10-я лекция курса "Теория дискретных функций"

(1-й курс; лектор - проф. А.С.Подколзин)

Распознавание событий конечными автоматами

Конечный автомат можно рассматривать как устройство, распознающее некоторое множество M входных слов. Поступление на вход автомата последней буквы такого слова вызывает (в тот же момент) особую внешнюю реакцию автомата. Займемся исследованием структуры множеств слов, распознаваемых в этом смысле конечными автоматами. Начнем с определений.

Пусть $V_q = (A, Q, B, \varphi, \psi, q)$ - инициальный конечный автомат, $B' \subseteq B$. Множество $M = \{\alpha | \alpha \in A^* \setminus \{\Lambda\}, \psi(q, \alpha) \in B'\}$ называем представимым в конечном автомате V_q с помощью подмножества B' выходных символов. Говорим также, что автомат V_q представляет M посредством B'.

Подмножества множества $A^* \setminus \{\Lambda\}$ далее называем событиями в алфавите A (или, короче, событиями). Заметим, что пустое слово Λ отбрасывается потому, что для появления на выходе автомата какого-то символа необходимо сначала подать какой-то символ на его вход. Значение $\psi(q, \Lambda)$ попросту не определено.

Если существует конечный автомат V_q, представляющий событие M посредством некоторого подмножества B', то событие M называем представимым.

Мы получим чисто алгебраическое описание семейства представимых событий, никак не связанное с конечными автоматами. Для этого введем следующие операции над событиями:

1. Произведение событий M_1 и M_2 (обозначаем $M_1 \cdot M_2$) есть множество всех слов вида $\alpha_1\alpha_2$, где $\alpha_1 \in M_1, \alpha_2 \in M_2$. Как и в случае умножения, точку обычно опускаем.

2. Итерация события M (обозначаем $< M >$)есть множество всех слов вида $\alpha_1 \dots \alpha_k$, где $\alpha_1 \in M, \dots, \alpha_k \in M, k \geq 1$. Иными словами, в итерацию включаются всевозможные слова, получаемые записыванием подряд нескольких (быть может, одного, но не менее чем одного) слов из M.

Заметим, что $\emptyset \cdot M = M \cdot \emptyset = \emptyset$,
$< \emptyset >= \emptyset$,
$< M >= M < M > \cup M$,
$M < M >=< M > M$.

Лемма 1. Соотношение $X = XC \cup D$ выполняется для событий C, D, X тогда и только тогда, когда $X = D < C > \cup D$.

Фактически, эта лемма позволяет решать простейшее "уравнение" относительно X.

Пусть сначала $X = D < C > \cup D$. Покажем, что тогда X удовлетворяет исходному уравнению. Имеем: $XC \cup D = D < C > C \cup DC \cup D = D(< C > C \cup C) \cup D = D < C > \cup D = X$. Таким образом, при подстановке X уравнение обратилось в тождество.

Пусть теперь $X = XC \cup D$.

Если $\neg(X \subseteq D < C > \cup D)$, то рассмотрим кратчайшее слово α, принадлежащее $X \setminus (D < C > \cup D)$. Имеем: $\alpha \in XC \cup D, \neg(\alpha \in D)$, откуда $\alpha = \alpha_1\alpha_2$, где $\alpha_1 \in X, \alpha_2 \in C$. Так как α - кратчайшее в $X \setminus (D < C > \cup D)$, то $\alpha_1 \in D < C > \cup D$. Но тогда $\alpha \in (D < C > \cup D)C$, причем $(D < C > \cup D)C = D < C > C \cup DC = D(< C > C \cup C) = D < C >$, и получаем противоречие с условием $\alpha \in X \setminus (D < C > \cup D)$. Поэтому $X \subseteq D < C > \cup D$.

