Checking Experiments with Labeled Transition Systems for Trace Equivalence *

Q. M. Tan†, A. Petrenko‡ and G. v. Bochmann†

†Département d'IRO, Université de Montréal
C.P. 6128, Succ. Centre-Ville, Montréal, (Québec) H3C 3J7, Canada
E-mail:(tanq,Bochmann)@iro.umontreal.ca Fax:(514)343-5834
‡CRIM, Centre de Recherche Informatique de Montréal
1801 Avenue McGill College, Montréal, (Québec) H3A 2N4, Canada
E-mail:petrenko@crim.ca Phone:(514)840-1234 Fax:(514)840-1244

ABSTRACT: We apply the state identification techniques for testing communication systems which are modeled labeled transition systems (LTSs). The conformance requirements of specifications are represented as the trace equivalence relation and derived tests have finite behavior and provide well-defined fault coverage. We redefine in the realm of LTSs the notions of state identification that were originally defined in the realm of input/output finite state machines (FSMs). Then we present the corresponding test generation methods and discuss their fault coverage. It is shown that for an FSM-based method with a notion of state identification we can have a corresponding LTS-based method with a similar notion of state identification, and if the FSM-based method guarantees complete fault coverage then the LTS-analogue also guarantees such coverage.

1 Introduction

One of the important issues of conformance testing is to derive useful tests for labeled transition systems (LTSs), which serve as a semantic model for various specification languages, e.g., LOTOS, CCS, and CSP. Testing theories and methods for test derivation in the LTS formalism have been developed in [3, 21, 16, 4, 7, 1, 18, 20]. In particular, a so-called **conf** relation and *canonical tester* [3] became the basis for a large body of work in this area.

Unfortunately, the canonical tester approach cannot be taken into account when test generation for real protocols is attempted. The canonical tester has infinite behavior whenever the specification describes an infinite behavior; no fault coverage is measured for the individual tests derived in [21] or n-testers derived in [16]. Moreover, we believe that the **conf** relation alone is too weak as a criterion to accept an implementation, because only the deadlocks that are implemented after the valid traces in the specification are to be checked. Since this

*This work was supported by the HP-NSERC-CITI Industrial Research Chair on Communication Protocols, Université de Montréal

relation does not deal with invalid traces, it allows for a trivial implementation which has a single state with looping transitions labeled with all possible actions, and such an implementation conforms to any LTS specification with the same alphabet with respect to the **conf** relation [19]. Thus even though an implementation is concluded being valid based on **conf**, another relation, such as *trace-equivalence*, has to be tested as well.

Observing and comparing traces of executed interactions is usual means for conformance testing of protocols, and in many cases it is required that an implementation should have the same traces as its specification. In particular, most existing protocols are deterministic, and in the case of determinism several other finer testing semantics [23], such as failure or failure trace, are reduced to the trace semantics. Based on the notion of such experiments and the trace equivalence relation, a number of competing test derivation methods with fault coverage have been elaborated [10, 5, 17, 24, 9, 14, 12, 13] for protocols in the formalism of input/output finite state machines (FSMs), many of which use the state identification techniques to obtain better fault coverage. Compared to FSMs, LTSs are in some sense a more general descriptive model which use rendezvous communication without distinction between input and output; there are various criteria determining whether an implementation conforms to a specification [23]; most existing test derivation methods use the exhaustive testing approach in order to prove the correctness of the implementation in respect to a given conformance relation. Apparently, such an approach is often impractical since it may involve a test suite of infinite length. The approximation approach [16, 21], such as n-testers, which is proposed to solve this problem, provides no fault coverage measure for conformity of the implementation with its specification.

Conformance testing should be developed in such a way that the given conformance relation is determined by the real conformance requirements and test suites have finite behavior and ensure well-defined fault coverage. Several attempts have been made to apply the ideas underlying the FSM-based methods to the LTS model [8, 4, 1, 18, 19] for several conformance relations. In particular, this research is directed towards redefining the notions of state identification in the LTS realm for a given relation. [4] tries the UIO-based state identification [17]. [8] considers the characterization sets [5]. [1] introduces the state identification machines. In [15, 18], another approach is taken, where an LTS is represented as an FSM model, an existing FSM-based method is applied, and then the derived tests are translated back into the LTS formalism. In [19], the HSI method [14, 13] is adapted for trace equivalence.

However, these attempts are limited to individual or informal applications of the notions of state identification underlying the FSM-based methods. In fact, the FSM-based notions can also be applied directly to the LTS model if an appropriate distinguishabilty of states is defined in the LTS model. In the FSM model, two states are distinguished if different output behaviors are observed when a common input sequence is applied to the two states, respectively. In the LTS model, two states can be distinguished if, after a common sequence of interactions, a given action be executed for one of the two states while the same action cannot be executed for the other. Therefore, a systematic approach based on the notions of state identification can also be developed in the LTS model such that we could devise alternative and competing techniques that guarantees fault coverage, for constructing useful tests for protocols based on the LTS semantics.

In this paper, based on the framework of testing LTSs [20] in respect to trace equivalence, we redefine in the LTS model the notions of state identification which were originally used in the FSM realm. Based on the adapted notions, the corresponding test derivation methods are

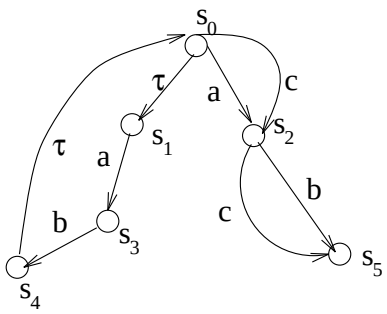

Figure 1: An LTS graph

presented, and it is shown that for an FSM-based method with a notion of state identification we can have a corresponding LTS-based method with a similar notion of state identification, and if the FSM-based method guarantees complete fault coverage then the LTS-analogue also guarantees complete fault coverage.

2 Labeled Transition Systems

Definition 1 (*Labeled transition system (LTS)*): A labeled transition system is a 4-tuple $< S, \Sigma, \Delta, s_0 >$, where

- S is a finite set of states, $s_0 \in S$, is the initial state.
- Σ is a finite set of labels, called observable actions; $\tau \notin \Sigma$ is called an internal action.
- $\Delta \subseteq S \times (\Sigma \cup \{\tau\}) \times S$ is a transitions set. $(p, \mu, q) \in \Delta$ is denoted by $p - \mu \rightarrow q$.

An LTS is said to be *nondeterministic* if it has some transition labeled with τ or there exist $p - a \rightarrow p_1, p - a \rightarrow p_2 \in \Delta$ but $p_1 \neq p_2$. A *deterministic* LTS has no internal actions and the outgoing transitions of any state are uniquely labeled.

An LTS can also be represented by a directed graph where nodes are states and labeled edges are transitions. An LTS graph is shown in Figure 1.

Given an LTS $\mathsf{S} =< S, \Sigma, \Delta, s_0 >$, let $p, q \in S$ and $\mu \in \Sigma \cup \{\tau\}$, the conventional notations shown in Table 1 are relevant to a given LTS, as introduced in [3]. In this paper we use $\mathsf{M}, \mathsf{P}, \mathsf{S}, \ldots$ to represent LTSs; $M, P, Q, \ldots$, for sets of states; $a, b, c, \ldots$, for actions; and $i, p, q, s \ldots$, for states. The sequences in $Tr(p)$ are called the *traces* of S in p.

Given a set of sequences $V \in \Sigma^*$, we use the notation $Pref(V)$ to represent all prefixes of sequences in V. Formally, $Pref(V) = \{\sigma_1 \in \Sigma^* \mid \exists \sigma_2 \in \Sigma^* \ (\sigma_1.\sigma_2 \in V)\}$. We also use "@" to represent the concatenation of two sets of sequences. Formally, assuming $V_1, V_2 \subseteq \Sigma^*$, $V_1 @ V_2 = \{\sigma_1.\sigma_2 \mid \sigma_1 \in V_1 \wedge \sigma \in V_2\}$. We also write $V^n = V @ V^{n-1}$ for $n > 0$ and $V^0 = \{\varepsilon\}$.

In the case of nondeterminism, after an observable action sequence, an LTS may enter a number of different states. In order to consider all these possibilities, a state subset (multi-state [8]), which contains all the states reachable by the LTS after this action sequence, is used.

