Алгебраические и логические методы теории формальных языков

М. В. Волков   Е. В. Прибавкина

2 октября 2016 г.

Оглавление

Предисловие

Предлагаемая книга основана на курсе лекций, который авторы в разные годы читали для студентов магистратуры математико-механического факультета Уральского государственного университета (УрГУ), а после вхождения УрГУ в состав Уральского федерального университета (УрФУ)— для магистрантов Института математики и компьютерных наук УрФУ.

Глава 1

Постановка задачи

1.1 Предварительные сведения

Мы предполагаем, что читатель знаком с основами теории формальных языков и конечных автоматов в пределах стандартного университетского курса дискретной математики. В частности, мы предполагаем известной теорему Клини о том, что класс языков над данным конечным алфавитом Σ, распознаваемых конечными детерминированными автоматами, совпадает с классом *рациональных* языков над Σ, т. е. с наименьшим классом языков, который

а) содержит пустой язык и все языки вида $\{a\}$, где $a \in \Sigma$;

б) вместе с любым языком L содержит его *итерацию* L^*, т. е. множество всевозможных конечных произведений слов из L (включая пустое произведение, которое считается равным пустому слову 1);

в) вместе с любыми двумя языками L и K содержит их теоретико-множественное объединение $L \cup K$ и их *произведение* LK, т. е. множество всевозможных произведений слов из L на слова из K.

Мы будем считать известным задание рациональных языков *регулярными выражениями* и будем пользоваться такими заданиями. Например, выражение $(ab)^*$ задает итерацию одноэлементного языка $\{ab\}$.

1.2 Беззвездные языки

Среди операций, используемых в определении рациональных языков, итерация является наиболее «сложной», так как фактически описывает некоторый бесконечный процесс:

$$L^* = \{1\} \cup L \cup L^2 \cup L^3 \cup \cdots \cup L^n \cup \ldots .$$

Действительно ли она необходима? Ясно, что просто удалить итерацию из определения рациональных языков нельзя, поскольку все остальные операции не могут произвести бесконечный язык из конечных языков. Но, может быть, можно заменить итерацию какой-нибудь более простой операцией, которая тем не менее может произвести бесконечный язык из конечных? Например, таким свойством обладает операция взятия *дополнения*. Напомним, что из теоремы Клини вытекает, что класс рациональных языков замкнут относительно взятия дополнений. Дадим соответствующее определение.

Определение 1.2.1. Класс *беззвездных* (star-free) языков над данным конечным алфавитом Σ – это наименьший класс языков, который

а) содержит пустой язык и все языки вида $\{a\}$, где $a \in \Sigma$;

б') вместе с любым языком L содержит его дополнение L^C;

в) вместе с любыми двумя языками содержит их объединение и их произведение.

Вопрос, который мы обсуждали выше, можно теперь сформулировать так: верно ли, что любой рациональных язык является беззвездным? Ответ на этот вопрос отрицателен – есть языки, которые не являются беззвездными. В качестве примера можно привести языки $(a^2)^*$ и $\{aba, b\}^*$. Мы докажем это позже, после того, как разовьем соответствующую технику.

Естественным образом возникает *проблема беззвездности*: как по данному языку над конечным алфавитом узнать, является ли он беззвездным. Эту проблему решил в 1966 г. Шютценберже[1]. Отметим, что проблема беззвездности далеко не тривиальна: если язык задан каким-то регулярным выражением, явно использующим итерацию *, это еще не означает, что язык не является беззвездным.

Пример 1.2.1. Рациональный язык $(ab)^*$ над алфавитом $\Sigma = \{a, b\}$ на самом деле является беззвездным. Действительно, несложно проверить, что

$$(ab)^* = (\varnothing^C a \cup b\,\varnothing^C \cup \varnothing^C a^2 \varnothing^C \cup \varnothing^C b^2 \varnothing^C)^C.$$

В самом деле, с учетом того, что $\varnothing^C = \Sigma^*$, выражение в правой части описывает в точности множество всех слов, которые

- не оканчиваются на a;
- не начинаются с b;
- не содержат двух вхождений буквы a подряд;
- не содержат двух вхождений буквы b подряд.

[1]Marcel-Paul (Marco) Schützenberger (1920–1996) – французский математик, сделавший существенный вклад в развитие теоретических компьютерных наук. Свою первую научную степень он получил по медицине в 1948 г., его диссертация была отмечена призом Французской академии медицины. Вторую диссертацию по теории информации Шютценберже защитил в 1953 г. Математические интересы Шютценберже были очень широки и включали теорию автоматов, теорию формальных языков, теорию информации. Также его можно по праву считать одним из основоположников комбинаторики слов, которая начала бурно развиваться с выходом в 1983 году одноименной книги, написанной под псевдонимом M. Лотэр (M. Lothaire) Шютценберже в соавторстве с учениками.

Ясно, что это множество состоит из пустого слова и всевозможных слов, которые начинаются с a, оканчиваются на b и в которых вхождения букв a и b чередуются. Но это в точности описание множества $(ab)^*$.

Упражнение 1.2.1. *Доказать, что языки* $\{ab, ba\}^*$ *и* $(a(ab)^*b)^*$ *являются беззвездными.*

1.3 Кусочно тестируемые языки

Определение 1.3.1. Язык над данным конечным алфавитом Σ называется *кусочно тестируемым*, если он может быть получен с помощью конечного числа операций объединения, пересечения и дополнения из языков вида $\Sigma^* a_1 \Sigma^* a_2 \Sigma^* \dots \Sigma^* a_k \Sigma^*$, где $a_i \in \Sigma$.

Можно определить класс кусочно тестируемых языков и с помощью соответствующих распознавателей – так называемых *автоматов-гидр.* (Напомним, что гидрой в греческой мифологии называлось многоглавое чудовище, см. рис. 1.1.)

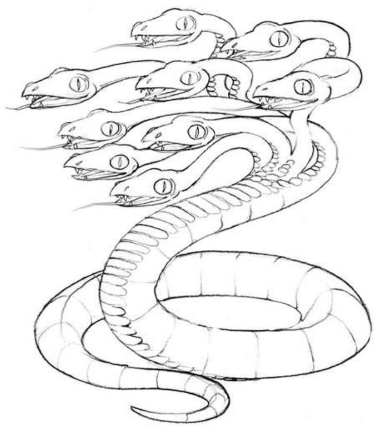


Рис. 1.1: Девятиглавая гидра

Автомат-гидра с h головками – это устройство, в состав которого входят:

- потенциально бесконечная лента, разделенная на ячейки, в которых могут быть вписаны буквы некоторого конечного алфавита Σ;
- h читающих головок, которые могут передвигаться вдоль ленты независимо друг от друга, но с сохранением взаимного порядка (первая головка всегда остается самой левой и т. д.), причем каждая головка может считывать символ из обозреваемой ей ячейки;
- конечной read-only памяти, которая содержит два списка слов длины $\le h$ над Σ: список паролей и список запретов.

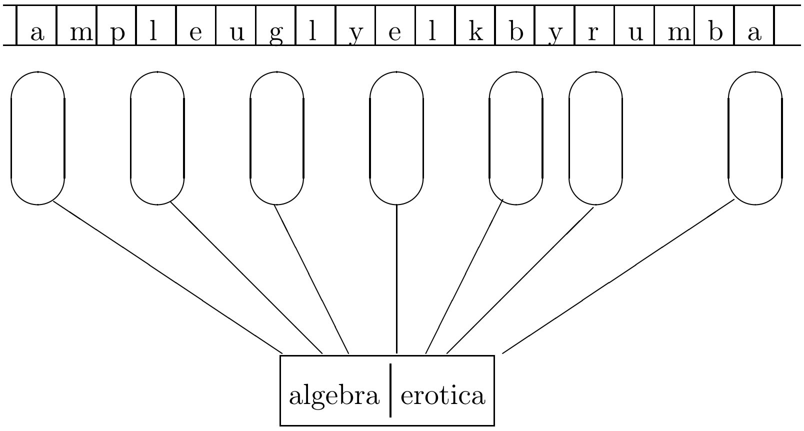


Рис. 1.2: Автомат-гидра с семью головками

Автомат-гидра *принимает* слово $w \in \Sigma^*$, если он находит в w один из паролей и при этом не обнаруживает в w ни одного из запретов. В противном случае он *отвергает* w. Например, автомат, изображенный на рис. 1.2, принимает слово, написанное на ленте (AmpleUglyElkByRumba), поскольку находит в этом слове пароль (algebra), но не находит в нем запрещенного слова (erotica). Язык $L \subseteq \Sigma^*$ *распознается* автоматом-гидрой, если данный автомат принимает в точности те слова, которые принадлежат L. Несложно понять, что класс языков, распознаваемых автоматами-гидрами, совпадает с классом кусочно тестируемых языков.

Пример 1.3.1. Язык $\Sigma^* ab \Sigma^*$ является кусочно тестируемым тогда и только тогда, когда $\Sigma = \{a, b\}$.

Утверждение «тогда» понятно, так как $\Sigma^* ab \Sigma^* = \Sigma^* a \Sigma^* b \Sigma^*$ – если в слове от букв a и b есть вхождение a, предшествующее вхождению b, то есть и вхождение a, непосредственно предшествующее вхождению b. А вот утверждение «только тогда» мы пока доказать не можем.

Возникает *проблема кусочной тестируемости*: как по данному языку над конечным алфавитом узнать, является ли он кусочно тестируемым. Эту проблему решил в 1972 г. Саймон[2].

1.4 Алгебраический метод

Результаты Шютценберже и Саймона объединяет одно важное обстоятельство: в обоих случаях ответ был получен в терминах алгебры, а точнее —

[2]Imre Simon (1943–2009) – бразильский математик и информатик венгерского происхождения. Проблему кусочной тестируемости Саймон решил в своей диссертации, выполненной под руководством Януша Бжозовского. Дальнейшие его исследования были связаны в основном с комбинаторикой слов и теорией автоматов. В связи с некоторыми вопросами этих областей Саймон ввел в рассмотрение множество действительных чисел с операциями $x \oplus y = \min\{x, y\}$ и $x \otimes y = x + y$. Этот объект получил название *тропическое полукольцо*, «тропическое» – в честь места, где жил автор этого понятия.

