Эксперименты с автоматами. Теоремы Мура.

Два автомата $V' = (A, B, Q', F', G')$, $V'' = (A, B, Q'', F'', G'')$ с одинаковыми входным и выходным алфавитом называются *изоморфными*, если существует взаимно однозначное отображение $\xi : Q' \to Q''$ такое, что $\xi(G'(q, a)) = G''(\xi(q), a)$ и $F'(q, a) = F''(\xi(q), a)$ для любых $q \in Q'$, $a \in A$.

Пусть $V = (A, B, Q, F, G)$ — конечный автомат. Функцию выходов F можно обобщить на функцию $\overline{F} : Q \times A^* \to B^*$, определяемую следующим рекурсивным образом:
$\overline{F}(q, a) = F(q, a)$ для $a \in A$;
$\overline{F}(q, aw) = F(q, a)\overline{F}(G(q, a), w)$ для $a \in A$, $w \in A^*$.
Другими словами, значением $\overline{F}(q, w)$ является слово над B, которое будет выдано на выходе автомата V, если на вход этого автомата, находящегося в начальном состоянии q, будет подано слово w. Функция переходов G также обобщается на функцию $\overline{G} : Q \times A^* \to Q$ следующим рекурсивным образом:
$\overline{G}(q, a) = G(q, a)$ для $a \in A$;
$\overline{G}(q, aw) = \overline{G}(G(q, a), w)$ для $a \in A$, $w \in A^*$.
Другими словами, значением $\overline{G}(q, w)$ является состояние автомата V, в которое он в итоге перейдет после того, как на вход этого автомата, находящегося в начальном состоянии q, будет подано слово w.

Пусть $V' = (A, B, Q', F', G')$, $V'' = (A, B, Q'', F'', G'')$ — два автомата с одинаковыми входным и выходным алфавитом (при этом, возможно, $V' = V''$), $q' \in Q'$, $q'' \in Q''$. Пусть $w \in A^*$ — произвольное входное слово. Будем говорить, что состояния q', q'' *отличимы* на слове w, если $\overline{F'}(q', w) \neq \overline{F''}(q'', w)$. В противном случае будем говорить, что q', q'' *неотличимы* на слове w. Пусть $W \subseteq A^*$ — произвольное множество входных слов. Будем говорить, что состояния q', q'' *отличимы* на множестве W, если q', q'' отличимы хотя бы на одном из слов множества W. В противном случае, т.е. если q', q'' неотличимы на любом слове из W, будем говорить, что q', q'' *неотличимы* на множестве W (неотличимость состояний q', q'' на множестве W обозначается через $q' \overset{W}{\sim} q''$). Состояния q', q'' называются *отличимыми*, если они отличимы на A^*, т.е. отличимы на хотя бы одном входном слове. В противном случае, т.е. если q', q'' неотличимы на любом слове из A^*, состояния q', q'' называются *неотличимыми* (неотличимость состояний q', q'' обозначается через $q' \sim q''$). Автоматы V', V'' называются *неотличимыми* ($V' \approx V''$), если для любого $q' \in Q'$ найдется $q'' \in Q''$ такое, что $q' \sim q''$ и для любого $q'' \in Q''$ найдется $q' \in Q'$ такое, что $q'' \sim q'$. Изоморфные автоматы являются неотличимыми. С другой стороны, неотличимые автоматы могут быть неизоморфными. Автомат называется *приведенным*, если любые его два состояния отличимы.

Теорема (о существовании и единственности приведенного автомата). Для любого автомата V существует единственный с точностью до изоморфизма приведенный автомат, неотличимый от V.

Доказательство. Пусть $V = (A, B, Q, F, G)$ — произвольный конечный автомат. Нетрудно заметить, что отношение неотличимости состояний автомата является отношением эквивалентности. Поэтому Q разбивается на классы эквивалентности относительно данного отношения, т.е. на такие классы состояний, что два состояния автомата содержатся в одном классе тогда и только тогда, когда эти состояния неотличимы. Пусть $\hat{Q}$ — множество всех этих классов состояний автомата V. Построим автомат $\hat{V} = (A, B, \hat{Q}, \hat{F}, \hat{G})$, определив в нем функции $\hat{G}, \hat{F}$ следующим образом. Пусть $\hat{q} \in \hat{Q}$, $a \in A$. Выберем произвольное состояние q из $\hat{q}$ и положим $\hat{G}(\hat{q}, a) = \hat{q}'$, где $\hat{q}'$ — класс, содержащий $G(q, a)$. Покажем, что данное определение $\hat{G}$ не зависит от выбора состояния q. Предположим противное: для некоторого состояния q_1 из $\hat{q}$ состояние $G(q_1, a)$ содержится в классе, отличном от $\hat{q}'$. Следовательно, состояния $G(q, a)$ и $G(q_1, a)$ отличимы, т.е. $\overline{F}(G(q, a), w) \neq \overline{F}(G(q_1, a), w)$ для некоторого $w \in A^*$. Следовательно, $\overline{F}(q, aw) \neq \overline{F}(q_1, aw)$, т.е. состояния q, q_1 являются отличимыми и не могут принадлежать одному классу $\hat{q}$, тем самым получили противоречие. Положим также $\hat{F}(\hat{q}, a) = F(q, a)$. Данное определение $\hat{G}$ также не зависит от выбора состояния q: если для некоторого состояния $q_1 \in \hat{q}$ имеем $F(q_1, a) \neq F(q, a)$, то состояния q, q_1 являются отличимыми и не могут принадлежать одному классу $\hat{q}$.

