Известия вузов. Математика
2009, № 9, с. 36–45

http://www.ksu.ru/journals/izv_vuz/
e-mail: izvuz.matem@ksu.ru

В.Н. САЛИЙ

АВТОМАТЫ, У КОТОРЫХ ВСЕ КОНГРУЭНЦИИ ВНУТРЕННИЕ

Аннотация. Конгруэнция автомата $\mathbf{A}$ называется внутренней, если она является ядром некоторого эндоморфизма автомата $\mathbf{A}$. Предлагается характеризация автоматов, у которых все конгруэнции являются внутренними.

Ключевые слова: автомат, конгруэнция, внутренняя конгруэнция, эндоморфизм.

УДК: 512.5

Abstract. A congruence on an automaton $\mathbf{A}$ is called inner if it is the kernel of a certain endomorphism on $\mathbf{A}$. We propose a characterization of automata, all of whose congruences are inner.

Keywords: automaton, congruence, inner congruence, endomorphism.

Рассматриваются автоматы без выхода. Конгруэнция такого автомата называется внутренней, если она является ядром некоторого его эндоморфизма. В настоящей работе предлагается характеризация автоматов, у которых каждая конгруэнция имеет указанный вид (такие автоматы названы i-автоматами). Основная теорема с помощью естественных для автоматов конструкций дает описание структуры i-автоматов и может служить также эффективным средством проверки принадлежности автомата этому классу (приводится соответствующий пример).

Считая автомат абстрактным представлением некоторой дискретной системы, можно трактовать его гомоморфные образы как в той или иной мере обедненные модели этой системы, сохраняющие те или иные ее функциональные особенности. В системе, представленной i-автоматом, все эти модели реализуются как подсистемы, т. е. воспроизводятся ее внутренними средствами. Системы такого вида представляют несомненный интерес.

Аналогичные вопросы для абелевых групп исследовались в [1], конечных дистрибутивных решеток — в [2] и [3], алгебр Де Моргана — в [3] (здесь при наличии двух сигнатурных констант естественно исключить из рассмотрения универсальную конгруэнцию), частный случай автономных автоматов рассмотрен в [4] (см. также [5]). Результаты автора были анонсированы в сообщении [6]. Алгебраическая теория автоматов трактуется в духе [7] и [5].

Автомат — это тройка $\mathbf{A} = (S, X, \delta)$, где S и X — конечные непустые множества, соответственно множество состояний и множество входных сигналов, а $\delta : S \times X \to S$ — отображение, называемое функцией переходов. Запись $\delta(s, x) = t$ для $s, t \in S$ и $x \in X$ означает, что автомат $\mathbf{A}$, находящийся в состоянии s, под действием входного сигнала x переходит в состояние t.

Поступили: первый вариант 04.05.2005, окончательный вариант 06.07.2007.

Небольшие автоматы удобно задавать диаграммой переходов, которая представляет собой ориентированный мультиграф с множеством вершин S и дугами, помеченными входными сигналами: дуга с меткой x ведет из вершины s в вершину t, если $\delta(s,x)=t$.

Подмножество $S' \subseteq S$ называется устойчивым в автомате $\mathbf{A}$, если $\delta(s,x) \in S'$ для любых $s \in S'$ и $x \in X$. Если S' устойчиво в $\mathbf{A}$, то, ограничивая функцию переходов δ на $S' \times X$, получают автомат $\mathbf{A}' = (S', X, \delta)$ — подавтомат автомата $\mathbf{A}$, соответствующий S'. Совокупность $\operatorname{Sub}\mathbf{A}$ всех подавтоматов автомата $\mathbf{A}$ (сюда включается и нулевой подавтомат $\mathbf{0} = (\emptyset, X, \emptyset)$) упорядочивается отношением $\mathbf{A}_1 \leq \mathbf{A}_2 :\Longleftrightarrow\ S_1 \subseteq S_2$, где $\mathbf{A}_i = (S_i, X, \delta)$, $i=1,2$. Упорядоченное множество $(\operatorname{Sub}\mathbf{A}, \leq)$ является дистрибутивной решеткой. В ней $\mathbf{A}_1 \wedge \mathbf{A}_2 = (S_1 \cap S_2, X, \delta)$ и $\mathbf{A}_1 \vee \mathbf{A}_2 = (S_1 \cup S_2, X, \delta)$.

Следующие алгебраические конструкции и предложения основаны на том очевидном факте, что автомат без выхода, по существу, является конечной унарной алгеброй.

Пусть $\mathbf{A} = (S, X, \delta)$ и $\mathbf{B} = (T, X, \delta)$ — автоматы с одним и тем же множеством входных сигналов (функции переходов всех автоматов будем обозначать символом δ). Отображение $\varphi : S \to T$ по определению является гомоморфизмом $\mathbf{A}$ в $\mathbf{B}$, если $\varphi(\delta(s,x)) = \delta(\varphi(s), x)$ для любых $s \in S$, $x \in X$. Взаимно однозначные гомоморфизмы автоматов называются вложениями, а их биективные гомоморфизмы — изоморфизмами. Эндоморфизмы автомата — это его гомоморфизмы в себя.

Отношение эквивалентности $\theta \subseteq S \times S$ называется конгруэнцией автомата $\mathbf{A} = (S, X, \delta)$, если оно согласовано с функцией переходов в том смысле, что $(\forall s,t \in S)\ (\forall x \in X)\ ((s,t) \in \theta \Rightarrow (\delta(s,x), \delta(t,x)) \in \theta)$. Каждая конгруэнция θ автомата $\mathbf{A}$ определяет его фактор-автомат $\mathbf{A}/\theta = (S/\theta, X, \delta)$, где $\delta(\theta(s), x) := \theta(\delta(s,x))$ для любых $s \in S$, $x \in X$.

Для гомоморфизмов и конгруэнций автоматов справедливы аналоги известных алгебраических теорем: 1) ядро любого гомоморфизма является конгруэнцией, 2) всякая конгруэнция оказывается ядром подходящего гомоморфизма, 3) гомоморфный образ автомата изоморфен его фактор-автомату по ядру соответствующего гомоморфизма.

Конгруэнция автомата называется внутренней, если она является ядром некоторого его эндоморфизма. Очевидно, конгруэнция θ автомата $\mathbf{A}$ будет внутренней тогда и только тогда, когда фактор-автомат $\mathbf{A}/\theta$ вкладывается в $\mathbf{A}$. В общем случае не всякая конгруэнция автомата будет внутренней. Например, если $\mathbf{A}$ не имеет тривиального (т. е. с одним состоянием) подавтомата, то универсальная конгруэнция $S \times S$ не внутренняя.

