Math-Net.Ru

Общероссийский математический портал

В. Г. Смирнов, Слои и циклические факторы конечных полугрупп, *Матем. вопр. криптогр.*, 2011, том 2, выпуск 4, 75–95

DOI: <https://doi.org/10.4213/mvk44>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.224.135.184

26 апреля 2023 г., 13:00:24

УДК 512.531.2

Слои и циклические факторы конечных полугрупп

В. Г. Смирнов

Академия криптографии Российской Федерации, Москва

Получено 23.VI.2010

Получены оценки периода и циклической глубины конечной полугруппы относительно фиксированного порождающего множества, а также условия принадлежности элементов полугруппы её слоям. Изучаются такие конгруэнции на полугруппе, фактор по которым является циклической группой. Результаты могут использоваться при анализе полугрупп конечных автоматов.

Ключевые слова: слой, оболочка, циклический фактор, графы Кэли конечной полугруппы

Layers and cyclic factors of finite semigroups

V. G. Smirnov

Academy of Cryptography of Russian Federation, Moscow

Abstract. Estimates of the period and cyclic depth of a finite semigroup with respect to a fixed generating set are obtained as well as conditions for the semigroup elements to belong to semigroup layers. We investigate congruences on semigroups such that factor with respect to them is a cyclic group. Results may be used for the analysis of finite automata.

Key words: layer, hull, cyclic factor, Cayley graph of finite semigroup

Citation: *Mathematical Aspects of Cryptography*, 2011, vol. 2, no. 4, pp. 75–95 (Russian).

© 2011 В. Г. Смирнов

§ 1. Введение

1.1. Исходные определения. В процессе анализа многих современных шифрсистем возникает необходимость в изучении и использовании алгебраических свойств полугруппы, порождаемой совокупностью частичных функций переходов шифрующего автомата. Регулярному случаю, когда исследуемая полугруппа является группой, посвящены многочисленные исследования (см., например, [1], где определены понятия слоя, глубины и ширины покрытия группы и исследованы их свойства). Менее изучен нерегулярный случай, который также интересен, так как встречается в практике анализа.

В [2] введены в рассмотрение и исследованы слои конечного автомата. Полученные в [2] результаты здесь развиваются и переносятся на конечные полугруппы.

Далее рассматривается конечная полугруппа с множеством элементов S и операцией « $\cdot$ ». Пусть $Q \subseteq S$ — некоторое фиксированное порождающее множество элементов этой полугруппы. Для полугруппы S с фиксированным порождающим множеством Q будем использовать обозначение (S, Q) .

Обозначим через $Q_r^+ = (Q^+, \circ_r)$ свободную полугруппу на множестве Q .

Элементами этой полугруппы являются конечные последовательности символов множества Q , называемых словами в алфавите Q . Операцией полугруппы Q_r^+ является правая конкатенация слов, при которой $w_1 \circ_r w_2 = w_1 w_2$, где $w_1, w_2 \in Q^+$, а слово $w_1 w_2$ получается приписыванием к слову w_1 справа слова w_2 .

Известно [3], что существует единственный гомоморфизм φ полугруппы Q_r^+ на полугруппу S , для которого $\varphi(q) = q$ при всех $q \in Q$. Если $a = q_1 \dots q_k$ — слово в алфавите Q и $q_1 \dots q_k = u$, то $\varphi(a) = u$. Будем говорить в этом случае, что слово a в алфавите Q является записью длины k элемента $u \in S$. Таким образом, $\varphi^{-1}(u)$ есть множество всех записей элемента u в алфавите Q .

Обозначим через T полугруппу с операцией « $\cdot$ », антиизоморфную полугруппе S . Множества элементов полугрупп S и T совпадают, для элементов $u, v \in S$ в полугруппе T имеем $u \cdot v = v \cdot u$, а множество Q , порождающее полугруппу S , порождает и полугруппу T .

Двойственным образом, существует единственный гомоморфизм ψ свободной полугруппы $Q_l^+ = (Q^+, \circ_l)$ с операцией левой конкатенации на полугруппу T , такой, что $\psi(q) = q$ для всех $q \in Q$. Для слова $a = q_1 \dots q_k \in Q_l^+$, где $q_k \dots q_1 = u$, имеем $\psi(a) = u$, и слово a является записью длины k в алфавите Q элемента $u \in T$.

Через « $\bullet$ » обозначим операцию полугруппы $T \times S$, являющейся прямым произведением полугрупп T, S . Для $(u, v), (w, x) \in T \times S$ имеем

$$(u, v) \bullet (w, x) = (w \cdot u, v \cdot x).$$

1.2. Сведения из теории полугрупп [3], [4], [5], [6]. Полугруппа S , содержащая единицу, называется моноидом. Обычно используется обозначение S^1 для полугруппы, которая совпадает с S , если S — моноид, и получается присоединением к полугруппе единицы $1 \notin S$ в противном случае.

Множество $D(u) = S^1 \cdot u \cdot S^1$ называют главным идеалом полугруппы S , порождённым элементом u . Множества $L(u) = S^1 \cdot u$, $R(u) = u \cdot S^1$ называют соответственно главным левым и главным правым идеалами полугруппы S , порождёнными элементом u .

D -классом (R -классом, L -классом) полугруппы S , содержащим элемент t , называют подмножество D_t (R_t , L_t) всех её элементов, порождающих тот же, что и t , главный (главный правый, главный левый) идеал. Наконец, H -класс полугруппы состоит из всех её элементов, порождающих одинаковые главный, а также главные левый и правый идеалы.

Каждый D -класс является объединением R -классов (L -классов), а каждый R -класс (L -класс) является объединением H -классов. Для всех элементов $t \in S$ имеет место равенство $|D_t| = |R_t| \cdot |L_t|$; H -классы, принадлежащие одному D -классу, равномощны.

Разбиения множества элементов полугруппы на указанные классы задают на ней соответствующие отношения эквивалентности. Элементы t, u полугруппы S являются D -эквивалентными (R -, L -, H -эквивалентными), если они принадлежат одному D -классу (R -, L -, H -классу соответственно). В этом случае пишут $t \sim_D u$ ($t \sim_R u, t \sim_L u, t \sim_H u$ соответственно). Отношение $\sim_D$ является конгруэнцией на конечной полугруппе S , отношения $\sim_R$ и $\sim_L$ — правой и левой конгруэнциями соответственно.

На множестве D -классов, естественно, вводится частичная упорядоченность $\leq_D$, при которой $D_i \leq_D D_u$ тогда и только тогда, когда $S^1 \cdot t \cdot S^1 \subseteq S^1 \cdot u \cdot S^1$. В случае строгого включения пишут $D_i <_D D_u$. Частично упорядоченное множество D -классов конечной полугруппы имеет минимальный элемент, который совпадает с её минимальным идеалом и называется *ядром* полугруппы. Для ядра полугруппы S примем обозначение $K(S)$.

В конечной полугруппе некоторая степень любого её элемента a является *идемпотентом* [4], и такой идемпотент — единственный. Обозначим этот идемпотент через e_a . Говорят, что элемент a принадлежит идемпотенту e_a . Если H -класс содержит идемпотент, то он является группой. Множество всех идемпотентов полугруппы обозначим $E(S)$.

Регулярным называется D -класс полугруппы, содержащий хотя бы один идемпотент. В этом случае каждый R -класс (L -класс), входящий в D -класс, также содержит хотя бы один идемпотент. Элементы регулярных D -классов называются *регулярными*. Множество регулярных элементов полугруппы обозначим $\text{Reg}(S)$.

Полугруппа S называется *регулярной*, если $S = \text{Reg}(S)$.

1.3. Краткое изложение содержания статьи. В § 2 даются определения слоёв и оболочки конечной полугруппы (S, Q) , её циклической глубины и периода относительно заданного порождающего множества. Исследовано строение оболочки полугруппы (теорема 1). Дается нижняя оценка циклической глубины полугруппы (теорема 2).

