Synthesis, Analysis, and Verification

Lecture 09a

Abstract Interpretation

Lectures:

Viktor Kuncak

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Abstract Interpretation

Way to infer properties of e.g. computations

Consider assignment: z = x+y

Interpreter:

$$\begin{pmatrix} x : 10 \\ y : -2 \\ z : 3 \end{pmatrix} \xrightarrow{z = x+y} \begin{pmatrix} x : 10 \\ y : -2 \\ z : 8 \end{pmatrix}$$

Abstract interpreter:

$$\begin{pmatrix} x \in [0,10] \\ y \in [-5,5] \\ z \in [0,10] \end{pmatrix}^{\in A} \xrightarrow{z = x+y} \begin{pmatrix} x \in [0,10] \\ y \in [-5,5] \\ z \in [-5,15] \end{pmatrix}$$

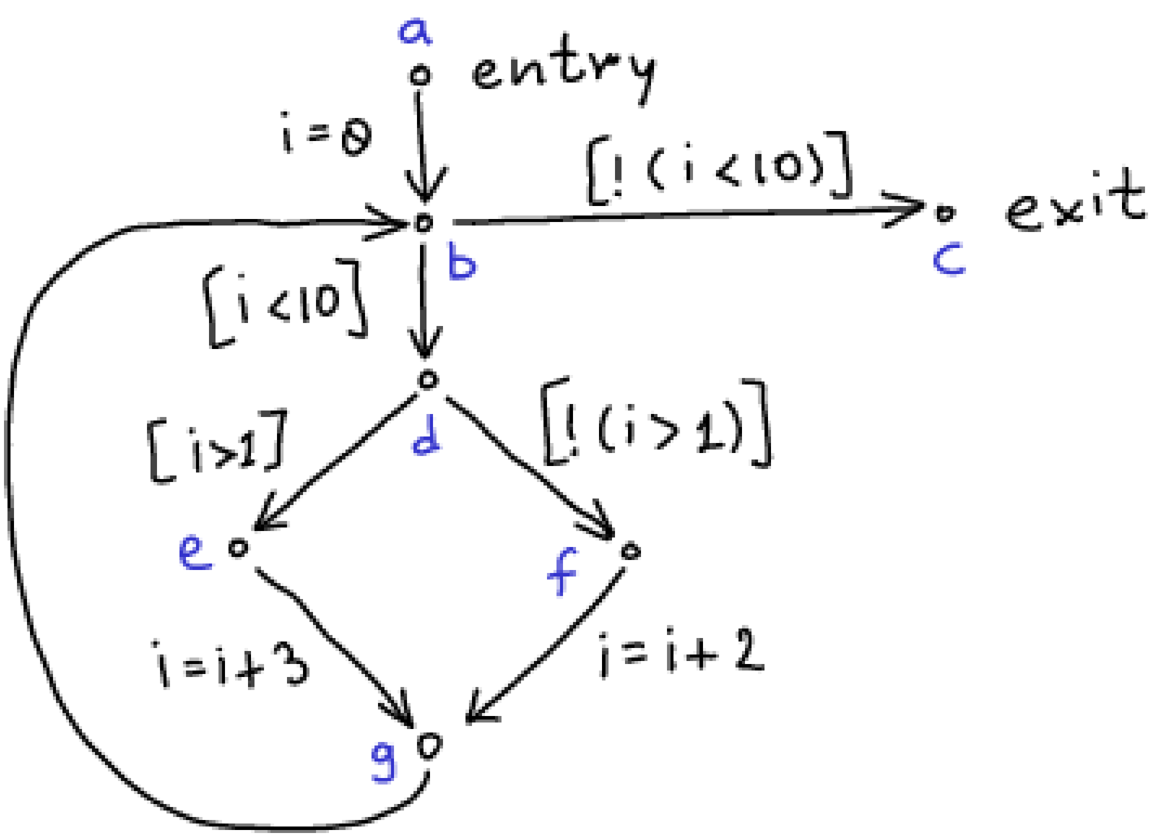
Adding and Multiplying Intervals

$$\begin{pmatrix} x \in [a_x, b_x] \\ y \in [a_y, b_y] \\ z \in \ldots \end{pmatrix} \xrightarrow{z = x + y} \begin{pmatrix} x \in [a_x, b_x] \\ y \in [a_y, b_y] \\ z \in [a_x + a_y, \; b_x + b_y] \end{pmatrix}$$

