М. А. Ройтберг, Эквивалентность схем с одной обратной связью, *Пробл. передачи информ.*, 1977, том 13, выпуск 2, 83–89

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том XIII 1977 Вып. 2

УДК 621.395.16

ЭКВИВАЛЕНТНОСТЬ СХЕМ С ОДНОЙ ОБРАТНОЙ СВЯЗЬЮ

М. А. Ройтберг

Исследуется так называемая схемная эквивалентность автоматов. Указывается алгоритм проверки схемной эквивалентности конечных автоматов, оценивается сложность эксперимента, устанавливающего схемную эквивалентность.

§ 1. Введение

Любая схема с одной обратной связью может быть представлена в виде так называемой стандартной схемы. Стандартная схема — это схема из двух автоматов, один из которых (базисный автомат) — автомат с двумя входами и с двумя выходами, другой (автомат обратной связи) — автомат с одним входом и одним выходом. При этом выходные сигналы со второго выхода базисного автомата подаются на вход автомата обратной связи, выходные сигналы автомата обратной связи подаются на второй вход базисного автомата.

Пусть $\mathfrak{A}$ — автомат с входным алфавитом $\Sigma_1\times\Sigma_2$ и выходным алфавитом $T_1\times T_2$; X — автомат с входным алфавитом T_2 и выходным алфавитом Σ_2. Если стандартная схема с базисным автоматом $\mathfrak{A}$ и автоматом обратной связи X определена корректно, то она задает автомат с входным алфавитом Σ_1 и выходным алфавитом T_1 (см. рисунок). Этот автомат будем обозначать $S(\mathfrak{A}, X)$.

В работе выделяется класс так называемых схемных автоматов, обладающих следующим свойством. Если $\mathfrak{A}$ — схемный автомат с входным алфавитом $\Sigma_1\times\Sigma_2$ и выходным алфавитом $T_1\times T_2$, то для любого автомата с входным алфавитом T_2 и выходным алфавитом Σ_2 стандартная схема определена корректно.

Схемные автоматы $\mathfrak{A}$ и $\mathfrak{B}$ называются s-эквивалентными (обозначение $\mathfrak{A}\underset{s}{\sim}\mathfrak{B}$), если для любого автомата обратной связи X автоматы $S(\mathfrak{A}, X)$ и $S(\mathfrak{B}, X)$ эквивалентны. Автомат X и слово $p\in\Sigma_1^*$ s-различают схемные автоматы $\mathfrak{A}$ и $\mathfrak{B}$, если $S(\mathfrak{A}, X)(p)\neq S(\mathfrak{B}, X)(p)$ (мы используем одинаковые обозначения для автомата и реализуемого им отображения слов).

В работе указывается алгоритм построения автомата минимального веса, s-эквивалентного данному. Этот автомат единствен с точностью до некоторого преобразования (теорема 1). Дается алгоритм проверки s-эквивалентности двух схемных автоматов (теорема 5). Оценивается сложность s-различения двух автоматов $\mathfrak{A}$ и $\mathfrak{B}$. В качестве меры сложности берется минимум по всем парам $\langle X, p\rangle$, s-различающим $\mathfrak{A}$ и $\mathfrak{B}$, следующих величин: 1) количество состояний автомата X—$|X|$; 2) длина слова p—$l(p)$; 3) сумма веса автомата X и длины слова p.

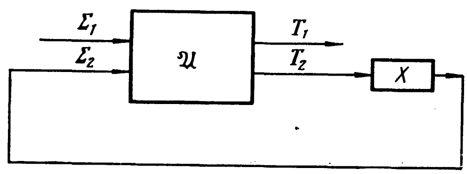
Доказывается, что, если автоматы $\mathfrak{A}$ и $\mathfrak{B}$ не s-эквивалентны, вес $\mathfrak{A}$ и вес $\mathfrak{B}$ не превосходит n, то найдутся такие автомат X и слово p, s-различающие $\mathfrak{A}$ и $\mathfrak{B}$, что

$$|X|\leqslant 2n+3,\quad l(p)\leqslant 3n-1,\quad |X|+l(p)\leqslant 4n+3.$$

Эти оценки не улучшаемы (теоремы 2—4). Другие задачи, касающиеся схем с одной обратной связью, изучались А. А. Летичевским (см., например, [1]).

Определение автомата и схемы автоматов приведены в [2, 3].

Мы используем следующие обозначения: строчные греческие буквы σ, τ, θ, ξ всюду обозначают буквы соответствующих алфавитов. Множество всех слов в алфавите Σ обозначается Σ^*; длина слова p обозначается



через $l(p)$. Если A, $B\subset\Sigma^*$, то $AB=\{z|\exists x\in A\exists y\in B\ (z=xy)\}$. Вместо $\{\sigma\}B$ будем писать σB.

Пусть Σ_1, Σ_2 — алфавиты, $p\in(\Sigma_1\times\Sigma_2)^*$. Через p^1 и p^2 обозначаются проекции слова p на Σ_1 и Σ_2 соответственно. Если $f: M\to(\Sigma_1\times\Sigma_2)^*$ — функция со значениями в $(\Sigma_1\times\Sigma_2)^*$, то через $f^1: M\to\Sigma_1^*$ обозначается функция $f^1(x)=(f(x))^1$. Функция $f^2: M\to\Sigma_2^*$ определяется аналогично.

Шестерка $\langle\Sigma, Q, \mathrm{T}, q_0, \varphi, \psi\rangle$ обозначает инициальный автомат Мили с входным алфавитом Σ, выходным алфавитом T, множеством внутренних состояний Q, начальным состоянием $q_0\in Q$, функцией переходов $\varphi: Q\times\Sigma\to Q$ и функцией выходов $\psi: Q\times\Sigma\to T$. Функции φ и ψ естественно продолжают до функций $\varphi: Q\times\Sigma^*\to Q$ и $\psi: Q\times\Sigma^*\to\mathrm{T}^*$. Если $\mathfrak{A}=\langle\Sigma, Q, \mathrm{T}, q_0, \varphi, \psi\rangle$; $x\in\Sigma^*$, то иногда вместо $\psi(q_0, x)$ будем писать $\mathfrak{A}(x)$. Через $|\mathfrak{A}|$ обозначается количество внутренних состояний автомата $\mathfrak{A}$.

