УДК 519.713

КОНЕЧНО-АВТОМАТНЫЕ МЕТОДЫ СИНТЕЗА ТЕСТОВ С ГАРАНТИРОВАННОЙ ПОЛНОТОЙ ДЛЯ ВХОДО-ВЫХОДНЫХ ПОЛУАВТОМАТОВ

И. Б. Бурдонов[1] [0000-0001-9539-7853], Н. В. Евтушенко[2] [0000-0002-4006-1161], А. С. Косачев[3] [0000-0001-5316-3813]

[1, 2, 3]Институт системного программирования им. В.П. Иванникова Российской академии наук, г. Москва

[1]igor@ispras.ru, [2]evtushenko@ispras.ru, [3]kos@ispras.ru

Аннотация

Рассмотрена проблема использования конечно-автоматных методов для построения конечных тестов с гарантированной полнотой для входо-выходных полуавтоматов. Предложен способ построения конечного автомата, соответствующего полуавтомату-спецификации, и показано, что конечные тесты, построенные по такому автомату, подаваемые на вход-выходной полуавтомат при выполнении специальных таймаутов, являются полными относительно различных моделей неисправности.

***Ключевые слова**: входо-выходной полуавтомат, конечный автомат, модель неисправности, полный тест*

ВВЕДЕНИЕ

Построение тестов на основе формальных моделей (MBT в англоязычной литературе) [1–8] в настоящее время широко применяется для различных дискретных и гибридных систем, поскольку такие тесты позволяют гарантировать отсутствие критических ошибок в реализации системы. В этом случае обычно предполагается, что поведение спецификации системы и проверяемой реализации описано одной и той же формальной моделью, и определено правило, согласно которому проверяемая реализация *соответствует* спецификации, т. е. не содержит ошибок. Для модели конечного автомата, в которой после каждого входного воздействия ожидается выходной сигнал, разработано большое количество методов синтеза полных конечных тестов относительно различных моделей неисправности (см., например, [1–4, 9–11]), т. е. тестов, обнаруживающих каждую некорректную реализацию из заданного конечного класса без явного перечисления возможных реализаций. Однако достаточно часто в качестве спецификации дискретных систем рассматривается модель входо-выходного полуавтомата, в которой после входного воздействия может отсутствовать выходная реакция или может появиться последовательность таких реакций. Возможно также наличие ненаблюдаемого действия, что может привести к возникновению тупиковых ситуаций. Несмотря на достаточно большое количество публикаций по синтезу проверяющих тестов на основе такой модели [5, 6], конечные тесты с гарантированной полнотой строятся по модели неисправности, в которой все полуавтоматы-реализации явно перечислены, или для наблюдения доступны состояния тестируемой системы, или бесконечный тест ограничивается некоторым случайным образом, в результате чего полнота тестирования остается неизвестной. В работе [12] нами предложены правила для подачи входных последовательностей на входо-выходной полуавтомат, которые позволяют избежать состязаний между входными и выходными воздействиями и тупиковых ситуаций. В этом случае по входо-выходному полуавтомату можно построить подходящий конечный автомат [13] и соответственно синтезировать тесты с гарантированной полнотой известными конечно автоматными методами. В настоящей работе мы подробно рассматриваем две модели неисправности на основе входо-выходных полуавтоматов, для которых возможен синтез таких конечных полных проверяющих тестов.

Структура статьи следующая. Второй раздел содержит необходимые определения и обозначения. В третьем разделе введены понятия модели неисправности, в то время как четвертый раздел посвящен методам синтеза полных проверяющих тестов относительно введенной модели неисправности. В заключении подведены итоги работы и обсуждены перспективы дальнейших научных исследований.