$$\begin{pmatrix} x \in [a_x, b_x] \\ y \in [a_y, b_y] \\ z \in \ldots \end{pmatrix} \xrightarrow{z = x * y} \begin{pmatrix} x \in [a_x, b_x] \\ y \in [a_y, b_y] \\ z \in [a_x * a_y, \; b_x * b_y] \quad a_x, a_y, b_x, b_y > 0 \\ B = \{a_x \cdot a_y, a_x \cdot b_y, b_x \cdot a_y, b_x \cdot b_y\} \\ z \in [\min(B), \max(B)] \end{pmatrix}$$

Programs as Control-Flow Graphs

a
i = 0;
while b (i < 10) {
d
 if (i > 1)
e
  i = i + 3;
 else
f
  i = i + 2;
g
}



- Suppose
  - program state given only by the value of i
  - initially, it is possible that i has any value
- Task: for each point, find set S of possible states

$S(a) = \{\ldots,-2,-1,0,1,2,3,\ldots\} = \mathbb{Z}$

$S(b) = \{0,$

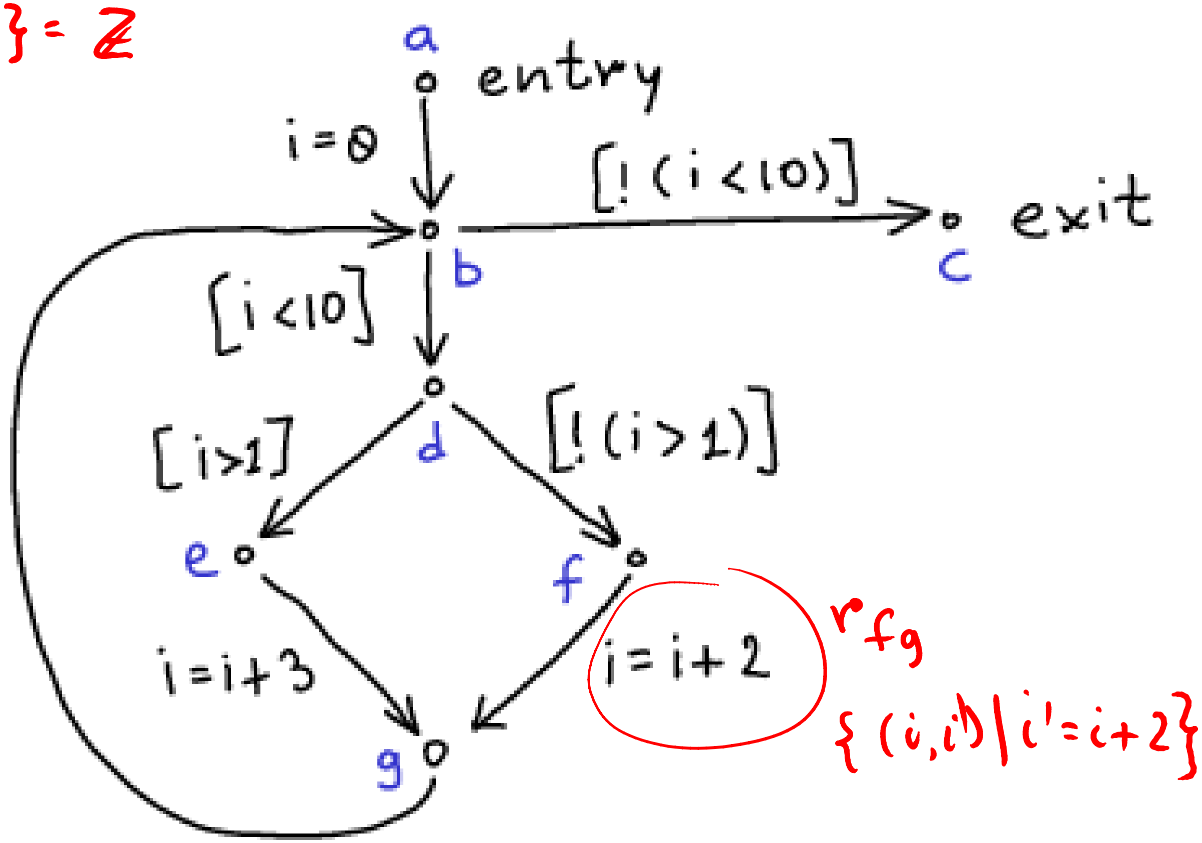
$S(d) = \{0,$

$S(e) = \{$

$S(f) = \{0$

$S(g) = \{2$

$S(c) = \{$



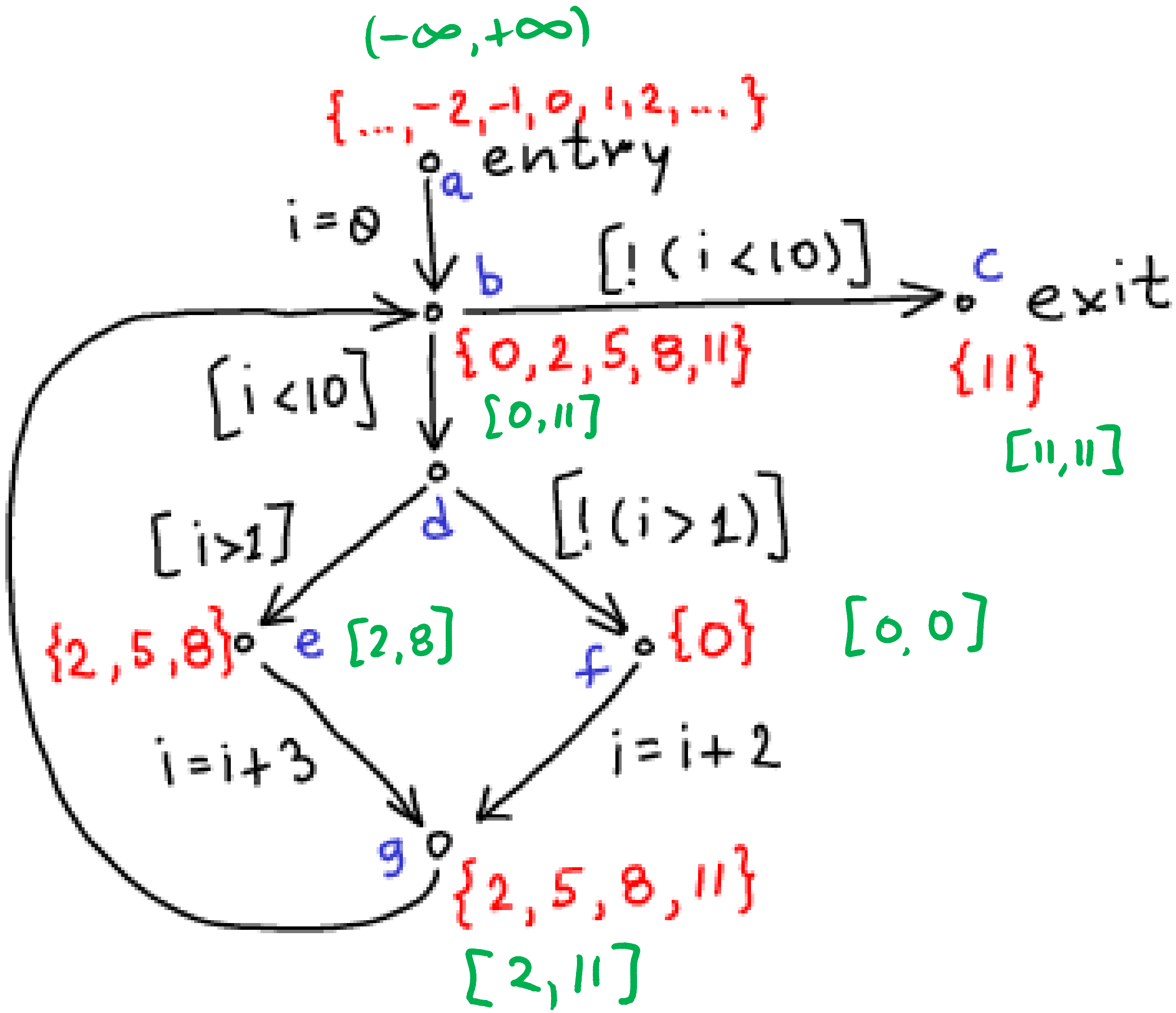
$S(g) = S(f) \circ r_{fg}$

$\quad\quad\;\; S(e) \circ r_{eg}$

$S(d) = \{0, 2, 5, 8\}$

$S^{\#}(d) = [0, 8]$

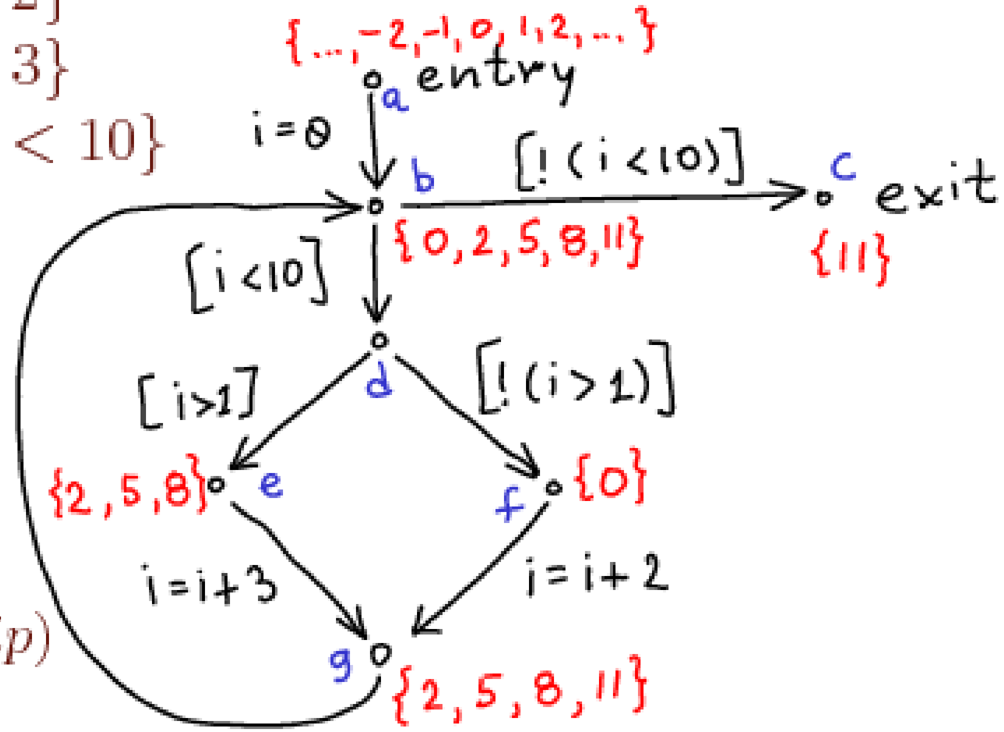
```
i = 0;
while (i < 10) {
  if (i > 1)
    i = i + 3;
  else
    i = i + 2;
}
```



Sets are Given by Equations

$R(i = 0) = \{(i, i') \mid i' = 0\}$
$R(i = i + 2) = \{(i, i') \mid i' = i + 2\}$
$R(i = i + 3) = \{(i, i') \mid i' = i + 3\}$
$R([i < 10]) = \{(i, i') \mid i' = i \wedge i < 10\}$

$T(S, r) = sp(S, r) = S \circ r$



$S(a) = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$
$S(b) = T(S(a), i = 0) \cup T(S(g), skip)$
$S(c) = T(S(b), [\neg(i < 10)])$
$S(d) = T(S(b), [i < 10])$
$S(e) = T(S(d), [i > 1])$
$S(f) = T(S(d), [\neg(i > 1)])$
$S(g) = T(S(e), i = i + 3) \cup T(S(f), i = i + 2)$