Множество всех конечных автоматов с входным алфавитом Σ и выходным алфавитом T обозначается через $k(\Sigma, \mathrm{T})$. Если $\mathfrak{A}=\langle\Sigma, Q, \mathrm{T}_1\times\mathrm{T}_2, q_0, \varphi, \psi\rangle$, то через $\mathfrak{A}^1$ обозначается автомат $\mathfrak{A}^1=\langle\Sigma, Q, \mathrm{T}_1, q_0, \varphi, \psi^1\rangle$. Эквивалентность инициальных автоматов $\mathfrak{A}$ и $\mathfrak{B}$ обозначается $\mathfrak{A}\sim\mathfrak{B}$.

§ 2. Минимизация числа состояний схемного автомата

Дадим точное определение схемного автомата.

Определение. Автомат $\mathfrak{A}=\langle\Sigma_1\times\Sigma_2, Q, \mathrm{T}_1\times\mathrm{T}_2, q_0, \varphi, \psi\rangle$ называется схемным, если $\psi^2(q, \langle\sigma_1, \sigma_2\rangle)$ не зависит от σ_2, т. е.

$$\forall q\in Q\forall\sigma_1\in\Sigma_1\forall\sigma_2, \sigma_3\in\Sigma_2\psi^2(q, \langle\sigma_1, \sigma_2\rangle)=\psi^2(q, \langle\sigma_1, \sigma_3\rangle).$$

Очевидно, если $\mathfrak{A}\in k(\Sigma_1\times\Sigma_2, \mathrm{T}_1\times\mathrm{T}_2)$ — автомат Мура, то $\mathfrak{A}$ — схемный.

Множество схемных автоматов с входным алфавитом $\Sigma_1\times\Sigma_2$ и выходным алфавитом $\mathrm{T}_1\times\mathrm{T}_2$ обозначается $sk(\Sigma_1\times\Sigma_2, \mathrm{T}_1\times\mathrm{T}_2)$. Подробное описание работы схемы приведено в [1].

Определение. Схемные автоматы $\mathfrak{A}$ и $\mathfrak{B}$ называются 1-эквивалентными (обозначение $\mathfrak{A}\underset{1}{\sim}\mathfrak{B}$), если $\mathfrak{A}^1\sim\mathfrak{B}^1$. Очевидно, если $\mathfrak{A}\sim\mathfrak{B}$, то $\mathfrak{A}\underset{1}{\sim}\mathfrak{B}$.

Определение. Пусть $\mathfrak{A}=\langle\Sigma_1\times\Sigma_2, Q, \mathrm{T}_1\times\mathrm{T}_2, q_0, \varphi, \psi\rangle$; $\sigma\in\Sigma_1$. Состояние $q\in Q$ называется σ-автономным, если для любых слов $x\in\sigma\Sigma_1^*$, x_1, $x_2\in\Sigma_2^*$, таких, что $l(x_1)=l(x_2)=l(x_3)$, выполнено $\psi^1(q, \langle x, x_1\rangle)=\psi^1(q, \langle x, x_2\rangle)$.

Лемма 1. *Схемные автоматы* $\mathfrak{A}$ *и* $\mathfrak{B}$ *s-эквивалентны тогда и только тогда, когда:* 1) $\mathfrak{A}\underset{1}{\sim}\mathfrak{B}$, 2) *если последние буквы слов* $\mathfrak{A}(p\langle\sigma, \sigma_1\rangle)$ *и* $\mathfrak{B}(p\langle\sigma, \sigma_2\rangle)$ *различны, то* $\varphi(q_0, p)$ *и* $\lambda(r_0, p)$ — *σ-автономные состояния.*

Доказательство леммы содержится в Приложении.

Фиксируем $\xi\in\mathrm{T}_2$.

Определение. Пусть $\mathfrak{A}=\langle\Sigma_1\times\Sigma_2,\ Q,\ \mathrm{T}_1\times\mathrm{T}_2,\ q_0,\ \varphi,\ \psi\rangle$ — схемный автомат. Нормальной формой автомата $\mathfrak{A}$ называется автомат $\mathfrak{A}^{\text{н}}=\langle\Sigma_1\times\Sigma_2,\ Q,\ \mathrm{T}_1\times\mathrm{T}_2,\ q_0,\ \varphi,\ \mu\rangle$, где $\mu^1(q,\sigma)=\psi^1(q,\sigma)$;

$$\mu^2(q,\langle\sigma_1,\sigma_2\rangle)=\begin{cases}\xi, & \text{если } q \text{ — } \sigma_1\text{-автономное состояние},\\ \psi^2(q,\langle\sigma_1,\sigma_2\rangle) & \text{— в противном случае.}\end{cases}$$

Очевидно, $\mathfrak{A}^{\text{н}}$ — схемный автомат.

Лемма 2. *Автоматы $\mathfrak{A}$ и $\mathfrak{A}^{\text{н}}$ s-эквивалентны.*

Доказательство сразу следует из леммы 1 и определения $\mathfrak{A}^{\text{н}}$.

