Б. ЧАКАНЬ, Ф. ГЕЧЕГ

О ГРУППЕ АВТОМАТНЫХ ПОДСТАНОВОК

УДК 519.95

В настоящей работе рассматривается группа автоматных подстановок конечно порожденной свободной полугруппы и устанавливается несколько ее свойств. При этом авторы хотят показать, как для упрощения некоторых рассуждений можно использовать предлагаемый ниже язык изометрических отображений.

X означает конечное множество символов, содержащее не менее двух элементов, $F(X)$ — свободную полугруппу с системой свободных образующих X, а $S(X)$ — множество всех (счетных) последовательностей с членами из X. Отображение T множества $S(X)$ в себя называется *ретроспективной последовательностной функцией*, если для любого натурального n совпадение первых n букв некоторых последовательностей влечет за собой совпадение первых n букв их образов при T [1] (слова «ретроспективная последовательностная» в дальнейшем будут упускаться).

Легко можно проверить, что взаимно однозначные функции, определенные в $S(X)$, образуют группу A_X, которая оказывается изоморфной группе $\mathbf{A}_X$ всех автоматных подстановок полугруппы $F(X)$. Требуемый изоморфизм получается, если произвольной автоматной подстановке $\mathbf{T}$ поставим в соответствие функцию T: $x_1 \ldots x_i \ldots \to x_1' \ldots x_i' \ldots$ (x_i, $x_i' \in X$), где для каждого натурального i имеет место $x_1 \ldots x_i\mathbf{T} = x_1' \ldots x_i'$. (Вообще в дальнейшем автоматная подстановка от соответствующей взаимно однозначной функции будет отличаться лишь жирным шрифтом).

Элементы $F(X)$ будут обозначаться латинскими, а элементы $S(X)$ — греческими строчными буквами. Если $a = x_1 \ldots x_n$, $\alpha = x_1' \ldots x_i' \ldots$, то $a\alpha$ — последовательность $x_1 \ldots x_n x_1' \ldots x_i' \ldots$. В таком случае a называется n-отрезком $a\alpha$. $aS(X)$ служит для обозначения совокупности всех последовательностей, имеющих слово a в качестве своего n-отрезка. Число букв, входящих в слово a, называется *длиной этого слова* (обозначение: $l(a)$). Если $T \in A_X$, $a \in F(X)$, то T^a означает функцию, для которой $\alpha T^a = \alpha'$ (α, $\alpha' \in S(X)$) тогда и только тогда, когда $(a\alpha)T = a'\alpha'$, где a' — слово, имеющее длину $l(a') = l(a)$ (см. [1]). Легко видеть, что $T^a \in A_X$ для всех $a \in F(X)$. Следуя Дж. Н. Рэни [1], функция T^a называется состоянием функции T. Мощность множества всех различных состояний функции T будем называть весом этой функции. Известно [2], что T можно отождествлять с некоторым приведенным инициальным автоматом, притом состояния этого автомата взаимно однозначным образом соответствуют состояниям T. Произведению функций тогда следует поставить в соответствие последовательное соединение отождествленных с ними автоматов.

Наш подход к изучению группы A_X заключается в рассмотрении взаимно однозначных функций как изометрических преобразований. Для этой цели введем в $S(X)$ метрику следующим образом: положим $\varrho(\alpha, \beta) = 1/n$ ($\alpha, \beta \in S(X)$), если n-тые буквы последовательностей α и β различны, в то же время $(n-1)$-отрезки α и β совпадают. При этом выполнение аксиом метрического пространства очевидно [3].

