Theorem Problem

SNU 4541.664A Program Analysis

Spring 2006

Note 8

Prof. Kwangkeun Yi

요약 해석 틀을 떠받치는 theorem들의 증명

- Facts On α And γ
- Fixpoint Transfter Theorems
- Widening/Narrowing Theorems

α와 γ의 성질들

갈로아 연결 정의:

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

- α는 최소를 보존한다(*strict*): $\alpha(\bot) = \hat{\bot}$.

  Proof. $\alpha(\bot) \sqsubseteq \hat{\bot}$ 왜냐면 $\bot \sqsubseteq \gamma(\hat{\bot})$.

- $id \sqsubseteq \gamma \circ \alpha$.

  Proof. $\alpha(x) \sqsubseteq \alpha(x)$ 이고 갈로아 연결로 $x \sqsubseteq \gamma(\alpha(x))$.

- $\alpha \circ \gamma \sqsubseteq id$.

  Proof. $\gamma(\hat{x}) \sqsubseteq \gamma(\hat{x})$ 이고 갈로아 연결로 $\alpha(\gamma(\hat{x})) \sqsubseteq \hat{x}$.

- γ 는 단조(*monotonic*) 함수이다.

  Proof. $\hat{x} \sqsubseteq \hat{y}$ 라면 $\alpha(\gamma(\hat{x})) \sqsubseteq \hat{y}$, 따라서 갈로아 연결로 $\gamma(\hat{x}) \sqsubseteq \gamma(\hat{y})$.

α와 γ의 성질들

갈로아 연결 정의:

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

- α 는 단조(*monotonic*) 함수이다.

  Proof. $x \sqsubseteq y$ 라면 $x \sqsubseteq \gamma(\alpha(y))$, 따라서 갈로아 연결로 $\alpha(x) \sqsubseteq \alpha(y)$.

- α 는 연속(*continuous*) 함수이다.

  Proof. 보일 것은 D의 임의의 체인 S에 대해서
  $\alpha(\bigsqcup_{x\in S} x) = \bigsqcup_{x\in S} \alpha(x)$. α가 단조함수 이므로,
  $\bigsqcup_{x\in S} \alpha(x) \sqsubseteq \alpha(\bigsqcup_{x\in S} x)$ 이다. 반대 방향도 성립한다. 왜냐하면,
  $id \sqsubseteq \gamma \circ \alpha$이고 γ가 단조(*monotonic*) 함수 이므로,

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

  이고, 갈로아 연결로 $\alpha(\bigsqcup_{x\in S} x) \sqsubseteq \bigsqcup_{x\in S} \alpha(x)$ 가 된다.

α와 γ의 성질들

- D와 $\hat{D}$가 $\sqcup$에 대해서 닫혀있으면 ($\sqcup$-semi-lattice), $\alpha(x \sqcup y) = \alpha(x) \sqcup \alpha(y)$.

  Proof. α는 단조(*monotonic*) 함수이므로, $\alpha(x) \sqcup \alpha(y) \sqsubseteq \alpha(x \sqcup y)$이다. 한편, $x \sqsubseteq \gamma(\alpha(x)) \sqsubseteq \gamma(\alpha(x) \sqcup \alpha(y))$ 이고 $y \sqsubseteq \gamma(\alpha(y)) \sqsubseteq \gamma(\alpha(y) \sqcup \alpha(y))$ 이므로 $x \sqcup y \sqsubseteq \gamma(\alpha(x) \sqcup \alpha(y))$. 갈로아 연결로, $\alpha(x \sqcup y) \sqsubseteq \alpha(x) \sqcup \alpha(y)$.

Fixpoint Transfer Theorem1

Theorem (fixpoint transfer)

D와 $\hat{D}$는 각각 CPO이고 갈로아 연결이 되어있다. 함수 $F : D \to D$는 연속함수이고 $\hat{F} : \hat{D} \to \hat{D}$는 단조함수이다. $\alpha \circ F \sqsubseteq \hat{F} \circ \alpha$ 이다. 그러면,

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

Proof. $\alpha \circ F \sqsubseteq \hat{F} \circ \alpha$로 부터

$$\forall n \in \mathbb{N} : \alpha \circ F^n \sqsubseteq \hat{F}^n \circ \alpha$$

