Experiments on Nondeterministic Systems for the Reduction Relation

Alexandre Petrenko, Nina Yevtushenko and Gregor v. Bochmann

Publication # 932

Département d'informatique et de recherche opérationnelle

Université de Montréal

Novembre 1994

Experiments on Nondeterministic Systems for the Reduction Relation

Alexandre Petrenko, Nina Yevtushenko✪, Gregor v. Bochmann

Université de Montréal, Canada
✪ Tomsk State University, Russia

Abstract

This paper studies the so-called reduction relation between systems represented as nondeterministic finite state machines. This relation requires that a machine produces a (sub)set of output sequences that can be produced by another machine in response to every input sequence. An approach to test generation for nondeterministic FSMs with respect to the reduction relation between implementations and their specification is elaborated. Results presented in this paper can also be used for analyzing relations between nondeterministic specifications.

1. INTRODUCTION

Nondeterministic behavior exhibited by complex concurrent systems is a challenging issue for validation and testing methods based on formal description techniques (FDT). In contrast to deterministic cases, various relations between investigated systems can be defined and used for different purposes and applications. For a labeled transition system (LTS) model, which is the semantic model used by the LOTOS language, there is an ever increasing spectrum of a large number of relations [Glab93]. In the realm of input/output finite state machines (FSM), the semantic model used in SDL and ESTELLE, there is not yet a big variety of relations used for verification and testing purposes [Petr93a]. An attractive feature of this model is that the theory of checking experiments on FSMs provides a solid basis for conformance test derivation with guaranteed fault coverage. Most FSM-based methods assume, however, that the behavior is specified by a deterministic machine, and rely on the equivalence relation, see for example, [Vasi73], [Chow78], [Sidh89], [Ural91], [Fuji91], [Petr92]. Very few results for nondeterministic machines have been so far reported [Yevt91], [Kloo92], [Trip92], [Petr93b], [Luo94a], [Luo94b].

The current paper focuses on a rather general "reduction" relation between nondeterministic machines, recently defined in [Petr93a]. For machine B to be a reduction of machine A, it is required to produce a (sub)set of output sequences that can be produced by A in response to every input sequence. In the deterministic case, this relation and the traditional equivalence relation coincide. The reduction relation between FSMs is needed for comparing specifications and testing conformance of a (deterministic or nondeterministic) implementation under test to a given nondeterminisitic specification. As demonstrated in [Petr93a], the results on checking experiments for FSMs can be imported to the LTS model as well. If a given LTS is transformed in one way or another into a nondeterministic FSM, then, for example, methods for test generation from FSMs w.r.t. the reduction relation could be adapted for deriving tests from LTSs w.r.t. various preorder relations. As recently shown in [Petr94a] and [Petr94b], testing of a component embedded in a compound system can also be reduced to the problem of test derivation from nondeterministic FSMs with respect to the reduction relation. In [Petr93b], a method for test derivation from a limited subclass of nondeterministic FSMs which have only deterministically reachable states was proposed. The purpose of this paper is to undertake a further study of this relation and to provide for a more comprehensive solution for test derivation from nondeterministic FSMs which may not possess this property.

The rest of this paper is organized as follows. Section 2 sets the theoretical basis for checking the reduction relation between states of the same machine as well as between different machines. In particular, we show how the reduction relation defined for infinite sequences can be verified with finite sequences only. In Section 3, checking experiments on nondeterministic FSMs w.r.t. the reduction relation are defined, and the major difficulties arising from their construction are discussed. In Section 4, we develop a general approach to checking experiment construction for various subclasses of nondeterministic FSMs w.r.t. the reduction relation. We also discuss similarities and differences between checking experiments on deterministic and nondeterministic machines.

2. NONDETERMINISTIC MACHINES AND THE REDUCTION RELATION

2.1. Definitions

We start with the definition of a completely specified nondeterministic finite state machine as given in [Star72]. A *nondeterministic finite state machine* (NFSM) A is a 5-tuple (S, X, Y, h, s_0), where S is a set of n states with s_0 as the initial state; X - a finite set of input symbols; Y - a finite set of output symbols ; h - a behavior function h: S x X --> P(S x Y), and P(S x Y) is the powerset of S x Y. Note that we only consider the initialized NFSMs with a given initial state and often call them simply machines. The machine A becomes *deterministic* FSM when |h(s,x)|=1 for all (s,x) $\square$ S x X.

We extend the behavior function to the set X* of all input words (sequences) containing the empty word e, i.e., h: S ∞ X* $\varnothing$ P(S ∞ Y*). Assume h(s,e) = (s,e) for all s $\square$ S, and suppose that h(s,β) is already specified. Then

$$h(s,\beta x) = \{ (s',\gamma y) \mid \exists\ s''\square\ S\ [(s'',\gamma) \square\ h(s,\beta)\ \&\ (s',y) \square\ h(s'',x)] \}.$$

Let h^1 be the first and h^2 - the second projections of the function h, i.e.,

$$h^1(s,\alpha) = \{ s' \mid \exists\ \gamma \square\ Y^*\ [(s',\gamma) \square\ h(s,\alpha)] \},\ h^2(s,\alpha)=\{ \gamma \mid \exists\ s'\square\ S\ [(s',\gamma) \square\ h(s,\alpha)] \}.$$

The function h^1 is actually the *next state* function, and h^2 - the *output* function of NFSM A. The set $h^1(s,\alpha)$ contains all the states from S that can be reached by the NFSM A starting from the state s after the input sequence α has been applied to this machine. The set $h^2(s,\alpha)$ contains all output sequences that can be produced in this case.

We say that state s_j is *reachable* from s_i in A if there exists an input sequence α such that $h^1(s_i,\alpha)$ contains s_j. If there exists an input sequence α such that $h^1(s_i,\alpha)$ = {sj} then s_j is said to be deterministically reachable, written *D-reachable* , from s_i in A.

Given a NFSM A=(S,X,Y,h,s_0), A is said to be *initially connected* if any state is reachable from the initial state. A is said to be *D-connected* if any state is D-reachable from the initial state.

Let $h^1_\gamma(s,\alpha)$ ={s'|(s',γ) $\square$ h(s,α)}, in other words, $h^1_\gamma(s,\alpha)$ consists of all states that can be reached from the state s with the I/O (input/output) sequence α/γ. Similarly, $h^2_s(s',\alpha)$ = {γ |(s,γ) $\square$ h(s',α)} [Star72]. Naturally, the sets $h^1_\gamma(s,\alpha)$ and $h^2_s(s',\alpha)$ might be empty for some γ, α, s, s'.

A NFSM A is said to be *observable* (ONFSM) if

$$\forall(s,x) \square\ S\infty X\ \ \forall y \square\ Y\ \ (|h^1_y(s,x)| \leq 1),$$

in other words, in observable machines a state and an I/O pair can uniquely determine at most one next state [Star72]. For the ONFSM A, we have the same property for any I/O sequence, i.e.,

$$\forall(s,\alpha) \square\ S\infty X^*\ \ \forall\gamma \square\ Y^*\ \ (|h^1_\gamma(s,\alpha)| \leq 1).$$

We note that all deterministic FSMs are observable.

The *equivalence* relation between two states s of the NFSM A and t of the NFSM B = (T,X,Y,H,t_0) holds if $\forall\alpha \square$ X* ($h^2(s,\alpha) = H^2(t,\alpha)$), otherwise, the states are nonequivalent.

The NFSMs A and B are said to be *equivalent* if their initial states are equivalent, otherwise, they are nonequivalent.

