Основы теории конечных автоматов

Т. А. Новикова

Факультет ВМиК
Казахстанский филиал МГУ им.М. В. Ломоносова

15 мая 2016 г.

Алфавит $A = \{a_1, a_2, \ldots, a_r\}$ будем называть входным алфавитом, $B = \{b_1, b_2, \ldots, b_m\}$ — выходным алфавитом, а через A^∞, B^∞ будем обозначать множества всевозможных последовательностей в алфавитах A, B соответственною

Definition

Отображение $\phi : A^\infty \to B^\infty$ называется детерминированной функцией, если для любого $t = 1, 2, \ldots$ $b(t)$ однозначно определяется по $a(1), a(2), \ldots, a(t)$.

Definition

Отображение $\phi : A^\infty \to B^\infty$ называется **детерминированной функцией**, если для любого $t = 1, 2, \ldots$ $b(t)$ однозначно определяется по $a(1), a(2), \ldots, a(t)$.

Фактически, д-функция переводит последовательности в последовательности: $a_1(1) \ldots a_1(t) \ldots \to b_1(1) \ldots b_1(t) \ldots$, $a_2(1) \ldots a_2(t) \ldots \to b_2(1) \ldots b_2(t) \ldots$, при этом если $a_1(1) = a_2(1)$, то верно, что $b_1(1) = b_2(1)$ и такой набор равенств может быть продолжен на дальнейшие промежутки времени.

Definition

Пусть задана д-функция $\phi : A^\infty \to B^\infty$. Рассмотрим произвольное слово $\bar{a} = a_1 a_2 \dots a_k \in A^*$. Пусть $a(1), \dots, a(t) \dots$ — произвольная входная последовательность. Рассмотрим

$$\phi(a_1 a_2 \dots a_k a(1) a(2) \dots a(t) \dots) = b_1 b_2 \dots b_k b(1) b(2) \dots b(t) \dots$$

и положим $\phi_{\bar{a}}(a(1)a(2) \dots a(t) \dots) = b(1)b(2) \dots b(t) \dots$. Полученную функцию $\phi_{\bar{a}}$ назовем остаточной функцией для ϕ по слову $\bar{a} \in A^*$.

Definition

Детерминированная функция называется ограниченно-детерминированной, если у нее имеется лишь конечное число различных остаточных функций.

Definition

Автоматом (инициальным) называется любая шестёрка (A, B, Q, G, F, q_0), где A, B, Q — кончные алфавиты, $G : A \times Q \to Q$, $F : A \times Q \to B$, $q_0 \in Q$ — начальное(инициальное) состояние.

Definition

Автоматом (инициальным) называется любая шестёрка (A, B, Q, G, F, q_0), где A, B, Q — кончные алфавиты, $G : A \times Q \to Q$, $F : A \times Q \to B$, $q_0 \in Q$ — начальное(инициальное) состояние.

Входом автомата служит последовательность $a(1)a(2)a(3)\dots a(t)\dots \in A^*$ (конечная или бесконечная), выходом автомата служит последовательность $z(t)$, при этом автомат задаётся системой канонических уравнений:

$$\begin{cases} z(t) & = & F(x(t), q(t-1)), \\ q(t) & = & G(x(t), q(t-1)), \\ q(0) & = & q_0 \end{cases}$$

Definition

Отображение $\phi : A^\infty \to B^\infty$ называется автоматной функцией, если существует автомат, который реализует это отображение.

Definition

Отображение $\phi : A^\infty \to B^\infty$ называется автоматной функцией, если существует автомат, который реализует это отображение.

Утв. Функция является автоматной тогда и только тогда, когда она является ограниченно детерминированной.

Пример. Пусть $A = B = Q = \{0, 1\}$ и система канонических уравнений выглядит следующим образом:

$$\begin{cases} z(t) & = & q(t-1), \\ q(t) & = & x(t), \\ q(0) & = & 0 \end{cases}$$

Такой автомат называется единичной задержкой.

