The Static Analysis of Linear Loops

Michael Lvov[1], Yulia Tarasich[1],

[1]Kherson State University, 40 rokiv Zhovtnya St. 27
73000, Kherson, Ukraine
{Lvov, YuTarasich}@ksu.ks.ua

Abstract. In the first part of the paper, we consider the problem of generation of polynomial invariants of iterative loops with operator of initialization of loop and non-singular linear operator in the loop body. In the article we also show the algorithm for calculating the basic invariants for linear operator of the Jordan cell, and an algorithm for calculating the basic invariants of diagonalizable linear operator with an irreducible minimal characteristic polynomial. The second part presents a new method for proving the invariance of the system of linear inequalities and of termination of certain linear iterative loops of imperative programs whose data are elements of the constructive linearly ordered field. The theoretical material of the paper is illustrated by examples.

Keywords. Static program analysis, polynomial invariant of a loop, invariant system of linear inequalities, eigenpolynomial of a linear operator.

Key Terms. VerificationProcess, Method, FormalMethod

1 Introduction

As for now, methods of program statistical analysis are being studied intensely. One of the important problems is a problem of the automatic generation of program invariants. Invariants of program are used particularly in methods of programs verification.

The problem of searching for loop invariants in imperative programs was offered by R. Floyd [1] and C. Hoare [2].

A correctness property of the program is formulated in terms of its total or partial correctness. Often, the proof of termination of the program should be implemented separately from the proof of its partial correctness. The algorithmic unsolvability of the termination problem shows that the general algorithm of proof of termination of the program does not exist. To prove the partial correctness of programs, P. Floyd and S. Hoare offered the idea of building loop invariants [1] and invariant relations in control points of programs [2], which allows to prove programs by method of math induction.

Thus, there is a problem of finding the invariants of the program as a key problem of analysis of programs properties.

Now, the main attention is paid to the problem of constructing polynomial invariant equalities. A set of invariant equalities forms the polynomial ideal, a finite basis of which one must build. Note that in a general case, the problem of constructing this basis has not been solved.

The existence and efficiency of algorithms to generate program invariants depend on the subject domain, i.e., on the properties of the data algebras the program deals with. Problems of automatic generation of program invariants for various data algebras have been being analyzed since beginning of 1970s at the Institute of cybernetics of NAS of Ukraine. Their main results are represented in [3,4].

Numerical data algebras are the most important from the practical point of view. The paper [5] outlines two methods of constructing polynomial invariant equalities types in programs whose data algebra is the domain of integrity (polynomially determinate programs) or a field (rationally determinate programs).

This idea used in [6] to generate polynomial invariants of bounded degree for polynomially determined programs. Program conditions such as $f(X) \neq 0$ were taken into account, where $f(X)$ are polynomials of program variables. In [7] they proposed a method to generate polynomial program invariants of bounded degree in linearly determinate (affine) programs containing recursive procedure calls.

In [8] they proposed a method to generate polynomial loop invariants as template polynomials with the use of the algorithm for computing Grobner bases. In [9] they described a method to generate nonlinear and, generally speaking, nonpolynomial invariant relation for linear loops. The method uses eigenvalues and eigenvectors of the linear operator in the loop body.

The paper [10] is devoted to the algebraic fundamentals of the problem of generating polynomial loop invariants. The main result of the study is an algorithm for generating all polynomial invariants for loops with so-called solvable assignment operators. In particular, affine operators with positive real eigenvalues are solvable. The same authors [11] proposed a method to generate polynomial loop invariants, including enclosed loops, as well as program conditions in the form of both polynomial equalities and inequalities. The paper considers a great number of examples and presents tables for the algorithm time depending on technical parameters of the program being analyzed.

In [12] they proposed an algorithm to search for loop invariants based on a system of recurrent relations with loop variables and parameter *n*, which is the loop index. The algorithm searches for the solution of this system not depended on *n*. It is implemented in Theorema software system and is illustrated with examples in detail.

The problem of the description of invariant inequalities is less studied. The main intricacy lies in the infinity of the basis of the metaideal [13] of polynomial inequalities [13, 14]. Iterative methods for solving the problem of the description of linear invariant inequalities were considered in [15-18]. In [15], the problem of generation of the simplest invariant inequalities is solved. In [16-17], general iterative methods are used to solve the problem of searching for linear invariant inequalities.

In [19] they described a method of proving the invariance of the system of linear inequalities for a class of linear iterative loops with real eigennumbers of linear

operators in the loop body. This method can be applied to the entire class of linear iterative loops and it can also be applied to prove their termination. The paper with description of it is under preparation for a publication.