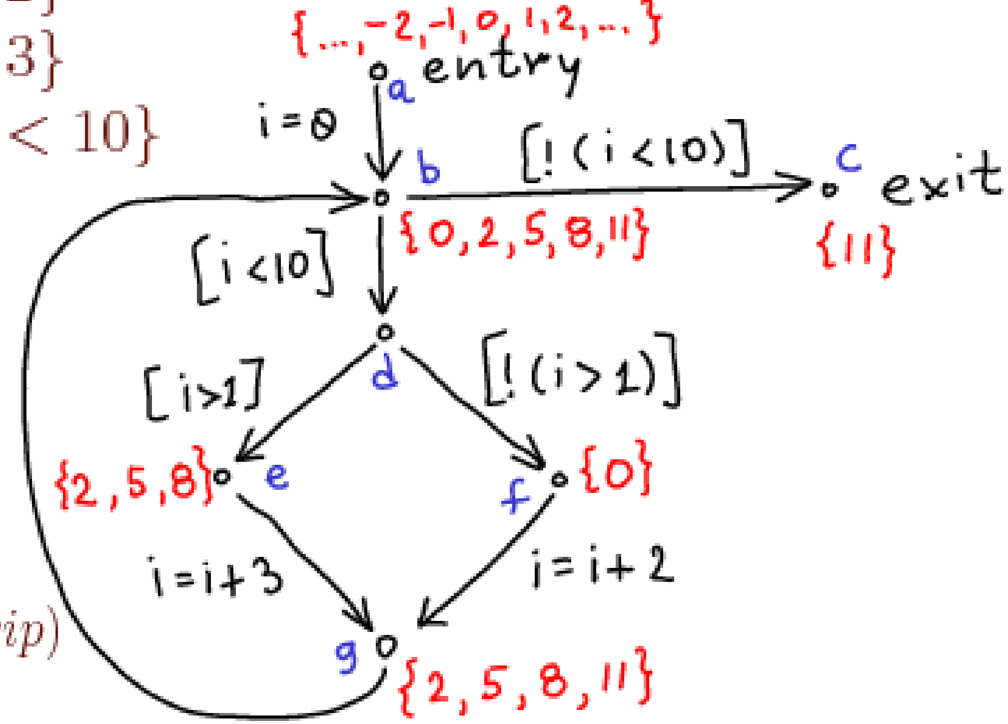
Sets are Given by Equations

$$R(i = 0) = \{(i, i') \mid i' = 0\}$$
$$R(i = i + 2) = \{(i, i') \mid i' = i + 2\}$$
$$R(i = i + 3) = \{(i, i') \mid i' = i + 3\}$$
$$R([i < 10]) = \{(i, i') \mid i' = i \wedge i < 10\}$$