Each NFSM can be transformed into an equivalent ONFSM [Star72], even though this transformation has a tight upper bound on the number of states in the corresponding ONFSM, namely 2^n, where n is the number of states in the NFSM. Furthermore, this ONFSM can always be constructed to be initially connected. Due to this, we assume in the rest of this paper that specifications are represented by initially connected observable machines unless stated otherwise.

2.2. Checking the reduction relation between states and machines

In this paper, we study the conformance relation which allows the implementations to be equally or less nondeterministic than their corresponding specification NFSM. Formally, we define the reduction relation between NFSMs as follows [Petr93a].

A state t of the NFSM B = (T, X, Y, H, t_0) is said to be a *reduction* of a state s of the NFSM A = (S, X, Y, h, s_0), written t≤ s, if $\forall\alpha$ □ X^* ($H^2(t,\alpha) / h^2(s,\alpha)$), otherwise, t is not a reduction of s, written t Š s.

Given the NFSM A = (S, X, Y, h, s_0) and NFSM B = (T, X, Y, H, t_0), B is said to be a *reduction* of A, written B ≤ A, if $t_0 \le s_0$, otherwise, B is not a reduction of A, written B Š A. If B ≤ A and B is a deterministic machine then we refer to B as a *D-reduction* of A.

The equivalence relation between NFSMs is stronger than the reduction relation, in the sense that it requires that B be equally nondeterministic as A. The NFSMs A and B are equivalent if and only if A is a reduction of B and B is a reduction of A. If these machines are deterministic then both relations reduce to the classical notion of the equivalence relation between these machines.

In order to establish rules for determining whether state t of B is a reduction of the state s, we first redefine the reduction relation to a finite set E of finite sequences. Given state s of the NFSM A = (S, X, Y, h, s_0), state t of the NFSM B = (T, X, Y, H, t_0), and a set of input sequences E / X^*, state t of the machine B is said to be an *E-reduction* of state s of A , written $t\ {}_E{\le}\ s$, if

$$\forall\alpha \ \square\ E \ \ (H^2(t,\alpha) / h^2(s,\alpha)).$$

If state t is an E-reduction of state s for all E in X*, then it is a reduction of s.

The machine B is an E-reduction of A, written B ${}_E{\le}$ A, if the initial state of B is an E-reduction of the initial state of A. If B is an E-reduction of A for all possible E, then it is a reduction of A.

In certain cases, it is possible to conclude whether a state is a reduction of another state based on information about the relations between other states.

A state t' of the NFSM B = (T, X, Y, H, t_0) is said to be a *successor* of state t w.r.t. an input/output sequence α/γ if $H^1_\gamma(s,\alpha)$] t'. If B is observable then $H^1_\gamma(s,\alpha) = \{t'\}$.

Proposition 2.1. Given state t of the NFSM B = (T, X, Y, H, t_0), and state s of the ONFSM A = (S, X, Y, h, s_0), if t is an $\alpha\delta$-reduction of s and γ □ $H^2(t,\alpha)$ then any successor t' of state t w.r.t. the input/output sequence α/γ is a δ-reduction of the successor s' of state s w.r.t. α/γ.

Proof. According to the definition of the behavior function, we have

$$h(s,\alpha\delta) = \{ (s',\varepsilon\beta) \mid \exists\, s'' \ \square\ S\ [(s'',\varepsilon)\ \square\ h(s,\alpha)\ \&\ (s',\beta)\ \square\ h(s'',\delta)] \}$$

Since A is observable $h^1_\gamma(s,\alpha) = \{s'\}$, and a set of the output reactions of A to the input sequence $\alpha\delta$ which start with γ, is equal to $\gamma h^2(s,\delta)$.

Similarly, a set of the output reactions of the NFSM B to the sequence $\alpha\delta$ which start with γ, is equal to $\gamma\Big(\bigcup\limits_{t'\in H^1_\gamma(t,\alpha)} H^2(t',\delta)\Big)$. State t is an $\alpha\delta$-reduction of s then $\gamma h^2(s,\delta)$ □ $\gamma\Big(\bigcup\limits_{t'\in H^1_\gamma(t,\alpha)} H^2(t',\delta)\Big)$, and therefore, $h^2(s',\delta)$ □ $H^2(t',\alpha)$ for any t' □ $H^1_\gamma(t,\alpha)$, i.e. t' ${}_\delta\!\le$ s'.

■

Corollary 2.2. Let s' and t' be the successors of s and t of A and B w.r.t. an input/output sequence α/γ, γ □ $H^2(t,\alpha)(h^2(s,\alpha)$, respectively. Then

t ≤ s □ t' ≤ s'. t' Š s' □ t Š s.

In fact, if t ≤ s then t ${}_{\alpha\delta}\!\le$ s for any sequence δ. From the proposition 2.1, it follows that t' ${}_\delta\!\le$ s' for any δ, i.e. t' ≤ s'. If t' is not a δ–reduction of s' for some sequence δ then by virtue of the same proposition, t cannot be an $\alpha\delta$–reduction of s, i.e. t Š s.

■

Let P be a set of the successor pairs of s and t for all input/output sequences α/γ such that 1) t ${}_\alpha\!\le$ s, and 2) γ □ $H^2(t,\alpha)$.

In other words,

$$P = \{ s't' \mid \forall\alpha\ \square\ X^*\ \forall\gamma\ \square\ H^2(t,\alpha)\ (\{s'\} = h^1_\gamma(s,\alpha),\ t'\ \square\ H^1_\gamma(t,\alpha),\ t\ {}_\alpha\!\le s\ ) \}.$$

Proposition 2.3. State t is a reduction of s iff for any pair s't' □ P, state t' is an x-reduction of state s' for all x □ X.

Proof. First part follows from the proposition 2.1 with $\delta = x$, x □ X.
Suppose t $\$$ s then there exist α □ X^*, x □ X, γ □ $H^2(t,\alpha)$, and y □ Y such that $t\ _{\alpha}\leq s$, γy □ $H^2(t,\alpha x)$, but γy □ $h^2(s,\alpha x)$. Thus, for some pair (s't') of successors of state s and t, we have y □ $H^2(t',x)$, but y □ $h^2(s',x)$, i.e. t is not a reduction of s.

■

The next proposition gives certain conditions for finding a finite set E_{AB} of input sequences such that if state t of an NFSM B is an E_{AB}-reduction of state s of the ONFSM A then $t \leq s$.

Consider a set E_{AB} of finite input sequences which has the following properties:

1) all proper prefixes of any sequence in E_{AB} are included in this set, i.e. if $\alpha\beta$ □ E_{AB} then α □ E_{AB} and the empty sequence e □ E_{AB};

2) if α □ X^* is a proper prefix of some sequence of E_{AB} then αx□ E_{AB} for all x □ X;

3) if α □ X^* is not a proper prefix of any sequence of $E_{AB,}$ and $t\ _{\alpha}\leq s$, then for any sequence γ □ $H^2(t,\alpha)$ and any t' □ $H^1_{\gamma}(t,\alpha)$, there is a sequence δ in the set E_{AB} such that

(a) δ is a proper prefix of some sequence of $E_{AB;}$

(b) $t\ _{\delta}\leq s$;

(c) there exists β □ $H^2(t,\delta)$ such that $H^1_{\beta}(t,\delta)$] t' and $h^1_{\beta}(s,\delta) = h^1_{\gamma}(s,\alpha)$.

In other words, if t is an α-reduction of s and α is not a proper prefix of any sequence in E_{AB}, then the pair of successors (s't') of states s and t w.r.t. any input/output sequence α/γ, γ □ $H^2(t,\alpha)$ coincides with the pair of successors w.r.t. the input/output sequence δ/β, where δ is a proper prefix of some sequence in E_{AB} and t is a δ-reduction of s.