Пусть $q \in \hat{q}$. Покажем, что тогда состояния q и $\hat{q}$ неотличимы, т.е. $\overline{F}(q, w) = \overline{\hat{F}}(\hat{q}, w)$ для любого $w \in A^*$. Доказательство проведем индукцией по длине слова w одновременно для всех q, $\hat{q}$ таких, что $q \in \hat{q}$. Если $w = a \in A$, то

$$\overline{\hat{F}}(\hat{q}, a) = \hat{F}(\hat{q}, a) = F(q, a) = \overline{F}(q, a).$$

Пусть теперь длина слова w больше 1 и $\overline{F}(q, w') = \overline{\hat{F}}(\hat{q}, w')$ для любых состояний $q \in \hat{q}$ и любого слова w' длины меньшей, чем длина w. Положим $w = aw'$, где $a \in A$. Тогда

$$\begin{aligned} \overline{F}(q, w) &= F(q, a)\overline{F}(G(q, a), w') \\ \overline{\hat{F}}(\hat{q}, w) &= \hat{F}(\hat{q}, a)\overline{\hat{F}}(\hat{G}(\hat{q}, a), w') \end{aligned}$$

Так как $q \in \hat{q}$, то согласно определению функции $\hat{G}$ имеем $G(q, a) \in \hat{G}(\hat{q}, a)$, поэтому в силу индуктивного предположения

$$\overline{F}(G(q, a), w') = \overline{\hat{F}}(\hat{G}(\hat{q}, a), w').$$

Кроме того, согласно определению функции $\hat{F}$, $\hat{F}(\hat{q},a) = F(q,a)$. Таким образом, $\overline{F}(q,w) = \overline{\hat{F}}(\hat{q},w)$. Из доказанного вытекает, что автоматы V и $\hat{V}$ неотличимы.

Покажем, что $\hat{V}$ является приведенным. Предположим противное: для некоторых состояний $\hat{q}', \hat{q}'' \in \hat{Q}$ имеем $\hat{q}' \sim \hat{q}''$. Тогда для любых $q' \in \hat{q}'$ и $q'' \in \hat{q}''$ выполняется $q' \sim \hat{q}' \sim \hat{q}'' \sim q''$, т.е. $q' \sim q''$, что противоречит тому, что q' и q'' содержатся в разных классах.

Пусть теперь $V' = (A, B, Q', F', G')$ — приведенный автомат, неотличимый от V. Покажем, что тогда V' изоморфен $\hat{V}$. Так как $V \approx \hat{V}$ и $V \approx V'$, то $V' \approx \hat{V}$. Поэтому для каждого состояния автомата V' в $\hat{V}$ найдется состояние, неотличимое от этого состояния, и, поскольку V' является приведенным, то все эти состояния автомата $\hat{V}$ должны быть различными. Таким образом, число состояний автомата $\hat{V}$ не меньше числа состояний автомата V'. Аналогично число состояний автомата V' не меньше числа состояний автомата $\hat{V}$. Следовательно, число состояний автомата $\hat{V}$ равно числу состояний автомата V', и между неотличимыми состояниями автоматов V' и $\hat{V}$ имеется взаимно однозначное соответствие $\xi : Q' \to \hat{Q}$ такое, что $q' \sim \xi(q')$ для любого $q' \in Q'$. Тем самым $G'(q',a) \sim \hat{G}(\xi(q'),a)$ для любых $q' \in Q'$ и $a \in A$, поэтому $\hat{G}(\xi(q'),a) = \xi(G'(q',a))$. Равенство $F'(q',a)) = \hat{F}(\xi(q'),a)$ вытекает из неотличимости состояний q' и $\xi(q')$. Таким образом, V' и $\hat{V}$ являются изоморфными.