Следствие. *Схемные автоматы s-эквивалентны тогда и только тогда, когда их нормальные формы s-эквивалентны.*

Лемма 3. *Схемные автоматы s-эквивалентны тогда и только тогда, когда их нормальные формы эквивалентны.*

Доказательство. Достаточность очевидна из следствия к лемме 2. Докажем необходимость. Пусть $\mathfrak{A}=\langle\Sigma_1\times\Sigma_2,\ Q,\ \mathrm{T}_1\times\mathrm{T}_2,\ q_0,\ \varphi,\ \psi\rangle$ и $\mathfrak{B}=\langle\Sigma_1\times\Sigma_2,\ R,\ \mathrm{T}_1\times\mathrm{T}_2,\ r_0,\ \lambda,\ \mu\rangle$ — схемные автоматы. Пусть автоматы $\mathfrak{A}^{\text{н}}$ и $\mathfrak{B}^{\text{н}}$ не эквивалентны и $x=y\langle\sigma_1,\sigma_2\rangle$ — слово минимальной длины, s-различающее $\mathfrak{A}^{\text{н}}$ и $\mathfrak{B}^{\text{н}}$ (здесь $\langle\sigma_1,\sigma_2\rangle\in\Sigma_1\times\Sigma_2$). Если $(\mathfrak{A}^{\text{н}}(x))^1\neq(\mathfrak{B}^{\text{н}}(x))^1$, то $\mathfrak{A}^1(x)\neq\mathfrak{B}^1(x)$ и, по лемме 1, $\mathfrak{A}\underset{s}{\not\sim}\mathfrak{B}$. Пусть $(\mathfrak{A}^{\text{н}}(x))^2\neq(\mathfrak{B}^{\text{н}}(x))^2$. Хотя бы одно из слов $\mathfrak{A}^2(x)$ и $\mathfrak{B}^2(x)$ не оканчивается буквой ξ (иначе $\mathfrak{A}^2(x)=\mathfrak{B}^2(x)$). В силу определения нормальной формы отсюда следует, что $\varphi(q_0,y)$ или $\lambda(r_0,y)$ — не σ_1-автономное состояние и по лемме 1, $\mathfrak{A}\underset{s}{\not\sim}\mathfrak{B}$.

Теорема 1. *Пусть $\mathfrak{A}\in sk(\Sigma_1\times\Sigma_2,\ \mathrm{T}_1\times\mathrm{T}_2)$. Существует алгоритм построения автомата минимального веса, s-эквивалентного $\mathfrak{A}$. Нормальные формы любых двух таких автоматов изоморфны.*

Доказательство. Рассмотрим инициальный автомат $\mathfrak{B}$ — приведенный автомат, эквивалентный $\mathfrak{A}^{\text{н}}$. В силу лемм 2 и 3, $\mathfrak{B}\underset{s}{\sim}\mathfrak{A}$. Заметим, что $\mathfrak{B}^{\text{н}}$ изоморфно $\mathfrak{B}$. Пусть автомат $\mathfrak{C}$ s-эквивалентен автомату $\mathfrak{A}$. По лемме 3, $\mathfrak{C}^{\text{н}}\sim\mathfrak{B}$. Если $|\mathfrak{C}|=|\mathfrak{C}^{\text{н}}|\leqslant|\mathfrak{B}|$, то по теореме Мура, $\mathfrak{C}^{\text{н}}$ и $\mathfrak{B}$ изоморфны.

§ 3. Оценки сложности s-различения автоматов

Пусть $\mathfrak{A}$, $\mathfrak{B}$ — не s-эквивалентные схемные автоматы. В качестве меры сложности рассматривается минимум по всем парам, состоявшим из автомата X и слова p, s-различающим $\mathfrak{A}$ и $\mathfrak{B}$, следующих величин: 1) $l(p)$ — длины слова p; 2) $|X|$ — количества состояний автомата X; 3) $l(p)+|X|$.

Лемма 4. *Пусть $\mathfrak{A}$, $\mathfrak{B}\in sk(\Sigma_1\times\Sigma_2,\ \mathrm{T}_1\times\mathrm{T}_2)$; $\mathfrak{A}\underset{1}{\not\sim}\mathfrak{B}$; $|\mathfrak{A}|\leqslant n$ и $|\mathfrak{B}|\leqslant n$. Тогда существует слово $p\in\Sigma_1^*$ и автомат $X\in k(\mathrm{T}_2,\Sigma_2)$, s-различающие $\mathfrak{A}$ и $\mathfrak{B}$, для которых $l(p)\leqslant 2n-1$ и $|X|\leqslant 2n-1$.*

Доказательство. По условию $\mathfrak{A}^1\not\sim\mathfrak{B}^1$. По теореме Мура существует слово z длины не более $2n-1$, различающее $\mathfrak{A}$ и $\mathfrak{B}$. Тогда z^1 и автомат, перерабатывающий любое слово из T_2^* в слово, начинающееся с z^2, или в начало z^2, s-различают $\mathfrak{A}$ и $\mathfrak{B}$. Очевидно, этот автомат можно выбрать так, чтобы его вес не превосходил $2n-1$.

Лемма 5. *Пусть $\mathfrak{A}$ и $\mathfrak{B}$ — схемные 1-эквивалентные автоматы, вес которых не превосходит n и $\mathfrak{A}\underset{s}{\not\sim}\mathfrak{B}$. Пусть $k>0$ и $\mathfrak{A}$ и $\mathfrak{B}$ не различимы никаким словом длины менее $n+k$. Тогда в $\mathfrak{A}$ и в $\mathfrak{B}$ не более $n-k$ классов 1-неразличимых состояний, т. е. вес $\mathfrak{A}^1$ и $\mathfrak{B}^1$ не более $n-k$.*

Доказательство леммы приведено в Приложении.

Теорема 2. *Пусть $\mathfrak{A}$ и $\mathfrak{B}$ — схемные не s-эквивалентные автоматы, вес которых не превосходит n. Существуют слово p и автомат X, s-различающие $\mathfrak{A}$ и $\mathfrak{B}$, такие, что*

1) $l(p)\leqslant 3n-1$;
2) $|X|\leqslant 2n-3$;
3) $l(p)+|X|\leqslant 4n+3$.

Теорема 3. *Существуют схемные не s-эквивалентные автоматы* $\mathfrak{A}$, $\mathfrak{B}\in sk(\{0\}\times\{0, 1\}, \{0, 1\}\times\{0, 1\})$ *такие, что*: 1) $|\mathfrak{A}|=|\mathfrak{B}|=n$; 2) *если слово* p *и автомат* X *s-различают* $\mathfrak{A}$ *и* $\mathfrak{B}$, *то* $l(p)\geqslant 3n-5$.

