ДИСКРЕТНЫЕ ФУНКЦИИ И АВТОМАТЫ

УДК 519.713

М.Л. Громов, Н.Г. Кушик, Н.В. Евтушенко

РАЗЛИЧАЮЩИЕ ЭКСПЕРИМЕНТЫ С НЕИНИЦИАЛЬНЫМИ НЕДЕТЕРМИНИРОВАННЫМИ АВТОМАТАМИ[1,2]

В статье исследуются различающие эксперименты с недетерминированными неинициальными автоматами. Показывается, как построить безусловный различающий эксперимент для множества начальных состояний, если множество начальных состояний является разделимым, т.е. существует входная последовательность, на которую множества выходных реакций в любых двух различных начальных состояниях не пересекаются. Кроме того, предлагается алгоритм построения условного эксперимента для множества начальных состояний, и устанавливаются свойства множества начальных состояний для существования такого эксперимента.

Ключевые слова: *недетерминированный автомат*, *неинициальный автомат*, *различающие эксперименты*, *разделимое множество состояний*, *разделяющая последовательность*, *условно-различимое множество состояний*, *различающий автомат.*

В последнее время появляется все больше исследований, посвященных недетерминированным автоматам. В частности, недетерминированные автоматы находят применение при разработке выигрышных стратегий в логических играх и криптографии, активно используются при синтезе и анализе дискретных систем управления, в частности при оптимизации дискретных систем и синтезе проверяющих и диагностических тестов для них. Однако большинство отношений совместимости и различимости между недетерминированными автоматами введено для инициальных автоматов.

В ряде приложений требуется различить несколько состояний автомата (несколько автоматов) простым безусловным или условным экспериментом. Известны необходимые и достаточные условия существования таких экспериментов для двух состояний заданного автомата (двух заданных инициальных автоматов). В данной работе мы устанавливаем необходимые и достаточные условия существования таких экспериментов для подмножества состояний автомата любой мощности, на основе которых можно установить необходимые и достаточные условия различимости конечного числа (неинициальных) полностью определенных автоматов простым безусловным и условным экспериментами.

---

[1] Авторы выражают благодарность проф. Американского университета Шарджа, ОАЭ, К. Эль-Факи за интересные дискуссии.
[2] Работа частично поддержана грантом РФФИ 10-08-92003.

1. Недетерминированные автоматы

Конечным автоматом, или просто *автоматом*, далее называется пятерка $\mathsf{S} = (S, I, O, h_\mathsf{S}, S')$, где S – конечное непустое множество состояний с выделенным непустым подмножеством S' начальных состояний, I и O – конечные входной и выходной алфавиты и $h_\mathsf{S} \subseteq S \times I \times O \times S$ – *отношение* или *множество переходов*. Если множество S' совпадает с множеством всех состояний автомата, то для обозначения такого автомата мы будем использовать четверку $\mathsf{S} = (S, I, O, h_\mathsf{S})$. Четверка $(s, i, o, s') \in h_\mathsf{S}$ описывает переход в автомате S из состояния s в состояние s' под действием входного символа i с выходным символом o. Если множество S' содержит только одно состояние, то автомат называется *инициальным* автоматом, в противном случае автомат называется *неинициальным*. Автомат называется *полностью определенным*, если для каждой пары $(s, i) \in S \times I$ существует хотя бы одна пара $(o, s') \in O \times S$, такая, что $(s, i, o, s') \in h_\mathsf{S}$; в противном случае автомат называется *частично определенным* или *частичным*. В данной работе мы рассматриваем только полностью определенные автоматы. Автомат называется *наблюдаемым*, если для каждой тройки $(s, i, o) \in S \times I \times O$ существует только одно состояние $s' \in S$, такое, что $(s, i, o, s') \in h_\mathsf{S}$; в противном случае автомат называется *ненаблюдаемым*. В данной работе мы рассматриваем только наблюдаемые автоматы. Автомат называется *детерминированным*, если для каждой пары $(s, i) \in S \times I$ существует не более чем одна пара $(o, s') \in O \times S$, такая, что $(s, i, o, s') \in h_\mathsf{S}$; в противном случае автомат называется *недетерминированным*. В общем случае в недетерминированном автомате в текущем состоянии для данного входного символа может существовать более одного перехода. Для неинициального автомата $\mathsf{S} = (S, I, O, h_S, S')$ далее через S/s_j обозначается инициальный автомат (S, I, O, h_S, s_j). Пусть $\mathsf{S} = (S, I, O, h_S, s_0)$ и $\mathsf{P} = (P, I, O, h_P, p_0)$ – инициальные автоматы. *Пересечением* $\mathsf{S} \cap \mathsf{P}$ автоматов S и P [1] называется наибольший связный подавтомат автомата $\mathsf{Q} = (S \times P, I, O, h_Q, s_0p_0)$, в котором $(sp, i, o, s'p') \in h_Q \Leftrightarrow (s, i, o, s') \in h_S \ \& \ (p, i, o, p') \in h_P$.

