A Class of Polynomially Solvable Range Constraints for Interval Analysis without Widenings and Narrowings

Zhendong Su
U.C. Davis
su@cs.ucdavis.edu

David Wagner
U.C. Berkeley
daw@cs.berkeley.edu

Motivation: Program Analysis of Integer Values

```
i := 0;
while (...)
  ...
  i := i+1;
  j := 2*i-3;
```

Question: How do we find upper, lower bounds for `i`, `j`?

Motivation: Program Analysis of Integer Values

```
i := 0;
while (...)
  ...
  i := i+1;
  j := 2*i-3;
```

Question: How do we find upper, lower bounds for `i`, `j`?
Answer: Integer range analysis.

Let X (resp. Y) be a range variable over-approximating the set of possible values of `i` (resp. `j`).

Motivation: Program Analysis of Integer Values

```
i := 0;
while (...)
  ...
  i := i+1;
  j := 2*i-3;
```

$$[0,0] \sqsubseteq X$$

$$X + 1 \sqsubseteq X$$

$$2X - 3 \sqsubseteq Y$$

Question: How do we find upper, lower bounds for `i`, `j`?
Answer: Integer range analysis.

Let X (resp. Y) be a range variable over-approximating the set of possible values of `i` (resp. `j`).
Least solution: $X = [0, \infty], Y = [-3, \infty]$

Our Focus

In this talk: How to solve range-constraint systems (precisely, and in polynomial time).

Background: Ranges

Range constants: $[l,u]$ denotes the interval of integers $\{l, l+1, l+2, \ldots, u\} \subseteq \mathbb{Z}$, for $l \in \mathbb{Z} \cup \{-\infty\}$, $u \in \mathbb{Z} \cup \{\infty\}$.

Operations on ranges: Define
$[l,u] + [l',u'] = [l+l', u+u']$, $-[l,u] = [-u,-l]$,
$n \times [l,u] = [n \times l, n \times u]$ (for $n \geq 0$), etc.

The range lattice: Define $\bot = \emptyset$, $\top = [-\infty, \infty] = \mathbb{Z}$,
$[l,u] \sqcup [l',u'] = [\min(l,l'), \max(u,u')]$,
$[l,u] \sqcap [l',u'] = [\max(l,l'), \min(u,u')]$.
This forms a lattice $(L, \sqcup, \sqcap)$ of infinite height.

Range Constraint Systems

Notation: $X, Y, \ldots \in \mathscr{V}$ denote range variables, $m, n \in \mathbb{Z}$.

Range expressions: $E ::= [l, u] \mid X \mid n \times X \mid E + E$.

Range constraints: $C ::= E \sqsubseteq X$.

Constraint systems: $\mathscr{C} ::= \{C_1, \ldots, C_n\}$.

Valuations: $\rho : \mathscr{V} \to L$. $\rho \sqsubseteq \rho'$ if $\rho(X) \sqsubseteq \rho'(X)\ \forall X \in \mathscr{V}$.
Lift to expressions: $\rho(E_1 + E_2) = \rho(E_1) + \rho(E_2)$, etc.

Solutions: ρ satisfies $E \sqsubseteq X$ if $\rho(E) \sqsubseteq \rho(X)$.
ρ satisfies $\mathscr{C}$ if ρ satisfies C_i for each $C_i \in \mathscr{C}$.
ρ is a least solution of $\mathscr{C}$ if ρ' satisfies $\mathscr{C}$ implies $\rho \sqsubseteq \rho'$.

Examples

$$\mathscr{C} = \{[5,7] \sqsubseteq X,\ \ X+1 \sqsubseteq Y\}.$$

Examples

$\mathscr{C} = \{[5,7] \sqsubseteq X,\ \ X+1 \sqsubseteq Y\}$.

Least solution: $X = [5,7]$, $Y = [6,8]$.

Examples

$\mathscr{C} = \{[5,7] \sqsubseteq X,\;\; X+1 \sqsubseteq Y\}$.
Least solution: $X = [5,7]$, $Y = [6,8]$.

$\mathscr{C} = \{[1,3] \sqsubseteq X,\;\; X+1 \sqsubseteq X\}$.

Examples

$\mathscr{C} = \{[5,7] \sqsubseteq X,\ \ X+1 \sqsubseteq Y\}$.
Least solution: $X = [5,7]$, $Y = [6,8]$.

$\mathscr{C} = \{[1,3] \sqsubseteq X,\ \ X+1 \sqsubseteq X\}$.
Least solution: $X = [1,\infty]$.

More Examples

$$\mathscr{C} = \{[1,3] \sqsubseteq X,\ \ 3X - 10 \sqsubseteq X\}.$$

More Examples

$\mathscr{C} = \{[1,3] \sqsubseteq X,\ \ 3X - 10 \sqsubseteq X\}$.
Least solution: $X = [-\infty, 3]$.

