

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 Soittola 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-

стов на ЛЯПАСе, пока не разработана ОС, поддерживающая ЛЯПАС изначально. Для достижения этой цели поставлены и решены следующие задачи:

- **Описание грамматики ЛЯПАСа-Т.** Из источников [3–5], а также из личной переписки с сотрудниками ТГУ собраны и обобщены сведения о синтаксисе и семантике ЛЯПАСа-Т.
- **Создание программы для построения синтаксического дерева.** Написаны программы для flex и Bison, связка которых генерирует LALR-парсер, строящий синтаксическое дерево программы на ЛЯПАСе-Т [6].
- **Создание трансляторов для ОС Windows и Linux.** Реализованы соответствующие программы, генерирующие код на языке ассемблера по синтаксическому дереву.

Реализованы некоторые алгоритмы дискретной математики на ЛЯПАСе-Т, демонстрирующие возможности языка:

- Алгоритм быстрого перемножения многочленов и длинных чисел на основе алгоритма Кули — Тьюки быстрого преобразования Фурье. Примеры комбинации его с алгоритмом Винограда для поиска свёртки длины маленьких простых чисел [7].
- Алгоритмы факторизации:  $\rho$ -метод Полларда, метод квадратичного решета [7].
- Алгоритм Миллера — Рабина проверки простоты чисел [7].

#### ЛИТЕРАТУРА

1. Агibalов Г. П. К возрождению русского языка программирования // Прикладная дискретная математика. 2012. № 3. С. 77–84.
2. Торопов Н. Р. Язык программирования ЛЯПАС // Прикладная дискретная математика. 2009. № 2. С. 9–25.
3. Агibalов Г. П., Липский В. Б., Панкратова И. А. О криптографическом расширении и его реализации для русского языка программирования // Прикладная дискретная математика. 2013. № 3. С. 93–104.
4. Broslavskiy O. V. AES in LYaPAS // Прикладная дискретная математика. Приложение. 2013. № 6. С. 102–104.
5. Гречнев С. Ю., Стефанцов Д. А. Модификация ЛЯПАСа для разработки ОС // Прикладная дискретная математика. Приложение. 2015. № 8. С. 129–131.
6. Ахо А. В., Лам М. С., Сети Р., Ульман Д. Д. Компиляторы: принципы, технологии и инструментарий. М.: Вильямс, 2008.
7. Крэндалл Р., Померанс К. Простые числа. Криптографические и вычислительные аспекты. М.: УРСС, 2011.

УДК 004.43+004.4'42+004.451

DOI 10.17223/2226308X/9/49

#### МОДУЛЬНЫЙ ТРАНСЛЯТОР С ЯЗЫКА ЛЯПАС

Д. А. Стефанцов, В. О. Сафонов, В. В. Першин, С. Ю. Гречнев, П. А. Томских

Сообщается о разработке модульного транслятора с языка программирования ЛЯПАС. Цель разработки — упрощение создания транслятора с ЛЯПАСа, написанного на ЛЯПАСе. Процесс трансляции разделяется на этапы, за каждый из которых ответствен один из модулей транслятора. Модули выполнены в виде исполняемых программ и обмениваются данными с помощью файлов. Для представления промежуточных результатов работы модулей используются вспомогательные языки программирования.

**Ключевые слова:** ЛЯПАС, язык программирования, операционная система.