Автомат называется i-автоматом, если все его конгруэнции внутренние.

Задача описания автономных (т. е. с одним входным сигналом) i-автоматов была решена в [4] (см. также [5], теорема 4.3): автономный автомат является i-автоматом тогда и только тогда, когда среди компонент связности его диаграммы переходов лишь одна не одноэлементна, причем эта компонента представляет собой петлю с входящими в нее цепями, из которых не более чем одна имеет длину, большую 1.

Пусть X^* — множество всех конечных слов над алфавитом X. Продолжим функцию переходов δ на множество $S \times X^*$, полагая $\delta(s,e) = s$, где $e \in X^*$ — пустое слово, и $\delta(s,px) = \delta(\delta(s,p),x)$ для любых $s \in S$, $x \in X$, $p \in X^*$. Говорят, что состояние t достижимо в автомате $\mathbf{A}$ из состояния s, если найдется входное слово $p \in X^*$ такое, что $\delta(s,p) = t$. Записывая это в виде $(s,t) \in \tau$, вводим отношение достижимости τ в $\mathbf{A}$. Понятно, что τ рефлексивно и транзитивно, т. е. является квазипорядком на S. Пусть $s \in S$ — произвольное состояние $\mathbf{A}$. Подмножество $\tau(s)$, объединяющее все состояния, достижимые из s, устойчиво в $\mathbf{A}$ и, следовательно, определяет подавтомат $\mathbf{A}(s) = (\tau(s), X, \delta)$ — главный подавтомат, порожденный состоянием s. Симметричная часть $\sigma = \tau \cap \tau^{-1}$ отношения достижимости называется отношением взаимной достижимости в $\mathbf{A}$. Очевидно, σ будет эквивалентностью на множестве состояний S. Классы этой эквивалентности называют слоями $\mathbf{A}$. Автомат, состоящий из одного слоя, по определению является сильно связным. Тривиальные (т. е. с одним состоянием) автоматы также считаются сильно связными. Сильно связные подавтоматы автомата $\mathbf{A}$ образуют множество всех атомов решетки подавтоматов $\operatorname{Sub}\mathbf{A}$.

Каркасом автомата $\mathbf{A}$ назовем упорядоченное множество $F(\mathbf{A}) = (S/\sigma, \tau^{-1})$. Его элементами являются слои $\mathbf{A}$, а порядком — отношение, обратное достижимости, перенесенное на слои: $(\sigma(t), \sigma(s)) \in \tau^{-1}$ равносильно тому, что $(s, t) \in \tau$. Понятно, что изоморфные автоматы имеют изоморфные каркасы, но обратное, конечно, не верно (например, у всех контуров — одноэлементный каркас). Если $\mathbf{A}$ вложим в автомат $\mathbf{B}$, то каркас $F(\mathbf{A})$ вложим как упорядоченное множество в каркас $F(\mathbf{B})$.

На множестве слоев S/σ автомата $\mathbf{A}$ можно задать некоторую структуру, связанную с функцией переходов этого автомата. Из слоя $\sigma(s)$ в слой $\sigma(t)$ для каждой тройки (s', x, t'), где $s' \in \sigma(s)$, $t' \in \sigma(t)$ и $\delta(s', x) = t'$, проведем дугу с меткой x. Полученный ориентированный мультиграф $DF(\mathbf{A})$ с помеченными дугами назовем динамическим каркасом автомата $\mathbf{A}$. Заметим, что из вершины (слоя) $\sigma(s)$ динамического каркаса $DF(\mathbf{A})$ исходит $|\sigma(s)| \cdot |X|$ помеченных дуг. Понятно, что изоморфные автоматы имеют изоморфные (как орграфы с помеченными дугами) динамические каркасы, но обратное не верно (например, у всех сильно связных автоматов с одинаковым числом состояний m и одинаковым n-буквенным входным алфавитом динамическим каркасом будет единственная вершина с m дугами для каждой из n меток). Если $\mathbf{A}$ вложим в $\mathbf{B}$, то динамический каркас $DF(\mathbf{A})$ вложи́м — как ориентированный мультиграф с помеченными дугами — в динамический каркас $DF(\mathbf{B})$.

Автомат $\mathbf{A}$ называется связным, если его диаграмма переходов связна как ориентированный мультиграф, что равносильно связности в этом смысле динамического каркаса $DF(\mathbf{A})$ и связности каркаса $F(\mathbf{A})$ как упорядоченного множества.

Лемма 1 (о сильно связных подавтоматах)**.** 1) *Все сильно связные подавтоматы i-автомата тривиальны.*

2) *Каждая связная компонента i-автомата содержит единственный сильно связный подавтомат.*

Доказательство. Пусть $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_k$ — нетривиальные сильно связные подавтоматы i-автомата $\mathbf{A} = (S, X, \delta)$ с множествами состояний соответственно $S_1, S_2, \ldots, S_k$.

1) Рассмотрим эквивалентность $\theta \subseteq S \times S$, неодноэлементными классами которой являются в точности подмножества S_i, $1 \leq i \leq k$. Понятно, что θ будет конгруэнцией автомата $\mathbf{A}$. При гомоморфизме одного автомата в другой образом тривиального подавтомата может быть только тривиальный подавтомат. У фактор-автомата $\mathbf{A}/\theta$ таковых больше, чем у автомата $\mathbf{A}$, и потому $\mathbf{A}/\theta$ не вкладывается в $\mathbf{A}$.

