УДК 004.414.28 + 004.415.52

МЕТОДИКА ВЕРИФИКАЦИИ АВТОМАТНЫХ ПРОГРАММ

К. В. Егоров,
магистрант
А. А. Шалыто,
доктор техн. наук, профессор
Санкт-Петербургский государственный университет информационных технологий, механики и оптики

Описывается разработанный верификатор автоматных программ, созданных при помощи инструментального средства для поддержки автоматного программирования UniMod. При его использовании отсутствует необходимость описывать модель на входном языке верификатора. Требования к программе записываются на языке темпоральной логики линейного времени.

Введение

С момента появления первых программ требовалось проверять их правильность. Причем не просто удостоверяться, что программа работает на конечном числе тестов, а уметь формально доказывать, что ее поведение соответствует заявленной спецификации.

Метод проверки того, что программная система обладает необходимыми свойствами или удовлетворяет определенным требованиям (утверждениям), называется верификацией. К сожалению, верифицировать систему обычно намного сложнее, чем ее создать. Поэтому для не очень ответственных систем верификация не всегда оправдана, и в них проще исправлять ошибки по мере обнаружения при тестировании и в процессе работы. Вместе с тем существуют такие системы, в которых ошибки допускать нельзя [1].

Одним из основных методов проверки программы на наличие ошибок является тестирование. На практике оно применяется в большинстве случаев. Однако «тестирование позволяет показать наличие ошибок, но не их отсутствие»[1]. При таком подходе к проверке можно удостовериться в правильности работы программы только при определенном ее поведении или каком-то конечном числе входных данных. Правда, некоторые ошибки могут появляться крайне редко. Поэтому для того чтобы исключить возможность их появления, требуется рассмотреть все возможные варианты поведения системы, что при тестировании невозможно.

[1] *Dijkstra E. W.* Structured Programming. EWD268 // Technical University. Eindhoven, Netherlands. 1969. P. 2.

Наиболее практичным в настоящее время является метод верификации, названный Model Checking [2, 3]. При его использовании процесс верификации состоит из трех частей: моделирование программы (преобразование программы в формальную модель с конечным числом состояний для последующей верификации) — спецификация (формальная запись утверждений, которые требуется проверить) — собственно верификация. Эти части связаны между собой — алгоритмы верификации зависят от способа построения модели и способа записи требований. При использовании этого метода для программ, написанных традиционно, возникают три проблемы:

- как для произвольной программы построить адекватную модель с конечным числом состояний;
- как переформулировать требования к программе (системе) в требования к модели;
- как при обнаружении ошибки (построении контрпримера) перейти от модели к программе?

Ответы [4, 5] на все эти вопросы могут быть найдены, если программы являются автоматными [6]. Здесь имеет место та же ситуация, что и при контроле аппаратуры, которая при сложной логике не может быть проверена, если она не спроектирована специальным образом с учетом контролепригодности.

Цель настоящей работы состоит в разработке верификатора для автоматных программ, созданных при помощи инструментального средства UniMod [7].

Особенности этого класса программ позволяют решить первую и третью проблемы верификации, так как каждая автоматная программа уже сама по себе является моделью, которая, в отличие от традиционно написанных программ, пригодна для

проверки определенных утверждений о ней либо без ее модификации, как в настоящей работе, либо за счет модификации, которая может быть выполнена автоматически. Вторая проблема в случае автоматных программ решается при проектировании автоматов, устраняя тем самым семантический разрыв между требованиями к программе и модели, который имеет место для традиционно написанных программ.

В настоящей работе требования к программе формулируются в виде формул темпоральной логики линейного времени (*Linear Time Logic, LTL*). Это определяет используемый алгоритм верификации на основе пересечения автоматов *Бюхи* [3].

В ходе работы создан верификатор, не использующий уже существующие верификаторы, применение которых связано с преобразованием модели автоматной программы в модель, описываемую на языке верификатора. Применяя такой язык, после доказательства невыполнимости утверждения об автомате (построении контрпримера) пришлось бы совершать обратное преобразование из модели в автоматную программу.