2 The Static Analysis of Polynomial Invariant Equations

2.1 L-invariants of Linear Maps and Invariants of Linear Loops.

Definition 1. Let W be an *n*-dimensional vector space over the field of rational numbers Q and let $\bar{Q}$ be the algebraic closure of the field Q. Let $X = (x_1,....x_n)$ be an n-dimensional vector of variables. A rational function $p(X) \in \bar{Q}(X)$ is called ***L***-invariant of a linear operator $A: W \to W$ if, for any vector $b \in W$ the following relationship holds:

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

Example 1. (a linear operator with characteristic polynomial $x^3 - 2$)
Let us consider a linear operator with the matrix

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

It's easy to calculate [26], 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 $\lambda_1 = \sqrt[3]{2}$, $\lambda_2 = \sqrt[3]{2}\varepsilon$, $\lambda_3 = \sqrt[3]{2}\varepsilon^2$, and $\varepsilon = \cos(\frac{2\pi}{3}) + i\sin(\frac{2\pi}{3})$ is the primitive third root of unity, is the L-invariant of this operator.

Definition 2. Let $X = (x_1,..., x_n)$ and $b = (b_1,..., b_n)$- be two collections of variables. The following fragment of an imperative program is called a linear loop:

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

Remark 1. Operators X:=b and X:=A*X are interpreted as simultaneous assignments of the values of the variables of the right sides to the variables on the left sides. In what follows, we ignore the condition Q(X, b) and consider that the linear loop is infinite and that its execution is nondeterministic. Thus, we consider loops of the form

```
X := b;
While True|False do X := A*X                    (3)
```

Definition 3. Let a vector $b^{(0)} = (b_1^{(0)},...,b_n^{(0)}) \in W$ be chosen as initial. Sequence of vectors, set by recurrent correlation $b^{(j+1)} = Ab^{(j)}$, will be called the orbit of linear operator A.

A loop sets the orbit of linear operator A in space W. Obviously, an orbit A lies in some one-dimensional variety, and the system of invariants characterizes this variety as algebraic.

Definition 4. Polynomial $P(b, X)$ is called loop invariant if, for any natural j and any $b^{(0)}$ $P(b^{(0)}, b^{(j)}) = 0$.

Theorem 1. If $p(X) = r(X)/q(X)$ is an L-invariant of a linear operator A, then the polynomial $r(X)q(b) - q(X)r(b)$ is an invariant of a linear loop over the field $\bar{Q}$.

We call such loop invariants *L*-invariants (of linear loops).

Example 2. (a linear loop with operator from example 1)

The linear loop corresponding to the operator A, has the form

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

L-invariant of this loop is defined by formula (2):

$$P(x,y,z,a,b,c) = (\lambda_1^2 x + \lambda_1 y + z)(\lambda_3^2 x + \lambda_3 y + z)(\lambda_2^2 a + \lambda_2 b + c)^2 - \\ -(\lambda_2^2 x + \lambda_2 y + z)^2 (\lambda_1^2 a + \lambda_1 b + c)(\lambda_3^2 a + \lambda_3 b + c) \quad (4)$$

Note that L-invariant of the loop $P(x, y, z, a, b, c)$ is defined over a field $\bar{Q}(\lambda_1, \lambda_2, \lambda_3)$. However, it has a set of L-invariants with coefficients from the field Q, which can be constructed, they are shown in (4) the canonical form to the polynomial from $\lambda_1, \lambda_2, \lambda_3$, and then - to the polynomial from λ_2 with using the relation $\lambda_1\lambda_3 = \lambda_2^2$ and Vieta's relation. Technique for computing L-invariants over a field Q is demonstrated in [20]. Note that if the variables a, b, c are the assigned numeric values, L-invariant is converted into a loop invariant.

In [22] they described the results, that link L-invariants to eigenvalues and eigenvectors of the operator A^T. The main result of this work:

Theorem 2 (about the multiplicative relations). Let $\lambda_1,...,\lambda_m$ be eigenvalues of a linear operator A and let $s_1,...,s_m$ be eigenvectors of the conjugate operator A^T

that correspond to these eigenvalues. We assume that there are integers $k_1,...,k_m$ such that

$$\lambda_1^{k_1} \cdot ... \cdot \lambda_m^{k_m} = 1 . \quad (5)$$

Then

$$p(X) = (s_1, X)^{k_1} \cdot ... \cdot (s_m, X)^{k_m} \quad (6)$$

is *L*-invariant of the linear operator A.

Proof of the theorem 2 can be found in [21]

Example 3 (continuation of example 2). Apply the theorem 2 to the example 2. Calculate the eigennumbers of operator A.

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

A characteristic polynomial has the form b $h(x) = x^3 - 2$. Its roots are $\lambda_1 = \sqrt[3]{2}, \; \lambda_2 = \sqrt[3]{2}\varepsilon, \; \lambda_3 = \sqrt[3]{2}\varepsilon^2$, where $\varepsilon = \exp(i\,2\pi/3)$ is the primitive cube root of unity.