이다. 왜냐하면,

$$\begin{array}{rcl}
\alpha \circ F^{n+1} & = & \alpha \circ F \circ F^n \\
& \sqsubseteq & \alpha \circ F \circ \gamma \circ \alpha \circ F^n \\
& & (\alpha \circ F\text{는 단조함수이고 } id \sqsubseteq \gamma \circ \alpha) \\
& \sqsubseteq & \alpha \circ F \circ \gamma \circ \hat{F}^n \circ \alpha \\
& & (\alpha \circ F \circ \gamma\text{는 단조함수이고 귀납가정}) \\
& \sqsubseteq & \hat{F} \circ \hat{F}^n \circ \alpha. \\
& & (\alpha \circ F \sqsubseteq \hat{F} \circ \alpha \text{ 이고 } \hat{F}\text{는 단조함수이므로 } \alpha \circ F \circ \gamma \sqsubseteq \hat{F} \circ \alpha \circ \gamma \sqsubseteq \hat{F})
\end{array}$$

따라서

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

즉

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

더불어 $\{\alpha(F^i\bot)\}_i$와 $\{\hat{F}^i\hat{\bot}\}_i$는 체인이므로 ($\alpha$, F, $\hat{F}$이 모두 단조함수이기때문) $\sqcup_i \alpha(F^i\bot)$와 $\sqcup_i(\hat{F}^i\hat{\bot})$이 존재하며

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

이다. α가 연속함수이므로 왼편식을 다시 쓰면,

$$\begin{array}{rcll}
\bigsqcup_{i \in \mathbb{N}} \alpha(F^i\bot) & = & \alpha(\bigsqcup_{i \in \mathbb{N}}(F^i\bot)) & (\alpha\text{는 연속함수}) \\
& = & \alpha(\mathit{lfp} F). & (\text{연속함수의 최소고정점})
\end{array}$$

즉,

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

$\square$

Fixpoint Transfer Theorem1b

Theorem (fixpoint transfer')

D와 $\hat{D}$는 각각 CPO이고 갈로아 연결이 되어있다. 함수 $F : D \to D$는 연속함수이고 $\hat{F} : \hat{D} \to \hat{D}$는 팽창함수 이다. $\alpha \circ \gamma = id$이다. $\alpha \circ F \sqsubseteq \hat{F} \circ \alpha$ 이다. 그러면,

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

Proof. $\alpha \circ F \sqsubseteq \hat{F} \circ \alpha$로 부터

$$\forall n \in \mathbb{N} : \alpha \circ F^n \sqsubseteq \hat{F}^n \circ \alpha$$

이다. 왜냐하면,

$$\begin{array}{rcl} \alpha \circ F^{n+1} & = & \alpha \circ F \circ F^n \\ & \sqsubseteq & \alpha \circ F \circ \gamma \circ \alpha \circ F^n \\ & & (\alpha \circ F\text{는 단조함수이고 } id \sqsubseteq \gamma \circ \alpha) \\ & \sqsubseteq & \alpha \circ F \circ \gamma \circ \hat{F}^n \circ \alpha \\ & & (\alpha \circ F \circ \gamma\text{는 단조함수이고 귀납가정}) \\ & \sqsubseteq & \hat{F} \circ \hat{F}^n \circ \alpha. \\ & & (\alpha \circ F \sqsubseteq \hat{F} \circ \alpha \text{ 이고 } \alpha \circ \gamma = id\text{이므로 } \alpha \circ F \circ \gamma \sqsubseteq \hat{F} \circ \alpha \circ \gamma = \hat{F}) \end{array}$$

따라서

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

즉

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

더불어 $\{\alpha(F^i\bot)\}_i$와 $\{\hat{F}^i\hat{\bot}\}_i$는 체인이므로($\alpha$와 F는 단조함수, $\hat{F}$는 팽창함수이기 때문) $\sqcup_i \alpha(F^i\bot)$와 $\sqcup_i(\hat{F}^i\hat{\bot})$이 존재하며

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

이다. α가 연속함수이므로 왼편식을 다시 쓰면,

$$\begin{array}{rcll} \bigsqcup_{i \in \mathbb{N}} \alpha(F^i\bot) & = & \alpha(\bigsqcup_{i \in \mathbb{N}}(F^i\bot)) & (\alpha\text{는 연속함수}) \\ & = & \alpha(lfpF). & (\text{연속함수의 최소고정점}) \end{array}$$

