СООБЩЕНИЯ
ОБЪЕДИНЕННОГО
ИНСТИТУТА
ЯДЕРНЫХ
ИССЛЕДОВАНИЙ
ДУБНА

Р11 - 7345

Г.К. Войков, Т.Т. Войкова

ОБ АВТОМАТАХ, ПОЛУГРУППЫ КОТОРЫХ ЯВЛЯЮТСЯ ГРУППАМИ

1973

ЛАБОРАТОРИЯ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И АВТОМАТИЗАЦИИ

P11 - 7345

Г.К. Войков, Т.Т. Войкова

ОБ АВТОМАТАХ, ПОЛУГРУППЫ КОТОРЫХ ЯВЛЯЮТСЯ ГРУППАМИ

ВВЕДЕНИЕ

B1. Определение

Пусть A и B – непустые множества и ΣA – свободная полугруппа, порожденная множеством A. Отображение $f: \Sigma A \to B$ называется машиной. Отношение $\equiv_f$ на ΣA определяется для всех $\alpha, \beta \in \Sigma A$ и $\alpha \equiv_f \beta$ тогда и только тогда, когда $f(\gamma\alpha\delta) = f(\gamma\beta\delta)$ для всех $\gamma, \delta \in (\Sigma A)^1$. $\equiv_f$ является конгруэнцией с сокращениями, а фактор-полугруппа $\Sigma A|_{\equiv f}$ – полугруппой с сокращениями. $\Sigma A|_{\equiv f}$ называется полугруппой машины f и обозначается f^S. Она изоморфна множеству состояний приведенной динамической системы с дискретным действием, одно и только одно из состояний которой соответствует отображению $f: \Sigma A \to B$.

B2. Замечание

Известно, что если каждый вход некоторого автомата пермутирует его состояния, то полугруппа этого автомата есть группа /1/, /2/, /3/.

Более точно имеет место следующее утверждение.

B3. Утверждение

Пусть $f: \Sigma A \to B$ – машина и пусть

$$M(f) = (\Sigma A, B, \{fL(\alpha) | \alpha \in \Sigma A\}, \lambda_f, \delta_f) -$$

минимальный приведенный автомат, реализующий f, где $L: \Sigma A \to F_L((\Sigma A)^1)$ есть левое регулярное представление свободной полугруппы ΣA. Пусть для каждого $\alpha \in \Sigma A$ существует целое число $n > 0$, такое, что $fL(\alpha^n) = f$, и если $fL(\alpha^m) = f$ для другого целого числа $m > 0$, то $m \geq n$.

Тогда полугруппа f^S есть группа, являющаяся объединением всех циклических групп конечного порядка, порождаемых элементами $\alpha \in \Sigma A$.

Доказательство

Класс эквивалентности по $mod \equiv f$, содержащий $\beta \in \Sigma A$, обозначаем $[\beta]_{\equiv f}$. Полугрупповая структура на $\Sigma A|_{\equiv f} = f^S$ порождается законом $[\alpha]_{\equiv f} \cdot [\beta]_{\equiv f} = [\alpha\beta]_{\equiv f}$. Тогда, по определению, для каждого $\alpha \in \Sigma A$ существует последовательность из непересекающихся классов

$$G_\alpha = [\alpha]_{\equiv f}, [\alpha^2]_{\equiv f}, \dots, [\alpha^n]_{\equiv f},$$

элементы которой образуют коммутативную циклическую группу с нормальным элементом $[\alpha^n]_{\equiv f}$. Также по определению $\emptyset \in [\alpha^n]_{\equiv f}$. Объединение $G = \bigcup_{\alpha \in \Sigma A} G_\alpha$ – есть группа с нормальным элементом $[\emptyset]_{\equiv f}$, который принадлежит всем G_α, $\alpha \in \Sigma A$ и который совпадает с $[\alpha^{i_\alpha}]_{\equiv f}$, где i_α – порядок циклической группы G_α. Очевидно, $G = f^S$.

B4. Замечание

Поскольку объединение циклических групп содержит собственные подгруппы, то оно не является циклической группой. Рассмотренная группа G коммутативна и каждая ее подгруппа G_α, $\alpha \in \Sigma A$ коммутативна. Следовательно, каждая подгруппа G_α группы G является нормальным делителем в G. И так как G_α, $\alpha \in \Sigma A$ не содержит собственных подгрупп, то каждая G_α, $\alpha \in \Sigma A$ проста.

