

На правах рукописи

**ГРОМОВ Максим Леонидович**

**РАЗРАБОТКА МЕТОДОВ СИНТЕЗА УСЛОВНЫХ ТЕСТОВ ДЛЯ  
АВТОМАТНЫХ МОДЕЛЕЙ С НЕДЕТЕРМИНИРОВАННЫМ  
ПОВЕДЕНИЕМ**

05.13.01 — системный анализ, управление и обработка информации  
(в отраслях информатики, вычислительной техники и автоматизации)

**АВТОРЕФЕРАТ**

диссертации на соискание ученой степени  
кандидата физико-математических наук

**Томск 2009**

Работа выполнена на кафедре информационных технологий в исследовании дискретных структур в ГОУ ВПО «Томский государственный университет»

**Научный руководитель:** доктор техн. наук, профессор  
Евтушенко Нина Владимировна

**Официальные оппоненты:** доктор физ.-мат. наук,  
старший научный сотрудник  
Бурдонов Игорь Борисович  
  
кандидат техн. наук, доцент  
Голубева Ольга Ивановна

**Ведущая организация:** Институт математики им. С.Л. Соболева СО РАН,  
г. Новосибирск

**Защита состоится:**

24 декабря 2009 года в 12:30 час. на заседании диссертационного совета Д 212.267.12 при ГОУ ВПО «Томский государственный университет» по адресу: 634050, г. Томск, пр. Ленина, 36, II уч. корпус, ауд. 212 б.

С диссертацией можно ознакомиться в Научной библиотеке ГОУ ВПО «Томский государственный университет» по адресу: 634050, г. Томск, пр. Ленина, 34а.

**Автореферат разослан 18 ноября 2009 г.**

Ученый секретарь  
диссертационного совета  
доктор технических наук,  
профессор

В.И. Смагин

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность проблемы.** Тестирование является неотъемлемой частью жизненного цикла любой системы. Под тестированием понимается процесс подачи входных воздействий на тестируемую систему, наблюдение выходных реакций и вывод заключения о правильном или неправильном поведении системы. Эмпирические тесты оказались недостаточными для систем управления сложными процессами, что, в свою очередь, привело к новому витку развития тестирования на основе формальных моделей. При синтезе тестов для дискретных управляющих систем одной из широко используемых моделей является автоматная модель, и методы синтеза проверяющих тестов с гарантированной полнотой хорошо развиты для детерминированных автоматов. Однако в ряде случаев поведение системы описывается недетерминированным автоматом. Причины появления недетерминизма в спецификациях и реализациях, вообще говоря, различные; среди них можно выделить наличие альтернатив при реализации, уровень абстракции описания, невозможность полной управляемости и наблюдаемости для реализации и так далее. Одной из основных проблем при синтезе тестов для недетерминированных реализаций является тот факт, что в общем случае недетерминированный (проверяемый) автомат может реагировать различными выходными последовательностями на одну и ту же входную последовательность. Поэтому обычно при тестировании реализаций с недетерминированным поведением делается допущение о «всех погодных условиях», то есть предполагается, что каждая тестовая входная последовательность подается на реализацию достаточно большое число раз в «различных погодных условиях», и поэтому можно считать, что тестер пронаблюдал все возможные выходные реакции реализации на каждую входную последовательность. Допущение о «всех погодных условиях» является скорее теоретическим, так как никто не знает, сколько раз достаточно подать входную последовательность, чтобы дать возможность тестеру «увидеть» все выходные реакции реализации. Более того, такому предположению невозможно удовлетворить, если проверяемый автомат является только частично контролируемым, что имеет место, например, при удаленном тестировании реализаций телекоммуникационных протоколов. В ряде работ предлагаются методы синтеза проверяющих тестов без использования предположения о «всех погодных условиях» при проведении безусловного эксперимента с проверяемой системой. Длины этих тестов большие, однако известно, что длина тестов может быть существенно сокращена, если использовать условный эксперимент при тестировании проверяемой системы. Таким образом, разработка методов синтеза условных проверяющих и диагностических тестов для систем с автоматным поведением без использования предположения о «всех погодных условиях» является актуальной задачей.

**Цель работы.** Разработка методов синтеза условных диагностических и проверяющих тестов для автоматных моделей с недетерминированным поведением, а именно для недетерминированных конечных автоматов, входо-выходных полуавтоматов и временных автоматов.

**Методы исследования.** Для решения поставленных задач применяется аппарат дискретной математики, в частности, теории автоматов, математической логики, а также используются компьютерные эксперименты с целью исследования эффективности предлагаемых методов.

## **Научная новизна.**

1. Показано, что два недетерминированных автомата различимы условным экспериментом, если и только если эти автоматы не имеют общей квази-редукции, то есть являются *r*-различимыми. Предложен способ представления условного эксперимента по распознаванию двух *r*-различимых автоматов в виде специального *r*-различающего автомата. Предложен метод построения полного проверяющего условного теста по недетерминированному автомату-спецификации относительно области неисправности, описанной мутационным автоматом.

2. Показано, что два входо-выходных полуавтомата различимы условным экспериментом, если и только если эти полуавтоматы не имеют общей **ioco**-реализации, то есть являются **ioco**-различимыми. Предложен способ представления условного эксперимента по распознаванию двух **ioco**-различимых полуавтоматов в виде специального **ioco**-различающего полуавтомата.

3. Показано, что задачу построения конечного полного проверяющего теста относительно модели входо-выходного полуавтомата можно свести к задаче построения такого теста для недетерминированного автомата, и тем самым показано, что при построении конечного полного проверяющего теста для входо-выходных полуавтоматов можно использовать известные методы синтеза таких тестов для конечных автоматов.

4. Введена модель временного автомата как частный случай известного расширенного временного автомата. Введены понятия пересечения и различимости двух временных недетерминированных автоматов, и показано, что два недетерминированных временных автомата различимы условным экспериментом, если и только если эти временные автоматы не имеют общей квази-редукции. Предложен алгоритм построения временного автомата, представляющего условный эксперимент по распознаванию двух различимых временных автоматов.

**Достоверность полученных результатов.** Все научные положения и выводы, содержащиеся в работе, основаны на утверждениях, доказанных с использованием аппарата дискретной математики.

**Практическая ценность.** Предложенные в работе методы и алгоритмы могут быть использованы в системах автоматизированного синтеза тестов для дискретных управляющих систем, в частности, в системах автоматического синтеза проверяющих и диагностических тестов для телекоммуникационных протоколов.

**Реализация и внедрение результатов работы.** Результаты диссертационной работы получены в рамках следующих проектов:

1. 6<sup>ая</sup> рамочная программа TAROT «Мобильность молодых учёных», 2003–2007 гг.

2. НИР «Разработка математических и программных средств обеспечения надёжного и безопасного доступа к электронным ресурсам коллективного пользования» (в рамках инновационного проекта ТГУ), 2006–2007 гг.

3. НИР «Проведение прикладных и проблемно-ориентированных поисковых исследований в области информационно-телекоммуникационных систем с участием научных организаций Франции» (шифр заявки «2009-04-1.4-00-02-003», госконтракт № 02.514.12.4002 от 09.06.2009).

Основные результаты работы используются в учебном процессе Томского государственного университета.

## **Основные положения, выносимые на защиту.**

1. Необходимые и достаточные условия распознавания двух недетерминированных автоматов условным экспериментом и представление такого условного эксперимента конечным автоматом.

2. Необходимые и достаточные условия распознавания двух входо-выходных полуавтоматов условным экспериментом и представление такого условного эксперимента конечным входо-выходным полуавтоматом.

3. Метод построения полного проверяющего теста относительно модели входо-выходного полуавтомата на основе построения полного теста для соответствующего недетерминированного автомата, что позволяет строить конечные проверяющие тесты для входо-выходных полуавтоматов с гарантированной полнотой относительно ряда моделей неисправности.

4. Модель конечного временного автомата, являющаяся частным случаем расширенного временного автомата; понятие различимости для временных недетерминированных автоматов и критерий различимости двух недетерминированных временных автоматов условным экспериментом; представление условного эксперимента, различающего два временных автомата, в виде временного автомата.

**Апробация работы.** Научные результаты, составившие основу данной работы, обсуждались на заседаниях объединенного научного семинара кафедры информационных технологий в исследовании дискретных структур радиофизического факультета, кафедры программирования и кафедры защиты информации и криптографии факультета прикладной математики и кибернетики ТГУ.

Результаты работы докладывались на российских и международных конференциях: «East-West Design and Test Workshop» (Одесса, 2005 и Львов, 2008); IX международном семинаре «Дискретная математика и её приложения» (Москва, 2007); Российской конференции с международным участием «Новые информационные технологии в исследовании сложных структур» (Иркутск, 2004 и Шушенское, 2006); международных конференциях TESTCOM-2007 (Таллин, 2007) и SYRCoSE (Санкт-Петербург, 2008).

По результатам проведенных исследований опубликовано 10 статей в научных журналах, докладов и тезисов докладов на конференциях различного уровня, в том числе в пяти рецензируемых журналах, один из которых входит в перечень изданий, рекомендованных ВАК РФ.

**Структура и объем диссертации.** Диссертация состоит из введения, четырех глав, заключения и списка литературы; изложена на 152 страницах, включая 7 рисунков и список литературы из 77 наименований.

