Методы синтеза установочных и различающих экспериментов с недетерминированными автоматами

Наталья Кушик, аспирант 3-го года обучения по специальности 05.13.01 – Системный анализ, управление, обработка информации

Научный руководитель: д.т.н., проф. Н.В. Евтушенко

Томский государственный университет

20 ноября 2012

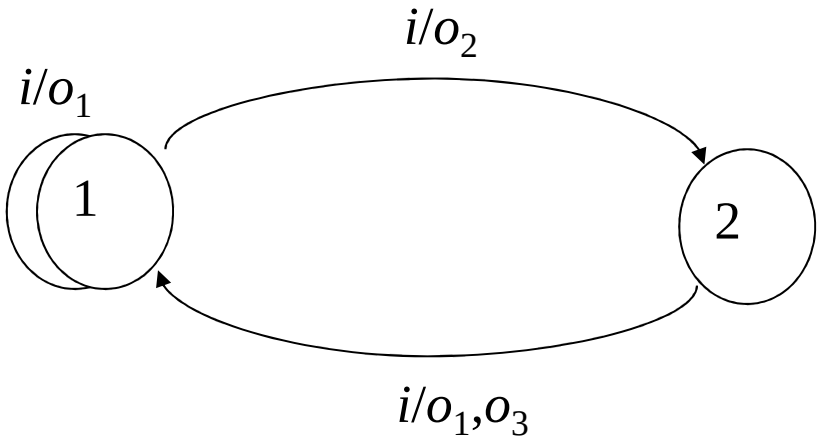
Содержание

- Недетерминированные автоматы
- Краткий обзор существующих методов синтеза умозрительных экспериментов с конечными автоматами
- Безусловные различающие и установочные эксперименты с недетерминированными автоматами
- Условные (адаптивные) различающие и установочные эксперименты с недетерминированными автоматами
- Недетерминированные автоматы в анализе и синтезе дискретных систем

Конечный автомат

Конечный автомат $S = (S, I, O, h_S, S')$

- S – конечное множество состояний с непустым подмножеством S' начальных состояний
- I и O – входной и выходной алфавиты
- $h_S \subseteq S \times I \times O \times S$ – отношение переходов



Конечный автомат (2)

$S = (S, I, O, h_S, S')$

- Автомат S *детерминированный*, если для каждой пары $(s, i) \in S \times I$ найдется не более одной пары $(o, s') \in O \times S$ такой, что $(s, i, o, s') \in h_S$

  иначе автомат S *недетерминированный*

- Автомат S *полностью определенный*, если для каждой пары $(s, i) \in S \times I$ найдется пара $(o, s') \in O \times S$ такая, что $(s, i, o, s') \in h_S$

  иначе автомат S *частичный*

- Автомат S *наблюдаемый*, если для каждой тройки $(s, i, o) \in S \times I \times O$ найдется не более одного состояния $s' \in S$ такого, что $(s, i, o, s') \in h_S$

  иначе автомат S *ненаблюдаемый*

Эксперименты с конечными автоматами

• Умозрительные эксперименты были введены Э. Муром в 1956 г.

• Под *экспериментом* понимается подача входной последовательности на автомат, наблюдение выходной реакции автомата и вывод заключения о свойствах автомата

• Среди экспериментов с автоматами рассматривают установочные, синхронизирующие, различающие (диагностические), проверяющие и распознающие эксперименты

Эксперименты с конечными автоматами (2)

Установочные, синхронизирующие, различающие (диагностические)

- Известна функция поведения автомата
- Позволяют определить начальное (до эксперимента) или финальное (после эксперимента) состояние автомата

Проверяющие,

Распознающие

- Известно множество, содержащие автомат
- Позволяют выявить некоторые свойства автомата, предъявленного к эксперименту, например, убедиться, что предъявленный автомат является эквивалентным эталонному автомату

Эксперименты с конечными автоматами (3)

Безусловный эксперимент

Входная последовательность формируется *ДО* эксперимента

Условный (адаптивный) эксперимент

Следующий входной символ формируется на основе выходной реакции на предыдущие входные символы

Длина адаптивного эксперимента может быть меньше (!), но такой эксперимент может быть сложнее для реализации (!)