Calculate the eigenvectors s_1, s_2, s_3 of matrix $A^T = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$:

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

It is easy to check that $\frac{\lambda_1 \lambda_3}{\lambda_2^2} = 1$. By the theorem 2 the operator A has a L-invariant (2).

Corollary 1. If the minimum characteristic polynomial $h(x)$ of linear operator A has a free term equal to ± 1 (i.e. $\det(A) = \pm 1$), then the linear operator A has a **L**-invariant.

Example 4. A loop of the points rotation of a plane (a,b) at an angle $\arctan(4/3)$.

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

Calculate the eigenvalues and eigenvectors of the operator A:

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

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

Since $\lambda_1\lambda_2=1$, L-invariant of the operator A is

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

And the loop invariant is $x^2+y^2-a^2-b^2$.

Example 5. Loop of Fibonacci sequence calculation, starting with a pair of (a,b).

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

Calculate the eigenvalues and eigenvectors of the operator A:

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

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

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

Since $\lambda_1\lambda_2=-1$, L-invariant of the operator A is

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

The invariant relation of loop is $(x^2-xy-y^2)^2=(a^2-ab-b^2)^2$.

Corollary 2. If the characteristic (minimum) polynomial $h(X)$ of linear operator A is x^m-a, then linear operator has an L-invariants.

Proofs of corollaries 1 and 2 are in [21]

Theorem 3. Let $h(x)$ be an polynomial from variable x with rational coefficients and $\Lambda=(\lambda_1,...,\lambda_m)$ are all its roots in an algebraic closure $\bar{Q}$ of the field Q. Consider the set $G(h)=\{x_1^{k_1}\cdot...\cdot x_m^{k_m}:\lambda_1^{k_1}\cdot...\cdot\lambda_m^{k_m}=1\}$ that is the set of monomials of the field of rational expressions $Q(X)$ (possibly with negative degrees), who receive a value of 1 when we substitute λ_i instead of x_i. Then $G(h)$ is a multiplicative abelian group with a finite number of generators.

The proof of theorem 3 is obvious, since the subgroup of an abelian group with a finite number of generators has a finite number of generators.

It follows from theorem 3 that the main problem for the generation of L-invariants is the problem of finding an algorithm for constructing a set that generate the groups $G(h)$.

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

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

These relations have relevant binomials

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

that form a Gröbner basis of the ideal $I(G_B) = I(G(h))$.

Corollary 3. The set of all L-invariant of operator A defines the field of rational expressions.

Proof of **corollary** 3 is in [21]

Theorem 4 Let $f(x)$ be irreducible over the field Q and reduced polynomial and $\{\lambda_1, \lambda_2, ...\lambda_m\}$ is the set of its roots over the field $\bar{Q}$. If we have a nontrivial multiplicative relationship $\lambda_1^{k_1}...\lambda_m^{k_m} = 1$ with integer indices $k_1,...,k_m$ between his roots, then the free term a_m $f(x)$ equal to ± 1 or $\sum_{i=1}^{m} k_i = 0$.

The proof is in [21]

Definition 5. L-invariants of operator A, defined of multiplicative relation between the roots of the characteristic polynomial $\lambda_1 \cdot ... \cdot \lambda_m = \pm 1$, will be called whole. L-invariants of operator A, defined of multiplicative relation $\lambda_1^{k_1} \cdot ... \cdot \lambda_m^{k_m} = 1, \sum k_i = 0$, will be called rational.

Theorem 5. If the characteristic polynomial of operator A is $h(x^k), k > 1$, then operator A has a rational L-invariants.

The **proof** of theorem 5 is in [21]

2.2 L-invariants of Jordan Cells

A nondegenerate linear operator A can be represented in a suitable basis by the following Jordan form of its matrix [18, 22].

$$A = \begin{bmatrix} J_1(\lambda_1) & 0 & ... & 0 \\ 0 & J_2(\lambda_2) & ... & 0 \\ . & . & ... & . \\ 0 & 0 & ... & J_m(\lambda_m) \end{bmatrix}, \qquad (7)$$

where $J_i(\lambda_i)$ are Jordan cells of different sizes. Jordan cell is of the form

$$J(\lambda)=\begin{bmatrix}\lambda & 1 & ... & 0\\ 0 & \lambda & ... & 0\\ 0 & ... & \lambda & 1\\ 0 & ... & 0 & \lambda\end{bmatrix} \qquad (8)$$

Thus, theorem 2 is applied only to the rows of the matrix of the linear operator A, that correspond to the eigenvectors of A, i.e., to the collection of the last rows of Jordan cells $J_i(\lambda_i)$, $i=1,...,m$. Below, we will extend this theorem to arbitrary nondegenerate linear operators by considering Jordan cells on the whole.

