Generating Loop Invariants via Polynomial Interpolation

Marc Moreno Maza
Joint work with
Rong Xiao

University of Western Ontario, Canada

East China Normal University
May 24, 2012

Plan

1. Preliminaries
   - Notions on loop invariants
   - Poly-geometric summations
   - A variation on Bezout's Theorem
2. Invariant ideal of P-solvable recurrences
   - Degree estimates for solutions of P-solvable recurrences
   - P-solvable recurrences
   - Degree estimates for solutions of P-solvable recurrences
   - Degree estimates for their invariant ideal
   - Dimension estimates for their invariant ideal
3. Loop invariant generation via polynomial interpolation
   - A direct approach
   - A modular method
   - Experimentation
   - Maple Package: `ProgramAnalysis`

Plan

Loop model under study

```
while C_0 do
    if C_1
    then
        X := A_1(X);
    elif C_2
    then
        X := A_2(X);
    ...
    elif C_m
    then
        X := A_m(X);
    end if
end while
```

1. Loop variables: $X = x_1, \ldots, x_s$, rational value scalar
2. Conditions: each C_i is a quantifier free formula in X over $\mathbb{Q}$.
3. Assignments: $A_i \in \mathbb{Q}[X]$ inducing a polynomial map $M_i : \mathbb{R}^s \mapsto \mathbb{R}^s$
4. Initial condition: X-values defined by a semi-algebraic system.

Basic notions

```
x := a;
y := b;
while x < 10 do
    x := x + y^5;
    y := y + 1;
end do;
```

- x, y, a, b are loop variables since they are updated in the loop or used to update other loop variables.
- The set of the initial values of the loop is

$$\{(x, y, a, b) \mid x = a, y = b, (a, b) \in \mathbb{R}^2\}.$$

- the loop trajectory of the above loop starting at $(x, y, a, b) = (1, 0, 1, 0)$ is the sequence:

$$(1, 0, 1, 0), (1, 1, 1, 0), (2, 2, 1, 0), (34, 3, 1, 0).$$

- The reachable set $R(L)$ of a loop L consists of all tuples of all trajectories of L.
- If $x_1, \ldots, x_s$ are the loop variables of L, then a polynomial $P \in \mathbb{Q}[x_1, \ldots, x_s]$ is a (plain) loop invariant of L whenever $R(L) \subseteq V(P)$ holds.

More notions

- The inductive reachable set $R_{\text{ind}}(L)$ of a loop L is the reachable set of the loop obtained from L by replacing the guard condition with true.
- The absolute reachable set $R_{\text{abs}}(L)$ of a loop L is the reachable set of the loop obtained from L by replacing the guard condition with true, ignoring the branch conditions and, at each iteration executing a branch action selected randomly.
- We clearly have
$$R(L) \subseteq R_{\text{ind}} \subseteq R_{\text{abs}}$$
- If $x_1, \ldots, x_s$ are the loop variables of L, then a polynomial $P \in \mathbb{Q}[x_1, \ldots, x_s]$ is an inductive (resp. absolute) loop invariant of L whenever $R_{\text{ind}}(L) \subseteq V(P)$ (resp. $R_{\text{abs}}(L) \subseteq V(P)$) holds.
- We denote by $\mathcal{I}(L)$ (resp. $\mathcal{I}_{\text{ind}}(L), \mathcal{I}_{\text{abs}}(L)$) the set of the polynomials that are plain (resp. inductive, absolute) loop invariants of L.
- These are radical ideals such that
$$\mathcal{I}_{\text{abs}}(L) \subseteq \mathcal{I}_{\text{ind}}(L) \subseteq \mathcal{I}(L)$$

Absolute invariants might be trivial

$y_1 := 0$;
$y_2 := 0$;
$y_3 := x_1$;
while $y_3 \neq 0$ **do**
    if $y_2 + 1 = x_2$
    then
        $y_1 := y_1 + 1$;
        $y_2 := 0$;
        $y_3 := y_3 - 1$;
    else
        $y_2 := y_2 + 1$;
        $y_3 := y_3 - 1$;
    end if
end do

- Consider $y_1 x_2 + y_2 + y_3 = x_1 \ (E)$.
- If $x_1 = 0$ then the equation (E) holds initially and the loop is not entered.
- If $x_1 \neq 0$ and $x_2 = 1$ then (E) and $y_2 + 1 = x_2$ hold before each iteration.
- If $x_1 \neq 0$ and $x_2 \neq 1$ then the second action preserves (E).
- Therefore $y_1 x_2 + y_2 + y_3 - x_1 \in \mathcal{I}(L)$ and $y_1 x_2 + y_2 + y_3 - x_1 \in \mathcal{I}_{\text{ind}}(L)$ both hold.

Absolute invariants might be trivial

$y_1 := 0$;
$y_2 := 0$;
$y_3 := x_1$;
while $y_3 \neq 0$ **do**
  if $y_2 + 1 = x_2$
  then
    $y_1 := y_1 + 1$;
    $y_2 := 0$;
    $y_3 := y_3 - 1$;
  else
    $y_2 := y_2 + 1$;
    $y_3 := y_3 - 1$;
  end if
end do

- Consider $y_1x_2 + y_2 + y_3 = x_1$ (E).
- If $x_1 = 0$ then the equation (E) holds initially and the loop is not entered.
- If $x_1 \neq 0$ and $x_2 = 1$ then (E) and $y_2 + 1 = x_2$ hold before each iteration.
- If $x_1 \neq 0$ and $x_2 \neq 1$ then the second action preserves (E).
- Therefore $y_1x_2 + y_2 + y_3 - x_1 \in \mathcal{I}(L)$ and $y_1x_2 + y_2 + y_3 - x_1 \in \mathcal{I}_{\text{ind}}(L)$ both hold.
- If conditions are ignored, $(x_1, x_2) = (0, 1)$ and execute the first branch once, then we obtain
$$y_1x_2 = 1 \text{ and } y_2 + y_3 = x_1.$$
- Then (E) is violated and we have
$$\mathcal{I}_{\text{abs}}(L) = \langle 0 \rangle.$$

Inductive invariants might not be plain invariants

$x := 1$;
while $x \neq 1$ **do**
    $x := x + 1$;
end do

- $x - 1 = 0$ is an invariant but not an inductive of the following loop.
- Thus $\mathcal{I}_{\mathrm{ind}}(L)$ is strictly smaller than $\mathcal{I}(L)$

Computing inductive invariants via elimination ideals

```
y := 1;
x := 0;
while true do
    z := x;
    x := y;
    y := z + y;
end while
```

