УДК 004.421.6

Розглянуто задачу побудови прикладів програм, що мають нетривіальні поліноміальні інваріанти. Ці приклади використовуються в математичній системі навчального призначення «Статичний аналіз програм». Запропоновані два методи: метод алгебраїчної залежності й метод L-інваріантів

Ключові слова: статичний аналіз програм, поліноміальні інваріанти програм, автоматична генерація прикладів

Рассматривается задача построения примеров программ, обладающих нетривиальными полиномиальными инвариантами. Эти примеры используются в математической системе учебного назначения «Статический анализ программ». Предложены два метода: метод алгебраической зависимости и метод L-инвариантов

Ключевые слова: статический анализ программ, полиномиальные инварианты программ, автоматическая генерация примеров

The problem of generation of program examples with nontrivial polynomial invariants is considered. These examples are used in mathematical system of educational purpose "Static Analysis Systems". The two methods are proposed: the method of algebraic dependencies and the method of L-invariants

Key words: static analysis of programs, polynomial invariants of programs, automatic generation of examples

МЕТОДЫ ГЕНЕРАЦИИ УЧЕБНЫХ ПРИМЕРОВ ПРОГРАММ С НЕТРИВИАЛЬНЫМИ ПОЛИНОМИАЛЬНЫМИ ИНВАРИАНТАМИ

М.С. Львов
Кандидат физико-математических наук, доцент
Директор НИИ информационных технологий
Херсонский государственный университет
ул. 40-летия Октября, 27. 73000 Херсон, Украина
Контектный тел: (0552) 32-67-81
E-mail: lvov@ksu.ks.ua

1. Введение

Проблема поиска инвариантов программ была поставлена в работах Р. Флойда [1] и С. Хоара [2] как ключевая проблема одной из основных задач статического анализа программ – задачи анализа свойств программ.

Исследования задачи автоматической генерации программных инвариантов для различных алгебр данных выполнялись, начиная в 70-х годов, в ИК НАН Украины. Их основные результаты изложены в [3-5]. Интерес к проблеме автоматической генерации инвариантов значительно возрос в начале 2000-х годов (6-12]).

В [5] изложены два метода построения программных инвариантов типа полиномов. Один из них заключается в построении алгебраических зависимостей между функциями-правыми частями оператора присваивания в теле цикла. Второй – метод неопределенных коэффициентов – строит все полиномиальные инварианты данного вида в произвольной контрольной точке программы. Вид инварианта задается полиномиальной формой с неопределенными коэффициентами. Третий метод, впервые излагаемый в этой работе, генерирует полиномиальные инварианты специального вида – L-инварианты. Данные методы мы планируем использовать в алгоритмах генерации учебных примеров программ, используемых в разрабатываемой математической системе учебного назначения (МСУН) SAS (Static Analysis System). МСУН «Статический анализ программ», в отличие от аналогичных систем производственного назначения, должна содержать достаточный для учебных целей список программ с нетривиальными инвариантами. Таким образом, возникает задача генерации учебных примеров программ – программ простой структуры, с небольшим количеством переменных, но заведомо обладающих нетривиальными инвариантами.

Определение 1. Пусть P - программа и $X=\{x_1,...,x_n\}$ - список ее переменных со значениями в поле K.

Многочлен $A(X) \in K[X]$ называется полиномиальным инвариантом P, если в заключительной контрольной точке P, вне зависимости от начальных значений переменных $S = (s_1^{(0)},...,s_n^{(0)})$, для заключительных значений этих переменных $S^* = (s_1^*,...,s_n^*)$ выполняется равенство $A(S^*) = 0$.

2. Метод алгебраических зависимостей

Определение 2. Набор полиномов $f_1(X),...,f_m(X)$ называется алгебраически зависимым, если существует полином $A \in K[u_1,...,u_m]$ такой, що $A(f_1(X),...,f_m(X)) \equiv 0$.