Отношение переходов естественным образом распространяется на входные и выходные последовательности. Пусть $s \in S$ и $i_1 \ldots i_k \in I^*$ – непустая последовательность входных символов. Четверка $(s, i_1 \ldots i_k, o_1 \ldots o_k, s') \in h_\mathsf{S}$, где $o_1 \ldots o_k \in O^*$, – последовательность из выходных символов, если существует последовательность состояний $s_1, \ldots, s_{k+1} \in S$ такая, что $s_1 = s$, $s_{k+1} = s'$ и для каждого $j = 1, \ldots, k$ справедливо $(s_j, i_j, o_j, s_{j+1}) \in h_\mathsf{S}$. Наличие четверки $(s, i_1 \ldots i_k, o_1 \ldots o_k, s')$ в множестве h_S означает, что автомат в состоянии s может переработать, т.е. *преобразовать* или *отобразить* входную последовательность $i_1 \ldots i_k$ в выходную $o_1 \ldots o_k$, причем после такого преобразования автомат будет находиться в состоянии s'. Пара последовательностей α/β, такая, что $(s, \alpha, \beta, s') \in h_\mathsf{S}$ для некоторого состояния $s' \in S$, называется *входо-выходной* последовательностью, или *траекторией* автомата, в состоянии s. Множество всех входо-выходных последовательностей автомата в состоянии s обозначается $Tr_\mathsf{S}(s)$. Для простоты дальнейшего повествования, будем использовать следующее обозначение: $Tr_\mathsf{S}(b) = \cup_{s \in b} Tr_\mathsf{S}(s)$, где $b \subseteq S$.

Для полностью определенного, возможно недетерминированного, автомата можно записать функции переходов *next_state* и выходов *out*, которые определены в каждом состоянии на всех входных последовательностях. Функция переходов описывает множество состояний, в которые автомат может перейти из состояния s под действием входной последовательности α. Функция выходов описывает множество выходных последовательностей, которые могут появиться на выходе автомата в этом случае. Таким образом, функции переходов и выходов отображают декартово произведение $S \times I$ в множества подмножеств множеств S и O^* соответственно, и для любых $s \in S$, $b \subseteq S$ и $\alpha \in I^*$ справедливо

- $next\_state(s, \alpha) \ni s'$, если и только если $\exists \beta \in O^*$ $[(s, \alpha, \beta, s') \in h_S]$,
- $next\_state(b, \alpha) = \cup_{s \in b}\, next\_state(s, \alpha)$.

Далее мы распространяем хорошо известные бинарные отношения на множестве состояний автомата [1] на отношения между подмножествами состояний.