## **СОДЕРЖАНИЕ РАБОТЫ**

Во **введении** дается общая характеристика работы, обосновывается актуальность исследований, определяется тематика и формулируется цель работы, кратко излагаются основные задачи и результаты, выносимые на защиту.

В **первой главе** диссертации вводятся основные определения и понятия, и предлагается краткий обзор известных результатов по синтезу тестов для автоматных моделей с недетерминированным поведением.

Под *детерминированным входо-выходным полуавтоматом* (или просто *полуавтоматом*) с входным алфавитом  $I$  и выходным алфавитом  $O$  будем понимать пятёрку

$L = \langle L, I, O, \hat{l}, \lambda_L \rangle$ , где  $L$  – непустое конечное множество состояний с выделенным начальным состоянием  $\hat{l}$ ;  $I$  и  $O$  – непересекающиеся конечные алфавиты входных и выходных действий (символов) соответственно,  $I \cup O \neq \emptyset$ . Отношение  $\lambda_L \subseteq L \times (I \cup O) \times L$  есть отношение переходов; если  $\langle l, a, l' \rangle \in \lambda_L$  и  $\langle l, a, l'' \rangle \in \lambda_L$ , то  $l' = l''$ . Переход  $\langle l, a, l' \rangle$  для удобства будем записывать как  $l \xrightarrow{a} l'$ . Состояние  $l$  полуавтомата  $L$  называется *молчащим*, если для любого действия  $a$  из  $O$  и любого состояния  $l'$  из  $L$  верно  $\langle l, a, l' \rangle \notin \lambda_L$ .

В данной работе мы предполагаем, что ситуацию, когда полуавтомат находится в молчащем состоянии, можно отличить от ситуации, когда полуавтомат находится в состоянии, в котором он готов произвести выходное действие. Для формального описания этой возможности вводится новое выходное действие  $\delta$ , и если некоторое состояние  $l$  – молчащее, то подразумевается, что  $l \xrightarrow{\delta} l$ . Естественным образом отношение переходов распространяется на последовательности из алфавита  $(I \times O \cup \{\delta\})^*$ .

Введём следующие обозначения:

1.  $\llbracket l \rrbracket_\sigma$  – множество всех состояний, достижимых из состояния  $l$  по последовательности  $\sigma \in (I \times O \cup \{\delta\})^*$ . В детерминированном полуавтомате  $|\llbracket l \rrbracket_\sigma| \leqslant 1$ .
2. **out**( $l$ ) – множество всех выходных действий, включая  $\delta$ , переходы по которым определены в состоянии  $l$ .
3. **in**( $l$ ) – множество всех входных действий, переходы по которым определены в состоянии  $l$ .
4. *s-traces* $_L$  – множество всех конечных последовательностей из  $(I \times O \times \{\delta\})^*$ , таких, что по ним возможны переходы из начального состояния полуавтомата  $L$ .

Полуавтомат  $L$  называется *полностью определённым по входам* (или просто *полностью определённым*), если для каждого его состояния  $l$  справедливо **in**( $l$ ) =  $I$ .

Полностью определённый полуавтомат  $L$  находится в отношении **ioco** с полуавтоматом  $K$  (обозначение:  $L \text{ ioco } K$ ), если для любой последовательности  $\sigma$  из *s-traces* $_K$  справедливо **out**( $\llbracket l \rrbracket_\sigma$ )  $\subseteq$  **out**( $\llbracket \hat{k} \rrbracket_\sigma$ ). Полуавтомат  $L$  будем называть *ioco-реализацией* полуавтомата  $K$ .

Суть отношения **ioco** состоит в том, что поведение реализации в любом её состоянии определено на всех тех входных воздействиях, на которых определено поведение спецификации в соответствующем состоянии, а множество выходных реакций содержит в множестве выходных реакций спецификации.

Под *наблюдаемым конечным автоматом* (или просто *автоматом*) с входным алфавитом  $I$  и выходным алфавитом  $O$  будем понимать пятёрку  $F = \langle F, I, O, \hat{f}, \lambda_F \rangle$ , где  $F$  – непустое конечное множество состояний с выделенным начальным состоянием  $\hat{f}$ ;  $I$  и  $O$  – непересекающиеся конечные алфавиты входных и выходных действий (символов) соответственно. Отношение  $\lambda_F \subseteq F \times I \times O \times F$  – есть отношение переходов, причём, если  $\langle f, i, o, f' \rangle \in \lambda_F$  и  $\langle f, i, o, f'' \rangle \in \lambda_F$ , то  $f' = f''$ . Отношение переходов естественным образом распространяется на входные и выходные последовательности, причём если  $\langle f, \alpha, \beta, f' \rangle \in \lambda_F$ , то пара  $\langle \alpha, \beta \rangle$  называется *входо-выходной последовательностью* автомата в состоянии  $f$ , а  $\beta$  называется *выходной реакцией* автомата на *входную последовательность*  $\alpha$  в состоянии  $f$ .

Введём следующие обозначения:

1.  $\llbracket f \rrbracket_\sigma$  – множество всех состояний, достижимых из состояния  $f$  по входо-выходной последовательности  $\sigma$ . В наблюдаемом автомате  $|\llbracket f \rrbracket_\sigma| \leqslant 1$ .
2. **out**( $f, i$ ) – множество всех выходных действий, переходы по которым в паре с

входным действием  $i$  определены в состоянии  $f$ .

3.  $\text{in}(f)$  – множество всех входных символов, переходы по которым определены в состоянии  $f$ .

4.  $\Gamma_F$  – множество всех конечных входо-выходных последовательностей в начальном состоянии автомата  $F$ .

Автомат  $F$  называется *полностью определённым*, если для каждого его состояния  $f$  справедливо  $\text{in}(f) = I$ .

Полностью определённый автомат  $F$  называется *квази-редукцией* автомата  $G$  (обозначение  $F \lesssim G$ ), если для любой входо-выходной последовательности  $\sigma$  из  $\Gamma_G$  и любого входного символа  $i$  из  $\text{in}([\![\hat{g}]\!]_\sigma)$  верно следующее:  $\text{out}([\![\hat{f}]\!]_\sigma, i) \subseteq \text{out}([\![\hat{g}]\!]_\sigma, i)$ .

Смысл отношения квази-редукции подобен смыслу отношения **ioco**: допустимых входных воздействий у реализации должно быть не меньше, чем у спецификации, а множество выходных реакций на каждую допустимую входную последовательность содержится в соответствующем множестве выходных реакций спецификации.

*Наблюдаемый временемой автомат*  $V$  (или просто *временной автомат*) есть шестёрка  $\langle V, I, O, \hat{v}, \lambda_V, \Delta_V \rangle$ , где  $V$  – конечное непустое множество состояний с выделенным начальным состоянием  $\hat{v}$ ,  $I$  и  $O$  непересекающиеся конечные входной и выходной алфавиты соответственно,  $\lambda_V \subseteq V \times I \times O \times V$  – отношение переходов, причём, если  $\langle v, i, o, v' \rangle \in \lambda_V$  и  $\langle v, i, o, v'' \rangle \in \lambda_V$ , то  $v' = v''$ ;  $\Delta_V : V \rightarrow V \times (\mathbb{N} \cup \{\infty\})$ , где  $\mathbb{N}$  – множество натуральных чисел, причём, если  $\Delta_V(v) = \langle v', \infty \rangle$ , то  $v = v'$ . Как обычно, переход  $\langle v, i, o, v' \rangle$  записывается как  $v \xrightarrow{i/o} v'$ , а переход  $\Delta_V(v) = \langle v'', t \rangle$  – как  $v \xrightarrow{t} v''$ , и этот переход будем называть *переходом по временному задержке*  $t$ .

С каждым временным автоматом  $V$  связаны часы (или таймер), отмеряющие количество (временных) тактов, прошедших после выдачи системой последнего выходного символа. Для измерения времени вводится специальная временная переменная. Предполагается, что изменения в системе происходят только по истечении некоторого целого количества тактов от начала работы системы, то есть в начальный момент времени, через один такт, через два такта и так далее. При этом, чтобы избежать неопределённости, входные воздействия разрешается подавать только в эти моменты времени. Если  $v \xrightarrow{i/o} v'$ , то временной автомат  $V$ , находясь в состоянии  $v$ , может принять входное воздействие  $i$  и отреагировать на него выходным действием (сигналом)  $o$ , в тот же момент временной автомат перейдёт в состояние  $v'$  и «сбросит» часы (то есть в состоянии  $v'$  время начнёт отсчитываться с 0). Если  $v \xrightarrow{t'} v''$ , и ни одно из возможных входных воздействий не прикладывается кциальному автомату в течение  $(t' - 1)$  такта после перехода временного автомата в состояние  $v$ , то в момент времени  $t'$  временной автомат перейдёт в состояние  $v''$ , и «сбросит» часы (то есть в состоянии  $v''$  время начнёт отсчитываться с 0). Здесь мы предполагаем, что если функция  $\Delta_V(v) = \langle v, \infty \rangle$ , то система может оставаться в состоянии  $v$  бесконечно долго.

