УДК 512.54

А. С. Олийнык

Группы *RS*-автоматных преобразований

(Представлено членом-корреспондентом НАН Украины В. В. Шарко)

Досліджено RS-автомати та групи, ними визначені. Встановлено зв'язки між групами лінійних RS-автоматних перетворень та групами нескінченних унітрикутних матриць.

1. Автоматы-преобразователи (синхронные или асинхронные) были введены в рассмотрение прежде всего в связи с потребностями математического моделирования вычислительных процессов. Алфавиты, над которыми рассматривались такие автоматы, предполагались конечными [1]. Позже сфера применений автоматов-преобразователей была существенно расширена за счет алгебры, геометрии, теории динамических систем и других разделов математики [2, 3]. С этой точки зрения конечность алфавитов не является необходимым ограничением и естественно возникает потребность рассматривать автоматы над произвольными алфавитами. При этом, учитывая прежде всего алгебраические аспекты исследований, приходится накладывать иные ограничения как на алфавиты, так и на функции выходов и переходов автоматов.

Данное сообщение посвящено синхронным автоматам-преобразователям над алфавитом R, который наделен структурой коммутативного кольца. Вводится понятие RS-автомата и рассматривается группа $GA_S(R)$ преобразований, определяемых RS-автоматами. Показано, что она раскладывается в бесконечно итерированное сплетение регулярных аддитивных групп кольца R. Доказано, что каждая неединичная подстановка из этой группы не имеет нетривиальных циклов конечной длины. Выделяются естественные подгруппы в группе $GA_S(R)$. К ним относятся подгруппа конечно RS-автоматных преобразований, подгруппы полиномиальных и линейных преобразований. Изучены связи между группой линейных RS-автоматных преобразований и группой бесконечных унитреугольных матриц над кольцом R. Охарактеризована подгруппа конечно RS-автоматных линейных преобразований.

2. Пусть R — коммутативное кольцо с единицей, которое мы рассматриваем как алфавит. Символом R^* обозначается множество всех слов над алфавитом R, e — пустое слово, а символом R^ω — множество всех ω-слов над R. Длину слова $u \in R^*$ будем обозначать $|u|$. Конкатенацией слова $u = t_1 \dots t_m$ и слова (либо ω-слова) $v = z_1 \dots z_n \dots$ называется слово (соответственно, ω-слово) $u \cdot v = t_1 \dots t_m z_1 \dots z_n \dots$. Слово u называется подсловом слова (или ω-слова) w, если существуют слово v_1 и слово (соответственно, ω-слово) v_2 такие, что $w = v_1 u v_2$. Если при этом $v_1 = e$, то слово u называется префиксом w.

Напомним, что синхронным автоматом над алфавитом R называется четверка

$$\mathcal{A} = \langle R, Q, \varphi, \psi \rangle,$$

где Q — непустое множество, множество внутренних состояний автомата $\mathcal{A}$; $\varphi\colon R \times Q \to Q$ — функция переходов автомата $\mathcal{A}$; $\psi\colon R \times Q \to R$ — функция выходов автомата $\mathcal{A}$.

Автомат $\mathcal{A}$ называется конечным, если множество его внутренних состояний конечно, и бесконечным — в противном случае.

Функции φ и ψ распространяются на множество $R^* \times Q$ согласно следующим рекурентным соотношениям:

$$\varphi(e,q) = q, \qquad \varphi(uz,q) = \varphi(z,\varphi(u,q))$$
$$\psi(e,q) = e, \qquad \psi(uz,q) = \psi(z,\varphi(u,q)),$$

где $q \in Q$, $z \in R$ и $u \in R^*$. По расширенной функции $\psi\colon R^* \times Q \to R^*$ для каждого $q \in Q$ определяется отображение $f_{\mathcal{A},q}\colon R^* \to R^*$ или $f_{\mathcal{A},q}\colon R^\omega \to R^\omega$ следующим образом. Для любого слова $z_1 z_2 \dots z_n \in R^*$ положим

$$f_{\mathcal{A},q}(z_1 z_2 \dots z_n) = \psi(z_1,q)\psi(z_1 z_2,q)\dots\psi(z_1 z_2 \dots z_n,q).$$

Если же $u = z_1 z_2 \dots$ — ω-слово, то

$$f_{\mathcal{A},q}(u) = \psi(z_1,q)\psi(z_1 z_2,q)\dots.$$

Отображение $f_{\mathcal{A},q}$ называется преобразованием множества R^* (или, соответственно, R^ω), определяемым автоматом $\mathcal{A}$ в состоянии q.