Теорема 1. Пусть $X = (x_1,...,x_n)$, $f_1(X),...,f_m(X) \in F[X]$ і $m > n$. Тога набор $f_1(X),...,f_m(X)$ алгебраически зависим.

Следствие. Пусть для некоторого набора переменных $X' \subset X$ цикл программы имеет вид

```
While U do X := (f1(X′), …,fn(X′)).      (1)
```

Тогда цикл имеет нетривиальный полиномиальный инвариант.

Теорема 2. Пусть набор полиномов $f_1(X),...,f_m(X) \in F[X]$ алгебраически зависим. Тодгда идеал $I = \{A \in F[U] \mid A(f_1(X),...,f_m(X)) \equiv 0\}$ обладает базисом Гребнера вида

$$(u_1 - f_1(X),...,u_m - f_m(X))_{Gr} \cap F[U]. \tag{2}$$

Следствие Алгоритм вычисления инвариантов цикла (1) заключается в вычислении базиса Гребнера.

Пример 1. Цикл с нетривиальным инвариантом.

$$\text{While}\, U\, \text{do}\, (x,y,z) := (x - y, xy, x + y)$$

Решение. Составим набор полиномов $(u_1 - x + y,\ u_2 - xy,\ u_3 - x - y)$. Исключим переменные x, y. Получим многочлен $4u_2 + (u_1 + u_3)(u_1 - u_3)$. Осуществим замену переменных $u_1 = x,\ u_2 = y,\ u_3 = z$. Получим иваривант цикла $A(x,y,z) = 4y + (x + z)(x - z)$.

3. Метод L-инвариантов линейных циклов

Определение 3. Пусть W - n-мерное векторное пространство над полем рациональных чисел Q и $\bar{Q}$ - алгебраическое замыкание поля Q. Рациональная функция $p(X) \in \bar{Q}(X)$ называется **L**-инвариантом линейного оператора $A : W \to W$, если для любого вектора $b \in W$ имеет место соотношение

$$p(A \cdot b) = p(b) \tag{3}$$

Пример 1. (линейный оператор с характеристическим многочленом $x^3 - 2$)

Рассмотрим линейный оператор с матрицей

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 0 \end{pmatrix}, X = (x,y,z).$$

Легко проверить, что рациональное выражение

$$p(x,y,z) = \frac{(\lambda_1^2 x + \lambda_1 y + z)(\lambda_3^2 x + \lambda_3 y + z)}{(\lambda_2^2 x + \lambda_2 y + z)^2} \tag{4}$$

где $\lambda_1 = \sqrt[3]{2},\ \lambda_2 = \sqrt[3]{2} * \varepsilon,\ \lambda_3 = \sqrt[3]{2} * \varepsilon^2$,

а $\varepsilon = \cos(\frac{2\pi}{3}) + i * \sin(\frac{2\pi}{3})$ - первообразный корень степени 3 из 1 – L–инвариант этого оператора.

Определение 2. Пусть $X = \{x_1,...,x_n\}$, $b = \{b_1,...,b_n\}$ - два набора переменных. Линейным циклом мы называем фрагмент императивной программы вида

```
X := b;
While Q(X, b) do X := A*X
```

Замечание. Операторы X:=b, X:=A*X интерпретируются как одновременные присвоения переменным левых частей значений правых частей. В дальнейшем условие $Q(X,b)$ мы будем игнорировать, считая линейный цикл бесконечным, а его выполнение недетерминированным.

Теорема 3. Если $p(X) = r(X)/q(X)$ -L-инвариант линейного оператора A, многочлен $r(X) * q(b) - q(X) * r(b)$ - инвариант линейного цикла над полем $\bar{Q}$.