2) Пусть $\mathbf{A}'$ — связная компонента i-автомата $\mathbf{A}$ и s'_i, $1 \leq i \leq k$, $k > 1$, — ее сильно связные подмножества (согласно предыдущему все они одноэлементны). Через d_i, $1 \leq i \leq k$, обозначается степень захода вершины s'_i в диаграмме переходов подавтомата $\mathbf{A}'$ без учета петель. Ясно, что $d_i \geq 1$ для любого i, $1 \leq i \leq k$. Эквивалентность $\theta \subseteq S \times S$ с единственным нетривиальным классом $\{s'_1, s'_2, \ldots, s'_k\}$, очевидно, является конгруэнцией $\mathbf{A}$. Автоматы $\mathbf{A}/\theta$ и $\mathbf{A}$ имеют одинаковое число компонент связности. Нетрудно понять, что каждое вложение фактор-автомата $\mathbf{A}/\theta$ в автомат $\mathbf{A}$ индуцирует вложение фактор-автомата $\mathbf{A}'/\theta$ в автомат $\mathbf{A}'$. При этом образом вершины $\theta(s'_1)$ будет одна из вершин $s'_1, s'_2, \ldots, s'_k$, что невозможно, так как $d_i < \sum_{i=1}^{k} d_i$, $1 \leq i \leq k$. □

Лемма 2 (о нетривиальных связных компонентах)**.** *В i-автомате лишь одна связная компонента нетривиальна.*

Доказательство. Заметим сначала, что если $\mathbf{A}$ — автомат с единственным сильно связным подавтоматом $\sigma(s_0)$, то слой $\sigma(s)$ будет атомным в каркасе $F(\mathbf{A})$ в точности тогда, когда все входные сигналы переводят состояния из $\sigma(s)$ в $\sigma(s)$ либо в $\sigma(s_0)$. Отсюда следует, что при вложении автомата $\mathbf{A}$ в автомат $\mathbf{B}$, имеющий также единственный сильно связный подавтомат, атомы каркаса $F(\mathbf{A})$ будут переходить при индуцированном вложении в атомы каркаса $F(\mathbf{B})$.

Пусть теперь $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_k$ — связные компоненты i-автомата $\mathbf{A}$, $\{s_i^0\}$, $1 \le i \le k$, — их сильно связные подмножества. Отношение эквивалентности $\theta \subseteq S \times S$ с единственным неодноэлементным классом $\{s_1^0, s_2^0, \ldots, s_k^0\}$, очевидно, будет конгруэнцией $\mathbf{A}$. Фактор-автомат $\mathbf{A}/\theta$ является связным, и всякое его вложение в автомат $\mathbf{A}$ будет вложением в один из автоматов $\mathbf{A}_i$, $1 \le i \le k$. Если среди $\mathbf{A}_i$, $1 \le i \le k$, есть несколько нетривиальных автоматов, такое вложение невозможно, так как количество атомов в каркасе $F(\mathbf{A}/\theta)$ фактор-автомата $\mathbf{A}/\theta$ будет больше, чем в любом из каркасов $F(\mathbf{A}_i)$, $1 \le i \le k$. $\square$

Замечание. Согласно лемме 2, далее будем рассматривать только связные автоматы и через s_0 обозначать состояние единственного в силу леммы 1 сильно связного подавтомата в i-автомате.

Упорядоченное множество с наименьшим элементом 0 называется веерной структурой, если в нем любые два несравнимых элемента не имеют общих верхних граней и имеют единственной общей нижней гранью 0.

Лемма 3 (о каркасе). *Каркас связного i-автомата является веерной структурой.*

Доказательство. 1) Покажем сначала, что в каркасе $F(\mathbf{A})$ i-автомата $\mathbf{A}$ каждый элемент (слой), отличный от $\{s_0\}$, содержит только один атом. Предположим, что это не так и $\sigma(u)$ — общая верхняя грань атомов $\sigma(s)$ и $\sigma(t)$ в $F(\mathbf{A})$. Пусть высота элемента $\sigma(u)$ в $F(\mathbf{A})$ равна l (под высотой элемента в конечном упорядоченном множестве понимается наибольшая из длин убывающих цепей, начинающихся с этого элемента). Тогда в динамическом каркасе $DF(\mathbf{A})$ имеются l-звенные цепи с началом $\sigma(u)$ и концом $\{s_0\}$. Пусть одна из них проходит через атом, отличный от $\sigma(s)$ (иначе вместо $\sigma(s)$ возьмем $\sigma(t)$). Рассмотрим в $DF(\mathbf{A})$ произвольную цепь P_1 с началом $\sigma(u)$ и концом $\{s_0\}$, проходящую через атом $\sigma(s)$. Выписывая для каждой дуги из P_1 в порядке ее прохождения метку и длину (т. е. разность высот начала и конца), получаем последовательность $\{(x_1', l_1^1), (x_2', l_2^1), \ldots, (x_{k-1}', l_{k-1}^1), (x_k', l_k^1), s_0\}$ — тип цепи P_1 (здесь $k \le l$, $\sum\limits_{i=1}^{k} l_i^1 = l$, s_0 указывает конец цепи). Эквивалентность $\theta = (\tau(s) \times \tau(s)) \cup \Delta_S$, где Δ_S — тождественное отношение на S, является конгруэнцией автомата $\mathbf{A}$. При факторизации $\mathbf{A}$ по θ (отождествляются состояния из $\sigma(s)$ с s_0) цепь P_1 трансформируется в цепь P_2 типа $\{(x_1', l_1^2), (x_2', l_2^2), \ldots, (x_{k-1}', l_{k-1}^2), s_0\}$ в динамическом каркасе $DF(\mathbf{A}/\theta)$, также имеющую длину l, т. е. $\sum\limits_{i=1}^{k-1} l_i^2 = l$. Так как $\mathbf{A}/\theta$ вкладывается в $\mathbf{A}$, то $DF(\mathbf{A}/\theta)$ вкладывается (как мультиграф) в $DF(\mathbf{A})$. Значит, в $DF(\mathbf{A})$ имеются цепи типа цепи P_2. По крайней мере одна из них должна проходить через $\sigma(s)$, иначе при факторизации по θ все эти цепи сохранились бы и к ним добавилась бы P_2, что сделало бы невозможным вложение динамического каркаса $DF(\mathbf{A}/\theta)$ в $DF(\mathbf{A})$. Но тогда в $DF(\mathbf{A}/\theta)$ обнаруживается цепь P_3 типа $\{(x_1', l_1^3), (x_2', l_2^3), \ldots, (x_{k-2}', l_{k-2}^3), s_0\}$ длиной l и т. д. Наконец, получаем, что в $DF(\mathbf{A}/\theta)$ должна быть однозвенная цепь (дуга) P_k типа $\{(x_1', l_1^k), s_0\}$, $l_1^k = l$. Имеющиеся в $DF(\mathbf{A})$ цепи (дуги) такого типа при факторизации по θ сохраняются в $DF(\mathbf{A}/\theta)$ и к ним присоединяется P_k. Поэтому вложение динамического каркаса $DF(\mathbf{A}/\theta)$ в $DF(\mathbf{A})$ невозможно. Полученное противоречие завершает доказательство утверждения об атомах в каркасе i-автомата.