Другими словами, если входное воздействие  $i$  подаётся на временный автомат в состоянии  $v$  в моменты времени  $0, 1, 2, \dots, t' - 1$ , то временной автомат выдаст на выходной сигнал  $o$  и мгновенно изменит своё состояние на состояние  $v'$ . Однако, если воздействие  $i$  на временный автомат в состоянии  $v$  будет подано в момент  $t'$  или позже, то временной автомат примет его, находясь уже не в состоянии  $v$ , а в состоянии  $v''$ , поскольку в момент времени  $t'$  временной автомат, руководствуясь переходом

$v \xrightarrow{t'} v''$ , перейдёт в состояние  $v''$ . При этом временной автомат «сбросит» часы, и воздействие, поданное в момент времени  $t'$ , поступит на временной автомат в состоянии  $v''$  в момент времени 0.

*Временным входным воздействием* назовём пару  $\langle i, t \rangle \in I \times \mathbb{Z}_0^+$ , где  $\mathbb{Z}_0^+$  – множество целых неотрицательных чисел. Пара  $\langle i, t \rangle$  означает, что входное воздействие  $i$  подано на временной автомат в момент времени  $t$ , считая от момента перехода временного автомата в состояние  $v$ .

Чтобы определить выходную реакцию временного автомата в состоянии  $v$  на входное временное воздействие  $\langle i, t \rangle$ , необходимо определить такое состояние  $v'$ , в которое временной автомат попадёт из состояния  $v$  за время  $t$ , используя переходы по временным задержкам. Затем, согласно отношению переходов, найти переход из состояния  $v'$  по входному воздействию  $i$ , то есть переход  $v' \xrightarrow{i/o} v''$ . Выходная реакция  $o$  будет выходной реакцией временного автомата в состоянии  $v$  на временное входное воздействие  $\langle i, t \rangle$ , а состояние  $v''$  – конечным состоянием перехода по временному входному воздействию  $\langle i, t \rangle$ . Понятие переходов по временным входным воздействиям естественным образом распространяется на временные входные и выходные последовательности, причём если  $v \xrightarrow{\sigma} v'$ , где  $\sigma \in (I \times \mathbb{Z}_0^+ \times O)^*$ , то  $\sigma$  называется *временной входо-выходной последовательностью* временного автомата в состоянии  $v$ .

Введём следующие обозначения:

1.  $\llbracket v \rrbracket_\sigma$  – множество всех состояний, достижимых из состояния  $v$  по временной входо-выходной последовательности  $\sigma$ .
2.  $\text{out}(v, i)$  – множество всех выходных символов  $o \in O$ , для каждого из которых существует такое  $v' \in V$ , что  $\langle v, i, o, v' \rangle \in \lambda_V$ .
3.  $\text{out}(v, \langle i, t \rangle)$  – множество всех выходных реакций временного автомата на временное входное воздействие  $\langle i, t \rangle$  в состоянии  $v$ .
4.  $\text{in}(v)$  – множество всех входных действий, переходы по которым определены в состоянии  $v$ .
5.  $\text{in}_\chi(v)$  – множество всех временных входных действий, переходы по которым определены в состоянии  $v$ .
6.  $\Gamma_V$  – множество всех конечных временных входо-выходных полследовательностей временного автомата  $V$  в начальном состоянии.

Временной автомат  $V$  называется *полностью определённым*, если для каждого его состояния  $v$  справедливо  $\text{in}_\chi(v) = I$ .

В разделе 1.5 первой главы даётся краткий обзор состояния дел в области синтеза тестов с гарантированной полнотой на основе конечных автоматов, входо-выходных полуавтоматов и временных автоматов. Отмечается, что существуют методы синтеза таких безусловных тестов для недетерминированных конечных и временных автоматов, но только при выполнении требования о «всех погодных условиях». Известные методы синтеза тестов с гарантированной полнотой для входо-выходных полуавтоматов доставляют бесконечные тесты.

**Вторая глава** посвящена различающим условным экспериментам с конечными автоматами.

Два автомата  $F$  и  $G$  назовём *r-совместимыми* (*r-различимыми*), если для них существует (не существует) общая полностью определённая квази-редукция.

*Пересечением* двух автоматов  $F$  и  $G$  называется автомат  $H = F \cap G = \langle H, I, O, \hat{h}, \lambda_H \rangle$ , где  $\hat{h} = \langle \hat{f}, \hat{g} \rangle$ ,  $H \subseteq F \times G$  – минимальное множество, полученное

с использованием следующего правила для  $\lambda_H$ : если  $\langle f, i, o, f' \rangle \in \lambda_F$  и  $\langle g, i, o, g' \rangle \in \lambda_G$ , то  $\langle \langle f, g \rangle, i, o, \langle f', g' \rangle \rangle \in \lambda_H$ .

Мы вводим понятие  $r$ -различающего автомата, который будет представлять условный эксперимент по распознаванию двух  $r$ -различимых автоматов. Под  $r$ -различающим автоматом понимается автомат  $R = \langle R, I, O, \hat{r}, \lambda_R \rangle$ , для которого справедливы следующие условия:

1.  $R \supseteq \{\perp_F, \perp_G, \perp\}$ .
2. Граф переходов автомата  $R$  – ациклический.
3. Для всякого  $r \in R \setminus \{\perp_F, \perp_G, \perp\}$  выполняется  $|\text{in}(r)| = 1$  и  $\text{out}(r, i) = O$ , где  $\text{in}(r) = \{i\}$ .
4. Состояния  $\perp_F$ ,  $\perp_G$  и  $\perp$  – тупиковые.

Говорят, что  $r$ -различающий автомат  $R$  *различает* автоматы  $F$  и  $G$ , если в пересечении  $H_{FR} = F \cap R$  для всех тупиковых состояний  $\langle f, r \rangle$ , верно  $r = \perp_F$ , в то время как в пересечении  $H_{GR} = G \cap R$  для всех тупиковых состояний  $\langle g, r \rangle$ , верно  $r = \perp_G$ .

Пусть для распознавания предъявлены автоматы  $F$  и  $G$ , для которых существует  $r$ -различающий автомат  $R_{FG}$ . Условный эксперимент с использованием автомата  $R_{FG}$  строится следующим образом. В начальный момент времени автомат  $R_{FG}$  находится в начальном состоянии  $\hat{r}$ .

Пусть автомат  $R_{FG}$  перешёл в состояние  $r$ , в котором определён переход по входному символу  $i \in I$ . В этом случае на предъявленный для распознавания автомат подаётся входной символ  $i$ . Предъявленный автомат реагирует на входной символ некоторым выходным символом  $o \in O$ , на основании которого вычисляются следующее состояние  $r$ -различающего автомата  $R_{FG}$  и следующий входной символ.

Эксперимент заканчивается, как только  $r$ -различающий автомат переходит в одно из специальных состояний  $\perp_F$ ,  $\perp_G$  или  $\perp$ . Если  $r$ -различающий автомат  $R_{FG}$  достиг состояния  $\perp_F$ , то предъявленный автомат распознаётся как автомат  $F$ ; если  $r$ -различающий автомат  $R_{FG}$  достиг состояния  $\perp_G$ , то предъявленный автомат распознаётся как автомат  $G$ . Если автомат  $R_{FG}$  достиг состояния  $\perp$ , то предъявленный автомат не является ни автоматом  $F$ , ни автоматом  $G$ . Поскольку граф переходов автомата  $R_{FG}$  ациклический, то условный эксперимент на основе  $r$ -различающего автомата является конечным.

**Теорема 1.** *Два автомата  $r$ -различимы тогда и только тогда, когда для них существует  $r$ -различающий автомат.*

Таким образом, два автомата различимы условным экспериментом, если и только если эти автоматы являются  $r$ -различимыми. Алгоритм 1 позволяет строить  $r$ -различающий автомат для заданных автоматов на основе понятий пересечения автоматов и недоопределённых состояний.

Пусть  $F$  и  $G$  – автоматы и  $H = F \cap G$ . Состояние  $\langle f, g \rangle \in H$  называется *1-недоопределённым*, если существует входное воздействие  $i \in \text{in}_F(f) \cap \text{in}_G(g)$  такое, что  $i \notin \text{in}_H(\langle f, g \rangle)$ . Состояние  $\langle f, g \rangle$  пересечения  $H$  называется *z-недоопределённым*,  $z > 1$ , если оно  $(z - 1)$ -недоопределённое или существует входное воздействие  $i \in \text{in}_F(f) \cap \text{in}_G(g)$  такое, что все состояния пересечения  $H$ , достижимые из  $\langle f, g \rangle$  по входному символу  $i$ , являются  $(z - 1)$ -недоопределёнными.

Построенный алгоритмом 1  $r$ -различающий автомат можно использовать в качестве тестового примера при построении проверяющих тестов с гарантированной полнотой для недетерминированных автоматов.