Definition 2 (*Multi-state set*): The multi-state set of LTS S is the set $\Pi_S = \{S_i \subseteq S \mid \exists \sigma \in \Sigma^* \ (s_0\textbf{-after-}\sigma = S_i)\}$.

notation	meaning
Σ^*	set of sequences over Σ; σ or $a_1 \ldots a_n$ denotes such a sequence
$p - \mu_1 \ldots \mu_n \rightarrow q$	there exists p_k, $1 \leq k < n$, such that $p - \mu_1 \rightarrow p_1 \ldots p_{n-1} - \mu_n \rightarrow q$
$p = \varepsilon \Rightarrow q$	$p - \tau^n \rightarrow q$ $(1 \leq n)$ or $p = q$ (note: τ^n means n times τ)
$p = a \Rightarrow q$	there exist p_1, p_2 such that $p = \varepsilon \Rightarrow p_1 - a \rightarrow p_2 = \varepsilon \Rightarrow q$
$p = a_1 \ldots a_n \Rightarrow q$	there exists p_k, $1 \leq k < n$, such that $p = a_1 \Rightarrow p_1 \ldots p_{n-1} = a_n \Rightarrow q$
$p = \sigma \Rightarrow$	there exists q such that $p = \sigma \Rightarrow q$
$p \neq \sigma \Rightarrow$	no q exists such that $p = \sigma \Rightarrow q$
$init(p)$	$init(p) = \{a \in \Sigma \mid p = a \Rightarrow\}$
p-**after**-σ	p-**after**-$\sigma = \{q \in S \mid p = \sigma \Rightarrow q\}$; S-**after**-$\sigma = s_0$-**after**-σ
$Tr(p)$	$Tr(p) = \{\sigma \in \Sigma^* \mid p = \sigma \Rightarrow\}$; $Tr(\mathsf{S}) = Tr(s_0)$

Table 1: Basic notations for labeled transition systems

Note that $S_0 = s_0$-**after**-ε is in Π_S and is called the *initial multi-state*. The multi-state set can be obtained by a known algorithm which performs the deterministic transformation of a nondeterministic automaton with trace equivalence [11, 8]. For Figure 1, the multi-state set is $\{\{s_0, s_1\}, \{s_2, s_3\}, \{s_2\}, \{s_0, s_1, s_4, s_5\}, \{s_5\}\}$.Obviously, each LTS has one and only one multi-state set.

After any observable sequence, a nondeterministic system reaches a unique multi-state. Thus from the test perspective, it makes sense to identify multi-states, rather than single states. This viewpoint is reflected in the FSM realm by the presentation of a nondeterministic FSM as an observable FSM [12], in which each state is a subset of states of the non-observable FSM. The viewpoint is also reflected by the *refusal graphs* [7], in which a node corresponds to a multi-state.

3 Conformance Testing

3.1 Conformance Relation

The starting point for conformance testing is a specification in some (formal) notation, an implementation given in the form of a black box, and the conformance requirements that the implementation should satisfy. In this paper, the notation of the specification is the LTS formalism; the implementation is assumed to be described in the same model as its specification; a conformance relation, called *trace equivalence*, is used to formalize the conformance requirements. We say that an implementation M conforms to a specification S if M is trace-equivalent to S.

Definition 3 (*Trace equivalence*): The trace equivalence relation between two states p and q, written $p \approx q$, holds iff $Tr(p) = Tr(q)$.
Given two LTSs S and M with initial states s_0 and m_0 respectively, we say that M is trace-equivalent to S, written $\mathsf{M} \approx \mathsf{S}$, iff $m_0 \approx s_0$.

We say that two states are *distinguishable* in trace semantics if they are not trace-equivalent. For any two states that are not trace-equivalent we can surely find a sequence of observable

actions, which is a trace one of the two states, not both, to distinguish them. We also say that an LTS is *reduced* in trace semantics if all of its states are distinguishable in trace semantics.

3.2 Testing Framework

Conformance testing is a finite set of experiments, in which a set of test cases, usually derived from a specification according to a given conformance relation, is applied by a tester or experimenter to the implementation under test (IUT), such that from the results of the execution of the test cases, it can be concluded whether or not the implementation conforms to the specification.

The behavior of the tester during testing is defined by the applied test case. Thus a test case is a specification of behavior, which, like other specifications, can be represented as an LTS. An experiment should last for a finite time, so a test case should have no infinite behavior. Moreover, the tester should have certain control over the testing process, so nondeterminism in a test case is undesirable [19, 22].

Definition 4 (*Test cases and test suite*): Given an LTS specification $\mathsf{S} =< S, \Sigma, \Delta, s_0 >$, a test case T for S is a 5-tuple $< T, \Sigma_T, \Delta_T, t_0, \ell >$ where:

- $\Sigma_T \subseteq \Sigma$;
- $< T, \Sigma_T, \Delta_T, t_0 >$ is a deterministic, tree-structured LTS such that for each $p \in T$ there exists exactly one $\sigma \in \Sigma_T^*$ with $t_0 = \sigma \Rightarrow p$;
- $\ell : T \rightarrow \{\mathbf{pass}, \mathbf{fail}, \mathbf{inconclusive}\}$ is a state labeling function.

A test suite for S is a finite set of test cases for S.

From this definition, the behavior of test case T is finite, since it has no cycles. Moreover, a trace of T uniquely determines a single state in T, so we define $\ell(\sigma) = \ell(t)$ for $\{t\} = t_0$-**after**-σ.

The interactions between a test case T and the IUT M can be formalized by the composition operator "$\|$" of LOTOS, that is, $\mathsf{T} \| \mathsf{M}$. When $t_0 \| m_0$ after an observable action sequence σ reaches a *deadlock*, that is, there exists a state $p \in T \times M$ such that for all actions $a \in \Sigma$, $t_0 \| m_0 = \sigma \Rightarrow p$ and $p \neq a \Rightarrow$, we say that this experiment completes a *test run*. In order to start a new test run, a global reset is always assumed in our testing framework.

Usually, LTSs are supposed to be nondeterministic. In order to test nondeterministic implementations, one usually makes the so-called *complete-testing assumption:* it is possible, by applying a given test case to the implementation a finite number of times, to exercise all possible execution paths of the implementation which are traversed by the test case [8, 13]. Therefore any experiment, in which M is tested by T, should include several test runs and lead to a complete set of observations $Obs_{(\mathrm{T,M})} = \{\sigma \in Tr(t_0) \mid \exists p \in T \times M, \forall a \in \Sigma\ ((t_0 \| m_0) = \sigma \Rightarrow p \neq a \Rightarrow)\}$. Note that for deterministic systems, such as most of real-life protocols, there is no need for this assumption.

Based on $Obs_{(\mathrm{T,M})}$, the success or failure of testing needs to be concluded. The way a verdict is drawn from $Obs_{(\mathrm{T,M})}$ is the *verdict assignment* for T: $Obs_{(\mathrm{T,M})} \Rightarrow \{pass, fail\}$. A *pass* verdict means success, which, intuitively, should mean that no unexpected behavior is found and the test purpose has been achieved; otherwise, the verdict should be *fail*. If we define *the test purpose* of T, written $Pur(\mathsf{T})$, to be $Pur(\mathsf{T}) = \{\sigma \in Tr(t_0) \mid \ell(\sigma) = \mathbf{pass}\}$, then the conclusion can be drawn as follows.

Definition 5 (*Verdict assignment*): Given an IUT M, a test case T, let $Obs_{fail} = \{\sigma \in Obs_{(\mathrm{T,M})} \mid \ell(\sigma) = \textbf{fail}\}$ and $Obs_{pass} = \{\sigma \in Obs_{(\mathrm{T,M})} \mid \ell(\sigma) = \textbf{pass}\}$,

$$\begin{cases} \mathsf{M} \text{ passes } \mathsf{T} & \text{iff } Obs_{fail} = \emptyset \wedge Obs_{pass} = Pur(\mathsf{T}) \\ \mathsf{M} \text{ fails } \mathsf{T} & \text{otherwise.} \end{cases}$$

Given a test suite TS, we also denote that M passes TS iff for all $\mathsf{T} \in TS$ M passes T, and M fails TS otherwise.

3.3 State Labelings of Test Cases

Given a specification S, the state labeling function of test cases T must be "sound", that is, for any implementation M, if M and S are trace-equivalent, then M passes T.

In the context of trace equivalence, a conforming implementation should have the same traces as a given specification. Therefore each test case specifies certain sequences of actions, which are either valid or invalid traces of the specification. The purpose of a test case is to verify that an IUT has implemented the valid ones and not any of the invalid ones. Accordingly, we conclude that all test cases for trace equivalence must be of the following form [20]:

Definition 6 (*Test cases for trace equivalence*): Given an LTS specification S, a test case T is said to be a test case for S w.r.t. $\approx$, if, for all $\sigma \in Tr(t_0)$ and $\{t_i\} = t_0$-**after**-σ, the state labeling of T satisfies

$$\ell_{\approx}(t_i) = \begin{cases} \textbf{pass} & \text{if } \sigma \in Tr(s_0) \wedge init(t_i) \cap out(s_0\text{-}\textbf{after}\text{-}\sigma) = \emptyset \\ \textbf{fail} & \sigma \notin Tr(s_0) \\ \textbf{inconclusive} & \text{otherwise.} \end{cases}$$

A test suite for S w.r.t. $\approx$ is a set of test cases for S w.r.t. $\approx$.

