FILOMAT (Niš) 9:3 (1995), 699–710
Algebra, Logic & Discrete Mathematics
Niš, April 14–16, 1995.

ЕЩЕ О ПРОБЛЕМЕ ВКЛЮЧЕНИЯ РЕГУЛЯРНЫХ И ЛИНЕЙНЫХ ЯЗЫКОВ В ГРУППОВЫЕ ЯЗЫКИ

Красимир Янков Йорджев

1. Введение

Пусть G - группа с множеством образующих

$$X = \Sigma \cup \Sigma^{-1} = \{x_1, x_2, ..., x_n, x_1^{-1}, x_2^{-1}, ..., x_n^{-1}\},$$

определяющими соотношениями θ, единицей e и с разрешимой проблемой равенства слов. Тогда множество слов $\mathcal{M} = \{\omega = x_{i_1}^{k_1} x_{i_2}^{k_2} \cdots x_{i_t}^{k_t} | \omega = e\} \subseteq \Sigma^*$ называется групповым языком, задающим группу G. Σ^* - это свободный моноид над Σ. Группа G задается контекстно-свободным языком, если соответствующий групповой язык $\mathcal{M}$ является контекстно-свободным. Группа G в этом случае называется контекстно-свободной группой. Ряд свойств групповых языков рассмотрены в [1, 2, 3, 4].

В [12] показано, что проблема включения и эквивалентности конечно-автоматных отображений алгоритмически разрешима. Этот результат стимулирует попытки найти полиноминальный алгоритм проверяющий однозначности конечно-автоматных отображений. Такие алгоритмы найдены в [10, 12, 13]. Раньше до выхода этих результатов А. В. Анисимов [3], решает более общую задачу. Он доказывает, что проблема определения однозначности конечно-автоматных отображений являются частным случаем проблемы включения контекстно-свободных языков в групповые языки. В работе [3] А. В. Анисимов предлагает алгоритм для проверки включения произвольного контекстно-свободного языка L в групповой язык $\mathcal{M}$ группы с разрешимой проблемой равенства слов. В предлагаемом алгоритме находится конечное множество W_1 тако е, что $W_1 \subseteq \mathcal{M}$ тогда и т олько тогда, когда $L \subseteq \mathcal{M}$. Более конкретно доказывается следующая теорема.

Теорема 1. *Пусть $\Gamma = (N, \Sigma, \Pi)$ контекстно-свободная грамматика, порождающая контекстно-свободный язык L, а $\mathcal{M}$ - групповой язык группы G с разрешимой проблемой равенства слов. Пусть Ω_1 - множество всех слов*

из L длиной меньше или равной p , а $\Omega_2 = \{uwvw^{-1} | \ |uwv| \leq q, \ uv \neq \varepsilon, \ \exists S \in N : S \Rightarrow uSv, S \Rightarrow w\}$, где p и q суть константы из известной $xuwvy$ - теоремы (см. напр. [5]). Тогда $L \subseteq \mathcal{M}$ тогда и только тогда, когда $W_1 = \Omega_1 \cup \Omega_2 \subseteq \mathcal{M}$.

Все необходимые сведения и обозначения из теории контекстно-свободных языков можно найти например в [5] или [7].

Цель настоящей работы - модифицировать алгоритм А. В. Анисимова так, чтобы он работал за полиномиальное время. Это мы сделаем для регулярных языков и для линейных языков, используя специфические свойства этих языков. Эта работа продолжение и дополнение работы [8]. Здесь мы опишем новые конечные множества, с помощью которых проверяется включение $L \subseteq \mathcal{M}$.

Диаграммой переходов будем называть четверку $H = (V, R, S, l)$, где (V, R) - конечный ориентированный граф с множеством вершин V и множеством ребер R, S - полугруппа, элементы которой будем называть метками, а l - функция из R в S, называемая функция разметок. Другими словами, каждое ребро графа помечено некоторым элементом полугруппы S. Если π - путь в диаграмме переходов H , то метка пути $l(\pi)$ - это произведение меток ребер, составляющих этот путь, причем метки берутся в порядке прохождения ребер. Если P - множество путей в H , то $l(P)$ будет множество $\{\omega \,|\, \exists \pi \in P : l(\pi) = \omega\}$

2. Включение регулярных языков в групповые языки

В теореме 1 утверждается, что для контекстно-свободного языка L можно конструктивным путем найти конечное множество $W_1 = \Omega_1 \cup \Omega_2$, такое, что L включается в данный групповой язык $\mathcal{M}$ группы G с разрешимой проблемой равенства слов, тогда и только тогда, когда W_1 включается в $\mathcal{M}$. В этом параграфе решим более конкретную задачу для регулярных языков, которые являются важным частным случаем контекстно-свободных языков и найдем еще два множества, обладающих этим свойством. Эти мно -жества будут различаться W_1 и между собой.

