ago and since then has undergone many modifications. In recent years there has been an increased interest in TAM. Software tools supporting practical usage of TAM for software engineering projects are under development, the method is being tested on different applications, its foundations are being studied.

Recent experiments with TAM have showed the need for further study in the case of non-deterministic multi-object modules. In this paper we investigate the expressiveness of the method for such modules. We present a formal model of a module and its TAM specification, show that the method requires some extensions and propose solutions. Our considerations are illustrated on TAM but could also be generally applied to modules with internal non-determinism.

The full version of our investigations, including all definitions, lemmas, proofs and examples, is presented in university technical reports.

KEY WORDS: software module, interface specification, non-determinism, trace assertion method, information hiding.

1 Introduction

The *trace assertion method* (in short: TAM) is a formal method for abstract specification of interfaces of software *modules* being designed according to the "information hiding" principle [10]. A trace specification is a "black-box" specification, i.e., it describes only those features of an object that are *externally observable* and hides details of its internal structure. The form of internal non-determinism can be considered as a hidden detail for an external observer. In many specification methods (like Z) this aspect is not hidden.

The trace assertion method was first formulated in [1], and since then has undergone many modifications [3, 4, 7, 9, 12, 13]. In recent years, there has been an increased interest in TAM, especially within the framework of the "functional approach" [11]. Software tools supporting practical usage of TAM are under development (e.g. [5, 13]), the method is being tested on different applications (e.g. [2]), and its foundations are being studied (e.g. [8, 13]).

A given module may be designed to implement either a single object or a number of objects. There is a distinct difference in the complexity of TAM in these two cases. The present paper is a continuation of [8] where TAM restricted to single-object modules was investigated and specifications were modelled with Mealy machines. Here we are studying the foundations of TAM for multi-object modules. In particular, we are interested in its expressiveness in the case of non-deterministic modules.

In Section 2 we present a formal model for multi-object modules. In Section 3, trace specifications for such modules are described. In Section 4 we show an example of a multi-object module that cannot be specified in the current version of TAM. A modified simple model of trace specifications which covers a wider class of non-determinism in multi-object modules is proposed in Section 5. Related changes in TAM and the expressiveness of a proposed version of TAM are discussed in Section 6. Final conclusions and future plans are briefly presented in Section 7.

2 Formal model for multi-object modules

In this section we characterize some basic notions, notably those of objects and modules. We also define a simple formal model of multi-object modules, fulfilling the given characteristic.

2.1 Introduction

We assume that time is discrete, linear, with an "initial" instant, and without a "final" one. Instants of time are represented by natural numbers.

The notion of an *object* can be characterized as follows. An object is any entity which has *states*, can be affected by *events*, and satisfies the following properties:

- at every instant of time the object is in one of its states; initially, the object is in the *initial* state,
- the object may change its state only as a result of an event; if the event occurs at the instant t, the object is in a new state at the instant $t + 1$.

Objects are grouped in modules: we say that a *module* implements a number of homogeneous and independent objects. If a module implements one object it is called *single-object.* A *multi-object* module can implement a given (including infinite) number of objects. In this paper we deal with multi-object modules.

Objects implemented by a given module are called *domestic*, while those implemented by other modules are called *foreign*. For each module there is a specific set of events that can affect its domestic objects.

There are two kinds of event that can affect an object:

- *access-program invocations* (calls of programs exported by the module),
- *input variable events* (changes of values of the module's input variables).

We assume that at most one event can occur at a given instant of time and that objects in the module can be affected only by a finite sequence of events.

In this paper we deal only with the first kind of event. However, we do not lose the generality of discussion since an input variable event can be expressed in terms of an access-program invocation. Input variables are described in detail in [2, 3, 12].

For each module there is a finite number of access-programs. Each access-program operates on at least one domestic object and possibly on foreign objects. As a result of an access-program invocation, the arguments can change their states, possibly non-deterministically. For the sake of simplicity, we will treat values returned by functions as arguments which can change their states but with irrelevant initial values. For each access-program invocation, the next state of each argument depends only on the previous states of the arguments of this invocation. We assume that all arguments of access-programs are different objects. In practice, however, one object can be passed through several arguments of an access-program. This does not cause any loss of generality because we can model an access-program whose arguments might possibly represent the same objects by several access-programs whose arguments are always different objects. For example, an access-program P with two domestic arguments, which can represent the same object, can be modeled by two access programs:

- one with two domestic arguments (representing different objects passed as arguments of P), and
- one with only one domestic argument (representing one object passed through both arguments of P).

2.2 Module

In this sub-section we define a formal model of multi-object modules and give some basic definitions used in the latter part of the article.

