CS615: Formal Specification and Verification of Programs 2019

Lecture 13: Abstract interpretation

Instructor: Ashutosh Gupta

IITB, India

Compile date: 2019-09-28

Topic 13.1

Abstract fixed point

Abstract operations

Let us suppose we have the following Galois connection

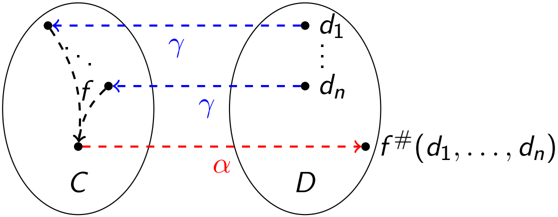
$$(C, \subseteq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (D, \sqsubseteq).$$

Let us suppose we also have a function $f : C^n \rightarrow C$ in concrete domain C.

Definition 13.1

We define an abstract operation $f^\# : D^n \rightarrow D$ *as follows*

$$f^\#(d_1, \dots, d_n) = \alpha \circ f(\gamma(d_1), \dots, \gamma(d_n))$$



Example: abstract operation

We use f, α, and γ to implement $f^{\#}$.

For example,

- We may implement $\sqcup$ as follows

Why would this be correct?

$$x \sqcup y = \alpha(\gamma(x) \cup \gamma(y))$$

- We may implement $\sqcap$ as follows

$$x \sqcap y = \alpha(\gamma(x) \cap \gamma(y))$$

Example 13.1

Consider interval domain. Let us compute $[0,3] \sqcup [8,11]$.

- $[0,3] \sqcup [8,11] = \alpha(\gamma([0,3]) \cup \gamma([8,11])) = \alpha([0,3] \cup [8,11]) = [0,11]$

Commentary: The $\sqcup$ computation may look a simple thing made complex. However, the above captures the idea that the function calculation

Abstract strongest post

Recall from earlier lecture, we discussed abstract post. Now we have the formal definition.

$$sp^{\#}(d, \rho) = \alpha \circ sp(\gamma(d), \rho)$$

Example 13.2 (Reminder)

Recall the following abstraction function

$$wideOne(X) = \{n+1, n | n \in X\}$$

We defined the following abstract post

$$sp^{\#}(F, \rho) = \underbrace{wideOne}_{\alpha}(sp(\underbrace{F}_{\gamma \text{ is identity}}, \rho))$$

Abstract reachability equations

For program $P = (V, L, \ell_0, \ell_e, E)$, we solve the following reachability equation in the abstract domain.

$$X_{\ell_0} = \alpha(\top)$$

$$\forall \ell' \in L \setminus \{\ell_0\}. \qquad X_{\ell'} = \bigsqcup_{(\ell,\rho,\ell') \in E} sp^{\#}(X_\ell, \rho)$$

Our goal is to show that $X_{\ell_e} = \bot$.

If a solution of the above equations exists with $X_{\ell_e} = \bot$, then the program is safe.

Abstract fixed-point equations

For each $\ell' \in L$, consider the following function $F^{\#}_{\ell'}$ where X is input and return a set of valuations.

$$F^{\#}_{\ell'}(X) = \underbrace{X_{\ell'}}_{\text{known reaching abstract state}} \sqcup \underbrace{\bigsqcup_{(\ell,\rho,\ell')\in E} sp^{\#}(X_{\ell}, \rho)}_{\text{more reaching abstract state due to neighbours}}$$

Now, let us define the following function.

$$F^{\#}(X) = [F^{\#}_{\ell_0}(X), F^{\#}_{\ell_1}(X), ...]$$

A fixed point of $F^{\#}$ approximates the reachable states.

Computing approximate least fixed point

We know $F : C \to C$ is a monotonic operator.

Our goal is to compute $lfp_a(F)$, which is in general impossible, where $a = [\top, \bot, ..., \bot]$.

Notation recall: $lfp_a(F)$ is a fixed point of f that is greater than a.

We compute an approximation of $lfp_a(f)$, i.e.,

$$lfp_{\alpha(a)}(F^{\#}).$$

Computing $lfp_{\alpha(a)}(F^\#)$

Both $\bigsqcup$ and $sp^\#$ can be implemented using

1. α,
2. $\cup$, and
3. γ.

If we have algorithms to implement the above three operations, we can implement fixed-point iterations.

Convergence/termination is still not guaranteed.

At least, we can implement.