Верификация автоматных программ

Как отмечено выше, цель настоящей работы состоит в разработке верификатора автоматных программ, созданных при помощи Switch-технологии [6] в инструментальном средстве UniMod [7]. В таких программах выделяются три типа объектов: поставщики событий, система управления и объекты управления.

Система управления представляет собой конечный автомат или систему взаимодействующих автоматов. Автомат — это множество состояний и переходов между ними. Каждый переход помечен событием, при котором он может осуществиться, и условием, выполнимость которого требуется для перехода. Поставщики событий генерируют события, а система управления по каждому событию может совершать переход, считывая значения входных переменных у объектов управления для проверки условия перехода. Такая система называется реагирующей[2] или событийной [8].

UniMod — инструментальное средство, обеспечивающее визуальное проектирование автоматных программ на основе Switch-технологии. Это позволяет вынести практически всю логику программы в автоматы, а остальные классы разбить на два типа: поставщики событий и объекты управления. UniMod написан на языке программирования Java и встраивается в среду разработки Eclipse как дополнительный модуль (plug-in) [7].

При верификации программ на языках типа Java или C++, написанных традиционным путем (без явного выделения состояний), требуется вручную строить по программе модель и описывать ее на языке, понятном используемому верификатору. При этом могут быть утеряны определенные данные и связи в программе, так как приходится переходить на другой уровень абстракции.

Возможны два подхода к использованию автоматной модели для верификации:

- ее формальное преобразование к виду, определяемому выбранным верификатором [5];
- создание верификатора, в котором применяется автоматная модель или некоторое уже существующее ее представление.

В настоящей работе используется второй подход, при котором автоматные программы создаются с помощью инструментального средства UniMod, а для верификации применяется XML-описание автоматов, являющееся внутренним представлением графов переходов автоматов в указанном средстве.

Автоматная модель, которая строится при создании системы в рамках Switch-технологии, может верифицироваться без изменений или с изменениями, которые не приводят к потере данных о ней. Другое достоинство автоматных программ, резко упрощающее их верификацию, — возможность достаточно просто переформулировать требования к системе в высказывания об автоматах, так как в этом случае при проектировании программы строится модель ее поведения, которая может применяться и при верификации.

В настоящей работе верифицируется не вся автоматная программа, а только ее модель, представленная в общем случае системой вложенных автоматов. При этом поставщики событий и объекты управления рассматриваются в качестве «внешней среды», которая ничего не помнит о последовательности переходов рассматриваемого автомата и вызванных действиях. Таким образом, в любой момент времени может быть совершен любой переход из текущего состояния автомата. Такой подход уже был рассмотрен в работе [9].

Для описания требований к автоматным программам будем применять, как уже отмечалось, язык LTL. В нем время линейно и дискретно. Синтаксис LTL включает в себя пропозициональные переменные Prop, булевы связки ($\neg$, $\wedge$, $\vee$) и темпоральные операторы. Последние применяются для составления утверждений о событиях в будущем.

Будем использовать следующие темпоральные операторы:

- **X** (ne**X**t) — «Xp» — в следующий момент выполнено p;
- **F** (in the **F**uture) — «Fp» — в некоторый момент в будущем будет выполнено p;
- **G** (**G**lobally in the future) — «Gp» — всегда в будущем выполняется p;
- **U** (**U**ntil) — «pUq» — существует состояние, в котором выполнено q и до него во всех предыдущих выполняется p;
- **R** (**R**elease) — «pRq» — либо во всех состояниях выполняется q, либо существует состояние,

[2] В русскоязычной литературе также употребляется термин «реактивная» система.

в котором выполняется p, а во всех предыдущих выполнено q.

Множество LTL-формул таково:

- пропозициональные переменные Prop;
- True, False;
- φ и ψ — формулы, то
  - $\neg\varphi, \varphi\wedge\psi, \varphi\vee\psi$ — формулы;
  - $X\varphi, F\varphi, G\varphi, \varphi U\psi, \varphi R\psi$ — формулы.