Def. 1 A *module* is the following tuple: (Q, q_0, O, F, I, E), where:

- Q is a non-empty set; its elements are called *states of domestic objects*,
- $q_0 \in Q$ and it is called the *initial state of domestic objects*,

- O is a non-empty set; its elements are called *names of domestic objects*,
- F is a non-empty set; its elements are called *states of foreign objects*,
- I is a non-empty finite set; its elements are called *names of access-programs*,
- $E = (E_i)_{i \in I}$ is a sequence of relations $E_i \subseteq Q^{k_i} \times F^{l_i} \times Q^{k_i} \times F^{l_i}$ such that $k_i \in N$ (natural numbers), $1 \le k_i \le |O|$, and

$$\forall q \in Q^{k_i}, r \in F^{l_i}\, \exists q' \in Q^{k_i}, r' \in F^{l_i}\, [E_i(q, r, q', r')]$$

For each $i \in I$, E_i is a relation specifying changes of states of arguments of the access-program i.

$E_i(q, r, q', r')$ means that if an invocation of the access-program i operates on certain domestic objects being in states q and certain foreign objects being in states r, then the states of these objects after the invocation can be, q' and r' respectively.

This definition can be seen as an extension of Mealy machines. (Mealy machines have been used as a model for single-object modules in [8].) Instead of a single state of an automaton we have many states of many objects.

Def. 2 A *state of a module* is a function $s: O \to Q$. It represents the states of all objects implemented by this module.

Def. 3 A *history of a module* is a function $H: N \to \wp(O \to Q) \setminus \{\emptyset\}$ (by $\wp(X)$ we denote the power set of X) such that $H(0) = \{s\}$, where $s(o) = q_0$ for all $o \in O$. It represents sets of possible states of this module at all instants of time. At the initial instant, all objects are in the initial state.

Def. 4 An *event* (i.e. access-program invocation) is a tuple $e = (i, o, r)$ where:

- $i \in I$,
- $o \in O^{k_i}$ is a vector of different names of domestic objects; its elements identify domestic arguments of the event,
- $r \in F^{l_i}$ is a vector; its elements represent states of foreign arguments of the event.

Def. 5 An *output* of an event (i, o, r) is a vector $r' \in F^{l_i}$; its elements represent new states of foreign arguments of the event.

Def. 6 A *step of computation* is a pair $c = (e, r')$ where e is an event and r' is an output of e.

A step of computation represents externally observable (observable outside the module) aspects of an access-program invocation, i.e.:

- which access-program is invoked,
- on which domestic objects the access-program operates,
- what are the states of passed foreign arguments, and
- what are the states of foreign arguments after the invocation.

Def. 7 A state s' of a module is *reachable* from a state s of the module in a step of computation $c = ((i, o, r), r')$ iff:

$$E_i((s(o_1), \ldots, s(o_{k_i})), r, (s'(o_1), \ldots, s'(o_{k_i})), r') \wedge \forall j \in O \setminus \{o_1, \ldots, o_{k_i}\}\, [s(j) = s'(j)]$$

We denote it by $s \xrightarrow{c} s'$.

For a given $c = (e, r')$, $s \xrightarrow{c} s'$ means that if a module is in a state s, an event e takes place and new states of its foreign arguments are equal to r' then a new state of the module can be s'.

Def. 8 A *computation* is a finite sequence of steps of computation, $((e_j, r'_j))_{j=0}^{m}$, where $m \ge -1$, $e_j = (i_j, o_j, r_j)$ is an event, and $r'_j \in F^{l_{i_j}}$ is an output of e_j.

A computation denotes externally observable aspects of a sequence of invocations of access-programs.

Def. 9 We say that a history H *satisfies a computation* $C = (c_j)_{j=0}^{m}$ iff for all $t \in N$:

$$(t \le m \Rightarrow H(t+1) = \{s' : O \to Q \mid \exists s \in H(t)\,[\, s \xrightarrow{c_t} s' \,]\}) \wedge (t > m \Rightarrow H(t+1) = H(t)) .$$

A history represents possible states of domestic objects during the computation. Notice that if there exists a history satisfying a given computation then there is only one such history.

Def. 10 We say that a computation is *feasible* if there exists a history satisfying this computation.

One should recall that the value of a history at a given moment in time is a non-empty set of possible states of the module. Hence, there can be (and usually are) histories that are not feasible.

The set of feasible computations fully characterizes an externally observable behavior of a module. According to the information hiding principle, we are interested only in externally observable aspects of a module, i.e., we are not interested in the concrete states of domestic objects — we observe only the identity of domestic arguments and the values of foreign arguments of events. Hence, there can be several modules that cannot be externally distinguished.

Def. 11 We say that two modules are *observationally equivalent* iff they have the same sets of feasible computations.

Sometimes we are interested in reduction of a module to a simpler, observationally equivalent module. A simple reduction can be done by removing states which can never appear.