Proposition 2.4. If state t of B is an E_{AB}-reduction of state s of A then t is a reduction of s.

Proof. To prove this statement it suffices to show, by virtue of proposition 2.3, that for any sequence α such that $t\ _{\alpha}\leq s$, any sequence γ □ $H^2(t,\alpha)$ and any state t' □ $H^1_{\gamma}(t,\alpha)$, there exists an input/output sequence δ/β with the following properties:

(P1) δ □ E_{AB}, and δ is proper prefix of some sequence of $E_{AB,}$

(P2) β □ $H^2(t,\delta)$, and t' □ $H^1_{\beta}(t,\delta)$, $h^1_{\gamma}(s,\alpha) = h^1_{\beta}(s,\delta)$.

To prove the latter, we use the induction on length of a sequence α such that t is an α-reduction of s.

Induction base. The proposition is valid for α = e, as it is possible to choose e/e as such an input/output sequence.

Induction hypothesis. Let αx be an input sequence, t is an αx-reduction of s, γy □ $H^2(t,\alpha x)$, and t'□ $H^1_{\gamma y}(t,\alpha x)$. By the induction assumption, for any t'' □ $H^1_{\gamma}(t,\alpha)$, there exist a sequence δ □ E_{AB} with the property (P1), and a sequence β □ $H^2(t,\delta)$ such that

(P3) t'' □ $H^1_{\beta}(t,\delta)$ and $h^1_{\gamma}(s,\alpha) = h^1_{\beta}(s,\delta)$.

The sequence δ is a proper prefix of some sequence in E_{AB}, then δx □ E_{AB} by construction of the set E_{AB}. Consider a sequence βy. By the definition of the behavior function, and because of (P3), βy □ $H^2(t,\delta x)$ and βy □ $h^2(t,\delta x)$; moreover, t'□ $H^1_{\beta y}(t,\alpha x)$ and $h^1_{\beta y}(s,\delta x) = h^1_{\gamma y}(s,\alpha x)$. Then the induction step is proven if δx is a proper prefix of some sequence in E_{AB}. Otherwise, by construction of E_{AB}, this set has a sequence ε which is a proper prefix of some sequence in E_{AB} and there is an output sequence θ □ $H^2(t,\varepsilon)$ such that t' □ $H^1_{\theta}(t,\varepsilon)$ and $h^1_{\theta}(s,\varepsilon) = h^1_{\beta y}(s,\delta x) = h^1_{\gamma y}(s,\alpha x)$.

■

One way to derive such a set E_{AB} is described below. We construct a truncated successors tree of these machines in the following way. The vertices represent pairs of states of both machines, the root of the tree is the pair of the given states (t,s) of B and A. The edges of the tree represent the matching transitions of both machines in respect to the reduction relation, and are labeled by input/output symbols. In particular, an edge with the label x/y connects a vertex (t_j,s_j) with the vertex (t_k,s_k) if (s_k,y) □ $h(s_j,x)$ and (t_k,y) □ $H(t_j,x)$. A vertex (t_j,s_j) is a leaf in two cases:

(1) its state pair has already been encountered in the tree as an intermediate vertex (the first type of leaf);

(2) for some x □ X there are no matching transitions in the two machines from states t_j and s_j, i.e., $\exists$ y □ $H^2(t_j,x)$ (y { $h^2(s_j,x)$) (the second type of leaf).

For any vertex of this tree, we include in the set E an input part α of a sequence which labels a path from the root to this vertex. If this vertex is a leaf of the second type, we include in E every sequence αx, for all x □ X.

Corollary 2.5. Let E be a set of sequences obtained from the successors tree. If t is an E-reduction of s then t is a reduction of s.

It is sufficient to prove that E has properties of E_{AB} in the proposition 2.4. If state t is an E-reduction of s, then t is an α-reduction of s for any sequence α □ E. Then the tree should not contain any leaf of the second type. In fact, let the pair α/γ label a path from the root to such a leaf (t's'). In this case, there are x □ X and y □ Y such that y □ $H^2(t',x)$ and y { $h^2(s',x)$. γy □ $H^2(t,\alpha x)$ since y □ $H^2(t',x)$. The latter is impossible because αx □ E for all x □ X. Therefore, t is a reduction of s.

If the pair α/γ label a path from the root to an intermediate vertex, then αx □ E for all x □ X. Thus, if α is not a proper prefix of any sequence in E, then for any sequence γ □ H^2(t,α) the pair α/γ labels a path to a leaf of the first type. By this condition, there exists a δ/β that labels a path to an intermediate vertex. This sequence possesses the properties (a, b, c) given in the definition of E_{AB}.

■

We have, in fact, proven the following corollary as well.

Corollary 2.6. State t is a reduction of s iff the tree does not contain any leaf of the second type.

■

Consider an example to illustrate the construction of a truncated successors tree. Assume that the NFSMs A and B (Figures 1 and 2) have the initial states numbered 1. We wish to verify if B ≤ A. The pairs a/x and b/x take both machines into the same states numbered 2, so one vertex is declared to be a leaf of the first type. The edge labeled b/x from the vertex (2,2) leads again to (2,2) and the other two edges, labeled a/x and a/y, lead to the leaf (3,1) of the second type since state 1 of B has a transition labeled a/y and state 3 does not. The pair a/y creates the edge from the root (1,1) to the leaf (3,1) of the second type. The truncated successors tree is given in Figure 3. Since there are leaves of the second type, we conclude that B Š A.

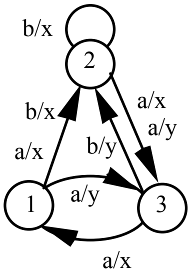

Figure 1: The NFSM A

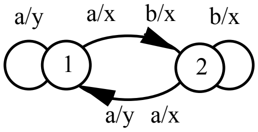

Figure 2: The NFSM B

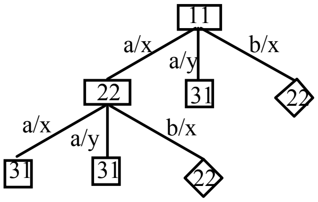

Figure 3: The tree

■

When checking the reduction relation for the given two states there exist some pairs of states of these machines for which this relation has been already verified, then we have additional termination rules. A vertex (t',s') is a leaf in two cases:

(3) if t'≤ s' (the first type of leaf);
(4) if t' Š s' (the second type of leaf).

In a similar way, the set E can be derived by use of the rules (3) and (4).

In certain cases, it is possible to conclude whether a state t can be a reduction of state s based on information about the relations for other states.

The states s and s' of the NFSM A are called *separable* [Star72], written s ò s', if there is a sequence α□ X* such that h^2(s,α) (h^2(s',α) = □.

Proposition 2.7. s ≤ s' & s' ò s" □ s Š s".

■

Separable states for the reduction relation play the role of distinct (distinguishable) states for the equivalence relation in test derivation, i.e. checking experiment construction from deterministic machines. If an NFSM A has separable successors of its initial state w.r.t. the two input/output sequences, then any reduction of A also has separable, i.e. different successors of its initial state w.r.t. these sequences.

3. CHECKING EXPERIMENTS ON NFSMS

An experiment performed on a finite state machine consists of applying one or more input sequences (tests), observing the produced output sequences, and drawing a conclusion based on these observations [Henn64], [Moor56]. In this paper, we consider preset multiple experiments which are based on a set of predefined input sequences (using the "reliable" reset assumption [Petr93a]).