---

**Алгоритм 1** Построение  $r$ -различающего автомата
 

---

- Вход:** Два наблюдаемых автомата  $F = \langle F, I, O, \hat{f}, \lambda_F \rangle$  и  $G = \langle G, I, O, \hat{g}, \lambda_G \rangle$ .
- Выход:**  $R$ -различающий автомат  $R_{FG}$ , если  $F$  и  $G$  –  $r$ -различимы.
- 1:  $H_0 := \{\perp, \perp_F, \perp_G\}; \lambda_R := \emptyset; H := F \cap G;$
  - 2: Строим  $Q_1$  – множество 1-недоопределённых состояний,  $Q_2$  – 2-недоопределённых состояний и так далее пока  $Q_j \neq Q_{j+1}$ .
  - 3: Если  $\forall j \langle \hat{f}, \hat{g} \rangle \notin Q_j$ , то
  - 4: Исходные автоматы не  $r$ -различимы; Конец.
  - 5: Пусть  $n$  – такое число, что  $\langle \hat{f}, \hat{g} \rangle \in Q_n$ , но  $\langle \hat{f}, \hat{g} \rangle \notin Q_{n-1}$ ;
  - 6:  $z := n; H_n := \{\langle \hat{f}, \hat{g} \rangle\}; H_{n-1} := \emptyset; H_{n-2} := \emptyset; \dots; H_1 := \emptyset;$
  - 7: Пока ( $z > 0$ )
  - 8: Для каждого  $(h \equiv \langle f, g \rangle \in H_z)$
  - 9: Выберем такое произвольное  $i \in \text{in}_F(f) \cap \text{in}_G(g)$ , что для всех  $o \in O$  выполняется  $[h]_{i/o} \subseteq Q_{z-1}$ ;
  - 10: Для каждого  $o \in O \setminus (\text{out}_F(f, i) \cup \text{out}_G(g, i))$  добавим в множество  $\lambda_R$  переходы  $\langle h, i, o, \perp \rangle$ ;
  - 11: Для каждого  $o \in \text{out}_F(f, i) \setminus \text{out}_G(g, i)$  добавим в множество  $\lambda_R$  переходы  $\langle h, i, o, \perp_F \rangle$ ;
  - 12: Для каждого  $o \in \text{out}_G(g, i) \setminus \text{out}_F(f, i)$  добавим в множество  $\lambda_R$  переходы  $\langle h, i, o, \perp_G \rangle$ ;
  - 13: Для каждого перехода  $\langle h, i, o, h' \rangle$  из  $\lambda_H$  добавим в множество  $\lambda_R$  переход  $\langle h, i, o, h' \rangle$ , а в множество  $H_{z'}$  состояние  $h'$ , где  $z' < z$  – такое число, что  $h' \in Q_{z'-1}$ , но  $h' \notin Q_{z'-1}$ ;
  - 14:  $z := z - 1$ ;
  - 15:  $R := \bigcup_{z=0}^n H_z$ ;
  - 16: Автомат  $\langle R, I, O, \hat{r}, \lambda_R \rangle$  – искомый автомат; Конец.
- 

Под (автоматной) моделью неисправности будем понимать тройку  $\langle F, \precsim, \mathfrak{E} \rangle$ , где  $F$  – автомат-спецификация, описывающий требуемое поведение тестируемой системы,  $\precsim$  – отношение квази-редукции, определяющее соответствие тестируемой системы спецификации,  $\mathfrak{E}$  – множество полностью определённых автоматов, описывающих поведение всех возможных реализаций системы с неисправностями из заданного класса.

Тестовым примером называется наблюдаемый автомат  $P = \langle P, I, O, \hat{p}, \lambda_P \rangle$  со следующими свойствами:

1.  $P \supseteq \{\top, \perp\}$ . Состояние  $\top$  соответствует вердикту «Тест пройден успешно», а  $\perp$  – «Обнаружена неисправность».
2. Граф переходов автомата  $P$  ациклический.
3. Для всякого  $p \in P \setminus \{\top, \perp\}$  выполняется  $|\text{in}(p)| = 1$  и  $\text{out}(p, i) = O$ , где  $\text{in}(p) = \{i\}$ .
4. Состояния  $\top$  и  $\perp$  тупиковые.

Будем говорить, что тестовый пример  $P$  не согласуется с полностью определённым автомром  $G$ , если в пересечении  $G \cap P$  для всех тупиковых состояний  $\langle g, p \rangle$  верно  $p = \perp$ . Тестовый пример  $P$  абсолютно согласуется с полностью определённым автомром  $G$ , если в пересечении  $G \cap P$  для всех тупиковых состояний  $\langle g, p \rangle$  верно  $p = \top$ .

Проверяющим тестом относительно модели  $\langle F, \precsim, \mathfrak{E} \rangle$  называется конечное множество  $T$  тестовых примеров, входной и выходной алфавиты которых совпадают с входным и выходным алфавитом автомата-спецификации.

Проверяющий тест  $T$  называется исчерпывающим относительно модели  $\langle F, \precsim, \mathfrak{E} \rangle$ , если для любого автомата  $G \in \mathfrak{E}$ , не являющегося квази-редукцией  $F$ , множество  $T$  содержит тестовый пример, который не согласуется с автомром  $G$ .

Проверяющий тест  $T$  называется непротиворечивым относительно модели  $\langle F, \precsim, \mathfrak{E} \rangle$ , если любой автомат  $G \in \mathfrak{E}$ , являющийся квази-редукцией автомата-спецификации  $F$ , абсолютно согласуется с каждым тестовым примером множества  $T$ .

Проверяющий тест  $T$  называется *полным* относительно модели  $\langle F, \lesssim, \mathfrak{E} \rangle$ , если тест является исчерпывающим и непротиворечивым.

Пусть задана модель неисправности  $\langle F, \lesssim, \mathfrak{E} \rangle$ , в которой множество  $\mathfrak{E}$  конечно, состоит из полностью определённых автоматов, и каждый автомат из множества  $\mathfrak{E}$  является либо квази-редукцией автомата  $F$ , либо  $r$ -различим с  $F$ . Тогда полный проверяющий тест для этой модели неисправности можно построить следующим образом.

Выбираем очередной автомат  $G$  из множества неисправностей  $\mathfrak{E}$  и применяем к автоматам  $F$  и  $G$  алгоритм 1. Если вердикт этого алгоритма «Автоматы  $F$  и  $G$   $r$ -совместимы», то переходим к следующему автомatu из  $\mathfrak{E}$ . Если автоматы  $F$  и  $G$   $r$ -различимы, то алгоритм построит автомат  $R$ ,  $r$ -различающий автоматы  $F$  и  $G$ . Отождествив состояние  $\perp_G$  с состоянием  $\perp$  и переобозначив состояние  $\perp_F$  как состояние  $\top$ , получим тестовый пример  $P$  для обнаружения автомата  $G$ , который заносим в тест. Затем переходим к следующему автомату из  $\mathfrak{E}$  и так далее.

Однако, в некоторых случаях в область неисправности попадают также автоматы  $r$ -совместимые со спецификацией. Такой, например, является область неисправности, состоящая из всех полностью определённых наблюдаемых подавтоматов заданного автомата  $M$ , называемого мутационным. В этом случае возможно сокращение перебора всех подавтоматов автомата  $M$ , поскольку если некоторый полностью определённый автомат  $r$ -совместим со спецификацией, то и любой другой автомат, содержащий данный в качестве подавтомата будет  $r$ -совместимым со спецификацией, поэтому его уже можно не проверять на  $r$ -различимость со спецификацией. Эти соображения легли в основу алгоритма, описывающего в диссертации процедуру синтеза непротиворечивого теста по мутационному автоматау. В этом алгоритме предлагается описывать наблюдаемые полностью определённые подавтоматы заданного мутационного автомата при помощи булевых векторов, называемых сигнатурами. Каждой компоненте сигнатуры соответствует некоторый переход в мутационном автоматае и в  $k$ -ой позиции ставится единица, если  $k$ -й переход принадлежит данному автоматау. Очевидно, что если автомат  $A$  является подавтоматом автомата  $B$ , то сигнтура автомата  $A$  предшествует сигнтуре  $B$ . Начинать перечислять автоматы предлагается с детерминированных автоматаов, и если некоторый автомат оказывается  $r$ -совместимым со спецификацией, то его сигнтура попадает в список запрещённых.

В качестве ещё одного применения условного эксперимента на основе  $r$ -различающего автомата, в диссертации рассматривается синтез диагностических тестов в случае, когда известно, как описать поведение системы для каждой заданной неисправности системы. Чтобы оценить диагностические возможности такого условного эксперимента, проводились компьютерные эксперименты по локализации неисправности в двухкомпонентной автоматаой сети. Эксперименты показали, что если число неисправных переходов не превышает 20% от общего числа переходов в компоненте сети, то с использованием различающего автомата неисправную компоненту можно идентифицировать примерно в 70% случаев.

В третьей главе исследуются условные различающие эксперименты с полуавтоматами.

Два полуавтомата  $L$  и  $K$  назовём *ioco-совместимыми* (*ioco-различимыми*), если для них существует (не существует) общая полностью определённая *ioco*-реализация.

Пересечением полуавтоматов  $L$  и  $K$  назовём полуавтомат  $J = L \cap K = \langle J, I, O \cup \{\Delta\}, \hat{j}, \lambda_J \rangle$ , где  $\Delta \notin I \cup O \cup \{\delta\}$ ,  $\hat{j} = \langle \hat{l}, \hat{k} \rangle$ ,  $J \subseteq L \times K$  – минимальное множество, полученное с использованием следующих правил для  $\lambda_J$ : если  $\langle l, a, l' \rangle \in \lambda_L$  и  $\langle k, a, k' \rangle \in$

$\lambda_K$ , то  $\langle \langle l, k \rangle, a, \langle l', k' \rangle \rangle \in \lambda_J$ ; если  $l$  – молчащее и  $k$  – молчащее, то  $\langle l, k \rangle \xrightarrow{\Delta} \langle l, k \rangle \in \lambda_J$ .