При такой метрике $S(X)$ оказывается дисконтинуумом. В самом деле, возьмем произвольную последовательность элементов $S(X)$. Для всех натуральных k существуют такие $p_k \in F(X)$, $l(p_k) = k$, что наша последовательность содержит бесконечно много элементов вида $p_k\xi$ ($\xi \in S(X)$), притом p_j является j-отрезком слова p_k, если $j < k$. Пусть i-ым членом последовательности π служит последняя буква слова p_i ($i = 1, 2, \ldots$). Тогда подпоследовательность $p_1\xi_1, \ldots, p_i\xi_i, \ldots$ исходной последовательности сходится к π. Итак, $S(X)$ — компактное пространство. Далее, $S(X)$ — совершенное множество, ибо $\xi = x_1 \ldots x_{i-1}x_i \ldots$ ($x_i \in X$, $i = 1, 2, \ldots$) является пределом последовательности $\xi_i = x_1 \ldots x_{i-1}x_i'x_{i+1}' \ldots$ ($x_j' \in X$, $x_j' \neq x_j$; $j = i, i+1, \ldots$), где $i = 1, 2, \ldots$. Наконец, $S(X)$ является нульмерным, так как для любого $\varepsilon > 0$ оно обладает конечным разбиением, состоящим из множеств диаметра меньше, чем ε. Таким разбиением служит совокупность всех множеств вида $qS(X)$, где q пробегает все слова длины n из $F(X)$, притом $n > 1/\varepsilon$.

Теорема 1. A_X совпадает с множеством всех изометрических отображений $S(X)$ в себя.

Для доказательства берем произвольную $T \in A_X$. Пусть $\varrho(\alpha, \beta) = 1/n$ ($\alpha, \beta \in S(X)$). Тогда α и β имеют одинаковые $(n-1)$-отрезки, поэтому тем же свойством обладают и αT, βT. Значит, $\varrho(\alpha T, \beta T) \leqq 1/n = \varrho(\alpha, \beta)$. Проведение аналогичного рассуждения относительно T^{-1} убеждает нас в изометричности T.

С другой стороны, допустим, что T — изометрическое отображение множества $S(X)$ в себя. Ясно, что T является взаимно однозначной функцией. Остается показать, что T отображает $S(X)$ на себя. Обозначим образ $S(X)$ при T через S'. Предположим, что существует $\alpha \in S(X)$, не входящая в S'. S' — непрерывный образ компакта $S(X)$, так что оно замкнуто в $S(X)$. Поэтому найдется такой $\varepsilon = 1/n > 0$, что ε-окрестность элемента α не пересекается с S'. Пусть теперь $s_i (i = 1,\ldots,k)$ — все элементы длины n в $F(X)$, а δ_i — некоторые последовательности с n-отрезками s_i соответственно. $\varrho(\delta_i T, \alpha) \geqq 1/n$ для всех i, то есть n-отрезок α не входит в n-отрезки образов $\delta_i T$. Следовательно, существуют $1 \leqq i$, $j \leqq k$ такие, что $\delta_i \neq \delta_j$ и $\varrho(\delta_i, \delta_j) \geqq 1/n$, тогда как n-отрезки $\delta_i T$ и $\delta_j T$ совпадают, откуда $\varrho(\delta_i T, \delta_j T) < 1/n$. Это противоречит изометричности T. Теорема доказана.

Теперь можем ввести метрику и в A_X обычным способом [4]: для $S, T \in A_X$ положим $\varrho(S,T) = \max\limits_{\alpha \in S(X)} \varrho(\alpha S, \alpha T)$. Тем самым A_X превращается в метрическую группу, что проверяется непосредственно. Такое определение расстояния между элементами A_X кажется довольно естественным, ибо вполне разумно считать инициальные автоматы тем более близкими, чем дольше совпадают их ответные реакции при одинаковых последовательностях входных сигналов. Так как реальные эксперименты с автоматами имеют конечную длину, то выражения «функции достаточно близки друг к другу» и «(соответствующие) автоматы практически неразличимы» оказываются синонимами.

