CS615: Formal Specification and Verification of Programs 2019

Lecture 8: Why abstraction?

Instructor: Ashutosh Gupta

IITB, India

Compile date: 2019-09-09

Topic 8.1

Labeled transition system (reminder)

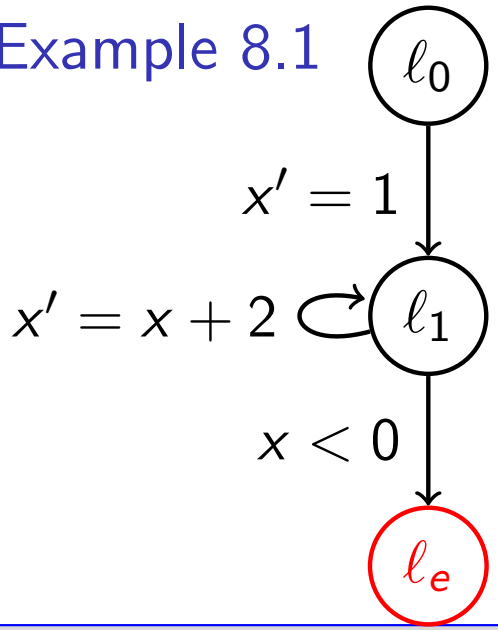
labeled transition system (LTS)

Definition 8.1

A program P is a tuple $(V, L, \ell_0, \ell_e, E)$, where

- *V is a vector of variables,*
- *L be set of program locations,*
- *ℓ_0 is initial location,*
- *ℓ_e is error location, and*
- *$E \subseteq L \times \Sigma(V, V') \times L$ is a set of labeled transitions between locations.*

Example 8.1



$$V = [\mathtt{x}]$$
$$L = \{\ell_0, \ell_1, \ell_e\}$$
$$E = \{(\ell_0, \mathtt{x}' = 1, \ell_1), (\ell_1, \mathtt{x}' = \mathtt{x} + 2, \ell_1), (\ell_1, \mathtt{x} < 0, \ell_e)\}$$

Notation:

If $e = (\ell, \rho(V, V'), \ell') \in E$, then

$e(V, V') \triangleq \rho(V, V')$,

$e(loc) \triangleq \ell$ and

$e(loc') \triangleq \ell'$

Semantics

Consider program $P = (V, L, \ell_0, \ell_e, E)$.

Definition 8.2

A state $s = (\ell, v)$ of a program is program location ℓ and a valuation v of V.

Let $v(x) \triangleq$ value of variable x in v
For state $s = (\ell, v)$, let $s(x) \triangleq v(x)$ and $s(loc) \triangleq \ell$

Definition 8.3

A path $\pi = e_1, \ldots, e_n$ in P is a sequence of transitions such that, for each $0 < i < n$, $e_i = (\ell_{i-1}, \_, \ell_i)$ and $e_{i+1} = (\ell_i, \_, \ell_{i+1})$.

Definition 8.4

An execution corresponding to path $e_1, \ldots, e_n$ is a sequence of states $(\ell_0, v_0), \ldots, (\ell_n, v_n)$ such that $\forall i \in 1..n$, $e_i(v_{i-1}, v_i)$ holds true.
An execution belongs to P if there is a corresponding path in P.

Definition 8.5

P is safe if there is no execution of P from ℓ_0 to ℓ_e.

Reminder: symbolic strongest post

$$sp : \Sigma(V) \times \Sigma(V, V') \to \Sigma(V)$$

We define symbolic post over labels of P as follows.

$$sp(F, \rho) \triangleq (\exists V : F(V) \wedge \rho(V, V'))[V/V']$$

Topic 8.2

Reachability and Abstraction

Reachability

Consider program $P = (V, L, \ell_0, \ell_e, E)$

We have seen in order to prove that no execution will reach ℓ_e, we need to compute the reachable valuations for each location in L.