1. ОПРЕДЕЛЕНИЯ И ОБОЗНАЧЕНИЯ

Конечный входо-выходной *полуавтомат* (или далее просто *полуавтомат*) [5, 6] есть четверка $\boldsymbol{S}=(S,s_0,I,O,h_S)$, где S – конечное непустое множество состояний с выделенным начальным состоянием s_0, I – конечное непустое множество входных действий, O – конечное непустое множество выходных действий, $I \cap O = \varnothing$, и $h_S \subseteq S \times (I \cup O) \times S$ есть отношение переходов. В полуавтомате есть переход из состояния s в состояние s' под действием символа a, если и только если тройка $(s,a,s') \in h_S$. Полуавтомат *наблюдаемый*, если в каждом состоянии для каждого действия определено не более одного перехода [12]. Полуавтомат является *недетерминированным* (по выходным символам), если в некотором состоянии определены переходы по нескольким выходным действиям [12]; в противном случае входо-выходной полуавтомат *детерминированный*. В настоящей работе мы рассматриваем только наблюдаемые полуавтоматы. Входной символ из I *определен* в состоянии s, если в этом состоянии есть переход под действием этого входного символа. Полуавтомат называется *полностью определенным* (по входным символам), если в каждом состоянии определен переход по любому входному действию; иначе полуавтомат называется *частично определенным*. Полуавтомат является трассовой моделью и описывает поведение моделируемой системы на трассах (последовательностях действий) из алфавита $I \cup O$. В состоянии s последовательность из $I \cup O$ является *допустимой*, если ее можно получить посредством последовательных переходов из этого состояния. Для *эквивалентных* полностью определенных полуавтоматов S и P (обозначение P≅S) множества их трасс совпадают. Если P есть *редукция* S (обозначение P≤S), то множество трасс полуавтомата P есть подмножество трасс полуавтомата S. Полуавтомат может иметь состояния, в которых нет переходов, помеченных выходными действиями; такие состояния часто называют *устойчивыми,* поскольку полуавтомат может оставаться в таком состоянии неограниченно долгое время, пока не будет подан входной сигнал. К таким состояниям, в частности, относятся тупиковые состояния, т. е. состояния, в которых не определено ни одного перехода. Трасса в состоянии s называется *полной*, если финальное состояние трассы является устойчивым. По определению, после выполнения полной трассы полуавтомат может оставаться в достигнутом состоянии до подачи нового входного воздействия. Для внешнего наблюдения перехода полуавтомата в устойчивое состояние вводится специальный «молчащий» выходной символ $\delta \notin I \cup O$ (англ. quiescence) [5]. Таким образом, можно полагать, что в каждом устойчивом состоянии полуавтомата есть петля, помеченная символом δ, который рассматривается как выходной символ, и расширенный полуавтомат с выходным алфавитом $O\cup\{\delta\}$ обозначается S^δ. Соответственно, трасса σ полуавтомата S в состоянии *s* является полной, если и только если в полуавтомате S^δ в состоянии *s* есть трасса σδ, так называемая δ-трасса. Фактически мы этим подчеркиваем, что ни один выходной символ из *O* не может появиться после трассы σ. По определению, из трассы полуавтомата S^δ можно получить трассу S после удаления δ, и обратно, после добавления любого количества символов δ после любого полного префикса трассы σ полуавтомата S получается трасса полуавтомата S^δ.

В *конечном автомате* $M=(M,m_0,I,O,h_M)$ [14] переходы в каждом состоянии помечены парами *i*/*o*, соответственно отношение переходов содержит четверки вида (m,i,o,m'). Автомат называется *детерминированным*, если в любом состоянии определено не более одного перехода по каждому входному действию; в противном случае автомат *недетерминированный*. Автомат называется *наблюдаемым*, если в каждом состоянии для каждой входо-выходной пары действия определено не более одного перехода; в противном случае автомат *ненаблюдаемый*. Автомат называется *полностью определенным*, если в каждом состоянии определен переход по любому входному символу; иначе полуавтомат называется *частичным* или *частично определенным*. Чтобы вычислить возможную выходную реакцию автомата в состоянии *s* на входную последовательность $i_1 \ldots i_k$, достаточно из состояния *s* пройти последовательно по переходам, которые помечены входо-выходной парой с соответствующим входным символом.

2. ТЕСТИРОВАНИЕ НА ОСНОВЕ ВХОДО-ВЫХОДНЫХ ПОЛУАВТОМАТОВ

Процесс тестирования интерактивных систем на основе формальных моделей (англ. Model Based Testing, MBT) обычно содержит три этапа: 1) на тестируемую реализацию подается тестовая (-ые) последовательность (-ти); 2) наблюдается выполняемая трасса; и 3) принимается решение о соответствии тестируемой реализации заданной спецификации. Процесс тестирования называется *безусловным* (англ. *preset*), если множество входных последовательностей определено заранее и не изменяется в процессе тестирования. Тестирование называется *адаптивным*, если следующий входной символ в тестовой последовательности зависит от реакции тестируемой реализации на предыдущие входные воздействия. Подобно классическим конечным автоматам [15], для входо-выходных полуавтоматов можно ввести модель неисправности, которая также является тройкой FM=$\langle S, \rhd, \Omega\rangle$. В этой тройке S – спецификация системы в виде входо-выходного полуавтомата, Ω – множество входо-выходных полуавтоматов, описывающих поведение любой предъявленной для тестирования реализации, входной и выходной алфавиты которой совпадают с таковыми для спецификации S, и $\rhd$ – отношение конформности между полуавтоматами S и $P \in \Omega$, определяющее «правильность» тестируемой реализации относительно спецификации, обозначение $S \rhd P$. Множество трасс, допустимых в спецификации, является *полным* тестом относительно модели неисправности FM, если и только если при подаче теста на входо-выходной полуавтомат P из Ω вердикт ‘pass’ выдается для полуавтоматов, конформных спецификации, и только для них.

Для входо-выходных полуавтоматов методы синтеза полных тестов разработаны для различных отношений конформности [5, 6], но построенный полный тест является конечным только для случая, когда множество тестируемых реализаций задано явным перечислением (модель «белого ящика») или при возможности наблюдения состояний тестируемой системы, т. е. для очень узкого класса моделей неисправности.