Если $\neg(D < C > \cup D \subseteq X)$, то рассмотрим кратчайшее слово α, принадлежащее $(D < C > \cup D) \setminus X$. Имеем: $\neg(\alpha \in X)$. Но $X = XC \cup D$, т.е. $D \subseteq X$. Поэтому $\neg(\alpha \in D)$ и $\alpha \in D < C >$. Но $D < C >= D(< C > C \cup C) = D < C > C \cup DC = (D < C > \cup D)C$. Таким образом, $\alpha = \alpha_1\alpha_2$, где $\alpha_1 \in D < C > \cup D, \alpha_2 \in C$. Так как α - кратчайшее из $(D < C > \cup D) \setminus X$, то $\alpha_1 \in X$ и $\alpha \in XC$, что с учетом $XC \cup D = X$ дает $\alpha \in X$. Это противоречит выбору α. Отсюда получается включение $D < C > \cup D \subseteq X$, а вместе с ранее доказанным обратным включением - равенство $X = D < C > \cup D$. Лемма доказана.

Оказывается, что класс представимых событий совпадает с классом событий, получаемых из некоторых простейших событий при помощи операций произведения, итерации и объединения.

Событие $M, M \subseteq A^*$, называем регулярным, если его можно получить из событий вида $\emptyset, \{a\}, a \in A$, применением конечного числа операций $\cup, \cdot, <>$. Более подробно, определение регулярных событий таково:

1. $\emptyset$ и $\{a\}$, где a - произвольный символ алфавита A, - регулярные события.
2. Если R_1 и R_2 - регулярные события, то $R_1 \cup R_2$, $R_1 \cdot R_2$, $< R_1 >$ - регулярные события.
3. Регулярность произвольного события устанавливается в соответствии с п.п. 1,2 за конечное число шагов.

Нашей целью будет доказательство совпадения классов представимых и регулярных событий. Сначала докажем ряд лемм.

Лемма 2. Пусть $R_{ij}, i = 0, \ldots, n, j = 1, \ldots, n$ - регулярные события, $X_1, \ldots, X_n$ - события, удовлетворяющие системе уравнений

$X_1 = X_1R_{11} \cup \ldots \cup X_nR_{n1} \cup R_{01}$,

$\ldots \quad \ldots \quad \ldots \quad \ldots$

$X_n = X_1R_{1n} \cup \ldots \cup X_nR_{nn} \cup R_{0n}$.

Тогда события $X_1, \ldots, X_n$ регулярны.

Доказательство проведем индукцией по n. В случае $n = 1$ имеем $X_1 = X_1R_{11} \cup R_{01}$, и по лемме 1 $X_1 = R_{01} < R_{11} > \cup R_{01}$, т.е. X_1 регулярно.

Пусть утверждение леммы доказано для некоторого $n = k - 1$; рассмотрим случай $n = k$. Используя лемму 1, разрешим последнее уравнение рассматриваемой в лемме системы относительно X_n:

$X_n = (X_1R_{1n} \cup \ldots \cup X_{n-1}R_{n-1,n} \cup R_{0n}) < R_{nn} > \cup X_1R_{1n} \cup \ldots \cup X_{n-1}R_{n-1,n} \cup R_{0n} = X_1(R_{1n} < R_{nn} > \cup R_{1n}) \cup \ldots \cup X_{n-1}(R_{n-1,n} < R_{nn} > \cup R_{n-1,n}) \cup R_{0n} < R_{nn} > \cup R_{0n}$.

Подставляя найденное для X_n выражение через "неизвестные" $X_1, \ldots, X_{n-1}$ в первые $n-1$ уравнений системы и группируя подобные члены, получаем систему уравнений для $X_1, \ldots, X_{n-1}$, вид которой аналогичен виду исходной системы, а коэффициенты при $X_1, \ldots, X_{n-1}$ и свободные члены регулярны. Согласно предположению индукции, отсюда вытекает регулярность событий $X_1, \ldots, X_{n-1}$. Так как X_n выражается через регулярные события $X_1, \ldots, X_{n-1}$,
$R_{0n}, R_{1n}, \ldots, R_{nn}$ при помощи операций $<>, \cdot, \cup$, то X_n регулярно. Лемма доказана.

Лемма 3. Каждое событие, представимое в конечном автомате, является регулярным.