Состояние s полностью определенного автомата $\mathsf{S} = (S, I, O, h_S, S')$ и состояние p полностью определенного автомата $\mathsf{P} = (P, I, O, h_P, P')$ называются *эквивалентными*, если для любой входной последовательности α имеет место $out(s, \alpha) = out(p, \alpha)$. Подмножества состояний m автомата S и b автомата P называются *эквивалентными*, если для любой входной последовательности α имеет место $out(m, \alpha) = out(b, \alpha)$. Автоматы S и P *эквивалентны*, если для каждого состояния множества S' в множестве P' существует эквивалентное состояние, и обратно. Автоматы S и P *слабо эквивалентны*, если множества S' и P' эквивалентны. Известно [2], что для любого недетерминированного автомата S существует эквивалентный наблюдаемый автомат. Наблюдаемая форма строится на основе детерминизации соответствующего полуавтомата. Кроме того, известно [3], что для полностью определенного автомата $\mathsf{S} = (S, I, O, h_S, S')$ можно построить слабо эквивалентный инициальный наблюдаемый автомат, т.е. такой автомат Q, что пара α/β есть входо-выходная последовательность автомата Q в начальном состоянии, если и только если α/β есть входо-выходная последовательность автомата S в одном из состояний множества S'.

Подмножество состояний m автомата S называется *разделимым*, если существует входная последовательность α, которая является *разделяющей последовательностью* для любых двух различных состояний s_1 и s_2 множества m, т.е. справедливо $out(s_1, \alpha) \cap out(s_2, \alpha) = \varnothing$. Отметим, что в общем случае последовательность α должна разделять любые два непересекающихся подмножества состояний множества m, однако в данной статье мы рассматриваем только наблюдаемые автоматы, поэтому введенное определение корректно. Если состояния разделимого множества m разделимы одним входным символом, то множество m также называть 1-*условно-различимым* множеством.

Пусть определены все максимальные $(k-1)$-условно-различимые подмножества, $k > 0$. Будем говорить, что m есть k-*условно-различимое* множество состояний, $k > 1$, если m есть $(k-1)$-условно-различимое множество или существует входной символ $i \in I$, такой, что для любого $o \in O$ множество i/o-преемников состояний из m пусто, содержит одно состояние или является $(k-1)$-условно-различимым множеством, причем в последних двух случаях любые два различные состояния из m не могут обладать одним и тем же i/o-преемником. Множество m называется *условно-различимым*, если m есть k-условно-различимое множество для некоторого k.

2. Различающие эксперименты с недетерминированными автоматами

Как обычно, под различающим экспериментом с (недетерминированным) полностью определенным автоматом понимается эксперимент, позволяющий определить состояние автомата до эксперимента. В предыдущем разделе были введены два понятия различимости для подмножеств состояний автомата S. В работах [4, 5] установлены необходимые и достаточные условия для различимости пары начальных состояний безусловным и условным экспериментами, и в этой работе мы расширяем эти результаты на произвольное множество начальных состояний недетерминированного автомата.

2.1 Безусловные различающие эксперименты

Для построения входной последовательности, разделяющей состояния разделимого множества состояний, можно воспользоваться следующим алгоритмом:

Алгоритм 1. Построение разделяющей последовательности для множества начальных состояний

Вход: Полностью определенный наблюдаемый автомат S = (S, I, O, h_S, S').

Выход: Входная последовательность, разделяющая состояния множества S', если S' – разделимое подмножество, или ответ «S' не является разделимым».

Шаг 1. Строим усеченное дерево преемников для автомата S. Вершина дерева, которая находится на нулевом уровне (корень дерева), помечается множеством, которое состоит из всех пар различных состояний вида $\overline{s_p, s_q}$, $s_p, s_q \in S'$; вершины дерева помечаются множествами, состоящими из пар состояний множества S. Пусть уже построены j уровней дерева, $j \geq 0$. Из нетерминальной вершины j-го уровня, помеченной множеством P пар состояний, есть ребро, помеченное входным символом i, в вершину, которая помечена множеством пар Q: пара $\overline{s_p, s_q} \in Q$, если существует выходной символ o, такой, что s_p и s_q суть i/o-преемники состояний из некоторой пары множества P. Вершина *Current* на k-м уровне, $k \geq 0$, помеченная множеством P пар состояний, является *листом* дерева, если для нее выполняется одно из условий:

Правило 1: Существует входной символ i, который разделяет каждую пару состояний в множестве P.