Оказывается, что как модель автоматной программы, так и LTL-формулу можно представить в виде автомата Бюхи. Формально он определяется пятеркой (S, E, T, s_0, F), где:

S — конечное множество состояний;

E — множество меток переходов;

$T \subseteq S\times E\times S$ — множество переходов;

s_0 — начальное состояние;

$F \subseteq S$ — множество допускающих состояний.

Тогда путь в этом графе $\pi = s_0, s_1, s_2, ..., s_n, ...$, для которого выполнено $T(s_{i-1}, e, s_i)$, где e — метка перехода, будет последовательностью вычислений системы. Путь является *допускающим*, если существует состояние из множества F, встречающееся бесконечно часто.

Подробно о трансляции LTL-формулы в автомат Бюхи изложено в работах [3, 10, 11].

При этом отметим, что в автоматной программе модель поведения может являться одним автоматом или системой вложенных автоматов. При использовании рассматриваемого подхода по системе автоматов строится автомат-произведение [12]. Автомат или автомат-произведение представляет собой автомат Бюхи, в котором метка на переходе — это выполнимость определенного предиката. Под предикатом будем понимать утверждение о текущем переходе, например, вызванные автоматом действия в объектах управления или состояние, в которое перешел автомат.

Для доказательства невыполнимости некоторой LTL-формулы на автомате Бюхи можно проверить, что пересечение верифицируемого автомата Бюхи и автомата Бюхи, соответствующего отрицанию LTL-формулы, пусто. Для этого требуется доказать, что язык автомата пересечения пуст. Из сказанного следует, что алгоритм верификации может быть следующим: строится автомат Бюхи для верифицируемой автоматной программы, по отрицанию LTL-формулы строится автомат Бюхи, затем строится автомат пересечения, а после этого проверяется, что этот автомат не допускает ни одного слова.

В связи с тем, что рассматриваются бесконечные слова, то, как доказано в работе [3], для пустоты пересечения достаточно доказать, что ни одно допускающее состояние не принадлежит сильной компоненте связанности, которая достижима из начального состояния (не существует цикла, проходящего через допускающее состояние). Таким образом, при нахождении цикла, достижимого из начального состояния, будет построен контрпример — путь, на котором не выполняется LTL-формула.

При верификации обычно применяют двойной обход в глубину [3], преимущество которого состоит в том, что для реализации этого алгоритма не требуется построение автомата-пересечения целиком — можно строить состояния пересечения автоматов по мере их достижения. Это дает выигрыш на больших моделях.

Общая идея алгоритма такова: обходим в глубину автомат пересечения, при достижении допускающего состояния для проверки достижимости самого себя запускаем второй обход в глубину из данного состояния. Если оказалось, что допускающее состояние достижимо из самого себя, то цикл найден. Следовательно, исходная LTL-формула не выполняется на автомате Бюхи, представляющем модель программы, и найден контрпример.

Верификация системы вложенных автоматов

Как было отмечено, алгоритм верификации *одного автомата* может быть записан следующим образом.

1. Модель программы представляется в виде автомата Бюхи.

2. Строится отрицание LTL-формулы.

3. По отрицанию LTL-формулы строится автомат Бюхи с переходами, помеченными специально введенными предикатами.

4. Производится двойной обход в глубину неявного пересечения двух автоматов Бюхи. Для построения пересечения выполняются следующие действия.

4.1. Перебираются все переходы верифицируемого автомата.

4.2. Перебираются все возможные переходы автомата, построенного по отрицанию LTL-формулы, для перехода верифицируемого автомата, полученного на шаге 4.1.

Для верификации *системы вложенных автоматов* применяется такой же алгоритм, только в качестве верифицируемого автомата строится автомат-произведение [12], состояния которого содержат информацию о состояниях всех автоматов иерархической системы. Каждое состояние нового автомата представляет собой дерево, структура которого совпадает со структурой системы вложенных автоматов. В узлах дерева размещены состояния, в которых находятся соответствующие конечные автоматы. Узел может быть активным, если соответствующий автомат может обрабатывать события, и неактивным, если автомат не может обрабатывать события. Переходы из такого состояния могут совершаться только по переходам одного из активных внутренних состояний. При этом активные и неактивные состояния могут вычисляться следующим образом.