теории полугрупп. А именно, с каждым формальным языком L некоторым каноническим образом связан алгебраический объект $M(L)$, именуемый *синтаксическим моноидом* этого языка. Если язык L рационален, то его синтаксический моноид $M(L)$ конечен и его можно эффективно вычислить по явному заданию L конечным автоматом или регулярным выражением. Оказалось, что такие свойства языка как беззвездность и кусочная тестируемость «транслируются» при соответствии $L \mapsto M(L)$ в некоторые свойства моноида $M(L)$, причем интересно то, что соответствующие беззвездности и кусочной тестируемости свойства весьма естественны с точки зрения абстрактной теории полугрупп и изучались в ней задолго до того, как выяснилось их значение для теории формальных языков[3]. Для каждого конечного моноида наличие или отсутствие этих свойств можно установить с помощью некоторых несложных вычислений; отсюда получаются основанные на алгебре алгоритмы для распознавания беззвездности и кусочной тестируемости.

[3]Здесь проявляется та удивительная закономерность, которую Вигнер [2] назвал «непостижимой эффективностью математики» и которую Бурбаки [1] сформулировали следующим образом: «...математика представляется скоплением абстрактных форм, причем определенные аспекты реальности как будто бы в результате предопределения укладываются в некоторые из этих форм».

Глава 2

Необходимые сведения из теории полугрупп

> Я приветствую полугруппу, где бы я ее ни встретил, а встречается она повсюду. Впрочем, от друзей я слышал, что в математике попадаются объекты, отличные от полугрупп.
>
> Эйнар Хилле [3]

2.1 Определения и примеры

Напомним, что *полугруппой* называется непустое множество, на котором определена бинарная операция, удовлетворяющая закону ассоциативности:

$$\forall a, b, c \ (ab)c = a(bc). \tag{2.1}$$

В записи закона ассоциативности (2.1) операция

Для полугруппы S через S^1 будем обозначать полугруппу S с единицей, возможно присоединенной.

2.2 Отношения Грина

Отношениями Грина называются следующие бинарные отношения:

1. $a\mathscr{R}b \Leftrightarrow aS^1 = bS^1$. Это означает, что $\exists \ u, v \in S^1 : a = bu, b = av$, т.е. элементы a и b делят друг друга справа (aS^1 – главный правый идеал, порожденный элементом a).

2. $a\mathscr{L}b \Leftrightarrow S^1a = S^1b$.

3. $a\mathscr{H}b \Leftrightarrow aS^1 = bS^1, S^1a = S^1b$, т.е. $\mathscr{H} = \mathscr{R} \cap \mathscr{L}$.

4. $a \mathscr{J} b \Leftrightarrow S^1aS^1 = S^1bS^1$. Это означает, что $\exists\ u,v,x,y \in S^1 : a = ubv, b = xay$ (S^1aS^1 – главный идеал, порожденный элементом a).

Упражнение 2.2.1. *Отношения Грина являются отношениями эквивалентности.*

Также можно рассмотреть связанные с отношениями Грина отношения предпорядка:

1. $a \leq_{\mathscr{R}} b \Leftrightarrow aS^1 \subseteq bS^1$.

2. $a \leq_{\mathscr{L}} b \Leftrightarrow S^1a \subseteq S^1b$.

3. $a \leq_{\mathscr{H}} b \Leftrightarrow aS^1 \subseteq bS^1, S^1a \subseteq S^1b$.

4. $a \leq_{\mathscr{J}} b \Leftrightarrow S^1aS^1 \subseteq S^1bS^1$.

Предложение 2.2.1. *Отношения $\leq_{\mathscr{L}}$ и $\mathscr{L}$ стабильны справа, а $\leq_{\mathscr{R}}$ и $\mathscr{R}$ – слева.*

Доказательство. $a \leq_{\mathscr{L}} b \Leftrightarrow a = ub$ для некоторого $u \in S^1$. Умножим на c справа: $ac = ubc \Leftrightarrow ac \leq_{\mathscr{L}} bc$. □

Если α и β бинарные отношения, то

$$\alpha\beta = \{(x,y) \mid \exists z : (x,z) \in \alpha, (z,y) \in \beta\}.$$

Предложение 2.2.2. *$\mathscr{L}\mathscr{R} = \mathscr{R}\mathscr{L}$ и потому отношение $\mathscr{D} = \mathscr{L}\mathscr{R}$ является наименьшим отношением эквивалентности, содержащим $\mathscr{L}$ и $\mathscr{R}$ одновременно.*

Доказательство. Пусть $a\mathscr{L}\mathscr{R}b$: $\exists c \in S$ такое, что $a\mathscr{L}c$ и $c\mathscr{R}b$, т.е. $\exists\ u,v \in S^1, \exists\ x,y \in S^1 : a = uc, c = va, c = bx, b = cy$. Через d обозначим $ay = ucy = ub$. Покажем, что $a\mathscr{R}d$ и $d\mathscr{L}b$. $a\mathscr{L}c \Rightarrow ay\mathscr{L}cy \Rightarrow d\mathscr{L}b$. $c\mathscr{R}b \Rightarrow uc\mathscr{R}ub \Rightarrow a\mathscr{R}d$. Получили, что $a\mathscr{R}\mathscr{L}b$, т.е. $\mathscr{L}\mathscr{R} \subseteq \mathscr{R}\mathscr{L}$. Аналогично получаем обратное включение. Таким образом, $\mathscr{L}\mathscr{R} = \mathscr{R}\mathscr{L}$. □

Ясно, что $\mathscr{L} \subset \mathscr{D}$ и $\mathscr{R} \subset \mathscr{D}$. Покажем, что $\mathscr{D}$ является отношением эквивалентности:

1. Рефлексивность – очевидно.

2. Симметричность – сразу следует из того, что $\mathscr{L}\mathscr{R} = \mathscr{R}\mathscr{L}$.

3. Транзитивность – пусть $a\mathscr{D}b$, $b\mathscr{D}c$, тогда $a\mathscr{L}x\mathscr{R}b\mathscr{L}y\mathscr{R}c$, $x\mathscr{R}\mathscr{L}y \Rightarrow x\mathscr{L}\mathscr{R}y$, т.е. $x\mathscr{L}z\mathscr{R}y$; $a\mathscr{L}z$, $z\mathscr{R}c$, тогда $a\mathscr{L}\mathscr{R}c$.

Таким образом, имеет место следующая диаграмма:

2.3 Пример: отношения Грина в моноиде преобразований

Пусть X – множество. Через T_X обозначим моноид всех преобразований множества X. Для $\alpha \in T_X$ через $\operatorname{Im}\alpha$ обозначается *образ* α, т. е. множество

$$\{y \in X \mid (\exists x \in X)\, y = x\alpha\},$$

а через $\ker\alpha$ обозначается *ядро* α, т. е. разбиение множества X, при котором элементы $x, y \in X$ принадлежат одному классу тогда и только тогда, когда $x\alpha = y\alpha$. Заметим, что мощность множества классов разбиения $\ker\alpha$ (обозначаемая $|\ker\alpha|$) равно мощности $|\operatorname{Im}\alpha|$ множества $\operatorname{Im}\alpha$.

Предложение 2.3.1. *Для любых $\alpha, \beta \in T_X$ имеем:*

1. $\alpha \leq_{\mathscr{L}} \beta \Longleftrightarrow \operatorname{Im}\alpha \subseteq \operatorname{Im}\beta$*;*

2. $\alpha \leq_{\mathscr{R}} \beta \Longleftrightarrow \ker\alpha \supseteq \ker\beta$*;*

3. $\alpha \leq_{\mathscr{J}} \beta \Longleftrightarrow |\operatorname{Im}\alpha| \leq |\operatorname{Im}\beta|$.

Доказательство. (1) Если $\alpha \leq_{\mathscr{L}} \beta$, то существует такое преобразование $\gamma \in T_X$, что $\alpha = \gamma\beta$. Тогда $\operatorname{Im}\alpha = \operatorname{Im}\gamma\beta = (\operatorname{Im}\gamma)\beta \subseteq \operatorname{Im}\beta$.

Обратно, если $\operatorname{Im}\alpha \subseteq \operatorname{Im}\beta$, то для каждого $x \in X$ существует такой $y \in X$, что $x\alpha = y\beta$. Рассмотрим отображение γ, сопоставляющее каждому x один из таких y. Тогда $\alpha = \gamma\beta$.

(2) Если $\alpha \leq_{\mathscr{R}} \beta$, то существует такое преобразование $\gamma \in T_X$, что $\alpha = \beta\gamma$.

Пусть $(x, y) \in \ker\beta$, т. е. $x\beta = y\beta$. Тогда $x\alpha = x\beta\gamma = y\beta\gamma = y\alpha$. Это значит, что $(x, y) \in \ker\alpha$.

Обратно, если $\ker\alpha \supseteq \ker\beta$, то соответствие $\gamma = \beta^{-1}\alpha$ является однозначным отображением и потому принадлежит T_X. Ясно, что $\alpha = \beta\gamma$.

(3) Если $\alpha \leq_{\mathscr{J}} \beta$, то существуют такие преобразования $\gamma, \delta \in T_X$, что $\alpha = \gamma\beta\delta$. Отсюда немедленно получаем, что $|\operatorname{Im}\alpha| \leq |\operatorname{Im}\beta|$.

Обратно, рассмотрим отображение $\varepsilon : X \to X$, которое каждому классу $\ker\alpha$ сопоставляет элемент из $\operatorname{Im}\beta$ так, что разным классам соответствуют

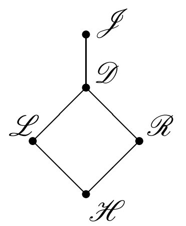


Рис. 2.1: Включения между отношениями Грина

разные элементы. Поскольку $|\ker\alpha| = |\operatorname{Im}\alpha| \le |\operatorname{Im}\beta|$, то организовать такое отображение возможно.

Так как $\ker\varepsilon = \ker\alpha$, по пункту (2) имеем $\varepsilon\mathscr{R}\alpha$. Далее, $\operatorname{Im}\varepsilon \subseteq \operatorname{Im}\beta$, поэтому по пункту (1) имеем $\varepsilon \le_{\mathscr{L}} \beta$. Отсюда $\alpha \le_{\mathscr{D}} \beta$ и потому $\alpha \le_{\mathscr{J}} \beta$. □

Отметим, что из доказательства пункта (3) вытекает, что в моноиде T_X отношения $\mathscr{D}$ и $\mathscr{J}$ совпадают.

Следствие 2.3.1. *Для любых $\alpha, \beta \in T_X$ имеем:*

1. $\alpha\mathscr{L}\beta \Longleftrightarrow \operatorname{Im}\alpha = \operatorname{Im}\beta$*;*
2. $\alpha\mathscr{R}\beta \Longleftrightarrow \ker\alpha = \ker\beta$*;*
3. $\alpha\mathscr{J}\beta \Longleftrightarrow \alpha\mathscr{D}\beta \Longleftrightarrow |\operatorname{Im}\alpha| = |\operatorname{Im}\beta|$.

