О восстановлении разбиения безопасности

А. В. Галатенко

В работе рассматривается автоматная система, часть состояний которой объявляется безопасной. Исследуется сложность восстановления разбиения множества состояний для безопасных и ε-безопасных языков, введенных в работе [1] «Автоматные модели защищенных компьютерных систем».

Ключевые слова: конечный автомат, автоматная модель, кратный условный эксперимент.

1. Основные понятия и результаты

Под конечным автоматом мы будем понимать четверку $V = (A, Q, \varphi, q_0)$, где A — конечное множество входных символов, Q — конечное множество состояний, $\varphi : A \times Q \to Q$ — функция переходов, $q_0 \in Q$ — начальное состояние. Пусть $Q = S \cup I$, причем $S \cap I = \varnothing$. Состояния из S назовем безопасными, состояния из I — небезопасными. Далее будем предполагать, что начальное состояние является безопасным, все состояния достижимы из начального, а $|Q| > 1$.

Обозначим через A^* множество всех конечных слов в алфавите A. Функция φ может быть продолжена на множество $A^* \times Q$ по мультипликативности.

Подмножество A^* называется языком. Каждому слову $\alpha \in A^*$ соответствует слово $\kappa(\alpha) \in Q^*$, $\kappa(\alpha) = \varphi(\alpha, q_0)$. Назовем слово $\alpha \in A^*$ безопасным, если $\kappa(\alpha) \in S^*$. Назовем язык $\mathcal{A} \subseteq A^*$ безопасным (S-языком), если все слова, составляющие $\mathcal{A}$, безопасны, и не существует безопасных слов, не принадлежащих $\mathcal{A}$.

Решается следующая задача. Пусть известны A, Q, φ и q_0. Пусть имеется оракул $\psi : A^* \to \{0,1\}$, для каждого входного слова $\alpha \in A^\times$ выдающий 1 в том и только том случае, когда α безопасно. Так как все безопасные языки являются регулярными ([1]) и в силу теоремы Клини ([2]), $\psi(\alpha, q_0)$ может быть реализован автоматно. Для этого в качестве состояний следует рассматривать пары (q, ind), где $q \in Q$, а $ind = 1$, если слово принадлежит безопасному языку, и $ind = 0$ в противном случае. В начальный момент времени $ind = 1$. В момент времени $t+1$ $ind = 0$ тогда и только тогда, когда либо $ind = 0$ в момент времени t, либо когда первая компонента состояния в момент времени $t+1$ не принадлежит S. Добвавив к автомату выходную функцию ψ, значения которой в момент t совпадают с ind в момент времени $t+1$. Для простоты изложения мы будем рассматривать только первую компоненту состояний и считать ψ оракулом. В этом случае можно считать, функция выхода автомата V является индикатором того, что очередное состояние принадлежит S, а выходное слово дополнительно обрабатывается автоматом, выход которого принимает значение 1 тогда и только тогда, когда все входные буквы равнялись 1. Без ограничения общности будем считать, что все состояния из S достижимы из начального состояния по путям, содержащим только состояния из S. Требуется восстановить разбиение множества Q на S и I с помощью кратного условного эксперимента, подав минимальное количество входных слов или входные слова минимальной суммарной длины.

Рассмотрим алгоритм, в процессе которого на вход автомату V подается заданное множество входных слов, просматриваются значения функции выхода и восстанавливается разбиение Q на S и I. Обозначим через $N(V)$ наименьшее число подаваемых на вход слов, а через $NL(V)$ — наименьшую суммарную длину слов. Справедливо следующее утверждение.

Лемма 1. *$N(V) \geqslant 1$, $NL(V) \geqslant 1$, и эти оценки неулучшаемы.*

Определим функции Шеннона $L(n)$ и $LL(n)$ следующим образом: $L(n) = \max\limits_{\{V:|Q|=n\}}(N(V))$, $LL(n) = \max\limits_{\{V:|Q|=n\}}(NL(V))$.