1. Состояние активно, если состояние, в которое вложен автомат, является родителем и активно.

2. Состояние неактивно, если состояние, в которое вложен автомат, не является родителем или неактивно.

При таком подходе, если состояние неактивно, то все вложенные в него состояния также неактивны. Это позволяет строить переходы из такого сложного состояния, просматривая не все узлы дерева, а только активные.

Такая структура является неявным произведением автоматов. Однако преимущество этого алгоритма состоит в том, что он позволяет строить произведение системы вложенных автоматов не сразу, а по мере их посещения при обходе в глубину. Это дает возможность обнаружить контрпример до того, как будет построено полное произведение автоматов.

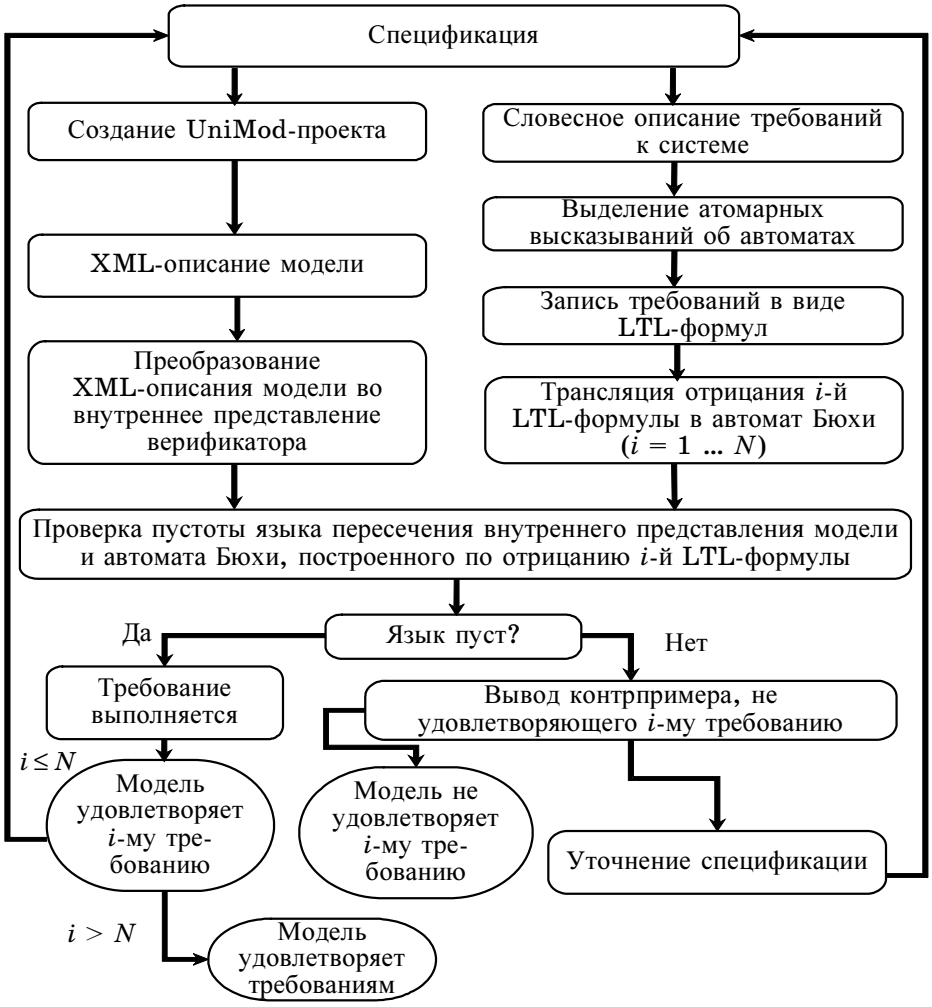
От произведения автоматов нельзя отказаться, так как если требуется делать утверждения о состоянии системы автоматов в целом, то необходимо иметь представление такого глобального состояния. Верификатор, разработанный в настоящей работе, предоставляет возможность проверять утверждения как об отдельном автомате иерархической системы, так и обо всей системе в целом.

