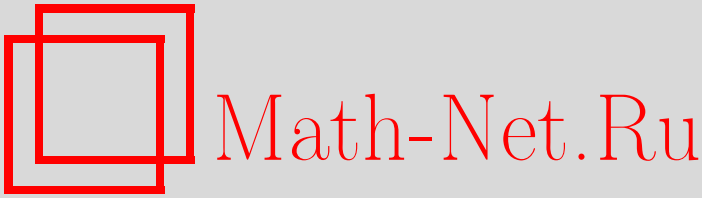

Math-Net.Ru
All Russian mathematical portal

V. L. Kurakin, Free shift registers. IV, *Mat. Vopr. Kriptogr.*, 2010, Volume 1, Issue 2, 57–92

DOI: 10.4213/mvk10

Use of the all-Russian mathematical portal Math-Net.Ru implies that you have read and agreed to these terms of use
http://www.mathnet.ru/eng/agreement

Download details:
IP: 3.239.97.34
November 10, 2024, 14:41:38

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2010 Т. 1 № 2 С. 57–92

УДК: 512.53, 519.113.6

Свободные регистры сдвига. IV

В. Л. Куракин

Российский государственный социальный университет, Москва

Получено 22.IV.2010

Исследуются полугруппы и группы вектор-периодов регистров сдвига на свободной полугруппе. Описаны свойства этих полугрупп. Разработан метод нахождения периода регулярного регистра сдвига, основанный на вычислении индекса его группы вектор-периодов. Определяются свободные регистры сдвига максимального периода и указаны условия их существования. Вводится и исследуется понятие наименьшего моноида регистра сдвига.

Ключевые слова: свободные полугруппы, регистр сдвига, максимальный период

Free shift registers. IV

V. L. Kurakin

Russian State Social University, Moscow

Abstract. Semigroups and groups of vectorial periods of a shift register over the free semigroup are considered. We suggest a method of derivation of a regular shift register period based on the computation of the index of vectorial periods group. Maximal period free shift registers are defined and conditions of their existence are found. A notion of minimal shift register monoid is introduced and investigated.

Key words: free semigroup, shift register, maximal period

Citation: *Mathematical Aspects of Cryptography*, 2010, vol. 1, no. 2, pp. 57–92 (Russian).

© 2010 В. Л. Куракин

В этой работе продолжается исследование регистров сдвига и периодических функций на свободной полугруппе, начатое в [1–4]. Данная четвертая часть работы является непосредственным продолжением первых трех частей [1–3], при этом продолжается нумерация параграфов, теорем, утверждений и формул.

Напомним, что в [1] было введено понятие свободного регистра сдвига, т. е. регистра, заданного на свободной полугруппе $X^* = [x_1, \ldots, x_k\rangle$. Это понятие обобщает известное понятие k-мерного регистра сдвига, который задается на свободной коммутативной полугруппе $\mathbb{N}_0^k$. С точки зрения приложений это расширяет класс многомерных регистров сдвига на случай, когда используемые в регистре преобразования сдвига не обязательно перестановочны друг с другом. С помощью свободного регистра сдвига можно реализовать k-канальную линию задержки (см. [1, пример 6.7]), которая давно используется для генерирования псевдослучайных последовательностей. Выходом свободного регистра является функция на свободной полугруппе, имеющая вид $u\colon X^* \to M$ и принимающая значения в некотором множестве M. Были определены и исследованы рекуррентные и периодические слева и справа функции на свободной полугруппе. Доказано, что функция периодична слева тогда и только тогда, когда она периодична справа. Исследовалось понятие периодичности по направлению.

В [2] было определено понятие регулярного регистра сдвига и доказан критерий регулярности. Исследовались чисто периодические и равномерно чисто периодические функции, определено понятие периода функции. Если функция u является выходом свободного регистра сдвига, заданного на диаграмме Ферре мощности n, то период функции u не превосходит $|M|^n$. Доказано существование рекуррентных функций максимального периода, которые по методу их построения можно назвать многомерными аналогами последовательностей де Брейна. Построена теоретико-автоматная модель свободного регистра сдвига.

В [3] изучены полугруппы (левых и правых) вектор-периодов и чистых вектор-периодов функций, заданных на полугруппе, и доказаны соотношения между полугруппами вектор-периодов. Согласно [2] каждая реверсивная периодическая справа функция u, заданная на полугруппе X^*, однозначно продолжается до периодической справа функции U, заданной на свободной группе $\langle X\rangle = \langle x_1, \ldots, x_k\rangle$, причем правые периоды этих функций совпадают: $T_r(u) = T_r(U)$. Это позволяет искать период реверсивной функции u как индекс группы чистых правых вектор-периодов функции U в свободной группе:

$$T_r(u) = T_r(U) = |\langle X\rangle \colon \hat{Q}_r(U)|,$$

причем оказывается, что $\hat{Q}_r(U)$ есть группа, порожденная полугруппой чистых правых вектор-периодов функции u:

$$\hat{Q}_r(U) = \langle Q_r(u) \rangle.$$

Как известно, подгруппу свободной группы можно задать в виде графа. Ряд примеров нахождения левых и правых периодов функций с использованием понятия фундаментальной группы графа приводится в [4].

В данной работе определяются полугруппы (левых и правых) вектор-периодов и чистых вектор-периодов регистров сдвига. Описаны свойства этих полугрупп и взаимосвязи между ними, аналогичные свойствам полугрупп вектор-периодов функций. Дается определение периода свободного регистра сдвига и доказывается, что для регулярного регистра сдвига период любой его выходной функции делит период регистра. Доказывается, что правый период регулярного регистра сдвига равен индексу группы его правых вектор-периодов:

$$T_r(\mathcal{F}, \Phi) = |\langle X \rangle : \hat{Q}_r(\mathcal{F}, \Phi)|.$$

Период свободного регистра сдвига, заданного на диаграмме Ферре мощности n, не превосходит величины $(|M|^n)!$. Показывается, что правый регистр имеет максимальный период тогда и только тогда, когда его отображения сдвига порождают всю симметрическую группу $S(M^n)$. Любой выход u такого регистра есть функция максимального правого периода, т. е. $T_r(u) = |M|^n$. При условии, что $|M|$ — степень двойки, доказывается теорема о существовании регистра сдвига максимального периода. Для этого строится ориентированный граф де Брейна и используется теорема Погорелова [7] о том, что примитивная группа подстановок $G < S_n$, где n — степень двойки, содержащая полный цикл, есть S_n или $\mathrm{PGL}(2, \mathbb{Z}_p)$.

В последнем параграфе работы вводится понятие наименьшего моноида функции, позволяющее сопоставить функции некоторый эпиморфизм полугрупп, обладающий свойством универсальности (в смысле теории категорий). Например, наименьшим моноидом обычной последовательности периода t и длины подхода l будет конечная полугруппа $[x\rangle$ порядка $l + t$ с образующим x, удовлетворяющим определяющему соотношению $x^l = x^{l+t}$. Наименьший моноид реверсивной периодической функции u является конечной группой, вкладывающейся в группу $S_m^{op} \times S_n$, где m и n — левый и правый периоды функции u. Показывается, что понятие наименьшего моноида функции позволяет изучать группы ее вектор-периодов. Рассматривается также понятие наименьшего моноида регистра сдвига. Доказано, что наименьший моноид правого регистра сдвига изоморфен полу-

группе этого регистра, т. е. полугруппе, порожденной его преобразованиями сдвига. В этом же параграфе дается определение рекуррентной функции и регистра сдвига на произвольной (не свободной) конечно порожденной полугруппе.

Отметим, что все перечисленные результаты получены для регистров сдвига, не являющихся линейными. Разработка теории линейных свободных регистров сдвига является открытой задачей.

Прежде чем перейти к изложению результатов, напомним основные определения из [1–3].

Пусть $X = \{x_1, \ldots, x_k\}$ — конечное множество (алфавит),

$$X^* = [x_1, \ldots, x_k\rangle = \bigcup_{n\geq 0} X^n$$

— свободная полугруппа слов над алфавитом X, M — некоторое множество, возможно бесконечное. Произвольная функция $u\colon X^* \to M$ рассматривается как аналог k-последовательности (т. е. функции $u\colon \mathbb{N}_0^k \to M$). По аналогии с k-последовательностями [9] мы рассматриваем понятия рекуррентной, реверсивной, периодической функции и др. Так как функция u задана на некоммутативной полугруппе, то эти понятия являются односторонними, например, мы различаем рекуррентные слева и справа функции. Множество всех функций $u\colon X^* \to M$ обозначим через M^{X^*}.

Будем считать, что на множестве X^* задано полное упорядочение $<$ слов, например, лексикографическое. Если $T = \{\overline{t}_1, \ldots, \overline{t}_n\}$, $\overline{t}_1 < \ldots < \overline{t}_n$, — произвольное конечное подмножество в X^*, то ограничение $u|_T$ функции u на множество T мы отождествляем с вектором $u[T] = (u(\overline{t}_1), \ldots, u(\overline{t}_n)) \in M^n$ и называем диаграммой значений функции u на множестве T. Левым и правым сдвигом множества $T \subset X^*$ на вектор $\overline{x} \in X^*$ называются соответственно множества

$$\overline{x}T = \{\overline{x}\overline{t}\colon \overline{t} \in T\} \quad \text{и} \quad T\overline{x} = \{\overline{t}\overline{x}\colon \overline{t} \in T\}.$$

Левым и правым сдвигом функции $u \in M^{X^*}$ на вектор $\overline{x} \in X^*$ называются соответственно функции $\overline{x}u$, $u\overline{x} \in M^{X^*}$, определяемые равенствами

$$(\overline{x}u)(\overline{z}) = u(\overline{z}\overline{x}), \quad (u\overline{x})(\overline{z}) = u(\overline{x}\overline{z}), \quad \overline{z} \in X^*.$$

Непустое подмножество $\mathcal{F} \subset X^*$ назовем правой диаграммой Ферре, если

$$\forall \overline{x}, \overline{y} \in X^* \quad \overline{x}\overline{y} \in \mathcal{F} \;\Rightarrow\; \overline{y} \in \mathcal{F}.$$

Левой границей множества $T \subset X^*$ в направлении $s \in \{1, \ldots, k\}$ называется множество $\partial_s T = x_s T \setminus T$. Левая граница множества T определяется равенством

$$\partial T = \bigcup_{s=1}^{k} \partial_s T.$$

Правым регистром сдвига на правой диаграмме Ферре $\mathcal{F}$ называется пара $(\mathcal{F}, \Phi)$, где $\Phi\colon M^{\mathcal{F}} \to M^{\partial\mathcal{F}}$ — произвольное отображение. Отображение Φ называется отображением граничного сдвига (а также функцией обратной связи, законом рекурсии).

Для правого регистра сдвига $(\mathcal{F}, \Phi)$ положим $r = |\partial\mathcal{F}|$, $\partial\mathcal{F} = \{\overline{z}_1, \ldots, \overline{z}_r\}$ и запишем отображение $\Phi\colon M^{\mathcal{F}} \to M^{\partial\mathcal{F}}$ через координатные функции:

$$\Phi = (\phi_1, \ldots, \phi_r) = (\phi_i, i \in \{1, \ldots, r\}), \quad \text{где } \phi_i\colon M^{\mathcal{F}} \to M.$$

Отображением граничного сдвига в направлении s называется отображение

$$\Phi_s = (\phi_i,\ \overline{z}_i \in \partial_s\mathcal{F})\colon M^{\mathcal{F}} \to M^{\partial_s\mathcal{F}}, \quad s \in \{1, \ldots, k\}.$$

Отображение $\Psi_s\colon M^{\mathcal{F}} \to M^{\mathcal{F}}$, определяемое следующим образом: $\Psi_s(u[\mathcal{F}]) = v[\mathcal{F}]$, где для $\overline{x} \in \mathcal{F}$

$$v(\overline{x}) = \begin{cases} u(x_s\overline{x}), & \text{если } x_s\overline{x} \in \mathcal{F}, \\ \phi_i(u[\mathcal{F}]), & \text{если } x_s\overline{x} = \overline{z}_i \in \partial_s\mathcal{F}, \end{cases}$$

называется отображением сдвига в направлении s ($s \in \{1, \ldots, k\}$).

Функция $u\colon X^* \to M$ называется выходом правого регистра сдвига $(\mathcal{F}, \Phi)$, если выполняются следующие равносильные условия: для любого слова $\overline{x} \in X^*$

$$\begin{aligned} &u[\overline{x} \cdot \partial\mathcal{F}] = \Phi(u[\overline{x}\mathcal{F}]), \\ &u[\overline{x} \cdot \partial_s\mathcal{F}] = \Phi_s(u[\overline{x}\mathcal{F}]),\ s \in \{1, \ldots, k\}, \\ &u[\overline{x}x_s\mathcal{F}] = \Psi_s(u[\overline{x}\mathcal{F}]), \quad s \in \{1, \ldots, k\}. \end{aligned} \tag{1}$$

При этом мы пишем $u \in (\mathcal{F}, \Phi)$ и называем $u[\mathcal{F}]$ диаграммой начальных значений функции u. Функция $u\colon X^* \to M$ называется правой рекуррентной функцией, если она является выходом некоторого правого регистра сдвига.

По теореме 5.3 если $(\mathcal{F}, \Phi)$ — правый регистр сдвига, то для любой диаграммы значений $u_0[\mathcal{F}] \in M^{\mathcal{F}}$ существует единственный выход $u\colon X^* \to M$

регистра сдвига $(\mathcal{F}, \Phi)$ такой, что $u[\mathcal{F}] = u_0[\mathcal{F}]$. В частности, если множество M конечно, то выходами регистра сдвига $(\mathcal{F}, \Phi)$ являются в точности $|M|^{|\mathcal{F}|}$ функций.

Функция u называется периодической слева, если множество $X^*u = \{\overline{x}u : \overline{x} \in X^*\}$ всех ее левых сдвигов конечно, и периодической справа — если множество uX^* всех ее правых сдвигов конечно. В теореме 7.8 доказано, что функция $u : X^* \to M$ периодична слева тогда и только тогда, когда она периодична справа. Поэтому корректно использовать термин «периодическая функция». Любая периодическая функция рекуррентна слева и справа (утверждения 7.4 и 7.5); если множество M конечно, то верно и обратное (теорема 7.7).

Обозначим через $\langle X \rangle$ свободную группу ранга k, порожденную множеством свободных образующих $X = \{x_1, \ldots, x_k\}$:

$$\langle X \rangle = \langle x_1, \ldots, x_k \rangle.$$

Функцию $U : \langle X \rangle \to M$ назовем продолжением функции $u : X^* \to M$, если $U|_{X^*} = u$. При $k = 1$ функция $U : \langle X \rangle \to M$ есть бипоследовательность, т. е. функция $U : \mathbb{Z} \to M$. В дальнейшем через u обозначается функция $u : X^* \to M$, а через U — функция $U : \langle X \rangle \to M$.

Для функций U аналогично вводятся понятия левого и правого сдвигов $\overline{x}U$ и $U\overline{x}$, $\overline{x} \in \langle X \rangle$, периодичности слева и справа и доказывается, что U периодична слева тогда и только тогда, когда она периодична справа (теорема 9.6). Функцию U называем выходом правого регистра сдвига $(\mathcal{F}, \Phi)$, если для любого $\overline{x} \in \langle X \rangle$ выполняются равносильные условия, аналогичные условиям (1), в которых u нужно заменить на U. При этом мы пишем $U \in (\mathcal{F}, \Phi)$.

Пусть $(\mathcal{F}, \Phi)$ — правый или левый регистр сдвига и $\Psi_s : M^{\mathcal{F}} \to M^{\mathcal{F}}$ — его отображения сдвига в направлении s ($s \in \{1, \ldots, k\}$). Регистр сдвига $(\mathcal{F}, \Phi)$ назовем регулярным (или реверсивным), если отображения Ψ_s, $s \in \{1, \ldots, k\}$, биективны. При $k = 1$ данное определение совпадает со стандартным определением регулярности для традиционного регистра сдвига, а в коммутативном случае — с определением регулярного k-регистра сдвига [6, 9].

Функцию $u : X^* \to M$ будем называть реверсивной справа, если u является выходом некоторого регулярного правого регистра сдвига. Если $(\mathcal{F}, \Phi)$ — регулярный правый регистр сдвига, то для любой функции $u \in (\mathcal{F}, \Phi)$ существует единственная функция $U \in (\mathcal{F}, \Phi)$ такая, что $U|_{X^*} = u$ (следствие 1 теоремы 10.4).