Правило 2: На j-м уровне j, $j < k$, существует вершина, помеченная множеством $R \subset P$.

Правило 3: Множество P содержит пару вида $\overline{s_p, s_p}$.

Шаг 2. Если все пути на шаге 1 заканчиваются с использованием правил 2 и 3, то множество S' не является разделимым множеством, т.е. его состояния не различимы простым безусловным экспериментом. Если некоторый путь на шаге 2 заканчивается применением правила 1, то последовательность αi, где α есть последовательность, помечающая искомый путь, есть последовательность, разделяющая состояния множества S'.

Теорема 1. Алгоритм 1 доставляет разделяющую последовательность αi, если и только если S' – разделимое множество и αi является разделяющей последовательностью для любых двух различных состояний множества S'.

Доказательство. $\Leftarrow$ Пусть алгоритм 1 доставляет разделяющую последовательность αi. По построению, если путь из корня дерева в вершину, помеченную множеством P, которое не содержит одноэлементных множеств, помечен последовательностью α, то множество P содержит все пары состояний автомата S, такие, что для каждой пары из P существует входо-выходная последовательность α/β, по которой эта пара достижима из некоторой пары начальных состояний. Поэтому, если существует входной символ i, который разделяет каждую пару состояний в множестве P, последовательность разделяет каждую пару различных начальных состояний. Таким образом, если алгоритм 1 доставляет разделяющую последовательность, то S' является разделимым множеством.

$\Rightarrow$ Предположим, что для разделимого множества S' с кратчайшей разделяющей последовательностью αi все пути в алгоритме 1 заканчиваются с использованием правил 2 и 3. Соответственно последовательность α не помечает ни один путь из корня дерева (иначе бы некоторый путь в дереве заканчивался с применением правила 1). Рассмотрим самый длинный префикс β последовательности α, $\alpha = \beta\gamma i$, который помечает путь из корня дерева в некоторую терминальную вершину. Этот путь не может заканчиваться с применением правила 3, так как в этом случае любое продолжение β не является разделяющей последовательностью. Пусть путь, помеченный последовательностью β, заканчивается в вершине на k-м уровне, $k > 0$, с множеством P пар состояний с применением правила 2. Последнее означает, что существует другой путь в дереве, помеченный последовательностью μ, в некоторую вершину на j-м уровне j, $j < k$, помеченную множеством $R \subset P$. Поскольку последовательность γi разделяет все пары множества P, то γi разделяет и все пары подмножества R, т.е. последовательность $\mu\gamma i$, которая короче последовательности αi, является разделяющей для множества S', что противоречит тому, что αi была выбрана как кратчайшая последовательность с таким свойством.

Пример. Рассмотрим автомат S = ({1, 2, 3, 4}, {a, b}, {0, 1}, h_S, {1, 2, 3}), представленный на рис. 1, на котором также приведено усеченное по алгоритму 1 дерево преемников для этого автомата. Поскольку все пути в этом дереве заканчиваются с применением правил 2 и 3, множество {1, 2, 3} не является разделимым и, следовательно, начальные состояния автомата S неразличимы безусловным экспериментом.

