Linear Invariant Generation Using Non-Linear Constraint Solving

Sriram Sankaranarayanan et. al
CAV'03 and SAS'04

Report date: March 23, 2021

Problem and Contribution

- Problem: Generation of linear invariant for linear transition system.
- Contribution: An exact method for finding the invariant which avoid the widening operator in the classical abstract interpretation.

Transition System and Invariant

Definition 1 (Transition System) A *transition system* $P : \langle V, L, l_0, \Theta, \mathcal{T} \rangle$ consists of a set of *variables* V, a set of *locations* L, an *initial location* l_0, an *initial assertion* Θ over the variables V, and a set of *transitions* $\mathcal{T}$. Each transition $\tau \in \mathcal{T}$ is a tuple $\langle l, l', \rho_\tau \rangle$, where $l, l' \in L$ are the *pre* and *post locations*, and ρ_τ is the *transition relation*, an assertion over $V \cup V'$, where V represents current-state variables and its primed version V' represents the next-state variables.

Definition 2 (Inductive Assertion Map) Given a program P with a cutset C and an assertion $\eta_c(l)$, for each cutpoint l, we say that η_c is an *inductive assertion map* for C if it satisfies the following conditions for all cutpoints l, l':

Initiation For each basic path π from l_0 to l, $\Theta \wedge \rho_\pi \models \eta_c(l)'$.
Consecution For each basic path π from l to l', $\eta_c(l) \wedge \rho_\pi \models \eta_c(l')'$.

Linear Constraint

Farkas' Lemma

Theorem 2.5 (Farkas' lemma). *The system $Ax = b$ has a nonnegative solution if and only if there is no vector y satisfying $y^T A \geq 0$ and $y^T b < 0$.*

Intuitive understanding of farkas lemma.

Corollary 2.5b. *Suppose that the system $Ax \leq b$ has at least one solution. Then for every solution x of $Ax \leq b$ one has $c^T x \leq \delta$ if and only if there exists a vector $y \geq 0$ such that $y^T A = c^T$ and $y^T b \leq \delta$.*

Farkas' Lemma

A better demonstration of the Corrollary.

Theorem 1 (Farkas' Lemma). *Consider the following system of linear inequalities over real-valued variables $x_1, \ldots, x_n$,*

$$S : \begin{bmatrix} a_{11}x_1 + \cdots + a_{1n}x_n + b_1 \le 0 \\ \vdots \qquad\qquad \vdots \qquad \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n + b_m \le 0 \end{bmatrix}$$

When S is satisfiable, it entails a given linear inequality

$$\psi : \; c_1x_1 + \cdots + c_nx_n + d \le 0$$

if and only if there exist non-negative real numbers $\lambda_0, \lambda_1, \ldots, \lambda_m$, such that

$$c_1 = \sum_{i=1}^{m} \lambda_i a_{i1}, \quad \ldots \quad , c_n = \sum_{i=1}^{m} \lambda_i a_{in}, \; d = (\sum_{i=1}^{m} \lambda_i b_i) - \lambda_0$$

Furthermore, S is unsatisfiable if and only if the inequality $1 \le 0$ can be derived as shown above.

Solving the Invariant of Transition System

Quantifier Elimination

- Exact quantifier elimination.
- Under-approximate elimination approach