Transformation $J := J * X$, where $X=(x_1,...,x_k)$, in the coordinate form is

$$x_1 := \lambda x_1 + x_2; ...; x_{k-1} := \lambda x_{k-1} + x_k; x_k := \lambda x_k$$

Introduce the following notation: $x_{k-1} \overset{df}{=} y,\ x_k \overset{df}{=} z$.

For each Jordan cell $J_k(\lambda_k)$ of the Jordan form of the operator A its own sequence of subspaces of eigenpolynomials is determined.

The main theory of the eigenpolynomials of Jordan cells as well as of the relationship between eigenpolynomials and *L*-invariants of linear operators is formulated in [23, 24].

The concept of eigenpolynomial of a linear operator can be of an independent interest for linear algebra applications.

If all eigennumbers of linear operator A are rational numbers, then the problem of constructing this basis is an algorithmically solvable with the help of theoretical&number algorithm.

In the [25] a direct method of finding invariants of Jordan cells is described. The main results of this work are discussed below.

Theorem 6 (about the structure of the ideal of invariants)**.** Let A be an arbitrary nondegenerate linear operator, presented in a suitable basis of matrix (7), $I_{J_1}(A),...,I_{J_k}(A)$ are ideals of his invariants, presented in homogeneous coordinates

$$u_{ij}=x_{ij}/z_i,\ u_i=y_i/z_i \qquad e_{ij}=a_{ij}/c_i, e_i=b_i/c_i$$

by basis of the form

$$u_j - q_j(\lambda,u,1),\ j=1,...,n-2$$

and $I_\Lambda(A)$ is an ideal of invariants of the operator A_{red}, and $I(A)$ is an ideal of invariants of the operator A (of the loop (3)). Then

$$GBase(I_\Lambda(A)) = GBase(I_{J_1}(A)) \cup ... \cup GBase(I_{J_k}(A)) \cup GBase(I_\Lambda(A))$$

Theorem 7. If a group of multiplicative relations of roots of an irreducible polynomial $f(x)$ is nontrivial $(MR(f)\neq(e))$, there may be two situations:

1. The set of roots $\Lambda = (\lambda_1,...,\lambda_n)$ is divided into certain number l of equally-powerful classes $\Lambda_1,...,\Lambda_l;\ \Lambda_j = \{\lambda_{(j-1)d+1},...\lambda_{jd}\};\ j = 1,...,l.$ wherein $d = len(\Lambda_j),\ n = ld$. Multiplicative relations from $MR(f)$ in this situation have the form $\Lambda_j = \varepsilon_j,\ j = 1,...,l$, where ε_j are roots from 1.
2. The equally-powerful classes $\Lambda_1,...,\Lambda_l,\ \Lambda_i = \{\lambda_{(i-1)d+1},...\lambda_{id}\};\ i = 1,...,k.$ Wherein $d = len(\Lambda_j),\ n = kd$. Multiplicative relations from $MR(f)\ MR(f)$ in this situation have the form $\Lambda_i = \varepsilon_{ij}\Lambda_j,\ i = 1,...,l$, where ε_j are roots from 1.

Both situations may occur simultaneously.

For the proof of theorem 7, take a look in [25]. This theorem has a key role for the algorithm of calculation of the system generators of the group $MR(f)$.

Theorem 8. Let $f(x) \in Q[x]$ is an irreducible polynomial and $\lambda_1,...,\lambda_m$ are its roots. The problem of constructing a basis of a set of generating the group $G_U(h) = \{x_1^{k_1}...x_m^{k_m} : \lambda_1^{k_1}...\lambda_m^{k_m} \in U\}$, where U is a group of all roots from 1 is algorithmically solvable.

The proof of theorem 8 is in [25].

Thus, by theorem 6, the invariants of a linear operator can be classified as intracellular - that are inherent to each Jordan cell of linear operator, and intercellular - those that are inherent in its diagonalisable part.

Intracellular invariants are computed directly from the formulas of [25]

$$x_j = \frac{z}{c}(a_j + \frac{C_1(\lambda\frac{cy-bz}{cz})}{\lambda}a_{j+1} + ... + \frac{C_{n-j}(\lambda\frac{cy-bz}{cz})}{\lambda^{n-j}}a_n)\ .$$

The existence of intercellular invariants depend on the existence of nontrivial multiplicative relations between the eigenvalues of the linear operator (theorem 2).

For linear operators with an irreducible minimum characteristic polynomial problem of constructing a basis of set of multiplicative relations between its eigenvalues is algorithmically solvable, but the algorithm of theorem 8 is ineffective due to a very large degree of the polynomial $S(x)$, which is be necessary to decompose into factors.

The problem of constructing a basis of set of multiplicative relations for arbitrary linear operators is still open.