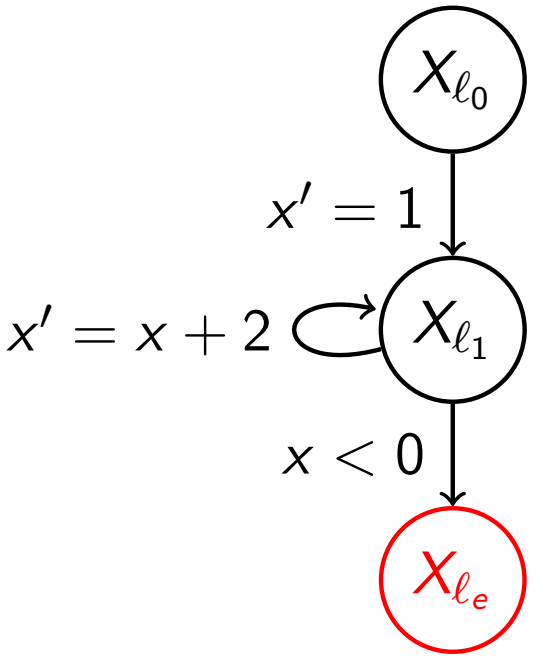
Earlier, we called the set of reachable valuations as invariants.

Reachable valuations

Let X_ℓ be a variable representing the reachable valuations at location $\ell \in L$

Let X denote the vector of X_ℓs.

Example 8.2

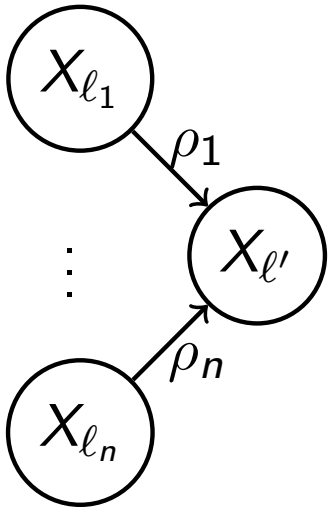


$X = [X_{\ell_0}, X_{\ell_1}, X_{\ell_0}]$

Reachability as equation

We trivially know $X_{\ell_0} = \top$.

For the other location, if we know reachable states for the sources of incoming edges we may compute the reachable states at the location.



Formally, we write the relation between reachable valuations using *sp*

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

Solving reachability equation

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

$$X_{\ell_0} = \top$$

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

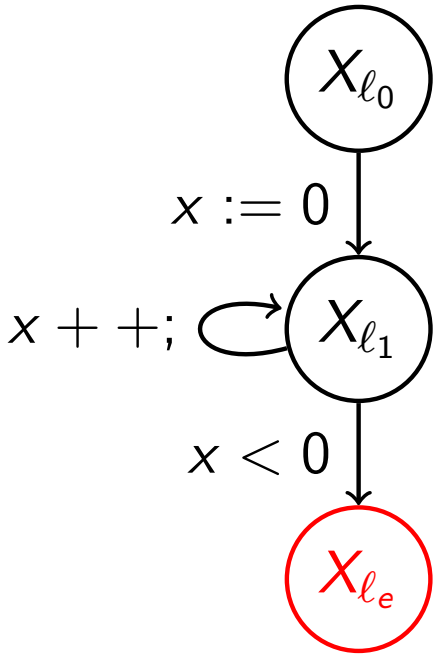
Our goal is to show that $X_{\ell_e} = \bot$.

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

Example: reachability equations

Example 8.3

Consider program:



Reachability equations:

$$X_{\ell_0} = \top$$

$$X_{\ell_1} = sp(X_{\ell_0}, x' = 0) \vee sp(X_{\ell_1}, x' = x + 1)$$

$$X_{\ell_e} = sp(X_{\ell_1}, x < 0 \wedge x' = x)$$

Since X_{ℓ_1} depends on itself, we can not compute it with some sp engine.

If somehow we have X_{ℓ_1}, we can compute others.

Hoare logic and invariants

We have seen guess and check methods for verification.

- Hoare logic
- Invariant checking

In the above, we do not truly compute X_ℓs.

