Locating a faulty component of an EFSM composition

Svetlana Prokopenko <s.prokopenko@sibmail.com>
Tomsk State University,
634050, 36 Lenin av., Tomsk,Russia

Abstract. When a component of a discrete event system is faulty there is a problem how to locate a faulty component. In this paper, we consider the composition of two Extended Finite State Machines and propose an approach for locating a faulty component using preset and adaptive experiments with Finite State Machines.

Keywords: Extended Finite State Machine; Finite State Machine; l-equivalent; transfer and output faults.

1. Introduction

Telecommunication systems are multi-component systems. When some of components are faulty the behavior of the whole system can be different from that of the specification system. The problem arises how to locate faulty components. In this paper, we propose an approach for locating a faulty component in sequential composition of two Extended Finite State Machines (EFSM). The joint behavior of these components is presented as a composed EFSM. We assume that only one component can have transfer or output faults. Faults of each type are described using a Mutation Machine. Since there are no formal methods for distinguishing two mutation EFSMs, we unfold those EFSMs as classical Finite State Machines (FSM) and use preset and adaptive experiments with FSM for distinguishing two EFSMs.

2. Preliminaries

A Finite State Machine (FSM) [1] A is a 5-tuple (S, I, O, h, s_0) where S is the non-empty finite set of states with the initial state s_0, I and O are input and output alphabets, $h \subseteq S \times I \times O \times S$ is a transition relation. An FSM is called *complete* if for any pair $(s, i) \in S \times I$ there exists a transition $(s, i, o, s') \in h$; otherwise the FSM is *partial*. If for every pair $(s, i) \in S \times I$ there exists at most one transition $(s, i, o, s') \in h$ then the FSM is called *deterministic*; otherwise the FSM is *non-deterministic*. If for any triple $(s, i, o) \in S \times I \times O$ there exists at most one state

$s' \in S$ such that a transition $(s, i, o, s') \in h$ then the FSM is called *observable*, otherwise, the FSM is *non-observable*.

An Extended FSM (EFSM) [2] M is a pair (S, T) where S is the set of states and T is the set of transitions between states of the set S, such that each transition $t \in T$ is a 7-tuple (s, i, P, op, up, o, s'), where s and s' are the initial and final states of the transition t; $i \in I$ is an input with the set $D_{inp\text{-}i}$ of *input parameter vectors*; $o \in O$ is an output with the set $D_{out\text{-}o}$ of *output parameter vectors*; $P: D_{inp\text{-}i} \times D_V \rightarrow \{\text{True, False}\}$ is a *predicate* where D_V is the set of *context vectors*; $op: D_{inp\text{-}i} \times D_V \rightarrow D_{out\text{-}o}$ is an output parameter *update* function; $vp: D_{inp\text{-}i} \times D_V \rightarrow D_V$ is a context *update* function.

A *configuration* of an EFSM M is a pair $(s, \mathbf{v})$ where s is a state of the EFSM and $\mathbf{v}$ is a context vector. A pair $(i, \boldsymbol{\rho})$ is a *parameterized* input symbol where $\boldsymbol{\rho} \in D_{inp\text{-}i.}$ An input sequence of parameterized inputs is a *parameterized input sequence*; however some of inputs may be non-parameterized.

An EFSM is *complete* if for each state s with an appropriate context vector $\mathbf{v}$ and any parameterized input $(i, \boldsymbol{\rho})$ there exists at least one transition (s, i, P, op, up, o, s') with the predicate that is true for given $(s, \mathbf{v})$ and $(i, \boldsymbol{\rho})$, otherwise the EFSM is *partial*. If for each state s with an appropriate context vector $\mathbf{v}$ and any parameterized input $(i, \boldsymbol{\rho})$ there exists at most one transition (s, i, P, op, up, o, s') for which the predicate is true for given $(s, \mathbf{v})$ and $(i, \boldsymbol{\rho})$ then the EFSM is called *deterministic*; otherwise the EFSM is *non-deterministic*.