В диссертации предлагаются методы синтеза **безусловных и условных различающих и установочных экспериментов** для недетерминированных автоматов

Представление эксперимента

Безусловный эксперимент

- Эксперимент представляется входной последовательностью
- Сложность эксперимента оценивается *длиной* входной последовательности

Условный (адаптивный) эксперимент

- Эксперимент представляется частичным ациклическим автоматом
- Сложность эксперимента оценивается *высотой* эксперимента, т.е. длиной самой длинной входо-выходной последовательности ациклического автомата

Краткий обзор существующих методов синтеза экспериментов

Безусловные различающие эксперименты

- Рассматривались для неинициальных детерминированных автоматов (Гилл, Агибалов, Кохави), и известны методы их синтеза

- Рассматривались для двух инициальных недетерминированных автоматов или двух состояний одного автомата (Янакакис, Алюр, Шабалдина, Эль-Факи, Евтушенко), и известны методы их синтеза

- В первом случае сложность полиномиальна относительно числа состояний автомата, предъявленного к эксперименту

Во втором случае сложность экспоненциальна относительно числа состояний автомата, предъявленного к эксперименту

Краткий обзор существующих методов синтеза экспериментов (2)

Условные различающие эксперименты

- Рассматривались для двух инициальных недетерминированных автоматов (Янакакис, Алюр, Шабалдина, Эль-Факи, Евтушенко) или двух состояний одного автомата, и известны методы их синтеза
- Полиномиальная сложность относительно числа состояний автомата, предъявленного к эксперименту
- В работах Петренко, Евтушенко, Громова эффективно представляются в виде конечного ациклического автомата

Для двух инициальных недетерминированных автоматов или двух состояний одного автомата переход от безусловного эксперимента к условному понижает сложность эксперимента с экспоненциальной до полиномиальной

Краткий обзор существующих методов синтеза экспериментов (3)

Безусловные установочные эксперименты

- Рассматривались для неинициальных детерминированных автоматов (Гилл, Агибалов, Кохави), и известны методы их синтеза
- Сложность оценивается полиномом второй степени относительно числа состояний автомата, предъявленного к эксперименту
- Показано, что для любого полностью определенного приведенного детерминированного автомата существует установочный эксперимент

Краткий обзор существующих методов синтеза экспериментов (4)

Условные установочные эксперименты

- Рассматривались для неинициальных детерминированных автоматов
- Показано (Хиббард), что переход от безусловного установочного эксперимента к условному для детерминированных автоматов не понижает его сложности
- *Не рассматривались* для недетерминированных автоматов

Краткий обзор существующих методов синтеза экспериментов (5)