From this definition, we have the following proposition [20]: Given a test case T for S w.r.t. $\approx$, for any LTS M, if $\mathsf{M} \approx \mathsf{S}$, then M passes T.

Since in trace semantics test cases for S are represented as valid or invalid traces of S, given a sequence $\sigma \in \Sigma^*$, let $\sigma = a_1.a_2 \ldots .a_n$, a test case T for S w.r.t. $\approx$ can be obtained by constructing an LTS $\mathsf{T} = t_0 - a_1 \rightarrow t_1 \ldots t_{n-1} - a_n \rightarrow t_n$ and then labeling T according to Definition 6. A sequence that is used to form a test case is also called a *test sequence*.

3.4 Fault Model and Fault Coverage

The goal of conformance testing is to gain confidence in the correct functioning of the implementation under test. Increased confidence is normally obtained through time and effort spent in testing the implementation, which, however, is limited by practical and economical considerations. In order to have a more precise measure of the effectiveness of testing, a fault model and fault coverage criteria [2] are introduced, which usually take the mutation approach [2], that is, a fault model is defined as a set of all faulty LTS implementations considered. Here we consider a particular fault model $\mathcal{F}(m)$ which consists of all LTS implementations over the alphabet of the specification S and with at most m multi-states, where m is a known integer. Based on $\mathcal{F}(m)$, a test suite with complete fault coverage for a given LTS specification with respect to the trace equivalence relation can be defined as follows.

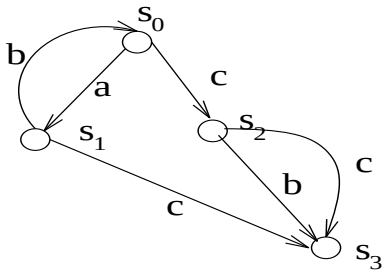

Figure 2: A corresponding trace observable system of Figure 1

Definition 7 (*Complete test suite*): Given an LTS specification S and the fault model $\mathcal{F}(m)$, a test suite *TS* for S w.r.t. $\approx$ is said to be complete, if for any M in $\mathcal{F}(m)$, M $\approx$ S iff M passes *TS*.

We also say that a test suite is *m-complete* for S if it is complete for S in respect to the fault model $\mathcal{F}(m)$. A complete test suite guarantees that for any implementation M in the context of the given fault model, if M passes all test cases, it must be a conforming implementation of the given specification with respect to the given conformance relation, and any faulty implementation in $\mathcal{F}(m)$ must be detected by failing at least one test case in the test suite.

4 State Identification in Specifications

Similar to the case of FSMs, in order to identify states in a given LTS specification, at first the specification is required to have certain testability properties, two of which are the so-called reducibility and observability.

4.1 Trace Observable System

Definition 8 (*Trace observable system (TOS)*): Given an LTS S, a deterministic LTS $\overline{\mathsf{S}}$ is said to be the trace observable system corresponding to S, if $\overline{\mathsf{S}} \approx \mathsf{S}$ and $\overline{\mathsf{S}}$ is reduced in trace semantics.

From the above definition, the TOS $\overline{\mathsf{S}}$ of S is deterministic, reduced and trace-equivalent to S; moreover, the TOS $\overline{\mathsf{S}}$ is unique for all LTSs trace-equivalent to S. There are the algorithms and tools that transform a given LTS into its TOS form [11, 4]. For the LTS in Figure 1, the TOS is given in Figure 2.

In the context of trace semantics, for any LTS, the corresponding TOS models all its observable behavior. Therefore, for test generation, any LTS considered can be assumed to be in the TOS form.

4.2 State Identification Facilities

There are the following facilities of state identification which can be adapted from the FSM model to the LTS model. Here we assume that the given LTS specification S is in the TOS form that has n states $s_0, s_1, \ldots s_{n-1}$, where s_0 is the initial state.

Distinguishing Sequence

Given an LTS S, we say that an observable sequence distinguishes two states if the sequence has a prefix that is a trace for one of the two states, but not for both. A *distinguishing sequence* for S is an observable sequence that distinguishes any two different states. Formally, $\sigma \in \Sigma^*$ is a distinguishing sequence of S if for all $s_i, s_j \in S, i \neq j$, there exists $\sigma' \in Pref(\sigma)$ such that $\sigma' \in Tr(s_i) \oplus Tr(s_j)$. Given two sets A and B, $A \oplus B = (A \backslash B) \cup (B \backslash A)$.

There are LTSs in the TOS form without any distinguishing sequence. As an example, the LTS in Figure 2 has no distinguishing sequence.

Unique Sequences

A *unique sequence* for a state is an observable sequence that distinguishes the given state from all others. Formally, $\sigma_i \in \Sigma^*$ is a unique sequence for $s_i \in S$, if, for all $s_j \in S, i \neq j$, there exists $\sigma'_i \in Pref(\sigma_i)$ such that $\sigma'_i \in Tr(s_i) \oplus Tr(s_j)$. Let S have n states, a tuple of unique sequences $< \sigma_0, \sigma_1, \ldots, \sigma_{n-1} >$ is said be set of unique sequences for S. If there exists $\sigma \in \Sigma^*$ such that $\sigma_i \in Pref(\sigma)$, for $0 \leq i \leq n-1$, then σ is a distinguishing sequence. The notion of unique sequences, also called unique event sequences in [4], corresponds to that of FSM-based UIO sequences [17].

For the LTS in Figure 2, we may choose $< a, b.a, b.a, c >$ as its unique sequences. Note that unique sequences do not always exist. For example, if the transition $s_2 \text{—} c \rightarrow s_3$ in Figure 2 is deleted, then no unique sequence exists for s_3 in the resulting LTS.

Characterization Set

If a set of observable sequences, instead of a unique distinguishing sequence, is used to distinguish all the states of S, we have a so-called *characterization set* for S. A characterization set for S is a set $W \subseteq \Sigma^*$ such that for all $s_i, s_j \in S, i \neq j$, there exists $\sigma_i \in Pref(W)$ such that $\sigma_i \in Tr(s_i) \oplus Tr(s_j)$.

There exists a characterization set W for any S in the TOS form. For the LTS in Figure 2, we may choose $W = \{a, b.a\}$.

Partial Characterization Set

A tuple of sets of observable sequences $< W_0, W_1, \ldots, W_{n-1} >$ is said to be *partial characterization sets*, if, for all $s_i \in S, 0 \leq i \leq n-1$, and for all $s_j \in S, i \neq j$, there exists $\sigma_i \in Pref(W_i)$ such that $\sigma_i \in Tr(s_i) \oplus Tr(s_j)$. The notion of partial characterization sets correspond to the notion of partial UIO sequences in [6].

Obviously, since the given S is in the TOS form, in other words, none of its two states are trace-equivalent, there exist partial characterization sets for S. We also note that the union of all partial characterization sets for S is a characterization set for S. For the LTS in Figure 2, we may choose $< \{a\}, \{b.a\}, \{b.a\}, \{a, b\} >$ as its partial characterization sets.

Harmonized State Identifiers

A tuple of sets of observable sequences $< H_0, H_1, \ldots, H_{n-1} >$ is said to be a set of *harmonized state identifiers* for S, if it is a tuple of partial characterization sets for S and for $i, j = 0, 1, \ldots, n-1, i \neq j$, there exists $\sigma \in Pref(H_i) \cap Pref(H_j)$. H_i also is said to be a harmonized identifier for $s_i \in S$. The harmonized identifier for s_i captures the following property: for any different state s_j, there exists a sequence σ_i in $Pref(H_i)$ that distinguishes s_i from s_j and σ_i is also in $Pref(H_j)$.

Harmonized state identifiers always exist, just as partial characterization sets do. As an example, for the LTS in Figure 2, we can choose the harmonized state identifiers $H_0 =$

$\{a,b\}, H_1 = \{b.a\}, H_2 = \{b.a\}, H_3 = \{a,b\}$. Considering H_0: a is used to distinguish $\overline{s}_0$ from $\overline{s}_3$, so a is also in H_3; b is used to distinguish $\overline{s}_0$ from $\overline{s}_1$ and $\overline{s}_2$, so H_1 and H_2 have $b.a$ where b is its prefix.

