Static Program Analysis

Part 5 – widening and narrowing

http://cs.au.dk/~amoeller/spa/

Anders Møller & Michael I. Schwartzbach
Computer Science, Aarhus University

Interval analysis

- Compute upper and lower bounds for integers
- Possible applications:
  - array bounds checking
  - integer representation
  - …
- Lattice of intervals:

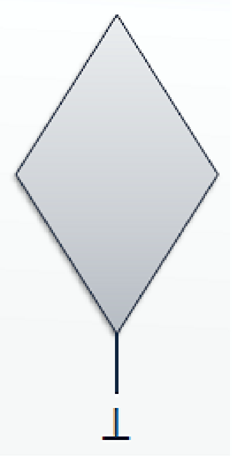
$$Interval = lift(\{\ [l\,,h]\ \mid\ l,h \in N \wedge l \leq h\ \})$$

where

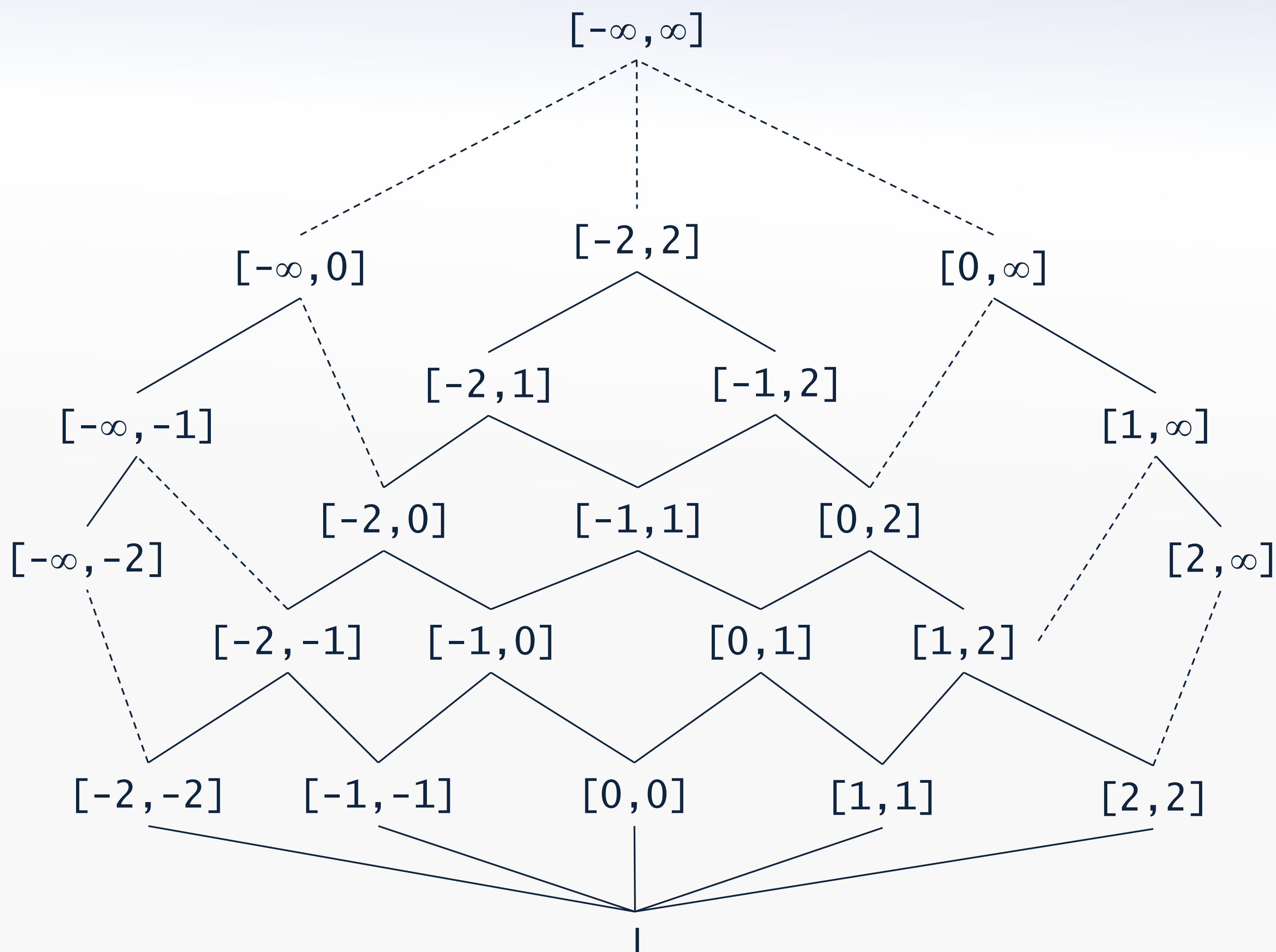
$$N = \{-\infty, \ldots, -2, -1, 0, 1, 2, \ldots, \infty\}$$

