Formalization of DFA using lattices

1

Recall worklist algorithm

```
let m: map from edge to computed value at edge
let worklist: work list of nodes

for each edge e in CFG do
   m(e) := ∅  ⊥

for each node n do
   worklist.add(n)

while (worklist.empty.not) do
   let n := worklist.remove_any;
   let info_in := m(n.incoming_edges);
   let info_out := F(n, info_in);
   for i := 0 .. info_out.length do
      let new_info := m(n.outgoing_edges[i]) ∪  ⊔
                      info_out[i];
      if (m(n.outgoing_edges[i]) ≠ new_info])
         m(n.outgoing_edges[i]) := new_info;
         worklist.add(n.outgoing_edges[i].dst);
```

2

Using lattices

- We formalize our domain with a powerset lattice
- What should be top and what should be bottom?

3

Using lattices

- We formalize our domain with a powerset lattice
- What should be top and what should be bottom?
- Does it matter?
  - It matters because, as we've seen, there is a notion of approximation, and this notion shows up in the lattice

4

Using lattices

- Unfortunately:
  - dataflow analysis community has picked one direction
  - abstract interpretation community has picked the other
- We will work with the abstract interpretation direction
- Bottom is the most precise (optimistic) answer, Top the most imprecise (conservative)

5

Direction of lattice

- Always safe to go up in the lattice
- Can always set the result to $\top$
- Hard to go down in the lattice
- Bottom will be the empty set in reaching defs

6

Worklist algorithm using lattices

```
let m: map from edge to computed value at edge
let worklist: work list of nodes

for each edge e in CFG do
   m(e) := ⊥

for each node n do
   worklist.add(n)

while (worklist.empty.not) do
   let n := worklist.remove_any;
   let info_in := m(n.incoming_edges);
   let info_out := F(n, info_in);
   for i := 0 .. info_out.length do
      let new_info := m(n.outgoing_edges[i]) ⊔
                           info_out[i];
      if (m(n.outgoing_edges[i]) ≠ new_info])
         m(n.outgoing_edges[i]) := new_info;
         worklist.add(n.outgoing_edges[i].dst);
```

7

Termination of this algorithm?

S = {1, 2}

{1}, {2}

{1}

∅

- For reaching definitions, it terminates...
- Why?
  - lattice is finite
- Can we loosen this requirement?
  - Yes, we only require the lattice to have a finite height
- Height of a lattice: length of the longest ascending or descending chain
- Height of lattice (2^S, ⊆) = |S|

8

Termination of this algorithm?

- For reaching definitions, it terminates...
- Why?
  - lattice is finite
- Can we loosen this requirement?
  - Yes, we only require the lattice to have a finite height
- Height of a lattice: length of the longest ascending or descending chain
- Height of lattice (2^S, ⊆) = | S |

9

Termination

- Still, it's annoying to have to perform a join in the worklist algorithm

```
while (worklist.empty.not) do
   let n := worklist.remove_any;
   let info_in := m(n.incoming_edges);
   let info_out := F(n, info_in);
   for i := 0 .. info_out.length do
      let new_info := m(n.outgoing_edges[i]) ⊔
                           info_out[i];
      if (m(n.outgoing_edges[i]) ≠ new_info])
         m(n.outgoing_edges[i]) := new_info;
         worklist.add(n.outgoing_edges[i].dst);
```

- It would be nice to get rid of it, if there is a property of the flow functions that would allow us to do so

10

Even more formal

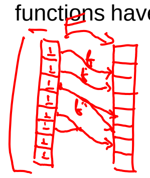
- To reason more formally about termination and precision, we re-express our worklist algorithm mathematically
- We will use fixed points to formalize our algorithm

11

Fixed points

$f(x) = x^2$

- Recall, we are computing m, a map from edges to dataflow information
- Define a global flow function F as follows: F takes a map m as a parameter and returns a new map m', in which individual local flow functions have been applied



$m = F(m)$

12

Fixed points

- We want to find a fixed point of F, that is to say a map m such that m = F(m)
- Approach to doing this?
- Define $\tilde{\bot}$, which is $\bot$ lifted to be a map:
  $\tilde{\bot} = \lambda e.\ \bot$
- Compute F($\tilde{\bot}$), then F(F($\tilde{\bot}$)), then F(F(F($\tilde{\bot}$))), ... until the result doesn't change anymore

13

Fixed points

- Formally:
  $$Soln = \bigsqcup_{i=0}^{\infty} F^i(\tilde{\bot})$$
- Outer join has same role here as in worklist algorithm: guarantee that results keep increasing
- BUT: if the sequence $F^i(\tilde{\bot})$ for i = 0, 1, 2 ... is increasing, we can get rid of the outer join!
- How? Require that F be monotonic:
  - $\forall$ a, b . a $\sqsubseteq$ b $\Rightarrow$ F(a) $\sqsubseteq$ F(b)

14

Fixed points

$$\tilde{\bot} \sqsubseteq F(\tilde{\bot})$$
$$F(\tilde{\bot}) \sqsubseteq FF(\tilde{\bot})$$
$$FF(\tilde{\bot}) \sqsubseteq FFF(\tilde{\bot})$$