A transition $t = (s, i, P, op, up, o, s')$ of an EFSM M has a *transfer* fault if the final state s'' of an implementation transition $t' = (s, i, P, op, up, o, s'')$ is different from the final state s' of the transition t. A transition $t = (s, i, P, op, up, o, s')$ has an *output* fault if an output symbol o' of a transition $t' = (s, i, P, op, up, o', s')$ is different from that of the transition t. An output fault of a transition t means that the output of the transition t has been changed when the specification EFSM was implemented. Transfer and output faults model many other faults in an EFSM.

Given an EFSM, its behavior can be described by a corresponding FSM. States of an FSM are configurations of an EFSM, inputs and outputs correspond to parameterized inputs and outputs of the EFSM. The FSM at current state $(s, \mathbf{v})$ under a parameterized input $(i, \boldsymbol{\rho})$ verifies which transition is valid for current values of context vector $\mathbf{v}$ and input parameter vector $\boldsymbol{\rho}$, calculates new value $\mathbf{v}'$ of context vector and output parameter vector $\boldsymbol{\mu}$, produces a parameterized output $(o, \boldsymbol{\mu})$ and moves to a final state s' of the corresponding transition. The corresponding transition of the FSM has the initial state $(s, \mathbf{v})$, input $(i, \boldsymbol{\rho})$, output $(o, \boldsymbol{\mu})$ and final state $(s', \mathbf{v}')$.

If a corresponding FSM is big enough the behavior can be described over all input sequences of length l [3], i.e., an FSM that is an l-equivalent of the initial EFSM can be derived. One can simulate a behavior of the FSM under all input sequences of length l accepted at the initial state of the FSM. In general case, the l-equivalent is a

partial (possible non-observable) FSM and its behavior coincides with that of the original FSM under all input sequences of length *l*.

Given two FSMs over the same input and output alphabets, the FSMs can be distinguished by a preset or adaptive distinguishing experiment. A preset distinguishing test case is an input sequence such that the output responses to this sequence of the two FSMs do not intersect. Since a corresponding FSM for a given EFSM can be partial and non-observable, an approach proposed in [4] can be applied. Sometimes when two FSMs cannot be distinguished by a preset distinguishing experiment they still can be distinguished by an adaptive distinguishing experiment.

An adaptive distinguishing test case is a single-input output-complete connected initialized FSM that has a finite number of traces. In other words, at each intermediate state of the test case only one input with all possible outputs is defined. Such a test case first has been derived for two states of an observable FSM [5, 6] and then was extended for any number of states of a non-observable FSM [7]. The test case is a distinguishing test case for the set of states of a given FSM if each trace of the test case from the initial to a deadlock state is a trace at most at one state of the given set of states.

Consider an observable FSM *S* with two initial states s_0 and s_1 in Fig. 1. Let *S*/1 denote the FSM *S* with initial state s_0 while *S*/2 denotes the FSM *S* with initial state s_1.

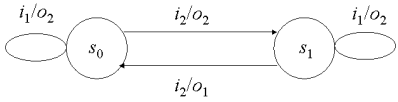


Fig. 1. FSM S with two initial states s_0 and s_1.

A test case *P* over alphabets $I = \{i_1, i_2\}$ and $O = \{o_1, o_2\}$ is an adaptive distinguishing test case of *S*/1 and *S*/2 and is shown in Fig. 2.We also notice that the machines can be separated with a single input, namely, the input i_2.

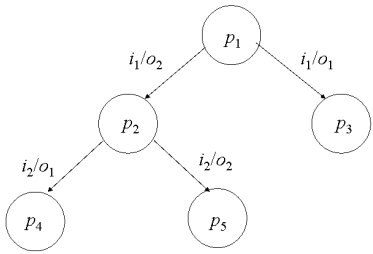


Fig. 2. A test case P.

3. Fault detection in sequential composition of two EFSMs

Consider a sequential composition N of two components A_1 and A_2 in Fig. 3.

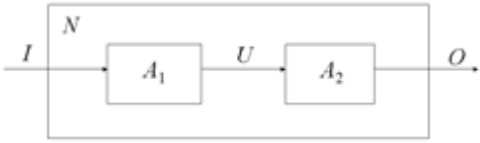


Fig. 3. A sequential composition of two EFSMs A_1 and A_2.

