About one type of polynomial invariants for linear loops

M.S. Lvov

Kherson State University, 40-Rokiv Zovtnja, 27, 73000, Kherson, Ukraine

Lvov@ksu.ks.ua

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.

In the work [5] two methods are presented for building polynomial invariants of type of equalities in the programs where the data algebra is the domain of integrity (polynomially determined programs) or the field (rationally determined programs). One method allows to construct algebraical dependencies between functions - right hand parts of assignments in an iteration body. The second method - a method of undefinite coefficients - allows to obtain all invariants of the given sort (templates) at any checkpoint of the program, with invariant sort being a set by the polynomial form with indefinite coefficients. The last method is based on Noether property of the ring of polynomials on many variables.

12. Laura Ildikó Kovács, Tudor Jebelean: Finding Polynomial Invariants for Imperative Loops in the *Theorema* System. In: Proceedings of Verify'06 Workshop, IJCAR'06, The 2006 Federated Logic Conference, S. Autexier and H. Mantel (ed.), pp. 52-67. August 15-16 2006.

Algorithm which finds all polynomial invariants for P-solvable imperative loops

P-solvable loop includes the simple situation when the expressions in the assignment statements are linear (i.e affine mappings)

Definition 1 Let W be an n-dimensional vector space on the field of rational numbers Q and $\overline{Q}$ - algebraic closure of field Q. Further on notation $X = (x_1, \ldots, x_n)$ is used for a n-dimentional vector of variables. Rational function $p(X) \in \overline{Q}(X)$ is called L-invariant of the linear operator $A : W \to W$ if for any vector $b \in W$ the relation takes place

$$p(A \cdot b) = p(b). \tag{1}$$

Example 1 (The linear operator with characteristic polynomial $x^3 - 2$).

Let's examine the linear operator with a matrix

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

and show that the rational expression

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

where $\lambda_1 = \sqrt[3]{2}$, $\lambda_2 = \sqrt[3]{2}\epsilon$, $\lambda_3 = \sqrt[3]{2}\epsilon^2$, and $\epsilon = \cos(\frac{2\pi}{3}) + i\sin(\frac{2\pi}{3})$ - is the a original root of degree 3 from 1 - L-invariant of this operator.

Definition 2 Let $X = (x_1, \ldots, x_n)$, $b = (b_1, \ldots, b_n)$ be two vectors of variables. We call as the linear loop a fragment of the imperative program of the form

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

Remark Operators $X := b$, $X := AX$ are interpreted as simultaneous assignments for variables of the left hand parts of values of the right hand parts. Further we will skip the condition $Q(X, b)$, considering the linear loop to be infinite, and its performance to be not determined. Thus we study the loops of the form

```
X := b;
While True do X := AX
```

Proposition 1 If $p(x) = r(x)/q(x)$ - L-invariant of linear operator, a polynomial $r(X)q(b) - q(X)r(b)$ is an invariant of the linear loop over $\overline{Q}$ field. Theese invariants of loops we will also call the L-invariants (of the linear loops).

Example 2 (The linear loop with the operator from Example 1). The linear loop matching to the operator has form

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

L-invariant of this loop is determined by the Eq.(2):

$$P(x,y,z,a,b,c) = (\lambda_1^2 x + \lambda_1 y + z)(\lambda_3^2 x + \lambda_3 y + z)(\lambda_2^2 a + \lambda_2 b + c)^2 - \\ -(\lambda_2^2 x + \lambda_2 y + z)^2(\lambda_1^2 a + \lambda_1 b + c)(\lambda_3^2 a + \lambda_3 b + c) \quad (3)$$

Proposition 2 Let $\lambda_1, \ldots, \lambda_m$ be the eigenvalues of the linear operator A and $s_1, \ldots, s_m$ - the corresponding to them eigenvectors of conjugate operator A^*. Suppose there exist integers $k_1, \ldots, k_m$ such that

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

Then

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

- L-invariant of linear operator A.

Proposition 2`. Let A – linear operator with mutually different eigenvalues $\lambda_1, \lambda_2, ..., \lambda_m$ and suppose that $p(X,b)$ - nontrivial polynomial invariant of the linear loop (Definition 2). Then there exists nontrivial multiplicative relation (6) and, consequently – nontrivial L-invariant of the loop (7).

Example 3 (continuation of the example 2). Let us apply Proposition 2 to the Example 2. First we have to compute the eigenvalues of operator A:

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

Thus the characteristic polynomial has the form $h(x) = x^3 - 2$ with roots $\lambda_1 = \sqrt[3]{2}$, $\lambda_2 = \sqrt[3]{2}\epsilon$, $\lambda_1 = \sqrt[3]{2}\epsilon^2$, $\epsilon = \cos(2\pi/3) + i\sin(2\pi/3)$ (ϵ - the original root of a degree 3 from 1).

the eigenvectors of operator A^* have the form

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

It is easy to show that $\lambda_1\lambda_3/\lambda_2^2 = 1$ and therefore operator A has L-invariant (2).

Corollary 1 If the characteristic (minimal) polynomial $h(x)$ of the linear operator A has a free term, equal to ± 1, the linear operator possesses L-invariant.

Proof Let c be the free term of polynomial $h(x)$. Then $c = (-1)^m \lambda_1 \dots \lambda_m = \pm 1$ and $(s_1, X) \dots (s_m, X)$, or $((s_1, X) \dots (s_m, X))^2$ is L-invariant of operator A. Notice that coefficients of this polynomial belong Q as they are symmetrical under permutations of the roots $\lambda_1 \dots \lambda_m$.