- Solving for (x, y) as a 2-variable recurrence
$$x(n+1) = y(n), y(n+1) = x(n) + y(n), \text{ with } x(0) = 0, y(0) = 1.$$
- We obtain
$$\begin{aligned} x(n) &= \frac{(\frac{\sqrt{5}+1}{2})^n}{\sqrt{5}} - \frac{(\frac{-\sqrt{5}+1}{2})^n}{\sqrt{5}}, \\ y(n) &= \frac{\sqrt{5}+1}{2}\,\frac{(\frac{\sqrt{5}+1}{2})^n}{\sqrt{5}} - \frac{-\sqrt{5}+1}{2}\,\frac{(\frac{-\sqrt{5}+1}{2})^n}{\sqrt{5}}. \end{aligned}$$
- Let $u = (\frac{\sqrt{5}+1}{2})^n$, $v = (\frac{-\sqrt{5}+1}{2})^n$, $a = \sqrt{5}$
- Taking the dependencies $u^2\,v^2 = 1, a^2 = 5$ into account, we want
$$\langle x - \frac{au}{5} + \frac{av}{5}, y - a\frac{a+1}{2}\frac{u}{5} + a\frac{-a+1}{2}\frac{v}{5}, a^2 - 5, u^2v^2 - 1\rangle \ \cap \ \mathbb{Q}[x, y],$$
- which is
$$\langle 1 - y^4 + 2xy^3 + x^2y^2 - 2x^3y - x^4\rangle.$$

A natural criterion

while C_0 **do**
  if C_1
  then
    $X := A_1(X)$;
  elif C_2
  then
    $X := A_2(X)$;
  $\ldots$
  elif C_m
  then
    $X := A_m(X)$;
  end if
end while

- Let $f \in \mathbb{Q}[X]$ vanishing at each initial condition.
- Assume that for all $i = 1 \cdots m$we have

$$Z_{\mathbb{R}}(A_i(Z_{\mathbb{R}}(f) \ \cap \ Z_{\mathbb{R}}(C_i))) \ \subseteq \ Z_{\mathbb{R}}(f)$$

- Then we have

$$f \in \mathcal{I}_{\text{ind}}(L).$$

- This can be tested with the commands of

  `RegularChains:-SemiAlgebraicSetTools`
  based on the
  `RegularChains:-RealTriangularize`
  (C. Chen, J.H. Davenport, M.M.M., B. Xia & R. Xiao, ISSAC 2010 & 2011).

Summary and notes

- Computing $\mathcal{I}_{\mathrm{ind}}(L)$ is a better approximation of $\mathcal{I}(L)$ than $\mathcal{I}_{\mathrm{abs}}(L)$.
- The loop invariant generation methods of (E. Rodriguez-Carbonell & D. Kapur, ISSAC04) and (L. Kovács, TACAS08) focus on $\mathcal{I}_{\mathrm{abs}}(L)$.

Summary and notes

- Computing $\mathcal{I}_{\rm ind}(L)$ is a better approximation of $\mathcal{I}(L)$ than $\mathcal{I}_{\rm abs}(L)$.
- The loop invariant generation methods of (E. Rodriguez-Carbonell & D. Kapur, ISSAC04) and (L. Kovács, TACAS08) focus on $\mathcal{I}_{\rm abs}(L)$.
- In this talk, we target $\mathcal{I}_{\rm ind}(L)$ (easier to compute than $\mathcal{I}(L)$) and call it the Invariant Ideal of the loop L. Same goal as in the preprint (Bin Wu, Liyong Shen, Min Wu, Zhengfeng Yang & Zhenbing Zeng, 2011).

Summary and notes

- Computing $\mathcal{I}_{\text{ind}}(L)$ is a better approximation of $\mathcal{I}(L)$ than $\mathcal{I}_{\text{abs}}(L)$.
- The loop invariant generation methods of (E. Rodriguez-Carbonell & D. Kapur, ISSAC04) and (L. Kovács, TACAS08) focus on $\mathcal{I}_{\text{abs}}(L)$.
- In this talk, we target $\mathcal{I}_{\text{ind}}(L)$ (easier to compute than $\mathcal{I}(L)$) and call it the Invariant Ideal of the loop L. Same goal as in the preprint (Bin Wu, Liyong Shen, Min Wu, Zhengfeng Yang & Zhenbing Zeng, 2011).
- We also want to avoid computing closed forms of loop variables, while
  - not making any assumptions on the shape of the polynomial invariants,
  - and avoiding an intensive use of expensive algebraic computations other than linear algebra, for which costs are predictable.

Summary and notes

- Computing $\mathcal{I}_{\text{ind}}(L)$ is a better approximation of $\mathcal{I}(L)$ than $\mathcal{I}_{\text{abs}}(L)$.
- The loop invariant generation methods of (E. Rodriguez-Carbonell & D. Kapur, ISSAC04) and (L. Kovács, TACAS08) focus on $\mathcal{I}_{\text{abs}}(L)$.
- In this talk, we target $\mathcal{I}_{\text{ind}}(L)$ (easier to compute than $\mathcal{I}(L)$) and call it the Invariant Ideal of the loop L. Same goal as in the preprint (Bin Wu, Liyong Shen, Min Wu, Zhengfeng Yang & Zhenbing Zeng, 2011).
- We also want to avoid computing closed forms of loop variables, while
  - not making any assumptions on the shape of the polynomial invariants,
  - and avoiding an intensive use of expensive algebraic computations other than linear algebra, for which costs are predictable.
- In (Sankaranarayanan, Sipma & Manna, SIGPLAN 2004) (Y. Chen, B. Xia, L. Yang, & N. Zhan, FMHRTS 2007) (D. Kapur Deduction and Applications 2005) template polynomials are used. Morever, the latter two use real QE.