Введём понятие **ioco**-различающего полуавтомата. Под **ioco**-различающим полуавтоматом будем понимать такой полуавтомат  $R = \langle R, I, O \cup \{\theta\}, \hat{r}, \lambda_R \rangle$ , где  $\theta \notin I \cup O \cup \{\delta\}$ , для которого справедливы следующие условия:

1.  $R \supseteq \{\perp_L, \perp_K, \perp\}$ .
2. Граф переходов полуавтомата  $R$  ациклический.
3. Для всякого  $r \in R \setminus \{\perp, \perp_L, \perp_K\}$  либо  $\text{in}(r) = \{i\}$ ,  $\text{out}(r) = \{\delta\}$  и  $\llbracket r \rrbracket_i \cap \{\perp_L, \perp_K, \perp\} = \emptyset$ , либо  $\text{in}(r) = \emptyset$  и  $\text{out}(r) = O \cup \{\theta\}$ .
4. Состояния  $\perp_L, \perp_K$  и  $\perp$  – тупиковые.

Пересечением полуавтомата  $L$  и **ioco**-различающего полуавтомата  $R$  назовём связанный полуавтомат  $J = L \cap_\theta R = \langle J, I, O \cup \{\theta\}, \hat{j}, \lambda_J \rangle$ , где  $\hat{j} = \langle \hat{l}, \hat{r} \rangle$ ,  $J \subseteq L \times R$  – минимальное множество, полученное с использованием следующих правил для  $\lambda_J$ : если  $\langle l, a, l' \rangle \in \lambda_L$  и  $\langle r, a, r' \rangle \in \lambda_R$ , то  $\langle \langle l, r \rangle, a, \langle l', r' \rangle \rangle \in \lambda_J$ ; если  $l$  – молчащее и  $\langle r, \theta, r' \rangle \in \lambda_R$ , то  $\langle l, r \rangle \xrightarrow{\theta} \langle l, r' \rangle \in \lambda_J$ .

Говорят, что **ioco**-различающий полуавтомат  $R$  различает полуавтоматы  $L$  и  $K$ , если в пересечении  $J_{LR} = L \cap_\theta R$  для всех тупиковых состояний  $\langle l, r \rangle$  верно  $r = \perp_L$ , в то время как в пересечении  $J_{KR} = K \cap_\theta R$  для всех тупиковых состояний  $\langle k, r \rangle$  верно  $r = \perp_K$ .

Условный эксперимент по распознаванию двух полуавтоматов  $L$  и  $K$ , для которых существует **ioco**-различающий полуавтомат  $R_{LK}$ , строится следующим образом. В начальный момент полуавтомат  $R_{LK}$  находится в начальном состоянии  $\hat{r}$ .

Пусть полуавтомат  $R_{LK}$  перешёл в состояние  $r$  и пусть в состоянии  $r$  определён переход по некоторому входному символу  $i$ . В этом случае на предъявленный для распознавания полуавтомат подаётся входное воздействие  $i$  и вычисляется новое состояние  $r'$  полуавтомата  $R_{LK}$  как  $\llbracket r \rrbracket_i$ .

Если  $\text{in}(r) = \emptyset$ , то ожидается выходная реакция от исследуемого полуавтомата. Если полуавтомат реагирует выходным символом  $o \in O$ , то следующее состояние  $r'$  полуавтомата  $R_{LK}$  есть  $\llbracket r \rrbracket_o$ . Если реакцией исследуемого полуавтомата является молчание, то следующее состояние полуавтомата  $R_{LK}$  есть  $\llbracket r \rrbracket_\theta$ .

Эксперимент заканчивается, как только **ioco**-различающий полуавтомат переходит в одно из специальных состояний  $\perp_L, \perp_K$  или  $\perp$ . Если полуавтомат  $R_{LK}$  достигает состояния  $\perp_L$ , то предъявленный полуавтомат распознаётся как полуавтомат  $L$ ; если полуавтомат  $R_{LK}$  достигает состояния  $\perp_K$ , то предъявленный полуавтомат распознаётся как полуавтомат  $K$ . Если полуавтомат  $R_{LK}$  достигает состояния  $\perp$ , то предъявленный полуавтомат не является ни полуавтоматом  $L$ , ни полуавтоматом  $K$ .

Поскольку граф переходов полуавтомата  $R_{FG}$  ациклический, то условный эксперимент **ioco**-различающего полуавтомата является конечным.

Пусть  $L$  и  $K$  два заданных полуавтомата и  $J = L \cap K$ . Состояние  $\langle l, k \rangle \in J$  называется *1-недоопределённым*, если оно молчащее. Состояние  $\langle l, k \rangle \in J$  пересечения  $J$  называется *z-недоопределённым*, если это состояние является  $(z-1)$ -недоопределённым, или существует такое входное воздействие  $i \in \text{in}_J(\langle l, k \rangle)$ , что все состояния в множестве  $\llbracket \langle l, k \rangle \rrbracket_i$  являются  $(z-1)$ -недоопределёнными, либо если для всех  $o \in \text{out}(\langle l, k \rangle)$  все состояния в  $\llbracket \langle l, k \rangle \rrbracket_o$  являются  $(z-1)$ -недоопределёнными.

**Теорема 2.** Два полуавтомата **ioco**-различимы тогда и только тогда, когда для них существует **ioco**-различающий полуавтомат.

---

**Алгоритм 2** Получение **ioco**-различающего полуавтомата
 

---

**Вход:** Два детерминированных полуавтомата  $L = \langle L, I, O, \hat{l}, \lambda_L \rangle$  и  $K = \langle K, I, O, \hat{k}, \lambda_K \rangle$ .

**Выход:** **ioco**-различающий полуавтомат  $R_{LK}$ , если  $L$  и  $K$  – **ioco**-различимы.

- 1:  $J_0 := \{\perp, \perp_L, \perp_K\}; \lambda_R := \emptyset; J := L \cap K;$
  - 2: Строим  $Q_1$  – множество 1-недоопределённых состояний,  $Q_2$  – 2-недоопределённых состояний и так далее пока  $Q_z \neq Q_{z+1}$ .
  - 3: **Если**  $\forall z \langle \hat{l}, \hat{k} \rangle \notin Q_z$ , **то**
  - 4:   Исходные полуавтоматы **ioco**-совместимы; **Конец**.
  - 5: Пусть  $n$  – такое число, что  $\langle \hat{l}, \hat{k} \rangle \in Q_n$ , но  $\langle \hat{l}, \hat{k} \rangle \notin Q_{n-1}$ ;
  - 6:  $z := n; J_n := \{\langle \hat{l}, \hat{k} \rangle\}; J_{n-1} := \emptyset; J_{n-2} := \emptyset; \dots; J_1 := \emptyset;$
  - 7: **Пока** ( $z > 0$ )
  - 8:   Для каждого  $(j \equiv \langle l, k \rangle) \in J_z$
  - 9:     Если  $\text{out}_J(j) = \delta$  или  $\llbracket j \rrbracket \text{out}_J(j) \subseteq Q_{z-1}$ , то
  - 10:       Для каждого  $o \in (O \cup \{\delta\}) \setminus (\text{out}_L(l) \cup \text{out}_K(k))$  добавим в множество  $\lambda_R$  переходы  $\langle j, o, \perp \rangle$  когда  $o \neq \delta$  и переход  $\langle j, \theta, \perp \rangle$  когда  $o = \delta$ ;
  - 11:       Для каждого  $o \in \text{out}_L(l) \setminus \text{out}_K(k)$  добавим в множество  $\lambda_R$  переходы  $\langle j, o, \perp_L \rangle$  когда  $o \neq \delta$  и переход  $\langle j, \theta, \perp_L \rangle$  когда  $o = \delta$ ;
  - 12:       Для каждого  $o \in \text{out}_K(k) \setminus \text{out}_L(l)$  добавим в множество  $\lambda_R$  переходы  $\langle j, o, \perp_K \rangle$  когда  $o \neq \delta$  и переход  $\langle j, \theta, \perp_K \rangle$  когда  $o = \delta$ ;
  - 13:       Для каждого перехода  $\langle j, o, j' \rangle$  из  $\lambda_J$  добавим в множество  $\lambda_R$  переход  $\langle j, o, j' \rangle$ , а в множество  $J_{z'}$  состояние  $j'$ , где  $z' < z$  – такое число, что  $j' \in Q_{z'}$  и  $j' \notin Q_{z'-1}$ ;
  - 14:     иначе
  - 15:       Выберем такое произвольное  $i \in \text{in}_L(l) \cap \text{in}_K(k)$ , что  $\llbracket \langle l, k \rangle \rrbracket_i \subseteq Q_{z-1}$ ;
  - 16:       Добавим в множество  $\lambda_R$  переход  $\langle j, i, j' \rangle$  из  $\lambda_J$ , а в множество  $J_{z'}$  состояние  $j'$ , где  $z' < z$  – такое число, что  $j' \in Q_{z'}$  и  $j' \notin Q_{z'-1}$
  - 17:      $z := z - 1$ ;
  - 18:      $R := \bigcup_{z=0}^n J_z$ ;
  - 19: Автомат  $R = \langle R, I, O \cup \{\theta\}, \hat{r}, \lambda_R \rangle$  – искомый автомат; **Конец**.
- 

Таким образом, два полуавтомата различимы условным экспериментом, если и только если эти полуавтоматы являются **ioco**-различимыми. Мы предлагаем способ построения **ioco**-различающего полуавтомата (алгоритм 2).