Пример 2. (линейный цикл с оператором примера 1)

Линейный цикл, соответствующий оператору A, имеет вид

```
(x,y,z) := (a,b,c);
While True|False do (x,y,z):=(y,z,2*x)
```

Инвариант этого цикла определен формулой (4):

$$\begin{aligned} &P(x,y,z,a,b,c) = \\ &= (\lambda_1^2 x + \lambda_1 y + z)(\lambda_3^2 x + \lambda_3 y + z)(\lambda_2^2 a + \lambda_2 b + c)^2 - \\ &-(\lambda_2^2 x + \lambda_2 y + z)^2(\lambda_1^2 a + \lambda_1 b + c)(\lambda_3^2 a + \lambda_3 b + c) \end{aligned} \tag{5}$$

Отметим, что L-инвариант цикла $P(x,y,z,a,b,c)$ определен над полем $\bar{Q}(\lambda_1, \lambda_2, \lambda_3)$. Однако, в учебных примерах можно подбирать линейные операторы с рациональными собственными значениями. Отметим также, что если переменным a,b,c придать числовые значения, L-инвариант преобразуется в инвариант цикла.

Метод L-инвариантов заключается в вычислении и анализе собственных значений и собственных векторов линейных операторов.

Теорема 4. Пусть $\lambda_1,...,\lambda_m$ - собственные значения линейного оператора A и $s_1,...,s_m$ соответствующие им собственные векторы сопряженного оператора A^*. Предположим, что существуют такие целые числа $k_1,...,k_m$, что

$$\lambda_1^{k_1} \cdot ... \cdot \lambda_m^{k_m} = 1 \tag{6}$$

Тогда

$$p(X) = (s_1, X)^{k_1} \cdot ... \cdot (s_m, X)^{k_m} \tag{7}$$

- **L**-инвариант линейного оператора A.

Соотношение (6) мы будем называть мультипликативным соотношением, определяющим **L**-инвариант (7).

Пример 3. (продолжение примера 2).

Рассмотрим метод теоремы 4 применительно к примеру 2. Вычислим собственные числа оператора A.

$$A=\begin{pmatrix}0&1&0\\0&0&1\\2&0&0\end{pmatrix},$$

$$h(\lambda)=|A-\lambda*E|=\begin{vmatrix}-\lambda&1&0\\0&-\lambda&1\\2&0&-\lambda\end{vmatrix}=-\lambda^3+2\,.$$

Таким образом, характеристический многочлен имеет вид $h(x)=x^3-2$. Его корни - $\lambda_1=\sqrt[3]{2},\ \lambda_2=\sqrt[3]{2}*\varepsilon,\ \lambda_3=\sqrt[3]{2}*\varepsilon^2,\ \ \varepsilon=\cos(\frac{2\pi}{3})+i*\sin(\frac{2\pi}{3})$.

Вычислим далее собственные векторы матрицы $A^*=\begin{pmatrix}0&0&2\\1&0&0\\0&1&0\end{pmatrix}$, причем вычисления будем осуществлять в поле $Q(\lambda)$ по модулю λ^3-2. Получим систему линейных уравнений $\begin{cases}\lambda x-2z=0\\x-\lambda y=0\\y-\lambda z=0\end{cases}$, ранг которой равен 2. Фундаментальное решение этой системы – вектор $s=(\lambda^2,\lambda,1)$. Поэтому собственными векторами оператора A^* являются векторы

$$s_1=(\lambda_1^2,\lambda_1,1),\ s_2=(\lambda_2^2,\lambda_2,1),\ s_3=(\lambda_3^2,\lambda_3,1)\,.$$

Легко установить, что $\frac{\lambda_1*\lambda_3}{\lambda_2^2}=1$.

Поэтому оператор A имеет L-инвариант (4).

Следствие 1. Если характеристический (минимальный) многочлен $h(x)$ линейного оператора A имеет свободный член, равный ±1, линейный оператор обладает **L**-инвариантом.

