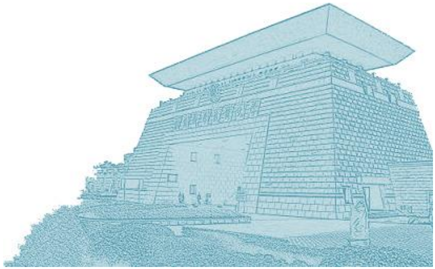
抽象解释
及其在静态分析中的应用

陈立前

国防科技大学



目录

- 一、抽象解释概述
- 二、抽象解释理论的数学基础
- 三、具体语义下的静态分析
- 四、抽象语义下的静态分析
- 五、基于抽象解释的静态分析工具

简单数值程序的语法

Arithmetic expressions:

$$
\begin{array}{lcll}
\texttt{exp} & ::= & \texttt{V} & \text{variable } \texttt{V} \in \mathbb{V} \\
 & | & -\texttt{exp} & \text{negation} \\
 & | & \texttt{exp} \diamond \texttt{exp} & \text{binary operation: } \diamond \in \{+,-,\times,/\} \\
 & | & [c, c'] & \text{constant range, } c, c' \in \mathbb{I} \cup \{\pm\infty\} \\
 & & & (c \text{ is a shorthand for } [c, c])
\end{array}
$$

Commands:

$$
\begin{array}{lcll}
\texttt{com} & ::= & \texttt{V := exp} & \text{assignment into } \texttt{V} \in \mathbb{V} \\
 & | & \texttt{exp} \bowtie 0 & \text{test, } \bowtie \in \{=,<,>,\leq,\geq,\neq\}
\end{array}
$$

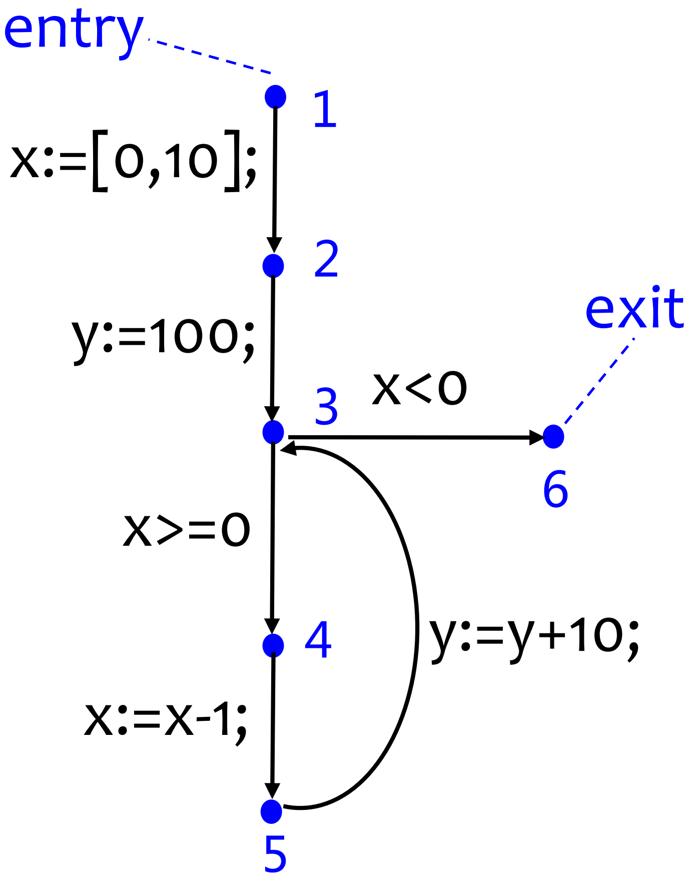
programs: control-flow graphs

$$
P \stackrel{\text{def}}{=} (L, e, A) \quad \left| \quad
\begin{array}{ll}
L & \text{program points (labels)} \\
e & \text{entry point: } e \in L \\
A & \text{arcs: } A \subseteq L \times \texttt{com} \times L
\end{array}\right.
$$

程序示例

```
1 x:=[0,10];
2 y:=100;
3 while ( x>=0)  do
4    x:=x-1;
5    y:=y+10;
  done 6
```

结构化的程序



控制流图

具体语义

- 表达式的具体语义

$$\mathrm{E}\llbracket e \rrbracket : \underbrace{(\mathbb{V} \to \mathbb{I})}_{\text{一个状态 } \rho \in \mathbb{V} \to I} \to \underbrace{\mathcal{P}}_{\text{值的集合}}(\mathbb{I}) \quad \text{where} \quad \underbrace{\mathbb{I} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}\}}_{\text{数据类型}}$$

$$\begin{array}{lcl}
\mathrm{E}\llbracket [c, c'] \rrbracket \rho & \overset{\text{def}}{=} & \{ x \in \mathbb{I} \mid c \leq x \leq c' \} \\
\mathrm{E}\llbracket \mathtt{V} \rrbracket \rho & \overset{\text{def}}{=} & \{ \rho(\mathtt{V}) \} \\
\mathrm{E}\llbracket - e \rrbracket \rho & \overset{\text{def}}{=} & \{ -v \mid v \in \mathrm{E}\llbracket e \rrbracket \rho \} \\
\mathrm{E}\llbracket e_1 + e_2 \rrbracket \rho & \overset{\text{def}}{=} & \{ v_1 + v_2 \mid v_1 \in \mathrm{E}\llbracket e_1 \rrbracket \rho, v_2 \in \mathrm{E}\llbracket e_2 \rrbracket \rho \} \\
\mathrm{E}\llbracket e_1 - e_2 \rrbracket \rho & \overset{\text{def}}{=} & \{ v_1 - v_2 \mid v_1 \in \mathrm{E}\llbracket e_1 \rrbracket \rho, v_2 \in \mathrm{E}\llbracket e_2 \rrbracket \rho \} \\
\mathrm{E}\llbracket e_1 \times e_2 \rrbracket \rho & \overset{\text{def}}{=} & \{ v_1 \times v_2 \mid v_1 \in \mathrm{E}\llbracket e_1 \rrbracket \rho, v_2 \in \mathrm{E}\llbracket e_2 \rrbracket \rho \} \\
\mathrm{E}\llbracket e_1 / e_2 \rrbracket \rho & \overset{\text{def}}{=} & \{ v_1 / v_2 \mid v_1 \in \mathrm{E}\llbracket e_1 \rrbracket \rho, v_2 \in \mathrm{E}\llbracket e_2 \rrbracket \rho,\ v_2 \neq 0 \}
\end{array}$$

具体语义

- 语句的具体语义

$$\mathsf{C}[\![\, c \,]\!] : \underline{\mathcal{D}} \to \underline{\mathcal{D}} \text{ where } \mathcal{D} \overset{\text{def}}{=} \mathcal{P}(\mathbb{V} \to \mathbb{I})$$

语句c的迁移函数　语句c执行前的状态　语句c执行后的状态

$$\begin{aligned}
\mathsf{C}[\![\, \mathtt{V} := e \,]\!]\mathcal{X} &\overset{\text{def}}{=} \{\, \rho[\, \mathtt{V} \mapsto v \,] \mid \rho \in \mathcal{X},\ v \in \mathsf{E}[\![\, e \,]\!]\rho \,\} \\
\mathsf{C}[\![\, e \bowtie 0 \,]\!]\mathcal{X} &\overset{\text{def}}{=} \{\, \rho \mid \rho \in \mathcal{X},\ \exists v \in \mathsf{E}[\![\, e \,]\!]\rho \colon v \bowtie 0 \,\}
\end{aligned}$$

条件测试语句：过滤一些环境

赋值语句：更新变量的值

具体语义

- 程序的具体语义（聚集语义）

$$\mathrm{P}[\![(L, e, A)]\!] : \underline{L} \rightarrow \underline{\mathcal{D}} \quad \text{where} \quad \mathcal{D} \overset{\text{def}}{=} \mathcal{P}(\mathbb{V} \rightarrow \mathbb{I})$$

程序点　　状态的集合

$\mathrm{P}[\![(L, e, A)]\!]\ell$ 是程序点 $\ell \in L$ 处最精确的不变式

也是如下递归方程系统的最小解

语义方程系统

$$\boxed{\begin{array}{lcl} \mathcal{X}_e & & \\ \mathcal{X}_{\ell \neq e} & = & \displaystyle\bigcup_{(\ell', c, \ell) \in A} \mathrm{C}[\![c]\!] \mathcal{X}_{\ell'} \end{array}}$$

给定的初始状态

迁移函数

具体语义

- 程序的具体语义（聚集语义）

$\mathsf{P}[\![(L, e, A)]\!] : L \to \mathcal{D}$ where $\mathcal{D} \stackrel{\text{def}}{=} \mathcal{P}(\mathbb{V} \to \mathbb{I})$

语义方程系统

$$\begin{array}{lcl} \mathcal{X}_e & & \\ \mathcal{X}_{\ell \neq e} & = & \displaystyle\bigcup_{(\ell', c, \ell) \in A} \mathsf{C}[\![c]\!] \mathcal{X}_{\ell'} \end{array}$$

给定的初始状态

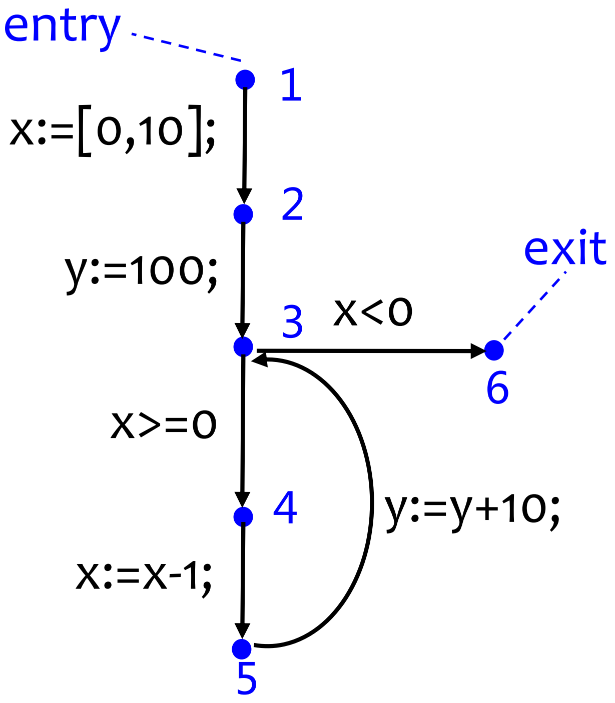
迁移函数

- $(\mathcal{D}, \subseteq, \cup, \cap, \emptyset, (\mathbb{V} \to \mathbb{I}))$ 是完全格
- $M_\ell : \mathcal{X}_\ell \mapsto \displaystyle\bigcup_{(\ell', c, \ell) \in A} \mathsf{C}[\![c]\!] \mathcal{X}_{\ell'}$ 是D上的单调函数

根据Tarski定理，函数 M_ℓ 的最小不动点存在且唯一 $\forall \ell$: $M_\ell(\mathcal{X}_\ell) = \mathcal{X}_\ell$

具体语义—示例

```
1 x:=[0,10];
2 y:=100;
3 while ( x>=0) do
4    x:=x-1;
5     y:=y+10;
   done 6
```



控制流图

$$
\left\{
\begin{aligned}
\mathcal{X}_1 &= (\{\,\mathtt{X},\mathtt{Y}\,\} \to \mathbb{Z}) \\
\mathcal{X}_2 &= \mathsf{C}\llbracket\, \mathtt{X} := [0,10] \,\rrbracket\, \mathcal{X}_1 \\
\mathcal{X}_3 &= \mathsf{C}\llbracket\, \mathtt{Y} := 100 \,\rrbracket\, \mathcal{X}_2 \cup \\
&\quad\ \mathsf{C}\llbracket\, \mathtt{Y} := \mathtt{Y} + 10 \,\rrbracket\, \mathcal{X}_5 \\
\mathcal{X}_4 &= \mathsf{C}\llbracket\, \mathtt{X} \geq 0 \,\rrbracket\, \mathcal{X}_3 \\
\mathcal{X}_5 &= \mathsf{C}\llbracket\, \mathtt{X} := \mathtt{X} - 1 \,\rrbracket\, \mathcal{X}_4 \\
\mathcal{X}_6 &= \mathsf{C}\llbracket\, \mathtt{X} < 0 \,\rrbracket\, \mathcal{X}_3
\end{aligned}
\right.
$$

语义方程系统

循环不变式

$$\mathcal{X}_3 = \{\, \rho \mid \rho(\mathtt{X}) \in [-1,10],\ 10\rho(\mathtt{X}) + \rho(\mathtt{Y}) \in [100,200] \cap 10\mathbb{Z} \,\}$$

具体语义下求解最小不动点

$$
\boxed{
\begin{array}{lll}
\mathcal{X}_e & & \\
\mathcal{X}_{\ell \neq e} & = & \displaystyle\bigcup_{(\ell',c,\ell)\in A} \mathrm{C}[\![\, c \,]\!]\, \mathcal{X}_{\ell'}
\end{array}
}
$$

- 计算最小不动点：Kleene迭代

$$
\left\{
\begin{array}{lll}
\mathcal{X}_e^0 & \stackrel{\mathrm{def}}{=} & \mathcal{X}_e \\
\mathcal{X}_{\ell \neq e}^0 & \stackrel{\mathrm{def}}{=} & \emptyset
\end{array}
\right.
\qquad
\left\{
\begin{array}{lll}
\mathcal{X}_e^{n+1} & \stackrel{\mathrm{def}}{=} & \mathcal{X}_e \\
\mathcal{X}_{\ell \neq e}^{n+1} & \stackrel{\mathrm{def}}{=} & \displaystyle\bigcup_{(\ell',c,\ell)\in A} \mathrm{C}[\![\, c \,]\!]\, \mathcal{X}_{\ell'}^n
\end{array}
\right.
$$