Summary and notes

- Computing $\mathcal{I}_{\text{ind}}(L)$ is a better approximation of $\mathcal{I}(L)$ than $\mathcal{I}_{\text{abs}}(L)$.
- The loop invariant generation methods of (E. Rodriguez-Carbonell & D. Kapur, ISSAC04) and (L. Kovács, TACAS08) focus on $\mathcal{I}_{\text{abs}}(L)$.
- In this talk, we target $\mathcal{I}_{\text{ind}}(L)$ (easier to compute than $\mathcal{I}(L)$) and call it the Invariant Ideal of the loop L. Same goal as in the preprint (Bin Wu, Liyong Shen, Min Wu, Zhengfeng Yang & Zhenbing Zeng, 2011).
- We also want to avoid computing closed forms of loop variables, while
  - not making any assumptions on the shape of the polynomial invariants,
  - and avoiding an intensive use of expensive algebraic computations other than linear algebra, for which costs are predictable.
- In (Sankaranarayanan, Sipma & Manna, SIGPLAN 2004) (Y. Chen, B. Xia, L. Yang, & N. Zhan, FMHRTS 2007) (D. Kapur Deduction and Applications 2005) template polynomials are used. Morever, the latter two use real QE.
- The "abstract interpretation" method (E. Rodriguez-Carbonell & D. Kapur, Science of Computer Programming 2007) does not use templates but uses of Gröbner bases heavily.

Plan

Poly-geometrical expression

Notations

Let $\alpha_1, \ldots, \alpha_k$ be k elements of $\overline{\mathbb{Q}}^* \setminus \{1\}$. Let n be a variable taking non-negative integer values. We regard $n, \alpha_1^n, \ldots, \alpha_k^n$ as independent variables and we call $\alpha_1^n, \ldots, \alpha_k^n$ n-exponential variables.

Definition

Any $f \in \overline{\mathbb{Q}}[n, \alpha_1^n, \ldots, \alpha_k^n]$ is called a poly-geometrical expression in n *over* $\overline{\mathbb{Q}}$ w.r.t. $\alpha_1, \ldots, \alpha_k$. For such an f, we denote by $f|_{n=i}$ the evaluation of f at i. For such f, g we write $f = g$ whenever $f|_{n=i} = g|_{n=i}$ holds for all i.

Canonical form of a poly-geometrical expression

Definition

We say that $f \in \overline{\mathbb{Q}}[n, \alpha_1^n, \dots, \alpha_k^n]$ is in canonical form if there exist

(1) $c_1, \dots, c_m \in \overline{\mathbb{Q}}^*$, and

(2) pairwise different couples $(\beta_1, e_1), \dots, (\beta_m, e_m)$ all in $(\overline{\mathbb{Q}}^* \setminus \{1\}) \times \mathbb{Z}_{\geq 0}$, and

(3) a polynomial $c_0(n) \in \overline{\mathbb{Q}}[n]$, such that

(4) each $\beta_1, \dots, \beta_m$ is a product of some of the $\alpha_1, \dots, \alpha_k$ and such that

(5) $f(n)$ and $\sum_{i=1}^{m} c_i\, \beta_i^n\, n^{e_i} \ + \ c_0(n)$ are equal.

When this holds, the polynomial $c_0(n)$ is the exponential-free part of $f(n)$.

Proposition

Let f a poly-geometrical expression in n over $\overline{\mathbb{Q}}$ w.r.t. $\alpha_1, \dots, \alpha_k$. There exists a unique poly-geometrical expression c in n over $\overline{\mathbb{Q}}$ w.r.t. $\alpha_1, \dots, \alpha_k$ such that c is in canonical form and such that f and c are equal. We call c the canonical form of f.

Examples of poly-geometrical expressions

Example

The closed form $f := \frac{(n+1)^2\, n^2}{4}$ of $\sum_{i=0}^{n} i^3$ is a poly-geometrical expression in n over $\overline{\mathbb{Q}}$ without n-exponential variables.

Example

The expression $g := n^2\, 2^{(n+1)} - n\, 2^n\, 3^{\frac{n}{2}}$ is a poly-geometrical in n over $\overline{\mathbb{Q}}$ w.r.t. $2, \sqrt{3}$.

Example

The sum $\sum_{i=1}^{n-1} i^k$ has $n-1$ terms while its closed form below

$$\sum_{i=1}^{k} \left\{ {k \atop i} \right\} \frac{n^{i+1}}{i+1},$$

where $\left\{ {k \atop i} \right\}$ the number of ways to partition k into i non-zero summands, has a fixed number of terms and thus is poly-geometrical in n over $\overline{\mathbb{Q}}$.

Multiplicative relation ideal

Definition

Let $A := (\alpha_1, \ldots, \alpha_k)$ be a sequence of k non-zero elements of $\overline{\mathbb{Q}}$. Let $\mathbf{e} := (e_1, \ldots, e_k)$ be a sequence of k integers. We say that $\mathbf{e}$ is a multiplicative relation on A if $\prod_{i=1}^{k} \alpha_i^{e_i} = 1$ holds. Such a relation is said *non-trivial* if there exists $i \in \{1, \ldots, n\}$ s. t. $e_i \neq 0$ holds. If there exists a non-trivial multiplicative relation on A, we say that A is *multiplicatively dependent*; otherwise, we say that A is multiplicatively independent. All multiplicative relations of A form the multiplicative relation lattice on A,

Definition

Let $A := (\alpha_1, \ldots, \alpha_k)$ be a sequence of k elements of $\overline{\mathbb{Q}}$. Assume w.l.o.g. that for some ℓ, with $1 \leq \ell \leq k$, we have $\alpha_1 \neq 0, \ldots, \alpha_\ell \neq 0, \ \alpha_{\ell+1} = \cdots \alpha_k = 0$. We associate each α_i with a "new" variable y_i. The binomial ideal $\mathrm{MRI}(A; y_1, \ldots, y_k)$ of $\mathbb{Q}[y_1, y_2, \ldots, y_k]$ generated by

$$\{ \prod_{j \in \{1,\ldots,\ell\},\, v_j > 0} y_j^{v_j} - \prod_{i \in \{1,\ldots,\ell\},\, v_i < 0} y_i^{-v_i} \ \mid \ (v_1, \ldots, v_\ell) \in Z\},$$

and $\{y_{\ell+1}, \ldots, y_k\}$, where Z is the multiplicative relation lattice.

Multiplicative relation ideal: example

Definition

Let $A := (\alpha_1, \ldots, \alpha_k)$ be a sequence of k elements of $\overline{\mathbb{Q}}$. Assume w.l.o.g. that for some ℓ, with $1 \le \ell \le k$, we have $\alpha_1 \neq 0$, ..., $\alpha_\ell \neq 0$, $\alpha_{\ell+1} = \cdots\ \alpha_k = 0$. We associate each α_i with a “new” variable y_i. The binomial ideal $\mathrm{MRI}(A; y_1, \ldots, y_k)$ of $\mathbb{Q}[y_1, y_2, \ldots, y_k]$ generated by

$$\{ \prod_{j \in \{1,\ldots,\ell\},\, v_j > 0} y_j^{v_j} - \prod_{i \in \{1,\ldots,\ell\},\, v_i < 0} y_i^{-v_i} \ \mid\ (v_1, \ldots, v_\ell) \in Z \},$$

and $\{y_{\ell+1}, \ldots, y_k\}$, where Z is the multiplicative relation lattice.