В декомпозиционной теории автоматов (и конечных полугрупп) К.Крона и Дж.Роудза /4/,/5/,/6/ нетривиальные простые группы, делящие полугруппу f^S, являются одновременно множествами входов, состояний и выходов для "групповых аккумуляторов", из которых можно синтезировать $f: \Sigma A \to B$, как композицию без циклов.

Исследуем вопрос о том, при каких необходимых и достаточных условиях полугруппа f^S машины f обладает групповой структурой.

В первой части работы доказывается, что если полугруппа f^S машины f определяется согласно BI, то f^S будет группой тогда и только тогда, когда ΣA наделена групповой структурой при помощи определяющих соотношений в множестве ΣA.

Во второй части, при решении задачи о нахождении необходимых и достаточных условий, используется одна теорема Круазо /7/. Изложение построено по Клиффорду и Престону /8/.

I. Структуры множества входных воздействий и полугруппы машины $f: \Sigma A \to B$

I.I. Определение

Пусть A, B – непустые множества. $F(A, B)$ есть множество всех отображений A в B. Если $A = B$, то $F(A, A)$ обозначаем через $F(A)$. $F_L(A)$ есть полугруппа на множестве $F(A)$ с композиционным законом $(f \circ g)(a) = f[g(a)]$ для всех $f, g \in F(A)$ и всех $a \in A$. Левым регулярным представлением L полугруппы ΣA называется отображение

$$L: \Sigma A \to F_L[(\Sigma A)^1],$$

определенное следующим образом: для $\alpha \in \Sigma A$ и $\alpha' \in (\Sigma A)^1$

$$L(\alpha)(\alpha') = \alpha \cdot \alpha' = (\alpha, \alpha')$$

и

$$L(\alpha)(1) = \alpha .$$

Левое регулярное представление группоидов является мономорфизмом (I:I-гомоморфизмом).

I.2. Теорема

Полугруппа $f^S = \Sigma A|_{\equiv f}$ имеет групповую структуру тогда и только тогда, когда ΣA наделена определяющими соотношениями группы.

Доказательство

Если $(\Sigma A)^1$ – группа, то, имея в виду, что композиция двух элементов $[\alpha]_{\equiv f}$, $[\beta]_{\equiv f}$ полугруппы $\Sigma A|_{\equiv f}$ равна

$$[\alpha]_{\equiv f} \cdot [\beta]_{\equiv f} = [\alpha\beta]_{\equiv f} ; \; \alpha, \beta \in (\Sigma A)^1,$$

получаем выполнение необходимого условия теоремы.

Пусть для всех $[\alpha]_{\equiv f}$, $[\beta]_{\equiv f} \in \Sigma A|_{\equiv f}$ существует $[\gamma]_{\equiv f} \in \Sigma A|_{\equiv f}$ такой, что

$$[\alpha]_{\equiv f} \cdot [\gamma]_{\equiv f} = [\alpha\gamma]_{\equiv f} = [\beta]_{\equiv f} .$$

По определению конгруэнции $\equiv_f$ получаем

$$f(\xi\alpha\gamma\zeta) = f(\xi\beta\zeta)$$

для всех $\xi, \zeta \in (\Sigma A)^1$.

Последнее равенство можно записать

$$fL(\xi\alpha\gamma)(\zeta) = fL(\xi\beta)(\zeta) \;;\; \xi,\zeta \in (\Sigma A)^1,$$

и поскольку оно выполняется для всех $\xi, \zeta \in (\Sigma A)^1$, получаем равенство отображений

$$fL(\xi\alpha\gamma) = fL(\xi\beta)$$

$$fL(\xi)L(\alpha\gamma) = fL(\xi)L(\beta)$$

и

$$L(\alpha\gamma) = L(\beta) \;.$$

Отображение L есть мономорфизм и, следовательно, $\alpha\gamma = \beta$. Таким образом, мы доказали, что полугруппа ΣA проста справа. Аналогично можно показать, что она проста и слева и, следовательно, имеет и групповой закон композиции.