We guess X_ℓs at the cut-points and check if there is a solution of the equation compatible with the following equations.

$$X_{\ell_0} = \top$$

$$\forall \ell' \in L \setminus \{\ell_0\}. \qquad \bigvee_{(\ell,\rho,\ell') \in E} sp(X_\ell, \rho) \Rightarrow X_{\ell'}$$

Not equality but implication

such that $X_{\ell_e} = \bot$.

Exercise 8.1

Write the reachability equation using wp

What if we want to compute X without guessing?

Let us try to avoid guessing and compute X.

We need to collect the reachable valuations.

Reachability as fixed point equation

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

$$F_{\ell'}(X) = \underbrace{X_{\ell'}}_{\text{known reaching valuations in X}} \vee \underbrace{\bigvee_{(\ell,\rho,\ell')\in E} sp(X_\ell, \rho)}_{\text{more reaching valuations due to neighbours}}$$

Now, let us define the following function.

$$F(X) = [F_{\ell_0}(X), F_{\ell_1}(X), ...]$$

A fixed point of F may be the solution of the reachability problem.

Exercise 8.2

a. Why may?

b. Give the least fixed point of F?

c. Give the greatest fixed point of F?

d. Are the above fixed points are solutions of the reachability?

A specific fixed point

We are interested in a specific fixed point such that

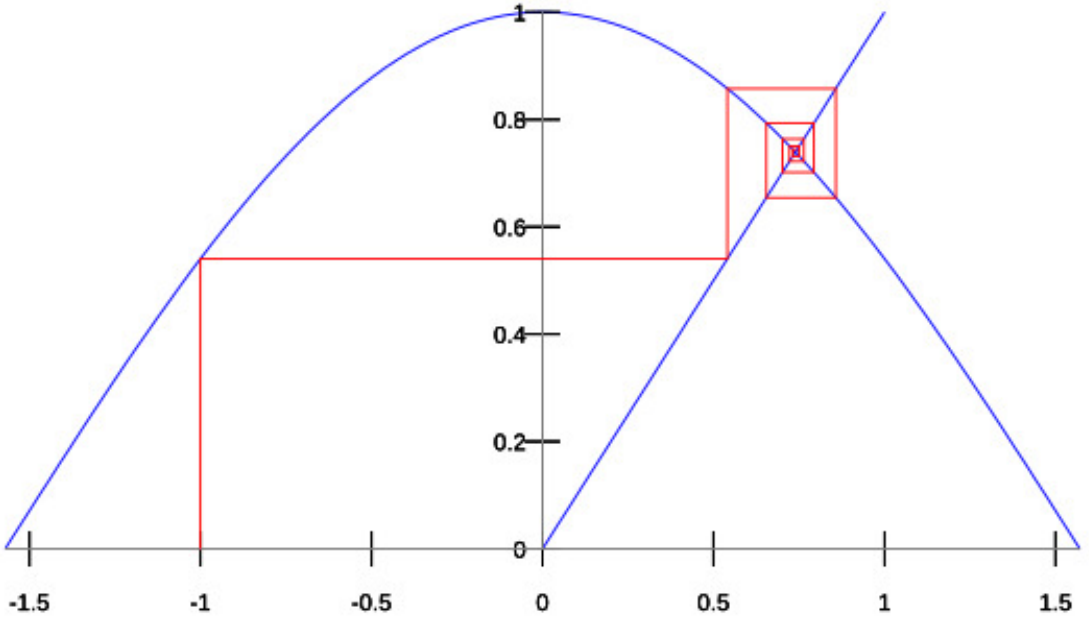
$$X_{\ell_0} = \top$$

$$X_{\ell_e} = \bot$$

The least fixed point of F violated the first requirement.

The greatest fixed point of F violated the last requirement.

Iterative fixed point computation



(source: wikipedia)

Solving $x = cos(x)$

Start with initial guess $x = -1$, keep applying cos, and hope for convergence

$$cos(cos(....cos(-1)...))$$

Similarly we may compute fixed point iteratively

Initial assignment to variables and iteratively compute the fixed point

Let $X_\ell^i \triangleq$ value of X_ℓ at ith iteration. As a vector, $X^i \triangleq [X_{\ell_0}^i, ...]$

Initially:

$$X_{\ell_0}^0 \triangleq \top \text{ and } X_\ell^0 \triangleq \bot$$

for each $\ell \neq \ell_0$.

