Курс лекций
«Теория дискретных функций»
Лекция 14

Вадим Васильевич Кочергин
vvkoch@yandex.ru

ЭКСПЕРИМЕНТЫ С АВТОМАТАМИ

Изоморфизм автоматов. Обобщения функций выходов и переходов

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 $\varphi : Q' \to Q''$ такое, что $\varphi(G'(a, q)) = G''(a, \varphi(q))$ и $F'(a, q) = F''(a, \varphi(q))$ для любых $q \in Q'$, $a \in A$.

Пусть $V = (A, B, Q, F, G)$ — конечный автомат. Функцию выходов F и функцию переходов G можно обобщить на функции

$$\overline{F} : A^+ \times Q \to B^+ \text{ и } \overline{G} : A^+ \times Q \to Q,$$

определяемые следующим рекурсивным образом:
$\overline{F}(a, q) = F(a, q)$, $\overline{G}(a, q) = G(a, q)$ для $a \in A$;
$\overline{F}(aw, q) = F(a, q)\overline{F}(w, G(q, a))$, $\overline{G}(aw, q) = \overline{G}(w, G(a, q))$ для $a \in A$, $w \in A^+$.

Пусть $V' = (A, B, Q', F', G')$, $V'' = (A, B, Q'', F'', G'')$ — два автомата с одинаковыми входным и выходным алфавитом (допускается случай $V' = V''$); $q' \in Q'$, $q'' \in Q''$, $w \in A^+$.

Состояния q' и q'' *отличимы на слове* w, если $\overline{F'}(q', w) \neq \overline{F''}(q'', w)$.
В противном случае состояния q' и q'' *неотличимы на слове* w.

Пусть $W \subseteq A^*$ — произвольное множество входных слов.
Состояния q' и q'' *отличимы на множестве* W, если q' и q'' отличимы хотя бы на одном из слов множества W.
В противном случае состояния q' и q'' *неотличимы на множестве* W.

Неотличимость состояний q' и q'' на множестве W обозначается через $q' \overset{W}{\sim} q''$.

Отличимость состояний, отличимость автоматов

Состояния q' и q'' называются *отличимыми*, если они отличимы на A^+.

В противном случае состояния q' и q'' называются *неотличимыми*.

Неотличимость состояний q', q'' обозначается через $q' \sim q''$.

Автоматы V' и V'' называются *неотличимыми* (обозначение: $V' \approx V''$), 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.

Неотличимые автоматы могут быть неизоморфными.

Автомат называется *приведенным*, если любые его два состояния отличимы.

Существование и единственность приведенного автомата

Теорема

Для любого конечного автомата V существует единственный с точностью до изоморфизма приведенный автомат, неотличимый от V.

Доказательство. Пусть $V = (A, B, Q, F, G)$ — произвольный конечный автомат. Разобьем множество состояний Q на классы эквивалентности относительно отношения неотличимости. Пусть $\hat{Q}$ — множество всех этих классов состояний автомата V. Построим новый автомат $\hat{V} = (A, B, \hat{Q}, \hat{F}, \hat{G})$.

Положим

$$\hat{G}(a, \hat{q}) = \hat{q}', \quad \hat{F}(a, \hat{q}) = F(a, q),$$

где q — некоторое состояние из класса $\hat{q}$, $\hat{q}'$ — класс, содержащий состояние $G(a, q)$.

Корректность такого определения функций переходов и выходов следует из неотличимости состояний из одного класса.

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 слова $w \in A^+$.

Индукция по длине слова w одновременно для всех q, $\hat{q}$ таких, что $q \in \hat{q}$.

Если $w = a \in A$, то

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

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

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

По предположению индукции $\overline{F}(w', G(a, q),) = \overline{\hat{F}}(w', \hat{G}(a, \hat{q}))$. Кроме того, $\hat{F}(a, \hat{q}) = F(a, q)$.

Таким образом, $\overline{F}(q, w) = \overline{\hat{F}}(\hat{q}, w)$.