5 State Identification in Implementations

Similar to FSM-based testing, we assume that the given implementation is an LTS M whose set of all possible actions is limited to the set of actions Σ of the specification S (the correct interface assumption [2]). We also have a reliable reset, such that the state entered when this implementation is started or after the reset is applied is the initial state (the reliable reset assumption [25]). In the case of nondeterminism, it makes no sense to identify single states of M, so M is also assumed to be a TOS, in which each multi-state consist of a single state. For this reason, we require that S is in the TOS form, so that a state identification facility can be developed from S and also can be used to identify the states of M.

In order to identify the states of the implementation M, the number of states of M is also assumed to be bound by a known integer m. Therefore, M is also a mutant according to the fault model $\mathcal{F}(m)$.

Similar to FSM-based testing [9], there are also the two phases for LTS-based testing. In the first phase, the used state identification facility is applied to M to check if it can also properly identify the states in M. Once M passes the first phase, we can in the second phase test whether each transition and its tail state are correctly implemented. We present the structure of tests for the two phases using harmonized state identifiers as an example. In order to perform the first testing phase, proper transfer sequences are needed to bring M from the initial state to those particular states in M to which H_i should be applied. Moreover, it should be guaranteed that all the sequences in H_i are applied to the same particular state in M. Since a reliable reset is assumed, we can guarantee this in a way similar to FSM based testing: after a sequence in H_i is applied, the implementation M is reset to the initial state, and brought into the same particular state by the same transfer sequence,and then another sequence in H_i is applied. This process is repeated until all the sequences are applied.

Accordingly, let Q be a *state cover for* S, i.e. for each state s_i of S, there exists exactly one input sequence σ in Q such that $s_0 - \sigma \rightarrow s_i$, similar to FSM based testing, we can use $< N_0, N_1, \ldots N_{n-1} >$ to cover all states of M (a *state cover for* M), where

$$N_i = \{\sigma \in Q @ (\Sigma^0 \cup \Sigma_1 \cup \ldots \cup \Sigma^{m-n}) \mid s_0 = \sigma \Rightarrow s_i\}$$

and construct a set of test sequences to be executed by M from the initial state in the first testing phase as follows:

$$TS_1 = \bigcup_{i=0}^{n} N_i @ H_i$$

Inituitively, sequences of the sets N_i are used to reach n required states, as well as all possible $(m-n)$ additional states in M. Harmonized state identifiers H_i are applied to identify all states in M. In order to execute a given sequence $\sigma = a_1.a_2 \ldots a_k$ from the initial state m_0, we can convert σ into an LTS $t_0 - a_1 \rightarrow t_2 \ldots - a_k \rightarrow t_k$ and then compose this LTS with M in parallel composition $t_0 \parallel m_0$. Due to nondeterminism, it is possible that this run ends

before the final action of this sequence is executed. Several runs are needed to exercise all the possible paths of M that can be traversed by this sequence (the complete testing assumption).

Using TS_1, we can make test cases for LTS S for the first testing phase by transforming the sequences in TS_1 into the corresponding LTSs as above and then labeling the LTSs according to Definition 6. In the following, this transforming and labeling process is always implied if we say that a test suite is obtained from a given set of test sequences.

After TS_1 is successfully executed, all the states of M which execute all traces of H_k are grouped in the same group $f(s_k)$, where $0 \leq k \leq n-1$.

In the second phase of testing, for testing a given defined transition $s_i - a \rightarrow s_j$ in S, it is necessary to first bring M into each state $m_k \in f(s_i)$, then apply a at this state to see if a can be executed; moreover, let M be in m_l after a is executed, it is necessary to check that $m_l \in f(s_j)$ which should be verified by H_j. (Note that due to nondeterminism, m_k may really be a multi-state, the action that is expected to check may not be executed in a time, so the above process should be tried several times.) On the other hand, we should further check if any undefined transition out of s_i has been implemented in M, i.e. for each $b \in \Sigma$, if $s_i \not- b \rightarrow$, then check that $m_k = b \Rightarrow$ does not exist. Because if $m_k - b \rightarrow$ exists, M is surely an invalid implementation, so it is not necessary to verify the tail state after b is executed.

Obviously, N_i may be used to bring M to any state $m_k \in f(s_i)$. Using this state cover, we can obtain a *valid transition cover* $< E_0, E_1, \ldots E_{n-1} >$, where

$$E_i = \{\sigma \in \bigcup_{k=0}^{n-1} (N_k @ \Sigma) \mid s_0 = \sigma \Rightarrow s_i\}$$

which covers all transitions that should be present in any conforming implementation, and an *invalid transition cover* $\overline{E}$,

$$\overline{E} = \{\sigma.a \in \bigcup_{k=0}^{n-1} (N_k @ \Sigma) \mid \exists s_i \in S \ (s_0 = \sigma \Rightarrow s_i \neq a \Rightarrow)\}$$

which covers all transitions that should be absent in any conforming implementation.

Next, H_i is used to verify the tail states of reached after each sequence in E_i. Excluding the transitions that have already been tested in the first testing phase, we can construct the set of test sequences for the second testing phase as follows:

$$TS_2 = \overline{E} \cup (\bigcup_{i=0}^{n-1} (E_i \backslash N_i) @ H_i)$$

We conclude that the set of test sequences is expressed as follow, by combining the two sets of test sequences for the first and second testing phases:

$$\begin{aligned} TS &= TS_1 \cup TS_2 = (\bigcup_{i=0}^{n-1} N_i @ H_i) \cup \overline{E} \cup (\bigcup_{i=0}^{n-1} (E_i \backslash N_i) @ H_i) \\ &= \overline{E} \cup (\bigcup_{i=0}^{n-1} E_i @ H_i) \end{aligned}$$

We have seen that the above checking experiments for the LTS model is an analogue of the checking experiments for the FSM model, except that invalid transitions need to be tested

although their tail states need not to be verified. Similarly, it is expected that a test suite which is derived from S based on the above process is complete with respect to trace equivalence for the fault model $\mathcal{F}(m)$. In the next section, we present the LTS-based test generation methods, based on various state identification facilities presented in Section 4.2.

6 Test Generation

6.1 Methods

Based on the existing state identification techniques, we have a number of methods for constructing a set TS of test sequences for a given LTS specification S and with certain fault coverage for the fault model $\mathcal{F}(m)$. Let S be given in the form of a TOS with n states. We can obtain the state cover for implementation $< N_0, N_1, \ldots N_{n-1} >$, the valid transition cover for implementation $< E_0, E_1, \ldots E_{n-1} >$ and the invalid transition cover for implementation $\overline{E}$ as presented in the above section. Let $E = \bigcup_{i=0}^{n-1} E_i$ and $N = \bigcup_{i=0}^{n-1} N_i$.

The DS-method

Similar to the FSM-based DS-method [10], we use a distinguishing sequence σ for S to form a test suite for S, as follows.

$$TS \quad = \quad E@\{\sigma\} \cup \overline{E} \tag{1}$$

Theorem 1 *Given an LTS specification* S *in the TOS form and a distinguishing sequence* σ *for* S*, the test suite obtained from TS as given in (1) is an* m*-complete test suite for* S *w.r.t.* $\approx$.

Unlike the traditional FSM-based DS-method, the LTS-based DS-method does not construct a single test sequence since a reliable reset exists. It seems that, in case of a deadlock, the reset is the only way to continue test execution.

The US-method

Let $< \sigma_0, \sigma_1, \ldots, \sigma_{n-1} >$ be a set of unique sequences for S, then a test suite for S, which is an analogue of that derived by the FSM-based UIO-method [17], can be formed as

$$TS \quad = \quad (\bigcup_{i=0}^{n-1} E_i@\{\sigma_i\}) \cup \overline{E} \tag{2}$$

As a specific case, unique sequences might be prefixes of the same (distinguishing) sequence. For the same reason explained in relation with the DS-method, the US-method does not combine unique sequences using the rural Chinese postman tour algorithm to obtain an optimal single test sequence.

Since unique sequences do not always exist, the US-method can be improved if partial characterization sets are used instead of unique sequences. This corresponds to the improvement on the UIO-method in [6]. Although partial characterization sets exist for any LTS in the form of a TOS, like the US-method, the improvement can not guarantee that a derived test suite is m-complete.

A similar LTS-based test derivation method borrowing the notion of UIO sequences in the FSM model is proposed in [4], in which unique sequences are called unique event sequences. This method does not check invalid transitions, so it may not cover a fault where an undefined transition has been implemented in the implementation.

The Uv-method

In order to obtain an m-complete test suite, the US-method can be improved such that

$$TS \quad = \quad N@(\bigcup_{i=0}^{n-1} \sigma_i) \cup (\bigcup_{i=0}^{n-1} (E_i \backslash N_i)@\{\sigma_i\}) \cup \overline{E} \tag{3}$$

Theorem 2 *Given an LTS specification* S *in the TOS form and a set of unique sequences* $< \sigma_0, \sigma_1, \ldots, \sigma_{n-1} >$ *for* S*, the test suite obtained from TS as given in (3) is an m-complete test suite for* S *w.r.t.* $\approx$*.*

The length of a set of test sequences derived by the Uv-method is usually larger than that of a set of test sequences derived by the US-method. However, unlike the US-method, it guarantees complete fault coverage. The Uv-method corresponds to the FSM-based UIOv-method [24].

