Synthesis of Ranking Functions via Constraint Solving

Andreas Podelski

January 16, 2012

Program Verification and Constraints

- Reasoning about program computations
- Computation is a sequence of program states
- Sequences generated by transition relation
- Transition relation defined by assume & update statements
- Assume & update statements = transition constraints

Program Properties

- Non-reachability: given state is not reachable
- Termination: no infinite computation exists
- Linear-time properties (LTL):
  reduced to reachability and termination
  (in automata-theoretic approach)

Verification = finding auxiliary assertions

- Proving reachability = finding inductive invariant
- Proving termination = finding ranking relation

  (ranking relation defined by ranking function, i.e., an expression over program variables which bounds number of steps)

Preliminaries

- Running example
- Control-flow graphs and transition relations
- Linear inequalities: matrix form, Farkas' lemma
- Constraint solvers

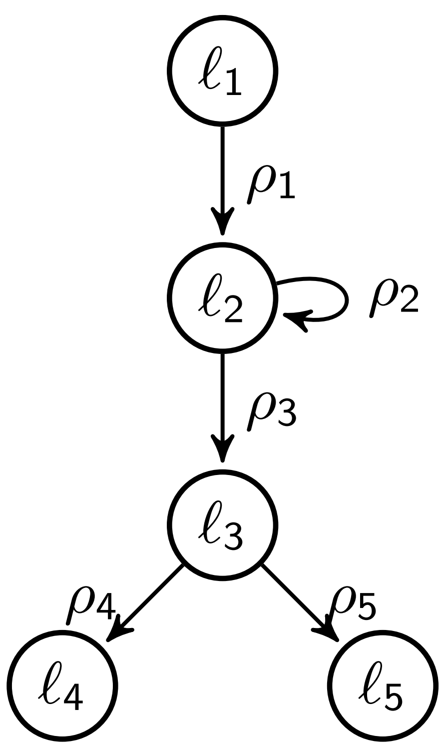
Running Example

```
main(int x, int y, int z) {
  assume(y >= z);
  while (x < y) {
    x++;
  }
  assert(x >= z);
}
```

- for constraint solving, treat x, y, and z as rationals

CFG and Transition Relations

```
main(int x, int y, int z) {
  assume(y >= z);
  while (x < y) {
    x++;
  }
  assert(x >= z);
}
```



$$\rho_1 = (y \geq z \wedge x' = x \wedge y' = y \wedge z' = z)$$

$$\rho_2 = (x + 1 \leq y \wedge x' = x + 1 \wedge y' = y \wedge z' = z)$$

$$\rho_3 = (x \geq y \wedge x' = x \wedge y' = y \wedge z' = z)$$

$$\rho_4 = (x \geq z \wedge x' = x \wedge y' = y \wedge z' = z)$$

$$\rho_5 = (x + 1 \leq z \wedge x' = x \wedge y' = y \wedge z' = z)$$

Transition Constraint => Matrix

$$\rho_2 = (x + 1 \leq y \wedge x' = x + 1 \wedge y' = y)$$

$$= (x - y \leq -1 \wedge -x + x' \leq 1 \wedge x - x' \leq -1 \wedge -y + y' \leq 0 \wedge y - y' \leq 0)$$

$$= \begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \\ x' \\ y' \end{pmatrix} \leq \begin{pmatrix} -1 \\ 1 \\ -1 \\ 0 \\ 0 \end{pmatrix}$$

Farkas' Lemma

- Mathematical tool for dealing with inequalities
- Informally: "implied inequalities are derivable"

$$\forall x\, \forall y : (x - 2y \leq 10 \wedge x + y \leq 1) \rightarrow x \leq 5$$

$$\frac{1}{3}(x - 2y \leq 10) \;+\; \frac{2}{3}(x + y \leq 1) \;=\; x \leq 4$$

$$\forall x : x \leq 4 \rightarrow x \leq 5$$

Farkas' Lemma

- "implied inequalities are derivable"

in matrix form:

$$\forall x\ \forall y : \begin{pmatrix} 1 & -2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \leq \begin{pmatrix} 10 \\ 1 \end{pmatrix} \rightarrow (1\ 0) \begin{pmatrix} x \\ y \end{pmatrix} \leq 5$$

$$\left(\tfrac{1}{3}\ \ \tfrac{2}{3}\right) \begin{pmatrix} 1 & -2 \\ 1 & 1 \end{pmatrix} = (1\ 0) \wedge \left(\tfrac{1}{3}\ \ \tfrac{2}{3}\right) \begin{pmatrix} 10 \\ 1 \end{pmatrix} = 4 \leq 5$$

Farkas' Lemma 2

- implied inequalities are derivable as weighted$_{\geq 0}$ sums

$$(\exists x : Ax \leq b) \wedge (\forall x : Ax \leq b \rightarrow cx \leq \delta)$$

iff

$$\exists \lambda : \lambda \geq 0 \wedge \lambda A = c \wedge \lambda b \leq \delta$$

