#### AAA616: Program Analysis

Lecture 5 — Abstract Interpretation Framework

Hakjoo Oh 2022 Fall

#### Abstract Interpretation Framework

A powerful framework for designing correct static analysis

- "framework": correct static analysis comes out, reusable
- "powerful": all static analyses are understood in this framework
- "simple": prescription is simple
- "eye-opening": any static analysis is an abstract interpretation

MATHAEL DESIGNATION & A DESIGN ACCESS NODE, FOR EXTEND ANALYSIS OF POSSAGE BY CONSIDERING ON APPRICIPATION OF POSSAGE THEORY EXAMPLES ANALYSIS ANALYSIS ANALYSIS INTERCENTED AND ANALYSIS ANALYSIS ANALYSIS ANALYSIS Intervalues of "Analysis" and analysis and analysis

#### 1. Deredantice

which is different parameters of the proper set of the parameters of the parameters

#### 2. Samery

buttles 5 succepts the spense and mathematical memorities of a soluboit Deschutzi Hommun, Scott and Titushen (T.). This authematical memorities in successful and the soluble association of the supporting of soluboit flow, Non-mobile to both of the summaries of program, is that the inserts that supporting of soluboit flow, Non-mobile is token to associate the soluboit of the soluboit of the solution of programs, Sociation & glows the formul Artificial of the description.

Jaamij a' 7.

\*\* Dis not an apprend by Dis-MOOR univergraphs 25-081 and 20-200. Amount spream regardle on which and a memory memory and the spream regardle a

#### appear out presenter of theory

th will use fight finebasis as a histophyproject superscenation of program.

(c) Spring of a program

many, grand 1 Soles+1<sup>8000</sup> | 0ccn-sec001

for, which [8] The continuity of a set 9.

the sole where "Encles", "Andparents", "least "Justical" and "Anita" partition the set Soles,

and sum macrosses. Converging - 81 and [[managinal] + 155.

CC77

#### 

Laboratelies of Defension and J. J. J. . . M. 200 2009 Connects Georg. Prants

#### 1. INTRODUCTION and Science

Security excluses of program on Franchise in weightable complete and program on Franklan payters. It were approximate the franklan, that for defendencies, generalizes of approximate the frank security of the second se

country, come a magnet/RL, for it crown (r) (12811251), market/RL, warket/RL, warket/RL, to a protocol distribution approach as a protocol distribution and a program and a protocol distribution and a program in a protocol distribution and a program base state and a protocol distribution and a program to a participant and a protocol distribution and a protocol participant and a protocol distribution and a protocol participant and a protocol distribution and a protocol participant and a procession and a protocol distribution and a proposed and a protocol distribution and a proposed and a protocol distribution and a protocol participant and a proposed a proposed and a proposed a proposed and a proposed a proposed and proposed and a proposed and a proposed and

Explosite programming analysis methods. In function on invisity methods too theorem and hardwards methods where an an effective strength and the second and as a formal limit is a main way proves the asymptotic of approximate programs analysis formatories. Institute 4 approximate programs analysis formatories. Institute 4 approximate programs and prior algorithm of the lattice formation of the main strength of the lattice of the property strength for approximation sensation sensities.

A is a solution of the soluti

Table descriptions are a competent network with the network of the second secon

This sum on apportal is part by (\*) DBL, promising Association (\*) and AP-Informations 12118 and is part by (\*) 2114-20201. main single starting of the start of the sta

alog theory 2016 were of theory. In the interval To fastion it as deputient a bibliothy of approxlands analyses are in defended according to the Provman of the approximations associated to a program marging frequency. Does absorb of the theorem or a bibliothy adultion and individed to the CONNET Literature.

In contrast, Tow Good 2010 (English analysis adated, The GENCIDS) Detection "Entrimotion" and Ameridational Control (Control (Con

CC79

#### Step 1: Define Concrete Semantics

The concrete semantics describes the real executions of the program. Described by semantic domain and function.