Definition

Диаграммой Мура для автомата называется ориентированный граф с множеством вершин Q, у которого каждой паре (a, q) сопоставляется дуга, идущая из вершины q в вершину, соответствующую $G(a, q)$. Этой дуге приписывается пометка $(a, F(a, q))$. Особым образом помечена вершина, соответствующая начальному состоянию. Диаграмма Мура однозначно задаёт автомат.

Definition

Схемой из функциональных элементов и элемента задержки(СФЭЗ) называется схема из функциональных элементов в функциональном базисе, к которому добавлен элемент, реализующий функцию единичной задержки. В схеме из функциональных элементов и элементов задержки допускаются ориентированные циклы, но любой ориентированный цикл должен проходить хотя бы через одну задержку.

В дальнейшем договоримся, что рассматриваем $A = B = \{0, 1\}$.

Theorem

Схема из функциональных элементов и задержки осуществляет автоматное отображение.

Доказательство. Пусть в схеме имеется r элементов задержки. Пусть i-я задержка R_i приписана вершине v_i, в которую идёт дуга из вершины w_i. Для всех $i = 1, \dots, r$ удалим из СФЭЗ дуги (w_i, v_i). Получим СФЭ.

Theorem

Схема из функциональных элементов и задержки осуществляет автоматное отображение.

Доказательство. Пусть в схеме имеется r элементов задержки. Пусть i-я задержка R_i приписана вершине v_i, в которую идёт дуга из вершины w_i. Для всех $i = 1, \ldots, r$ удалим из СФЭЗ дуги (w_i, v_i). Получим СФЭ.

Входами этой СФЭ будут все входы исходной схемы, а также все вершины $v_i, i = 1, \ldots, r$. Выходами полученной СФЭ объявим все выходы исходной схемы и вершины $w_i, i = 1, \ldots, r$.

Theorem

Схема из функциональных элементов и задержки осуществляет автоматное отображение.

Доказательство. Пусть в схеме имеется r элементов задержки. Пусть i-я задержка R_i приписана вершине v_i, в которую идёт дуга из вершины w_i. Для всех $i = 1, \ldots, r$ удалим из СФЭЗ дуги (w_i, v_i). Получим СФЭ.

Входами этой СФЭ будут все входы исходной схемы, а также все вершины $v_i, i = 1, \ldots, r$. Выходами полученной СФЭ объявим все выходы исходной схемы и вершины $w_i, i = 1, \ldots, r$.

Пусть в исходной схеме выходам приписаны переменные $z_1, \ldots, z_m$, входам — переменные $x_1, \ldots, x_n$. Вершинам v_i припишем переменные $q'_1, \ldots, q'_r$, а вершинам w_i — переменные $q_1, \ldots, q_r$.

В соответствии с определением функционирования СФЭ, для некоторых функций алгебры логики f_i, g_j справедливо:

$$\begin{cases} z_i & = & f_i(x_1, \ldots, x_n, q'_1, \ldots, q'_r), i = 1, \ldots, m \\ q_j & = & g_j(x_1, \ldots, x_n, q'_1, \ldots, q'_r), \ = 1, \ldots, r \end{cases}$$

Но поскольку это выполняется в каждый момент времени, то:

$$\begin{cases} z_i(t) & = & f_i(x_1(t), \ldots, x_n(t), q'_1(t), \ldots, q'_r(t)), i = 1, \ldots, m \\ q_j(t) & = & g_j(x_1(t), \ldots, x_n(t), q'_1(t), \ldots, q'_r(t)), j = 1, \ldots, r \end{cases}$$

Но для элемента единичной задержки его выход в момент t совпадает с его входом в момент $t-1$, тогда:

$$\begin{cases} z_i(t) & = & f_i(x_1(t), \ldots, x_n(t), q_1(t-1), \ldots, q_r(t-1)), i = 1, \ldots, m \\ q_j(t) & = & g_j(x_1(t), \ldots, x_n(t), q_1(t-1), \ldots, q_r(t-1)), j = 1, \ldots, r \\ q_j(0) & = & 0. \end{cases}$$

Но для элемента единичной задержки его выход в момент t совпадает с его входом в момент $t-1$, тогда:

$$\begin{cases} z_i(t) &= f_i(x_1(t),\ldots,x_n(t),q_1(t-1),\ldots,q_r(t-1)), i=1,\ldots,m \\ q_j(t) &= g_j(x_1(t),\ldots,x_n(t),q_1(t-1),\ldots,q_r(t-1)), j=1,\ldots,r \\ q_j(0) &= 0. \end{cases}$$

Полученные равенства — канонические уравнения СФЭЗ.