Approximation guarantees

Theorem 13.1

Let $(C, \subseteq, \emptyset, \mathbb{Q}^V, \cup, \cap)$ *and* $(D, \sqsubseteq, \bot, \top, \sqcup, \sqcap)$ *are complete lattices,*

$$(C, \subseteq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (D, \sqsubseteq),$$

and $f : C \to C$ *and* $f^{\#}$ *are continuous operators then*

$$lfp_a(f) \subseteq \gamma(lfp_{\alpha(a)}(f^{\#}))$$

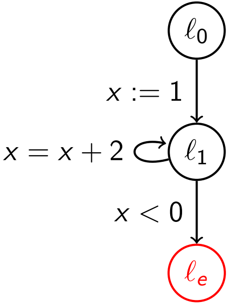
Exercise 13.1

Prove the above theorem *Hint: First show iterates on both the sides are related*

Example : abstract fixed point computation

Example 13.3

Consider program:



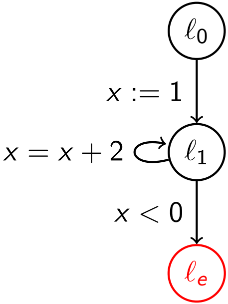
Let us use sign abstraction *to analyze the program*
$D = \{\top, +, -, 0, \bot\}$

Initial abstract state:
$X^0_{\ell_0} := \alpha(\top) = \top,$
$X^0_{\ell_1} := \alpha(\bot) = \bot,$
$X^0_{\ell_e} := \alpha(\bot) = \bot$

Example : abstract fixed point computation (contd.) II

First iteration:

Consider program:



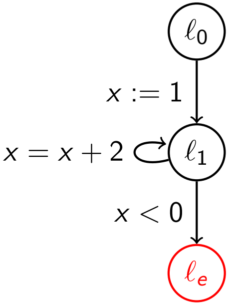
$$X^1_{\ell_0} = X^0_{\ell_0} = \top$$

$$X^1_{\ell_1} = X^0_{\ell_1} \sqcup sp^{\#}(x' = 1, X^0_{\ell_0}) \sqcup sp^{\#}(x' = x + 2, X^0_{\ell_1})$$
$$= \bot \sqcup \alpha(sp(x' = 1, \gamma(X^0_{\ell_0}))) \sqcup \alpha(sp(x' = x+2, \gamma(X^0_{\ell_1})))$$
$$= \alpha(sp(x' = 1, \gamma(\top))) \sqcup \alpha(sp(x' = x + 2, \gamma(\bot)))$$
$$= \alpha(sp(x' = 1, \gamma(\top))) \sqcup \alpha(\bot)$$
$$= \alpha(x = 1) \sqcup \alpha(\bot) = + \sqcup \alpha(\bot) = +$$

$$X^1_{\ell_e} := X^0_{\ell_e} \sqcup sp^{\#}(x < 0, X^0_{\ell_1}) = \bot$$
$$= \bot \sqcup \alpha(sp(x < 0, \gamma(X^0_{\ell_0})))$$
$$= \bot \sqcup \alpha(sp(x < 0, \gamma(\bot)))$$
$$= \bot \sqcup \alpha(sp(x < 0, \bot)) = \bot \sqcup \alpha(\bot) = \bot$$

Example : abstract fixed point computation (contd.) III

Consider program:



Second iteration:

$$X^2_{\ell_0} = X^1_{\ell_0} = \top$$

$$\begin{aligned}X^2_{\ell_1} &= X^1_{\ell_1} \sqcup sp^{\#}(x' = 1, X^1_{\ell_0}) \sqcup sp^{\#}(x' = x + 2, X^1_{\ell_1})\\ &= + \sqcup \alpha(sp(x' = 1, \gamma(X^1_{\ell_0}))) \sqcup \alpha(sp(x' = x + 2, \gamma(X^1_{\ell_1})))\\ &= + \sqcup \alpha(sp(x' = 1, \gamma(\top))) \sqcup \alpha(sp(x' = x + 2, \gamma(+)))\\ &= + \sqcup \alpha(sp(x' = 1, \gamma(\top))) \sqcup \alpha(x > 2)\\ &= + \sqcup \alpha(x = 1) \sqcup \alpha(x > 2) = + \sqcup + \sqcup + = +\end{aligned}$$