В данной работе, подобно [12, 13], мы вводим специальные ограничения на работу системы, поведение которой описано входо-выходным полуавтоматом, и покажем, что при выполнении этих ограничений можно перейти к тестам, которые суть последовательности входных символов и таймаутов, используемых для ожидания выходного символа. В этом случае по модели неисправности для входо-выходных полуавтоматов строится модель неисправности для классических автоматов, и полный тест, построенный относительно этой модели, является полным относительно исходной модели неисправности для входо-выходных полуавтоматов. В следующем разделе мы проиллюстрируем наш подход для двух наиболее часто используемых отношений конформности для входо-выходных полуавтоматов.

($T_{вх}$,$T_{вых}$)-входо-выходные полуавтоматы. Мы далее предположим, что поведение системы, описанной входо-выходным полуавтоматом, удовлетворяет

следующим правилам. После достижения системой текущего состояния она ожидает входной символ в пределах таймаута $T_{вх}$. Если входной символ подан, то система переходит в следующее предписанное состояние, таймер «сбрасывается», и система ожидает следующий входной символ. Если входной символ не появился в пределах таймаута $T_{вх}$, то он «сбрасывается», система начинает подготовку допустимого в состоянии выходного символа, который должен появиться в пределах таймаута $T_{вых}$, и никакие входные символы в этот период на систему не подаются. Если выходной сигнал появляется, то таймер «сбрасывается», и система готова к принятию следующего входного сигнала. Если выходной символ не появляется в течение $T_{вых}$, то полагаем, что полуавтомат выдает «молчащий» символ δ, и таймер «сбрасывается». Полуавтоматы, работающие по таким правилам, будем называть входо-выходными ($T_{вх}$,$T_{вых}$)-*полуавтоматами*. Рассмотрим подачу входной последовательности ?*i*?*i* на входо-выходной полуавтомат на рис. 1а. Входной символ ?*i* подается в пределах таймаута $T_{вх}$, таймер «сбрасывается», и на систему подается второй входной символ ?*i*. После этого входной символ в пределах таймаута $T_{вх}$ не подается, таймер «сбрасывается», и система начинает подготовку допустимого в состоянии 2 выходного символа !o_2, который должен появиться в пределах таймаута $T_{вых}$.

Для преобразования входо-выходного ($T_{вх}$,$T_{вых}$)-полуавтомата S^δ в конечный автомат $M^{\delta\omega}{}_S$ введем специальный входной символ $\omega \notin I$, соответствующий отсутствию входного символа, т. е. ожиданию выходного символа. Соответственно, по такому полуавтомату можно построить конечный автомат с тем же множеством трасс [13], по которому можно построить полные тесты относительно различных моделей неисправности известными конечно автоматными методами. Множество состояний конечного автомата $M^{\delta\omega}{}_S$ совпадает с таковым для полуавтомата S. Для полуавтомата S с входным и выходным алфавитами *I* и *O* входной и выходной алфавиты автомата суть ($I\cup\{\omega\}$) и ($O\cup\{\delta\}$). Автомат $M^{\delta\omega}{}_S$ строится по следующим правилам:

– существует переход из состояния *s* в состояние *q* с выходным символом δ под действием входного символа $i \in I$, если и только если в полуавтомате S существует переход из *s* в *q* под действием *i*;

– существует переход из состояния *s* в состояние *q* с выходным символом *o* под действием входного символа ω, если и только если в полуавтомате S существует переход из *s* в *q* с выходным символом *o*;

– в состоянии *s* есть петля, помеченная парой ω/δ, если и только если *s* есть устойчивое состояние полуавтомата S.

В качестве примера рассмотрим полуавтомат $\boldsymbol{S}$ на рис. 1, в котором входные символы помечены знаком ?, а выходные символы – знаком !, и соответствующий ему автомат $M^{\delta\omega}{}_S$.

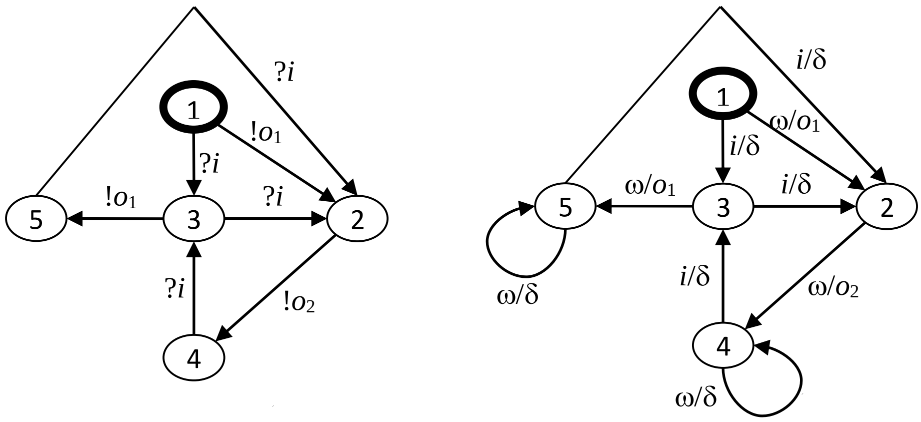

Рис. 1. Полуавтомат $\boldsymbol{S}$ и соответствующий ему конечный автомат $M^{\delta\omega}{}_S$.