Построенный алгоритмом 2 **ioco**-различающий полуавтомат можно использовать в качестве тестового примера при построении проверяющих тестов с гарантированной полнотой для входо-выходных полуавтоматов.

Под *полуавтоматной моделью неисправности* будем понимать тройку  $\langle L, \text{ioco}, \mathfrak{E} \rangle$ , где  $L$  – полуавтомат-спецификация, описывающая требуемое поведение некоторой системы, **ioco** – отношение **ioco**, выступающее в качестве отношения соответствия спецификации,  $\mathfrak{E}$  – множество полностью определённых полуавтоматов, описзывающих все возможные реализации системы.

Если  $K$  есть полуавтомат-реализация, **ioco**-различимый со спецификацией  $L$ , то тестовый пример получается из **ioco**-различающего автомата  $R_{LK}$  заменой состояния  $\perp_L$  на  $\top$ , и отождествлением состояния  $\perp_K$  с состоянием  $\perp$ . Состоянию  $\top$  соответствует вердикт «Тест пройден успешно», а  $\perp$  – «Обнаружена неисправность».

Будем говорить, что тестовый пример  $P$  не согласуется с полностью определённым полуавтоматом  $K$ , если в пересечении  $K \cap_\theta P$  для всех тупиковых состояний  $\langle k, p \rangle$ , верно  $p = \perp$ . Тестовый пример  $P$  абсолютно согласуется с полностью определённым полуавтоматом  $K$ , если в пересечении соответствия  $K \cap_\theta P$  для всех тупиковых состояний  $\langle k, p \rangle$ , верно  $p = \top$ .

*Проверяющим тестом* относительно модели  $\langle L, \text{ioco}, \mathfrak{E} \rangle$  называется конечное множество  $T$  тестовых примеров, входной и выходной алфавиты которых совпадают с входным и выходным алфавитами полуавтомата-спецификации  $L$ . Понятия исчерпывающего, непротиворечивого и полного теста относительно модели неисправности

$\langle L, \text{ioco}, \mathfrak{E} \rangle$  определяются так же как и для автоматной модели неисправности.

Пусть  $\langle L, \text{ioco}, \mathfrak{E} \rangle$  – модель неисправности, в которой конечное множество  $\mathfrak{E}$ , состоит из полностью определённых полуавтоматов, и каждый полуавтомат из множества является либо **ioco**-реализацией спецификации  $L$ , либо **ioco**-различим с ней. Тогда полный проверяющий тест для этой модели неисправности можно построить перебором полуавтоматов из области неисправности. Для каждого выбранного полуавтомата, **ioco**-различимого со спецификацией, строится тестовый пример на основе алгоритма 2, который включается в проверяющий тест.

Две рассмотренные модели – конечный автомат и входо-выходной полуавтомат – очень близки между собой, а отношения квази-редукции и **ioco** имеют одинаковую семантику. Поэтому возникает вопрос, нельзя ли свести задачу синтеза проверяющего теста с гарантированной полнотой относительно полуавтоматной модели неисправности к задаче синтеза таких тестов для автоматной модели неисправности. Напомним, что для ряда автоматных моделей неисправности существуют методы синтеза конечных полных проверяющих тестов.

С этой целью вводится следующее преобразование полуавтомата  $L$  к автоматау  $F_\varepsilon^L$ :  $F = L$  и если  $\langle l, a, l' \rangle$  и  $a \in I$ , то  $\langle l, a, \varepsilon_o, l' \rangle \in \lambda_F$ ; если  $\langle l, a, l' \rangle$  и  $a \in O$ , то  $\langle l, \varepsilon_i, a, l' \rangle \in \lambda_F$ ; если  $l$  – молчашее состояние, то  $\langle l, \varepsilon_i, \delta, l' \rangle \in \lambda_F$ .

**Теорема 3.**  $L \text{ ioco } K$  тогда и только тогда, когда  $F_\varepsilon^L \precsim F_\varepsilon^K$ .

Таким образом, благодаря теореме 3, становится возможным переходить от полуавтоматной модели неисправности  $\langle L, \text{ioco}, \{L_1, L_2, \dots\} \rangle$  к автоматной модели неисправности  $\langle F_\varepsilon^L, \precsim, \{F_\varepsilon^{L_1}, F_\varepsilon^{L_2}, \dots\} \rangle$ . Пусть  $P$  – автоматный тестовый пример для модели неисправности  $\langle F_\varepsilon^L, \precsim, \{F_\varepsilon^{L_1}, F_\varepsilon^{L_2}, \dots\} \rangle$ . Переход от него к полуавтоматному тестовому примеру  $P_L$  можно осуществить по следующим правилам: если  $\text{in}(p) = i \in I$  и  $\langle p, i, \varepsilon_o, p' \rangle \in \lambda_P$ , то  $\langle p, i, p' \rangle \in \lambda_{P_L}$ ; если  $\text{in}(p) = \varepsilon_i$  и  $\langle p, \varepsilon_i, o, p' \rangle \in \lambda_P$ , и  $o \neq \varepsilon_o$ , то  $\langle p, o, p' \rangle \in \lambda_{P_L}$ .

**Теорема 4.** Пусть задана полуавтоматная модель неисправности  $\langle L, \text{ioco}, \{L_1, L_2, \dots\} \rangle$ , по которой построена автоматная модель неисправности  $\langle F_\varepsilon^L, \precsim, \{F_\varepsilon^{L_1}, F_\varepsilon^{L_2}, \dots\} \rangle$ . Тогда, если  $T = \{P^1, P^2, \dots\}$  – полный проверяющий тест относительно модели неисправности  $\langle F_\varepsilon^L, \precsim, \{F_\varepsilon^{L_1}, F_\varepsilon^{L_2}, \dots\} \rangle$ , то  $T_L = \{P_L^1, P_L^2, \dots\}$  – полный проверяющий тест для модели неисправности  $\langle L, \text{ioco}, \{L_1, L_2, \dots\} \rangle$ .

В четвёртой главе исследуется условный различающий эксперимент для временных конечных автоматов.

Полностью определённый временной автомат  $U$  называется *квази-редукцией* в временного автомата  $V$  (обозначение  $U \precsim V$ ), если для любой временной входной-выходной последовательности  $\sigma$  из  $\Gamma_V$  и всякого временного входного воздействия  $\langle i, t \rangle$  из  $\text{in}_X(\llbracket \hat{v} \rrbracket_\sigma)$  верно следующее:  $\text{out}(\llbracket \hat{u} \rrbracket_\sigma, \langle i, t \rangle) \subseteq \text{out}(\llbracket \hat{v} \rrbracket_\sigma, \langle i, t \rangle)$ .

Два временных автомата называются *r-совместимыми* (*r-различимыми*) если для них существует (не существует) общая полностью определённая квази-редукция.

Для построения условного эксперимента, различающего два временных автомата мы вводим понятие пересечения этих автоматаов. *Пересечением* временных автоматаов  $U$  и  $V$  назовём временной автомат  $W = \langle W, I, O, \hat{w}, \lambda_W, \Delta_W \rangle$ , где  $\hat{w} \equiv \langle \hat{u}, 0, \hat{v}, 0 \rangle$ ,  $K = \{0, 1, \dots, k\}$ ,  $k = \min(\max(\Delta_U \downarrow_{z_0^+}), \max(\Delta_V \downarrow_{z_0^+}))$ , и  $W \subseteq U \times K \times V \times K$  – минимальное множество, полученное согласно следующим правилам для отношения  $\lambda_W$  и функции  $\Delta_W$ :

1. Если  $k_1 < d_u$  и  $k_2 < d_v$ , и  $\langle u, i, o, u' \rangle \in \lambda_U$ , и  $\langle v, i, o, v' \rangle \in \lambda_V$ , то  $\langle \langle u, k_1, v, k_2 \rangle, i, o, \langle u', 0, v', 0 \rangle \rangle \in \lambda$ , где  $\Delta_U(u) = \langle s_u, d_u \rangle$ ,  $\Delta_V(v) = \langle s_v, d_v \rangle$ .