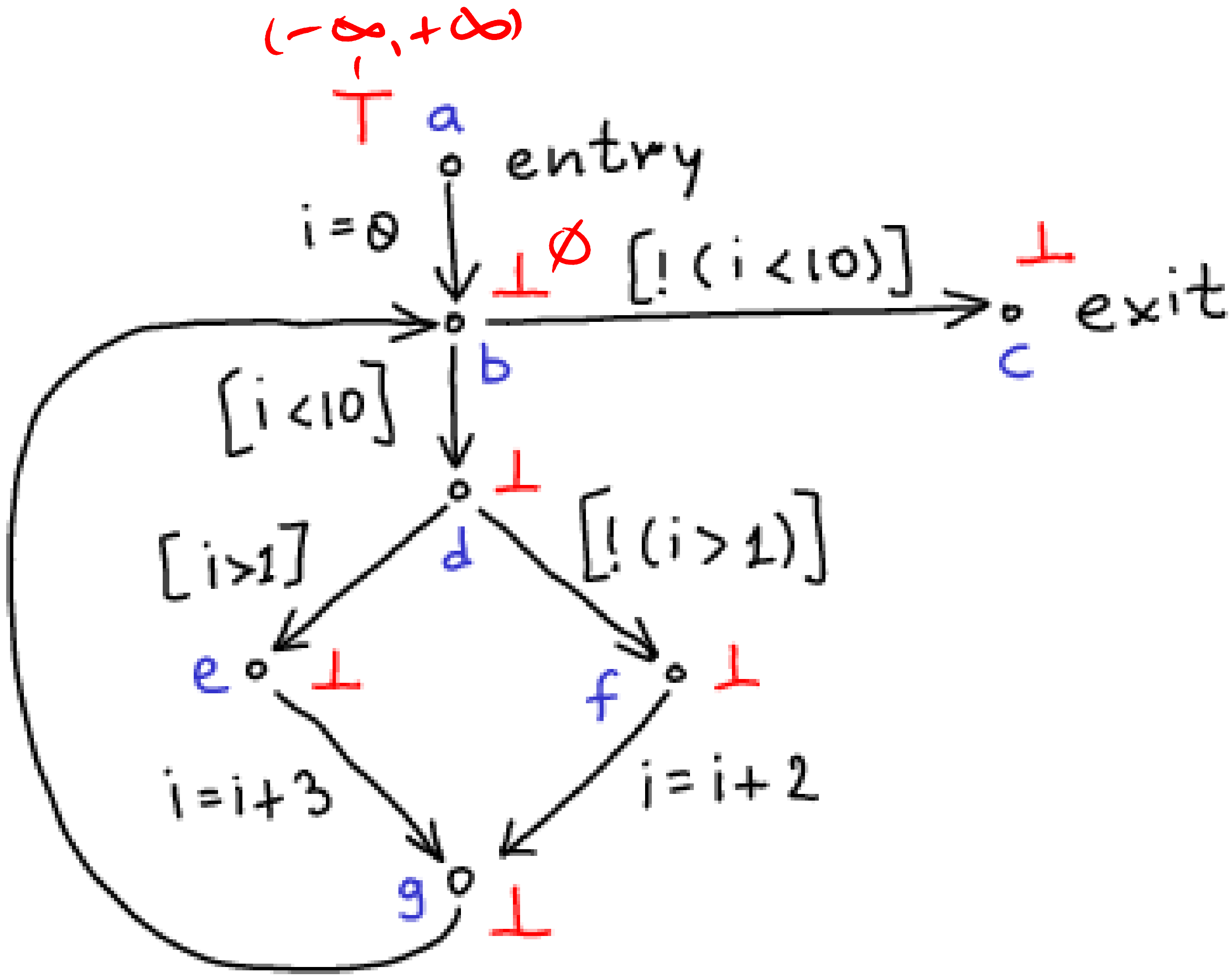
$T(S, r) = sp(S, r) = S \circ r$

$T^{\#}(S^{\#}, r) = sp^{\#}(S^{\#}, r) \supseteq sp(S, r)$

safe approximation



$$S^{\#}(a) = \top$$
$$S^{\#}(b) = T^{\#}(S^{\#}(a), i = 0) \sqcup T(S(g), skip)$$
$$S^{\#}(c) = T^{\#}(S^{\#}(b), [\neg(i < 10)])$$
$$S^{\#}(d) = T^{\#}(S^{\#}(b), [i < 10])$$
$$S^{\#}(e) = T^{\#}(S^{\#}(d), [i > 1])$$
$$S^{\#}(f) = T^{\#}(S^{\#}(d), [\neg(i > 1)])$$
$$S^{\#}(g) = T^{\#}(S^{\#}(e), i = i + 3) \sqcup T(S(f), i = i + 2)$$



