Math-Net.Ru

Общероссийский математический портал

С. В. Алешин, Об одном следствии теоремы Крона–
Роудза, *Дискрет. матем.*, 1999, том 11, выпуск 4, 101–
109

DOI: <https://doi.org/10.4213/dm392>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 3.85.7.115

26 апреля 2023 г., 16:49:41

УДК 519.7

Об одном следствии теоремы Крона–Роудза

© 1999 г. С. В. Алешин

Теорема Крона–Роудза о каскадных соединениях автоматов была доказана в предположении, что базис содержит специальные групповые автоматы. В настоящей статье показывается, что при наличии в базисе константных автоматов это ограничение может быть снято и для любой простой группы G достаточно взять любой групповой автомат, группа которого имеет G в качестве делителя.

Будем использовать основные понятия из [2]. Обозначим через E_2^n множество наборов из 0, 1 длины n , P_{bd}^n — множество всех ограниченно-детерминированных функций (о.-д. функций) от n переменных. Если $f(x_1, \dots, x_n) \in P_{bd}^n$, то существует единственный инициальный автомат $\mathcal{A}_f$ с n входами и выходом, с попарно отличимыми достижимыми состояниями (приведенный автомат), который реализует (вычисляет) функцию $f(x_1, \dots, x_n)$, $\mathcal{A}_f = (E_2^n, Q, E_2, \varphi, \psi)$. В каждом состоянии $q \in Q$ автомата $\mathcal{A}_f$ реализуется некоторая функция алгебры логики $\psi(q, x_1, \dots, x_n)$. Через $O_{bd}^{n,m}$ обозначим множество всех о.-д. (n, m) -операторов, то есть наборов о.-д. функций вида $W = (f(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n))$ таких, что все функции оператора имеют одинаковый набор переменных. Для каждого о.-д. оператора W существует единственный приведенный автомат $\mathcal{A}_W = (E_2^n, Q, E_2^m, \varphi, \psi)$, реализующий оператор W . В каждом состоянии q автомата $\mathcal{A}_W$ реализуется некоторый булев оператор $\psi(q, x_1, \dots, x_n)$.

Пусть $\mathcal{A}_f$ — автомат, реализующий о.-д. функцию f . Входная буква $a \in E_2^n$, $a = (a_1, \dots, a_n)$, индуцирует подстановку π_a на множестве состояний автомата по правилу $\pi_a(q) = \varphi(q, a)$, $q \in Q$.

Входное слово $\alpha = a(1)a(2)\dots a(s)$ длины s индуцирует подстановку $\pi_\alpha = \pi_{a(s)}\pi_{a(s-1)}\dots\pi_{a(1)}$, равную произведению подстановок, входящих в α букв (мы используем для записи произведения подстановок порядок, соответствующий порядку применения подстановки к элементам множества:

$$\pi_{ab}(q) = (\pi_b\pi_a)(q) = \pi_b(\pi_a(q)).$$

Таким образом, с автоматом $\mathcal{A}_f$ связана полугруппа подстановок на множестве Q , порожденная множеством подстановок π_a , $a \in E_2^n$. В силу единственности автомата $\mathcal{A}_f$ эта полугруппа определена однозначно, обозначим ее через Π_f . В случае, когда Π_f является группой, назовем автомат (и функцию) групповым.

Аналогично можно говорить о полугруппе о.-д. оператора Π_W , поскольку в определении полугруппы выходная функция не участвует.

Очевидно, что если G — абстрактная группа, то существует много различных о.-д. функций (и операторов), полугруппы которых изоморфны группе G .

Однако, в определенном смысле, для любой полугруппы G можно указать о.-д. функцию (оператор), которая единственным образом строится по G .

Пусть $\xi: E_2^n \rightarrow E_2^n$ — некоторое отображение. Распространим действие ξ на слова в алфавите E_2^n ; для $\alpha = a(1)a(2)\dots a(s)$, $a(i) \in E_2^n$, $i = 1, \dots, s$, положим

$$\xi(\alpha) = \xi(a(1))\xi(a(2))\dots\xi(a(s)).$$

Напомним, что о.-д. оператор $W(x_1, \dots, x_n)$, т. е. отображение

$$(E_2^*)^n \rightarrow (E_2^*)^m$$

может рассматриваться как отображение

$$(E_2^n)^* \rightarrow (E_2^m)^*,$$

т. е. множество всех слов в алфавите E_2^n отображается в множество всех слов в алфавите E_2^m .