具体语义下求解最小不动点—示例

第 0 次迭代

```
1 x:=[0,10];
2 y:=100;
3 while ( x>=0)  do
4    x:=x-1;
5    y:=y+10;
  done 6
```

$$
\left\{
\begin{array}{ll}
\mathcal{X}_1 = \mathbb{Z}^2 & \mathbb{Z}^2 \\
\mathcal{X}_2 = \mathsf{C}[\![\, \mathtt{X} := [0,10] \,]\!]\, \mathcal{X}_1 & \Phi \\
\mathcal{X}_3 = \mathsf{C}[\![\, \mathtt{Y} := 100 \,]\!]\, \mathcal{X}_2 \cup & \Phi \\
\qquad\; \mathsf{C}[\![\, \mathtt{Y} := \mathtt{Y} + 10 \,]\!]\, \mathcal{X}_5 & \\
\mathcal{X}_4 = \mathsf{C}[\![\, \mathtt{X} \geq 0 \,]\!]\, \mathcal{X}_3 & \Phi \\
\mathcal{X}_5 = \mathsf{C}[\![\, \mathtt{X} := \mathtt{X} - 1 \,]\!]\, \mathcal{X}_4 & \Phi \\
\mathcal{X}_6 = \mathsf{C}[\![\, \mathtt{X} < 0 \,]\!]\, \mathcal{X}_3 & \Phi
\end{array}
\right.
$$

具体语义下求解最小不动点—示例

```
1 x:=[0,10];
2 y:=100;
3 while ( x>=0)  do
4    x:=x-1;
5    y:=y+10;
  done 6
```

	第 1 次迭代
$\mathcal{X}_1 = \mathbb{Z}^2$	$\mathcal{Z}^2$
$\mathcal{X}_2 = \mathrm{C}[\![\, \mathtt{X} := [0,10] \,]\!]\, \mathcal{X}_1$	$[0,10] \times \mathcal{Z}$
$\mathcal{X}_3 = \mathrm{C}[\![\, \mathtt{Y} := 100 \,]\!]\, \mathcal{X}_2 \cup \mathrm{C}[\![\, \mathtt{Y} := \mathtt{Y} + 10 \,]\!]\, \mathcal{X}_5$	Φ
$\mathcal{X}_4 = \mathrm{C}[\![\, \mathtt{X} \geq 0 \,]\!]\, \mathcal{X}_3$	Φ
$\mathcal{X}_5 = \mathrm{C}[\![\, \mathtt{X} := \mathtt{X} - 1 \,]\!]\, \mathcal{X}_4$	Φ
$\mathcal{X}_6 = \mathrm{C}[\![\, \mathtt{X} < 0 \,]\!]\, \mathcal{X}_3$	Φ

具体语义下求解最小不动点—示例

第 2 次迭代

$$\left\{\begin{array}{ll}
\mathcal{X}_1 = \mathbb{Z}^2 & \mathcal{Z}^2 \\[2ex]
\mathcal{X}_2 = \mathrm{C}[\![\, \mathtt{X} := [0,10] \,]\!]\, \mathcal{X}_1 & [0,10] \times \mathcal{Z} \\[2ex]
\mathcal{X}_3 = \mathrm{C}[\![\, \mathtt{Y} := 100 \,]\!]\, \mathcal{X}_2 \cup & \{ (0,100),\ldots,(10,100) \} \\
\qquad\ \ \mathrm{C}[\![\, \mathtt{Y} := \mathtt{Y} + 10 \,]\!]\, \mathcal{X}_5 & \\[2ex]
\mathcal{X}_4 = \mathrm{C}[\![\, \mathtt{X} \geq 0 \,]\!]\, \mathcal{X}_3 & \Phi \\[2ex]
\mathcal{X}_5 = \mathrm{C}[\![\, \mathtt{X} := \mathtt{X} - 1 \,]\!]\, \mathcal{X}_4 & \Phi \\[2ex]
\mathcal{X}_6 = \mathrm{C}[\![\, \mathtt{X} < 0 \,]\!]\, \mathcal{X}_3 & \Phi
\end{array}\right.$$

```
1 x:=[0,10];
2 y:=100;
3 while ( x>=0)  do
4    x:=x-1;
5    y:=y+10;
  done 6
```

具体语义下求解最小不动点—示例

第 3 次迭代

$$\left\{\begin{array}{ll}
\mathcal{X}_1 = \mathbb{Z}^2 & \mathcal{Z}^2 \\
\mathcal{X}_2 = \mathsf{C}[\![\, \mathtt{X} := [0,10] \,]\!]\, \mathcal{X}_1 & [0,10] \times \mathcal{Z} \\
\mathcal{X}_3 = \mathsf{C}[\![\, \mathtt{Y} := 100 \,]\!]\, \mathcal{X}_2 \cup & \{ (0,100),\ldots,(10,100) \} \\
\qquad\ \ \mathsf{C}[\![\, \mathtt{Y} := \mathtt{Y} + 10 \,]\!]\, \mathcal{X}_5 & \\
\mathcal{X}_4 = \mathsf{C}[\![\, \mathtt{X} \geq 0 \,]\!]\, \mathcal{X}_3 & \{ (0,100),\ldots,(10,100) \} \\
\mathcal{X}_5 = \mathsf{C}[\![\, \mathtt{X} := \mathtt{X} - 1 \,]\!]\, \mathcal{X}_4 & \Phi \\
\mathcal{X}_6 = \mathsf{C}[\![\, \mathtt{X} < 0 \,]\!]\, \mathcal{X}_3 & \Phi
\end{array}\right.$$

```
1 x:=[0,10];
2 y:=100;
3 while ( x>=0)  do
4    x:=x-1;
5    y:=y+10;
  done 6
```

具体语义下求解最小不动点—示例

```
1 x:=[0,10];
2 y:=100;
3 while ( x>=0)  do
4    x:=x-1;
5    y:=y+10;
  done 6
```

第 4 次迭代

	第 4 次迭代
$\mathcal{X}_1 = \mathbb{Z}^2$	$\mathcal{Z}^2$
$\mathcal{X}_2 = \mathrm{C}[\![\, \mathtt{X} := [0,10] \,]\!]\, \mathcal{X}_1$	[0,10] x $\mathcal{Z}$
$\mathcal{X}_3 = \mathrm{C}[\![\, \mathtt{Y} := 100 \,]\!]\, \mathcal{X}_2 \cup \mathrm{C}[\![\, \mathtt{Y} := \mathtt{Y} + 10 \,]\!]\, \mathcal{X}_5$	{ (0,100),...,(10,100) }
$\mathcal{X}_4 = \mathrm{C}[\![\, \mathtt{X} \geq 0 \,]\!]\, \mathcal{X}_3$	{ (0,100),...,(10,100) }
$\mathcal{X}_5 = \mathrm{C}[\![\, \mathtt{X} := \mathtt{X} - 1 \,]\!]\, \mathcal{X}_4$	{ (-1,100),...,(9,100) }
$\mathcal{X}_6 = \mathrm{C}[\![\, \mathtt{X} < 0 \,]\!]\, \mathcal{X}_3$	Φ

具体语义下求解最小不动点—示例

	第 5 次迭代
$\mathcal{X}_1 = \mathbb{Z}^2$	$\mathcal{Z}^2$
$\mathcal{X}_2 = \mathsf{C}[\![\, \mathtt{X} := [0,10] \,]\!]\, \mathcal{X}_1$	[0,10] x $\mathcal{Z}$
$\mathcal{X}_3 = \mathsf{C}[\![\, \mathtt{Y} := 100 \,]\!]\, \mathcal{X}_2 \cup$ $\mathsf{C}[\![\, \mathtt{Y} := \mathtt{Y} + 10 \,]\!]\, \mathcal{X}_5$	{ (0,100),…,(10,100), (-1,110),…,(9,110) }
$\mathcal{X}_4 = \mathsf{C}[\![\, \mathtt{X} \geq 0 \,]\!]\, \mathcal{X}_3$	{ (0,100),…,(10,100) }
$\mathcal{X}_5 = \mathsf{C}[\![\, \mathtt{X} := \mathtt{X} - 1 \,]\!]\, \mathcal{X}_4$	{ (-1,100),…,(9,100) }
$\mathcal{X}_6 = \mathsf{C}[\![\, \mathtt{X} < 0 \,]\!]\, \mathcal{X}_3$	Φ

```
1 x:=[0,10];
2 y:=100;
3 while ( x>=0)  do
4   x:=x-1;
5   y:=y+10;
  done 6
```

具体语义下求解最小不动点—示例

```
1 x:=[0,10];
2 y:=100;
3 while ( x>=0)  do
4    x:=x-1;
5    y:=y+10;
  done 6
```

第 6 次迭代

$$\mathcal{X}_1 = \mathbb{Z}^2$$

$\mathcal{Z}^2$

$$\mathcal{X}_2 = \mathrm{C}[\![\, \mathtt{X} := [0, 10] \,]\!]\, \mathcal{X}_1$$

$[0,10] \times \mathcal{Z}$

$$\mathcal{X}_3 = \mathrm{C}[\![\, \mathtt{Y} := 100 \,]\!]\, \mathcal{X}_2 \cup \mathrm{C}[\![\, \mathtt{Y} := \mathtt{Y} + 10 \,]\!]\, \mathcal{X}_5$$

{ (0,100),…,(10,100),
(-1,110),…,(9,110) }

$$\mathcal{X}_4 = \mathrm{C}[\![\, \mathtt{X} \geq 0 \,]\!]\, \mathcal{X}_3$$

{ (0,100),…,(10,100),
(0,110),…,(9,110) }

$$\mathcal{X}_5 = \mathrm{C}[\![\, \mathtt{X} := \mathtt{X} - 1 \,]\!]\, \mathcal{X}_4$$

{ (-1,100),…,(9,100) }

$$\mathcal{X}_6 = \mathrm{C}[\![\, \mathtt{X} < 0 \,]\!]\, \mathcal{X}_3$$

{ (-1,110) }

具体语义下求解最小不动点—示例

第 7 次迭代

$$\begin{cases}
\mathcal{X}_1 = \mathbb{Z}^2 & \mathcal{Z}^2 \\
\mathcal{X}_2 = \mathsf{C}[\![\, \mathtt{X} := [0,10] \,]\!]\, \mathcal{X}_1 & [0,10] \times \mathcal{Z} \\
\mathcal{X}_3 = \mathsf{C}[\![\, \mathtt{Y} := 100 \,]\!]\, \mathcal{X}_2 \cup & \{ (0,100),\ldots,(10,100), \\
\qquad \mathsf{C}[\![\, \mathtt{Y} := \mathtt{Y} + 10 \,]\!]\, \mathcal{X}_5 & (-1,110),\ldots,(9,110) \} \\
\mathcal{X}_4 = \mathsf{C}[\![\, \mathtt{X} \geq 0 \,]\!]\, \mathcal{X}_3 & \{ (0,100),\ldots,(10,100), \\
 & (0,110),\ldots,(9,110) \} \\
\mathcal{X}_5 = \mathsf{C}[\![\, \mathtt{X} := \mathtt{X} - 1 \,]\!]\, \mathcal{X}_4 & \{ (-1,100),\ldots,(9,100), \\
 & (-1,110),\ldots,(8,110) \} \\
\mathcal{X}_6 = \mathsf{C}[\![\, \mathtt{X} < 0 \,]\!]\, \mathcal{X}_3 & \{ (-1,110) \}
\end{cases}$$

```
1 x:=[0,10];
2 y:=100;
3 while ( x>=0)  do
4   x:=x-1;
5   y:=y+10;
  done 6
```

具体语义下求解最小不动点—示例

第 8 次迭代

```
1 x:=[0,10];
2 y:=100;
3 while ( x>=0)  do
4    x:=x-1;
5    y:=y+10;
  done 6
```

$\mathcal{X}_1 = \mathbb{Z}^2$	$\mathcal{Z}^2$
$\mathcal{X}_2 = \mathrm{C}[\![\, \mathtt{X} := [0,10] \,]\!]\, \mathcal{X}_1$	[0,10] x $\mathcal{Z}$
$\mathcal{X}_3 = \mathrm{C}[\![\, \mathtt{Y} := 100 \,]\!]\, \mathcal{X}_2 \cup \mathrm{C}[\![\, \mathtt{Y} := \mathtt{Y} + 10 \,]\!]\, \mathcal{X}_5$	{ (0,100),…,(10,100), (-1,110),…,(9,110), (-1,120),…,(8,120) }
$\mathcal{X}_4 = \mathrm{C}[\![\, \mathtt{X} \geq 0 \,]\!]\, \mathcal{X}_3$	{ (0,100),…,(10,100), (0,110),…,(9,110) }
$\mathcal{X}_5 = \mathrm{C}[\![\, \mathtt{X} := \mathtt{X} - 1 \,]\!]\, \mathcal{X}_4$	{ (-1,100),…,(9,100), (-1,110),…,(8,110) }
$\mathcal{X}_6 = \mathrm{C}[\![\, \mathtt{X} < 0 \,]\!]\, \mathcal{X}_3$	{ (-1,110) }