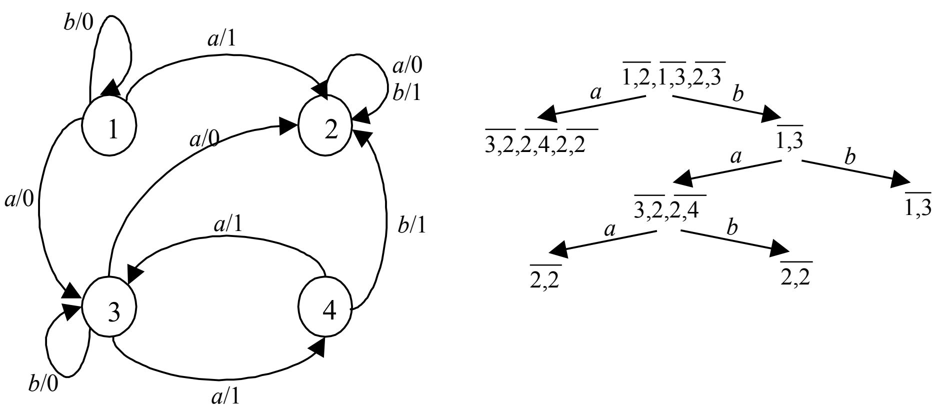

Рис. 1. Автомат, начальные состояния которого не различимы безусловным экспериментом, и его усеченное дерево преемников

Заметим, что для наблюдаемого автомата $\mathcal{S} = (S, I, O, h, S')$ с n состояниями и m начальными состояниями длина кратчайшей разделяющей последовательности не превосходит величины $2^{C_n^2 - C_m^2}$. Причиной является тот факт, что длина разделяющей последовательности ограничивается длиной пути в усеченном дереве преемников, которая, в свою очередь, согласно правилу 2, не превосходит числа множеств, не содержащих множество всех пар различных начальных состояний. Число таких подмножеств пар состояний равно $2^{C_n^2 - C_m^2}$. Как известно [4], для автомата с n состояниями, два из которых являются начальными, для любого $n \geq 2$ можно построить автомат, в котором кратчайшая входная последовательность, разделяющая начальные состояния, имеет длину $2^{\frac{n^2}{4} - 1}$, и, таким образом, безусловные различающие эксперименты с неинициальными автоматами имеют экспоненциальную сложность.

Если множество начальных состояний неинициального автомата не является разделимым, то в ряде случаев состояния этого множества можно различить посредством условного эксперимента.

2.2 Условные различающие эксперименты с недетерминированными автоматами

В этом разделе мы показываем, что состояния множества m различимы условным экспериментом, если m является условно-различимым множеством, т.е. если существует такое целое неотрицательное число k, что m есть k-условно-различимое множество состояний. Поскольку число состояний n автомата $\mathcal{S}$ конечно, то число k не превышает $2^n - 1$, т.е. проверка множества начальных состояний автомата на различимость может быть осуществлена конструктивно, за конечное число шагов.

Частичный наблюдаемый автомат $\mathsf{R} = (R, I, O, T_R, r_0)$ со специальными состояниями $\perp_1, \ldots, \perp_k$ называется *различающим* для автомата $\mathsf{S} = (S, I, O, h, S')$, если выполняются следующие условия:

1. Граф переходов автомата R ациклический.
2. Состояния $\perp_1, \ldots, \perp_k$ тупиковые.
3. Если $r \notin \{\perp_1, \ldots, \perp_k\}$, то в состоянии r определен переход в точности по одному входному символу i.
4. Для любого $j = 1, \ldots k$ все тупиковые состояния пересечения $\mathcal{S}/s_j \cap \mathcal{R}$ являются парами вида $(s, \perp_j)$, $s \in S$, и для любого нетупикового состояния sr пересечения $\mathcal{S}/s_j \cap \mathcal{R}$ и входного символа i, по которому определен переход в состоянии r автомата $\mathcal{R}$, пересечение $\mathcal{S}/s_j \cap \mathcal{R}$ в состоянии sr содержит каждую входо-выходную пару i/o автомата $\mathcal{S}$ в состояния s.

По определению различающего автомата справедливо следующее утверждение.

Предложение 1. Начальные состояния автомата различимы условным экспериментом, если и только если для автомата $\mathsf{S} = (S, I, O, h, S')$ существует различающий автомат.