Будем говорить, что два (n, m) -о.-д. оператора W_1, W_2 изоморфны, если существуют взаимно однозначные отображения

$$\xi: E_2^n \rightarrow E_2^n, \quad \eta: E_2^m \rightarrow E_2^m$$

такие, что $\eta(W_1(\alpha)) = W_2(\xi(\alpha))$ для любого слова α в алфавите E_2^n , т. е. коммутативна диаграмма

$$\begin{array}{ccc} (E_2^n)^* & \xrightarrow{W_1} & (E_2^m)^*, \\ \downarrow \xi & & \downarrow \eta \\ (E_2^n)^* & \xrightarrow{W_2} & (E_2^m)^*. \end{array}$$

Пусть теперь G — некоторая абстрактная полугруппа с единицей, $|G| = r$ и n — наименьшее целое такое, что $n \geq \log_2 r$. Всякое отображение E_2^n на G будем называть кодированием. Если $\gamma: E_2^n \rightarrow G$ — кодирование, то для всякого элемента $g \in G$ найдется набор $a = (a_1, \dots, a_n) \in E_2^n$ такой, что $\gamma(a) = g$.

Зафиксируем некоторое кодирование γ и рассмотрим автомат

$$\mathfrak{A} = (E_2^n, G, E_2^n, \varphi, \psi)$$

с n входами и n выходами, множество состояний которого совпадает с множеством элементов полугруппы G , начальное состояние — единичный элемент $e \in G$, а функция переходов соответствует умножению в полугруппе G :

$$\varphi(g, a) = g * \gamma(a).$$

Функция выходов ψ определена следующим образом:

$$\psi(g, a) = \overline{\gamma^{-1}(g)},$$

где $\overline{\gamma^{-1}(g)}$ — произвольный набор из E_2^n такой, что $\gamma(\overline{\gamma^{-1}(g)}) = g$.

Будем называть построенный автомат автоматом полугруппы G , а о.-д. оператор, реализуемый $\mathfrak{A}$, специальным о.-д. оператором полугруппы G . Такое название правомерно, так как справедлива следующая лемма об изоморфизме.

Рис. 1.

Лемма. Любые два специальных о.-д. оператора полугруппы G изоморфны.

Доказательство непосредственно следует из определений.

Нетрудно видеть, что специальный о.-д. оператор полугруппы — это автомат полугруппы в терминологии работы Крона-Роудза с той лишь разницей, что мы кодируем абстрактные алфавиты наборами из 0 и 1.

Обозначим специальный о.-д. оператор полугруппы G через $S_p(G)$. Ясно, что полугруппа оператора $S_p(G)$ есть снова полугруппа G , и мы имеем представление G как полугруппы подстановок, действующих на множестве элементов G . Таким образом, здесь полугруппа G действует на себя как полугруппа подстановок (представление Кэли).

Любой автомат, у которого полугруппа изоморфна группе G , дает нам некоторое представление группы G как группы подстановок на множестве состояний. При этом роль образующих этой группы подстановок играет входной алфавит. Таким образом, разные о.-д. функции с одной и той же (абстрактной) группой отличаются как разные представления этой группы с учетом выбора системы образующих.

Сформулируем теперь теорему Крона-Роудза.

Пусть G_0 — о.-д. функция единичной задержки и T — о.-д. функция триггера. Их диаграммы представлены на рис. 1.

Пусть также $\text{Ch}(x_1, x_2)$ — функция Шеффера, то есть о.-д. функция с одним состоянием, в котором вычисляется штрих Шеффера.

Будем говорить, что группа G — делитель полугруппы Π , если G является гомоморфным образом подгруппы полугруппы Π . Множество всех делителей полугруппы Π обозначим через $\text{Del}(\Pi)$.

Как обычно, знак $[\cdot]_c$ обозначает замыкание множества о.-д. операторов относительно операций суперпозиции.

Пусть $\mathcal{M}$ — множество о.-д. операторов. Через $\text{Del}(\mathcal{M})$ обозначим множество делителей полугрупп операторов из $\mathcal{M}$.