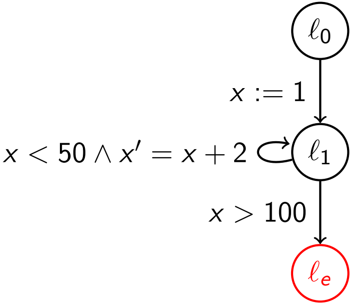
Fixed point reached

$$\begin{aligned}X^2_{\ell_e} &:= X^1_{\ell_e} \sqcup sp^{\#}(x < 0, X^1_{\ell_1}) = \bot\\ &= \bot \sqcup \alpha(sp(x < 0, \gamma(X^1_{\ell_0})))\\ &= \bot \sqcup \alpha(sp(x < 0, \gamma(+)))\\ &= \bot \sqcup \alpha(sp(x < 0, x > 0)) = \bot \sqcup \alpha(\bot) = \bot\end{aligned}$$

Exercise: sign abstraction fixedpoint

Exercise 13.2

Apply sign abstraction on the following example?



Exercise: sign abstraction fixedpoint

Exercise 13.3

Apply sign abstraction on the following example?

```
main (){
  x := 0;
  y := -1;
  while( x < 20 ) {
    if( x < 10 ) {
      y := y - 1;
    }else{
      y := y + 1;
    }
    x = x + 1;
  }
}
```

Note that there is no error location in the above program.

Demo - The Interproc Analyzer

http://pop-art.inrialpes.fr/interproc/interprocweb.cgi

Exercise 13.4

Run Interproc on the following code

```
var i:int;
begin
  i = 0;
  while (i<=10) do
    i = i+2;
  done;
end
```

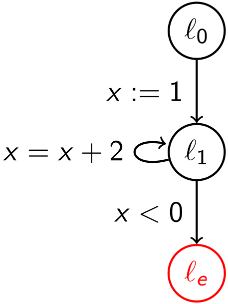
Example: interval abstraction

One may feel sign abstraction is too coarse. Let us try more precise/refined

interval abstraction.

Example 13.4

Consider program:



Let us use interval abstraction:

$\bot \sqsubseteq [a, b] \sqsubseteq \top$

Initial abstract state:

$X^0_{\ell_0} := \top,$

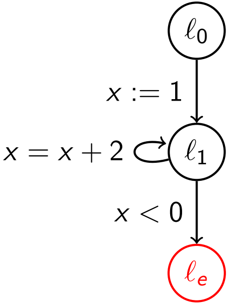
$X^0_{\ell_1} := \bot,$

$X^0_{\ell_e} := \bot$

Example: interval abstraction(contd.)

First iteration

Consider program:



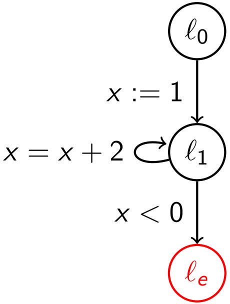
$X^1_{\ell_0} := X^0_{\ell_0} = \top$

$$X^1_{\ell_1} := X^0_{\ell_1} \sqcup sp^{\#}(x' = 1, X^0_{\ell_0}) \sqcup sp^{\#}(x' = x + 2, X^0_{\ell_1})$$
$$= \bot \sqcup \alpha(sp(x' = 1, \gamma(X^0_{\ell_0}))) \sqcup \alpha(sp(x' = x+2, \gamma(X^0_{\ell_1})))$$
$$= \alpha(sp(x' = 1, \gamma(\top))) \sqcup \bot$$
$$= \alpha(sp(x' = 1, \gamma(\top))) = \alpha(x = 1) = [1, 1]$$

$$X^1_{\ell_e} := X^0_{\ell_e} \sqcup sp^{\#}(x < 0, X^0_{\ell_1}) = \bot$$
$$= \bot \sqcup \alpha(sp(x < 0, \gamma(X^0_{\ell_0})))$$
$$= \bot \sqcup \alpha(sp(x < 0, \gamma(\bot)))$$
$$= \bot \sqcup \alpha(sp(x < 0, \bot)) = \bot \sqcup \alpha(\bot) = \bot$$

Example: interval abstraction(contd.)