Не всегда утверждение об одном автомате имеет тот же результат, что и утверждение о системе вложенных автоматов. Например, утверждение «$G(isInState(A2.s1) \rightarrow X(isInState(A2.s2)))$» (Если автомат *A2* находится в состоянии *s1*, то следующим состоянием будет *s2*) вполне может быть истинным для автомата *A2*. Однако если автомат *A2* вложен в *A1*, то это утверждение не будет выполняться для такой системы автоматов, так как если автомат *A2* находится в состоянии *s1*, то следующий переход может совершить автомат *A1*, и тогда утверждение не будет выполнено.

Методика верификации автоматных программ

Приведем методику использования созданного верификатора. На рис. 1 изображена схема процесса верификации автоматных программ, созданных при помощи инструментального средства UniMod.

Разрабатывается спецификация будущей программы. Она описывает поведение программы и требования к ней, которые должны выполняться. Это необходимо для того, чтобы в дальнейшем была возможность проверить утверждения о программе. Иначе во время верификации не понятно,



■ ***Рис. 1****. Методика верификации UniMod-моделей*

какие свойства программы требуется проверять, и какие из них должны выполняться, а какие нет.

После создания спецификации возможны два варианта: сначала создать UniMod-проект, а затем записать для него словесные требования к системе, проверяемые верификатором, или же сначала сформулировать проверяемые требования, а затем создать программу. Не исключено также, что спецификация уже включает в себя четко сформулированные требования об автоматной программе, выполнение которых планируется проверять.

Модель UniMod-проекта сохраняется в виде XML-файла, который и будет использоваться верификатором для проверки утверждений. XML-файл автоматически генерируется инструментальным средством UniMod при создании программы. Поэтому можно ожидать, что в нем нет ошибок, свойственных построению вручную.

После словесного описания требований из них выделяются атомарные высказывания (предикаты), соответствующие утверждениям о переходах и состояниях в UniMod-модели. Например, требование системе «*После возникновения аппаратной ошибки система отменит последнюю операцию*» может быть переформулировано в высказывание об автомате: «*После события p1.e10, рано или поздно, будет вызвано действие o1.z10*», где *p1.e10* — событие, посылаемое при аппаратной ошибке, а *o1.z10* — откат последней операции.

Такие преобразования над утверждениями позволяют записать требования к модели в виде LTL-формул. Если выразительная способность языка LTL не позволяет записать требования в виде LTL-формул, то они должны быть переформулированы.

По XML-описанию модели и LTL-формулам (их отрицаниям) начинается работа созданного верификатора. В ходе работы верификатор подтверждает выполнимость утверждения или выдает контрпример в виде последовательности переходов автомата пересечения автомата модели и автомата Бюхи, построенного по инверсии LTL-формулы. Пользователю доступен выбор между верификацией одного автомата или иерархической системы автоматов.

Продолжим описание работы верификатора. Верификатор читает XML-файл и автоматически строит по нему модель для верификации.

Затем по LTL-формуле строится ее отрицание, и оно транслируется в автомат Бюхи. Трансляция в автомат Бюхи может быть осуществлена как разработанным авторами транслятором, так и при помощи транслятора LTL2BA [13]. Оба способа трансляции автоматические, и пользователь верификатора может не заметить, какой из трансляторов был использован для построения автомата Бюхи.

Затем верификатор совершает двойной обход в глубину по пересечению модели автоматной программы и автомата Бюхи, полученного по инверсии LTL-формулы. При этом пересечение двух автоматов строится не сразу, а по мере посещения состояний автомата пересечения. Как отмечалось выше, при невыполнимости формулы это позволяет обнаружить контрпример, не строя пересечение автоматов в целом.