Теорема 4. *Существуют схемные не s-эквивалентные автоматы* $\mathfrak{A}$, $\mathfrak{B}\in sk(\{0\}\times\{0, 1, 2\}, \{0, 1\}\times\{0, 1\})$, *такие, что*: 1) $|\mathfrak{A}|=|\mathfrak{B}|=n$; 2) *если слово* p *и автомат* X *s-различают* $\mathfrak{A}$ *и* $\mathfrak{B}$, *то* $|X|\geqslant 2n-4$; $l(p)+|X|\geqslant 4n+6$.

Доказательство теорем 2—4 приведено в Приложении.

Из теоремы 2 следует

Теорема 5. *Существует алгоритм проверки s-эквивалентности схемных конечных автоматов.*

Другой алгоритм проверки схемной эквивалентности следует из леммы 3 и алгоритма проверки эквивалентности конечных автоматов.

Автор благодарит А. А. Мучника за постановку задачи и постоянное внимание к работе и А. Л. Семенова за помощь при подготовке работы к печати.

ПРИЛОЖЕНИЕ

1. Доказательство леммы. 1. Необходимость. Если $\mathfrak{A}\underset{1}{\nsim}\mathfrak{B}$, то, очевидно $\mathfrak{A}\underset{s}{\nsim}\mathfrak{B}$. Пусть $\mathfrak{A}\underset{1}{\sim}\mathfrak{B}$; $\mathfrak{A}^2(p\langle\sigma, \sigma_1\rangle)\neq\mathfrak{B}^2(p\ \langle\sigma, \sigma_2\rangle)$ и $q=\varphi(q_0, p)$ — не σ-автономное состояние. По определению σ-автономного состояния найдутся $u\in\sigma\Sigma_1^*$; v, $w\in\Sigma_2^*$, такие, что $\psi^1(q, \langle u, v\rangle)\neq\psi_1(q, \langle u, w\rangle)$. Пусть $\lambda(r_0, p)=r$. Так как $\mathfrak{A}\underset{1}{\sim}\mathfrak{B}$, то $\psi^1(q, \langle u, v\rangle)=\mu^1(r, \langle u, v\rangle)$, следовательно, $\psi^1(q, \langle u, w\rangle)\neq\mu^1(r, \langle u, v\rangle)$. Ясно, что существует автомат $X\in k(\mathrm{T}, \Sigma)$, такой что X и $p_1\cdot\in\Sigma_1^*$ s-различают $\mathfrak{A}$ и $\mathfrak{B}$.

Достаточность. Пусть автомат X и $t\in\Sigma_1^*$ s-различают $\mathfrak{A}$ и $\mathfrak{B}$. Рассмотрим слово p_1 (соответственно p_2), которое поступает на вход $\mathfrak{A}(\mathfrak{B})$ при работе стандартной схемы с базисным автоматом $\mathfrak{A}(\mathfrak{B})$ и автоматом обратной связи X над входом t. По определению работы схемы, $\mathfrak{A}^1(p_1)\neq\mathfrak{B}^1(p_2)$. Если $p_1=p_2$, то $\mathfrak{A}^1\underset{1}{\nsim}\mathfrak{B}^1$, и лемма доказана.

Пусть $p_1\neq p_2$. Из определения стандартной схемы ясно, что найдется p_3 — общее начало p_1 и p_2, такое, что $p_1=p_3\langle\sigma, \sigma_1\rangle z_1$; $p_2=p_3\langle\sigma, \sigma_2\rangle z_2$ и $\mathfrak{A}^2(p_3\langle\sigma, \sigma_1\rangle)\neq\mathfrak{B}^2(p_3\langle\sigma, \sigma_2\rangle)$. Если $\varphi(q_0, p_3)$ и $\lambda(r_0, p_3)$ — σ-автономные состояния, то $\mathfrak{A}^1(p_2)=\mathfrak{A}^1(p_1)\neq\mathfrak{B}^1(p_2)$ вопреки предположению, что $\mathfrak{A}\underset{1}{\sim}\mathfrak{B}$. Следовательно, $\varphi(q_0, p_3)$ или $\lambda(r_0, p_3)$ — σ-автономное состояние.

2. Доказательство леммы 5. Можно считать, что $\mathfrak{A}$ и $\mathfrak{B}$ — приведенные автоматы. Достаточно доказать лемму для автомата $\mathfrak{B}$. Пусть $\mathfrak{A}=\langle\Sigma_1\times\Sigma_2, Q, \mathrm{T}_1\times\mathrm{T}_2, q_0, \varphi, \psi\rangle$; $\mathfrak{B}=\langle\Sigma_1\times\Sigma_2, R, \mathrm{T}_1\times\mathrm{T}_2, r_0, \lambda, \mu\rangle$ и $x=\sigma_1\ldots\sigma_{n+k}$ — слово минимальной длины, различающее $\mathfrak{A}$ и $\mathfrak{B}$. Пусть $q^0q^1\ldots q^{n+k}(r^0r^1\ldots r^{n+k})$ — внутреннее слово автомата $\mathfrak{A}(\mathfrak{B})$ при работе над словом x. Введем новое обозначение. Если r_1, $r_2\in R$, то $r_1\sim r_2$ обозначает, что для любого $z\in(\Sigma_1\times\Sigma_2)^*$ выполнено $\mu^1(r_1, z)=\mu(r_2, z)$. Для $q\in Q$, $r\in R$ отношение $q\underset{1}{\nsim}r$ определяется аналогично.

Пусть $q^i=q^j$ $(i<j<n+k)$. Тогда

(П.1) $\qquad r^i\neq r^j$,

(П.2) $\qquad r^i\underset{1}{\sim}r^j$.

Действительно, если $r^i=r^j$, то $\sigma_1\ldots\sigma_i\sigma_{j+1}\ldots\sigma_{n+k}$ — слово длины менее $n+k$, различающее $\mathfrak{A}$ и $\mathfrak{B}$. Если $r^i\underset{1}{\nsim}r^j$, то или $r^i\underset{1}{\nsim}q^i$, или $r^j\underset{1}{\nsim}q^j$. Пусть, например, $q^i\underset{1}{\nsim}r^i$ и $\psi^1(q^i, y)\neq\mu^1(r^i, y)$ для некоторого $y\in(\Sigma_1\times\Sigma_2)^*$. Тогда $\psi^1(q_0, \sigma_1\ldots\sigma_iy)\neq\mu^1(r_0, \sigma_1\ldots\sigma_iy)$ вопреки условию $\mathfrak{A}^1\sim\mathfrak{B}^1$.

