Секция 4

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ, ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

УДК 519.682 DOI 10.17223/2226308X/15/20

О ПОЛИНОМИАЛЬНЫХ ГРАММАТИКАХ, ПОРОЖДАЮЩИХ БЕСКОНЕЧНОЕ МНОЖЕСТВО ЯЗЫКОВ

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

Исследуются формальные грамматики — системы полиномиальных уравнений относительно некоммутативных переменных, которые решаются в виде формальных степенных рядов, выражающих нетерминальные символы алфавита через терминальные; первая компонента решения является формальным языком. Рассмотрено определение грамматики, имеющей бесконечно много решений (порождающей бесконечное множество языков). Такие грамматики могут возникать в ситуации, когда якобиан коммутативного образа грамматики тождественно равен нулю. Показано, что в этом случае описание множества решений грамматики сложнее, чем для аналогичных полиномиальных систем с вещественными или комплексными переменными, поскольку могут реализовываться все возможные ситуации: такая грамматика может иметь бесконечно много решений, любое конечное число решений либо не иметь решений вовсе.

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

Как известно, теория формальных языков имеет фундаментальное значение как для лингвистики, так и программирования. Многочисленные приложения используют взаимосвязи языка (как множества возможных текстов) с грамматикой (сводом формальных правил, определяющих языковые конструкции и их равнозначимость). В этой связи нужны быстрые качественные алгоритмы формальных построений грамматики по языку и языка по грамматике, а также синтаксического анализа конструкций, что невозможно без серьёзного теоретического обоснования.

Рассмотрим систему полиномиальных уравнений

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

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

Системы такого вида обобщают важные классы формальных грамматик [1, 2] и называются полиномиальными грамматиками [3, 4]. Одним из достоинств полиномиальных, в частности контекстно-свободных, грамматик является возможность задания широкого класса языков при сохранении относительной компактности представления [1 – 4].

Символы $x_1, \ldots, x_m$ называются терминальными, они образуют словарь языка, а символы $z_1, \ldots, z_n$ — нетерминальными, они необходимы для задания грамматических

правил. Над всеми символами определена некоммутативная операция конкатенации и коммутативная операция формальной суммы, а также коммутативная операция умножения на числа, что позволяет рассматривать ФСР с числовыми коэффициентами. Мономы от терминальных символов рассматриваются как предложения языка, а каждый ФСР (сумма всех «правильных» мономов) — компонент решения системы (1) понимается как порождённый грамматикой язык [1, 2].

Для полиномиальных грамматик актуальны вопросы существования, единственности и бесконечности решений, причём для понимания последней ситуации необходимо сделать уточнения. Дадим следующее

Определение 1. Будем говорить, что полиномиальная грамматика (1) имеет бесконечно много решений (порождает бесконечное множество языков), если множество решений системы (1) зависит хотя бы от одного произвольного ФСР от символов $x_1, \ldots, x_m$.

Так, система из двух одинаковых уравнений

$$x_1 z_1 - z_2 x_2 = 0$$

имеет тождественно равный нулю якобиан и бесконечно много решений, поскольку решения можно записать в виде

$$z_1 = s x_2, \;\; z_2 = x_1 s,$$

где s — произвольный ФСР от $x_1, \; x_2$.

Поскольку исследовать системы с некоммутативными символами трудно, в работах [3 – 5] предложено использовать коммутативный образ системы (1), который получается, если считать все переменные коммутативными. Обозначая коммутативный образ ФСР s через $\mathrm{ci}(s)$, рассмотрим коммутативный образ

$$\mathrm{ci}(P_j(z, x)) = 0, \quad j = 1, \ldots, n, \tag{2}$$

системы уравнений (1). Отметим, что из совместности некоммутативной системы (1) следует совместность коммутативной системы (2), а обратное утверждение неверно, что подчёркивает актуальность вопросов, связанных с совместностью системы уравнений (1). Используем для их решения такой инструмент, как якобиан.

Пусть

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

— якобиан системы уравнений (2) относительно переменных $z_1, \ldots, z_n$.

Для систем уравнений с вещественными либо комплексными переменными хорошо известна следующая

Теорема 1. Пусть выполнено равенство

$$J(z, x) \equiv 0,$$

тогда система уравнений (2) либо не имеет решения для каждого x в пространстве $\mathbb{C}_z^n$, либо все её решения в этом пространстве неизолированные.

Таким образом, суть теоремы состоит в том, что такие системы не могут иметь изолированных решений.

Для систем с некоммутативными переменными ситуация с описанием множества решений сложнее, а именно получена следующая

Теорема 2. Пусть для якобиана коммутативной системы (2) выполнено равенство

$$J(z, x) \equiv 0,$$

тогда некоммутативная система уравнений (1) либо не имеет решений (в виде ФСР $z = z(x)$), либо имеет любое конечное число решений, либо бесконечно много решений.

Суть теоремы 2 состоит в том, что равенство нулю якобиана не ограничивает свойств некоммутативной системы уравнений.

Учитывая, что система

$$f = 0, \ \ldots, \ f = 0,$$

из n одинаковых уравнений с n некоммутативными неизвестными $z_1, \ldots, z_n$, имеющая тождественно равный нулю якобиан, эквивалентна одному уравнению $f = 0$, сформулируем следствие: одно уравнение с некоммутативными неизвестными $P_1(z, x) = 0$ может не иметь решений, а также иметь конечное и бесконечное число решений.

В этом состоит фундаментальное отличие от одного уравнения над полем комплексных чисел, которое всегда имеет решения в виде аналитических функций.

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. *Егорушкин О. И., Колбасина И. В., Сафонов К. В.* О совместности систем символьных полиномиальных уравнений и их приложении // Прикладная дискретная математика. Приложение. 2016. № 9. С. 119–121.
4. *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.
5. *Семёнов А. Л.* Алгоритмические проблемы для степенных рядов и контекстно-свободных грамматик // Доклады АН СССР. 1973. № 212. С. 50–52.

УДК 004.056.5, 004.94 DOI 10.17223/2226308X/15/21

ПРИЕМЫ ДЕДУКТИВНОЙ ВЕРИФИКАЦИИ ПРОГРАММНОГО КОДА С ИСПОЛЬЗОВАНИЕМ AstraVer Toolset

А. О. Кокорин, С. Д. Тиевский, П. Н. Девянин

Описывается ряд практических приёмов дедуктивной верификации программного кода на языке Си на соответствие спецификациям его функций, заданных на языке ACSL. Для такой верификации используется основанный на платформе Frama-C набор инструментов AstraVer Toolset. Апробация этих приёмов осуществлена при верификации программного кода модуля управления доступом, реализованного в подсистеме безопасности PARSEC отечественной защищённой операционной системы специального назначения Astra Linux Special Edition. Благодаря использованию этих приёмов удалось упростить спецификации функций PARSEC, уменьшить трудоёмкость и ускорить процесс их дедуктивной верификации.

Ключевые слова: *дедуктивная верификация программного кода, ACSL, Frama-C, AstraVer Toolset, Astra Linux.*