Если верификатор обнаружил контрпример, то, возможно, найдена ошибка в UniMod-модели. Тогда требуется внесение изменения в UniMod-модель, ее сохранение в виде XML-файла, а затем повторная верификация. Если же контрпример не является ошибкой в UniMod-модели из-за неправильной формулировки требований или же из-за неучтенной внутренней реализации поставщиков событий и объектов управления, то необходимо уточнение утверждения, повторная его запись в виде LTL-формулы и повторная верификация.

Если верификатор подтвердил выполнимость всех LTL-формул, то можно полагать, что модель удовлетворяет заявленным требованиям. Повторная верификация может быть запущена при внесении в модель изменений в целях проверки заявленных свойств.

Для простоты повторной верификации предлагается оформлять каждое проверяемое утверждение в виде отдельного Unit-теста. Тогда при внесении изменения в UniMod-модель имеется возможность повторного запуска всех тестов. При их выполнимости можно утверждать, что модель соответствует заявленным требованиям.

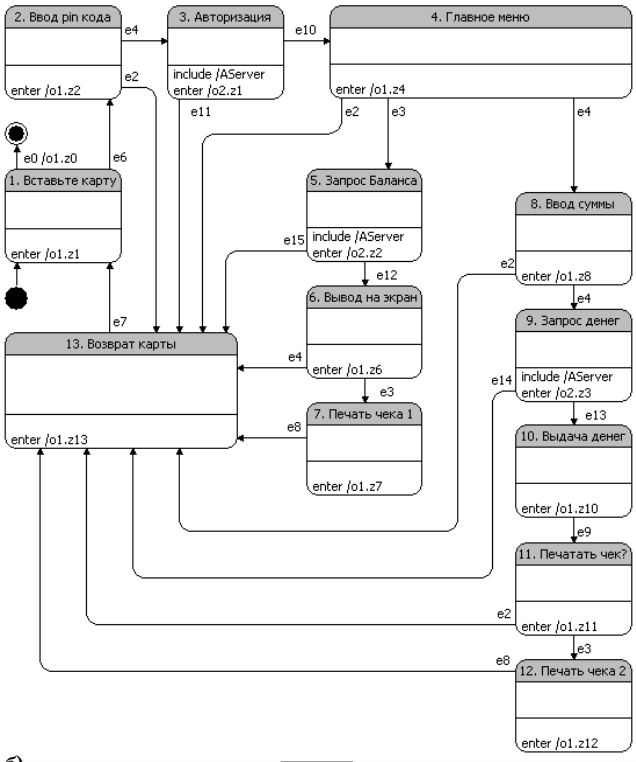
Тестирование верификатора

Во время разработки верификатора проводилось тестирование всех его частей на UniMod-проектах [14, 15]. На автоматной модели этих проектов были проверены некоторые свойства. Верификатор доказал верные утверждения и опроверг неверные, тем самым подтвердив возможность своего применения.

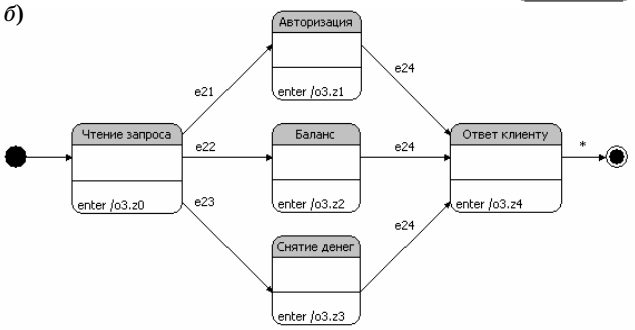
Проект [15] реализует банкомат (рис. 2, *а, б*), позволяющий пользователю совершать такие операции, как снятие наличных денег и просмотр доступных средств на счете. Модель банкомата представляет собой двухуровневую структуру автоматов, где автомат AServer вложен в автомат AClient. Рассмотрим одно из проверенных утверждений про банкомат: «*Пользователь не может запросить снятие наличных или запросить баланс до тех пор, пока не пройдет авторизацию*». При выделении из утверждения предикатов получаем утверждение про автомат: «*Автомат AClient не попадет в состояние "Запрос баланса" или в состояние "Запрос денег" до тех пор, пока не произойдет событие p3.e10*». В утверждении применяется предикат об обработке события *p3.e10*, а не посещение состояния «*Авторизация*», так как это событие означает прохождение авторизации, а состояние — обращение к серверу для проверки правильности введения pin-кода.