At k^{th} iteration, we compute X^k

$$\forall \ell' \in L.\ X_{\ell'}^k = X_{\ell'}^{k-1} \vee \bigvee_{(\ell,\rho,\ell') \in E} sp(X_\ell^{k-1}, \rho)$$

Convergence of fixed-point iterations

If $X^k = X^{k+1}$, then we say that the iterations have converged at iteration k and we have computed the fixed point.

We can prove that the fixed point obtained by the iterative method is a least fixed point of the following function.

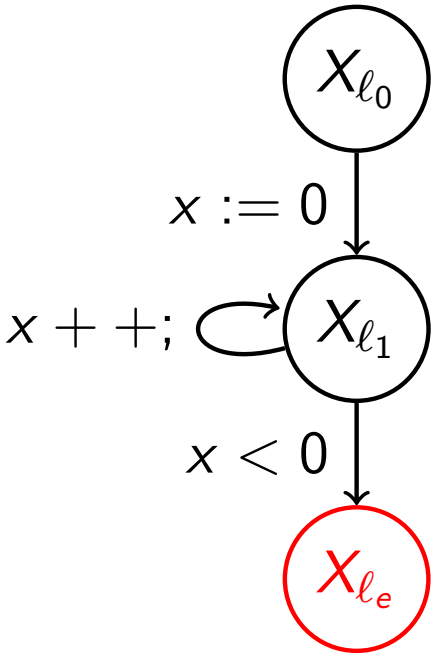
$$F(X) = [\top \vee F_{\ell_0}(X), F_{\ell_1}(X), ...]$$

We will get to the proof later.

Example: Fixed-point equations

Example 8.4

Consider program:



Fixed-point equations:

$$X_{\ell_0} = X_{\ell_0}$$

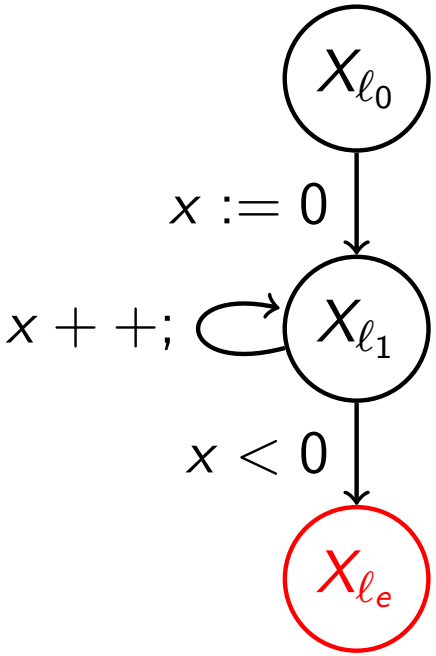
$$X_{\ell_1} = X_{\ell_1} \vee sp(X_{\ell_0}, x' = 0) \vee sp(X_{\ell_1}, x' = x + 1)$$

$$X_{\ell_e} = X_{\ell_e} \vee sp(X_{\ell_1}, x < 0 \wedge x' = x)$$

Example: Iterative fixed point with *sp*

Example 8.5

Consider program:



Initial value:

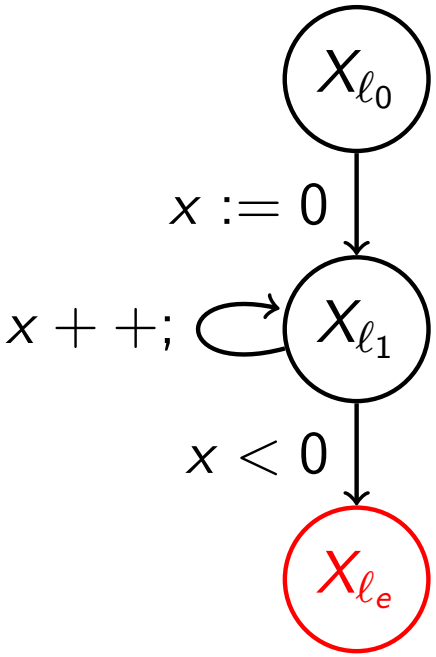
$$X^0_{\ell_0} := \top$$
$$X^0_{\ell_1} := \bot$$
$$X^0_{\ell_e} := \bot$$