The W-method

Given a characterization set W for S, we form a test suite for S by the following formula. This is an LTS-analogue of the FSM-based W-method [5].

$$TS \quad = \quad E@W \cup \overline{E} \tag{4}$$

Theorem 3 *Given an LTS specification* S *in the TOS form and a characterization set W for* S*, the test suite obtained from TS as given in (4) is an m-complete test suite for* S *w.r.t.* $\approx$*.*

We note that in the case that $|W| = 1$, the W-method is the DS-method.

The Wp-method

Let W be a characterization set for S and $< W_0, W_1, \ldots, W_{n-1} >$ be partial characterization sets for S, similar to the FSM-based Wp-method [9], the Wp-method uses the following test sequences to form a test suite for S

$$TS \quad = \quad N@W \cup (\bigcup_{i=0}^{n-1} (E_i \backslash N_i)@W_i) \cup \overline{E} \tag{5}$$

Theorem 4 *Given an LTS specification* S *in the TOS form, a characterization set W and partial characterization sets* $< W_0, W_1, \ldots, W_{n-1} >$ *for* S*, the test suite obtained from TS as given in (5) is an m-complete test suite for* S *w.r.t.* $\approx$*.*

Obviously, a test suite derived from the Wp-method is a subset of a test suite derived by the W-method using the union of the W_i as the W set. We note that the Uv-method is a specific case of the Wp-method, in which the union $\bigcup_{i=0}^{n-1} \sigma_i$ is a characterization set and $< \{\sigma_0\}, \{\sigma_1\}, \ldots, \{\sigma_{n-1}\} >$ are partial characterization sets.

The HSI-method

Let $< H_0, H_1, \ldots, H_{n-1} >$ be harmonized state identifiers for S, similar to the FSM-based HSI-method [14, 13], The HSI-method follows completely the approach presented in the above section to form a test suite for S.

$$TS = (\bigcup_{i=0}^{n-1} E_i @ H_i) \cup \overline{E} \tag{6}$$

Theorem 5 *Given an LTS specification* S *in the TOS form and harmonized state identifiers* $< H_0, H_1, \ldots, H_{n-1} >$ *for* S*, the test suite obtained from TS as given in (6) is an m-complete test suite for* S *w.r.t.* $\approx$.

Since the union $\bigcup_{i=0}^{n-1} H_i$ is a characterization set, the length of a test suite derived by the HSI-method is usually less than that of a test suite derived by the W-method.

The Wp-method and the HSI-method are two basic methods; all the other methods are reduced to their specific or simplified cases. For example, the DS-method is a specific case of the W-method, the Uv-method is a specific case of the Wp-method, while the Wp-method is an improved case of the W-method. On the other hand, the HSI-method is an improved case not only of the US-method, but also of the W-method. Thus in order to prove all the above theorems, it is enough to prove the Wp-method and the HSI-method.

6.2 Examples

Assuming that the specification is given in Figure 2, with the HSI-method, we can derive a 4-complete test suite, which checks trace equivalence with respect to this specification, as well as to the specification in Figure 1 which has the same traces, as follows.

	s_0	s_1	s_2	s_3
State Identifiers H_i	$a,\ b$	$b.a$	$b.a$	$a,\ b$
State Cover Q	ε	a	c	$a.c$
Valid Transition Cover E_i	$\varepsilon,\ a.b$	a	c	$a.c,\ c.b,\ c.c$
Invalid Transition Cover $\overline{E} = \{b,\ a.a,\ c.a,\ a.c.a,\ a.c.b,\ a.c.c\}$				

$TS = \{b,\ a.a,\ c.a,\ a.b.b,\ a.b.a,\ a.c.a,\ a.c.b,\ a.c.c,\ c.b.a,\ c.b.b,\ c.c.a,\ c.c.b\}$. The corresponding test cases are shown in Figure 3.

Similarly, we could also use the Wp-method to derive a 4-complete test suite for the specification.

	s_0	s_1	s_2	s_3
W_i	a	$b.a$	$b.a$	$a,\ b$
Q	ε	a	c	$a.c$
E_i	$\varepsilon,\ a.b$	a	c	$a.c,\ c.b,\ c.c$
$W = \{a,\ b.a\}$ $\overline{E} = \{b,\ a.a,\ c.a,\ a.c.a,\ a.c.b,\ a.c.c\}$				

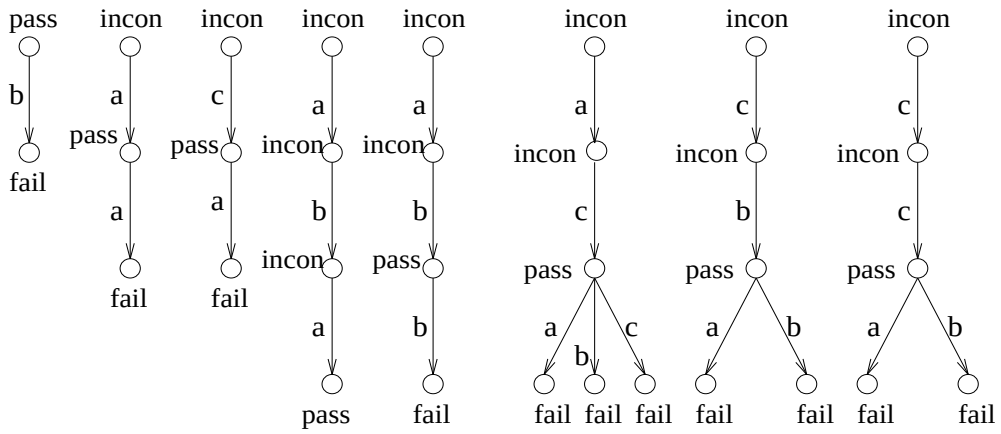

Figure 3: A complete test suite for the LTS specification in Figure 2.1

$TS = \{b.a,\ a.a,\ c.a,\ a.b.a,\ a.c.a,\ a.c.b.a,\ a.c.c,\ c.b.a,\ c.b.b,\ c.c.a, c.c.b\}$.

We note that a characterization set W may contain sequences whose suffixes are not necessary for the identification of some states; thus it follows that the tests derived by the Wp-method may have certain redundancy. For example, the W set in the above example includes $b.a$, in which the suffix a is not necessary to identify the initial state s_0 because b should be blocked in the corresponding state for any conforming implementation. The HSI-method can avoid the redundancy if appropriate harmonized state identifiers are selected such that they do not contain such suffixes.

7 Conclusion

Labeled transition systems (LTSs) are the basic semantics for the LOTOS language and other specification formalisms. In this paper, we have redefined, in the LTS model, the notions of state identification, which were originally defined in the formalism of input/output finite state machines (FSMs). Then we presented corresponding test derivation methods for specifications given in the LTS formalism that derive finite tests with fault coverage for the so-called trace equivalence relation. Note that the existing FSM-based methods are not directly applicable to LTSs, because LTSs assume rendezvous interactions making no distinction between inputs and outputs.

The notions of state identification in the LTS realm are distinguishing sequence, unique sequences, the characterization set, partial characterization sets and harmonized state identifiers. The test generation methods based on these state identification techniques are the DS-method, the US-method, the Uv-method, the W-method, the Wp-method and HSI-method. Among these methods, the DS-method, Uv-method, the W-method, the Wp-method and the HSI-method guarantee complete fault coverage.

References

[1] J. Arkko. On the existence and production of state identification machines for labeled transition systems. In *IFIP Formal Description Techniques VI*, pages 351–365, 1993.

[2] G. v. Bochmann and A. Petrenko. Protocol testing: Review of methods and relevance for software testing. In *Proceedings of the ACM 1994 International Symposium on Software Testing and Analysis*, pages 109–124, 1994.

[3] E. Brinksma. A theory for the derivation of tests. In *IFIP Protocol Specification, Testing, and Verification VIII*, pages 63–74, 1988.

[4] A. R. Cavalli and S. U. Kim. Automated protocol conformance test generation based on formal methods for LOTOS specifications. In *IFIP 5th International Workshop on Protocol Test Systems*, pages 212–220, 1992.

[5] T. S. Chow. Testing software design modeled by finite-state machines. *IEEE Transactions on Software Engineering*, SE-4(3):178–187, 1978.

[6] W. Chun and P. D. Amer. Improvements on UIO sequence generation and partial UIO sequences. In *IFIP Protocol Specification, Testing, and Verification XII*, pages 245–259, 1992.

