Lecture 11
Abstract Interpretation on Control-Flow Graphs

Example

k=1; while(k < 100) { k=k+3 }; assert(k <= 255)

k=1; loop {assume(k < 100); k=k+3};
assume(k>=100); assert(k <= 255)

$$r = \{(k,k') \mid (k < 100 \wedge k' = k + 3)\}$$

Approximating sp({1},r*)

post(P) = {1} U sp(P,r) = {1} U {k+3 | k ∈ P, k < 100}

$post^n(\{\})$:
{}, {1}, {1,4}, …, {1,…,97},{1,…,97,100},
{1,…,97,100}

Multiple variables

Wish to track an interval for each variable

We track not [L,U] but ([L1,U1],[L2,U2])

If program state is (x,y), define

$\gamma_2(([L1,U1],[L2,U2])) = \{(x,y) \mid L1 \le x \le U1,\ L2 \le y \le U2\ \}$

$= \gamma_1[L1,U1] \times \gamma_1[L2,U2]$

$\alpha(p) = ([L1,U1],[L2,U2])$

L1 = U1 =

L2 = U2 =

Product of Partial Orders

$(A_i, \leq_i)$ partial orders for $i \in J$

$(A, \leq)$ given by $A = \{f : J \rightarrow \cup_{i \in J} A_i\ , \forall\ i.\ f(i) \in A_i\}$

$f,g \in A$ ordered by

$$f \leq g \Leftrightarrow \forall\ i.\ f(i) \leq_i g(i)$$

example: J={1,2}

Then $(A, \leq)$ is a partial order. Morever:

If $(A_i, \leq_i)$ all have lub, then so does $(A, \leq)$.

If $(A_i, \leq_i)$ all have glb, then so does $(A, \leq)$.

Example: Counter and a Mode

```
mode = 1
x =0
while (-100 < x && x < 100) {
  if (mode == 1) {
    x = x + 10
    mode = 2
  } else {
    x = x - 1
    mode = 1
  }
}
assert(1 <= mode && mode <= 2 && x <= 109)
```

Two Counters

```
x =0
y = 0
while (x < 100) {
  x = x + 1
  y = y + 2
}
assert(y <= 200)
```

Non-relational analysis: tracks each variable separately.
It often loses correlations between them.

Beyond One Loop

- Precise formulation of one-step relation for a CFG
- The form of post in new form: deriving collecting semantics
- Example collecting semantics for a program
- Abstraction of this semantics in example
- Abstract Interpretation Recipe
- Termination of fixpoint computation
- Choatic iteration
- Widening