3 The Static Analysis of Linear Inequalities.

Let $W = K^n$ be an n-dimensional vector space over a linearly ordered and constructive field K and $\bar{K}$ is an algebraic closure of K.

Definition 6. As a linear semi-algebraic set $M(x_1,...,x_n)$ is called the area W, that is defined by a quantifier-free formula in the signature of the logical connectives $<\vee,\&,\neg>$ with linear inequalities in the variables $x_1,...,x_n$ as atoms. If the field M is given by the formula $F(X)$, i.e. $M=\{X : F(X)\}$, We shall denote it by $M(F(X))$.

Definition 7. Let $X=(x_1,...,x_n)$, and $\bar{b}=(b_1,...,b_n)$ be two vectors of variables. The linearly loop with the precondition is a fragment of imperative program in the form

```
X := b; //  S(b̄)  - a precondition
While U(X, b) do X := A*X                                    (9)
```

where $S(\bar{b})$, and $U(X,\bar{b})$ are quantifier-free formulas of applied logic of linear semi-algebraic sets, A is a matrix of the linear operator $W \to W$.

Non-deterministic and associated with loop (9) we call the loop of the form

```
X := b; //  S(b̄) - a precondition
While True|False do X := A*X                                 (10)
```

whose number of repeats is nondeterministic.

Remark 2. Definition 7 of loops differs from the definitions 2 and 3 because of its precondition $S(\bar{b})$ that limited the initial values of the loops variables by a linear semi-algebraic set and an introduction to the consideration of the conditions of the loop $U(X,\bar{b})$.

Definition 8. Linear inequality $P(X,b)\in K^1[X,b]$ is called an invariant for the loop (9) with a precondition $S(b)$, if it is executed whenever the loop body is executed.

$$P(X,b)\overset{df}{=}a_1x_1+...+a_nx_n<a_1'b_1+...+a_n'b_n$$

Thus, the invariance means performing of a sequence of formulas

$S(b)\to P(b,b)$, // Invariant is executed in the input in the loop

$U(b,b)\to P(Ab,b)$, // Invariant is executed after the first iteration

$U(Ab,b)\to P(A^2b,b)$, // Invariant is executed after the second iteration

...

$U(A^kb,b)\to P(A^{k+1}b,b)$, // Invariant is executed after the k-th iteration

$\neg U(A^kb,b)\to P(A^kb,b)$ // Invariant is executed at the completion of the loop

Theorem 9. If all eigenvalues $\Lambda = (\lambda_1,...,\lambda_n), \lambda_i \in \overline{K}$ of operator A are real, the problem of proving of the invariance $P(X,b)$ for the loop (9) is algorithmically solvable.

The main content of the proof of theorem 9 is formulated in lemmas 1-5 [13].

Definition 9. The linearly defined loop (10) is called completed if for any $\bar{b} \in M(S(X))$ the sequence

$$\bar{b}^{(0)} = \bar{b},\ \bar{b}^{(m+1)} = A\bar{b}^{(m)}, m = 0,1,... \quad (11)$$

for some natural $m^* = m^*(\bar{b})$ satisfies the relationship $\neg U(\bar{b}^{(m^*)}, \bar{b})$.

Thus, if the loop is completed, for each $\bar{b} \in M(S(X))$ is the smallest positive integer $m^*(\bar{b})$, on which the loop (9) is completed.

Definition 10. Let $\bar{a}, \bar{c} \in K^n$. A linear inequality

$$L(\bar{a},\bar{c},X,\bar{b}) \overset{df}{=} (\bar{a},X) \le (\bar{c},\bar{b}) \quad (12)$$

is called conditional invariant of linear certain loop (9) (with a precondition $S(\bar{b})$), if for any $\bar{b} \in M(S(X))$ $Orbit(A,\bar{b})$ (11) is satisfies to relations $S(\bar{b}) \to L(\bar{a},\bar{c},\bar{b},\bar{b})$, $U(\bar{b}^{(m-1)},\bar{b}) \to L(\bar{a},\bar{c},\bar{b}^{(m)},\bar{b}),\ m = 1,2,...,m^*(\bar{b})$.

Remark 3. If the loop (10) is not completed (is branched) at some point $\bar{b}$, $m^*(\bar{b})$ it should be considered equal to infinity.: $m^*(\bar{b}) = +\infty$.

Example 7.

$S(x,y) = (0 \le x \le 1) \& (0 \le y \le 1)$,

$U(x,y,b_1,b_2) = \neg(|x + b_1| \le \varepsilon) \& (|y + b_2| \le \varepsilon)$,

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

$L = x + y \le 2b_1 + 2b_2 \,//\, \bar{a} = (1,1),\ \bar{c} = (2,2)$.