В § 3 определяются цикловые элементы полугруппы, вводятся модуль однозначности и цикловой индекс элемента полугруппы (S, Q) . Описаны основные свойства введенных параметров (теоремы 3, 4, 5). Получено выражение периода полугруппы через цикловые индексы максимальных регулярных D -классов (теорема 6). Найдены необходимые условия принадлежности элементов полугруппы (S, Q) её слоям, являющиеся необходимыми и достаточными для регулярных полугрупп (теорема 7).

В § 4 вводятся левый, правый и двусторонний графы Кэли полугруппы (S, Q) . Определяются левый и правый цикловые классы и цикловые индексы и рассматриваются соотношения между ними (леммы 5, 6, 7). Показано, что левый и правый цикловые индексы могут различаться только у нерегулярных элементов полугруппы (теорема 8).

В § 5 приведен ряд примеров, иллюстрирующих возможные соотношения между введенными в §§ 3, 4 параметрами.

В § 6 получены условия существования циклических факторов конечной полугруппы (теоремы 9, 10).

§ 2. Слой и оболочка полугруппы

2.1. Слои полугруппы. Очевидно, что множество всех подмножеств конечной полугруппы $S = (S, Q)$ относительно операции умножения подмножеств является полугруппой [5]. В этой полугруппе множество Q порождает циклическую подполугруппу, состоящую из элементов

$$Q, Q^2, \dots, Q^{\rho(Q)}, \dots, Q^{\rho(Q)+\omega(Q)-1}, \quad (1)$$

где $Q^{\rho(Q)} = Q^{\rho(Q)+\omega(Q)}$ — первое повторение в последовательности степеней множества Q . Таким образом, $(S, Q) = \bigcup_{i=1}^{\rho(Q)+\omega(Q)-1} Q^i$.

По аналогии с [1] введём некоторые понятия, связанные с фиксированным порождающим множеством полугруппы.

Определение 1. Множество Q^k , $k = 1, \dots, \rho(Q) + \omega(Q) - 1$, элементов полугруппы (S, Q) назовём её k -м слоем, число $\rho(Q)$ — циклической глубиной полугруппы (S, Q) , число $\omega(Q)$ — периодом полугруппы (S, Q) .

ЗАМЕЧАНИЕ 1. Термины «циклическая глубина» и «период» общеприняты для циклических полугрупп [3].

Из определения умножения подмножеств вытекает, что слой Q^k состоит из всех элементов полугруппы, записываемых хотя бы одним способом словом длины k в алфавите Q .

В случае $1 \notin S$ полагаем, что для полугруппы S^1 порождающим является множество $Q^1 = Q \cup 1$, но при этом длина записи элемента 1 принимается равной 0.

2.2. Оболочка полугруппы. В отличие от группы, в полугруппе S могут быть элементы, для которых существует лишь конечное число записей словами в алфавите Q . Это элементы, принадлежащие множеству

$$W(S) = S \setminus \left(\bigcup_{k=\rho(Q)}^{\rho(Q)+\omega(Q)-1} Q^k \right),$$

если только оно не пусто. Можно сказать, что множество $W(S)$ состоит из элементов полугруппы S , длина любой записи которых в алфавите Q строго меньше циклической глубины $\rho(Q)$.

Определение 2. Множество $W(S)$ назовём оболочкой полугруппы S .

Лемма 1. Если $t \in W(S)$, то $|D_t| = 1$.

Доказательство. Пусть $t \in S$ и $|D_t| > 1$, т. е. существует элемент $u \neq t$, $u \in D_t$. Из определения D -класса следует существование таких элементов $v, w, x, y \in S^1$, что $u = v \cdot t \cdot w$, $t = x \cdot u \cdot y$ и при этом $v \cdot w \in S$, $x \cdot y \in S$. Отсюда

$$t = (x \cdot v)^n \cdot t \cdot (w \cdot y)^n \quad (2)$$

для произвольного целого положительного n , причём $v \cdot w \cdot x \cdot y \in S$. Следовательно, при любом выборе порождающего множества Q существуют записи элемента t длины большей, чем $\rho(Q) - 1$, т. е. $t \notin W(S)$. Лемма доказана.

Теорема 1. Оболочка полугруппы совпадает с объединением её D -классов D_b , $t \in S$, удовлетворяющих условию: не существует такого регулярного D -класса D_e , что $D_t \leq_D D_e$.

Доказательство. Обозначим через W объединение D -классов, удовлетворяющих условию теоремы. Если существует такой идемпотент $e \in E(S)$, что $D_t \leq_D D_e$, то найдутся такие элементы $u, v \in S^1$, $u \cdot v \in S$, что $t = u \cdot e^n \cdot v$ для любого n , следовательно, $t \notin W(S)$, поэтому $W(S) \subseteq W$. Необходимость утверждения теоремы доказана.

Перейдём к доказательству его достаточности. Пусть $|D_t| > 1$. Не теряя общности, положим в соотношении (2) $x \cdot y \in S$ и выберем число n так, что-

бы $(xy)^n = e_{xy}$. Очевидно, что $D_t \leq_D D_{e_{xy}}$, откуда $D_t \not\subseteq W$. Следовательно, если $D_t \subseteq W$, то необходимо $|D_t| = 1$. Зададим на множестве W частичный порядок, соответствующий частичной упорядоченности D -классов. Обозначим через $W^{(1)}$ множество максимальных элементов в W , через $W^{(2)}$ — множество максимальных элементов в $W \setminus W^{(1)}$ и т. д. На некотором шаге $r \geq 1$ получим, что множество

$$W^{(r)} = W \setminus \bigcup_{j=1}^{r-1} W^{(j)}$$

не пусто и не содержит сравнимых элементов. Окончательно,

$$W = \bigcup_{j=1}^r W^{(j)}.$$

Покажем, что элементы $t \in W^{(j)}$, $j = 1, \dots, r$, не имеют записей в алфавите Q длины, большей j . При $j = 1$ это верно, так как каждый элемент, принадлежащий $W^{(1)}$, образует один из максимальных D -классов полугруппы. Предположим, что $r > 1$, $j \geq 2$ и утверждение верно при $k \leq j - 1$. Пусть, далее, $t \in W^{(j)}$ и $t = q_{i_1} \cdot \dots \cdot q_{i_m}$, где $m > 1$. Положим $u = q_{i_1} \cdot \dots \cdot q_{i_{m-1}}$. Так как $u \geq t$, то $u \in W$. Если $u = t$, то $t = t \cdot q_{i_m} = t \cdot e_{q_{i_m}}$ и $t \notin W$. Итак, $u > t$ и, по предположению индукции, $m - 1 \leq j - 1$, откуда $m \leq j$. Такое рассуждение применимо к любой записи элемента t в алфавите Q . Следовательно, $W \subseteq W(S)$. Теорема доказана.

Обозначим через $r(S)$ длину максимального пути в частично упорядоченном множестве $W(S)$, если только $W(S) \neq \emptyset$. Если $W(S) = \emptyset$, то положим $r(S) = 0$. Параметр $r(S)$ назовём *глубиной оболочки полугруппы*.

Следующие два утверждения являются очевидными следствиями теоремы 1.

Следствие 1. *Оболочка полугруппы не зависит от выбора её порождающего множества.*

Действительно, согласно теореме 1 оболочка полностью определяется свойствами D -классов полугруппы.

Следствие 2. *Для каждого D -класса $D_t \subseteq S \setminus W(S)$ существует такой регулярный D -класс D_e , что $D_t \leq_D D_e$.*

В самом деле, если для D -класса D_t не существует такого D -класса D_e , что $D_t \leq_D D_e$, то по теореме 1 имеем $D_t \subseteq W(S)$.