2.4 Лемма Грина

Пусть $a \in S$, договоримся обозначать

$\mathscr{R}$-класс, содержащий a, через R_a;
$\mathscr{L}$-класс, содержащий a, через L_a;
$\mathscr{H}$-класс, содержащий a, через H_a;
$\mathscr{D}$-класс, содержащий a, через D_a.

Заметим, что $H_a = L_a \cap R_a$ для любого a.

Лемма 2.4.1. *Пусть L – $\mathscr{L}$-класс, R – $\mathscr{R}$-класс. Тогда $R \cap L \ne \varnothing$ тогда и только тогда, когда L и R содержатся в одном D-классе.*

Доказательство. Пусть $a \in L \cap R$. Тогда ясно, что L и R содержатся в D_a.

Обратно, пусть L и R содержатся в $\mathscr{D}$-классе D. Возьмем произвольные $x \in L$ и $y \in R$. Тогда $x\mathscr{D}y$, т. е. существует такой элемент a, что $x\mathscr{L}a\mathscr{R}y$. Тогда $a \in L \cap R$, откуда $L \cap R \ne \varnothing$. □

Лемма 2.4.1 подсказывает, что $\mathscr{D}$-классы удобно мыслить себе как прямоугольные таблицы (по традиции именуемые *egg-box картинками*), в которых строки изображают $\mathscr{R}$-классы, столбцы – $\mathscr{L}$-классы, а ячейки – $\mathscr{H}$-классы.

Следующий важный результат показывает, что элементы каждого $\mathscr{D}$-класса распределены по ячейкам соответствующей egg-box картинки равномерно.

Предложение 2.4.1 (Лемма Грина)**.** *Пусть $a\mathscr{R}b$, т. е. существуют $u, v \in S^1$, такие, что $au = b$ и $bv = a$. Рассмотрим отображения $\rho_u : S \to S$, задаваемое правилом $x\rho u = xu$, и $\rho_u : S \to S$, задаваемое правилом $x\rho v = xv$. Тогда ограничение ρ_u на класс L_a – это биекция L_a на L_b, ограничение ρ_v на класс L_b – обратная к ней биекция, и оба ограничения сохраняют $\mathscr{H}$-классы.*

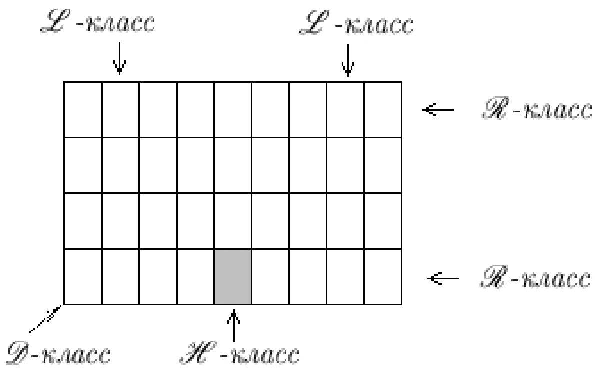


Рис. 2.2: egg-box картинка

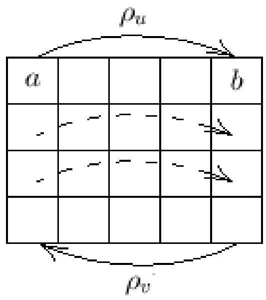


Рис. 2.3: Иллюстрация к лемме Грина

Доказательство. Возьмем произвольный элемент $x \in L_a$. Из $x \mathscr{L} a$ следует, что $xu \mathscr{L} au = b$, поскольку отношение $\mathscr{L}$ стабильно справа. Следовательно, $L_a \rho_u \subseteq L_b$. Далее, существует элемент $t \in S^1$, такой, что $x = ta$. Имеем

$$x\rho_u\rho_v = xuv = tauv = tbv = ta = x,$$

т. е. ограничение ρ_v на класс L_b – обратное отображение к ограничению ρ_u на класс L_a.

Получается, что ограничение ρ_v на класс L_b отображает L_b на L_a, следовательно, ограничения ρ_u и ρ_v на соответственно L_a на L_b – взаимно обратные биекции. Поскольку $xuv = x$, имеем $x\mathscr{R}xu$, и если $x \mathscr{H} y$, то $xu \mathscr{H} yu$. Обратно, если $xu \mathscr{H} yu$, то $x \mathscr{H} y$ $\square$

В качестве примера рассмотрим $\mathscr{D}$-строение моноида T_3 всех преобразований 3-элементного множества $\{1, 2, 3\}$. Согласно доказанному в §2.3, у него ровно три $\mathscr{D}$-класса: класс D_3 всех преобразований с 3-элементным образом, класс D_2 всех преобразований с 2-элементным образом и класс D_1 всех преобразований с 1-элементным образом. Ясно, что преобразование 3-элементного множества, образ которого 3-элементен, есть не что иное как перестановка этого множества. Таким образом, класс D_3 состоит из 6 перестановок исходного множества. Класс D_1 состоит из трех константных

	$\{1,2\}$	$\{1,3\}$	$\{2,3\}$
$1 \mid 23$	$\left(\begin{smallmatrix}1&2&3\\1&2&2\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\2&1&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&2&3\\1&3&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\3&1&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&2&3\\2&3&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\3&2&2\end{smallmatrix}\right)$
$2 \mid 13$	$\left(\begin{smallmatrix}1&2&3\\1&2&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\2&1&2\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&2&3\\1&3&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\3&1&3\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&2&3\\2&3&2\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\3&2&3\end{smallmatrix}\right)$
$3 \mid 12$	$\left(\begin{smallmatrix}1&2&3\\1&1&2\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\2&2&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&2&3\\1&1&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\3&3&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&2&3\\2&2&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\3&3&2\end{smallmatrix}\right)$

Таблица 2.1: $\mathscr{D}$-класс моноида T_3, состоящий из всех преобразований с 2-элементным образом. Над каждым $\mathscr{L}$-классом показано параметризующее его 2-элементное подмножество, а левее каждого $\mathscr{R}$-класса – параметризующее его разбиение.

преобразований. Интереснее всего устроен класс D_2. Его egg-box картинка показана ниже.

2.5 Роль идемпотентов

Элемент e называется *идемпотентом*, если $e^2 = e$.

Лемма 2.5.1. *В конечной полугруппе для любого элемента, найдется его степень, которая является идемпотентом.*

Доказательство. Пусть S – конечная полугруппа, $a \in S$, рассмотрим элементы $a, a^2, a^3, \dots$. Найдутся такие n и k, что $a^n = a^{n+k}$. Рассмотрим a^{nk}. Имеем $(a^{nk})^2 = a^{2nk} = a^{nk+nk} = a^{nk}$. Следовательно, nk – искомая степень. □

Упражнение 2.5.1. *Для данного элемента полугруппы найти наименьшую степень, в которой он является идемпотентом.*

Упражнение 2.5.2. *Пусть полугруппа S имеет порядок n. Доказать, что для любого $a \in S$ элемент $a^{n!}$ является идемпотентом.*

Предложение 2.5.1. *В конечной полугруппе $\mathscr{D} = \mathscr{J}$.*

Доказательство. Включение $\mathscr{D} \subseteq \mathscr{J}$ выполняется в любой полугруппе в силу того, что $\mathscr{D}$ – наименьшее отношение эквивалентности, содержащее отношения $\mathscr{R}$ и $\mathscr{L}$.

Пусть $a \mathscr{J} b$. Найдутся такие $u, v, x, y \in S^1 : uav = b, xby = a$, отсюда $xuavy = a$. Следовательно для любого k получим $(xu)^k a (vy)^k = a)$. Отсюда по лемме найдется такое k, что $(xu)^k = e, (vy)^k = f$, следовательно $eaf = a$, откуда $ea = a$ и $af = a$.

Покажем, что $ua \mathscr{L} a$. Ясно, что $ua \in S^1 a$. Обратно, $a = ea = (xu)^k a = (xu)^{k-1} x \cdot ua \in S^1 ua$. Аналогично $a \mathscr{R} av$. Получаем $ua \mathscr{R} uav = b$ и $a \mathscr{L} ua \mathscr{R} b$, т. е. $a \mathscr{L}\mathscr{R} b$ и $a \mathscr{D} b$ □

Теперь мы снова рассматриваем произвольные полугруппы.

Предложение 2.5.2 (Теорема Миллера-Клиффорда)**.** *Пусть $a, b \in S$, тогда $ab \in R_a \cap L_b$ тогда и только тогда, когда пересечение $R_b \cap L_a$ содержит идемпотент.*

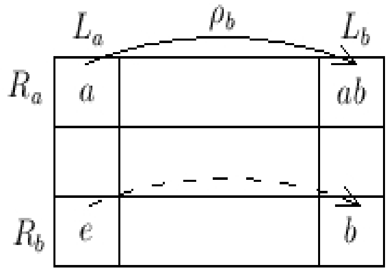


Рис. 2.4: Иллюстрация к теореме Миллера–Клиффорда

Доказательство. $\Rightarrow$ Если $ab \in R_a \cap L_b$, то по лемме Грина $\rho_b|_{L_a}$ – биекция L_a на L_b. Пусть $e \in R_b \cap L_a$ – такой элемент, что $e\rho_b = eb = b$. Тогда $e\mathscr{R}b$, в частности, $e = bu$ для некоторого $u \in S^1$. Имеем $e^2 = e(bu) = (eb)u = bu = e$, т.е. e – идемпотент.
$\Leftarrow$ Пусть e – идемпотент из $R_b \cap L_a$. Из $e\mathscr{R}b$ следует, что $eb = b$, а из $e\mathscr{L}a$ следует, что $ae = a$. Умножив соотношение $e\mathscr{R}b$ слева на a, получим $a = ae\mathscr{R}ab$. Аналогично, умножив соотношение $e\mathscr{L}a$ справа на b, получим $b = eb\mathscr{R}ab$. Следовательно $ab \in R_a \cap L_b$. □

Следствие 2.5.1. *Пусть H – $\mathscr{H}$-класс, тогда следующие условия эквивалентны:*

(1) H содержит идемпотент;

(2) существуют $a, b \in H$, такие, что $ab \in H$;

(3) H – группа.