I.3. Замечание

Пусть на ΣA определено отношение E_f : "для произвольных $\alpha, \beta \in \Sigma A$, $\alpha \equiv \beta \,(mod\; E_f)$ тогда и только тогда, когда $f(\eta\alpha) = f(\eta\beta)$ для всех $\eta \in (\Sigma A)^1$ ". E_f – есть левая конгруэнция и $\equiv_f \subseteq E_f$. Если в условии Теоремы I.2 заменить $\equiv_f$ на E_f , то достаточная часть утверждения не будет верной. Действительно, если $[\alpha]_{E_f} \cdot [\gamma]_{E_f} = [\beta]_{E_f}$,

то выполняется только

$$fL(\xi)(\alpha\gamma) = fL(\xi)(\beta),$$

а это недостаточно для выполнения равенства $\alpha\gamma = \beta$. В интерпретации для автоматов это означает, что равенство выходов $f(\xi\alpha\gamma)$ и $f(\xi\beta)$ не равносильно эквивалентности (неразличимости) состояний $fL(\xi\alpha\gamma)$ и $fL(\xi\beta)$.

Если мы определим на ΣA правую конгруэнцию Q_f: "для всех $\alpha, \beta \in \Sigma A$, $\alpha \equiv \beta \,(mod\; Q_f)$ тогда и только тогда, когда $f(\alpha\eta) = f(\beta\eta)$ для всех $\eta \in (\Sigma A)^1$ ", то достаточное условие Теоремы I.2 вообще имеет место, но только для автоматов "без предистории".

I.4. Утверждение

Конгруэнция $\equiv_f$ порождается соотношением $f^{-1} \circ f$ на ΣA , где $f : \Sigma A \to B$.

Доказательство

Для каждого $b \in B$ определяем $f^{-1}(b) = \{\alpha \in \Sigma A \mid f(\alpha) = b\}$. Композицию $f^{-1} \circ f : \Sigma A \to \Sigma A$ можно рассматривать как отношение на ΣA . Очевидно, $\alpha \equiv \beta \,(mod\; f^{-1}\circ f)$ тогда и только тогда, когда $f(\alpha) = f(\beta)$. Отношение $f^{-1}\circ f$ является отношением эквивалентности на ΣA . Нетрудно видеть, что $\equiv_f$ есть транзитивное замыкание $f^{-1}\circ f$, то есть

$$\equiv_f = \bigcup_{n=1}^{\infty} (f^{-1}\circ f)^n = (f^{-1}\circ f) \cup [(f^{-1}\circ f)\circ(f^{-1}\circ f)] \cup \cdots \;.$$

I.5. Замечание

Циклические группы, рассмотренные в Утверждении В.3, иллюстрируют один из способов наделения $(\Sigma A)^1$ групповой структурой при помощи определяющих соотношений. Его можно свести к следующему построению. Пусть $A = A' \cup A''$, $|A'| = |A''|$ (A' и A'' – равномощны) и $A' \cap A'' = \emptyset$. Пусть $\eta : A' \to A''$ – фиксированное сюрективное и инъективное отображение. Положим $a''a' = a'a'' = 1$ для всех $a' \in A'$ и $a'' \in A''$. Тогда $(\Sigma A)^1$ превращается в группу. В более общем случае определяют на $(\Sigma(A' \cup A''))^1$ отношение

$$\rho_0 = \{(a'a'', 1) \mid a' \in A'\} \cup \{(a''a', 1) \mid a' \in A'\}$$

и строят конгруэнцию ρ , порожденную ρ_0 . Тогда $(\Sigma A)^1|_\rho$ есть группа, называемая свободной.

2. Билатеральная эквивалентность $\mathcal{P}_{\{\phi\}}$ на ΣA и машины $f : \Sigma A \to B$ с полугруппой $\Sigma A|\mathcal{R}_{\{\phi\}}$

2.I. Замечание

Из Теоремы I.2. стало видно, что реализация групповой структуры на $\Sigma A|_{\equiv_f}$ при сохранении строго полугрупповой на ΣA , невозможна. На основе одной теоремы Круазо мы определим главную конгруэнцию Дюбрея $\mathcal{P}_{\{\emptyset\}}$ (билатеральную эквивалентность), порождающую на $\Sigma A|\mathcal{P}_{\{\emptyset\}}$ структуру группы. Затем определим класс машин, полугруппы которых являются фактор-группами полугруппы ΣA по mod $\mathcal{P}_{\{\emptyset\}}$.