Теорема 2. *Для циклической глубины полугруппы (S, Q) верна следующая оценка:*

$$\rho(Q) \geq r(S) + 1.$$

Доказательство. Если $r(S) = 0$, то утверждение тривиально. Пусть $r(S) > 0$, т. е. $W(S) \neq \emptyset$. Покажем по индукции, что каждый элемент $t \in W^{(j)}$,

$1 \leq j \leq r(S)$, имеет хотя бы одну запись длины i в любом алфавите Q . При $i = 1$ утверждение верно, так как очевидно, что $W^{(1)} \subseteq Q$. Предположим, что $r(S) > 1$, $2 \leq i \leq r(S)$, и при каждом $j < i$ любой элемент, принадлежащий множеству $W^{(j)}$, имеет хотя бы одну запись длины j в любом алфавите Q . Пусть $t \in W^{(i)}$. Тогда, по построению, найдётся хотя бы один элемент $u \in W^{(i-1)}$, $u > t$. Это означает, что найдутся такие элементы $v, w \in S^1$, $v \cdot w \in S$, что $t = v \cdot u \cdot w$. В ходе доказательства теоремы 1 было установлено, что элемент $t \in W^{(i)}$ не может иметь записей длины, большей j . Так как элемент u , по предположению индукции, имеет в любом алфавите запись длины $i-1$, то либо $v = 1$, $w \in Q$, либо $v \in Q$, $w = 1$, откуда следует, что элемент t в любом алфавите имеет запись длины i . Таким образом, $W^{(r)} \subseteq Q^r$, $W^{(r)} \cap Q^{r+1} = \emptyset$ и указанная в теореме оценка верна.

Отметим, что при $Q = S$ имеем $\alpha(S) = 1$, $\rho(Q) = r(S) + 1$. Следовательно, в рассматриваемом случае достигается верхняя граница указанной в теореме 2 оценки циклической глубины полугруппы.

§ 3. Модуль однозначности и цикловой индекс для элементов полугруппы

3.1. Модуль однозначности элемента полугруппы. Скажем, что множество Λ натуральных чисел при $|\Lambda| > 1$ принадлежит вычету ν по модулю δ , где $0 \leq \nu < \delta$, если все числа $k \in \Lambda$ удовлетворяют сравнению $k \equiv \nu \pmod{\delta}$.

Множество длин слов в алфавите Q , принадлежащих прообразу $\varphi^{-1}(t)$, где $t \in S$, обозначим $\Lambda_Q(t)$. При рассмотрении полугруппы S^1 для элемента $1 \notin S$ положим $\Lambda_Q(1) = \{0\}$.

Определение 3. Для элемента $t \in S$, $|\Lambda_Q(t)| > 1$, максимальное значение модуля, вычету по которому принадлежит множество $\Lambda_Q(t)$, назовём его модулем однозначности в полугруппе (S, Q) , который обозначим $\delta_t(Q)$. Будем говорить, что элемент $t \in S$ принадлежит вычету $\nu_t(Q)$ по модулю $\delta_t(Q)$, если для всех чисел $\lambda \in \Lambda_Q(t)$ имеем $\lambda \equiv \nu_t(Q) \pmod{\delta_t(Q)}$.

Поскольку порождающее множество предполагается фиксированным, далее будем использовать обозначения $\Lambda(u)$, δ_u , ν_u .

Лемма 2. Справедливо равенство $\delta_t = \text{НОД}\{|\lambda_1 - \lambda_2| : \lambda_1, \lambda_2 \in \Lambda(t)\}$.

Это утверждение является очевидным следствием определения 3.

ЗАМЕЧАНИЕ 2. Множество $\Lambda(t)$ принадлежит некоторому вычету $\nu \pmod{\delta}$ для всех чисел $\delta \mid \delta_t$ и только для них.

Теорема 3. 1) Если $t \in S \setminus W(S)$, то $\delta_t \mid \alpha(Q)$.

2) Если $t, u \in S \setminus W(S)$ и $D_\nu \leq_D D_t$, то $\delta_\nu \mid \delta_t$.

3) Если $|D_t| > 1$, $t \sim v$, то $\delta_v = \delta_t$.

Доказательство. 1) Из условия $t \in S \setminus W(S)$ следует что $t \in Q^k$ хотя бы для одного k , $\rho(Q) \leq k \leq \rho(Q) + \omega(Q) - 1$. Тогда для любого целого положительного k имеем $j + k\omega(Q) \in \Lambda(t)$. Отсюда следует, что $\delta_t | \omega(Q)$.

2) Из условия $D_v \leq_D D_t$ следует существование таких элементов $w, x \in S^1$, что $v = w \cdot t \cdot x$. Тогда для любой константы $c \in \Lambda(w) + \Lambda(x)$ имеем $\Lambda(v) \supseteq \Lambda(t) + c$, откуда вытекает справедливость второго утверждения теоремы.

3) Справедливость третьего утверждения теоремы следует из второго утверждения по соображениям симметрии.

Общий модуль однозначности элементов класса $D \subseteq S \setminus W(S)$ обозначим δ_D .

3.2. Цикловые элементы полугруппы и их цикловые индексы

Определение 4. Пару $(u, v) \in (T^1 \times S^1)$, где $u, v \in S$, назовём t -циклом, если для элемента $t \in S$ выполняется соотношение $u \cdot t \cdot v = t$.

Множество всех t -циклов назовём стабилизатором элемента t и обозначим $\text{St}(t)$.

Если $(u_i, v_i) \in \text{St}(t)$, $i = 1, 2$, то $(u_2 \cdot u_1, v_1 \cdot v_2) = (u_1, v_1) \cdot (u_2, v_2) \in \text{St}(t)$. Следовательно, множество $\text{St}(t)$ является подполугруппой полугруппы $(T^1 \times S^1)$.

Элементы $t \in S$, для которых $\text{St}(t) \neq \emptyset$, назовём *цикловыми элементами* полугруппы. Множество цикловых элементов полугруппы обозначим $C(S)$. Из определения ясно, что множество цикловых элементов не зависит от выбора порождающего множества Q .

Если полугруппа S является моноидом, то очевидно, что $C(S) = S$.

Если $t \in \text{Reg}(S)$, то найдутся идемпотент $e \in D_t$ и такие элементы полугруппы u, v, x, y , что $u \cdot t \cdot v = e$, $x \cdot e \cdot y = t$, откуда вытекает, что $x u \cdot t \cdot v \cdot y = t$. Следовательно, $t \in C(S)$ и справедлива цепочка включений

$$\text{Reg}(S) \subseteq C(S) \subseteq S \setminus W(S) \subseteq S,$$

причём, как показано в примере 6 (§ 5), возможен случай, когда все включения строгие.

Теорема 4. 1) Элемент $t \in S$ является цикловым элементом тогда и только тогда, когда он имеет левую или правую единицу, поэтому

$$C(S) = \bigcup_{e, f \in E(S)} (e \cdot S \cup S \cdot f).$$

2) Если $t \in C(S)$ или $|D_t| > 1$, то $D_t \subseteq C(S)$.

Доказательство. 1) Пусть $t \in C(S)$ и $(u, v) \in \text{St}(t)$. Из того, что $(u, v) \cdot (u, v) = (u^2, v^2)$, получаем $(e_u, e_v) \in \text{St}(t)$. При этом выполняется условие $e_u \cdot e_v \in S$, т. е. элемент t имеет в S левую или правую единицу. Тривиально обратное утверждение: элемент $t \in S$, имеющий единицу любого вида, является цикловым элементом полугруппы. Так как множество $\bigcup_{e \in E(S)} e \cdot S$ (соответственно, множество $\bigcup_{f \in E(S)} S \cdot f$) состоит из всех элементов полугруппы, имеющих левую (соответственно, правую) единицу, первое утверждение теоремы доказано.

2) Если $|D_t| = 1$ и $t \in C(S)$, то, очевидно, $D_t \subseteq C(S)$. Пусть $|D_t| > 1$, $u \in D_t$, $t \neq u$. Тогда найдутся такие элементы $v, w, x, y \in S^1$, $v \cdot w \in S$, $x \cdot y \in S$, что $v \cdot t \cdot w = u$, $x \cdot u \cdot y = t$, откуда $v \cdot x \cdot u \cdot y \cdot w = u$, $x \cdot v \cdot t \cdot w \cdot y = t$. Так как эти соотношения справедливы для любого элемента $u \in D_t$, то $D_t \subseteq C(S)$. Теорема доказана.