По построению для автомата $M^{\delta\omega}{}_S$ имеют место следующие утверждения.

Утверждение 1. Полуавтомат S^δ содержит трассу σ, если и только если автомат $M^{\delta\omega}{}_S$ содержит трассу, построенную по σ следующим образом: сначала перед каждым выходным символом $o \in (O \cup \{\delta\})$ вставлен символ ω; после этого после каждого входного символа из алфавита *I* добавлен символ δ.

Утверждение 2. Если S – полностью определенный по входным символам входо-выходной ($T_{вх}$,$T_{вых}$)-полуавтомат, то полуавтомат S^δ имеет выходную реакцию $\beta_1\beta_2\ldots\ \beta_k\beta_{k+1}$, $\beta_j \in (O \cup \{\delta\})^*$, $|\beta_j| = t_j$, на входную последовательность $\alpha = \omega^{t1} i_1 \omega^{t2} \ldots \omega^{t(k)} i_k \omega^{t(k+1)}$, $t(j) \in \{0, 1, \ldots\}$, $j = 1, \ldots, k+1$, если и только в автомате $M^{\delta\omega}{}_S$ существует выходная реакция $\beta_1\delta\beta_2\ldots\ \beta_k\delta\beta_{k+1}$ на входную последовательность α.

Утверждение достаточно просто доказывается по индукции по числу *k*, поскольку выходная реакция в полуавтомате S^δ существует только в случае, когда входной символ не подается в ограниченный промежуток времени, т. е. подается «искусственно введенный» входной символ ω. Если полуавтомат S^{δ} имеет выходную реакцию $\beta_1\beta_2 \in (O \cup \{\delta\})^*$, $|\beta_1|=t_1$, $|\beta_2|=t_2$, на входную последовательность $\alpha=\omega^{t1}i_1\omega^{t2}$, то, по определению, автомат $M^{\delta\omega}{}_S$ на данную входную последовательность имеет выходную реакцию $\beta_1\delta\beta_2$.

В качестве примера рассмотрим полуавтомат на рис. 1а. Пусть на вход полуавтомата подается входная последовательность $?i?i$, в которой оба входных символа подаются в пределах таймаута $T_{вх}$. После подачи второго входного символа $?i$ таймер «сбрасывается», и система начинает подготовку допустимого в состоянии 2 выходного символа $!o_2$, который должен появиться в пределах таймаута $T_{вых}$, т. е. полуавтомат выдает $!o_2$ при подаче входной последовательности $?i?i?\omega$. Непосредственно проверкой можно убедиться, что автомат $M^{\delta\omega}{}_S$ на рис. 1б имеет выходную последовательность $\delta\delta o_2$ на входную последовательность $i?i?\omega$, которая превращается в последовательность o_2 после удаления «искусственных» выходных символов δ на входной символ i.

Таким образом, полуавтомат S^{δ} можно преобразовать в конечный автомат, наблюдаемые трассы которого будут совпадать с таковыми для исходного входо-выходного ($T_{вх}$,$T_{вых}$)-полуавтомата S при выполнении ограничений для таймаутов при подаче входных и выдаче выходных последовательностей. Соответственно, для таких полуавтоматов в ряде случаев понятие модели неисправности и проверяющего теста можно преобразовать таким образом, чтобы воспользоваться известными методами построения тестов с гарантированной полнотой для конечных автоматов. В следующем разделе более подробно рассмотрены две такие модели неисправности.

3. ПОСТРОЕНИЕ ПОЛНЫХ ПРОВЕРЯЮЩИХ ТЕСТОВ ДЛЯ ВХОДО-ВЫХОДНЫХ ПОЛУАВТОМАТОВ

Модель неисправности, в которой полуавтомат-спецификация детерминированный по выходам

Рассмотрим модель неисправности FM=$<S,\cong,\Omega>$, в которой спецификация системы S и все элементы множества Ω суть полностью определенные по входным символам ($T_{вх}$,$T_{вых}$)-полуавтоматы для выбранных значений $T_{вх}$ и $T_{вых}$, и $\cong$ есть отношение (трассовой) эквивалентности между полуавтоматами S^{δ} и P^{δ}. В этом случае *проверяющим тестом* относительно FM называется последовательность входных символов и символа ω, который означает ожидание выходного символа или «молчащего» символа δ в пределах таймаута $T_{вых}$. Тест подается на тестируемый полуавтомат следующим образом.