Преобразование $f\colon R^* \to R^*$ или $f\colon R^\omega \to R^\omega$ будем называть автоматным преобразованием, если существует автомат $\mathcal{A}$ над алфавитом R и состояние q этого автомата такие, что $f = f_{\mathcal{A},q}$. Если при этом автомат $\mathcal{A}$ является конечным, то f называют конечно автоматным преобразованием. Имеет место аналог хорошо известного [4] критерия автоматности. А именно, преобразование $f\colon R^* \to R^*$ будет автоматным в том и только том случае, когда оно удовлетворяет таким двум условиям:

а) f сохраняет длины слов;

б) f не уменьшает длину общего начала слов.

Символом Π_n обозначим оператор вычеркивания первых n букв в словах из R^* или ω-словах их R^ω. Для автоматного отображения $f\colon R^* \to R^*$ определим его состояние в слове $u \in R^*$ как отображение $f_u\colon R^* \to R^*$, значение которого на произвольном слове $v \in R^*$ определяется равенством

$$f_u(v) = \Pi_{|u|} f(uv).$$

Множество всех состояний автоматного отображения f обозначим $R(f)$. Тогда, как и в [4], можно показать, что отображение $f\colon Z^* \to Z^*$, удовлетворяющее условиям а, б, будет конечно автоматным в том и только том случае, когда множество $R(f)$ конечно.

Функция выходов ψ автомата $\mathcal{A}$ определяет для каждого состояния $q \in Q$ некоторое преобразование алфавита R, которое будем обозначать ψ_q, т. е.

$$\psi_q(r) = \psi(r,q), \qquad r \in R.$$

Автомат $\mathcal{A}$ называется групповым или подстановочным автоматом, если для любого состояния $q \in Q$ функция ψ_q является биекцией множества R.

Определение 1. Подстановочный автомат $\mathcal{A} = \langle R, Q, \varphi, \psi\rangle$ называется RS-автоматом, если в любом состоянии $q \in Q$ функция ψ_q является сдвигом на некоторый элемент $s_q \in R$:

$$\psi_q(r) = r + s_q, \qquad r \in R.$$

Лемма 1. *Каждое преобразование множества R^* или R^ω, задаваемое подстановочным автоматом, обратимо, причем обратное также задается некоторым подстановочным автоматом. Преобразование, обратное к преобразованию, заданному RS-автоматом, также задается RS-автоматом.*

Доказательство. Пусть $\mathcal{A} = \langle R, Q, \varphi, \psi\rangle$ — некоторый подстановочный автомат. Это означает, что для каждого состояния $q \in Q$ функция $\psi_q\colon R \to R$ является обратимой. Определим новый автомат $\mathcal{A}_1 = \langle R, Q, \varphi_1, \psi_1\rangle$ с тем же множеством внутренних состояний, функции выходов и переходов которого определяются согласно равенствам:

$$\varphi_1(r, q) = \varphi(\psi_q^{-1}(r), q), \qquad \psi_1(r, q) = \psi_q^{-1}(r), \qquad r \in R, \qquad q \in Q.$$

Заметим, что построенный автомат будет подстановочным, а в случае, если $\mathcal{A}$ является RS-автоматом, то и $\mathcal{A}_1$ также будет RS-автоматом. Непосредственная проверка показывает, что для каждого $q \in Q$ обе суперпозиции $f_{\mathcal{A}_1,q}(f_{\mathcal{A},q})$ и $f_{\mathcal{A},q}(f_{\mathcal{A}_1,q})$ являются тождественными преобразованиями, откуда следуют утверждения леммы.

На множестве всех автоматов над алфавитом R определим операцию их суперпозиции.

Определение 2. Суперпозицией автоматов $\mathcal{A}_1 = \langle R, Q_1, \varphi_1, \psi_1\rangle$ и $\mathcal{A}_2 = \langle R, Q_2, \varphi_2, \psi_2\rangle$ называется автомат $\mathcal{A}_1 * \mathcal{A}_2 = \langle R, Q, \varphi, \psi\rangle$ такой, что $Q = Q_1 \times Q_2$, а его функции переходов и выходов определяются равенствами

$$\varphi(r, (q_1, q_2)) = (\varphi_1(r, q_1), \varphi_2(\psi_1(r, q_1), q_2)),$$

$$\psi(r, (q_1, q_2)) = \psi_2(\psi_1(r, q_1), q_2).$$

Автомат $\mathcal{A}_1 * \mathcal{A}_2$ обрабатывает слова или ω-слова посимвольно так, что вначале символ алфавита R перерабатывается автоматом $\mathcal{A}_1$, а затем полученный символ — автоматом $\mathcal{A}_2$.

