This note is summary of Abstract interpretation Framework (lec. 5)

I will focus on "Galois connection"

Step 1: Define "Concrete Sematics (Collecting Semantics)

- domain D가 CPO이고
- F가 D→D의 연속함수라면

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

Step 2) Define Abstract Semantics

- abstract semantic domain CPO $\hat{D}$를 정의
- abstract semantic function $\hat{F} : \hat{D} \to \hat{D}$를 정의
  - $\hat{F}$는 반드시 monotone 해야 함

    it means, $\forall \hat{x}, \hat{y} \in \hat{D}.\ \hat{x} \sqsubseteq \hat{y} \Rightarrow \hat{F}(\hat{x}) \sqsubseteq \hat{F}(\hat{y})$

  (or extensive. $\forall x \in \hat{D},\ x \sqsubseteq \hat{F}(x)$)

이때 static analysis는,

$\bigsqcup_{i \in N} \hat{F}^i(\bot)$ ($fix F \sqsubseteq \bigsqcup \hat{F}(\bot)$)

Okay, 이번장에서 우리가 궁금한 것:

어떻게 저런 요약이 concrete semantic을 sound하게 요약하는 것을 보장할 수 있지?

Req 1) Galois Connection

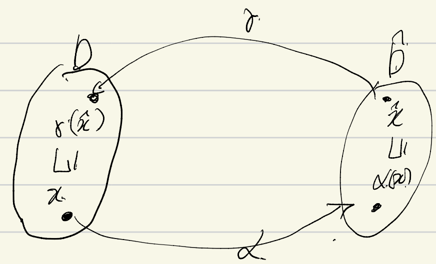
" $D \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \hat{D}$ "

α: abstraction function $\alpha \in D \to \hat{D}$

⇒ D를 $\hat{D}$으로 표현해줌

γ: concretization function: $\gamma \in \hat{D} \to D$

⇒ $\hat{D}$의 의미를 줌 (D 대신에)



▶ Galois connection이 성립하는 조건

" $\alpha(x) \sqsubseteq \hat{x} \iff x \sqsubseteq \gamma(\hat{x})$ "

▶ α와 γ는 D와 $\hat{D}$에서의 순서를 보존

cf) Req 1.2) 갈루아 커넥션의 또다른 조건 ($\alpha(x) \sqsubseteq \hat{x} \iff x \sqsubseteq \gamma(\hat{x})$) 와 동치.

1. α와 γ는 monotone function이어야 한다.
2. $\gamma \circ \alpha$는 extensive하다. 즉, $\gamma \circ \alpha \sqsupseteq \lambda x.x$
3. $\alpha \circ \gamma$은 reductive하다. 즉, $\alpha \circ \gamma \sqsubseteq \lambda x.x$

proof 1)

가정 $\forall x \in D, \hat{x} \in \hat{D}.\ \alpha(x) \sqsubseteq \hat{x} \iff x \sqsubseteq \gamma(\hat{x})$

then,

▷ $\lambda x.x \sqsubseteq \gamma \circ \alpha$: $\alpha(x) \sqsubseteq \alpha(x)$ 이면, $x \sqsubseteq \gamma(\alpha(x))$

▷ $\alpha \circ \gamma \sqsubseteq \lambda x.x$: $\gamma(\hat{x}) \sqsubseteq \gamma(\hat{x})$ 이면. $\alpha(\gamma(\hat{x})) \sqsubseteq \hat{x}$

▷ γ is montone, if $\hat{x} \sqsubseteq \hat{y}$, $\alpha(\gamma(\hat{x})) \sqsubseteq \hat{x} \sqsubseteq \hat{y}$ $\therefore \gamma(\hat{x}) \sqsubseteq \gamma(\hat{y})$

▷ α is monotone, if $x \sqsubseteq y$; $x \sqsubseteq \gamma(\alpha(y))$ $\therefore \alpha(x) \sqsubseteq \alpha(y)$

proof 2) $\Leftarrow$

가정 1) $\alpha(x) \sqsubseteq \hat{x}$ 이면 γ는 단조함수이므로, $\gamma(\alpha(x)) \sqsubseteq \gamma(\hat{x})$

여기서 $\gamma \circ \alpha$는 extensive 하므로, $x \sqsubseteq \gamma(\hat{x})$

2) $x \sqsubseteq \gamma(\hat{x})$를 가정, α는 단조함수으로 $\alpha(x) \sqsubseteq \alpha(\gamma(\hat{x}))$

여기서 $\alpha \circ \gamma$는 reductive하므로, $\alpha(x) \sqsubseteq \hat{x}$

* Galois-connection의 성질.