More Examples

$\mathscr{C} = \{[1,3] \sqsubseteq X,\ \ 3X - 10 \sqsubseteq X\}$.
Least solution: $X = [-\infty, 3]$.

$\mathscr{C} = \{[-1,2] \sqsubseteq X,\ \ 2X \sqsubseteq Y,\ \ Y + 1 \sqsubseteq X\}$.

More Examples

$\mathscr{C} = \{[1,3] \sqsubseteq X,\ \ 3X - 10 \sqsubseteq X\}$.

Least solution: $X = [-\infty, 3]$.

$\mathscr{C} = \{[-1,2] \sqsubseteq X,\ \ 2X \sqsubseteq Y,\ \ Y + 1 \sqsubseteq X\}$.

Least solution: $X = [-1, \infty]$, $Y = [-2, \infty]$.

Prior Work: Fixpoints with Widening

Chaotic iteration: Associate to $\mathscr{C}$ the map $F(\rho) = \lambda X.\rho(X) \sqcup \bigsqcup_{E_i \sqsubseteq X \in \mathscr{C}} \rho(E_i)$. The least solution of $\mathscr{C}$ is the least fixpoint of f. Compute $\bot, F(\bot), F(F(\bot)), \ldots$.

Problem: Iteration might not terminate.
Solution: Widening. Define $[l,u]\Delta[l',u'] =$ [if $l' < l$ then $-\infty$ else l, if $u' > u$ then ∞ else u].
Compute $a_1 = F(\bot)$, $a_{i+1} = a_i \Delta F(a_i)$.

Example: $\mathscr{C} = \{[1,3] \sqsubseteq X,\ \ X+1 \sqsubseteq X\}$.
Iteration without widening: $F(r) = r \sqcup [1,3] \sqcup (r+1)$.
$F(\bot) = [1,3]$. $F^{(2)}(\bot) = [1,4]$. $F^{(3)}(\bot) = [1,5]$. etc.
With widening: $a_1 = [1,3]$. $a_2 = [1,3]\Delta[1,4] = [1,\infty]$.

Widening is Imprecise

Chaotic iteration with widening finds a solution to any range-constraint system in polynomial time.
However: Not necessarily the *least* solution.

Example: $\mathscr{C} = \{[0,0] \sqsubseteq X,\ \ [1,1] \sqsubseteq Y,\ \ Y \sqsubseteq X\}$.
Least solution: $(\rho(X), \rho(Y)) = ([0,1],[1,1])$.
Iteration with widening: $a_1 = ([0,0],[1,1])$.
$a_2 = a_1 \Delta([0,1],[1,1]) = ([0,\infty],[1,1])$. Imprecise!

Our algorithm fixes this defect.

Overview of Our Work

The Problem:

Given a range constraint system $\mathscr{C}$, find its least solution.

Our Main Result:

The least solution can be found in polynomial time.

Ideas Behind Our Algorithm

Restriction (for this talk): Focus on single-variable constraints. $E ::= [l,u] \mid aX + [l,u]$.

Idea 1: Let $f(X) = aX + [l,u]$ be affine, $a > 0$, $a \in \mathbb{Z}$. Widening is precise for $\mathscr{C} = \{[l',u'] \sqsubseteq X,\ \ f(X) \sqsubseteq X\}$.

Idea 2: Let f, g be affine. Then $f(X) \sqsubseteq Y$, $g(Y) \sqsubseteq Z$ implies $(g \circ f)(X) \sqsubseteq Z$. Also $g \circ f$ is affine.

Ideas Behind Our Algorithm

Idea 3: Let $f_1(X_1) \sqsubseteq X_2$, $f_2(X_2) \sqsubseteq X_3$, . . . , $f_n(X_n) \sqsubseteq X_1$ be a cycle of constraints. Then $g(X_1) \sqsubseteq X_1$, where $g = f_n \circ \cdots \circ f_1$. If $r = \rho(X)$, use widening to find least solution r' of $\{r \sqsubseteq X_1,\ g(X_1) \sqsubseteq X_1\}$, and set $\rho'(X) := r'$.

Idea 4: Call a cycle *active* if $g(X_1) \sqsubseteq X_1$ is unsatisfied by ρ. If chaotic iteration diverges, there is an active cycle.

Idea 5: After processing $2n$ active cycles we're done.

Proof. Applying Idea 3 to an active cycle sets some variable's bound to $\pm\infty$. This can only be done twice per variable. $\square$

Our Algorithm (Intuition)

1. Set $\rho := \lambda X.\bot$.
2. While ρ doesn't satisfy $\mathscr{C}$, do:
3.   Apply n steps of chaotic iteration: $\rho := F^{(n)}(\rho)$.
4.   Apply widening to each active cycle.

This is just the intuition. See the paper for details, optimizations, and extensions.

Summary

Range-constraint systems:

- are useful for program analysis.
- can be solved in polynomial time, without loss of precision.

An example of fixpoint computation in a non-distributive lattice of infinite height. Perhaps these techniques have applications elsewhere?