Заметим, что суперпозиция RS-автоматов снова будет RS-автоматом.

Операция суперпозиции автоматов представляет интерес в связи со следующим хорошо известным утверждением.

Лемма 2. *Предположим, что автоматы $\mathcal{A}_1 = \langle R, Q_1, \varphi_1, \psi_1\rangle$ и $\mathcal{A}_2 = \langle R, Q_2, \varphi_2, \psi_2\rangle$ в состояниях $q_1 \in Q_1$ и $q_2 \in Q_2$ определяют функции $f_{\mathcal{A}_1,q_1}$ и $f_{\mathcal{A}_2,q_2}$. Тогда их суперпозиция $\mathcal{A}_1 * \mathcal{A}_2$ в состоянии (q_1, q_2) определяет функцию $f_{\mathcal{A}_1*\mathcal{A}_2,(q_1,q_2)}$, являющуюся суперпозицией $f_{\mathcal{A}_2,q_2}(f_{\mathcal{A}_1,q_1})$.*

Отсюда как следствие получаем, что множество всех RS-автоматных преобразований на R^* или R^ω образует группу. Как абстрактные группы группа RS-автоматных преобразований множества R^* и группа RS-автоматных преобразований множества R^ω изоморфны между собой. Будем обозначать так определяемую абстрактную группу $GA_S(R)$.

В дальнейшем образ элемента $x \in X$ под действием подстановки g на множестве X будем обозначать x^g, т. е. будем придерживаться правосторонней записи действия подстановки на элемент.

Группа $GA_S(R)$ может быть получена из аддитивной группы кольца R с помощью конструкции бесконечно итерированного сплетения групп подстановок. Напомним соответствующее определение [5].

Определение 3. Сплетением по бесконечной последовательности групп подстановок (G_1, X_1), $(G_2, X_2), \ldots$ называется группа всевозможных преобразований g декартова произведения $X = \prod\limits_{i\geqslant 1} X_i$, которое для каждого $i \geqslant 1$ удовлетворяет таким двум условиям:

1) i-тая координата y_i образа $(x_1, x_2, \ldots)^g = (y_1, y_2, \ldots)$ зависит только от i первых координат элемента $(x_1, x_2, \ldots) \in X$;

2) если зафиксировать первые $i-1$ координат $x_1^0,\ x_2^0,\ldots,x_{i-1}^0$, то преобразование g_i множества X_i, определяемое равенством

$$(x_1^0, x_2^0, \ldots, x_{i-1}^0, x_i, \ldots)^g = (y_1^0, y_2^0, \ldots, y_{i-1}^0, x_i^{g_i}, \ldots),$$

принадлежит группе G_i.

Обозначим сплетение по бесконечной последовательности (G_1, X_1), $(G_2, X_2), \ldots$ символом $\wr\limits_{i=1}^{\infty} G_i$.

Из условий 1 и 2 определения сплетения следует, что любое преобразование $g \in \wr\limits_{i=1}^{\infty} G_i$ определяет бесконечную последовательность $g_1, g_2, \ldots$, где $g_1 \in G_1$, $g_i\colon X_1 \times \cdots \times X_{i-1} \to G_i$ $(i \geqslant 2)$. Обратно, каждая такая последовательность определяет преобразование декартового произведения $\prod\limits_{i=1}^{\infty} X_i$, удовлетворяющее условиям 1 и 2. А именно, последовательности такого вида можно охарактеризовать бесконечными кортежами, которые, следуя Л. А. Калужнину, называют таблицами:

$$g = [g_1, g_2(x_1), g_3(x_1, x_2), \ldots], \tag{1}$$

где $g_1 \in G_1$, $g_i\colon X_1 \times \ldots \times X_{i-1} \to G_i$ $(i \geqslant 2)$. Таблица (1) действует на последовательность $u = (t_1, t_2, \ldots) \in \prod\limits_{i=1}^{\infty} X_i$ согласно правилу

$$u^g = (t_1^{g_1}, t_2^{g_2(t_1)}, t_3^{g_3(t_1,t_2)}). \tag{2}$$

Пусть $R^{(i)}$, $i \in \mathbb{N}$ — копия алфавита R. Счетную декартову степень $\prod\limits_{i=1}^{\infty} R^{(i)}$ алфавита R естественным образом отождествим с множеством R^ω всех ω-слов над R. Тогда сплетение $\wr\limits_{i=1}^{\infty} (R,+)^{(i)}$ регулярных аддитивных групп $(R,+)^{(i)}$, $i \in \mathbb{N}$, кольца R действует на множестве R^ω согласно равенству (2).