Действительно, свойства 1 – 3 определяют условный эксперимент с автоматом S, а свойство 4 является необходимым и достаточным для того, чтобы такой эксперимент различал начальные состояния автомата S. ■

В работе [4] показано, как построить r-различающий автомат для двух наблюдаемых инициальных автоматов, которые являются r-различимыми. Ниже мы предлагаем алгоритм построения такого различающего автомата для случая, когда автомат имеет k начальных состояний, $k \geq 2$.

Алгоритм 2. Построение различающего автомата для произвольного множества начальных состояний.

Вход: Полностью определенный наблюдаемый автомат $\mathsf{S} = (S, I, O, h, S')$, $|S'| = k$.

Выход: Автомат R, различающий состояния множества S', если S' – условно-различимое множество, или сообщение о том, что S' не является условно-различимым множеством.

Строим автомат $\mathsf{R} = (R, I, O, h_R, r_0)$: состояниями автомата R являются непустые подмножества состояний автомата S и состояния $\perp_1, \ldots, \perp_k$; начальное состояние r_0 автомата R есть подмножество S'

$R := \{S', \perp_1, \ldots, \perp_k\}$; $h_R := \varnothing$; $k := 1$;

Шаг 1. Если в автомате не существует ни одного разделимого множества мощности 2,
то выдать сообщение «S' не является условно-различимым подмножеством» и END
Иначе найти все k-условно-различимые подмножества.

Шаг 2. Если S' является k-условно-различимым множеством, то
для каждого j- условно-различимого подмножества P ($j > 1$)
определить входной символ $i \in I$, такой, что для любого $o \in O$ множество i/o-преемников состояний из P пусто, содержит одно состояние или является $(j-1)$-условно-различимым множеством P', причем любые два различные состояния из P не обладают одним и тем же i/o-преемником;
добавить в R каждый переход (P, i, o, P'), $|P'| > 1$;
Для каждого начального состояния $s_j \in S'$
построить пересечение $\mathsf{S}/s_j \cap \mathsf{R}$;
Для каждого состояния (s, P) пересечения $\mathsf{S}/s_j \cap \mathsf{R}$, достижимого из начального состояния по некоторой входо-выходной последовательности
Если (s, P) – тупиковое состояние пересечения,
определить входной символ $i_s \in I$, такой, что для любого $o \in O$ в автомате R множество i/o-преемников состояний из P пусто или содержит одно состояние;
Иначе, обозначить через i_s входной символ, по которому определен переход из состояния (s, P)
Для каждой входо-выходной пары i_s/o в состоянии s, по которой нет перехода в состоянии (s, P) пересечения $\mathsf{S}/s_j \cap \mathsf{R}$ добавить в R переход $(P, i_s, o, \perp_j)$;
Удалить из R состояния, недостижимые из начального состояния

END

Если все k-условно-различимые подмножества являются $(k-1)$-условно-различимыми, то выдать сообщение «S' не является условно-различимым подмножеством» и END
Иначе, увеличить k на 1, и перейти на Шаг 1. ■

Теорема 2. Алгоритм 2 доставляет автомат R, различающий состояния множества S', если и только если S' – условно-различимое множество.

Действительно, если S' есть условно-различимое множество, т.е. S' есть k-условно-различимое множество для некоторого k, алгоритм 2 строит автомат R, который переходит в тупиковое состояние $\perp_j$, если и только если начальное состояние автомата S есть s_j (шаг 2). С другой стороны, если S' не является условно-различимым множеством, то алгоритм 2 формирует соответствующее сообщение, и автомат R не строится. ■

По правилам построения различающего автомата можно показать, что подобно автомату с двумя начальными состояниями [5], если множество S' не является k-условно-различимым для некоторого k, то для автомата S нельзя построить различающий автомат, т.е. не существует условного эксперимента, который различает начальные состояния автомата S (предложение 1).