In the context of fault detection, so-called checking experiments have been defined [Henn64] for deterministic machines. In fact, these experiments are based on the following fault model. A machine under test is declared to be *faulty* if it is not equivalent to the given reference machine (a non-conforming implementation). The reason is that the equivalence relation is taken as a conformance relation for the deterministic machines. A test suite is a set of input sequences since the corresponding set of output sequences is uniquely determined by this test suite. In case of nondeterministic machines, there are, in fact, several relations as possible candidates for a conformance relation (see, for example, [Star72], [Petr93a]). In this paper, we restrict ourselves to the reduction relation.

We consider the problem of deciding whether or not a machine under test is operating correctly w.r.t. the reduction relation, or in other words, the machine is operating as a certain reduction of the given reference machine. As in the deterministic case, this problem is in general not solvable, unless the machine at hand is known to belong to a finite class of machines. An experiment that enables us to do this is called a *checking experiment w.r.t. the reduction relation*.

To perform such an experiment the machine under test is required to produce all output sequences defined by its behavior function, i.e., the complete-testing assumption is satisfied:

it is possible, by applying a given input sequence to a given implementation a finite number of times, to exercise all of its possible execution paths which are traversed by this sequence [Petr93a], [Luo94a]. In particular, implementations might be deterministic for which the complete testing assumption is always satisfied. Without this assumption, it is impossible to have any guarantee for error detection, as pointed out, for example, in [Fuji91].

Let (A, ≤) be a set of all possible reductions of the given NFSM A and no two machines in this set are equivalent to each other; a be a finite set of machines with the input alphabet X. The set a\(A, ≤) represents all machines of a that are not reductions of A and is called a *fault model.*

A finite set E of finite input sequences of A is said to be a *complete* test suite for the NFSM A in the class a w.r.t. the reduction relation if for any machines B □ a\(A, ≤) there is a sequence α in E such that $H^2(t_0,\alpha)$ ” $h^2(s_0,\alpha)$.

In words, for every possible machine from a that is not a reduction of the NFSM A, the test suite E should have at least one sequence which detects this machine.[*] This property of a test suite guarantees complete coverage of all faults from the predefined fault model.

In contrast to the classical checking experiments for a single machine (see, e.g., [Moor56], [Koha78]), we are facing the problem of constructing checking experiments for a family of reference machines, since the given NFSM represents a set of its reductions and it might be interpreted as a compressed notation of this set.

The well known identification experiments defined in [Gill62] for deterministic machines also deal with a set of FSMs. In fact, a complete test suite w.r.t. the reduction relation can be obtained in a similar fashion if the class a contains only deterministic machines. Even though we are eventually interested in a general case of nondeterministic machines, let us for a moment confine ourselves to deterministic implementations and try to see the possible difficulties facing this approach.

Let $\leftarrow_A$ ∏ a be a set of all possible D-reductions of the NFSM A and no two FSMs in this set are equivalent to each other. Each machine of $\leftarrow_A$ is deterministic, and the reduction relation reduces to the equivalence relation. We thus could construct a complete test suite in the class a for each machine from the set $\leftarrow_A$ separately. Now we should apply all the input sequences from the obtained suite for every D-reduction to the given machine under test. If we find that each input sequence produces the same output sequence in this machine as it does in a proper machine from $\leftarrow_A$, then we may conclude that the machine under test is equivalent to this D-reduction; otherwise the machine under test is not equivalent to any D-

[*] In the case of deterministic FSMs, the set a necessarily includes the reference machine itself. In our case, this set might not include it. It is not nessarily true that every output sequence of the reference machine is produced by a conforming machine in response to an input sequence. A more appropriate definition of a complete test suite could choose an appropriate subset of output sequences. It is, however, outside the scope of this paper.

reduction of A, that is, it is not a D-reduction of the given NFSM A. To follow this approach, it is necessary to associate every output sequence with the name of a D-reduction which produces this output sequence and to save them during testing. According to this presented method we must first explicitly enumerate all possible machines from the set $\leftarrow_A$, i.e. the D-reductions of the given NFSM A. This set may be exponentially large. Moreover, as will be shown later in this section, in general, the list of D-reductions cannot be obtained in a straightforward way. At the same time, this constructed test suite is capable not only of checking the equivalence of the machine under test to any D-reduction of A, but also of identifying that D-reduction which is equivalent to the given machine under test. Since in the context of fault detection, we need not to make such an identification, we might wish not to save the name of the D-reduction along with an output sequence; that is, we may save only the set of all output sequences of all the machines from $\leftarrow_A$. Unfortunately, in general, this does not work as the following example [Petr93b] shows.

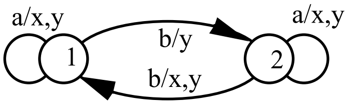

Figure 4: The NFSM A

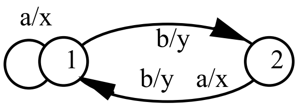

Figure 5: The FSM B

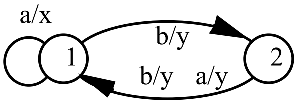

Figure 6: The FSM C

The problem is that the set of input sequences obtained by merging complete test suites derived for each reduction from the set $\leftarrow_A$ separately, is not a complete test suite for A in the same class. In fact, the set X^3 is a complete test suite for every (deterministic) FSM that is a reduction of A (Figure 4) in the class of all deterministic machines with at most two states [Moor56]. However, X^3 is not complete for A in this class as can be seen from the FSM B in Figure 5. Its responses to any input sequence from X^3 are contained in the set of responses of A to this input sequence, but the response of B to the sequence babb is not. The reason for this is that while merging suites we allow the machine under test to respond to different input sequences with output sequences belonging to different machines from $\leftarrow_A$.

We finally demonstrate that a set of possible reductions of the given NFSM cannot be determined in a straightforward way. To illustrate the problem we first introduce the notion of a submachine for the given NFSM A. An NFSM A' = (S', X', Y', h', s_0) is said to be a *submachine* of the NFSM A = (S, X, Y, h, s_0) if S'⁄S, X'⁄X, Y'⁄Y and h'(s,x)⁄h(s,x) holds for all (s,x) □ S'xX'.

It is obvious that all submachines of A are its reductions. However, the set of all the submachines does not coincide with the set of reductions, as the following example shows (Figure 4 and Figure 6). Assume all machines start from the states numbered 1. It is easy to check that the FSM C is a reduction of the NFSM A, but it is not equivalent to any submachine of A, because under the input a it enters the state 1 from both states and A does not change its state under this input. Thus, it is impossible to replace the set of all the reductions of A with the set of all its submachines.

In the next section, we develop an approach for deriving a complete test suite directly from the given machine w.r.t. the reduction relation.

4. TEST DERIVATION

In this section, we develop an approach to solve the problem of deriving a complete test suite for the ONFSM A w.r.t. the reduction relation in the class Υ_m of NFSMs which is a universal set of all (deterministic and nondeterministic) machines with the same input alphabet and with at most m states.

The proposition 2.4 and its corollaries establish the termination rules for obtaining a finite test suite E from infinite sequences in the special case when the machine under test is known. In particular, we should expand the successors tree until a pair of states is repeated or we find that B is not a reduction of A.

If the machine under test is an arbitrary NFSM from the universal set Υ_m then actual states of this machine are unknown and we can only try to estimate the number of their appearances along a particular path in the successors tree. The upper bounds for the number and the length of input sequences in a complete test suite for the n-state ONFSM A in the class Υ_m can be established. By X^r we denote the set of all sequences in the alphabet X of length up to r, including the empty sequence e.

Proposition 4.1. Let X be the input alphabet and n be the number of states in an ONFSM A. The set X^{mn} is a complete test suite for A in the class Υ_m.