Покажем, что A_X является *дисконтинуумом*. Рассмотрим произвольную последовательность $T_1,\ldots,T_n,\ldots$, состоящую из элементов A_X. Для $T \in A_X$ обозначим через $\mathbf{T}^k$ отображение, определенное в множестве слов $p \in F(X)$, $l(p) \leqq k$ и совпадающее там с $\mathbf{T}$. Число различных $\mathbf{T}^{(k)}$ конечно, поэтому для всех $k (k = 1, 2,\ldots)$ существуют такие $\mathbf{T}^{(k)}$, что найдутся T_{i_k}, для которых $\mathbf{T}_{i_k}^{(k)} = \mathbf{T}^{(k)}$, притом в случае $j < k$ $\mathbf{T}^{(j)}$ из $\mathbf{T}^{(k)}$ получается ограничением области определения. Если теперь $\mathbf{T}$ — отображение, определенное посредством $a\mathbf{T} = a\mathbf{T}^{(k)} (a \in F(X);\ l(a) = k)$ то последовательность $T_{i_1},\ldots,T_{i_k},\ldots$ сходится к T. Таким образом, A_X компактно. Далее, пусть $T \in A_X$. Для произвольной $\alpha = a\alpha' (l(a) = k)$ положим $\alpha T^{(k)} = a\mathbf{T}^{(k)} \cdot \alpha'$. Тогда $T^{(k)}$ сходится к T, если $k \to \infty$. Значит, A_X — совершенное множество. Для установления нульмерности A_X заметим, что для любого $\varepsilon > 0$ A_X допускает конечное разбиение, состоящее из множеств диаметром меньше, чем ε. Так получается при причислении к одному классу S и T всякий раз, когда $\mathbf{S}^{(k)} = \mathbf{T}^{(k)}$, где $k > 1/\varepsilon$.

Заметим, что A_X (так же, как и $S(X)$) при любом конечном X оказывается топологически эквивалентным канторову совершенному множеству.

Функция $T (\in A_X)$ обладает конечным весом тогда и только тогда, когда $\mathbf{T}$ является конечно-автоматной подстановкой полугруппы $F(X)$. Справедливость этого утверждения вытекает из [1] и теорем 8, 9 в [2]. Конечноавтоматные подстановки составляют подгруппу в $\mathbf{A}_X$ [5], откуда в силу предыдущего высказывания следует, что множество всех функций конечного веса будет подгруппой в A_X. Эту группу обозначим через G_X.

Теорема 2. G_X всюду плотно в A_X.

Пусть $T \in A_X$. Мы раньше видели, что последовательность $T^{(k)} (k = 1, 2,\ldots)$ сходится к T. Поэтому достаточно показать, что $T^{(k)} \in G_X$ для всех k. Если $p \in F(X)$, $l(p) \geqq k$, $p = rs(l(r) = k)$, то для произвольного $\alpha \in S(X)$ имеем: $(p\alpha) T^{(k)} = (r \cdot s\alpha) T^{(k)} = r\mathbf{T}^{(k)} \cdot s\alpha$, откуда $\alpha (T^{(k)})^p = \alpha$. Таким образом, состояние $(T^{(k)})^p$ является тождественной функцией всякий раз, когда $l(p) \geqq k$, так что $T^{(k)}$ обладает лишь конечным числом различных состояний, то есть $T^{(k)} \in G_X$, что и требовалось доказать.

$A_X^{(k)}$ означает множество всех $T^{(k)} (T \in A_X)$, а $\mathbf{A}_X^{(k)}$ — множество всех $\mathbf{T}^{(k)} (\mathbf{T} \in \mathbf{A}_X)$. Согласно одной лемме Л. А. Калужнина [6], всякая система образующих $\mathbf{A}_X^{(k)}$ содержит не менее k элементов. Очевидно, $A_X^{(k)}$ и $\mathbf{A}_X^{(k)}$ изоморфны между собой, так что утверждение этой леммы остается в силе и для $A_X^{(k)}$.

Говорят, что подмножество M топологической группы G является базисом этой группы, если M не содержится ни в какой истинной топологической (то есть замкнутой) подгруппе группы G.

Известно [6], [7], что группы A_X и G_X не являются конечно порожденными. Уточнением этого результата служит такая теорема.

Теорема 3. Топологические группы A_X и G_X не обладают конечным базисом.