具体语义下求解最小不动点—示例

```
1 x:=[0,10];
2 y:=100;
3 while ( x>=0)  do
4    x:=x-1;
5    y:=y+10;
  done 6
```

	第 9 次迭代
$\mathcal{X}_1 = \mathbb{Z}^2$	$\mathcal{Z}^2$
$\mathcal{X}_2 = C\llbracket\, \mathtt{X} := [0,10] \,\rrbracket\, \mathcal{X}_1$	[0,10] x $\mathcal{Z}$
$\mathcal{X}_3 = C\llbracket\, \mathtt{Y} := 100 \,\rrbracket\, \mathcal{X}_2 \cup C\llbracket\, \mathtt{Y} := \mathtt{Y} + 10 \,\rrbracket\, \mathcal{X}_5$	{ (0,100),…,(10,100), (-1,110),…,(9,110), (-1,120),…,(8,120) }
$\mathcal{X}_4 = C\llbracket\, \mathtt{X} \geq 0 \,\rrbracket\, \mathcal{X}_3$	{ (0,100),…,(10,100), (0,110),….,(9,110), (0,120),….,(8,120) }
$\mathcal{X}_5 = C\llbracket\, \mathtt{X} := \mathtt{X} - 1 \,\rrbracket\, \mathcal{X}_4$	{ (-1,100),…,(9,100), (-1,110),…,(8,110) }
$\mathcal{X}_6 = C\llbracket\, \mathtt{X} < 0 \,\rrbracket\, \mathcal{X}_3$	{ (-1,110), (-1,120) }

具体语义下求解最小不动点—示例

```
1 x:=[0,10];
2 y:=100;
3 while ( x>=0)  do
4    x:=x-1;
5    y:=y+10;
  done 6
```

第 10 次迭代

$\mathcal{X}_1 = \mathbb{Z}^2$	$\mathcal{Z}^2$
$\mathcal{X}_2 = \mathrm{C}[\![\, \mathtt{X} := [0,10] \,]\!]\, \mathcal{X}_1$	[0,10] x $\mathcal{Z}$
$\mathcal{X}_3 = \mathrm{C}[\![\, \mathtt{Y} := 100 \,]\!]\, \mathcal{X}_2 \cup$ $\mathrm{C}[\![\, \mathtt{Y} := \mathtt{Y} + 10 \,]\!]\, \mathcal{X}_5$	{ (0,100),…,(10,100), (-1,110),…,(9,110), (-1,120),…,(8,120) }
$\mathcal{X}_4 = \mathrm{C}[\![\, \mathtt{X} \geq 0 \,]\!]\, \mathcal{X}_3$	{ (0,100),…,(10,100), (0,110),…,(9,110), (0,120),…,(8,120) }
$\mathcal{X}_5 = \mathrm{C}[\![\, \mathtt{X} := \mathtt{X} - 1 \,]\!]\, \mathcal{X}_4$	{ (-1,100),…,(9,100), (-1,110),…,(8,110), (-1,120),…,(7,120) }
$\mathcal{X}_6 = \mathrm{C}[\![\, \mathtt{X} < 0 \,]\!]\, \mathcal{X}_3$	{ (-1,110), (-1,120) }

具体语义下求解最小不动点—示例

```
1 x:=[0,10];
2 y:=100;
3 while ( x>=0)  do
4    x:=x-1;
5    y:=y+10;
  done 6
```

	第 ... 次迭代
$\mathcal{X}_1 = \mathbb{Z}^2$	$\mathcal{Z}^2$
$\mathcal{X}_2 = \mathrm{C}[\![\, \mathtt{X} := [0,10] \,]\!]\, \mathcal{X}_1$	[0,10] x $\mathcal{Z}$
$\mathcal{X}_3 = \mathrm{C}[\![\, \mathtt{Y} := 100 \,]\!]\, \mathcal{X}_2 \cup$ $\mathrm{C}[\![\, \mathtt{Y} := \mathtt{Y} + 10 \,]\!]\, \mathcal{X}_5$	{ (0,100),…,(10,100), (-1,110),…,(9,110), (-1,120),…,(8,120),… }
$\mathcal{X}_4 = \mathrm{C}[\![\, \mathtt{X} \geq 0 \,]\!]\, \mathcal{X}_3$	{ (0,100),…,(10,100), (0,110),…,(9,110), (0,120),…,(8,120),… }
$\mathcal{X}_5 = \mathrm{C}[\![\, \mathtt{X} := \mathtt{X} - 1 \,]\!]\, \mathcal{X}_4$	{ (-1,100),…,(9,100), (-1,110),…,(8,110), (-1,120),…,(7,120),… }
$\mathcal{X}_6 = \mathrm{C}[\![\, \mathtt{X} < 0 \,]\!]\, \mathcal{X}_3$	{ (-1,110),…,(-1,120),… }

本讲内容介绍

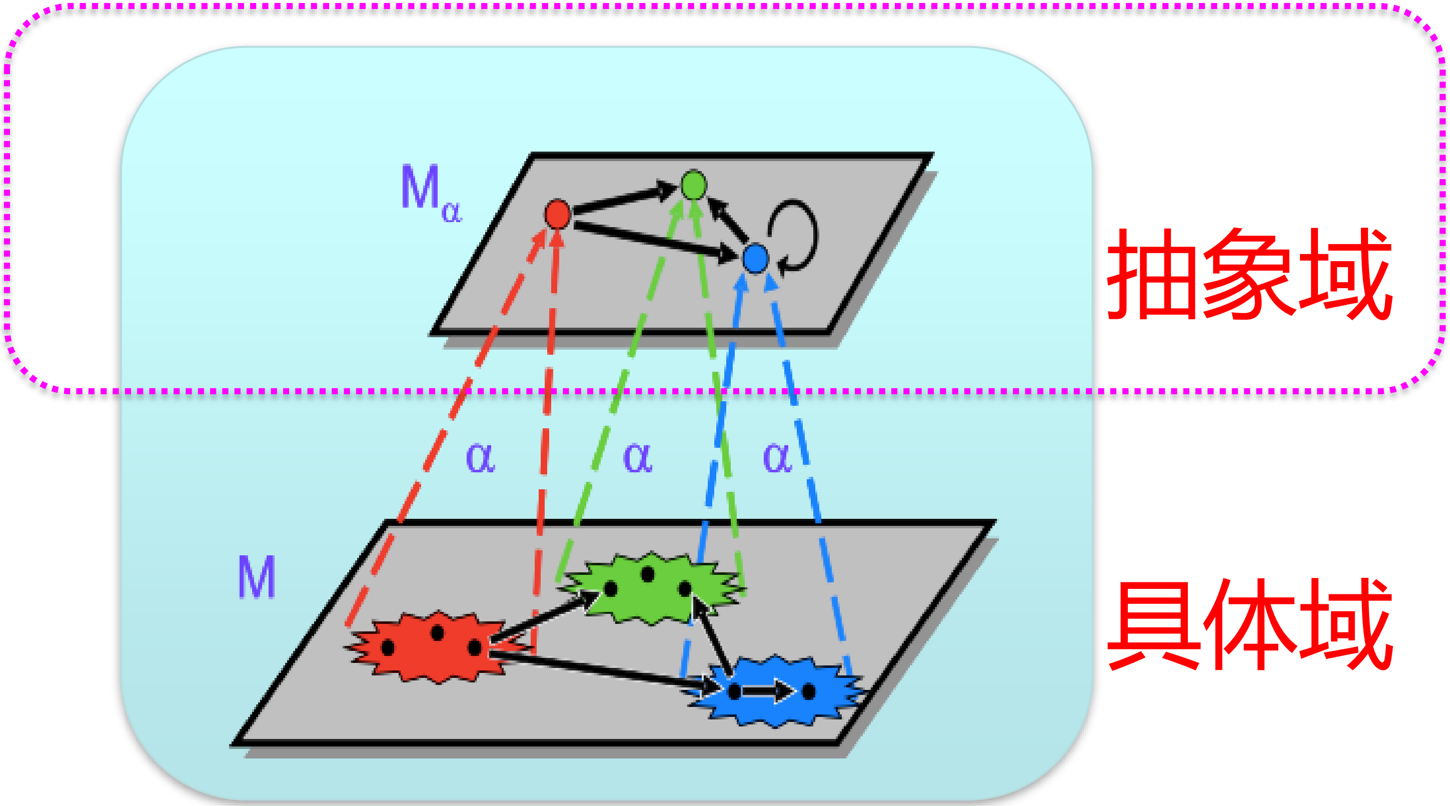
- 一、抽象解释理论的概述
- 二、抽象解释理论的数学基础
- 三、具体语义下的静态分析
- 四、抽象语义下的静态分析
- 五、基于抽象解释的静态分析工具

本讲内容介绍

- 一、抽象解释理论的概述
- 二、抽象解释理论的数学基础
- 三、具体语义下的静态分析
- 四、抽象语义下的静态分析
  - ➢抽象域
  - ➢基于抽象域的静态分析
- 五、基于抽象解释的静态分析工具

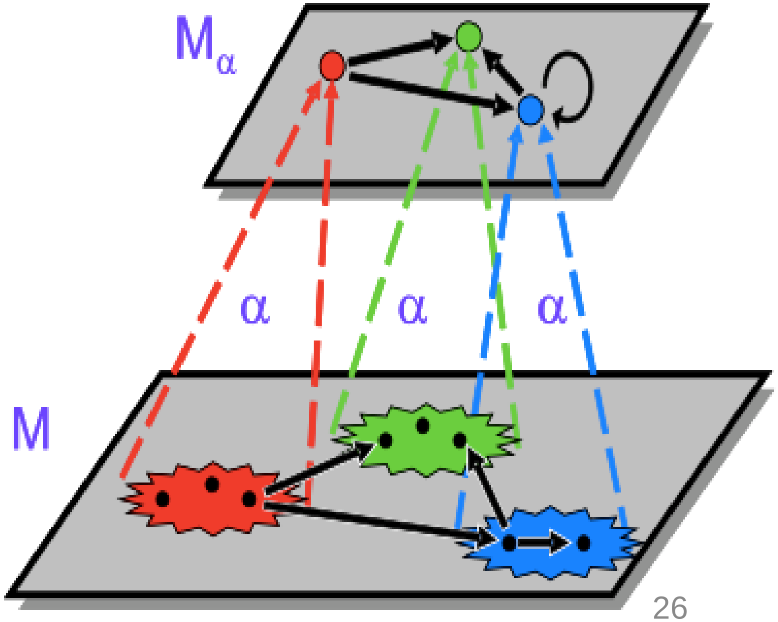
抽象域：抽象解释的核心要素

- 静态分析相关的计算都在抽象域上开展



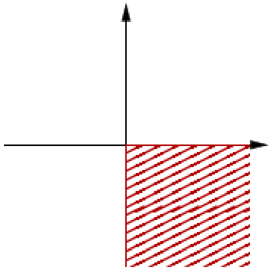
抽象域的构成

- **域元素**：对程序状态进行抽象
  - 表示方法: 约束形式, …
  - E.g. 区间: $a<=x<= b$
- **域操作**：对程序语义动作进行抽象
  - **交** (assume语句)
  - **控制流接合** (if-then-else-endif)
  - **投影**（非确定赋值，过程间分析）
  - **迁移函数**
    - 赋值迁移语句 (赋值语句)
    - 测试迁移语句 (if 语句)
  - **加宽**（循环）
  - …



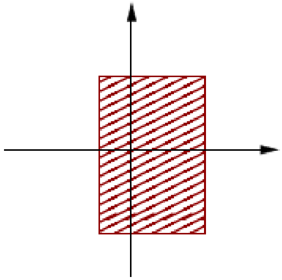
数值抽象域

- 刻画程序变量之间的数值关系
- 用途：发现程序中某程序点处的数值不变式，即每次程序执行均满足的数值关系
  - 除零错、数组越界、整数溢出等运行时错误
  - 安全方面"缓冲区溢出"问题: 地址（指针）和长度（范围）之间的数值关系