[7] K. Drira, P. Azema, and F. Vernadat. Refusal graphs for conformance tester generation and simplification: a computational framework. In *IFIP Protocol Specification, Testing, and Verification XIII*, pages 257–272, 1994.

[8] S. Fujiwara and G. v. Bochmann. Testing nonterministic finite state machine with fault coverage. In *IFIP 4th International Workshop on Protocol Test Systems*, pages 267–280, 1991.

[9] S. Fujiwara et al. Test selection based on finite state models. *IEEE Transactions on Software Engineering*, SE-17(6):591–603, 1991.

[10] F. C. Hennie. Fault-detecting experiments for sequential circuits. In *5th Symposium on Switching Circuit Theory and Logical Design*, 1964.

[11] Z. Kohavi. *Switching and Finite Automata Theory.* McGraw-Hill Computer Science Series, New York, 1970.

[12] G. Luo, G. v. Bochmann, and A. Petrenko. Test selection based on communicating nondeterministic finite state machines using a generalized Wp-method. *IEEE Transactions on Software Engineering*, SE-20(2):149–162, 1994.

[13] G. Luo, A. Petrenko, and G. v. Bochmann. Selecting test sequences for partially-specified nondeterministic finite machines. In *IFIP 7th International Workshop on Protocol Test Systems*, pages 91–106, 1994.

[14] A. Petrenko. Checking experiments with protocol machines. In *IFIP 4th International Workshop on Protocol Test Systems*, pages 83–94, 1991.

[15] A. Petrenko, G. v. Bochmann, and R. Dssouli. Conformance relations and test derivation. In *IFIP 6th International Workshop on Protocol Test Systems*, pages 91–106, 1993.

[16] D. H. Pitt and D. Freestone. The derivation of conformance tests from LOTOS specifications. *IEEE Transactions on Software Engineering*, SE-16(12):1337–1343, 1990.

[17] K. Sabnani and A. T. Dahbura. A protocol test generation procedure. *Computer Networks and ISDN Systems*, 15(4):285–297, 1988.

[18] Q. M. Tan, A. Petrenko, and G. v. Bochmann. Modeling basic LOTOS by FSMs for conformance testing. In *IFIP Protocol Specification, Testing, and Verification XV*, pages 137–152, 1995.

[19] Q. M. Tan, A. Petrenko, and G. v. Bochmann. Testing trace equivalence for labeled transition systems. Technical Report 976, Dept.of I.R.O., University of Montreal, 1995.

[20] Q. M. Tan, A. Petrenko, and G. v. Bochmann. A framework for conformance testing of

systems communicating through rendezvous. In *IEEE 26th International Symposium on Fault-Tolerant Computing*, pages 230–238, 1996.

[21] J. Tretmans. *A Formal Approach to Conformance Testing.* Ph.D. thesis, Hengelo, The Netherlands, 1992.

[22] J. Tretmans. Testing labelled transition systems with inputs and outputs. In *IFIP 8th International Workshop on Protocol Test Systems*, 1995.

[23] R. J. van Glabbeek. The linear time-branching time spectrum. *Lecture Notes on Computer Science*, 458:278–297, 1990.

[24] S. T. Vuong and et al. The UIOv-method for protocol test sequence generation. In *IFIP 2th International Workshop on Protocol Test Systems*, pages 203–225, 1990.

[25] M. Yao. *On the Development of Conformance Test Suites in View of Their Fault Coverage.* Ph.D. thesis, University of Montreal, Canada, 1996.

Biographies

Qiang-Ming Tan received the B.S. degree and the M.S degree in computer science from Chongqing University, Chongqing, China, in 1982 and 1984, respectively. Since 1993, he has been with the Université de Montréal, PQ, Canada for the Ph.D. degree in conformance testing on communication protocols. From 1984 to 1992, he was a lecturer in the Department of Computer Science of Chongqing University. Now he is also working with Claremont Technology Inc. Canada.

Alexandre Petrenko Alexandre Petrenko received the Dipl. degree in electrical and computer engineering from Riga Polytechnic Institute and the Ph.D. in computer science from the Institute of Electronics and Computer Science, Riga, USSR. In 1996, he has joined CRIM, Centre de Recherche informatique de Montréal, Canada. He is also an adjunct professor of the Université de Montréal, where he was a visiting professor/researcher from 1992 to 1996. From 1982 to 1992, he was the head of a research department of the Institute of Electronics and Computer Science in Riga. From 1979 to 1982, he was with the Networking Task Force of the International Institute for Applied Systems Analysis (IIASA), Vienna, Austria. His current research interests include high-speed networks, communication software engineering, formal methods, conformance testing, and testability.

Gregor v. Bochmann (M'82-SM'85) received the Dipl. degree in physics from the University of Munich, Munich, West Germany, in 1968 and the Ph.D. degree from McGill University, Montréal, P.Q., Canada, in 1971. He has worked in the areas of programming languages, compiler design, communication protocols, and software engineering and has published many papers in these areas. He holds the Hewlett-Packard-NSERC-CITI chair of industrial research on communication protocols in Université de Montréal, Montréal. His present work is aimed at design methods for communication protocols and distributed systems. He has been actively involved in the standardization of formal description techniques for OSI. From 1977 to 1978 he was a Visiting Professor at the Ecole Polytechnique Fédérale, Lausanne, Switzerland. From 1979 to 1980 he was a Visiting Professor in the Computer Systems Laboratory, Stanford University, Stanford, CA. From 1986 to 1987 he was a Visiting Researcher at Siemens, Munich. He is presently one of the scientific directors of the Centre de Recherche Informatique de Montréal (CRIM).

Appendix

In this appendix we give the proof of Theorem 4 and Theorem 5. First we recall the basic assumptions and introduce several notations to help the proof, then we prove a series of lemmas among which Lemmas 1, 2, 3, 4, 7, 8, 9 and 10 lead to Theorem 5 and Lemmas 1, 2, 4, 5, 6, 7, 8, 9 and 10 lead to Theorem 4.

Given an LTS specification S and an LTS implementation M, we assume the following:
(1) All states of S and M are reachable from the initial state s_0 and m_0, respectively.
(2) $\overline{\mathsf{S}}$ is the TOS of S and has at most n states with $n > 1$.
(3) $\overline{\mathsf{M}}$ is the TOS of M and has at most m states with $m \geq n$.
(4) $\overline{s}_i, \overline{s}_j, \overline{s}_k, \overline{s}_l$ and $\overline{m}_i, \overline{m}_j, \overline{m}_k, \overline{m}_l$ represent the states of $\overline{\mathsf{S}}$ and $\overline{\mathsf{M}}$, respectively.
(5) A tuple of harmonized state identifiers $\{H_0, H_1, \ldots, H_{n-1}\}$ (for Theorem 5).
(6) A characterization set W and a tuple of partial characterization sets $\{W_0, W_1, \ldots, W_{n-1}\}$ (for Theorem 4).
(7) Q is a state cover for $\overline{\mathsf{S}}$ (See Section 5).
(8) $< N_0, N_1, \ldots N_{n-1} >$ is a state cover for M (See Section 5) and $N = \bigcup_{i=0}^{n-1} N_i$.
(10) TS is a set of test sequences obtained by Theorem 5 or Theorem 4.
(11) TS' be the test suite that is obtained from TS by converting each $a_1.a_2 \ldots a_k \in TS$ into an LTS $t_0 - a_1 \rightarrow t_2 \ldots - a_k \rightarrow t_k$ and then labeling the LTS according to Definition 6.