Теорема (Крон-Роудз [1]). Пусть $\mathcal{N}$ — множество о.-д. операторов и $\mathcal{M}$ — множество специальных о.-д. операторов полугрупп. Для того чтобы

$$\mathcal{M} \subseteq [\mathcal{N}, G_0, T, \text{Ch}]_c,$$

необходимо и достаточно, чтобы

$$\text{Del}(\mathcal{M}) \subseteq \text{Del}(\mathcal{N}).$$

Следствие. Чтобы система групповых специальных о.-д. операторов $\mathfrak{N}$ обладала свойством

$$P_{bd} \subseteq [\mathfrak{N}, G_0, T, \text{Ch}]_c$$

необходимо и достаточно, чтобы множество $\text{Del}(\mathfrak{N})$ содержало все простые группы.

Мы покажем, что слово специальные можно убрать, добавив в базис все константные о.-д. функции.

Множество всех константных о.-д. функций обозначим через K .

Теорема 1. Пусть G — простая некоммутативная группа, f — произвольная групповая о.-д. функция такая, что Π_f изоморфна G , и $S_p(G)$ — специальный о.-д. оператор группы G . Тогда

$$S_p(G) \in [f, G_0, Ch, K]_c.$$

Доказательство. Пусть $f(x_1, \dots, x_n)$ реализуется автоматом

$$\mathfrak{A} = (E_2^n, Q, E_2, \varphi, \psi, q_0).$$

Тогда G порождается подстановками $\{\Pi_a, a \in E_2^n\}$. Рассмотрим последовательность подмножеств элементов группы G :

$$\begin{aligned} G_1 &= \{\pi_a, a \in E_2^n\}, \\ G_2 &= \{\pi_{ab}, a, b \in E_2^n\}, \\ &\dots \\ G_k &= \{\pi_{a_1 a_2 \dots a_k}, a_i \in E_2^n\}, \\ &\dots \end{aligned}$$

В силу конечности группы G эта последовательность, начиная с некоторого t , периодическая, то есть

$$\Gamma = \{G_t, G_{t+1}, \dots, G_{t+s}, G_t, \dots\}.$$

Очевидно, мощности G_i совпадают при $i \geq t$, так как

$$|G_i| \leq |G_{i+1}| \leq |G_i|.$$

Предположим, что $|G_i| < G$. Тогда G действует на элементах последовательности Γ как циклическая группа порядка s , а отображение

$$\pi_{a_1 a_2 \dots a_m} \rightarrow m \pmod{s}$$

есть гомоморфизм G на Z_s . В силу простоты G справедливы равенства $s = 1$, $G_i = G$.

Таким образом, существует r такое, что любой элемент группы G может быть представлен словом длины r :

$$g \rightarrow \pi_{a_1 a_2 \dots a_r}.$$

Обозначим слово длины r , представляющее элемент g , через $R(g)$.

Теперь покажем, что из о.-д. функции f можно построить о.-д. оператор с группой Π_f , у которого функция выходов в каждом состоянии выдает двоичный код номера состояния.

Так как у автомата $\mathcal{A}$, вычисляющего f , состояния попарно отличимы, для любой пары состояний q_i, q_j найдется слово α_{ij} такое, что $\psi(q_i, \alpha_{ij}) \neq \psi(q_j, \alpha_{ij})$.

Обозначим через α_{ij}^{-1} слово во входном алфавите E_2^n такое, что слово $\alpha_{ij}\alpha_{ij}^{-1}$ индуцирует тождественную подстановку во множестве состояний, то есть $\alpha_{ij}\alpha_{ij}^{-1}$ — единица группы G .

Тогда слово

$$\beta_f = \alpha_{12}\alpha_{12}^{-1}\alpha_{13}\alpha_{13}^{-1} \dots \alpha_{d-1d}\alpha_{d-1d}^{-1}, \quad |Q| = d,$$

будет отличать любую пару состояний автомата $\mathcal{A}$ и при этом слово β_f является единицей группы G :

$$\varphi(q, \beta) = q, \quad q \in Q, \quad \psi(q, \beta) \neq \psi(q', \beta), \quad q \neq q'.$$

Рассмотрим о.-д. оператор B с n входами и n выходами, который осуществляет следующее преобразование последовательностей букв алфавита E_2^n в последовательности букв алфавита E_2^n :

$$B: (E_2^n)^* \rightarrow (E_2^n)^*.$$

Пусть $\alpha_1\alpha_2\alpha_3 \dots$ — последовательность слов, каждое длины $r + p$, где r — такое число, что для любого элемента $g \in G$ существует слово $R(g)$ в алфавите E_2^n , которое индуцирует g , а число p — это длина последовательности β_f .