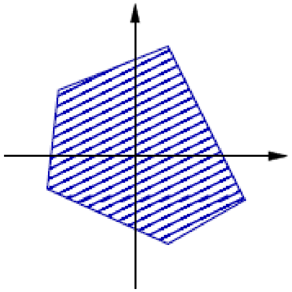
符号抽象域

$x_i \le 0$, $x_i \ge 0$



区间抽象域

$x_i=[a_i, b_i]$

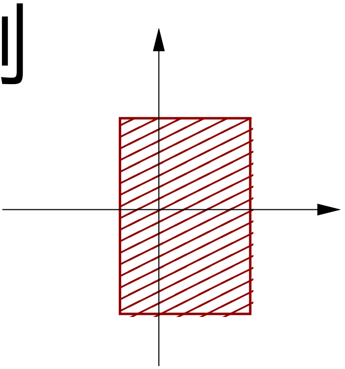


多面体抽象域

$\sum_i a_i x_i \le c$

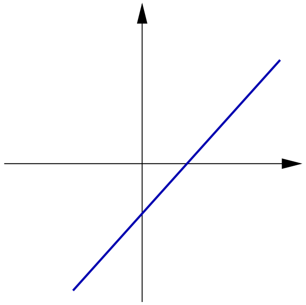
数值抽象域

- 以两个数值抽象域为例
  - 区间抽象域



$x_i=[a_i, b_i]$

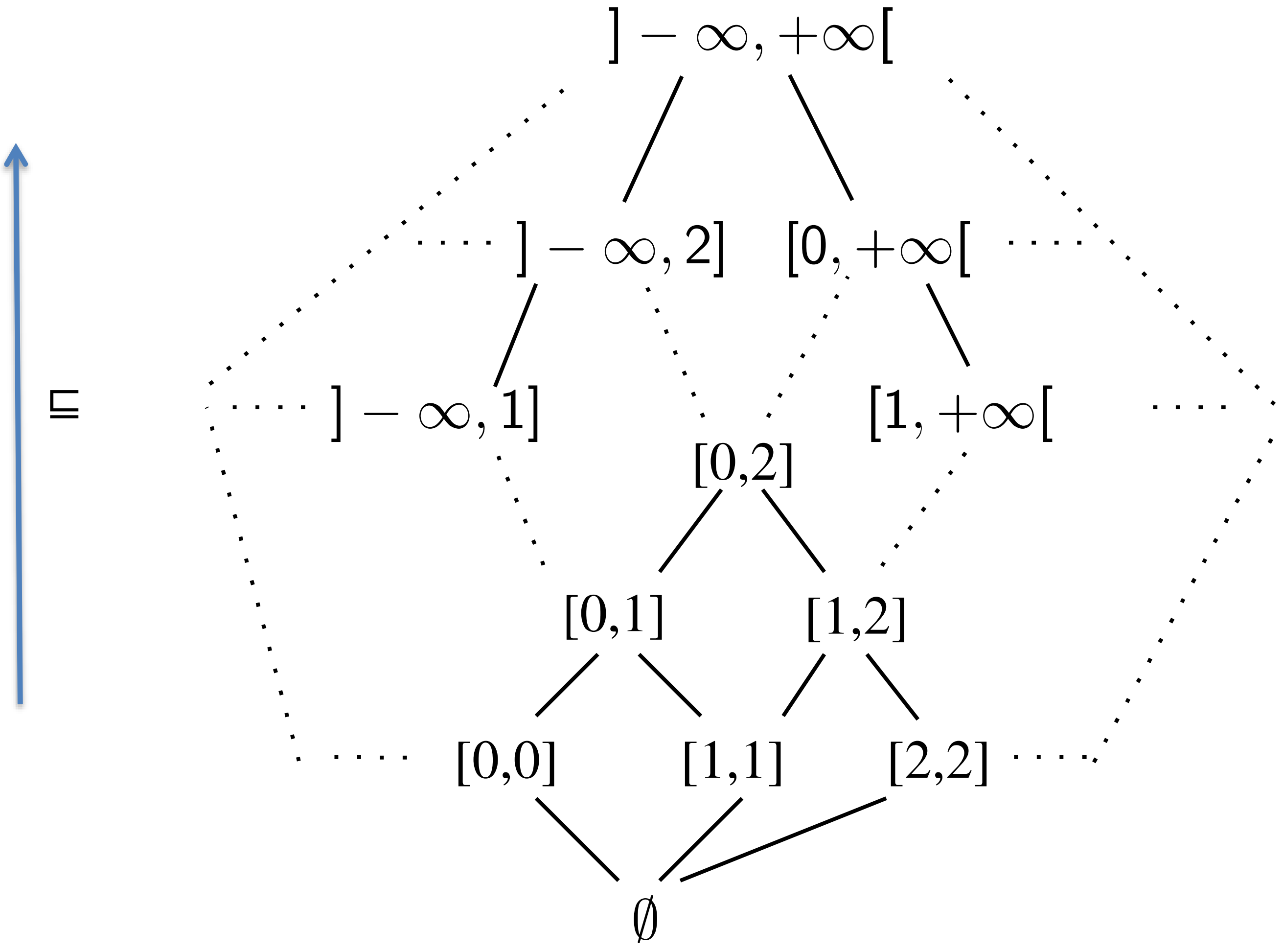
  - 线性等式抽象域



$\sum_i a_i x_i = c$

区间抽象域

- 区间格 $B^{\#} = \{[a,b] \mid a \in R \cup \{-\infty\}, b \in R \cup \{+\infty\}, a \leq b\} \cup \{\perp^{\#}\}$



区间抽象域

- Galois连接

$$\begin{tikzcd}\wp(R) \arrow[r, shift right, "\alpha_b"'] & B^{\#} \arrow[l, shift right, "\gamma_b"']\end{tikzcd}$$

$$\gamma_b([a,b]) \triangleq \{x \in R \mid a \leq x \leq b\}$$

$$\alpha_b(X) \triangleq \begin{cases} \bot^{\#} & \text{if } X = \emptyset \\ [\min X, \max X] & \text{otherwise} \end{cases}$$

区间抽象域

- 格相关操作

$$
\begin{array}{rcll}
[a,b] \subseteq^\sharp [c,d] & \overset{\text{def}}{\iff} & a \geq c \text{ and } b \leq d & \\
\top^\sharp & \overset{\text{def}}{=} &]-\infty, +\infty[& \\
[a,b] \cup^\sharp [c,d] & \overset{\text{def}}{=} & [\min(a,c), \max(b,d)] & \\
[a,b] \cap^\sharp [c,d] & \overset{\text{def}}{=} & \begin{cases} [\max(a,c), \min(b,d)] & \text{if } \max \leq \min \\ \bot^\sharp & \text{otherwise} \end{cases} &
\end{array}
$$

$\wp$(R)对应的 $(B^\sharp, \subseteq^\sharp, \cup^\sharp, \cap^\sharp, \bot^\sharp, \top^\sharp)$ 是一个完全格

区间抽象域

- 区间算术操作

$$
\begin{array}{rcl}
[c, c']^\sharp & \stackrel{\text{def}}{=} & [c, c'] \\
-^\sharp\ [a, b] & \stackrel{\text{def}}{=} & [-b, -a] \\
[a, b] +^\sharp [c, d] & \stackrel{\text{def}}{=} & [a + c, b + d] \\
[a, b] -^\sharp [c, d] & \stackrel{\text{def}}{=} & [a - d, b - c] \\
[a, b] \times^\sharp [c, d] & \stackrel{\text{def}}{=} & [\min(ac, ad, bc, bd), \max(ac, ad, bc, bd)] \\
[a, b] /^\sharp [c, d] & \stackrel{\text{def}}{=} & \begin{cases} \bot^\sharp & \text{if } c = d = 0 \\ [\min(a/c, a/d, b/c, b/d), & \text{if } 0 \leq c \\ \ \max(a/c, a/d, b/c, b/d)] & \\ [-b, -a] /^\sharp [-d, -c] & \text{if } d \leq 0 \\ ([a, b] /^\sharp [c, 0]) \cup^\sharp ([a, b] /^\sharp [0, d]) & \text{otherwise} \end{cases}
\end{array}
$$

$$
\text{where} \left| \begin{array}{l} \pm\infty \times 0 = 0, \quad 0/0 = 0, \quad \forall x\colon x/\pm\infty = 0 \\ \forall x > 0\colon x/0 = +\infty, \quad \forall x < 0\colon x/0 = -\infty \end{array} \right.
$$

区间抽象域

- 赋值操作

$$\mathsf{C}^\sharp[\![\, \mathtt{V} := e \,]\!]\, \mathcal{X}^\sharp \stackrel{\text{def}}{=} \begin{cases} \bot^\sharp & \text{if } \mathcal{V}^\sharp = \bot^\sharp \\ \mathcal{X}^\sharp[\mathtt{V} \mapsto \mathcal{V}^\sharp] & \text{otherwise} \end{cases}$$

$$\text{where } \mathcal{V}^\sharp = \mathsf{E}^\sharp[\![\, e \,]\!]\, \mathcal{X}^\sharp.$$

  - 其中表达式e的值的计算

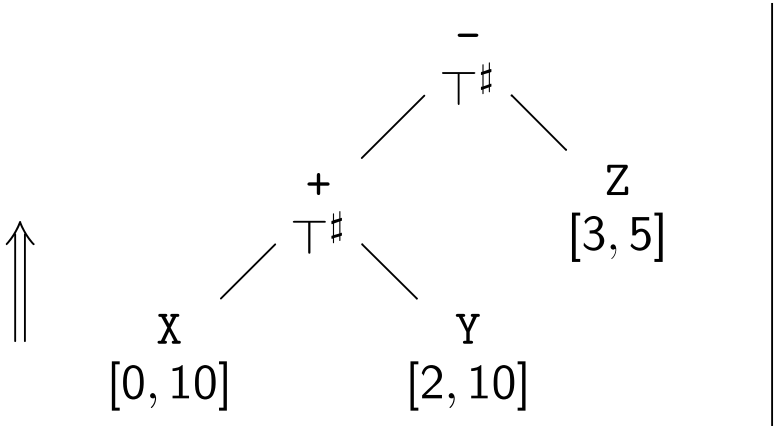
$$\begin{array}{lcl} \mathsf{E}^\sharp[\![\, [c, c'] \,]\!]\, \mathcal{X}^\sharp & \stackrel{\text{def}}{=} & [c, c']^\sharp \\ \mathsf{E}^\sharp[\![\, \mathtt{V} \,]\!]\, \mathcal{X}^\sharp & \stackrel{\text{def}}{=} & \mathcal{X}^\sharp(\mathtt{V}) \\ \mathsf{E}^\sharp[\![\, -e \,]\!]\, \mathcal{X}^\sharp & \stackrel{\text{def}}{=} & -^\sharp\, \mathsf{E}^\sharp[\![\, e \,]\!]\, \mathcal{X}^\sharp \\ \mathsf{E}^\sharp[\![\, e_1 + e_2 \,]\!]\, \mathcal{X}^\sharp & \stackrel{\text{def}}{=} & \mathsf{E}^\sharp[\![\, e_1 \,]\!]\, \mathcal{X}^\sharp +^\sharp \mathsf{E}^\sharp[\![\, e_2 \,]\!]\, \mathcal{X}^\sharp \\ \vdots & & \end{array}$$

区间抽象域

- 赋值操作-示例

$$\mathcal{Y}^\sharp \overset{\text{def}}{=} \mathsf{C}^\sharp[\![\, \texttt{X} := \texttt{X} + \texttt{Y} - \texttt{Z} \,]\!]\, \mathcal{X}^\sharp$$

with $\mathcal{X}^\sharp = \{\, \texttt{X} \mapsto [0, 10], \texttt{Y} \mapsto [2, 10], \texttt{Z} \mapsto [3, 5] \,\}$

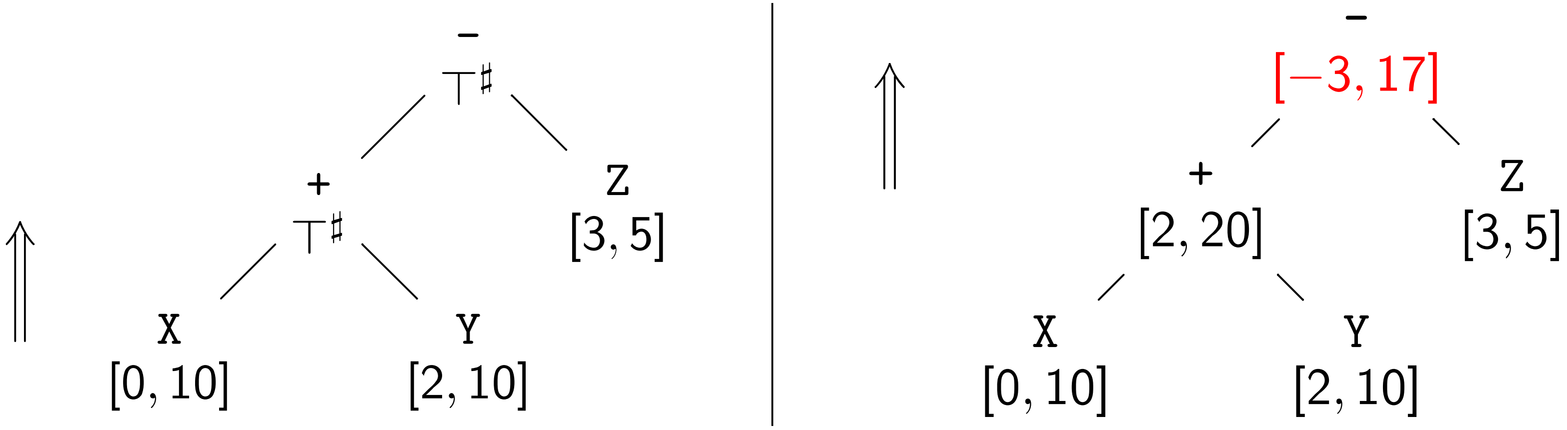


区间抽象域

- 赋值操作-示例

$$\mathcal{Y}^\sharp \overset{\text{def}}{=} \mathsf{C}^\sharp[\![\, \mathtt{X} := \mathtt{X} + \mathtt{Y} - \mathtt{Z} \,]\!]\, \mathcal{X}^\sharp$$

with $\mathcal{X}^\sharp = \{\, \mathtt{X} \mapsto [0, 10], \mathtt{Y} \mapsto [2, 10], \mathtt{Z} \mapsto [3, 5] \,\}$



$$\boxed{\mathcal{Y}^\sharp = \{\, \mathtt{X} \mapsto [-3, 17], \mathtt{Y} \mapsto [2, 10], \mathtt{Z} \mapsto [3, 5] \,\}}$$