Доказательство. Импликации (1) $\Rightarrow$ (2) и (3) $\Rightarrow$ (1) очевидны.
(2) $\Rightarrow$ (3) Имеем $H = R_a \cap L_b = R_b \cap L_a$. По теореме Миллера–Клиффорда в H найдется идемпотент e. Применяя ту же теорему в обратную сторону, заключаем, что для любых $g, h \in H$ произведение gh принадлежит H, т.е. H – полугруппа. Для любого $h \in H$ отображение $\rho_h|_H$ – биекция H на H. Отсюда, в частности, следует, что $ge = g$ для любого $g \in H$. В силу симметричных рассуждений $eg = g$ для любого $g \in H$, т.е. e – единица в H. Наконец, из того, что $\rho_h|_H$ – биекция H на H, следует, что для любого $h \in H$ существует элемент h', такой, что $h'h = e$. Следовательно H – группа. □

Заметим, что если H – группа, то H – максимальная подгруппа. Действительно, если G – какая-то подгруппа полугруппы S, то любые два элемента $g, h \in G$ делят друг друга и справа, и слева: $g = h \cdot h^{-1}g$, $h = g \cdot g^{-1}h$ и аналогично слева. Поэтому G содержится в некотором $\mathscr{H}$-классе H. Поскольку H содержит идемпотент (а именно, единицу подгруппы G), по только что доказанному следствию H есть подгруппа. Итак, каждая подгруппа полугруппы содержится ровно в одной максимальной подгруппе, а именно, в $\mathscr{H}$-классе единицы этой подгруппы.

Предложение 2.5.3. *Любые две максимальные подгруппы внутри одного $\mathscr{D}$-класса изоморфны.*

Доказательство. Пусть H_1 и H_2 – две такие подгруппы. По следствию из теоремы Миллера-Клиффорда существуют идемпотенты e и f такие, что $H_1 = H_e$ и $H_2 = H_f$. Поскольку все происходит внутри одного $\mathscr{D}$-класса, имеем $e \mathscr{D} f$. Таким образом, $e \mathscr{R} a \mathscr{L} f$ для некоторого $a \in S$. Из того, что $a \mathscr{L} f$, получаем, что существует элемент $a' \in S^1$, для которого $f = a'a$.

На H_e рассмотрим отображение, определенное правилом $x \mapsto a'xa$. Из леммы Грина и утверждения, двойственного к ней, следует, что это отображение есть биекция H_e на H_f. Осталось проверить, что это отображение является гомоморфизмом.

Заметим, что $aa'a = af = a$. Отсюда $(aa')(aa') = (aa'a)a' = aa'$, т. е. aa' — идемпотент из R_a.

Для произвольных $x, y \in H_e$, поскольку $(aa')y = y$, получаем

$$(a'xa)(a'ya) = a'x(aa'y)a = a'xya,$$

что и показывает, что отображение $x \mapsto a'xa$ есть гомоморфизм. □

Элемент $a \in S$ называется *регулярным*, если существует такой $x \in S$, что $axa = a$. Класс отношения Грина называется *регулярным*, если все его элементы регулярны.

Предложение 2.5.4. *Пусть D – некоторый $\mathscr{D}$-класс. Следующие условия эквивалентны:*

(1) D – регулярный $\mathscr{D}$-класс;

(2) в D есть регулярный элемент;

(3) каждый $\mathscr{R}$-класс внутри D содержит идемпотент;

(4) каждый $\mathscr{L}$-класс внутри D содержит идемпотент;

(5) в D есть идемпотент;

(6) существуют такие $x, y \in D$, что $xy \in D$.

Доказательство. Эквивалентность условий (1)–(5) вытекает из следующей леммы и двойственного ей утверждения:

Лемма 2.5.2. *$\mathscr{R}$-класс регулярен тогда и только тогда, когда он содержит идемпотент.*

Доказательство. Пусть $a \mathscr{R} e$, где e — идемпотент. Тогда существует такой элемент $u \in S^1$, что $e = au$. Имеем следующую цепочку равенств: $a = ea = e^2a = (au)ea = a(ue)a$. Поскольку $ue \in S$, видим, что элемент a регулярен.

Обратно, если $axa = a$ для некоторого $x \in S$, то ax — идемпотент, лежащий в R_a. □

Очевидно, что $(5) \Rightarrow (6)$, а импликация $(6) \Rightarrow (5)$ следует из теоремы Миллера-Клиффорда. □

2.6 Алгоритм вычисления регулярных $\mathscr{D}$-классов в конечных полугруппах преобразований

Предложение 2.6.1. *Пусть S – подполугруппа в T_X и $\alpha, \beta \in S$. Тогда:*

(1) Если $\alpha \leq_{\mathscr{R}} \beta$, то $\ker\alpha \supseteq \ker\beta$ и если $\alpha \mathscr{R} \beta$, то $\ker\alpha = \ker\beta$.

(2) Если $\alpha \leq_{\mathscr{L}} \beta$, то $\operatorname{Im}\alpha \subseteq \operatorname{Im}\beta$ и если $\alpha \mathscr{L} \beta$, то $\operatorname{Im}\alpha = \operatorname{Im}\beta$.

(3) Если $\alpha \leq_{\mathscr{J}} \beta$, то $|\operatorname{Im}\alpha| \leq |\operatorname{Im}\beta|$ и если $\alpha \mathscr{J} \beta$, то $|\operatorname{Im}\alpha| = |\operatorname{Im}\beta|$.

Это предложение является простым следствием описания отношений Грина в T_X. Отметим, что обратные импликации в общем случае (т. е. для произвольной подполугруппы S) неверны, хотя они верны для T_X.

Пусть Y – подмножество множества X, а π – разбиение X. Говорят, что Y – *трансверсаль* разбиения π, если каждый π-класс содержит ровно один элемент из Y.

Предложение 2.6.2. *Пусть X – конечное множество и S – подполугруппа в T_X. Элемент $\alpha \in S$ принадлежит некоторой подгруппе в S тогда и только тогда, когда $\operatorname{Im}\alpha$ есть трансверсаль разбиения $\ker\alpha$.*

Доказательство. Необходимость. Пусть $\alpha \in S$ лежит в некоторой подгруппе, тогда $\alpha^n = \alpha$ для некоторого n. Поэтому $\alpha|_{\operatorname{Im}\alpha}$ – биекция (перестановка).

Пусть K – произвольный класс разбиения $\ker\alpha$. Если $|K \cap \operatorname{Im}\alpha| \geq 2$, то по крайней мере два элемента из $\operatorname{Im}\alpha$ склеиваются под действием α, что невозможно, поскольку α – биекция. Значит, $|K \cap \operatorname{Im}\alpha| \leq 1$ для любого K. Если предположить, что для некоторого K выполняется $K \cap \operatorname{Im}\alpha = \varnothing$, то

$$|\operatorname{Im}\alpha| = \sum_{K \in \ker\alpha} |K \cap \operatorname{Im}\alpha| < |\ker\alpha|,$$

что также невозможно, поскольку $|\operatorname{Im}\alpha| = |\ker\alpha|$.

Достаточность. Если $\operatorname{Im}\alpha$ – трансверсаль в $\ker\alpha$, то $\alpha|_{\operatorname{Im}\alpha}$ – перестановка, тогда существует n такое, что $\alpha^n = \alpha$. Отсюда следует, в частности, что $\alpha^2 \mathscr{H} \alpha$, а значит, $\mathscr{H}$-класс элемента α является подгруппой, поскольку содержит идемпотент. □

Изложим теперь алгоритм построения регулярных $\mathscr{D}$-классов конечной полугруппы преобразований.

0. Находим групповой элемент $x \in S$.

1. Вычисляем образы $\operatorname{Im} xr$ для всех $r \in S^1$ такие, что $|\operatorname{Im} xr| = |\operatorname{Im} x|$. Для каждого такого образа I сохраним такое r, что $I = \operatorname{Im} xr$.

2. Параллельно вычисляем все такие преобразования xr ($r \in S^1$), что $\operatorname{Im} xr = \operatorname{Im} x$. *Из этих преобразований состоит $\mathscr{H}$-класс H_x.*

3. Вычисляем все разбиения вида $\ker sx$ ($s \in S^1$), такие, что $|\ker sx| = |\ker x|$. Для каждого такого разбиения сохраняем значение s, при котором оно получается.

4. Среди образов, построенных на шаге 1, сохраняем только те, которые служат трансверсалями для каких-то из разбиений, построенных на шаге 3, а среди разбиений, построенных на шаге 3, сохраняем только те, для которых хотя бы одно из множеств, построенных на шаге 1, является трансверсалью. Получим набор множеств $I_1(=\operatorname{Im} x), \dots, I_k$ с соответствующими элементами $r_1(=1), \dots r_k \in S^1$ и набор разбиений $\pi_1(=\ker x), \dots, \pi_\ell$ с соответствующими элементами $s_1(=1), \dots s_\ell \in S^1$. *Тогда $\mathscr{D}$-класс элемента x состоит в точности из элементов вида $s_i h r_j$, где h пробегает H_x.*

	$\operatorname{Im} x$	$\dots$	$\operatorname{Im} xr_j$	$\dots$	$\operatorname{Im} xr_k$
$\ker x$	H_x				
$\dots$					
$\ker s_i x$			H_{ij}		
$\dots$					
$\ker s_\ell x$					

Для обоснования алгоритма нужна следующая лемма. В ее формулировке участвуют отношения Грина $\mathscr{R}$ и $\mathscr{L}$ в полугруппе T и ее подполугруппе S. Будем с помощью верхних индексов ^{T} или ^{S} указывать, в какой полугруппе рассматривается соответствующее отношение. Аналогичное соглашение используется для классов отношений Грина.

Лемма 2.6.1 (о четвертом угле)**.** *Пусть S – подполугруппа конечной полугруппы T, $x \in S$, $a, b \in S^1$, $e = e^2 \in T$. Если*

$$e \mathscr{R}^T bx \mathscr{L}^T x \mathscr{R}^T xa \mathscr{L}^T e,$$

то $e \in S$ и

$$e \mathscr{R}^S bx \mathscr{L}^S x \mathscr{R}^S xa \mathscr{L}^S e.$$

Доказательство. Пересечение $L^T_{xa} \cap R^T_{bx}$ содержит идемпотент (а именно, e). По теореме Миллера-Клиффорда имеем

$$xabx \in L^T_{bx} \cap R^T_{xa} = H^T_x,$$

следовательно, по лемме Грина $\rho_{abx}|_{H^T_x}$ – биекция, а значит, существует k такое, что ρ^k_{abx} – тождественная перестановка. Отсюда $x(abx)^k = x$, а потому $xa \mathscr{R}^S x \mathscr{L}^S bx$. Так как $xabx \in L^S_{bx} \cap R^S_{xa}$, пересечение $L^S_{xa} \cap R^S_{bx}$ содержит идемпотент по теореме Миллера-Клиффорда. Ясно, что $L^S_{xa} \cap R^S_{bx} \subseteq L^T_{xa} \cap R^T_{bx}$, а e – единственный идемпотент в $L^T_{xa} \cap R^T_{bx}$. Итак, $e \in L^S_{xa} \cap R^S_{bx}$. $\square$

Займемся обоснованием алгоритма, т. е. докажем утверждения, сформулированные в его описании (они выделены курсивом).