and intervals are ordered by inclusion:

$$[l_1\,,h_1] \sqsubseteq [l_2\,,h_2]\ \text{ iff } l_2 \leq l_1 \wedge h_1 \leq h_2$$



The interval lattice



bottom element here interpreted as “not an integer”

Interval analysis lattice

- The total lattice for a program point is

  $$L = \mathit{Vars} \rightarrow \mathit{Interval}$$

  that provides bounds for each (integer) variable

- If using the worklist solver that initializes the worklist with only the *entry* node, use the lattice *lift*(L)
  - bottom value of *lift*(L) represents "unreachable program point"
  - bottom value of L represents "maybe reachable, but all variables are non-integers"

- This lattice has *infinite height*, since the chain

  $$[0,0] \sqsubseteq [0,1] \sqsubseteq [0,2] \sqsubseteq [0,3] \sqsubseteq [0,4] \ldots$$

  occurs in *Interval*

Interval constraints

- For assignments:

$$[\![\, x = E \,]\!] = JOIN(\mathrm{v})[x \rightarrow eval(JOIN(\mathrm{v}),E)]$$

- For all other nodes:

$$[\![\mathrm{v}]\!] = JOIN(\mathrm{v})$$

where $JOIN(\mathrm{v}) = \bigsqcup_{\mathrm{w} \in pred(\mathrm{v})} [\![\mathrm{w}]\!]$

Evaluating intervals

- The *eval* function is an *abstract evaluation*:
  - $eval(\sigma, x) = \sigma(x)$
  - $eval(\sigma, intconst) = [intconst, intconst]$
  - $eval(\sigma, E_1 \text{ op } E_2) = \overline{\text{op}}(eval(\sigma,E_1), eval(\sigma,E_2))$
- Abstract arithmetic operators:
  - $\overline{\text{op}}([l_1, h_1], [l_2, h_2]) =$

not trivial to implement!

$$\left[\min_{x \in [l_1,h_1],\, y \in [l_2,h_2]} x \text{ op } y,\ \max_{x \in [l_1,h_1],\, y \in [l_2,h_2]} x \text{ op } y\right]$$

$$\boxed{\widehat{+}([1,10],[-5,7]) = [1-5, 10+7] = [-4,17].}$$

- Abstract comparison operators (could be improved):
  - $\overline{\text{op}}([l_1, h_1], [l_2, h_2]) = [0, 1]$

Fixed-point problems

- The lattice has infinite height, so the fixed-point algorithm does not work ☹

- In L^n, the sequence of approximants

  $$f^i(\perp, \perp, \ldots, \perp)$$

  is not guaranteed to converge
- (Exercise: give an example of a program where this happens)

- Restricting to 32 bit integers is not a practical solution
- *Widening* gives a useful solution…