Число j $(0<j<n+k)$ будем называть повторным номером, если найдется $i<j$, для которого $q^i=q^j$. Так как вес $\mathfrak{A}$ не более n, то повторных номеров не менее k. Пусть имеется l повторных номеров $i_1<\ldots<i_l<n+k$. Обозначим $i_m'=\min\{j\,|\,q^j=q^{i_m}\}$ $(m=1,\ldots, l)$ и рассмотрим следующую последовательность $D_0, D_1,\ldots, D_l$ разбиений множества R. Разбиение D_0 — единичное (никакие два состояния не лежат на одном классе разбиения). Пусть построено D_{m-1} $(1\leqslant m\leqslant l)$. Разбиение D_m получается из D_{m-1} объединением классов, которые содержат q^{i_m} и $q^{i'_m}$. Покажем, что для любого $m\leqslant l$ разбиение D_{m-1} — собственное подразбиение D_m, т. е.

(П.3) $\qquad \forall m\, r^{i_m}\underset{D_{m-1}}{\nsim}r^{i'_m}$.

В силу (П.1) и (П.3) в разбиении D_l ровно $|R|-l\leqslant n-l$ классов. Ввиду (П.2) D_l – подразбиение разбиения, соответствующего отношению 1-эквивалентности. Поэтому, доказав (П.3), мы докажем лемму.

Пусть для некоторого m $r^{i_m} \underset{D_{m-1}}{\sim} r^{i_m'}$, т. е. найдутся $j_1<j_m, \ldots, j_t<i_m$, такие, что

(П.4) $\qquad r^{i'_m}=r^{j_1};\ q^{j_1}=q^{j_2};\ r^{j_2}=r^{j_3}; \ldots ;\ q^{j_{t-1}}=q^{j_t};\ r^{j_t}=r^{j_m}.$

Для удобства обозначим i_m' через j_0. Рассмотрим слова вида

$$\sigma_1 \ldots \sigma_{j_s}\sigma_{i_m+1} \ldots \sigma_{n+k} \qquad (s=0, 1, \ldots, t).$$

Так как длина каждого такого слова меньше $n+k$, то для всех $s=0, 1, \ldots, t$

$$\psi(q_0, \sigma_1 \ldots \sigma_{j_s}\sigma_{i_m+1} \ldots \sigma_{n+k})=\mu(r_0, \sigma_1 \ldots \sigma_{j_s}\sigma_{i_m+1} \ldots \sigma_{n+k}),$$

т. е.

(П.5) $\qquad \psi(q^{j_s}, \sigma_{i_m+1} \ldots \sigma_{n+k})=\mu(r^{j_s}, \sigma_{i_m+1} \ldots \sigma_{n+k}).$

Но

(П.6) $\qquad q^{j_0}=q^{i_m'}=q^{i_m}.$

Из (П.4) – (П.6) следует, что $\psi(q^{i_m}, \sigma_{i_m+1} \ldots \sigma_{n+k})=\mu(r^{i_m}, \sigma_{i_m+1} \ldots \sigma_{n+k})$ вопреки предположению, что $\sigma_1 \ldots \sigma_{n+k}$ различает $\mathfrak{A}$ и $\mathfrak{B}$.

3. Доказательство теоремы 2. Если $\mathfrak{A}\underset{1}{\nsim}\mathfrak{B}$, то все уже доказано в лемме 4. Поэтому в дальнейшем будем считать, что $\mathfrak{A}\underset{1}{\sim}\mathfrak{B}$. По лемме 3, $\mathfrak{A}^{\text{н}}$ и $\mathfrak{B}^{\text{н}}$ — нормальные формы автоматов $\mathfrak{A}$ и $\mathfrak{B}$ – не эквивалентны. Пусть $x\sigma$, где $\sigma\in\Sigma_1\times\Sigma_2$,– слово минимальной длины, различающее $\mathfrak{A}$ и $\mathfrak{B}$ и $l(x\sigma)=n+k$ (для простоты мы далее считаем, что $k\geqslant0$; если $k<0$, то достаточно оценки $l(x\sigma)\leqslant n$). Фиксируем слово $x\sigma$ и состояние $q_1=\varphi(q_0, x)$.

Можно считать, что q_1 не σ^1-автономное состояние. Далее мы всюду, говоря «состояние $q\in Q$», будем иметь в виду состояние, достижимое из q_1 таким словом z, что первая буква z^1 совпадает с σ^1. Пусть $\mathfrak{A}^{\text{п}}=\langle\Sigma_1\times\Sigma_2, Q^{\text{п}}, \mathrm{T}_1, q_0^{\text{п}}, \varphi^{\text{п}}, \psi^{\text{п}}\rangle$ — приведенный автомат, эквивалентный $\mathfrak{A}^1$. Для каждого $q\in Q$ через $q^{\text{п}}$ будем обозначать соответствующее состояние автомата $\mathfrak{A}^{\text{п}}$.

Введем новые обозначения. Для каждого $q^{\text{п}}\in Q^{\text{п}}$, отличного от $q_1^{\text{п}}$, через $l(q^{\text{п}})$ обозначим

$$l(q^{\text{п}}=\min \{l' \mid \exists y_1\in\Sigma_1^*\exists y_2,\ y_3\in\Sigma_2^*(l(y_1)=l(y_2)=$$
$$=l(y_3)=l'\wedge\psi^{\text{п}}(q^{\text{п}}, \langle y_1, y_2\rangle)\neq\psi^{\text{п}}(q^{\text{п}}, \langle y_1, y_2\rangle))\}.$$

Через $l(q_1^{\text{п}})$ обозначим

$$l(q_1^{\text{п}})=\min\{l' \mid \exists y_1\in\sigma^1\Sigma_1^*\exists y_2,\ y_3\in\Sigma_2^*(l(y_1)=$$
$$=l(y_2)=l(y_3)=l'\wedge\psi^{\text{п}}(q_1^{\text{п}}, \langle y_1, y_2\rangle)\neq\psi^{\text{п}}(q_1^{\text{п}}, \langle y_1, y_3\rangle))\}.$$

Через l обозначим минимум $l(q^{\text{п}})$ по всем состояниям $q^{\text{п}}\in Q^{\text{п}}$, для которых $l(q^{\text{п}})$ определено. Так как q_1 – не σ^1-автономное состояние, то l определено.

