9-я лекция курса "Теория дискретных функций"

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

Эквивалентность конечных автоматов

Сравнение поведений конечных автоматов приводит к ряду отношений эквивалентности между автоматами, а также между состояниями одного и того же автомата.

Пусть $V = (A, Q, B, \varphi, \psi)$, $V' = (A, Q', B, \varphi', \psi')$ - конечные автоматы. Если для любого слова α из A^* выполняется $\overline{\psi}(q, \alpha) = \overline{\psi'}(q', \alpha)$, где $q \in Q, q' \in Q'$, то говорим, что состояние q автомата V неотличимо от состояния q' автомата V'. Если же при некотором $\alpha, \alpha \in A^*$, имеет место $\overline{\psi}(q, \alpha) \neq \overline{\psi'}(q', \alpha)$, то состояние q называем отличимым от состояния q'. Говорим в этом случае, что состояния q, q' отличимы словом α или что слово α отличает состояния q и q'.

В частном случае, когда $V = V'$, приходим к отношению неотличимости, определенному на множестве Q состояний автомата V. Очевидно, оно является отношением эквивалентности и разбивает Q на классы попарно неотличимых состояний.

Если любые два различных состояния автомата отличимы друг от друга, то говорим, что V есть автомат приведенного вида.

Предположим, что для любого состояния q автомата V существует неотличимое от него состояние q' автомата V', и обратно, для любого состояния q' автомата V' существует неотличимое от него состояние автомата V. Тогда говорим, что автоматы V и V' неотличимы. Если ограничиться рассмотрением автоматов с фиксированными входным и выходным алфавитами A, B и алфавитом состояний Q, содержащимся в некотором заданном счетном множестве, то отношение неотличимости автоматов оказывается отношением эквивалентности, разбивающим данное множество на классы попарно неотличимых автоматов.

Отношения отличимости состояний и автоматов используются в технической диагностике, при создании тестов, позволяющих отличать исправные автоматы от неисправных.

Нам понадобится еще одно отношение эквивалентности для автоматов. Пусть $V = (A, Q, B, \varphi, \psi)$, $V' = (A, Q', B, \varphi', \psi')$ - конечные автоматы, причем существует такое взаимно-однозначное отображение ξ множества Q на множество Q', для которого выполняются тождественно следующие соотношения:

$\xi(\varphi(q, a)) = \varphi'(\xi(q), a)$

$\psi(q, a) = \psi'(\xi(q), a) \quad (q \in Q, a \in A).$

Тогда говорим, что автоматы V и V' изоморфны.

Легко видеть, что изоморфные автоматы неотличимы; нетрудно также привести пример неотличимых автоматов, не являющихся изоморфными.

Теорема. Для любого конечного автомата V существует единственный с точностью до изоморфизма конечный автомат приведенного вида, неотличимый от V.

Данная теорема позволяет "упрощать" конечные автоматы путем отождествления групп попарно неотличимых состояний, не заботясь о порядке таких отождествлений. С точностью до изоморфизма, окончательный результат будет один и тот же.

Пусть $V = (A, Q, B, \varphi, \psi)$. Рассмотрим разбиение множества Q на классы $Q_1, \ldots, Q_n$ попарно неотличимых состояний. Пусть $q, q' \in Q_i,\ i \in \{1, \ldots, n\},\ a \in A$. Если $\varphi(q, a) \in Q_j, \varphi(q', a) \in Q_{j'}$, где $j \neq j'$, то существует слово $\alpha, a \in A^*$, для которого

$\overline{\psi}(\varphi(q, a), \alpha) \neq \overline{\psi}(\varphi(q', a), \alpha)$.

Но тогда

$\overline{\psi}(q, a\alpha) = \psi(q, a)\overline{\psi}(\varphi(q, a), \alpha) \neq \psi(q', a)\overline{\psi}(\varphi(q', a), \alpha) = \overline{\psi}(q', a\alpha)$,

и состояния q, q' оказываются отличимыми. Полученное противоречие доказывает, что $j = j'$, и можно положить по определению $Q_j = \varphi'(Q_i, a)$. Таким образом, определена функция $\varphi' : \{Q_1, \ldots, Q_n\} \times A \to \{Q1, \ldots, Q_n\}$.

Далее, при $q, q' \in Q_i,\ a \in A, i \in \{1, \ldots, n\}$, в силу неотличимости состояний q, q', имеем $\psi(q, a) = \psi(q', a) = b$. Это позволяет положить по определению $b = \psi'(Q_i, a)$; в результате имеем функцию $\psi' : \{Q_1, \ldots, Q_n\} \times A \to B$.