Example

Consider $A = (1/2, 1/3, -1/6, 0)$. The multiplicative relation lattice of $(1/2, 1/3, -1/6)$ is generated by $(2, 2, -2)$. Thus the MRI of A associated with y_1, y_2, y_3, y_4 is

$$\langle y_1^2 y_2^2 - y_3^2, y_4 \rangle.$$

Weak multiplicative independence

Definition

Let $A := (\alpha_1, \dots, \alpha_k)$ be a sequence of k non-zero algebraic numbers over $\overline{\mathbb{Q}}$ and let $\beta \in \overline{\mathbb{Q}}$. We say β is weakly multiplicatively independent w.r.t. A, if there exist no non-negative integers $e_1, e_2, \dots, e_k$ such that $\beta = \prod_{i=1}^{k} \alpha_1^{e_i}$ holds.

Furthermore, we say that A is weakly multiplicatively independent if

(i) $\alpha_1 \neq 1$ holds, and

(ii) α_i is weakly multiplicatively independent w.r.t. $\{\alpha_1, \dots, \alpha_{i-1}, 1\}$, for all $i = 2, \dots, s$.

Degree estimates for x satisfying $x(n+1) = \lambda x(n) + h(n)$

Lemma

Let $\alpha_1, \ldots, \alpha_k \in \overline{\mathbb{Q}} \setminus \{0, 1\}$. Let $\lambda \in \overline{\mathbb{Q}} \setminus \{9\}$. Let $h(n) \in \overline{\mathbb{Q}}[n, \alpha_1^n, \ldots, \alpha_k^n]$. Consider the following single-variable recurrence relation R:

$$x(n+1) = \lambda x(n) + h(n).$$

Then, there exists $s(n) \in \overline{\mathbb{Q}}[n, \alpha_1^n, \ldots, \alpha_k^n]$ such that we have

$$\deg(s(n), \alpha_i^n) \leq \deg(h(n), \alpha_i^n) \quad \text{and} \quad \deg(s(n), n) \leq \deg(h(n), n) + 1,$$

and such that

- if $\lambda = 1$ holds, then $s(n)$ solves R,
- if $\lambda \neq 1$ holds, then there exists a constant c depending on $x(0)$ (that is, the initial value of x) such that $c\,\lambda^n + s(n)$ solves R.

Moreover, in both cases, if the exponential-free part of the canonical form of $(\frac{1}{\lambda})^n\, h(n)$ is 0, then $\deg(s(n), n) \leq \deg(h(n), n).$ can be required.
This latter hypothesis holds as soon as λ is weakly multiplicatively independent w.r.t. $\alpha_1, \ldots, \alpha_k$

Plan

Degree of an algebraic variety

Notations

Let $\mathbb{K}$ be an algebraically closed field. Let $F \subset \mathbb{K}[x_1, x_2, \ldots, x_s]$. We denote by $V_{\mathbb{K}^s}(F)$ (or simply by $V(F)$ when no confusion is possible) the zero set in $\mathbb{K}^s$ of F.

Definition

Let $V \subset \mathbb{K}^s$ be an r-dimensional equidimensional algebraic variety. The number of points of intersection of V with an $(n-r)$-dimensional generic linear subspace $L \subset \mathbb{K}^s$ is called the degree of V, denoted by $\deg(V)$.

The degree of a non-equidimensional variety is defined to be the sum of the degrees of its equidimensional components.

The degree of an ideal $I \subseteq \mathbb{K}[x_1, x_2, \ldots, x_s]$ is defined to be the degree of the variety of I in $\mathbb{K}^s$.

A few well-known properties

Lemma

Let $V \subset \mathbb{K}^s$ be an r-dimensional equidimensional algebraic variety of degree δ. Let L be an $(n-r)$-dimensional linear subspace. Then, $L \cap V$ is either of positive dimensional or consists of no more than δ points.

Lemma

Let $V \subset \mathbb{K}^s$ be a algebraic variety. Let L be a linear map from $\mathbb{K}^s$ to $\mathbb{K}^k$. Then we have $\deg(L(V)) \leq \deg(V)$.

Lemma (J. Heintz. Theor. Comput. Sci., 1983)

Let $I \subset \mathbb{Q}[x_1, x_2, \ldots, x_s]$ be a radical ideal of degree δ. Then there exist finitely many polynomials in $\mathbb{Q}[x_1, x_2, \ldots, x_s]$ generating I and such that each of this polynomial has total degree less than or equal to δ.

Lemma

Let $V, W, V_1, \ldots, V_e \subset \mathbb{K}^s$ be algebraic varieties s. t. $V := W \cap \cap_{i=1}^{e} V_i$ holds with $\dim(W) = r$. Then we have

$$\deg(V) \leq \deg(W) \max(\{\deg(V_i) \mid i = 1 \cdots e\})^r.$$

A variation on Bezouts Theorem

Proposition

- Let $X = x_1, x_2, \ldots, x_s$ and $Y = y_1, y_2, \ldots, y_t$ be pairwise different $s + t$ variables.
- Let M be an ideal in $\mathbb{Q}[Y]$ of degree d_M and dimension r.
- Let $f_1, f_2, \cdots, f_s$ be s polynomials in $\mathbb{Q}[Y]$, with maximum total degree d_f.
- Denote by I the ideal $\langle x_1 - f_1, x_2 - f_2, \ldots, x_s - f_s \rangle$.

Then, we have

$$\deg(I + M) \; \leq \; d_M \, {d_f}^r.$$

Remark

Since $I + M$ is an ideal of $\mathbb{Q}[X, Y]$, a direct application of one of the previous lemmas gives

$$\deg(I + M) \; \leq \; d_M \, {d_f}^{s+r}.$$

This bound is tight

Example

Consider the polynomials of $\mathbb{Q}[x, y, n, m]$

$$g_1 := x - n^2 - n - m \ \text{ and } \ g_2 := y - n^3 - 3n + 1$$

and the ideals

$$M := \langle n^2 - m^3 \rangle \ \text{ and } \ J := M + \langle g_1, g_2 \rangle$$

With the notations of the proposition we have

$$d_M := 3, \ r := 1 \ \text{ and } \ d_f := 3$$

Thus the estimated degree is 3×3. Meanwhile, the true degree of J is indeed 9, which is computed as the (linear space) dimension of

$$\mathbb{Q}(a, b, c, d, e)[x, y, m, n]/(J + \langle a\,x + b\,y + c\,n + d\,m + e \rangle),$$

where a, b, c, d, e are indeterminates.