Напомним, что k-последовательность $u\colon \mathbb{N}_0^k \to M$ называется чисто периодической, если

$$\forall\, \boldsymbol{i} \in \mathbb{N}_0^k \quad \exists \boldsymbol{j} \in \mathbb{N}_0^k\colon \boldsymbol{x}^{\boldsymbol{j}}(\boldsymbol{x}^{\boldsymbol{i}}u) = u.$$

Функцию $u\colon X^* \to M$ будем называть чисто периодической справа, если она периодична справа и

$$\forall \overline{x}\ \exists \overline{y} \quad u\overline{xy} = u.$$

Если функция u периодична справа, то существует ее правый сдвиг, который чисто периодичен справа (теорема 12.2).

Правым периодом $T_r(u)$ периодической справа функции u назовем число ее правых сдвигов, являющихся чисто периодическими справа функциями. Правой длиной подхода $\Lambda_r(u)$ функции u назовем число правых сдвигов функции u, не являющихся чисто периодическими справа функциями. Таким образом,

$$\Lambda_r(u) + T_r(u) = |uX^*|, \quad \Lambda_r(u) \geq 0, \quad T_r(u) \geq 1.$$

Периодическая справа функция u чисто периодична справа тогда и только тогда, когда $T_r(u) = |uX^*|$, т. е. $\Lambda_r(u) = 0$.

Если множество M конечно и функция u является выходом правого регистра сдвига $(\mathcal{F}, \Phi)$, то функция u периодична справа и

$$\Lambda_r(u) + T_r(u) \leq |M|^{|\mathcal{F}|}$$

(утверждение 12.4). Функцию u будем называть функцией максимального правого периода, если u является выходом правого регистра сдвига $(\mathcal{F}, \Phi)$ над конечным множеством M и имеет правый период $T_r(u) = |M|^{|\mathcal{F}|}$. В теореме 12.5 доказано, что для любого конечного множества M и любой правой диаграммы Ферре $\mathcal{F}$ существует функция максимального правого периода над M и $\mathcal{F}$. Среди диаграмм значений $u[\overline{x}\mathcal{F}]$ такой функции u при всевозможных $\overline{x} \in X^*$ появляется любая диаграмма значений из $M^{\mathcal{F}}$ (эффект окна).

Для функций $U\colon \langle X\rangle \to M$ аналогично вводится понятие чистой периодичности. Правым периодом $T_r(U)$ периодической функции U назовем число ее правых сдвигов $U\overline{x}$, $\overline{x} \in \langle X\rangle$, являющихся чисто периодическими справа функциями. Правой длиной подхода $\Lambda_r(U)$ функции U назовем число правых сдвигов функции U, не являющихся чисто периодическими справа функциями. По теореме 13.1 периодическая функция U всегда чисто периодична слева и справа,

$$\Lambda_r(U) = 0, \qquad T_r(U) = |U \cdot \langle X\rangle| = |UX^*|;$$

если при этом $u = U|_{X^*}$, то функция u равномерно чисто периодична слева и справа и $T_r(u) = T_r(U)$.

21. Вектор-периоды регистров сдвига

Пусть $S \subset M^{X^*}$ — произвольное подмножество функций $u\colon X^* \to M$. Обозначим через $P_r(S)$ и $Q_r(S)$ множества всех правых и всех чистых правых вектор-периодов множества S соответственно:

$$P_r(S) = \{\overline{t} \in X^*\colon \exists n \in \mathbb{N}_0 \ \ \forall \overline{z} \in X^{]n[} \ \ \forall u \in S \quad u\overline{z}\overline{t} = u\overline{z}\},$$
$$Q_r(S) = \{\overline{t} \in X^*\colon \forall u \in S \quad u\overline{t} = u\}$$

(где $X^{]n[} = X^n \cup X^{n+1} \cup \ldots$ — множество всех слов длины, не меньшей n в алфавите X). Множества $P_l(S)$ и $Q_l(S)$ всех левых и всех чистых левых вектор-периодов множества S определяются аналогично и обладают аналогичными свойствами, поэтому мы часто их не приводим. Если $S = \{u\}$, то $P_r(\{u\}) = P_r(u)$ и $Q_r(\{u\}) = Q_r(u)$, так что новые обозначения согласованы с использовавшимися ранее в § 18 для полугрупп вектор-периодов и чистых вектор-периодов функции u.

Утверждение 21.1. *Справедливы соотношения*

$$\begin{aligned} &P_r(S) \lhd X^*, && Q_r(S) < X^*,\\ &P_r(X^*S) = P_r(S), && Q_r(X^*S) = Q_r(S),\\ &P_r(SX^*) \supset Q_r(SX^*), && Q_r(SX^*) = Q_l(X^*S),\\ &P_r(S) \subset \bigcap_{u\in S} P_r(u), && Q_r(S) = \bigcap_{u\in S} Q_r(u). \end{aligned} \tag{21.1}$$

Если множество S конечно, то включение в (21.1) *обращается в равенство.*

Доказательство. Соотношения $P_r(S) \lhd X^*$ и $Q_r(S) < X^*$ доказываются так же, как в утверждении 18.1(а). Следующие три соотношения следуют из определений. Докажем, что $Q_r(SX^*) = Q_l(X^*S)$. Если $\overline{t} \in Q_r(SX^*)$, то $u\overline{z}\overline{t}(\overline{x}) = u\overline{z}(\overline{x})$ для любых $\overline{z}, \overline{x} \in X^*$, откуда

$$\overline{t}\overline{x}u(\overline{z}) = u(\overline{z}\overline{t}\overline{x}) = u\overline{z}\overline{t}(\overline{x}) = u\overline{z}(\overline{x}) = u(\overline{z}\overline{x}) = \overline{x}u(\overline{z}).$$

Следовательно, $\overline{t}\overline{x}u = \overline{x}u$, т. е. $\overline{t} \in Q_l(X^*S)$. Таким образом, $Q_r(SX^*) \subset$ $\subset Q_l(X^*S)$. Обратное включение доказывается аналогично.

Соотношения (21.1) очевидны. Пусть S конечно и $\overline{t} \in \bigcap_{u\in S} P_r(u)$. Тогда

$$\forall u \in S \ \exists n = n(u) \ \forall \overline{z} \in X^{]n(u)[} \quad u\overline{z}\overline{t} = u\overline{z}.$$

Так как S конечно, то можно найти $n = \max\{n(u)\colon u \in S\}$. Для этого n имеем:

$$\forall \overline{z} \in X^{]n[} \ \forall u \in S \quad u\overline{z}\overline{t} = u\overline{z}.$$

Следовательно, $\overline{t} \in P_r(S)$. Таким образом, включение в соотношении (21.1) обращается в равенство. Утверждение доказано.

Определение 21.1. Пусть $S = (\mathcal{F}, \Phi)$ — множество всех выходов регистра сдвига $(\mathcal{F}, \Phi)$. Полугруппы правых и чистых правых вектор-периодов множества S будем называть *полугруппами правых* и *чистых правых вектор-периодов регистра сдвига* $(\mathcal{F}, \Phi)$ и обозначать их $P_r(\mathcal{F}, \Phi)$ и $Q_r(\mathcal{F}, \Phi)$ соответственно.

Произвольный элемент полугруппы $P_r(\mathcal{F}, \Phi)$ (соответственно $Q_r(\mathcal{F}, \Phi)$) назовем (*чистым*) *правым вектор-периодом регистра сдвига* $(\mathcal{F}, \Phi)$.

Аналогично определяются полугруппы $P_l(\mathcal{F}, \Phi)$ и $Q_l(\mathcal{F}, \Phi)$.

В данном определении регистр сдвига $(\mathcal{F}, \Phi)$ может быть как левым, так и правым. Однако так как правый сдвиг $\overline{x}u$ выхода u левого регистра сдвига может не быть выходом того же регистра сдвига, то для левого регистра сдвига имеет смысл рассматривать левые вектор-периоды, а для правого регистра сдвига — правые вектор-периоды.

Утверждение 21.2. *Пусть $(\mathcal{F}, \Phi)$ — произвольный правый регистр сдвига, $\Psi_{\overline{x}}$, $\overline{x} \in X^*$, — его отображения сдвига. Тогда*

$$P_r(\mathcal{F}, \Phi) = \{\overline{t} \in X^* \colon \exists n \in \mathbb{N}_0 \ \ \forall \overline{z} \in X^{]n[} \quad \Psi_{\overline{z}\overline{t}} = \Psi_{\overline{z}}\},$$
$$Q_r(\mathcal{F}, \Phi) = \{\overline{t} \in X^* \colon \Psi_{\overline{t}} = \epsilon\}.$$

Справедливо включение $Q_r(\mathcal{F}, \Phi) \subset P_r(\mathcal{F}, \Phi)$. Если регистр сдвига регулярен, то это включение обращается в равенство.

Доказательство. Пусть $u \in (\mathcal{F}, \Phi)$ и $\overline{x}, \overline{y} \in X^*$. Из утверждения 5.2 следует, что $u\overline{x}, u\overline{y} \in (\mathcal{F}, \Phi)$, и ввиду теоремы 5.3 условие $u\overline{x} = u\overline{y}$ равносильно условию $u\overline{x}[\mathcal{F}] = u\overline{y}[\mathcal{F}]$. Последнее равенство в силу утверждения 5.4 можно записать в виде $\Psi_{\overline{x}}(u[\mathcal{F}]) = \Psi_{\overline{y}}(u[\mathcal{F}])$. Если u пробегает все выходы регистра сдвига $(\mathcal{F}, \Phi)$, то $u[\mathcal{F}]$ пробегает все множество $M^{\mathcal{F}}$ в силу теоремы 5.3. Следовательно,

$$\forall u \in (\mathcal{F}, \Phi) \quad u\overline{x} = u\overline{y} \quad \Leftrightarrow \quad \Psi_{\overline{x}} = \Psi_{\overline{y}}.$$

Полагая здесь $\overline{x} = \overline{z}\overline{t}$, $\overline{y} = \overline{z}$, получим требуемое равенство для $P_r(\mathcal{F}, \Phi)$, а полагая $\overline{x} = \overline{t}$, $\overline{y} = \theta$, получим равенство для $Q_r(\mathcal{F}, \Phi)$.

Так как из равенства $\Psi_{\overline{t}} = \epsilon$ следует, что $\Psi_{\overline{z}\overline{t}} = \Psi_{\overline{z}}\Psi_{\overline{t}} = \Psi_{\overline{z}}$, то $Q_r(\mathcal{F}, \Phi) \subset P_r(\mathcal{F}, \Phi)$ (это включение следует также из утверждения 21.1). Если регистр сдвига регулярен, то отображение $\Psi_{\overline{z}}$ биективно и верно обратное включение. Утверждение доказано.

Следствие. *Для любого правого регистра сдвига* $(\mathcal{F}, \Phi)$ *и слов* $\overline{x}, \overline{y} \in X^*$ *условие* $\forall u \in (\mathcal{F}, \Phi)$ $u\overline{x} = u\overline{y}$ *равносильно тому, что* $\Psi_{\overline{x}} = \Psi_{\overline{y}}$.

Пусть теперь $S \subset M^{\langle X \rangle}$ — произвольное подмножество функций $U : \langle X \rangle \to M$. Обозначим через $\hat{P}_r(S)$ и $\hat{Q}_r(S)$ множества всех правых и всех чистых правых вектор-периодов множества S соответственно:

$$\hat{P}_r(S) = \{\overline{t} \in \langle X \rangle : \forall \overline{z} \in \langle X \rangle \ \ \forall U \in S \quad U\overline{z}\overline{t} = U\overline{z}\},$$
$$\hat{Q}_r(S) = \{\overline{t} \in \langle X \rangle : \forall U \in S \quad U\overline{t} = U\}.$$

Если $S = \{U\}$, то $\hat{P}_r(\{U\}) = \hat{P}_r(U)$ и $\hat{Q}_r(\{U\}) = \hat{Q}_r(U)$, поэтому новые обозначения согласованы с ранее использовавшимися в § 19.

Определение 21.2. Пусть S — множество всех выходов $U : \langle X \rangle \to M$ регистра сдвига $(\mathcal{F}, \Phi)$. Группы $\hat{P}_r(S)$ и $\hat{Q}_r(S)$ будем называть *группами правых* и *чистых правых вектор-периодов регистра сдвига* $(\mathcal{F}, \Phi)$ *в множестве* $\langle X \rangle$ и обозначать $\hat{P}_r(\mathcal{F}, \Phi)$ и $\hat{Q}_r(\mathcal{F}, \Phi)$ соответственно.

Группы $\hat{P}_l(\mathcal{F}, \Phi)$ и $\hat{Q}_l(\mathcal{F}, \Phi)$ определяются аналогично.

Напомним (см. § 19), что сердцевиной подгруппы H группы G называется пересечение $\operatorname{core} H = \bigcap_{g \in G} g^{-1} H g$ всех подгрупп, сопряженных с H. Группа $\operatorname{core} H$ является наибольшей нормальной подгруппой группы G, лежащей в H.

Утверждение 21.3. *Для любых* $S \subset M^{\langle X \rangle}$ *и* $\overline{x} \in \langle X \rangle$ *выполняются соотношения*

$$\hat{P}_r(S) \lhd \langle X \rangle, \quad \hat{Q}_r(S) < \langle X \rangle, \quad \hat{P}_r(S) \subset \hat{Q}_r(S),$$
$$\hat{P}_r(\langle X \rangle \cdot S) = \hat{P}_r(S \cdot \langle X \rangle) = \hat{P}_r(S),$$
$$\hat{Q}_r(\langle X \rangle \cdot S) = \hat{Q}_r(S), \qquad \hat{Q}_r(S\overline{x}) = \overline{x}^{-1} \hat{Q}_r(S) \overline{x},$$
$$\hat{Q}_r(S \cdot \langle X \rangle) = \hat{Q}_l(\langle X \rangle \cdot S) = \operatorname{core} \hat{Q}_r(S) = \operatorname{core} \hat{Q}_l(S) = \hat{P}_r(S) = \hat{P}_l(S).$$

Для любого правого регистра сдвига $(\mathcal{F}, \Phi)$

$$\hat{P}_r(\mathcal{F}, \Phi) = \hat{Q}_r(\mathcal{F}, \Phi) \lhd \langle X \rangle.$$

Доказательство. Из определения видно, что

$$\hat{P}_r(S) = \bigcap_{U \in S} \hat{P}_r(U), \qquad \hat{Q}_r(S) = \bigcap_{U \in S} \hat{Q}_r(U). \tag{21.2}$$

Поэтому соотношения $\hat{P}_r(S) \lhd \langle X\rangle$ и $\hat{Q}_r(S) < \langle X\rangle$ следуют из утверждения 19.1. Следующие четыре соотношения вытекают непосредственно из определений. Равенство $\hat{Q}_r(S\langle X\rangle) = \hat{Q}_l(\langle X\rangle S)$ проверяется по той же схеме, что и в утверждении 21.1. Из равенства $\hat{Q}_r(S\overline{x}) = \overline{x}^{-1}\hat{Q}_r(S)\overline{x}$ следует, что $\hat{Q}_r(S\langle X\rangle) = \operatorname{core}\hat{Q}_r(S)$. Непосредственно из определения вытекает, что $\hat{Q}_r(S\langle X\rangle) = \hat{P}_r(S)$. Аналогично $\hat{Q}_l(\langle X\rangle S) = \operatorname{core}\hat{Q}_l(S) = \hat{P}_l(S)$. Тем самым доказаны все требуемые соотношения.

Если $S = (\mathcal{F}, \Phi)$ — множество всех выходов правого регистра сдвига, то $S\langle X\rangle = S$, и в силу уже доказанного $\hat{P}_r(S) = \hat{Q}_r(S\langle X\rangle) = \hat{Q}_r(S)$. Конец доказательства.