Consider program:



Second iteration

$$X^2_{\ell_0} := X^1_{\ell_0} = \top$$

$$\begin{aligned}X^2_{\ell_1} &= X^1_{\ell_1} \sqcup sp^{\#}(x' = 1, X^1_{\ell_0}) \sqcup sp^{\#}(x' = x + 2, X^1_{\ell_1})\\ &= [1,1] \sqcup \alpha(sp(x' = 1, \gamma(\top)))\sqcup\\ &\quad \alpha(sp(x' = x + 2, \gamma([1,1])))\\ &= [1,1] \sqcup \alpha(sp(x' = 1, \top)) \sqcup \alpha(sp(x' = x + 2, [1,1]))\\ &= [1,1] \sqcup [1,1] \sqcup [3,3] = [1,3]\end{aligned}$$

$$X^2_{\ell_e} := \bot$$

After third iteration $X^3_{\ell_0} := \top, X^3_{\ell_1} := [1,5], X^3_{\ell_e} := \bot$

... the process will go on forever

Acceleration

Many interesting abstract domains are of infinite size.

Abstraction may only provide simple calculations, but not convergence.

For convergence we need acceleration using a special operator widening.

If we do too much widening then we may need narrowing.

Widening

Definition 13.2

A *widening* $\nabla : D \times D \to D$ *on a poset* $(D, \sqsubseteq)$ *satisfies*

- $\forall x, y \in D.\ x \sqsubseteq x \nabla y \land y \sqsubseteq x \nabla y$
- *for an increasing chain* $x_0 \sqsubseteq x_1 \ldots$, *the increasing chain*

$$y^0 \triangleq x^0 \qquad y^n \triangleq y^{n-1} \nabla x^n$$

is not strictly increasing.

Definition 13.3

widening iterates $(\mathrm{I}^k, k < n)$ *for monotone function* f *from* $a \in prefp(f)$

- $\mathrm{I}^0 \triangleq a$
- $\mathrm{I}^{n+1} \triangleq \mathrm{I}^n \qquad if\ f(\mathrm{I}^n) \sqsubseteq \mathrm{I}^n$
- $\mathrm{I}^{n+1} \triangleq \mathrm{I}^n \nabla f(\mathrm{I}^n) \quad if\ f(\mathrm{I}^n) \not\sqsubseteq \mathrm{I}^n$

Theorem 13.2

There exists $k \in \mathbb{N}$, $f(\mathrm{I}^k) \sqsubseteq \mathrm{I}^k$ *and* $lfp_a(f) \sqsubseteq \mathrm{I}^k$.

widening for interval domain

We define a widening operator for interval as follows:

- $[a, b] \nabla \bot = [a, b]$
- $\bot \nabla [a, b] = [a, b]$
- $[a, b] \nabla [a', b'] = [((a' < a)? - \infty : a), ((b' > b)? \infty : b)]$

Exercise 13.5

Apply the ∇ operator

- $[2, 3] \nabla [-3, 2] =$
- $[2, 3] \nabla [4, 6] =$
- $[2, 3] \nabla [1, 6] =$
- $\bot \nabla \bot =$

Exercise 13.6

a. Show ∇ for interval domain satisfies the definition of widening

b. Show ∇ is not symmetric and monotone

Abstract fixed-point equations with widening

For each $\ell' \in L$, consider the following function $F^{\nabla}_{\ell'}$ where X is input and return a set of valuations.

$$F^{\nabla}_{\ell'}(X) = \underbrace{X_{\ell'}}_{\text{known reaching abstract state}} \quad \nabla \quad \underbrace{\bigsqcup_{(\ell,\rho,\ell')\in E} sp^{\#}(X_\ell, \rho)}_{\text{more reaching abstract state due to neighbours}}$$

Now, let us define the following function.

$$F^{\nabla}(X) = [F^{\nabla}_{\ell_0}(X), F^{\nabla}_{\ell_1}(X), ...]$$

A $lfp_a(F^{\nabla})$ will be in $postfp_a(F^{\#})$.(why?)

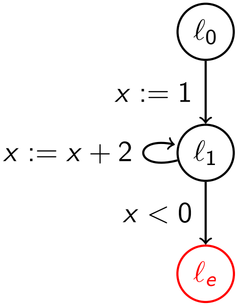
Exercise 13.7

The iterations generated by $F^{\#}$ do not exactly match with widening iterates of definition 13.3. What we need to assume on ∇ to match them?