Definition 9 *V–equivalence.* Given a set $V \subseteq \Sigma^*$, The V–equivalence relation between two states p and q, written $p \approx_V q$, holds if and only if for all $\sigma \in Pref(V)$, $\sigma \in Tr(p) \Leftrightarrow \sigma \in Tr(q)$.
Given two LTSs S and M with initial states s_0 and m_0 respectively, we say that M is V-equivalent to S, written $\mathsf{S} \approx_V \mathsf{M}$, if only if $s_0 \approx_V m_0$.

notation	meaning
$[\overline{s}_i, \overline{m}_i] - a \rightarrow [\overline{s}_j, \overline{m}_j]$	For $a \in \Sigma$, $\overline{s}_i - a \rightarrow \overline{s}_j$ and $\overline{m}_i - a \rightarrow \overline{m}_j$
$[\overline{s}_i, \overline{m}_i] = \sigma \Rightarrow [\overline{s}_j, \overline{m}_j]$	For $\sigma \in \Sigma^*$, $\overline{s}_i = \sigma \Rightarrow \overline{s}_j$ and $\overline{m}_i = \sigma \Rightarrow \overline{m}_j$
$[\overline{s}_i, \overline{m}_i]$-**after**-$V$	given a pair of states $[\overline{s}_i, \overline{m}_i] \in \overline{S} \times \overline{M}$, and a set $V \subseteq \Sigma^*$
	$[\overline{s}_i, \overline{m}_i]$-**after**-$V = \{[\overline{s}_j, \overline{m}_j] \mid \forall \sigma \in Pref(V)\ ([\overline{s}_i, \overline{m}_i] = \sigma \Rightarrow [\overline{s}_j, \overline{m}_j])\}$
D	$D = [\overline{s}_0, \overline{m}_0]$-**after**-$\Sigma^*$
D_r	$D_r = \{[\overline{s}_i, \overline{m}_j] \in D \mid \overline{s}_i \approx_{H_i} \overline{m}_j\}\ (\{[\overline{s}_i, \overline{m}_j] \in D \mid \overline{s}_i \approx_W \overline{m}_j\})$
$\overline{\Sigma}^k$	$\overline{\Sigma}^k = \bigcup_{i=0}^{k} \Sigma^i$

Lemma 1 *For $V \subseteq \Sigma^*$, assume $|[\overline{s}_0, \overline{m}_0]$-**after**-$V| \geq k$. If $|D| > k$, then $|[\overline{s}_0, \overline{m}_0]$-**after**-$V.\overline{\Sigma}^1| \geq k+1$; if $|D| \leq k$, then $[\overline{s}_0, \overline{m}_0]$-**after**-$V@\overline{\Sigma}^1 = [\overline{s}_0, \overline{m}_0]$-**after**-$V$.*

Proof:
(I) To prove that the lemma holds when $|D| > k$.
The lemma holds when $|[\overline{s}_0, \overline{m}_0]$-**after**-$V| > k$. Consider the case that $|[\overline{s}_0, \overline{m}_0]$-**after**-$V| = k$.

(1)	$\lvert D\rvert > k$ and $\lvert[\overline{s}_0, \overline{m}_0]$-**after**-$V\rvert = k$	hypothesis
(2)	$[\overline{s}_0, \overline{m}_0]$-**after**-$V \subseteq D$	definition of D
(3)	$\exists [\overline{s}_k, \overline{m}_k] \in D \backslash [\overline{s}_0, \overline{m}_0]$-**after**-$V$	(1),(2)
	$\exists [\overline{s}_i, \overline{m}_i] \in [\overline{s}_0, \overline{m}_0]$-**after**-$V$	(1)
	$\exists \sigma \in Pref(V)\ \exists \sigma.a \in \Sigma^*([\overline{s}_0, \overline{m}_0] = \sigma \Rightarrow [\overline{s}_i, \overline{m}_i] - a \rightarrow [\overline{s}_k, \overline{m}_k])$	(2)
(4)	$[\overline{s}_k, \overline{m}_k] \in [\overline{s}_0, \overline{m}_0]$-**after**-$V@\overline{\Sigma}^1 \backslash [\overline{s}_0, \overline{m}_0]$-**after**-$V$	(3)
(5)	$[\overline{s}_0, \overline{m}_0]$-**after**-$V@\overline{\Sigma}^1 \geq k+1$	(4).

(II) To prove that the lemma holds when $|D| \leq k$.

(1)	$\|D\| \leq k$ and $\|[\overline{s}_0, \overline{m}_0]$-**after**-$V\| = k$	hypothesis
(2)	$[\overline{s}_0, \overline{m}_0]$-**after**-$V \subseteq D$	definition of D
(3)	$[\overline{s}_0, \overline{m}_0]$-**after**-$V@\overline{\Sigma}^1 = [\overline{s}_0, \overline{m}_0]$-**after**-$V$	(1),(2).

Lemma 2 *Assume* $\overline{s}_0 \approx_Q \overline{m}_0$. *If* $|D| > m$, *then* $|[\overline{s}_0, \overline{m}_0]$-**after**-$Q@\overline{\Sigma}^{m-n}| \geq m$; *and if* $|D| \leq m$, *then* $[\overline{s}_0, \overline{m}_0]$-**after**-$Q@\overline{\Sigma}^{m-n} = D$.

Proof:

(I) To prove that the lemma holds when $|D| > m$.

(1)	$\overline{s}_0 \approx_Q \overline{m}_0$ and $\|D\| > m$	hypothesis
(2)	$\|[\overline{s}_0, \overline{m}_0]$-**after**-$Q\| \geq n$	initially connected $\overline{\mathsf{S}}$, (1)
(3)	$\|[\overline{s}_0, \overline{m}_0]$-**after**-$Q@\overline{\Sigma}^{m-n}| \geq m$	Lemma 1, (1),(2).

(II) It is evident from Lemma 1 when $|D| \leq m$.

Lemma 3 *If* $\overline{s}_i \approx_{H_i} \overline{m}_k$ *and* $\overline{s}_j \approx_{H_j} \overline{m}_k$, *then* $i = j$.

Proof:

(1)	For $V \subseteq \Sigma^*, \overline{s}_i \approx_V \overline{m}_k \Leftrightarrow \overline{s}_i \approx_{Pref(V)} \overline{m}_k$	evident
(2)	$\overline{s}_i \approx_{H_i} \overline{m}_k$ and $\overline{s}_j \approx_{H_j} \overline{m}_k$	hypothesis
(3)	$\overline{s}_i \approx_{Pref(H_i)} \overline{m}_k$ and $\overline{s}_j \approx_{Pref(H_j)} \overline{m}_k$	(1),(2)
(4)	$i \neq j$	assumption
(5)	$\exists \sigma \in Tr(\overline{s}_i) \oplus Tr(\overline{s}_j) \cap Pref(H_i) \cap Pref(H_j)$	definition of H_i, (4)
(6)	let $\sigma \in Tr(\overline{s}_i)$, then $\sigma \in Tr(\overline{m}_k)$	(3)
(7)	$\sigma \in Tr(\overline{s}_j)$	(3),(6)
(8)	$i = j$	(6),(7)$\not\Leftrightarrow Tr(\overline{s}_i) \oplus Tr(\overline{s}_j)$.

Lemma 4 $|D_r| \leq m$.

Proof:

(1)	$\|\overline{M}\| \leq m$	hypothesis
(2)	$\|D_r\| > m$	assumption
(3)	$\exists[\overline{s}_i, \overline{m}_k], [\overline{s}_j, \overline{m}_k](i \neq j, \overline{s}_i \approx_{H_i} \overline{m}_k \wedge \overline{s}_j \approx_{H_j} \overline{m}_k)$ $(\exists[\overline{s}_i, \overline{m}_k], [\overline{s}_j, \overline{m}_k](i \neq j, \overline{s}_i \approx_W \overline{m}_k \wedge \overline{s}_j \approx_W \overline{m}_k))$	(1),(2)
(4)	$\|D_r\| \leq m$	(3)$\not\Leftrightarrow$Lemma 3 (definition of W).

Lemma 5 *If* $\overline{s}_0 \approx_{N@W} \overline{m}_0$, *then* $\forall[\overline{s}_i, \overline{m}_k] \in D$ $(\exists[\overline{s}_j, \overline{m}_k] \in D_r)$.

Proof:

(1)	$\overline{s}_0 \approx_{N@W} \overline{m}_0$	hypothesis
(2)	$\overline{s}_0 \approx_Q \overline{m}_0$	(1)
(3)	not $(\forall[\overline{s}_i, \overline{m}_k] \in D$ $(\exists[\overline{s}_j, \overline{m}_k] \in D_r))$	assumption
(4)	$[\overline{s}_0, \overline{m}_0]$-**after**-$Q@\overline{\Sigma}^{m-n} \subseteq D_r \subset D$	(1),(3)
(5)	$\|D\| > m$	(2),(4),Lemma 2
(6)	$[\overline{s}_0, \overline{m}_0]$-**after**-$Q.\overline{\Sigma}^{m-n} \geq m$	(2),(5),Lemma 2
(7)	$\|D_r\| \geq m$	(4),(6)
(8)	$\exists[\overline{s}_j, \overline{m}_k], [\overline{s}_l, \overline{m}_k] \in D_r$ $(j \neq l, \overline{s}_j \approx_W \overline{m}_k \wedge \overline{s}_l \approx_W \overline{m}_k))$	(7)
(9)	not $(\overline{s}_j \approx_W \overline{s}_l)$	definition of W
(10)	$\forall[\overline{s}_i, \overline{m}_k] \in D$ $(\exists[\overline{s}_j, \overline{m}_k] \in D_r)$	(8)$\not\Leftrightarrow$(9).

Lemma 6 *If* $\overline{s}_0 \approx_{N@W} \overline{m}_0$, *then* $\forall[\overline{s}_i, \overline{m}_k] \in D$ $(\overline{s}_i \approx_{W_i} \overline{m}_k \Leftrightarrow \overline{s}_i \approx_W \overline{m}_k)$.