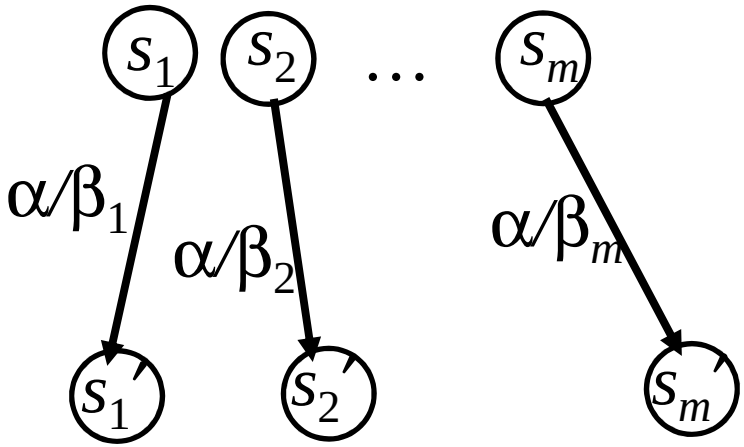
Синхронизирующие эксперименты

- Рассматривались только безусловные эксперименты
- Рассматривались для неинициальных детерминированных автоматов (Спивак, Рысцов)
- В работах научной группы Волкова (УФУ, Россия) рассматриваются методы синтеза синхронизирующих экспериментов для полуавтоматов, в том числе, недетерминированных, и исследуются различные классы автоматов для оценки сложности таких экспериментов
- Для детерминированных полуавтоматов полиномиальная сложность относительно числа состояний автомата, предъявленного к эксперименту

Различающий эксперимент

- Позволяет идентифицировать состояние автомата до подачи α
- После подачи α в любом состоянии s_i и наблюдения выходной реакции β_i начальное состояние s_i становится известным

Разделяющая последовательность α



Эксперимент = подать α + пронаблюдать β_i + принять решение насчет s_i

Синтез безусловных различающих экспериментов

Корень дерева помечается множеством всех пар начальных состояний

- Строим дерево преемников автомата

$\exists\, o_1\ ((s_1, i_j, o_1, s_1',) \in h_S\ \&\ (s_2, i_j, o_1, s_2') \in h_S\ \&\ s_1' \neq s_2')$

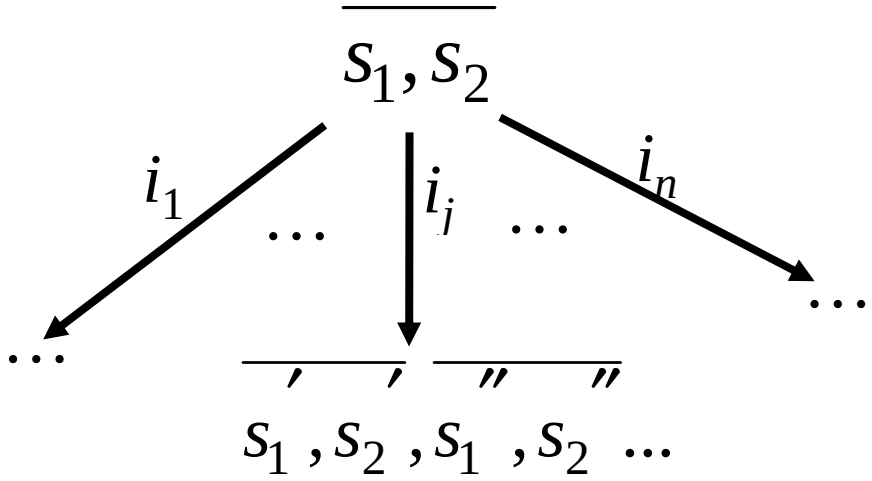
- Правила усечения

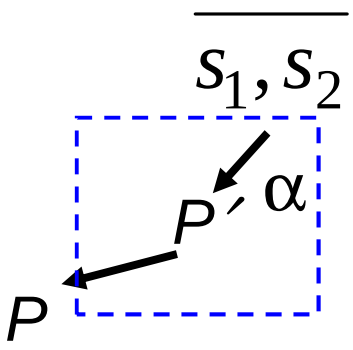
Правило 1 Множество *P* пусто

Правило 2 Множество *P* содержит подмножество, помечающее узел на пути от корня к узлу, помеченному *P*

Правило 3 *P* содержит одноэлементное подмножество

Узлы дерева помечаются множествами пар состояний





Синтез безусловных различающих экспериментов (2)