2.  $\Delta(\langle u, k_1, v, k_2 \rangle) = \langle \langle u', k'_1, v', k'_2 \rangle, k \rangle$ , где  $\Delta_U(u) = \langle s_u, d_u \rangle$ ,  $\Delta_V(v) = \langle s_v, d_v \rangle$ ,  $k = \min(d_u - k_1, d_v - k_2)$  и если  $d_u = \infty$  или  $d_v = \infty$ , или  $d_u - k_1 = d_v - k_2$ , то  $\langle u', k'_1, v', k'_2 \rangle = \langle s_u, 0, s_v, 0 \rangle$ ; если  $(d_u - k_1) \in \mathbb{Z}_0^+$  и  $(d_v - k_2) \in \mathbb{Z}_0^+$ , и  $(d_u - k_1) < (d_v - k_2)$ , то  $\langle u', k'_1, v', k'_2 \rangle = \langle s_u, 0, v, k_2 + k \rangle$ ; если  $(d_u - k_1) \in \mathbb{Z}_0^+$  и  $(d_v - k_2) \in \mathbb{Z}_0^+$ , и  $(d_u - k_1) > (d_v - k_2)$ , то  $\langle u', k'_1, v', k'_2 \rangle = \langle u, k_1 + k, s_v, 0 \rangle$ .

Под  $r$ -различающим временным автоматом понимается временной автомат  $R = \langle R, I, O, \hat{r}, \lambda_R, \Delta_R \rangle$ , для которого справедливы следующие условия:

$$1. R \supseteq \{\perp_U, \perp_V, \perp\}.$$

2. Граф переходов автомата  $R$  ациклический, не считая петель  $\perp \xrightarrow{\infty} \perp$ ,  $\perp_U \xrightarrow{\infty} \perp_U$  и  $\perp_V \xrightarrow{\infty} \perp_V$ .

3. Для всякого  $r \in R \setminus \{\perp_U, \perp_V, \perp\}$  выполняется либо  $|\text{in}(r)| = 1$  и  $\text{out}(r, i) = O$ , где  $\text{in}(r) = \{i\}$ , и в этом случае  $\Delta_R(r) = \langle \perp, t \rangle$ ,  $t \in \mathbb{N}$ ; либо  $\text{in}(r) = \emptyset$  и в этом случае  $\Delta_R(r) = \langle r', t \rangle$ ,  $t \in \mathbb{N}$ ,  $r' \notin \{\perp, \perp_U, \perp_V\}$ .

4. Из состояний  $\perp_U$ ,  $\perp_V$  и  $\perp$  не определено ни одного перехода по входо-выходным парам и  $\Delta_R(\perp) = \langle \perp, \infty \rangle$ ,  $\Delta_R(\perp_U) = \langle \perp_U, \infty \rangle$ ,  $\Delta_R(\perp_V) = \langle \perp_V, \infty \rangle$ .

Говорят, что  $r$ -различающий временной автомат  $R$  различает временные автоматы  $U$  и  $V$ , если в подмножестве  $\{\langle u, k_u, r, k_r \rangle \in W_{UR} \mid \text{in}(\langle u, k_u, r, k_r \rangle) = \emptyset\}$  множества состояний пересечения  $W_{UR} = U \cap R$  найдутся состояния, для которых  $r = \perp_U$  и для всех состояний подмножества  $r \neq \perp_V$ , все переходы, ведущие в состояния вида  $\langle u, k_u, \perp, k_\perp \rangle$ , помечены только временными задержками, и если  $(\Delta_W(\langle u, k_u, r, k_r \rangle)) \downarrow W = \langle u', k'_u, \perp, k'_\perp \rangle$ , то  $r = \perp$ ; в то время как в подмножестве  $\{\langle v, k_v, r, k_r \rangle \in W_{VR} \mid \text{in}(\langle v, k_v, r, k_r \rangle) = \emptyset\}$  множества состояний пересечения  $W_{VR} = V \cap R$  найдутся состояния, для которых  $r = \perp_V$  и для всех состояний подмножества  $r \neq \perp_U$ , все переходы, ведущие в состояния вида  $\langle v, k_v, \perp, k_\perp \rangle$ , помечены только временными задержками, и если  $(\Delta_W(\langle v, k_v, r, k_r \rangle)) \downarrow W = \langle v', k'_v, \perp, k'_\perp \rangle$ , то  $r = \perp$ .

Пусть для распознавания представлены временные автоматы  $U$  и  $V$ , для которых существует  $r$ -различающий временной автомат  $R_{UV}$ . Условный эксперимент с использованием автомата  $R_{UV}$  строится следующим образом. В начальный момент значение переменной  $t$  равно 0, а  $R_{UV}$  находится в начальном состоянии  $\hat{r}$ .

Пусть  $t = D$  и временной автомат  $R_{UV}$  перешёл в состояние  $r$ , в котором определён переход по входному символу  $i \in I$ . В этом случае на предъявленный для распознавания временной автомат подаётся входной символ  $i$  в момент времени  $t'$ ,  $D \leq t' < D + d_r$ , где  $d_r$  – значение временной задержки в состоянии  $r$  (время отсчитывается от момента получения последней выходной реакции предъявленного для эксперимента временного автомата). Предъявленный временной автомат реагирует на входной символ некоторым выходным символом  $o$ , на основании которого вычисляется следующее состояние  $r$ -различающего временного автомата  $R_{UV}$ , значение переменной  $t$  обнуляется. Если в текущем состоянии  $r$ -различающего временного автомата не определён переход по любому входному символу, то к значению  $D$  переменной  $t$  прибавляется величина временной задержки в текущем состоянии, и следующее состояние  $r$ -различающего временного автомата  $R_{UV}$  вычисляется по значению  $\Delta_R(r)$ . Эксперимент заканчивается, как только  $r$ -различающий временной автомат переходит в одно из специальных состояний  $\perp_U$  или  $\perp_V$ . Если  $r$ -различающий временной автомат  $R_{UV}$  достигает состояния  $\perp_U$ , то предъявленный временной автомат

---

**Алгоритм 3** Получение  $r$ -различающего временного автомата
 

---

**Вход:** Два наблюдаемых временных автомата  $U = \langle U, I, O, \hat{u}, \lambda_U, \Delta_U \rangle$  и  $V = \langle V, I, O, \hat{v}, \lambda_V, \Delta_V \rangle$ .  
**Выход:**  $R$ -различающий временной автомат  $R_{UV}$ , если  $U$  и  $V$  –  $r$ -различимы.

- 1:  $W_0 := \{\perp, \perp_U, \perp_V\}; \lambda_R := \emptyset; W := U \cap V;$
- 2: Строим  $Q_1$  – множество 1-недоопределённых состояний,  $Q_2$  – 2-недоопределённых состояний и так далее пока  $Q_j \neq Q_{j+1}$ .
- 3: Если  $\forall j \langle \hat{u}, 0, \hat{v}, 0 \rangle \notin Q_j$ , то
- 4: Исходные временные автоматы  $r$ -совместимы; **Конец**.
- 5: Пусть  $n$  – такое число, что  $\langle \hat{u}, 0, \hat{v}, 0 \rangle \in Q_n$ , но  $\langle \hat{u}, 0, \hat{v}, 0 \rangle \notin Q_{n-1}$ ;
- 6:  $z := n; W_n := \{\langle \hat{u}, 0, \hat{v}, 0 \rangle\}; W_{n-1} := \emptyset; W_{n-2} := \emptyset; \dots; W_1 := \emptyset;$
- 7: **Пока** ( $z > 0$ )
- 8: Для каждого  $(w \equiv \langle u, k_u, v, k_v \rangle \in W_z)$
- 9:   Если для всех  $i \in \text{in}_U(u) \cap \text{in}_V(v)$  и всех  $o \in O$  выполняется  $\llbracket w \rrbracket_{i/o} \not\subseteq Q_{z-1}$ , то
- 10:     Положим  $\Delta_R(w) := \langle w', t \rangle$ , где  $\langle w', t \rangle = \Delta_W(w)$ ;
- 11:     Добавим состояние  $w'$  в множество  $W_z$ ;
- 12:   иначе
- 13:     Выберем такое произвольное  $i \in \text{in}_U(u) \cap \text{in}_V(v)$ , что для всех  $o \in O$  выполняется  $\llbracket w \rrbracket_{i/o} \subseteq Q_{z-1}$ ;
- 14:     Для каждого  $o \in O \setminus (\text{out}_U(u, i) \cup \text{out}_V(v, i))$  добавим в множество  $\lambda_R$  переходы  $\langle w, i, o, \perp \rangle$ ;
- 15:     Для каждого  $o \in \text{out}_U(u, i) \setminus \text{out}_V(v, i)$  добавим в множество  $\lambda_R$  переходы  $\langle w, i, o, \perp_U \rangle$ ;
- 16:     Для каждого  $o \in \text{out}_V(v, i) \setminus \text{out}_U(u, i)$  добавим в множество  $\lambda_R$  переходы  $\langle w, i, o, \perp_V \rangle$ ;
- 17:     Для каждого перехода  $\langle w, i, o, w' \rangle$  из  $\lambda_W$  добавим в множество  $\lambda_R$  переход  $\langle w, i, o, w' \rangle$ , а в множество  $W_{z'}$  состояние  $w'$ , где  $z' < z$  – такое число, что  $w' \in Q_{z'}$ , но  $w' \notin Q_{z'-1}$ ;
- 18:     Если  $\Delta_W(w) = \langle w, \infty \rangle$ , то положим  $\Delta_R(w) := \langle \perp, 1 \rangle$ , иначе Если  $\Delta_W(w) = \langle w'', t \rangle \in W \times \mathbb{N}$ , то положим  $\Delta_R(w) := \langle \perp, t \rangle$ ;
- 19:      $z := z - 1$ ;
- 20:      $R := \bigcup_{z=0}^n W_z$ ;
- 21: Временной автомат  $\langle R, I, O, \hat{r}, \lambda_R, \Delta_R \rangle$  – искомый временной автомат; **Конец**.