Let $A_1 = (C, T_1)$ and $A_2 = (Q, T_2)$ be completely specified and deterministic EFSMs. We suppose that the set of outputs of A_1 coincides with the set of inputs of A_2 which are not parameterized, i.e., predicates of the EFSM A_2 depend only on context variables. Each transition of an EFSM A_1 is a 6-tuple $(c, i, P_1, up_1, u_{out1}, c')$ and every transition of an EFSM A_2 is a 7-tuple $(q, u_{inp2}, P_2, op_2, up_2, o, q')$.

The composition of A_1 and A_2 is an EFSM $N = (Z, R)$ where $Z = C \times Q$ and $R = \{(z, i, P_1 \,\&\, P_2, op_2, \{up_1, up_2\}, o, z') \mid \exists\, (c, i, P_1, up_1, u_{out1}, c') \in T_1 \;\exists\, (q, u_{inp2}, P_2, op_2, up_2, o, q') \in T_2\, (u_{out1} = u_{inp2}),\; z = (c, q),\; z' = (c', q')\}$ [8].

As a formal model, we consider a composition of two Extended Finite State Machines and suppose that only one of two components can be faulty. Moreover, we assume that the faulty component has transfer and/or output faults. In this paper, we describe such faults using a special EFSM called a Mutation Machine *MM* [9].

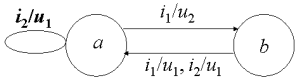
Let the component A_1 have transfer or output faults and EFSMs MM_{Tr1} and MM_{Out1} describe these faults in the component A_1. We note that mutation machines can become non-deterministic. EFSMs $MM_{Tr1} \,@\, A_2$ and $MM_{Out1} \,@\, A_2$ correspond to a behavior of faulty composition N. Let the component A_2 have transfer or output faults and EFSMs MM_{Tr2} and MM_{Out2} describe these faults in A_2. Let EFSMs $A_1 \,@\, MM_{Tr2}$ and $A_1 \,@\, MM_{Out2}$ correspond to the behavior of a faulty composition N.

To detect transfer or output faults in the composition N one can use a strategy proposed in [4]. An input sequence α is called a *separating* sequence for states s and s' of an FSM if it is defined at states s and s' and sets of outputs to this sequence at both states do not intersect. An input sequence α is called a separating sequence for two FSMs if it separates initial states of FSMs.

If two FSMs that correspond to $A_1 \,@\, MM_{Tr2}$ and $MM_{Tr1} \,@\, A_2$ (or $A_1 \,@\, MM_{Out2}$ and $MM_{Out1} \,@\, A_2$) without traces of the specification composed FSM can be distinguished by a preset or adaptive experiment, i.e., there exists a separating sequence or an adaptive test case such that after applying this test case, then we could learn which component is faulty after applying such a test case. If there is no chance to construct FSMs corresponded to $A_1 \,@\, MM_{Tr2}$ and $MM_{Tr1} \,@\, A_2$ (or $A_1 \,@\, MM_{Out2}$ and $MM_{Out1} \,@\, A_2$) due to their complexity then an approach based on l-equivalents can be used. For each mutation machine input sequences and

corresponding traces are derived for both machines one by one and each two traces are checked for the distinguishability. In this case, it is unnecessary to construct the composed EFSM; it is sufficient to model the behavior of the compositions on input sequences of length *l*. Experiments with telecommunication protocols [10] show that more than 80 % of transfer and output faults in protocol implementations can be detected using 5-equivalents of corresponding EFSMs.

An example of utilizing a proposed approach for sequential composition of two FSMs is given below. Consider component FSMs in Figs 3a and 3b and assume that a transition shown in bold can have any transition or output fault.



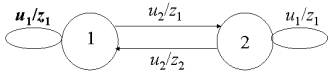


Fig. 3a. The head component FSM. *Fig. 3b. The tail component FSM.*

After deleting the specification traces from the component FSMs the mutation machines shown in Figs 4a and 4b are obtained.