2) Элемент a конечного упорядоченного множества называется верхним (нижним) соседом элемента b, если $a > b$ (соответственно $a < b$) и не существует элемента c со свойством

$a > c > b$ (соответственно $a < c < b$). Веерную структуру можно описать как упорядоченное множество с 0, в котором у каждого ненулевого элемента есть точно один нижний сосед и у каждого ненулевого элемента, не являющегося максимальным, есть точно один верхний сосед. Используя свойство, установленное в 1), покажем, что именно так устроен каркас i-автомата.

Предположим, что в каркасе $F(\mathbf{A})$ i-автомата $\mathbf{A}$ у элемента $\sigma(s) \neq \{s_0\}$ есть два верхних соседа: $\sigma(t)$ и $\sigma(u)$. В каркасе $F(\mathbf{A}/\theta)$ фактор-автомата автомата $\mathbf{A}$ по конгруэнции $\theta = (\tau(s) \times \tau(s)) \cup \Delta_S$ классы $\{\sigma(t)\}$ и $\{\sigma(u)\}$ становятся атомами. Но тогда число атомов в $F(\mathbf{A}/\theta)$ на единицу больше, чем в $F(\mathbf{A})$. Поскольку при вложении фактор-автомата $\mathbf{A}/\theta$ в $\mathbf{A}$ атомные (в смысле каркаса $F(\mathbf{A}/\theta)$) слои должны индуцированно перейти в атомные (в смысле каркаса $F(\mathbf{A})$) слои, получаем, что вложение фактор-автомата $\mathbf{A}/\theta$ в i-автомат $\mathbf{A}$ невозможно, — противоречие.

Предположим теперь, что в каркасе $F(\mathbf{A})$ i-автомата $\mathbf{A}$ у элемента $\sigma(s)$ есть два нижних соседа: $\sigma(t)$ и $\sigma(u)$. Для произвольного $s' \in S$ через $L(s')$ обозначим теоретико-множественное объединение всех слоев автомата $\mathbf{A}$, строго меньших чем $\sigma(s')$ в каркасе $F(\mathbf{A})$ (это состояния, которые достижимы из s', но из которых s' не достижимо). Эквивалентность $\theta = (L(t) \cup L(u))^2 \cup \Delta_S$ является конгруэнцией автомата $\mathbf{A}$. В каркасе $F(\mathbf{A}/\theta)$ фактор-автомата $\mathbf{A}/\theta$ классы $\{\sigma(t)\}$ и $\{\sigma(u)\}$ становятся атомами. Но тогда число атомов в $F(\mathbf{A}/\theta)$ на единицу больше, чем в $F(\mathbf{A})$. Значит, и в этом случае вложение фактор-автомата $\mathbf{A}/\theta$ в i-автомат $\mathbf{A}$ невозможно,— противоречие. □

Пусть $\sigma(s)$ — некоторый слой автомата $\mathbf{A}$. Присоединим к нему элемент 0 и для произвольных $s' \in \sigma(s)$, $x \in X$ положим $\delta(s', x) = 0$, если $\delta(s', x) \notin \sigma(s)$, и $\delta(0, x) = 0$. Тем самым на множестве $\sigma(s) \cup \{0\}$ задается структура автомата, оставим для него обозначение слоя $\sigma(s)$, т. е. это слой $\sigma(s)$, рассматриваемый как автомат.

Лемма 4 (об изоморфности сравнимых слоев)**.** *Если в каркасе $F(\mathbf{A})$ i-автомата $\mathbf{A}$ два ненулевых слоя сравнимы, то они изоморфны как автоматы.*

Доказательство. Пусть $\{s_0\} = \sigma(s_0) < \sigma(s_1) < \cdots < \sigma(s_k)$ — некоторая максимальная цепь в каркасе $F(\mathbf{A})$ и в ней есть неизоморфные как автоматы слои. Двигаясь вверх по цепи, отмечаем первый слой $\sigma(s_i)$, не изоморфный атомному слою $\sigma(s_1)$. Эквивалентность $\theta = (\tau(s_{i-1}) \times \tau(s_{i-1})) \cup \Delta_S$, отождествляющая все состояния главного подавтомата $\mathbf{A}(s_{i-1})$, является конгруэнцией на $\mathbf{A}$. В каркасе $F(\mathbf{A}/\theta)$ слой $\sigma(s_i)$ становится атомным, и мы имеем в $F(\mathbf{A}/\theta)$ атомных слоев, не изоморфных слою $\sigma(s_1)$, на один больше, чем в $F(\mathbf{A})$. Отсюда следует, что фактор-автомат $\mathbf{A}/\theta$ не вложим в i-автомат $\mathbf{A}$, что невозможно для i-автомата $\mathbf{A}$. Полученное противоречие показывает, что в $F(\mathbf{A})$ нет ненулевых сравнимых неизоморфных слоев. □

Лемма 5 (об изоморфных несравнимых слоях)**.** *Если два атомных слоя связного i-автомата $\mathbf{A}$ изоморфны, то хотя бы один из них будет максимальным элементом каркаса $F(\mathbf{A})$.*

Доказательство. Пусть $\sigma(s)$ и $\sigma(t)$ — различные атомные слои автомата $\mathbf{A}$ и φ — изоморфизм главных подавтоматов $\mathbf{A}(s)$ и $\mathbf{A}(t)$. Рассмотрим эквивалентность θ на множестве S состояний автомата $\mathbf{A}$, все неодноэлементные классы которой имеют вид $\{s', \varphi(s')\}$, где $s' \in \sigma(s)$. Пусть x — произвольный входной сигнал. Если $\delta(s', x) \in \sigma(s)$ для $s' \in \sigma(s)$, то обязательно $\delta(\varphi(s'), x) \in \sigma(t)$, поскольку допустив $\delta(\varphi(s'), x) = s_0$, мы получили бы $\varphi(\delta(s', x)) \neq s_0 = \delta(\varphi(s'), x)$, что невозможно для изоморфизма. Так как φ — изоморфизм, то $\delta(\varphi(s'), x) = \varphi(\delta(s', x))$ и, значит, $(\delta(s', x), \delta(\varphi(s'), x)) \in \theta$. Кроме того, при $\delta(s', x) = s_0$ будет $\delta(\varphi(s'), x) = \varphi(\delta(s', x)) = s_0$, откуда снова $(\delta(s', x), \delta(\varphi(s'), x)) \in \theta$. Таким образом, θ — конгруэнция автомата $\mathbf{A}$.