Пусть L - регулярный язык. Тогда существует конечный автомат - распознаватель (детерминированный или недетерминированный)

$$A = (Q, \Sigma, \delta, q_1, Z)$$

такой, что $L = T(A)$, где $Q = \{q_1, q_2, ..., q_n\}$- множество состояний;$\Sigma = \{x_1, x_2, ..., x_m\}$- входной алфавит; δ- функция переходов; q_1- начальное состояние;Z- множество заключительных состояний; $T(A)$- множество слов распознаваемых A. Построим диаграмму переходов $H_A = (Q, R, \Sigma^*, l_A)$, где множество вершин Q совпадает с множеством состояний автомата A; множество ребер R образовано следующим образом: $\rho \in R$, где $\rho =$

(q_i, q_j), тогда и только тогда, когда существует $x \in \Sigma \cup \{\varepsilon\}$ такое,что $q_j \in \delta(q_i, x)$ и при этом $l_A(\rho) = x$. ε - это пустое слово. Тогда слово $\omega \in L = T(A)$ тогда и только тогда, когда существует путь π в H_A с началом q_1, концом - элемент из Z и с метко цхар26 пути ω. Пусть G - группа с множеством образующих $X = \{x_1, x_2, ..., x_m, x_1^{-1}, x_2^{-1}, ..., x_m^{-1}\}$ и пусть $\mathcal{M}$ - соответствующий групповой язык. Рассмотрим диаграмму переходов $H_G = (Q, R, G, l_G)$ с тем же множеством вершин и ребер как и в H_A, только метки ребер считаем как элементы группы G.

Пусть $F_G = (2^G, \cup, \cdot, \phi, \{e\})$ - замкнутое полукольцо с элементами всех подмножеств группы G, включая и пустое множество. Операции в F_G будут соответственно обьединение и произведение множеств, единичный элемент - это множество $\{e\}$, содержащее только единицу e группы G, а нулевой элемент - пустое множество ϕ. Замкнутые полукольца и их приложения хорошо изучены в [11]. Это понятие дефинированно и используется и в [6, 9].

В замкнутом полукольце F_G определяем бинарную операцию $[x, y]$ следующим образом: если $a, b \in G$, то $[\{a\}, \{b\}] = \{aba^{-1}\}$ и для $x, y, z \in F_G$ выполнено $[x \cup y, z] = [x, z] \cup [y, z]$ и $[x, y \cup z] = [x, y] \cup [x, z]$. Очевидно, это корректно введенная операция в силу дистрибутивного закона в F_G.

Пусть P - множество всех путей в H_G с началом q_1 и концом - элемент из Z. Тогда очевидно $L \subseteq \mathcal{M}$ тогда и только тогда, когда $l_G(P) = \{e\}$.

Пусть P_1 - множество всех путей из P не содержащих циклов и пусть $\Omega_3 = l_G(P_1)$.

Элементарным циклом назовем цикл в H_G без кратных вершин, т.е. цикл типа $(q_{i_1}, q_{i_2})(q_{i_2}, q_{i_3}) \cdots (q_{i_{k-1}}, q_{i_k})(q_{i_k}, q_{i_1})$, где $q_{i_s} \neq q_{i_t}$ для $s \neq t$ и пусть C - множество элементарных циклов в H_G. Тогда, если π - путь из P , то, очевидно, π принадлежит P_1 или π можно представит, в виде $\pi = \pi_1\pi_2\pi_3$, где π_1 не содержит циклов $\pi_2 \in C$, а π_3 начинает с конца π_1 и кончает в элементе из Z. Но тогда и пути $\pi_1\pi_2^k\pi_3$, $k = 0, 1, 2, ...$ тоже принадлежат P.

Рассмотрим множество Ω_4 , состоящее из всех элементов группы G вида $\alpha = uvu^{-1}$, где $u = l_G(\pi_1)$ для некоторого пути $\pi_1 \in H_G$ с началом q_1 и не имеющих циклов, $v = l_G(\pi_2)$ для некоторого пути $\pi_2 \in C$, переходящих через конца π_1 и существует путь $\pi_3 \in H_G$ с началом конец π_1 и концом - некоторый элемент из Z. Ω_3 и Ω_4 являются элементами замкнутого полукольца F_G. Полагаем $W_2 = \Omega_3 \cup \Omega_4$.

Обазуем множества путей в H_G, C_{ij}^k, где $i, j, k = 1, 2, ..., n$; $n = |Q|$ следующим образом:

$$C_{ij}^0 = \{\rho | \rho \text{ - ребро из } q_i \text{ в } q_j\}$$
$$C_{ij}^k = C_{ij}^{k-1} \cup C_{ik}^{k-1} C_{kj}^{k-1}, \quad k = 1, 2, ..., n$$

Нетрудно заметить, что C'^k_{ij} состоит только из путей длиной меньше или равной $k+1$ с началом q_i, концом q_j и все узлы, которых кроме быть может начала или конца принадлежат множеству $\{q_1, q_2, ..., q_k\}$.

Рассмотрим следующие элементы замкнутого полукольца F_G:

$\Omega_5 = \{l_G(C'^n_{1j})\}$, где j такое, что $q_j \in Z$;

$\Omega_6 = \{[l_G(C'^n_{1j}), l_G(C'^n_{jj})]\}$, где j такое, что существует путь с началом q_j и концом q_t для некоторого $q_t \in Z$, т.е. $C'^n_{jt} \neq \phi$.