Тогда, если на входе оператора B появляется слово вида

$$\alpha_1\alpha_2\alpha_3 \dots,$$

то на его выходе появляется слово в алфавите E_2^n вида

$$R(e)\beta_f R(\alpha_1)\beta_f R(\alpha_2)\beta_f \dots, \quad R(\alpha_i) = R(\pi_{\alpha_i}), \quad \pi_{\alpha_i} \in G.$$

Такой о.-д. оператор может быть построен из задержки, функции Шеффера и константных о.-д. функций (для примера можно посмотреть, как это делается в работе [3]).

Если выходы оператора B соединить с входами о.-д. функции f , то получится о.-д. функция $\hat{f}$. Сравним ее с f .

Нетрудно видеть, что если под действием последовательности $\alpha_1\alpha_2\alpha_3 \dots$ автомат $\mathcal{A}$ функции f в моменты времени $r + p, 2(r + p), 3(r + p), \dots$ окажется в состояниях соответственно $q_1, q_2, q_3, \dots$, то на выходе $\hat{f}$ в моменты времени соответственно $2r + p, r + 2(r + p), r + 3(r + p), \dots$ появятся слова $\bar{\psi}(q_0, \beta), \bar{\psi}(q_1, \beta), \bar{\psi}(q_2, \beta), \dots$. В силу отличающего свойства последовательности β для состояний нам осталось теперь преобразовать выходную последовательность в последовательность номеров состояний.

Пусть в момент $r + t(r + p)$ на выходе появилось слово γ длины p . По этому слову однозначно определяется состояние автомата $\mathcal{A}$ в момент $t(r + p)$. Так как нам известно и входное слово с момента $t(r + p)$ до момента $(t + 1)(r + p)$, пара (γ, α_t) однозначно определяет номер состояния автомата $\mathcal{A}$ в момент $(t + 1)(r + p)$. Теперь нам достаточно присоединить к выходу $\hat{f}$ соответствующий преобразователь,

Рис. 2.

который может быть построен из задержки, функции Шеффера и константных о.-д. функций.

Продолжая наши построения, считая, что мы уже располагаем о.-д. оператором, у которого группа есть G , а выходная функция в каждый момент выдает двоичный код номера состояния.

Так как существует r такое, что любой элемент группы реализуется как входное слово длины r , нетрудно видеть, что в силу транзитивности группы G всякое состояние автомата $\mathcal{A}$ достижимо из начального некоторым словом длины r .

Обозначим через γ_i слово, которое переводит $\mathcal{A}$ из начального состояния в состояние q_i .

Пусть i , $1 \leq i \leq |Q|$, — натуральное число. Рассмотрим отображение C_i множества последовательностей в алфавите E_2^m в множество последовательностей в алфавите E_2^n

$$C_i: (E_2^m)^* \rightarrow (E_2^n)^*,$$

$m \geq \log_2 G$, $\xi: E_2^m \rightarrow G$ — кодирование G такое, что, если начало входного слова длины r индуцирует подстановку на множестве Q , $d = |Q|$, состояний автомата $\mathcal{A}$ вида

$$\xi(a(1)) * \xi(a(2)) * \dots * \xi(a(r)) = \begin{pmatrix} 1 & 2 & \dots & i & \dots & d \\ l_1 & l_2 & \dots & l_i & \dots & l_d \end{pmatrix},$$

где $*$ — умножение в G , то начало выходного слова длины r — это слово γ_{l_i} , переводящее $\mathcal{A}$ из начального состояния в состояние l_i . Последующие куски входного слова длины r переводятся в слова во входном алфавите автомата $\mathcal{A}$ так, что элемент группы G , равный $\xi(a(1)) * \xi(a(2)) * \dots * \xi(a(r))$, где ξ — кодирование, совпадает с элементом группы Π_f , который индуцируется словом $C_i(a(1)a(2)\dots a(r))$.

