Week 1.2

Thursday, January 11, 2024 4:22 PM

dataflow analysis (DFA)

- replace concrete values w/ abstract values
- replace concrete semantics w/ abstract semantics
- "execute" the program on abstract using abstract semantics

DFA = abstract values + abstract semantics + abstract execution

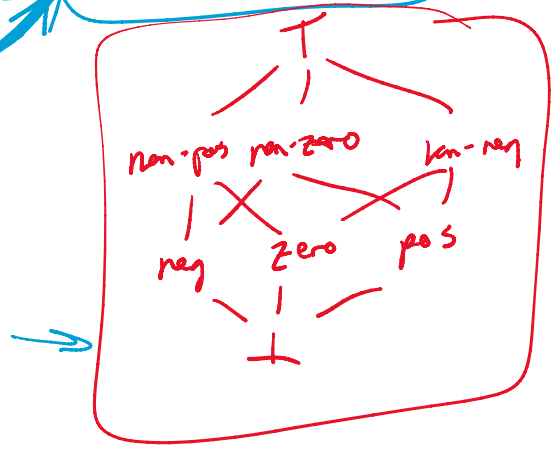
---

Sign analysis (+, −, ∅)

abstract domain

abstract values

- pos : $\{ n \mid n > 0 \}$
- neg : $\{ n \mid n < 0 \}$
- zero : $\{ 0 \}$
- $\bot$ (bottom) : $\{\}$
- $\top$ (top) : $\mathbb{Z}$



abstract semantics

zero + zero = zero

zero + pos = pos

⋮

pos + pos = pos

pos + neg = ⊤

⋮

```
x = input(∅, 100)        x ← T
if x > ∅ {               x ← pos
    y = x * x            y ← pos
    z = 1 / y            z ← T
}
else {                   x ← T
    y = x - x            y ← ∅
    z = 1 / y            z ← ⊥
}
```

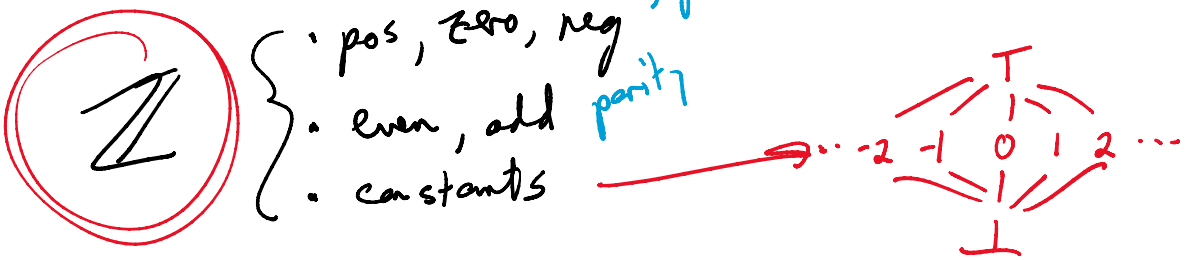
control-flow graph (CFG)

CFG is a graph w/ nodes being "basic blocks" & edges representing possible control flow between blocks

basic block = a linear sequence of instructions that can only entered at the beginning and exited at the end

DFA = abstract domain + abstract Semantics + abstract execution

sign



- the abstract domain
  - determines what answers your analysis can provide
  - also what precision it can give

abstract domain = sign × parity

(+, e)

$$\alpha : \mathbb{Z} \to \mathbb{Z}^{\#}$$

$$\gamma : \mathbb{Z}^{\#} \to \mathcal{P}(\mathbb{Z})$$

sign

$$\alpha(x) = \begin{cases} \text{pos} & \text{if } x > \emptyset \\ \text{zero} & \text{if } x = \emptyset \\ \text{neg} & \text{if } x < \emptyset \end{cases}$$

$$\gamma(\hat{x}) = \begin{cases} \{n \mid n > \emptyset\} & \text{if } \hat{x} = \text{pos} \\ \{\emptyset\} & \text{if } \hat{x} = \text{zero} \\ \{n \mid n < \emptyset\} & \text{if } \hat{x} = \text{neg} \end{cases}$$

$$x \in \gamma(\alpha(x))$$

$$\gamma(\underbrace{\alpha(1)}_{\text{pos}}) = \{n \mid n > \emptyset\}$$

$U(\alpha(b)) = \{n \mid n > 0\}$

pos

abstract semantics (abstract transfer functions)

+	⊥	pos	zero	neg	⊤
⊥	⊥	⊥	⊥	⊥	⊥
pos	⊥	pos	pos	⊤	⊤
zero	⊥	pos	zero	neg	⊤
neg	⊥	⊤	neg	neg	⊤
⊤	⊥	⊤	⊤	⊤	⊤

<	⊥	pos	zero	neg	⊤
⊥	⊥	⊥	⊥	⊥	⊥
pos	⊥	⊤	zero	zero	⊤
zero	⊥	pos	zero	zero	⊤
neg	⊥	pos	pos	⊤	⊤
⊤	⊥	⊤	⊤	⊤	⊤