즉,

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

□

Fixpoint Transfer Theorem2

Theorem (fixpoint transfer2)

CPO D와 $\hat{D}$는 갈로아 연결 $D \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \hat{D}$ 되어있다. 함수 $F : D \to D$ 는 연속함수 이고, $\hat{F} : \hat{D} \to \hat{D}$ 는 단조함수이거나 팽창함수이다. $\alpha\, f \sqsubseteq \hat{f}$ 이면 $\alpha(F\ f) \sqsubseteq \hat{F}\ \hat{f}$ 이다. 그러면,

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

Proof. 갈로아 연결시켜주는 α는 최소를 보존하므로 $\alpha \perp \sqsubseteq \hat{\perp}$이다. 조건 "$\alpha\, f \sqsubseteq \hat{f}$ 이면 $\alpha(F\ f) \sqsubseteq \hat{F}\ \hat{f}$" 으로부터

$$\alpha(F \perp) \sqsubseteq \hat{F}\ \hat{\perp}$$

이고, 같은 조건때문에 결국은,

$$\forall i \in \mathbb{N} : \alpha(F^i \perp) \sqsubseteq \hat{F}^i \hat{\perp}.$$

한편 $\{\alpha(F^i \perp)\}_i$와 $\{\hat{F}^i \hat{\perp}\}_i$는 체인이므로($\alpha$와 F는 단조함수 이고 $\hat{F}$는 단조함수이거나 팽창함수이기 때문) $\sqcup_i \alpha(F^i \perp)$ 와 $\sqcup_i (\hat{F}^i \hat{\perp})$가 존재하며

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

α가 연속함수이므로,

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

즉, F가 연속함수이므로,

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

□

Widening Theorem

축지법의 조건:

$$\forall a, b \in \hat{D} : (a \sqsubseteq a \bigtriangledown b) \ \wedge \ (b \sqsubseteq a \bigtriangledown b) \tag{1}$$

이고

$$\forall 증가하는\ 체인 \{x_i\}_i : 체인 y_0 = x_0, y_{i+1} = y_i \bigtriangledown x_{i+1} 는\ 유한 \tag{2}$$

축지해서 정의되는 체인:

$$\begin{array}{rcll} \hat{X}_0 & = & \hat{\perp} & \\ \hat{X}_{i+1} & = & \hat{X}_i & \hat{F}(\hat{X}_i) \sqsubseteq \hat{X}_i \text{ 이면} \\ & = & \hat{X}_i \bigtriangledown \hat{F}(\hat{X}_i) & \text{아니면,} \end{array} \tag{3}$$

Theorem (widen's safety)

$\hat{D}$는 CPO 이고, $\hat{F} : \hat{D} \to \hat{D}$는 단조(monotonic) 함수이고, $\bigtriangledown : \hat{D} \times \hat{D} \to \hat{D}$는 조건 (1) 과 (2)을 만족하면, (3)로 정의되는 체인 $\{\hat{X}_i\}_i$ 은 유한하고 그 끝은 $\lim_{i \in \mathbb{N}} \hat{X}_i \sqsupseteq \bigsqcup_{i \in \mathbb{N}} \hat{F}^i(\hat{\perp})$이다.

축지법의 조건:

$$\forall a, b \in \hat{D} : (a \sqsubseteq a \triangledown b) \wedge (b \sqsubseteq a \triangledown b) \tag{4}$$

이고

$$\forall \text{증가하는 체인}\{x_i\}_i : \text{체인} y_0 = x_0, y_{i+1} = y_i \triangledown x_{i+1} \text{는 유한} \tag{5}$$

축지해서 정의되는 체인:

$$\begin{aligned} \hat{X}_0 &= \hat{\bot} \\ \hat{X}_{i+1} &= \hat{X}_i \qquad\qquad \hat{F}(\hat{X}_i) \sqsubseteq \hat{X}_i \text{ 이면} \\ &= \hat{X}_i \triangledown \hat{F}(\hat{X}_i) \quad \text{아니면,} \end{aligned} \tag{6}$$