Рассмотрим схему, приведенную на рис. 2.

Нетрудно видеть, что на выходах этой схемы с задержкой r появляются наборы двоичных кодов подстановок такие, что если на вход схемы к моменту t поступило входное слово, являющееся кодом подстановки $\pi \in G$,

$$\pi = \begin{pmatrix} 1 & 2 & \dots & d \\ l_1 & l_2 & \dots & l_d \end{pmatrix},$$

из группы G , то на выходе в момент $t + r$ появится набор двоичных кодов вида

$$(l_1, l_2, \dots, l_d).$$

Теперь тем же приемом, что и выше, можно достроить эту схему до схемы, реализующей специальный о.-д. оператор группы G . При этом все построения требовали только использования задержки, булевых операторов и константных автоматов. Теорема доказана.

Эта теорема, однако, требует наличия автомата, группа которого изоморфна данной простой группе G . Мы усилим результат, если вместо автомата с группой G возьмем автомат, группа которого имеет G в качестве делителя.

Теорема 2. Пусть G — простая нециклическая группа, f — произвольная групповая о.-д. функция такая, что группа Π_f имеет G в качестве делителя. Тогда

$$S_p(G) \in [f, G_0, \text{Ch}, K]_c.$$

Доказательство. Пусть в Π_f имеется подгруппа P , гомоморфным образом которой является G , и φ — этот гомоморфизм. Пусть Π_f порождается подстановками π_a , $a \in E_2^n$. Как и в доказательстве предыдущей теоремы, рассмотрим последовательность подмножеств группы Π_f

$$\Pi_1 = \{\pi_a, a \in E_2^n\}, \quad \Pi_2 = \{\pi_{a,b}, a, b \in E_2^n\}, \quad \dots$$

Эта последовательность периодическая, начиная с некоторого t .

Рассмотрим также последовательность

$$\Gamma_l = \Pi_l \cap P, \quad l \geq t.$$

Предположим, что для всякого i

$$\varphi(\Gamma_l) \neq G, \quad \varphi(\Gamma_l) = G_l.$$

Пусть $\alpha_1, \dots, \alpha_d$ — слова такие, что $\alpha_i \in P$ и $\{\varphi(\alpha_i, i = 1, \dots, d)\}$ — система образующих в группе G . Такие слова очевидно найдутся в силу гомоморфизма φ . Заметим, что $R\Pi_{\alpha_i} = P$ для всякого i .

Таким образом, подстановки π_{α_i} действуют на элементах последовательности, а соответственно элементы $\varphi(\alpha_i)$, $i = 1, \dots, d$, группы G действуют на наборе $\{\Gamma_t, \Gamma_{t+1}, \dots, \Gamma_{t+s}\}$ как элементы циклической группы. Поэтому мы можем указать гомоморфизм группы G на циклическую группу Z_s так, что

$$\varphi(\alpha_i)(m) = m + \partial(\alpha_i) \pmod{s}.$$

Так как G — простая группа, наше предположение, что $\varphi(\Gamma_l) \neq G$, противоречиво.

Таким образом, существует такое натуральное r , что множество Π_r содержит полный прообраз группы G относительно гомоморфизма φ , то есть существует r такое, что для всякого элемента $g \in G$ найдется слово $\alpha_g = a(1)a(2) \dots a(r)$ во входном алфавите, которое задает на множестве Q подстановку π такую, что $\varphi(\pi) = g$.

Пусть теперь ξ — некоторое кодирование группы G наборами длины m и p — длина диагностического слова β , то есть такой единицы группы Π_f , которая отличает любые два состояния автомата.

Построим преобразователь из алфавита E_2^m в алфавит E_2^n , который куски входного слова длины $p + r$ последовательно заменяет на слова в алфавите E_2^n так, что слово

$$\alpha_1 \alpha_2 \alpha_3 \dots, \quad \partial(\alpha_i) = p + r, \quad \alpha_i = a^i(1) a^i(2) \dots a^i(p + r),$$

переходит в слово

$$\gamma_0 \beta \gamma_1 \beta \gamma_2 \beta \gamma_3 \beta \dots, \quad \partial(\gamma_i) = r,$$

где π_{γ_0} — единица G , при этом

$$\varphi(\pi_{\gamma_i}) = \xi(a^i(p + r)) * \gamma(a^i(p + r - 1)) * \dots * \xi(a^i(1)),$$

где $*$ — умножение в G .