Рассмотрим автомат $V' = (A, \{Q_1, \ldots, Q_n\}, B, \varphi', \psi')$. Из определения функций φ', ψ' вытекает, что при $q \in Q_i, \alpha \in A^*$ имеем $\varphi(q, \alpha) \in \varphi'(Q_i, \alpha)$ и $\overline{\psi}(q, \alpha) = \overline{\psi'}(Q_i, \alpha)$. Поэтому автоматы V, V' неотличимы.

Если $i \neq j,\ i, j \in \{1, \ldots, n\}$, то рассматриваем состояния q, q' автомата V, такие, что $q \in Q_i, q' \in Q_j$. Существует отличающее их слово α из A^*: $\overline{\psi}(q, \alpha) \neq \overline{\psi}(q', \alpha)$. Тогда выполняется и $\overline{\psi'}(Q_i, \alpha) \neq \overline{\psi'}(Q_j, \alpha)$, так что состояния автомата V' попарно отличимы, и он является автоматом приведенного вида.

Покажем, что любой неотличимый от V автомат $V'' = (A, Q'', B, \varphi'', \psi'')$, являющийся автоматом приведенного вида, изоморфен автомату V'. Пусть $Q'' = \{q''_1, \ldots, q''_m\}$. Каждое состояние q''_i неотличимо от некоторого состояния автомата V, а следовательно - от некоторого состояния Q_j автомата V'. Так как состояния $q''_1, \ldots, q''_m$ попарно отличимы, они не могут оказаться неотличимы от одного и того же состояния Q_j. Поэтому число n состояний Q_j не менее числа m. Точно такими же рассуждениями, меняя местами автоматы V' и V'', получаем противоположное неравенство $n \leq m$. Следовательно, $m = n$, и каждому состоянию Q_i автомата V' соответствует единственное неотличимое от него состояние автомата V''; $i = 1, \ldots, n\}$. Покажем, что отображение ξ, сопоставляющее состоянию Q_i автомата V' неотличимое от него состояние автомата V'', устанавливает изоморфизм автоматов V' и V''. Очевидно, отображение ξ взаимно однозначно. Так как Q_i и $\xi(Q_i)$ неотличимы, то для каждого $a \in A$ неотличимы также состояния $\varphi'(Q_i, a)$ и $\varphi''(\xi(Q_i), a)$. Это означает, что $\xi(\varphi'(Q_i, a)) = \varphi''(\xi(Q_i), a)$, т.е. имеет место первое из условий определения изоморфизма. Второе условие - равенство $\psi(Q_i, a) = \psi''(\xi(Q_i), a)$ - вытекает из неотличимости состояний $Q_i, \xi(Q_i)$. Таким образом, автоматы V', V'' изоморфны. Теорема доказана.

Как уже говорилось выше, задача различения двух состояний автомата возникает при необходимости проверить его на исправность или диагностировать тип неисправности. Тогда представляют интерес кратчайшие различающие слова или слова, наиболее "дешевые" в смысле некоторого другого оценочного функционала. Ответ

на вопрос о возможной длине кратчайшего различающего слова дает следующая теорема:

Теорема (Мур). Если два состояния автомата $V = (A, Q, B, \varphi, \psi)$ отличимы, то существует различающее их слово длины $|Q| - 1$, причем, вообще говоря, эта оценка не улучшаема.

Пусть $V = (A, Q, B, \varphi, \psi)$, причем состояния q_1, q_2 этого автомата отличимы. На множестве Q рассмотрим отношение ρ_k неотличимости словами длины k:

$q\rho_k q' \leftrightarrow \forall_\alpha(\alpha \in A^k \rightarrow \overline{\psi}(q, \alpha) = \overline{\psi}(q', \alpha)$

Здесь $q\rho_k q'$ означает, что состояния q, q' находятся в отношении ρ_k; A^k - множество слов в алфавите A, имеющих длину k.

Очевидно, ρ_k - отношение эквивалентности, т.е. оно разбивает Q на классы эквивалентности. Множество этих классов обозначим R_k.

Заметим, что $|R_1| \geq 2$. Действительно, так как q_1, q_2 отличимы, то можно рассмотреть кратчайшее отличающее их слово α. Оно непусто, т.е. его можно представить в виде $\alpha' a$, где $\alpha' \in A^*, a \in A$. Ввиду того, что α кратчайшее, различение состояний q_1, q_2 должно осуществляться последней его буквой, т.е. $\psi(\varphi(q_1, \alpha'), a) \neq \psi(\varphi(q_2, \alpha'), a)$. Это означает, что состояния $\varphi(q_1, \alpha'), \varphi(q_2, \alpha')$ принадлежат различным классам отношения ρ_1, и $|R_1| \geq 2$.