Докажем это сначала для A_X. Пусть $T_1, \ldots, T_n$ — произвольные элементы A_X. В силу леммы Калужнина, $\{T_1^{(n+1)}, \ldots, T_n^{(n+1)}\} = T^*$ является истинной подгруппой в $A_X^{(n+1)}$. Если $P \in A_X^{(n+1)}$, $P \overline{\in} T^*$, а Q — произвольный элемент из T^*, то существует $\alpha \in S(X)$, для которого $\alpha P \neq \alpha Q$, и, ввиду определения $A_X^{(n+1)}$, $\varrho(\alpha P, \alpha Q) \geqq 1/(n+1)$. Отсюда, $\varrho(P, Q) \geqq 1/(n+1)$. Заметим, что $(T_i T_j)^{(k)} = T_i^{(k)} T_j^{(k)}$, а также $(T_i^{-1})^{(k)} = (T_i^{(k)})^{-1}$ $(i, j = 1, \ldots, n;\ k = 1, 2, \ldots)$. Если теперь $R \in \{T_1, \ldots, T_n\}$, то $R^{(n+1)} \in T^*$, так что $\varrho(P, R^{(n+1)}) \geqq 1/(n+1)$. Принимая во внимание, что $\varrho(R, R^{(n+1)}) < 1/(n+1)$, получим $\varrho(P, R) \geqq 1/(n+1)$. Значит, функция P не является предельной точкой для подгруппы $\{T_1, \ldots, T_n\}$. Таким образом, подгруппа $\{T_1, \ldots, T_n\}$ не является всюду плотной в A_X, поэтому ее замыкание, являющееся топологической подгруппой в A_X, содержащей функции $T_1, \ldots, T_n$, не совпадает с A_X. Этим показано, что система элементов $T_1, \ldots, T_n \in A_X$ не является базисом группы A_X.

Ввиду транзитивности отношения плотности из теоремы 2 сразу вытекает, что базис группы G_X оказывается базисом и для A_X. Отсюда следует утверждение теоремы 3, относящееся к G_X.

Авторам пока неизвестно, имеет ли место алгебраический аналог следующей теоремы.

Теорема 4. A_X и G_X обладают минимальным базисом. Ясно, что $A_X^{(k)} \subseteq A_X^{(l)}$, если $k \leqq l$. Поэтому $\bigcup_{k=1}^{\infty} A_X^{(k)} = A_X^{(\infty)}$ является подгруппой в A_X. Легко усмотреть, что $A_X^{(\infty)}$ всюду плотное множество в G_X и A_X. Но тогда для доказательства теоремы 4 достаточно найти минимальный базис для группы $A_X^{(\infty)}$. Предположим ради простоты, что X состоит в точности из двух элементов. Наши рассуждения без значительных изменений переносятся и для общего случая.

0 и 1 будут означать элементы, а φ — нетождественную подстановку множества X. 0^k означает слово, состоящее из k нулей. Рассмотрим следующие функции $U_i (i = 1, 2, \ldots)$: пусть для $\alpha = p x \alpha'$ $(\in S(X))$, где $p \in F(X)$, $l(p) = i - 1$, $x \in X$, $\alpha' \in S(X)$,

$$\alpha U_i = \begin{cases} p(x\varphi)\alpha', & \text{если } p = 0^{i-1}, \\ \alpha & \text{— в остальных случаях.} \end{cases}$$

Очевидно, $U_i \in A_X^{(i)}$ для всех натуральных i. Покажем, что $\langle U_i \rangle$ — то есть множество всех U_i — является минимальной системой образующих для $A_X^{(\infty)}$. Среди всех U_i лишь единственный U_j преобразует j-тые буквы последовательностей $S(X)$. Стало быть, никакое истинное подмножество $\langle U_i \rangle$ не может быть базисом для $A_X^{(\infty)}$. Далее, элементы $U_1, \ldots, U_i$ порождают группу $A_X^{(i)}$. Действительно, это ясно для случая $i = 1$. Допустим, что $A_X^{(i-1)} = \{U_1, \ldots, U_{i-1}\}$. Берем произвольный $T \in A_X^{(i)}$. По предположению $T^{(i-1)} \in \{U_1, \ldots, U_{i-1}\}$. Если теперь $px\mathrm{T} = p\mathrm{T}^{(i-1)} \cdot x\varphi_p$ (p и x — как и выше, а φ_p — подстановка множества $\langle 0, 1 \rangle$), то пусть $V_p^{(i-1)}$ — подстановка из $\mathrm{A}_X^{(i-1)}$, выполняющее равенство $p\mathrm{V}_p^{(i-1)} = 0^{i-1}$. Тогда