Теорема 1. *Если мощность входного алфавита неограничена, то* $L(n) = n - 1$*; если* $|A| = k \geqslant 2$*, то* $L(n) = (n-1) - [\frac{n-2}{k}]$*. Если мощность входного алфавита неограничена, то* $LL(n) = \frac{n^2}{4}$ *при четных* n*,* $LL(n) = \frac{(n-1)^2}{4}$ *при нечетных* n*; если мощность входного алфавита ограничена и больше или равна 2, то* $\frac{n^2}{6} \leqslant LL(n) \leqslant \frac{n^2}{4}$*.*

Напомним введенное в [1] понятие ε-безопасности. Рассмотрим произвольное $\varepsilon > 0$. Введем функции $s : Q^* \to \mathbb{N} \cup \{0\}$ и $i : Q^* \to \mathbb{N} \cup \{0\}$ следующим образом. Пусть $\kappa \in Q^*$. Функция $s(\kappa)$ равняется числу букв κ, содержащихся в S, $i(\kappa)$ равняется числу букв κ, содержащихся в I. Обозначим через $|\kappa|$ число букв в слове κ. Назовем слово κ ε-безопасным, если $\frac{i(\kappa)}{|\kappa|} \leqslant \varepsilon$. Назовем язык $\mathcal{A}$ ε-безопасным (S_ε-языком), если все слова из $\mathcal{A}$ ε-безопасны, и не существует ε-безопасных слов, не принадлежащих $\mathcal{A}$. Отметим, что можно рассматривать и $\varepsilon = 0$; в этом случае получим безопасные языки.

Рассмотрим задачу восстановления параметров ε-безопасности. Будем считать, что имеется оракул $\psi : A^* \to \{0, 1\}$, представляющий собой индикатор ε-безопасности, то есть принимающий значение 1 тогда и только тогда, когда $\frac{i(\kappa)}{|\kappa|} \leqslant \varepsilon$. Вообще говоря, оракул не является автоматным, например, в силу того, что ε-безопасные языки могут быть нерегулярными ([1]). Пусть известно разбиение множества состояний Q на S и I, а значение ε неизвестно. Будем говорить, что ε_1 эквивалентно ε_2, если ε_1- и ε_2-безопасные языки совпадают. Легко увидеть, что введенное отношение действительно является эквивалентностью. Требуется восстановить значение ε с точностью до класса эквивалентности, подавая на вход автомату V конечное число слов из $A^\times$ и анализируя выход, или, другими словами, восстановить распознаваемый автоматом ε-безопасный язык.

Рассмотрим множество Δ значений $\frac{i(\kappa)}{|\kappa|}$ на всех словах из $A^\times$. Пусть $\delta \in \mathbb{Q}$, $0 \leqslant \delta \leqslant 1$. Скажем, что δ принадлежит спектру автомата V, если δ является предельной точкой множества Δ, то есть в любой проколотой окрестности δ найдется хотя бы одна точка из Δ.

Спектр автомата может быть охарактеризован в терминах диаграммы Мура.

Теорема 2. *Пусть $\delta \in \mathbb{Q}$, $0 \leqslant \delta \leqslant 1$, V — автомат. Тогда δ принадлежит спектру V тогда и только тогда, когда выполнено хотя бы одно из следующих условий.*

1. *В диаграмме Мура V есть циклы C_1 и C_2, причем доля небезопасных состояний C_1 меньше δ, доля небезопасных состояний C_2 больше δ, и существует путь из C_1 в C_2 или из C_2 в C_1.*
2. *В диаграмме Мура V есть цикл C, в котором доля небезопасных состояний равна δ, $0 < \delta < 1$.*
3. *$\delta = 0$, в диаграмме Мура V есть цикл C, в котором все состояния безопасны, и существует путь, соединяющий C с некоторым небезопасным состоянием.*
4. *$\delta = 1$, в диаграмме Мура V есть цикл C, в котором все состояния небезопасны, и существует путь, соединяющий C с некоторым безопасным состоянием, при этом безопасное состояние не является первым в этом пути.*

Следствие 1. *Существует алгоритм, по диаграмме Мура автомата и разбиению множества состояний строящий спектр.*

Следствие 2. *Спектр любого автомата непуст тогда и только тогда, когда в диаграмме Мура существует путь, начинающийся с начального состояния и содержащий по крайней мере одну небезопасную вершину и одну безопасную вершину, не являющуюся первым элементом пути.*

Теорема 3. *Задача восстановления параметров ε-безопасности не может быть решена с помощью конечного эксперимента, если одновременно не выполнены следующие два условия:*

1) ε не принадлежит спектру автомата V;

2) $\varepsilon = 1$, и не существует перехода из начального состояния в небезопасное состояние по слову длины 1.