Пример 4. Цикл поворота точки плоскости (a,b) на угол $\arctan(4/3)$.

```
(x,y) := (a,b);
While True|False do (x, y):= (4/5*x-3/5*y, 3/5*x+4/5*y)
```

Вычислим собственные значения и собственные векторы оператора A:

$$A=\begin{pmatrix}4/5&-3/5\\3/5&4/5\end{pmatrix}.$$

$$h(\lambda)=|A-\lambda*E|=\begin{vmatrix}4/5-\lambda&-3/5\\3/5&4/5-\lambda\end{vmatrix}=\lambda^2-\frac{8}{5}\lambda+1\,.$$

$$\lambda_1=\frac{4}{5}-i*\frac{3}{5},\lambda_2=\frac{4}{5}+i*\frac{3}{5}.\ \ s_1=(i,1),\ s_2=(-i,1)\,.$$

Поскольку $\lambda_1\lambda_2=1$, L-инвариант A имеет вид $p(x,y)=(ix+y)(-ix+y)=x^2+y^2$

Инвариант цикла имеет вид $x^2+y^2-a^2-b^2$.

Пример 5. Цикл вычисления чисел Фибоначчи, начиная с пары (a, b).

```
(x,y) := (a,b);
While True|False do (x, y):= (x + y, x)
```

Вычислим собственные значения и собственные векторы оператора A:

$$A=\begin{pmatrix}1&1\\1&0\end{pmatrix}.\ \ h(\lambda)=|A-\lambda E|=\begin{vmatrix}1-\lambda&1\\1&-\lambda\end{vmatrix}=\lambda^2-\lambda-1\,.$$

$$\lambda_1=\frac{1}{2}-\frac{1}{2}\sqrt{5},\ \lambda_2=\frac{1}{2}+\frac{1}{2}\sqrt{5}\,.$$

$$s_1=(\frac{1}{2}-\frac{1}{2}\sqrt{5},1),\ s_2=(\frac{1}{2}+\frac{1}{2}\sqrt{5},1)\,.$$

Поскольку $\lambda_1\lambda_2=-1$, L-инвариант оператора A имеет вид

$$p(x,y)=((\lambda_1x+y)(\lambda_2x+y))^2=(x^2-xy-y^2)^2.$$

Инвариантное соотношение цикла имеет вид $(x^2-xy-y^2)^2=(a^2-ab-b^2)^2$.

Следствие 2. Если характеристический (минимальный) многочлен $h(X)$ линейного оператора A имеет вид x^m-a, линейный оператор обладает L-инвариантами.

В самом деле, легко убедиться в том, что если $\lambda_{i-1},\lambda_i,\lambda_{i+1}$ - три последовательных корня $h(x)=x^m-a$, имеет место мультипликативное соотношение $\lambda_{i-1}\lambda_{i+1}=\lambda_i^2$.

Определение 3. L-инварианты оператора A, определенные мультипликативным соотношением между корнями характеристического многочлена $\lambda_1\cdot\ldots\cdot\lambda_m=\pm1$, будем называть целыми. L-инварианты оператора A, определенные мультипликативным соотношением $\lambda_1^{k_1}\cdot\ldots\cdot\lambda_m^{k_m}=1,\sum k_i=0$, будем называть рациональными.

Теорема 5. Если характеристический многочлена оператора A имеет вид $h(x^k),k>1$, оператор A обладает рациональными L-инвариантами.

Заключительные замечания

Задача изучения L-инвариантов линейных операторов еще не завершена. Однако метод L-инвариантов позволяет быстро генерировать учебные примеры линейных циклов с нетривиальными инвариантами.