Далее, обозначим через r минимальный элемент множества

(П.7) $$\{r' \mid \exists y_1\in\sigma^1\Sigma_1^*\exists y_2,\ y_3\in\Sigma_2^*(l(y_1)=l(y_2)=l(y_3)=$$
$$=r'\wedge\varphi^{\text{п}}(q_1^{\text{п}}, \langle y_1,y_2\rangle)\neq\varphi^{\text{п}}(q_1^{\text{п}}, \langle y_1, y_3\rangle))\}.$$

Если множество (П.7) пусто, то будем считать, что $r=\infty$. Если $r=\infty$, то $l=1$ (иначе q_1 – σ^1-автономное состояние). Если $r<\infty$, то, очевидно, $r\leqslant|\mathfrak{A}^{\text{п}}|\leqslant n-k$ (см. лемму 5). Следовательно, $\min \{l, r\}\leqslant n-k$. Рассмотрим отдельно случаи $l\leqslant r$ и $l>r$:

а) $l\leqslant r$. Пусть $q_2^{\text{п}}\in Q^{\text{п}}$, z_1, z_2, z_3, таковы, что $l(z_1)=l(z_2)=l(z_3)=l$ и $\psi^{\text{п}}(q_2^{\text{п}}, \langle z_1, z_2\rangle)\neq\psi^{\text{п}}(q_2^{\text{п}}, \langle z_1, z_3\rangle)$ (если $q_2^{\text{п}}=q_1^{\text{п}}$, то потребуем, чтобы $z_1\in\sigma^1\Sigma_1^*$). Пусть v – такое кратчайшее слово, что первая буква v^1 совпадает с σ^1 и $\varphi^{\text{п}}(q_1^{\text{п}}, v)=$ $=q_2^{\text{п}}$ (если $q_2^{\text{п}}=q_1^{\text{п}}$, то $v=\Lambda$). Очевидно, $l(v)\leqslant|\mathfrak{A}^{\text{п}}|\leqslant n-k$, т. е. $l(v^1z_1)\leqslant n-k+\min\{l, r\}$ и $\psi^{\text{п}}(q_1^{\text{п}}\langle v^1z_1, v^2z_2\rangle)\neq\psi^{\text{п}}(q_1^{\text{п}}, \langle v^1z_1, v^2z_3\rangle)$.

б) $l\geqslant r+1$. Пусть $z_1\in\sigma_1\Sigma_1^*$; $z_1, z_2\in\Sigma_2^*$; $l(z_1)=l(z_2)=l(z_3)=r$ и $\varphi^{\text{п}}(q_1^{\text{п}}, \langle z_1, z_2\rangle)\neq$ $\neq\varphi^{\text{п}}(q_1^{\text{п}}, \langle z_1, z_3\rangle)$. Пусть v – слово минимальной длины, различающее состояния $\varphi^{\text{п}}(q_1^{\text{п}}, \langle z_1, z_2\rangle)$ и $\varphi^{\text{п}}(q_1^{\text{п}}, \langle z_1, z_3\rangle)$. Очевидно, $l(v)\leqslant|\mathfrak{A}^{\text{п}}|-1\leqslant n-k-1$. Поэтому $l(z_1, v^1)\leqslant n-k+\min \{l, r\}$ и $\psi^{\text{п}}(q_1^{\text{п}}, \langle z_1v^1, z_2v^2\rangle)\neq\psi^{\text{п}}(q_1^{\text{п}}, \langle z_1v^1, z_2v^3\rangle)$.

Фиксируем такие слова $y_1\in\sigma^1\Sigma_1^*$ и y_2, $y_3\in\Sigma_2^*$ минимальной длины, что $\psi^{\text{п}}(q_1^{\text{п}}, \langle y_1, y_2\rangle)\neq\psi^{\text{п}}(q_1^{\text{п}}, \langle y_1, y_3\rangle)$. В силу вышеизложенного $l(y_1)=l(y_2)=l(y_3)\leqslant$ $\leqslant n-k+\min\{l, r\}$. Фиксируем $\theta\in\Sigma_2$. Можно считать, что

(П.8) $\qquad \psi^{\text{п}}(q_1^{\text{п}}, \langle y_1, y_2\rangle)\neq\psi^{\text{п}}(q_1^{\text{п}}, \langle y_1, \theta^{l(y_1)}\rangle)$

(иначе $\psi^{\text{п}}(q_1{}^{\text{п}}, \langle y_1, y_3\rangle)\neq\psi^{\text{п}}(q_1{}^{\text{п}}, \langle y_1, \theta^{l(y_1)}\rangle)$). Положим

$$s=\begin{cases} r, & \text{если} \quad r<\infty, \\ l(y_1), & \text{если} \quad r=\infty. \end{cases}$$

Пусть $\langle u, v\rangle$ – начало $\langle y_1, y_2\rangle$ длины $s-1$; $y_2=vv_1$ и $v'\in\Sigma_2{}^*$ – произвольное слово длины $s-1$. Очевидно, $\varphi^{\text{п}}(q_1{}^{\text{п}}, \langle u, v\rangle)=\varphi^{\text{п}}(q_1{}^{\text{п}}, \langle u, v'\rangle)$ и $\psi^{\text{п}}(q_1{}^{\text{п}}, \langle y_1, y_2\rangle)=\psi^{\text{п}}(q_1{}^{\text{п}}, \langle y_1, v'v_1\rangle)$. Из определения l следует, что $l(v_1)>l-1$. Пусть $v_1=zw$, где $l(w)=l-1$ и $w'\in\Sigma_2{}^*$ – произвольное слово длины $l-1$. Тогда