Пусть $V_{q_1} = (A, Q, B, \varphi, \psi, q_1)$ - инициальный конечный автомат и $B' \subseteq B$. Рассмотрим событие M, представимое в V_{q_1} посредством B': $M = \{\alpha | \alpha \in A^* \setminus \{\Lambda\}, \psi(q_1, \alpha) \in B'\}$. Введем обозначения для состояний автомата: $Q = \{q_1, \ldots, q_n\}$.

Рассмотрим множества M_i непустых входных слов, переводящих автомат из состояния q_1 в состояние q_i:

$M_i = \{\alpha | \alpha \in A^*, \alpha \neq \Lambda, \varphi(q_1, \alpha) = q_i\}$; $i = 1, \ldots, n$.

Рассмотрим также множество M_i' входных букв, на которые находящийся в состоянии q_i автомат реагирует выходой буквой из B':

$M_i' = \{a | a \in A, \psi(q_i, a) \in B'\}$.

Если совсем точно, то M_i' - это, все-таки, не буквы, а образованные ими однобуквенные слова. Тогда M_i' будет событием.

Как легко видеть,

$M = M_1 M_1' \cup \ldots \cup M_n M_n' \cup M_1'$.

Это равенство легко устанавливается разбором случаев. Если слово α из M имеет длину 1, то оно принадлежит M_1'. Если его длина больше 1, то оно может быть представлено в виде $\alpha' a$, где $\alpha' \in A^*, \alpha' \neq \Lambda, a \in A$. Слово α' переводит автомат из состояния q_1 в какое-то состояние q_i. После этого подача на вход буквы a приводит к появлению на выходе символа из B'. Следовательно, $\alpha' \in M_i, a \in M_i', \alpha \in M_i M_i'$.

Событие M_i' имеет вид $\{a_1, \ldots, a_s\}$, где $a_j \in A, j = 1, \ldots, s, s \geq 0$. При $s = 0$ имеем $M_i' = \emptyset$, при $s > 0$ - $M_i' = \{a_1\} \cup \ldots \cup \{a_s\}$, т.е. события $M_1', \ldots, M_n'$ регулярны. Поэтому для установления регулярности события M достаточно установить регулярность событий $M_1, \ldots, M_n$.

Обозначим $R_{ij} = \{a | a \in A, \varphi(q_i, a) = q_j\}, i = 1, \ldots, n, j = 1, \ldots, n$. Очевидно, события R_{ij} регулярные (аналогично $M_1', \ldots, M_n'$). При этом выполнены следующие соотношения:

$M_1 = M_1 R_{11} \cup \ldots \cup M_n R_{n1} \cup R_{11}$

$\ldots \quad \ldots \quad \ldots \quad \ldots$

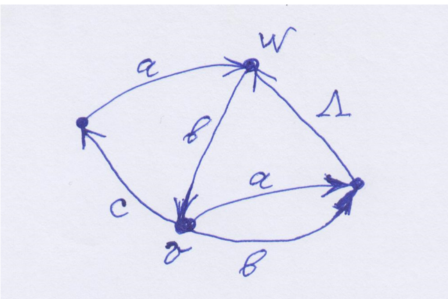
$M_n = M_1 R_{1n} \cup \ldots \cup M_n R_{nn} \cup R_{1n}$

Они устанавливаются разбором случаев, как и приведенное выше соотношение для M. По лемме 2, события $M_1, \ldots, M_n$ регулярны, и лемма доказана.

Для доказательства представимости регулярных событий нам понадобятся два перехода. Введем некоторый промежуточный способ задания событий - при помощи так называемых обобщенных источников. Сначала мы покажем, что каждое регулярное событие может быть задано обобщенным источником, а затем - что каждое определяемое обобщенным источником событие представимо.