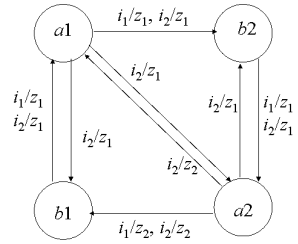
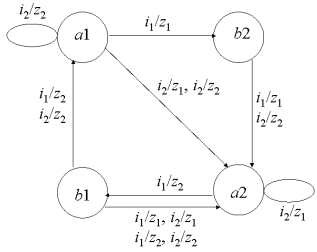


Fig. 4a. The mutation machine for the head component FSM



.Fig. 4b. The mutation machine for the tail component FSM.

By direct inspection, one can assure that the machines in Figs 4a and 4b can be distinguished by the input sequence $i_2i_2i_1$. If the output sequence to i_2 is z_2 then only the tail component can be faulty. If the output sequence to i_2 is z_1 then the next input i_2 is applied. If the output to the next input i_2 is z_1 then only the head component can

be faulty. If the output sequence to i_2 is z_2 then the next input i_1 is applied. Output sequences to i_1 are different and both mutation machines are distinguished.

In case when a separating sequence does not exist, one can try to construct an adaptive distinguishing test case [7]. If an adaptive distinguishing test case exists then based on the output response of the composition to this adaptive test case one can conclude which component FSM is faulty.

4. Conclusion

In the paper, we have discussed how to locate a faulty component in sequential composition of two EFSMs. The corresponding *l*-equivalents of mutation EFSMs which describe component faults can be derived based on the composed EFSM as well as by simulating the composition behavior under input sequences of length *l*. Moreover, the use of *l*-equivalents simplifies the problem of deleting the specification traces from the mutation machine and the approach allows eliminating the state explosion problem of an EFSM unfolding when *l* is not very big. Additional research is necessary in order to evaluate the integer *l* for appropriate cases, for example, for locating faults in protocol implementations as well as for considering other kinds of faults such as predicate faults and faults in the implementations of the update functions.

Acknowledgment

This research is partially supported by project 739 (Goszadanie RF).

References

[1]. T. Villa, N. Yevtushenko, A. Mishenko, R. K.Brayton, A. Petrenko, A. Sangiovanni-Vincentelli The unknown component problem: theory and applications. – Berlin: Springer, 2012. 311 p.

[2]. A. Petrenko, S. Boroday, and R. Groz. Confirming Configurations in EFSM Testing, IEEE Trans. Software Eng. 30(1), 2004. pp. 29-42.

[3]. V. Karibskiy, P. Parhomenko, E. Sogomonyan, V. Halchev. Basics of technical diagnostics, M.: Energya, 1976 (in Russian).

[4]. N. Kushik, N. Yevtushenko, A. Cavalli. On testing against partial non-observable specifications. QUATIC 2014 : 9th International Conference on Quality of Information and Communication Technology, Sept. 23-26, 2014, Portugal.

[5]. R. Alur, C. Courcoubetis, M. Yannakakis. Distinguishing tests for nondeterministic and probabilistic machines. In Proc. of the 27th ACM Symposium on Theory of Computing, 1995. pp. 363-372.

[6]. A. Petrenko, N. Yevtushenko, G. v. Bochmann. Testing Deterministic Implementations from their Nondeterministic Specifications. In Proc. of the IFIP Ninth International Workshop on Testing of Communicating Systems, 1996. pp. 125-140.

[7]. N. Kushik, K. El-Fakih, N. Yevtushenko, A. R. Cavalli: On adaptive experiments for nondeterministic finite state machines. Software Tools for Technology Transfer, Springer, DOI 10.1007/s10009-014-0357-7 (2014) (in press).

[8]. Fedoseev A.O. Kompozicija rasshirennyx avtomatov [Composition of Extended Finite State Machines]. Diplomnaja rabota [Diploma project], Tomsk, 2005 (in Russian).
[9]. Kolomeets A.V. Algoritmy sinteza proverjajuwix testov dlja upravljajuwix sistem na osnove rasshirennyx avtomatov [Diagnostic test derivation methods for telecommunication systems based on an EFSM model]. Dissertacija na soiskanie uchenoj stepeni kandidata texnicheskix nauk [PhD thesis], Tomsk, 2010. 129 p.
[10]. N. Kushik, M. Forostyanova, S. Prokopenko, and N. Yevtushenko. Studying the optimal height of the EFSM equivalent for testing telecommunication protocols, Proc. of the Second Intl. Conf. on Advances In Computing, Communication and Information Technology- CCIT 2014. pp. 159-163, ISBN: 978-1-63248-051-4, DOI 10.15224/ 978-1-63248-051-4-94.