D -класс, содержащий цикловые элементы полугруппы, назовём *цикловым D -классом*.

Элементы D -класса $D_t \subseteq S \setminus W(S)$, принадлежащие вычету v , $0 \leq v \leq \delta_{D_t} - 1$, объединим в подмножество $D_t^{(v)}$, так что

$$D_t = D \bigcup_{v=0}^{\delta_{D_t}-1} D_t^{(v)}. \quad (3)$$

Лемма 3. Если $D \subseteq C(S)$, то в разложении (3) отсутствуют пустые компоненты.

Доказательство. Пусть $D_t \subseteq C(S)$, $(u, v) \in \Theta(t)$, и $u \cdot v \in S$. Рассмотрим произвольные записи $u = u_m \cdot \dots \cdot u_1$, $v = v_1 \cdot \dots \cdot v_n$ элементов u, v в алфавите Q . Из свойств частичной упорядоченности D -классов вытекает, что при любых $i = 1, \dots, m, j = 1, \dots, n$ имеем $u_i \cdot \dots \cdot u_1 \cdot t \in D_t$, $t \cdot v_1 \cdot \dots \cdot v_j \in D_t$, $u_i \cdot \dots \cdot u_1 \cdot t \cdot v_1 \cdot \dots \cdot v_j \in D_t$. Следовательно, $v_{u_i \dots u_1 t v_1 \dots v_j} \equiv v_t + i + j \pmod{\delta_D}$. Случаи $u \in S$, $v = 1$ и $v \in S$, $u = 1$ рассматриваются аналогично. Лемма доказана.

В примере 8 (§ 5) показано, что при $D_t \not\subseteq C(S)$ в разложении (3) могут быть пустые компоненты.

Спектром длин t -цикла $(u, v) \in \text{St}(t)$ назовём множество чисел $\Omega(u, v) = \Lambda(u) + \Lambda(v)$. *Спектром длин стабилизатора $\text{St}(t)$* назовём множество чисел

$$\Theta(t) = \bigcup_{(u,v) \in \text{St}(t)} \Omega(u, v).$$

Определение 5. Для элемента $t \in C(S)$ наибольший общий делитель спектра длин t -циклов назовём *цикловым индексом* элемента t и обозначим его ω_t .

Теорема 5. Пусть $t, u \in C(S)$. Тогда:

- 1) множество $\Theta(t)$ замкнуто относительно сложения u , следовательно, содержит все кратные ω_t , кроме, возможно, их конечного числа;
- 2) если $t \underset{D}{\sim} u$, то $\omega_t = \omega_u$;
- 3) если $D_u \leq_D D_v$, то δ_u / ω_t . В частности, δ_t / ω_t ;
- 4) если $t \in \text{Reg}(S)$, то $\delta_t = \omega_t$.

Доказательство. 1) Если $(u_j, v_j) \in \text{St}(t)$, $j = 1, 2$, то $(u_2 \cdot u_1, v_1 \cdot v_2) \in \text{St}(t)$, откуда вытекает справедливость первого утверждения теоремы.

2) Если $|D_t| = 1$, то второе утверждение теоремы тривиально. Пусть $|D_t| > 1$ и $u \neq t$. Так как $t \underset{D}{\sim} u$, то найдутся элементы $v, w, x, y \in S^1$, $v \cdot w, x \cdot y \in S$, для которых выполняются равенства $u = v \cdot t \cdot w$, $t = x \cdot u \cdot y$. Поэтому

$$x \cdot v \cdot t \cdot y \cdot w = t, v \cdot x \cdot u \cdot y \cdot w = u,$$

означающие, что $(x \cdot v, y \cdot w) \in \text{St}(t)$, $(v \cdot x, y \cdot w) \in \text{St}(u)$. Положив $c = \lambda(x \cdot v, y \cdot w) = \lambda(v \cdot x, y \cdot w)$, получаем:

$$\Theta(u) \supseteq \{c, \Theta(t) + c\}, \Theta(t) \supseteq \{c, \Theta(u) + c\}.$$

Из этих включений вытекает справедливость второго утверждения теоремы.

3) Из $t \underset{D}{\sim} u$ следует существование таких элементов $v, w \in S^1$, что $u = v \cdot t \cdot w$. Для каждого t -цикла (x, y) имеем $u = v \cdot x \cdot t \cdot y \cdot w$, следовательно, для любого числа $\lambda \in \Omega(x, y)$ множество $\Lambda(u)$ содержит такие числа λ_1, λ_2 , что $|\lambda_1 - \lambda_2| = \lambda$. Отсюда следует справедливость третьего утверждения теоремы.

4) Пусть $e \in E(S) \cap Dt$ и $k \in \Lambda(e)$. Так как $e^2 = e$, имеем $k \in \Omega(e)$, откуда следует, что $\Lambda(e) \subseteq \Omega(e)$ и $\omega e / \delta e$. С учётом утверждений 2, 3 теоремы 4 заключаем, что $\delta t = \omega t$.

Теорема доказана.

Как показано в примере 7 (§ 5), для нерегулярного D -класса возможно соотношение $\delta_t < \omega_t$.

Общий цикловой индекс элементов, принадлежащих цикловому D -классу D_t , будем обозначать ω_{D_t} . Цикловой индекс ядра полугруппы обозначим $\omega_{K(S)}$.

Следствие 3. Для любого циклового D -класса D_t выполняется соотношение $\omega_{K(S)} / \omega_{D_t}$.

Доказательство вытекает из утверждений 3, 4 теоремы 5.

3.3. Период полугруппы (S, Q) . Из следствия 2 вытекает, что максимальные циклические D -классы являются регулярными классами.

Множество максимальных циклических D -классов полугруппы S обозначим $D^{(\text{Reg})}$.

Положим $D^{(\text{Reg})} = \{D^{(1)}, \dots, D^{(h)}\}$. Обозначим

$$\omega' = \text{НОК}(\omega_{D^{(1)}}, \dots, \omega_{D^{(h)}}).$$

Лемма 4. Если $t \in C(S)$, то $\omega_t \mid \omega'$.

Доказательство. Из утверждения 1 теоремы 4 вытекает, что найдутся идемпотенты $e, f \in S^1$ со свойствами $e \cdot f \in S$ и $(e, f) \in \text{St}(t)$. Пусть, для определённости, $e \in S$. Тогда $e \cdot t = t$, откуда следует, что $\Omega(t) \supseteq \Omega(e)$, и, следовательно, $D_t \leq_D D_e$ и $\omega_t \mid \omega_e$. Значит, $\omega_t \mid \omega'$.

Теорема 6. Для периода полугруппы S имеет место соотношение

$$\alpha(Q) = \text{НОК}(\omega_{D^{(1)}}, \dots, \omega_{D^{(h)}}).$$

Доказательство. Из утверждений 1, 2 теоремы 3 и утверждения 4 теоремы 5 следует, что $\omega' \mid \alpha(Q)$. Покажем, что $\alpha(Q) \mid \omega'$.

а) Если $t \in C(S) \cap Q^k$, то из леммы 4 вытекает, что $t \in Q^{k+\omega'}$.

б) Пусть $t \in S \setminus (W(S) \cup C(S)) \cap Q^j$ и $t = r_1 \cdot \dots \cdot r_m$ — произвольная запись элемента t в алфавите Q длины $m > |S|$, $m \equiv k \pmod{\alpha(Q)}$. Рассмотрим последовательность элементов полугруппы:

$$r^{(1)} = r_1, r^{(2)} = r_1 \cdot r_2, \dots, r^{(m)} = r_1 \cdot \dots \cdot r_m.$$

Из условия $m > |S|$ вытекает, что в этой последовательности найдётся хотя бы одно повторение. Пусть $r^{(a)} = r^{(b)} = v$, $a < b$. Тогда $v \cdot r_{a+1} \cdot \dots \cdot r_b = v$, следовательно, $v \in C(S)$ и $u \neq v$. Поэтому $b < m$ и $u = v \cdot r_{b+1} \cdot \dots \cdot r_m$. Так как $\omega_b \mid \omega'$, то из $u \in Q^k$ вытекает, что $u \in Q^{k+\omega'}$.

