

пользователя. Язык Transalg — это фактически самостоятельный язык с С-подобным синтаксисом. Семантика языка определяет правила построения логических уравнений по соответствующему описанию алгоритма. Ниже приведены основные этапы трансляции алгоритмов в комплексе Transalg.

- 1) Анализ текста программы и построение дерева синтаксического разбора.
- 2) Обход построенного дерева, выполнение семантических действий: «пропозициональная свертка» условных переходов (см. [5]) за счет преобразований Цейтина, построение систем логических уравнений.
- 3) Приведение систем логических уравнений к нормальным формам; преобразование в формат И-НЕ графов.

Пропозициональные кодировки многих алгоритмов, реализованные в трансляторе Transalg, по объему существенно меньше известных аналогов (например, пропозициональная кодировка алгоритма DES компактнее кодировки, представленной в [1], более чем в два раза).

Дополнительной возможностью комплекса Transalg является сведение к SAT (или к системе логических уравнений в любой нормальной форме) задач 0-1-целочисленного линейного программирования (0-1-ЦЛП). Получаемые кодировки по компактности также превосходят известные аналоги [6].

ЛИТЕРАТУРА

1. *Massacci F., Marraro L.* Logical Cryptanalysis as a SAT Problem // J. Automated Reasoning. 2000. V. 24. No. 1–2. P. 165–203.
2. *Буранов Е. В.* Программная трансляция процедур логического криптоанализа симметричных шифров // Вестник Томского госуниверситета. Приложение. 2004. № 9(1). С. 60–65.
3. <http://www.veripool.org/>
4. Berkeley Logic Synthesis and Verification Group, ABC: A System for Sequential Synthesis and Verification. <http://www.eecs.berkeley.edu/~alanmi/abc/>.
5. *Семёнов А. А.* Трансляция алгоритмов вычисления дискретных функций в выражения пропозициональной логики // Прикладные алгоритмы в дискретном анализе. Сер. Дискретный анализ и информатика. Иркутск: Изд-во ИГУ, 2008. Вып. 2. С. 70–98.
6. *Een N., Sorensson N.* Translating Pseudo-Boolean Constraints into SAT // J. Satisfiability, Boolean Model. Computat. 2006. No. 2. P. 1–25.

УДК 519.682

О ПРЕДСТАВЛЕНИИ КОНТЕКСТНО-СВОБОДНЫХ ЯЗЫКОВ ДИАГОНАЛЯМИ ЛИНЕЙНЫХ ЯЗЫКОВ

К. В. Сафонов, Д. А. Калугин-Балашов

В теории контекстно-свободных языков (кс-языков) и грамматик словарь языка $X = \{x_1, \dots, x_n\}$ обычно называют терминальным множеством, тогда как нетерминальным называют конечное множество $Z = \{z_1, \dots, z_m\}$ вспомогательных символов, необходимых для задания грамматических правил (грамматики) данного языка. Для элементов этих множеств определены операции конкатенации и формальной суммы, приводящие к мономам и многочленам.

Если последние построены в соответствии с грамматическими правилами данного кс-языка, то эти мономы и многочлены интерпретируются как его предложения и совокупности предложений. Рассмотрение совокупности всех грамматически правиль-

ных предложений кс-языка приводит к необходимости изучать формальные степенные ряды от терминальных символов.

Кс-грамматике сопоставляется система символьных уравнений

$$z_j = p_j(x, z), j = 1, \dots, m, \quad (1)$$

называемая системой уравнений Хомского — Щютценберже. Ее решением является совокупность $(z_1(x), \dots, z_m(x))$ формальных степенных рядов от терминальных переменных $x = (x_1, \dots, x_n)$, а ряд $z_1(x)$ и является кс-языком, определяемым данной грамматикой [1].

Эффективным инструментом изучения решений систем уравнений Хомского — Щютценберже является коммутативный образ этой системы — новая система уравнений, переменные в которой рассматриваются уже как коммутативные, например, из поля комплексных чисел [2]. Понятно, что и формальные степенные ряды $(z_1(x), \dots, z_m(x))$, являющиеся решениями исходной системы (1), переходят в степенные ряды, представляющие алгебраические функции. Осталось заметить, что коммутативный образ некоторого многочлена или ряда r удобно обозначать как $ci(r)$ (commutative image).

Хорошо изучен подкласс линейных кс-языков, для которых уравнения системы (1) линейны по переменным $z_j, j = 1, \dots, m$. А именно, достаточно изучена структура формальных степенных рядов, представляющих такие языки. Оказалось [2], что существуют так называемые аффинные кс-языки над терминальным множеством X , коммутативные образы которых являются диагоналями коммутативных образов линейных языков над терминальным множеством $\{x_0\} \cup X$, содержащем один дополнительный символ. В диагональ «выбираются» те мономы, у которых степень по x_1 равна степени по x_0 .

Запишем систему уравнений (1) в виде

$$q_j(x, z) = 0, j = 1, \dots, m, \quad (2)$$

возьмем ее подсистему $q_j(x, z) = 0, j = 2, \dots, m$, и рассмотрим систему уравнений

$$q_j^*(x, z) = 0, j = 2, \dots, m, \quad (3)$$

составленную из старших взвешенно-однородных по переменным $z_2, \dots, z_m$ с весом $(w_2, \dots, w_m)$ составляющих многочленов $q_j(x, z)$. Тогда имеет место теорема 1.

Теорема 1. Пусть подсистема уравнений (3) не зависит от x и z_1 и имеет единственный корень $z_2 = \dots = z_m = 0$. Тогда существует линейный язык над терминальным множеством $\{x_0\} \cup X$, такой, что коммутативный образ кс-языка, определяемого системой (2), является диагональю его коммутативного образа.

Ранее подобное утверждение было доказано только для случая однородных частей многочленов $q_j(x, z)$.

ЛИТЕРАТУРА

1. Глушков В. М., Цейтлин Г. Е., Ющенко Е. Л. Алгебра, языки, программирование. Киев: Наукова думка, 1974. 328 с.
2. Сафонов К. В., Егорушкин О. И. О синтаксическом анализе и проблеме В. М. Глушкова распознавания контекстно-свободных языков Хомского // Вестник Томского государственного университета. Приложение. 2006. № 17. С. 63–66.