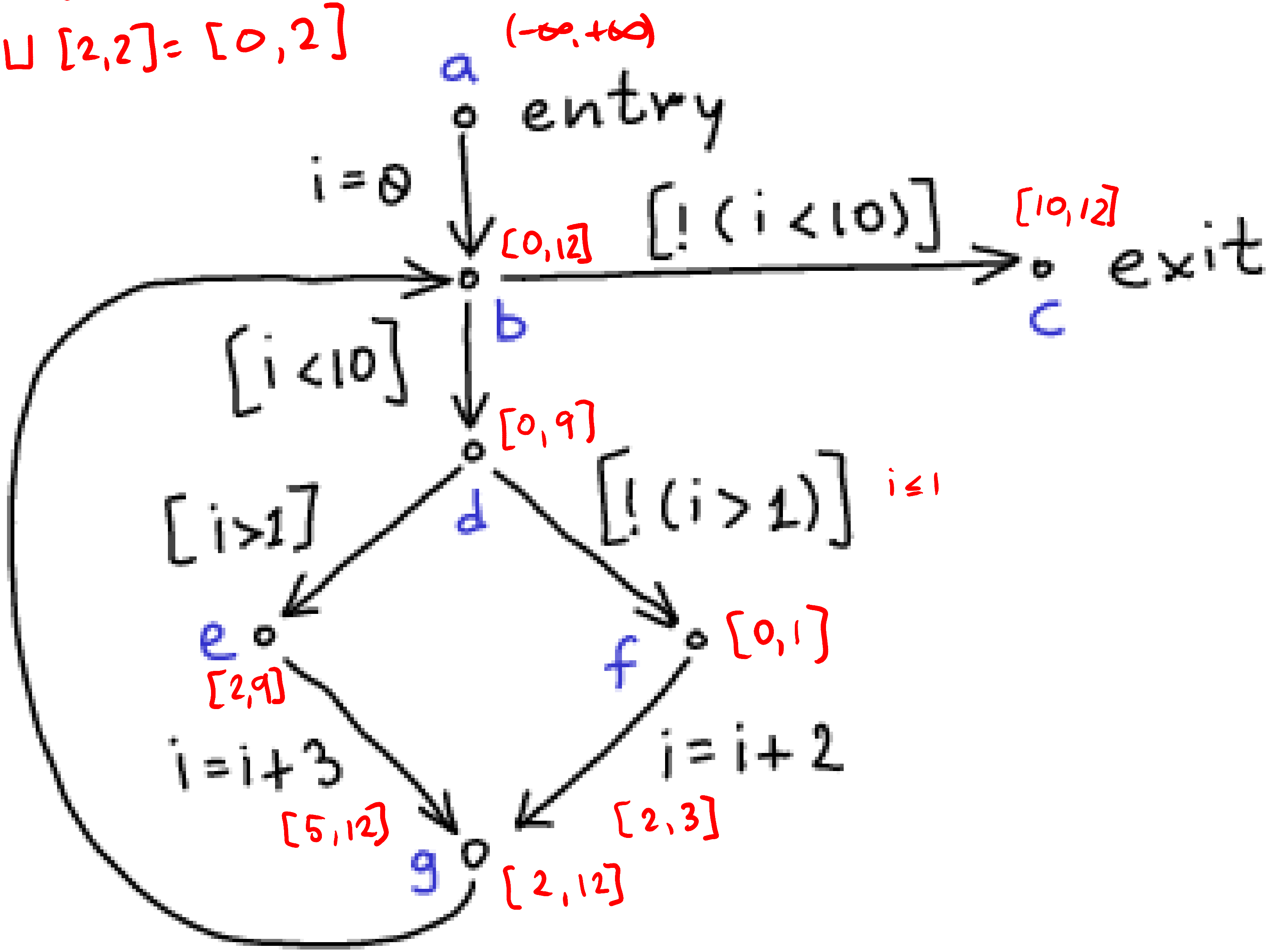
(-∞,+∞)
⊤
a
entry
i=0
⊥
∅
[!(i<10)]
⊥
exit
b
c
[i<10]
⊥
d
[i>1]
[!(i>1)]
e
⊥
f
⊥
i=i+3
i=i+2
g
⊥

grow the intervals

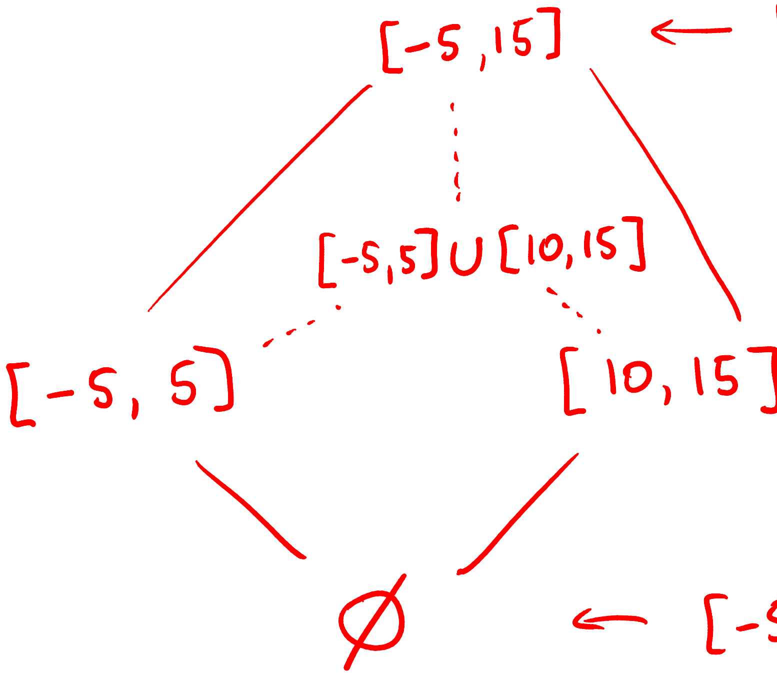
$S^{\#}(f) . r_{fg} \subseteq S^{\#}(g)$

