Секция 7

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

УДК 519.682 DOI 10.17223/2226308X/9/47

О СОВМЕСТНОСТИ СИСТЕМ СИМВОЛЬНЫХ ПОЛИНОМИАЛЬНЫХ УРАВНЕНИЙ И ИХ ПРИЛОЖЕНИИ

О. И. Егорушкин, И. В. Колбасина, К. В. Сафонов

Разрабатываются подходы к решению систем некоммутативных полиномиальных уравнений, возникающих в математической теории языков и грамматик; системы решаются в виде формальных степенных рядов (ФСР), которые выражают символьные неизвестные через символьные параметры. Всякому ФСР поставлен в соответствие его коммутативный образ — степенной ряд, который получается в предположении, что все символы обозначают коммутативные переменные, принимающие значения из поля комплексных чисел. Изучаются вопросы совместности системы некоммутативных символьных уравнений на основе исследования коммутативного образа этой системы.

Ключевые слова: *некоммутативные переменные, полиномиальные уравнения, формальный степенной ряд, коммутативный образ.*

Рассмотрим систему полиномиальных уравнений

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

$P_j(0,0)=0$, $j=1,\ldots,n$, которая решается относительно символов $z=(z_1,\ldots,z_n)$ в виде формальных степенных рядов, зависящих от символов $x=(x_1,\ldots,x_m)$.

В математической теории языков и грамматик символы $z_1,\ldots,z_n,x_1,\ldots,x_m$ интерпретируют как алфавит, над которым определена некоммутативная операция умножения (конкатенации) и коммутативная операция формальной суммы, кроме того, определена коммутативная операция умножения на комплексные числа, и потому можно рассматривать символьные многочлены и ФСР с числовыми (комплексными) коэффициентами. В теории формальных языков приложение систем уравнений (1) состоит в том, что они являются грамматиками, порождающими определённые классы контекстно-свободных языков, языков непосредственно составляющих, языков в нормальной форме Грейбах и др. [1, 2]. При этом 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; мономы являются предложениями (словами) языка, а ФСР, который является решением системы (1), рассматривают как порождённый грамматикой формальный язык, представляющий собой формальную сумму всех «правильных» предложений [1, 2].

Вопросы, связанные с решением символьных систем (1), изучены мало: основные трудности связаны с некоммутативностью умножения и отсутствием деления, препятствующих исключению неизвестных.

Целью данной работы является получение условий разрешимости системы (1) в терминах коммутативного образа этой системы, который получается в предположении, что все переменные, входящие в систему, принимают значения из поля комплексных чисел.

Предположим, что все мономы от $x_1, \ldots, x_m$ занумерованы в лексикографическом порядке по возрастанию степеней в последовательность $\{u_i : i = 0, 1, \ldots\}$, играющую роль универсального базиса. Тогда каждый ряд s можно однозначно записать в виде разложения по этому базису с числовыми коэффициентами $\langle s, u_i \rangle$ при мономах u_i:

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

Поставим в соответствие ФСР (2) его коммутативный образ $\mathrm{ci}(s)$ — степенной ряд, который получается из s в предположении, что символы $x_1, \ldots, x_m$ обозначают коммутативные переменные, принимающие значения из поля комплексных чисел [3].

Обозначим $z = z(x) = (z_1(x), \ldots, z_n(x))$ решение системы (1), представленное ФСР.

Теорема 1. Если $z = z(x)$ — решение некоммутативной системы уравнений (1) в виде символьных ФСР, то коммутативные ФСР $z = \mathrm{ci}(z(x))$ над полем комплексных чисел сходятся в окрестности нуля, определяя ростки голоморфных алгебраических функций, и являются решением коммутативной системы уравнений

$$\mathrm{ci}(P_1(z, x)) = \cdots = \mathrm{ci}(P_n(z, x)) = 0. \tag{3}$$

Обратное утверждение, вообще говоря, неверно. Так, система уравнений $z_1 - z_2 = x_1 x_2$, $z_1 - z_2 = x_2 x_1$ несовместная, тогда как её коммутативный образ имеет бесконечно много решений: $z_1 = t + x_1 x_2$, $z_2 = t$, где t — произвольный ФСР.