При факторизации по θ слои $\sigma(s)$ и $\sigma(t)$ сливаются. Если в $F(\mathbf{A})$ максимальная цепь, содержащая $\sigma(s)$, и максимальная цепь, содержащая $\sigma(t)$, имеют длину больше 1, то в каркасе $F(\mathbf{A}/\theta)$ слой, полученный слиянием $\sigma(s)$ и $\sigma(t)$, будет иметь два верхних соседа. Но тогда каркас $F(\mathbf{A}/\theta)$ не является веерной структурой и не может быть вложен в веерную структуру (лемма 3) $F(\mathbf{A})$. Следовательно, фактор-автомат $\mathbf{A}/\theta$ не вкладывается в автомат $\mathbf{A}$, что невозможно для i-автомата $\mathbf{A}$, противоречие. $\square$

Максимальная цепь $\{s_0\} = \sigma(s_0) < \sigma(s_1) < \cdots < \sigma(s_k)$ динамического каркаса $DF(\mathbf{A})$ автомата $\mathbf{A}$ называется однородной, если фактор-автомат $\mathbf{A}(s_k)/\theta_i$ изоморфен главному подавтомату $\mathbf{A}(s_{k-i})$, где $\theta_i = (\tau(s_i) \times \tau(s_i)) \cup \Delta_{\tau(s_k)}$, $1 \le i \le k$.

Лемма 6 (об однородности максимальных динамических цепей)**.** *Все максимальные цепи динамического каркаса $DF(\mathbf{A})$ i-автомата $\mathbf{A}$ однородны.*

Доказательство. Допустим, что некоторая максимальная цепь $\{s_0\} = \sigma(s_0) < \sigma(s_1) < \cdots < \sigma(s_k)$ динамического каркаса $DF(\mathbf{A})$ i-автомата $\mathbf{A}$ неоднородна. Тогда для подходящего i, $0 \le i \le k$, фактор-автомат $\mathbf{A}(s_k)/\theta_i$ не изоморфен главному подавтомату $\mathbf{A}(s_{k-i})$. Автомат $\mathbf{A}/\theta_i'$, где $\theta_i' = \theta \cup \Delta_S$, получается из автомата $\mathbf{A}$ заменой максимальной (в смысле динамического каркаса $DF(\mathbf{A})$) цепи слоев $\sigma(s_0) < \sigma(s_1) < \cdots < \sigma(s_k)$ на максимальную (в смысле динамического каркаса $DF(\mathbf{A}/\theta_i')$) цепь слоев $\sigma(s_0) < \sigma(s_{i+1}) < \cdots < \sigma(s_k)$, порождающую в $\mathbf{A}/\theta_i'$ подавтомат, не изоморфный подавтомату $\mathbf{A}(s_{k-i})$ автомата $\mathbf{A}$. Следовательно, фактор-автомат $\mathbf{A}/\theta_i'$ не вкладывается в i-автомат $\mathbf{A}$, что невозможно. $\square$

Класс конгруэнции θ, содержащий элемент s_0, будем называть нулевым θ-классом.

Лемма 7 (конгруэнции и достижимость)**.** *Для любой конгруэнции θ i-автомата $\mathbf{A}$ выполняется условие $s_0 \notin \theta(s) \,\&\, t \in (\theta \cap \tau)(s) \Rightarrow t = s$, т. е. отношение достижимости τ тождественно на ненулевых θ-классах.*

Доказательство. От противного. Пусть θ — конгруэнция i-автомата $\mathbf{A}$ и существуют $s, t \in S$ такие, что $s_0 \notin \theta(s)$, $t \in (\theta \cap \tau)(s)$ и $t \ne s$. Из всех подобных пар (s, t) выберем такую пару (s', t'), чтобы слой $\sigma(t')$ имел наименьшую возможную высоту в упорядоченном множестве $F(\mathbf{A})$. Далее возможны следующие два случая.

1) Конгруэнция θ тождественна на множестве $\sigma(t')$.

Это означает, что $\sigma(t') < \sigma(s')$ в $F(\mathbf{A})$. Можно считать, что $\sigma(s')$ является верхним соседом для $\sigma(t')$ в $F(\mathbf{A})$: если верхним соседом для $\sigma(t')$ окажется другой слой $\sigma(s'')$, то при подходящем $p \in X^*$ будет $\delta(s', p) = s''$ и, так как θ-эквивалентный с s'' элемент $t'' = \delta(t', p)$ лежит в слое $\sigma(t')$ по выбору этого слоя, то вместо (s', t') можно будет взять пару (s'', t'').

Аналогичными рассуждениями устанавливается, что каждому элементу слоя $\sigma(s')$ сопоставляется θ-эквивалентный ему элемент из слоя $\sigma(t')$, причем единственный согласно исходному в 1) предположению.

С другой стороны, для каждого элемента из $\sigma(t')$ существует θ-эквивалентный ему элемент из $\sigma(s')$. Действительно, если это не так, то поскольку в слоях $\sigma(s')$ и $\sigma(t')$ по лемме 4 одинаковое число элементов, в $\sigma(s')$ найдутся $s_1' \ne s_1''$ такие, что $\{s_1', s_1''\} \subseteq \theta(t_1)$ для некоторого $t_1 \in \sigma(t')$. Пусть φ — изоморфизм слоя $\sigma(t')$ на слой $\sigma(s')$ в смысле леммы 4. Возьмем максимальную по длине цепочку вида $\{s_1', s_1''\}t_1 s_2 t_2 s_3 t_3 \ldots$, где $s_i = \varphi(t_{i-1})$ и $(s_i, t_i) \in \theta$, $i \ge 2$. Если последним ее элементом является t_k, то $\varphi(t_k) \in \{s_1', s_1''\}$. Пусть $\varphi(t_k) = s_1'$. Выберем слово $p \in X^*$ такое, что $\delta(s_1', p) = s_1''$. Под действием этого слова все элементы цепочки, начиная с t_1, переходят в себя. Отсюда следует, что и $\delta(s_1', p) = s_1'$, — противоречие. Если же последним элементом цепочки является s_k, то $(s_k, t_i) \in \theta$ для некоторого i, $1 \le i \le k$. Тогда имеем цепочку $\{s_1, s_k\} t_i s_{i+1} t_{i+1} \ldots s_{k-1} t_{k-1}$ уже рассмотренного вида (при $i = 1$ в качестве s_1 берется отличный от s_k элемент из $\{s_1', s_1''\}$).