Задача может быть решена с помощью конечного эксперимента, если выполнено хотя бы одно из следующих условий:

1) задано $\nu > 0$, такое что ε удалено от спектра автомата V не менее, чем на ν;

2) $\varepsilon = 1$, и не существует перехода из начального состояния в небезопасное состояние по слову длины 1.

Автор выражает глубокую благодарность своему научному руководителю, д.ф.-м.н., проф. В. Б. Кудрявцеву за постановки задач и внимание к работе.

2. Доказательства утверждений

2.1. Доказательство леммы 1

Для восстановления множества S необходимо проверить, есть ли переходы из начального состояния в состояния множества S. Для этого на вход необходимо подать по крайней мере одну букву, следовательно $N(V) \geqslant 1$, $NL(V) \geqslant 1$. Покажем, что оценка неулучшаема. Рассмотрим автомат с диаграммой Мура, изображенной на рис. 1. Пусть множество S состоит только из начального состояния q_0. Чтобы восстановить такое разбиение, на вход достаточно подать произвольную букву. Лемма доказана.

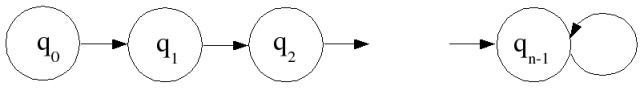

Рис. 1. Диаграмма автомата, на котором достигается нижняя оценка в лемме 1.

2.2. Вспомогательные утверждения

Лемма 2 (о максимальном числе листьев). *Рассмотрим дерево с корнем, содержащее n вершин, $n > 1$. Если степень вершин неограничена, дерево содержит не более $n-1$ листьев (корень не считается листом), и эта оценка достижима. Если степень вершин ограничена константой $k \in \mathbb{N}$, дерево содержит не более $(n-1) - [\frac{n-2}{k}]$ листьев, и эта оценка достижима.*

Доказательство. Пусть степень вершин неограничена. Так как корень дерева не считается листом, число листьев не превосходит общего числа вершин минус 1. Оценка достигается на дереве из двух ярусов (рис. 2).

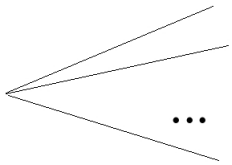

Рис. 2. Дерево из двух ярусов.

Пусть степень вершин ограничена константой k. Покажем, что в этом случае максимальное число листьев имеет равномерно загруженное дерево, определяемое следующим образом:

1) все вершины, кроме, может быть, вершин предпоследнего яруса, имеют степень k;
2) На предпоследнем ярусе все вершины, кроме, может быть, одной, имеют степень k.

Действительно, рассмотрим произвольное дерево T, не являющееся равномерно загруженным. Если не выполнено условие 1, построим дерево T_1 следующим образом. Рассмотрим недогруженную вершину. Если она является листом, перевесим в нее поддерево с предпоследнего яруса. При этом число листьев не изменится. Если вершина не является листом, перевесим произвольное ребро с предпоследнего яруса. При этом число листьев не уменьшится. Будем последовательно строить деревья T_i, пока все вершины нижних ярусов не окажутся полностью загруженными. На последнем этапе будем последовательно перевешивать ребра на предпоследнем ярусе, догружая недогруженные вершины. При этом число листьев не будет уменьшаться, так как при каждом таком преобразовании удаляется один лист, а добавляется — один или два. Учитывая, что на каждом шаге число листьев не уменьшалось, а на выходе получилось равномерно загруженное дерево, получаем искомое утверждение.