- A semantic domain **D**, which is a CPO:
  - D is a partially ordered set with a least element  $\perp$ .
  - Any increasing chain  $d_0 \sqsubseteq d_1 \sqsubseteq \dots$  in D has a least upper bound  $\bigsqcup_{n \ge 0} d_n$  in D.
- A semantic function F:D o D, which is continuous: for all chains  $d_0\sqsubseteq d_1\sqsubseteq\ldots$ ,

$$F(\bigsqcup_{n\geq 0}d_i)=\bigsqcup_{n\geq 0}F(d_n).$$

Then, the concrete semantics (or collecting semantics) is defined as the least fixed point of semantic function  $F: D \rightarrow D$ :

$$fixF = \bigsqcup_{i \in N} F^i(\bot).$$

#### Step 2: Define Abstract Semantics

Define the abstract semantics of the input program.

- Define an abstract semantic domain CPO  $\hat{D}$ .
  - Intuition:  $\hat{D}$  is an abstraction of D
- Define an abstract semantic function  $\hat{F}:\hat{D}
  ightarrow\hat{D}.$ 
  - Intuition:  $\hat{F}$  is an abstraction of F.
  - $\hat{F}$  must be monotone:

$$orall \hat{x}, \hat{y} \in \hat{D}. \ \hat{x} \sqsubseteq \hat{y} \implies \hat{F}(\hat{x}) \sqsubseteq \hat{F}(\hat{y})$$

(or extensive: 
$$orall x \in \hat{D}. \ x \sqsubseteq \hat{F}(x))$$

Then, static analysis is to compute an upper bound of:

$$igsqcup_{i\in\mathbb{N}}\hat{F}^i(ot)$$

How can we ensure that the result soundly approximate the concrete semantics?

## Requirement 1: Galois Connection

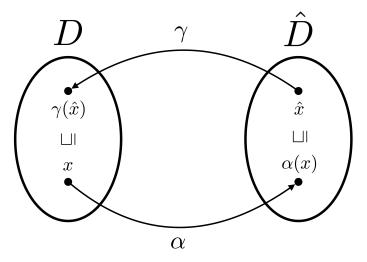
D and  $\hat{D}$  must be related with Galois-connection:

$$D \stackrel{\gamma}{\underset{\alpha}{\longleftarrow}} \hat{D}$$

That is, we have

- abstraction function:  $lpha\in D o \hat{D}$ 
  - $\blacktriangleright$  represents elements in D as elements of  $\hat{D}$
- concretization function:  $\gamma\in\hat{D} o D$ 
  - lacksim gives the meaning of elements of  $\hat{D}$  in terms of D
- $\forall x \in D, \hat{x} \in \hat{D}. \ \alpha(x) \sqsubseteq \hat{x} \iff x \sqsubseteq \gamma(\hat{x})$ 
  - lpha and  $\gamma$  respect the orderings of D and  $\hat{D}$
  - If an element x ∈ D is safely described by x̂ ∈ D̂, i.e., α(d) ⊑ d̂, then the element described by x̂ is also safe w.r.t. x, i.e., x ⊑ γ(x̂)

#### Galois-Connection



Example: Sign Abstraction

$$\wp(\mathbb{Z}) \stackrel{\gamma}{\underbrace{\longleftrightarrow}} (\{\bot, +, 0, -, \top\}, \sqsubseteq)$$
$$\alpha(Z) = \begin{cases} \bot & Z = \emptyset \\ + & \forall z \in Z. \ z > 0 \\ 0 & Z = \{0\} \\ - & \forall z \in Z. \ z < 0 \\ \top & \text{otherwise} \end{cases}$$
$$\gamma(\bot) = \emptyset$$
$$\gamma(\top) = \mathbb{Z}$$
$$\gamma(+) = \{z \in \mathbb{Z} \mid z > 0\}$$
$$\gamma(0) = \{0\}$$
$$\gamma(-) = \{z \in \mathbb{Z} \mid z < 0\}$$