Лемма 1. *В C'^k_{ij}, $k = 2, 3, ..., n$, возможно существование пути содержащего цикла.*

Доказательство. Очевидно для всех $s, t = 1, 2, ..., n$ выполнено $C'^0_{st} \subseteq C'^1_{st} \subseteq \cdots \subseteq C'^n_{st}$. Кроме этого для всех $r, s, t = 1, 2, ..., n$ докажем индукцией по r , что в C'^r_{st} возможно существование пути $(q_s, q_1)(q_1, q_2) \cdots (q_r, q_t)$. В самом деле для $r = 1$ утверждение очевидно. Пусть для $r \leq r_0$ в C'^r_{st} возможно существование пути $(q_s, q_1)(q_1, q_2) \cdots (q_r, q_t)$ и рассмотрим $C'^{r+1}_{st} \subseteq C'^r_{s\ r+1} C'^r_{r+1\ t}$. Из индукционного предположения имеем, что в $C'^r_{s\ r+1}$ возможен путь $(q_s, q_1)(q_1, q_2) \cdots (q_r, q_{r+1})$, и так как $C'^0_{r+1\ t} \subseteq C'^r_{r+1\ t}$ и в $C'^0_{r+1\ t}$ возможно существование реб ра (q_{r+1}, q_t) , то в C'^{r+1}_{st} возможно существование пути $(q_s, q_1)(q_1, q_2) \cdots (q_r, q_{r+1})(q_{r+1}, q_t)$.

Следовательно, в C'^{k-1}_{ik} возможен путь $(q_i, q_1)(q_1, q_2) \cdots (q_{k-1}, q_k)$, а в C'^{k-1}_{kj} возможен путь $(q_k, q_1)(q_1, q_2) \cdots (q_{k-1}, q_j)$. Тогда в $C'^k_{ij} \subseteq C'^{k-1}_{ik} C'^{k-1}_{kj}$ возможен путь $(q_i, q_1)(q_1, q_2) \cdots (q_{k-1}, q_k)(q_k, q_1)(q_1, q_2) \cdots (q_{k-1}, q_j)$ в котором содержится цикл $(q_1, q_2)(q_2, q_3) \cdots (q_{k-1}, q_k)(q_k, q_1)$. Лемма доказана. □

Следствие 1. *Для определенных выше множеств $\Omega_3, \Omega_4, \Omega_5$ и Ω_6 из элементов группы G имеем $\Omega_3 \subseteq \Omega_5$ и $\Omega_4 \subseteq \Omega_6$ при том в общем случае $\Omega_3 \neq \Omega_5$ и $\Omega_4 \neq \Omega_6$.*

Также нетрудно заметить, что в общем случае множества Ω_1 и Ω_2 (если ихние элементы рассматриваем как элементы группы G) из теоремы 1 , введенные А. В. Анисимовым различаются множествами введенными нами в этом параграфе. В силу следующая теорема:

Теорема 2. *Для введенных выше обозначений, следующие условия эквивалентны:*

(i) $L \subseteq \mathcal{M}$;
(ii) $W_1 = \Omega_1 \cup \Omega_2 = \{e\}$;
(iii) $W_2 = \Omega_3 \cup \Omega_4 = \{e\}$;
(iv) $W_3 = \Omega_5 \cup \Omega_6 = \{e\}$.

Доказательство. Так как регулярные языки являются частными случаями контекстно-свободных языков, то эквивалентность условий (i) и (ii) установлена А. В. Анисимовым в [3]. Кроме этого $W_2 \subseteq W_3$ (Следствие 1), т.е. из $W_3 = \{e\}$ следует $W_2 = \{e\}$, или доказали, что из (ив) следует (iii). Чтобы доказать теорему нам достаточно доказать, что из (iii) следует (i) и из (i) следует (iv).

(iii)→(i). Пусть $W_2 = \Omega_3 \cup \Omega_4 = \{e\}$ и пусть $\omega \in L$. Тогда существует путь π в H_A с началом q_1 и концом элемент из Z, такой, что $l_A(\pi) = \omega$. Если π не содержит циклов, то $l_G(\pi) \in l_G(P_1) = \Omega_3 = \{e\}$ и следовательно $\omega \in \mathcal{M}$.

Пусть π содержит цикл. Тогда π содержит элементарный цикл. Другими словами π можно представит, в виде $\pi = \pi_1\pi_2\pi_3$, где

$$l_G(\pi_1)l_G(\pi_2)(l_G(\pi_1))^{-1} \in \Omega_4 = \{e\}.$$

Отсюда следует, что $l_G(\pi_1)l_G(\pi_2) = l_G(\pi_1)$ или все равно $l_G(\pi_1\pi_2\pi_3) = l_G(\pi_1\pi_3)$. Так как $\pi_2 \in C$, то длина π_2 больше 1. Следовательно, существует путь в H_G с меньшей длиной, чем длина π, метка которого равна ω в группе G. Этот процесс сокращения можно продолжать конечное число раз, так как длина ω - конечная. В конце этого процесса получим путь без циклов с меткой равной ω в группе G. Но $l_G(P_1) = \Omega_3 = \{e\}$. Следовательно, $\omega = e$ в группе G т.е. $L \subseteq \mathcal{M}$.