Очевидно, что R_{k+1} - подразбиение разбиения R_k, т.е. $|R_k| \leq |R_{k+1}|$. Рассмотрим разбиение R_∞ множества Q на классы попарно неотличимых состояний. Покажем, что если $R_k = R_{k+1}$, то $R_k = R_\infty$. Пусть это не так. Тогда существуют такие $q, q' \in M, M \in R_k$, которые отличимы. Выберем пару состояний q, q' и класс M так, чтобы кратчайшее отличающее состояния q, q' слово α имело наименьшую возможную длину. Так как $q, q' \in M, M \in R_k$ и $k \geq 1$, то длина слова a не менее 2. Представим его в виде $a\alpha'$, где $a \in A, \alpha' \in A^*$. Рассмотрим состояния $\tilde{q} = \varphi(q, a)$ и $\hat{q} = \varphi(q', a)$. Слово α' отличает состояния $\tilde{q}, \hat{q}$, причем длина его меньше длины слова α. В силу того, что α - каратчайшее, способное отличить два состояния одного класса, состояния $\tilde{q}, \hat{q}$ должны принадлежать различным классам в R_k. Пусть $\tilde{q} \in M_1, \hat{q} \in M_2; M_1, M_2 \in R_k$. Тогда существует слово α'' длины k, различающее $\tilde{q}$ и $\hat{q}$: $\overline{\psi}(\tilde{q}, \alpha'') \neq \overline{\psi}(\hat{q}, \alpha'')$. Рассмотрим слово $\alpha''' = a\alpha''$. Имеем: $\overline{\psi}(q, \alpha''') = \psi(q, a)\overline{\psi}(\tilde{q}, \alpha'') \neq \psi(q', a)\overline{\psi}(\hat{q}, \alpha'') = \overline{\psi}(q', \alpha''')$. Таким образом, слово α''' разичает состояния q, q' и имеет длину $k + 1$. Следовательно, состояния q, q' должны принадлежать различным классам разбиения R_{k+1}. Это противоречит тому, что $R_k = R_{k+1}$.

Итак, если $R_k = R_{k+1}$, то $R_k = R_\infty$.

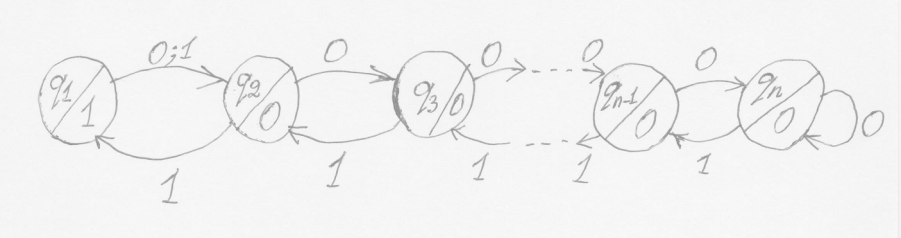
Рассмотрим последовательность $|R_1|, R_2|, |R_3|, \ldots$. Она монотонно неубывает, причем каждый ее член не превосходит числа $|Q|$ состояний автомата. Следовательно, она должна стабилизироваться начиная с некоторого k: $|R_k| = |R_{k+1}|$. Тогда и $R_k = R_{k+1} = R_\infty$. Имеем:

$2 \leq |R_1| < |R_2| < \ldots |R_k| \leq |Q|$.

Индукцией по i легко получить неравенство $|R_i| \geq i + 1$; $i = 1, \ldots, k$. Отсюда $|Q| \geq |R_k| \geq k + 1$; $k \leq |Q| - 1$, и любые два отличимые состояния автомата (в том числе q_1, q_2) отличимы словом длины $|Q| - 1$.