区间抽象域

- 条件测试

$$\mathcal{X}^\sharp(\mathtt{X}) = [a, b] \qquad \mathcal{X}^\sharp(\mathtt{Y}) = [c, d]$$

$$C^\sharp[\![\, \mathtt{X} - c \leq 0 \,]\!]\, \mathcal{X}^\sharp \overset{\text{def}}{=} \begin{cases} \bot^\sharp & \text{if } a > c \\ \mathcal{X}^\sharp[\, \mathtt{X} \mapsto [a, \min(b, c)]\,] & \text{otherwise} \end{cases}$$

$$C^\sharp[\![\, \mathtt{X} - \mathtt{Y} \leq 0 \,]\!]\, \mathcal{X}^\sharp \overset{\text{def}}{=} \begin{cases} \bot^\sharp & \text{if } a > d \\ \mathcal{X}^\sharp[\; \mathtt{X} \mapsto [a, \min(b, d)], & \text{otherwise} \\ \qquad\;\; \mathtt{Y} \mapsto [\max(c, a), d]\,] & \end{cases}$$

$$C^\sharp[\![\, e \bowtie 0 \,]\!]\, \mathcal{X}^\sharp \overset{\text{def}}{=} \mathcal{X}^\sharp \quad \text{otherwise}$$

$\bowtie \in \{=, <, >, \leq, \geq, \neq\}$

可靠的

区间抽象域

- 区间加宽（区间格的高度是无穷的）

$$\bot^\sharp \quad \nabla \quad X^\sharp \quad \stackrel{\text{def}}{=} \quad X^\sharp$$

$$[a, b] \quad \nabla \quad [c, d] \quad \stackrel{\text{def}}{=} \quad \left[\begin{cases} a & \text{if } a \leq c \\ -\infty & \text{otherwise} \end{cases}, \begin{cases} b & \text{if } b \geq d \\ +\infty & \text{otherwise} \end{cases} \right]$$

把增长的上界变成+oo
把减小的下界变成-oo

区间抽象域

- 区间加宽（区间格的高度是无穷的）

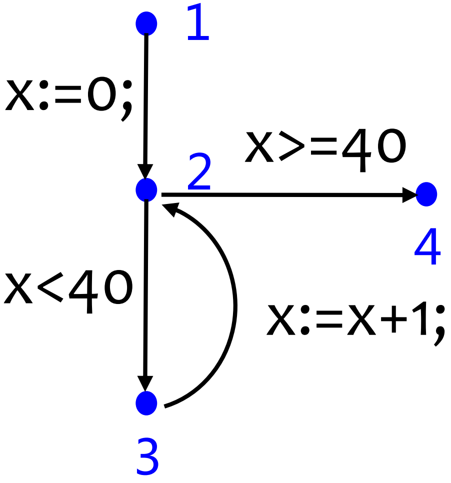
$$
\begin{aligned}
\bot^\sharp \quad \nabla \quad X^\sharp &\stackrel{\text{def}}{=} X^\sharp \\
[a,b] \quad \nabla \quad [c,d] &\stackrel{\text{def}}{=} \left[\begin{cases} a & \text{if } a \leq c \\ -\infty & \text{otherwise} \end{cases}, \begin{cases} b & \text{if } b \geq d \\ +\infty & \text{otherwise} \end{cases} \right]
\end{aligned}
$$

把增长的上界变成+oo
把减小的下界变成-oo

不稳定的要素

区间抽象域

- 区间加宽—示例

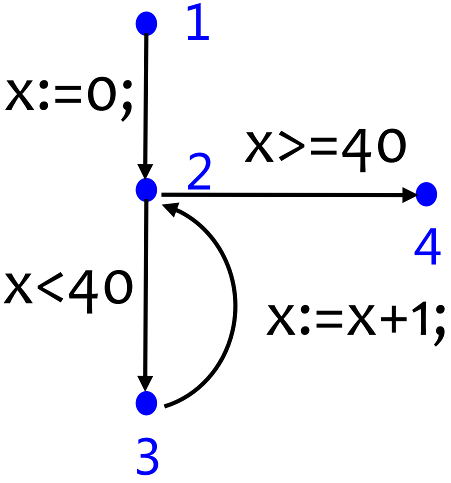


```
1 x:=0;
2 while ( x<40) do
3    x:=x+1;
done; 4
```

区间抽象域

- 区间加宽—示例

```
1 x:=0;
2 while ( x<40) do
3   x:=x+1;
done; 4
```

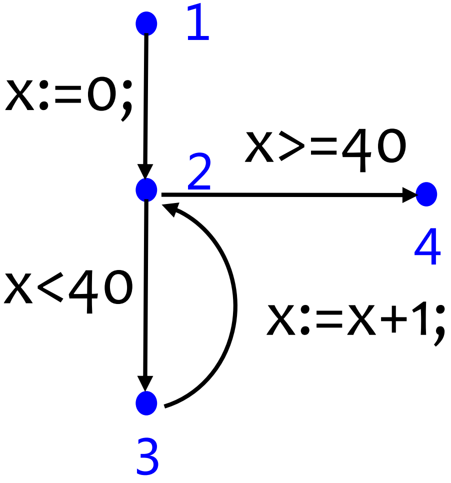


ℓ	$X_\ell^{\#0}$					
1	$\top^\#$					
2 ∇	$\bot^\#$					
3	$\bot^\#$					
4	$\bot^\#$					

区间抽象域

- 区间加宽—示例

```
1 x:=0;
2 while ( x<40) do
3    x:=x+1;
done; 4
```



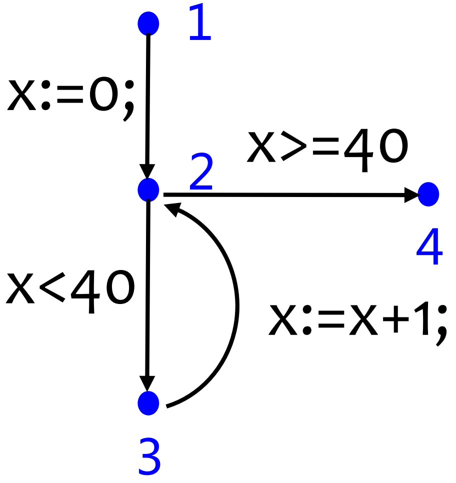
ℓ	$X_\ell^{\#0}$	$X_\ell^{\#1}$			
1	$\top^\#$	$\top^\#$			
2 ∇	$\bot^\#$	=0			
3	$\bot^\#$	$\bot^\#$			
4	$\bot^\#$	$\bot^\#$			

$$X_2^{\#1} = \bot^\# \nabla ([0,0] \cup^\sharp \bot^\#) = \bot^\# \nabla [0,0] = [0,0]$$

区间抽象域

- 区间加宽—示例

```
1 x:=0;
2 while ( x<40) do
3    x:=x+1;
done; 4
```



ℓ	$X_\ell^{\#0}$	$X_\ell^{\#1}$	$X_\ell^{\#2}$			
1	$\top^\#$	$\top^\#$	$\top^\#$			
2 ∇	$\bot^\#$	=0	=0			
3	$\bot^\#$	$\bot^\#$	=0			
4	$\bot^\#$	$\bot^\#$	$\bot^\#$			

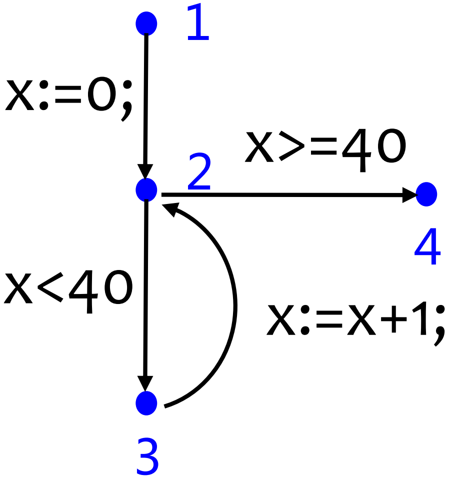
$$X_2^{\#1} = \bot^\# \nabla ([0,0] \cup^\# \bot^\#) = \bot^\# \nabla [0,0] = [0,0]$$

$$X_2^{\#2} = [0,0] \nabla ([0,0] \cup^\# \bot^\#) = [0,0] \nabla [0,0] = [0,0]$$

区间抽象域

- 区间加宽—示例

```
1 x:=0;
2 while ( x<40) do
3    x:=x+1;
done; 4
```



ℓ	$\mathcal{X}_\ell^{\#0}$	$\mathcal{X}_\ell^{\#1}$	$\mathcal{X}_\ell^{\#2}$	$\mathcal{X}_\ell^{\#3}$		
1	$\top^\#$	$\top^\#$	$\top^\#$	$\top^\#$		
2 ∇	$\perp^\#$	$=0$	$=0$	≥ 0		
3	$\perp^\#$	$\perp^\#$	$=0$	$=0$		
4	$\perp^\#$	$\perp^\#$	$\perp^\#$	$\perp^\#$		

$$\mathcal{X}_2^{\#1} = \perp^\# \nabla ([0,0] \cup^\# \perp^\#) = \perp^\# \nabla [0,0] = [0,0]$$

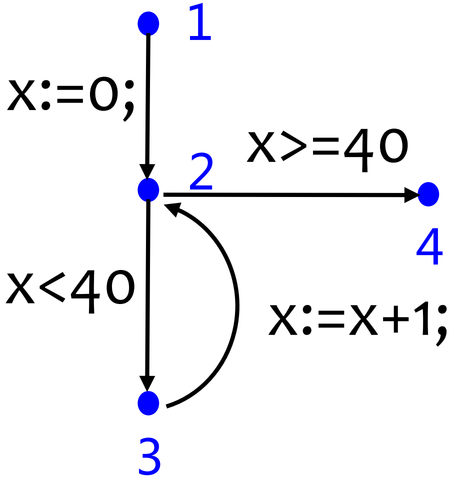
$$\mathcal{X}_2^{\#2} = [0,0] \nabla ([0,0] \cup^\# \perp^\#) = [0,0] \nabla [0,0] = [0,0]$$

$$\mathcal{X}_2^{\#3} = [0,0] \nabla ([0,0] \cup^\# [1,1]) = [0,0] \nabla [0,1] = [0,+oo[$$

区间抽象域

- 区间加宽—示例

```
1  x:=0;
2  while ( x<40) do
3     x:=x+1;
done; 4
```



ℓ	$\mathcal{X}_\ell^{\#0}$	$\mathcal{X}_\ell^{\#1}$	$\mathcal{X}_\ell^{\#2}$	$\mathcal{X}_\ell^{\#3}$	$\mathcal{X}_\ell^{\#4}$
1	$\top^\#$	$\top^\#$	$\top^\#$	$\top^\#$	$\top^\#$
2 ∇	$\bot^\#$	$=0$	$=0$	≥ 0	≥ 0
3	$\bot^\#$	$\bot^\#$	$=0$	$=0$	$[0,39]$
4	$\bot^\#$	$\bot^\#$	$\bot^\#$	$\bot^\#$	≥ 40

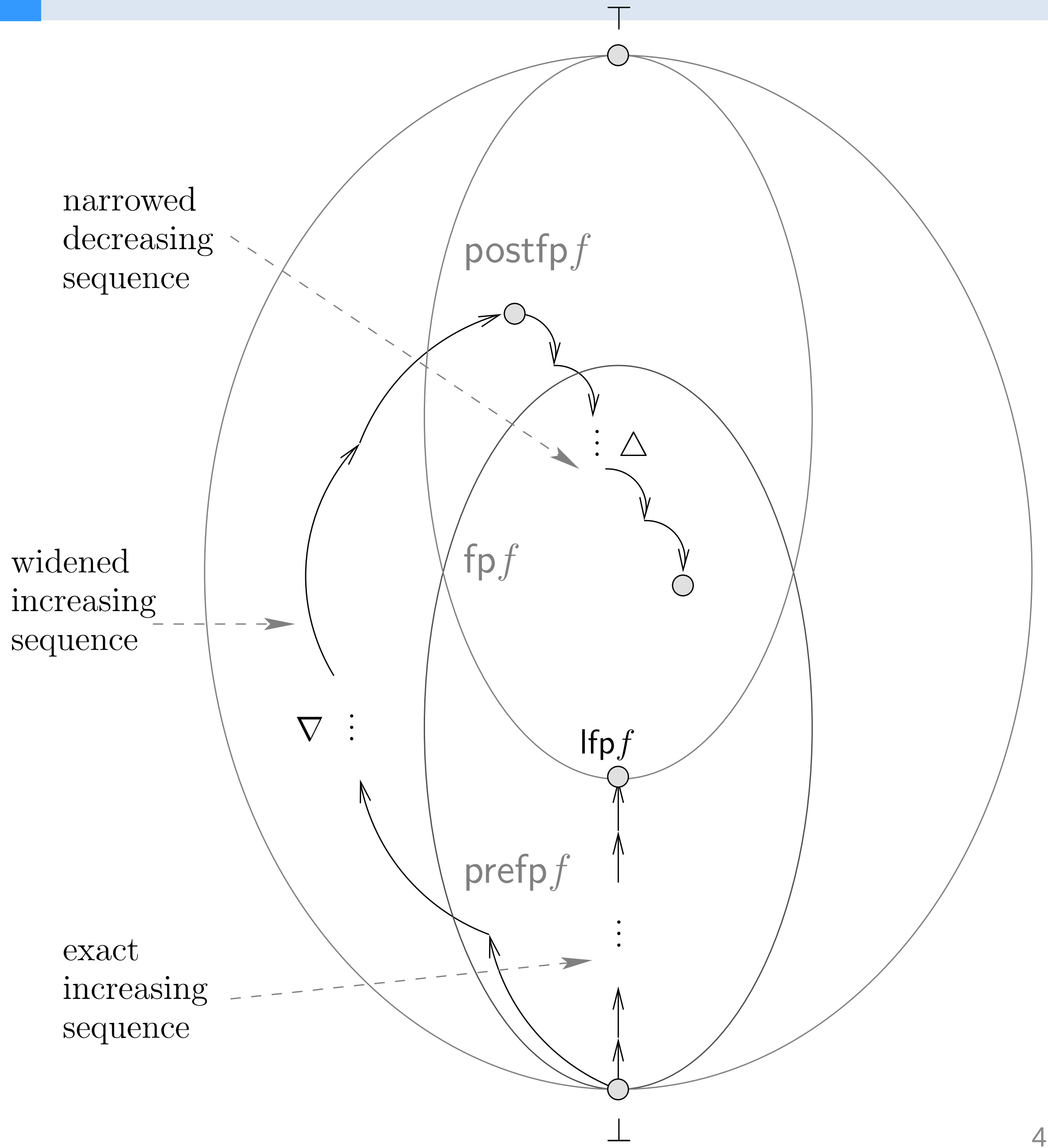
$$\mathcal{X}_2^{\#1} = \bot^\# \nabla ([0,0] \cup^\# \bot^\#) = \bot^\# \nabla [0,0] = [0,0]$$

$$\mathcal{X}_2^{\#2} = [0,0] \nabla ([0,0] \cup^\# \bot^\#) = [0,0] \nabla [0,0] = [0,0]$$

$$\mathcal{X}_2^{\#3} = [0,0] \nabla ([0,0] \cup^\# [1,1]) = [0,0] \nabla [0,1] = [0,+oo[$$

$$\mathcal{X}_2^{\#4} = [0,+oo[\nabla ([0,0] \cup^\# [1,40]) = [0,+oo[\nabla [0,40] = [0,+oo[$$