Для (полу)групп вектор-периодов регистра сдвига можно рассматривать соотношения, аналогичные соотношениям (19.3)–(19.7). Перечислим их (предостережение: некоторые соотношения в общем случае могут быть неверными, пока мы лишь перечисляем то, что будет доказываться при дополнительных условиях):

$$P_r(\mathcal{F},\Phi) \subset \langle P_r(\mathcal{F},\Phi)\rangle \cap X^*, \qquad Q_r(\mathcal{F},\Phi) \subset \langle Q_r(\mathcal{F},\Phi)\rangle \cap X^*, \tag{21.3}$$

$$\hat{P}_r(\mathcal{F},\Phi) \supset \langle \hat{P}_r(\mathcal{F},\Phi) \cap X^*\rangle, \qquad \hat{Q}_r(\mathcal{F},\Phi) \supset \langle \hat{Q}_r(\mathcal{F},\Phi) \cap X^*\rangle, \tag{21.4}$$

$$P_r(\mathcal{F},\Phi) \supset \hat{P}_r(\mathcal{F},\Phi) \cap X^*, \qquad Q_r(\mathcal{F},\Phi) \supset \hat{Q}_r(\mathcal{F},\Phi) \cap X^*, \tag{21.5}$$

$$\hat{P}_r(\mathcal{F},\Phi) \supset \langle P_r(\mathcal{F},\Phi)\rangle, \qquad \hat{Q}_r(\mathcal{F},\Phi) \supset \langle Q_r(\mathcal{F},\Phi)\rangle, \tag{21.6}$$

$$P_r(\mathcal{F},\Phi) \supset Q_r(\mathcal{F},\Phi), \qquad \hat{P}_r(\mathcal{F},\Phi) = \hat{Q}_r(\mathcal{F},\Phi). \tag{21.7}$$

Обратим внимание на то, что по сравнению с включениями (19.7) в первом соотношении из (21.7) знак включения направлен в другую сторону.

Теорема 21.1. (1) *Пусть* $(\mathcal{F}, \Phi)$ *— произвольный правый регистр сдвига. Тогда справедливы соотношения* (21.3)*,* (21.4) *и* (21.7)*. Если выполняется хотя бы одно из условий*: *любой выход* $U \in (\mathcal{F}, \Phi)$ *периодичен, множество* M *конечно, регистр сдвига* $(\mathcal{F}, \Phi)$ *коммутативен или регулярен — то справедливы включения* (21.6)*. Если множество* M *конечно, то включения* (21.3) *обращаются в равенства.*

(2) *Пусть* $(\mathcal{F}, \Phi)$ *— регулярный правый регистр сдвига. Тогда справедливы все соотношения* (21.3)–(21.7)*, включения в* (21.3)*,* (21.5) *и* (21.7) *обращаются в равенства, и*

$$\hat{P}_r(\mathcal{F},\Phi) = \hat{Q}_r(\mathcal{F},\Phi) = \{\overline{t} \in \langle X\rangle :\ \Psi_{\overline{t}} = \epsilon\} \lhd \langle X\rangle. \tag{21.8}$$

Если при этом множество M *конечно, то все включения в* (21.3)–(21.7) *обращаются в равенства.*

Доказательство. (1) Включения (21.3) и (21.4) очевидны. Соотношения (21.7) доказаны в утверждениях 21.2 и 21.3.

В силу (21.7) для доказательства включений (21.6) достаточно убедиться в том, что

$$P_r(\mathcal{F},\Phi)\subset\hat{Q}_r(\mathcal{F},\Phi). \tag{21.9}$$

Вначале докажем это включение в предположении, что любой выход U регистра сдвига $(\mathcal{F},\Phi)$ периодичен. Пусть $\overline{t}\in P_r(\mathcal{F},\Phi)$. По утверждению 21.2 существует число $n\in\mathbb{N}_0$ такое, что $\Psi_{\overline{z}\overline{t}}=\Psi_{\overline{z}}$ для любого слова $\overline{z}\in X^*$ длины, не меньшей n. Возьмем произвольное слово $\overline{y}\in X^*$ длины, не меньшей n. Если $U\in(\mathcal{F},\Phi)$, то функция U периодична, поэтому $U\overline{y}^m=U$ для некоторого $m\geq 1$ по лемме 9.3. По утверждению 9.4 существует отображение $\tau\colon\langle X\rangle\to X^*$ такое, что $U\overline{z}\overline{x}=U\overline{z}\tau(\overline{x})$ для любых $\overline{z},\overline{x}\in\langle X\rangle$. Тогда для любого $\overline{x}\in\langle X\rangle$

$$\begin{aligned}U\overline{t}[\overline{x}\mathcal{F}]&=U\overline{y}^m\overline{t}\overline{x}[\mathcal{F}]=U\overline{y}^m\overline{t}\tau(\overline{x})[\mathcal{F}]=U[\overline{y}^m\overline{t}\tau(\overline{x})\mathcal{F}]=\\&=\Psi_{\overline{y}^m\overline{t}\tau(\overline{x})}(U[\mathcal{F}])=\Psi_{\overline{y}^m\overline{t}}\Psi_{\tau(\overline{x})}(U[\mathcal{F}])=\Psi_{\overline{y}^m}\Psi_{\tau(\overline{x})}(U[\mathcal{F}])=\\&=U[\overline{y}^m\tau(\overline{x})\mathcal{F}]=U\overline{y}^m\tau(\overline{x})[\mathcal{F}]=U\tau(\overline{x})[\mathcal{F}]=U\overline{x}[\mathcal{F}]=U[\overline{x}\mathcal{F}]\end{aligned}$$

(мы используем отображение τ, так как не можем написать $\Psi_{\overline{x}}$ для $\overline{x}\notin X^*$). Следовательно, $U\overline{t}=U$, т. е. $\overline{t}\in\hat{Q}_r(\mathcal{F},\Phi)$, и включение (21.9) доказано.

Если множество M конечно, то по теореме 9.5 любая функция $U\in\in(\mathcal{F},\Phi)$ периодична, и включение (21.9) следует из уже доказанного.

Докажем включение (21.9) для коммутативного регистра сдвига. Мы не будем заменять X^* на $\mathbb{N}_0^k$, что привело бы к смене обозначений, а будем считать, что буквы алфавита X попарно перестановочны. Пусть $\overline{t}\in P_r(\mathcal{F},\Phi)$. По утверждению 21.2 существует такое число $n\in\mathbb{N}_0$, что $\Psi_{\overline{z}\overline{t}}=\Psi_{\overline{z}}$ для любого слова $\overline{z}\in X^*$ длины, не меньшей n. Зафиксируем произвольное слово $\overline{z}\in X^*$ длины, не меньшей n. Заметим, что для любого $U\in(\mathcal{F},\Phi)$ сдвиг $U\overline{z}^{-1}\in(\mathcal{F},\Phi)$. Тогда для любого $\overline{x}\in\langle X\rangle$

$$\begin{aligned}U\overline{t}[\overline{x}\mathcal{F}]&=U\overline{z}^{-1}\overline{z}\overline{t}\overline{x}[\mathcal{F}]=U\overline{z}^{-1}[\overline{z}\overline{t}\overline{x}\mathcal{F}]=U\overline{z}^{-1}[\overline{x}\overline{z}\overline{t}\mathcal{F}]=\\&=\Psi_{\overline{z}\overline{t}}(U\overline{z}^{-1}[\overline{x}\mathcal{F}])=\Psi_{\overline{z}}(U\overline{z}^{-1}[\overline{x}\mathcal{F}])=U\overline{z}^{-1}[\overline{x}\overline{z}\mathcal{F}]=\\&=U[\overline{z}^{-1}\overline{x}\overline{z}\mathcal{F}]=U[\overline{z}^{-1}\overline{z}\overline{x}\mathcal{F}]=U[\overline{x}\mathcal{F}].\end{aligned}$$

Следовательно, $U\overline{t}=U$, т. е. $\overline{t}\in Q_r(\mathcal{F},\Phi)$, и включение (21.9) доказано.

Докажем, что если множество M конечно, то включения (21.3) обращаются в равенства. Сначала рассмотрим второе включение в (21.3). Согласно утверждению 18.4 достаточно проверить условие (18.9):

$$\forall\overline{a},\overline{b},\overline{x},\overline{y}\in X^*\quad\overline{xa},\overline{ba},\overline{by}\in Q_r(\mathcal{F},\Phi)\quad\Rightarrow\quad\overline{xy}\in Q_r(\mathcal{F},\Phi). \tag{21.10}$$

Действительно, так как $\overline{b}\overline{a} \in Q_r(\mathcal{F}, \Phi)$, то $\Psi_{\overline{b}\overline{a}} = \Psi_{\overline{b}}\Psi_{\overline{a}} = \epsilon$. Так как множество M конечно, отсюда следует, что отображения $\Psi_{\overline{b}}$ и $\Psi_{\overline{a}}$ обратимы, поэтому $\Psi_{\overline{b}} = \Psi_{\overline{a}}^{-1}$ и $\Psi_{\overline{a}}\Psi_{\overline{b}} = \epsilon$. Следовательно,

$$\Psi_{\overline{xy}} = \Psi_{\overline{x}}\Psi_{\overline{y}} = \Psi_{\overline{x}}(\Psi_{\overline{a}}\Psi_{\overline{b}})\Psi_{\overline{y}} = (\Psi_{\overline{x}}\Psi_{\overline{a}})(\Psi_{\overline{b}}\Psi_{\overline{y}}) = \Psi_{\overline{xa}}\Psi_{\overline{b}\overline{y}} = \epsilon, \qquad (21.11)$$

т. е. $\overline{xy} \in Q_r(\mathcal{F}, \Phi)$. Таким образом, второе включение в (21.3) обращается в равенство.

Докажем теперь, что первое включение в (21.3) обращается в равенство. Нужно проверить условие (21.10) с заменой $Q_r(\mathcal{F}, \Phi)$ на $P_r(\mathcal{F}, \Phi)$. Как легко понять, для этого достаточно убедиться в том, что для любого $\overline{z} \in X^*$ из равенств

$$\Psi_{\overline{z}}\Psi_{\overline{xa}} = \Psi_{\overline{z}}, \quad \Psi_{\overline{z}}\Psi_{\overline{b}\overline{a}} = \Psi_{\overline{z}}, \quad \Psi_{\overline{z}}\Psi_{\overline{b}\overline{y}} = \Psi_{\overline{z}}$$

следует равенство $\Psi_{\overline{z}}\Psi_{\overline{xy}} = \Psi_{\overline{z}}$. Обозначим $K = \Im\Psi_{\overline{z}}$. Тогда K — конечное подмножество в $M^{\mathcal{F}}$, и приведенные три равенства эквивалентны тому, что отображения $\Psi_{\overline{xa}}$, $\Psi_{\overline{b}\overline{a}}$, $\Psi_{\overline{b}\overline{y}}$ отображают K в K и тождественны на K. Так как множество K конечно, отсюда следует, что отображения $\Psi_{\overline{b}}$ и $\Psi_{\overline{a}}$ биективны на K, поэтому $\Psi_{\overline{a}}\Psi_{\overline{b}} = \epsilon$ на K. Теперь так же, как в (21.11), проверяется, что $\Psi_{\overline{z}}\Psi_{\overline{xy}} = \Psi_{\overline{z}}$. Тем самым доказано, что первое включение в (21.3) обращается в равенство.

(2) Пусть теперь регистр сдвига регулярен. Докажем сначала равенства (21.8). Так как отображения сдвига Ψ_s, $s \in \{1, \ldots, k\}$, биективны, то для всех $\overline{x} \in \langle X \rangle$ определены отображения сдвига $\Psi_{\overline{x}}$, все они биективны, и

$$\forall U \in (\mathcal{F}, \Phi) \quad U[\overline{x}\mathcal{F}] = \Psi_{\overline{x}}(U[\mathcal{F}]), \quad \overline{x} \in \langle X \rangle.$$

Следовательно, условие $\overline{t} \in \hat{Q}_r(\mathcal{F}, \Phi)$ равносильно тому, что

$$\forall U \in (\mathcal{F}, \Phi) \quad \Psi_{\overline{t}}(U[\mathcal{F}]) = U[\mathcal{F}].$$

Так как по теореме 10.4 для любой диаграммы значений $v[\mathcal{F}] \in M^{\mathcal{F}}$ регулярный регистр сдвига $(\mathcal{F}, \Phi)$ имеет выход U такой, что $U[\mathcal{F}] = v[\mathcal{F}]$, то это условие равносильно тому, что $\Psi_{\overline{t}} = \epsilon$. С учетом второго равенства в (21.7) отсюда следуют равенства (21.8). То, что подгруппа $\hat{P}_r(\mathcal{F}, \Phi)$ нормальна, следует из утверждения 21.3.

Сравнивая равенства (21.8) с соотношениями из утверждения 21.2, получаем, что включения (21.5) обращаются в равенства.

По утверждению 21.2 первое включение в (21.7) обращается в равенство. Теперь с учетом (21.7) при доказательстве формул (21.3)–(21.6) для регулярного регистра сдвига достаточно проверять только второе соотношение в каждой формуле.

Докажем включения (21.6). Пусть $\overline{t} \in Q_r(\mathcal{F}, \Phi)$. Тогда $\Psi_{\overline{t}} = \epsilon$ и для любых $U \in (\mathcal{F}, \Phi)$ и $\overline{x} \in \langle X \rangle$

$$U\overline{t}[\overline{x}\mathcal{F}] = U[\overline{t}\overline{x}\mathcal{F}] = \Psi_{\overline{t}\overline{x}}(U[\mathcal{F}]) = \Psi_{\overline{t}}\Psi_{\overline{x}}(U[\mathcal{F}]) = \Psi_{\overline{x}}(U[\mathcal{F}]) = U[\overline{x}\mathcal{F}].$$

Следовательно, $U\overline{t} = U$, т. е. $\overline{t} \in \hat{Q}_r(\mathcal{F}, \Phi)$. Поэтому $Q_r(\mathcal{F}, \Phi) \subset \hat{Q}_r(\mathcal{F}, \Phi)$, что и требовалось доказать.

Докажем теперь, что включения (21.3) обращаются в равенства. Для этого достаточно проверить условие (21.10). Так как $\overline{b}\overline{a} \in Q_r(\mathcal{F}, \Phi)$, то $\Psi_{\overline{b}\overline{a}} = \Psi_{\overline{b}}\Psi_{\overline{a}} = \epsilon$. Ввиду регулярности регистра сдвига отображения $\Psi_{\overline{b}}$ и $\Psi_{\overline{a}}$ обратимы, поэтому $\Psi_{\overline{b}} = \Psi_{\overline{a}}^{-1}$ и $\Psi_{\overline{a}}\Psi_{\overline{b}} = \epsilon$. Тогда справедливы соотношения (21.11), из которых следует, что $\overline{xy} \in Q_r(\mathcal{F}, \Phi)$, т. е. условие (21.10) выполнено.

Пусть теперь множество M конечно. Нам остается доказать, что включения (21.4) и (21.6) обращаются в равенства. Так как включения (21.5) обращаются в равенства, то соотношения (21.4) и (21.6) совпадают. Поэтому достаточно проверить, что включения (21.6) обращаются в равенства. Пусть $u_1, \ldots, u_n$ — все выходы регистра сдвига $(\mathcal{F}, \Phi)$, где $n = |M^{\mathcal{F}}|$. По следствию теоремы 13.2 функции $u_1, \ldots, u_n$ равномерно чисто периодичны справа. В силу утверждения 13.1

$$\forall i \in \{1, \ldots, n\} \;\; \exists m_i \geq 1 \;\; \forall \overline{x}, \overline{z} \in X^* \quad u_i\overline{z}\overline{x}^{m_i} = u_i\overline{z}.$$

Взяв $m = [m_1, \ldots, m_n]$, получим, что $u\overline{z}\overline{x}^m = u\overline{z}$ для любых $u \in (\mathcal{F}, \Phi)$ и $\overline{x}, \overline{z} \in X^*$. Отсюда следует, что

$$\forall \overline{x} \in X^* \;\; \exists \overline{y} \in X^* \;\; \forall \overline{z} \in X^* \;\; \forall u \in (\mathcal{F}, \Phi) \quad u\overline{z}\overline{x}\overline{y} = u\overline{z}\overline{y}\overline{x} = u\overline{z} \qquad (21.12)$$

(достаточно взять $\overline{y} = \overline{x}^{m-1}$).