Локализация неисправной компоненты в композиции расширенных автоматов

Светлана Прокопенко <s.prokopenko@sibmail.com>
НИ ТГУ, 634050, Россия, г. Томск, пр. Ленина, дом 36

Аннотация. Проблема локализации неисправной компоненты в автоматной сети хорошо известна, и в данной работе мы решаем эту проблему для бинарной сети из расширенных автоматов. Для каждой из компонент строится мутационный расширенный автомат, описывающий наиболее вероятные неисправности компоненты. Для композиции мутационного автомата со спецификацией другой компоненты посредством моделирования определяется древовидный конечный автомат, поведение которого совпадает с поведением исходного расширенного автомата на всех последовательностях длины не больше l (l-эквивалент). Из l-эквивалентов удаляются вход-выходные последовательности, принадлежащие композиции-спецификации, и для полученных мутационных l-эквивалентов строится диагностический эксперимент. Если такой диагностический эксперимент существует, то по реакции композиции, предъявленной для тестирования, достаточно часто можно определить, какая из компонент является неисправной, при условии, что неисправности возможны только в одной компоненте.

Ключевые слова: расширенный автомат, конечный автомат, l-эквивалент, ошибки переходов и выходов

Список литературы

[1]. T. Villa, N. Yevtushenko, A. Mishenko, R. K.Brayton, A. Petrenko, A. Sangiovanni-Vincentelli The unknown component problem: theory and applications. – Berlin: Springer, 2012. 311 p.
[2]. A. Petrenko, S. Boroday, and R. Groz. Confirming Configurations in EFSM Testing, IEEE Trans. Software Eng. 30(1), 2004. pp. 29-42.
[3]. V. Karibskiy, P. Parhomenko, E. Sogomonyan, V. Halchev. Basics of technical diagnostics, M.: Energya, 1976 (in Russian).
[4]. N. Kushik, N. Yevtushenko, A. Cavalli. On testing against partial non-observable specifications. QUATIC 2014 : 9th International Conference on Quality of Information and Communication Technology, Sept. 23-26, 2014, Portugal.
[5]. R. Alur, C. Courcoubetis, M. Yannakakis. Distinguishing tests for nondeterministic and probabilistic machines. In Proc. of the 27th ACM Symposium on Theory of Computing, 1995. pp. 363-372.

[6]. A. Petrenko, N. Yevtushenko, G. v. Bochmann. Testing Deterministic Implementations from their Nondeterministic Specifications. In Proc. of the IFIP Ninth International Workshop on Testing of Communicating Systems, 1996. pp. 125-140.

[7]. N. Kushik, K. El-Fakih, N. Yevtushenko, A. R. Cavalli: On adaptive experiments for nondeterministic finite state machines. Software Tools for Technology Transfer, Springer, DOI 10.1007/s10009-014-0357-7 (2014) (in press).

[8]. Fedoseev A.O. Kompozicija rasshirennyx avtomatov [Composition of Extended Finite State Machines]. Diplomnaja rabota [Diploma project], Tomsk, 2005 (in Russian).

[9]. Kolomeets A.V. Algoritmy sinteza proverjajuwix testov dlja upravljajuwix sistem na osnove rasshirennyx avtomatov [Diagnostic test derivation methods for telecommunication systems based on an EFSM model]. Dissertacija na soiskanie uchenoj stepeni kandidata texnicheskix nauk [PhD thesis], Tomsk, 2010. 129 p.

[10]. N. Kushik, M. Forostyanova, S. Prokopenko, and N. Yevtushenko. Studying the optimal height of the EFSM equivalent for testing telecommunication protocols, Proc. of the Second Intl. Conf. on Advances In Computing, Communication and Information Technology- CCIT 2014. pp. 159-163, ISBN: 978-1-63248-051-4, DOI 10.15224/ 978-1-63248-051-4-94.