Iteration 1

$$X^1_{\ell_0} := \top$$
$$\begin{aligned} X^1_{\ell_1} &:= X^0_{\ell_1} \vee sp(X^0_{\ell_1}, x' = x+1) \vee sp(X^0_{\ell_0}, x' = 0) \\ &:= \bot \vee sp(\bot, x' = x+1) \vee sp(\top, x' = 0) \\ &:= \bot \vee \bot \vee sp(\top, x' = 0) \\ &:= \bot \vee \bot \vee x = 0 := (x = 0) \end{aligned}$$
$$\begin{aligned} X^1_{\ell_e} &:= sp(X^0_{\ell_1}, x < 0 \wedge x' = x) \\ &:= sp(\bot, x < 0 \wedge x' = x) := \bot \end{aligned}$$

Example: Iterative fixed point with *sp*

Consider program:



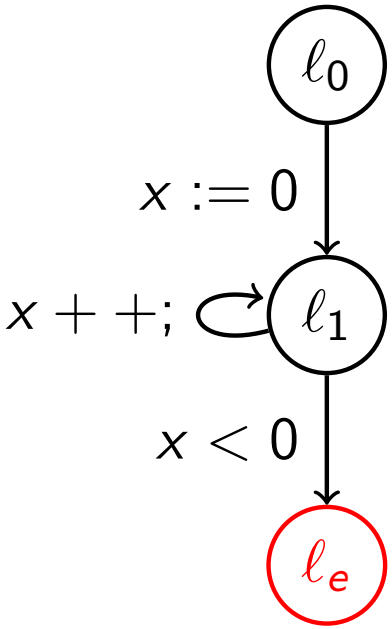
Iteration 2

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

$$\begin{aligned} X^2_{\ell_1} &:= X^1_{\ell_1} \vee sp(X^1_{\ell_1}, x' = x+1) \vee sp(X^1_{\ell_0}, x' = 0) \\ &:= (x = 0) \vee sp(x = 0, x' = x+1) \vee sp(\top, x' = 0) \\ &:= (x = 0 \vee x = 1 \vee x = 0) \\ &:= (0 \leq x \leq 1) \end{aligned}$$

$$\begin{aligned} X^2_{\ell_e} &:= sp(X^1_{\ell_1}, x < 0 \wedge x' = x) \\ &:= sp(x = 0, x < 0 \wedge x' = x) := \bot \end{aligned}$$

Example: diverging analysis with *sp*(contd.)



Iterates(contd.):

$$X^3_{\ell_0} := \top, X^3_{\ell_1} := (0 \leq x \leq 2), X^3_{\ell_e} := \bot$$

$$\vdots$$

$$X^n_{\ell_0} := \top, X^n_{\ell_1} := (0 \leq x \leq n-1), X^n_{\ell_e} := \bot$$

...will never converge

How to compute fixed point effectively?

Abstract post $sp^{\#}$

Now we introduce the key method of verification

Let us define abstract post.

$$sp^{\#} : \Sigma(V) \times \Sigma(V, V') \to \Sigma(V)$$

Abstract post must satisfy the following condition

$$sp(F, \rho) \Rightarrow sp^{\#}(F, \rho)$$

It is up to us how we choose $sp^{\#}$ that satisfies the above condition

Example: abstract post

Example 8.6

Consider the following widening function

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

We may define the following abstract post

$$sp^{\#}(F, \rho) = wideOne(sp(F, \rho))$$

Exercise 8.3

Apply the above abstract post on the following formulas

- $sp^{\#}(x > 0, x > 1 \wedge x' = x)$
- $sp^{\#}(x > 0, x < 10 \wedge x' = x)$
- $sp^{\#}(x > 0, x' = x + 1)$
- $sp^{\#}(x < 5, x' = x + 1)$