Пусть полученные канонические уравнения задают отображение ψ, осуществляемое схемой σ. Введем переменные $X = (x_1, \dots, x_n)$, $Q = (q_1, \dots, q_r)$, $Z = (z_1, \dots, z_m)$, принимающие значения из E_2^n, E_2^r, E_2^m соответственно. Положим $q_0 = (0, \dots, 0)$. Тогда каноническая система может быть переписана в виде:

$$\begin{cases} Z(t) = F(X(t), Q(t-1)), \\ Q(t) = G(X(t), Q(t-1)), \\ Q(0) = q_0, \end{cases}$$

где функции F, G не зависят явно от t. Отсюда видно, что отображение, осуществляемое схемой, совпадает с отображением, задаваемым автоматом $(E_2^n, E_2^r, E_2^m, G, F, q_0)$ то есть является автоматной функцией. $\square$

Definition

Пусть автоматная функция ϕ отображает последовательности в конечном алфавите A в последовательности в конечном алфавите B. Пусть СФЭЗ Σ осуществляет преобразование ψ последовательностей с элементами из E_2^n в последовательности с элементами из E_2^m. Будем говорить, что Σ моделирует ϕ, если существуют отображения $K_1 : A \to E_2^n$, $K_2 : B \to E_2^m$, сопоставляющие разным элементам разные элементы и обладающие свойством: для любой последовательности $p = a(1)a(2)\dots a(t)$ в алфавите A, если $\phi(P) = T = b(1)b(2)\dots b(t)$, то $\psi(K_1(P)) = K_2(T)$, где $K_1(P) = K_1(a(1))K_1(a(2))\dots K_1(a(t))$, $K_2(T) = K_2(b(1))K_2(b(2))\dots K_2(b(t))$.

Theorem

Для любой автоматной функции существует моделирующая её СФЭЗ в базисе из функциональных элементов дизъюнкции, конъюнкции, отрицания и элемента задержки.

Theorem

Для любой автоматной функции существует моделирующая её СФЭЗ в базисе из функциональных элементов дизъюнкции, конъюнкции, отрицания и элемента задержки.

Доказательство. Приведем этапы построения такой схемы. Пусть автоматная функция задана своим автоматом $D = (A, B, Q, G, F, q_0)$. Выберем n, m, r так, что $2^n \geq |A|, 2^m \geq |B|, 2^r \geq |Q|$. Рассмотрим произвольные отображения $K_1 : A \to E_2^n$, $K_2 : B \to E_2^m$, $K_3 : Q \to E_2^r$. Потребуем дополнительно, чтобы $K_3(q_0) = (0, \dots, 0)$.

Theorem

Для любой автоматной функции существует моделирующая её СФЭЗ в базисе из функциональных элементов дизъюнкции, конъюнкции, отрицания и элемента задержки.

Доказательство. Приведем этапы построения такой схемы. Пусть автоматная функция задана своим автоматом $D = (A, B, Q, G, F, q_0)$. Выберем n, m, r так, что $2^n \geq |A|, 2^m \geq |B|, 2^r \geq |Q|$. Рассмотрим произвольные отображения $K_1 : A \to E_2^n$, $K_2 : B \to E_2^m$, $K_3 : Q \to E_2^r$. Потребуем дополнительно, чтобы $K_3(q_0) = (0, \ldots, 0)$.