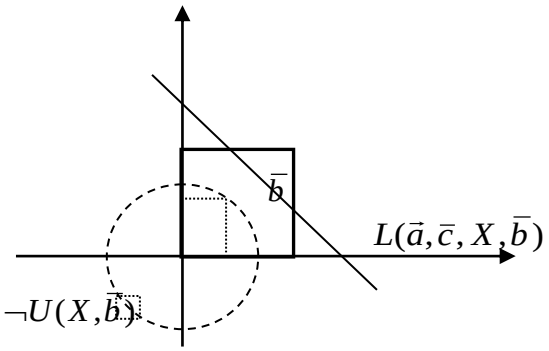

Fig. 2. Geometric illustration of the linear defined loop.

In this example, the linear operator A is an operator of rotation for angle $\alpha = arctg(4/3)$. A starting point $\bar{b}$ belongs to the unit square. The orbit of a linear operator A is a sequence, each point of which lies on the loop $x^2 + y^2 = b_1^2 + b_2^2$. The condition of repeating of the loop is a «point (x, y) that lies outside the square with side 2ε and center at $(-b_1,-b_2)$». Therefore, a loop is completed when the point gets inside this square, i.e. a point will make the rotation by angle $\pi + 2k\pi$ with accuracy equal to ε. Since the angle α is incommensurate with π, the orbit of the operator A is a dense set on the circle $x^2 + y^2 = b_1^2 + b_2^2$, therefore, the loop is complete. In this example, the basic algorithm is used to prove that $L = x + y \le 2b_1 + 2b_2$ is a conditional invariant of loop.

Let $f(x)$ be a minimal characteristic polynomial of the operator A, $\Lambda = \{\lambda_1,...,\lambda_n\}$ is a set of its roots (spectrum A). Suppose further that, $\lambda_1,...,\lambda_{2k}$ is a set of complex eigenvalues, and $\lambda_{2k+1},...,\lambda_n$ is a set of real eigennumbers and $\lambda_1 = \overline{\lambda}_2,...,\lambda_{2k-1} = \overline{\lambda}_{2k}$ than we obtain a representation of a linear operator in the so-called real Jordan form:

$$A' = \begin{bmatrix} B_1 & 0 & . & 0 & . & . & 0 \\ 0 & B_2 & . & 0 & . & . & 0 \\ . & . & . & . & . & . & . \\ 0 & ... & 0 & B_k & . & ... & 0 \\ 0 & . & . & 0 & \lambda_{2k+1} & ... & 0 \\ . & . & . & . & . & . & . \\ 0 & . & . & . & 0 & ... & \lambda_n \end{bmatrix}$$

Where $B_j = r_j \begin{bmatrix} \alpha_j & \beta_j \\ -\beta_j & \alpha_j \end{bmatrix}$.

Remark 4. After the transition to a basis of eigenvectors the coefficients of inequality will be changed. If $S(\Lambda)$ is a transition matrix, then the new values of the vectors $\bar{a}, \bar{b}$ calculated by the formulas $\bar{a}^{(S)} = S\bar{a}S^{-1}, \bar{b}^{(S)} = S\bar{b}S^{-1}$. But in order not to overload the text by new notations, we will use the old notations.

Note, that the matrix of the form $B \overset{df}{=} \begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix}$, where $\alpha^2 + \beta^2 = 1$ is a matrix of rotation of vector of two-dimensional space on the angle φ, that is defined by ratios $\cos(\varphi) = \alpha, \sin(\varphi) = \beta$. That is why

$$B_j = r_j \begin{bmatrix} \cos(\varphi_j) & \sin(\varphi_j) \\ -\sin(\varphi_j) & \cos(\varphi_j) \end{bmatrix}, \; r_j = \left|\lambda_j\right| = \sqrt{\alpha_j{}^2 + \beta_j{}^2}\,.$$

inequality (12), whose invariance is regarded by a loop (11) with a specific initial value $\bar{b}$, indicates that $\forall X \in Orbit(A, \bar{b})(\bar{a}, X) \le (\bar{c}, \bar{b})$. Algorithm of prove of the invariance of (12) will be formulated in the equivalent form:

$$\underset{X \in Orbit(A,\bar{b})}{Sup} (\bar{a}, X) \le (\bar{c}, \bar{b}).$$

Let us consider the linear form $a_1x_1 + a_2x_2 + \ldots + a_nx_n \overset{df}{=} (\bar{a}, X)$. The transformation $X := A * X$ converting this form in (a, AX), and m is a multiple iteration of loop, that is described by the transformation $X := A^m * X$ - in $(a, A^m X)$.