Example: widening in action

Example 13.5

Consider program:



Initial:
$X^0_{\ell_0} := \top, X^0_{\ell_1} := \bot, X^0_{\ell_e} := \bot$

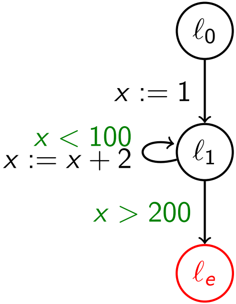
First iteration:(nothing changed)
$X^1_{\ell_0} := \top, X^1_{\ell_1} := [1,1], X^1_{\ell_e} := \bot$

Second iteration:
$X^2_{\ell_0} := \top,$
$X^2_{\ell_1} := X^1_{\ell_1} \nabla (sp^\#(x' = 1, X^1_{\ell_0}) \sqcup sp^\#(x' = x + 2, X^1_{\ell_1}))$
$= [1,1] \nabla ([1,1] \sqcup [3,3]) = [1,1] \nabla [1,3] = [1, +\infty]$
$X^2_{\ell_e} := \bot$

Third iteration:
$X^3_{\ell_0} := \top,$
$X^3_{\ell_1} := X^2_{\ell_1} \nabla (sp^\#(x' = 1, X^2_{\ell_0}) \sqcup sp^\#(x' = x + 2, X^2_{\ell_1}))$
$= [1,1] \nabla ([1,1] \sqcup [1, +\infty]) = [1, +\infty]$
$X^3_{\ell_e} := \bot$ .... fixed point reached

Example: too much widening

Now consider:



$$X^0_{\ell_1} := \bot, X^0_{\ell_e} := \bot$$

$$X^1_{\ell_1} := [1,1], X^0_{\ell_e} := \bot$$

$$X^2_{\ell_1} = [1,1] \nabla ([1,1] \sqcup sp^\#(x < 100 \wedge x' = x + 2, X^1_{\ell_1}))$$
$$= [1,1] \nabla ([1,1] \sqcup [3,3]) = [1, +\infty]$$
$$X^2_{\ell_1} := [1, +\infty], X^2_{\ell_e} := \bot$$

$$X^3_{\ell_e} = X^2_{\ell_e} \nabla (sp^\#(x > 200 \wedge x' = x, X^2_{\ell_1}))$$
$$X^3_{\ell_e} = \bot \nabla (sp^\#(x > 200 \wedge x' = x, [1, +\infty]))$$
$$X^3_{\ell_e} = \bot \nabla [200, +\infty] = [200, +\infty]$$
$$X^2_{\ell_1} := [1, +\infty], X^3_{\ell_e} = [200, +\infty]$$

... reaching error location

Narrowing

Unfortunate misnomer!!
Narrowing is not the dual of widening!

Definition 13.4

A narrowing $\triangle : D \times D \rightarrow D$ *on a poset* $(D, \sqsubseteq)$ *satisfies*

- $\forall x, y \in D.\ y \sqsubseteq x \Rightarrow y \sqsubseteq x \triangle y \sqsubseteq x$
- *for an decreasing chain* $\dots x_1 \sqsubseteq x_0$, *the decreasing chain*

$$y^0 \triangleq x^0 \qquad y^n \triangleq y^{n-1} \triangle x^n$$

is not strictly decreasing.

Definition 13.5

narrowing iterates $(\mathrm{I}^k, k < n)$ *for monotone function* f *from* $a \in postfp(f)$

- $\mathrm{I}^0 \triangleq a$
- $\mathrm{I}^{n+1} \triangleq \mathrm{I}^n \qquad$ *if* $f(\mathrm{I}^n) = \mathrm{I}^n$
- $\mathrm{I}^{n+1} \triangleq \mathrm{I}^n \triangle f(\mathrm{I}^n) \quad$ *if* $\mathrm{I}^n \sqsubseteq f(\mathrm{I}^n)$

Theorem 13.3

For all $x \in X.\ x = f(x) \sqsubseteq a \Rightarrow \exists k.\ x \sqsubseteq \mathrm{I}^k = \mathrm{I}^{k+1} \sqsubseteq a$

Narrowing for interval abstraction

A definition of narrowing for the interval domain

- $\bot \triangle [a, b] = \bot$
- $[a, b] \triangle [a', b'] = [((a = -\infty)?a' : a), ((b = \infty)?b' : b)]$ if $[a', b'] \sqsubseteq [a, b]$

Exercise 13.8

Apply the $\triangle$ operator

- $[1, 3] \triangle [1, 2] =$
- $[2, 3] \triangle [4, 6] =$
- $[-\infty, 6] \triangle [1, 3] =$
- $\bot \triangle [1, 3] =$

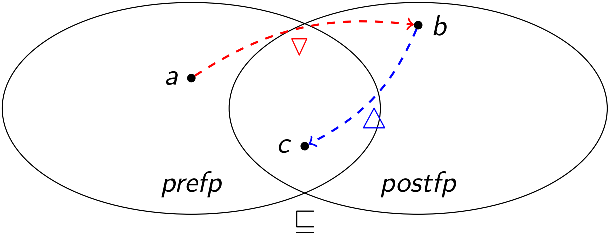
Exercise 13.9

Show $\triangle$ for interval domain satisfy the definition of the narrowing operator.