Given $D \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \hat{D}$)

▷ $\gamma \circ \alpha \circ \gamma = \gamma$

$\Rightarrow \begin{cases} \underbrace{\boxed{\gamma \circ \alpha}}_{\text{extensive}} \circ \gamma \sqsupseteq \gamma \\ \gamma \circ \underbrace{\alpha \circ \gamma}_{\text{reductive}} \sqsubseteq \gamma \end{cases}$ $\therefore \gamma \circ \alpha \circ \gamma = \gamma$

▷ $\alpha \circ \gamma \circ \alpha = \alpha$ ∵ 위와 같은 이유.

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

▷ γ를 이용한 α의 정의! α(D, $\hat{D}$ complete lattice)

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

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

Req 2) $\hat{F}$ and F

- $\hat{F}$ is a sound abstraction of F.

$(\alpha \circ F \sqsubseteq \hat{F} \circ \alpha) \Rightarrow \hat{F}$의 soundness

* Best Abstract Semantics

in Galois connection, $F \circ \gamma \sqsubseteq \gamma \circ \hat{F}$,

$\Rightarrow \alpha \circ F \circ \gamma \sqsubseteq \alpha \circ \gamma \circ \hat{F}$

$\sqsubseteq \hat{F}$

$\because \alpha \circ \gamma \sqsubseteq \lambda x.x$

※ Fixpoint Transfer Theorems

Thm 1)

1) D와 $\hat{D}$가 Galois-Connection이 있고, 2) F가 D→D인 연속함수이며 3) $\hat{F}: \hat{D} \to \hat{D}$이 단조함수일 때,

$\alpha \circ F \sqsubseteq \hat{F} \circ \alpha$, Then.

"$\alpha(\mathrm{fix} F) \sqsubseteq \bigsqcup_{i \in N} \hat{F}^i(\hat{\bot})$"

proof)

$\alpha \circ F \sqsubseteq \hat{F} \circ \alpha$

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

$$\begin{aligned}
\alpha \circ F^{n+1} &= \alpha \circ F \circ F^n \\
&\sqsubseteq \alpha \circ F \circ \gamma \circ \alpha \circ F^n \\
&\sqsubseteq \alpha \circ F \circ \gamma \circ \hat{F}^n \circ \alpha \\
&\sqsubseteq \hat{F} \circ \hat{F}^n \circ \alpha \\
&= \hat{F}^{n+1} \circ \alpha
\end{aligned}$$

▷ $\alpha, F, \hat{F}$가 단조함수기 때문에! $\{\alpha(F^i(\bot))\}_i$, $\{\hat{F}^i(\hat{\bot})\}_i$은 chain!

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

▷ $\bigsqcup_{i \in N} \alpha(F^i(\bot)) = \alpha\left(\bigsqcup_{i \in N}(F^i(\bot))\right) = \alpha(\mathrm{fix} F)$

※ But, $\hat{D}$이 무한한 높이(height)를 가질 수 있기 때문에 $\alpha(\mathrm{fix} F) \sqsubseteq \bigsqcup \hat{F}^i(\hat{\bot})$라고 해도 직접 계산하는 건 불가능

이 케이스에 우리는 유한 체인 $\hat{X}$을 만들고, 다음과 같은 걸 계산한다.

"$\bigsqcup_{i \in N} \hat{F}^i(\hat{\bot}) \sqsubseteq \lim_{i \in N} \hat{X}_i$"

※ Fixpoint Accerlation with Widening

유한한 chain $\hat{X}_i$에 대해 $\nabla: \hat{D} \times \hat{D} \to \hat{D}$를 정의해보자!