Окончательно, при всех $k \geq \rho(Q)$ имеем $Q^k = Q^{k+\omega'}$. Из определения периода полугруппы следует, что $\alpha(Q) \mid \omega'$, следовательно, $\alpha(Q) = \omega'$. Теорема доказана.

Следствие 4. Пусть S — моноид и D^* — группа обратимых элементов моноида. Тогда $\alpha(Q) = \omega_{D^*}$ для любого порождающего множества Q моноида S .

Доказательство. Если S — моноид, то регулярный D -класс D^* является единственным максимальным D -классом полугруппы S . С учётом этого утверждение следствия очевидно.

3.4. Условия принадлежности элемента полугруппы её слоям.

В следующем утверждении приведены условия принадлежности элементов $t \in S \setminus W(S)$ слоям полугруппы в зависимости от значений введённых выше параметров δ_t , v_t , ω_t .

Теорема 7. Пусть S — конечная полугруппа, Q — порождающее множество её элементов. Тогда:

1) если $t \in S \setminus W(S)$ и $t \in Q^k$, где $k \geq \rho(Q)$, то $k \equiv v_t \pmod{\delta_t}$;

2) если $t \in C(S)$, и $t \in Q^k$, где $k \geq \rho(Q)$, то $t \in Q^m$ для всех $m \equiv k \pmod{\omega}$, $m \geq \rho(Q)$;

3) если $t \in \text{Reg}(S)$, то $t \in Q^k$, где $k \geq \rho(Q)$, тогда и только тогда, когда $k \equiv \nu_t \pmod{\omega_t}$.

Доказательство. 1) Из определения 1 следует, что $t \in Q^k$ тогда и только тогда, когда $k \in \Lambda(t)$. Согласно определению 3, из $k \in \Lambda(t)$ вытекает, что $k \equiv \nu_t \pmod{\delta_t}$.

2) Если $m \equiv k \pmod{\omega}$, то при всех достаточно больших l имеем $m + l\omega \in \Lambda(t)$. Отсюда, с учётом леммы 4 и теоремы 6, следует справедливость второго утверждения теоремы.

3) Третье утверждение теоремы следует из первого и второго с учётом того, что в рассматриваемом случае $\delta_t = \omega_t$. Теорема доказана.

§ 4. Графы Кэли конечной полугруппы

При исследовании характеристик группы G , порождаемой системой образующих M , часто рассматривается соответствующий паре (G, M) ориентированный граф Кэли [1], [7]. Специфика конечной полугруппы делает целесообразным рассмотрение трёх его различных аналогов, совпадающих с графом Кэли, если полугруппа является группой.

Напомним, что T обозначает полугруппу, антиизоморфную полугруппе S (см. § 1).

Определение 6. 1) *Правым графом Кэли полугруппы S* , соответствующим порождающему множеству Q , назовём граф $\Gamma^{(r)}(S, Q)$, в котором вершинами являются элементы полугруппы S и вершины $t, u \in S$ соединены ребром из t в u , если существует такой элемент $q \in Q$, что $t \cdot q = u$.

2) *Левым графом Кэли полугруппы S* , соответствующим порождающему множеству Q , назовём граф $\Gamma^{(l)}(S, Q)$, в котором вершинами являются элементы полугруппы S и вершины $t, u \in S$ соединены ребром из t в u , если существует такой элемент $q \in Q$, что $q \cdot t = u$.

3) *Двусторонним графом Кэли полугруппы S* , соответствующим порождающему множеству Q , назовём граф $\Gamma(S, T, Q)$, в котором вершинами являются элементы полугруппы S и вершины $t, u \in S$ соединены ребром из t в u , если существуют такие элементы $q, r \in Q^1$, $q \cdot r \in S$, что $q \cdot t \cdot r = u$.

Очевидно, что элементы каждого циклового D -класса полугруппы образуют компоненту сильной связности графа $\Gamma(S, T, Q)$. Аналогично, элементы каждого циклового R -класса (L -класса) образуют компоненту сильной связности графа $\Gamma^{(r)}(S, Q)$ (соответственно, графа $\Gamma^{(l)}(S, Q)$).

Если $\text{St}(t) \neq \emptyset$ и $(u, v) \in \text{St}(t)$, то каждому числу $\lambda \in \Lambda(u, v)$ в графе $\Gamma(S, T, Q)$ соответствует хотя бы один контур длины λ , проходящий через вершину t . Обратно, каждому контуру длины λ соответствуют такие t -циклы (u, v) , что вершина t принадлежит рассматриваемому контуру и $\lambda \in \Lambda(u, v)$. В этом случае цикловой индекс D -класса равен наибольшему общему делителю длин контуров, принадлежащих этой компоненте. Длина каждого пути в графе $\Gamma(S, T, Q)$, начинающегося в одной из вершин множества Q и оканчивающегося в вершине $t \in S \setminus W(S)$, сравнима с вычетом $v_t \pmod{\delta_t}$.

Аналогично цикловому индексу введём в рассмотрение правый и левый цикловые индексы элементов полугруппы, которые определяются свойствами графов $\Gamma^{(r)}(S, Q)$ и $\Gamma^{(l)}(S, Q)$.

Определение 7. Элемент $u \in S$ назовём *правым t -циклом* (*левым t -циклом*), если имеет место равенство $t \cdot u = t$ ($u \cdot t = t$). Множество правых t -циклов (*левых t -циклов*) обозначим $\text{St}^{(r)}(t)$ ($\text{St}^{(l)}(t)$). Элементы $t \in S$, для которых $\text{St}^{(r)}(t) \neq \emptyset$ ($\text{St}^{(l)}(t) \neq \emptyset$), назовём *цикловыми справа* (*цикловыми слева*) *элементами полугруппы*. Множество цикловых справа (*цикловых слева*) элементов полугруппы обозначим $C^{(r)}(S)$ ($C^{(l)}(S)$).

Очевидно, что $C^{(r)}(S) \subseteq C(S)$, $C^{(l)}(S) \subseteq C(S)$.

Непустые множества $\text{St}^{(r)}(t)$, $\text{St}^{(l)}(t)$ являются, очевидно, подполугруппами полугруппы S . Если же $\text{St}^{(r)}(t) = \emptyset$ ($\text{St}^{(l)}(t) = \emptyset$), то обязательно $|R_t| = 1$ ($|L_t| = 1$).

Для элементов полугруппы справедливы следующие утверждения, аналогичные доказанным ранее.

Лемма 5. 1) $C^{(l)}(S) = \bigcup_{e \in E} eS$; $C^{(r)}(S) = \bigcup_{e \in E} Se$; $C(S) = C^{(r)}(S) \cup C^{(l)}(S)$.

2) Если $|R_s| > 1$ ($|L_s| > 1$), то $R_s \subseteq C^{(r)}(S)$ ($L_s \subseteq C^{(l)}(S)$).

3) Если $s \sim_R t$, то $\text{St}^{(l)}(s) = \text{St}^{(l)}(t)$.

4) Если $s \sim_H t$, то $\text{St}^{(l)}(s) = \text{St}^{(l)}(t)$, $\text{St}^{(r)}(s) = \text{St}^{(r)}(t)$.

Наибольший общий делитель множества чисел $\Omega^{(r)} = \bigcup_{u \in \text{St}^{(r)}(t)} \Lambda(u)$ назо-

вём *правым цикловым индексом* элемента $t \in C^{(r)}(S)$ и обозначим его $\omega_t^{(r)}$. *Левый цикловой индекс* определяется двойственным образом. Из определения следует, что правый (левый) цикловой индекс элемента $t \in S$ определён, если через вершину t графа $\Gamma^{(r)}(S, Q)$ (соответственно, $\Gamma^{(l)}(S, Q)$) проходит хотя бы один контур. В этом случае правый (левый) цикловой индекс равен наибольшему общему делителю длин всех контуров соответствующего графа, проходящих через вершину t .