Using narrowing after widening

Let us suppose we have monotonic $f : D \to D$, $a \in prefp(f)$, widening ∇, and narrowing $\triangle$.

- Apply widening iterates to obtain b such that $a \sqsubseteq b \in postfp(f)$
- Then, apply narrowing iterates to obtain c such that $c = f(c) \sqsubseteq b$



Exercise 13.10

Show $a \sqsubseteq c$.

Example: narrowing interval domain

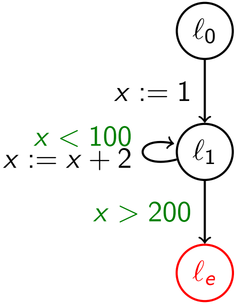
Example 13.6

Result of widening iterates:

$X^3_{\ell_1} := [1, +\infty], X^3_{\ell_e} := [200, +\infty]$

Now consider:

Forth iteration with narrowing:



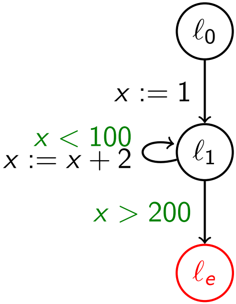
$$
\begin{aligned}
X^4_{\ell_1} &:= X^3_{\ell_1} \triangle ([1,1] \sqcup sp^{\#}(x < 100 \wedge x' = x + 2, X^3_{\ell_1})) \\
&= [1,\infty] \triangle ([1,1] \sqcup sp^{\#}(x < 100 \wedge x' = x + 2, [1,\infty])) \\
&= [1,\infty] \triangle ([1,1] \sqcup [3,101]) \\
&= [1,\infty] \triangle ([1,101]) = [1,101]
\end{aligned}
$$

$$
\begin{aligned}
X^4_{\ell_e} &:= X^3_{\ell_e} \triangle (sp^{\#}(x > 200 \wedge x' = x, X^3_{\ell_1})) \\
&= [200,+\infty] \triangle (sp^{\#}(x > 200 \wedge x' = x, [1,+\infty])) \\
&= [200,+\infty] \triangle [200,+\infty] = [200,+\infty]
\end{aligned}
$$

Example: narrowing interval domain

Example 13.7

Now consider:



Fifthe iteration with widening

$$X^5_{\ell_1} := X^4_{\ell_1} \triangle ([1,1] \sqcup sp^\#(x < 100 \wedge x' = x + 2, X^4_{\ell_1})) = [1, 101]$$

$$X^5_{\ell_e} := X^4_{\ell_e} \triangle (sp^\#(x > 200 \wedge x' = x, X^4_{\ell_1})) = [200, +\infty] \triangle (sp^\#(x > 200 \wedge x' = x, [1, 101])) = [200, +\infty] \triangle \bot = \bot$$

Fixed point reached

Widening and narrowing policy

We need not apply narrowing/widening of at every iteration or for every variable.

- use narrowing/widening operators only at cut points
- use narrowing/widening operators at every ith iteration

Exercise 13.11

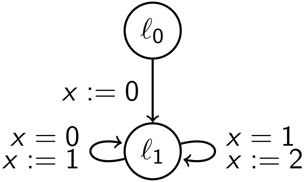
What would be definitions of duals of ∇ and $\triangle$ operators.

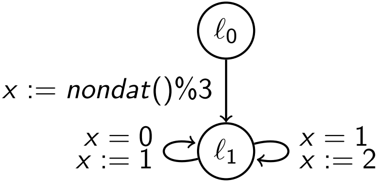
Exercise : widening chaos

The proposed machinery may have unpredictable behaviors!!

Exercise 13.12

Apply widening iterates of interval domain on the following examples





Abstract domain

An abstract domain consists of

- a lattice $(D, \sqsubseteq, \sqcup, \sqcap)$,
- a abstraction function $\alpha : C \to D$ and a concretization function $\gamma : D \to C$ such that
$$(D, \sqsubseteq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (C, \subseteq),$$
- a widening operator $\nabla : D \times D \to D$, and
- a narrowing operator $\triangle : D \times D \to D$.

End of Lecture 13