Def. 12 The set A of *reachable states of objects* of a module $M = (Q, q_0, O, F, I, E)$ is the subset of Q of all states appearing in histories satisfying feasible computations:

$$A = \{q \in Q \mid \exists C\text{- feasible}, H\text{- satisfying } C, t \in N, s \in H(t), o \in O\,[q = s(o)]\}$$

Notice that always $q_0 \in A$. Non-reachable states of a module do not appear in any history satisfying any feasible computation. Hence they are irrelevant to the behavior of the module.

Def. 13 Let $M = (Q, q_0, O, F, I, E)$ be a module, A be the set of reachable states of objects of M, $\overline{M}$ be a module $\overline{M} = (A, q_0, O, F, I, \overline{E})$, where $\overline{E} = (\overline{E_i})_{i \in I}$, $E_i \subseteq Q^{k_i} \times F^{l_i} \times Q^{k_i} \times F^{l_i}$, $\overline{E_i} = E_{i \mid A^{k_i} \times F^{l_i} \times A^{k_i} \times F^{l_i}}$.

$\overline{M}$ is the *reachable reduction* of M.

Notice that if $\overline{M}$ is the reachable reduction of a module M, then every computation is feasible for M iff it is feasible for $\overline{M}$. Hence M and $\overline{M}$ are observationally equivalent.

3 Trace specifications of multi-object modules

In this section we focus on trace specifications of multi-object modules, their form and their model. In Section 3.1 we define a sub-class of modules, called trace-modules, which we use later as models of trace specifications. In Section 3.2 we briefly describe the form of trace specifications of multi-object modules, and we show how trace specifications can be modelled by trace-modules and vice versa, i.e., how trace-modules can be specified.

3.1 Trace-modules

Def. 14 A *trace-module* is a module (Q, q_0, O, F, I, E) such that for each $i \in I$ there exist:

- a relation $R_i \subseteq Q^{k_i} \times F^{l_i} \times F^{l_i}$,
- a function $X_i : r_i \to Q^{k_i}$,

such that $\forall q, q' \in Q^{k_i}, r, r' \in F^{l_i}\,[E_i(q, r, q', r') \Leftrightarrow R_i(q, r, r') \wedge X_i(q, r, r') = q']$.

R_i is called a *return relation* (between values of arguments of an access-program invocation and its output); X_i is called an *extension function* and describes the values of domestic arguments after this invocation, depending on the values of arguments and the output of the invocation.

Intuitively, a module (Q, q_0, O, F, I, E) is a trace-module iff (for each $i \in I$) the relation E_i can be viewed as a composition of a relation (R_i) denoting new states of foreign arguments and a function (X_i) denoting new states of do-

mestic arguments. Generally, states of trace-modules have simpler forms than states of modules — for each feasible computation and a moment in time, there is only one possible state of a trace-module.

Lemma 1: If M is a trace-module, C is a computation, H is a history satisfying C, and $t \in N$, then $H(t)$ is a singleton.

Proof of this lemma can be found in [5]. Note that if the given module is deterministic then it is also a trace-module, since for each $i \in I$, E_i is a function.

3.2 Trace specifications

One of the basic notions in TAM is the notion of traces. Intuitively, a *trace* is a term describing a fragment of a feasible computation of a trace-module, containing all steps that can influence the current state of a given object. Each reachable state is represented by one or more traces. A trace specification defines a subset of traces called *canonical traces* — one canonical trace for each reachable state. States of objects are represented in specifications by canonical traces. Detailed descriptions of traces can be found in [5, 7, 12].

A trace specification (i.e., a specification in TAM) of a module is a document consisting of the following five parts: Characteristics Section, Syntax Section, Canonical Section, Equivalence Section, Return Values Section.

Precise descriptions of trace specifications can be found in [7, 12]. Here, we only briefly summarize the contents of trace specifications.

The Characteristics Section contains information about:

- the name of the module specified by the given specification,
- foreign modules used by this module; they implicitly define the set of states of foreign objects,
- the set of names of objects implemented by the module, and
- features of the module (whether it is deterministic or non-deterministic, single-object or multi-object, and parameterized or not parameterized).

Usually, the set of names of objects implemented by the module is the set of canonical traces of another module.

In this paper we deal only with non-parameterized specifications of multi-object modules. As non-deterministic modules are more general than deterministic ones, we focus on the specifications of non-deterministic modules.

The Syntax Section defines the set of access-programs and the types of their arguments (i.e. modules in which they are implemented). In particular, for each access-program, it defines the number of domestic and foreign arguments. The Syntax Section provides some information that is not expressed in our model, e.g., the order of domestic and foreign arguments for each access-program. In our model this order is fixed. Nor does our model distinguish types of foreign arguments.