Plan

Plan

The univariate case: recall

Definition

Given a recurrence $R:\ x(n+1) = \lambda\, x(n) + h(n)$ in $\mathbb{Q}$, if $h(n)$ is a poly-geometrical expression in n over $\mathbb{Q}$, then R is called a univariate P-solvable recurrence.

The multivariate case: setting

Let $n_1, \ldots, n_k$ be positive integers and define $s := n_1 + \cdots + n_k$. Let M be a block-diagonal square matrix over $\mathbb{Q}$ of order s, with shape:

$$M := \begin{pmatrix} \mathbf{M}_{n_1 \times n_1} & \mathbf{0}_{n_1 \times n_2} & \ddots & \mathbf{0}_{n_1 \times n_k} \\ \mathbf{0}_{n_2 \times n_1} & \mathbf{M}_{n_2 \times n_2} & \ddots & \mathbf{0}_{n_2 \times n_k} \\ \ddots & \ddots & \ddots & \ddots \\ \mathbf{0}_{n_k \times n_1} & \mathbf{0}_{n_k \times n_2} & \ddots & \mathbf{M}_{n_k \times n_k} \end{pmatrix}.$$

Consider an s-variable recurrence relation R in $x_1, x_2, \ldots, x_s$, with shape:

$$\begin{pmatrix} x_1(n+1) \\ x_2(n+1) \\ \vdots \\ x_s(n+1) \end{pmatrix} = M \times \begin{pmatrix} x_1(n) \\ x_2(n) \\ \vdots \\ x_s(n) \end{pmatrix} + \begin{pmatrix} \mathbf{f}_{1_{n_1 \times 1}} \\ \mathbf{f}_{2_{n_2 \times 1}} \\ \vdots \\ \mathbf{f}_{k_{n_k \times 1}} \end{pmatrix},$$

where $\mathbf{f}_1$ is a vector of length n_1 with coordinates in $\mathbb{Q}$ and where $\mathbf{f}_i$ is a tuple of length n_i with coordinates in the polynomial ring $\mathbb{Q}[x_1, \ldots, x_{n_1 + \cdots + n_{i-1}}]$, for $i = 2, \ldots, k$.

The multivariate case: definition

Setting (recall)

$$\begin{pmatrix} x_1(n+1) \\ x_2(n+1) \\ \vdots \\ x_s(n+1) \end{pmatrix} = M \times \begin{pmatrix} x_1(n) \\ x_2(n) \\ \vdots \\ x_s(n) \end{pmatrix} + \begin{pmatrix} \mathbf{f}_{1_{n_1 \times 1}} \\ \mathbf{f}_{2_{n_2 \times 1}} \\ \vdots \\ \mathbf{f}_{k_{n_k \times 1}} \end{pmatrix},$$

where $\mathbf{f}_1$ is a vector over $\mathbb{Q}$ of length n_1 and where $\mathbf{f}_i$ is a tuple of length n_i with coordinates in $\mathbb{Q}[x_1, \ldots, x_{n_1+\cdots+n_{i-1}}]$, for $i = 2, \ldots, k$.

Definition

Then, the recurrence relation R is called P-solvable over $\mathbb{Q}$ and the matrix M is called the coefficient matrix of R.

The notion of P-solvable recurrence is equivalent to that of *solvable mapping* in (E. Rodriguez-Carbonell & D. Kapur, ISSAC04) or that of *solvable loop* in (L. Kovocs TACAS08) the respective contexts.

Plan

Degree estimates for solutions of P-solvable recurrences: theorem

Assume M is in a Jordan normal form. Assume the eigenvalues $\lambda_1, \ldots, \lambda_s$ of M (counted with multiplicities) are different from $0, 1$, with λ_i being the i-th diagonal element of M. Assume for each block j the total degree of any polynomial in $\mathbf{f}_j$ (for $i = 2 \cdots k$) is upper bounded by d_j. For each i, we denote by $b(i)$ the block number of the index i, that is,

$$\sum_{j=1}^{b(i)-1} n_j < i \leq \sum_{j=1}^{b(i)} n_j.$$

Let $D_1 := n_1$ and for $all j \in \{2, \ldots, k\}$ let $D_j := d_j \, D_{j-1} + n_j$. Then, there exists a solution $(y_1, y_2, \ldots, y_s)$ for R of the following form:

$$y_i := c_i \lambda_i^n + g_i, \quad i = 1 \cdots s \quad \text{where}$$

(a) c_i is a constant depending only on the initial value of the recurrence;
(b) g_i is a poly-geometrical expression in n w.r.t. $\lambda_1, \ldots, \lambda_{i-1}$, such that

$$\deg(g_i) \leq D_{b(i)}.$$

Moreover, if $\{\lambda_1, \ldots, \lambda_s\}$ is weakly multiplicatively independent, then, for all $i = 1, \ldots, k$, we can further choose y_i such that we have

$$\deg(g_i, n) = 0 \quad \text{and} \quad \deg(g_i) \leq \prod_{2 \leq t \leq b(i)} \max(d_t, 1).$$

Degree estimates for solutions of P-solvable recurrences: example

Consider the recurrence:

$$\begin{pmatrix} x(n+1) \\ y(n+1) \\ z(n+1) \end{pmatrix} := \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix} \times \begin{pmatrix} x(n) \\ y(n) \\ z(n) \end{pmatrix} + \begin{pmatrix} 0 \\ x(n)^2 \\ x(n)^3 \end{pmatrix}$$

Viewing the recurrence as two blocks (x) and (y, z), the degree upper bounds are

$$D_1 := n_1 = 1 \text{ and } D_2 := d_2 D_1 + n_2 = 3 \times 1 + 2.$$

If we decouple the (y, z) block to the following two recurrences

$$y(n+1) = 3\,y(n) + x(n)^2 \text{ and } z(n+1) = 3\,z(n) + x(n)^3,$$

then we deduce that the degree of the poly-geometrical expression for y and z are upper bounded by 2 and 3 respectively.