Входной символ из алфавита I подается достаточно «быстро» в пределах таймаута $T_{вх}$, и таймер «сбрасывается». Если в тесте встречается символ ω, то никакой входной символ на тестируемую систему не подается, и в течение промежутка времени $T_{вых}$ начинает формироваться и ожидается выходной символ или «молчащий» символ δ. Тест называется *полным* относительно $<S,\cong,\Omega>$, если для любого полуавтомата $P \in \Omega$, такого что S^δ и P^δ не являются эквивалентными, в тесте есть последовательность, множества реакций (реакции) на которую полуавтоматов S^δ и P^δ различны.

Рассмотрим автоматную модель $FM_{FSM}=<M^{\delta\omega}{}_S,\cong_{FSM},\Omega^{\delta\omega}>$, в которой спецификация системы есть конечный автомат $M^{\delta\omega}{}_S$, множество $\Omega^{\delta\omega}$ содержит все автоматы P^δ, $P \in \Omega$, и $\cong$ есть отношение (трассовой) эквивалентности между автоматами $M^{\delta\omega}{}_S$ и $M^{\delta\omega}{}_P$.

Утверждение 3. Проверяющий тест является полным относительно модели неисправности $FM=<S,\cong,\Omega>$, в которой спецификация системы S и все элементы множества Ω суть полностью определенные по входным символам ($T_{вх}$,$T_{вых}$)-полуавтоматы для выбранных значений $T_{вх}$ и $T_{вых}$, и $\cong$ есть отношение (трассовой) эквивалентности между полуавтоматами S^δ и P^δ, если и только если тест является полным относительно автоматной модели неисправности FM_{FSM} $<M^{\delta\omega}{}_S,\cong_{FSM},\Omega^{\delta\omega}>$.

Проверяющие тесты относительно моделей неисправности $<S,\cong,\Omega>$ и $<M^{\delta\omega}{}_S,\cong_{FSM},\Omega^{\delta\omega}>$ содержат входные последовательности в алфавите $I \cup \{\omega\}$. Проверяющий тест *TS* полный относительно $FM=<S,\cong,\Omega>$, если и только если для любого полуавтомата $P \in \Omega$, такого, что S^δ не является эквивалентным полуавтомату P^δ, существует тестовая последовательность, множества реакций на которую полуавтоматов S^δ и P^δ различны, т. е. различными являются множества реакций автоматов $M^{\delta\omega}{}_S$ и $M^{\delta\omega}{}_P$ (утверждение 2), и, следовательно, тест является полным относительно автоматной модели FM_{FSM}.

Для автоматной модели FM_{FSM} существуют методы построения полных тестов относительно FM_{FSM} для недетерминированных и детерминированных, полностью определенных и частичных автоматов-спецификаций. Наиболее хорошо развиты методы построения полных проверяющих тестов для случая, когда автомат-спецификация является приведенным детерминированным автоматом, а множество $\Omega^{\delta\omega}$ содержит все детерминированные полностью определенные автоматы с числом состояний не более некоторого заданного числа m. Рассмотрим более подробно метод построения проверяющего теста для случая, когда автомат-спецификация $M^{\delta\omega}{}_S$ является полностью определенным приведенным автоматом.

Пусть в модели FM=<S,$\cong$,$\Omega(m)$> полуавтомат-спецификация является полностью определенным по входным символам и детерминированным по выходным символам, и $\Omega(m)$ есть множество полностью определенных детерминированных (по выходным символам) полуавтоматов с числом состояний не более m. Пусть, кроме того, конечный автомат $M^{\delta\omega}{}_S$ имеет n состояний, $n \leq m$, и является приведенным, т. е. любые два состояния отличаются по реакции на некоторую входную последовательность. Для любых двух состояний существует входная последовательность, на которую выходные реакции в этих состояниях различны. Полный проверяющий тест для автоматной модели <$M^{\delta\omega}{}_S$,$\cong_{FSM}$,$\Omega^{\delta\omega}(m)$> можно построить W-методом или его различными модификациями [4] с использованием различающих и передаточных последовательностей. На первом шаге строятся множество различимости W, содержащее различающую последовательность для каждой пары состояний, и множество достижимости, содержащее передаточную последовательность для каждого из состояний. Тогда множество $V.W \cup VI.W \cup \ldots \cup VI^{m-n+1}.W$ является полным тестом относительно модели неисправности <$M^{\delta\omega}{}_S$,$\cong_{FSM}$,$\Omega^{\delta\omega}(m)$>, следовательно, согласно утверждению 3, полным тестом относительно <S,$\cong$,$\Omega(m)$>. Напомним, что тестовые последовательности содержат входные символы и символ ω и подаются на тестируемый полуавтомат выше описанным образом.

Если автомат-спецификация не является приведенным, то достаточно воспользоваться его приведенной формой. Если m совпадает с числом состояний приведенной формы автомата-спецификации $M^{\delta\omega}{}_S$, то сложность построения и общая длина полного проверяющего теста являются полиномиальными относительно m. Если m больше числа n состояний приведенной формы автомата $M^{\delta\omega}{}_S$, то общая длина полного проверяющего теста пропорциональна $(|I|+1)^{m-n+1}$, где I – входной алфавит полуавтомата-спецификации.