Widening

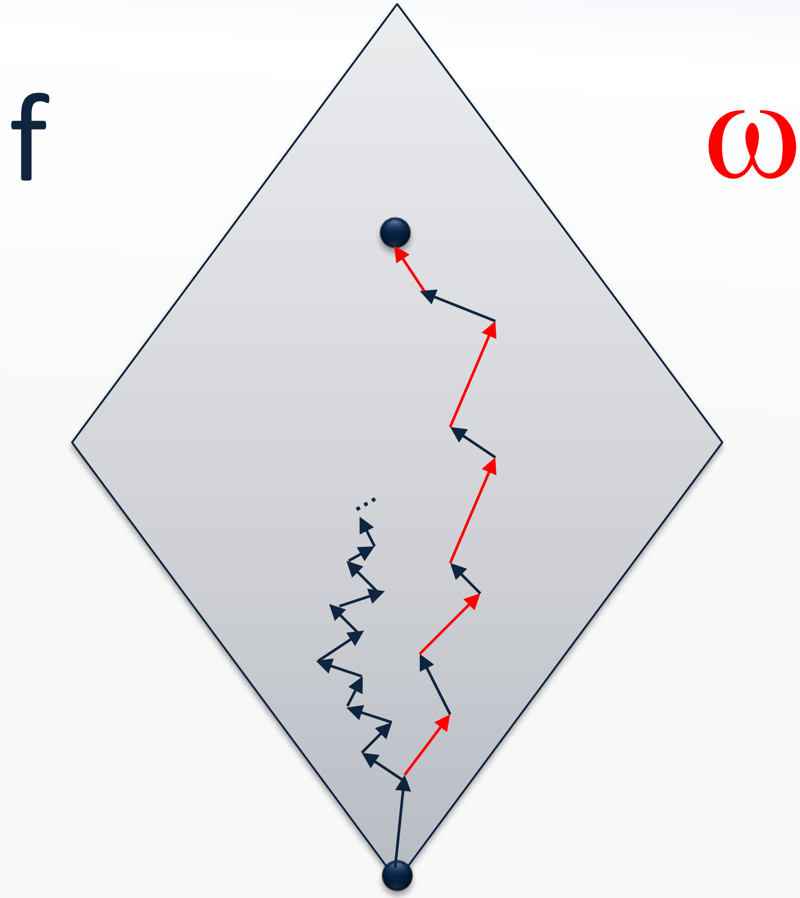
- Introduce a *widening* function $\omega: L^n \rightarrow L^n$ so that

  $$(\omega \circ f)^i(\perp, \perp, \ldots, \perp)$$

  converges on a fixed-point that is a safe approximation of each $f^i(\perp, \perp, \ldots, \perp)$

- i.e. the function ω coarsens the information

Turbo charging the iterations



Widening for intervals

- The function ω is defined pointwise on L^n
- Parameterized with a fixed finite subset $B \subset \mathcal{N}$
  - must contain $-\infty$ and ∞ (to retain the $\top$ element)
  - typically seeded with all integer constants occurring in the given program
- Idea: Find the nearest enclosing allowed interval
- On single elements from *Interval* :

$$\omega([a, b]) = [\ \mathit{max}\{i \in B \mid i \leq a\},\ \mathit{min}\{i \in B \mid b \leq i\}\ ]$$

$$\omega(\bot) = \bot$$

Divergence in action

```
y = 0;
x = 7;
x = x+1;
while (input) {
  x = 7;
  x = x+1;
  y = y+1;
}
```

$[x \to \bot, y \to \bot]$
$[x \to [8,8], y \to [0,1]]$
$[x \to [8,8], y \to [0,2]]$
$[x \to [8,8], y \to [0,3]]$
…

Widening in action

```
y = 0;
x = 7;
x = x+1;
while (input) {
  x = 7;
  x = x+1;
  y = y+1;
}
```

$[x \to \perp, y \to \perp]$
$[x \to [7,\infty], y \to [0,1]]$
$[x \to [7,\infty], y \to [0,7]]$
$[x \to [7,\infty], y \to [0,\infty]]$

$B = \{-\infty, 0, 1, 7, \infty\}$

Correctness of widening

- Widening works when:
  - ω is an *extensive* and *monotone* function, and
  - $\omega(L)$ is a *finite-height* lattice

Exercise 4.14: A function $f : L \to L$ where L is a lattice is *extensive* when $\forall x \in L : x \sqsubseteq f(x)$.