#### Example: Interval Abstraction

$$egin{aligned} \wp(\mathbb{Z}) & \stackrel{\gamma}{\underset{\alpha}{\longleftarrow}} \{\bot\} \cup \{[a,b] \mid a \in \mathbb{Z} \cup \{-\infty\}, b \in \mathbb{Z} \cup \{+\infty\}\} \ & \gamma(\bot) &= \emptyset \ & \gamma([a,b]) &= \{z \in \mathbb{Z} \mid a \leq z \leq b\} \ & lpha(\emptyset) &= \bot \ & lpha(X) &= [\min X, \max X] \end{aligned}$$

# cf) Alternate Formulation

D and  $\hat{D}$  are related with Galois-connection:

$$D \stackrel{\gamma}{\underset{\alpha}{\longleftarrow}} \hat{D}$$

iff  $(\alpha, \gamma)$  satisfies the following conditions:

- lpha and  $\gamma$  are monotone functions
- $\gamma \circ \alpha$  is extensive, i.e.,  $\gamma \circ \alpha \sqsupseteq \lambda x.x$ 
  - abstraction typically loses precision
  - $(\gamma \circ \alpha)(\{1,3\}) = \{1,2,3\}$
- $\alpha \circ \gamma$  is reductive: i.e.,  $\alpha \circ \gamma \sqsubseteq \lambda x.x$ 
  - If  $\alpha \circ \gamma = \lambda x . x$ , Galois-insertion.
  - With Galois-insertion, no two abstract elements describe the same concrete element, which may be true with Galois-connection.

# $\mathsf{Proof}\ (\Rightarrow)$

#### If we have a Galois-connection:

$$orall x \in D, \hat{x} \in \hat{D}. \ lpha(x) \sqsubseteq \hat{x} \iff x \sqsubseteq \gamma(\hat{x})$$

then

- $\lambda x.x \sqsubseteq \gamma \circ \alpha$ :  $\alpha(x) \sqsubseteq \alpha(x)$  and hence  $x \sqsubseteq \gamma(\alpha(x))$  by Galois-connection.
- $\alpha \circ \gamma \sqsubseteq \lambda x.x$ :  $\gamma(\hat{x}) \sqsubseteq \gamma(\hat{x})$  and hence  $\alpha(\gamma(\hat{x})) \sqsubseteq \hat{x}$  by Galois-connection.
- $\gamma$  is monotone: if  $\hat{x} \sqsubseteq \hat{y}$ , then  $\alpha(\gamma(\hat{x})) \sqsubseteq \hat{y}$ . Hence  $\gamma(\hat{x}) \sqsubseteq \gamma(\hat{y})$  by Galois-connection.
- $\alpha$  is monotone: if  $x \sqsubseteq y$ , then  $x \sqsubseteq \gamma(\alpha(y))$ . Hence  $\alpha(x) \sqsubseteq \alpha(y)$  by Galois-connection.

# $\mathsf{Proof}(\Leftarrow)$

- Assume  $\alpha(x) \sqsubseteq \hat{x}$ . Since  $\gamma$  is monotone,  $\gamma(\alpha(x)) \sqsubseteq \gamma(\hat{x})$ . Because  $\gamma \circ \alpha$  is extensive, we have  $x \sqsubseteq \gamma(\hat{x})$ .
- Assume  $x \sqsubseteq \gamma(\hat{x})$ . Since  $\alpha$  is monotone,  $\alpha(x) \sqsubseteq \alpha(\gamma(\hat{x}))$ . Because  $\alpha \circ \gamma$  is reductive, we have  $\alpha(x) \sqsubseteq \hat{x}$ .