Если автомат-спецификация является детерминированным приведенным, но частичным, то можно воспользоваться гармонизированными идентификаторами состояний, которые используются вместо множества различимости. В примере на рис. 1б система гармонизированных идентификаторов имеет вид $H=\{H_1,H_2,H_3,H_4,H_5\}$, в которой $H_1=H_2=H_3=\{\omega\omega\}$ и $H_4=H_5=\{\omega\omega i\omega\}$. В качестве множества достижимости используем множество $V=\{\varepsilon,\omega,i, i\omega, \omega\omega\}$, где ε – пустая последовательность. В результате получим множество входных последовательностей $TS=\{ii\omega\omega,i\omega i\omega\omega,i\omega\omega\omega\omega i\omega,\omega\omega i\omega\omega,\omega\omega\omega\omega\omega i\omega\}$, которое является полным проверяющим тестом относительно модели неисправности $<S,\cong_q,\Omega(5)>$, в которой спецификация есть полуавтомат S на рис. 1а, а отношение конформности $\cong_q$ требует, чтобы поведение проверяемого автомата, конформного спецификации, совпадало с поведением спецификации на допустимых для спецификации входных последовательностях.

Следует отметить, что если соответствующий частичный автомат не является приведенным, то тесты получаются более длинными, чем для полностью определенного полуавтомата-спецификации, однако теоретические оценки сложности построения и общей длины полного проверяющего теста совпадают с таковыми для полностью определенных полуавтоматов.

Модель неисправности, в которой полуавтомат-спецификация может быть недетерминированным по выходам

Рассмотрим модель неисправности $FM=<S,\leq,\Omega(n)>$, в которой полуавтомат-спецификация есть полностью определенный по входным символам наблюдаемый, возможно, недетерминированный по выходам полуавтомат, причем соответствующий автомат $M^{\delta\omega}{}_S$ имеет n состояний. Все полуавтоматы множества Ω детерминированные, имеют не более n состояний, и отношение конформности является отношением редукции, т. е. множество трасс конформного полуавтомата должно содержаться в множестве трасс полуавтомата-спецификации.

Пусть автомат $M^{\delta\omega}{}_S$ обладает разделяющей последовательностью γ, т. е. для любых двух состояний автомата множества выходных реакций на последовательность γ не пересекаются. Предположим также, что любое состояние s в автомате $M^{\delta\omega}{}_{S}$ *детерминировано достижимо* (*д-достижимо*) из начального по некоторой входной последовательности β_s, т. е. β_s переводит автомат в это состояние независимо от выходной реакции. Множество таких д-передаточных последовательностей для всех состояний назовем множеством д-достижимости V_d. Тогда множество $V_d.\gamma \cup V_d I.\gamma$ является полным тестом относительно модели неисправности $<M^{\delta\omega}{}_{S}, \leq_{FSM}, \Omega^{\delta\omega}(n)>$, следовательно, согласно утверждению 3, полным тестом относительно $<S, \leq, \Omega(n)>$, при условии выполнения требований таймаутов при подаче входной и наблюдении выходной последовательности.

Если полуавтомат-спецификация является наблюдаемым, но может быть частично определенным, то вместо отношения редукции рассматривается отношение квази-редукции, которое, вообще говоря, очень близко к отношению *ioco* [5]. В этом случае отмечается, что полный проверяющий тест должен быть адаптивным, и в работе [11] приведен алгоритм построения такого теста для конечно автоматной модели относительно отношений квази-эквивалентности и квази-редукции. Построенные полные тесты могут быть использованы при тестировании входо-выходных ($T_{вх}$,$T_{вых}$)-полуавтоматов. Если полуавтоматы множества Ω могут быть недетерминированными по выходам, то при подаче полного теста должно выполняться требование о «всех погодных условиях», т. е. каждая тестовая последовательность подается на тестируемый полуавтомат достаточное количество раз, чтобы пронаблюдать все выходные реакции.

Тесты, построенные автоматными методами, активно используются при тестировании телекоммуникационных протоколов, а также программного обеспечения для микропроцессоров (см., например, [7, 8, 16], где приведены примеры протоколов, в реализациях которых были найдены несоответствия спецификациям). В работе [17] рассмотрено использование полуавтоматной модели для проверки наличия состязаний в композиции SDN контроллера и переключателя.

ЗАКЛЮЧЕНИЕ

В настоящей работе проблема построения конечных тестов с гарантированной полнотой на основе входо-выходного полуавтомата для модели «черного ящика» сведена к построению такого теста для конечно автоматной модели. Соответственно, оценки сложности для таких тестов для подходящей модели неисправности совпадают с оценками сложности для подходящих классических конечных автоматов. Поскольку для конечных автоматов адаптивность в некоторых случаях позволяет снизить сложность построения и длину проверяющего теста, в дальнейшем авторы предполагают рассмотреть адаптивные тестовые последовательности для полуавтоматов, а также выделить классы с «хорошими» оценками сложности для таких экспериментов.