(П.9) $$\psi^{\text{п}}(q_1{}^{\text{п}}, \langle y_1, v'zw'\rangle)=\psi^{\text{п}}(q_1{}^{\text{п}}, \langle y_1, y_2\rangle),$$

(П.10) $$l(z)\leqslant n-k-s-l+2\leqslant n-k-\min\{l, r\}+2.$$

Рассмотрим такой автомат X, что при работе стандартной схемы с базисным автоматом $\mathfrak{A}$ (соответственно $\mathfrak{B}$) и автоматом обратной связи X над словом x^1y_1 на вход базисного автомата поступает слово $\langle x^1y_1, x^2v^{\text{п}}z\tilde{w}\rangle$ (соответственно $\langle x^1y_1, x^2\theta^{l(y_1)}\rangle$), где $l(v^{\text{п}})=s-1$; $l(\tilde{w})=l-1$. В силу (П.8) и (П.9) слово x^1y_1, и автомат X s-различают $\mathfrak{A}$ и $\mathfrak{B}$.

Мы построим автомат X, удовлетворяющий приведенным выше требованиям, причем $|X|\leqslant 2n+3-\min\{l, r\}$. Этим теорема будет доказана. Автомат X строится по-разному в случаях $r>1$ и $r=1$. Мы разберем только случай $r>1$, в случае $r=1$ искомый автомат строится аналогично. Пусть $z=z_1\ldots z_t$; $x^2=a_1\ldots a_{n+k}$; $h=\operatorname{rest}(s-1, t)$. Искомым автоматом будет автомат $\langle \mathrm{T}_2, C, \Sigma_2, f_1, \alpha, \beta\rangle$, где $C=\{f_1,\ldots,f_{n+k}, d, c_1,\ldots,c_t\}$.

$$\alpha(f_i, \tau)=f_{i+1} \quad (i=1,\ldots,n-k-1;\ \tau\in\mathrm{T}_2),$$

$$\alpha(f_{n+k}, \tau)=\begin{cases} c_1, & \text{если} \quad \tau=\psi^2(x\sigma), \\ d, & \text{если} \quad \tau\neq\psi^2(x\sigma), \end{cases}$$

$$\alpha(d, \tau)=d \quad (\tau\in\mathrm{T}_2),$$

$$\alpha(c_i, \tau)=\begin{cases} c_{i+1}, & \text{если} \quad i<t, \\ c_1, & \text{если} \quad i=t \end{cases} \quad (\tau\in\mathrm{T}),$$

$$\beta(f_i, \tau)=a_i, \quad (i=1,\ldots,n+k-1;\ \tau\in\mathrm{T}_2),$$

$$\beta(f_{n+k}, \tau)=\beta(d, \tau)=\theta \quad (\tau\in\mathrm{T}_2),$$

$$\beta(c_i, \tau)=\begin{cases} z_{t+h-i}, & \text{если} \quad i=1,\ldots,h, \\ z_{i-h}, & \text{если} \quad i=h+1,\ldots,t \end{cases} \quad (\tau\in\mathrm{T}_2).$$

В силу (П.10) $|X|=n+k+t+1\leqslant 2n+3-\min\{r, l\}$. Теорема доказана.

4. Доказательство теоремы 3. Пусть $\mathfrak{A}=\langle\{0\}\times\{0, 1\}, Q, \{0, 1\}\times\{0, 1\}, q_1, \varphi, \psi\rangle$, где $Q=\{q_1,\ldots,q_n\}$; $\varphi(q_i, \sigma)=q_{i+1}$, где $i=1,\ldots,n-3$; $\sigma=\langle 0, 0\rangle, \langle 0, 1\rangle$,

$$\varphi(q_{n-2}, \sigma)=\begin{cases} q_{n-1}, & \sigma=\langle 0,0\rangle, \\ q_n, & \sigma=\langle 0,1\rangle, \end{cases}$$

$$\varphi(q_{n-1}, \sigma)=q_2; \quad \varphi(q_n, \sigma)=q_1 \quad (\sigma=\langle 0, 0\rangle, \langle 0, 1\rangle),$$

$$\psi(q_i, \sigma)=\langle 0, 0\rangle \quad (i=1,\ldots,n-1;\ \sigma=\langle 0, 0\rangle, \langle 0, 1\rangle),$$

$$\psi(q_n, \sigma)=\langle 1, 0\rangle \quad (\sigma=\langle 0, 0\rangle, \langle 0, 1\rangle).$$

Автомат $\mathfrak{B}=\langle\{0\}\times\{0, 1\}, Q, \{0, 1\}\times\{0, 1\}, q, \varphi, \mu\rangle$ отличается от $\mathfrak{A}$ лишь тем, что $\mu(q_n, \langle 0, \theta\rangle)=\langle 1, 1\rangle$ при $\theta=1, 2$. Для всех остальных $q\in Q$ и $\sigma\in\{0\}\times\{0, 1\}$ выполнено $\mu(q, \sigma)=\psi(q, \sigma)$. Очевидно, $\mathfrak{A}\underset{1}{\sim}\mathfrak{B}$ и, если $\mathfrak{A}(v)\neq\mathfrak{B}(v)$, то $l(v)\geqslant n-2$; $\varphi(q_1, v)=q_1$. Далее, если для p_1, p_2, p_3 верно $\psi^1(q_1, \langle p_1, p_2\rangle)\neq\mu^1(r_1, \langle p_1, p_3\rangle)$, то $l(p_1)=l(p_2)=l(p_3)\geqslant 2n-3$. Следовательно, если слово p и автомат X s-различают $\mathfrak{A}$ и $\mathfrak{B}$, то $l(p)\geqslant 3n-5$.