Прежде всего, напомним определение ориентированного графа. Ориентированным графом называем тройку (V, R, φ) где V - множество вершин графа, R - множество ребер графа, φ - отображение, ставящее в соответствие каждому ребру $r \in R$ упорядоченную пару вершин (v_1, v_2). Говорим, что это ребро ведет от вершины v_1 к вершине v_2. Графы изображают, рисуя вершины в виде небольших кругов (в частности, жирных точек), а ребра - в виде стрелок, ведущих от одной вершины к другой. Знакомая нам диаграмма Мура - это, по сути дела, ориентированный граф, у которого вершины и ребра снабжены некоторыми пометками. Граф называется конечным, если множества V, R конечные.

Обобщенным источником в алфавите A называем конечный ориентированный граф G, у которого выделены начальная вершина v и финальная вершина w, $v \neq w$, причем каждому ребру приписано либо пустое слово Λ, либо символ алфавита A. Допускается наличие в графе G параллельных ребер, т.е. различных ребер, соединяющих в заданном направлении одну и ту же пару вершин.

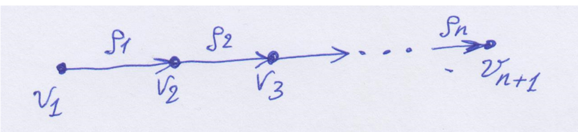


Заметим, что исторически первыми были введены "обычные" источники, у которых не допускались пустые отметки и имелись небольшие другие отличия. Однако, для доказательства совпадения классов представимых и регулярных событий более удобными оказались обобщенные источники.

Главное отличие источника от диаграммы Мура состоит в том, что из одной и той же вершины может выходить несколько ребер с одной и той же отметкой, а может не выходить ни одного ребра с данной отметкой.

Путем в обобщенном источнике G называем последовательность π чередующихся вершин и ребер: $v_1, \rho_1, v_2, \rho_2, \ldots, \rho_n, v_{n+1}$, где ребро ρ_i ведет от вершины v_i к вершине v_{i+1}; $i = 1, \ldots, n$.

Говорим, что π - путь от вершины v_1 к вершине v_{n+1}.



Пути π сопоставляем слово $[\pi] = a_1 \ldots a_n$, где a_i - отметка ребра ρ_i; $i = 1, \ldots, n$. Пустые отметки Λ пропускаются. Иными словами, берется конкатенация отметок, рассматриваемых как слова - пустые либо однобуквенные.

Говорим, что путь π определяет слово $[\pi]$ или соответствует этому слову.

Пусть $\alpha \in A^*, \alpha \neq \Lambda$; u - вершина обобщенного источника G. Обозначим $\theta(u, \alpha)$ множество всех таких вершин u', что существует ведущий от u к u' путь π, соответствующий слову α (т.е. $[\pi] = \alpha$).

Событием, определяемым обобщенным источником G с начальной вершиной v и финальной вершиной w, называем множество

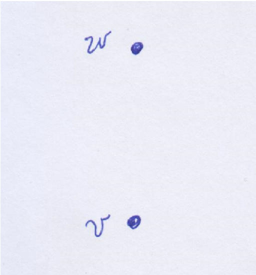
$|G| = \{\alpha | \alpha \in A^* \setminus \{\Lambda\}, w \in \theta(v, \alpha)\}$.

Иными словами, обобщенный источник задает событие, образованное всеми словами, определяемыми путями от его начальной вершины к финальной вершине.

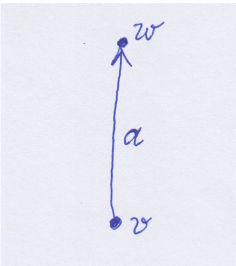
Лемма 4. Если событие R регулярно, то существует обобщенный источник G, для которого $|G| = R$.

Доказательство поведем индукцией по определению регулярного события.