Следовательно, автоматы V и $\hat{V}$ неотличимы.

Продолжение доказательства теоремы (2)

Построенный автомат $\hat{V}$ приведенный, т. е. все его состояния отличимы.

Действительно, если $\hat{q}', \hat{q}'' \in \hat{Q}$, $\hat{q}' \neq \hat{q}''$, $\hat{q}' \sim \hat{q}''$, то для любых $q' \in \hat{q}'$ и $q'' \in \hat{q}''$

$$q' \sim \hat{q}' \sim \hat{q}'' \sim q'',$$

т. е. $q' \sim q''$, что противоречит тому, что q' и q'' содержатся в разных классах.

Осталось показать единственность (с точностью до изоморфизма) приведенного автомата.

Пусть $V' = (A, B, Q', F', G')$ — приведенный автомат, неотличимый от V. Покажем, что тогда V' изоморфен $\hat{V}$.

Завершение доказательства теоремы

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 $\varphi : Q' \to \hat{Q}$ такое, что $q' \sim \varphi(q')$ для любого $q' \in Q'$.

Тем самым $G'(a, q') \sim \hat{G}(a, \varphi(q'))$ для любых $q' \in Q'$ и $a \in A$, поэтому $\hat{G}(a, \varphi(q')) = \varphi(G'(a, q'))$. Равенство $F'(a, q')) = \hat{F}(a, \varphi(q'))$ вытекает из неотличимости состояний q' и $\varphi(q')$. Таким образом, автоматы V' и $\hat{V}$ являются изоморфными.

Теорема доказана.

Теорема (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. Достаточно показать, что любые два состояния автомата, неотличимые на множестве A^{k-1}, неотличимы.

Для любого натурального i отношение неотличимости на множестве A^i является отношением эквивалентности. Поэтому множество Q разбивается на классы эквивалентности относительно данного отношения. Обозначим через $R_i = \{\hat{q}_1^i, \hat{q}_2^i, \ldots, \hat{q}_{k_i}^i\}$ множество всех таких классов.

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, $|R_i| \leq |R_{i+1}|$, причем $|R_i| = |R_{i+1}|$ тогда и только тогда, когда $R_i = R_{i+1}$.

Так как $|R_i| \leq |R_{i+1}|$ и $|R_i| \leq k$ при всех i, то найдется минимальный номер s, такой, что $|R_s| = |R_{s+1}|$, т. е. $R_s = R_{s+1}$. Покажем, что тогда $R_s = R_{s+1} = R_{s+2} = \ldots$

Пусть это не так, т. е. для некоторого $t > s$ верно $R_t \neq R_{t+1}$. Тогда существуют два состояния $q', q'' \in Q$ такие, что $q' \overset{A^t}{\sim} q''$, но q' и q'' отличимы на A^{t+1}, т. е. существует входное слово w длины $t+1$ такое, что $\overline{F}(w, q') \neq \overline{F}(w, q'')$.

Пусть u — префикс длины $t-s$ в слове w. Положим

$$q_1' = \overline{G}(u, q'), \quad q_1'' = \overline{G}(u, q'').$$

Покажем, что $q_1' \overset{A^s}{\sim} q_1''$. Рассмотрим произвольное входное слово $v \in A^s$ и составим слово $uv \in A^t$.

Продолжение доказательства 1-й теоремы Мура (2)

Так как $q' \overset{A^t}{\sim} q''$, то

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

при этом

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

Следовательно,

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

т. е. $\overline{F}(u, q') = \overline{F}(u, q'')$ и $\overline{F}(v, q_1'') = \overline{F}(v, q_1'')$.
Первое равенство используем позже, а из второго следует, что

$$q_1' \overset{A^s}{\sim} q_1''.$$

Возвращаясь к слову $w \in A^{t+1}$, имеющему префикс u и удовлетворяющему условию

$$\overline{F}(w, q') \neq \overline{F}(w, q''),$$

обозначим в слове w через v' суффикс длины $s+1$, получая представление $w = uv'$.