Теорема 1. *Группа RS-автоматных преобразований $GA_S(R)$ совпадает со сплетением по бесконечной последовательности регулярных аддитивных групп кольца R:*

$$GA_S(R) = \wr\limits_{i=1}^{\infty} (R,+)^{(i)}.$$

Теорема 2. *Если группа $(R,+)$ без кручения, то в группе подстановок $(GA_S(R), R^\infty)$ каждая неединичная подстановка не имеет конечных циклов длины, большей* 1.

3. Выделим в группе $GA_S(R)$ несколько естественных подгрупп, пользуясь условиями, которые аналогичны ранее возникавшим в теории групп автоматных подстановок над конечными алфавитами.

Если преобразования f_1, f_2 множества R^∞ определяются конечными RS-автоматами, то из доказательства леммы 1 и леммы 2 следует, что их суперпозиция и обратные к ним также задаются конечными RS-автоматами. Поэтому все конечно RS-автоматные преобразования образуют подгруппу в $GA_S(R)$, которую будем обозначать символом $FGA_S(R)$.

В терминах таблиц она может быть охарактеризована следующим образом. Для любой таблицы

$$u = [g_1, g_2(x), \ldots] \in GA_S(R)$$

и слова $t = z_1 \ldots z_s \in R^*$ осуществим подстановку t в u. Получим последовательность вида

$$[g_1, g_2(z_1), \ldots, g_{s+1}(z_1, \ldots, z_s), g_{s+2}(z_1, \ldots, z_s, x_{s+1}), \ldots].$$

Отбрасывая первые s членов этой последовательности и меняя названия переменных, получаем новую таблицу

$$u_t = [h_1, h_2(x_1), \ldots],$$

$h_1 = g_{s+1}(z_1, \ldots, z_s)$, $h_k(x_1, \ldots, x_{k-1}) = g_{s+k}(z_1, \ldots, z_s, x_1, \ldots, x_{k-1})$ $(k \geqslant 2)$. Таблицу u_t назовем t-остатком таблицы u, а множество всех остатков u обозначим символом $R(u)$:

$$R(u) = \{u_t \mid t \in R^*\}.$$

Лемма 3. *Таблица u определяет конечно автоматное преобразование множества R^∞ тогда и только тогда, когда множество $R(u)$ конечно.*

Обозначим символом Δ оператор вычеркивания первого члена последовательности (или первой буквы слова или ω-слова), т. е. если $t = (t_1, t_2, t_3, \ldots)$, то $\Delta t = (t_2, t_3, \ldots)$. Применяя Δ повторно k раз подряд $(k \geqslant 0)$, получаем последовательность $\Delta^k t = (t_{k+1}, t_{k+2}, \ldots)$.

Напомним что последовательность $t = (t_1, t_2, t_3, \ldots)$ (или ω-слово $t_1 t_2 t_3 \ldots$) называется остаточно периодической, если существуют неотрицательное целое число m и натуральное число n такие, что для всех $k > m$ имеет место равенство $t_{n+k} = t_k$. Это равносильно выполнению равенства $\Delta^m t = \Delta^{m+n} t$. Число m называется предпериодом, а n — периодом остаточно периодической последовательности t. Пара чисел (m, n) определяется последовательностью t неоднозначно. Среди всех таких пар выделяется такая пара (m_0, n_0), что m_0 — наименьшее возможное число, для которого последовательность $\Delta^{m_0} t$ является периодической, а n_0 — минимальный период этой последовательности.

Лемма 4. *Множество остаточно периодических ω-слов инвариантно относительно действия группы $FGA_S(R)$.*

Преобразование множества R^* или R^∞, определяемое таблицей из $GA_S(R)$, назовем полиномиальным, если все координаты этой таблицы можно задать полиномами над кольцом R от соответствующего числа переменных. Такую таблицу также будем называть полиномиальной. Произведение полиномиальных преобразований и обратное к полиномиальному преобразованию также будут полиномиальными, т. е. все полиномиальные преобразования образуют подгруппу в $GA_S(R)$. Обозначим группу полиномиальных преобразований символом $PGA_S(R)$.