Теперь доказательство включения $\hat{P}_r(\mathcal{F}, \Phi) \subset \langle P_r(\mathcal{F}, \Phi) \rangle$ проводится по той же схеме, что и в теореме 19.4. Пусть $\overline{t} \in \hat{P}_r(\mathcal{F}, \Phi)$. Запишем слово $\overline{t}$ в виде

$$\overline{t} = \overline{x}_1\overline{x}_2^{-1}\overline{x}_3\overline{x}_4^{-1} \ldots \overline{x}_{n-1}\overline{x}_n^{-1}\overline{x}_{n+1}, \quad \text{где } \overline{x}_i \in X^*.$$

Ввиду (21.12) существует $\overline{y}_1 \in X^*$ такое, что для любых $\overline{z} \in X^*$ и $u \in (\mathcal{F}, \Phi)$ выполняется равенство $u\overline{z}\overline{x}_1\overline{y}_1 = u\overline{z}$. Тогда $\overline{t}_1 = \overline{x}_1\overline{y}_1 \in P_r(\mathcal{F}, \Phi)$ и

$$\overline{t} = \overline{t}_1\overline{y}_1^{-1}\overline{x}_2^{-1}\overline{x}_3\overline{x}_4^{-1} \ldots \overline{x}_{n-1}\overline{x}_n^{-1}\overline{x}_{n+1}.$$

Ввиду (21.12) существует $\overline{y}_2 \in X^*$ такое, что для любых $\overline{z} \in X^*$ и $u \in (\mathcal{F}, \Phi)$ выполняется равенство $u\overline{z}\overline{y}_2\overline{x}_2\overline{y}_1 = u\overline{z}$. Тогда $\overline{t}_2 = \overline{y}_2\overline{x}_2\overline{y}_1 \in P_r(\mathcal{F}, \Phi)$ и

$$\overline{t} = \overline{t}_1\overline{t}_2^{-1}\overline{y}_2\overline{x}_3\overline{x}_4^{-1} \ldots \overline{x}_{n-1}\overline{x}_n^{-1}\overline{x}_{n+1}.$$

Ввиду (21.12) существует $\overline{y}_3 \in X^*$ такое, что для любых $\overline{z} \in X^*$ и $u \in (\mathcal{F}, \Phi)$ выполняется равенство $u\overline{z}\overline{y}_2\overline{x}_3\overline{y}_3 = u\overline{z}$. Тогда $\overline{t}_3 = \overline{y}_2\overline{x}_3\overline{y}_3 \in P_r(\mathcal{F}, \Phi)$ и

$$\overline{t} = \overline{t}_1\overline{t}_2^{-1}\overline{t}_3\overline{y}_3^{-1}\overline{x}_4^{-1} \ldots \overline{x}_{n-1}\overline{x}_n^{-1}\overline{x}_{n+1}.$$

Рассуждая аналогично, получим, что

$$\overline{t} = \overline{t}_1\overline{t}_2^{-1}\overline{t}_3\overline{t}_4^{-1} \ldots \overline{t}_{n-1}\overline{t}_n^{-1}\overline{y}_n\overline{x}_{n+1}, \quad \overline{t}_i \in P_r(\mathcal{F}, \Phi),\ \overline{y}_n \in X^*.$$

Так как включения (21.5) обращаются в равенства, то $\overline{t}_i \in \hat{P}_r(\mathcal{F}, \Phi)$. Тогда для любого $U \in (\mathcal{F}, \Phi)$ и любого $\overline{z} \in \langle X \rangle$

$$U\overline{z} = U\overline{z}\overline{t} = U\overline{z}\overline{y}_n\overline{x}_{n+1}.$$

Следовательно, $\overline{y}_n\overline{x}_{n+1} \in \hat{P}_r(\mathcal{F}, \Phi) \cap X^* = P_r(\mathcal{F}, \Phi)$, и мы получаем, что $\overline{t} \in \langle P_r(\mathcal{F}, \Phi) \rangle$.

Таким образом, первое включение в (21.6) обращается в равенство.

Чтобы доказать, что второе включение в (21.6) обращается в равенство, достаточно в проведенных рассуждениях положить $\overline{z} = \theta$ и заменить $P_r(\mathcal{F}, \Phi)$, $\hat{P}_r(\mathcal{F}, \Phi)$ на $Q_r(\mathcal{F}, \Phi)$, $\hat{Q}_r(\mathcal{F}, \Phi)$ соответственно. Теорема доказана.

Из доказательства видно, что соотношение (21.12) остается справедливым и в случае, когда множество M бесконечно, но у регулярного правого регистра сдвига $(\mathcal{F}, \Phi)$ все отображения сдвига $\Psi_{\overline{x}}$, $\overline{x} \in X^*$, имеют конечные порядки, ограниченные в совокупности. Пример такого регистра сдвига приведен в доказательстве теоремы 8.2. В этом случае включения (21.4) и (21.6) обращаются в равенства.

Следствие. *Пусть $(\mathcal{F}, \Phi)$ — регулярный правый регистр сдвига, символы U, и означают произвольные выходы этого регистра, и пусть $\overline{x}, \overline{y} \in X^*$ — фиксированные слова. Тогда*

$$\forall u \quad u\overline{x} = u\overline{y} \quad \Leftrightarrow \quad \forall U \quad U\overline{x} = U\overline{y} \quad \Leftrightarrow \quad \Psi_{\overline{x}} = \Psi_{\overline{y}}.$$

Доказательство. По следствию утверждения 21.2 условие $\forall u\ u\overline{x} = u\overline{y}$ равносильно равенству $\Psi_{\overline{x}} = \Psi_{\overline{y}}$. Так же, как при выводе соотношения (21.8), получаем, что и условие $\forall U\ U\overline{x} = U\overline{y}$ равносильно равенству $\Psi_{\overline{x}} = \Psi_{\overline{y}}$.

Следующие примеры показывают, что включения (21.3) и первое включение в (21.7) могут быть строгими, а включения (21.5) и (21.6) в общем случае неверны.

ПРИМЕР 21.1. Покажем, что включения (21.3) могут быть строгими. Пусть $k = 4$, $X = \{x, y, a, b\}$, $M = \mathbb{N}$, $\mathcal{F} = \{\theta\}$. Рассмотрим правый регистр сдвига $(\mathcal{F}, \Phi)$ со следующими отображениями сдвига:

$$\Psi_x(n) = 2n,\ \Psi_b(n) = 2n-1,\ \Psi_a(n) = \left[\frac{n+1}{2}\right],\ \Psi_y(n) = \left[\frac{n+2}{2}\right],\ n \in \mathbb{N}.$$

Обозначим $P = P_r(\mathcal{F}, \Phi)$ и $Q = Q_r(\mathcal{F}, \Phi)$. Непосредственно проверяется, что $\Psi_x\Psi_a = \Psi_b\Psi_a = \Psi_b\Psi_y = \epsilon$ и $\Psi_x\Psi_y(n) = n+1$, поэтому $\Psi_x\Psi_y \neq \epsilon$. Более того, если $\overline{z} \in X^*$, то $\Psi_{\overline{z}xy}(n) = \Psi_{\overline{z}}(n) + 1$, поэтому $\Psi_{\overline{z}xy} \neq \Psi_{\overline{z}}$. В силу утверждения 21.2

$$xa, ba, by \in P, \quad xy \notin P, \qquad xa, ba, by \in Q, \quad xy \notin Q.$$

Поэтому $P \neq \langle P\rangle \cap X^*$ и $Q \neq \langle Q\rangle \cap X^*$ согласно утверждению 18.4. Таким образом, включения (21.3) строгие.

ПРИМЕР 21.2. В этом примере рассматриваются включения (21.5) и (21.7). Пусть $k = 1$, $M = \{0, 1\}$, $\mathcal{F} = \{\theta\}$ и отображение сдвига $\Psi\colon M \to M$ задано соотношениями $\Psi(1) = 0$, $\Psi(0) = 0$. Такой регистр сдвига $(\mathcal{F}, \Phi)$ рассматривался в примере 9.1. Он имеет два выхода $u = 0$ и $u = (1, 0, 0, \dots)$ и один выход $U = 0$. Поэтому $Q_r(\mathcal{F}, \Phi) = \theta$, $\hat{Q}_r(\mathcal{F}, \Phi) = \langle X\rangle$, и второе включение в (21.5) не выполняется (первое включение в (21.5) при этом выполняется). Так как $P_r(\mathcal{F}, \Phi) = X^*$, то для этого регистра сдвига первое включение в (21.7) строгое.

Пусть $k = 2$, $M = \{1, 2, 3\}$, $\mathcal{F} = \{\theta\}$ и отображения сдвига $\Psi_1, \Psi_2\colon M \to M$ правого регистра сдвига $(\mathcal{F}, \Phi)$ заданы следующим образом:

$$\Psi_1\colon\ 1 \to 2 \to 3 \to 3, \qquad \Psi_2\colon\ 2 \to 1 \to 3 \to 3.$$

Так как $L = \bigcap_{\overline{x} \in X^*} \Im\Psi_{\overline{x}} = \{3\}$, то по утверждению 9.2 выходом $U \in (\mathcal{F}, \Phi)$ является единственная функция: константа $U \equiv 3$. Поэтому $\hat{P}_r(\mathcal{F}, \Phi) = \langle X\rangle$. Рассмотрим теперь выход $u \in (\mathcal{F}, \Phi)$ с начальным значением $u(\theta) = 1$. Так как $u(x_1) = \Psi_1(1) = 2$, то $ux_1 \neq u$. Так как $u(x_1x_2) = \Psi_2(\Psi_1(1)) = 1$, то $ux_1x_2 = u$. Отсюда получаем, что $u(x_1x_2)^n x_1 \neq u$ для любого n. Следовательно, $x_1 \notin P_r(u)$ и значит, $x_1 \notin P_r(\mathcal{F}, \Phi)$. Таким образом, первое включение в (21.5) не выполняется.

Покажем, что первое включение в (21.5) может не выполняться при $k = 1$, если M бесконечно. Пусть $M = \bigcup_{i=1}^{\infty} M_i$, где $M_i = \{m_{i1}, m_{i2}, \dots, m_{ii}\}$. Рассмотрим традиционный регистр сдвига длины 1 (т. е. $\mathcal{F} = \{\theta\}$), у которого отображение сдвига $\Psi_1\colon M \to M$ задается соотношениями

$$\Psi_1\colon\ m_{i1} \to m_{i2} \to \dots \to m_{ii} \to m_{ii}, \quad i \geq 1.$$

Ввиду утверждения 9.2 выходная последовательность $U \in (\mathcal{F}, \Phi)$ может содержать только символы m_{ii}, $i \geq 1$. Отсюда легко получить, что U — константа. Поэтому $\hat{P}_r(\mathcal{F}, \Phi) = \langle X \rangle$. С другой стороны, $P_r(\mathcal{F}, \Phi) = \theta$. Действительно, если $t \in P_r(\mathcal{F}, \Phi)$, то

$$\exists n \in \mathbb{N} \ \ \forall i \geq n \ \ \forall u \in (\mathcal{F}, \Phi) \quad u(i+t) = u(i). \tag{21.13}$$

Однако выходная последовательность $u \in (\mathcal{F}, \Phi)$ с начальным значением $u(0) = m_{n+1,1}$ имеет вид

$$u = (m_{n+1,1}, m_{n+1,2}, \ldots, m_{n+1,n}, m_{n+1,n+1}, m_{n+1,n+1}, \ldots),$$

и для нее условие (21.13) не выполняется. Таким образом, $P_r(\mathcal{F}, \Phi) = \theta$, и первое включение в (21.5) неверно.

Можно показать, что если $k = 1$ и множество M конечно, то первое включение в (21.5) выполняется.

Пример 21.3. Покажем, что оба включения в (21.6) могут не выполняться. В силу теоремы 21.1 в этом случае $k > 1$, $|M| = \infty$, а регистр сдвига некоммутативен и нерегулярен. Пусть $k = 2$, $M = \mathbb{N}_0$, $\mathcal{F} = \{\theta\}$ и отображения сдвига $\Psi_1, \Psi_2 \colon \mathbb{N}_0 \to \mathbb{N}_0$ правого регистра сдвига $(\mathcal{F}, \Phi)$ определены равенствами

$$\Psi_1 = \epsilon, \quad \Psi_2(a) = \max\{a - 2,\, 0\}.$$

Отображение Ψ_2 можно наглядно изобразить в виде

$$\Psi_2 \colon \begin{array}{l} \cdots \to 6 \to 4 \to 2 \searrow \\ \cdots \to 5 \to 3 \to 1 \nearrow \end{array} 0 \to 0.$$

Таким образом, граф Ψ_2 есть цикл в точке 0 с двумя бесконечными подходами. Так как $\Psi_1 = \epsilon$, то по утверждению 21.2

$$x_1 \in Q_r(\mathcal{F}, \Phi) \subset P_r(\mathcal{F}, \Phi).$$

Так как $\hat{P}_r(\mathcal{F}, \Phi) = \hat{Q}_r(\mathcal{F}, \Phi)$, то достаточно доказать, что $x_1 \notin \hat{Q}_r(\mathcal{F}, \Phi)$. Для этого достаточно найти функцию $U \in (\mathcal{F}, \Phi)$ такую, что $Ux_1 \neq U$.

Определим функцию $U \colon \langle X \rangle \to \mathbb{N}_0$ индуктивно:

$$U(\theta) = 0, \quad U(\overline{x}x_1) = \Psi_1(U(\overline{x})) = U(\overline{x}), \quad U(\overline{x}x_2) = \Psi_2(U(\overline{x})), \tag{21.14}$$

$$U(\overline{x}x_1^{-1}) = U(\overline{x}), \quad U(\overline{x}x_1^{-1}) = \begin{cases} U(\overline{x}) + 2, & \text{если } \overline{x} \neq \theta, \\ U(\overline{x}) + 1 = 1, & \text{если } \overline{x} = \theta, \end{cases}$$

где $\overline{x} \in \langle X \rangle$, причем слова $\overline{x}x_1$, $\overline{x}x_2$, $\overline{x}x_1^{-1}$, $\overline{x}x_2^{-1}$ в каждом из соотношений являются несократимыми, т. е., например, определение $U(\overline{x}x_1^{-1}) = U(\overline{x})$ действует только для слов $\overline{x}$, не оканчивающихся на x_1. Смысл определения U заключается в том, что символ x_2^{-1} вызывает обратное движение по первому подходу функции Ψ_2, за исключением точки θ, в которой происходит обратное движение по второму подходу.

Покажем, что $U \in (\mathcal{F}, \Phi)$. Согласно определению нужно убедиться в том, что

$$U[\overline{z}x_s\mathcal{F}] = \Psi_s(U[\overline{z}\mathcal{F}]), \quad \text{т. е.} \quad U(\overline{z}x_s) = \Psi_s(U(\overline{z})), \quad \overline{z} \in \langle X \rangle.$$

Если слово $\overline{z}x_s$ несократимо, то эти соотношения вытекают из (21.14). В противном случае слово $\overline{z}x_s$ имеет вид $\overline{z}x_s = \overline{x}x_s^{-1}x_s = \overline{x}$ для некоторого несократимого слова $\overline{x} \in \langle X \rangle$, и доказываемое соотношение принимает вид

$$\Psi_s(U(\overline{x}x_s^{-1})) = U(\overline{x}).$$

Проверим это равенство. Если $s = 1$, то $\Psi_1(U(\overline{x}x_1^{-1})) = U(\overline{x}x_1^{-1}) = U(\overline{x})$. Если $s = 2$, $\overline{x} \neq \theta$, то $\Psi_2(U(\overline{x}x_2^{-1})) = \Psi_2(U(\overline{x}) + 2) = U(\overline{x})$. Если $s = 2$, $\overline{x} = \theta$, то $\Psi_2(U(\overline{x}x_2^{-1})) = \Psi_2(1) = 0 = U(\overline{x})$. Таким образом, $U \in (\mathcal{F}, \Phi)$.

Наконец, заметим, что

$$Ux_1(x_2^{-1}) = U(x_1x_2^{-1}) = U(x_1) + 2 = 2, \quad U(x_2^{-1}) = 1.$$

Следовательно, $Ux_1 \neq U$, и для функции U оба включения в (21.6) неверны.

Если регистр сдвига $(\mathcal{F}, \Phi)$ регулярен, то по теореме 21.1 включения (21.5) обращаются в равенства, и тогда соотношения (21.4) и (21.6) равносильны. В силу теоремы 21.1 только они среди включений (21.3)–(21.7) могут быть строгими (когда M бесконечно). Покажем на примере, что это действительно возможно.