Покажем по индукции, что число $T(n)$ листьев равномерно загруженного дерева с n вершинами равна $(n-1)-[\frac{n-2}{k}]$. При $n=2$ равенство очевидно. Пусть утверждение истинно для всех n, не превосходящих некоторого $N \in \mathbb{N}$. Покажем, что равенство справедливо при $n = N+1$. Возможны два случая. Если одна из вершин предпоследнего яруса равномерно загруженного дерева с N вершинами недогружена, то $T(N+1) = T(N)+1$, в противном случае $T(N+1) = T(N)$. Легко увидеть, что второму случаю соответствуют значения N вида $1+C\times k$ для некоторого натурального C. В первом случае $T(N+1) = T(N)+1 = (N-1)-[\frac{N-2}{k}]+1 = ((N+1)-1)-[\frac{N-1}{k}]$, так как N отличен от 1 по модулю k, а целая часть увеличивается, когда $N-1$ кратно k. Во втором случае $T(N+1) = T(N) = (N-1)-[\frac{N-2}{k}] = (N+1-1)-[\frac{N-2}{k}+1]$. Так как $N = 1+C\times k$, $[\frac{N-2}{k}+1] = [\frac{N-1}{k}]$. Лемма доказана.

Рассмотрим дерево T с корнем с n вершинами. Обозначим через $C(T)$ суммарную длину всех цепей, начинающихся от корня и заканчивающихся в листьях.

Лемма 3 (о длине цепей). *Для любого n существует бинарное дерево с корнем и n вершинами, для которого $C(T) > \frac{n^2}{6}$.*

Доказательство. Рассмотрим класс деревьев, изображенный на рис. 3. Пусть $n-l$ четно. Для дерева $T(n)$ с n вершинами имеем: $C(T(n)) = (l+1)+(l+2)+\ldots+(l+(\frac{n-l}{2})) = \frac{n-l}{4}\times(2l+\frac{n-l}{2}+1) = -\frac{3}{8}(l^2-2l(\frac{n-1}{3})-\frac{n^2+2n}{3})$. Рассмотрим значение l, при котором $C(T(n))$ максимально. Так как выражение представляет собой квадратичную по l функцию с отрицательным старшим коэффициентом, максимум достигается при $l = \frac{n-1}{3}$. Учитывая симметрию, монотонность левой ветви параболы, тот факт, что ровно одно из чисел $\{\frac{n-2}{3}, \frac{n-1}{3}, \frac{n}{3}\}$ является целым, и соображение, что для обеспечения четности $n-l$ из l, возможно, придется вычесть еще 1, получаем, что максимальное значение $C(T(n))$ не меньше значения, получаемого подстановкой вместо l значения $\frac{n}{3}-1$, то есть $C((T(n)) \geqslant \frac{n^2}{6}+\frac{n}{6}+\frac{9}{12} > \frac{n^2}{6}$. Последнее неравенство доказывает лемму.

Лемма 4 (о максимальных цепях). *Рассмотрим дерево с n вершинами. Суммарная длина простых цепей от корня к листьям не*

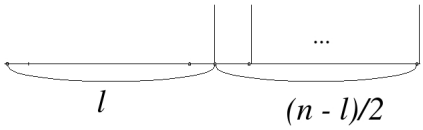

Рис. 3. Класс деревьев для доказательства леммы о длине цепей.

превосходит $\frac{n^2}{4}$ *при четных* n *и* $\frac{(n-1)^2}{4}$ *— при нечетных* n*, при этом обе оценки достигаются.*

Доказательство. Покажем, что достаточно рассматривать деревья, изображенные на рис. 4. Действительно, рассмотрим произвольное дерево с n вершинами. Пусть k — максимальная длина простой цепи от корня к листьям. Обозначим цепь максимальной длины через γ. Будем последовательно выполнять следующее преобразование. Будем перевешивать листья, не прикрепленные к предпоследней вершине γ N, к N. В силу того, что длина γ максимальная, в результате суммарная длина цепей не уменьшится, так как в результате преобразования исчезнет цепь длины, не превосходящей k, и появится цепь длины k.