Отметим, что в общем случае полиномиальное преобразование можно задать полиномиальной таблицей не единственным способом. Если же кольцо R является простым полем характеристики p, то группа $PGA_S(R)$ в этом случае совпадает с $GA_S(R)$ и является силовской p-подгруппой группы всех автоматных подстановок над p-элементным алфавитом.

Таблицу из $PGA_S(R)$ назовем линейной, если все ее координаты являются линейными многочленами, т. е. не содержат одночленов степени $\geqslant 2$. Ясно, что произведение линейных таблиц и обратная к линейной таблице будут линейными, т. е. все линейные таблицы

образуют группу. Будем называть ее группой линейных RS-автоматных преобразований и обозначать $LGA_S(R)$.

Группа $LGA_S(R)$ допускает естественную матричную характеризацию. А именно, пусть $UT_\infty(R)$ — бесконечномерная унитреугольная матричная группа над кольцом R, $AffUT_\infty(R) = UT_\infty(R) \ltimes R^\infty$ — соответствующая афинная группа. Группа $AffUT_\infty(R)$ действует на R-модуле R^∞ согласно правилу

$$x^{(A,b)} = xA + b, \qquad x, b \in R^\infty, \qquad A \in UT_\infty(R).$$

Определение корректно, поскольку произведение последовательности на унитреугольную матрицу в этом случае определено корректно.

Теорема 3. *Группы подстановок* $(LGA_S(R), R^\omega)$ *и* $(AffUT_\infty(R), R^\infty)$ *изоморфны.*

Таким образом, группу линейных RS-автоматных преобразований можно рассматривать, как группу афинных унитреугольных преобразований и даже унитреугольных преобразований. Соответствующий изоморфизм группы $AffUT_\infty(R)$ в группу $UT_\infty(R)$ задается правилом

$$(A, b) \mapsto \begin{pmatrix} 1 & b \\ 0 & A \end{pmatrix},$$

где $(A, b) \in AffUT_\infty(R)$, $\begin{pmatrix} 1 & b \\ 0 & A \end{pmatrix} \in UT_\infty(R)$.

Охарактеризуем теперь группу линейных конечно RS-автоматных преобразований, т. е. пересечение $LGA_S(R) \bigcap FGA_S(R)$. В общем случае справедлива теорема, аналогичная теореме 4.2 из работы [6]. Для бесконечного кольца R при некоторых дополнительных предположениях имеет место следующая характеризация.

Теорема 4. *Пусть в кольце* R *дополнения к аннуляторам всех ненулевых элементов бесконечны. Пара* (A, b), $A \in UT_\infty(R)$, $b \in R^\infty$ *определяет преобразование множества* R^∞, *содержащееся в* $FGA_S(R)$, *в том и только том случае, когда матрица* A *является единичной, а последовательность* b *— остаточно периодической.*

1. *Eilenberg S.* Automata, languages and machines. Vol. A. – New York; London: Academic Press, 1974. – 452 p.
2. *Григорчук Р. И., Некрашевич В. В., Сущанский В. И.* Автоматы, динамические системы и группы // Тр. Мат. ин-та им. В. А. Стеклова. – 2000. – **231**. – С. 134–214.
3. *Nekrashevych V.* Self-similar groups. – Providence, RI: AMS, 2005. – 232 p.
4. *Raney G. N.* Sequential functions // J. Assoc. Comput. Mach. – 1958. – **5**, No 2. – P. 177–180.
5. *Kaloujnine L. A., Beleckij P. M., Fejnberg V. Z.* Kranzprodukte. – Leipzig: Teubner, 1987. – 168 p.
6. *Olijnyk A., Sushchansky V.* Representations of free products by infinite unitriangular matrices over finite fields // Int. J. Alg. Comput. – 2004. – **14**, No 5–6. – P. 741–749.

Киевский национальный университет им. Тараса Шевченко

Поступило в редакцию 12.03.2010

A. S. Oliynyk

Groups of *RS*-automaton transformations

RS-automata and groups defined by them are investigated. Connections between the groups of linear RS-automaton transformations and the groups of infinite unitriangular matrices are established.