$$T = \prod_{p \in F(X), l(p) = i-1, \varphi_p = \varphi} (V_p^{(i-1)} U_i (V_p^{(i-1)})^{-1}) . T^{(i-1)} \in$$

$$\in \{U_1, \ldots, U_i\},$$

что и требовалось доказать.

Если X содержит больше двух элементов, то минимальный базис для группы A_X^{∞} принимает такой вид: $U_{11}, U_{12}, \ldots, U_{i1}, U_{i2}, \ldots$, где

$$\alpha U_{ij} = \begin{cases} p(x\varphi_j)\alpha', & \text{если } p = 0^{i-1}, \\ \alpha & \text{— в остальных случаях;} \end{cases}$$

здесь $j = 1, 2, \ldots$; φ_1, φ_2 — два порождающих элемента группы всех подстановок множества X; $0 \in X$. Доказательство при этом может вестись по такому же плану, как и в предыдущем, более простом случае.

Наконец, имеет место следующая теорема.

Теорема 5. A_X и G_X — группы бесконечного общего ранга [8].

Для доказательства достаточно показать, что для всякого натурального k существует в G_X такая конечно порожденная подгруппа, которая не содержится ни в какой подгруппе G_X, порождаемой k элементами. Однако докажем более сильное утверждение о том, что теорема 5 справедлива и в топологическом смысле, то есть нет такого k, при котором каждая конечная система элементов G_X (A_X) содержалась бы в некоторой подгруппе группы G_X (A_X), обладающей базисом из k элементов. При этом наша цель будет достигнута, если мы покажем, что для произвольного натурального k и $T_1, \ldots, T_k \in A_X$ $A_X^{(k+1)}$ не входит в замыкание группы $\{T_1, \ldots, T_k\}$. Это доказывается точно так же, как теорема 3.

В заключение отметим, что последним трем теоремам можно придавать такую наглядную форму.

Нельзя найти такого конечного набора (конечных) автоматов, последовательными соединениями которых можно было бы с *произвольной точностью* подражать любому (конечному) автомату [7]. В то же время бесконечный минимальный набор автоматов с указанным свойством существует. Нет такого натурального числа k, при котором последовательными соединениями подходящего k-членного набора автоматов можно было бы с произвольной точностью подражать любому члену всякой конечной совокупности автоматов. (В этом абзаце мы употребляли термин «автомат» ради краткости вместо точного термина «инициальный автомат, взаимно однозначно отображающий свою входную полугруппу в себя»).

ЛИТЕРАТУРА

1. Дж. Н. Рэнн, Последовательностные функции, «Кибернетический сборник», вып. 3, 1961.
2. В. М. Глушков, Абстрактная теория автоматов, УМН, 16, 5, 1961.
3. П. С. Александров, Введение в общую теорию множеств и функций, ОГИЗ, М.—Л., 1948.
4. Л. С. Понтрягин, Непрерывные группы, ГИТЛ, М., 1954
5. F. Hořejš, Преобразования, определенные конечными автоматами, сб. «Проблемы кибернетики», вып. 9, 1963.
6. В. П. Заровный, Автоматные подстановки и сплетения групп, Доклады АН СССР, 160, 3, 1965.
7. Ф. Гечег, О группе взаимно однозначных преобразований, определённых конечными автоматами, журн. «Кибернетика», № 1, 1965.
8. А. Г. Курош, Теория групп, ГИТЛ, М., 1953.

Поступила в редакцию 19.V 1965