(i)→(iv). Пусть $L \subseteq \mathcal{M}$, т.е. $l_G(P) = \{e\}$ и так как $\Omega_5 \subseteq l_G(P)$, то $\Omega_5 = \{e\}$.

Пусть $z \in \Omega_6$. Тогда z можно представит, в виде $z = uvu^{-1}$, где $u \in l_G(C^n_{1j})$, $v \in l_G(C^n_{jj})$ для некоторого j, такого, что существует путь π_3 с началом q_j, концом элемент из Z и пусть $l_G(\pi_3) = w$. Кроме этого очевидно u -это метка некоторого пути π_1 с началом q_1 и концом q_j, а v - это метка некоторого цикла, проходящего через q_j. Следовательно пути $\pi' = \pi_1\pi_2\pi_3$ и $\pi'' = \pi_1\pi_3$ принадлежат P и так как $L \subseteq \mathcal{M}$, то $l_G(\pi') = l_G(\pi'') = e$ и следовательно $uvw = uw$, т.е. $uvu^{-1} = e$. Следовательно $z = e$ и так как z произвольное, то $\Omega_6 = \{e\}$. Теорема доказана. □

Следующий алгоритм базируется на эквивалентности (i) и (iv) из теоремы 2. Для удобства $i \in Z$ будет означать $q_i \in Z$, а g^k_{ij} - это $l_G(C^k_{ij})$. Здесь k в g^k_{ij} индекс и не означает степень.

Алгоритм 1. *Проверяет включение $L \subseteq \mathcal{M}$ для регулярного языка L и группового языка $\mathcal{M}$ группы G с разрешимой проблемой равенства слов.*

Вход: $g^0_{ij} = l_G(C^0_{ij}), \quad i, j = 1, 2, ..., n$

Выход: Логическая переменная T , получающая стоимость **Истина**, если $L \subseteq \mathcal{M}$ и стоимость **Ложь**, в противном случае. Алгоритм останавливает сразу после получения стоимости T :=**Ложь**.

Начало
1. T :=**Истина;**
2. **Для** $1 \leq k \leq n$ **Делать**
3. **Для** $1 \leq i, j \leq n$ **Делать**
4. $g_{ij}^{k} := g_{ij}^{k-1} \cup g_{ik}^{k-1} g_{kj}^{k-1}$
5. **Конец Делать**
6. **Конец Делать**
7. **Для** $j \in Z$ **Делать**
8. **Если** $g_{1j}^{n} \neq \phi$ **и** $g_{1j}^{n} \neq \{e\}$ **То**
9. **Начало** T :=**Ложь ; Останов Конец ;**
10. **Конец Делать**
11. **Для** $1 \leq j \leq n$ **Делать**
12. **Для** $t \in Z$ **Делать**
13. **Если** $g_{jt}^{n} \neq \phi$ **и** $g_{1j}^{n} \neq \phi$ **и** $g_{jj}^{n} \neq \phi$ **То**
14. **Если** $[g_{1j}^{n}, g_{jj}^{n}] \neq \{e\}$ **То**
15. **Начало** T :=**Ложь ; Останов Конец**
16. **Конец Делать**
17. **Конец Делать**

Конец.

Теорема 3. *Алгоритм 1 выполняется не более $O(n^3)$ операции сложения, произведения и $[x, y]$ элементов из замкнутого полукольца F_G и проверяет включение $L \subseteq \mathcal{M}$, где L - регулярный язык, распознаваемый конечным автоматом A, $\mathcal{M}$ - групповой язык группы G с разрешимой проблемой равенства слов, n - число состояний автомата.*

Доказательство. Согласно теоремы 3 и учитывая аксиомы замкнутого полукольца F_G, то в рядах 9 и 15 алгоритма 1 логическая перементая T принимает стоимость **Ложь** тогда и только тогда, когда L не включается в $\mathcal{M}$. В противном случае T принимает стоимость **Истина**. Следовательно, алгоритм 1 коректно проверяет выполняется ли включение $L \subseteq \mathcal{M}$.

Легко проверить, что строка 4 выполняется не более n^3 раз, причем каждый раз выполняются две операции в замкнутом полукольце F_G. Строки 13 и 14 выполняется не более n^2 раз каждая. Следовательно, алгоритм 1 выполняет не более $O(n^3)$ операции сложения, умножения и $[x, y]$ в замкнутом полукольце F_G. Теорема доказана. □

Следствие 2. *Если операции сложение, умножение и $[x, y]$ в замкнутом полукольце F_G можно выполнить за полиномиальное время, то алгоритм 1 является полиномиальным.*

3. Включение линейных языков в групповые языки

В этом параграфе будем продолжать использовать идею А. В. Анисимова для нахождения конечных множеств, с помощью которых можно определить включается ли данный контекстно-свободный язык в групповой язык группы с разрешимой проблемой равенства слов. Это сделаем для линейных языков. Как известно, класс линейных языков включается в класс контекстно-свободных языков. Анализируя доказательство А. В. Анисимова[3], можно заключить, что задача о проверке включения линейного яз ыка в групповой язык группы с разрешимой проблемой равенства слов решает и задачу о проверке однозначности конечно-автоматного отображения.