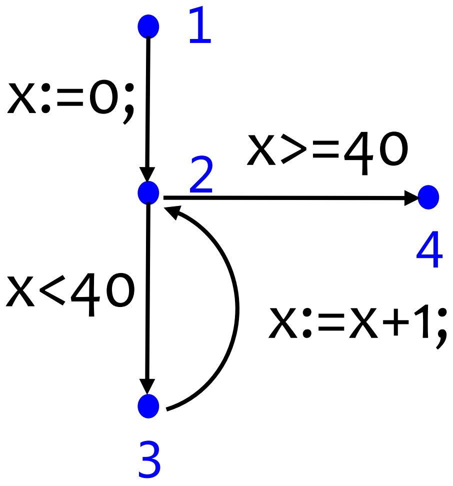
基于加宽/变窄的不动点迭代


⊤
narrowed decreasing sequence
postfp f
△
widened increasing sequence
fp f
▽
lfp f
prefp f
exact increasing sequence
⊥

区间抽象域

- 区间变窄—示例

```
1 x:=0;
2 while ( x<40) do
3    x:=x+1;
done; 4
```

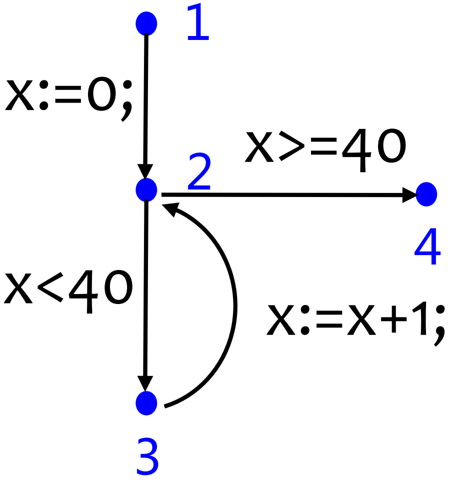


ℓ	$\Upsilon_{\ell}^{\#0}$			
1	$T^{\#}$			
2 Δ	≥0			
3	[0,39]			
4	≥40			

区间抽象域

- 区间变窄—示例

```
1 x:=0;
2 while ( x<40) do
3    x:=x+1;
done; 4
```



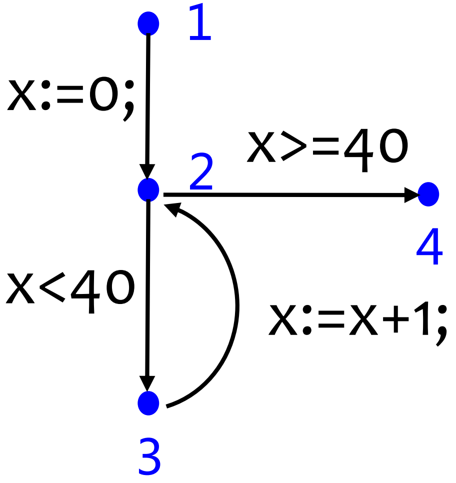
ℓ	$\mathcal{Y}_\ell^{\#0}$	$\mathcal{Y}_\ell^{\#1}$		
1	$\top^\#$	$\top^\#$		
2 Δ	≥0	[0,40]		
3	[0,39]	[0,39]		
4	≥40	≥40		

$$\mathcal{Y}_2^{\#1} = [0,+oo[\ \Delta\ ([0,0]\ \cup^\sharp [1,40]) = [0,+oo[\ \Delta\ [0,40] = [0,40]$$

区间抽象域

- 区间变窄—示例

```
1 x:=0;
2 while ( x<40) do
3    x:=x+1;
done; 4
```



ℓ	$\Upsilon_\ell^{\#0}$	$\Upsilon_\ell^{\#1}$	$\Upsilon_\ell^{\#2}$
1	$\top^\#$	$\top^\#$	$\top^\#$
2 Δ	≥0	[0,40]	[0,40]
3	[0,39]	[0,39]	[0,39]
4	≥40	≥40	=40

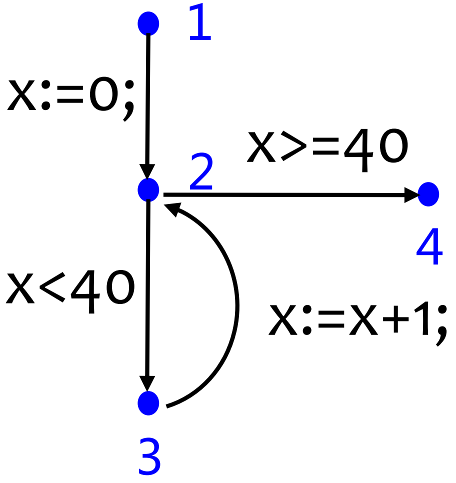
$$\Upsilon_2^{\#1} = [0,+oo[\ \Delta\ ([0,0] \cup^\sharp [1,40]) = [0,+oo[\ \Delta\ [0,40] = [0,40]$$

$$\Upsilon_2^{\#2} = [0,40[\ \Delta\ ([0,0] \cup^\sharp [1,40]) = [0,40] \ \Delta\ [0,40] = [0,40]$$

区间抽象域

- 区间变窄—示例

```
1 x:=0;
2 while ( x<40) do
3     x:=x+1;
done; 4
```



ℓ	$\Upsilon_\ell^{\#0}$	$\Upsilon_\ell^{\#1}$	$\Upsilon_\ell^{\#2}$	$\Upsilon_\ell^{\#3}$
1	$\top^\#$	$\top^\#$	$\top^\#$	$\top^\#$
2 Δ	≥0	[0,40]	[0,40]	[0,40]
3	[0,39]	[0,39]	[0,39]	[0,39]
4	≥40	≥40	=40	=40

$\Upsilon_2^{\#1}$ = [0,+oo[Δ ([0,0] $\cup^\sharp$[1,40]) = [0,+oo[Δ [0,40] = [0,40]

$\Upsilon_2^{\#2}$ = [0,40[Δ ([0,0] $\cup^\sharp$[1,40]) = [0,40] Δ [0,40] = [0,40]

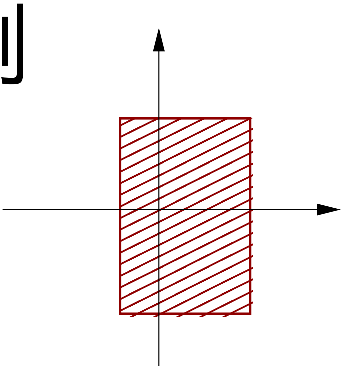
从而得到：在2处 x∈[0,40], 在4处x=40

区间抽象域的局限性

- 区间抽象域是非关系型抽象域
  - 只能表达单个变量的取值范围
  - 不能表达多个变量之间的关系

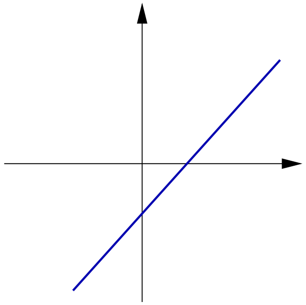
数值抽象域

- 以两个数值抽象域为例
  - 区间抽象域



x_i=[a_i, b_i]

  - 线性等式抽象域



$\sum_i a_i x_i = c$

线性等式抽象域

- 域表示
  - 约束表示：线性等式系统 Ax=b
    - x ∈ R^n 表示程序变量x1, …, xn构成的向量
    - A ∈ $R^{m\times n}$ ，b ∈ R^m 为系数，由静态分析自动分析得到

$$\begin{cases} 2X + Y + Z = 19 \\ 2X + Y - Z = 9 \\ 3Z = 15 \end{cases}$$

线性等式抽象域

- 域表示
  - 约束表示：线性等式系统 Ax=b
  - 规范型：唯一表示
    - 化简后的行阶梯形矩阵 (Reduced Row Echelon Form)
    - 高斯消元法（ Gaussian Elimination ）
      - 把线性等式系统转换为其规范型

$$\left\{\begin{array}{rcrcrcr} 2X & + & Y & + & Z & = & 19 \\ 2X & + & Y & - & Z & = & 9 \\ & & & & 3Z & = & 15 \end{array}\right. \Rightarrow \left\{\begin{array}{rcrrcr} X & + & 0.5Y & & = & 7 \\ & & & Z & = & 5 \end{array}\right.$$

线性等式抽象域

- 域表示： <A, b>

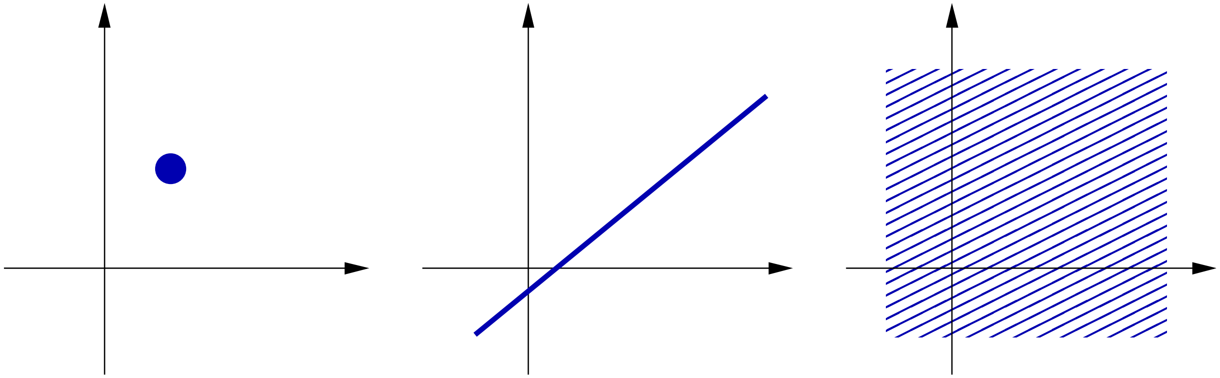
$$\begin{tikzcd}
\wp(\mathrm{R}) \arrow[r, shift right, "\alpha_{\mathrm{b}}"'] & LE^{\#} \arrow[l, shift right, "\gamma_{\mathrm{b}}"']
\end{tikzcd}$$

$$\gamma(<A,b>) \triangleq \{x \in R^n \mid Ax=b\}$$

线性等式系统的解集

$$\alpha(X) \triangleq \{<A,b> \mid Ax=b, \forall x \in X\}$$

X中的点所在的仿射空间



线性等式抽象域

- 域操作

$$\mathcal{X}^\sharp \cap^\sharp \mathcal{Y}^\sharp \triangleq \mathit{Gauss}\left(\left\langle \begin{bmatrix} \mathrm{A}_{\mathcal{X}^\sharp} \\ \mathrm{A}_{\mathcal{Y}^\sharp} \end{bmatrix}, \begin{bmatrix} \mathrm{b}_{\mathcal{X}^\sharp} \\ \mathrm{b}_{\mathcal{Y}^\sharp} \end{bmatrix} \right\rangle\right)$$

$$\mathcal{X}^\sharp =^\sharp \mathcal{Y}^\sharp \overset{\Delta}{\iff} \mathrm{A}_{\mathcal{X}^\sharp} = \mathrm{A}_{\mathcal{Y}^\sharp} \quad \text{and} \quad \mathrm{b}_{\mathcal{X}^\sharp} = \mathrm{b}_{\mathcal{Y}^\sharp}$$

$$\mathcal{X}^\sharp \sqsubseteq^\sharp \mathcal{Y}^\sharp \overset{\Delta}{\iff} \mathcal{X}^\sharp \cap^\sharp \mathcal{Y}^\sharp =^\sharp \mathcal{X}^\sharp$$

$$\mathrm{C}[\![\textstyle\sum_j \alpha_j \mathtt{V}_\mathtt{j} - \beta = 0]\!]^\sharp(\mathcal{X}^\sharp) \triangleq \mathit{Gauss}\left(\left\langle \begin{bmatrix} \mathrm{A}_{\mathcal{X}^\sharp} \\ \alpha_1 \cdots \alpha_n \end{bmatrix}, \begin{bmatrix} \mathrm{b}_{\mathcal{X}^\sharp} \\ \beta \end{bmatrix} \right\rangle\right)$$

$$\mathrm{C}[\![e \bowtie 0]\!]^\sharp(\mathcal{X}^\sharp) \triangleq \mathcal{X}^\sharp \qquad \text{for other tests}$$

