Теорема 1. Решая расширенную систему уравнений Хомского — Щутценберже (2) методом последовательных приближений и считывая мономы нужной степени относительно терминальных символов, можно за конечное число шагов провести беступиковый синтаксический анализ (с учётом порядка применения продукций) любого монома КС-языка, заданного грамматикой (1).

ЛИТЕРАТУРА

1. *Глушков В. М., Цейтлин Г. Е., Ющенко Е. Л.* Алгебра. Языки. Программирование. Киев: Наукова думка, 1973.
2. *Salomaa A. and Soitolla M.* Automata-Theoretic Aspects of Formal Power Series. N.Y.: Springer Verlag, 1978.
3. *Egorushkin O. I., Kolbasina I. V., and Safonov K. V.* On solvability of systems of symbolic polynomial equations // Журн. СФУ. Сер. Матем. и физ. 2016. Т. 9. Вып. 2. С. 166–172.
4. *Егорушкин О. И., Колбасина И. В., Сафонов К. В.* Аналог теоремы о неявном отображении для формальных грамматик // Прикладная дискретная математика. Приложение. 2017. № 10. С. 149–151.

УДК 519.682 DOI 10.17223/2226308X/12/55

УСЛОВИЕ РАЗРЕШИМОСТИ ПРОИЗВОЛЬНЫХ ФОРМАЛЬНЫХ ГРАММАТИК

И. В. Колбасина, К. В. Сафонов

Продолжено исследование систем некоммутативных полиномиальных уравнений, которые интерпретируются как грамматики формальных языков. Такие системы решаются в виде формальных степенных рядов (ФСР), выражающих нетерминальные символы через терминальные символы алфавита и рассматриваемых как формальные языки. Всякому ФСР поставлен в соответствие его коммутативный образ, который получается в предположении, что все символы обозначают коммутативные переменные, принимающие значения из поля комплексных чисел. В продолжение исследований совместности систем некоммутативных полиномиальных уравнений, которая напрямую не связана с совместностью её коммутативного образа, получено достаточное условие совместности в виде обобщения теоремы о неявном отображении на формальные грамматики, содержащие произвольное число уравнений. Доказано, что если для коммутативного образа системы ранг матрицы Якоби коммутативного образа системы уравнений в начале координат максимален, то исходная система некоммутативных уравнений имеет единственное решение в виде ФСР.

Ключевые слова: *системы полиномиальных уравнений, некоммутативные переменные, формальный степенной ряд, коммутативный образ, матрица Якоби.*

Продолжая исследование, начатое в работах [1, 2], рассмотрим систему полиномиальных уравнений

$$P_j(z, x) = 0, \quad P_j(0, 0) = 0, \quad j = 1, \ldots, k, \tag{1}$$

которая решается относительно символов $z = (z_1, \ldots, z_n)$ в виде ФСР, зависящих от символов $x = (x_1, \ldots, x_m)$.

Такие системы имеют приложения в теории формальных языков, поскольку являются грамматиками, порождающими важные классы формальных языков: контекстно-свободных, языков непосредственно составляющих, языков в нормальной форме Грейбах и др. [3, 4].

В теории формальных языков символы $x_1, \ldots, x_m$ называются терминальными и образуют словарь (алфавит) данного языка, а символы $z_1, \ldots, z_n$ называются нетерминальными и необходимы для задания грамматических правил. Над всеми символами определена некоммутативная операция умножения (конкатенации) и коммутативная операция формальной суммы, а также определена коммутативная операция умножения на комплексные числа, и потому можно рассматривать символьные многочлены и ФСР с числовыми (комплексными) коэффициентами. Наконец, мономы от терминальных символов интерпретируются как предложения языка, а каждый ФСР, который является решением системы (1), рассматривается как порождённый грамматикой формальный язык, т. е. формальная сумма всех «правильных» предложений этого языка [3, 4].

Исследовать решения символьных систем (1) достаточно трудно, поскольку некоммутативность умножения и отсутствие деления не дают возможности исключать неизвестные, и потому в работах [1, 2] наряду с некоммутативной системой (1) рассмотрен её коммутативный образ, который получается в предположении, что все переменные, входящие в систему, принимают значения из поля комплексных чисел.