15

Fixed points

$$\tilde{\bot} \sqsubseteq F(\tilde{\bot})$$
$$F(\tilde{\bot}) \sqsubseteq F(F(\tilde{\bot}))$$
$$F^k(\tilde{\bot}) \sqsubseteq F^{k+1}(\tilde{\bot})$$
$$F^{k+1}(\tilde{\bot}) \sqsubseteq F^{k+2}(\tilde{\bot})$$

16

Back to termination

- So if F is monotonic, we have what we want: finite height $\Rightarrow$ termination, without the outer join
- Also, if the local flow functions are monotonic, then global flow function F is monotonic

17

Another benefit of monotonicity

- Suppose Marsians came to earth, and miraculously give you a fixed point of F, call it fp.
- Then:

$$\tilde{\bot} \sqsubseteq fp$$
$$F(\tilde{\bot}) \sqsubseteq fp$$
$$FF(\tilde{\bot}) \sqsubseteq fp$$
$$ofp \sqsubseteq fp$$

18

Another benefit of monotonicity

- Suppose Marsians came to earth, and miraculously give you a fixed point of F, call it fp.
- Then:

$$\tilde{I} \sqsubseteq fp$$
$$F(\tilde{I}) \sqsubseteq F(fp)$$
$$F(\tilde{I}) \sqsubseteq fp$$
$$F^2(\tilde{I}) \sqsubseteq fp$$
$$\vdots$$
$$lfp \sqsubseteq fp$$

19

Another benefit of monotonicity

- We are computing the least fixed point...

20

Recap

- Let's do a recap of what we've seen so far
- Started with worklist algorithm for reaching definitions

21

Worklist algorithm for reaching defns

```
let m: map from edge to computed value at edge
let worklist: work list of nodes

for each edge e in CFG do
   m(e) := ∅

for each node n do
   worklist.add(n)

while (worklist.empty.not) do
   let n := worklist.remove_any;
   let info_in := m(n.incoming_edges);
   let info_out := F(n, info_in);
   for i := 0 .. info_out.length do
      let new_info := m(n.outgoing_edges[i]) ∪
                      info_out[i];
      if (m(n.outgoing_edges[i]) ≠ new_info])
         m(n.outgoing_edges[i]) := new_info;
         worklist.add(n.outgoing_edges[i].dst);
```

22

Generalized algorithm using lattices

```
let m: map from edge to computed value at edge
let worklist: work list of nodes

for each edge e in CFG do
   m(e) := ⊥

for each node n do
   worklist.add(n)

while (worklist.empty.not) do
   let n := worklist.remove_any;
   let info_in := m(n.incoming_edges);
   let info_out := F(n, info_in);
   for i := 0 .. info_out.length do
      let new_info := m(n.outgoing_edges[i]) ⊔
                      info_out[i];
      if (m(n.outgoing_edges[i]) ≠ new_info])
         m(n.outgoing_edges[i]) := new_info;
         worklist.add(n.outgoing_edges[i].dst);
```

23

Next step: removed outer join

- Wanted to remove the outer join, while still providing termination guarantee
- To do this, we re-expressed our algorithm more formally
- We first defined a "global" flow function F, and then expressed our algorithm as a fixed point computation

24

Guarantees

- If F is monotonic, don't need outer join
- If F is monotonic and height of lattice is finite: iterative algorithm terminates
- If F is monotonic, the fixed point we find is the least fixed point.

25

What about if we start at top?

- What if we start with $\tilde{\top}$: $F(\tilde{\top})$, $F(F(\tilde{\top}))$, $F(F(F(\tilde{\top})))$

26

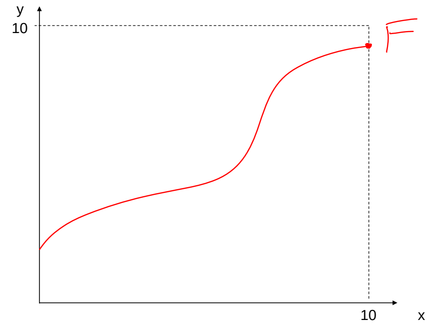
What about if we start at top?

- What if we start with $\tilde{\top}$: $F(\tilde{\top})$, $F(F(\tilde{\top}))$, $F(F(F(\tilde{\top})))$
- We get the greatest fixed point
- Why do we prefer the least fixed point?
  - More precise

27

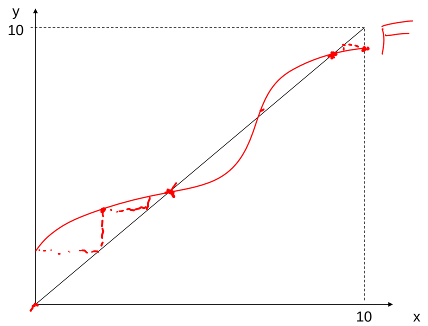
$a \sqsubseteq b \Rightarrow F(a) \sqsubseteq F(b)$

Graphically



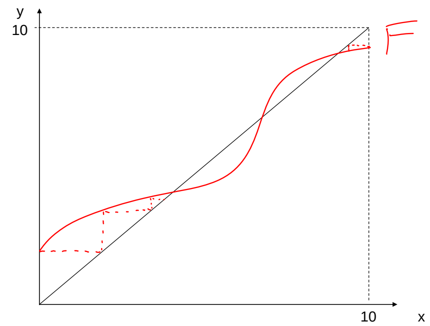
28

Graphically



29

Graphically



30

Graphically, another way

31