Верифицируемое утверждение записывается в виде LTL-формулы: «*wasEvent(p3.e10) R*

а)



б)



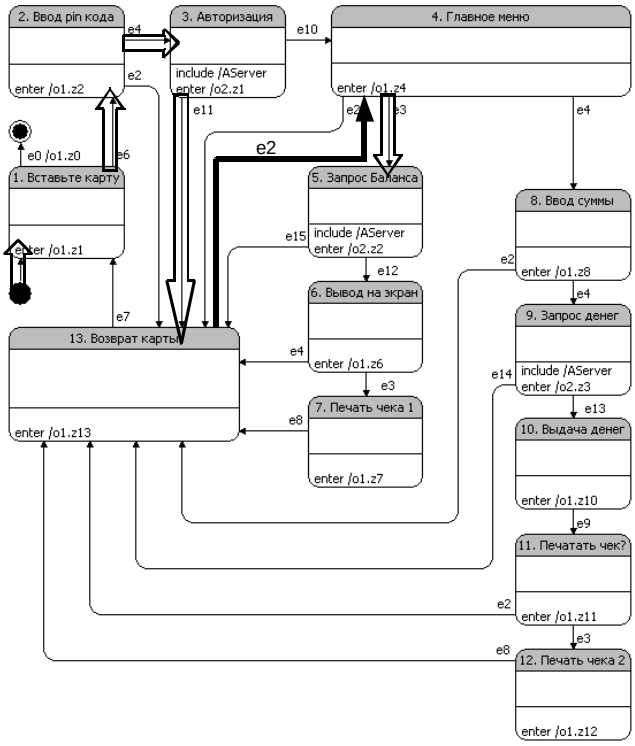
■ ***Рис. 2.*** *Модель банкомата: а — автомат AClient; б — вложенный автомат AServer*

(!isInState (AClient[«Запрос баланса»]) && !isInState(AClient[«Запрос денег»]))».

Здесь используется оператор *R* (Release), а не *U* (Until), так как событие *p3.e10* может вообще не произойти из-за недоступности сервера или из-за того, что пользователь забыл свой pin-код. Данное утверждение выполняется для модели банкомата.

Предположим, что кто-то внес в автомат AClient еще один переход из состояния «*Возврат карты*» в состояние «*Главное меню*» по событию *e2* (рис. 3). Такое изменение модели нарушает спецификацию банкомата, так как появляется возможность снять наличные или запросить баланс без авторизации. При верификации измененной модели верификатор обнаруживает контрпример, нарушающий спецификацию.

Этот контрпример верификатор выдает в виде последовательности переходов: [*s1, s1*]→[«*Вставьте карту*», *s1*]→[«*Ввод pin-кода*», *s1*]→[«*Авторизация*», *s1*]→[«*Авторизация*», «*Чтение запроса*»]→[«*Авторизация*», «*Авторизация*»]→[«*Авторизация*», «*Ответ клиенту*»]→[«*Авторизация*», *s2*]→[«*Возврат карты*», *s2*]→[«*Главное меню*», *s2*]→[«*Запрос баланса*», *s2*]. В квадратных скобках указаны состояния автоматов AClient и AServer; *s1* — стартовое состояние автомата, а *s2* — завершающее.



■ ***Рис. 3.*** *Измененная модель банкомата* (*жирной и крупными стрелками выделена последовательность переходов, нарушающая спецификацию*)

Из предложенной последовательности переходов следует, что достичь состояния «*Запрос баланса*» можно, не пройдя авторизацию, так как в ней отсутствует переход по событию *p3.e10*. Достижение данного состояния таким способом свидетельствует о возможности запросить баланс без прохождения авторизации.

