Science of Computer Programming 80 (2014) 343–355

Contents lists available at ScienceDirect

Science of Computer Programming

www.elsevier.com/locate/scico

A practical approach for testing timed deterministic finite state machines with single clock

Khaled El-Fakih [a,*,1], Nina Yevtushenko [b], Adenilso Simao [c]

[a] American University of Sharjah, PO Box 26666, Sharjah, United Arab Emirates
[b] Tomsk State University, Russia
[c] University of Sao Paulo, Brazil

ARTICLE INFO

Article history:
Received 22 November 2012
Received in revised form 17 September 2013
Accepted 19 September 2013
Available online 3 October 2013

Keywords:
Conformance testing
Finite state machine testing
Timed finite state machines

ABSTRACT

Finite State Machines (FSMs) are widely used for verification and testing of many reactive systems and many methods are proposed for generating tests from FSMs with the guaranteed fault coverage. However, some systems can only be properly described when time constraints are considered, advocating the adoption of models with the notion of time. In this paper, a method for deriving conformance tests with the guaranteed fault coverage from a Timed FSM (TFSM) with a single clock is presented. Test derivation is based on a given fault domain that allows the derivation of test suites with reasonable length. More precisely, the fault domain includes every possible faulty TFSM implementation with the known largest time constraints boundaries and minimal duration of time guards. Given a deterministic possibly partial TFSM specification, a complete test suite that guarantees the detection of all faulty implementations with respect to the above fault domain is derived. Experiments with randomly generated timed FSMs are conducted to determine length of obtained test suites and assess the impact of varying the TFSM specification parameters on length of obtained test suites. Further, experiments with both untimed and timed machines are conducted and these experiments show that similar patterns for timed and untimed machines are obtained with respect to varying the number of states, inputs, and outputs of machines.

1. Introduction

Testing from formal specifications offers a rigorous discipline to functional conformance testing of communication protocols and other reactive systems. A widely used formal model for the specification of many reactive systems is the Finite State Machine (FSM) model. FSMs are also used as the underlying models for industrial specification techniques such as SDL, Statecharts, and UML. Many FSM-based methods are proposed for deriving tests and the purpose of these tests is to check whether an implementation is correct with respect (or conforms) to its specification. Usually a conforming implementation is required to have the same input/output behavior as defined by the FSM specification. Well-known FSM-based test derivation methods are based on the W-method [1,2] and its derivatives such as the Wp [3], UIOv [4], HSI [5–7], H [8], and the SPY [9] test derivation methods. For related some surveys and experimental evaluation the reader may refer to [10,11].

In FSM-based testing, it is usually assumed that the specification and Implementation Under Test (IUT) can be modeled as FSMs. A *test* (or a *test case*) is an input sequence that is applied to the given IUT and observed outputs produced by the

* Corresponding author.
E-mail addresses: kelfakih@aus.edu (K. El-Fakih), ninayevtushenko@yahoo.com (N. Yevtushenko), adenilso@icmc.usp.br (A. Simao).
[1] Partially supported by AUS 2012 FRG-III.

0167-6423/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.scico.2013.09.008

IUT are compared with expected outputs. If the outputs do not match, then the implementation has a fault, i.e., its behavior is different from the behavior of the given specification FSM. Given an upper bound m on the number of states of an IUT and the number of states n of a given (reduced or minimal) specification FSM, a *test suite* (a set of test cases) derived by the W-method, and any of its above mentioned derivatives, provides the *complete fault coverage guarantee* that any IUT with up to m states will only pass the test suite if and only if it conforms to the specification, i.e., the IUT is equivalent to the specification. All of the above mentioned methods assume that an IUT has the reliable reset and each test case starts with the reset operation.