2.2. Замечание

Известно, что на полугруппах вообще нельзя определить когруэнцию при помощи только одного класса эквивалентности разбиения (как в теории групп). Но для некоторых типов конгруэнции это возможно; например, в интересующем нас случае, когда S – полугруппа, а ρ – такая конгруэнция на S, что $S|\rho$ есть группа.

Напомним еще, что если подгруппа H группы G является нормальным делителем в G, то H определяет на G конгруэнцию. В частности, если $g_1 \equiv g_2 (mod;\rho)$; $g_1, g_2 \in G$ тогда и только тогда, когда $g_1 \cdot g_2 \in H$, то ρ есть правая конгруэнция, классами эквивалентности которой являются множества gH, $g \in G$.

2.3. Определение

а) пусть U – подполугруппа полугруппы S. Говорят, что U унитарна слева (справа), если из $u \in U$, $s \in S$ и $us \in U$ ($su \in U$) следует $s \in U$. U унитарна, если она унитарна слева и справа.

б) пусть H – произвольное подмножество полугруппы S. Для любого $a \in S$ определяем подмножество произведения $S \times S$

$$H..a = \{(x,y) \in S \times S \mid xay \in H\}.$$

в) отношение $\mathcal{P}_H$, определяемое на S

$$\mathcal{P}_H = \{(a,b) \in S \times S \mid H..a = H..b\},$$

является отношением эквивалентности и конгруэнцией на S, называемой главной конгруэнцией на S, соответствующей подмножеству H.

г) подмножество H из S называется бисильным в S, если для всех $a, b \in S$ из $(H..a) \cap (H..b) \neq \emptyset$ следует $(H..a) = (H..b)$.

д) Бивычетом W множества H называется множество

$$W = \{a \in S \mid H..a = \emptyset\}.$$

2.4. Лемма

Пусть подполугруппа S свободной полугруппы ΣA свободна. Очевидно, тогда существует $A^* \subseteq A$ такое, что $S = \Sigma A^*$ и выполняется следующее утверждение.

а) подполугруппа ΣA^* полугруппы ΣA унитарна.

б) $\mathcal{P}_{\Sigma A^*}$ является конгруэнцией с сокращениями.

в) ΣA^* бисильна в ΣA.

Доказательство

а) Пусть $a \in \Sigma A^*$, $b \in \Sigma A$ и $ab \in \Sigma A^*$. Но полугруппа свободна тогда и только тогда, когда любой ее элемент может быть однозначно представлен как произведение из элементов ее порождающего множества. Следовательно, $b \in \Sigma A^*$. Аналогично показывается, что ΣA^* унитарна и справа.

б) $\mathcal{P}_{\Sigma A^*}$ конгруэнция по определению. Отношение $(x,y) \in H..ac$ эквивалентно $(xc,y) \in H..a$; но $(xc,y) \in H..b$ эквивалентно $(x,y) \in H..cb$. Следовательно, $(H..a) \subseteq (H..b)$. Аналогично показывается и обратное включение. Таким же путем можно доказать, что $\mathcal{P}_{\Sigma A^*}$ сократима и слева. (Здесь заметим, что если S – полугруппа с сокращениями и ρ – конгруэнция с сокращениями, то фактор – полугруппа $S|\rho$ также является полугруппой с сокращениями).

в) из определения свободной полугруппы следует, что если $(\Sigma A^*..a) \cap (\Sigma A^*..b) \neq \emptyset$, то $a, b \in \Sigma A^*$. Тогда, если для $x, y \in \Sigma A$, $xay \in \Sigma A^*$, то $x, y \in \Sigma A^*$ и, следовательно, $xby \in \Sigma A^*$. Аналогично показывается и обратное –

$$(\Sigma A^*..b) \subseteq (\Sigma A^*..a).$$

2.5. Замечание

Подполугруппа S свободной полугруппы не обязательно свободна. Для наших целей, однако, не нужно выполнения условий Леммы 24. для произвольных подполугрупп свободной полугруппы ΣA.

2.6. Замечание

Мы уже использовали обозначение S^1. Обычно под ним понимают объединение $S \cup 1$, где $1 \bar{\in} S$ и $1s = s1 = s$ для всех $s \in S$. Таким образом, S^1 – это моноид с нормальным элементом 1 и для свободной полугруппы его можно поставить в однозначном соответствии с пустым множеством $\varnothing$.