$[0,0] \cup [2,2] = \{0,2\}$

$[0,0] \sqcup [2,2] = [0,2]$



Approximation of Sets by Supersets



$\leftarrow [-5,5] \sqcup [10,15]$

Least Upper Bound

LUB

supremum

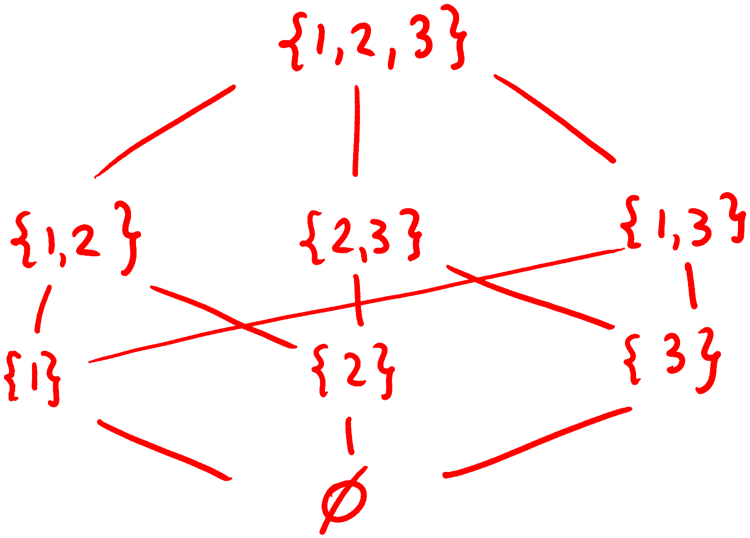
sup

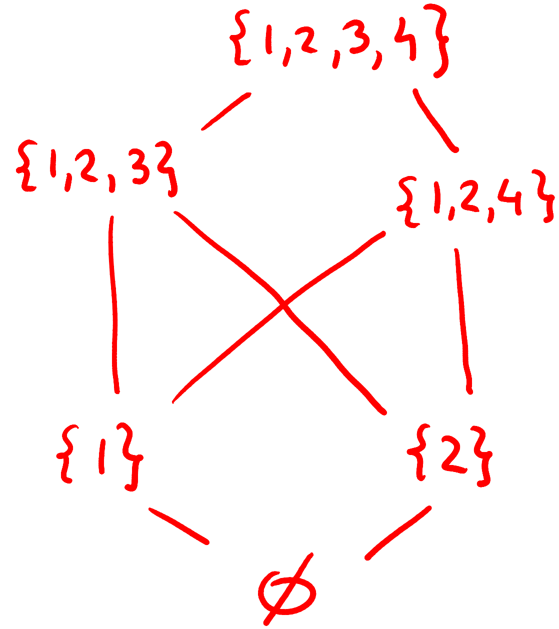
Best approximation of union that we have in our current lattice

$\leftarrow [-5,5] \sqcap [10,15]$

Partially Ordered Families of Sets

$\subseteq$



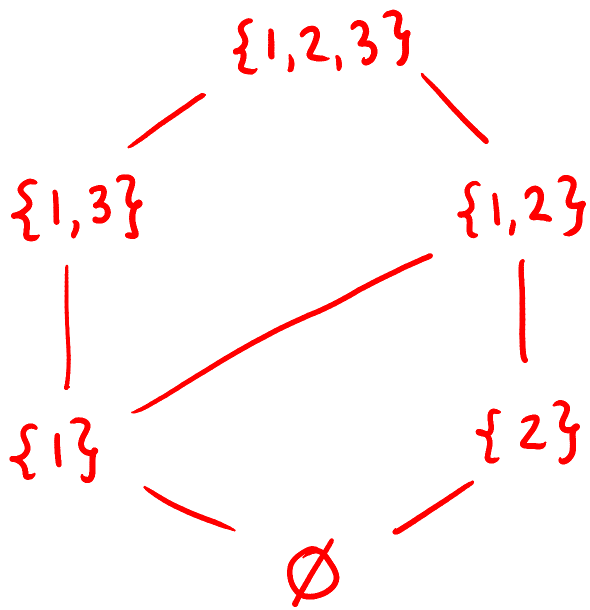


$\{1\} \sqcup \{2\} = \{1,2\}$

$\{1\} \sqcup \{2\} =$ does not exist

not a lattice

Does every element in this order have least upper bound?



yes, this is SEMI-lattice, $\sqcup$ exist

Dually, does it have **greatest lower bound**? yes, IT IS LATTICE