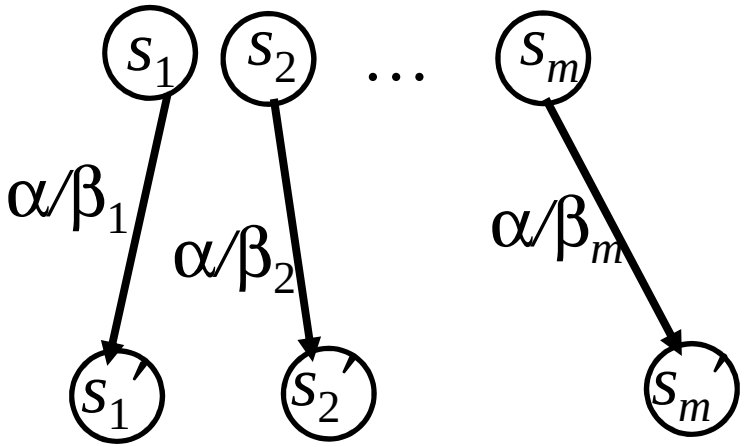
• Множество начальных состояний автомата $S = (S, I, O, h_S, S')$ назовем *разделимым*, если существует входная последовательность α, которая является *разделяющей последовательностью* для любых двух различных состояний s_1 и s_2 множества S', т.е. справедливо $out(s_1, \alpha) \cap out(s_2, \alpha) = \varnothing$

• Последовательность α является разделяющей последовательностью для множества начальных состояний автомата, если и только если она помечает путь в дереве преемников, ведущий в вершину, усеченную по Правилу 1

Установочный эксперимент

- Позволяет идентифицировать состояние автомата после подачи α
- После подачи α в любом состоянии s_i и наблюдения выходной реакции β_i финальное состояние s_i' становится известным

Установочная последовательность α



Эксперимент = подать α + пронаблюдать β_i + принять решение насчет s_i'

Установочная последовательность для недетерминированного автомата

Задан конечный автомат $S = (S, I, O, h_S, \{s_1, s_2\})$

$\alpha \in I^*$ – это **установочная последовательность** для S, если для пары $\{s_1, s_2\}$ начальных состояний выполняется

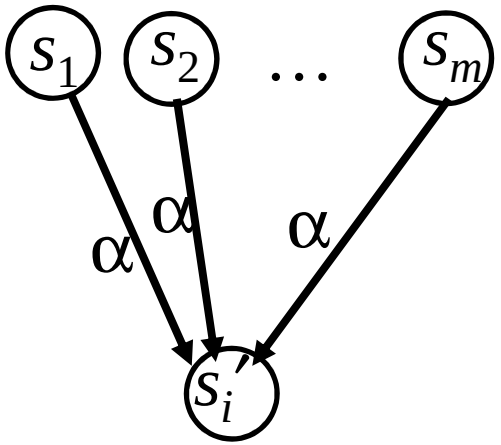
$$\forall \beta \in output(s_1, \alpha) \cap output(s_2, \alpha)\ [next\_state(s_1, \alpha/\beta) = next\_state(s_2, \alpha/\beta)]$$

Для наблюдаемых автоматов установочная последовательность для множества S' есть последовательность, которая является установочной для каждой пары состояний из S'

Синхронизирующий эксперимент

- Позволяет идентифицировать состояние автомата после подачи α
- После подачи α в любом состоянии s_i финальное состояние s_i' известно, и оно является уникальным

Синхронизирующая последовательность α



Эксперимент = подать α + принять решение насчет s_i'

Синтез безусловных установочных/синхронизирующих экспериментов

Строится дерево преемников, НО изменяются правила усечения

Установочный эксперимент

- **Правило 1** Множество *P* пусто
- **Правило 2** Множество *P* содержит подмножество, помечающее узел на пути от корня к узлу, помеченному *P*
- **Правило 3** *P* состоит из одноэлементных подмножеств

α – установочная последовательность $\Leftrightarrow$ α помечает путь в вершину, усеченную по Правилу 1 или 3

Синхронизирующий эксперимент

- **Правило 1** Множество *P* пусто
- **Правило 2** Множество *P* содержит подмножество, помечающее узел на пути от корня к узлу, помеченному *P*
- **Правило 3** $|P| = 1$