Пример 21.4. Включения (21.4) и (21.6) могут быть строгими. Для $k = 2$, $M = \mathbb{Z}$, $\mathcal{F} = \{\theta\}$ рассмотрим коммутативный регулярный регистр сдвига $(\mathcal{F}, \Phi)$, реализующий арифметическую прогрессию с разностью $(1, 1)$ (см. пример 6.3):

$$\Psi_s \colon \mathbb{Z} \to \mathbb{Z}, \quad \Psi_s(a) = a + 1, \quad s = 1, 2.$$

Произвольный выход u этого регистра имеет вид

$$u(\overline{x}) = u(\theta) + l(\overline{x}), \quad \overline{x} \in X^*,$$

а произвольный выход U задается равенством

$$U(\overline{x}) = U(\theta) + d(\overline{x}), \quad \overline{x} \in \langle X \rangle,$$

где $d(\overline{x})$, $\overline{x} \in \langle X \rangle$, определяется следующим образом:

$$d(\theta) = 0, \quad d(x_s) = 1, \quad d(x_s^{-1}) = -1, \quad d(\overline{xy}) = d(\overline{x}) + d(\overline{y}).$$

Так как равенство $u\overline{t} = u$, $\overline{t} \in X^*$, выполняется только для слова $\overline{t} = \theta$, то полугруппа $Q_r(\mathcal{F}, \Phi) = \{\theta\}$ тривиальна. С другой стороны, легко видеть, что $x_1 x_2^{-1} \in \hat{Q}_r(\mathcal{F}, \Phi)$. Следовательно, включения (21.6) строгие.

Покажем теперь, что любая нормальная под(полу)группа является (полу)группой периодов некоторого регистра сдвига (ср. с утверждениями 18.3 и 19.2).

Теорема 21.2. (а) *Для любой нормальной подполугруппы $H \lhd X^*$ существует правый регистр сдвига $(\mathcal{F}, \Phi)$ такой, что $P_r(\mathcal{F}, \Phi) = Q_r(\mathcal{F}, \Phi) = H$.* (б) *Для любой нормальной подгруппы $H \lhd \langle X \rangle$ существует регулярный правый регистр сдвига $(\mathcal{F}, \Phi)$ такой, что $\hat{P}_r(\mathcal{F}, \Phi) = \hat{Q}_r(\mathcal{F}, \Phi) = H$.*

Доказательство. (а) Любая нормальная подполугруппа является прообразом единицы при эпиморфизме полугруппы на некоторый моноид. Пусть $\phi\colon X^* \to M$ — эпиморфизм с ядром H на моноид M. Рассмотрим правый регистр сдвига $(\mathcal{F}, \Phi)$ над множеством M, у которого $\mathcal{F} = \{\theta\}$, а отображения сдвига $\Psi_s\colon M \to M$ задаются следующим образом: если $m \in M$, то $m = \phi(\overline{x})$ для некоторого $\overline{x} \in X^*$, и тогда $\Psi_s(m) = \phi(\overline{x}x_s)$, $s \in \{1, \ldots, k\}$. Если при этом $m = \phi(\overline{y})$, то $\phi(\overline{x}x_s) = \phi(\overline{x})\phi(x_s) = \phi(\overline{y})\phi(x_s) = \phi(\overline{y}x_s)$, так что данное определение корректно. Непосредственно проверяется, что для любого слова $\overline{t} \in X^*$ справедливо равенство $\Psi_{\overline{t}}(m) = \phi(\overline{x}\overline{t})$.

Покажем, что $P_r(\mathcal{F}, \Phi) = Q_r(\mathcal{F}, \Phi) = H$. Если $\overline{t} \in H$, то

$$\Psi_{\overline{t}}(m) = \phi(\overline{x}\overline{t}) = \phi(\overline{x})\phi(\overline{t}) = \phi(\overline{x}) \cdot 1 = \phi(\overline{x}) = m,$$

т. е. $\overline{t} \in Q_r(\mathcal{F}, \Phi)$. Так как $Q_r(\mathcal{F}, \Phi) \subset P_r(\mathcal{F}, \Phi)$ по утверждению 21.2, то $\overline{t} \in P_r(\mathcal{F}, \Phi)$. Обратно, пусть $\overline{t} \in P_r(\mathcal{F}, \Phi)$. По утверждению 21.2 существует n такое, что $\Psi_{\overline{z}\overline{t}} = \Psi_{\overline{z}}$ для любого слова $\overline{z} \in X^*$ длины, не меньшей n. Это означает, что $\phi(\overline{x}\overline{z}\overline{t}) = \phi(\overline{x}\overline{z})$, $\overline{x} \in X^*$. При $\overline{x} = \theta$ получим равенство $\phi(\overline{z}\overline{t}) = \phi(\overline{z})$. Если $H \neq \theta$, то H содержит слово $\overline{z}$ длины, не меньшей n. Тогда $\phi(\overline{t}) = 1$, поэтому $\overline{t} \in H$ и все доказано.

Если же $H = \theta$, то $M = X^*$ и отображения сдвига $\Psi_s\colon X^* \to X^*$ задаются равенствами $\Psi_s(\overline{x}) = \overline{x}x_s$. Тогда любой выход $u \in (\mathcal{F}, \Phi)$ имеет вид $u(\overline{x}) = u(\theta)\overline{x}$. Понятно, что группы периодов такой функции нулевые, поэтому $P_r(\mathcal{F}, \Phi) = Q_r(\mathcal{F}, \Phi) = \theta = H$.

(б) Искомый регистр сдвига получается при таком же построении, что и в п. (а). Пусть $M = \langle X\rangle/H$ — множество всех левых смежных классов группы $\langle X\rangle$ по подгруппе H. Рассмотрим правый регистр сдвига $(\mathcal{F}, \Phi)$ над множеством M, у которого $\mathcal{F} = \{\theta\}$, а отображения сдвига $\Psi_s\colon M \to M$ задаются следующим образом: $\Psi_s(\overline{x}H) = \overline{x}x_sH$, $\overline{x} \in \langle X\rangle$, $s \in \{1, \ldots, k\}$. Проверим корректность определения: если $\overline{x}H = \overline{y}H$, то $\overline{x}x_sH = \overline{x}Hx_s = \overline{y}Hx_s = \overline{y}x_sH$. Отображение Ψ_s биективно, обратное отображение задается равенством $\Psi_s^{-1}(\overline{x}H) = \overline{x}x_s^{-1}H$, поэтому регистр сдвига $(\mathcal{F}, \Phi)$ регулярен. Непосредственно проверяется, что $\Psi_{\overline{t}}(\overline{x}H) = \overline{x}\overline{t}H$ для любых $\overline{x}, \overline{t} \in \langle X\rangle$.

Проверим, что $\hat{P}_r(\mathcal{F}, \Phi) = \hat{Q}_r(\mathcal{F}, \Phi) = H$. Ввиду (21.7) достаточно доказать, что $\hat{Q}_r(\mathcal{F}, \Phi) = H$. С учетом (21.8) имеем:

$$\overline{t} \in \hat{Q}_r(\mathcal{F}, \Phi) \quad \Leftrightarrow \quad \Psi_{\overline{t}} = \epsilon \quad \Leftrightarrow \quad \forall \overline{x} \in \langle X\rangle\ \overline{x}\overline{t}H = \overline{x}H \quad \Leftrightarrow \quad \overline{t} \in H,$$

что и требовалось доказать. Теорема доказана.

Укажем задачи, требующие исследования.

21.1. Верно ли, что для любой подполугруппы $H \lhd X^*$, удовлетворяющей условию (18.8): $\overline{x}, \overline{xy} \in H \Rightarrow \overline{y} \in H$, существует правый регистр сдвига $(\mathcal{F}, \Phi)$ такой, что $Q_r(\mathcal{F}, \Phi) = H$?

21.2. Множество функций S назовем *правым семейством функций*, если оно замкнуто относительно правых сдвигов: $S\overline{x} \subset S$ для любого слова $\overline{x}$. Примером является множество всех выходов правого регистра сдвига. Выяснить, какие утверждения этого параграфа остаются верными для (полу)групп периодов правых семейств функций. Дать критерий того, что правое семейство функций совпадает с множеством всех выходов некоторого правого регистра сдвига.

22. Период регистра сдвига

Пусть $(\mathcal{F}, \Phi)$ — правый регистр сдвига, $\Psi_1, \ldots, \Psi_k$ — его отображения сдвига. Через $\Pi(M^{\mathcal{F}})$ будем обозначать полугруппу всех преобразований и через $S(M^{\mathcal{F}})$ — группу всех биективных преобразований множества $M^{\mathcal{F}}$.

Определение 22.1. Полугруппу $[\Psi_1, \ldots, \Psi_k\rangle < \Pi(M^{\mathcal{F}})$ будем называть *полугруппой регистра сдвига* $(\mathcal{F}, \Phi)$. Если регистр сдвига $(\mathcal{F}, \Phi)$ регулярен, то группу $\langle\Psi_1, \ldots, \Psi_k\rangle < S(M^{\mathcal{F}})$ будем называть *группой регулярного регистра сдвига* $(\mathcal{F}, \Phi)$.

Так как $\Psi_{\overline{x}}\Psi_{\overline{y}} = \Psi_{\overline{xy}}$, то

$$[\Psi_1, \ldots, \Psi_k\rangle = \{\Psi_{\overline{x}}\colon \overline{x} \in X^*\}, \quad \langle\Psi_1, \ldots, \Psi_k\rangle = \{\Psi_{\overline{x}}\colon \overline{x} \in \langle X\rangle\}.$$

Если регистр сдвига регулярен и множество M конечно, то $S(M^{\mathcal{F}})$ — конечная группа и

$$[\Psi_1, \ldots, \Psi_k\rangle = \langle \Psi_1, \ldots, \Psi_k\rangle < S(M^{\mathcal{F}}). \tag{22.15}$$

Для правого регистра сдвига $(\mathcal{F}, \Phi)$ определим отношение эквивалентности $\sim$ на множестве X^*, полагая

$$\overline{x} \sim \overline{y} \quad \Leftrightarrow \quad \forall u \in (\mathcal{F}, \Phi) \quad u\overline{x} = u\overline{y}. \tag{22.16}$$

Утверждение 22.1. *Отношение $\sim$ является конгруэнцией на X^*. Фактормоноид $X^*/\sim$ изоморфен полугруппе регистра сдвига*: $X^*/\sim \cong$ $\cong [\Psi_1, \ldots, \Psi_k\rangle$.

Доказательство. По утверждению 5.2 из включения $u \in (\mathcal{F}, \Phi)$ следует, что $u\overline{z} \in (\mathcal{F}, \Phi)$ для любого $\overline{z} \in X^*$. Поэтому если $\overline{x} \sim \overline{y}$, то $\overline{zx} \sim \overline{zy}$, а также очевидно, $\overline{xz} \sim \overline{yz}$. Следовательно, отношение $\sim$ является конгруэнцией. Ввиду следствия утверждения 21.2

$$\overline{x} \sim \overline{y} \quad \Leftrightarrow \quad \Psi_{\overline{x}} = \Psi_{\overline{y}}. \tag{22.17}$$

Поэтому отображение $\phi\colon X^*/\sim \ \to [\Psi_1, \ldots, \Psi_k\rangle$, $\phi([\overline{x}]_\sim) = \Psi_{\overline{x}}$, является корректно определенным изоморфизмом моноидов.

В дальнейшем нас будут интересовать числа конечных и бесконечных классов $[\overline{x}]_\sim$.

Утверждение 22.2. *Множество L всех слов $\overline{x} \in X^*$, для которых класс $[\overline{x}]_\sim$ конечен, является левой диаграммой Ферре* (*возможно, пустой или бесконечной*). *Если множество M конечно, то и L конечно.*

Доказательство. Пусть $\overline{xy} \in L$. Требуется доказать, что $\overline{x} \in L$. Предположим противное. Тогда класс $[\overline{x}]_\sim$ бесконечен и $\overline{x} \sim \overline{x}_1 \sim \overline{x}_2 \sim \ldots$. В этом случае $\overline{xy} \sim \overline{x}_1\overline{y} \sim \overline{x}_2\overline{y} \sim \ldots$, т. е. класс $[\overline{xy}]_\sim$ бесконечен и $\overline{xy} \notin L$, противоречие. Следовательно, $\overline{x} \in L$, и значит, L — левая диаграмма Ферре. Если множество M конечно, то $\Pi(M^{\mathcal{F}})$ конечно и $|L| \le |X^*/\sim| \le |\Pi(M^{\mathcal{F}})|$.

Определение 22.2. *Правой длиной подхода* $\Lambda_r(\mathcal{F}, \Phi)$ регистра сдвига $(\mathcal{F}, \Phi)$ назовем число классов $[\overline{x}]_\sim$, $\overline{x} \in X^*$, являющихся конечными. *Правым периодом* $T_r(\mathcal{F}, \Phi)$ регистра сдвига $(\mathcal{F}, \Phi)$ назовем число классов $[\overline{x}]_\sim$, $\overline{x} \in X^*$, являющихся бесконечными.

Таким образом,

$$\Lambda_r(\mathcal{F}, \Phi) = |L/\sim|,$$
$$T_r(\mathcal{F}, \Phi) = |X^*/\sim| - |L/\sim| = |(X^* \setminus L)/\sim|.$$

Справедливо равенство

$$\Lambda_r(\mathcal{F}, \Phi) + T_r(\mathcal{F}, \Phi) = |X^*/{\sim}| = |[\Psi_1, \ldots, \Psi_k\rangle|. \tag{22.18}$$

Замечание 22.1. Класс $[\theta]_\sim$ представляет особый интерес. Из утверждения 22.2 следует, что если этот класс бесконечен, то все классы $[\overline{x}]_\sim$, $\overline{x} \in X^*$, бесконечны. Из определения полугруппы чистых правых периодов регистра сдвига следует равенство $[\theta]_\sim = Q_r(\mathcal{F}, \Phi)$. Поэтому класс $[\theta]_\sim$ либо бесконечен, либо состоит из одного элемента θ. Справедливы импликации

$$\Lambda_r(\mathcal{F}, \Phi) = 0 \quad \Leftrightarrow \quad [\theta]_\sim \text{ бесконечен} \quad \Leftrightarrow \quad Q_r(\mathcal{F}, \Phi) \neq \theta. \tag{22.19}$$

Пример 22.1. Рассмотрим традиционный линейный регистр сдвига над полем P с характеристическим многочленом $x^l(x^t - 1)$. Отношение $\sim$ разбивает множество X^* на классы $[x_1^i]_\sim$, $0 \leq i \leq l + t - 1$, из которых первые l конечны, а оставшиеся t бесконечны:

$$[x_1^k]_\sim = \{x_1^k\}, \quad 0 \leq k < l, \qquad [x_1^k]_\sim = \{x_1^{k+ti} : i \geq 0\}, \quad l \leq k < l + t - 1.$$

Следовательно, длина подхода этого регистра сдвига равна l, а период равен t.

В следующей теореме показывается, как вычислить период регулярного регистра сдвига с помощью групп вектор-периодов.

Теорема 22.1. *Если $(\mathcal{F}, \Phi)$ — регулярный правый регистр сдвига, то*

$$\langle \Psi_1, \ldots, \Psi_k\rangle \cong \langle X\rangle/\hat{Q}_r(\mathcal{F}, \Phi),$$
$$\Lambda_r(\mathcal{F}, \Phi) + T_r(\mathcal{F}, \Phi) \leq |\langle X\rangle : \hat{Q}_r(\mathcal{F}, \Phi)| \leq |\langle X\rangle : \langle Q_r(\mathcal{F}, \Phi)\rangle|.$$

Если при этом множество M конечно, то $\Lambda_r(\mathcal{F}, \Phi) = 0$ и

$$T_r(\mathcal{F}, \Phi) = |\langle X\rangle : \hat{Q}_r(\mathcal{F}, \Phi)| = |\langle X\rangle : \langle Q_r(\mathcal{F}, \Phi)\rangle| = |\langle \Psi_1, \ldots, \Psi_k\rangle| \leq |M|^{|\mathcal{F}|}!.$$

Доказательство. Рассмотрим отображение

$$\phi : \langle X\rangle \to S(M^{\mathcal{F}}), \quad \phi(\overline{x}) = \Psi_{\overline{x}}, \quad \overline{x} \in \langle X\rangle. \tag{22.20}$$

Так как $\Psi_{\overline{xy}} = \Psi_{\overline{x}}\Psi_{\overline{y}}$, то ϕ — гомоморфизм групп. При этом $\operatorname{Im}\phi = \langle \Psi_1, \ldots, \Psi_k\rangle$ и $\operatorname{Ker}\phi = \hat{Q}_r(\mathcal{F}, \Phi)$ в силу теоремы 21.1. Тогда $\operatorname{Im}\phi \cong \langle X\rangle/\operatorname{Ker}\phi$, т. е. $\langle \Psi_1, \ldots, \Psi_k\rangle \cong \langle X\rangle/\hat{Q}_r(\mathcal{F}, \Phi)$. Следовательно,

$$\Lambda_r(\mathcal{F}, \Phi) + T_r(\mathcal{F}, \Phi) = |[\Psi_1, \ldots, \Psi_k\rangle| \leq |\langle \Psi_1, \ldots, \Psi_k\rangle| = |\langle X\rangle : \hat{Q}_r(\mathcal{F}, \Phi)|.$$

По теореме 21.1 справедливы включения (21.6), т. е. $\hat{Q}_r(\mathcal{F},\Phi) \supset \langle Q_r(\mathcal{F},\Phi)\rangle$. Отсюда

$$|\langle X\rangle\colon \hat{Q}_r(\mathcal{F},\Phi)| \le |\langle X\rangle\colon \langle Q_r(\mathcal{F},\Phi)\rangle|.$$

В результате получаем требуемые соотношения.