Degree estimates: reduction to the Jordan normal form case

Let Q be a non-singular matrix such that $J := Q\,M\,Q^{-1}$ is a Jordan form of M. Let the original recurrence R be

$$X(n+1) = M\,X(n) + F.$$

Consider the following recurrence R_Q

$$Y(n+1) = J\,Y(n) + QF.$$

It is easy to check that if

$$(y_1(n), y_2(n), \ldots, y_s(n))$$

solves R_Q, then

$$Q^{-1}\ (y_1(n), y_2(n), \ldots, y_s(n))$$

solves R. Note that an invertible matrix over $\overline{\mathbb{Q}}$ maps a tuple of poly-geometrical expressions to another tuple of poly-geometrical expressions; moreover it preserves the highest degree among the expressions in the tuple.

Plan

Degree estimates for the invariant ideal: theorem

- Let R be a P-solvable recurrence relation with variables $(x_1, x_2, \ldots, x_s)$.
- Let $\mathcal{I} \subset \mathbb{Q}[x_1, x_2, \ldots, x_s]$ be the invariant ideal of R.
- Let $A = \alpha_1, \alpha_2, \ldots, \alpha_s$ be the eigenvalues (counted with multiplicities) of the coefficient matrix of R.
- Let $\mathcal{M}$ be the multiplicative relation ideal of A associated with variables $y_1, \ldots, y_k$. Let r be the dimension of $\mathcal{M}$.
- Let $f_1(n, \alpha_1^n, \ldots, \alpha_k^n), \ldots, f_s(n, \alpha_1^n, \ldots, \alpha_k^n)$ be s poly-geometrical expressions in n w.r.t. $\alpha_1, \alpha_2, \ldots, \alpha_s$ solving R.
- Suppose R has a k-block configuration as $(n_1, 1), \ldots, (n_k, d_k)$.
- Let $D_1 := n_1$; and for all $j \in \{2, \ldots, k\}$, let $D_j := d_j\, D_{j-1} + n_j$.

Then, we have

$$\deg(\mathcal{I}) \leq \deg(\mathcal{M})\, D_k^{r+1}.$$

Moreover, if the degrees of n in f_i, for $i = 1 \cdots s$, are all 0, then we have

$$\deg(\mathcal{I}) \leq \deg(\mathcal{M})\, D_k^{r}.$$

Degree estimates for the invariant ideal: example

Consider again solving for (x, y) as a 2-variable recurrence

$$x(n+1) = y(n), y(n+1) = x(n) + y(n), \text{ with } x(0) = 0, y(0) = 1.$$

Recall that we obtained

$$\begin{array}{rcl} x(n) & = & \frac{(\frac{\sqrt{5}+1}{2})^n}{\sqrt{5}} - \frac{(\frac{-\sqrt{5}+1}{2})^n}{\sqrt{5}}, \\ y(n) & = & \frac{\sqrt{5}+1}{2} \frac{(\frac{\sqrt{5}+1}{2})^n}{\sqrt{5}} - \frac{-\sqrt{5}+1}{2} \frac{(\frac{-\sqrt{5}+1}{2})^n}{\sqrt{5}}. \end{array}$$

Observe that $A := \frac{-\sqrt{5}+1}{2}, \frac{\sqrt{5}+1}{2}$ is weakly multiplicatively independent. The multiplicative relation ideal of A associated with variables u, v is generated by $u^2v^2 - 1$ and thus has degree 4 and dimension 1 in $\mathbb{Q}[u, v]$. Therefore, the previous theorem implies that the degree of invariant ideal bounded by 4×1^1. This is sharp since this ideal is

$$\langle 1 - y^4 + 2xy^3 + x^2y^2 - 2x^3y - x^4 \rangle.$$

Plan

Dimension estimates for the invariant ideal: theorem

Theorem

Using the same notations as in the definition of P-solvable recurrences.

- Let $\lambda_1, \lambda_2, \ldots, \lambda_s$ be the eigenvalues of M counted with multiplicities.
- Let $\mathcal{M}$ be the multiplicative relation ideal of $\lambda_1, \lambda_2, \ldots, \lambda_s$.
- Let r be the dimension of $\mathcal{M}$. Let $\mathcal{I}$ be the invariant ideal of R.

Then, we have

$$\dim(\mathcal{I}) \leq r + 1.$$

Moreover, for generic initial values,

1. we have $r \leq \dim(\mathcal{I})$,
2. if 0 is not an eigenvalue of M and $\lambda_1, \lambda_2, \ldots, \lambda_s$ is weakly multiplicatively independent, then we have $r = \dim(\mathcal{I})$.

Corollaries

1. If $r + 1 < s$ holds, then $\mathcal{I}$ is not the zero ideal in $\mathbb{Q}[x_1, x_2, \ldots, x_s]$.
2. Assume that $x_1(0) := a_1, \ldots, x_s(0) := a_s$ are independent indeterminates. If the eigenvalues of R are multiplicatively independent, then the inductive invariant ideal of the loop is the zero ideal in $\mathbb{Q}[a_1, \ldots, a_s, x_1, x_2, \ldots, x_s]$.

Dimension estimates for the invariant ideal: example 1

Consider the recurrence:

$$(x(n+1), y(n+1)) := (3\,x(n) + y(n), 2\,y(n))$$

with $x(0) = a, y(0) = b$.

On one hand, the two eigenvalues are 2 and 3 which are multiplicatively independent.

Therefore, using the previous corollary, the invariant ideal of the corresponding loop is trivial.

On the other hand, for loop variables (a, b, x, y), the reachable set of the loop is

$\mathfrak{R} := \{(a,\, b,\, (a{+}b)\, 3^i {-} b\, 2^i,\, b\, 2^i) \mid (a, b) \in \mathbb{Q}^2,\ i$ is a non-negative integer$\}$.

Therefore, any polynomial vanishes on all points of $\mathfrak{R}$ must be 0.

Dimension estimates for the invariant ideal: example 2

Consider the linear recurrence

$$x(n+1) = 3\,x(n) - y(n), y(n+1) = 2\,y(n)$$

with $(x(0), y(0)) = (a, b)$.

The eigenvalues of the coefficient matrix are $2, 3$, which are multiplicatively independent.

One can check that, when $a = b$, the invariant ideal is generated by $x - y$.

However, generically, that is when $a \neq b$ holds, the invariant ideal is the zero ideal.

Plan

Loop model under study: recall

```
while C_0 do
    if C_1
    then
        X := A_1(X);
    elif C_2
    then
        X := A_2(X);
    ...
    elif C_m
    then
        X := A_m(X);
    end if
end while
```

1. Loop variables: $X = x_1, \ldots, x_s$, rational value scalar
2. Conditions: each C_i is a quantifier free formula in X over $\mathbb{Q}$.
3. Assignments: $A_i \in \mathbb{Q}[X]$ inducing a polynomial map $M_i : \mathbb{R}^s \mapsto \mathbb{R}^s$
4. Initial condition: X-values defined by a semi-algebraic system.