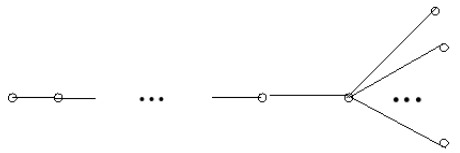

Рис. 4. Класс деревьев для доказательства леммы о максимальных цепях.

Посчитаем суммарную длину простых цепей в получившемся дереве. Во всех ярусах, исключая последний, оказывается k вершин, следовательно, в дереве имеется $n-k$ листьев, а суммарная длина равна $k(n-k)$. Максимум достигается при $k=\frac{n}{2}$ и равен $\frac{n^2}{4}$. Если n нечетно, максимум достигается при $k=\frac{n-1}{2}$ и равен $\frac{(n-1)^2}{4}$. Так как оценки построены конструктивно, они достигаются на деревьях

из класса на рис. 4 с соответствующими значениями k. Лемма доказана.

Лемма 5 (о склеивании значений ε). *Пусть $\varepsilon_1, \varepsilon_2 \in \mathbb{Q}$, $0 \leqslant \varepsilon_1 < \varepsilon_2 < 1$, таковы, что для некоторого натурального n не существует таких $p, q \in \mathbb{N}$, $p, q \leqslant n$, что $\varepsilon_1 \leqslant \frac{p}{q} < \varepsilon_2$. Тогда ε_1 и ε_2 безопасные подъязыки, содержащие слова длины не более n, совпадают для любого автомата V и любого разбиения.*

Доказательство. Предположим противное. Пусть существует автомат V и разбиение множества его состояний на S и I, при котором существует слово α длины, не превосходящей n, являющееся ε_2-безопасным и не являющееся ε_1-безопасным (обратный случай, очевидно, невозможен). Пусть длина α равна q, число состояний из множества I равно p. Из построения ясно, что $p, q \leqslant n$. Из ε_2-безопасности α следует, что $\frac{p}{q} > \varepsilon_2$, из ε_1-небезопасности — что $\frac{p}{q} \leqslant \varepsilon_1$. Полученное противоречие доказывает лемму.

2.3. Доказательство теоремы 1

Построим эксперимент следующим образом. Будем подавать на вход слова по одной букве. Подача слова заканчивается, если либо автомат переводится в вершину из множества I (то есть на выход выдается символ 0), либо из состояния, в которое перешел автомат, невозможны переходы в состояния, в которые автомат еще не попадал. Слова подаются, пока есть возможность достичь еще не рассмотренной вершины из множества S, то есть существуют пути в диаграмме Мура, начинающиеся в начальном состоянии, заканчивающиеся в еще не рассмотренном состоянии и содержащие только вершины, про которые либо известно, что они входят в S, либо ничего не известно. Легко увидеть, что в результате в диаграмме Мура автомата будет построено поддерево со следующими свойствами:

1) все вершины из множества S входят в дерево (это следует из достижимости всех состояний множества S из начального по путям, содержащим только состояния из S);
2) вершины из множества I могут входить только в качестве листьев (это следует из построения эксперимента).

Первое свойство гарантирует, что разбиение множества Q будет восстановлено правильно.

В силу леммы о максимальном числе листьев, общее число поданных слов для автомата с n состояниями не превосходит $n-1$, если входной алфавит неограничен, и $(n-1)-[\frac{n-2}{k}]$ — если мощность входного алфавита равна k. Нижняя оценка $L(n)$ следует из рассмотрения автомата, диаграмма Мура которого получается из построенного в доказательстве леммы о максимальном числе листьев в дереве приписыванием произвольных входных символов имеющимся ребрам с условием, что функция переходов сохранит однозначность определения, и добавлением недостающих переходов в виде петель. При этом $S=Q$, то есть дерево включит в себя все n состояний.

В силу леммы о максимальных цепях, верхняя оценка $LL(n)$ справедлива. Нижняя оценка получается из построенных в леммах о максимальных цепях и о длине цепей классов деревьев аналогично оценке $L(n)$. Теорема доказана.