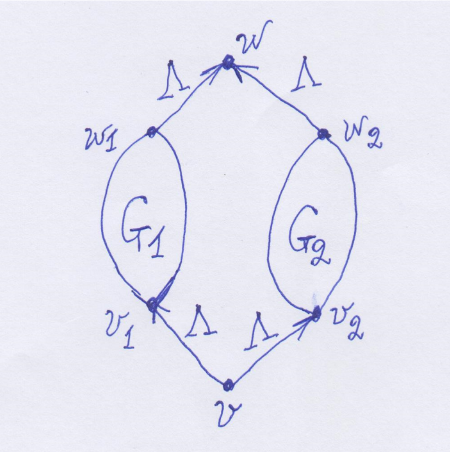
Если $R = \emptyset$, то берем следующий источник:



Если $R = \{a\}$, то берем следующий источник:

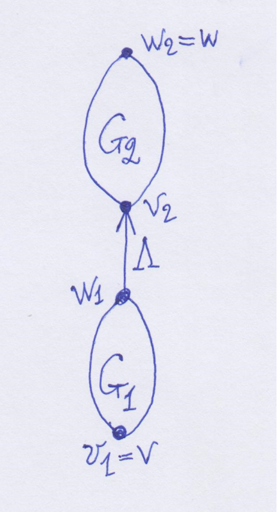


Если $R = R_1 \cup R_2$, то по предположению индукции существуют обобщенные источники G_1, G_2, такие что $|G_1| = R_1, |G_2| = R_2$. В качестве источника G, определяющего R, берем следующий источник:

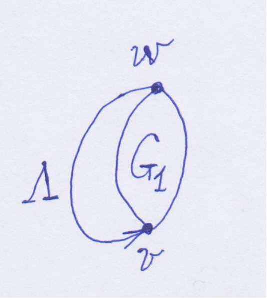


Заметим, что ребра с пустыми отметками введены для исключения "ложных" путей. Если просто отождествить финальные вершины G_1, G_2 и их начальные вершины, то можно было бы, например, пройдя от v_1 к w_1, зайти в источник G_2, сделать в нем петлю и снова вернуться к w_1. Вообще говоря, это добавило бы новые слова.

Если $R = R_1 \cdot R_2$ и $R_1 = |G_1|, R_2 = |G_2|$, то для задания R берем следующий источник:



Наконец, если $R =< R_1 >$ и $R_1 = |G_1|$, то берем следующий источник:



Лемма доказана.

Лемма 5. Если G - обобщенный источник, то событие $|G|$ представимо.

Пусть $M = \{v_1, \ldots, v_n\}$ - множество вершин обобщенного источника G в алфавите A; v_1 - начальная вершина; v_n - финальная вершина. Обозначим Q множество всех подмножеств множества M, включая пустое множество и само M. Рассмотрим автомат $V_{\{v_1\}} = (A, Q, \{0, 1\}, \varphi, \psi, \{v_1\})$, у которого функции переходов и выходов определены следующим образом:

$$\varphi(q, a) = \bigcup_{v, v \in q} \theta(v, a);$$

$$\psi(q, a) = (1, \text{ если } v_n \in \varphi(q, a), \text{ иначе } 0)$$

.

Из последнего определения вытекает, что для любого слова $\alpha \in A^* \setminus \{\Lambda\}$ соотношение $\psi(q, \alpha) = 1$ эквивалентно соотношению $v_n \in \varphi(q, \alpha)$. Действительно, представим α в виде $\alpha' a$, где $a \in A$. Тогда $\psi(q, \alpha) = \psi(\varphi(q, \alpha'), a), \varphi(q, \alpha) = \varphi(\varphi(q, \alpha'), a)$. Следовательно, $\psi(q, \alpha) = 1 \leftrightarrow \psi(\varphi(q, \alpha'), a) = 1 \leftrightarrow v_n \in \varphi(\varphi(q, \alpha'), a) \leftrightarrow v_n \in \varphi(q, \alpha)$.