1-я теорема Мура. Пусть $V = (A, B, Q, F, G)$ — конечный автомат с k состояниями. Тогда любые два состояния автомата V являются неотличимыми тогда и только тогда, когда они неотличимы на множестве A^{k-1}.

Доказательство. Очевидно, что, если два состояния A являются неотличимыми, то они неотличимы на A^{k-1}. Докажем теорему в обратную сторону.

Отметим, что для любого натурального i отношение неотличимости на множестве A^i является отношением эквивалентности. Поэтому Q разбивается на классы эквивалентности относительно данного отношения, т.е. на такие классы состояний, что два состояния автомата содержатся в одном классе тогда и только тогда, когда эти состояния неотличимы на A^i. Обозначим через $R_i = \{\hat{q}_1^i, \hat{q}_2^i, \ldots, \hat{q}_{k_i}^i\}$ множество всех таких классов. Заметим, что если два состояния содержатся в одном классе из R_{i+1}, то они содержатся в одном классе из R_i, поэтому каждый класс из R_i является объединением некоторых классов из R_{i+1}. Таким образом, $|R_i| \le |R_{i+1}|$, и при этом $|R_i| = |R_{i+1}|$ тогда и только тогда, когда $R_i = R_{i+1}$. Заметим, что для любого i имеем $|R_i| \le k$, Поэтому найдется минимальный номер s, такой, что $|R_s| = |R_{s+1}|$, т.е. $R_s = R_{s+1}$. Покажем, что тогда $R_s = R_{s+1} = R_{s+2} = \ldots$. Предположим противное: пусть для некоторого $t > s$ имеем $R_t \ne R_{t+1}$, т.е. существуют два состояния $q', q'' \in Q$ такие, что $q' \overset{A^t}{\sim} q''$, но q', q'' отличимы на A^{t+1}, т.е. существует входное слово w длины $t+1$ такое, что $\overline{F}(q',w) \ne \overline{F}(q'',w)$. Пусть u — префикс длины $t-s$ в слове w. Обозначим через q_1' состояние $\overline{G}(q',u)$ и через q_1'' состояние $\overline{G}(q'',u)$. Покажем, что $q_1' \overset{A^s}{\sim} q_1''$. Для этого рассмотрим произвольное входное слово v длины s. Так как $q' \overset{A^t}{\sim} q''$, имеем

$$\overline{F}(q',uv) = \overline{F}(q'',uv),$$

при этом

$$\overline{F}(q',uv) = \overline{F}(q',u)\overline{F}(q_1',v),$$
$$\overline{F}(q'',uv) = \overline{F}(q'',u)\overline{F}(q_1'',v).$$

Следовательно,

$$\overline{F}(q',u)\overline{F}(q_1',v) = \overline{F}(q'',u)\overline{F}(q_1'',v),$$

т.е. $\overline{F}(q_1'',v) = \overline{F}(q_1'',v)$. Таким образом, $q_1' \overset{A^s}{\sim} q_1''$.

Отметим, что различие слов $\overline{F}(q',w)$, $\overline{F}(q'',w)$ в j-м символе при $j \le t$ означает, что состояния q' и q'' отличимы на префиксе длины j в слове w, что противоречит неотличимости состояний q', q'' на словах длины t. Таким образом, слова $\overline{F}(q',w)$, $\overline{F}(q'',w)$ должны различаться на последнем символе. Обозначим через v' суффикс длины $s+1$ в слове w, т.е. $w = uv'$. Тогда мы имеем

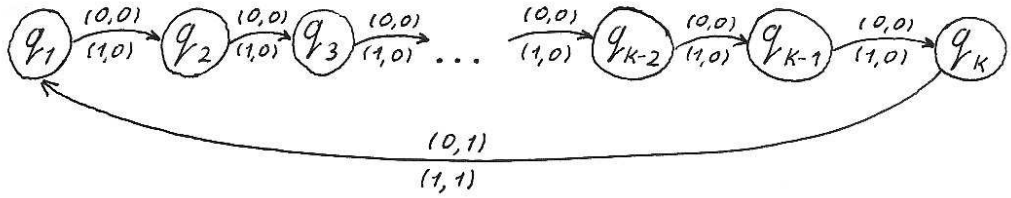
$$\overline{F}(q',w) = \overline{F}(q',uv') = \overline{F}(q',u)\overline{F}(q_1',v'),$$
$$\overline{F}(q'',w) = \overline{F}(q'',uv') = \overline{F}(q'',u)\overline{F}(q_1'',v').$$