В этом параграфе будем рассматривать линейную грамматику $\Gamma = (N, \Sigma, \Pi)$ где $N = \{A_1, A_2, ..., A_n\}$ - множество нетерминалов,

$$\Sigma = \{x_1, x_2, ..., x_m\}$$

- множество терминалов, Π - множество правил, а L будет означать линейный язык $L = L(\Gamma, A_1)$. Контекстно-свободная грамматика $\Gamma = (N, \Sigma, \Pi)$ называется линейной, если все правила в Π имеют вид $A_i \to \alpha A_j \beta$ или $A_i \to \alpha$, где $A, B \in N$ - нетерминалы, α, β - терминалные слова из свободного моноида Σ^*. Язык L называется линейным, если существует линейная грамма тика Γ и нетерминальный символ $A_i \in N$ такие, что $L = L(\Gamma, A_i)$.

Пусть S - моноид с единицей 1. Рассмотрим множество $U_S = S \times S = \{(x, y) | x, y \in S\}$. В U_S вводим операция "o" следующим образом: если (x, y), $(z, t) \in U_S$ то $(x, y) \circ (z, t) = (xz, ty)$. Нетрудно видеть, что U_S с этой операцией моноид с единицей (1,1). Если S - группа, то и U_S будет группа, при этом если $a = (x, y) \in U_S$, то обратным элементом a будет $a^{-1} = (x^{-1}, y^{-1})$. Образуем отображения f_l, f_r, f_d из U_S в S следующим образом:

$$f_l(x, y) = x$$
$$f_r(x, y) = y$$
$$f_d(x, y) = xy$$

Очевидно $f_d(x, y) = f_l(x, y) f_r(x, y)$

Рассмотрим диаграмму переходов $H_\Gamma = (V, R, U_{\Sigma^*}, l_\Gamma)$ с множеством вершин $V = N \cup \{A_{n+1}\}$, где $A_{n+1} \notin N$, U_{Σ^*} - рассматриваемый выше моноид с множеством элементов $\{(\alpha, \beta) | \alpha, \beta \in \Sigma^*\}$ и операцией "o"; множество ребер R образовано следующим образом:

а) если в Π существует правило $A_i \to \alpha A_j \beta$, $A_j, A_j \in N$, то в R существует ребро с началом A_i, концом A_j и меткой (α, β);

b) если в Π существует правило $A_i \to \alpha$, где $A_i \in N$, $\alpha \in \Sigma^*$, то в R существует ребро с началом A_i, концом A_{n+1} и меткой (α, ε), ε -пустое слово.

v) не существуют другие ребра в R, кроме описанных в пунктах а) и б).

Пусть G - группа с множеством образующих

$$X = \Sigma \cup \Sigma^{-1} = \{x_1, x_2, ..., x_m, x_1^{-1}, ..., x_m^{-1}\},$$

множеством определяющих соотношений θ, единицей e и с разрешимой проблемой равенства слов. Пусть $\mathcal{M}$ - соответствующий групповой язык, а U_G - группа, полученная описанным выше способом. Рассмотрим диаграмму переходов $H_U = (V, R, U_G, l_U)$, где множества вершин V и ребер совпадают с соответствующими множествами в диаграмме переходов H_Γ, а метки р ебер считаем как элементы группы U_G. Как и в параграфе 2 можно рассмотреть замкнутые полукольца $F_U = (U_G, \cup, \circ, \phi, \{(e, e)\})$ и $F_G = (G, \cup, \cdot, \phi, \{e\})$. Тогда отображения f_l, f_r и f_d естественным способом можно продолжить. до отображения из F_U в F_G.

В F_G вводим операцию $\langle x, y, z\rangle$ следующим образом: если $a, b, c \in G$, то $\langle\{a\}, \{b\}, \{c\}\rangle = \{abcb^{-1}\}$ и для $x, y, z, t \in F_G$ выполнено:

$$\langle x \cup y, z, t\rangle = \langle x, z, t\rangle \cup \langle y, z, t\rangle$$
$$\langle x, y \cup z, t\rangle = \langle x, y, t\rangle \cup \langle x, z, t\rangle$$
$$\langle x, y, z \cup t\rangle = \langle x, y, z\rangle \cup \langle x, y, t\rangle$$

В силу дистрибутивного закона в F_G, $\langle x, y, z\rangle$ - коректно введенная операция.

Пусть P_Γ - множество всех путей в H_Γ с началом A_1 и концом A_{n+1}, а P_U - множество всех путей в H_U с началом A_1 и концом A_{n+1}.

Лемма 2. *Для введенных выше обозначений исполнено* $L = f_d(l_\Gamma(P_\Gamma))$.