Пусть множество M конечно. Тогда элемент Ψ_1 конечной группы $S(M^{\mathcal{F}})$ имеет конечный порядок, поэтому $\Psi_1^m = \epsilon$ и $x_1^m \in Q_r(\mathcal{F},\Phi)$ для некоторого $m \in \mathbb{N}$. В силу (22.19) $\Lambda_r(\mathcal{F},\Phi) = 0$. Ввиду (22.15) первое из приведенных выше неравенств обратится в равенство. По теореме 21.1 включения (21.6) обращаются в равенства, т. е. $\hat{Q}_r(\mathcal{F},\Phi) = \langle Q_r(\mathcal{F},\Phi)\rangle$. Поэтому второе из приведенных выше неравенств также обратится в равенство. В итоге

$$T_r(\mathcal{F},\Phi) = |\langle \Psi_1,\dots,\Psi_k\rangle| = |\langle X\rangle : \hat{Q}_r(\mathcal{F},\Phi)| = |\langle X\rangle : \langle Q_r(\mathcal{F},\Phi)\rangle|.$$

Так как $\langle \Psi_1,\dots,\Psi_k\rangle$ — подгруппа в $S(M^{\mathcal{F}})$, то $T_r(\mathcal{F},\Phi) \le |M|^{|\mathcal{F}|}!$. Теорема доказана.

Определение 22.3. Регулярный правый регистр сдвига $(\mathcal{F},\Phi)$ над конечным множеством M назовем *правым регистром сдвига максимального периода* над множеством M и диаграммой Ферре $\mathcal{F}$, если $T_r(\mathcal{F},\Phi) = |M|^{|\mathcal{F}|}!$.

Исследуем взаимосвязь между периодом регистра сдвига и периодами его выходных функций.

Утверждение 22.3. *Если период $T_r(\mathcal{F},\Phi)$ регистра сдвига конечен, то любая функция $u \in (\mathcal{F},\Phi)$ периодична справа и $T_r(u) \le T_r(\mathcal{F},\Phi)$.*

Доказательство. Если $\overline{x} \sim \overline{y}$, то $u\overline{x} = u\overline{y}$. Поэтому число правых сдвигов функции u не превосходит числа классов отношения $\sim$:

$$|uX^*| \le |X^*/\!\sim|.$$

Следовательно, функция u периодична справа. Докажем, что $T_r(u) \le$ $\le T_r(\mathcal{F},\Phi)$.

Пусть сдвиг $u\overline{x}$ чисто периодичен справа. Так как период $T_r(\mathcal{F},\Phi)$ конечен, то множество L из утверждения 22.2 конечно, и можно выбрать слово $\overline{y}$ так, что $\overline{xy} \notin L$. Поскольку функция u чисто периодична, существует такое слово $\overline{z} \in X^*$, что $u\overline{x} = u\overline{xyz}$. Так как L — левая диаграмма Ферре, то $\overline{xyz} \notin L$, т. е. класс $[\overline{xyz}]_\sim$ бесконечен. Таким образом, правому сдвигу $u\overline{x}$, являющемуся чисто периодической справа функцией, мы сопоставили

бесконечный класс $[\overline{xyz}]_\sim$. Пусть $u\overline{x}'$ — другой сдвиг, который чисто периодичен справа, и $[\overline{x}'\overline{y}'\overline{z}']_\sim$ — соответствующий ему бесконечный класс. Тогда $u\overline{xyz} = u\overline{x} \neq u\overline{x}' = u\overline{x}'\overline{y}'\overline{z}'$, откуда $[\overline{xyz}]_\sim \neq [\overline{x}'\overline{y}'\overline{z}']_\sim$. Следовательно, разным сдвигам соответствуют разные классы. Поэтому число сдвигов $u\overline{x}$, являющихся чисто периодическими справа функциями, не превосходит числа бесконечных классов отношения $\sim$. По определению это означает, что $T_r(u) \leq T_r(\mathcal{F}, \Phi)$. Конец доказательства.

ПРИМЕР 22.2. Регистр сдвига может не иметь конечный период даже если любой его выход периодичен. Например, пусть $k = 1$, $M = C(p^\infty)$ — группа всех комплексных корней степени p^k, $k \in \mathbb{N}$, из единицы и $(\mathcal{F}, \Phi)$ — традиционный регистр сдвига длины 1 с отображением сдвига $\Psi_1(x) = x^p$. Каждая выходная последовательность этого регистра сдвига имеет конечный период p^k, $k \in \mathbb{N}_0$, но периоды всех выходных последовательностей не ограничены в совокупности.

Если G — группа преобразований на множестве A, то обозначим через $G_\alpha = \{g \in G\colon g(\alpha) = \alpha\}$ стабилизатор элемента $\alpha \in A$ в группе G.

Теорема 22.2. *Пусть $(\mathcal{F}, \Phi)$ — регулярный правый регистр сдвига над конечным множеством M с группой $G = \langle \Psi_1, \ldots, \Psi_k \rangle$. Тогда для любого выхода $u \in (\mathcal{F}, \Phi)$*

$$T_r(u) \cdot |G_{u[\mathcal{F}]}| = T_r(\mathcal{F}, \Phi).$$

В частности, период функции u делит период регистра сдвига $(\mathcal{F}, \Phi)$.

Доказательство. Пусть U — правое продолжение функции u на множество $\langle X \rangle$ относительно регулярного правого регистра сдвига $(\mathcal{F}, \Phi)$, определенное в § 10, $\hat{Q}_r(U)$ — группа чистых периодов функции U. Рассмотрим гомоморфизм ϕ, заданный соотношением (22.20), и докажем, что $\phi(\hat{Q}_r(U)) = G_{u[\mathcal{F}]}$.

Пусть $\overline{t} \in \hat{Q}_r(U)$. Тогда $U\overline{t} = U$, поэтому $U\overline{t}[\mathcal{F}] = U[\mathcal{F}]$, или $\Psi_{\overline{t}}(u[\mathcal{F}]) = u[\mathcal{F}]$. Следовательно, $\phi(\overline{t}) = \Psi_{\overline{t}} \in G_{u[\mathcal{F}]}$, и мы доказали, что $\phi(\hat{Q}_r(U)) \subset G_{u[\mathcal{F}]}$. Обратно, пусть $\Psi_{\overline{t}} \in G_{u[\mathcal{F}]}$. Тогда $\Psi_{\overline{t}}(u[\mathcal{F}]) = u[\mathcal{F}]$, или $U\overline{t}[\mathcal{F}] = U[\mathcal{F}]$. Согласно теореме 10.4 регулярный правый регистр сдвига $(\mathcal{F}, \Phi)$ имеет в точности один выход U с заданной диаграммой значений $U[\mathcal{F}] \in M^{\mathcal{F}}$. Поэтому $U\overline{t} = U$, т. е. $\overline{t} \in \hat{Q}_r(U)$. Отсюда $\Psi_{\overline{t}} = \phi(\overline{t}) \in \phi(\hat{Q}_r(U))$, что доказывает включение $G_{u[\mathcal{F}]} \subset \phi(\hat{Q}_r(U))$.

Таким образом, $\phi(\hat{Q}_r(U)) = G_{u[\mathcal{F}]}$. Поскольку $\operatorname{Ker}\phi = \hat{Q}_r(\mathcal{F}, \Phi) \subset \hat{Q}_r(U)$ согласно (21.2), постольку по теореме об эпиморфизме для групп

$$\hat{Q}_r(U)/\hat{Q}_r(\mathcal{F}, \Phi) \cong G_{u[\mathcal{F}]}. \tag{22.21}$$

Рассмотрим цепочку подгрупп

$$\hat{Q}_r(\mathcal{F},\Phi) < \hat{Q}_r(U) < \langle X\rangle.$$

Заметим, что $|\langle X\rangle\colon \hat{Q}_r(U)| = T_r(u)$ по следствию теоремы 20.2 и по теореме 22.1 $|\langle X\rangle\colon \hat{Q}_r(\mathcal{F},\Phi)| = T_r(\mathcal{F},\Phi)$. Отсюда и из (22.21) следует, что $T_r(u)\cdot|G_{u[\mathcal{F}]}| = T_r(\mathcal{F},\Phi)$.

Следствие. *Если в условиях теоремы G является регулярной группой подстановок на множестве $M^{\mathcal{F}}$, то $T_r(u) = T_r(\mathcal{F},\Phi)$.*

Доказательство. По определению регулярной группы подстановок G_α есть единичная группа.

Укажем открытые вопросы.

22.1. Верны ли теоремы 22.1 и 22.2 в случае бесконечного множества M?

22.2. Можно ли привести пример правого (не регулярного) регистра сдвига $(\mathcal{F},\Phi)$ и его выхода u такого, что $T_r(u)$ не делит $T_r(\mathcal{F},\Phi)$?

23. Регистры сдвига максимального периода

В этом параграфе мы изучим правые регистры сдвига максимального периода, т. е. регулярные правые регистры сдвига $(\mathcal{F},\Phi)$ над конечным множеством M такие, что $T_r(\mathcal{F},\Phi) = |M|^{|\mathcal{F}|}!$.

Утверждение 23.1. *Регулярный правый регистр сдвига $(\mathcal{F},\Phi)$ является регистром сдвига максимального периода тогда и только тогда, когда его отображения сдвига порождают всю симметрическую группу*:

$$\langle\Psi_1,\dots,\Psi_k\rangle = S(M^{\mathcal{F}}).$$

При этом любой выход $u\in(\mathcal{F},\Phi)$ есть функция максимального правого периода над M и $\mathcal{F}$, т. е. $T_r(u) = |M|^{|\mathcal{F}|}$.

Доказательство. Пусть $|M^{\mathcal{F}}| = n$ и $G = \langle\Psi_1,\dots,\Psi_k\rangle$. Так как $T_r(\mathcal{F},\Phi) = |G| \le n!$ по теореме 22.1, то равенство $T_r(\mathcal{F},\Phi) = n!$ равносильно тому, что $G = S(M^{\mathcal{F}}) = S_n$. Если при этом $u\in(\mathcal{F},\Phi)$, то стабилизатор $G_{u[\mathcal{F}]}$ есть S_{n-1}. Тогда $T_r(u) = n!/(n-1)! = n$ по теореме 22.2 , и по определению u — функция максимального правого периода над M и $\mathcal{F}$.

Приведем пример построения правого регистра сдвига максимального периода.

ПРИМЕР 23.1. Пусть $k = 2$, $M = \{0, 1\}$, $\mathcal{F} = \{\theta, x_1, x_2\}$. Зададим отображения сдвига $\Psi_1, \Psi_2 \colon M^{\mathcal{F}} \to M^{\mathcal{F}}$ следующей таблицей.

$u[\mathcal{F}]$	$\begin{smallmatrix}0\\0\wedge 0\end{smallmatrix}$ 1	$\begin{smallmatrix}0\\0\wedge 1\end{smallmatrix}$ 2	$\begin{smallmatrix}0\\1\wedge 0\end{smallmatrix}$ 3	$\begin{smallmatrix}0\\1\wedge 1\end{smallmatrix}$ 4	$\begin{smallmatrix}1\\0\wedge 0\end{smallmatrix}$ 5	$\begin{smallmatrix}1\\0\wedge 1\end{smallmatrix}$ 6	$\begin{smallmatrix}1\\1\wedge 0\end{smallmatrix}$ 7	$\begin{smallmatrix}1\\1\wedge 1\end{smallmatrix}$ 8
$\Psi_1(u[\mathcal{F}])$	$\begin{smallmatrix}0\\0\wedge 1\end{smallmatrix}$	$\begin{smallmatrix}0\\0\wedge 0\end{smallmatrix}$	$\begin{smallmatrix}1\\0\wedge 1\end{smallmatrix}$	$\begin{smallmatrix}1\\0\wedge 0\end{smallmatrix}$	$\begin{smallmatrix}0\\1\wedge 0\end{smallmatrix}$	$\begin{smallmatrix}0\\1\wedge 1\end{smallmatrix}$	$\begin{smallmatrix}1\\1\wedge 1\end{smallmatrix}$	$\begin{smallmatrix}1\\1\wedge 0\end{smallmatrix}$
$\Psi_2(u[\mathcal{F}])$	$\begin{smallmatrix}0\\1\wedge 0\end{smallmatrix}$	$\begin{smallmatrix}1\\1\wedge 0\end{smallmatrix}$	$\begin{smallmatrix}0\\1\wedge 1\end{smallmatrix}$	$\begin{smallmatrix}1\\0\wedge 1\end{smallmatrix}$	$\begin{smallmatrix}0\\0\wedge 1\end{smallmatrix}$	$\begin{smallmatrix}1\\1\wedge 1\end{smallmatrix}$	$\begin{smallmatrix}0\\0\wedge 0\end{smallmatrix}$	$\begin{smallmatrix}1\\0\wedge 0\end{smallmatrix}$

Эти отображения являются отображениями сдвига, т. е. удовлетворяют условию (5.5): если $v[\mathcal{F}] = \Psi_s(u[\mathcal{F}])$, $\overline{x} \in \mathcal{F}$ и $x_s\overline{x} \in \mathcal{F}$, то $v(\overline{x}) = u(x_s\overline{x})$. Для нашей диаграммы Ферре $\mathcal{F}$ это означает следующее: если $s = 1$, то $v(\theta) = u(x_1)$, если $s = 2$, то $v(\theta) = u(x_2)$; в других обозначениях:

$$\Psi_1\Big(\begin{smallmatrix}a\\b\wedge c\end{smallmatrix}\Big) = \begin{smallmatrix}b\\*\wedge *\end{smallmatrix}, \qquad \Psi_2\Big(\begin{smallmatrix}a\\b\wedge c\end{smallmatrix}\Big) = \begin{smallmatrix}c\\*\wedge *\end{smallmatrix}.$$

Согласно утверждению 5.1 отображения Ψ_1, Ψ_2 определяют правый регистр сдвига $(\mathcal{F}, \Phi)$. Так как отображения Ψ_1 и Ψ_2 биективны, то регистр сдвига регулярен. Занумеровав диаграммы значений на $\mathcal{F}$ числами от 1 до 8, получим, что Ψ_1 и Ψ_2 являются следующими подстановками группы S_8:

$$\Psi_1 = (12)(5364)(78), \quad \Psi_2 = (13468527).$$

Можно проверить, что эти две подстановки порождают группу S_8. По утверждению 23.1 регистр сдвига $(\mathcal{F}, \Phi)$ имеет максимальный правый период. Любой выход u этого регистра сдвига является функцией максимального правого периода: $T_r(\mathcal{F}, \Phi) = 8!$, $T_r(u) = 8$.

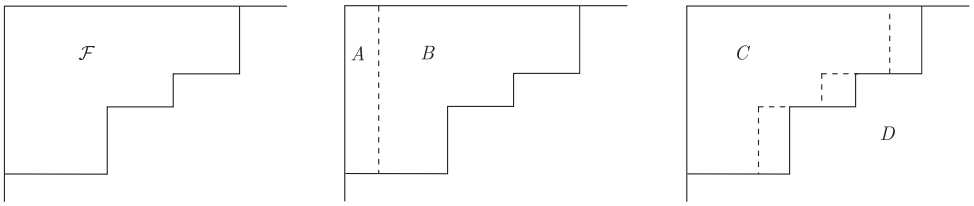
Для доказательства следующей теоремы напомним обозначения, введенные в § 10. Пусть $\mathcal{F}$ — правая диаграмма Ферре. Для фиксированного $s \in \{1, \ldots, k\}$ рассмотрим два разбиения множества $\mathcal{F}$:

$$\mathcal{F} = A \cup B, \quad \text{где } A = \mathcal{F} \setminus x_s\mathcal{F}, \quad B = \mathcal{F} \cap x_s\mathcal{F}, \quad A \cap B = \emptyset,$$

и

$$\mathcal{F} = C \cup D, \text{ где } C = \{\overline{x} \in \mathcal{F} \colon x_s\overline{x} \in \mathcal{F}\}, \quad D = \{\overline{x} \in \mathcal{F} \colon x_s\overline{x} \notin \mathcal{F}\}, \quad C \cap D = \emptyset.$$

Эти разбиения показаны на рисунке (для наглядности изображена диаграмма Ферре в $\mathbb{N}_0^2$, а не в X^*). Множества A и D имеют «ширину» 1.