Proof. 체인 $\{\hat{X}_i\}_i$이 유한하다는 것과 $\forall i \in \mathbb{N} : \hat{F}^i(\hat{\bot}) \sqsubseteq \hat{X}_i$임을 보이면 된다.
$\{\hat{F}(\hat{X}_i)\}_i$가 증가하는 체인이면, 체인 $\{\hat{X}_i\}_i$은 (5)의 조건을 만족하므로 유한하게 된다. $\{\hat{F}(\hat{X}_i)\}_i$가 증가하는 체인인가? 그렇다. 왜냐면, (6)에 의해서 $\hat{F}(\hat{X}_{i+1})$는 $\hat{F}(\hat{X}_i)$ 이거나 $\hat{F}(\hat{X}_i \triangledown \hat{F}(\hat{X}_i))$ 이다. 조건 (4)으로 $\hat{X}_i \sqsubseteq \hat{X}_i \triangledown \hat{F}(\hat{X}_i)$ 이고 $\hat{F}$는 단조(*monotonic*) 함수이므로, 항상 $\hat{F}(\hat{X}_i) \sqsubseteq \hat{F}(\hat{X}_{i+1})$이다.
이제 $\forall i \in \mathbb{N} : \hat{F}^i(\hat{\bot}) \sqsubseteq \hat{X}_i$을 보이자. 기초는 당연하다 $\hat{F}^0(\hat{\bot}) = \hat{\bot} \sqsubseteq \hat{X}_0$. $\hat{F}^i(\hat{\bot}) \sqsubseteq \hat{X}_i$라고 하자. $\hat{F}$가 단조(*monotonic*) 함수 이므로 $\hat{F}^{i+1}(\hat{\bot}) \sqsubseteq \hat{F}(\hat{X}_i)$이다.
(6)에 의해 $\hat{X}_{i+1}$는 두 경우가 있다. $\hat{F}(\hat{X}_i) \sqsubseteq \hat{X}_i$일 때는 $\hat{X}_{i+1} = \hat{X}_i$이므로, 이때는 $\hat{F}(\hat{X}_i) \sqsubseteq \hat{X}_{i+1}$, 따라서 $\hat{F}^{i+1}(\hat{\bot}) \sqsubseteq \hat{X}_{i+1}$이다.
$\hat{F}(\hat{X}_i) \not\sqsubseteq \hat{X}_i$일 때는 $\hat{X}_{i+1} = \hat{X}_i \triangledown \hat{F}(\hat{X}_i)$이므로, 이때도 $\triangledown$의 조건에 의해 $\hat{F}(\hat{X}_i) \sqsubseteq \hat{X}_i \triangledown \hat{F}(\hat{X}_i) = \hat{X}_{i+1}$. 귀납가정에 의해 $\hat{F}^{i+1}(\hat{\bot}) \sqsubseteq \hat{F}(\hat{X}_i)$이므로, $\hat{F}^{i+1}(\hat{\bot}) \sqsubseteq \hat{X}_{i+1}$이다. □

Narrowing Theorem

좁히기 $\triangle$의 조건:

$$\forall a, b \in \hat{D} : x \sqsupseteq y \Rightarrow x \sqsupseteq (x \triangle y) \sqsupseteq y \tag{7}$$

이고

$$\forall \text{감소하는 체인}\{x_i\}_i : \text{체인} y_0 = x_0, y_{i+1} = y_i \triangle x_{i+1} \text{는 유한} \tag{8}$$

좁히기로 정의하는 체인:

$$\begin{aligned} \hat{Y}_0 &= \hat{\mathcal{A}} \\ \hat{Y}_{i+1} &= \hat{Y}_i \triangle \mathcal{F}(\hat{Y}_i) \end{aligned} \tag{9}$$

Theorem (narrow's safety)

$\hat{D}$는 CPO 이고, $\hat{F} : \hat{D} \to \hat{D}$는 단조(monotonic) 함수 이고, $\triangle : \hat{D} \times \hat{D} \to \hat{D}$는 조건 (7) 과 (8)을 만족하고, $\hat{F}(\hat{\mathcal{A}}) \sqsubseteq \hat{\mathcal{A}}$ 이면, (9)로 정의되는 체인 $\{\hat{Y}_i\}_i$ 은 유한하고 그 끝도 $\lim_{i \in \mathbb{N}} \hat{Y}_i \sqsupseteq \bigsqcup_{i \in \mathbb{N}} \hat{F}^i(\hat{\bot})$ 이다.