Доказательство. Пусть $\omega \in L$. Тогда существует вывод в Γ:

$$A_1 \to \alpha_1 A_{i_1}\beta_1 \to \alpha_1\alpha_2 A_{i_2}\beta_2\beta_1 \to \cdots \to \alpha_1\alpha_2\cdots\alpha_k A_{i_k}\beta_k\beta_{k-1}\cdots\beta_1$$
$$\to \alpha_1\alpha_2\cdots\alpha_k\gamma\beta_k\beta_{k-1}\cdots\beta_1,$$

где $A_{i_j} \in N$, $\alpha_j, \beta_j, \gamma \in \Sigma^*$. Но тогда существует путь в H_Γ $\pi = \rho_1\rho_2\cdots\rho_k\tau$, где ρ_1 - ребро из A_1 в A_{i_1}, ρ_j ребра из $A_{i_{j-1}}$ в A_{i_j}, τ - ребро из A_{i_k} в A_{n+1}; $l_\Gamma(\rho_j) = (\alpha_j, \beta_j)$, $l_\Gamma(\tau) = (\gamma, \varepsilon)$. Но тогда $l_\Gamma(\pi) = l_\Gamma(\rho_1) \circ l_\Gamma(\rho_2) \circ \cdots \circ l_\Gamma(\rho_k) \circ l_\Gamma(\tau) = (\alpha_1, \beta_1) \circ (\alpha_2, \beta_2) \circ \cdots \circ (\alpha_k, \beta_k) \circ (\gamma, \varepsilon) = (\alpha_1\alpha_2\cdots\alpha_k\gamma, \beta_k\beta_{k-1}\cdots\beta_1)$. Отсюда следует, что $f_d(l_\Gamma(\pi)) = \omega$. Следовательно $L \subseteq f_d(l_\Gamma(P_\Gamma))$.

Наоборот, если $\omega \in f_d(l_\Gamma(P_\Gamma))$, то ω можно представить в виде $\omega = \alpha\beta$, где (α, β) - метка некоторого пути π из P_Γ и пусть $\pi = \rho_1\rho_2\cdots\rho_k$, где ρ_1

- ребро из A_1 в A_{i_1}, ρ_j, $j = 2, 3, ..., k-1$ ребра из $A_{i_{j-1}}$ в A_{i_j}, ρ_k - ребро из A_{i_k} в A_{n+1} и пусть $l_\Gamma(\rho_j) = (\alpha_j, \beta_j)$ $l_\Gamma(\rho_k) = (\gamma, \varepsilon)$ для некоторых $\alpha_j, \beta_j, \gamma \in \Sigma^*$, таких что $A_1 \to \alpha_1 A_{i_1}\beta_1$, $A_{i_j} \to \alpha_{j+1}A_{i_{j+1}}\beta_{j+1}$, $A_{k-1} \to \gamma$ суть правила в Γ и $\alpha_1\alpha_2\cdots\alpha_{k-1}\gamma = \alpha$, $\beta_{k-1}\beta_{k-2}\cdots\beta_1 = \beta$. Но тогда существует вывод в Γ:

$$A_1 \to \alpha_1 A_{i_1}\beta_1 \to \cdots \to \alpha_1\alpha_2\cdots\alpha_{k-1}A_{i_{k-1}}\beta_{k-1}\beta_{k-2}\cdots\beta_1$$
$$\to \alpha_1\alpha_2\cdots\alpha_{k-1}\gamma\beta_{k-1}\beta_{k-2}\cdots\beta_1 = \alpha\beta = \omega.$$

Следовательно $f_d(l_\Gamma(P_\Gamma)) \subseteq L$. Лемма доказана. □

Следствие 3. *Для введенных выше обозначений $L \subseteq \mathcal{M}$ тогда и только тогда, когда $f_d(l_U(P_U)) = \{e\}$*

Пусть $P_1 \subseteq P_U$ - множество всех путей с началом A_1, концом A_{n+1} и не содержащих циклов и пусть

$\Omega_7 = f_d(l_U(P_1))$

Пусть C - множество элементарных циклов в H_U. Пусть

P' - множество всех путей из H_U, начинающихся в A_1

P'' - множество всех путей из H_U не содержащих циклов и кончающихся в A_{n+1}.

Очевидно $P_U \subseteq P'$, $P_1 \subseteq P''$ и в общем случае $P_U \neq P'$ и $P_1 \neq P''$. Рассмотрим множество путей $P_2 = \{\pi = \pi_1\pi_2\pi_3 | \pi_1 \in P', \pi_2 \in C, \pi_3 \in P''$. Для всех $\pi = \pi_1\pi_2\pi_3 \in P_2$ рассмотрим множество

$$\Omega_8 = \{\langle f_l(l_u(\pi_2)), f_d(l_U(\pi_3)), f_r(l_U(\pi_2))\rangle | \text{ существует путь } \pi = \pi_1\pi_2\pi_3 \in P_2\}.$$

Если проанализировать способ образования множества $\Omega_1, \Omega_2\Omega_7$ и Ω_8, где Ω_1 и Ω_2 суть множества, введенные А. В. Анисимовым (теорема 1), элементы которых рассматриваем как элементы группы G, то нетрудно заметить, что $\Omega_7 \subseteq \Omega_1$, $\Omega_8 \subseteq \Omega_2$ и в общем случае $\Omega_7 \neq \Omega_1$ и $\Omega_8 \neq \Omega_2$.