Справедливы соотношения

$$\mathcal{F} = A \cup B = C \cup D, \quad B = x_s C, \quad |A| = |D| = |x_s \mathcal{F}|, \quad |B| = |C|.$$

Теорема 23.1. *Если $k \geq 2$, $|M| \geq 2$, $|M|$ — степень числа 2, то для любой правой диаграммы Ферре $\mathcal{F}$ существует регулярный правый регистр сдвига $(\mathcal{F}, \Phi)$ максимального правого периода над M и $\mathcal{F}$.*

Доказательство. Рассмотрим ориентированные графы де Брейна Γ_s, $s \in \{1, \ldots, k\}$, введенные в доказательстве теоремы 12.5. Напомним, что множеством вершин графа Γ_s является множество M^C всех диаграмм значений $u[C] \in M^C$, а ориентированное ребро, помеченное диаграммой значений $u[\mathcal{F}] \in M^{\mathcal{F}}$, идет из вершины $u[C]$ в вершину $u[B]$. Из каждой вершины $u[C]$ выходит $|M^D|$ ребер, и в каждую вершину $u[B]$ входит $|M^A|$ ребер. Так как $|A| = |D|$, то степень исхода каждой вершины равна степени захода. Так как граф сильно связен, то в нем существует ориентированный эйлеров цикл, проходящий в точности один раз по каждому ребру графа. Записав этот цикл по ребрам:

$$u_1[\mathcal{F}],\ u_2[\mathcal{F}],\ \ldots,\ u_n[\mathcal{F}],\ u_1[\mathcal{F}], \quad \text{где} \quad n = |M|^{|\mathcal{F}|},$$

получим биективное отображение $\Psi_s \colon M^{\mathcal{F}} \to M^{\mathcal{F}}$, определенное по правилу $\Psi_s(u_i[\mathcal{F}]) = u_{i+1}[\mathcal{F}]$, $\Psi_s(u_n[\mathcal{F}]) = u_1[\mathcal{F}]$. Ввиду способа построения графа Γ_s отображение Ψ_s является отображением сдвига в направлении s, т. е. удовлетворяет условию (5.5): если $v[\mathcal{F}] = \Psi_s(u[\mathcal{F}])$, $\overline{x} \in \mathcal{F}$ и $x_s\overline{x} \in \mathcal{F}$, то $v(\overline{x}) = u(x_s\overline{x})$.

Пусть вначале $k = 2$. Выберем эйлеровы циклы в Γ_1 и Γ_2 некоторым специальным образом. Будем считать, что множество M содержит элементы 0 и 1. Рассмотрим функцию

$$u \colon X^* \to M, \quad u(\overline{x}) = \begin{cases} 1, & \text{если } l(\overline{x}) \equiv 0 \pmod 4, \\ 0, & \text{если } l(\overline{x}) \not\equiv 0 \pmod 4. \end{cases}$$

Функция u изображена на следующем рисунке слева (так как функция u симметрична, мы изображаем ее на множестве $\mathbb{N}_0^2$).

$$u = \begin{array}{|ccccccc|}\hline 1&0&0&0&1&0&0\\ 0&0&0&1&0&0&0\\ 0&0&1&0&0&0&1\\ 0&1&0&0&0&1&0\\ 1&0&0&0&1&0&0\\ 0&0&0&1&0&0&0\\ 0&0&1&0&0&0&1\\ \hline\end{array} \qquad u = \begin{array}{|ccccccc|}\hline 0&1&2&3&0&1&2\\ 1&2&3&0&1&2&3\\ 2&3&0&1&2&3&0\\ 3&0&1&2&3&0&1\\ 0&1&2&3&0&1&2\\ 1&2&3&0&1&2&3\\ 2&3&0&1&2&3&0\\ \hline\end{array} \tag{23.22}$$

Справедливы соотношения

$$ux_1^i = ux_2^i, \quad i \geq 0, \qquad ux_1^4 = ux_2^4 = u. \tag{23.23}$$

Предположим дополнительно, что $|\mathcal{F}| \geq 4$. В этом случае легко увидеть, что диаграммы значений

$$u[\mathcal{F}],\ u[x_1\mathcal{F}],\ u[x_1^2\mathcal{F}],\ u[x_1^3\mathcal{F}] \quad \text{различны.} \tag{23.24}$$

Тогда в графе Γ_1 есть цикл длины 4, состоящий из ребер (23.24). Ввиду (23.23) в графе Γ_2 есть точно такой же цикл. После удаления этих циклов длины 4 из графов Γ_1, Γ_2 они остаются сильно связными. Тогда эти циклы можно продолжить до эйлеровых циклов в графах Γ_1 и Γ_2. Рассмотрим соответствующие им отображения $\Psi_1, \tilde{\Psi}_2 \colon M^{\mathcal{F}} \to M^{\mathcal{F}}$. Каждое из них удовлетворяет условию (5.5). Занумеруем диаграммы значений из $M^{\mathcal{F}}$ числами $1, 2, \ldots, n$ так, чтобы отображение Ψ_1, рассматриваемое как подстановка на множестве $M^{\mathcal{F}}$, записывалось в виде $\Psi_1 = (1, 2, \ldots, n)$. Тогда

$$\Psi_1 = (1, 2, 3, 4, 5, \ldots, n), \quad \tilde{\Psi}_2 = (1, 2, 3, 4, i_5, \ldots, i_n).$$

Пусть v — функция тождественно равная 1 на X^*. В графе Γ_2 ребро $v[\mathcal{F}]$ образует петлю. При обходе Γ_2 по эйлерову циклу, задающему отображение $\tilde{\Psi}_2$, не будем проходить эту петлю. Получим отображение Ψ_2 вида

$$\Psi_2 = (1, 2, 3, 4, i_5, \ldots, i_n)(i_t),$$

где i_t — номер диаграммы значений $v[\mathcal{F}]$ в принятой нумерации.

Рассмотрим регулярный правый регистр сдвига $(\mathcal{F}, \Phi)$ с отображениями сдвига Ψ_1, Ψ_2. Его группа есть $G = \langle g, h \rangle$, где

$$g = \Psi_1 = (1, 2, 3, 4, 5, \ldots, n), \quad h = \Psi_2 = (1, 2, 3, 4, i_5, \ldots, i_n)(i_t).$$

Группа G является подгруппой в S_n и содержит полный цикл длины n, где $n = |M|^{|\mathcal{F}|}$ — степень двойки. Предположим, что G импримитивна и Δ — ее нетривиальный блок, содержащий i_t. Так как $h(i_t) = i_t$, то $h(\Delta) = \Delta$, следовательно, $g^i(\Delta) = \Delta$ для любого $i \geq 1$, что невозможно. Таким образом, группа G примитивна. Согласно [7] примитивная группа подстановок $G < S_n$, где n — степень двойки, содержащая полный цикл, есть S_n или $\mathrm{PGL}(2, \mathbb{Z}_p)$. Здесь $\mathrm{PGL}(2, \mathbb{Z}_p)$ рассматривается как группа подстановок порядка $p+1$ (и значит, $n = p+1$), действующая на множестве всех одномерных подпространств в $\mathbb{Z}_p^2$. Покажем, что равенство $G = \mathrm{PGL}(2, \mathbb{Z}_p)$ невозможно.

Любая матрица из $\mathrm{GL}(2, \mathbb{Z}_p)$, не являющаяся скалярной, имеет не более двух собственных значений и значит — не более двух одномерных собственных подпространств. Это означает, что любая не тождественная подстановка из $\mathrm{PGL}(2, \mathbb{Z}_p)$ имеет не более двух неподвижных точек. Так как подстановка

$$gh^{-1} = (1, 2, 3, 4, 5, \ldots, n)(1, 2, 3, 4, i_5, \ldots, i_n)^{-1} = (1)(2)(3)\ldots,$$

принадлежащая G, имеет не менее трех неподвижных точек, то $G \neq \mathrm{PGL}(2, \mathbb{Z}_p)$. В итоге $G = S_n$, что и требовалось доказать.

Рассмотрим оставшиеся случаи. Если $|M| \geq 4$, то вместо функции u, изображенной в соотношении (23.22) слева, можно рассмотреть функцию u, изображенную в (23.22) справа. Для нее остаются справедливыми все рассуждения, причем условие $|\mathcal{F}| \geq 4$ для выполнения (23.24) не требуется. Если $|M| = 2$ и $|\mathcal{F}| = 1, 2, 3$, то примеры регистров сдвига максимального правого периода легко строятся непосредственно. Все они простые, за исключением случая, когда $|\mathcal{F}| = 3$ и $\mathcal{F} = \{\theta, x_1, x_2\}$ — эта ситуация рассмотрена в примере 23.1. Для $k = 2$ теорема полностью доказана.

Если $k > 2$, то отображения Ψ_1, Ψ_2 строятся аналогично, а $\Psi_3, \ldots, \Psi_k$ можно взять произвольными. Теорема доказана.

Сформулируем нерешенные задачи.

23.1. Доказать, что для любого конечного множества M ($|M|$ — не степень двойки) и диаграммы Ферре $\mathcal{F}$ существует правый регистр сдвига максимального периода над M и $\mathcal{F}$.

23.2. Исследовать *линейные* правые регистры сдвига максимального периода.

24. Наименьший моноид функции

В этом параграфе мы рассмотрим понятия наименьшего моноида функции и регистра сдвига, а также два подхода к определению рекуррентной функции на произвольной конечно порожденной полугруппе.

Зафиксируем функцию $u\colon X^* \to M$.

Определение 24.1. Пусть H — некоторое множество. Сюръективное отображение $\sigma\colon X^* \to H$ называется *допустимым для функции* u, если

$$\sigma(\overline{x}) = \sigma(\overline{y}) \quad \Rightarrow \quad u(\overline{x}) = u(\overline{y}). \tag{24.25}$$

Если отображение σ допустимо для u, то существует единственная функция $\tilde{u}\colon H \to M$ такая, что $\sigma\tilde{u} = u$, т. е. $\tilde{u}(\sigma(x)) = u(x)$, $x \in X^*$; другими словами, коммутативна диаграмма

$$\begin{array}{ccc} X^* & \stackrel{u}{\to} & M \\ {\scriptstyle\sigma}\downarrow & & \| \\ H & \stackrel{\tilde{u}}{\to} & M \end{array}.$$

А именно, при условии (24.25) функция u постоянна на множестве $\sigma^{-1}(h)$ для любого $h \in H$, и можно определить

$$\tilde{u}\colon H \to M, \qquad \tilde{u}(h) = u(\sigma^{-1}(h)).$$

Определение 24.2. Функцию $\tilde{u}$ будем назвать *проекцией функции* u *на* H.

В дальнейшем будем считать, что H — моноид и отображение $\sigma\colon X^* \to H$ является эпиморфизмом моноидов.

Пример 24.1. Пусть $u\colon X^* \to M$ — симметричная функция (см. замечание 6.1), т. е. $u(\overline{x}) = u(\overline{y})$, если слова $\overline{x}$ и $\overline{y}$ отличаются лишь перестановкой букв. Тогда отображение мультистепени

$$\sigma\colon X^* \to \mathbb{N}_0^k, \quad \sigma(\overline{x}) = (\deg_{x_1}\overline{x}, \ldots, \deg_{x_k}\overline{x}),$$

является допустимым для u, и проекция функции u на $\mathbb{N}_0^k$ есть k-последовательность

$$\tilde{u}\colon \mathbb{N}_0^k \to M, \qquad \tilde{u}(i_1, \ldots, i_k) = u(x_1^{i_1} \ldots x_k^{i_k}).$$

Таким образом, симметричные функции $u\colon X^* \to M$ — это в точности функции, для которых отображение мультистепени допустимо и которые поэтому можно рассматривать как k-последовательности со значениями в множестве M.

На множестве X^* введем отношение эквивалентности:

$$\overline{x}\,\rho\,\overline{y} \quad \Leftrightarrow \quad \forall \overline{z} \in X^* \quad \overline{xzu} = \overline{yzu} \ \text{ и } \ u\overline{zx} = u\overline{zy}. \tag{24.26}$$

Легко увидеть, что отношение ρ является конгруэнцией полугруппы X^*.

ЗАМЕЧАНИЕ 24.1. Отметим, что в соотношении (24.26) можно оставить только одно из двух условий $\overline{xz}u = \overline{yz}u$ и $u\overline{zx} = u\overline{zy}$, так как они равносильны. Действительно, пусть $u\overline{zx} = u\overline{zy}$ для любого $\overline{z} \in X^*$. Тогда $u\overline{zx}(\overline{t}) = u\overline{zy}(\overline{t})$ для любого $\overline{t} \in X^*$. Отсюда $u(\overline{zx}\overline{t}) = u(\overline{zy}\overline{t})$, или $\overline{x}\overline{t}u(\overline{z}) = \overline{y}\overline{t}u(\overline{z})$. Следовательно, $\overline{x}\overline{t}u = \overline{y}\overline{t}u$ для любого $\overline{t} \in X^*$, что и требовалось доказать.

Утверждение 24.1. *Если эпиморфизм моноидов $\sigma\colon X^* \to H$ допустим для функции u, то для любых $\overline{x}, \overline{y} \in X^*$*

$$\sigma(\overline{x}) = \sigma(\overline{y}) \quad \Rightarrow \quad \overline{x}\,\rho\,\overline{y}.$$

При этом $\operatorname{Ker}\sigma \subset [\theta]_\rho = Q_l(S) = Q_r(S)$, *где* $S = X^*uX^*$.

Доказательство. Пусть $\sigma(\overline{x}) = \sigma(\overline{y})$. Тогда для любых $\overline{z}, \overline{t} \in X^*$

$$\sigma(\overline{zx}\overline{t}) = \sigma(\overline{zy}\overline{t}) \quad \Rightarrow \quad u(\overline{zx}\overline{t}) = u(\overline{zy}\overline{t}) \quad \Rightarrow \quad u\overline{zx}(\overline{t}) = u\overline{zy}(\overline{t}),$$

откуда $u\overline{zx} = u\overline{zy}$. Аналогично $\overline{xz}u = \overline{yz}u$. Следовательно, $\overline{x}\,\rho\,\overline{y}$.

Так как множество S замкнуто относительно левых и правых сдвигов, то в силу утверждения 21.1

$$Q_l(S) = Q_l(X^*S) = Q_r(SX^*) = Q_r(S).$$

Если $\overline{t} \in \operatorname{Ker}\sigma$, то по доказанному $\overline{t}\,\rho\,\theta$, т. е. $\overline{t} \in [\theta]_\rho$. Класс $[\theta]_\rho$ состоит из таких слов $\overline{t}$, что $\overline{t}v = v$ и $v\overline{t} = v$ для любой функции $v \in S$. По определению полугрупп $Q_l(S)$ и $Q_r(S)$ (см. § 21) получаем, что $[\theta]_\rho = Q_l(S) = Q_r(S)$.

Пусть $\pi\colon X^* \to X^*/\rho$, $\pi(\overline{x}) = [\overline{x}]_\rho$, — естественный эпиморфизм моноидов. Этот эпиморфизм полностью определяется функцией u. В следующем утверждении доказывается свойство универсальности полугруппы X^*/ρ.

Утверждение 24.2. *Пусть $u\colon X^* \to M$ — произвольная функция. Эпиморфизм моноидов $\sigma\colon X^* \to H$ является допустимым для u тогда и только тогда, когда существует эпиморфизм моноидов $\tau\colon H \to X^*/\rho$ такой, что $\sigma\tau = \pi$, т. е. коммутативна диаграмма*

$$\begin{array}{ccc} X^* & \xrightarrow{\sigma} & H \\ {\scriptstyle\pi}\downarrow & \swarrow{\scriptstyle\tau} & \\ X^*/\rho & & \end{array}$$

Доказательство. Пусть σ — допустимый эпиморфизм для u. Определим $\tau\colon H \to X^*/\rho$ следующим образом: если $h \in H$, то положим $\tau(h) = \pi(\overline{x})$,

где $\overline{x} \in X^*$ — произвольное слово, для которого $\sigma(\overline{x}) = h$. Это определение корректно, поскольку если $\sigma(\overline{x}) = \sigma(\overline{y})$, то $\overline{x}\,\rho\,\overline{y}$ по утверждению 24.1 и $\pi(\overline{x}) = \pi(\overline{y})$. Из того, что σ и π — эпиморфизмы моноидов, следует, что τ — эпиморфизм моноидов. При этом $\sigma\tau(\overline{x}) = \tau(\sigma(\overline{x})) = \pi(\overline{x})$ по определению τ.