Пусть h – произвольный элемент из H_x. Рассмотрим элемент hr такой, что $\operatorname{Im} hr \in \{I_1(=\operatorname{Im} x), \dots, I_k\}$. Тогда среди разбиений $\pi_1(=\ker x), \dots, \pi_\ell$ найдется такое разбиение $\pi = \ker sh$, для которого $\operatorname{Im} hr$ является трансверсалью. Рассмотрим преобразование $e \in T_X$, которое переводит каждый класс K разбиения $\pi = \ker sh$ в единственный элемент множества

$K \cap \operatorname{Im} hr$. Тогда e – идемпотент в $T = T_X$ такой, что $\ker e = \ker sh$ и $\operatorname{Im} e = \operatorname{Im} hr$, откуда $e \mathscr{R}^T hr$ и $e \mathscr{L}^T sh$. Тогда по лемме о четвертом угле $e \in S$ и

$$e \mathscr{R}^S sh \mathscr{L}^S h \mathscr{R}^S hr \mathscr{L}^S e. \tag{2.2}$$

Возьмем сначала в качестве h исходный элемент x и пусть $r \in S^1$ таково, что $\operatorname{Im} xr = \operatorname{Im} x$. Тогда в роли s можно взять 1, а идемпотент e – это не то иное как единица подгруппы H_x. Из (2.2) заключаем, что $xr \in H_x$. Так как очевидно, что любой элемент из H_x можно представить в виде xr для некоторого $r \in S^1$ такого, что $\operatorname{Im} xr = \operatorname{Im} x$, мы доказали утверждение, сформулированное на шаге 2 алгоритма.

Теперь снова возьмем произвольный элемент $h \in H_x$ и рассмотрим произвольный элемент вида $s_i h r_j$. По построению, существуют такое p, что $\operatorname{Im} hr_j$ является трансверсалью для $\ker s_p h$, и такое q, что $\operatorname{Im} hr_q$ является трансверсалью для $\ker s_i h$. Применяя (2.2) с $r = r_j$ и $s = s_p$ заключаем, что $h \mathscr{R}^S hr_j$, а тот же аргумент, примененный к $r = r_p$ и $s = s_i$, дает $h \mathscr{L}^S s_i h$, откуда $hr_j \mathscr{L}^S s_i h r_j$ (напомним, что отношение $\mathscr{L}$ стабильно справа). Итак, $h \mathscr{R}^S hr_j \mathscr{L}^S s_i h r_j$, т. е. $s_i h r_j$ принадлежит $\mathscr{D}$-классу элемента x. Обратно, очевидно, что любой элемент из этого $\mathscr{D}$-класса можно представить в виде $s_i h r_j$ для подходящего $h \in H_x$. Мы доказали утверждение, сформулированное на шаге 4 алгоритма.

	$\operatorname{Im} x$	$\dots$	$\operatorname{Im} xr_j$	$\dots$	$\operatorname{Im} xr_q$
$\ker x$	h		hr_j		
$\dots$					
$\ker s_i x$	$s_i h$		$s_i h r_j$		$*$
$\dots$					
$\ker s_p x$			$*$		

Глава 3

Синтаксический моноид и минимальный автомат

3.1 Моноид переходов автомата

Пусть даны конечный алфавит Σ и язык $L \subseteq \Sigma^*$. Пусть M – моноид. Говорят, что язык L распознаётся моноидом M, если существуют такой гомоморфизм $\varphi\colon \Sigma^* \Rightarrow M$ и такое подмножество $P \subseteq M$, что для любого слова $w \in \Sigma^*$ выполнена эквивалентность $w \in L \Longleftrightarrow w\varphi \in P$.

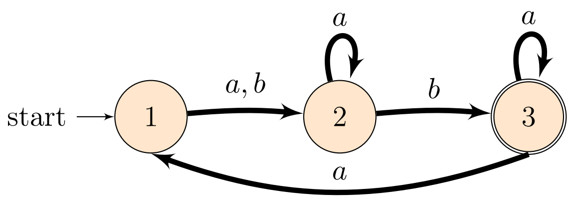
Теорема 3.1.1. *Для языка $L \subseteq \Sigma^*$ следующие два условия эквивалентны:*
(1) L распознаётся некоторым конечным моноидом;
(2) L распознаётся некоторым конечным автоматом.

Доказательство. (1) $\Rightarrow$ (2)
Пусть L распознаётся конечным моноидом M. Построим автомат, который распознаёт тот же язык L. Построим автомат следующим образом:

- M — множество его состояний.
- Σ — его алфавит.
- $\delta : M \times \Sigma \to M$, определённая следущим образом: $\delta(m, a) := m(a\varphi)$ — функция переходов.
- 1(нейтральный элемент)— начальное состояние.
- P — множество заключительных состояний.

Покажем, что определённый выше автомат распознаёт язык L. Для этого покажем, что языкL состоит в точности из тех слов, что если мы начнём из начального состояния автомата, то перейдём в конечное его состояние.
Берём слово $w = a_1 a_2 \ldots a_n$, где $a_i \in \Sigma$
$\delta(1, a_1, \ldots, a_n) = 1 \cdot (a_1\varphi)(a_2\varphi) \cdot \ldots (a_n\varphi)$
Вспомним, что φ — гомоморфизм и $(uv)\varphi = u\varphi v\varphi$, получим следущее:
$1 \cdot (a_1\varphi)(a_2\varphi) \cdot \ldots (a_n\varphi)(1 \cdot a_1 \cdot \ldots a_n)\varphi = 1 \cdot w\varphi = w\varphi \in P$.
(2) $\Rightarrow$ (1)

Пусть дан автомат $\mathcal{A} = (Q, \Sigma, \delta, q_0, F)$,
где Q — множество состояний автомата,
Σ — входной алфавит,
δ — функция перехода,
q_0 — начальное состояние автомата,
F — множество конечных состояний автомата. Автомат $\mathcal{A}$ распознаёт наш язык, то есть $w \in L \Longleftrightarrow \delta(q_0, w) \in F$.
Поступим следующим образом: каждое слово из Σ^* вызывает некоторое преобразование множества Q, обозначим это преобразование $\delta(\sqcup, w)$.
Пример-пояснение преобразования $\delta(\sqcup, w)$.
Пусть дан автомат:



Рассмотрим преобразование, вызванное буквой a: $\delta(\sqcup, a) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 3 \end{pmatrix}$
То есть из состояния 1 посредством буквы a мы можем перейти в состояние 2, из состояния 2 так же посредством буквы a можем перейти в состояние 2, из состояния 3 — в состояние 3.
Аналогично для преобразований, вызванных b, ab: $\delta(\sqcup, b) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ и
$\delta(\sqcup, ab) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 3 & 1 \end{pmatrix}$
Моноидом переходов автомата $\mathcal{A}$ называется моноид,состоящий из всех таких преобразований $\Big($ например, преобразование $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ не будет лежать в моноиде переходов для данного автомата $\Big)$. То преобразование, которое вызвано w, и есть образw: $w\varphi := \delta(\sqcup, w)$.
В качестве множества P возьмём преобразования, вызванные словами из L. Действительно, если $w \in L$, то по определению $w\varphi \in P$(в одну сторону это следует из определения P).
Обратно: пусть $w\varphi \in P$. Тогда существует такое слово $v \in L$, что $v\varphi = w\varphi$. Если отображение φ действуют одинаково на v и w, то оно будет действовать одинаково и на пустое слово. Тогда $q_0(v\varphi) = q_0(w\varphi)$, то есть $\delta(q_0, v) = \delta(q_0, w)$, где $\delta(q_0, v) \in F$, так как $v \in L \to w \in L$ $\square$

3.2 Алгоритм построения моноида переходов

Пусть есть автомат $\mathcal{A} = (Q = \{1, 2, \ldots, n\}, \Sigma, \delta, , q_0, F)$,
где Q — множество состояний автомата,
Σ — входной алфавит,
δ — функция перехода
q_0 — начальное состояние автомата,
F — множество конечных состояний автомата.
Основная таблица будет иметь следующий вид:

	1	2	3	...n
a				
b				
c				
$\vdots$				

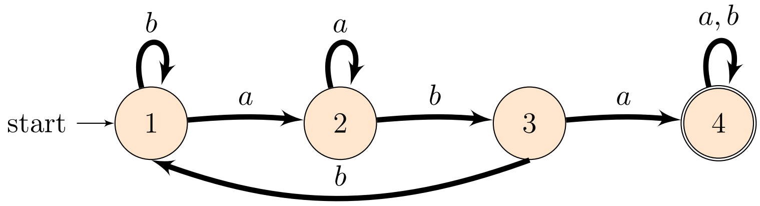
Название столбцов в таблице — множество состояний автомата, а строк — символы входного алфавита.
Первым уровнем основной таблицы будем называть все возможные действия слов длины один, другими словами, это все слова длины один, которые вызваны буквами входного алфавита Σ, и основная таблица будет иметь вид:

	1	2	3	...n
a	$\delta(1, a)$	$\delta(2, a)$	$\delta(3, a)$	...
b	$\delta(1, b)$	$\delta(2, b)$	$\delta(3, b)$	...
c	...	$\delta(\sqcup, c)$	...	
$\vdots$				

Под i-м уровнем основной таблицы будем понимать все возможные действия слов длины i, то есть все слова длины i, которые получены из слов длины $i-1$ посредством действия на них слов алфавита Σ.
При построении моноида переходов также появится таблица соотношений, суть которой будет раскрыта ниже.
Заполнять основную таблицу будем следующим образом: к каждому слову u длины i, которое есть в таблице, применяем буквы из входного алфавитаΣ, получая при этом $(i+1)$-й уровень основной таблицы.
На самом деле в таблице будут не все слова длины i, так как в таблице только действия слов длины i, а различные слова могут порождать одни и те же действия, таким образом слов конкретной длины будет больше, чем их действий.
Вычисляем действие слова $u\cdot$«очередная буква алфавита Σ », то есть к строке со словом u применяем буквы алфавита Σ. Если такого действия ещё нет в основной таблице, то дописываем слово $u+$очередная буква алфавита Σ и его действие в таблицу; а если такое действие уже было в строке, отвечающей слову v, то не записываем действие в основную таблицу, а записываем его в таблицу соотношений.