Заключение

Представленный разработанный авторами верификатор автоматных программ, создаваемых при помощи инструментального средства UniMod, позволяет верифицировать модели программ, которые автоматически строятся верификатором по XML-описанию, создаваемому указанным средством по автоматной модели программы. Требования к модели записываются на языке LTL. Верификатор предоставляет набор классов и интерфейсов на языке программирования Java для проверки выполнимости LTL-формул.

При создании верификатора были решены следующие подзадачи:

- трансляция XML-описания модели во внутреннее представление верификатора;
- трансляция LTL-формулы в автомат Бюхи;
- проверка пустоты языка пересечения модели и автомата Бюхи, построенного по отрицанию LTL-формулы.

Для трансляции LTL-формулы в автомат Бюхи был реализован собственный транслятор и использовался уже существующий транслятор LTL2BA [13].

Применение автоматного подхода к написанию программ и созданного верификатора позволяет разрабатывать более надежное программное обеспечение по сравнению с традиционным подходом. Предлагается использовать созданный верификатор для построения и проверки Unit-тестов, которые можно запускать на любой стадии жизненного цикла проекта.

Литература

1. **Hoffman L.** In Search of Dependable Design // Communications of the ACM. 2008. Vol. 51. N 7. P. 14–16.
2. **Hoffman L.** Talking Model-Checking Technology // Communications of the ACM. 2008. Vol. 51. N 7. P. 110–112.
3. **Кларк Э., Грамберг О., Пелед Д.** Верификация моделей программ: Model Checking. М.: МЦНМО, 2002. 416 с.
4. **Корнеев Г. А., Парфенов В. Г., Шалыто А. А.** Верификация автоматных программ // Компьютерные науки и технологии: Тез. докл. Междунар. науч. конф., посвященной памяти профессора А. М. Богомолова. Саратов: СГУ, 2007. С. 66–69.
5. **Васильева К. А., Кузьмин Е. В., Соколов В. А.** Верификация автоматных программ с использованием LTL // Моделирование и анализ информационных систем. 2007. № 1. С. 3–14.
6. **Шалыто А. А.** Switch-технология. Алгоритмизация и программирование задач логического управления. СПб.: Наука, 1998. 628 с.
7. **Гуров В. С., Мазин М. А., Нарвский А. С., Шалыто А. А.** UML. SWITCH-технология. Eclipse // Информационно-управляющие системы. 2004. № 6. С. 12–17.
8. **Harel D., et al.** Statemate: A Working Environment for the Development of Complex Reactive Systems // IEEE Trans. Software Eng. 1990. N 4. P. 403–414.
9. **Разработка** технологии верификации управляющих программ со сложным поведением, построенных на основе автоматного подхода. Второй этап. СПбГУ ИТМО, 2007. 105 с. http://is.ifmo.ru/verification/_2007_02_report-verification.pdf
10. **Gerth R., Peled D., Vardi M. Y., Wolper P.** Simple On-the-fly Automatic Verification of Linear Temporal Logic: Proc. of the 15th Workshopon Protocol Specification. Warsaw: Testing, and Verification, 1995. P. 3–18.
11. **Courcoubetis C., Vardi M., Wolper P., Yannakakis M.** Memory-Efficient Algorithms for the Verification of Temporal Properties // Formal Methods in System Design. 1992. P. 275–288.
12. **Хопкрофт Д., Мотвани Р., Ульман Д.** Введение в теорию автоматов, языков и вычислений. М.: Вильямс, 2002. 528 с.
13. **LTL 2 BA project.** http://www.lsv.ens-cachan.fr/~gastin/ltl2ba/
14. **Егоров К. В., Райков П. М.** Игра «Побег». СПбГУ ИТМО. 2007. http://is.ifmo.ru/unimod-projects/la_redada/
15. **Козлов В. А., Комалева О. А.** Моделирование работы банкомата. СПбГУ ИТМО. 2006. http://is.ifmo.ru/unimod-projects/bankomat/