2.4. Доказательство теоремы 2

Покажем, что если выполнено условие 1, то $\delta=\frac{p}{q}$ принадлежит спектру. Без ограничения общности, существует путь из C_1 в C_2, и неравенство для C_1 является строгим. Пусть доля небезопасных состояний в C_1 равна $\frac{p_1}{q_1}$, где q_1 — длина C_1, доля небезопасных состояний в C_2 равна $\frac{p_2}{q_2}$, где q_2 — длина C_2, $\frac{p'}{q'}$ и $\frac{p''}{q''}$ — доли небезопасных состояний в пути, ведущем в C_1 и в пути из C_1 в C_2 соответственно. Рассмотрим последовательность, состоящую из пути в C_1, l_1 обходов C_1, пути в C_2 и l_2 обходов C_2. Рассмотрим последовательность значений $r_{l_1,l_2}=\frac{i(\kappa)}{|\kappa|}=\frac{p'+p''+l_1\times p_1+p_2\times l_2}{q'+q''+l_1\times q_1+l_2\times q_2}$. Рассмотрим произвольное $\gamma>0$. Так как $\frac{p_1}{q_1}<\frac{p}{q}$, а $\lim_{l_1\to\infty} r_{l_1,1}=\frac{p_1}{q_1}$, то существует $L_1\in\mathbb{N}$, что $r_{l_1,1}<\frac{p}{q}$ для всех $l_1\geqslant L_1$. Рассмотрим разность $r_{l_1,l_2+1}-r_{l_1,l_2}$ при $l_1\geqslant L_1$. Легко увидеть, что в этом случае при фиксированном l_1 r_{l_1,l_2} монотонно возрастает по l_2. Действительно, r_{l_1,l_2} можно записать в виде $\frac{a+p_2\times l_2}{b+q_2\times l_2}$. Функция дифференцируема на $\mathbb{R}^+$, и знак производной постоянный, следовательно функция монотонна. При $l_2=1$ значение по построению меньше $\frac{p}{q}$, при $l_2\to infty$ значение стремит-

ся к $\frac{p_2}{q_2} > \frac{p}{q}$, следовательно функция возрастает, и рассматриваемая разность положительна. Оценим ее, заменив в знаменателе первой дроби $l_2 + 1$ на l_2. $r_{l_1,l_2+1} - r_{l_1,l_2} \geqslant \frac{p_2}{q'+q''+l_1\times q_1+l_2\times q_2}$. Выберем L'_1 таким образом, чтобы дробь в правой части оказалась меньше $\frac{\gamma}{2}$ при всех $l_1 \geqslant L'_1$. Обозначим через L максимум из L_1 и L'_1 и рассмотрим последовательность r_{L,l_2}. Первый ее член меньше, чем $\frac{p}{q}$. Так как $\lim_{l_2\to\infty} r_{L,l_2} = \frac{p_2}{q_2} > \frac{p}{q}$, все члены, начиная с некоторого, больше, чем $\frac{p}{q}$. Учитывая, что шаг последовательности меньше $\frac{\gamma}{2}$, получаем, что в проколотой γ-окрестности $\frac{p}{q}$ есть значения $\frac{i(\kappa)}{|\kappa|}$.

Покажем, что если выполнено условие 2, то $\delta = \frac{p}{q}$, где q — длина цикла C, принадлежит спектру. Рассмотрим последовательность, состоящую из пути, ведущего в C (возможно, пустого), и k шагов по циклу C. Легко увидеть, что при стремлении k к бесконечности $\frac{i(\kappa)}{|\kappa|} \to \frac{p}{q}$. Так как δ не равно 0 и 1, для слов, длина которых является простым числом, значения $\frac{i(\kappa)}{|\kappa|}$ получаются несократимые дроби с знаменателями, равными рассматриваемым простым числам, получаем, что в любой проколотой окрестности δ имеются значения $\frac{i(\kappa)}{|\kappa|}$.

Покажем, что если выполнено условие 3, то 0 принадлежит спектру. Действительно, рассмотрим последовательность, состоящую из k обходов цикла C, все состояния которого безопасны, и пути, ведущего в небезопасное состояние. Так как одно из состояний небезопасно, $\frac{i(\kappa)}{|\kappa|} > 0$. Так как число небезопасных состояний конечно, при стремлении k к бесконечности $\frac{i(\kappa)}{|\kappa|}$ будет стремиться к 0.