Согласно лемме 4 слои $\sigma(s')$ и $\sigma(t')$ изоморфны как автоматы. Тогда у них имеется одинаковое число "выходов" — пар вида (u, x), $x \in X$, таких, что u принадлежит, а $\delta(u, x)$ не принадлежит данному слою. Пусть (t'_1, x) — выход из $\sigma(t')$ и s'_1 — элемент в $\sigma(s')$, θ-эквивалентный элементу t'_1. Тогда $(\delta(s', x), \delta(t'_1, x)) \in \theta$. В силу выбора элементов s' и t' получаем, что обязательно $\delta(s'_1, x) = \delta(t'_1, x)$. Отсюда следует, что для любого выхода (s'_i, x') из слоя $\sigma(s')$ имеем $\sigma(\delta(s'_i, x')) < \sigma(t')$. Но $\sigma(s')$ является верхним соседом для $\sigma(t')$, поэтому хотя бы для одного выхода (s''_j, x'') из слоя $\sigma(s')$ должно быть $\sigma(\delta(s''_j, x'')) = \sigma(t')$. Получили противоречие.

2) Конгруэнция не тождественна на множестве $\sigma(t')$.

Рассмотрим на множестве S эквивалентность $\theta'_0 = \theta' \cup \Delta_S$, где θ' — ограничение конгруэнции θ на главном подавтомате $\mathbf{A}(t')$. Эта эквивалентность является конгруэнцией автомата $\mathbf{A}$.

Если все слои, которые в $F(\mathbf{A})$ лежат ниже $\sigma(t')$, содержатся в нулевом θ'_0-классе, то в $F(\mathbf{A}/\theta'_0)$ число атомных слоев с $|\sigma(t')/\theta'_0| < |\sigma(t')|$ элементами будет больше, чем в $\mathbf{A}$ и, значит, фактор-автомат $\mathbf{A}/\theta'_0$ не будет вкладываться в $\mathbf{A}$. Если же в $F(\mathbf{A})$ есть слои, которые лежат ниже $\sigma(t')$ и не содержатся в нулевом θ'_0-классе, то согласно выбору слоя $\sigma(t')$ конгруэнция θ, а значит, и θ'_0 будет тождественной на них. Тогда в $F(\mathbf{A}/\theta'_0)$ появятся сравнимые слои, не изоморфные как автоматы, что вследствие леммы 4 препятствует вложению фактор-автомата $\mathbf{A}/\theta'_0$ в $\mathbf{A}$. Получаем, что конгруэнция θ'_0 не является внутренней в i-автомате $\mathbf{A}$. Пришли к противоречию. □

Заметим, что условие, рассматриваемое в лемме 7, может быть представлено в следующей форме: $t \neq s \,\&\, t \in (\theta \cap \tau)(s) \Rightarrow s_0 \in \theta(s)$. В этом виде оно допускает эффективную проверку.

Теорема (характеризация связных i-автоматов). *Все конгруэнции связного автомата* $\mathbf{A}$ *будут внутренними тогда и только тогда, когда выполняются следующие условия*:

(1) *автомат* $\mathbf{A}$ *имеет только один сильно связный подавтомат, и этот подавтомат тривиален* (*его состояние обозначается через* s_0);
(2) *каркас* $F(\mathbf{A})$ *автомата* $\mathbf{A}$ *является веерной структурой*;
(3) *если два нетривиальных слоя автомата* $\mathbf{A}$ *сравнимы по отношению достижимости* τ, *то они изоморфны как автоматы*;
(4) *если два атомных слоя изоморфны как автоматы, то хотя бы один из них максимален в каркасе* $F(\mathbf{A})$;
(5) *все максимальные цепи динамического каркаса* $DF(\mathbf{A})$ *однородны*;
(6) *для любой конгруэнции автомата* $\mathbf{A}$ *выполняется соотношение* $s_0 \notin \theta(s) \,\&\, t \in (\theta \cap \tau)(s) \Rightarrow t = s$.

Доказательство. Необходимость условий теоремы следует из лемм 1–7.

Достаточность. Пусть в связном автомате $\mathbf{A}$ выполнены условия (1)–(6) и пусть θ — произвольная конгруэнция этого автомата. Посмотрим, как устроены θ-классы.

1) Нулевой θ-класс.

Пусть $s \neq s_0$ и $s \in \theta(s_0)$. Тогда для любого $x \in X$ будет $\delta(s, x) \in \theta(s_0)$, так как $\delta(s_0, x) = s_0$ (согласно условию (1)). Отсюда следует, что $\theta(s_0)$ является устойчивым подмножеством в автомате $\mathbf{A}$ и, значит, образует подавтомат в $\mathbf{A}$. Как и всякий подавтомат он будет объединением в $\mathrm{Sub}(\mathbf{A})$ всех содержащихся в нем главных подавтоматов. Таким образом, $\theta(s_0)$ представляет собой объединение слоев, составляющих в каркасе $F(\mathbf{A})$ начальные отрезки каких-либо максимальных цепей. Можно сказать также, что множество $\theta(s_0)/\sigma$ является порядковым идеалом в каркасе $F(\mathbf{A})$.

2) Ненулевые θ-классы.

Согласно условию (6) $\theta(s)$ является селективным множеством для некоторого набора σ-классов и при этом входящие в один θ-класс состояния взаимно не достижимы. Пусть

$s', t' \in S$, $s' \neq t'$, таковы, что $(s', t') \in \theta$, слой $\sigma(t')$ имеет наименьшую возможную высоту в упорядоченном множестве $F(\mathbf{A})$, а $\sigma(s')$ при этих условиях тоже имеет наименьшую возможную высоту в $F(\mathbf{A})$. Возьмем произвольный элемент $s'' \in \sigma(s')$. Ввиду сильной связности слоя $\sigma(s')$ найдется слово $p' \in X^*$ такое, что $\delta(s', p') = s''$. Элемент $t'' = \delta(t', p')$ находится в слое $\sigma(t')$, так как, предположив противное, мы получили бы $s'' \in \sigma(s')$, $(s'', t'') \in \theta$ и $\sigma(t'') < \sigma(t')$, что противоречит выбору t'. Таким образом, каждому элементу s'' слоя $\sigma(s')$ сопоставляется элемент $t'' \in \sigma(t')$ — единственный в слое $\sigma(t')$, находящийся в одном θ-классе с s''. Тем самым определяется отображение $\varphi : \sigma(s') \to \sigma(t')$, $s'' \mapsto t''$, где $\theta(s') \cap \sigma(t') = \{t''\}$. Оно инъективно, так как равенство $\varphi(s'_1) = \varphi(s'_2)$ для различных состояний $s'_1, s'_2 \in \sigma(s')$ означало бы, что $(s'_1, s'_2) \in \theta$, а это противоречит условию (6).