Чтобы доказать неулучшаемость оценки, рассмотрим следующий пример. Пусть $V = (A, Q, B, \varphi, \psi)$ - автомат Мура, у которого $A = B = \{0, 1\}$, $Q = \{q_1, \ldots, q_n\}$. Диаграмма Мура этого автомата имеет вид, приведенный на следующем рисунке. Здесь в

каждом круге верхнюю часть занимает символ состояния, нижнюю - выходной символ. Стрелкам сопоставлены только входные символы:



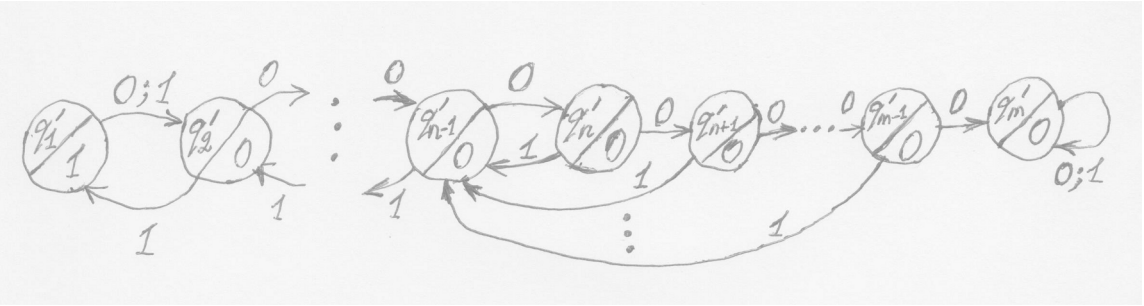
Чтобы отличить состояния q_{n-1} и q_n, необходимо хотя бы одно из них перевести в состояние q_1, так как только в нем на выходе будет получаться единица. Очевидно, что самое короткое слово, которое это делает - слово, образованное $n-2$ единицами. Оно переводит q_{n-1} в q_1, в то время как q_n пока не "успевает" дойти до q_1. Для различения теперь достаточно подать любой входной символ: в первом случае на выходе появится 1, во втором - 0. Длина кратчайшего различающего слова равна $n-1$. Теорема доказана.

Для различения состояний в двух автоматах имеет место аналогичная теорема:

Теорема(Мур) Если состояние q_1 автомата $V=(A,Q,B,\varphi,\psi)$ отличимо от состояния q_2 автомата $V'=(A,Q',B,\varphi',\psi')$, то существует различающее их слово длины $|Q|+|Q'|-1$, причем, вообще говоря, эта оценка неулучшаема.

Без ограничения общности можно считать, что множества Q,Q' не пересекаются (в противном случае переобозначим состояния второго автомата так, чтобы они отличались от состояний первого). Построим автомат $V''=(A,Q\cup Q',B,\varphi'',\psi'')$. По определению, считаем, что $\varphi''(q,a)=\varphi(q,a),\psi''(q,a)=\psi(q,a)$ при $q\in Q$ и $\varphi''(q,a)=\varphi'(q,a),\psi''(q,a)=\psi'(q,a)$ при $q\in Q'$. Диаграмма Мура автомата V'' получается объединением диаграмм Мура автоматов V,V'. Состояния q,q_2 становятся состояниями одного и того же автомата V'', т.е. по предыдущей теореме существует отличающее их слово длины $|Q|+|Q'|-1$. Очевидно, оно же будет различать их и как состояния автоматов V,V'.

Остается привести пример, доказывающий неулучшаемость оценки. Пусть заданы числа n,m состояний автоматов V,V'. В силу симметрии, можно считать, что $m\geq n$. Автомат V зададим той же диаграммой, что и в предыдущей теореме. Автомат V' зададим следующей диаграммой:



Попробуем найти кратчайшее слово, отличающее состояния q_1,q_1'. Сопоставим каждому состоянию q_i', где $i\leq n$, состояние q_i, а каждому состоянию $q_{n+1}',\ldots,q_{m-1}'$ -

состояние q_n. Если состояние автомата V сопоставлено состоянию автомата V', то будем называть эти состояния соответствующими. Легко заметить, что в соответствующих состояниях автоматы на одни и те же входные символы реагируют одними и теми же выходными символами. Более того, под действием одного и того же входного символа соответствующие состояния переходят в соответствующие - за единственным исключением: при подаче 0 на состояние q_{m-1} автомат V' попадает в "ловушку" q'_m, и далее из нее не выходит. Соответствие при этом нарушается. Таким образом, если какое-то слово α различает состояния q_1, q'_1, то некоторая его начальная часть α' переводит автомат V' в состояние q'_m. Наименьшая длина такой части равна $m-1$. После того, как автомат V' перешел в состояние q'_m, автомат V окажется в состоянии q_n. Чтобы теперь на выходе получить единицу, различающую оба автомата, необходимо подать еще $n-1$ символ для перевода автомата V в состояние q_1, а затем - любой символ для получения на выходе этого аватомата единицы. Общее число символов равно $(m-1)+(n-1)+1 = m+n-1$, что и требовалось. Теорема доказана.