좁히기 $\triangle$의 조건:

$$\forall a, b \in \hat{D} : x \sqsupseteq y \Rightarrow x \sqsupseteq (x \triangle y) \sqsupseteq y \tag{10}$$

이고

$$\forall \text{감소하는 체인}\{x_i\}_i : \text{체인 } y_0 = x_0, y_{i+1} = y_i \triangle x_{i+1} \text{ 는 유한} \tag{11}$$

좁히기로 정의하는 체인:

$$\begin{aligned} \hat{Y}_0 &= \hat{\mathcal{A}} \\ \hat{Y}_{i+1} &= \hat{Y}_i \triangle \hat{\mathcal{F}}(\hat{Y}_i) \end{aligned} \tag{12}$$

Proof. 체인 $\{\hat{Y}_i\}_i$이 유한하다는 것과 $\forall i \in \mathbb{N} : \hat{F}^i(\hat{\bot}) \sqsubseteq \hat{Y}_i$임을 보이면 된다.
$\{\hat{F}(\hat{Y}_i)\}_i$가 감소하는 체인이면, 체인 $\{\hat{Y}_i\}_i$은 (11)의 조건을 만족하므로 유한하게 된다. $\{\hat{F}(\hat{Y}_i)\}_i$가 감소하는 체인인가? 그렇다, 다음이 사실이라면:

$$\forall i \in \mathbb{N} : \hat{Y}_i \sqsupseteq \hat{F}(\hat{Y}_i). \tag{13}$$

왜냐면, $\hat{Y}_i \sqsupseteq \hat{F}(\hat{Y}_i)$ 이라면 조건 (10)에 의해서 $\hat{Y}_i \sqsupseteq \hat{Y}_i \triangle \hat{F}(\hat{Y}_i) \sqsupseteq \hat{F}(\hat{Y}_i)$. $\hat{F}$는 단조(*monotonic*) 함수이므로 $\hat{F}(\hat{Y}_i) \sqsupseteq \hat{F}(\hat{Y}_i \triangle \hat{F}(\hat{Y}_i)) = \hat{F}(\hat{Y}_{i+1})$ 이다.
위의 (13)은 사실인가? 그렇다. 기초 경우, 정의 (12)와 조건 $\hat{\mathcal{A}} \sqsupseteq \hat{F}(\hat{\mathcal{A}})$에 의해서 $\hat{Y}_0 \sqsupseteq \hat{F}(\hat{Y}_0)$. 귀납 경우: $\hat{Y}_i \sqsupseteq \hat{F}(\hat{Y}_i)$라고 하자. 조건 (10)에 의해서, $\hat{Y}_i \sqsupseteq \hat{Y}_i \triangle \hat{F}(\hat{Y}_i) \sqsupseteq \hat{F}(\hat{Y}_i)$. 정의 (12)에 의해 다시 쓰면, $\hat{Y}_i \sqsupseteq \hat{Y}_{i+1} \sqsupseteq \hat{F}(\hat{Y}_i)$. 여기에, $\hat{F}$는 단조(*monotonic*) 함수 이므로, 왼편 두개로 부터 $\hat{F}(\hat{Y}_i) \sqsupseteq \hat{F}(\hat{Y}_{i+1})$이고, 오른쪽에 연결하면 $\hat{Y}_{i+1} \sqsupseteq \hat{F}(\hat{Y}_{i+1})$.
체인 $\{\hat{Y}_i\}_i$이 유한하다는 것은 보였고, $\forall i \in \mathbb{N} : \hat{F}^i(\hat{\bot}) \sqsubseteq \hat{Y}_i$임을 보이자. 기초 경우, $\hat{F}^0(\hat{\bot}) = \hat{\bot}$이므로 당연하다. 귀납 경우: $\hat{F}^i(\hat{\bot}) \sqsubseteq \hat{Y}_i$라고 하자. $\hat{F}$는 단조(*monotonic*) 함수이므로, $\hat{F}^{i+1}(\hat{\bot}) \sqsubseteq \hat{F}(\hat{Y}_i)$. 항상 $\hat{Y}_i \sqsupseteq \hat{F}(\hat{Y}_i)$이므로(13) 조건 (10)에 의해서 $\hat{Y}_i \triangle \hat{F}(\hat{Y}_i) \sqsupseteq \hat{F}(\hat{Y}_i)$이므로,
$\hat{F}^{i+1}(\hat{\bot}) \sqsubseteq \hat{F}(\hat{Y}_i) \sqsubseteq \hat{Y}_i \triangle \hat{F}(\hat{Y}_i) = \hat{Y}_{i+1}$. □