---

распознается как временный автомат  $U$ ; если  $r$ -различающий временный автомат  $R_{UV}$  достигает состояния  $\perp_V$ , то предъявленный временный автомат распознается как временной автомат  $V$ .

Поскольку граф переходов временного автомата  $R_{UV}$  ациклический (за исключением петель с пометками  $\infty$ ), и в каждом состоянии, в котором не определён переход по любому входному символу, задержка является конечной, то условный эксперимент на основе  $r$ -различающего временного автомата является конечным.

**Теорема 5.** Два временных автомата  $r$ -различимы тогда и только тогда, когда для них существует  $r$ -различающий временной автомат.

Алгоритм 3 описывает построение  $r$ -различающего временного автомата по пересечению двух временных автоматов с использованием понятия недоопределённых состояний.

Состояние  $w = \langle u, k_u, v, k_v \rangle$  пересечения  $W = U \cap V$  называется 1-недоопределённым, если найдётся такой входной символ  $i$  из  $\text{in}_U(u') \cap \text{in}_V(v')$ , по которому нет ни одного перехода из состояния  $w$ . Также состояние называется 1-недоопределённым, если из него можно перейти в другое 1-недоопределённое состояние по временной задержке. Состояние  $w$  пересечения  $W$  называется  $z$ -недоопределённым,  $z > 1$ , если оно  $(z-1)$ -недоопределённым, или найдётся такой входной символ  $i \in \text{in}(\langle u, k_u, v, k_v \rangle)$ , что все состояния, достижимые из  $w$  по входному символу  $i$ , являются  $(z-1)$ -недоопределёнными. Состояние  $w$  будет  $z$ -недоопределённым также в случае, когда из него по временной задержке достижимо некоторое  $z$ -недоопределённое состояние.

Так же как и в случае конечных автоматов и входо-выходных полуавтоматов,  $r$ -различающий временной автомат можно использовать при построении проверяющих тестов для временных автоматов. Под *моделью неисправности временных автоматов* будем понимать тройку  $\langle U, \precsim, \mathfrak{E} \rangle$ , где  $U$  – временной автомат-спецификация, описывающий требуемое поведение тестируемой системы,  $\precsim$  – отношение квази-редукции, выступающее в качестве отношения соответствия спецификации, а  $\mathfrak{E}$  – множество полностью определённых временных автоматов, описывающих все возможные реализации системы.

При построении тестов с гарантированной полнотой вместо различающего полуавтомата используют понятие тестового примера. Если  $V$  есть временной автомат-реализация, различимый со спецификацией  $U$ , то тестовый пример получается из различающего автомата  $R_{UV}$  заменой состояния  $\perp_U$  на состояние  $\top$ , отождествлением состояния  $\perp_V$  с состоянием  $\perp$ , введением нового состояния  $\perp$ , и заменой всех переходов  $r \xrightarrow{t} \perp$  на  $r \xrightarrow{t} \perp$ , где  $t \in \mathbb{N}$ . Состояние  $\top$  соответствует вердикту «Тест пройден успешно», состояние  $\perp$  – «Обнаружена неисправность», а состояние  $\perp$  – «Результат не определён».

Будем говорить, что тестовый пример  $P$  не согласуется с полностью определённым временным автоматом  $V$ , если в подмножестве  $\{\langle v, k_v, p, k_p \rangle \mid \text{in}(\langle v, k_v, p, k_p \rangle) = \emptyset\}$  множества состояний пересечения  $W = V \cap P$  найдутся состояния, для которых  $p = \perp$ , для всех состояний этого подмножества  $p \neq \top$  и если  $\Delta_W(\langle v, k_v, p, k_p \rangle) = \langle \langle v', k'_v, \perp, k \rangle, t \rangle$  для некоторого  $t$ , то  $p = \perp$ . Тестовый пример  $P$  абсолютно согласуется с полностью определённым временным автоматом  $V$ , если в подмножестве  $\{\langle v, k_v, p, k_p \rangle \mid \text{in}(\langle v, k_v, p, k_p \rangle) = \emptyset\}$  множества состояний пересечения  $W = V \cap P$  найдутся состояния, для которых  $p = \top$ , для всех состояний этого подмножества  $p \neq \perp$  и если  $\Delta_W(\langle v, k_v, p, k_p \rangle) = \langle \langle v', k'_v, \perp, k \rangle, t \rangle$  для некоторого  $t$ , то  $p = \perp$ .

Понятия проверяющего теста, исчерпывающего, непротиворечивого и полного проверяющего теста определяются так же как и для автоматной модели неисправности. Точно так же, как для конечных автоматов, можно построить полный проверяющий тест относительно модели неисправности  $\langle U, \precsim, \mathfrak{E} \rangle$ , в которой множество  $\mathfrak{E}$  конечное, состоит из полностью определённых временных автоматов, и каждый временной автомат из множества является квази-редукцией спецификации  $U$  или  $r$ -различим с ней.

## ЗАКЛЮЧЕНИЕ

В диссертационной работе исследованы условные эксперименты по различению (распознаванию) недетерминированных конечных автоматов, входо-выходных полуавтоматов и временных конечных автоматов.

Установлены необходимые и достаточные условия различимости двух автоматов условным экспериментом и предложен алгоритм построения такого эксперимента как  $r$ -различающего автомата. Введено понятие тестового примера для автоматной модели неисправности, как  $r$ -различающего автомата специального вида. Предложен метод построения непротиворечивого теста по мутационному автомату.

Установлены необходимые и достаточные условия различимости двух входо-выходных полуавтоматов условным экспериментом, и предложен алгоритм построения такого эксперимента как **ioco**-различающего полуавтомата. Введено понятие тестового примера для полуавтоматной модели неисправности, как **ioco**-различающего входо-выходного полуавтомата специального вида.

Показано, что возможен переход от полуавтоматной модели неисправности с отношением **ioco** в качестве отношения конформности к автоматной модели с отношением квази-редукции в качестве отношения конформности. Предложен метод построения конечного полного проверяющего теста для полуавтоматной модели неисправности на основе использования автоматных методов синтеза тестов с гарантированной полнотой.

Введены понятия временного автомата и пересечения двух наблюдаемых временных автоматов. Установлены необходимые и достаточные условия различимости двух временных автоматов условным экспериментом и предложен алгоритм построения такого эксперимента как  $r$ -различающего временного автомата. Введено понятие тестового примера для модели неисправности с временными автоматами, как  $r$ -различающего временного автомата специального вида.

Алгоритмы и их программные реализации, разработанные в процессе выполнения диссертационной работы, могут быть использованы в системах автоматического синтеза проверяющих и диагностических тестов для систем логического управления, в частности, в системах автоматического синтеза проверяющих и диагностических тестов для протоколов телекоммуникационных систем.

### Список публикаций по теме диссертации

1. Громов М.Л., Евтушенко Н.В., Коломеец А.В. К синтезу условных тестов для недетерминированных автоматов // Программирование. — 2008. — №6. — С. 1–11.
2. Громов М.Л., Коломеец А.В., Евтушенко Н.В. Синтез диагностических тестов для автоматных сетей // Вестник ТГУ. Приложение. — 2004. — №9(І). — С. 204–209.
3. Gromov M., Willemse T. Testing and Model-Checking Techniques for Diagnosis // Vol.4581 of LNCS. — Springer, 2007. — P.138–154.
4. Громов М.Л., Шабалдина Н.В. О распознавании недетерминированного автомата в заданном классе // Материалы IX Международного семинара «Дискретная математика и её приложения» / Под ред. О.М. Касим-Заде. — М.: ММФ МГУ, 2007. — С. 157–160.
5. Громов М.Л. Метод построения полного проверяющего теста для входо-выходных полуавтоматов // Вестник ТГУ. Управление, вычислительная техника и информатика. — 2008. — №3(4). — С. 85–98.
6. Gromov M., Evtushenko N., Kolomeets A. On the synthesis of adaptive tests for nondeterministic finite state machines // Program. Comput. Softw. — 2008. — Vol. 34. N. 6. — P. 322–329.
7. Громов М.Л., Кондратьева О.В. Об одном классе автоматов с полиномиальной оценкой числа состояний в наблюдаемой форме // Журнал СФУ. Серия: Математика и физика — 2008. — Т. 1, №3. — С. 257–261.
8. Gromov M. A novel method for derivation of a test with guaranteed coverage for LTS // Proceedings of SYRCoSE 2008. — St.Peterburg: S-PSU, 2008. — P. 47–49.
9. Gromov M., Popov D., Yevtushenko N. Deriving test suites for timed Finite State Machines // Proceedings of IEEE East-West Design & Test Symposium'08. — Kharkov, Ukraine: SPD FL Stepanov V.V., 2008. — P. 339–343.
10. Gromov M., El-Fakih K., Shabaldina N., Yevtushenko N. Distinguishing Non-deterministic Timed Finite State Machines // Vol. 5522 of LNCS. — Springer, 2009. — P. 137–151.