Many software systems such as telecommunication protocols, plant and traffic controllers and others are written using formal models with time constraints. For more information about application areas, languages and tools used for timed systems, the reader may refer to [21–25]. A number of papers consider test derivation for timed automata and Timed FSMs (TFSMs). For example, the methods given in [12,13] are based on deriving from a given timed automaton (or timed FSM) an untimed FSM and then applying FSM-based test derivation methods for the obtained FSM. More precisely, Springintveld et al. [12] proposed a rigorous strategy for deriving a complete test suite for a timed automaton. The authors show that under the assumption that the specification and an IUT have deterministic behavior and the upper bound on the number of time regions of an IUT is known, a complete test suite can be derived using the well-known W-method [1,2]. The main idea behind the approach is to divide time into very small grids such that to assure that each input is applied at some time instance of each time region of each IUT. The same grids are used for all states and inputs. As mentioned in [12], the proposed method is not practical since it returns test suites with huge length (number of inputs of corresponding test cases); however, the method has theoretic significance as it demonstrates that there exists an opportunity to derive test suites with the guaranteed fault coverage for timed FSMs without explicit enumeration of all possible implementations. Many papers inherit the idea proposed in [12]; for example, the work in [13] extends the method to non-deterministic behaviors. We note that test derivation approaches that rely on deriving complete finite tests for a given timed automaton [12,13] by first transforming the timed automaton into an untimed FSM and then applying tradition FSM based testing methods produce superfluous (or redundant) tests [31]. For this reason, we propose a method that derives tests directly from a given timed FSM.

Recently, a number of studies (see, for example, [14,15]) described a timed possibly non-deterministic FSM model where time constraints limit a time elapsed when an output has to be produced after an input has been applied to the FSM. When an output is produced the clock variable is reset to zero. The model also takes into account time-outs; if no input is applied at a current state for some time-out period, the (timed) FSM can move from a current state to another state using a time-out function. Another timed FSM model is considered in [16]. However, [14] and [16] do not consider test derivation, namely, the authors in [14,15] establish a number of conformance relations and the authors in [16] propose methods for distinguishing timed non-deterministic FSMs. Test derivation for stochastic non-deterministic timed FSMs is considered in [15]. For a more detailed review of the above papers and other relevant methods the reader may refer to [12–14]. We note that many test derivation methods are proposed for models that do not relate to the model considered in this paper, and thus we do not consider these methods in this paper.

In this paper, we consider the TFSM model from [16] and show how a complete test suite can be derived under a given test assumption. In particular, we consider deterministic possibly partial timed FSM (TFSMs) where time constraints are used to limit time elapsed at states and one clock variable is used and the clock is reset at the execution of a transition. As a TFSM specification can be partial, time instances when inputs are applied to an IUT depend also on the current state of the specification. In other words, different time partitions can be used for different states and inputs. In addition, an appropriate fault model is considered that allows the derivation of test suites of reasonable length. More precisely, we consider TFSMs with integer boundaries and implementations with the known upper bound on the number of states (as all W-based methods), known largest finite boundary and smallest duration of time guards under each input. A largest finite boundary over an input can be reasonably determined based on the TFSM specification guards over that input. Based on this, a test derivation with the guaranteed fault coverage is proposed, i.e., the method derives tests that can detect every faulty IUT in the considered fault model. The test derivation method is based on the HSI method [5–7] which is an adaptation of the W method for partial, possibly non-reduced FSMs. In particular, we extend the HSI method by defining appropriate fault model and test derivation algorithm for TFSMs. In addition, experiments with the proposed method for TFSMs and the HSI method for untimed FSMs are conducted to assess the impact on length of test suites of increasing the number of states, inputs, and outputs of a machine and to compare length of test suites for untimed machines with those of timed machines when the smallest duration of a time guard equals the largest finite boundary. According to conducted experiments, as the value of smallest integer duration of time guards doubles, test suites become 2.2 times shorter. In addition, as the number of states of a TFSM doubles, length of test suites triples. Similar results are obtained for untimed FSMs. As the number of inputs doubles, test suites of TFSMs become 1.85 times longer (i.e., almost double) where for untimed FSMs, as the number of inputs doubles, test suites become 2.4 times longer. For TFSMs, test suites become 1.35 times shorter as the number of outputs doubles and similar results are obtained with untimed FSMs. Furthermore, when the smallest duration of a time guard equals the largest finite boundary, the ratio of the length of obtained test suite of a TFSM to the size of the TFSM is only double than that of untimed FSM. We note that the size of a machine is defined as the number of transitions of that machine.

A preliminary version of the proposed test derivation method is presented in [17]. Here, the method is generalized such that the largest finite boundary and minimal (integer) durations of a finite time guards of an IUT are considered for each