Покажем, что если выполнено условие 4, то 1 принадлежит спектру. Действительно, рассмотрим последовательность, состоящую из k обходов цикла C, все состояния которого небезопасны, и пути, ведущего в безопасное состояние. Так как одно из состояний безопасно, и входит в состав κ (то есть это не первое вхождение начального состояния), $\frac{i(\kappa)}{|\kappa|} < 1$. Так как число безопасных состояний конечно, при стремлении k к бесконечности $\frac{i(\kappa)}{|\kappa|}$ будет стремиться к 1.

Покажем, что если для $\delta = \frac{p}{q}$ не выполнено ни одно из условий 1–4, то δ не принадлежит спектру. Если $\delta = 1$, то либо все циклы содержат безопасные состояния, либо существуют циклы, состоящие из небезопасны состояний, но все пути, содержащие такие циклы,

состоят только из небезопасных состояний. В первом случае значения $\frac{i(\kappa)}{|\kappa|}$ для всех слов, начиная с некоторой длины, отделены от 1, во втором случае значение 1 является изолированной точкой.

Если $\delta = 0$, то либо все циклы содержат небезопасные состояния, либо существуют циклы, состоящие из безопасных состояний, но все пути, содержащие такие циклы, состоят только из безопасных состояний. В первом случае значения $\frac{i(\kappa)}{|\kappa|}$ для всех слов, начиная с некоторой длины, отделены от 0, во втором случае значение 0 является изолированной точкой.

Рассмотрим случай $\delta \in (0;1)$. Назовем компонентой диаграммы Мура подграф, порожденный множеством циклов. Два цикла попадают в одну компоненту тогда и только тогда, когда в диаграмме Мура есть путь, соединяющий эти циклы. Если $0 < \delta < 1$, то в каждой компоненте либо доля небезопасных состояний во всех циклах больше δ, либо либо доля небезопасных состояний во всех циклах меньше δ. Без ограничения общности рассмотрим первый случай. Пусть $\delta' > \delta$ — минимальная доля небезопасных состояний в циклах компоненты. Минимум существует и достигается на простом цикле, так как цикл, не являющийся простым, можно разделить на простые компоненты, причем минимальная доля небезопасных состояний в простой компоненте будет меньше или равна доли небезопасных состояний большого цикла. Рассмотрим множество частичных пределов $\frac{i(\kappa)}{|\kappa|}$ для данной компоненты. $\frac{\delta'-\delta}{2}$ будет нижней гранью этого множества, так как для всех слов, начиная с некоторой длины, $\frac{i(\kappa)}{|\kappa|} > \frac{\delta'-\delta}{2}$. Следовательно, в $\frac{\delta'-\delta}{2}$-окрестности δ имеется только конечное множество точек множества Δ. Рассматривая поочередно все компоненты, получаем искомое утверждение.

2.5. Доказательство теоремы 3

Пусть $\varepsilon \in \mathbb{Q}$, $0 \leqslant \varepsilon < 1$, принадлежит спектру. Предположим, что существует конечный эксперимент, восстанавливающий параметры безопасности в этом случае. Пусть n — максимальная длина входного слова, поданного в процессе эксперимента. Выберем проколотую окрестность ε, в которой нет рациональных точек вида $\frac{p}{q}$, $p \leqslant n$,

$q \leqslant n$. Выберем два элемента Δ, принадлежащих этой окрестности; обозначим их ε' и ε'', $\varepsilon' < \varepsilon''$. По лемме о склеивании значений ε, результаты эксперимента для ε' и ε'' совпадут. Легко увидеть, что ε'- и ε''-безопасные языки различаются. Действительно, рассмотрим входное слово α, на котором достигается значение ε''. Слово α ε''-безопасно, но не ε'-безопасно. Следовательно, однозначное восстановление параметров невозможно — противоречие.