A direct approach

Input

(i) $M := m_1, m_2, \ldots, m_c$ is a sequence of monomials in the loop variables X,

(ii) $S := s_1, s_2, \ldots, s_r$ is a set of r points on the inductive trajectory of the loop,

(iii) E is a polynomial system defining the loop initial values,

(iv) B is the transitions $(C_1, A_1), \ldots, (C_m, A_m)$ of the loop.

Algorithm

1. $L := \texttt{BuildLinSys}(M, S)$
2. $N := \texttt{LinSolve}(\texttt{L})$ is full row rank and generates the null space of L.
3. $F := \emptyset$
4. For each row vector $\mathbf{v} \in N$ do
$$F := F \cup \{\texttt{GenPoly}(M, \mathbf{v})\}$$
5. If $Z(E) \not\subseteq Z(F)$ then return FAIL
6. For each branch $(C_i, A_i) \in B$ do
$$\text{if } A_i(Z(F) \cap Z(C_i)) \not\subseteq Z(F) \text{ then return FAIL}$$
7. Return F, a list of polynomial equation invariants for the target loop.

Plan

A small-prime approach: algorithm

Algorithm

1. $p :=$ `MaxMachinePrime`$()$; $L_p :=$ `BuildLinSysModp`(M, S, p);
2. $N_p :=$ `LinSolveModp`$(\mathtt{L_p}, \mathtt{p})$
3. $d := \dim(N_p)$; $\mathbf{N} := (N_p)$; $\mathbf{P} := (p)$;
4. While $p > 2$ do
    1. If $d = 0$ then return FAIL
    2. $N :=$ `RatRecon`$(\mathbf{N}, \mathbf{P})$
    3. If $N \neq$ FAIL then break;
    4. $p :=$ `PrevPrime`(p); $L_p :=$ `BuildLinSysModp`(M, S, p);
       $N_p :=$ `LinSolveModp`$(\mathtt{L_p}, \mathtt{p})$
    5. If $d > \dim(N_p)$ then $d := \dim(N_p)$; $\mathbf{N} := (N_p)$; $\mathbf{P} := (p)$
    6. else $\mathbf{N} :=$ `Append`$(\mathbf{N}, N_p)$; $\mathbf{P} :=$ `Append`$(\mathbf{P}, p)$
5. If $p = 2$ then return FAIL
6. $F := \emptyset$
7. For each row vector $\mathbf{v} \in N$ do
   $$F := F \cup \{\mathtt{GenPoly}(M, \mathbf{v})\}$$
8. If $Z(E) \not\subseteq Z(F)$ then return FAIL
9. For each branch $(C_i, A_i) \in B$ do
   $$\text{if } A_i(Z(F) \cap Z(C_i)) \not\subseteq Z(F) \text{ then return FAIL}$$
10. Return F, a list of polynomial equation invariants for the target loop.

A small-prime approach: complexity result

Proposition

Both algorithms run in singly exponential time w.r.t. number of loop variables.

Indeed

- the number of monomials of M is singly exponential w.r.t. number of loop variables.
- applying our criterion to certify the result can be reduced to an ideal membership problem, which is singly exponential w.r.t. number of loop variables.

A small-prime approach: example

Consider the following recurrence relation on (x, y, z):

$$\begin{pmatrix} x(n+1) \\ y(n+1) \\ z(n+1) \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -3 \\ 0 & 1 & 3 \end{pmatrix} \begin{pmatrix} x(n) \\ y(n) \\ z(n) \end{pmatrix}$$

with initial value $(x(0), y(0), z(0)) = (1, 2, 3)$.

- Note that the characteristic polynomial of the coefficient matrix has 1 as a triple root and the mult. rel. ideal of the eigenvalues is 0-dimensional.
- So the invariant ideal of this recurrence has dimension either 0 or 1.
- On the other hand, we can show that for all $k \in \mathbb{N}$, we have $M^k \neq M$; so there are infinitely many points in the set $\{(x(k), y(k), z(k)) \mid k \in \mathbb{N}\}$, whenever $(x(0), y(0), z(0)) \neq (0, 0, 0)$.
- With our method, we compute the following invariant polynomials

$$x + y + z - 6, y^2 + 4yz + 4z^2 - 6y - 24z + 20,$$

which generate a prime ideal of dimension 1, thus the invariant ideal

Plan

Implementation of the small-prime approach

- In MAPLE using `LinearAlgebra` and `RegularChains`.
- The interpolation part is done **naively**: the template set M consists of all monomials up to the target degree.
- A sparse interpolation scheme is work in progress.
- We handle semi-algebraic condiitons thenks to `RegularChains:-SemiAlgebraicSetTools`
- We have applied our code to all example programs used in (E. Rodriguez-Carbonell & D. Kapur, 2007):
  - We are able to find the loop invariants by trying total degree up to 4 for most loops within 60 seconds.
  - In each case, we return a system of generators of the invariant ideal, though we do not have a proof for that fact.

Benchmarks procedure

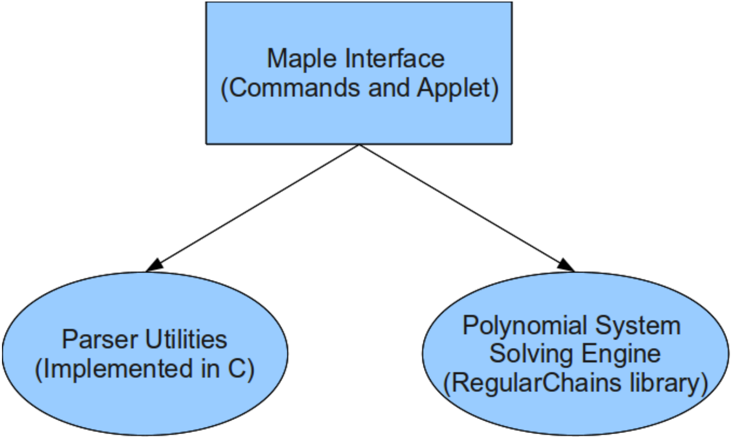
- "# vars" is the number of loop variables,
- "deg" is the total degree tried for the methods which use a degree bound,
- "PI" is the timing of the our method,
- "AI" (Abstract Interpretation) is the timing of the method described in (E. Rodriguez-Carbonell & D. Kapur, TCS 2007)
- "FP" (ideal fix point, direct use of Gröbner basis techniques) is the timing of the method described in (E. Rodriguez-Carbonell & D. Kapur, JSC 2007)
- "SE" (solving and elimination , direct use of Gröbner basis techniques) is the timing of the method described in (L. Kovocs TACAS08) and implementated in the software ALIGATOR.
- The time unit is the second;
- the "NA" symbol in a time field means that the related method does support the input program;
- the "FAIL" symbol in a time field means that the output is not "correct".
- All the tests were done using an Intel Core 2 Quad CPU 2.40GHz with 8.0GB memory.
- Computations of multiplicative relation lattice were done (not needed for "PI") on the same machine with GAP 4.4.12 + Alnuth 2.3.1 + KASH 2.5.