The Canonical Section defines the characteristic predicate (*canonical)* of the set of canonical traces, and distinguishes a canonical trace representing the initial state. The set of canonical traces depends on the particular specification. The set of states of domestic objects is the set of canonical traces. This section of the specification can also define some auxiliary functions and/or relations used in the rest of the specification.

For each access-program, the Equivalence Section contains a definition of the *extension function*. The domain of this function contains states of all arguments of the access-program before the invocation and new states of all of its foreign arguments after the invocation. The range of this function contains new states of all domestic arguments of the access-program, and a sort of a marker (called *a token*) describing the correctness of the invocation. This marker is not expressed in our model. The value of the token has no effect on the behavior of the module. In a later part of this paper we assume that every invocation is specified as a correct one.

The Return Values Section for each access-program defines a relation called the *return relation*. This is a relation between states of all arguments of the access-program before the invocation, and new states of all of its foreign arguments. This relation determines possible new states of foreign arguments of the access-program.

A trace specification can be modelled by a trace-module as follows:

- Q is the set of canonical traces,
- $q_0 \in Q$ is the canonical trace representing the initial state,
- O is the set of names of objects implemented by the module,
- F is the union of sets of canonical traces of foreign modules,
- I is the set of names of access-programs,
- R_i is a return relation for an access-program i,
- X_i is an extension function for an access-program i,
- E_i is such that: $\forall q, q' \in Q^{k_i}, r, r' \in F^{l_i} [E_i(q, r, q', r') \Leftrightarrow R_i(q, r, r') \wedge X_i(q, r, r') = q']$.

A trace-module thus defined is called the *trace-module obtained from a trace specification.*

Def. 15 We say that a *module satisfies a trace specification* iff it is observationally equivalent to the trace-module obtained from the trace specification. In this case we also say that the *specification specifies the module.*

We are not only able to represent trace specifications by trace-modules but we can specify every trace-module, which is more interesting.

Theorem: For each trace-module there exists a trace specification satisfied by this module.

Proof of this theorem can be found in [5].

This theorem proves that the class of modules that can be specified in TAM is equal to the class of modules observationally equivalent to certain trace-modules. One should also note that since every deterministic module is a trace-module, every deterministic module can be specified in TAM.

4 Non-determinism non-expressible in the trace assertion method

In this section we prove that not every module can be specified in TAM. The counter-example we construct is a non-deterministic multi-object module.

Theorem: There exists a module that does not satisfy any trace specification.

Proof: Let $M = (Q, q_0, O, F, I, E)$ be a module, where:

- $Q = \wp(\{0, 1\})$,
- $q_0 = \emptyset$,
- $O = \{a, b\}$,
- $F = \{0, 1, true, false\}$,
- $I = \{Ins, In, Cross\}$,
- $E_{Ins} \subseteq Q \times F \times Q \times F$, $\quad E_{Ins}(q, r, q', r') \equiv r' = r \wedge q' = q \cup (\{r\} \cap \{0, 1\})$,
- $E_{In} \subseteq Q \times F \times Q \times F$, $\quad E_{In}(q, r, q', r') \equiv q = q' \wedge r' = (r \in q)$,
- $E_{Cross} \subseteq Q^2 \times Q^2$, $\quad E_{Cross}(q_1, q_2, q'_1, q'_2) \equiv q_1 \cup q_2 = q'_1 \cup q'_2 \wedge q'_1 \cap q'_2 = \emptyset$.

The module M implements two sets that both can contain two elements, 0 and 1, with the following operations:

- *Ins* inserts an element into a set,
- *In* checks if an element is in a set,
- *Cross* takes two sets and divides non-deterministically their union into two disjoint sets.

We will show that there does not exist a trace specification satisfied by M. The proof is by contradiction. Let us assume that such a trace specification X exists. Let $\overline{M} = (\overline{Q}, \overline{q}_0, F, I, \overline{E})$ be a trace-module obtained from X. Let us consider the following computations:

$$C_1 = (((Ins, a, 1), 1), ((Cross, a, b)), ((In, a, 1), true), ((In, b, 1), false)),$$

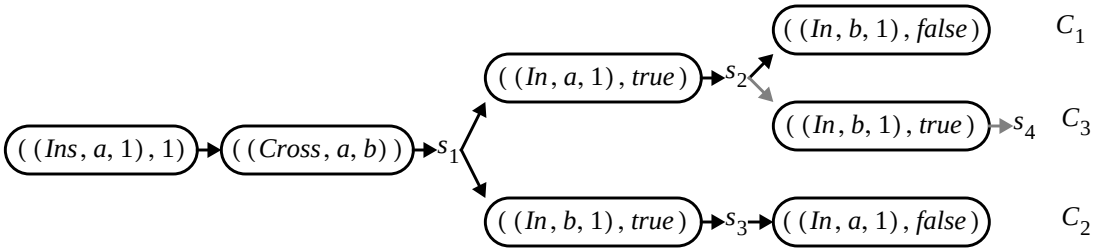
$$C_2 = (((Ins, a, 1), 1), ((Cross, a, b)), ((In, b, 1), true), ((In, a, 1), false)),$$

$$C_3 = (((Ins, a, 1), 1), ((Cross, a, b)), ((In, a, 1), true), ((In, b, 1), true)).$$