Лемма 6. $\omega_t \mid \text{НОД}(\omega_t^{(r)}, \omega_t^{(l)})$.

Это утверждение следует непосредственно из определений.

В примере 5 (§ 5) показано, что не всегда $\omega_t = \text{НОД}(\omega_t^l, \omega_t^r)$.

Лемма 7. Если $R_t \subseteq C^{(r)}(S)$ и $t \underset{R}{\sim} u$, то $\omega_t^{(r)} = \omega_u^{(r)}$.

Доказательство аналогично доказательству утверждения 2 теоремы 5.

Верно также и двойственное утверждение.

Покажем, что левый, правый и двусторонний цикловые индексы могут различаться только у нерегулярных элементов полугруппы.

Теорема 8. Если t — регулярный элемент полугруппы S , то $\omega_t^{(l)} = \omega_t^{(r)} = \omega_t = \delta_t$.

Доказательство. Справедливость последнего равенства установлена в теореме 5. Пусть $e \in E(S) \cap R_t$ (такой идемпотент существует в силу регулярности класса D_t). Тогда $\Lambda(e) \subseteq \Omega^{(r)}(e) \cap \Omega^{(l)}(e)$. Учитывая, что множество чисел $\Lambda(e)$ принадлежит вычету $0 \pmod{\delta_e}$, заключаем, что $\omega_e^{(l)} \mid \delta_e, \omega_e^{(r)} \mid \delta_e$.

Отсюда, с учётом леммы 7 и равенства $\delta_e = \omega_e$, следуют все утверждения теоремы.

Следствие 5. Наибольшие общие кратные длин всех контуров каждого из графов $\Gamma^{(r)}(S, Q), \Gamma^{(l)}(S, Q)$ равны периоду полугруппы (S, Q) .

Доказательство. Утверждение следствия вытекает из теорем 6, 8.

Следствие 6. Левый, правый и двусторонний цикловые индексы всех элементов группы G равны между собой.

Доказательство. Если G — группа, то G является регулярным D -классом. Утверждение следствия является частным случаем теоремы 8.

§ 5. Примеры полугрупп

Рассмотрим примеры полугрупп, иллюстрирующие некоторые крайние случаи и возможные соотношения между введёнными выше параметрами.

Пример 1. Полугруппа S называется *нильпотентной*, если S содержит элемент 0 и при некотором числе n выполняется равенство $S^n = \{0\}$. Для nilьпотентной полугруппы имеем $W(S) = S \setminus 0$ и $r(S) = \min\{n : S^n = \{0\}\}$.

Пример 2. Напомним, что через $K(S)$ обозначается минимальный идеал конечной полугруппы S .

Полугруппа S называется *ниль-полугруппой*, если идеальный фактор полугруппы S по ядру $K(S)$ является nilьпотентной полугруппой. Это означает, что при некотором числе n выполняется равенство $S^n = K(S)$. Для nilь-полугруппы имеем $W(S) = S \setminus K(S)$ и $r(S) = \min\{n : S^n = K(S)\}$.

Пример 3. Полугруппа S называется *полугруппой левых нулей*, если для любых её элементов s, t верно $s \cdot t = s$. В такой полугруппе существует единственное порождающее множество $Q = S$, единственный слой, единственный D -класс $K(S) = S$, содержащий один L -класс и $|S|$ разных R -классов, каждый из которых содержит один элемент. Граф $\Gamma^{(r)}(S, Q)$ содержит только петли, а граф $\Gamma^{(l)}(S, Q)$ является полным ориентированным псевдографом. Очевидно, что для всех элементов t полугруппы имеем $\omega_t^{(l)} = \omega_t^{(r)} = \omega_t = \omega_{K(S)} = 1$.

Пример 4. Полугруппа S называется *простой*, если $S = K(S)$. В этом случае $W(S) = \emptyset$ и ядро $K(S)$ является единственным D -классом полугруппы S . Цикловой индекс ядра полугруппы обозначим $\omega_{K(S)}$. Согласно лемме 3, дизъюнктное разложение

$$S = S^{(0)} \cup \dots \cup S^{(\omega_{K(S)} - 1)} \quad (4)$$

не содержит пустых компонент.

Приведём необходимые для рассмотрения разложения (4) сведения о нормальных подполугруппах.

Говорят, что конгруэнция ρ допускает подмножество A полугруппы S , если множество A является классом конгруэнции ρ . Множество конгруэнций, допускающих A , замкнуто относительно объединения и пересечения, поэтому существуют максимальная и минимальная конгруэнции, допускающие A .

Подмножество A элементов полугруппы S называется:

- а) *рефлексивным*, если для любых $a, b \in S$ из $a \cdot b \in A$ следует, что $b \cdot a \in A$;
- б) *унитарным*, если для любых $a \in A, t \in S$ из условия $a \cdot t \in A$ или $t \cdot a \in A$ следует, что $t \in A$.

Непустое подмножество N полугруппы S называют *нормальной подполугруппой*, если N является полным прообразом единицы при некотором гомоморфизме φ полугруппы S на полугруппу с единицей.

Если нормальная подполугруппа N является классом конгруэнции ρ , то говорят, что ρ нормально допускает подполугруппу N .

Известно, что N — нормальная подполугруппа полугруппы S тогда и только тогда, когда N — рефлексивная и унитарная подполугруппа, а классами максимальной конгруэнции ρ^N , нормально допускающей подполугруппу N , являются непустые члены следующего семейства множеств:

$$\{Nx^{[-1]} \mid x \in S\}, V_N,$$

где через $Nx^{[-1]}$ обозначено множество таких элементов $a \in S$, что $a \cdot x \in N$, а V_N — множество, состоящее из таких элементов $x \in S$, что $Nx^{[-1]} = \emptyset$.

Имеют место следующие утверждения [5], [6].

1) Если $V_N = \emptyset$, то конгруэнция ρ^N является единственной конгруэнцией, нормально допускающей N . В этом случае факторполугруппа S/N является группой.

2) Если $V_N \neq \emptyset$, то конгруэнция ρ^N является единственной конгруэнцией, нормально допускающей N и такой, что факторполугруппа S/N является группой с нулём.

Теперь легко показать, что множество $S^{(0)}$ в разложении (4) является нормальной подполугруппой полугруппы S , так как свойства рефлексивности и унитарности подполугруппы $S^{(0)}$ следуют непосредственно из определений. Множества $S^{(j)}$, $j = 1, \dots, \omega_{K(S)} - 1$, являются классами максимальной конгруэнции ρ полугруппы S , нормально допускающей $S^{(0)}$, так как очевидно, что $V_{S^{(0)}} = \emptyset$, а для $x \in S^{(j)}$, $j = 1, \dots, \omega_{K(S)} - 1$, имеем $\{a \mid a \cdot x \in S^{(0)}\} = S^{\omega_{K(S)} - j}$.

Пример 5. Рассмотрим полугруппу S , заданную её копредставлением [3], состоящим из порождающего множества $Q = \{p, q\}$ и определяющих соотношений:

$$p^4 = p, q^4 = q, p^2 q^2 = pq, qp = 0.$$

Полугруппа S состоит из следующих четырёх D -классов:

$$D_p = \{p, p^2, p^3\}, D_q = \{q, q^2, q^3\}, D_{pq} = \{pq, p^2 q, p^3 q, pq^2, pq^3\}, K(S) = \{0\}.$$

Легко видеть, что

$$Z^{(r)}(pq) = \{p^3\}, Z^{(l)}(pq) = \{q^3\}, Z(pq) = \{(p, q), p^2, q^2, (p^3, q^3), (p^3, 1), (1, q^3)\}.$$

$$\omega_{pq}^{(r)} = \omega_{pq}^{(l)} = 3, \omega_{pq} = 1.$$

Таким образом, возможно, что $\omega_{pq} < (\omega_{pq}^{(r)}, \omega_{pq}^{(l)})$. Этот пример показывает, что утверждение леммы 6 не может быть усилено.