Proof:

(1)	$\overline{s}_0 \approx_{N@W} \overline{m}_0$	hypothesis
(2)	$[\overline{s}_i, \overline{m}_k] \in D, \overline{s}_i \approx_{W_i} \overline{m}_k$	assumption
(3)	$\overline{s}_j \approx_W \overline{m}_k$	(1),(2), Lemma 5
(4)	$\overline{s}_i \approx_W \overline{s}_j$	(2),(3), $W_i \subseteq Pref(W)$
(5)	$i = j$	(4), definition of W_i
(6)	$\forall[\overline{s}_i, \overline{m}_k] \in D$ $(\overline{s}_i \approx_{W_i} \overline{m}_k \Rightarrow \overline{s}_i \approx_W \overline{m}_k)$	(2),(5)
(7)	$\forall[\overline{s}_i, \overline{m}_k] \in D$ $(\overline{s}_i \approx_W \overline{m}_k \Rightarrow \overline{s}_i \approx_{W_i} \overline{m}_k)$	definition of W_i
(8)	$\forall[\overline{s}_i, \overline{m}_k] \in D$ $(\overline{s}_i \approx_{W_i} \overline{m}_k \Leftrightarrow \overline{s}_i \approx_W \overline{m}_k)$.	

Lemma 7 *If* $\overline{s}_0 \approx_{TS} \overline{m}_0$, *then* $[\overline{s}_0, \overline{m}_0]$-**after**-$Q@\overline{\Sigma}^{m-n} = D_r = D$.

Proof:

(I) To prove that the lemma holds when $|D| \leq m$.

(1)	$\lvert D\rvert \leq m$	hypothesis
(2)	$\overline{s}_0 \approx_{TS} \overline{m}_0$	hypothesis
(3)	$\overline{s}_0 \approx_Q \overline{m}_0$	(2)
(4)	$[\overline{s}_0, \overline{m}_0]$-**after**-$Q@\overline{\Sigma}^{m-n} = D$	(1),(3),Lemma 2
(5)	$\forall[\overline{s}_i, \overline{m}_j] \in [\overline{s}_0, \overline{m}_0]$-**after**-$Q@\overline{\Sigma}^{m-n}(\overline{s}_i \approx_{H_i} \overline{m}_j)$ $(\forall[\overline{s}_i, \overline{m}_j] \in [\overline{s}_0, \overline{m}_0]$-**after**-$Q@\overline{\Sigma}^{m-n}(\overline{s}_i \approx_W \overline{m}_j))$	(2)
(6)	$D = Dr$	(4),(5),definition of D_r.

(II) To prove that the lemma holds when $|D| > m$.

(1)	$\lvert D\rvert > m$	assumption
(2)	$\overline{s}_0 \approx_{\mathcal{K}} \overline{m}_0$	hypothesis
(3)	$[\overline{s}_0, \overline{m}_0]$-**after**-$Q@\overline{\Sigma}^{m-n+1} \subseteq D$	definition of D
(4)	$\forall[\overline{s}_i, \overline{m}_j] \in [\overline{s}_0, \overline{m}_0]$-**after**-$Q@\overline{\Sigma}^{m-n+1}(\overline{s}_i \approx_{H_i} \overline{m}_j)$ $(\forall[\overline{s}_i, \overline{m}_j] \in [\overline{s}_0, \overline{m}_0]$-**after**-$Q@\overline{\Sigma}^{m-n+1}(\overline{s}_i \approx_W \overline{m}_j))$	(2)
(5)	$[\overline{s}_0, \overline{m}_0]$-**after**-$Q@\overline{\Sigma}^{m-n+1} \subseteq D_r$	(3),(4),definition of D_r
(6)	$\lvert[\overline{s}_0, \overline{m}_0]$-**after**-$Q@\overline{\Sigma}^{m-n+1}\rvert \geq m+1$	(1),(2),Lemma 2,Lemma 1
(7)	$\lvert D_r\rvert \geq m+1$	(3),(4)
(8)	$\lvert D\rvert \leq m$	(5)$\not\Leftrightarrow$Lemma 4
(9)	$[\overline{s}_0, \overline{m}_0]$-**after**-$Q@\overline{\Sigma}^{m-n} = D_r = D$	(6),Lemma 2.

Lemma 8 *If* $\overline{s}_0 \approx_{TS} \overline{m}_0$, *then* $\overline{s}_0 \approx \overline{m}_0$.

Proof:

(1)	$\overline{s}_0 \approx_{TS} \overline{m}_0$	hypothesis
(2)	$\forall[\overline{s}_i, \overline{m}_i] \in D$ $\exists\sigma \in Q@\overline{\Sigma}^{m-n}$ $([\overline{s}_0, \overline{m}_0] = \sigma \Rightarrow [\overline{s}_i, \overline{m}_i])$	(1),Lemma 7
(3)	$\overline{s}_i \approx_\Sigma \overline{m}_i$	(1)
(4)	$not(\overline{s}_0 \approx \overline{m}_0)$	assumption
(5)	$\exists a \in \Sigma$ $\exists[\overline{s}_i, \overline{m}_i] \in D$ $not(\overline{s}_i \approx_{\{a\}} \overline{m}_i))$	(4)
(6)	$\overline{s}_0 \approx \overline{m}_0$	(5)$\not\Leftrightarrow$(3).

Lemma 9 $\overline{s}_0 \approx_{TS} \overline{m}_0$ *iff* $s_0 \approx m_0$.

Proof:

(1)	$\overline{s}_0 \approx_{TS} \overline{m}_0 \Rightarrow \overline{s}_0 \approx \overline{m}_0$	Lemma 8
(2)	$\overline{s}_0 \approx \overline{m}_0 \Rightarrow \overline{s}_0 \approx_{TS} \overline{m}_0$	evident
(3)	$\overline{s}_0 \approx_{TS} \overline{m}_0 \Leftrightarrow \overline{s}_0 \approx \overline{m}_0$	(1),(2)
(4)	$\overline{s}_0 \approx s_0, \overline{m}_0 \approx m_0$	definition of TOS
(5)	$\overline{s}_0 \approx_{TS} \overline{m}_0 \Leftrightarrow s_0 \approx m_0$	(3),(4).

Lemma 10 *For all* $\mathsf{M} \in \mathcal{F}(m)$, M *passes* TS' *iff* $\mathsf{S} \approx \mathsf{M}$.

Proof:

(I) To prove $\mathsf{S} \approx \mathsf{M} \Longrightarrow \mathsf{M}$ passes TS'.

(1)	$\mathsf{S} \approx \mathsf{M}$	hypothesis
(2)	M fails TS', i.e. $\exists \mathsf{T} \in TS$ M fails T	assumption
(3)	$\exists \sigma \in Obs_{(\mathrm{T,M})}$ $(\ell(\sigma) = \mathbf{fail})$ or $\exists \sigma \in Tr(t_0$ $(ell(\sigma) = \mathbf{pass} \wedge \sigma \notin Obs_{(\mathrm{T,M})})$	definition 5, (2)
(4)	$\exists \sigma \in Tr(\mathsf{M}) \backslash Tr(\mathsf{S})$ or $\exists \sigma \in Tr(\mathsf{S}) \backslash Tr(\mathsf{M})$	definition 6, (3)
(5)	not $(\mathsf{S} \approx \mathsf{M})$	definition 3, (4)
(6)	M passes TS' $(5) \not\Leftrightarrow (1)$.	

(II) To prove M passes $TS' \Longrightarrow \mathsf{S} \approx \mathsf{M}$.

(1)	$\forall \mathsf{M} \in \mathcal{F}(m)$ (M passes TS')	hypothesis
(2)	$\exists \mathsf{M} \in \mathcal{F}(m)$ (not $(\mathsf{S} \approx \mathsf{M})$)	assumption
(3)	$\exists \sigma \in TS$ $(\sigma \in Tr(\mathsf{M}) \backslash Tr(\mathsf{S})$ or $\sigma \in Tr(\mathsf{S}) \backslash Tr(\mathsf{M}))$	Lemma 9
(4)	let $\mathsf{T} \in TS$ where $\sigma \in Tr(t_0)$	T made by σ
(5)	$\ell(\sigma) = \mathbf{fail} \wedge \sigma \in Obs_{(\mathrm{T,M})}$ or $\ell(\sigma) = \mathbf{pass} \wedge \sigma \notin Obs_{(\mathrm{T,M})}$	definition 6, (3)
(6)	M fails T, i.e. M fails TS'	definition 5 (5)
(7)	$\mathsf{S} \approx \mathsf{M}$	$(5) \not\Leftrightarrow (1)$.

æ