# Properties of Galois-Connection (1)

Given 
$$D \stackrel{\gamma}{\longleftrightarrow lpha} \hat{D}$$
, we have:

• 
$$\gamma \circ \alpha \circ \gamma = \gamma$$

- From α ∘ γ ⊑ λx.x and monotonicity of γ, we have γ ∘ α ∘ γ ⊑ γ.
   We have γ ∘ α ∘ γ ⊒ γ from γ ∘ α ⊒ λx.x.
- $\alpha \circ \gamma \circ \alpha = \alpha$
- $\alpha \circ \gamma$  and  $\gamma \circ \alpha$  are idempotent:

$$(\alpha \circ \gamma)^2 = \alpha \circ \gamma, (\gamma \circ \alpha)^2 = \gamma \circ \alpha$$

•  $\gamma$  uniquely determines  $\alpha(D, \hat{D} \text{ complete lattices})$ :

$$\alpha(d) = \bigcap \{ \hat{d} \mid d \sqsubseteq \gamma(\hat{d}) \}$$

which implies that  $\alpha(d)$  is the best abstraction of d.

•  $\alpha$  uniquely determines  $\gamma$ :

$$\gamma(\hat{d}) = \bigsqcup \{ d \mid \alpha(d) \sqsubseteq \hat{d} \}$$

## Properties of Galois-Connection (2)

- $\alpha$  is strict, i.e.,  $\alpha(\perp) = \hat{\perp}$ . Proof. From  $\perp \sqsubseteq \gamma(\hat{\perp})$ , we have  $\alpha(\perp) \sqsubseteq \hat{\perp}$  by Galois-connection.
- lpha is continuous: for any chain S in D,

$$lpha(\bigsqcup_{x\in S}x)=\bigsqcup_{x\in S}lpha(x).$$

Proof. Since  $\alpha$  is monotonic,

$$\bigsqcup_{x\in S}lpha(x)\sqsubseteqlpha(\bigsqcup_{x\in S}x).$$

Since  $\lambda x.x \sqsubseteq \gamma \circ \alpha$  and  $\gamma$  is monotonic,

$$\bigsqcup_{x\in S} x \sqsubseteq \bigsqcup_{x\in S} \gamma(\alpha(x)) \sqsubseteq \gamma(\bigsqcup_{x\in S} \alpha(x))$$

By Galois-connection, we have

$$lpha(\bigsqcup_{x\in S}x)\sqsubseteq\bigsqcup_{x\in S}lpha(x)$$

#### **Deriving Galois-Connections**

• Pointwise lifting: Given  $D \xleftarrow{\gamma}{lpha} \hat{D}$  and a set S, then

$$S o D \xleftarrow{\gamma'}{\alpha'} S o \hat{D}$$

with  $\alpha'(f) = \lambda s \in S.\alpha(f(s))$  and  $\gamma(f) = \lambda s \in S.\gamma(f(s))$ . • Composition: Given  $X_1 \xrightarrow{\gamma_1} X_2 \xrightarrow{\gamma_2} X_3$ , we have

$$X_1 \xleftarrow{\gamma_1 \circ \gamma_2}{\alpha_2 \circ \alpha_1} X_3$$

# Requirement 2: $\hat{F}$ and F

• 
$$\hat{F}$$
 is a sound abstraction of  $F$ :

$$F\circ\gamma\sqsubseteq\gamma\circ\hat{F}\quad(lpha\circ F\sqsubseteq\hat{F}\circlpha)$$

• or, alternatively,

$$lpha(x) \sqsubseteq \hat{x} \implies lpha(F(x)) \sqsubseteq \hat{F}(\hat{x})$$

Best Abstract Semantics  
From 
$$D \xrightarrow{\gamma} \hat{D}$$
 and  $F \circ \gamma \sqsubseteq \gamma \circ \hat{F}$ , we have  
 $\alpha \circ F \circ \gamma \sqsubseteq \alpha \circ \gamma \circ \hat{F}$   $\alpha$  is monotone  
 $\sqsubseteq \hat{F}$   $\alpha \circ \gamma \sqsubseteq \lambda x.x$ 

The result means that  $\alpha \circ F \circ \gamma$  is the best abstraction of F and any sound abstraction  $\hat{F}$  of F is greater than  $\alpha \circ F \circ \gamma$ .