Работа выполнена при поддержке Российского научного фонда, проект № 22-29-01189.

СПИСОК ЛИТЕРАТУРЫ

1. *Hennie F.C.* Fault-Detecting Experiments for Sequential Circuits // The Fifth Ann. Symp. Switching Circuit Theory and Logical Design. 1964. P. 95–110.

2. *Василевский М. П.* О распознавании неисправности автоматов // Кибернетика. 1973. № 4. С. 98–108.

3. *Bochmann G., Petrenko A.* Protocol testing: review of methods and relevance for software testing // Intern. Symp. on Software Testing and Analysis. 1994. P. 109–123.

4. *Dorofeeva R., El-Fakih K., Cavalli A., Maag S., Yevtushenko N.* FSM-based conformance testing methods: A survey annotated with experimental evaluation // Information & Software Technology. 2010. Vol. 52. No 12. P. 1286–1297.

5. *Tretmans J.* A formal approach to conformance testing // The Intern. Workshop on Protocol Test Systems. 1993. P. 257–276.

6. *Бурдонов И.Б., Косачев А.С., Кулямин В.В.* Теория соответствия для систем с блокировками и разрушением. М.: Наука, Глав. ред. физ.-мат. лит., 2008. 412 с.

7. *Kushik N., Forostyanova M., Prokopenko S., Yevtushenko N.* Studying the optimal height of the EFSM equivalent for testing telecommunication protocols // Intern. Conf. on Advances in Computing, Communication and Information Technology. 2014. P. 159–163.

8. *Жигулин М.В., Коломеец А.В., Кушик Н.Г., Шабалдин А.В.* Тестирова-

ние программной реализации протокола IRC на основе модели расширенного автомата // Известия Томского политехнического университета. 2011. Т. 318. № 5. С. 81–84.

9. *Lee D, Yannakakis M.* Principles and methods of testing finite-state machines – a survey // Proceedings of the IEEE. 1996. Vol. 84. No. 8. P. 1089–1123.

10. *Petrenko A., Y*evtushenko N. Testing from Partial Deterministic FSM Specifications // IEEE Trans. Computers. 2005. Vol. 54. No. 9. P. 1154–1165.

11. *Petrenko A., Yevtushenko N.* Conformance Tests as Checking Experiments for Partial Nondeterministic FSM // Lecture Notes in Computer Science. 2005. Vol. 3997. P. 118–133.

12. *Yevtushenko N., Burdonov I., Kossachev A.* Deriving Distinguishing Sequences for Input/Output Automata // The IEEE East-West Design & Test Symposium. 2020. P. 1–5.

13. *Бурдонов И.Б., Евтушенко Н.В., Косачев А.С.* Синтез тестов с гарантированной полнотой для входо-выходных полуавтоматов // XXIV Всероссийская научная конференция «Научный сервис в сети Интернет». 2022. С. 93–103.

14. *Гилл А.* Введение в теорию конечных автоматов. Наука, 1966. 272 с.

15. *Petrenko A., Yevtushenko N., Bochmann G.* Fault models for testing in context // Intern. Conf. on Formal Description Techniques IX. 1996. P. 163–178.

16. *Жигулин М.В.* Методы синтеза проверяющих тестов с гарантированной полнотой для контроля дискретных управляющих систем на основе временных автоматов. Дис. ... канд. тех. наук. 2012. 109 с.

17. *Vinarskii E., Lopez J., Kushik N., Yevtushenko N., Zeghlache D.* A model checking based approach for detecting sdn races // The 31st IFIP WG 6.1 Intern. Conf. on Testing Software and Systems. 2019. P. 194–211.

USING FSM-BASED STRATEGIES FOR DERIVING TESTS WITH GUARANTEED FAULT COVERAGE FOR INPUT/OUTPUT AUTOMATA

I. Burdonov[1] [0000-0001-9539-7853], N. Yevtushenko[2] [0000-0002-4006-1161], A. Kossachev[3] [0000-0001-5316-3813]

[1, 2,3]*Ivannikov Institute for system programming of the Russian Academy of Sciences, Moscow*

[1]igor@ispras.ru, [2]evtushenko@ispras.ru, [3]kos@ispras.ru

Abstract

In this paper, we study the possibility of using Finite State Machine (FSM-) based methods for deriving finite test suites with guaranteed fault coverage for Input / Output automata. A method for deriving an FSM for a given automaton is proposed and it is shown that finite test suites derived for such an FSM are complete for two fault models based on Input/Output automata if they are applied within the framework of proper timeouts.

