CS615: Formal Specification and Verification of Programs 2019

Lecture 19: Refinement and Interpolation

Instructor: Ashutosh Gupta

IITB, India

Compile date: 2019-11-05

Computing refinement

In order to automate CEGAR, we need an effective method for computing new predicates that result in the desired refinement.

Here, we discuss the following two methods for refinement of a predicate abstraction.

- Syntax based refinement
- Interpolation based refinement

Let us first define(remind) some notations.

Path constraints for spurious counterexample (reminder)

V_i be the vector of variables obtained by adding subscript i after each variable in V.

Definition 19.1

For a spurious counterexample $e_1 \dots e_n$, path constraints $pathCons(e_1 \dots e_n)$ is

$$\bigwedge_{i \in 1..n} e_i(V_{i-1}, V_i)$$

A path is feasible if corresponding path constraints is satisfiable.

Note: Path constraints are also known as "SSA formulas".

Syntax based refinement

$core = \text{unsatCore}(\ pathCons(e_1 \dots e_n)\ ).$

$preds$ = atoms of *core* after erasing subscripts in its variables

Add *preds* in the predicate domain to obtain the refined abstract domain

Interpolation

Definition 19.2

Let A and B be formulas such that $A \land B$ is unsat. An interpolant I between A and B is a formula such that

- $A \Rightarrow \mathrm{I}$
- $B \land \mathrm{I} \Rightarrow \bot$
- $vars(\mathrm{I}) \subseteq vars(A) \cap vars(B)$

Theorem 19.1 (Craig interpolation theorem)

Interpolant always exists.

Example 19.1

Consider:

$A = x_1 + x_2 \leq 2 \land x_3 - x_2 \leq 0$

$B = 6x_4 - 2x_1 \leq -8 \land -3x_4 - x_3 \leq 0$

$vars(A) = \{x_1, x_2, x_3\} \quad vars(B) = \{x_1, x_3, x_4\} \quad vars(\mathrm{I}) \subseteq \{x_1, x_3\}$

$\mathrm{I} = x_1 + x_3 \leq 2$

Interpolation chain

We can extend the definition of interpolant to our setting

Definition 19.3

Consider unsat formula $\bigwedge_{i \in 1..m} e_i(V_{i-1}, V_i)$*. An* *interpolant chain* *is a sequence of formulas such that* $\mathrm{I}_0 \ldots \mathrm{I}_m$ *such that*

- $\mathrm{I}_0 = \top$
- $\forall i \in 1..m \; \mathrm{I}_{i-1} \wedge e_i(V_{i-1}, V_i) \Rightarrow \mathrm{I}_i$
- $\mathrm{I}_m = \bot$
- $vars(\mathrm{I}_i) \subseteq V_i$

Interpolation for refinement

We compute interpolation chain $\mathrm{I}_0 \ldots \mathrm{I}_m$ for *pathCons*(*cons*)

preds $=$ atoms in $\mathrm{I}_0 \ldots \mathrm{I}_m$ after erasing subscripts in its variables

Add *preds* in the predicate domain to obtain the refined abstract domain

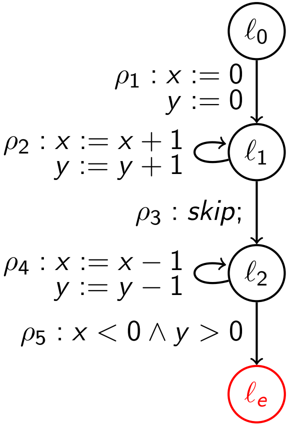
Theorem 19.2

The new abstract domain eliminates spurious counterexample $e_1 \ldots e_n$

Example: interpolation for refinement

Spurious counterexample: $\rho_1\rho_2\rho_3\rho_4\rho_4\rho_5$.

Program:



$\top$

$\rho_1(x_0, y_0, x_1, y_1) = (x_1 = 0 \land y_1 = 0)$

$\mathrm{I}_1 = y_1 \leq 0$

$\rho_2(x_1, y_1, x_2, y_2) = (x_2 = x_1 + 1 \land y_2 = y_1 + 1)$

$\mathrm{I}_2 = y_2 \leq 1$ $\leftarrow$ New predicate

$\rho_3(x_2, y_2, x_3, y_3) = (x_3 = x_2 \land y_3 = y_2)$

$\mathrm{I}_3 = y_3 \leq 0$

$\rho_4(x_3, y_3, x_4, y_4) = (x_4 = x_3 - 1 \land y_4 = y_3 - 1)$

$\mathrm{I}_4 = y_4 \leq 0$

$\rho_4(x_4, y_4, x_5, y_5) = (x_5 = x_4 - 1 \land y_5 = y_4 - 1)$

$\mathrm{I}_5 = y_5 \leq 0$

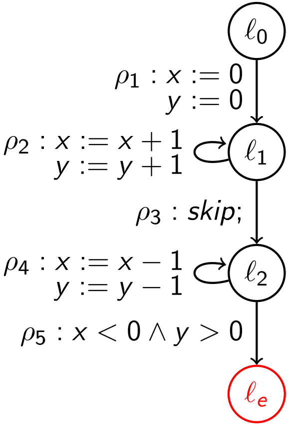
$\rho_5(x_5, y_5, x_6, y_6) = (x_5 < 0 \land y_5 > 0)$