Построим схему Σ

Как при доказательстве теоремы 1, мы можем присоединить к выходу схемы преобразователь так, что теперь на выходе схемы появляются двоичные коды номеров состояний автомата $\mathcal{A}$. Пусть Q' — множество всех состояний, номера которых появляются на выходе схемы при подаче всевозможных входных последовательностей. Это множество состояний можно назвать множеством, выделяемым групповым делителем G группы Π_f . Нетрудно видеть, что делитель G транзитивно действует на множестве Q' ; кроме того, существует такое r , что всякое состояние Q' достижимо из начального словом длины r (в алфавите E_2^m). Таким образом, мы можем применить технику доказательства теоремы 1 в полном объеме: взять прямое произведение автоматов для моделирования специального о.-д. оператора группы G . Теорема доказана.

Заметим, что требование быть групповым для автомата из теоремы 2 нам понадобилось лишь для того, чтобы гарантировать существование диагностической единицы. В случае произвольной негрупповой о.-д. функции, вообще говоря, не удастся построить единицу полугруппы, различающую состояния. Можно, однако, развить эту идею для подгрупп полугруппы автомата в случае, когда имеется множество состояний, сохраняемых этой подгруппой и среди единиц подгруппы есть диагностическая.

Теорема 3. Пусть $\mathcal{M}$ — множество групповых о.-д. операторов. Равенство

$$P_{bd} = [\mathcal{M}, G_0, \text{Ch}, T, K]_c$$

справедливо тогда и только тогда, когда для любой простой нециклической группы G найдется $f \in \mathcal{M}$ такая, что G делит Π_f .

Доказательство. Необходимость следует из теоремы Крона–Роудза, а достаточность — из теоремы 2.

Следствие. Система всех о.-д. функций от двух переменных полна в P_{bd} относительно суперпозиции.

Рис. 3.

В самом деле, достаточно для каждого n взять автомат с одним входом и n состояниями, группа которого есть полная симметрическая группа на n элементах. Любая простая группа является делителем некоторой симметрической группы, что и требовалось доказать.

Заметим, что полнота системы функций двух переменных была доказана в [3].

Два следующих примера показывают, что примененные нами средства являются в известном смысле минимальными.

Первый пример показывает важную роль константных о.-д. функций. Если из системы $\tilde{\Phi}$ (см. теорему 3.12 в [2]) выбросить любую функцию, то оставшаяся часть не будет полной. Но если мы имеем все константные функции, то для полноты достаточно добавить к ним любую бесконечную подсистему системы $\tilde{\Phi}$.

Второй пример говорит о том, что групповой делитель может быть спрятан в полугруппе автомата так, что для его извлечения необходимо использовать негрупповые элементы полугруппы автомата.

Из диаграммы автомата на рис. 3 видно, что входные буквы $\{e, a\}$ порождают на множестве состояний автомата группу Z_2 .

Они оставляют на месте множество q_1, q_2 и на этом множестве Z_2 точно представлена подстановками e, a . Однако, чтобы отличить эту пару состояний, необходимо использовать эксперимент bb , который выводит автомат из группы состояний q_1, q_2 , кроме того для элемента bb в полугруппе $\mathcal{A}$ нет обратного элемента. Поэтому с помощью автомата $\mathcal{A}$ нельзя моделировать групповую о.-д. функцию $S_p(Z_2)$ и даже ее константную последовательность периода 2.

Список литературы

1. Арбиб М.А., *Алгебраическая теория автоматов, полугрупп и языков*. Наука, Москва, 1975.
2. Кудрявцев В.Б., Алешин С.В., Подколзин А.С., *Введение в теорию автоматов*. Наука, Москва, 1985.
3. Бабин Д.Н., О полноте двуместных о.-д. функций относительно суперпозиции. *Дискретная математика* (1989) 1, №4, 86–91.

Статья поступила 15.02.1999.