Покажем, что для любого $\alpha \in A^* \setminus \{\Lambda\}$ выполнено:

$\varphi(\{v_1\}, \alpha) = \theta(v_1, \alpha)$. Доказательство поведем индукцией по длине слова α. Если $\alpha = a \in A$, то равенство верно по определению функции φ. Пусть оно доказано для всех слов α длины l; $l \geq 1$. Рассмотрим слово α длины $l + 1$. Представим его в виде $\alpha' a$, где $a \in A$. Тогда, используя предположение индукции, имеем:

$$\varphi(\{v_1\}, \alpha) = \varphi(\varphi(\{v_1\}, \alpha'), a) = \varphi(\theta(v_1, \alpha'), a) = \bigcup_{v, v \in \theta(v_1, \alpha')} \theta(v, a).$$

Таким образом, достаточно доказать равенство

$$\theta(v_1, \alpha) = \bigcup_{v, v \in \theta(v_1, \alpha')} \theta(v, a).$$

В общем-то, оно достаточно очевидно. Тем не менее, приведем подробное доказательство. Установим сначала включение левой части в правую. Если $w \in \theta(v_1, \alpha)$, то существует путь π от v_1 к w, такой, что $[\pi] = \alpha$. Его можно разбить на две части π_1, π_2, такие, что $[\pi_1] = \alpha', [\pi_2] = a$. Путь π_1 ведет от v_1 к некоторой вершине u, путь π_2 - от вершины u к вершине w. Следовательно, $u \in \theta(v_1, \alpha'), w \in \theta(u, a)$, и получаем

$$w \in \bigcup_{v, v \in \theta(v_1, \alpha')} \theta(v, a)$$

.

Перейдем к доказательству включения правой части в левую. Пусть

$$w \in \bigcup_{v \in \theta(v_1, \alpha')} \theta(v, a).$$

Тогда существует вершина $u \in \theta(v_1, \alpha')$, такая, что $w \in \theta(u, a)$. Рассмотрим путь π_1 от v_1 к u, такой, что $[\pi_1] = \alpha'$, а также путь π_2 от u к w, такой, что $[\pi_2] = a$. Тогда $\pi = \pi_1 \pi_2$ - путь от v_1 к w, и $[\pi] = \alpha' a = \alpha$, т.е. $w \in \theta(v_1, \alpha)$.

Итак, $\varphi(\{v_1\}, \alpha) = \theta(v_1, \alpha)$ для всех $\alpha \in A^* \setminus \{\Lambda\}$. Имеем следующие эквивалентности: $\alpha \in |G| \leftrightarrow v_n \in \theta(v_1, \alpha) \leftrightarrow v_n \in \varphi(\{v_1\}, \alpha) \leftrightarrow \psi(\{v_1\}, \alpha) = 1$. Последнее означает принадлежность слова α событию, представимому в автомате $V_{\{v_1\}}$ с помощью подмножества $\{1\}$. Таким образом, событие $|G|$ представимо в данном автомате, и лемма доказана.

Из доказанных лемм вытекает

Теорема (С.К.Клини) Событие E в алфавите A представимо тогда и только тогда, когда оно регулярно.

Так как представимые события можно взаимно-однозначно закодировать конечными словами, задающими конечный автомат и подмножество его выходных символов, то множество представимых событий счетно. С другой стороны, множество всех событий в непустом алфавите A континуально. Следовательно, существуют непредставимые события. Приведем конкретный пример непредставимого события.

Пусть M - множество всех слов в алфавите $\{0, 1\}$, у которых число нулей равно числу единиц. Предположим, что M представимо в конечном автомате $V_q = (\{0, 1\}, Q, B, \varphi, \psi, q)$ посредством подмножества $B' \subseteq B$. Так как Q конечно, то существуют такие $i_1, i_2; i_1 \neq i_2$, что $\varphi(q, 0^{i_1}) = \varphi(q, 0^{i_2})$. Напомним, что 0^k обозначает слово из k нулей. Но тогда $\psi(q, 0^{i_1}1^{i_1}) = \psi(\varphi(q, 0^{i_1}), 1^{i_1}) = \psi(\varphi(q, 0^{i_2}), 1^{i_1}) = \psi(q, 0^{i_2}1^{i_1})$. Однако, $\psi(q, 0^{i_1}1^{i_1}) \in B'$, $\neg(\psi(q, 0^{i_2}1^{i_1}) \in B')$, и получаем противоречие. Следовательно, M непредставимо.