Proof. Assume B = (T, X, Y, H, t_0) and $B\square\Upsilon_m$. Since B has no more than m states, and A has exactly n states there are no more than mn different pairs of states A and B. If the machine B is an X^{mn}-reduction of A then for any sequence $\alpha\square X^{mn}$ and any γ in $H^2(t_0,\alpha)$ there exist a proper prefix δ of α and a proper prefix β of γ such that $t'\square\ H^1_\beta(t,\delta)$ and $h^1_\gamma(s,\alpha) = h^1_\beta(s,\delta)$ for any $t' \square\ H^1_\gamma(t,\alpha)$.

■

The set X^{mn} is in a sense a universal complete test suite. It can be used for any reference machine with the same alphabet X and the number of states up to n. However, it can be reduced if additional properties of the ONFSM A are taken into account. If the reference machine A is deterministic and reduced then the structure of a complete test suite might be defined as the concatenation of three sets: VEW. The set V is a set of input sequences called a *state cover* of the reference machine. E = X^{m-n+1} is the set of all input sequences of length up to m-n+1. W is a *characterization set* of the reference machine [Vasi73], [Chow78], [Petr91], [Fuji91]. The set VE ensures that all the transitions in the machine under test are traversed. The set W is used to identify initial and final states of any transition. As shown in [Luo94a], [Luo94b] a complete test suite for an ONFSM w.r.t. the equivalence relation can be constructed following this structure. In our case, the relation between an IUT and the specification is the reduction relation, thus the structure VEW does not fit to this more general framework and needs certain adjustments. At the time, it is interesting to identify such a subclass of ONFSMs for which this structure can still be preserved.

We define a *D-reachable state cover set* V for the given ONFSM A in the following way. For each D-reachable state s_i of A we choose an input sequence α_i which uniquely brings A from the initial state into s_i. The union of all these sequences gives us the set V. This set is not empty since the initial state is a D-reachable from itself. We consider first the class of reference ONFSMs that are D-connected.

Proposition 4.2. The set $VX^{(m-1)n+1}$ is a complete test suite for the D-connected ONFSM A in the class Υ_m.

Proof. It is again straightforward to show that E = $X^{(m-1)n+1}$ can be selected as a set E_{AB} for any B from Υ_m. In fact, there are n different pairs (s_i,t_i) as successors of the states s_0 and t_0 w.r.t. the input/output sequences α_i/γ_i, α_i □ V, γ_i □ $H^2(t_i,\alpha)$. Any α_i is a proper prefix of some sequence of $VX^{(m-1)n+1}$ and αx □ $VX^{(m-1)n+1}$ for all x□X. Therefore, among the (m-1)n+1 pairs of successors of any states (s_i,t_i), s_i □ S and t_i □ $H^2_{\gamma i}(t_0,\alpha_i)$ which are traversed by A and B under any input/output sequence α/γ of length (m-1)n+1, either there exist the same pairs of states or the pair (s_i,t_i), s_i □ S.

■

Thus, based on the state cover of the specification ONFSM, it is possible to reduce a complete test suite. Next we consider how a characterization set can be used for the same purpose, but first we make a necessary adjustment to the definition of a characterization set for ONFSMs and the reduction relation.

A sequence β_{ij} *separates states* s_i and s_j in the ONFSM A, if the output reactions of A to β_{ij} in these states do not intersect, i.e., $h^2(s_i,\beta_{ij}) \leftrightarrow h^2(s_j,\beta_{ij}) = \square$. Such a sequence exists only for separable states.

Assume that such a single input sequence is found and fixed for each pair of separable states. The set W of these words is said to be a *characterization set* for the ONFSM A; it can have up to n(n-1)/2 words. If the given machine A happens to be deterministic and reduced (minimal) then our definition reduces to the classical definition of a characterization set (see, e.g. [Koha78], [Fuji91]). The set $W_i = \{ \beta_{ij} \mid \beta_{ij} \square W \ \& \ s_j \square S \ \& \ s_j$ ò $s_i \}$ is said to be a *state* s_i *identifier in the set S* of states of A.

Proposition 4.3. Let the given ONFSM A be D-connected and have all states pairwise separable. The set $VX^{m-n+1}W$ is a complete test suite for A w.r.t. the reduction relation in the class Υ_m.

Proof. Let B = (T,X,Y,H,t_0) be an NFSM with at most m states which is an $VX^{m-n+1}W$-reduction of A. We demonstrate that the set VX^{m-n+1} has all the properties of a set E_{AB}.

According to construction of the set VX^{m-n+1} if α is a proper prefix of another sequence then $\alpha x \square VX^{m-n+1}$ for all $x \square X$. We shall show that for any sequence $\alpha_i\alpha$, $\alpha_i \square V$, (α has length m-n+1), for any reaction γ of B to α, and any $t' \square H^2_\gamma(t_0,\alpha_i\alpha)$ there exist a sequence $\delta \square VX^{m-n}$ and a reaction of B to δ such that $t' \square H^1_\beta(t_0,\delta)$ and $h^1_\gamma(s,\alpha_i\alpha) = h^1_\beta(s,\delta)$.

For $s_i \square S$, let $T(s_i)$ be a subset of states of B, where each element in $T(s_i)$ is a W-reduction of s_i. Since any two distinct states s_i and s_j of A are separable $T(s_i) \leftrightarrow T(s_j) = \square$ holds.

Let $V = \{ \alpha_i \mid h^1(s_0,\alpha_i) = \{s_i\}, s_i \square S \}$. Fix for any $\alpha_i \square V$ an output sequence of B to α_i, i.e. $\gamma_i \square H^2(t_0,\alpha_i)$. Since B is a V-reduction of A $\gamma_i \square h^2(s_0,\alpha_i)$. A pair of successors of initial states of A and B w.r.t. the input/output sequence α_i/γ_i, $\alpha_i \square V$, is denoted by (s_i,t_i), $t_i \square H^2_{\gamma_i}(t_0,\alpha_i)$.

The NFSM B is α_iW-reduction of A. By virtue of proposition 2.1, every state t_i is a W-reduction of s_i, i.e. $t_i \square T(s_i)$. Since $T(s_i) \leftrightarrow T(s_j) = \square$ for $s_i \neq s_j$ there are n different successors in B of its initial state w.r.t. the input/output sequence α_i/γ_i, $\alpha_i \square V$. Because of this, and the fact that B has at most m states, any state t of B is a successor of some state t_i w.r.t. a proper sequence α/γ of a length at most (m-n). Since B is an $\alpha_i\alpha$-reduction of A there exists $s_j \square S$ such that $\{s_j\} = h^1_\gamma(s_i,\alpha)$. Moreover, since B is an $\alpha_i\alpha$W-reduction of A, state t is a W-reduction of s_j, i.e. $t \square T(s_j)$. Thus the following is true for any $t \square T$. There exists a single state $s \square S$ such that $t \square T(s)$; moreover, the pair (s,t) is a pair of successors of s_0 and t_0 w.r.t. some sequence δ/β, where $\delta \square VX^{m-n}$.

Consider a sequence δ □ VX^{m-n} and β □ $H^2(t_0,\delta)$. B is a VX^{m-n}-reduction of A, then β □ $h^2(s_0,\delta)$. Let t□ $H^1_{\beta}(t_0,\delta)$, $\{s\} = h^1_{\beta}(s_0,\delta)$, x□X and y □$H^2(t,x)$. Since B is a VX^{m-n+1}-reduction of A, B is a δx-reduction of A as well and y □$h^2(s,x)$. B is also a δxW-reduction of A, so by virtue of the proposition 2.1 every state t'□$H^1_y(t,x)$ is a W-reduction of s', $\{s'\} = h^1_y(s,x)$, i.e. t'□T(s').

Thus the pair (s',t') has already been encountered as a pair of successors of the initial states of A and B w.r.t. some sequence α/γ, where α□VX^{m-n} and γ□$H^2(t_0,\alpha)$. The input sequence α is a proper prefix of a sequence from VX^{m-n+1} .