## Composition

When F, F' are concrete operators and  $\hat{F}, \hat{F}'$  are abstract operators, if  $\hat{F}$  and  $\hat{F}'$  are sound abstractions of F and F', respectively, then  $\hat{F} \circ \hat{F}'$  is a sound abstraction of  $F \circ F'$ .

# **Fixpoint Transfer Theorems**

#### Theorem (Fixpoint Transfer)

Let D and  $\hat{D}$  be related by Galois-connection  $D \xleftarrow{\gamma}{\alpha} \hat{D}$ . Let  $F : D \to D$  be a continuous function and  $\hat{F} : \hat{D} \to \hat{D}$  be a monotone function such that  $\alpha \circ F \sqsubseteq \hat{F} \circ \alpha$ . Then,

$$lpha(\mathit{fix}F) \sqsubseteq \bigsqcup_{i \in \mathbb{N}} \hat{F}^i(\hat{\perp}).$$

#### Theorem (Fixpoint Transfer2)

Let D and  $\hat{D}$  be related by Galois-connection  $D \xleftarrow{\gamma}{\alpha} \hat{D}$ . Let  $F: D \to D$  be a continuous function and  $\hat{F}: \hat{D} \to \hat{D}$  be a monotone function such that  $\alpha(x) \sqsubseteq \hat{x} \implies \alpha(F(x)) \sqsubseteq \hat{F}(\hat{x})$ . Then,

$$lpha(\mathit{fix}F) \sqsubseteq \bigsqcup_{i \in \mathbb{N}} \hat{F}^i(\hat{\perp}).$$

#### Proof of Fixpoint Transfer

• From  $\alpha \circ F \sqsubseteq \hat{F} \circ \alpha$ , we can derive

 $\forall n \in \mathbb{N}. \ \alpha \circ F^n \sqsubseteq \hat{F}^n \circ \alpha \quad (\forall n \in \mathbb{N}. \ \alpha(F^n(\bot)) \sqsubseteq \hat{F}^n(\hat{\bot}))$ 

by induction as follows:

$$\begin{array}{rcl} \alpha \circ F^{n+1} & = & \alpha \circ F \circ F^n \\ & \sqsubseteq & \alpha \circ F \circ \gamma \circ \alpha \circ F^n & \cdots \alpha \circ F \text{ is mono. and } \lambda x.x \sqsubseteq \gamma \circ \alpha \\ & \sqsubseteq & \alpha \circ F \circ \gamma \circ \hat{F}^n \circ \alpha & \cdots \alpha \circ F \circ \gamma \text{ is mono. and by I.H.} \\ & \sqsubseteq & \hat{F} \circ \hat{F}^n \circ \alpha & \cdots \alpha \circ F \circ \gamma \sqsubseteq \hat{F} \end{array}$$

• Since  $lpha,F,\hat{F}$  are monotone,  $\{lpha(F^i(otn))\}_i$  and  $\{\hat{F}^i(otn)\}_i$  are chains, and

$$\bigsqcup_{i\in\mathbb{N}}\alpha(F^{i}(\bot))\sqsubseteq\bigsqcup_{i\in\mathbb{N}}\hat{F}^{i}(\hat{\bot})$$
(1)

• Since  $\alpha$  and F are continuous,

$$\bigsqcup_{i\in\mathbb{N}}lpha(F^i(\bot))=lpha(\bigsqcup_{i\in\mathbb{N}}(F^i(\bot)))=lpha(\mathit{fix}F)$$