Рассмотрим отображения $G' : E_2^n \times E_2^r \to E_2^r$, $F' : E_2^n \times E_2^r \to E_2^m$ такие, что для любых $a \in A, q \in Q$ выполнено:

$$\begin{cases} G'(K_1(a), K_3(q)) & = & K_3(G(a, q)), \\ F'(K_1(a), K_3(q)) & = & K_2(F(a, q)) \end{cases}$$

Полученные равенства определяют отображения G', F' только для тех пар слов, которые являются кодами некоторых букв в алфавитах A, B. Для остальных пар отображения G', F' доопределяются произвольно.

Полученные равенства определяют отображения G', F' только для тех пар слов, которые являются кодами некоторых букв в алфавитах A, B. Для остальных пар отображения G', F' доопределяются произвольно.

Рассмотрим автомат $H = (E_2^n, E_2^m, E_2^r, G', F', \widetilde{0})$ с каноническими уравнениями:

$$\begin{cases} Z(t) & = & F'(X(t), Q(t-1)), \\ Q(t) & = & G'(X(t), Q(t-1)), \\ Q(0) = \widetilde{0}, & & \end{cases}$$

По построению видно, что если автомат D преобразует последовательность P в алфавите A в последовательность T в алфавите B, то H преобразует код $K_1(P)$ последовательности P в код $K_2(T)$ последовательности T. Осталось показать, что построенную автоматную функцию можно реализовать схемой.

Рассмотрим каждую из переменных X, Q, Z в виде вектор-набора переменных. Тогда система аналогична следующей:

$$\begin{cases} z_i(t) & = & f_i(x_1(t), \dots, x_n(t), q'_1(t), \dots, q'_r(t)), \\ q_j(t) & = & g_j(x_1(t), \dots, x_n(t), q'_1(t), \dots, q'_r(t)), \end{cases}$$

Рассмотрим каждую из переменных X, Q, Z в виде вектор-набора переменных. Тогда система аналогична следующей:

$$\begin{cases} z_i(t) & = & f_i(x_1(t), \ldots, x_n(t), q'_1(t), \ldots, q'_r(t)), \\ q_j(t) & = & g_j(x_1(t), \ldots, x_n(t), q'_1(t), \ldots, q'_r(t)), \end{cases}$$

Тогда можно построить СФЭ в базисе $\{\vee, \&, \neg\}$ с $n + r$ входами и $m + r$ выходами, реализующую семейство функций:

$$\begin{cases} z_i & = & f_i(x_1, \ldots, x_n, q'_1, \ldots, q'_r), \\ q_j & = & g_j(x_1, \ldots, x_n, q'_1, \ldots, q'_r). \end{cases}$$

Пусть в этой СФЭ входная переменная q'_j приписана вершине v_j, а выходная переменная q_j — вершине w_j. Добавим дугу (w_j, v_j) и сопоставим вершине v_j элемент задержки. Проделав это для всех пар q'_j, q_j получим СФЭЗ, функционирование которой описывается каноническими уравнениями

$$\begin{cases} z_i(t) & = & f_i(x_1(t), \ldots, x_n(t), q_1(t-1), \ldots, q_r(t-1)), \\ q_j(t) & = & g_j(x_1(t), \ldots, x_n(t), q_1(t-1), \ldots, q_r(t-1)), \\ q_j(0) & = & 0. \end{cases}$$

$\square$

Будем рассматривать автоматы — пятерки вида (A, B, Q, G, F).

Расширим функции F, G таким образом, чтобы они были определены для любого слова $\overline{a} = (a(1), a(2), \ldots, a(m))$ и любого состояния $q \in Q$.

Definition

Два состояния q_i и q_j автомата (A, B, Q, G, F) называются отличимыми, если существует входное слово $\overline{a} \in A^*$ такое, что $F(\overline{a}, q_i) \neq F(\overline{a}, q_j)$. При этом слово $\overline{a}$ называют экспериментом, отличающим состояния q_i, q_j, а величину $l(\overline{a})$ — длиной этого эксперимента.

Definition

Два состояния q_i и q_j автомата (A, B, Q, G, F) называются отличимыми, если существует входное слово $\overline{a} \in A^*$ такое, что $F(\overline{a}, q_i) \neq F(\overline{a}, q_j)$. При этом слово $\overline{a}$ называют экспериментом, отличающим состояния q_i, q_j, а величину $l(\overline{a})$ — длиной этого эксперимента.