Let $X_1 = (x_1, x_2), \ldots, X_k = (x_{2k-1}, x_{2k})$, $\bar{a}_1 = (a_1, a_2), \ldots, \bar{a}_k = (a_{2k-1}, a_{2k})$. Then

$$(\bar{a}, X) = (\bar{a}_1, X_1) + \ldots + (\bar{a}_k, X_k) + a_{2k+1}x_{2k+1} + \ldots + a_nx_n \qquad (13)$$

Conversion $(\bar{a}, AX)$ of a linear form can be written as

$$(\bar{a}, AX) = (\bar{a}_1, B_1X_1) + \ldots + (\bar{a}_k, B_kX_k) + \lambda_{2k+1}a_{2k+1}x_{2k+1} + \ldots + \lambda_n a_n x_n \qquad (14)$$

And its m-th iteration can be written as

$$(\bar{a}, A^m X) = (\bar{a}_1, B_1^m X_1) + \ldots + (\bar{a}_k, B_k^m X_k) + \lambda_{2k+1}^m a_{2k+1}x_{2k+1} + \ldots + \lambda_n^m a_n x_n \qquad (15)$$

Passing in (14) to the representation in the form $B_j = r_j B_j$, we obtain:

$$(\bar{a}, A^m X) = r_1^m (\bar{a}_1, B_1^m X_1) + \ldots + r_k^m (\bar{a}_k, B_k^m X_k) + \lambda_{2k+1}^m a_{2k+1}x_{2k+1} + \ldots + \lambda_n^m a_n x_n$$

Consider the question of the set of values of the operator orbit $(\bar{a}_1, B_1^m X_1) + ... + (\bar{a}_k, B_k^m X_k)$ for the initial value $\bar{b}^{(0)} = (\bar{b}_1^{(0)},...,\bar{b}_k^{(0)})$, where $\bar{b}_j = (b_{2j-1}, b_{2j})$, $j = 1,...,k$. The interpreted pair X_j shall be as points on the two-dimensional plane, and the conversion of $\widehat{B}_j \overset{df}{=} \begin{bmatrix} \cos(\varphi_j) & \sin(\varphi_j) \\ -\sin(\varphi_j) & \cos(\varphi_j) \end{bmatrix}$ - as a rotations of points X_j on the angle φ_j.

The proof is formulated in lemmas 1-7 in [20].

Theorem 10. The problem of proving the invariance of inequality $L(\bar{a}, \bar{c}, X, \bar{b})$ for the loop (9) with diagonalizable linear operator A and with an initial point $\bar{b}$ is algorithmically solvable.

Theorem 11. The problem of proving the invariance of inequality $L(\bar{a}, \bar{c}, X, \bar{b})$ for the loop (9) (i.e., with the precondition $S(b)$) is algorithmically solvable.

Theorem 12. The problem of termination of the loop (9) is algorithmically solvable. Proof of theorems 10-12 is in [20].

4 Conclusion

This review represents main results of several works of one of the authors of the theory of program invariants. Subject of the research is an invariant of linear iteration loops. A new approach to the problems of static analysis of linear loops is represented: the problem of generating of polynomial invariance equations and the problem of proving the invariance of linear inequalities. This approach uses the representation of a linear operator in the loop body in the Jordan form and is based on the analysis of the spectrum of this operator.

The main results about invariant equality are the theorem 2 about multiplicative relations, a formula of invariant equations for the Jordan cell, a theorem 6 of the structure of a basis of the ideal of polynomial invariants, and, also, the algorithm of constructing of the basis of ideal of polynomial invariants for operators with irreducible over the field of rational numbers characteristic polynomial. Thus, for a given problem the problem of constructing of the basis of ideal of polynomial invariants for operators with a reducible characteristic polynomial remains open. From the practical view, the interest is in constructing the corresponding effective algorithms.

Unlike polynomial equations, the set of linear invariant inequalities does not have a finite basis. Therefore, a method of generating the basis is not applicable to this task. This paper represents the basic idea of the direct method of proof of the invariance of linear inequalities. There is a need to note, that the key role in the method is played by the set of maximal (from the modulus) eigenvalues of operator A. In this case, the case of maximal real eigenvalues and the maximal complex eigenvalues are significantly different. In the second case, the method uses the original method of

finding the maximum of the linear form in the orbit of a linear operator, and various algorithms of computation in the field of algebraic number.

There is a need to assume that this method can be used as a basis for a general algorithm of proving the invariance of a system of linear inequalities for linear-certain programs, similar to the method of proof of invariance of polynomial equations [5, 6], and to prove the invariance of polynomial inequalities for linear-certain programs.