By replacing the left-hand side of (1), we have

$$lpha(\mathit{fix}F) \sqsubseteq igsqcup_{i\in\mathbb{N}}\hat{F}^i(\hat{ot})$$

# Computing $igsqcup_{i\in\mathbb{N}}\hat{F}^{i}(\hat{ot})$

• If the abstract domain  $\hat{D}$  has finite height (i.e., all chains are finite), we can directly calculate

$$igsqcup_{i\in\mathbb{N}}\hat{F}^{i}(\hat{ot}).$$

$$igsqcup_{i\in\mathbb{N}}\hat{F}^i(\hat{ot})\sqsubseteq \lim_{i\in\mathbb{N}}\hat{X}_i$$

#### Fixpoint Accerlation with Widening

Define finite chain  $\hat{X}_i$  by an widening operator  $\nabla: \hat{D} \times \hat{D} \rightarrow \hat{D}$ :

$$\begin{aligned} \hat{X}_0 &= \hat{\perp} \\ \hat{X}_i &= \hat{X}_{i-1} & \text{if } \hat{F}(\hat{X}_{i-1}) \sqsubseteq \hat{X}_{i-1} \\ &= \hat{X}_{i-1} \bigtriangledown \hat{F}(\hat{X}_{i-1}) & \text{otherwise} \end{aligned}$$
 (2)

Conditions on  $\nabla$ :

•  $\forall a,b\in \hat{D}.\;(a\sqsubseteq a\bigtriangledown b)\;\wedge\;(b\sqsubseteq a\bigtriangledown b)$ 

• For all increasing chains  $(x_i)_i$ , the increasing chain  $(y_i)_i$  defined as

$$y_i = \left\{egin{array}{cc} x_0 & ext{if } i=0 \ y_{i-1}ig x_i & ext{if } i>0 \end{array}
ight.$$

eventually stabilizes (i.e., the chain is finite).

#### Decreasing Iterations with Narrowing

- We can refine the widening result  $\lim_{i\in\mathbb{N}}\hat{X}_i$  by a narrowing operator  $\hat{\Delta}:\hat{D}\times\hat{D}\to\hat{D}$ .
- Compute chain  $(\hat{Y}_i)_i$

$$\hat{Y}_{i} = \begin{cases} \lim_{i \in \mathbb{N}} \hat{X}_{i} & \text{if } i = 0\\ \hat{Y}_{i-1} \bigtriangleup \hat{F}(\hat{Y}_{i-1}) & \text{if } i > 0 \end{cases}$$
(3)

- Conditions on ∆
  - $\blacktriangleright \, \forall a,b \in \hat{D}. \ a \sqsubseteq b \implies a \sqsubseteq a \bigtriangleup b \sqsubseteq b$
  - $\blacktriangleright$  For all decreasing chain  $(x_i)_i$ , the decreasing chain  $(y_i)_i$  defined as

$$y_i = \left\{egin{array}{cc} x_i & ext{if } \mathrm{i} = 0 \ y_{i-1} igtriangleq x_i & ext{if } i > 0 \end{array}
ight.$$

eventually stabilizes.

# Safety of Widening and Narrowing

#### Theorem (Widening's Safety)

Let  $\hat{D}$  be a CPO,  $\hat{F} : \hat{D} \to \hat{D}$  a monotone function,  $\nabla : \hat{D} \times \hat{D} \to \hat{D}$ a widening operator. Then, chain  $(\hat{X}_i)_i$  defined as (2) eventually stabilizes and

$$igsqcup_{\in\mathbb{N}}\hat{F}^i(\hat{ot})\sqsubseteq \lim_{i\in\mathbb{N}}\hat{X}_i.$$

#### Theorem (Narrowing's Safety)

Let  $\hat{D}$  be a CPO,  $\hat{F} : \hat{D} \to \hat{D}$  a monotone function,  $\Delta : \hat{D} \times \hat{D} \to \hat{D}$ a narrowing operator. Then, chain  $(\hat{Y}_i)_i$  defined as (3) eventually stabilizes and

$$igsqcup_{i\in\mathbb{N}}\hat{F}^i(\hat{ot})\sqsubseteq \lim_{i\in\mathbb{N}}\hat{Y}_i.$$