α – синхронизирующая последовательность $\Leftrightarrow$ α помечает путь в вершину, усеченную по Правилу 3

Необходимые и достаточные условия существования безусловного эксперимента

• Для наблюдаемого автомата *S* существует простой *безусловный различающий* эксперимент, если и только множество начальных состояний автомата является разделимым множеством, т.е. существует последовательность, разделяющая каждую пару начальных состояний *S*

• Для наблюдаемого автомата *S* существует простой *безусловный установочный* эксперимент, если и только для *S* существует установочная последовательность

Сложность безусловных экспериментов

• Сложность эксперимента оценивается длиной последовательности, помечающей путь в дереве преемников к вершине, усеченной по соответствующему правилу

• Длина кратчайшей разделяющей последовательности для наблюдаемого полностью определенного автомата $S = (S, I, O, h, S')$, $|S| = n$, $|S'| = m$, не превосходит $2^{C_n^2} - 2^{C_n^2 - C_m^2}$

• Существует класс автоматов, для которых разделяющая последовательность и только она является установочной

Сложность безусловных экспериментов (2)

• Доказано (Янакакис и др.), что сложность различающего эксперимента для двух инициальных автоматов или автомата с двумя состояниями является экспоненциальной относительно числа состояний автомата

• В работах Шабалдиной, Эль-Факи, Евтушенко показывается точная величина и достижимость экспоненциальной оценки, НО число входных символов у соответствующего автомата также экспоненциально зависит от числа его состояний

• В диссертации приводится новый класс автоматов с достижимой экспоненциальной оценкой сложности для безусловного установочного эксперимента

Автомат с экспоненциальной установочной последовательностью

- Рассматривается недетерминированный автомат S_n, $n > 3$, с множеством состояний $S = \{0, 1, 2, \ldots, n - 1\}$, множеством входных символов $I = \{i_0, i_1, \ldots, i_{n-2}\}$ и множеством выходных символов

  $O = \{(i, j): i, j = 0, \ldots, n - 1 \text{ и } i < j\}$
- Показывается, что кратчайшая установочная последовательность покрывает путь в дереве преемников, помеченный множествами пар состояний из следующих множеств

$\{0, 1, \ldots, n - 1\}, \{1, 2, \ldots, n - 1\}, \{0, 2, \ldots, n - 1\}, \{2, 3, \ldots, n - 1\}, \ldots, \{0, n - 1\}$

- Длина такой последовательности $2^{n-1} - 1$

Тестовый пример

- Используется для представления условного эксперимента
- *Тестовый пример* – частичный наблюдаемый автомат ***R***, граф переходов которого ациклический и в каждом не тупиковом состоянии определены переходы только по одному входному символу со всеми возможными выходными символами
- Тестовый пример определяется относительно входного алфавита *I* и выходного алфавита *O*, т.е. представляет условный эксперимент с любым автоматом с этими алфавитами

Пересечение неинициальных автоматов

$S = (S, I, O, h_S, S')$ и $P = (P, I, O, h_P, P')$ суть полностью определенные недетерминированные автоматы

Пересечение $S \cap P$ есть наибольший связный подавтомат автомата Q, состояниями которого являются пары (b, c), где $b \subseteq S$ и $c \subseteq P$ с начальным состоянием (S', P')

Для входо-выходной пары i/o существует переход

$((b, c), i, o, (b', c'))$ из состояния (b, c), если и только если в каждом из подмножеств b и c существует состояние, в котором есть переход по паре i/o, и b' и c' суть i/o-преемники подмножеств b и c

Различающий тестовый пример

Тестовый пример $P = (P, I, O, h_P, p_0)$ называется *различающим* для автомата $S = (S, I, O, h_S, S')$, если