В этом случае мы отклонимся от установленного определения для ΣA и будем считать $\Sigma\{\varnothing\}$ хорошо дефинированной свободной полугруппой. Естественно, $\{\varnothing\} \neq \varnothing$.

Более того, будем предполагать, что $\varnothing$ содержится во всех подмножествах множества A.

2.7. <u>Лемма</u>

Если $A^* = \{\varnothing\}$, то бивычет $W = \{\alpha \in \Sigma A \mid \Sigma A^* \cdot\cdot\, \alpha = \varnothing\}$ пуст.

2.8. <u>Теорема (Круазо[7])</u>

Если ρ – такая конгруэнция на ΣA, что $\Sigma A|_\rho$ является группой и $\{\varnothing\}$ – единица группы $\Sigma A|_\rho$, то $\{\varnothing\}$ – есть бисильная унитарная подполугруппа с пустым вычетом и, кроме того, $\rho = \mathcal{P}_{\{\varnothing\}}$.

Обратно, пусть H – бисильная подполугруппа полугруппы ΣA и ее бивычет пуст. Тогда H содержится в некотором $\mathcal{P}_H$ классе. $\{\varnothing\}$ и $\{\varnothing\}$ – есть бисильная унитарная подполугруппа из ΣA с пустым вычетом. $\mathcal{P}_H = \mathcal{P}_{\{\varnothing\}}$ и $\Sigma A|_{\mathcal{P}_{\{\varnothing\}}}$ является группой.

Соответствие между $\{\varnothing\}$ и $\mathcal{P}_{\{\varnothing\}}$, описанное выше, является взаимно однозначным.

2.9. <u>Следствие</u>

Если $\alpha, \beta \in \Sigma A$ и $\alpha \equiv \beta (\mathrm{mod}\ \mathcal{P}_{\{\varnothing\}})$, то

$$\{(x,y) \in \Sigma A \times \Sigma A \mid x\alpha y \in \{\varnothing\}\} = \{(\bar{x},\bar{y}) \in \Sigma A \times \Sigma A \mid \bar{x}\beta\bar{y} \in \{\varnothing\}\}.$$

Интерпретируя $f^{-1} \circ f$ как отношение, порожденное $f: \Sigma A \to B$, получаем

$$\alpha \equiv \beta (\mathrm{mod}\ \mathcal{P}_{\{\varnothing\}}) \Leftrightarrow f(x\alpha y) = f(x\beta y)$$

для тех $x, y \in (\Sigma A)^1$, для которых одновременно $x\alpha y$ и $x\beta y$ принадлежат некоторому фиксированному $\xi\, \Sigma\{\varnothing\}\, \eta$; $\xi, \eta \in \Sigma A$.

Работа выполнена в Отделе развития и эксплуатации математического обеспечения и имеет отношение к некоторым проблемам организации системы ЭВМ.

Авторы выражают В.П.Ширикову свою благодарность за обсуждения.

ЛИТЕРАТУРА

1. J.Hartmanis, R.Stearns (1966), Algebraic Structure Theory of Sequential Machines, Prentice-Hall, Inc., Englewood Cliffs, N.J.
2. M.Arbib, J.Rhodes, B.Tilson (1968), Complexity and group Complexity of Finite-State Machines and Finite Semigroups, Chapter 6 in /4/.
3. Р.Калман, П.Фалб, М. Арбиб, (1969), Очерки по математической теории систем, Москва, "Мир" 1971.
4. M.Arbib (ed) (1968), The Algebraic Theory of Machines, Languages and Semigroups, Chapters 1, 5-9, Academic Press, N.J. and London.
5. K.Krohn, R.Mateosian, J.Rhodes (1967), Methods of the Algebraic Theory of Machines I, J.Computer System Sci., Vol 1, 55-85.
6. B.Tilson (1971), Decomposition and Complexity of Finite Semigroups, Semigroup Forum, Vol 3, 189-250.
7. R.Croisot (1957), Equivalences principales bilatère définies dans un demi-groupe, J.Math. Pures Appl. (9) 36, 373-417.
8. А.Клиффорд, Г.Престон (1967). Алгебраическая теория полугрупп, том 2, "Мир", Москва 1972.

Рукопись поступила в издательский отдел
20 июля 1973 года.