5. Доказательство теоремы 4. Пусть $\mathfrak{A}=\langle\{0\}\times\{0, 1, 2\}, Q, \{0, 1\}\times\{0, 1\}, q_1, \varphi, \psi\rangle$, где $Q=\{q_1,\ldots,q_n\}$,

$$\varphi(q_i, \langle 0, \theta\rangle)=\begin{cases} q_{i+1}, & \text{если} \quad \theta=0, \\ q_1, & \text{если} \quad \theta=1, 2 \end{cases} \quad [i=1,\ldots,n-3),$$

$$\varphi(q_{n-2}, \langle 0, \theta\rangle)=\begin{cases} q_1 & \text{если} \quad \theta=0,\\ q_{n-1}, & \text{если} \quad \theta=1,\\ q_n, & \text{если} \quad \theta=2,\end{cases}$$

$$\varphi(q_{n-1}, \langle 0, \theta\rangle)=\varphi(q_n, \langle 0, \theta\rangle)=q_1,$$

$$\psi(q_i, \langle 0, \theta\rangle)=\begin{cases} \langle 0, 0\rangle, & \text{если} \quad i=1,\ldots,n-2,\\ \langle 0, 1\rangle, & \text{если} \quad i=n-1,\\ \langle 1, 0\rangle, & \text{если} \quad i=n \quad (\theta=0, 1, 2).\end{cases}$$

Автомат $\mathfrak{B}=\langle\{0\}\times\{0, 1, 2\}, Q, \{0, 1\}\times\{0, 1\}, q_1, \varphi, \mu\rangle$ отличается от $\mathfrak{A}$ лишь тем, что $\mu(q_{n-1}, \langle 0, \theta\rangle)=\langle 0, 0\rangle$ при $\theta=1, 2, 3$. Для всех остальных состояний q и входных сигналов σ выполнено $\mu(q, \sigma)=\psi(q, \sigma)$. Очевидно,

(П.11) $\quad \mathfrak{A}\underset{1}{\sim}\mathfrak{B}.$

Рассмотрим автомат $X=\langle\{0, 1\}, C, \{0, 1, 2\}, c_0, \alpha, \beta\rangle$ и слово $p\in\Sigma_1^*$, s-различающие $\mathfrak{A}$ и $\mathfrak{B}$. Пусть $\langle p, v\rangle$ (соответственно $\langle p, w\rangle$) – слово, которое подается на вход базисного автомата при работе стандартной схемы с базисным автоматом $\mathfrak{A}$ (соответственно $\mathfrak{B}$) и автоматом обратной связи X над словом p. Очевидно,

(П.12) $\quad \psi^1(q_1, \langle p, v\rangle)\neq\mu^2(q_1, \langle p, w\rangle).$

Из доказательства леммы 1 видно, что найдется общее начало $\langle s, u\rangle$ слов $\langle p, v\rangle$ и $\langle p, w\rangle$ и буквы $\sigma_1\in\Sigma_1$; σ, $\xi\in\Sigma_2$, такие, что

$$\psi^2(q_1, \langle s\sigma_1, u\sigma\rangle)\neq\mu(q_1, \langle s\sigma_1, u\xi\rangle)$$

и для некоторых слов $p_1\in\Sigma_1^*$ и v_1, $w_1\in\Sigma_2^*$

(П.13) $\quad \langle p, v\rangle=\langle s\sigma_1p_1, u\sigma v_1\rangle; \quad \langle p, w\rangle=\langle s\sigma_1p_1, u\xi w_1\rangle.$

В силу определения автоматов $\mathfrak{A}$ и $\mathfrak{B}$ получаем, что для некоторых слов s' и u'

(П.14) $\quad \langle s, u\rangle=\langle s'0^{n-2}, u'0^{n-3}1\rangle,$

(П.15) $\quad \varphi(q_1, \langle s', u'\rangle)=q_1,$

(П.16) $\quad \varphi(q_1\langle s\sigma_1, u\sigma\rangle)=\varphi(q_1, \langle s\sigma_1, u\xi\rangle)=q_1.$

Из (П.11) – (П.13) и (П.16) следует

$$\psi^1(q_1, \langle p_1, v_1\rangle)\neq\psi^1(q_1, \langle p_1, w_1\rangle).$$

Очевидно, одно из слов $\langle p_1, v_1\rangle$ и $\langle p_1, w_1\rangle$ имеет вид $\langle p_2, 0^{n-1}, x0^{n-3}2\theta\rangle$, где $\theta\in\{0, 1, 2\}$, причем

(П.17) $\quad \varphi(q_1, \langle p_2, x\rangle)=q_1.$

Пусть, например,

(П.18) $\quad \langle p_1, v_1\rangle=\langle p_20^{n-1}, x0^{n-3}2\theta\rangle.$

Из (П.13), (П.14), (П.18) следует, что $l(p)\geqslant 2n-2$.

Обозначим $\psi^2(q_1, \langle s', u'\rangle)$ через z_1 и $\psi^2(q_1, \langle s\sigma_1p_2, u\sigma x\rangle)$ через z_2; $\alpha(c_0, z_1)$ — через c_1 и $\alpha(c_0, z_2)$ – через c_2. Так как $\psi(q_1, \langle 0^{n-2}, 0^{n-3}1\rangle)=\psi(q_1, \langle 0^{n-2}, 0^{n-3}2\rangle)=\langle 0^{n-2}, 0^{n-2}\rangle$, то из (П.15) и (П.14), (П.17) и (П.18) получаем $\beta(c_1, 0^{n-2})=0^{n-3}1$; $\beta(c_2, 0^{n-2})=0^{n-3}2$.

Очевидно, все состояния вида $\alpha(c_1, 0^i)$ и $\alpha(c_2, 0^i)$, где $i=0,\ldots,n-3$, попарно различны, т. е. $|X|\geqslant 2n-4$.

ЛИТЕРАТУРА

1. *Летичевский А. А.* Функциональная эквивалентность дискретных преобразователей, III. Кибернетика, 1972, *1*, 1—4.
2. *Кобринский Н. К., Трахтенброт Б. А.* Введение в теорию конечных автоматов. М., Физматгиз, 1962.
3. *Трахтенброт Б. А., Барздинь Я. М.* Конечные автоматы. Поведение и синтез. М., «Наука», 1970.

Поступила в редакцию
23 июня 1975 г.