1) каждое тупиковое состояние (b, c) пересечения $P \cap S$ состоит из одноэлементных подмножеств b и c
2) для любого перехода $((b, c), i, o, (b', c'))$ пересечения $P \cap S$ в подмножестве c не существует двух различных состояний, из которых есть переходы в одно и то же состояние по вход-выходной паре i/o, т. е.

$$\forall s_1, s_2 \in c\ ((s_1, i, o\ , s') \in h_S\ \&\ (s_2, i, o\ , s') \in h_S \Rightarrow s_1 = s_2)$$

Установочный/синхронизирующий тестовый пример

Тестовый пример $P = (P, I, O, h_P, p_0)$ называется *установочным* для автомата $S = (S, I, O, h_S, S')$, если

1) каждое тупиковое состояние (b, c) пересечения $P \cap S$ состоит из одноэлементных подмножеств b и c

Установочный тестовый пример называется *синхронизирующим*, если

1) каждое тупиковое состояние (b, c) состоит из одного и того же одноэлементного подмножества

Необходимые и достаточные условия существования условного эксперимента

Для полностью определенного наблюдаемого недетерминированного автомата $S = (S, I, O, h_S, S')$ существует различающий/установочный/синхронизирующий эксперимент, если и только если для этого автомата существует различающий/установочный/синхронизирующий тестовый пример

Условная различимость

Различающий тестовый пример строится на основе *k-условно-различимых* подмножеств состояний

Подмножество $m \subseteq S$ называется*1-условно-различимым*, если оно разделимо одним входным символом

Подмножество $m \subseteq S$ называется *k-условно-различимым, если m* является (*k* – 1)-условно-различимым или найдется такой входной символ $i \in I$, что для любого выходного символа $o \in O$ множество всех *i*/*o*-преемников *m* пусто, содержит одно состояние или является (*k* – 1)-условно-различимым, причем в последних двух случаях любые два состояния из *m* имеют различные *i*/*o*-преемники

Алгоритм синтеза различающего тестового примера

Вход: $S = (S, I, O, h, S')$, первые m состояний – начальные, S' – k-условно-различимо; множество всех 1, 2, …, k-условно-различимых множеств

Выход: Различающий тестовый пример P для S

1. Множество состояний P: S', p_1, p_2, …, p_m, 1, 2, …, k-условно-различимые множества состояний автомата S

$p_0 = S'$; $p_i = s_i$, $i \in \{1, \ldots, m\}$; $h_P = \varnothing$

2. Для j от 2 до k выполнять для j-условно-различимого подмножества R

2.1. Определить $i \in I$, такой, что для любого $o \in O$ множество i/o-преемников состояний из R пусто, содержит одно состояние или является $(j-1)$-условно-различимым множеством R', $|R'| > 1$, причем любые два различные состояния из R не обладают одним и тем же i/o-преемником

2.2. *Если* множество i/o-преемников состояний из R пусто или содержит одно состояние, добавить в множество h_P переход (R, i, o, p')

Иначе добавить в h_P каждый переход (R, i, o, R')

Алгоритм синтеза различающего тестового примера (2)

3. 3.1 Удалить из *P* все состояния, недостижимые из начального состояния, и итеративно удалить все переходы *в* и *из* этих состояний

3.2 Для тупикового состояния p' автомата *P* найти множество $\Sigma_{p'}$ входо-выходных последовательностей, переводящих автомат *P* из начального состояния в состояние p'

3.3 Для каждой входо-выходной последовательности $\alpha \in \Sigma_{p'}$ найти начальное состояние $s_j \in S'$ автомата *S*, в котором реализуется данная входо-выходная последовательность и заменить переход (R, i, o, p') в автомате *P* на переход (R, i, o, p_j) для всех подмножеств *R*, соответствующих состояниям автомата *P*

Если последовательность α не реализуется ни в одном из состояний автомата S, то заменить переход (R, i, o, p') в автомате P на любой переход (R, i, o, p_j) и ВЫХОД