C_1 and C_2 are feasible computations for M and hence also for $\overline{M}$ but C_3 is not feasible for M. This means that when we insert 1 into set a, and then apply the access-program *Cross* to sets a and b, 1 is in one of these sets but not in both.

We will obtain the contradiction by proving that the computation C_3 is feasible for module $\overline{M}$.

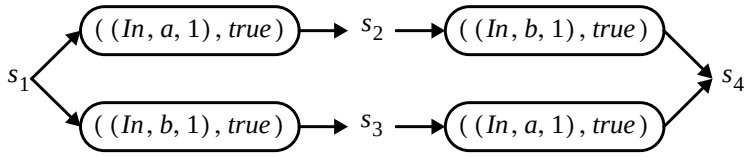
Let H_1, H_2 be two histories of a trace-module $\overline{M}$ satisfying, respectively, computations C_1 and C_2. H_1 and H_2 have the same first two elements and hence, $H_1(2) = H_2(2)$. From lemma 1 on page 5, $H_1(t)$ and $H_2(t)$ are singletons (for each $t \in N$). Let $H_1(2) = H_2(2) = \{s_1\}$, $H_1(3) = \{s_2\}$, and $H_2(3) = \{s_3\}$.



Notice that $s_1(b) = s_2(b)$ because $C_{1,2} = C_{3,2} = ((In, a, 1), true)$ cannot change the state of object b, and $s_1(a) = s_3(a)$ because $C_{2,2} = ((In, b, 1), true)$ cannot change the state of object a. To prove that C_3 is feasible for $\overline{M}$ we show that for $C_{3,3} = ((In, b, 1), true)$ there exists a state s_4 of a trace-module $\overline{M}$ such that $s_2 \xrightarrow{C_{3,3}} s_4$. Notice that $C_{3,3}$ cannot change the value of object a, so $s_4(a) = s_2(a)$. On the other hand, $s_4(b) = s_3(b)$ because $s_2(b) = s_1(b)$ and $C_{3,3} = C_{2,2} = ((In, b, 1), true)$. Hence state s_4 can be defined as follows:

$$s_4(j) = \begin{cases} s_2(a) & \text{if } j = a \\ s_3(b) & \text{if } j = b \end{cases}$$

Notice that for $z = ((In, a, 1), true)$ also $s_3 \xrightarrow{z} s_4$.



A history H_3 satisfying computation C_3 is defined as follows:

$$H_3(t) = \begin{cases} H_1(t) & \text{if } t \le 3 \\ \{s_4\} & \text{if } t > 3 \end{cases}$$

Thus, computation C_3 is feasible for $\overline{M}$ but not feasible for M. Module $\overline{M}$ is not observationally equivalent to M, and M does not satisfy X.

■

5 “New” trace-module

In this section we will redefine the notion of trace-modules and show that for every module there exists an observationally equivalent new trace-module. This reduces the problem of specification of multi-object modules in TAM to

that of specification of new trace-modules.

Def. 16 A new trace-module is such a module (Q, q_0, O, F, I, E) that for each E_i there exist:

- a number $1 \le p_i \le k_i$,
- a relation $R_i \subseteq Q^{k_i} \times F^{l_i} \times Q^{k_i - p_i} \times F^{l_i}$,
- a function $X_i : r_i \to Q^{p_i}$,

such that $\forall q \in Q^{k_i}, r \in F^{l_i}\, \exists q' \in Q^{k_i - p_i}, r' \in F^{l_i}\, [r_i(q, r, q', r')]$, and

$$\forall q, q' \in Q^{k_i}, r, r' \in Q^{l_i}\, [E_i(q, r, q', r') \Leftrightarrow R_i(q, r, (q'_{p_i+1}, \ldots, q'_{k_i}), r') \wedge X_i(q, r, (q'_{p_i+1}, \ldots, q'_{k_i}), r') = (q'_1, \ldots, q'_{p_i})\ ]$$

R_i is called a *return relation*, X_i is called an *extension function* and p_i is called a *number of primary domestic arguments* of access-program i. The largest p_i is called the *maximum number of primary domestic arguments* of access-program i.

Intuitively, in new trace-modules we allow new states of some domestic arguments to be specified by the return relation. One should note that for a given new trace-module and the numbers of primary domestic arguments, for each access-program there exist exactly one return relation and one extension function.