Как известно [5], если автомат имеет n состояний, два из которых являются начальными, то для любого n можно построить условный эксперимент, в котором входная последовательность, различающая два начальных состояния (если существует), имеет длину порядка n^2, и, таким образом, условные различающие эксперименты с неинициальными автоматами с двумя начальными состояниями имеют полиномиальную сложность.

Для k начальных состояний сложность условного эксперимента оценивается суммой числа сочетаний из k по 2, 3, …, k. Поэтому при $k = n$, где n – число состояний неинициального автомата, сложность условного эксперимента не более $2^k - k - 1$. Требуются дополнительные исследования, чтобы выяснить, является ли такая оценка точной или может быть уменьшена.

Пример. Рассмотрим автомат S на рис. 1. Построим различающий автомат по алгоритму 2 для множества начальных состояний {1, 2, 3} (рис. 2).

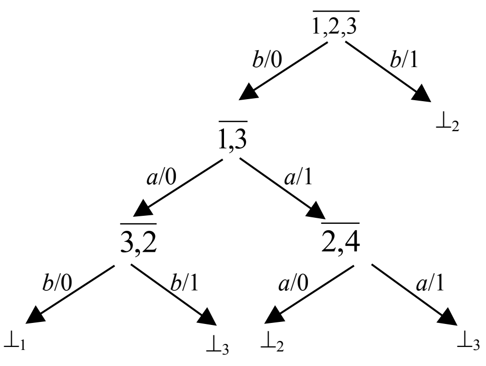

Рис. 2. Различающий автомат для автомата *A*

Таким образом, начальные состояния автомата S (рис. 1), неразличимые безусловным экспериментом, различимы условным экспериментом. Заметим, что если в автомате S каждое состояние может быть начальным, то начальные состояния такого автомата неразличимы и условным экспериментом, так как множество {1, 2, 3, 4} не является условно-различимым множеством. В частности, общую полностью определенную редукцию имеют множества {1, 2, 3} и {4}.

Заключение

В данной статье рассмотрена проблема различимости состояний неинициальных недетерминированных автоматов. Показано, что начальные состояния полностью определенного наблюдаемого автомата различимы безусловным экспериментом, если и только если множество начальных состояний является разделимым. Для того чтобы начальные состояния автомата можно было различить посредством условного эксперимента, необходимо и достаточно, чтобы множество начальных состояний было условно-различимым. Полученные результаты можно использовать при распознавании наблюдаемых недетерминированных автоматов в классе из $l \geq 2$ автоматов, если построить безусловный или условный эксперимент для прямой суммы распознаваемых автоматов. В статье приводятся верхние оценки высоты условного и безусловного экспериментов для наблюдаемых полностью определенных недетерминированных автоматов, однако анализ точности этих оценок требует дополнительных исследований.

ЛИТЕРАТУРА

1. *Евтушенко Н.В.*, *Петренко А.Ф.*, *Ветрова М.В.* Недетерминированные автоматы: анализ и синтез. Ч. 1. Отношения и операции: учеб. пособие. Томск: ТГУ, 2006. 142 с.
2. *Starke P.* Abstract automata. American Elsevier, 1972. 419 с.
3. *Трахтенброт Б.А.* Конечные автоматы: анализ и синтез. М.: Наука, 1970. 400 с.
4. *Spitsyna N.*, *El-Fakih K.*, *Yevtushenko N.* Studying the separability relation between finite state machines software testing // Verification and Reliability. 2007. V. 17(4). P. 227–241.
5. *Громов М.Л.* Разработка методов синтеза условных тестов для автоматных моделей с недетерминированным поведением: дис. ... канд. физ.-мат. наук. Томск: ТГУ, 2009.

Громов Максим Леонидович
Кушик Наталья Генадьевна
Евтушенко Нина Владимировна
Томский государственный университет
E-mail: gromov@sibmail.com; kushiknatalya@yahoo.com;
ninayevtushenko@yahoo.com

Поступила в редакцию 20 июля 2011 г.