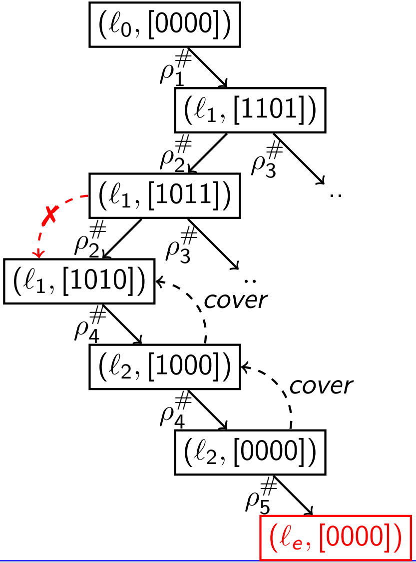
$\bot$

Example: refined reachability graph

$$Preds = \{x \geq 0, y \leq 0, x \geq 1, y \leq 1\}$$

Program:



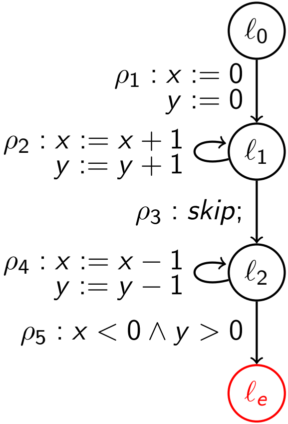


Exercise 19.1

Complete the ARG

Example: good refinement

Program:



Consider the earlier spurious counterexample again: $\rho_1\rho_2\rho_3\rho_4\rho_4\rho_5$.

$\top$

$\rho_1(x_0, y_0, x_1, y_1) = (x_1 = 0 \wedge y_1 = 0)$

$\mathrm{I}_1 = y_1 \leq x_1$

$\rho_2(x_1, y_1, x_2, y_2) = (x_2 = x_1 + 1 \wedge y_2 = y_1 + 1)$

$\mathrm{I}_2 = y_2 \leq x_2$ $\leftarrow$ New predicate

$\rho_3(x_2, y_2, x_3, y_3) = (x_3 = x_2 \wedge y_3 = y_2)$

$\mathrm{I}_3 = y_3 \leq x_3$

$\rho_4(x_3, y_3, x_4, y_4) = (x_4 = x_3 - 1 \wedge y_4 = y_3 - 1)$

$\mathrm{I}_4 = y_4 \leq x_4$

$\rho_4(x_4, y_4, x_5, y_5) = (x_5 = x_4 - 1 \wedge y_5 = y_4 - 1)$

$\mathrm{I}_5 = y_5 \leq x_5$

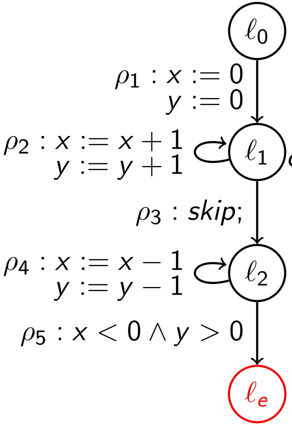
$\rho_5(x_5, y_5, x_6, y_6) = (x_5 < 0 \wedge y_5 > 0)$

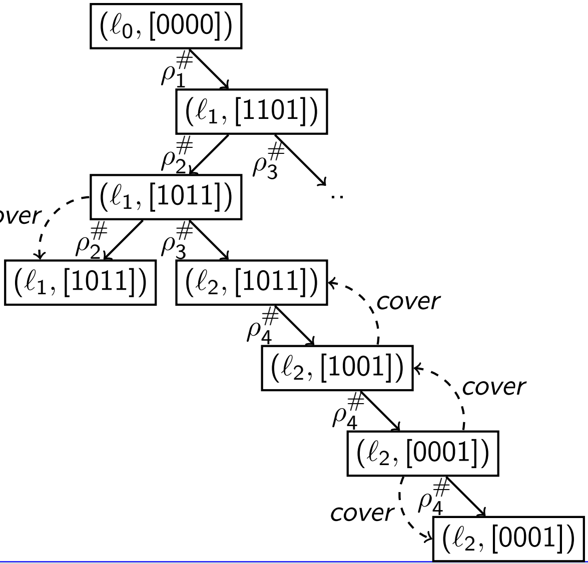
$\bot$

Example: ARG without spurious counterexample

$$Preds = \{x \geq 0, y \leq 0, x \geq 1, y \leq x\}$$

Program:





Exercise 19.2

Complete the ARG

End of Lecture 19