Bytecode

Program $P ::= I^*$

Instr $I ::= p = rv \mid \text{goto } i \mid \text{if } p \text{ goto } i_1 \text{ else } i_2$

Place $p ::= x$ Rvalue $rv ::= c \mid p \mid p_1 \oplus p_2$

w = 0

1: x = 1
2: y = (x = w)
3: if y goto 4 else 5
4: z = y + x
5: z = y

given a program P,
find all instructions $p_1 = p_2 / p_3$
where p_3 could be zero

x = 1
y = x = 0
if y goto 4 else 5
z = y + x   z = y

Flow-sensitivity:

abstract state changes
line-by-line

x = 0 $x \in \sigma$
y = 1
x = 2 $x \notin \sigma$
z = x $x \in \sigma \Rightarrow z \in \sigma$
w = y / z $z \in \sigma$?

x = 0
...
y = 0   y = 1
w = x / y

state σ set of zero variables

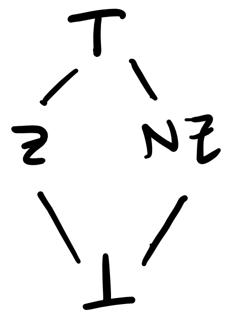
x = 0 $x \in \sigma$
y = 1
z = x $x \in \sigma \Rightarrow z \in \sigma$
w = y / z $z \in \sigma$?

Lattices

unknown

Z or NZ

$SI = \{Z, NZ, \bot, \top\}$ $\qquad Z \sqsupset \bot \qquad \le \; < \qquad \sqsubset \; \sqsubseteq$



$\bot \sqsubset Z$

$\bot \sqsubset NZ$

$\bot \sqsubseteq \bot$

$Z \sqsubseteq Z$

$Z \sqsubset \top$

$Z \not\sqsubseteq NZ$

$Z \not\sqsubset NZ$

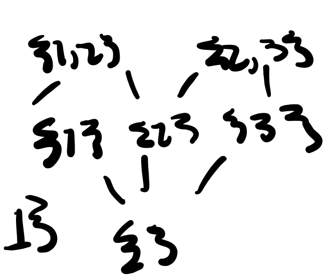
$\bot \sqcup \bot = \bot$

$\bot \sqcup Z = Z$

$Z \sqcup NZ = \top$

$\sqcup$ = set union ($\cup$)

$\{1,2\} \sqcup \{2,3\} = \{1,2,3\}$



$\sqsubset$ = strict subset ($\subset$)

$\sqsubseteq$ = subset ($\subseteq$)

$\{x \mapsto \bot, y \mapsto \bot, z \mapsto \bot\}$

$x = 0$	$\{x \mapsto Z\}$
$y = 1$	$\{x \mapsto Z, y \mapsto NZ\}$
$z = x$	$\{x \mapsto Z, y \mapsto NZ, z \mapsto Z\}$
$w = y/z$	

Transfer function

$F : \text{Instr} \to \text{Domain} \to \text{Domain}$

$F(I, \sigma) = \text{match } I$

$x = 0 \Rightarrow \sigma[x \mapsto Z]$

$x = c \text{ if } c \mathrel{!}= 0$

$\Rightarrow \sigma[x \mapsto NZ]$

$x = p_1 \oplus p_2$

$\Rightarrow \sigma[x \mapsto \sigma[x] \sqcup Z]$

$x = y \Rightarrow \sigma[x \mapsto \sigma[y]]$

$\_ \Rightarrow \sigma$

$\sigma_{start} \to \sigma_1^{in} \to \boxed{x = 10} \to \sigma_1^{out} \to \sigma_2^{in} \to \boxed{\text{if } x == -1 \ \ldots} \to \sigma_2^{out}$

$\sigma_3^{in} \to \boxed{y = 1/x} \to \sigma_3^{out} \to \sigma_4^{in} \to \boxed{x = x-1} \to \sigma_4^{out} \to \sigma_5^{in} \to \boxed{\text{goto}} \to \sigma_5^{out}$

$$\sigma_2^{out} = f(P_2, \sigma_2^{in})$$

$$\sigma_3^{in} = \bigsqcup_{j \in \{2\}} \sigma_j^{out}$$

$$\vdots$$

$$\sigma_5^{out} = f(P_5, \sigma_5^{in})$$

$$\sigma_2^{in} = \sigma_5^{out} \sqcup \sigma_1^{out}$$

$$\sigma_{start} = \{* \mapsto \bot\}$$

$$\sigma_1^{in} = \sigma_{start}$$

$$\sigma_1^{out} = \{x \mapsto NZ, * \mapsto \bot\}$$

$$\sigma_2^{in} = \sigma_1^{out} \sqcup \sigma_5^{out}$$

$$\{x \mapsto NZ, * \mapsto \bot\}$$

$$\sigma_2^{out} = \sigma_2^{in}$$

$$\sigma_3^{in} = \sigma_2^{out}$$

$$\sigma_3^{out} = \{x \mapsto NZ, y \mapsto Z\}$$

$$\sigma_4^{in} = \sigma_3^{out}$$

$$\sigma_4^{out} = \{x \mapsto Z, y \mapsto Z\}$$

$$\sigma_5^{in} = \sigma_4^{out}$$

$$\sigma_5^{out} = \sigma_5^{in}$$

$$\sigma_2^{in} = \underset{\{x \mapsto NZ\}}{\underset{\uparrow}{\sigma_1^{out}}} \sqcup \underset{\{x \mapsto Z,\ y \mapsto Z\}}{\underset{\uparrow}{\sigma_5^{out}}} = \{x \mapsto \top, y \mapsto Z\}$$

$$\sigma_i^{in} = \bigsqcup_{j \in pred(i)} \sigma_j^{out}$$

$$\sigma_i^{out} = f(P_i, \sigma_i^{in}$$