Each trace-module is also a new trace-module (for $p_i = k_i$); however, the class of new trace-modules is wider than the class of trace-modules.

Theorem: For each module M, there exists a new trace-module $\overline{M}$ observationally equivalent to M.

Proof: For a given module $M = (Q, q_0, O, F, I, E)$ $(E_i \subseteq Q^{k_i} \times F^{l_i} \times Q^{k_i} \times F^{l_i})$ we will construct a new trace-module $\overline{M} = (\overline{Q}, \bar{q}_0, O, F, I, \overline{E})$ such that $\overline{M}$ will be observationally equivalent to M and each access-program of $\overline{M}$ will have one primary domestic argument $(p_i = 1)$. Let: $\overline{Q} = \wp(Q) \setminus \{\varnothing\}$, $\bar{q}_0 = \{q_0\}$, and

$$\overline{R}_i(\bar{q}, r, (\bar{q}'_2, \ldots, \bar{q}'_{k_i}), r') \equiv \exists q \in \bar{q}_1 \times \ldots \times \bar{q}_{k_i}, q' \in Q^{k_i}\, [\forall j \in \{2, \ldots, k_i\}\ [\bar{q}'_j = \{q'_j\}] \wedge E_i(q, r, q', r')]$$

$$\overline{X}_i(\bar{q}, r, (\bar{q}'_2, \ldots, \bar{q}'_{k_i}), r') = \{q'_1 \in Q \mid \exists q \in \bar{q}_1 \times \ldots \times \bar{q}_{k_i}, q'_2 \in \bar{q}'_2, \ldots, q'_{k_i} \in \bar{q}'_{k_i}\, [E_i(q, r, q', r')]\}.$$

For this construction we define the inclusion relation on states of modules M and $\overline{M}$.

Def. 17 For each state s of module M and state $\bar{s}$ of module $\overline{M}$ we say that $s \ll \bar{s}$ iff $\forall j \in O\, [s(j) \in \bar{s}(j)]$.

Our proof is based on the two lemmas given below. Their proofs can be found in [5].

Lemma 2: For modules M and $\overline{M}$ as defined above, each $s, s' : O \to Q$, $\bar{s} : O \to \overline{Q}$ and a step of computation c, if $s \xrightarrow{c} s' \wedge s \ll \bar{s}$ then there exists $\bar{s}' : O \to \overline{Q}$ such that $\bar{s} \xrightarrow{c} \bar{s}'$ and $s' \ll \bar{s}'$.

Lemma 3: For modules M and $\overline{M}$ as defined above, let $\overline{H} : N \to \wp(O \to \overline{Q})$ be the history of module $\overline{M}$ satisfying a feasible computation C. There exists a history $H : N \to \wp(O \to Q)$ of M satisfying C such that: $\forall t \in N\, [H(t) = \{s : O \to Q \mid \exists \bar{s} \in \overline{H}(t)\ [s \ll \bar{s}]\}]$.

Let us assume that M and $\overline{M}$ are not observationally equivalent. Then there exists such a computation that it is feasible for one and only one of these modules. Let $C = (c_j)_{j=0}^{\alpha}$, $\alpha \ge 0$ be one of the shortest such computations. Hence $C' = (c_j)_{j=0}^{\alpha - 1}$ is feasible for both modules. Let H and $\overline{H}$ be the histories of, respectively, M and $\overline{M}$ satisfying the computation C'. Let us consider two cases:

1. C is feasible for M. This implies that $\exists s \in H(\alpha), s' : O \to Q\, [\, s \xrightarrow{c_\alpha} s'\ ]$.

   Applying lemma 3 to C' for $t = \alpha$ we obtain that $H(\alpha) = \{s : O \to Q \mid \exists \bar{s} \in \overline{H}(\alpha)\ [s \ll \bar{s}]\}$

From the above two formulae it follows that $\exists s \in H(\alpha), \bar{s} \in \overline{H}(\alpha), s' : O \to Q\ [\ s \ll \bar{s} \wedge s \xrightarrow{c_\alpha} s'\ ]$.

From lemma 2, $\exists \bar{s} \in \overline{H}(\alpha), \bar{s}' : O \to \overline{Q}\ [\ \bar{s} \xrightarrow{c_\alpha} \bar{s}'\ ]$. Hence, C is feasible for $\overline{M}$.

2. C is feasible for $\overline{M}$. This implies that there exists a history of $\overline{M}$ satisfying C. From lemma 3, there exists a history of M satisfying C, so C is feasible for M.

We have obtained a contradiction. Hence the assumption that M and $\overline{M}$ are not observationally equivalent is false.