Как и в параграфе 2, образуем множества путей C^k_{ij} (длиной меньше или равной $k+1$) из P_U $(1 \leq i, j, k \leq n+1)$.

Пусть $g^k_{ij} = l_U(C^k_{ij}) \in F_U$. Здесь k индекс и не означает степень. Рассмотрим элементы замкнутого полукольца F_G:

$$\Omega_9 = f_d(g^n_{1\ n+1})$$
$$\Omega_{10} = \{\langle f_l(g^n_{ii}), f_d(g^n_{i\ n+1}), f_r(g^n_{ii})\rangle$$

Аналогично доказательства леммы 1 можно доказать, что в C^k_{ij} возможно существование путей, содержащих циклы и, имея ввиду способ образования Ω_7, Ω_8, Ω_9 и Ω_{10}, получаем следующее утверждение:

Лемма 3. *Для введенных выше обозначений исполнено $\Omega_7 \subseteq \Omega_9$ и $\Omega_8 \subseteq \Omega_{10}$, при этом в общем случае $\Omega_7 \neq \Omega_9$ и $\Omega_8 \neq \Omega_{10}$.*

Теорема 4. *Для введенных выше обозначений следующие условия эквивалентны:*

(i) $L \subseteq \mathcal{M}$;
(ii) $W_1 = \Omega_1 \cup \Omega_2 = \{e\}$;
(iii) $W_4 = \Omega_7 \cup \Omega_8 = \{e\}$;
(iv) $W_5 = \Omega_9 \cup \Omega_{10} = \{e\}$.

Доказательство. Эквивалентность условий (i) и (ii) доказана А. В. Анисимовым в [3] (см. Теорему 1). Как заметили выше $W_4 \subseteq W_1$ и следовательно из $W_1 = \{e\}$ следует $W_4 = \{e\}$. Из Леммы 3 следует, что если выполнено $W_5 = \{e\}$, то выполнено $W_4 = \{e\}$. Чтобы доказать теорему осталось доказать, что (i) влечет (iv) и (iii) влечет (i).

(i)→(iv). Пусть $L \subseteq \mathcal{M}$. Тогда (Следствие 3) $f_d(l_U(P_U)) = \{e\}$. Но очевидно $C^n_{1\ n+1} \subseteq P_U$ и следовательно $\Omega_9 = \{e\}$.

Пусть $z \in \Omega_{10}$. Тогда $z = uvwv^{-1}$, где $u \in f_l(g^n_{ii})$, $v = f_d(g^n_{i\ n+1})$, $w = f_r(g^n_{ii}$ для некоторого i такое, что существует путь π_1 в H_U из A_1 в A_i и пусть $l_U(\pi_1) = (x, y)$. Тогда очевидно (u, w) метка некоторого цикла π_2, проходящего через A_i, а v можно представить в виде $v = v_1v_2$, где (v_1, v_2) - метка некоторого пути π_3 из A_i в A_{n+1}. Рассмотрим пути $\pi' = \pi_1\pi_2\pi_3$ и $\pi'' = \pi_1\pi_3$. Очевидно они начинаются в A_1 и заканчиваются в A_{n+1}. Имеем:

$$l_U(\pi_1\pi_2\pi_3) = (x, y) \circ (u, w) \circ (v_1, v_2) = (xuv_1, v_2wy)$$
$$l_U(\pi_1\pi_3) = (x, y) \circ (v_1, v_2) = (xv_1, v_2y)$$

Согласно Следствию 3, $xuvwy = xvy = e$, откуда следует что $uvwv^{-1} = e$, т.е. $z = e$. Так, как z - произвольное из Ω_{10}, то $\Omega_{10} = \{e\}$.

(iii)→(i). Пусть $W_4 = \Omega_7 \cup \Omega_8 = \{e\}$ и пусть $\omega \in L$. Согласно леммы 2 $\omega \in f_d(l_\Gamma(P_\Gamma))$, т.е. ω можно представить в виде $\omega = \omega_1\omega_2$, где (ω_1, ω_2) - метка некоторого пути в H_Γ с началом A_1 и концом A_{n+1} и пусть π - соответствующий ему путь в H_U. Если $\pi \in P_1$ (т.е. если π не содержит цикла), то $f_d(l_U(\pi)) \in f_d(l_U(P_1)) = \Omega_7 = \{e\}$ и следовательно $\omega \in \mathcal{M}$.