С другой стороны, если $t''_1 \in \sigma(t')$, то $\delta(t', q') = t''_1$ для некоторого входного слова $q' \in X^*$, а тогда $s''_1 = \delta(s', q')$ принадлежит слою $\sigma(s')$ согласно выбору s' и при этом $(s''_1, t''_1) \in \theta$, т. е. $t''_1 = \varphi(s''_1)$. Так что отображение φ сюръективно и, следовательно, является биекцией.

Более того, если доопределить φ, полагая $\varphi(0) = 0$, то φ будет изоморфизмом слоя $\sigma(s')$ как автомата на слой $\sigma(t')$, рассматриваемый как автомат. В самом деле, если $\delta(s'', x) \in \sigma(s')$, то для $t'' = \varphi(s'')$ будет $\delta(t'', x) \in \sigma(t')$, иначе $\sigma(\delta(t'', x)) < \sigma(t')$ и пара $\sigma(\delta(t'', x))$, $\sigma(\delta(s'', x))$ вступает в противоречие с выбором слоев $\sigma(t'), \sigma(s')$. Но тогда $\delta(t'', x) = \varphi(\delta(s'', x))$, т. е. $\varphi(\delta(s'', x)) = \delta(\varphi(s''), x)$ и, значит, φ — гомоморфизм. Если же $\delta(s'', x) \notin \sigma(s')$, т. е. $\sigma(\delta(s'', x)) < \sigma(s')$, то не может быть, чтобы $\delta(t'', x) \in \sigma(t')$, иначе пара $\sigma(t'), \sigma(\delta(s'', x))$ вступала бы в противоречие с выбором слоев $\sigma(t'), \sigma(s')$. Отсюда следует, что если (s'', x) — выход из слоя $\sigma(s')$, то (t'', x) — выход из слоя $\sigma(t')$, и в соответствующих автоматах имеем $\varphi(\delta(s'', x)) = 0 = \delta(t'', x) = \delta(\varphi(s''), x)$.

Итак, φ — изоморфизм слоя $\sigma(s')$ как автомата на слой $\sigma(t')$, рассматриваемый как автомат. Но тогда согласно условию (3) изоморфными будут атомный слой цепи, содержащей $\sigma(s')$, и атомный слой цепи, содержащей $\sigma(t')$. В силу условия (4) один из них максимален в каркасе $F(\mathbf{A})$.

Перейдем к завершающему этапу доказательства достаточности.

При факторизации автомата $\mathbf{A}$ по конгруэнции θ нулевой θ-класс, согласно 1) образующий порядковый идеал в каркасе $F(\mathbf{A})$, отождествляет состояния, входящие в слои, из которых составлены начальные отрезки некоторого набора максимальных цепей упорядоченного множества $F(\mathbf{A})$. Вследствие однородности максимальных цепей в динамическом каркасе $DF(\mathbf{A})$ (условие (5)), фактор-автомат $\mathbf{A}/\theta_0$, где $\theta_0 = (\theta(s_0) \times \theta(s_0)) \cup \Delta_S$, вкладывается в автомат $\mathbf{A}$. Пусть $\theta(s)$ — ненулевой θ-класс. Согласно 2) он состоит из элементов, взятых по одному из некоторых изоморфных между собой слоев. Все эти слои, кроме одного, будут атомными и максимальными в $F(\mathbf{A})$ (а значит, и в $F(\mathbf{A}/\theta_0)$). При этом исключительный слой, если он есть, будет атомным в $F(\mathbf{A}/\theta_0)$, но не обязательно максимальным в этом упорядоченном множестве. При отождествлении состояний автомата $\mathbf{A}$ (и автомата $\mathbf{A}/\theta_0$) в каждом ненулевом θ-классе произойдет "укладка" изоморфных между собой атомных максимальных в $F(\mathbf{A})$ слоев на исключительный слой, если он есть, либо на один из этих слоев, если исключительного слоя нет. Полученный в итоге фактор-автомат $\mathbf{A}/\theta$ изоморфен подавтомату автомата $\mathbf{A}$, который получается исключением из каждой максимальной (в $F(\mathbf{A})$) цепи слоев стольких "верхних" ее элементов, сколько "нижних" ненулевых ее элементов попало в класс $\theta(s_0)$.

Из всего сказанного следует, что конгруэнция θ внутренняя. □

Покажем, что характеризация автономных i-автоматов получается как следствие доказанной теоремы.

Пусть $\mathbf{A} = (S, \delta)$ — связный автономный автомат (считаем δ преобразованием множества S). Его диаграмма представляет собой контур с входящими в него деревьями. Если $\mathbf{A}$ является i-автоматом, то согласно [4]:

а) контур вырождается в петлю;

б) все входящие в него деревья будут цепями;

в) только одна из них имеет длину, большую 1.

Для такого автомата выполняются все требования характеризационной теоремы. Действительно, выполнимость условия (1) теоремы следует из а). Но тогда справедливо и условие (6): для любой конгруэнции θ из $(s,t) \in \theta \cap \tau$, $t \neq s$, следует $s_0 \in \theta(s)$. Каркас $F(\mathbf{A})$ представляет собой диаграмму переходов автомата $\mathbf{A}$ с исключенной петлей и, значит, б) обеспечивает выполнимость условия (2). Нетривиальных слоев в $\mathbf{A}$ нет, так что имеет место и условие (3). Из в) и того факта, что все слои в $\mathbf{A}$ изоморфны, следует условие (4). Динамический каркас $DF(\mathbf{A})$ совпадает с диаграммой переходов автомата $\mathbf{A}$, поэтому б) влечет условие (5).

С другой стороны, если связный автономный автомат удовлетворяет условиям теоремы, то из условия (1) следует а), после чего справедливы сделанные выше замечания о строении каркаса $F(\mathbf{A})$ и динамического каркаса $DF(\mathbf{A})$. Тогда из условия (2) вытекает б), и из условия (4) следует в). Условия (3), (5) и (6) не налагают на $\mathbf{A}$ никаких дополнительных ограничений.