## Proof of Widening's Safety

• We first show that  $\{\hat{F}(\hat{X}_i)\}_i$  is an increasing chain (if so, by the second condition of widening, the widening sequence  $\{\hat{X}_i\}_i$  eventually stabilizes). Note that, by (2),  $\hat{F}(\hat{X}_{i+1})$  is either  $\hat{F}(\hat{X}_i)$  or  $\hat{F}(\hat{X}_i \bigtriangledown \hat{F}(\hat{X}_i))$ . Since  $\hat{X}_i \sqsubseteq \hat{X}_i \bigtriangledown \hat{F}(\hat{X}_i)$  and  $\hat{F}$  is monotone, for all i we have

$$\hat{F}(\hat{X}_i) \sqsubseteq \hat{F}(\hat{X}_{i+1})$$

- We next show that  $orall i \in \mathbb{N}.\ \hat{F}^i(\hat{\perp}) \sqsubseteq \hat{X}_i.$ 
  - Base case.  $\hat{F}^0(\perp) = \hat{\perp} \sqsubseteq \hat{X}_0.$
  - ▶ Inductive case. From the induction hypothesis (I.H.), i.e.,  $\hat{F}^i(\hat{\perp}) \sqsubseteq \hat{X}_i$ , and the monotonicity of  $\hat{F}$ , we have

$$\hat{F}^{i+1}(\hat{\perp}) \sqsubseteq \hat{F}(\hat{X}_i) \tag{4}$$

There are two cases to consider:

- When  $\hat{F}(\hat{X}_i) \sqsubseteq \hat{X}_i$  and  $\hat{X}_{i+1} = \hat{X}_i$ : we have  $\hat{F}(\hat{X}_i) \sqsubseteq \hat{X}_{i+1}$  and therefore  $\hat{F}^{i+1}(\hat{\bot}) \sqsubseteq \hat{X}_{i+1}$ .
- **2** When  $\hat{F}(\hat{X}_i) \not\sqsubseteq \hat{X}_i$  and  $\hat{X}_{i+1} = \hat{X}_i \bigtriangledown \hat{F}_i(\hat{X}_i)$ : by the condition of  $\bigtriangledown, \hat{F}(\hat{X}_i) \sqsubseteq \hat{X}_i \bigtriangledown \hat{F}_i(\hat{X}_i) = \hat{X}_{i+1}$ . Thus,  $\hat{F}(\hat{X}_i) \sqsubseteq \hat{X}_{i+1}$  for all  $i \in \mathbb{N}$ . By (4), we have  $\hat{F}^{i+1}(\hat{\bot}) \sqsubseteq \hat{X}_{i+1}$ .

## Proof of Narrowing's Safety

• We first show that  $\{\hat{F}(\hat{Y}_i)\}_i$  is a decreasing chain (if so, by the second condition of narrowing, the narrowing sequence  $\{\hat{Y}_i\}_i$  eventually stabilizes). We can show that  $\{\hat{F}(\hat{Y}_i)\}_i$  is a decreasing chain by showing the following

$$\forall i \in \mathbb{N}. \ \hat{Y}_i \sqsupseteq \hat{F}(\hat{Y}_i).$$
(5)

This is because, from (5), we have  $\hat{Y}_i \supseteq \hat{Y}_i \triangle \hat{F}(\hat{Y}_i) \supseteq \hat{F}(\hat{Y}_i)$  and by the mono. of  $\hat{F}$ , we have

$$\hat{F}(\hat{Y}_i) \sqsupseteq \hat{F}(\hat{Y}_i \bigtriangleup \hat{F}(\hat{Y}_i)) = \hat{F}(\hat{Y}_{i+1})$$

Proof of (5): exercise.

• We next show that  $\forall i \in \mathbb{N}$ .  $\hat{F}^i(\hat{\perp}) \sqsubseteq \hat{Y}_i$  by induction (exercise).