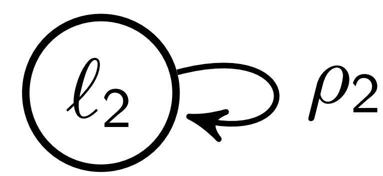
Constraint Solvers

- Black-box tools for solving constraints
  - Linear Programming
  - SAT (satisfiability)
  - SMT (satisfiability modulo theory)
  - CLP (constraint logic programming)

Ranking Functions

- Ranking function, say *f*, maps states to distance until terminating state

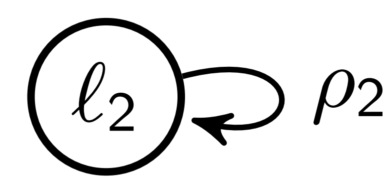
```
while (x < y) {
  x++;
}
```



- *f*(10, 10) = 0, *f*(5, 10) = 5, *f*(0, 10) = 10, ...
- $f(x, y) = (y-x)$
  - decrease at each step
  - bounded from below

Ranking Function Constraint ∃∀

- ranking function $f(x, y) = f_x\, x + f_y\, y$
- lower bound δ_0
- decrease amount δ



$$\delta \geq 1 \wedge$$

$$\forall x\ \forall y\ \forall x'\ \forall y' :$$

$$\rho_2 \rightarrow (f_x x + f_y y \geq \delta_0 \wedge$$

$$f_x x' + f_y y' \leq f_x x + f_y y - \delta)$$

Quantifier Alternation $\exists\forall$

$$\exists f_x\ \exists f_y\ \exists \delta_0\ \exists \delta$$
$$\forall x\ \forall y\ \forall x'\ \forall y' :$$
$$\delta \geq 1 \wedge$$
$$\rho_2 \rightarrow (f_x x + f_y y \geq \delta_0 \wedge$$
$$f_x x' + f_y y' \leq f_x x + f_y y - \delta)$$

- Difficult to solve

Eliminating ∀-Quantifier (1)

$$\rho_2 = \begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \\ x' \\ y' \end{pmatrix} \leq \begin{pmatrix} -1 \\ 1 \\ -1 \\ 0 \\ 0 \end{pmatrix}$$

implies

$$f_x x + f_y y \geq \delta_0 = \begin{pmatrix} -f_x & -f_y & 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ x' \\ y' \end{pmatrix} \leq -\delta_0$$

Eliminating ∀-Quantifier (2)

$$\forall x\ \forall y\ \forall x'\ \forall y' : \rho_2 \rightarrow f_x x + f_y y \geq \delta_0$$

iff (by Farkas' lemma)

$$\exists \lambda : \lambda \geq 0 \wedge \lambda \begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & 1 & 0 & -1 \end{pmatrix} = \begin{pmatrix} -f_x & -f_y & 0 & 0 \end{pmatrix} \wedge \lambda \begin{pmatrix} -1 \\ 1 \\ -1 \\ 0 \\ 0 \end{pmatrix} \leq -\delta_0$$

Ranking Function Constraint ∃

- Find ranking function $f(x, y) = f_x\, x + f_y\, y$, δ_0, and δ

$\delta \geq 1 \wedge$

$\exists\lambda\ \exists\mu :$

$$\lambda \geq 0 \wedge \lambda \begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & 1 & 0 & -1 \end{pmatrix} = \begin{pmatrix} -f_x & -f_y & 0 & 0 \end{pmatrix} \wedge \lambda \begin{pmatrix} -1 \\ 1 \\ -1 \\ 0 \\ 0 \end{pmatrix} \leq -\delta_0 \wedge$$

$$\mu \geq 0 \wedge \mu \begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & 1 & 0 & -1 \end{pmatrix} = \begin{pmatrix} -f_x & -f_y & f_x & f_y \end{pmatrix} \wedge \mu \begin{pmatrix} -1 \\ 1 \\ -1 \\ 0 \\ 0 \end{pmatrix} \leq -\delta$$

- Linear inequality constraints to solve

Ranking Function Constraint Solved

- Find ranking function $f(x, y) = f_x\, x + f_y\, y$, δ_0, and δ

$$\lambda = (1\ 0\ 0\ 0\ 0)$$
$$\mu = (0\ 0\ 1\ 1\ 0)$$
$$f_x = -1$$
$$f_y = 1$$
$$\delta_0 = 1$$
$$\delta = 1$$

```
while (x < y) {
  x++;
}
```

- Ranking function $f(x, y) = (-1\ x + 1\ y) = y - x$

Ranking Function Algorithm

- Input $\rho(v, v') = R \begin{pmatrix} v \\ v' \end{pmatrix} \leq r$
- Defining constraint

$$\exists f \ \exists \delta_0 \ \exists \delta \ \forall v \ \forall v' : \delta \geq 1 \wedge \rho(v, v') \rightarrow (fv \geq \delta_0 \wedge fv' \leq fv - \delta)$$

- Linear constraint to solve

$$\exists f \ \exists \delta_0 \ \exists \delta \ \exists \lambda \ \exists \mu : \delta \geq 1 \wedge$$

$$\lambda \geq 0 \wedge \lambda R = (-f \ \ 0) \wedge \lambda r \leq -\delta_0 \wedge$$

$$\mu \geq 0 \wedge \mu R = (-f \ \ f) \wedge \mu r \leq -\delta$$