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 содержит их объединение и их произведение.

Мы будем считать известным задание рациональных языков *регулярными выражениями* и будем пользоваться такими заданиями.

1.2 Беззвездные языки

Среди операций, используемых в определении рациональных языков, итерация является наиболее «сложной», так 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 более 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;

[1] M. P. Schützenberger

- не содержат двух вхождений буквы b подряд.

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 называется *кусочно тестируемым*, если он является булевой комбинацией 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.)

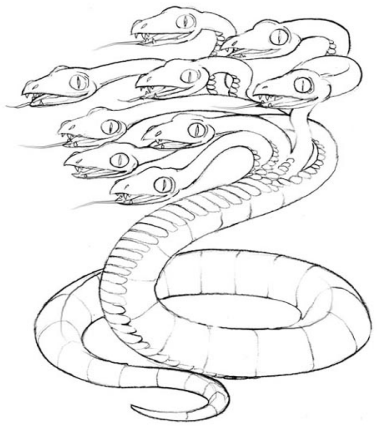

Рис. 1.1: Девятиглавая гидра

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;

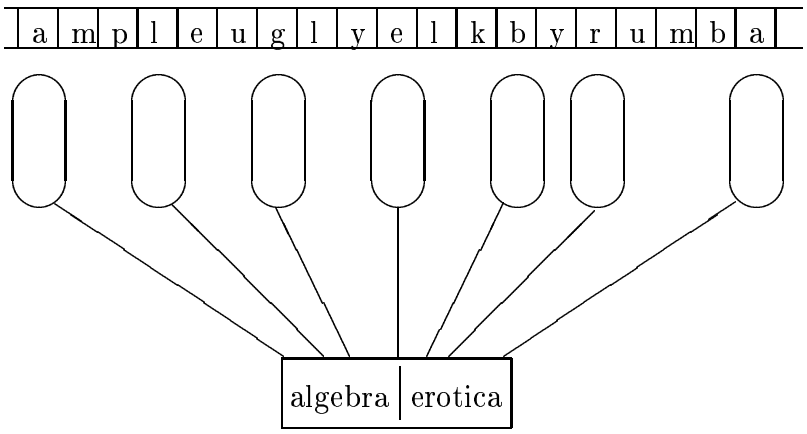

Рис. 1.2: Автомат-гидра с семью головками

- конечной read-only памяти, которая содержит два списка слов длины $\leq h$ над Σ: список паролей и список запретов.

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 $\mathscr{H}$, если $\mathscr{H}$ 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 (I. Simon).

Глава 2

Необходимые сведения из теории полугрупп

2.1 Отношения Грина

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

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 2.1.1. *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 2.1.1. *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 2.1.2. $\mathscr{L}\mathscr{R} = \mathscr{R}\mathscr{L}$ *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:

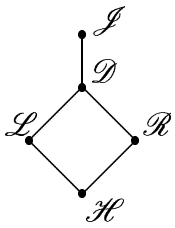

Рис. 2.1: Включения между отношениями Грина

2.2 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 2.2.1. *Для любых $\alpha, \beta \in T_X$ имеем:*

1. $\alpha \leq_{\mathscr{L}} \beta \iff \operatorname{Im}\alpha \subseteq \operatorname{Im}\beta$;
2. $\alpha \leq_{\mathscr{R}} \beta \iff \ker\alpha \supseteq \ker\beta$;
3. $\alpha \leq_{\mathscr{J}} \beta \iff |\operatorname{Im}\alpha| \leq |\operatorname{Im}\beta|$.

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 разные элементы. Поскольку $|\ker\alpha| = |\operatorname{Im}\alpha| \leq |\operatorname{Im}\beta|$, 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 $\varepsilon \leq_{\mathscr{L}} \beta$. Отсюда $\alpha \leq_{\mathscr{D}} \beta$ и потому $\alpha \leq_{\mathscr{J}} \beta$. □

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

Следствие 2.2.1. *Для любых $\alpha, \beta \in T_X$ имеем:*

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

2.3 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 2.3.1. *Пусть L – $\mathscr{L}$-класс, R – $\mathscr{R}$-класс. Тогда $R \cap L \neq \varnothing$ 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 $L \cap R \neq \varnothing$. □

Лемма 2.3.1 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.

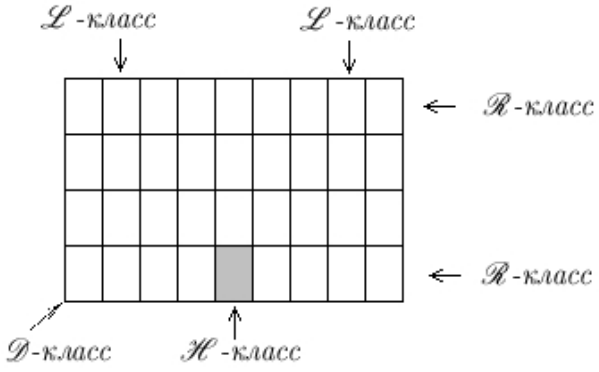

Рис. 2.2: egg-box картинка

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

Предложение 2.3.1 (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.*

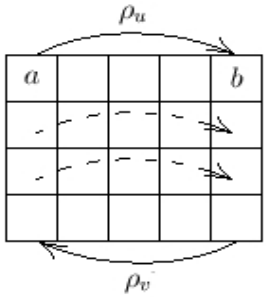

Рис. 2.3: Иллюстрация к лемме Грина

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 $x \mathscr{H} y$ □

В качестве примера рассмотрим $\mathscr{D}$-строение моноида T_3 всех преобразований 3-элементного множества $\{1, 2, 3\}$. Согласно доказанному в §2.2, 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 преобразований. Интереснее всего устроен класс D_2. Его egg-box картинка показана ниже.

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

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.

2.4 Роль идемпотентов

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

Лемма 2.4.1. *В конечной полугруппе для любого элемента, найдется его степень, которая является идемпотентом.*

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

Упражнение 2.4.1. *Для данного элемента полугруппы найти наименьшую степень, в которой он является идемпотентом.*

Упражнение 2.4.2. *Пусть полугруппа S имеет порядок n. Доказать, что для любого $a \in S$ элемент $a^{n!}$ является идемпотентом.*

Предложение 2.4.1. *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 2.4.2 (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.*

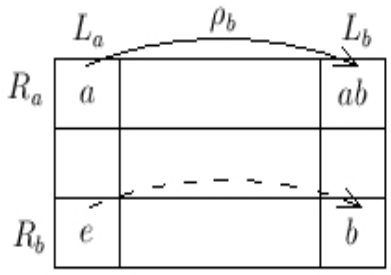

Рис. 2.4: Иллюстрация к теореме Миллера–Клиффорда

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 2.4.1. *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 2.4.3. *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 2.4.4. *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 2.4.2. *$\mathscr{R}$-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. □