■

An example. We consider an NFSM in Figure 7.

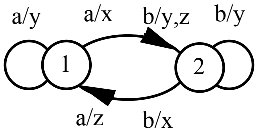

Figure 7: The NFSM

The states 1 and 2 are D-reachable from the initial state 1, the state cover set V = {e, b}. These states are separable and W = {a}. We derive test suite E according to proposition 4.3 in the class Υ_2, the result is E = {aa, baa, bba}.

■

The above proposition characterizes a subclass of ONFSMs for which a complete test suite w.r.t. the reduction relation can be derived in a way similar to the subclass of deterministic FSMs.

Note that the test suite $VX^{m-n+1}W$ can be actually reduced in size without loss of its completeness using a method similar to the Wp-method [Fuji91]. To identify the state in a leaf of the VX^{m-n+1}-tree there is no need to use all the sequences of the set W; it is sufficient to apply the sequences forming an identifier of the state of A in that leaf. If the reference machine is D-connected machine with pairwise separable states, then we can guarantee that under the input sequences from the set VX^{m-n}, a machine under test reaches all of its reachable states, or we can conclude that it is not a reduction of the reference machine w.r.t. the input sequences from the set $VX^{m-n}W$.

As shown above, the structures of a complete test suite w.r.t. the reduction relation and w.r.t. the equivalence relation are alike if all the states of the reference ONFSM are separable. The cardinal difference lies in characterization sets W and state identifiers. Separable states are not equivalent, however, nonequivalent states are not necessarily separable. If not all the states are pairwise separable then for some state t of B, there might be two states s and s' of A such that t is a W-reduction of s and t is a W-reduction of s'. However, the first part $VX^{m-n}W$ of the experiment cannot identify of which state s or s' this state t is a reduction. This is one of the reasons why the traditional state identification approach developed for deterministic machines w.r.t. the equivalence relation cannot be applied to derive a complete test suite for nondeterministic machines w.r.t. the reduction relation.

In our next step, we consider a general class of arbitrary ONFSMs which might not be D-connected and might contain states which are not pairwise separable. These machine may have several different (possibly overlapping) sets of pairwise separable states. We shall use this information in order to reduce the total length of a test suite.

Let $P_1,...,P_k$ be all maximal sets of pairwise separable states from S in the given ONFSM A. Consider a set P_i. Let R_i∏P_i be a subset of states which are D-reachable from the initial state. R_i can be empty for certain P_i. Let V be a D-reachable state cover set (note that at least one state is always D-reachable from s_0, namely s_0 itself) and W be a characterization set of A.

For each D-reachable state s_j we define a set I_j of input sequences by induction:

(1) An empty word e is in I_j.

(2) Let α [I_j. If there exists a sequence γ [$h^2(s_j,\alpha)$ such that a sequence of states that the NFSM A traverses from the state s_j when executing the input/output sequence α/γ, includes states of any P_q less than $(m-|R_q|+1)$ times then αx [I_j for all x [X.

(3) There are no other sequences in I_j.

We denote by $I_j@W$ a set of sequences obtained by concatenating all the prefixes (including the empty sequence e) of sequences of I_j by all the sequences of W. We claim the following.

Proposition 4.4. The set E' = $\bigcup_{\alpha_j \in V} \alpha_j I_j@W$ is a complete test suite for the ONFSM A w.r.t. the reduction relation in the class Υ_m.

Proof. Let B = (T,X,Y,H,t_0), |T| = m, and $B_{E'} \leq A$. Similarly to the proofs of the above statements, it suffices to show that the set E = $\bigcup_{\alpha_j \in V} \alpha_j I_j$ has all the properties of the set E_{AB} as well.

For every sequence α_j□V which takes the machine A to a D-reachable state s_j we consider a sequence γ_j □ $H^2(t_0,\alpha_j)$. B is a V-reduction of A, therefore, γ_j □ $h^2(s_0,\alpha_j)$. For every state s_j, we assign state t_j such that t_j □ $H^1_{\gamma j}(t_0,\alpha_j)$. States s_j, t_j are the successors of the initial states s_0, t_0 w.r.t. the input/output sequence α_j/γ_j.

In order to demonstrate that the set E has the properties of E_{AB} it suffices to show that for any sequence $\alpha_j\alpha$, α_j [V, α is not a proper prefix of any sequence in E, for any γ [$H^2(t_j,\alpha)$, and for any t' [$H^1_\gamma(t_j,\alpha)$ there exists in E a sequence $\alpha_r\delta$, α_r [V, in E_{AB} such that:

(S1) length of the sequence δ is less than that of α.

(S2) there exists β [$H^2(t_r,\delta)$ such that t' [$H^1_\beta(t_r,\delta)$ and $h^1_\beta(s_r,\delta) = h^1_\gamma(s_j,\alpha)$.

If such a sequence $\alpha_r\delta$ exists then there are two possible cases: 1) $\alpha_r\delta$ is a proper prefix of an appropriate sequence in E, 2) $\alpha_r\delta$ is not a proper prefix of any sequence in E.

In the first case, δ has all the necessary properties of $\alpha_j\alpha$ [E. In the second case, we can consider δ as another α and for it, there exists a shorter sequence δ with the properties (S1) and (S2). Since α has a finite length one can find a sequence δ (possibly the empty sequence) such that $\alpha_r\delta$ is a proper prefix of an appropriate sequence in E.

We denote by $W(P_q)$ a characterization set of the set of states P_q. $W(P_q)$ is a set of input sequences that separate states in P_q. By $W_{i,q}$ we denote an identifier of state s_i [P_q in the set P_q. By definition

$$W \;\square\; W(Pq) \;\square\; W_{i,q}. \qquad (1)$$

As previously, let $T(s_i)$ be a subset of states of T that are W-reductions of state s. Then, for any P_q and s_i [P_q, let a set $T_q(s_i)$ contain all the states of T that are $W_{i,q}$-reductions of state s_i. Because of (1), $T(s_i) \prod T_q(s_i)$ holds for any q and i. Since any two states in P_q are separable, we have

$$Tq(s_i) \leftrightarrow Tq(s_j) = \square,\ \ s_i, s_j \;[\; P_q, s_i \neq s_j\,. \qquad (2)$$

moreover,

$$T(s_i) \leftrightarrow T(s_j) = \square,\ s_i \text{ ò } s_j. \qquad (3)$$

The NFSM B is a VW-reduction of the ONFSM A. Consider a state t_r that is assigned to s_r reachable under the input sequence α_r [V. Since B is an α_rW-reduction of A, state t_r is a W-reduction of s_r by virtue of proposition 2.1, and therefore t_r [$T(s_r)$, i.e. t_r [$T_q(s_r)$ for all P_q э s_r.

Let $\alpha = x_1...x_k$ [I_j, α be not a proper prefix of any other sequence of I_j, and $\gamma = y_1...y_k$ [$H^2(t_j, x_1...x_k)$, therefore, $y_1...y_k$ [$h^2(s_j,x_1...x_k)$. Let also $\alpha]_a = x_1...x_a$ be a prefix of α of length a. We denote by

$$\begin{matrix} s^0 & s^1 & ... & s^k \\ t^0 & t^1 & ... & t^k \end{matrix}$$

the sequences of successors of states $s_j=s^0$ and $t_j=t^0$ of A and B w.r.t. the input/output sequences $\alpha]_a/\gamma]_a$, a = 1,...,k. In other words, $\{s^a\} = h^1_\gamma]_a(s_j, \alpha]_a)$ and t^a [$H^1_\gamma]_a(t_j, \alpha]_a)$.