Для построения ряда дальнейших примеров применим конструкцию свободного произведения полугрупп [5]. Пусть U, V — конечные полугруппы, $U \cap V = \emptyset$, а P — свободная полугруппа на множестве $U \cup V$. Определим операцию приведения на словах полугруппы P : все максимальные подслова любого слова $p \in P$, состоящие из букв одного алфавита U или V , заменяются соответствующими элементами полугрупп U или V . Очевидно, что приведение является гомоморфным отображением P на полугруппу $P(U, V)$, элементами которой являются слова в алфавите $U \cup V$, не содержащие двух рядом стоящих букв одного из алфавитов. Операция умножения в полугруппе $P(U, V)$ сводится к конкатенации слов с последующим (при необходимости) применением операции приведения.

В полугруппе $P(U, V)$ подмножество $P_k(U, V)$, состоящее из всех слов с числом букв не менее k , является идеалом, а идеальный фактор $P(U, V) / P_k(U, V)$ является конечной полугруппой.

В качестве полугрупп U, V выберем циклические полугруппы с определяющими соотношениями $u^2 = u^{\omega_1+1}$ и $v^2 = v^{\omega_2+1}$ соответственно. Для последующих примеров мы используем полугруппу $P' = P(U, V) / P_4(U, V)$, состоящую из всех слов полугруппы $P(U, V)$, содержащих не более трёх букв, и нуля. Операция в полугруппе P' сводится к операции в полугруппе $P(U, V)$, и если результат произведения двух элементов после приведения содержит более трёх букв, то в полугруппе P' это произведение равно нулю.

Пример 6. Опишем D -классы полугруппы P' . Циклические группы, порождаемые элементами u^2, v^2 , обозначим G, H соответственно.

Оболочку полугруппы составляют шесть одноэлементных D -классов:

$$W(P') = \{u; v; u \cdot v; v \cdot u; u \cdot v \cdot u; v \cdot u \cdot v\}.$$

Полугруппа содержит три регулярных D -класса:

$$\text{Reg}(P') = \{G; H; 0\}.$$

Множество цикловых элементов полугруппы является объединением следующих D -классов:

$$\begin{aligned} C(P') = \{ & 0; G; H; t \cdot H; v \cdot G; G \cdot v; G \cdot H; H \cdot u; H \cdot G; \\ & U \cdot v^x \cdot G, G \cdot v^x \cdot u, G \cdot v^x \cdot G \ (x = 1, \dots, \omega_2 + 1); \cdot u^y \cdot Hu^y, H \cdot u^y \cdot v, \\ & H \cdot u^y \cdot H \ (y = 1, \dots, \omega_1 + 1) \}. \end{aligned}$$

Наконец,

$$P' \setminus (W(P') \cup C(P')) = \{u \cdot v^x \cdot u, x = 1, \dots, \omega_2 + 1; v \cdot u^y \cdot v, y = 1, \dots, \omega_1 + 1\}.$$

Таким образом, в рассматриваемом случае $P' \setminus (W(P') \cup C(P')) \neq \emptyset$ и имеют место строгие включения $\text{Reg}(P') \subset C(P') \subset P' \setminus W(P') \subset P'$.

Далее положим $Q = \{u, v\}$.

Максимальными среди регулярных классов D -классами полугруппы P' являются D -классы G и H , при этом $\omega_G = \omega_1$, $\omega_H = \omega_2$. По теореме 6 имеем $\omega(Q) = \text{НОК}(\omega_1, \omega_2)$.

Пример 7. Рассмотрим D -классы vG и vu^2H . Имеем $vu^2H <_D vG$. Очевидно, что $\omega_{vG} = \delta_{vG} = \omega_1$, $\omega_{vu^2H} = \omega_2$. Следовательно, с учётом произвола в выборе чисел ω_1 и ω_2 , между цикловыми индексами нерегулярных классов, связанных отношением $<_D$, могут быть любые соотношения делимости. Далее, например, для элемента $vu^2v^2 \in vu^2H$ имеем: $\Lambda(vu^2v^2) = 5 + k_1\omega_1 + k_2\omega_2$, где k_1, k_2 — любые неотрицательные числа. Отсюда получаем $\delta_{vu^2H} = (\omega_1, \omega_2)$. Таким образом, в дополнение к утверждению 4 теоремы 5 показано, что для нерегулярного D -класса возможен случай, когда $\delta_D < \omega_D$.

Пример 8. Если $D \not\subset C(S)$, то из второго утверждения теоремы 4 следует, что $|D| = 1$, однако может оказаться, что $\delta_D > 1$. Очевидно, в этом случае

в разложении (3) содержится только одна непустая компонента. Так, для класса $D = \{vuv^xv\}$ при $2 \leq x \leq \omega_1$ имеем $D \subseteq S \setminus (W(S) \cup C(S))$, $A(vuv^xv) = \{2 + x + \omega_1\}$, $\delta_D = \omega_1$, $v_{vuv^xv} \equiv (2 + x) \pmod{\omega_1}$, и $D = D^{(v_{vuv^xv})}$.

Пример 9. Рассмотрим конечный автомат без выхода $A = (X, B, P)$. Знаку $x \in X$ входного алфавита соответствует частичная функция переходов автомата p_x . Множество $P = \{p_x \mid x \in X\}$ порождает полугруппу S автомата A . Начальному состоянию a_0 автомата и входной последовательности $x_1, \dots, x_n$ соответствуют последовательности

$$p_{x_1}, \dots, p_{x_n} \quad (5)$$

частичных функций перехода и $a_1, \dots, a_n$ его состояний. Последовательности (5) поставим в соответствие прямую последовательность

$$\sigma_1^{(r)}, \dots, \sigma_n^{(r)}$$

и обратную последовательность

$$\sigma_1^{(l)}, \dots, \sigma_n^{(l)}$$

суммарных функций переходов автомата, где положено

$$\sigma_i^{(r)} = \prod_{j=1}^i p_{x_j}, \quad \sigma_i^{(l)} = \prod_{j=i}^1 p_{x_{n-j+1}},$$

так что для $i = 1, \dots, n$ имеем:

$$a_i = a_0 \sigma_i^{(r)}, \quad a_n = a_{n-i} \sigma_i^{(l)}.$$

Можно отметить некоторые свойства прямой и обратной последовательностей.

1) Если $t \in W(S)$, то равенство $\sigma_i^{(r)} = t$ или $\sigma_i^{(l)} = t$ возможно не более одного раза в каждой из рассматриваемых последовательностей и только для $i < \rho$;

2) если $|A(t)| > 1$, то равенство $\sigma_i^{(r)} = t$ или $\sigma_i^{(l)} = t$ возможно только при выполнении условия $i \equiv \nu_t \pmod{\delta_t}$;

3) если $t \notin C^{(r)}(S)$, то равенство $\sigma_i^{(r)} = t$ возможно не более одного раза в любой прямой последовательности суммарных функций переходов;

4) если $t \in C^{(r)}(S)$, то равенства $\sigma_i^{(r)} = t$, $\sigma_j^{(r)} = t$ возможны только при условии $\omega_t^{(r)} \mid (i - j)$.

Для обратной последовательности суммарных функций переходов справедливы утверждения, двойственные утверждениям 3, 4.

§ 6. Циклические факторы полугруппы

Как следует из утверждения 2 теоремы 3 и утверждения 3 теоремы 5, наибольшие общие делители длин контуров графов $\Gamma(S, Q)$, $\Gamma^{(r)}(S, Q)$, $\Gamma^{(l)}(S, Q)$ равны между собой и совпадают с цикловым индексом $\omega_{K(S)}$ ядра полугруппы.

Лемма 8. Для любого элемента t полугруппы S , для любого делителя ω числа $\omega_{K(S)}$ и для любых $\lambda_1, \lambda_2 \in \Lambda(t)$ выполняется сравнение $\lambda_1 \equiv \lambda_2 \pmod{\omega}$.