Так, предположим, следуя [1], что все мономы от $x_1, \ldots, x_m$ занумерованы в лексикографическом порядке по возрастанию степеней в последовательность $u_0, u_1, \ldots$, играющую роль базиса, тогда каждый ряд s можно единственным образом записать в виде разложения по этому базису с числовыми коэффициентами $\langle s, u_i \rangle$ при мономах u_i:

$$s = \sum_{i=0}^{\infty} \langle s, u_i \rangle u_i. \tag{2}$$

Теперь поставим в соответствие ФСР (2) его коммутативный образ $ci(s)$ — степенной ряд, который получается из s в предположении, что символы $x_1, \ldots, x_m$ (равно как и $z_1, \ldots, z_n$) обозначают коммутативные переменные, принимающие значения из поля комплексных чисел [5].

В работе [1] рассмотрен коммутативный образ системы уравнений (1)

$$ci(P_j(z, x)) = 0, \quad j = 1, \ldots, k, \tag{3}$$

и отмечено, что из совместности некоммутативной системы (1) следует совместность коммутативной системы (3), однако обратное утверждение неверно. Как результат, вопрос о достаточном условии совместности системы уравнений (1), важный для приложений, оставался открытым.

В [2] получено достаточное условие совместности и единственности решения исходной некоммутативной системы (1) в терминах якобиана коммутативной системы (3), в котором предполагается, что число уравнений равно числу неизвестных.

Однако формальные полиномиальные грамматики, возникающие в приложениях, могут иметь любое число уравнений. В связи с этим обобщим аналог теоремы о неявном отображении на случай произвольных формальных грамматик, содержащих произвольное число уравнений.

Пусть

$$J(z, x) = ((ci(P_i(z, x)))'_{z_j})$$

— матрица Якоби системы уравнений (3) относительно переменных $z_1, \ldots, z_n$.

Обобщением дискретного (символьного) аналога теоремы о неявном отображении на произвольные формальные грамматики является следующая

Теорема 1. Если для некоммутативной символьной системы уравнений (1) выполнено условие

$$\operatorname{rank}(J(0,0)) = n,$$

то она имеет единственное решение в виде ФСР.

Замечание 1. Из условия теоремы вытекает существование и единственность решения для коммутативного образа системы полиномиальных уравнений; кроме того, оказывается, что из этого условия вытекает также существование и единственность решения исходной некоммутативной символьной системы уравнений (1).

Поскольку ФСР, которые являются компонентами решения системы (1), интерпретируются как формальные языки, порождённые грамматикой (1), то теорема 1 позволяет установить случаи, когда грамматика действительно определяет формальный язык.

ЛИТЕРАТУРА

1. *Egorushkin O. I., Kolbasina I. V., and Safonov K. V.* On solvability of systems of symbolic polynomial equations // Журн. СФУ. Сер. Матем. и физ. 2016. Т. 9. Вып. 2. С. 166–172.
2. *Егорушкин О. И., Колбасина И. В., Сафонов К. В.* Аналог теоремы о неявном отображении для формальных грамматик // Прикладная дискретная математика. Приложение. 2017. № 10. С. 149–151.
3. *Глушков В. М., Цейтлин Г. Е., Ющенко Е. Л.* Алгебра. Языки. Программирование. Киев: Наукова думка, 1973.
4. *Salomaa A. and Soitolla M.* Automata-Theoretic Aspects of Formal Power Series. N.Y.: Springer Verlag, 1978.
5. *Семёнов А. Л.* Алгоритмические проблемы для степенных рядов и контекстно-свободных грамматик // Докл. АН СССР. 1973. № 212. С. 50–52.

УДК 510.52 DOI 10.17223/2226308X/12/56

О ГЕНЕРИЧЕСКОЙ СЛОЖНОСТИ ПРОБЛЕМЫ ДЕКОДИРОВАНИЯ ЛИНЕЙНЫХ КОДОВ[1]

А. Н. Рыбалов

Изучается генерическая сложность проблемы декодирования линейных кодов. Эта проблема лежит в основе известной криптосистемы Мак-Эллиса. Доказывается, что её естественная подпроблема генерически трудноразрешима (то есть трудна для почти всех входов) при условии, что проблема декодирования линейных кодов трудноразрешима в классическом смысле.

Ключевые слова: *генерическая сложность, линейные коды, криптосистема Мак-Эллиса.*

Введение

Криптосистема Мак-Эллиса [1] является одной из первых криптосистем с открытым ключом. В отличие от популярных криптосистем с открытым ключом, использующих теоретико-числовые и алгебраические конструкции [2], система Мак-Эллиса основана на теории кодов, исправляющих ошибки. В этой области были найдены эффективные семейства методов преобразования и восстановления информационных блоков —

[1]Работа поддержана грантом РФФИ, проект № 18-41-550001.