Since B is an $\alpha_j\alpha]_a$W-reduction of A for any $\alpha]_a$, every state t^a is a W-reduction of state s^a, therefore

$$t^a [T(s^a) \text{ and } t^a [Tq(s^a), P_q \ni s^a. \qquad (4)$$

Let states $s^{i1},...,s^{ie}$ belong to some set P_q of pairwise separable states. Assume that these states occur in the sequence s^1 ... s^k not less than (m-$|R_q|$+1) times. Since α is not a proper prefix of any another sequence in I_j, such a P_q exists. Due to (4),
t^{ia} [$T(s^{ia})$ and t^{ia} [$Tq(s^{ia})$, a = 1,...,e.

There are two possible cases:
1) among states t^{ia}, a = 1,...,e, there exists state t_r that is assigned to some state s_r [R_q;
2) there is no such state among states t^{ia}, a=1,...,e.

In the first case, since all the states in Pq are pairwise separable, i.e. $T_q(s^{ia}) \leftrightarrow Tq(s^{ib})$ = □ if $s^{ia} \neq s^{ib}$, state s^{ia} can only be state s_r [R_q. Therefore, we can use the sequence $x_{a+1}...x_k$ as a sequence δ with the properties (S1) and (S2) and $\beta = y_{a+1}...y_k$.

In the second case, |Rq| different states are absent among states t^{ia} that are assigned to states s_r [R_q. Then a number of different states in the sequence $t^{i1}...t^{ie}$ does not exceed (m-|Rq|). Since e≥(m-|Rq|+1) then at least two states t^{ia} and t^{ib}, a<b, coincide. Because of t^{ia} [$T(s^{ia})$ and t^{ib} [$T(s^{ib})$ and $T_q(s^{ia}) \leftrightarrow Tq(s^{ib})$ = □ for $s^{ia} \neq s^{ib}$, the states s^{ia} and s^{ib} coincide as well. Thus, we can use a sequence $x_1...x_ax_{b+1}...x_k$ as a sequence δ with the properties (S1) and (S2) and $\beta = y_1...y_ay_{b+1}...y_k$.

■

Remark 1. As it follows from the above proof, to check the state reached after any sequence α_j [V, it is sufficient to use only a subset of W that is an identifier of s_j in the set S of all states of A.

Remark 2. Let α [I_j, α be a non-proper prefix of another sequence in I_j and P be a union of all P_q, q=1,…,k, such that for any γ [$h^2(s_j,\alpha)$ the NFSM A passes not less than (m-$|R_q|$+1) states of a some P_q executing an input/output sequence α/γ. According to the proof, for any output response γ to the input α, it is sufficient to separate not all the states but only those which are in this particular P_q. To do this, we can use a subset W(P) rather then the whole set W. Moreover, if for some sequence $\alpha_j\alpha]_a$, we have $h^{1}_{\beta}(s_j,\alpha]_a)$ □ P for any β [$h^2(sj,\alpha]_a)$ then there is no need to use any subset of W after $\alpha]_a$.

An example. For the ONFSM A (Figure 8) with the initial state 1 we wish to derive a complete test suite in the class Υ_3, in other words, assuming that any conforming implementation should have at most three states.

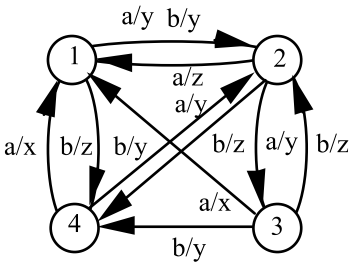

Figure 8: The ONFSM A

In the given machine, there are three D-reachable states 1, 2, and 4, so the D-reachable state cover set is V = {e, a, ab}, where e is the empty sequence. All the states are pairwise separable except for the pair 1 and 4, there are thus two maximal sets of separable states: P_1 = {1,2,3} and P_2 = {2,3,4}. Since state 3 is not D-reachable the corresponding subsets are R_1 = {1,2} and R_2 = {2,4}. The characterization set is W = {aa, bb}.

Our next step is to construct the sets I_1, I_2, and I_4 of input sequences following the above given rules. I_1 = { aa, ab, baa, bab, bb }. I_2 = { aa, baa, bab, aba, abb, bb }, I_4 = { aa, aba, abb, ba, bb }. The test suite is E' = eI_1@W " aI_2@W " abI_4@W = { baaaa, baabb, babaa, babbb, bbaa, bbbb, aaaaa, aaabb, aabaaa, aababb, aabbaa, aabbbb, abaaaa, abaabb, ababaaa, abababb, ababbaa, ababbbb, abbaaa, abbabb, abbbbaa, abbbbb }.

Next, we demonstrate how the result can simplified following optimization suggested by Remarks 1 and 2. First, the set VW is constructed: VW = {e, a, ab}{aa, bb} = {aaa, abaa, bb, abb, abbb}. Then, we choose a proper set P for every sequence in the sets I_1, I_2, and I_4. Take the set I_1 as an example. {1,2,3} is the only set for the sequence aa, and {2,3,4} is the only set for ab. For the remaining sequences in I_1, we choose the set {1,2,3}. We need the following state identifiers: W_1(1,2,3) = W_2(1,2,3) = W_3(1,2,3) = aa and W_2(2,3,4) = W_3(2,3,4) = W_4(2,3,4) = bb. The resulting complete test suite is {aaaaa, abbbbb, abaaaa, baaaa, bbaa, babaa, aabbaa, ababbb, abaabb, ababaaa, ababbaa, abbaaa}. Total length of this test suite is twice less than that of E'.

■

The approach, developed in this section for test derivation from nondeterministic FSMs w.r.t. the reduction relation, can be viewed as a generalization of the existing methods for deterministic FSMs, namely, the W-, Wp-, UIOv-, DS-methods, as well as the methods based on harmonized state identifiers [Yevt90], [Petr91], [Luo94b]. Note all these methods guarantee complete fault coverage within the predefined fault domain Υ_m. In particular, if the specification machine happens to be deterministic and reduced then:

1) all states are deterministically reachable from the initial state, and the set V becomes a traditional state cover set;

2) the reduction relation reduces to the equivalence relation, separable states become nonequivalent (distinguishable) states, and the set W becomes a traditional characterization set;

3) all the states are deterministically reachable and separable, all sets of pairwise separable states P_1, …,P_k as well their subsets R_q of D-reachable states coincide with the set S of all states of the given FSM;

4) the sets of input sequences I_j applied to every D-reachable state s_j become equal to X^{m-n+1} as $|R_q| = |S| = n$ for all q and $m-|R_q|+1 = m-n+1$;

5) if every state of the given machine possesses a Unique Input/Output (UIO) sequence then the characterization set W can be chosen as a union of these UIO-sequences (m has to be assumed equal to n); this also implies that our approach never yields a longer complete test suite than the UIOv-method for deterministic machines;

6) if the given machine possesses a distinguishing (diagnostic - DS) sequence (which is a common UIO-sequence for all the states) then this sequence could serve as a characterization set W, this also implies that our approach never yields a longer complete test suite than the DS-method for deterministic machines.

We also note that the Wp-method originally proposed for deterministic FSMs was later generalized in [Luo94a] for the equivalence relation to cover nondeterministic machines. This method cannot be applied to generate tests in the context of the reduction relation. The reason is that states distinguishable w.r.t. the equivalence relation may be non-separable states. However, separable states are not equivalent. Thus, the method presented in this paper can be easily adapted to generate tests in the context of the equivalence relation.