$\sqsubseteq^\sharp$, $=^\sharp$, $\cap^\sharp$, $=^\sharp$, $\mathrm{C}[\![\sum_j \alpha_j \mathtt{V}_\mathtt{j} - \beta = 0]\!]^\sharp$ 是精确的，因为

$$\mathcal{X}^\sharp \sqsubseteq^\sharp \mathcal{Y}^\sharp \iff \gamma(\mathcal{X}^\sharp) \subseteq \gamma(\mathcal{Y}^\sharp), \quad \gamma(\mathcal{X}^\sharp \cap^\sharp \mathcal{Y}^\sharp) = \gamma(\mathcal{X}^\sharp) \cap \gamma(\mathcal{Y}^\sharp)$$

线性等式抽象域

- 域操作

$$\mathsf{C}[\![\, \mathtt{V}_\mathtt{j} := \textstyle\sum_i \alpha_i \mathtt{V}_\mathtt{i} + \beta \,]\!]^\sharp(\mathcal{X}^\sharp) \triangleq$$

if $\alpha_j \neq 0, \mathcal{X}^\sharp$ where $\mathtt{V}_\mathtt{j}$ is replaced with$(\mathtt{V}_\mathtt{j} - \sum_{i \neq j} \alpha_i \mathtt{V}_\mathtt{i} - \beta)/\alpha_j$

if $\alpha_j = 0, (\mathsf{C}[\![\, \sum_i \alpha_i \mathtt{V}_\mathtt{i} - \mathtt{V}_\mathtt{j} + \beta = 0 \,]\!]^\sharp \circ \mathsf{C}[\![\, \mathtt{V}_\mathtt{j} := \ ?(-\infty, +\infty) \,]\!]^\sharp)(\mathcal{X}^\sharp)$

$\mathsf{C}[\![\, \mathtt{V}_\mathtt{j} := ?(-\infty, +\infty) \,]\!]^\sharp(\mathcal{X}^\sharp) \triangleq$ GuassElimination(<$A_{\mathcal{X}^\#}$, $b_{\mathcal{X}^\#}$>, V_j)

$\mathsf{C}[\![\, \mathtt{V}_\mathtt{j} := e \,]\!]^\sharp(\mathcal{X}^\sharp) \triangleq \mathsf{C}[\![\, \mathtt{V}_\mathtt{j} := ?(-\infty, +\infty) \,]\!]^\sharp(\mathcal{X}^\sharp)$ for other assignments

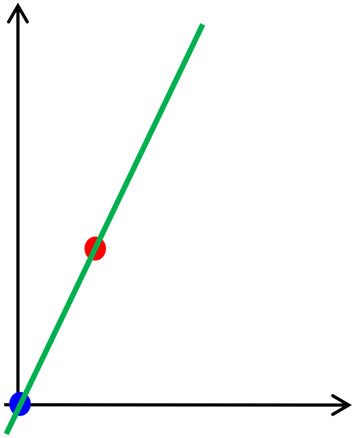
$\mathsf{C}[\![\, \mathtt{V}_\mathtt{j} := \sum_i \alpha_i \mathtt{V}_\mathtt{i} + \beta \,]\!]^\sharp, \mathsf{C}[\![\, \mathtt{V}_\mathtt{j} := ?(-\infty, +\infty) \,]\!]^\sharp$ 是精确的

线性等式抽象域

- 域操作： $\mathcal{X}^\sharp \cup^\sharp \mathcal{Y}^\sharp$

目标：给定 $\gamma(\mathcal{X}^\sharp) = \{x \mid Ax = b\}, \gamma(\mathcal{Y}^\sharp) = \{x \mid A'x = b'\}$

求仿射闭包 $\mathcal{X}^\sharp_H$ 使得 $\gamma(\mathcal{X}^\sharp) \subseteq \gamma(\mathcal{X}^\sharp_H)$ 且 $\gamma(\mathcal{Y}^\sharp) \subseteq \gamma(\mathcal{X}^\sharp_H)$



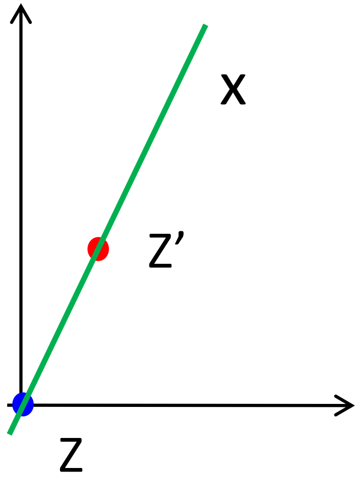
线性等式抽象域

- 域操作： $\mathcal{X}^\sharp \cup^\sharp \mathcal{Y}^\sharp$

目标：给定 $\gamma(\mathcal{X}^\sharp) = \{x \mid Ax = b\}, \gamma(\mathcal{Y}^\sharp) = \{x \mid A'x = b'\}$

求仿射闭包 $\mathcal{X}_H^\sharp$ 使得 $\gamma(\mathcal{X}^\sharp) \subseteq \gamma(\mathcal{X}_H^\sharp)$ 且 $\gamma(\mathcal{Y}^\sharp) \subseteq \gamma(\mathcal{X}_H^\sharp)$

$$\gamma(\mathcal{X}_H^\sharp) = \left\{ x \;\middle|\; \begin{array}{c} x = \sigma_1 z + \sigma_2 z' \wedge \sigma_1 + \sigma_2 = 1 \wedge \\ Az = b \quad \wedge \quad A'z' = b' \end{array} \right\}$$



线性等式抽象域

- 域操作： $\mathcal{X}^\sharp \cup^\sharp \mathcal{Y}^\sharp$

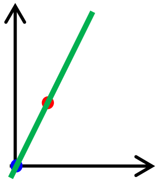
目标：给定 $\gamma(\mathcal{X}^\sharp) = \{x \mid Ax = b\}, \gamma(\mathcal{Y}^\sharp) = \{x \mid A'x = b'\}$

求仿射闭包 $\mathcal{X}^\sharp_H$ 使得 $\gamma(\mathcal{X}^\sharp) \subseteq \gamma(\mathcal{X}^\sharp_H)$ 且 $\gamma(\mathcal{Y}^\sharp) \subseteq \gamma(\mathcal{X}^\sharp_H)$

$$\gamma(\mathcal{X}^\sharp_H) = \left\{ x \;\middle|\; \begin{array}{c} x = \sigma_1 z + \sigma_2 z' \wedge \sigma_1 + \sigma_2 = 1 \wedge \\ Az = b \quad \wedge \quad A'z' = b' \end{array} \right\}$$

引入变量 $y = \sigma_1 z$
$y' = \sigma_2 z'$

$$\gamma(\mathcal{X}^\sharp_{AH}) = \left\{ x \;\middle|\; \begin{array}{c} x = y + y' \quad \wedge \sigma_1 + \sigma_2 = 1 \;\; \wedge \\ Ay \leq \sigma_1 b \;\; \wedge \;\; A'y' \leq \sigma_2 b' \end{array} \right\}$$



从 $\gamma(\mathcal{X}^\sharp_{AH})$ 中投影掉变量 $\sigma_1, \sigma_2, y, y'$ 即可

线性等式抽象域

$\mathcal{X}^\sharp \cup^\sharp \mathcal{Y}^\sharp$ 是最佳的但不是精确的

- 域操作： $\mathcal{X}^\sharp \cup^\sharp \mathcal{Y}^\sharp$

目标：给定 $\gamma(\mathcal{X}^\sharp) = \{x \mid Ax = b\}, \gamma(\mathcal{Y}^\sharp) = \{x \mid A'x = b'\}$

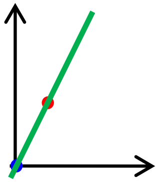
求仿射闭包 $\mathcal{X}^\sharp_H$ 使得 $\gamma(\mathcal{X}^\sharp) \subseteq \gamma(\mathcal{X}^\sharp_H)$ 且 $\gamma(\mathcal{Y}^\sharp) \subseteq \gamma(\mathcal{X}^\sharp_H)$

$$\gamma(\mathcal{X}^\sharp_H) = \left\{ x \;\middle|\; \begin{array}{c} x = \sigma_1 z + \sigma_2 z' \wedge \sigma_1 + \sigma_2 = 1 \wedge \\ Az = b \quad \wedge \quad A'z' = b' \end{array} \right\}$$

引入变量 $\begin{array}{l} y = \sigma_1 z \\ y' = \sigma_2 z' \end{array}$

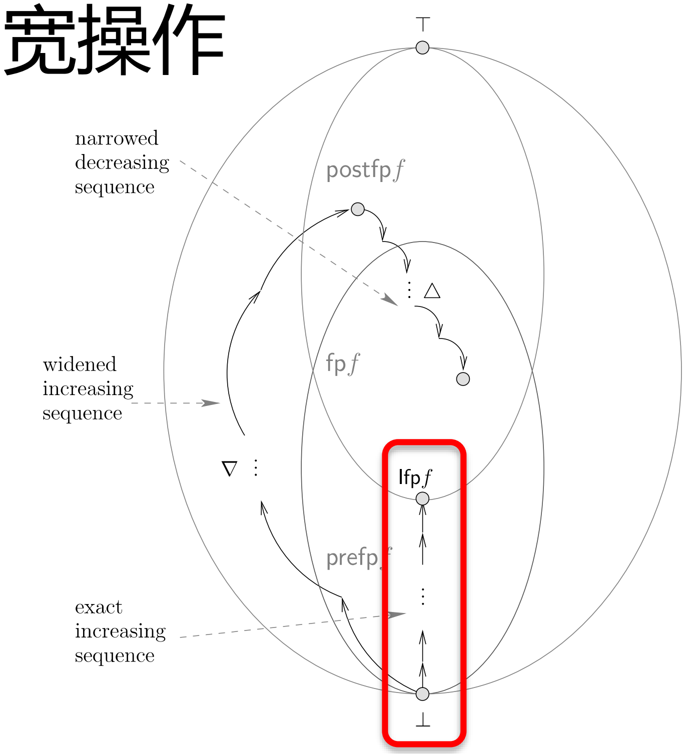
$$\gamma(\mathcal{X}^\sharp_{AH}) = \left\{ x \;\middle|\; \begin{array}{c} x = y + y' \quad \wedge \sigma_1 + \sigma_2 = 1 \ \wedge \\ Ay \leq \sigma_1 b \ \wedge \ A'y' \leq \sigma_2 b' \end{array} \right\}$$

从 $\gamma(\mathcal{X}^\sharp_{AH})$ 中投影掉变量 $\sigma_1, \sigma_2, y, y'$ 即可



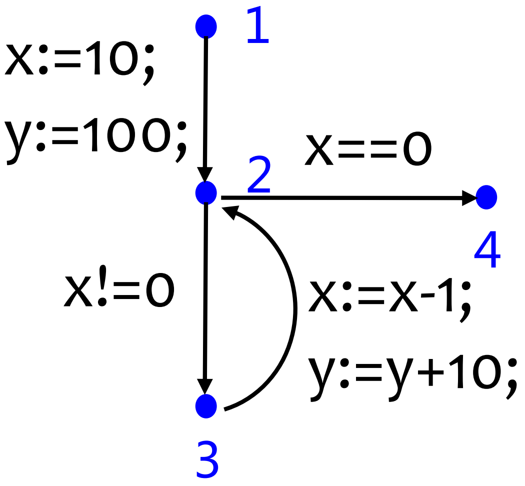
线性等式抽象域

- 程序变量间线性等式集合构成的格的高度是有穷的
  - n个程序变量之间最多存在n个线性等式
  - 所以不需要加宽操作



线性等式抽象域

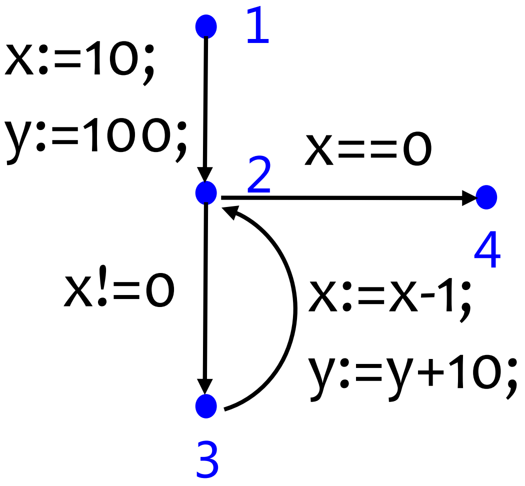
- 程序分析示例



```
1 x:=10;  y:=100;
2 while ( x!=0)  do
3    x:=x-1; y:=y+10;
  done 4
```