$\hat{X}_0 = \hat{\bot}$

$$\hat{X}_i = \begin{cases} \hat{X}_{i-1} & \text{if } \hat{F}(\hat{X}_{i-1}) \sqsubseteq \hat{X}_{i-1} \\ \hat{X}_{i-1} \nabla \hat{F}(\hat{X}_{i-1}) & \text{otherwise} \end{cases}$$

▷ ∇의 조건

- $\forall a, b \in \hat{D}.\ (a \sqsubseteq a \nabla b) \wedge (b \sqsubseteq a \nabla b)$
- 모든 증가체인 $(x_i)_i$, 모든 증가체인 $(y_i)_i$는 다음과 같이 정의됨

$$y_i = \begin{cases} x_0 & \text{if } i = 0 \\ y_{i-1} \nabla x_i & \text{if } i > 0 \end{cases}$$

ex)

$x: x_0 \sqsubseteq x_1 \sqsubseteq x_2$ ← 얘가 종료는 강제함

$y: \underbrace{x_0}_{y_0} \quad \underbrace{y_0 \nabla x_1}_{y_1} \quad \underbrace{y_1 \nabla x_2}_{y_2}$

* Narrowing

→ 우리는 widening의 Result "$\lim_{i\in N} \hat{X}_i$"를 얻고 이를 정제할 것임

$\triangle : \hat{D} \times \hat{D} \to \hat{D}$

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

- △의 조건.
  - ▷ $a, b \in \hat{D}$, $a \sqsubseteq b \Rightarrow a \sqsubseteq a \triangle b \sqsubseteq b$
  - ▷ 감소체인 $(x_i)_i$ 에서 감소체인 $(y_i)_i$는 다음과 같이 정의된다.

$$y_i = \begin{cases} x_i & \text{if } i = 0 \\ y_{i-1} \triangle x_i & \text{if } i > 0 \end{cases}$$

ex.

$$x_0 \sqsupseteq x_1 \sqsupseteq x_2$$
$$y_0 \sqsupseteq \underbrace{y_0 \triangle x_1}_{y_1} \sqsupseteq \underbrace{y_1 \triangle x_2}_{y_2} \cdots$$

Thm. (widening's Safety)

$\hat{D}$이 cpo고, $\hat{F}: \hat{D} \to \hat{D}$인 단조함수일 때 $\{\hat{X}_i\}_i$가 $\hat{\nabla}$로 정의되면 항상 stabilize되고,

"$\bigsqcup_{i\in N} \hat{F}^i(\hat{\bot}) \sqsubseteq \lim_{i\in N} \hat{X}_i$"

pf)

1) 먼저 $\{\hat{F}(\hat{X}_i)\}$이 increasing chain라는 걸 보이자.

∵ if so, widening의 두 번째 조건으로 인해 $\{\hat{X}_i\}_i$ 결국 stabilize 되므로.

$\hat{F}(\hat{X}_i) \sqsubseteq \hat{F}(\hat{X}_{i+1})$ ∵ 1) $F(X_i)$ 2) $F(X_i \nabla F(X_i))$

2) 그 다음, $\forall i \in N$, $\hat{F}^i(\hat{\bot}) \sqsubseteq \hat{X}_i$ (soundness)

- ▷ base case $\hat{F}^0(\hat{\bot}) = \hat{\bot} \sqsubseteq \hat{X}_0$
- ▷ inductive case. (h.) $\hat{F}^i(\hat{\bot}) \sqsubseteq \hat{X}_i$

→ $\hat{F}$는 단조함수, $\hat{F}^{i+1}(\hat{\bot}) \sqsubseteq \hat{F}(\hat{X}_i)$

case1) $\hat{F}(\hat{X}_i) \sqsubseteq \hat{X}_i \to \hat{X}_{i+1} = \hat{X}_i$

∴ $\hat{F}(\hat{X}_i) \sqsubseteq \hat{X}_{i+1} \to \hat{F}^{i+1}(\hat{\bot}) \sqsubseteq \hat{X}_{i+1}$

case2) $\hat{F}(\hat{X}_i) \not\sqsubseteq \hat{X}_i \to \hat{X}_{i+1} = \hat{X}_i \nabla \hat{F}(\hat{X}_i)$

→ $\hat{F}(\hat{X}_i) \sqsubseteq \hat{X}_{i+1}$ ∴ $\hat{F}^{i+1}(\hat{\bot}) \sqsubseteq \hat{F}(\hat{X}_i) \sqsubseteq \hat{X}_{i+1}$