Keywords: *Input/Output automaton, Finite State machine, fault model, complete test suite*

REFERENCES

1. *Hennie F.C.* Fault-Detecting Experiments for Sequential Circuits // The Fifth Ann. Symp. Switching Circuit Theory and Logical Design. 1964. P. 95–110.
2. *Vasilevskii M.P.* Failure diagnosis of automata. translated from Kibernetika. 1973. No. 4. P. 98–108.
3. *Bochmann G.V., Petrenko A.* Protocol testing: review of methods and relevance for software testing // Intern. Symp. on Software Testing and Analysis. 1994. P. 109–123.
4. *Dorofeeva R., El-Fakih K., Cavalli A., Maag S., Yevtushenko N.* FSM-based conformance testing methods: A survey annotated with experimental evaluation // Information & Software Technology. 2010. Vol. 52. No. 12. P. 1286–1297.
5. *Tretmans J.* A formal approach to conformance testing // The Intern. Workshop on Protocol Test Systems. 1993. P. 257–276.

6. *Burdonov I.B., Kossachev A.S., Kuliamin V.V.* Conformance theory for systems with blocking and destruction. Nauka, 2008. 412 p.

7. *Kushik N., Forostyanova M., Prokopenko S., Yevtushenko N.* Studying the optimal height of the EFSM equivalent for testing telecommunication protocols // Intern. Conf. on Advances in Computing, Communication and Information Technology. 2014. P. 159–163.

8. *Zhigulin M.V., Kolomeez A.V., Kushik N.G., Shabaldin A.V.* Testing an IRC implementation using an extended FSM model // Bulletin of the Tomsk Polytechnic University. 2011. Vol. 318. No. 5. P. 81–84.

9. *Lee D, Yannakakis M.* Principles and methods of testing finite-state machines – a survey // Proceedings of the IEEE. 1996. Vol. 84. No. 8. P. 1089–1123.

10. *Petrenko A., Y*evtushenko N. Testing from Partial Deterministic FSM Specifications // IEEE Trans. Computers. 2005. Vol. 54. No. 9. P. 1154–1165.

11. *Petrenko A., Yevtushenko N.* Conformance Tests as Checking Experiments for Partial Nondeterministic FSM // Lecture Notes in Computer Science. 2005. Vol. 3997. P. 118–133.

12. *Yevtushenko N., Burdonov I., Kossachev A.* Deriving Distinguishing Sequences for Input/Output Automata // The IEEE East-West Design & Test Symposium.. 2020. P. 1–5.

13. *Yevtushenko N., Burdonov I., Kossachev A.* Deriving complete test suites for Input / Output Automata // XXIV Russian conference «Scientific Service on the Internet». 2022. P. 93–103.

14. *Gill A.* Introduction to automata theory. M.: Nauka, 1966. 272 p.

15. *Petrenko A., Yevtushenko N., Bochmann G.V.* Fault models for testing in context // Intern. Conf. on Formal Description Techniques IX. 1996. P. 163–178.

16. *Zhigulin M.V.* Timed FSM based test derivation methods for checking control systems. PhD thesis. 2012. 109 p.

17. *Vinarskii E., Lopez J., Kushik N., Yevtushenko N., Zeghlache D.* A model checking based approach for detecting sdn races // The 31st IFIP WG 6.1 Intern. Conf. on Testing Software and Systems. 2019. P. 194–211.

СВЕДЕНИЯ ОБ АВТОРАХ

БУРДОНОВ Игорь Борисович – ведущий научный сотрудник Института системного программирования им. В.П. Иванникова РАН. Сфера научных интересов – моделирование и верификация программных систем, теория графов, теория автоматов

Igor Borisovich BURDONOV *– Leading Researcher, Ivannikov Institute for System Programming of the RAS. Research interests – modeling and verification of software systems, graph theory, automata*

email: igorburdonov@yandex.ru; igor@ispras.ru

ORCID: 0000-0001-9539-7853

ЕВТУШЕНКО Нина Владимировна – ведущий научный сотрудник Института системного программирования им. В.П. Иванникова РАН. Сфера научных интересов – теория автоматов, моделирование, верификация и верификация программных систем, телекоммуникационные протоколы и сервисы.

Nina Vladimirovna YEVTUSHENKO *– leading researcher of Ivannikov Institute for System Programming of the RAS. Research interests – automata theory, modeling, verification and testing of software systems, telecommunication protocols and services*

email: nyevtush@gmail.com; evtushenko@ispras.ru

ORCID: 0000-0002-4006-1161

КОСАЧЕВ Александр Сергеевич – ведущий научный сотрудник Института системного программирования им. В.П. Иванникова РАН. Сфера научных интересов – моделирование и верификация программных систем, теория графов, теория автоматов

Alexander Sergeevich KOSSACHEV *– Leading Researcher, Ivannikov Institute for System Programming of the RAS. Research interests - modeling and verification of software systems, graph theory, automata*

email: askosachev@gmail.com; kos@ispras.ru

ORCID: 0000-0001-5316-3813

Материал поступил в редакцию 23 января 2023 года