Timings

prog.[1]	# vars	deg	PI	AI	FP	SE
cohencu	4	3	0.6	0.93	0.28	0.13
cohencu	4	2	0.06	0.76	0.28	0.13
fermat	5	4	3.74	0.79	0.37	0.1
prodbin	5	3	1.4	0.74	0.36	0.13
rk07	6	3	3.1	2.23	NA	0.35
kov08	3	3	0.2	0.57	0.22	0.01
sum5	4	5	12	1.60	2.25	0.16[2]
wensley2	3	3	0.4	0.84	0.39	0.21
int-factor	6	3	60.9	1.28	160.7	0.9
fib(coupled)	4	4	2.4	0.71	NA	NA
fib(decoupled)	6	4	4.3	1.28	160.7	FAIL
non-inv2*	4	3	1.2	3.83	NA	FAIL
coupled-5-1*	4	4	1.1	9.58	NA	NA
coupled-5-2*	5	4	5.38	15.8	NA	NA
mannadiv	3	3	0.1	0.83	NA	0.04

Plan

ProgramAnalysis: package architecture



Maple session: the input program in a file

```
wensley2 := proc(P, Q, E)
local a, b, d, y;
    a := 0;
    b := 1/2*Q;
    d := 1;
    y := 0;
    #PRE : Q > P and P ≥ 0 and E > 0
    while E ≤ d do
     if P < a + b then
      b := 1/2*b;
      d := 1/2*d
     else
      a := a + b;
      y := y + 1/2*d;
      b := 1/2*b;
      d := 1/2*d
     end if
    end do;
    # POST : P/Q ≥ y and y > P/Q - E
    return y
end proc
```

Maple session: the sample points

$$\left[\left[0, \frac{5}{2}, 1, 0\right], \left[\frac{5}{2}, \frac{5}{4}, \frac{1}{2}, \frac{1}{2}\right], \left[\frac{5}{2}, \frac{5}{8}, \frac{1}{4}, \frac{1}{2}\right], \left[\frac{5}{2}, \frac{5}{16}, \frac{1}{8}, \frac{1}{2}\right], \left[\frac{45}{16}, \frac{5}{32}, \frac{1}{16}, \frac{9}{16}\right], \left[\frac{95}{32}, \frac{5}{64}, \frac{1}{32}, \frac{19}{32}\right], \left[\frac{95}{32}, \frac{5}{128}, \frac{1}{64}, \frac{19}{32}\right], \left[\frac{95}{32}, \frac{5}{256}, \frac{1}{128}, \frac{19}{32}\right], \left[\frac{765}{256}, \frac{5}{512}, \frac{1}{256}, \frac{153}{256}\right], \left[\frac{1535}{512}, \frac{5}{1024}, \frac{1}{512}, \frac{307}{512}\right], \left[\frac{1535}{512}, \frac{5}{2048}, \frac{1}{1024}, \frac{307}{512}\right], \left[\frac{1535}{512}, \frac{5}{4096}, \frac{1}{2048}, \frac{307}{512}\right], \left[\frac{12285}{4096}, \frac{5}{8192}, \frac{1}{4096}, \frac{2457}{4096}\right], \left[\frac{24575}{8192}, \frac{5}{16384}, \frac{1}{8192}, \frac{4915}{8192}\right], \left[\frac{24575}{8192}, \frac{5}{32768}, \frac{1}{16384}, \frac{4915}{8192}\right], \left[\frac{24575}{8192}, \frac{5}{65536}, \frac{1}{32768}, \frac{4915}{8192}\right], \left[\frac{196605}{65536}, \frac{5}{131072}, \frac{1}{65536}, \frac{39321}{65536}\right], \left[\frac{393215}{131072}, \frac{5}{262144}, \frac{1}{131072}, \frac{78643}{131072}\right], \left[\frac{393215}{131072}, \frac{5}{524288}, \frac{1}{262144}, \frac{78643}{131072}\right], \left[\frac{393215}{131072}, \frac{5}{1048576}, \frac{1}{524288}, \frac{78643}{131072}\right], \left[\frac{3145725}{1048576}, \frac{5}{2097152}, \frac{1}{1048576}, \frac{629145}{1048576}\right], \left[\frac{6291455}{2097152}, \frac{5}{4194304}, \frac{1}{2097152}, \frac{1258291}{2097152}\right]\right]$$

Maple session: verifying the program

```
> mplfile := cat(getenv("MXHOME"),"/mx-2012/programs/wensley2.mpl"):
  precond := [[Q>P, P>=0, E>0]];
  postcond := [[P >= Q*y ,  Q*y > P - Q*E  ]];
  guard := [[E<=d]];
  ineq_invs := [ P - Q*d < Q*y, Q*y <= P,y>=0];
```

$$precond := [[P < Q, 0 \leq P, 0 < E]]$$

$$postcond := [[Q\,y \leq P, P - Q\,E < Q\,y]]$$

$$guard := [[E \leq d]]$$

$$ineq\_invs := [-d\,Q + P < Q\,y, Q\,y \leq P, 0 \leq y] \quad \textbf{(2.3.1)}$$

```
> st := time():
  eq_invs := LoopEqInv(mplfile); # compute equation invariants
  time()-st;
```

$$eq\_invs := [y\,Q - a, d\,Q - 2\,b, -2\,b\,y + a\,d]$$

$$0.210 \quad \textbf{(2.3.2)}$$

```
> # verify the specification of the program
  st:=time():
  LoopVerify(precond, guard, [[op(eq_invs), op(ineq_invs)]], postcond);
  time()-st;
```

$$true$$

$$1.380 \quad \textbf{(2.3.3)}$$

Xie Xie!