Обратно, пусть $\tau\colon H \to X^*/\rho$ — такой эпиморфизм моноидов, что $\sigma\tau = \pi$. Если $\sigma(\overline{x}) = \sigma(\overline{y})$, то $\pi(\overline{x}) = \pi(\overline{y})$, т. е. $\overline{x}\,\rho\,\overline{y}$. Отсюда $u\overline{x} = u\overline{y}$, следовательно, $u(\overline{x}) = u(\overline{y})$. Таким образом, σ — допустимый для u.

Следствие. *Моноид X^*/ρ является наименьшим моноидом, на который возможен допустимый для u эпиморфизм моноидов.*

Определение 24.3. Моноид X^*/ρ будем называть *наименьшим моноидом функции u*.

Теорема 24.1. *Наименьший моноид X^*/ρ функции u конечен тогда и только тогда, когда функция u периодична. При этом X^*/ρ гомоморфно вкладывается в моноид $\Pi(\{1,\dots,m\})^{op} \times \Pi(\{1,\dots,n\})$, где $m = |X^*u|$, $n = |uX^*|$. В частности, $|X^*/\rho| \le m^m n^n$.*

Доказательство. Пусть наименьший моноид функции u конечен. Тогда существует лишь конечное число классов отношения ρ. Если $\overline{x}u \ne \overline{y}u$, то $[\overline{x}]_\rho \ne [\overline{y}]_\rho$, поэтому существует лишь конечное число левых и аналогично лишь конечное число правых сдвигов функции u. Следовательно, множества X^*u и uX^* конечны и функция u периодична слева и справа.

Обратно, пусть функция u периодична. В силу теоремы 7.8 она периодична слева и справа. Обозначим через $\overline{x}_1u,\dots,\overline{x}_mu$ все левые и через $u\overline{y}_1,\dots,u\overline{y}_n$ все правые сдвиги функции u. С каждым элементом $\overline{x} \in X^*$ свяжем два вектора $(i_1,\dots,i_m)$ и $(j_1,\dots,j_n)$ над множествами $\{1,\dots,m\}$ и $\{1,\dots,n\}$ соответственно, определяемые из равенств

$$(\overline{x}\overline{x}_1u,\dots,\overline{x}\overline{x}_mu) = (\overline{x}_{i_1}u,\dots,\overline{x}_{i_m}u), \qquad (u\overline{y}_1\overline{x},\dots,u\overline{y}_n\overline{x}) = (u\overline{y}_{j_1},\dots,u\overline{y}_{j_n}).$$

Легко видеть, что два элемента $\overline{x},\overline{y} \in X^*$ связаны отношением ρ тогда и только тогда, когда им соответствует одна и та же пара векторов. Следовательно, число классов в X^*/ρ не превосходит числа пар векторов, т. е. $|X^*/\rho| \le m^m n^n$.

Сопоставим каждому классу $[\overline{x}]_\rho$ два элемента из множеств $\Pi(\{1,\dots,m\})$ и $\Pi(\{1,\dots,n\})$ соответственно:

$$[\overline{x}]_\rho \to \begin{pmatrix} 1 & \dots & m \\ i_1 & \dots & i_m \end{pmatrix} \in \Pi(\{1,\dots,m\}), \quad [\overline{x}]_\rho \to \begin{pmatrix} 1 & \dots & n \\ j_1 & \dots & j_n \end{pmatrix} \in \Pi(\{1,\dots,n\}).$$

Легко видеть, что первое сопоставление является антигомоморфизмом, а второе — гомоморфизмом. В результате получаем гомоморфное вложение X^*/ρ в моноид $\Pi(\{1,\dots,m\})^{op} \times \Pi(\{1,\dots,n\})$. Теорема доказана.

Следствие. *Если функция $u\colon X^* \to M$ реверсивна и периодична, то ее наименьший моноид есть конечная группа, гомоморфно вкладывающаяся в группу $S_m^{op} \times S_n$, где $m = T_l(u)$, $n = T_r(u)$. В частности, $|X^*/\rho| \le m!n!$.*

Доказательство. Ввиду утверждения 10.2 векторы $(i_1, \ldots, i_m)$ и $(j_1, \ldots, j_n)$ в доказательстве теоремы 24.1 являются перестановками. Поэтому X^*/ρ — конечная группа, и ее вложение в моноид $\Pi(\{1, \ldots, m\})^{op} \times \times \Pi(\{1, \ldots, n\})$ является вложением в группу $S_m^{op} \times S_n$. Остается заметить, что $T_l(u) = |X^*u|$ и $T_r(u) = |uX^*|$ ввиду (20.1).

Теорема 24.2. *Если $u\colon X^* \to M$ — реверсивная и периодическая функция, X^*/ρ — ее наименьший моноид, то* $\operatorname{core}\langle Q_l(u)\rangle = \operatorname{core}\langle Q_r(u)\rangle$ *и*

$$X^*/\rho \cong \langle X\rangle/\operatorname{core}\langle Q_l(u)\rangle = \langle X\rangle/\operatorname{core}\langle Q_r(u)\rangle.$$

При этом $|X^*/\rho|$ делится на $T_l(u)$ и на $T_r(u)$.

Доказательство. Пусть U — продолжение функции u на множество $\langle X\rangle$, которое существует и единственно по теореме 14.2. Отметим, что по теореме 14.3 функция U периодична и $U \cdot \langle X\rangle = UX^*$ по утверждению 9.4. В силу следствия 1 теоремы 19.4 имеем $\hat{Q}_l(U) = \langle Q_l(u)\rangle$ и $\hat{Q}_r(U) = \langle Q_r(u)\rangle$, а по утверждению 19.1 $\operatorname{core}\hat{Q}_l(U) = \operatorname{core}\hat{Q}_r(U)$. Следовательно, $\operatorname{core}\langle Q_l(u)\rangle = \operatorname{core}\langle Q_r(u)\rangle$.

Обозначим $Q = \operatorname{core}\hat{Q}_r(U) = \operatorname{core}\langle Q_r(u)\rangle$ и зададим отображение

$$\phi\colon X^*/\rho \to \langle X\rangle/Q, \quad \phi([\overline{x}]_\rho) = Q\overline{x}, \quad \overline{x} \in X^*.$$

Проверим, что ϕ определено корректно. Если $[\overline{x}]_\rho = [\overline{y}]_\rho$, то $\overline{x}\,\rho\,\overline{y}$, поэтому $u\overline{zx} = u\overline{zy}$ для любого $\overline{z} \in X^*$. По следствию 2 теоремы 10.4 равенство $U\overline{zx} = U\overline{zy}$ выполняется для любого $\overline{z} \in X^*$. Тогда $\overline{xy}^{-1} \in \hat{Q}_r(UX^*)$. Так как, с учетом утверждения 19.1

$$Q = \bigcap_{\overline{x}\in\langle X\rangle} \overline{x}^{-1}\hat{Q}_r(U)\overline{x} = \bigcap_{\overline{x}\in\langle X\rangle} \hat{Q}_r(U\overline{x}) = \hat{Q}_r(U \cdot \langle X\rangle) = \hat{Q}_r(UX^*),$$

то $\overline{xy}^{-1} \in Q$. Следовательно, $Q\overline{x} = Q\overline{y}$ и отображение ϕ определено корректно. Очевидно, ϕ — гомоморфизм моноидов. Покажем, что ϕ — изоморфизм.

Если $\phi([\overline{x}]_\rho) = \phi([\overline{y}]_\rho)$, то $Q\overline{x} = Q\overline{y}$, значит, $\overline{xy}^{-1} \in Q = \hat{Q}_r(UX^*)$. Отсюда $U\overline{zx} = U\overline{zy}$ для любого $\overline{z} \in X^*$, и, как следствие, $u\overline{zx} = u\overline{zy}$. Ввиду замечания 24.1 имеем $\overline{x}\,\rho\,\overline{y}$, поэтому $[\overline{x}]_\rho = [\overline{y}]_\rho$ и отображение ϕ инъективно.

Пусть $\overline{x} \in \langle X\rangle$. По утверждению 9.4 существует $\overline{y} \in X^*$ такое, что $U\overline{zx} = U\overline{zy}$ для любого $\overline{z} \in \langle X\rangle$. Тогда $\overline{xy}^{-1} \in \hat{Q}_r(UX^*) = Q$, т. е. $Q\overline{x} = Q\overline{y}$. Следовательно, $Q\overline{x} = \phi([\overline{y}]_\rho)$ и отображение ϕ сюръективно. В итоге ϕ — изоморфизм и $X^*/\rho \cong \langle X\rangle/Q$.

Так как $T_r(u) = |\langle X\rangle : \langle Q_r(u)\rangle|$ по теореме 20.2 и $Q = \operatorname{core}\langle Q_r(u)\rangle$ есть подгруппа в $\langle Q_r(u)\rangle$, то $|X^*/\rho|$ делится на $T_r(u)$. Теорема доказана.

Пример 24.2. Наименьшим моноидом периодической последовательности $u\colon \mathbb{N}_0 \to M$ с периодом t и длиной подхода λ является циклическая полугруппа $H = [x\rangle$, где элемент x удовлетворяет соотношению $x^{\lambda+t} = x^\lambda$. Если последовательность u чисто периодична, то $\lambda = 0$ и $H = \mathbb{Z}_t$. Поэтому чисто периодическую последовательность периода t можно рассматривать как функцию на конечной группе $\mathbb{Z}_t$.

Рассмотрим конструкцию наименьшего моноида для произвольного правого регистра сдвига $(\mathcal{F}, \Phi)$.

Определение 24.4. Эпиморфизм моноидов $\sigma\colon X^* \to H$ называется *допустимым для правого регистра сдвига* $(\mathcal{F}, \Phi)$, если он допустим для любого выхода u этого регистра, т. е.

$$\forall\, u \in (\mathcal{F}, \Phi) \qquad \sigma(\overline{x}) = \sigma(\overline{y}) \quad \Rightarrow \quad u(\overline{x}) = u(\overline{y}).$$

Пусть $\sim$ — конгруэнция множества X^*, введенная в (22.16):

$$\overline{x} \sim \overline{y} \quad \Leftrightarrow \quad \forall u \in (\mathcal{F}, \Phi) \quad u\overline{x} = u\overline{y}.$$

Обозначим через $\nu\colon X^* \to X^*/\sim$ естественный эпиморфизм. Следующее свойство универсальности полугруппы $X^*/\sim$ доказывается так же, как утверждение 24.2.

Утверждение 24.3. *Пусть $(\mathcal{F}, \Phi)$ — правый регистр сдвига. Эпиморфизм моноидов $\sigma\colon X^* \to H$ является допустимым для $(\mathcal{F}, \Phi)$ тогда и только тогда, когда существует такой эпиморфизм моноидов $\tau\colon H \to X^*/\sim$, что $\sigma\tau = \nu$.*

Следствие. *Моноид $X^*/\sim$ является наименьшим моноидом, на который возможен допустимый для $(\mathcal{F}, \Phi)$ эпиморфизм моноидов.*

Определение 24.5. Моноид $X^*/\sim$ будем называть *наименьшим моноидом правого регистра сдвига* $(\mathcal{F}, \Phi)$.

Утверждение 24.4. *Наименьший моноид правого регистра сдвига* $(\mathcal{F}, \Phi)$ *изоморфен полугруппе этого регистра сдвига*:

$$X^*/\sim \cong [\Psi_1, \ldots, \Psi_k\rangle,$$

при этом $|X^*/\sim| = \Lambda_r(\mathcal{F}, \Phi) + T_r(\mathcal{F}, \Phi)$. *Пусть множество* M *конечно. Тогда моноид* $X^*/\sim$ *конечен, и если регистр сдвига* $(\mathcal{F}, \Phi)$ *регулярен, то* $X^*/\sim$ — *конечная группа, изоморфная группе регистра сдвига*:

$$X^*/\sim \cong \langle \Psi_1, \ldots, \Psi_k\rangle \cong \langle X\rangle/\hat{Q}_r(\mathcal{F}, \Phi),$$

при этом $|X^*/\sim| = T_r(\mathcal{F}, \Phi)$.

Доказательство. Соотношение $X^*/\sim \cong [\Psi_1, \ldots, \Psi_k\rangle$ следует из утверждения 22.1, равенство $|X^*/\sim| = \Lambda_r(\mathcal{F}, \Phi) + T_r(\mathcal{F}, \Phi)$ — из формулы (22.18). В случае, когда M конечно и регистр сдвига регулярен, нужно применить теорему 22.1.

Покажем теперь, как с помощью понятия допустимого отображения можно дать определения рекуррентной функции и регистра сдвига на произвольной конечно порожденной полугруппе.

Определение 24.6. Пусть H — конечно порожденная полугруппа с нейтральным элементом (моноид). Функцию $v\colon H \to M$ будем называть *правой рекуррентной функцией на полугруппе* H, если существуют конечный алфавит X, рекуррентная справа функция $u\colon X^* \to M$ на свободной полугруппе X^* и допустимый эпиморфизм моноидов $\sigma\colon X^* \to H$ такие, что $\tilde{u} = v$, т. е. v есть проекция функции u на H.

Аналогично можно дать определение проекции регистра сдвига относительно допустимого отображения $\sigma\colon X^* \to H$ и ввести понятие регистра сдвига на конечно порожденной полугруппе H.

Данные определения рекуррентной функции и регистра сдвига на полугруппе H можно назвать внешними, так как они используют другую полугруппу X^*. Этот подход позволяет определить понятия периодических, реверсивных и других функций на H и развить соответствующую теорию. Возможен, конечно, и внутренний подход, когда определения регистра сдвига и рекуррентной функции на H даются просто по аналогии с данными в § 5 определениями регистра сдвига и рекуррентной функции на X^*.

Сформулируем открытые вопросы.

24.1. Описать реверсивные и периодические функции, для которых: а) наименьший моноид X^*/ρ совпадает с группой $S_m^{op} \times S_n$ или б) $|X^*/\rho| = T_r(u)$.

24.2. Как связана мощность наименьшего моноида функции u с мощностью множества $X^* u X^*$ ее двусторонних сдвигов (ср. с теоремами 20.3 и 24.2)?

24.3. Развить теорию рекуррентных функций на конечно порожденной полугруппе H, используя внешний и внутренний подходы. Являются ли эти подходы эквивалентными?

24.4. В этой статье в основном исследуются односторонние регистры сдвига и связанные с этим понятия, например, левые и правые сдвиги, левые и правые периоды функций. Изучить двусторонние аналоги этих понятий: двусторонние регистры сдвига (см. задачи 5.2 и 5.4 в конце § 5), двусторонние периоды функций, полугруппы двусторонних вектор-периодов и т. д.

Список литературы

1. *Куракин В. Л.* Свободные регистры сдвига. I. — В сб.: Труды по дискретной математике. Т. 9. — М.: Гелиос АРВ, 2006, с. 77–109.
2. *Куракин В. Л.* Свободные регистры сдвига. II. — В сб.: Труды по дискретной математике. Т. 10. — М.: ФИЗМАТЛИТ, 2007, с. 123–174.
3. *Куракин В. Л.* Свободные регистры сдвига. III. — В сб.: Труды по дискретной математике. Т. 11. — М.: ФИЗМАТЛИТ, 2008, с. 63–85.
4. *Куракин В. Л.* Периодические функции на свободной полугруппе. — Матем. сб., 2006, т. 197, № 10, с. 109–128.
5. *Кузьмин А. С., Куракин В. Л., Нечаев А. А.* Псевдослучайные и полилинейные последовательности. — В сб.: Труды по дискретной математике. Т. 1. — М.: ТВП, 1997, с. 139–202.
6. *Нечаев А. А.* Многомерные регистры сдвига и сложность мультипоследовательностей. — В сб.: Труды по дискретной математике. Т. 6. — М.: ФИЗМАТЛИТ, 2002, с. 150–164.
7. *Погорелов Б. А.* Примитивные группы подстановок, содержащие 2^m-цикл. — Алгебра и логика, 1980, т. 19, № 2, с. 236–241.
8. *Холл М.* Теория групп. — М.: ИЛ, 1962.
9. *Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A.* Linear recurring sequences over rings and modules. — J. Math. Sci., 1995, v. 76, № 6, p. 2793–2915.