线性等式抽象域

- 程序分析示例

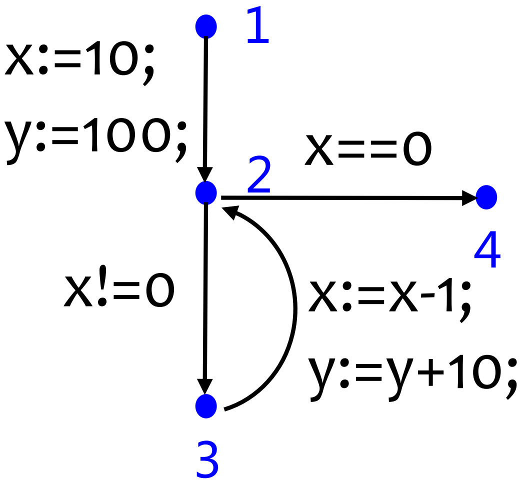


ℓ	$X_\ell^{\#0}$				
1	$\top^\#$				
2	$\bot^\#$				
3	$\bot^\#$				
4	$\bot^\#$				

```
1 x:=10;  y:=100;
2 while ( x!=0)  do
3    x:=x-1; y:=y+10;
  done 4
```

线性等式抽象域

- 程序分析示例

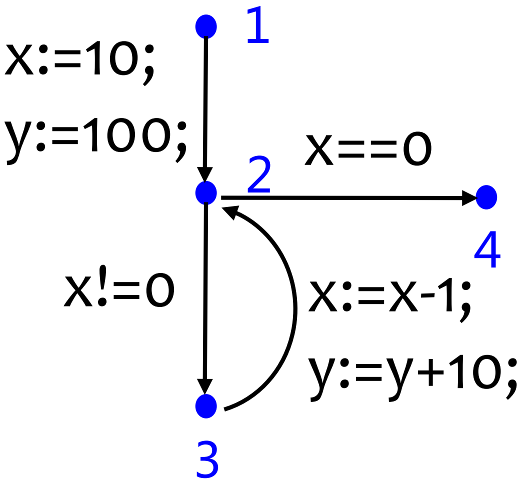


ℓ	$\mathcal{X}_\ell^{\#0}$	$\mathcal{X}_\ell^{\#1}$			
1	$\top^\#$	$\top^\#$			
2	$\bot^\#$	(10,100)			
3	$\bot^\#$	$\bot^\#$			
4	$\bot^\#$	$\bot^\#$			

```
1 x:=10;  y:=100;
2 while ( x!=0)  do
3    x:=x-1; y:=y+10;
  done 4
```

线性等式抽象域

- 程序分析示例

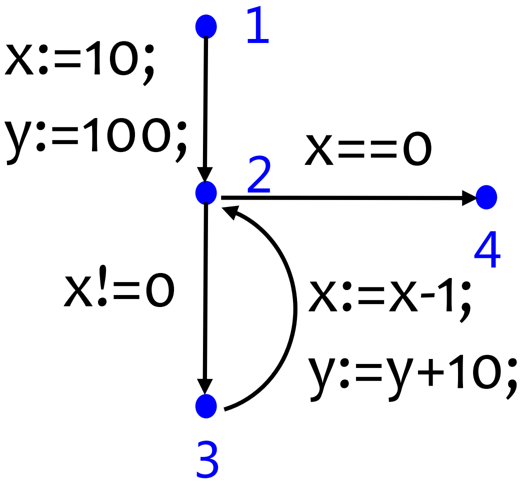


ℓ	$X_\ell^{\#0}$	$X_\ell^{\#1}$	$X_\ell^{\#2}$		
1	$\top^\#$	$\top^\#$	$\top^\#$		
2	$\bot^\#$	(10,100)	(10,100)		
3	$\bot^\#$	$\bot^\#$	(10,100)		
4	$\bot^\#$	$\bot^\#$	$\bot^\#$		

```
1 x:=10;  y:=100;
2 while ( x!=0)  do
3    x:=x-1; y:=y+10;
  done 4
```

线性等式抽象域

- 程序分析示例



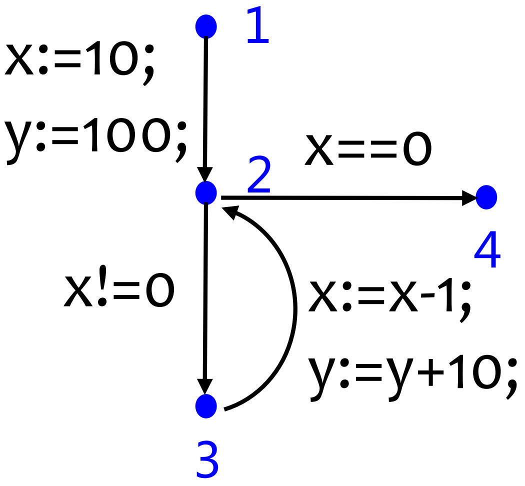
ℓ	$X_\ell^{\#0}$	$X_\ell^{\#1}$	$X_\ell^{\#2}$	$X_\ell^{\#3}$
1	$\top^\#$	$\top^\#$	$\top^\#$	$\top^\#$
2	$\bot^\#$	(10,100)	(10,100)	10x+y=200
3	$\bot^\#$	$\bot^\#$	(10,100)	(10,100)
4	$\bot^\#$	$\bot^\#$	$\bot^\#$	$\bot^\#$

```
1 x:=10;  y:=100;
2 while ( x!=0)  do
3    x:=x-1; y:=y+10;
  done 4
```

$$X_2^{\#3} = \{(10,100)\} \cup^{\#} \{(9,110)\} = \{(x,y) \mid 10x+y=200\}$$

线性等式抽象域

- 程序分析示例



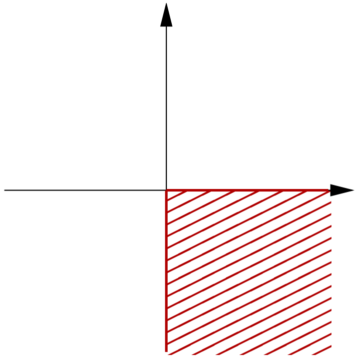
ℓ	$X_\ell^{\#0}$	$X_\ell^{\#1}$	$X_\ell^{\#2}$	$X_\ell^{\#3}$	$X_\ell^{\#4}$
1	$\top^\#$	$\top^\#$	$\top^\#$	$\top^\#$	$\top^\#$
2	$\bot^\#$	(10,100)	(10,100)	10x+y=200	10x+y=200
3	$\bot^\#$	$\bot^\#$	(10,100)	(10,100)	10x+y=200
4	$\bot^\#$	$\bot^\#$	$\bot^\#$	$\bot^\#$	(0,200)

```
1 x:=10;  y:=100;
2 while ( x!=0)  do
3     x:=x-1; y:=y+10;
  done 4
```

$$X_2^{\#3} = \{(10,100)\} \cup^{\#} \{(9,110)\} = \{(x,y) \mid 10x+y=200\}$$

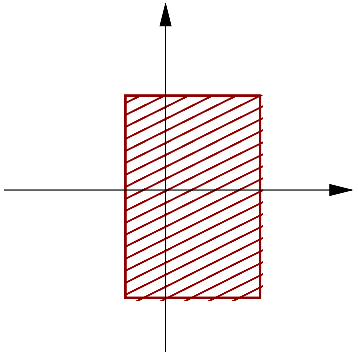
数值抽象域—谱系

非关系型



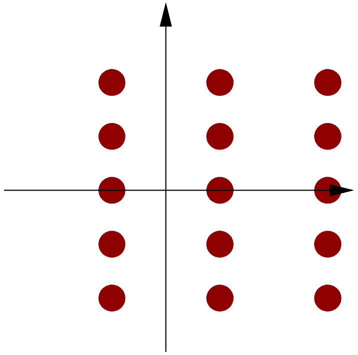
$X_i \geqslant 0,\ X_i \leqslant 0$

符号域



$X_i \in [a_i, b_i]$

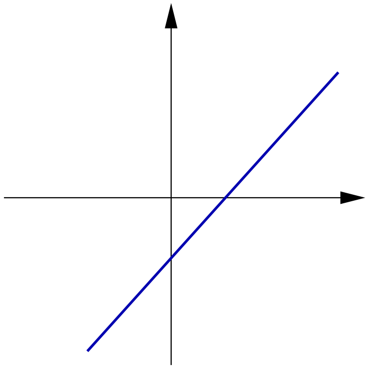
区间域



$X_i \equiv a_i [b_i]$

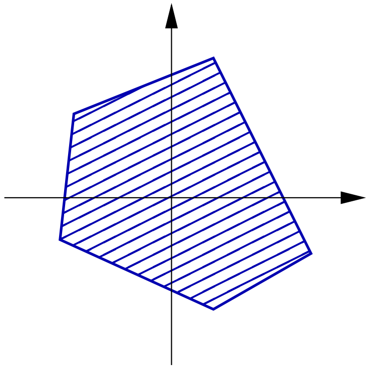
同余域

关系型



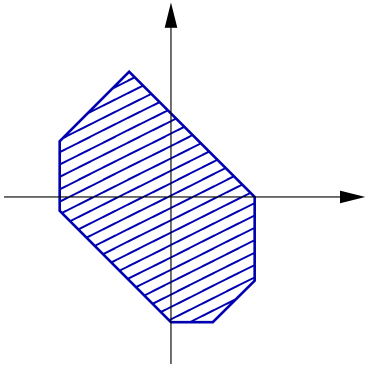
$\sum_i \alpha_{ij} X_i = \beta_j$

线性等式域



$\sum_i \alpha_{ij} X_i \leqslant \beta_j$

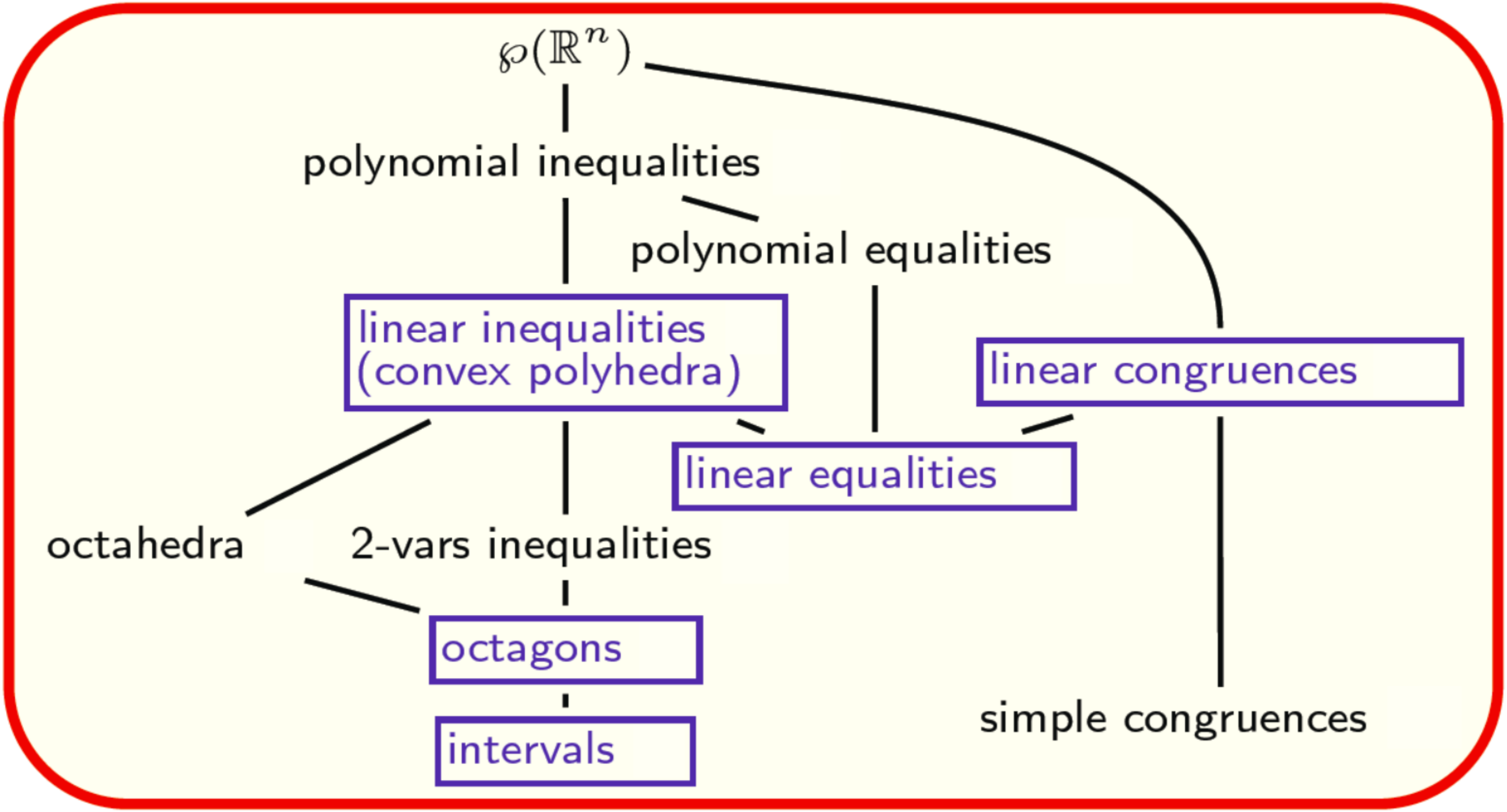
多面体域



$\pm X_i \pm X_j \leq c$

八边形域

数值抽象域—谱系


$\wp(\mathbb{R}^n)$
polynomial inequalities
polynomial equalities
linear inequalities (convex polyhedra)
linear congruences
linear equalities
octahedra
2-vars inequalities
octagons
intervals
simple congruences

谢谢！