Доказательство. Если $t \in S$ и $|\Lambda(t)| = 1$, то утверждение леммы тривиально. Пусть $|\Lambda(t)| > 1$ и $\lambda_1, \lambda_2 \in \Lambda(t)$, $\lambda_1 \neq \lambda_2$. Возьмём произвольный элемент $u \in K(S)$. Найдутся такие элементы $x, y \in S^1$, $x \cdot y \in S$, что $x \cdot t \cdot y = u$. Пусть $\lambda_x \in \Lambda(x)$, $\lambda_y \in \Lambda(y)$. Тогда $\lambda_x + \lambda_j + \lambda_y \equiv \nu_u \pmod{\omega_{K(S)}}$, $j = 1, 2$, откуда вытекает утверждение леммы.

Отметим, что если $t \in S \setminus W(S)$, то утверждение леммы, с учётом замечания 2, следует из утверждения 2 теоремы 3.

Для элемента $t \in S$ вычит по $\text{mod } \omega_{K(S)}$, которому принадлежат все числа из множества $\Lambda(t)$, обозначим μ_t . Для любых таких ω, μ , что $\omega \mid \omega_{K(S)}$ и $0 \leq \mu \leq \omega - 1$, через $S_\mu^{(\omega)}$ обозначим множество элементов t полугруппы S , для которых выполняется сравнение $\mu \equiv \mu_t \pmod{\omega}$.

Теорема 9. При любом $\omega \mid \omega_{K(S)}$, $\omega > 1$:

- 1) множества $S_\mu^{(\omega)}$, $\mu = 0, \dots, \omega - 1$, являются классами максимальной конгруэнции $\rho^{S_0^{(\omega)}}$, допускающей $S_0^{(\omega)}$;
- 2) $S_0^{(\omega)}$ — нормальная подполугруппа полугруппы S ;
- 3) фактор-полугруппа $S / S_0^{(\omega)}$ изоморфна циклической группе порядка ω ,
- 4) $P \subseteq S_1^{(\omega)}$;
- 5) $E(S) \subseteq S_0^{(\omega)}$.

Доказательство. Для произвольного числа ω , удовлетворяющего условиям теоремы, определим отношение $\rho^{S_0^{(\omega)}}$ на множестве элементов полугруппы S , положив $x \rho^{S_0^{(\omega)}} y$ тогда и только тогда, когда $\mu_x \equiv \mu_y \pmod{\omega}$. Легко установить, что отношение $\rho^{S_0^{(\omega)}}$ является конгруэнцией с классами $S_\mu^{(\omega)}$, $\mu = 0, \dots, \omega - 1$. Если $x \in S_\mu^{(\omega)}$, $y \in S_\nu^{(\omega)}$, то из определений следует, что $x \cdot y \in S_{\mu+\nu \pmod{\omega}}^{(\omega)}$. Таким образом, фактор-полугруппа $S / \rho^{S_0^{(\omega)}}$ изоморфна циклической группе порядка ω , а класс $S_0^{(\omega)}$ является полным прообразом единицы, т. е. нормальной подполугруппой полугруппы S . Максимальность

конгруэнции $\rho^{s_0^{(\omega)}}$ следует из единственности конгруэнции, нормально допускающей подполугруппу, фактор по которой есть группа. Первые три утверждения теоремы доказаны. Справедливость четвёртого утверждения следует непосредственно из определений. Наконец, если $e \in E(S)$, то из равенства $e^c = e$, верном при любом целом c , заключаем, что $c \cdot \mu_e \equiv \mu_e \pmod{\omega}$, откуда следует справедливость пятого утверждения. Теорема доказана.

Пусть числа $\omega_1, \dots, \omega_k$ — некоторые попарно различные собственные делители индекса $\omega_{K(S)}$ и $\omega = \text{НОК}(\omega_1, \dots, \omega_k)$. Тогда, как следует из определений, $\rho^{s_0^{(\omega)}} = \rho^{s_0^{(\omega_1)}} \cap \dots \cap \rho^{s_0^{(\omega_k)}}$. Поэтому конгруэнция $\rho^{s_0^{(\omega_{K(S)})}}$ тогда и только тогда является максимальным элементом в частично упорядоченном множестве конгруэнций θ со свойством: фактор S / θ — циклическая группа, когда $\omega_{K(S)}$ — простое число.

Аналогично предыдущему устанавливается, что верно утверждение, обратное в некотором смысле теореме 6.

Теорема 10. Пусть θ — конгруэнция на полугруппе S , для которой фактор S / θ изоморфен циклической группе порядка ω . Тогда полный прообраз любого порождающего элемента циклической группы будет порождающим множеством полугруппы S , и циклический индекс полугруппы относительно такого порождающего множества равен ω .

Вопрос о множестве всех циклических факторов полугруппы S сводится к вопросу о циклических факторах некоторой группы.

Известно следующее утверждение [8]. Пусть S — полугруппа с идеалом I и $\theta: I \rightarrow T$ — гомоморфизм I на полугруппу с единицей T . Тогда существует единственное расширение φ эпиморфизма θ на S .

Используя это утверждение и тот очевидный факт, что эпиморфизм отображает ядро полугруппы на ядро её образа, заключаем, что групповые образы полугруппы совпадают с групповыми образами её минимального идеала $K(S)$. Полугруппа $K(S)$ является простой и изоморфна рисовской полугруппе матричного типа [4], которую обозначим $M(G, I, \Lambda, P)$. Здесь G — структурная группа, I, Λ — конечные множества, $P = (p_{\lambda i})$ — сэндвич-матрица, элементы которой принадлежат группе G , каждый элемент рисовской полугруппы записывается в виде (a, i, λ) , где $a \in G, i \in I, \lambda \in \Lambda$. Операция в рисовской полугруппе задаётся следующим образом: $(a, i, \lambda) \cdot (b, j, \mu) = (a \cdot p_{\lambda j} \cdot b, i, \mu)$.

Пусть теперь γ — гомоморфизм структурной группы G в некоторую группу G' с единицей e' , удовлетворяющий условию $\gamma(p_{\lambda i}) = e'$ для всех $i \in I, \lambda \in \Lambda$. Тогда равенство $\theta(a, i, \lambda) = \gamma(a)$ определяет гомоморфизм θ полугруппы $K(S)$ в G' . Равенство $\varphi(s) = \theta(e \cdot s \cdot e)$, где $s \in S$, а e — произволь-

ный идемпотент из $K(S)$, определяет гомоморфизм полугруппы S в группу G' , и каждый гомоморфизм S в G' получается указанным способом.

Пусть N_G — нормальный делитель группы G , порождённый элементами матрицы P . Группа G / N_G является максимальным групповым образом полугруппы S [4, с. 150]. Поэтому циклические факторы полугруппы S совпадают с циклическими факторами группы G / N_G .

Список литературы

1. Глухов М. М. О числовых параметрах, связанных с заданием конечных групп системами образующих элементов. — В сб.: Труды по дискретной математике. Т. 1. — М.: ТВП, 1997, с. 43–66.
2. Смирнов В. Г. Слои конечного автомата. — Математические вопросы криптографии, 2011, т. 2, вып. 1, с. 97–118.
3. Лаллеман Ж. Полугруппы и комбинаторные приложения. — М.: «Мир», 1985.
4. Клиффорд А., Престон Г. Алгебраическая теория полугрупп. Т. 1. — М.: «Мир», 1972.
5. Клиффорд А., Престон Г. Алгебраическая теория полугрупп. Т. 2. — М.: «Мир», 1972.
6. Ляпин Е. С. Полугруппы. — М.: Физматлит, 1960.
7. Магнус В., Каррас А., Солитэр Д. Комбинаторная теория групп. — М.: Наука, 1974.
8. Крон К., Роудз Дж., Тилсон Б. Р. Гомоморфизмы и полулокальная теория. — В сб.: Алгебраическая теория автоматов, языков и полугрупп. — М.: Статистика, 1975, с. 190–226.