Example 4 A loop of rotation of a point of plane (a, b) to angle $\arctan(4/3)$.

```
(x, y) := (a, b);
while  True  do  (x, y):= (4/5x - 3/5y, 3/5x + 4/5y);
```

Let us compute the eigenvalues and eigenvectors of operator A:

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

$$\lambda_1 = \frac{4}{5} - i\frac{3}{5}, \quad \lambda_2 = \frac{4}{5} + i\frac{3}{5}.$$

$$s_1 = (i, 1), \quad s_2 = (-i, 1).$$

As $\lambda_1\lambda_2 = 1$, L-invariant of operator A takes form

$$p(x, y) = (ix + y)(-ix + y) = x^2 + y^2$$

and finally loop invariant is given by

$$P(x, y, a, b) = x^2 + y^2 - a^2 - b^2.$$

Example 5 A loop of computation of Fibonacci sequence with initial values (a, b).

```
(x, y) := (a, b);
while  True  do  (x, y) := (x + y, x)
```

Eigenvalues and eigenvectors of operator A^* have the form:

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

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

,

$$s_1 = (\lambda_1, 1) = (\frac{1}{2} - \frac{1}{2}\sqrt{5}, 1), \quad s_2 = (\lambda_2, 1) = (\frac{1}{2} + \frac{1}{2}\sqrt{5}, 1)$$

As $\lambda_1\lambda_2 = -1$, L-invariant of operator A takes form

$$p(x, y) = ((\lambda_1 x + y)(\lambda_2 x + y))^2 = (x^2 - xy - y^2)^2.$$

The invariant relation of a loop looks like

$$(x^2 - xy - y^2)^2 = (a^2 - ab - b^2)^2.$$

Corollary 2 If characteristic (minimal) polynomial $h(X)$ of linear operator A has the form $x^n - a$, the linear operator A possesses L-invariants.

Proposition 3 Let $h(x)$ be a polynomial from variable x with rational coefficients and $\Lambda = (\lambda_1, \ldots, \lambda_m)$ are all its roots from algebraic closure $\overline{Q}$ of field Q. Let us consider the set

$$G(h) = \left\{ {x_1}^{k_1} \ldots x_m^{k_m} : \ \lambda_1^{k_1} \ldots \lambda_m^{k_m} = 1 \right\}.$$

This is set of monomials from the field of rational expressions $Q(X)$ (probably, with the subzero degrees) with the following property: substitution of λ_i instead of x_i yields 1. Then $G(h)$ is a multiplicative Abelian group with a finite number of generators.

Example 6 (Continuation of the Example 3). It is easy to see that for polynomial $h(x) = x^3 - 2$ the following multiplicative relations between its roots exist:

$$\lambda_1^2 = \lambda_2\lambda_3, \quad \lambda_1\lambda_2 = \lambda_3^2, \quad \lambda_1\lambda_3 = \lambda_2^2, \quad \lambda_2^3 = \lambda_3^3$$

Corresponding binomials are

$$x_1^2 - x_2x_3, \quad x_1x_2 - x_3^2, \quad x_1x_3 - x_2^2, \quad x_2^3 - x_3^3$$

and they form Gröbner basis of ideal $I(G_B) = I(G(h))$.

Corollary 1 Let $h(x)$ be a polynomial on variable x with rational coefficients and $\Lambda = (\lambda_1, \ldots, \lambda_m)$ are all its roots from algebraic closure $\overline{Q}$ of field Q. Let us regard the set

$$G_Q(h) = \left\{ {x_1}^{k_1} \ldots {x_m}^{k_m} : \lambda_1^{k_1} \ldots \lambda_m^{k_m} \in Q \right\}.$$

This is the set of monomials from the field of rational expressions $Q(X)$ (possibly, with the subzero degrees) which get rational values after substitution λ_i instead of x_i . Then $G_Q(h)$ - multiplicative Abelian group with a finite number of generators.

Corollary 2 The set of of all L-invariants of operator A forms a field of rational expressions.

Proposition 4 Let $p(x)$ be a normalized polynomial, irreducible over field Q, and $\{\lambda_1, \lambda_2, \ldots, \lambda_m\}$ is a set of its roots over field $\overline{Q}$. If between its roots there exists a nontrivial multiplicative relation $\lambda_1^{k_1} \ldots \lambda_m^{k_m} = 1$ with integer indexes $k_1, \ldots, k_m$, the free term a_m of polynomial $f(x)$ is equal to ± 1, or $\sum_{i=1}^{m} k_i = 0$.

Definition 3 L-invariants of operator A, determined as a multiplicative relation between radicals of characteristic polynomial $\lambda_1 \cdot \ldots \cdot \lambda_m = \pm 1$, are called integer L-invariants. L-invariants of operator A $\lambda_1^{k_1} \ldots \lambda_m^{k_m} = 1, \sum k_i = 0$ are called rational L-ivariants.

Proposition 5 If characteristic polynomial of the operator A has form $h(x^k)$, $k > 1$, the operator A possesses rational L-invariants.

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1} x \pm 1$$

$$f(x) = x^{md} + a_1 x^{(m-1)d} + \ldots + a_{m-1} x^d + a_m$$