■

Example: A new trace-module (Q, q_0, O, F, I, E) with the "Cross" access-program (see Section 4) can be defined as follows:

- $Q = \wp(\{0, 1\})$,
- $q_0 = \emptyset$,
- $O = \{a, b\}$,
- $F = \{0, 1, true, false\}$,
- $I = \{Ins, In, Cross\}$,
- $R_{Ins} \subseteq Q \times F \times F, \quad R_{Ins}(q, r, r') \equiv r' = r$,
- $X_{Ins} : R_{Ins} \to Q, \quad X_{Ins}(q, r, r') = q \cup (\{r\} \cap \{0, 1\})$
- $R_{In} \subseteq Q \times F \times F, \quad R_{In}(q, r, r') \equiv r' = (r \in q)$,
- $X_{In} : R_{In} \to Q, \quad X_{Ins}(q, r, r') = q$
- $R_{Cross} \subseteq Q^2 \times Q, \quad R_{Cross}(q_1, q_2, q'_2) \equiv q'_2 \subseteq q_1 \cup q_2$,
- $X_{Cross} : R_{Cross} \to Q, \quad X_{Cross}(q_1, q_2, q'_2) = (q_1 \cup q_2) \setminus q'_2$.

6 "New" trace specifications

In this section we discuss the form of traces and trace specifications used to describe new trace-modules. We also investigate which new trace-modules can be specified in the proposed version of TAM, and how this can be done.

The basic difference between new trace-modules and trace-modules is that:

- in trace-modules, an extension function determines new states of all domestic arguments of an access-program,
- in new trace-modules, an extension function defines only new values of some (at least one) domestic arguments, called *the primary (domestic) arguments*; possible new values of the rest of domestic arguments, called *the secondary (domestic) arguments*, are defined by the return relation. For simplicity, in our model primary arguments precede secondary ones, however in general they can be in any order.

This difference is reflected in the form and the interpretation of traces. A proposal of a new form of traces can be found in [5]. A trace represents a new value of one of the primary domestic arguments of its last invocation. It can happen that some reachable states are not represented by any traces. States that are represented by one or more traces are called *trace-expressible*.

The form of a new trace specification is similar to the form of a trace specification. The form of the Characteristics Section is the same. The Syntax Section defines also numbers of primary arguments of access-programs. The Canonical Section defines a set of canonical new traces, and a canonical trace representing the initial state. The Equivalence Section defines an extension function for each access program. The range of this function contains only canonical traces, representing new states of the primary arguments. The Return Values Section defines a return relation for each access program. However this relation is defined on states of all arguments passed to the access-program, and new states of all secondary domestic arguments and all foreign arguments of the access-program.

A new trace specification can be modelled as a new trace-module (Q, q_0, O, F, I, E) in the following way:

- Q is the set of canonical new traces,

- q_0 is the canonical new trace representing the initial state,
- O is the set of names of objects implemented by the module,
- F is the union of sets of canonical traces of all foreign modules,
- I is the set of names of access programs,
- for each $i \in I$, E_i is a relation defined as follows:

$$\forall q, q' \in Q^{k_i}, r, r' \in F^{l_i} [E_i(q, r, q', r') \Leftrightarrow R_i(q, r, r', (q'_{p_i+1}, \ldots, q'_{k_i})) \wedge X_i(q, r, r', (q'_{p_i+1}, \ldots, q'_{k_i})) = (q'_1, \ldots, q'_{p_i})\ ]$$

It turns out that not all new trace-modules can be specified in the proposed version of TAM. It can happen that some of the reachable states are not trace-expressible. In such a case we are simply unable to represent these states in the specification. But if all reachable states of a new trace-module are trace-expressible then we can specify such a module in the proposed version of TAM.

Theorem: Let $M = (Q, q_0, O, F, I, E)$ be a new trace-module. If all reachable states of M are trace-expressible then there exists a new trace specification satisfied by M.

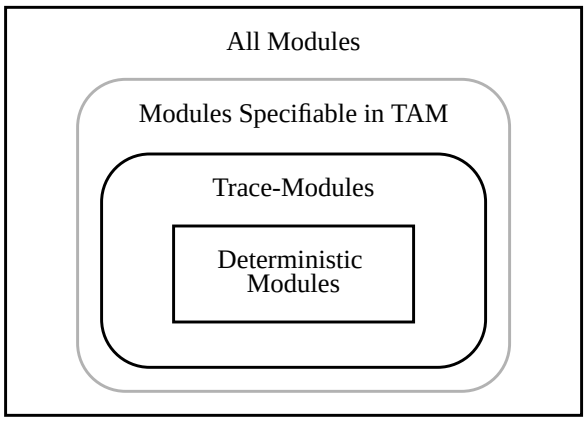
Proof of this theorem can be found in [5].