Проведенные рассуждения показывают, что полученное в [4] описание связных автономных i-автоматов является следствием доказанной теоремы.

Конструкции, участвующие в теореме, наглядно объясняет следующий

Пример. Рассмотрим автомат $\mathbf{A} = (S, X, \delta)$, где $S = \{s_0, s_1, s_2, \ldots, s_{2n-1}, s_{2n}\}$, $n \geq 1$, $X = \{0,1\}$ и функция переходов $\delta : S \times X \to S$ задана равенствами $\delta(s_{2k-1}, 0) = s_{2k}$ при $k \geq 1$, $\delta(s_{2k}, 0) = s_0$ при $k \geq 0$, $\delta(s_0, 1) = \delta(s_1, 1) = s_0$, $\delta(s_{2k-1}, 1) = s_{2k-3}$ при $k > 1$, $\delta(s_{2k}, 1) = s_{2k-1}$ при $k > 0$.

Заметим, что начальное состояние s_{2n-1} и финальное подмножество $\{s_1\}$ представляют в автомате $\mathbf{A}$ каскадный язык L_1, состоящий из слов вида $\Big(\prod\limits_{i=1}^{n-1}((01)^{k_i}1)\Big)(01)^{k_n}$, где $k_1, k_2, \ldots, k_n \geq 0$ (нулевые показатели итерации обозначают отсутствие соответствующих подслов), а пара $(s_{2n-1}, \{s_2\})$ — каскадный язык L_2, состоящий из слов вида $\Big(\prod\limits_{i=1}^{n-1}((01)^{k_i}1)\Big)(01)^{k_n}0$.

Покажем, что $\mathbf{A}$ является i-автоматом.

1) Состояние s_0 образует в $\mathbf{A}$ единственный сильно связный подавтомат.

2) Слоями в $\mathbf{A}$ являются подмножества $\{s_0\}$ и $\{s_{2k-1}, s_{2k}\}$, $k \geq 1$. Поэтому каркас $F(\mathbf{A})$ изоморфен цепи $s_{2n-1} > s_{2n-3} > \cdots > s_1 > s_0$ и, значит, будет веерной структурой.

3) Все нетривиальные слои очевидным образом изоморфны как автоматы.

4) Атомный слой в $\mathbf{A}$ один — это $\{s_1, s_2\}$.

5) Динамический каркас $DF(\mathbf{A})$ представляет собой мультиграф, в каждой вершине которого имеется петля с меткой 0 и петля с меткой 1, все непетлевые дуги с меткой 0 ведут в слой $\{s_0\}$, а непетлевые дуги с меткой 1 образуют цепь, изоморфную цепи $s_{2n-1} \to s_{2n-3} \to \cdots \to s_1 \to s_0$. Однородность цепи $DF(\mathbf{A})$ очевидна.

6) Пусть θ — произвольная конгруэнция автомата $\mathbf{A}$ и $(s,t) \in \theta \cap \tau$, причем $t \neq s$. Следующие соображения показывают, что $s_0 \in \theta(s)$ и, значит, условие (6) теоремы выполняется. Вместо $(s,t) \in \theta$ будем писать $s \equiv t$.

Если $s = s_{2m-1}$, $t = s_{2k-1}$, $k < m \leq n$, то

$$s_{2m-1} \equiv s_{2k-1} = \delta(s_{2m-1}, 1^{m-k}) \equiv \delta(s_{2m-1}, 1^{2(m-k)}) \equiv \cdots \equiv s_0$$

после некоторого числа итераций входного слова 1^{m-k}.

Если $s = s_{2m-1}$, $t = s_{2k}$, то $s_{2m-1} \equiv s_{2k} = \delta(s_{2m-1}, (01)1^{m-k}0) \equiv \delta(s_{2k}, (01)1^{m-k}0) = s_0$.

Аналогично действуем в случаях $s = s_{2m}, t = s_{2k-1}$ и $s = s_{2m}, t = s_{2k}$, $k < m \leq n$. Таким образом, для автомата $\mathbf{A}$ выполняются все условия теоремы.

Модифицируя рассмотренный пример, можно строить самые разнообразные i-автоматы.

Автор выражает искреннюю благодарность рецензенту за весьма существенные замечания, способствовавшие улучшению текста, и за информацию о работе [8], где результаты, полученные в [3], переносятся на алгебры Оккама специального вида.

Литература

[1] Fuchs L., Kertesz A., Szele T. *On abelian groups in which every homomorphic image can be embedded* // Acta Math. Hung. – 1956. – V. 7. – № 3–4. – P. 467–475.

[2] Rival I., Sands B. *Weak embeddings and embeddings of finite distributive lattices* // Arch. Math. – 1975. – V. 26. – № 1. – P. 346–352.

[3] Blyth T.S., Fang J., Silva H.J. *The endomorphism kernel property in finite distributive lattices and de Morgan algebras* // Commun. Algebra. – 2004. – V. 32. – № 6. – P. 2225–2242.

[4] Киреева А.В. *Подграфы и факторизации функциональных графов* // УМН. – 1993. – Т. 48. – № 2. – С. 183–184.

[5] Богомолов А.М., Салий В.Н. *Алгебраические основы теории дискретных систем.* – М.: Наука, 1997. – 368 с.

[6] Салий В.Н. *О внутренних конгруэнциях автоматов* // Международн. алгебр. конф., посв. 250-летию Моск. ун-та. Тез. докл. – Москва, 2004. – С. 109–110.

[7] Салий В.Н. *Универсальная алгебра и автоматы.* – Саратов: Изд-во Сарат. ун-та, 1988. – 72 с.

[8] Fang J. *An extended Ockam algebra with endomorphism kernel property* // Acta Math. Sinica. – 2007. – V. 23. – № 9. – P. 1611–1620.

В.Н. Салий

профессор, заведующий кафедрой теоретических основ компьютерной безопасности и криптографии, Саратовский государственный университет, 410012, г. Саратов, ул. Астраханская, д. 83,

e-mail: SaliiVN@info.sgu.ru

V.N. Salii

Professor, Head of the Chair of Theoretical Foundations of Computer Security and Cryptography, Saratov State University, 83 Astrakhanskaya str., Saratov, 410012 Russia,

e-mail: SaliiVN@info.sgu.ru