Таблица соотношений	
$u\cdot$ «очередная буква алфавита »	v

То есть слова $u\cdot$ «очередная буква алфавита и v вызывают одно и то же действие.
Останавливается всё тогда, когда не можем ничего в таблицу дописать.
Пример.
Дан минимальный автомат, язык $L = \Sigma^* aba \Sigma^*$.



Построим для этого автоматат моноид переходов.

	1	2	3	4
a	2	2	4	4
b	1	3	1	4

Подействуем буквой a. Получим следующую таблицу:

	1	2	3	4
a	2	2	4	4
b	1	3	1	4
ba	2	4	2	4

В таблицу соотношений при этом запишется $aa = a^2 = a$, так как такое действие уже есть в таблице.
Подействуем буквой b. Получим следующую таблицу:

	1	2	3	4
a	2	2	4	4
b	1	3	1	4
ba	2	4	2	4
ab	3	3	4	4
b^2	1	1	1	4

Итерируем процесс,записывая произведение на букву. Получим следующую таблицу:

	1	2	3	4
a	2	2	4	4
b	1	3	1	4
ba	2	4	2	4
ab	3	3	4	4
b^2	1	1	1	4
aba	4	4	4	4
ab^2	1	1	4	4
bab	3	4	3	4
b^2a	2	2	2	4
bab^2	1	4	1	4
b^2ab	3	3	3	4

Таблица соотношений при этом будет состоять из записей

Таблица соотношений	
$aa = a^2$	a
b^2ab^2	b^2
b^3	b^2
$baba$	aba
$abab$	aba
ab^2a	a

То есть слова, записанные в данной таблице соотношений, различны, но порождёны одними и теми же действиями. Поясним на первой строке таблицы. Действуя буквой a дважды или трижды, мы вновь получим то же действие, которое уже есть в основной таблице.

Глава 4

Теорема Саймона

Напомним определение кусочно тестируемого языка.

Определение 4.0.1. Язык над данным конечным алфавитом Σ называется *кусочно тестируемым*, если он может быть получен с помощью конечного числа операций объединения, пересечения и дополнения из языков вида $\Sigma^* a_1 \Sigma^* a_2 \Sigma^* \ldots \Sigma^* a_k \Sigma^*$, где $a_i \in \Sigma$.

Данное определение не позволяет эффективно проверять кусочную тестируемость данного регулярного языка (заданного, например, автоматом). Эффективная характеризация класса кусочно тестируемых языков была получена Саймоном. Он доказал, что язык является кусочно тестируемым тогда и только тогда, когда его синтаксический моноид $\mathscr{J}$-тривиален. Необходимость этого условия доказывается довольно просто. Вся сложность заключается в доказательстве достаточности этого условия. Существуют различные доказательства достаточности, использующие разные техники: оригинальное комбинаторное доказательство Саймона, доказательство Страубинга и Терьена, использующее свойства упорядоченных моноидов, доказательство Алмейды, основывающееся на сложной проконечной топологии, доказательство Хиггинса через полугруппы переходов. В данной главе мы изложим два доказательства, основанных на комбинаторике слов: доказательство Саймона и доказательство, предложенное недавно чешским математиком Ондрой Климой.

Дадим необходимые определения.

Определение 4.0.2. Слово $u = a_1 a_2 \cdots a_k \in \Sigma^*$, где $a_1, a_2, \ldots, a_k \in \Sigma$, называется *подсловом* слова $v \in \Sigma^*$, если существуют слова $v_0, v_1, \ldots, v_k \in \Sigma^*$ такие, что $v = v_0 a_1 v_1 a_2 \cdots a_k v_k$.

Например, слово “date” является подсловом слова “derivative”, а слово “пиво” – подсловом слова “производная”. Легко видеть, что отношение «быть подсловом» на множестве всех слов является отношением частичного порядка. Для обозначения этого отношения будем использовать символ $\trianglelefteq$: пишем $u \trianglelefteq v$, если слово u является подсловом слова v.

Для слова $u \in \Sigma^*$ через L_u обозначим язык всех слов, содержащих в качестве подслова слово u: $L_u = \{v \in \Sigma^* \mid u \trianglelefteq v\}$. Если $u = a_1 a_2 \cdots a_\ell$, где

$a_1, a_2, \ldots, a_\ell \in \Sigma$, то

$$L_u = \Sigma^* a_1 \Sigma^* a_2 \Sigma^* \cdots \Sigma^* a_\ell \Sigma^*.$$

Для $v \in \Sigma^*$ через $\mathsf{Sub}_k(v)$ обозначим множество всех подслов слова v длины не более k:

$$\mathsf{Sub}_k(v) = \{u \in \Sigma^* \mid u \trianglelefteq v, |u| \leq k\}.$$

На множестве всех слов Σ^* зададим отношение *равноподсловности* $\sim_k$ по правилу $u \sim_k v \Leftrightarrow \mathsf{Sub}_k(u) = \mathsf{Sub}_k(v)$. Например, $abbac \sim_1 cba$, поскольку оба этих слова содержат одинаковые буквы, и $ababab \sim_3 bababa$, поскольку оба слова содержат все подслова длины не более 3. Очевидно, $\sim_k$ является *конгруэнцией* на Σ^*, т.е. отношением эквивалентности, для которого справедлива импликация $u \sim_k v \Rightarrow wu \sim_k wv$, $uw \sim_k vw$ для любых слов $u, v, w \in \Sigma^*$.

Для регулярного языка $L \subseteq \Sigma^*$ определим отношение $\sim_L$: для любых слов $u, v \in \Sigma^*$

$$u \sim_L v \;\Leftrightarrow\; (\forall x, y \in \Sigma^*)(xuy \in L \Leftrightarrow xvy \in L).$$

Легко видеть, что отношение $\sim_L$ является конгруэнцией на Σ^*. Это отношение называется *синтаксической конгруэнцией* языка L, а соответствующий фактор-моноид $\Sigma^*/\sim_L$ называется *синтаксическим моноидом* языка L. Одним из базовых утверждений алгебраической теории рациональных языков является утверждение о том, что моноид $\Sigma^*/\sim_L$ изоморфен моноиду переходов минимального автомата языка L. В частности, моноид $\Sigma^*/\sim_L$ конечен, а значит, конгруэнция $\sim_L$ имеет конечный индекс. Кроме того, как легко заметить, язык L является объединением некоторых классов разбиения, заданного эквивалентностью $\sim_L$.

Определение 4.0.3. Конгруэнция $\sim$ на Σ^* называется $\mathscr{J}$-тривиальной, если фактор-моноид $\Sigma^*/\sim$ $\mathscr{J}$-тривиален.

Упражнение 4.0.1. *Доказать, что $\mathscr{J}$-тривиальность конгруэнции $\sim$ на Σ^* эквивалентна следующему условию:*

$$w_1 w_2 u w_3 w_4 \sim u \;\Rightarrow\; w_2 u w_3 \sim u$$

для любых слов $u, w_1, w_2, w_3, w_4 \in \Sigma^*$.

В рассматриваемых в этой главе доказательствах теоремы Саймона удобно пользоваться эквивалентным определением кусочно тестируемого языка. Это определение можно дать, благодаря следующей лемме.

Лемма 4.0.1. *Пусть L – регулярный язык над алфавитом Σ. Следующие условия эквивалентны.*

(1) Существует натуральное число k такое, что $\sim_k \subseteq \sim_L$.

(2) Язык L кусочно тестируем.

Доказательство. Если $\sim_k \subseteq \sim_L$ для некоторого натурального k, то каждый класс разбиения $\Sigma^*/\sim_L$ является объединением классов разбиения $\Sigma^*/\sim_k$. Поскольку L является объединением классов разбиения $\Sigma^*/\sim_L$, достаточно показать, что каждый класс разбиения $\Sigma^*/\sim_k$ может быть получен из языков вида L_u при помощи конечного числа операций объединения, пересечения и дополнения. Зафиксируем $v \in \Sigma^*$. Обозначим через $x \sim_k$ класс эквивалентности слова v, т.е. $v \sim_k = \{w \in \Sigma^* \mid w \sim_k v\}$. Непосредственно проверяется, что

$$v \sim_k = \bigcap_{u \in \mathsf{Sub}_k(v)} L_u \cap \bigcap_{u \notin \mathsf{Sub}_k(v), |u| \leq k} \overline{L}_u.$$

В обратную сторону, пусть язык L кусочно тестируем, т.е. представляется в виде конечного объединения конечных пересечений языков вида L_u и их дополнений. Пусть k – такое натуральное число, что $|u| \leq k$ для всех слов u, использованных в представлении языка L. Докажем, что $\sim_k \subseteq \sim_L$. Итак, пусть $v, w \in \Sigma^*$ и $v \sim_k w$, т.е. $\mathsf{Sub}_k(v) = \mathsf{Sub}_k(w)$. Рассмотрим произвольные слова $x, y \in \Sigma^*$ такие, что $xvy \in L$. Докажем, что $xwy \in L$. Без ограничения общности можно считать, что

$$xvy \in K = L_{u_1} \cap L_{u_2} \cap \cdots \cap L_{u_m} \cap \overline{L}_{v_1} \cap \overline{L}_{v_2} \cap \cdots \cap \overline{L}_{v_n},$$

где K – один из членов объединения в представлении языка L. Длина каждого из слов $u_1, u_2, \ldots, u_m, v_1, v_2, \ldots, v_n$ меньше k. Для каждого $i = 1, \ldots, m$ имеем $xvy \in L_{u_i}$, а для каждого $j = 1, \ldots, n$ слово $xvy \notin L_{v_j}$. Для каждого $i = 1, \ldots, m$ по определению языка L_{u_i} имеем $u_i \trianglelefteq xvy$. Поскольку $\mathsf{Sub}_k(v) = \mathsf{Sub}_k(w)$, получаем $u_i \trianglelefteq xwy$ для каждого $i = 1, \ldots, m$. Следовательно, $xwy \in L_{u_i}$ для каждого $u = 1, \ldots, m$. Далее $xwy \notin L_{v_j}$ для каждого $j = 1, \ldots, n$, поскольку $xwy \in L_{v_j}$ влечет $xvy \in L_{v_j}$, что неверно. В итоге получаем, что слово $xwy \in K$, а следовательно, и $xwy \in L$. Поменяв местами слова v и w, мы получим доказательство обратной импликации $xwy \in L \Rightarrow xvy \in L$. ☐

Теорема 4.0.1 (Саймон). *Пусть Σ – конечный алфавит. Регулярный язык L над алфавитом Σ кусочно тестируем тогда и только тогда, когда конгруэнция $\sim_L$ на Σ^* $\mathscr{J}$-тривиальна.*

Сначала изложим классическое доказательство Саймона. Оно основано на ряде предложений из комбинаторики слов, которые представляют и самостоятельный интерес.