Условная установочность

Установочный тестовый пример строится на основе *k-условно-установочных* подмножеств состояний

Подмножество $m \subseteq S$ называется *1-условно-установочным*, если существует установочная последовательность длины 1

Подмножество $m \subseteq S$ *называется k-условно-установочным, если* m является (k – 1)-условно-установочным или найдется такой входной символ $i \in I$, что для любого выходного символа $o \in O$ множество всех i/o-преемников m пусто, содержит одно состояние или является (k – 1)-условно-установочным

Алгоритм синтеза установочного тестового примера

Вход: $S = (S, I, O, h, S')$, S' – k-условно-установочно; множество всех 1, 2, …, k-условно-установочных множеств

Выход: Установочный тестовый пример P для S

1. Множество состояний P: S', p_1, p_2, …, p_n, 1, 2, …, k-условно-установочные множества состояний автомата S

$p_0 = S'$; $p_i = s_i$, $i \in \{1, \ldots, n\}$; $h_P = \varnothing$

2. Для j от 2 до k выполнять для j-условно-установочного подмножества R

2.1. Определить $i \in I$, такой, что для любого $o \in O$ множество i/o-преемников состояний из R пусто, содержит одно состояние или является $(j - 1)$-условно-установочным множеством R', $|R'| > 1$

2.2. *Если* множество i/o-преемников состояний из R пусто или содержит одно состояние, добавить в множество h_P переход (R, i, o, p')

Иначе добавить в h_P каждый переход (R, i, o, R')

Алгоритм синтеза установочного тестового примера (2)

3. 3.1 Удалить из *P* все состояния, недостижимые из начального состояния, и итеративно удалить все переходы *в* и *из* этих состояний

3.2 Для тупикового состояния p' автомата *P* найти множество $\Sigma_{p'}$ входо-выходных последовательностей, переводящих автомат *P* из начального состояния в состояние p'

3.3 Для каждой входо-выходной последовательности $\alpha \in \Sigma_{p'}$ найти найти финальное состояние $s_j \in S$ автомата *S*, в которое автомат *S* переводится данной входо-выходной последовательностью, и заменить переход (R, i, o, p') в автомате *P* на переход (R, i, o, p_j) для всех подмножеств *R*, соответствующих состояниям автомата *P*

Если последовательность α не реализуется ни в одном из состояний автомата S, то заменить переход (R, i, o, p') в автомате P на любой переход (R, i, o, p_j) и ВЫХОД

Сложность условных экспериментов

- Ограничивается числом различных подмножеств *n*-элементного множества *S* мощности *m* и меньше
- Сложность безусловного различающего/установочного эксперимента не превосходит $\sum_{i=2}^{m} C_n^i$
- В диссертации приводится автомат с множеством состояний {1, 2, 3, 4}, каждое из которых может быть начальным, | *I* | = 11

  Кратчайший условный эксперимент для автомата имеет трассу, покрывающую цепочку множеств состояний

{1, 2, 3, 4}, {1, 2, 3}, {1, 2, 4}, {1, 3, 4}, {2, 3, 4}, {3, 4}, {2, 4}, {1, 4}, {1, 3}, {2, 3}, {1, 2}

- Высота эксперимента равна 11

Приложения недетермини-рованных автоматов к задачам анализа и синтеза сложных систем

Анализ и синтез неизвестной компоненты автоматной сети

Рассматривается задача оптимизации логических схем на основе решения автоматных уравнений

Тестирование дискретных систем

Рассматривается задача тестирования протокольной реализации на соответствие ее RFC спецификации

Оптимизация логических схем на основе решения автоматных уравнений

- Логическая схема представляется в виде каскадной композиции двух подсхем, одна из которых перепроектируется
- Поведение каждой подсхемы и всей схемы в целом описывается структурным автоматом
- Решается уравнение для перепроектируемой подсхемы
- Наибольшее решение – недетерминированный автомат, из которого выбирается оптимальное решение