References

1. Floyd, R.: Assigning Meanings to Programs. In: Proceedings of Symposium on Applied Mathematics, J.T. Schwartz (Ed.), American Mathematical Society, vol. 19, pp. 19--32, Providence, R.I. (1967)
2. Hoare, C.: An Axiomatic Basis for Computer Programming. Communications of the ACM 12(10), 576--580 (1969)
3. Letichevsky, A..: About One Approach to Program Analysis. Cybernetics 6, 1--8 (1979)
4. Godlevsky, A., Kapitonova, Y., Krivoy, S., Letichevsky, A.: Iterative Methods of Program Analysis. Cybernetics 2, 9--19 (1989)
5. Letichevsky, A., Lvov, M.: Discovery of Invariant Equalities in Programs over Data Fields. Applicable Algebra in Engineering, Communication and Computing 4, 21--29 (1993)
6. Müller-Olm, M., Seidl, H.: Precise Interprocedural Analysis Through Linear Algebra. In: Proc. of Symposium on Principles of Programming Languages, pp. 330--341, ACM, New York (2004)
7. Lvov M.: About One Algorithm of Program Polynomial Invariants Generation. Technical report, RISC Report Series (2007) (electronic).
8. Müller-Olm, M., Seidl, H.: Computing Polynomial Program Invariants. Inf. Process. Lett. 91(5), 233--244 (2004)
9. Sankaranarayanan, S., Sipma, H., Manna, Z.: Non-linear Loop Invariant Generation Using Gröbner Bases. In: Proc. of Symposium on Principles of Programming Languages, pp. 318--329, ACM, New York (2004)
10. Caplain, M.: Finding Invariant Assertions for Proving Programs. In: Proc. of the intern. Conf. on Reliable Software, pp. 165--171, ACM, New York (1975)
11. Rodríguez-Carbonell, E., Kapur, D.: Automatic Generation of Polynomial Loop Invariants: Algebraic Foundations. In: Proc. Of International Symposium on Symbolic and Algebraic Computation, pp. 266--273, ACM, New York (2004)
12. Rodríguez-Carbonell, E., Kapur, D.: Automatic Generation of Polynomial Invariants of Bounded Degree Using Abstract Interpretation. Sci. Comput. Program 64(1), 54--75 (2007)
13. Lvov, M.: A Method of Proving the Invariance of Linear Inequalities for Linear Loops. Cybernetics and Systems Analysis 4, 80--85 (2014)
14. Kovács, L. I., Jebelean, T.: An Algorithm for Automated Generation of Invariants for Loops with Conditionals. In: Proc. of Intern. Symposium on Symbolic and Numeric Algorithms for Scientific Computing. pp. 245--249, IEEE Computer Society, Timisoara (2005)
15. Kurosh, A.: Theory of Groups. 3-rd ed. Science, Moscow (1967)
16. Postnikov, M.: Galois Theory. Fizmatgiz, Moscow (1963)
17. Buchberger, B:. Gröbner Bases. An Algorithmic Method in the Theory of Polynomial Ideals. Computer algebra. Symbolic and algebraic computations. Mir, Moscow (1986)
18. Van Der Waerden: Algebra, B. the 2-th edition. GRFML, Moscow (1979)
19. Dieudonné, J. Carroll, Dj. Mumford, D.: Geometric Invariant Theory. Mir, Moscow (1974)

20. Lvov, M.: Analysis of Linear Defined Iterative Loops. Cybernetics and Systems Analysis 4 (2015) (In print)
21. Lvov, M.: Polynomial Invariants for Linear Loops. Cybernetics and Systems Analysis 4, 159--168 (2010)
22. Hodge, V., Pido, D.: Methods of Algebraic Geometry, Moscow (1954)
23. Lvov, M., Kreknin, V.: Nonlinear Invariants for Linear Loops and Eigenpolynomials of Linear Operators. Cybernetics and Systems Analysis 2, 126--139 (2012)
24. Kreknin, V., Lvov, M.: Eigenpolynomials of Linear Operators and Polynomial Invariants of Linear Loops of Program. Scientific Journal NEA Dragomanov 1(11), 150—169 (2010)
25. Lvov, M.: On the Structure of Polynomial Invariants of Linear Loops. (In print)
26. Cousot P., Halbwachs N.: Automatic Discovery of Linear Restraints among Variables of a Program. In: Conference Record of the Fifth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, pp. 84--97, ACM Press, New York (1978)
27. Krivoy, S., Raksha, S.: Search of Invariant Linear Dependencies in Programs. Cybernetics 6, 23--28 (1984)
28. Godlewski, A., Kapitonova, Y, Krivoy, S., Letichevsky, A.: Iterative Methods of Programs Analysis. Equalities and Inequalities. Cybernetics 3, 1--10 (1990)
29. Lvov, M.: Invariant Inequalities in Programs Interpreted over an Ordered Field. Cybernetics 5, 22--27 (1986)
30. Lvov, M.: About Invariant Inequalities for States of the Program Schemes, that Interpreted Over the Vector Space. Cybernetics 2, 111--112 (1985)
31. Lvov, M.: A Method of Proving the Invariance of Linear Inequalities for Linear Loops. Cybernetics and Systems Analysis 4, 80--85 (2014)