Предложение 4.0.1. *Пусть $a \in \Sigma$, $u, v \in \Sigma^*$. Если $uav \sim_{2n-1} uv$, то либо $ua \sim_n u$, либо $av \sim_n v$.*

Доказательство. Пусть $ua \nsim_n u$ и $av \nsim_n v$. Тогда в ua есть подслово xa длины $\leq n$, которого нет в u, и аналогично, в av есть подслово ay длины $\leq n$, которого нет в v. Рассмотрим xay, его длина $\leq 2n-1$. Оно есть в uav, но его нет в uv. Противоречие. ☐

Обозначим через $c(w)$ содержание слова w, т.е. множество букв слова w.

Предложение 4.0.2. *Пусть $uv \in \Sigma^*$ и $n > 0$. Тогда $u \sim_n vu$ в том и только в том случае, когда найдутся такие слова $u_1, \dots, u_n \in \Sigma^*$, что $u = u_1 \dots u_n$ и $c(v) \subseteq c(u_1) \subseteq c(u_2) \subseteq \dots \subseteq c(u_n)$.*

Доказательство. Необходимость. Индукция по n. База индукции. $n = 1$. Если $u \sim_1 vu$, то $c(v) \subseteq c(u)$ и $u_1 = u$.

Шаг индукции. Пусть $u \sim_{n+1} vu$. Обозначим через u_{n+1} наикратчайший суффикс слова u такой, что $c(u_{n+1}) = c(u)$. Если записать $u_{n+1} = au'$, где $a \in \Sigma$, то ясно по построению, что a не встречается в u'. Если w таково, что $u = wu_{n+1}$, то для доказательства достаточно доказать, что $w \sim_n vw$, так как тогда к слову w можно будет применить предположение индукции. Пусть x – какое-то подслово длины $\leq n$ в vw. Тогда xa подслово длины $\leq n+1$ в $vu = vwau'$. Из условия $u \sim_{n+1} vu$ следует, что xa есть подслово в u, но $u = wau'$ и a не появляется в u'. Поэтому x является подсловом в w.

Достаточность. База индукции. $u = u_1$ и $c(v) \subseteq c(u_1)$. Тогда понятно, что $c(vu) = c(u)$, т.е. $vu \sim_1 u$.

Шаг индукции. Допустим, что $u = u_1 \dots u_{n+1}$ и при этом $c(v) \subseteq c(u_1) \subseteq c(u_2) \subseteq \dots \subseteq c(u_{n+1})$. Надо доказать, что тогда $u \sim_{n+1} vu$. По предположению индукции $u_1 u_2 \dots u_n \sim_n vu_1 u_2 \dots u_n$. Теперь возьмем произвольное подслово x длины $\leq n+1$ в слове vu. Обозначим через x' наидлиннейший суффикс слова x, который является подсловом в u_{n+1} и пусть $x = x''x'$. Поскольку $c(u_{n+1}) = c(vu)$, по крайней мере последняя буква слова x попадает в x'. Тогда x'' имеет длину $\leq n$ и является подсловом в $vu_1 \dots u_n$. По предположению индукции x'' является подсловом в $u_1 \dots u_n$. А тогда x является подсловом в $u_1 \dots u_{n+1} = u$. □

Следствие 4.0.1. *Для любых слов $u, v \in \Sigma^*$ имеем $(uv)^n \sim_n v(uv)^n \sim_n (uv)^n u$.*

Доказательство. Достаточно представить $(uv)^n$ как $\underbrace{(uv)(uv)\dots(uv)}_{n\,\text{раз}}$. □

Раз $\sim_n$ – конгруэнция конечного индекса, то $\Sigma^*/\sim_n$ – конечный моноид. Из следствия вытекает, что это $\mathscr{J}$-тривиальный моноид. Допустим, что $\bar{a}\mathscr{R}\bar{b}$ (через $\bar{a}$ обозначаем образ слова a в $\Sigma^*/\sim_n$), $\bar{a} = \bar{b}p$ и $\bar{b} = \bar{a}q$. Тогда $\bar{a} = \bar{a}qp = \bar{a}(qp)^n$. Пусть $q = \bar{u}$, $p = \bar{v}$, имеем

$$(\bar{u}\bar{v})^n = \overline{(uv)^n} = \overline{(uv)^n u} = (\bar{u}\bar{v})^n \bar{u} = (qp)^n q.$$

Значит, $\bar{a}(qp)^n = \bar{a}(qp)^n q = \bar{a}q = \bar{b}$.

Аналогично, если $\bar{a}\mathscr{L}\bar{b}$, то $\bar{a} = \bar{b}$.

Итак, необходимость в теореме Саймона доказана.

Предложение 4.0.3. *Если $f \sim_n g$, то существует такое h, что $f \sim_n h \sim_n g$ и f, g являются подсловами в h.*

Доказательство. $f \wedge g$ – наидлиннейшая приставка слов f и g.

Индукция по $k = |f| + |g| + 2|f \wedge g|$.

База индукции: $k = 0$ очевидно, так как в этом случае $f = g$.

Можно считать, что ни одно из слов f и g не является подсловом в другом. Тогда можно записать f и g в таком виде: $f = uav$, $g = ubw$, где $u = f \wedge g$ (самая длинная общая приставка), а $a \neq b$ буквы. Хотим доказать что либо $ubw \sim_n ubav$, либо $uav \sim_n uabv$.

Докажем от противного: раз $ubw = g \sim_n f$, а f является подсловом в $ubav$, значит, есть такое слово r длины не более чем n, которое наличествует в $ubav$, но отсутствует в ubw.

Аналогично, есть слово s длины не более чем n, которое есть в $uabw$, но отсутствует в ubv.

Ясно, что выделенное вхождение $ubav$ буквы b входит в r, а выделенное вхождение a в $uabw$ входит в слово s.

Слово g: $\overbrace{\qquad\qquad}^{u}\overbrace{\quad}^{b}\overbrace{\qquad\qquad}^{w}$

r: $\overbrace{\qquad}^{r_1}\overbrace{\quad}^{b}\overbrace{\qquad}^{r_2}$

$ubav$: $\overbrace{\qquad\qquad}^{u}\overbrace{\quad}^{b}\overbrace{\quad}^{a}\overbrace{\qquad}^{v}$

Слово f: $\overbrace{\qquad\qquad}^{u}\overbrace{\quad}^{a}\overbrace{\qquad\qquad}^{v}$

s: $\overbrace{\qquad}^{s_1}\overbrace{\quad}^{a}\overbrace{\quad}^{s_2}$

$uabv$: $\overbrace{\qquad\qquad}^{u}\overbrace{\quad}^{a}\overbrace{\quad}^{b}\overbrace{\qquad}^{w}$

Более точно: $r = r_1br_2$, где r_1 - подслово в u, а r_2 подслово в av.
А $s = s_1as_2$, где s_1 - подслово в u, а s_2 подслово в bw.

Тогда r_1b - не подслово в u, и аналогично, s_1a - не подслово в u.

Запишем r_2 как $r_2 = {r_2}''{r_2}'$, где ${r_2}'' = 1$ или a, а ${r_2}'$ - подслово в v.
Аналогично, $s_2 = {s_2}''{s_2}'$, где ${s_2}'' = 1$ или a, а ${s_2}'$ - подслово в w.
$\left|r_1b{s_2}'\right| + \left|s_1a{r_2}'\right| \leq |r_1br_2| + |s_1as_2| = |r| + |s| \leq 2n$,значит, одно из этих слов имеет длину не больше чем n.

Пусть слово $\left|r_1b{s_2}'\right| \leq n$. Это подслово в $ubw = g$, а значит, оно является подсловом в f.

$\overbrace{\qquad}^{r_1}\overbrace{\quad}^{b}\overbrace{\quad}^{{s_2}'}$

$\overbrace{\qquad\qquad}^{u}\overbrace{\quad}^{a}\overbrace{\qquad}^{w}$

Отсюда $b{s_2}'$ - подслово в v, т.е. s_2 - подслово в v. Но тогда s_1as_2 - подслово f, а это не так по выбору, т.е. получили противоречие.

Итак, доказали что либо $ubw \sim_n ubav$, либо $uav \sim_n uabw$.

Пусть, для определенности, $f = uav \sim_n uabw$. Тогда считаем: $|uav| + |uabw| - 2(|uav \wedge uabw| + 1) \leq |f| + |g+1| - 2(|f \wedge g| + 1) = \underbrace{|f| + |g| - 2\,|f \wedge g|}_{k} - 1 < k$

По предположению индукции, существует слово h такое, что $h \sim_n f$ и $h \sim_n uabw$ и содержит f и $uabv$ в качестве подслова.

Но g есть подслово в $uabw$, а значит, g есть подслово в h. □

Теперь мы готовы к доказательству достаточности в теореме Саймона.

Пусть L распознается некоторым $\mathscr{J}$-тривиальным моноидом M, т.е. существует гомоморфизм $\varphi\colon \Sigma^* \to M$ такой, что $L = L\varphi\varphi^{-1}$. Обозначим через $\overline{f}$ образ элемента f языка L при этом гомоморфизме.