Пусть π содержит цикл. Тогда π можно представить в виде $\pi = \pi_1\pi_2\pi_3$, где $\pi_1 \in P'$, $\pi_2 \in C$, $\pi_3 \in P''$ и пусть $l_U(\pi_1) = (a_1, b_1)$, $l_U(\pi_2) = (a_2, b_2)$, $l_U(\pi_3) = (a_3, b_3)$. Тогда

$$f_d(l_U(\pi)) = f_d((a_1, b_1) \circ (a_2, b_2) \circ (a_3, b_3)) = f_d(a_1a_2a_3, b_3b_2b_1) = a_1a_2a_3b_3b_2b_1.$$

Но $a_2a_3b_3b_2(a_3b_3)^{-1} \in \Omega_8$, т.е. $a_2a_3b_3b_2(a_3b_3)^{-1} = e$, или $a_1a_2a_3b_3b_2b_1 = a_1a_3b_3b_1$. Нетрудно заметить, что (a_1a_3, b_3b_1) - это метка пути $\pi_1\pi_3$, которая получается из π, опуская цикл π_2. Продолжая таким образом опускать циклы в π, то так как слово ω - конечное, через конечное число шагов получим, что $f_d(l_u(\pi)) = f_d(l_U(\pi'))$, где π' путь из A_1 в A_{n+1} не имеющий

циклов. Но $f_d(l_U(\pi')) \in \Omega_7 = \{e\}$. Следовательно $f_d(l_U(P_2)) = \{e\}$ и согласно следствию 3 получаем, что $L \subseteq \mathcal{M}$. Теорема доказана. □

На базе Теоремы 4 ((i)↔(iv) получаем следующий алгоритм, проверяющий включения $L \subseteq \mathcal{M}$.

Алгоритм 2. *Проверяет включения $L \subseteq \mathcal{M}$, для линейного языка L и группового языка $\mathcal{M}$ группы G с разрешимой проблемой равенства слов.*

Вход: $g_{ij}^0 = l_U(C_{ij}^0), \quad i,j = 1,2,...,n+1$

Выход: Логическая переменная T , получающая стоимость **Истина**, если $L \subseteq \mathcal{M}$ и стоимость **Ложь**, в противном случае.

Начало

1. $T :=$ **Истина** ;

2. **Для** $1 \le k \le n$ **Делать**

3. **Для** $1 \le i,j \le n+1$ **Делать**

4. $g_{ij}^k := g_{ij}^{k-1} \cup g_{ik}^{k-1} \circ g_{kj}^{k-1}$

5. **Конец Делать**

6. **Конец Делать;**

7. **Если** $g_{1\ n+1}^n \neq \phi$ **и** $f_d(g_{1\ n+1}^n) \neq \{e\}$ **То**

8. **Начало** $T :=$ **Ложь; Останов Конец;**

9. **Для** $1 \le i \le n+1$ **Делать**

10. **Если** $g_{1i}^n \neq \phi$ **и** $g_{ii}^n \neq \phi$ **и** $g_{i\ n+1}^n \neq \phi$ **То**

11. **Если** $\langle f_l(g_{ii}^n), f_d(g_{i\ n+1}^n), f_r(g_{ii}^n)\rangle \neq \{e\}$ **То**

12. **Начало** $T :=$ **Ложь ; Останов Конец**

13. **Конец Делать**

Конец.

Теорема 5. *Алгоритм 2 выполняет не более $O(n^3)$ операции сложения и произведения в замкнутом полукольце F_U, не более $O(n^2)$ операции $\langle x,y,z\rangle$ в замкнутом полукольце F_G и проверяет включение $L \subseteq \mathcal{M}$, где L - линейный язык, порождаемый линейной грамматикой с n нетерминалов, $\mathcal{M}$ - групповой язык группы G с разрешимой проблемой равенства слов.*

Доказательство теоремы повторяет доказательство Теоремы 3.

Следствие 4. *Если существуют алгоритмы, выполняющие операции умножения и сложения в F_U и $\langle x,y,z\rangle$ в F_G за полиномиальное время, то алгоритм 2 является полиномиальным.*

Литература

[1] Анисимов А. В, *О групповых языках*, Кибернетика **4** (1971), 18–24.

[2] Анисимов А. В, *О некоторых алгоритмических вопросах для групп и контекстно-свободных языков*, Кибернетика **2** (1972), 4–11.

[3] Анисимов А. В, *Полугрупповые конечно-автоматные отображения*, Кибернетика **5** (1981), 1–7.

[4] Анисимов А. В, Лисовик Л. П, *Проблемы эквивалентности конечно-автоматных отображений в свободную и коммутативную полугруппу*, Кибернетика **3** (1978), 1–8.

[5] Гинсбург С, *Математическая теория контекстно-свободных языков*, М., Мир, 1970.

[6] Ахо А., Хопкрофт Дж., Ульман Дж, *Построение и анализ вычислителных алгоритмов*, М., Мир, 1978.

[7] Ахо А., Ульман Дж, *Теория синтактического анализа,перевода и компиляции*, М., Мир, 1978.

[8] Йорджев К. Я, *О включении контекстно-свободных языков в групповые языки*, Модели и системы обработки информации, вып. **10** (1991), 21–27.

[9] Кук Д., Бейс Г, *Компьютерная математика*, М., Наука, 1990.

[10] Kuich W, *Unambiguous automata* bull. EATCS (1989), 62–67.

[11] Kuich W, Salomaa A, *Semigroups, Automata, Languages* Springer, 1986.

[12] Stearns R, Hunt H, *On the equivalens and containment problēms for unambiguous regular expressions, regular grammars and finite automata* 22nd FOCS (1981), 74–81.

[13] Weber A, Seidl H, *On the degree ambiguity of finite automata*, Lecture Notes in Computer Science, **233** (1986), 620–629.

Пед. Институт, Ямбол, Болгария