A class of modules which can be specified in the proposed version of TAM is the class of modules observationally equivalent to some new trace-modules having all (reachable) states trace-expressible.

7 Conclusions

The main goal of this paper is to investigate the expressiveness of TAM. As it was proved in [8], every single-object module can be specified in TAM. Also every deterministic multi-object module can be specified in TAM. However, there exists a non-deterministic multi-object module which cannot be specified in TAM.

We have defined a sub-class of modules (called trace-modules) which effectively characterizes the expressiveness of TAM. Each trace-module can be specified in TAM and each specification can be modelled by a trace-module. Hence, the class of multi-object modules which can be specified in TAM is the class of modules observationally equivalent to some trace-modules. This situation can be illustrated by the following diagram:



We have also proposed some modifications in TAM and we have defined an appropriate sub-class of modules (called new trace-modules) to model specifications in the proposed version of TAM. It is a property of this class that each module is observationally equivalent to some new trace-module. We have extended the expressiveness of TAM, although we have not covered the whole class of non-deterministic multi-object modules. Not all new trace-modules can be specified in the proposed version of TAM because it can happen that some (reachable) states of objects implemented by the module cannot be expressed by traces.

If we could express by traces all (reachable) states of objects implemented by new trace-modules then we would be able to specify all modules in TAM. This problem still limits the usefulness of TAM in specification of some non-deterministic multi-object modules. Extension of the expressiveness of traces, to cover all reachable states of new trace-modules, will be one of our goals in future research.

7 Bibliography

1. Bartussek, W., Parnas, D.L., "Using Traces to Write Abstract Specifications for Software Modules", in: *Proceedings of 2nd Conference of European Cooperation in Informatics*, Lecture Notes in Computer Science, 65. Springer-Verlag, Venice, 1978.
2. Bojanowski, J., Iglewski, M., Madey, J., Obaid, A., "Functional Approach to Protocol Specification", in: *Proceedings of the 14th International IFIP Symposium on Protocol Specification, Testing and Verification, PSTV'94*, Vancouver, B.C., pp. 371-378.
3. Erskine, N., "The usefulness of the trace assertion method for specifying device module interfaces", *CRL Report* No. 258, McMaster University, CRL, Telecommunication Research Institute of Ontario (TRIO), Hamilton, Ontario, Canada, 1992.
4. Hoffman, D.M., "The Trace Specification of Communications Protocols", *IEEE Transactions on Computers*, Vol. C-34, No. 12, December 1985, pp. 1102-1113.
5. Iglewski, M., Madey, J., Kubica, M, "Editor for the Trace Assertion Method", in: *Proceedings of the 10th International Conference of CAD/CAM, Robotics and Factories of the Future: CARs & FOF'94, M.Zaremba (Ed.)*, OCRI, Ottawa, Ontario, Canada, 1994, pp.976-881.
6. Iglewski, M., Madey, J., Kubica, M, "Trace Specifications of Non-deterministic Multi-object Modules", in: *Technical Report* TR 95-03 (204), Warsaw University, Institute of Informatics, Warsaw, Poland, 1995.
7. Iglewski, M., Madey, J., Parnas, D.L., Kelly, P.C., "Documentation Paradigms", *CRL Report* No. 270, McMaster University, CRL, Telecommunication Research Institute of Ontario (TRIO), Hamilton, Ontario, Canada, 1993.
8. Iglewski, M., Madey, J., Stencel, K., "On Fundamentals of the Trace Assertion Method", *Technical Report* TR 94-09 (198), Warsaw University, Institute of Informatics, Warsaw, Poland, 1994.
9. McLean, J.D., "A Formal Foundation for the Abstract Specification of Software", *Journal of the ACM*, Vol. 31, No. 3, July 1984, pp. 600-627.
10. Parnas, D.L., "On the Criteria to be used in Decomposing Systems into Modules", *Communications of the ACM*, Vol. 15, No. 12, December 1972, pp. 1053-1058.
11. Parnas, D.L., Madey, J., "Functional Documentation for Computer Systems Engineering. (Version 2)", *CRL Report* No. 237, McMaster University, CRL, Telecommunication Research Institute of Ontario (TRIO), Hamilton, Ontario, Canada, 1991; to appear in: *Science of Computer Programming*.
12. Parnas, D.L., Wang, Y., "The Trace Assertion Method of Module Interface Specification", *Technical Report* 89-261, Queen's University, C&IS, Telecommunication Research Institute of Ontario (TRIO), Kingston, Ontario, Canada, 1989.
13. Wang, Y., "Specifying and Simulating the Externally Observable Behavior of Modules", (Ph.D. Thesis), *CRL Report* No. 292, McMaster University, CRL, Telecommunication Research Institute of Ontario (TRIO), Hamilton, Ontario, Canada, 1994.