На M отношение $\leq_{\mathscr{J}}$ является порядком в силу $\mathscr{J}$-тривиальности M. Пусть n – длина максимальной цепи в этом моноиде. Покажем, что L есть объединение классов относительно $\sim_{2n-1}$. Для этого достаточно доказать, что если $f \sim_{2n-1} g$, то $\overline{f} = \overline{g}$. По предложению 4.0.3 можно считать, что f – подслово в g. Поскольку $f \sim_{2n-1} g$, то g получается из f вставкой букв, которые не дают новых подслов длины не более $2n-1$, причем на каждом шаге вставка букв не меняет отношение $f \sim_{2n-1} g$, следовательно можно считать, что g получается из f вставкой всего одной буквы. Значит $f = uv$, $g = uav$ для некоторых $u, v \in \Sigma^*$, $a \in \Sigma$ и мы находимся в условиях предложения 4.0.1, тогда будем считать, что выполняется $av \sim_n v$. По предложению 4.0.2 $v = v_1 v_2 \dots v_n$, $c(a) = \{a\} \subseteq c(v_1) \subseteq c(v_2) \subseteq \dots \subseteq c(v_n)$. Рассмотрим последовательность

$$1,\ v_n,\ v_{n-1}v_n,\ \dots\ , v_1 v_2 \dots v_n,$$

тогда

$$\overline{1} \geq_{\mathscr{J}} \overline{v_n} \geq_{\mathscr{J}} \overline{v_{n-1}v_n} \geq_{\mathscr{J}} \dots \geq_{\mathscr{J}} \overline{v_1 \dots v_n}.$$

По выбору n в этой цепи есть 2 одинаковых элемента (поскольку ее длина равна $n+1$), т.е найдутся i, j такие что $\overline{v_i \dots v_j \dots v_n} = \overline{v_j \dots v_n} = s$. Пусть $b \in c(v_i)$. Тогда $v_i = v_i' b v_i''$ и

$$s = \overline{v_i \dots v_n} \leq_{\mathscr{J}} \overline{b v_i'' \dots v_n} \leq_{\mathscr{J}} \overline{v_i'' \dots v_n} \leq_{\mathscr{J}} \overline{v_j \dots v_n} = s.$$

Значит, все элементы в этой цепочке неравенств равны s, $\Rightarrow \overline{b}s = s$. Среди букв b встречается и $a, \Rightarrow \overline{a}s = s \Rightarrow \overline{av} = \overline{av_1 \dots v_n} = \overline{v_1 \dots v_n} = \overline{v}$, откуда $\overline{g} = \overline{uav} = \overline{uav} = \overline{uv} = \overline{uv} = \overline{f}$. □

4.0.1 Доказательство Климы

Доказательство. Необходимость. Пусть язык L кусочно тестируем. По лемме 4.0.1 это означает, что $\sim_k \subseteq \sim_L$ для некоторого k. Рассмотрим слова $u, w_1, w_2, w_3, w_4 \in \Sigma^*$ такие, что $w_1 w_2 u w_3 w_4 \sim_L u$. Поскольку $\sim_L$ – конгруэнция на Σ^*, выполняется

$$(w_1 w_2)^2 u (w_3 w_4)^2 \sim_L w_1 w_2 u w_3 w_4 \sim_L u.$$

Обозначим $u_n = (w_1w_2)^n u(w_3w_4)^n$. Индукцией по n легко доказать, что $u_n \sim_L u$ для любого натурального n. Ясно, что $u \trianglelefteq u_1 \trianglelefteq u_2 \trianglelefteq \dots$, следовательно, $\mathsf{Sub}_k(u) \subseteq \mathsf{Sub}_k(u_1) \subseteq \mathsf{Sub}_k(u_2) \subseteq \dots$. Поскольку существует лишь конечное число различных множеств вида $\mathsf{Sub}_k(v)$, $v \in \Sigma^*$, мы видим, что $\mathsf{Sub}_k(u_n) = \mathsf{Sub}_k(u_{n'})$ для некоторых $n < n'$. Тогда включения $\mathsf{Sub}_k(u_n) \subseteq \mathsf{Sub}_k(w_2u_nw_3) \subseteq \mathsf{Sub}_k(u_{n'})$ превращаются в равенства. Таким образом, $\mathsf{Sub}_k(u_n) = \mathsf{Sub}_k(w_2u_nw_3)$, а это означает, что $u_n \sim_k w_2uw_3$. Поскольку $u_n \sim_L u$ и $\sim_k \subseteq \sim L$, получаем, что $u \sim_L w_2uw_3$. Следовательно, по упражнению 4.0.1 конгруэнция $\sim_L$ $\mathscr{J}$-тривиальна.

Достаточность. Предположим, что регулярный язык $L \subseteq \Sigma^*$ таков, что конгруэнция $\sim_L$ $\mathscr{J}$-тривиальна. Пусть m – индекс этой конгруэнции. Мы докажем, что $\sim_k \subseteq \sim_L$ для $k = 2m-2$.

Рассмотрим слова $u = a_1a_2\cdots a_p$ и $v = b_1b_2\cdots b_q$, где $p,q \geq 0$, $a_1, a_2, \dots, a_p$, $b_1, b_2, \dots, b_q \in \Sigma$, такие, что $u \sim_k v$. Через u_i обозначим префикс слова u длины i, а именно $u_i = a_1a_2\cdots a_i$ для каждого $i = 0, 1, \dots, p$ (отметим, что $u_0 = 1$). Из $\mathscr{J}$-тривиальности конгруэнции $\sim_L$ мы получаем, что условие $u_i \sim_L u_j$ для некоторых $i < j$ влечет $u_i \sim_L u_{i'}$ для всех $i' = i, i+1, \dots, j$. Назовем индекс $i \in \{1, \dots, p\}$ *синим* в слове u, если $u_{i-1} \nsim_L u_{i-1}a_i$. Поскольку число классов в разбиении $\Sigma^*/\sim_L$ равно m, существует не более $m-1$ синего индекса $i_1 < i_2 < \dots < i_r$ в u, $r \leq m-1$. Для несинего индекса i выполняется $u_{i-1} \sim_L u_{i-1}a_i$. Таким образом, для синего индекса i_t и произвольного индекса $i \in \{i_t+1, \dots, i_{t+1}-1\}$ мы имеем

$$u_{i_t} \sim_L u_{i_t}a_{i_t+1} \sim_L \cdots \sim_L u_{i_t}a_{i_t+1}\cdots a_{i-2} \sim_L u_{i-1} \sim_L u_i.$$

Поскольку $\sim_L$ – конгруэнция и $u_{i_t} \sim_L u_{i-1}$, мы получаем $u_{i_t}a_i \sim_L u_i \sim_L u_{i_t}$. Таким образом, мы можем сделать следующее наблюдение.

Факт 1: Пусть u' – подслово слова u, содержащее все вхождения букв на синих позициях (и, возможно, на других). Тогда $u' \sim_L a_{i_1}a_{i_2}\cdots a_{i_r} \sim_L u$.

Заметим кроме того, что синими индексами помечено самое левое вхождение слова $u_{\mathsf{left}} = a_{i_1}a_{i_2}\cdots a_{i_r}$ как подслова в слово u, т.е. для любого $r' \leq r$ слово $a_{i_1}a_{i_2}\cdots a_{i_{r'}}$ не является подсловом слова $u_{i_{r'}-1}$. Поскольку $u \sim_k v$, то мы можем рассмотреть самое левое вхождение слова u_{left} в слово v. Соответствующие индексы из множества $\{1, 2, \dots, q\}$ обозначим через $\bar{i}_1 < \bar{i}_2 < \cdots < \bar{i}_r$ и назовем синими индексами в слове v.

Применим теперь двойственную конструкцию к слову v. Рассмотрим *красные* индексы j в слове v, т.е. такие индексы, что $b_jv_{j+1} \nsim v_{j+1}$, где v_{j+1} – суффикс слова v, начинающийся после j-й буквы. Для красных индексов $j_1 < j_2 < \cdots < j_s$, $s \leq m-1$, справедливо двойственное свойство, т.е. эти индексы определяют самое правое вхождение слова $u_{\mathsf{right}} = b_{j_1}b_{j_2}\cdots b_{j_s}$ в слово v. Мы будем рассматривать также самое правое вхождение слова u_{right} в слово u и обозначать соответствующие красные индексы через $\bar{j}_1 < \bar{j}_2 < \cdots < \bar{j}_s$.

Теперь мы сделаем главный шаг и докажем, что буквы слов u_{left} и u_{right} чередуются в слове u в том же порядке, что и в слове v.

Факт 2: Пусть $\bar{u}$ – подслово слова u, полученное из букв, стоящих на синих и красных позициях в u, а слово $\bar{v}$ – полученное аналогичным образом подслово слова v. Тогда $\bar{u} = \bar{v}$.

Доказательство. Рассмотрим вхождение буквы a_{i_k} на синей позиции i_k и вхождение буквы b_{j_ℓ} на красной позиции $\bar{j}_\ell$ в слове u. Предположим сначала, что это разные буквы, т.е. $a_{i_k} \neq b_{j_\ell}$. В этом случае $i_k < \bar{j}_\ell$ тогда и только тогда, когда слово

$$w_{k\ell} = a_{i_1} \cdots a_{i_k} b_{j_\ell} \cdots b_{j_s} = a_{i_1} \cdots a_{i_k} a_{\bar{j}_\ell} \cdots a_{\bar{j}_s}$$

является подсловом слова u. Прямая импликация очевидна. Для доказательства обратной импликации допустим, что $w_{k\ell} \trianglelefteq u$. Пусть $h_1 < h_2 < \cdots < h_k < h'_\ell < \cdots < h'_s$ – соответствующие индексы, т.е. $w_{k\ell} = a_{h_1} \cdots a_{h_k} a_{h'_\ell} \cdots a_{h'_s}$. Поскольку синие индексы $i_1, \ldots, i_r$ задают самое левое вхождение слова $u_{textsfleft}$ в слово u, то индукцией по $t = 1, \ldots, k$ можно доказать, что $i_t \leq h_t$. Симметрично, для $t = \ell, \ldots, s$ получаем $h'_t \leq \bar{j}_t$. Следовательно, $i_k \leq h_k < h'_\ell \leq \bar{j}_\ell$.

Теперь рассмотрим случай, когда $a_{i_k} = b_{j_\ell}$.

(1) Если $w_{k\ell} \trianglelefteq u$, то $i_k < \bar{j}_\ell$, и обратно;

(2) если $w_{k\ell} \ntrianglelefteq u$, но $w'_{k\ell} = a_{i_1} \cdots a_{i_k} b_{j_\ell + 1} \cdots b_{j_s} \trianglelefteq u$, то $i_k = \bar{j}_\ell$, т.е. рассматриваемый индекс является синим и красным одновременно;

(3) если слово $w'_{k\ell} \ntrianglelefteq u$, то $\bar{j}_\ell < i_k$.

Таким образом, в любом случае взаимное расположение рассматриваемых синего и красного индексов определяется подсловами слова u длины не более k, поскольку $|w'_{k\ell}|, |w_{k\ell}| \leq |u_{\mathsf{left}} u_{\mathsf{right}}| \leq 2m - 2 = k$. Итак, утверждение факта 2 следует из условия $u \sim_k v$.

В итоге мы доказали, что $\bar{u} = \bar{v}$, и $\bar{u} \sim_L u$. Аналогично $\bar{v} \sim_L v$, следовательно, $u \sim_L \bar{u} = \bar{v} \sim_L v$.

□

Литература

[1] Н. Бурбаки. Очерки по истории математики. М.: Мир., 1965.

[2] Е. Вигнер. Непостижимая эффективность математики в естественных науках. Успехи физических наук. 1968. Т.94, №3. С.535–546.

[3] Э. Хилле. Функциональный анализ и полугруппы. М.: Изд. иностранной литературы, 1951.

Предметный указатель

Именной указатель