Подчеркнём, что совместность, т. е. наличие решения, понимается для некоммутативной системы (1) и коммутативной системы (3) по-разному: в первом случае решением являются символьные ФСР, а во втором — точки в $\mathbb{C}^n$, параметризованные голоморфным в нуле алгебраическим отображением.

Теорему 1 можно сформулировать в эквивалентном виде.

Теорема 2. Если коммутативная система уравнений (3) несовместна, то и некоммутативная система (1) несовместна.

Таким образом, условия несовместности коммутативной системы уравнений также представляют интерес.

Известна теорема: если для якобиана системы голоморфных функций $\mathrm{ci}(P_1(z, x)), \ldots, \mathrm{ci}(P_n(z, x))$ имеет место тождество

$$\det \left(\frac{\partial (\mathrm{ci}(P_i(z, x)))}{\partial z_j} \right) \equiv 0,$$

то система уравнений (3) при каждом x либо не имеет решения в пространстве $\mathbb{C}^n_z$, либо все её решения в этом пространстве неизолированные [4, с. 39].

Покажем, что для некоммутативных систем уравнений (1) подобная альтернатива (решений нет либо решений бесконечно много) не имеет места.

Пример. Рассмотрим систему, состоящую из двух одинаковых уравнений:

$$x_1 z_1 + x_2 z_2 - x_1 x_2 - x_2 x_1 = 0.$$

Коммутативный образ этой системы имеет якобиан, тождественно равный нулю, и неизолированные решения.

Тем не менее исходная система некоммутативных уравнений имеет единственное решение. В самом деле, записав уравнение в виде $x_1(z_1 - x_2) - x_2(z_2 - x_1) = 0$, получим, что первое слагаемое принадлежит левостороннему идеалу, порождённому x_1, а второе — левостороннему идеалу, порождённому x_2. Очевидно, что сумма этих слагаемых может быть равна нулю только в случае, когда равны нулю оба слагаемых: $z_1 - x_2 = 0$, $z_2 - x_1 = 0$, следовательно, исходная система уравнений имеет единственное решение $z_1 = x_2$, $z_2 = x_1$.

Далее, можно показать, что одно символьное полиномиальное уравнение может 1) не иметь решений; 2) иметь конечное число решений; 3) иметь бесконечно много решений, что принципиально отличается от свойств уравнений с комплексными переменными.

Более подробно указанные вопросы изложены в работе [5].

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. *Семенов А. Л.* Алгоритмические проблемы для степенных рядов и контекстно-свободных грамматик // Доклады АН СССР. 1973. №212. С. 50–52.
4. *Айзенберг Л. А., Южаков А. П.* Интегральные представления и вычеты в многомерном комплексном анализе. Новосибирск: Наука, 1979.
5. *Egorushkin O. I., Kolbasina I. V., and Safonov K. V.* On solvability of systems of symbolic polynomial equations // J. Siberian Federal University. Mathematics and Physics. 2016. No. 2(9). P. 166–172.

УДК 004.4'422 DOI 10.17223/2226308X/9/48

ТРАНСЛЯТОР ЯЗЫКА ЛЯПАС-Т НА ЯЗЫК АССЕМБЛЕРА ДЛЯ ОС WINDOWS И LINUX

В. Н. Князев, М. С. Князева

Представлены результаты по созданию транслятора с языка ЛЯПАС-Т на язык ассемблера fasm. Цель разработки — популяризация ЛЯПАСа как претендента на роль национального языка программирования для создания доверенных программ и построения защищённых компьютерных систем. Для написания транслятора использовались генераторы лексических и синтаксических анализаторов flex и Bison в целях приведения грамматики ЛЯПАСа к общепринятому виду и получения эффективного LALR-анализатора.

Ключевые слова: *ЛЯПАС-Т, транслятор, компьютерная безопасность, программирование.*

ЛЯПАС — русский язык программирования, возрождаемый Томским государственным университетом (ТГУ) в целях создания доверенного программного обеспечения и защищённых компьютерных систем [1, 2]. Учитывая масштабы этих целей, считаем важным создание и распространение свободного транслятора с ЛЯПАСа для современных операционных систем (ОС). Это необходимо для обучения программи-