Lemma

Пусть в автомате (A, B, Q, G, F) есть 2 состояния q_u и q_v, отличимые экспериментом длины p и не отличимые более коротким экспериментом. Тогда для любого k, где $1 \leq k \leq p$, существуют 2 состояния, отличимые экспериментом длины k и не отличимые более коротким экспериментом.

Доказательство. Пусть состояния q_u, q_v отличимы экспериментом $\overline{a}$ длины p и не отличимы экспериментом меньшей длины. Пусть $F(\overline{a}, q_u) = \overline{b}$, $F(\overline{a}, q_v) = \overline{c}$. Тогда $\overline{b} \neq \overline{c}$, причем отличаются они последней буквой. Разобьем все слова $\overline{a}, \overline{b}, \overline{c}$ на два подслова $\overline{a} = \overline{a_1 a_2}$, $\overline{b} = \overline{b_1 b_2}$, $\overline{c} = \overline{c_1 c_2}$, где $l(\overline{a_2}) = l(\overline{b_2}) = l(\overline{c_2})$.

Доказательство. Пусть состояния q_u, q_v отличимы экспериментом $\overline{a}$ длины p и не отличимы экспериментом меньшей длины. Пусть $F(\overline{a}, q_u) = \overline{b}$, $F(\overline{a}, q_v) = \overline{c}$. Тогда $\overline{b} \neq \overline{c}$, причем отличаются они последней буквой. Разобьем все слова $\overline{a}, \overline{b}, \overline{c}$ на два подслова $\overline{a} = \overline{a_1 a_2}$, $\overline{b} = \overline{b_1 b_2}$, $\overline{c} = \overline{c_1 c_2}$, где $l(\overline{a_2}) = l(\overline{b_2}) = l(\overline{c_2})$.

Пусть $G(\overline{a_1}, q_u) = q'$, $G(\overline{a_1}, q_v) = q''$. Тогда $F(\overline{a_2}, q') = \overline{b_2}$, $F(\overline{a_2}, q'') = \overline{c_2}$. Так как $\overline{b_2}$ и $\overline{c_2}$ отличаются только последней буквой, то q', q'' отличимы экспериментом длины $l(\overline{a_2}) = k$.

Продолжение. Допустим теперь, что q' и q'' отличимы экспериментом $\overline{a_3}$ длины $l(\overline{a_3} < k)$. Тогда $F(\overline{a_3}, q') = \overline{b_3}$, $F(\overline{a_3}, q'') = \overline{c_3}$, $\overline{b_3} \neq \overline{c_3}$.

Продолжение. Допустим теперь, что q' и q'' отличимы экспериментом $\overline{a_3}$ длины $l(\overline{a_3} < k)$. Тогда $F(\overline{a_3}, q') = \overline{b_3}$, $F(\overline{a_3}, q'') = \overline{c_3}$, $\overline{b_3} \neq \overline{c_3}$.

Но тогда $F(\overline{a_1 a_3}, q_u) = \overline{b_1 b_3}$, $F(\overline{a_1 a_3}, q_v) = \overline{c_1 c_3}$ и $\overline{b_1 b_3} \neq \overline{c_1 c_3}$. А это значит, что состояния q_u, q_v отличимы экспериментом длины $l(\overline{a_1 a_3}) = p$, а это противоречит условию. $\square$

Theorem (Теорема Мура)

Если в автомате (A, B, Q, G, F) состояния q_i и q_j отличимы и $|Q| = r$, то существует эксперимент $\overline{a}$, отличающий q_i и q_j, длины $l(\overline{a}) \leq r - 1$.

Theorem (Теорема Мура)

Если в автомате (A, B, Q, G, F) состояния q_i и q_j отличимы и $|Q| = r$, то существует эксперимент $\overline{a}$, отличающий q_i и q_j, длины $l(\overline{a}) \leq r - 1$.