Экспериментальные результаты

Критерии оптимизации: число вентилей и длина пути от входов к выходам схемы

Бенчмарки ISCAS'89

- Удалось оптимизировать схемы s208.bench, s420.bench, s27.bench
- Удалось оптимизировать схемы, оптимизированные системой ABC

Первый S-блок DES

- Удалось оптимизировать схему первого S-блока DES
- Схема для этого S-блока была получена синтезом от системы булевых функций при помощи пакета ABC

Тестирование реализации протокола IRC

- По RFC спецификации строится расширенный автомата, моделирующий серверную часть протокола IRC
- Расширенный автомат «разворачивается» в конечный автомат с ограничением на число состояний
- По полученному конечному автомату синтезируется тест методом обхода графа переходов
- Полученный тест подается на реализацию *ngIRCd*, расположенную в свободном доступе
- Тестом были обнаружены три несоответствия *ngIRCd* реализации RFC спецификации протокола IRC

На защиту выносится

- Необходимые и достаточные условия существования безусловных и условных различающих, установочных и синхронизирующих экспериментов с наблюдаемыми недетерминированными автоматами
- Методы синтеза безусловных и условных различающих и установочных экспериментов для наблюдаемых недетерминированных автоматов
- Оценки сложности безусловных и условных различающих и установочных экспериментов для наблюдаемых недетерминированных автоматов

  Достижимость экспоненциальной оценки сложности безусловного установочного эксперимента относительно размерности предъявленного автомата

Апробация работы

- Результаты докладывались

  - на **3** Российских конференциях

  - на **7** международных конференциях (в России и за рубежом)

  - на **3** Школах международных Школах TAROT

  - на семинаре лаборатории логического проектирования ОИПИ НАН Беларуси

- Опубликованы в **12** статьях в научных журналах, докладах и материалах конференций различного уровня, в том числе **5** статей в рецензируемых журналах из перечня ВАК

Основные публикации

- *Кушик Н. Г.* Оптимизация комбинационных схем на основе решения уравнений / Н. Г. Кушик, М. В. Рекун // Журнал СФУ. Математика и физика. – Красноярск, 2008. – 1 (3). С. 290-295.
- *Kushik N.* Preset and Adaptive Homing Experiments for Nondeterministic Finite State Machines / N. Kushik, K. El-Fakih, N. Yevtushenko // Proc. of the CIAA 2011, LNCS №6807, 2011. P. 215-224.
- *М. В. Жигулин* Тестирование программной реализации протокола IRC на основе модели расширенного автомата / М. В. Жигулин, А. В. Коломеец, Н. Г. Кушик, А. В. Шабалдин // Известия Томского политехнического университета. – Томск, 2011. – Т. 318, № 5 – С. 81-84.
- *М. Л. Громов* Различающие эксперименты с неинициальными недетерминированными автоматами / М. Л. Громов, Н. Г. Кушик, Н. В. Евтушенко // Вестник Томского государственного университета. – Томск, 2011. – Т. 17, № 4 – С. 93-101.
- *Н. Г. Кушик.* Синтез условных синхронизирующих экспериментов для недетерминированных автоматов / Кушик Н. Г., Евтушенко Н. В. // Известия высших учебных заведений. Физика, 2012. – Т. 55, № 9/2 – С. 315-316.

Перспективы

- ? Достижимость оценок сложности условных различающих и установочных экспериментов
- ? Методы синтеза безусловных и условных различающих и установочных экспериментов с **не**наблюдаемыми автоматами
- ? Методы синтеза безусловных и условных различающих и установочных экспериментов с **частичными** автоматами
- ? Эксперименты по анализу и синтезу технических систем с недетерминированным поведением, которые не обладают сигналом СБРОСа

Спасибо за внимание!