Тогда

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

Слова $\overline{F}(w, q')$ и $\overline{F}(w, q'')$ отличаются, а префиксы $\overline{F}(u, q')$ и $\overline{F}(u, q'')$ — нет. Поэтому

$$\overline{F}(v', q_1') \neq \overline{F}(v', q_1'').$$

Получаем, что q_1' и q_1'' содержатся в одном классе из R_s, но в разных классах из R_{s+1}, что противоречит равенству $R_s = R_{s+1}$.

Завершение доказательства 1-й теоремы Мура

Таким образом, $R_s = R_{s+1} = R_{s+2} = \ldots$

Следовательно, если два состояния из Q неотличимы на множестве A^s, то они неотличимы на любом входном слове, т. е. являются неотличимыми.

С другой стороны,

$$|R_1| < |R_2| < \ldots < |R_s|.$$

Если $|R_1| = 1$, то все состояния неотличимы.

Если $|R_1| \geq 2$, из неравенства $|R_s| \leq k$ следует, что $s \leq k - 1$.

Таким образом,

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

Теорема доказана.

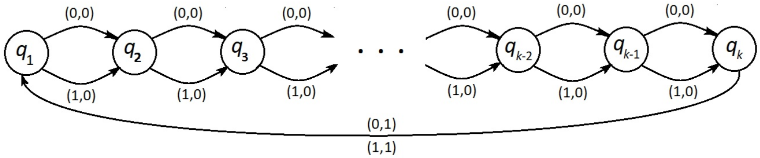
Следствие. Невозможность усилить 1-ю теорему Мура

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 на следущем слайде приведен автомат, заданный диаграммой Мура.

Пример



Для этого автомата с k состояниями, с одной стороны, выполняется соотношение

$$q_1 \overset{A^{k-2}}{\sim} q_2,$$

а с другой — соотношение

$$q_1 \not\sim q_2.$$

Теорема (2-я теорема Мура)

Пусть $V' = (A, B, Q', F', G')$, $V'' = (A, B, Q'', F'', G'')$ — *конечные автоматы,* $|Q'| = k'$, $|Q''| = k''$, $q' \in Q'$, $q'' \in Q''$. *Тогда состояния* q' *и* q'' *являются неотличимыми тогда и только тогда, когда они неотличимы на множестве* $A^{k'+k''-1}$.

Доказательство. Достаточно применить первую теорему Мура для автомата $V''' = (A, B, Q''', F''', G''')$, у которого

$$Q''' = Q' \cup Q'',$$

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

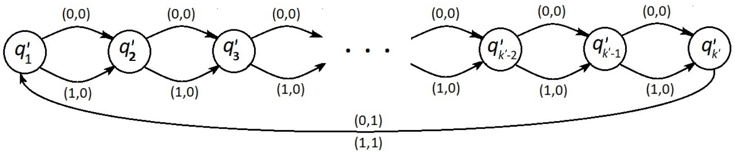
$$F'''(q, a) = \begin{cases} F'(q, a), & \text{если } q \in Q', \\ F''(q, a), & \text{если } q \in Q''. \end{cases}$$

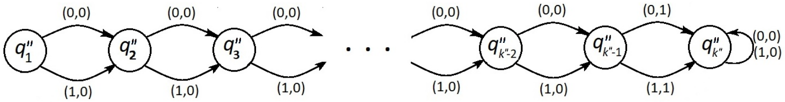
Следствие

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 на следущем слайде приведены два автомата, заданные диаграммами Мура.

Пример





С одной стороны, при $k' \geq k'' \geq 2$ выполняется соотношение

$$q_1'' \overset{A^{k'+k''-2}}{\sim} q'_{k'-k''+2},$$

так как на любых входных словах длины $k'+k''-2$ в этих состояниях на выходе выдается слово $\underbrace{00\ldots0}_{k''-2}1\underbrace{00\ldots0}_{k'-1}$, а с другой стороны, справедливо соотношение $q_1'' \not\sim q'_{k'-k''+2}$.