Abstract Fixed point

Replace sp by $sp^{\#}$ for faster convergence

initially: $X^0_{\ell_0} \triangleq \top$ and $X^0_{\ell} \triangleq \bot$ for each $\ell \neq \ell_0$
and at each iteration

$$X^{k+1}_{\ell_0} = \top$$

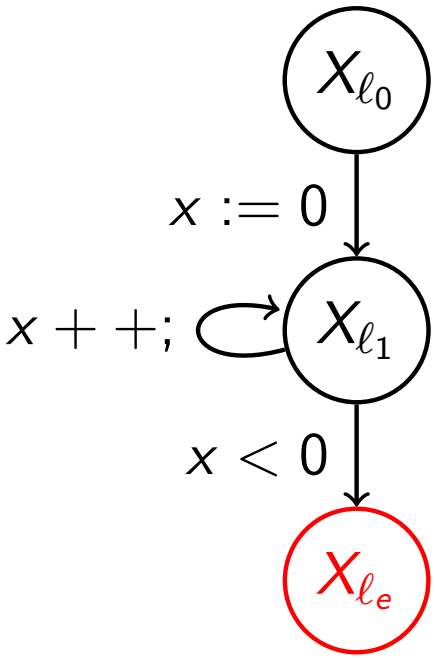
$$\forall \ell' \in L \setminus \{\ell_0\}.\ X^{k+1}_{\ell'} = X^k_{\ell'} \vee \bigvee_{(\ell,\rho,\ell') \in E} sp^{\#}(X^k_{\ell}, \rho)$$

After convergence, X_ℓ will be a superset of reachable states at ℓ.

Example: Abstract fixed-point equation

Example 8.7

Consider program:



Fixed-point equations:

$$X_{\ell_0} = X_{\ell_0}$$

$$X_{\ell_1} = X_{\ell_1} \vee sp^{\#}(X_{\ell_0}, x' = 0) \vee sp^{\#}(X_{\ell_1}, x' = x + 1)$$

$$X_{\ell_e} = X_{\ell_e} \vee sp^{\#}(X_{\ell_1}, x < 0 \wedge x' = x)$$

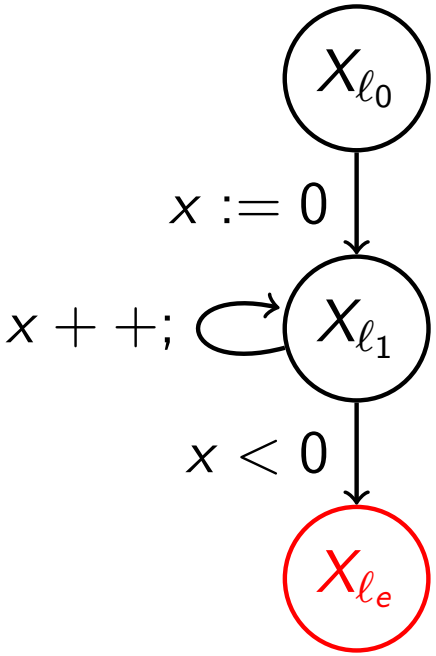
Let us use the following abstract post

$$sp^{\#}(F, \rho) = wideOne(sp(F, \rho))$$

Example: Iterative fixed point with $sp^{\#}$

Example 8.8

Consider program:



Initial value:

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

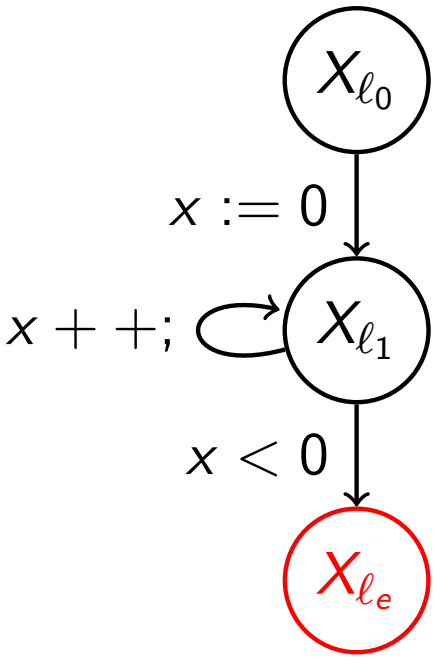
Iteration 1

$$X^1_{\ell_0} := \top$$
$$\begin{aligned} X^1_{\ell_1} &:= X^0_{\ell_1} \vee sp^{\#}(X^0_{\ell_1}, x' = x+1) \vee sp^{\#}(X^0_{\ell_0}, x' = 0) \\ &:= \bot \vee sp^{\#}(\bot, x' = x+1) \vee sp^{\#}(\top, x' = 0) \\ &:= \bot \vee \bot \vee 0 \leq x \leq 1 := 0 \leq x \leq 1 \end{aligned}$$

$$\begin{aligned} X^1_{\ell_e} &:= sp^{\#}(X^0_{\ell_1}, x < 0 \wedge x' = x) \\ &:= sp^{\#}(\bot, x < 0 \wedge x' = x) := \bot \end{aligned}$$

Example: Iterative fixed point with $sp^{\#}$

Consider program:



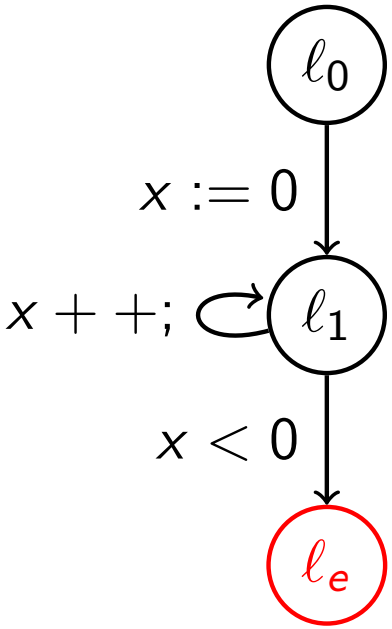
Iteration 2

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

$$\begin{aligned} X^2_{\ell_1} &:= X^1_{\ell_1} \vee sp^{\#}(X^1_{\ell_1}, x' = x+1) \vee sp^{\#}(X^1_{\ell_0}, x' = 0) \\ &:= (0 \leq x \leq 1) \vee sp^{\#}(0 \leq x \leq 1, x' = x+1) \vee \\ &\quad sp^{\#}(\top, x' = 0) \\ &:= (0 \leq x \leq 1 \vee 1 \leq x \leq 3 \vee 0 \leq x \leq 1) \\ &:= (0 \leq x \leq 3) \end{aligned}$$

$$\begin{aligned} X^2_{\ell_e} &:= sp^{\#}(X^1_{\ell_1}, x < 0 \wedge x' = x) \\ &:= sp^{\#}(0 \leq x \leq 1, x < 0 \wedge x' = x) := \bot \end{aligned}$$

Example: diverging analysis with $sp^{\#}$(contd.)



Iterates(contd.):

$$X^3_{\ell_0} := \top, X^3_{\ell_1} := (0 \leq x \leq 5), X^3_{\ell_e} := \bot$$

$$\vdots$$

$$X^n_{\ell_0} := \top, X^n_{\ell_1} := (0 \leq x \leq 2n-1), X^n_{\ell_e} := \bot$$