Поэтому из того, что слова $\overline{F}(q',w)$, $\overline{F}(q'',w)$ отличаются на последнем символе, вытекает, что слова $\overline{F}(q_1',v')$ и $\overline{F}(q_1'',v')$ также отличаются на последнем символе. Таким образом, состояния q_1', q_1'' отличимы на слове v' длины $s+1$, т.е. q_1', q_1'' отличимы на множестве A^{s+1}. Получаем, что q_1', q_1'' содержатся в одном классе из R_s, но в разных классах из R_{s+1}, что противоречит $R_s = R_{s+1}$. Таким образом, $R_s = R_{s+1} = R_{s+2} = \ldots$. Отсюда вытекает, что, если два состояния из Q неотличимы на множестве A^s, то они неотличимы на любом входном слове, т.е. являются неотличимыми. С другой стороны, согласно определению числа s имеем $|R_1| < |R_2| < \ldots < |R_s|$, при этом, исключая из рассмотрения тривиальный случай, можно полагать $|R_1| \ge 2$. Следовательно, $s+1 \le |R_s| \le k$, т.е. $s \le k-1$. Таким образом,

$$q' \overset{A^{k-1}}{\sim} q'' \quad \Rightarrow \quad q' \overset{A^s}{\sim} q'' \quad \Rightarrow \quad q' \sim q''.$$

Следствие. Два состояния автомата с k состояниями отличимы тогда и только тогда, когда они отличимы на множестве A^{k-1}.

1-я теорема Мура не может быть усилена. В качестве контрпримера можно привести автомат со следующей диаграмой Мура.



Нетрудно заметить, что $q_1 \overset{A^{k-2}}{\sim} q_2$, однако $q_1 \not\sim q_2$.

2-я теорема Мура. Пусть $V' = (A, B, Q', F', G')$, $V'' = (A, B, Q'', F'', G'')$ — конечные автоматы, такие, что $|Q'| = k'$, $|Q''| = k''$, q' — состояние автомата V', q'' — состояние автомата V''. Тогда q' и q'' являются неотличимыми тогда и только тогда, когда они неотличимы на множестве $A^{k'+k''-1}$.

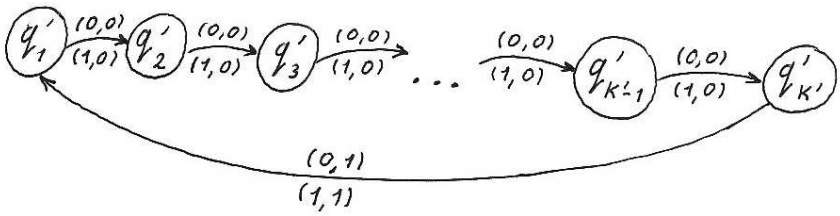
Для доказательства теоремы можно рассмотреть автомат $V''' = (A, B, Q''', F''', G''')$ такой, что $Q''' = Q' \cup Q''$ и

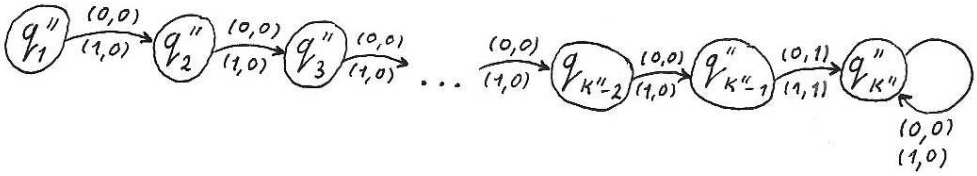
$$G'''(q,a) = \begin{cases} G'(q,a), & \text{если } q \in Q', \\ G''(q,a), & \text{если } q \in Q'' \end{cases} \qquad F'''(q,a) = \begin{cases} F'(q,a), & \text{если } q \in Q', \\ F''(q,a), & \text{если } q \in Q'' \end{cases}$$

и применить к этому автомату 1-ю теорему Мура.

Следствие. Состояния двух автоматов, один из которых имеет k' состояний, а другой — k'' состояний, отличимы тогда и только тогда, когда они отличимы на множестве $A^{k'+k''-1}$.

2-я теорема Мура не может быть усилена. В качестве контрпримера можно привести два автомата со следующими диаграммами Мура (при условии $k' \geq k'' \geq 2$).





Нетрудно заметить, что $q''_1 \overset{A^{k'+k''-2}}{\sim} q'_{k'-k''+2}$, так как на любых входных словах длины $k'+k''-2$ в этих состояниях на выходе выдается слово $\underbrace{00\ldots0}_{k''-2}1\underbrace{00\ldots0}_{k'-1}$, однако $q''_1 \not\sim q'_{k'-k''+2}$.