Литература

1. R. W. Floyd. Assigning Meanings to Programs. In Proc/ Symposia in Applied Mathematics 19, pp 19-37, 1967.
2. C. A. R. Hoare. An Axiomatic Basis for Computer Programming. Comm. ACM, 12, 1969.
3. A.A. Letichevskiy. About one approach to program analysis // Cybernetics. - 1979.-№ 6.-c.1-8.
4. A.B. Godlevskiy, Y.V. Kapitonova, S.SL. Krivoy, A.A. Letichevskiy. Iterative methods of program analysis // Cybernetics. – 1989. - №2, P.9-19.
5. A.Letichevsky, M.Lvov. Discovery of invariant Equalities in Programs over Data fields. Applicable Algebra in Engineering, Communication and Computing. – 1993. – №4. – pp. 21-29.
6. Markus M]ller-Olm, Helmut Seidl: Precise interprocedural analysis through linear algebra. POPL 2004: 330-341.
7. Markus M]ller-Olm, Helmut Seidl: Computing polynomial program invariants. Inf. Process. Lett. 91(5): 233-244 (2004).
8. Sriram Sankaranarayanan, Henny Sipma, Zohar Manna: Non-linear loop invariant generation using Grobner bases. POPL 2004: 318-329.

9. Michael Caplain: Finding Invariant Assertions for Proving Programs. In Proceedings of the international Conference on Reliable Software (Los Angeles, California, April 21 - 23, 1975): 165-171.
10. Enric Rodriguez-Carbonell, Deepak Kapur: Automatic generation of polynomial loop invariants: algebraic foundations. ISSAC 2004: 266-273.
11. Enric Rodriguez-Carbonell, Deepak Kapur: Automatic generation of polynomial invariants of bounded degree using abstract interpretation. Sci. Comput. Program. 64(1): 54-75 (2007).
12. Laura Ildiko Kovacs, Tudor Jebelean: An Algorithm for Automated Generation of Invariants for Loops with Conditionals. SYNASC 2005: 245-249.

УДК 656.96

ВЫБОР ОПТИМАЛЬНЫХ СТРАТЕГИЙ ПЕРЕВОЗЧИКА НА РЫНКЕ ТРАНСПОРТНО-ЭКСПЕДИЦИОННЫХ УСЛУГ

Запропонована методика вибору перевізником оптимальних стратегій на ринку транспортно-експедиційних послуг відносно парку рухомого складу

Ключові слова: експедиційне обслуговування, стратегія перевізника

Предложена методика выбора перевозчиком оптимальных стратегий на рынке транспортно-экспедиционных услуг относительно парка подвижного состава

Ключевые слова: экспедиционное обслуживание, стратегия перевозчика

The method of choice of an optimal strategy by the carrier at a freight forwarding market with regard to a fleet structure has been proposed

Key words: freight forwarding, strategy of the carrier

В.С. Наумов
Кандидат технических наук, доцент
Кафедра транспортных технологий*
Контактный тел.: (057) 707-37-20
E-mail: naumov-vs@mail.ru

Ю.В. Пересыпкин
Контактный тел.: 099-278-75-51
*Харьковский национальный автомобильно-дорожный университет
ул. Петровского, 25, г. Харьков, Украина, 61002

1. Введение

Переход отечественных транспортных предприятий в 90-ых годах прошлого века на новую систему хозяйствования обусловил необходимость развития новых подходов к формированию организационных структур и систем управления перевозками грузов. Особую актуальность данная проблема приобрела на автомобильном транспорте, где роль организации транспортного процесса от автотранспортных объединений перешла к отдельным субъектам транспортного рынка – экспедиторам. Выбор перевозчика относится к одной из основных задач, позволяющих решить указанную проблему.

2. Анализ публикаций

Согласно терминологии теории игр [1], под стратегией понимается правила действия в каждой из возможных ситуаций игры – упрощенной формализованной модели реальной конфликтной ситуации. В [2] выделены основные типы конфликтных ситуаций, возникающих между субъектами рынка транспортных услуг: конфликт между транспортно-экспедиционным предприятием (ТЭП) и перевозчиком и конфликт между ТЭП и грузовладельцем при установлении платы за услугу. В данном исследовании будет рассматриваться, очевидно, первая из обозначенных ситуаций.