...will never converge

Example: another abstract post

Example 8.9

Consider the following widening function

$$wideAny(X) = \{n + j | n \in X, j \geq 0\}$$

Let us define the following abstract post

$$sp^{\#}(F, \rho) = wideAny(sp(F, \rho))$$

Exercise 8.4

Apply the above abstract post on the following formulas

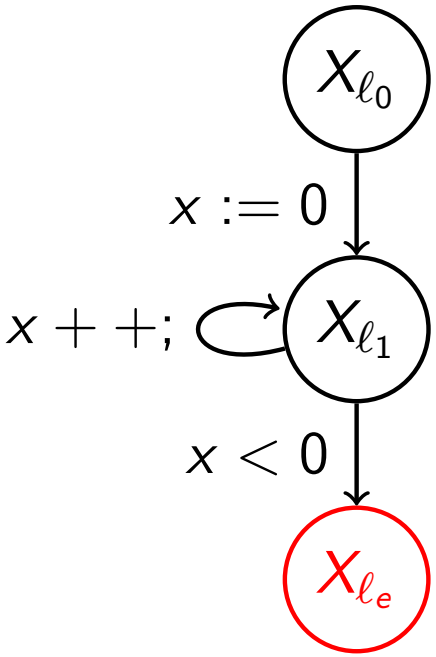
- $sp^{\#}(x > 0, x > 1 \wedge x' = x)$
- $sp^{\#}(x > 0, x < 10 \wedge x' = x)$
- $sp^{\#}(x > 0, x' = x + 1)$
- $sp^{\#}(x < 5, x' = x + 1)$

Example: Iterative fixed point with another $sp^{\#}$

Example 8.10

Now we are using $sp^{\#}(F, \rho) = \mathit{wideAny}(sp(F, \rho))$

Consider program:



Initial value: usual

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

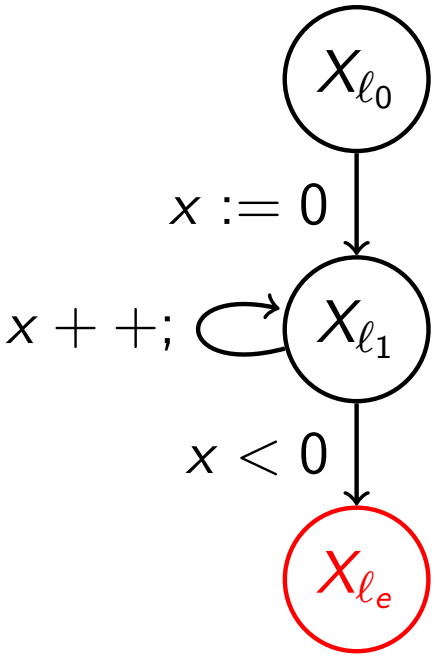
Iteration 1

$$
\begin{aligned}
X^1_{\ell_0} &:= \top \\
X^1_{\ell_1} &:= X^0_{\ell_1} \vee sp^{\#}(X^0_{\ell_1}, x' = x + 1) \vee sp^{\#}(X^0_{\ell_0}, x' = 0) \\
&:= \bot \vee sp^{\#}(\bot, x' = x + 1) \vee sp^{\#}(\top, x' = 0) \\
&:= \bot \vee \bot \vee 0 \leq x := 0 \leq x
\end{aligned}
$$

$$
\begin{aligned}
X^1_{\ell_e} &:= sp^{\#}(X^0_{\ell_1}, x < 0 \wedge x' = x) \\
&:= sp^{\#}(\bot, x < 0 \wedge x' = x) := \bot
\end{aligned}
$$

Example: Iterative fixed point with another $sp^{\#}$

Consider program:



Iteration 2

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

$$\begin{aligned} X^2_{\ell_1} &:= X^1_{\ell_1} \vee sp^{\#}(X^1_{\ell_1}, x' = x+1) \vee sp^{\#}(X^1_{\ell_0}, x' = 0) \\ &:= (0 \leq x) \vee sp^{\#}(0 \leq x, x' = x+1) \vee sp^{\#}(\top, x' = 0) \\ &:= (0 \leq x \vee 1 \leq x \vee 0 \leq x) \\ &:= (0 \leq x) \end{aligned}$$

$$\begin{aligned} X^2_{\ell_e} &:= sp^{\#}(X^1_{\ell_1}, x < 0 \wedge x' = x) \\ &:= sp^{\#}(0 \leq x, x < 0 \wedge x' = x) := \bot \end{aligned}$$

We have converged. Congratulations!!

Exercise 8.5

Let $wideNAny(X) = \{x - j | n \in X \wedge j \geq 0\}$.
What will happen if we choose $sp^{\#}(F, \rho) = wideNAny(sp(F, \rho))$*?*

How do we choose $sp^{\#}$?

We will learn lattice theory to guide us in choosing $sp^{\#}$ such that we have better guarantee of convergence.

End of Lecture 8