Generalised Interpolation by Solving Recursion-free Horn Clauses

Corneliu Popeea

joint work with Ashutosh Gupta, Andrey Rybalchenko

Technische Universität München

IST AUSTRIA
Institute of Science and Technology

Motivation

- Verification via CEGAR approach
- Spurious counterexamples
- Interpolation problems

Spurious counterexample 1

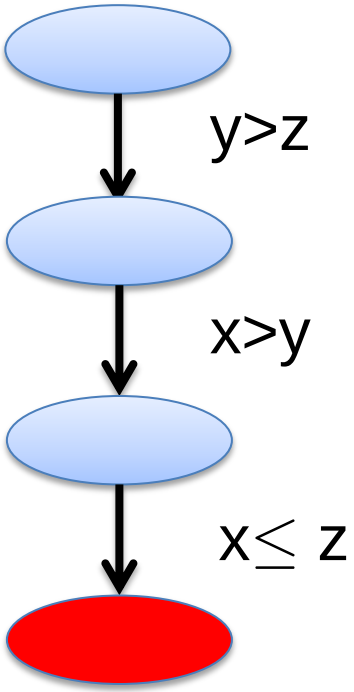
- Path

$\exists I0, I1:$

$\forall x,y,z:\ y>z \rightarrow I0(x, y, z)$

$\forall x,y,z:\ I0(x, y, z) \wedge x>y \rightarrow I1(x, y, z)$

$\forall x,y,z:\ I1(x, y, z) \wedge x \leq z \rightarrow \bot$



Spurious counterexample 2

- Nested path with procedure calls

∃I1,I2,...:

$X \leq 100 \rightarrow I1(X,Xm,Res,Resm)$

$I1(X,Xm,Res,Resm) \wedge Xm'=X+11 \rightarrow I2(X,Xm',Res,Re$

$I2(X,Xm,Res,Resm) \wedge X'=Xm \rightarrow I3(Xp,Xm',Resp$

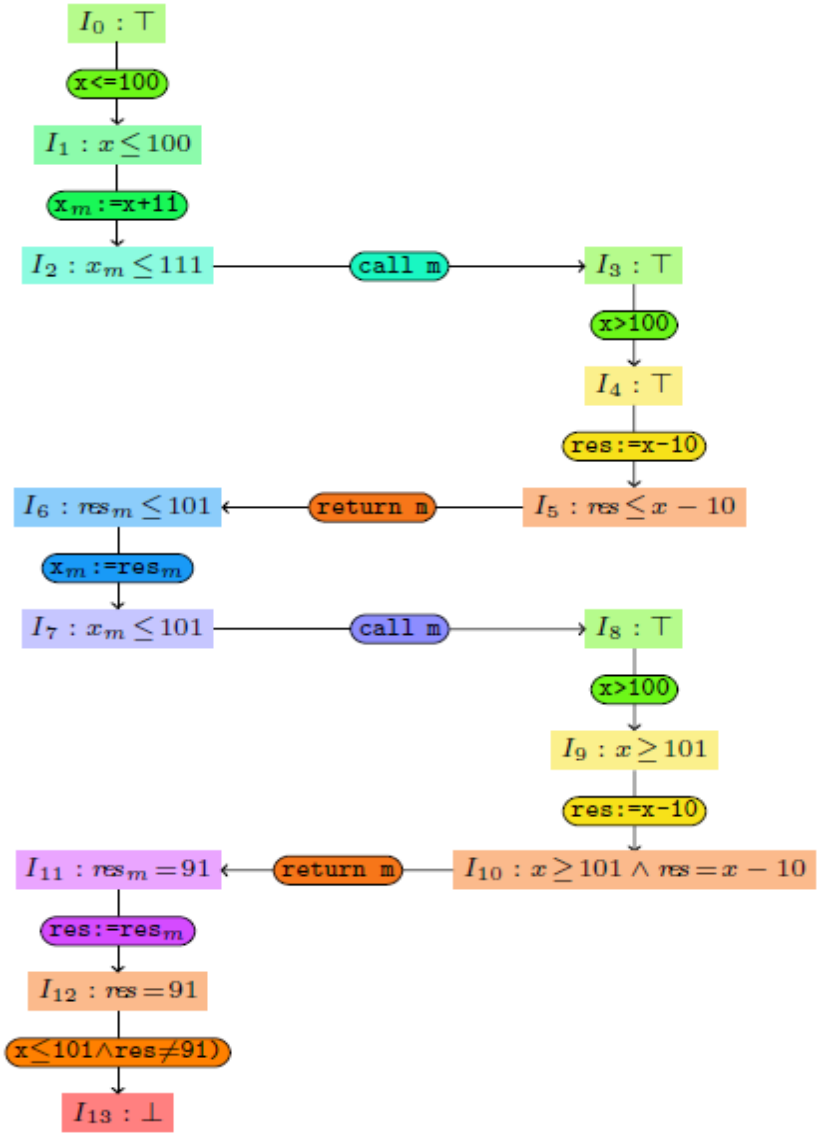
$I3(X,Xm,Res,Resm) \wedge X>100 \rightarrow I4(X,Xm,Res,Re$

$i4(X,Xm,Res,Resm) \wedge Res'=X-10 \rightarrow I5(X,Xm,Res',Re$

$i2(X,\_,\_,\_) \wedge i5(\_,\_,Res,\_) \wedge Resm'=Res \rightarrow I6(X,Xm,$

...