- Safety: $\forall i$: $f^i(\bot, \bot, \ldots, \bot) \sqsubseteq (\omega \circ f)^i(\bot, \bot, \ldots, \bot)$
  since f is monotone and ω is extensive
- $\omega \circ f$ is a monotone function $\omega(L) \to \omega(L)$
  so the fixed-point exists

- Almost "correct by definition"!
- When used in the worklist algorithm, it suffices to apply widening on back-edges in the CFG

Narrowing

- Widening generally shoots over the target
- *Narrowing* may improve the result by applying f
- Define:

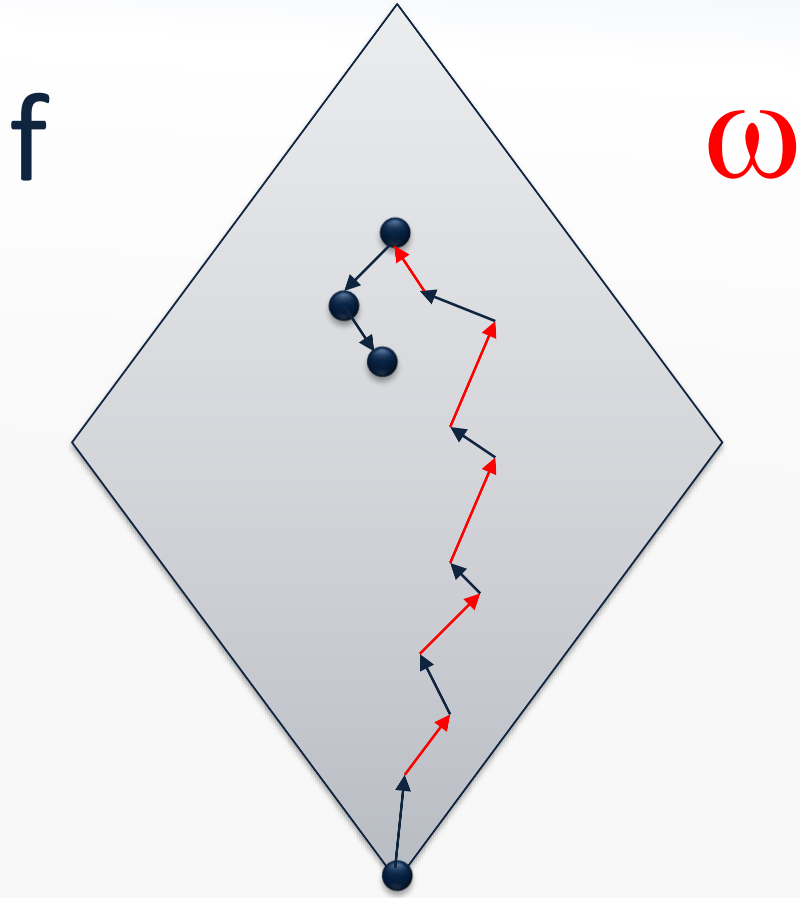
  $fix = \bigsqcup f^i(\bot, \bot, \ldots, \bot) \quad fix\omega = \bigsqcup (\omega \circ f)^i(\bot, \bot, \ldots, \bot)$

  then $fix \sqsubseteq fix\omega$
- But we also have that

  $fix \sqsubseteq f(fix\omega) \sqsubseteq fix\omega$

  so applying f again may improve the result and remain sound!
- This can be iterated arbitrarily many times
  - may diverge, but safe to stop anytime

Backing up



Correctness of (repeated) narrowing

- $f(\mathit{fix}\omega) \sqsubseteq \omega(f(\mathit{fix}\omega)) = (\omega \circ f)(\mathit{fix}\omega) = \mathit{fix}\omega$
  since ω is extensive
  - by induction we also have, for all i:

    $f^{i+1}(\mathit{fix}\omega) \sqsubseteq f^{i}(\mathit{fix}\omega) \sqsubseteq \mathit{fix}\omega$
  - i.e. $f^{i+1}(\mathit{fix}\omega)$ is at least as precise as $f^{i}(\mathit{fix}\omega)$
- $\mathit{fix} \sqsubseteq \mathit{fix}\omega$ hence $f(\mathit{fix}) = \mathit{fix} \sqsubseteq f(\mathit{fix}\omega)$
  by monotonicity of f
  - by induction we also have, for all i:

    $\mathit{fix} \sqsubseteq f^{i}(\mathit{fix}\omega)$
  - i.e. $f^{i}(\mathit{fix}\omega)$ is a sound approximation of *fix*

Narrowing in action

```
y = 0;
x = 7;
x = x+1;
while (input) {
  x = 7;
  x = x+1;
  y = y+1;
}
```

$[x \to \bot, y \to \bot]$
$[x \to [7,\infty], y \to [0,1]]$
$[x \to [7,\infty], y \to [0,7]]$
$[x \to [7,\infty], y \to [0,\infty]]$
…
$[x \to [8,8], y \to [0,\infty]]$

$B = \{-\infty, 0, 1, 7, \infty\}$

More powerful widening

- Defining the widening function based on constants occurring in the given program may not work

```
f(x) { // "McCarthy's 91 function"
  var r;
  if (x > 100) {
    r = x - 10;
  } else {
    r = f(f(x + 11));
  }
  return r;
}
```

https://en.wikipedia.org/wiki/McCarthy_91_function

- Note: requires interprocedural analysis…

More powerful widening

二元widening算子支持从不动点计算的
前一次和当前迭代来组合出抽象信息

- A *widening* is a function $\nabla: L^n \times L^n \to L^n$ that is extensive in both arguments and satisfies the following property:
  for all increasing chains $x_0 \sqsubseteq x_1 \sqsubseteq \ldots$,
  the sequence $y_0 = x_0, \ldots, y_{i+1} = y_i \nabla x_{i+1}, \ldots$ converges
  (i.e. stabilizes after a finite number of steps)

- Now replace the basic fixed point solver by computing $y_0 = \perp, \ldots, y_{i+1} = y_i \nabla F(y_i), \ldots$ until convergence

- (This is the notion of widening found in the literature,
  except that an arbitrary lattice is typically used instead of L^n)

More powerful narrowing

- Similarly, we can generalize narrowing
- A *narrowing* is a function Δ: $L^n \times L^n \rightarrow L^n$ such that

  $\forall x,y \in L^n$: $(y \sqsubseteq x) \Rightarrow (y \sqsubseteq (x \,\Delta\, y) \sqsubseteq x)$

  and

  for all decreasing chains $x_0 \sqsupseteq x_1 \sqsupseteq \ldots$,

  the sequence $y_0 = x_0, \ldots, y_{i+1} = y_i \,\Delta\, x_{i+1}, \ldots$ converges

- After computing the fixed point y_k with widening, continue with $y_{i+1} = y_i \,\Delta\, F(y_i)$ (until convergence or bounded number of iterations)

More powerful narrowing for interval analysis

- Widening (extrapolates unstable bounds to infinity):

$$\bot \,\nabla\, x = x$$
$$x \,\nabla\, \bot = x$$
$$[a_1, b_1] \,\nabla\, [a_2, b_2] = [\text{if } a_2 < a_1 \text{ then } -\infty \text{ else } a_1,\ \text{if } b_2 > b_1 \text{ then } +\infty \text{ else } b_1]$$

- Narrowing (improves infinite bounds):

$$\bot \,\Delta\, x = \bot$$
$$x \,\Delta\, \bot = \bot$$
$$[a_1, b_1] \,\Delta\, [a_2, b_2] = [\text{if } a_1 = -\infty \text{ then } a_2 \text{ else } a_1,\ \text{if } b_1 = +\infty \text{ then } b_2 \text{ else } b_1]$$