It is interesting to note that all the currently existing test derivation methods which are based on the FSM model and guarantee complete fault coverage, assume that faults either do not increase the number of states (m=n) or increase it up to a certain limit m, m≥n. The reason is that an implementation conforming to the specification w.r.t. the equivalence relation cannot have less states than the specification. It is not the case, however, when we deal with nondeterministic FSMs and the reduction relation. A conforming implementation is, in fact, a reduction of the given specification and it may have less states. The intuition is that to implement a part of specified behavior a subset of states in the specification may suffice. On the other hand, it becomes more difficult to fix an upper bound on the number of states in implementations, i.e. to limit a fault domain, as the domain of the state number is not directly related to the number of states in the given specification machine. Further study is needed in this direction, the results could possibly provide a further optimization of the presented approach to deriving tests for the reduction relation.

5. CONCLUSION

In this paper, we have considered nondeterministic FSMs and a rather general relation defined for these machine, namely, the reduction relation. It differs from the equivalence relation by allowing a reduction of the given FSM to be less nondeterministic or even deterministic. We have shown that similar to the equivalence relation, the reduction relation defined over infinite sequences can be checked using finite number of finite sequences. We have introduced the notion a checking experiment for a nondeterministic FSMs with respect to the reduction relation and demonstrated that the problem of its construction cannot be reduced to the known problem of checking and identification experiments for deterministic model w.r.t. the equivalence relation. Based on these results, an approach for test derivation from nondeterministic FSMs with respect to the reduction relation has been elaborated. This approach can be applied to both deterministic and nondeterministic specifications and implementations. It guarantees full fault coverage within the predefined bound on the number of states in implementations. We have also demonstrated that our approach is a nontrivial generalization of currently existing methods for deterministic machines. The method for test derivation developed in this paper includes these methods as its special cases. In other words, we have generalized the existing results on checking experiments for deterministic FSMs to cover nondeterministic behavior and the reduction relation. It is believed that these results provide for a basis for conformance test derivation from nondeterministic specifications in cases where a conformance relation can be a preorder. The current work is to further relax the constraints on the class of machines considered and to investigate how our method could be additionally optimized.

Acknowledgments. This work was partly supported by the HP-NSERC-CWARC Industrial Research Chair on Communication Protocols, Université de Montréal, and by the Russian Found for Fundamental Research. The authors would like to thank S. A. Ezust for comments.

REFERENCES

[Chow78] T. S. Chow, "Testing Software Design Modeled by Finite-State Machines", IEEE Transactions on Software Engineering, Vol. SE-4, No.3, 1978, pp.178-187.

[Fuji91] S. Fujiwara, G. v. Bochmann, F. Khendek, M. Amalou, A. Ghedamsi, "Test Selection Based on Finite State Models", IEEE Transactions on Software Engineering, Vol SE-17, No.6, 1991, pp.591-603.

[Gill62] A. Gill, Introduction to the Theory of Finite-State Machines, McGraw-Hill, 1962.

[Glab93] R. J. v. Glabbeek, "The linear Time - Branching Time Spectrum II", LNCS, 715, 1993, pp.67-81.

[Henn64] F. C. Hennie, "Fault Detecting Experiments for Sequential Circuits", Proc. of the IEEE 5th Ann. Symp. on Switching Circuits Theory and Logical Design, 1964.

[Kloo92] H. Kloosterman, "Test Derivation from Nondeterministic Finite State Machines", IFIP Transactions, Protocol Test Systems, V, (the Proceedings of IFIP TC6 Fifth International Workshop on Protocol Test Systems, 1992), Ed. by G. v. Bochmann, R. Dssouli and A. Das, 1993, North-Holland, pp.297-308.

[Koha78] Z. Kohavi, Switching and Finite Automata Theory, N.Y., McGraw-Hill, 1978.

[Luo94a] G. Luo, A. Petrenko, G. v. Bochmann, "Test Selection based on Communicating Nondeterministic Finite State Machines using a Generalized Wp-Method", IEEE Transactions on Software Engineering, Vol. SE-20, No. 2, 1994, pp.149-162.

[Luo94b] G. Luo, A. Petrenko, and G. v. Bochmann, "Selecting Test Sequences for Partially-Specified Nondeterministic Finite State Machines", IWPTS'94.

[Moor56] E. F. Moore, "Gedanken-Experiments on Sequential Machines", Automata Studies, Princeton University Press, Princeton, New Jersey, 1956, pp.129-153.

[Petr91] A. Petrenko, "Checking Experiments with Protocol Machines", IFIP Transactions, Protocol Test Systems, IV (the Proceedings of IFIP TC6 Fourth International Workshop on Protocol Test Systems, 1991), Ed. by Jan Kroon, Rudolf J. Heijink and Ed Brinksma, 1992, North-Holland, pp.83-94.

[Petr92] A. Petrenko, N. Yevtushenko, "Test Suite Generation for a FSM with a Given Type of Implementation Errors", IFIP Transactions, Protocol Specification, Testing, and Verification, XII (the Proceedings of IFIP TC6 12th International Symposium on Protocol Specification, Testing, and Verification, 1992), Ed. by R.J. Linn. Jr. and M.U. Uyar, 1992, North-Holland, pp.229-243.

[Petr93a] A. Petrenko, G. v. Bochmann, R. Dssouli, "Conformance Relations and Test Derivation", IFIP Transactions, Protocol Test Systems, VI, (the Proceedings of IFIP TC6 Fifth International Workshop on Protocol Test Systems, 1993), Ed. by O. Rafiq, 1994, North-Holland, pp.157-178.

[Petr93b] A. Petrenko, N. Yevtushenko, A. Lebedev, A. Das, "Nondeterministic State Machines in Protocol Conformance Testing", IFIP Transactions, Protocol Test Systems, VI, (the Proceedings of IFIP TC6 Fifth International Workshop on Protocol Test Systems, 1993), Ed. by O. Rafiq, 1994, North-Holland, pp.363-378.

[Petr94a] A. Petrenko, N. Yevtushenko, R. Dssouli, "Grey-Box FSM-based Testing Strategies", Department Publication 911, Université de Montréal, 1994, 22p.

[Petr94b] A. Petrenko, N. Yevtushenko, and R. Dssouli, "Testing Strategies for Communicating FSMs", IWPTS'94.

[Sidh89] D. P. Sidhu, T. K. Leung, "Formal Methods for Protocol Testing: A Detailed Study", IEEE Transactions on Software Engineering, Vol SE-15, No.4, 1989, pp.413-426.

[Star72] P. H. Starke, Abstract Automata, North-Holland/American Elsevier, 1972, 419p.

[Trip92] P. Tripathy and K. Naik, "Generation of Adaptive Test Cases from Nondeterministic Finite State Models", IFIP Transactions, Protocol Test Systems, V, (the Proceedings of IFIP TC6 Fifth International Workshop on Protocol Test Systems, 1992), Ed. by G. v. Bochmann, R. Dssouli and A. Das, 1993, North-Holland, pp.309-320.

[Ural91] H. Ural, "Formal Methods for Test Sequence Generation", Computer Communications, Vol. 15, No. 5, 1992, pp. 311-325.

[Vasi73] M. P. Vasilevski, "Failure Diagnosis of Automata", Cybernetics, Plenum Publishing Corporation, N. Y., No.4, 1973, pp.653-665.

[Yevt90] N. Yevtushenko, A. Petrenko, "Method of Constructing a Test Experiment for an Arbitrary Deterministic Automaton", Automatic Control and Computer Sciences, Allerton Press, Inc., N.Y., Vol.24, No.5, 1990, pp.65-68.

[Yevt91] N. Yevtushenko, A. Lebedev, A. Petrenko, "On the Checking Experiments with Nondeterministic Automata", Automatic Control and Computer Sciences, Allerton Press, Inc., N.Y., Vol.25, No.6, 1991, pp.81-85.