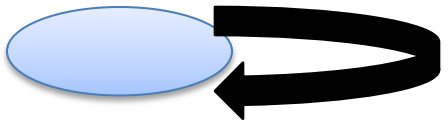
$i12(X,Xm,Res,Resm) \wedge X \leq 101 \wedge Res=91 \rightarrow \bot$



Spurious counterexample 3

- Path with well-foundedness (WF) conditions

$x+1 \leq y \wedge x'=x+1 \wedge y'=y$



$\exists I0, r:$

$x+1 \leq y \wedge x'=x+1 \wedge y'=y \rightarrow I0(x, y, x', y')$

$I0(x, y, x', y') \rightarrow r(x, y) > r(x', y') \wedge r(x, y)$

wf(I0)

An observation

Solving rec.-free Horn clauses with WF-conditions

gives solutions to interpolation problems

Recursion-free Horn clauses with WF

$\phi \in$ P background predicates, e.g., QF_LRA

q $\in$ Q query symbols

body ::= q(v,..,v) | ϕ | body $\wedge$ body

head ::= q(v,..,v) | ϕ | wf(q)

cl ::= $\forall$v,..,v: body $\rightarrow$ head

cls ::= cl $\wedge$ cls | cl

- Recursion-free
  Def. (q1 depends on q2): q2 $\in$ body and q1 $\in$ head
  Def. (rec.-free Horn clauses): no circular dependencies

Steps of solving algorithm

- Resolution
  - remove clausal structure
- Farkas' lemma
  - introduce weights for linear inequalities
  - for WF, get rid of quantifier alternation
- Call SMT-solve
- Obtain solution for clauses
  - use weights and SMT solution

Farkas' lemma

Constants:
- A – matrix
- b, 0 – vectors
- d - number

Unknowns:
- λ,t - vectors

$\neg(\exists v: Av \leq b) \wedge \forall v: Av \leq b \rightarrow 0v \leq -1$

iff

$\exists \lambda: \lambda \geq 0 \wedge \lambda A = 0 \wedge \lambda b \leq -1$

For WF clauses:

$\exists t: (\exists v: Av \leq b \wedge \forall v: Av \leq b \rightarrow tv \leq d)$

iff

$\exists t: (\exists \lambda: \lambda \geq 0 \wedge \lambda A = t \wedge \lambda b \leq d)$

EXAMPLES

1. Spurious path

- Clauses:

$\forall x,y,z:\ y \geq z \rightarrow p(x, y, z)$
$\forall x,y,z:\ p(x, y, z) \wedge x \geq y \rightarrow q(x, y, z)$
$\forall x,y,z:\ q(x, y, z) \rightarrow x \geq z$

- Resolution: $\forall x,y,z:\ y \geq z \wedge x \geq y \rightarrow x \geq z$
- Farkas' lemma:
  $\exists \lambda_1,\lambda_2:\ \lambda_1 \geq 0 \wedge \lambda_2 \geq 0 \wedge (\lambda_1\ \lambda_2)\begin{pmatrix} 0 & -1 & 1 \\ -1 & 1 & 0 \end{pmatrix} = (-1\ 0\ 1)$
- SMT-solve: $\lambda_1 = 1,\ \lambda_2 = 1$
- Solution for clauses:

$p(x, y, z) = 1*(y \geq z) = y \geq z$
$q(x, y, z) = 1*(y \geq z) + 1*(x \geq y) = x \geq z$

2. Genuine path

- Clauses:

$\forall x,y,z:\ y \geq z \rightarrow p(x, y, z)$
$\forall x,y,z:\ p(x, y, z) \wedge x \geq y \rightarrow q(x, y, z)$
$\forall x,y,z:\ q(x, y, z) \rightarrow x \leq z$

- Resolution: $\forall x,y,z:\ y \geq z \wedge x \geq y \rightarrow x \leq z$
- Farkas' lemma:
  $\exists \lambda_1,\lambda_2:\ \lambda_1 \geq 0 \wedge \lambda_2 \geq 0 \wedge (\lambda_1\ \lambda_2)\begin{pmatrix} 0 & -1 & 1 \\ -1 & 1 & 0 \end{pmatrix} = (1\ 0\ -1)$
- SMT-solve: unsat
- Solution for clauses:

unsat

3. Spurious path with WF-condition

- Clauses: $\forall x,y,x',y'\colon\ x+1 \leq y \wedge x'=x+1 \wedge y'=y \rightarrow q(x, y, x', y')$
  $\forall x,y,x',y'\colon\ q(x, y, x', y') \rightarrow (t_x*x'+t_y*y'+1 \leq t_x*x+t_y*y \wedge t_x*x+t_y*y \geq 0)$
- Resolution:
  $\exists t_x, t_y\colon\ \forall x,y,x',y'\colon\ x+1 \leq y \wedge x'=x+1 \wedge y'=y \rightarrow$ (...decrease... $\wedge$ ...bound...)
- Farkas' lemma: $\exists t_x, t_y\colon \exists \lambda\colon \lambda \geq 0 \wedge \ldots$
- SMT-solve: $t_x = -1, t_y = 1, \lambda_1 = \ldots,$
- Solution for clauses:

$q(x, y, x', y') = y'-x'+1 \leq y-x \wedge y-x \geq 0$
$rank(x, y) = -x+y$

Further details

- Solving recursion-free clauses over QF_LRA [POPL'11]
- Solving recursion-free clauses over QF_UFLRA [APLAS'11]
- Solving recursion-free clauses with WF [TACAS'12]

Applications:

- Proof rules for multi-threaded programs [CAV'11] [ATVA'10]
- Solving recursive clauses with WF [PLDI'12]
- Proof rules for CTL properties [CAV'13]
- Verification competitions [SV-COMP'12] [SV-COMP'13]

www.model.in.tum.de/~popeea

Summary

- Recursion-free Horn clauses
- Declarative specification of interpolation problems

Goal
common interpolation back-end
useful for diverse verification tools

Thank you!

- Questions?