Доказательство. Пусть состояния q_i и q_j отличимы экспериментом длины p и не отличимы более коротким экспериментом. Разобьем все состояния нашего автомата на несколько классов R_m таким образом, что два состояния попадают в один класс R_m, если они не отличимы экспериментом длины m. R_m, устроенное таким образом, задает отношение эквивалентности на множестве вершин. Полученные таким образом классы эквивалентности обозначим $Q_1^{(m)}, Q_2^{(m)}, \dots, Q_m^{(m)}$. Заметим, что $s(0) = 1, Q = Q_1^{(0)}$.

Продолжение. Рассмотрим, как изменяются классы при увеличении длины эксперимента. Два состояния, различимых экспериментом длины m будут различимы экспериментами длины $m+1$, т.е. они останутся в разных классах.

По лемме для любого $m = 0, 1, \ldots, p-1$ существуют 2 состояния, отличимые экспериментом длины $m+1$ и не отличимые экспериментом длины m. Значит, хотя бы один из классов эквивалентности относительно R_m распадется на два при R_{m+1}. Тогда

$$1 = s(0) < s(1) < \ldots < s(p-1) < s(p) \leq r \Rightarrow p \leq r-1.$$

$\square$

Существует пример автомата, показывающий, что эксперимент меньшей длины не обязан различать состояния.

Definition

Пусть 2 автомата (A, B, Q_1, G_1, F_1) и (A, B, Q_2, G_2, F_2) имеют одинаковые входной и выходной алфавиты. Пусть $q_i \in Q_1, q_j \in Q_2$. Будем говорить, что эксперимент $\overline{a} \in A^*$ отличается состояния q_i и q_j, если $F(\overline{a}, q_i) \neq F(\overline{a}, q_j)$.

Definition

Пусть 2 автомата (A, B, Q_1, G_1, F_1) и (A, B, Q_2, G_2, F_2) имеют одинаковые входной и выходной алфавиты. Пусть $q_i \in Q_1, q_j \in Q_2$. Будем говорить, что эксперимент $\overline{a} \in A^*$ отличается состояния q_i и q_j, если $F(\overline{a}, q_i) \neq F(\overline{a}, q_j)$.

Theorem

Пусть даны 2 автомата (A, B, Q_1, G_1, F_1) и (A, B, Q_2, G_2, F_2). Пусть $|Q_1| = r$, $|Q_2| = m$ и $q_i \in Q_1$, $q_j \in Q_2$. Тогда, если q_i и q_j отличимы, то существует отличающий их эксперимент $\overline{a} : l(\overline{a}) \leq r + m - 1$.

Доказательство. Рассмотрим автомат (A, B, Q, G, F), в котором $Q = Q_1 \bigcup Q_2$ и диаграмма которого получается объединением диаграмм исходных автоматов. Тогда $|Q| = r + m$ и по теореме Мура эти два состояния отличимы экспериментом длины $l(\overline{a}) \leq r + m - 1$.

Доказательство. Рассмотрим автомат (A, B, Q, G, F), в котором $Q = Q_1 \bigcup Q_2$ и диаграмма которого получается объединением диаграмм исходных автоматов. Тогда $|Q| = r + m$ и по теореме Мура эти два состояния отличимы экспериментом длины $l(\overline{a}) \leq r + m - 1$.

Существует автомат, для которого указанная оценка не может быть понижена.

Примеры. Пусть $f(x(1), x(2), \ldots, x(t), \ldots) = y(1)y(2)\ldots y(t)\ldots$. Выяснить, является ли эта функция детерминированной:

1. $y(1) = x(1)$, $y(t) = x(1) \oplus x(2) \oplus \ldots \oplus x(t)$ при $t \geq 2$.
2. $y(t) = x(1) \cdot x(2) \cdot \ldots x(t) \cdot x(t+2) \to x(1)$, $t \geq 1$.
3. $y(t) = x(\sqrt{[3/2t]})$, $t \geq 1$.
4. $y(1) = y(2) = 1$, $y(t) = x(2^{t-1} - t)$ при $t \geq 3$.