Пусть $\varepsilon = 1$, и не существует перехода из начального состояние в небезопасное состояние по слову длины 1. Предположим, что существует конечный эксперимент, восстанавливающий параметры безопасности в этом случае. Пусть n — максимальная длина входного слова, поданного в процессе эксперимента. Следовательно, значения $\frac{i(\kappa)}{|\kappa|}$ для поданных слов имеют вид $\frac{p}{q}$, где $p < q$ (так как при переходах на любом входном слове попадаем по крайней мере в одно безопасное состояние), $q \leqslant n$. По теореме 2, в диаграмме Мура есть цикл C, состоящий только из небезопасных состояний, связанный путем P с безопасным состоянием. Пусть такой путь состоит из l_1 безопасных и l_2 небезопасных состояний. Добавим к P k обходов цикла C и обозначим получившийся путь через P_k. Для P_k $\frac{i(\kappa)}{|\kappa|} \to 1$, $k \to \infty$, следовательно, можно выбрать слово, для которого $\frac{i(\kappa)}{|\kappa|} > \frac{n}{n+1}$. Такое слово 1-безопасно, но не $\frac{n}{n+1}$-безопасно, но эксперимент не различает 1- и $\frac{n}{n+1}$-безопасные языки — противоречие.

Рассмотрим следующий эксперимент. Если в диаграмме Мура есть переход из начального состояния в небезопасное по слову длины 1, сначала подадим на вход такое слово. Если оно окажется безопасным, $\varepsilon = 1$, и ε-безопасный язык представляет собой A^*.

Для каждой компоненты диаграммы Мура выделим циклы с минимальной и максимальной долей небезопасных состояний. Обозначим минимальную долю через λ_1, максимальную долю — через λ_2. Будем подавать на вход слова α_k и β_k, соответствующие k шагам обходу минимального и максимального цикла с учетом предпериодов и, возможно, постпериодов. Рассмотрим последовательность α_k; последовательность β_k рассматривается аналогично и подается параллельно с α_k. Постпериод добавляется, если существует такой постпериод, что доля небезопасных состояний в предпериоде и постпериоде боль-

ше доли небезопасных состояний в минимальном цикле, и выбирается минимальным по длине.

Пусть такой постпериод существует. Тогда возможны два случая. Если ε меньше доли небезопасных состояний в минимальном цикле, для некоторых k и $\gamma > 0$ $\frac{i(\kappa)}{|\kappa|}$ для α_k не превосходит доли небезопасных состояний минимального цикла минус γ, но α_k не является безопасным. Учитывая, что во всех словах, содержащихся в рассматриваемой компоненте, длина которых не меньше некоторой константы, доля небезопасных состояний не меньше $\lambda_1 - \gamma$, получаем, что для данной компоненты достаточно проверить принадлежность ε-безопасному языку конечного множества слов, так как остальные слова заведомо не являются ε-безопасными. Предельная длина легко находится по конкретной компоненте диаграммы Мура. Во втором случае, учитывая теорему 2 и проводя аналогичные рассуждения для β_k, получаем, что для восстановления достаточно рассмотреть конечное множество слов, так как более длинные слова заведомо ε-безопасны.

Пусть такого постпериода не существует. Если $\lambda_1 = \lambda_2$, в этом случае рассматриваем последовательность β_k, пока $\frac{i(\kappa)}{|\kappa|} - \lambda_1 \geqslant \nu$, или пока слово не окажется безопасным. Если слово окажется безопасным, значит, все слова с длиной, большей некоторой константы, также безопасны. В противном случае все слова большей длины оказываются небезопасными (в силу условия 2 теоремы). Если $\lambda_1 < \lambda_2$, проводим аналогичные рассуждения с помощью последовательности α_k, выясняя, как соотносится ε с нижней границей, затем рассматриваем верхнюю границу и объединяем результаты. Легко увидеть, что при выполнении условий теоремы построенный эксперимент окажется конечным. Теорема доказана.

Список литературы

[1] Галатенко А. В. Автоматные модели защищенных компьютерных систем // Интеллектуальные системы. Т. 11, вып. 1–4. М., 2007.

[2] Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. М.: Наука, 1985.