SNU 4541.664A Program Analysis
Note 5

Prof. Kwangkeun Yi

요약 해석 틀을 떠받치는 theorem들의 증명

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

α와 γ의 성질들

갈로아 연결 정의:

$$\forall x \in D, x^\sharp \in D^\sharp : \alpha(x) \sqsubseteq x^\sharp \iff x \sqsubseteq \gamma(x^\sharp).$$

- α는 최소를 보존한다(*strict*): $\alpha(\bot) = \bot^\sharp$.

  Proof. $\alpha(\bot) \sqsubseteq \bot^\sharp$ 왜냐면 $\bot \sqsubseteq \gamma(\bot^\sharp)$.
- $id \sqsubseteq \gamma \circ \alpha$.

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

  Proof. $\gamma(x^\sharp) \sqsubseteq \gamma(x^\sharp)$ 이고 갈로아 연결로 $\alpha(\gamma(x^\sharp)) \sqsubseteq x^\sharp$.
- γ 는 단조(*monotonic*) 함수이다.

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

α와 γ의 성질들

갈로아 연결 정의:

$$\forall x \in D, x^\sharp \in D^\sharp : \alpha(x) \sqsubseteq x^\sharp \iff x \sqsubseteq \gamma(x^\sharp).$$

- 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 $D^\sharp$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 Theorem

Theorem (fixpoint transfer)

D와 $D^\sharp$는 각각 CPO이고 갈로아 연결이 되어있다. 함수 $F : D \to D$는 연속함수이고 $F^\sharp : D^\sharp \to D^\sharp$는 단조함수이거나 팽창함수이다. $F \circ \gamma \sqsubseteq \gamma \circ F^\sharp$ 이다. 그러면,

$$lfp F \sqsubseteq \gamma(\bigsqcup_{i \in \mathbb{N}} F^{\sharp i}(\bot^\sharp)).$$

Proof. $F \circ \gamma \sqsubseteq \gamma \circ F^\sharp$로 부터

$$\forall n \in \mathbb{N} : F^n(\bot) \sqsubseteq \gamma(F^{\sharp n}(\bot^\sharp))$$

이다. 귀납법으로 증명된다. 즉 $n = 0$일때 왼편은 $\bot$이고 오른편은 $\gamma(\bot)$ 이므로 성립한다. 귀납경우를 따지면

$$\begin{array}{rcl}
F^{n+1}(\bot) & = & F(F^n(\bot)) \\
 & \sqsubseteq & F(\gamma(F^{\sharp n}(\bot^\sharp))) \quad (\text{귀납가정과 단조 } F) \\
 & \sqsubseteq & \gamma(F^\sharp(F^{\sharp n}(\bot^\sharp))) \\
 & & (\text{조건 } F \circ \gamma \sqsubseteq \gamma \circ F^\sharp) \\
 & = & \gamma(F^{\sharp n+1}(\bot^\sharp)).
\end{array}$$

이로부터, 최종 증명목표인

$$lfp F \sqsubseteq \gamma(\bigsqcup_{i \in \mathbb{N}} F^{\sharp i}(\bot^\sharp))$$

를 증명할 수 있다. F는 연속함수여서 단조함수이므로 $\{F^i \bot\}_i$는 체인이고 $\sqcup_i(F^i\bot)$가 존재한다. $F^\sharp$는 단조함수이거나 팽창함수이므로 $\{F^{\sharp i}\bot^\sharp\}_i$는 체인이고 γ는 단조함수이므로 $\{\gamma(F^{\sharp i}\bot^\sharp)\}_i$도 체인이어서 $\sqcup_i(\gamma(F^{\sharp i}\bot^\sharp))$도 존재한다. 따라서,

$$\forall n \in \mathbb{N} : F^n(\bot) \sqsubseteq \gamma(F^{\sharp n}(\bot^\sharp))$$

로 부터 다음이 성립한다:

$$\begin{array}{rcl}
\bigsqcup_{i \in \mathbb{N}} F^i(\bot) & \sqsubseteq & \bigsqcup_{i \in \mathbb{N}} \gamma(F^{\sharp i}(\bot^\sharp)) \\
 & \sqsubseteq & \gamma(\bigsqcup_{i \in \mathbb{N}} F^{\sharp i}(\bot^\sharp)). \quad (\gamma \text{ 는 단조함수})
\end{array}$$

□

Widening Theorem

축지법의 조건:

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

이고

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

축지해서 정의되는 체인:

$$\begin{array}{rcll} X_0^\sharp & = & \perp^\sharp & \\ X_{i+1}^\sharp & = & X_i^\sharp & F^\sharp(X_i^\sharp) \sqsubseteq X_i^\sharp \text{ 이면} \\ & = & X_i^\sharp \bigtriangledown F^\sharp(X_i^\sharp) & \text{아니면,} \end{array} \tag{3}$$

Theorem (widen's safety)

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

축지법의 조건:

$$\forall a, b \in D^\sharp : (a \sqsubseteq a \bigtriangledown b) \ \wedge \ (b \sqsubseteq a \bigtriangledown b) \tag{4}$$

이고

$$\forall \text{증가하는 체인} \{a_i\}_i : \text{체인} \, x_0 = a_0, x_{i+1} = x_i \bigtriangledown a_{i+1} \, \text{는 유한} \tag{5}$$

축지해서 정의되는 체인:

$$\begin{aligned} X_0^\sharp &= \bot^\sharp \\ X_{i+1}^\sharp &= X_i^\sharp & F^\sharp(X_i^\sharp) \sqsubseteq X_i^\sharp \text{ 이면} \\ &= X_i^\sharp \bigtriangledown F^\sharp(X_i^\sharp) & \text{아니면,} \end{aligned} \tag{6}$$

Proof. 체인 $\{X_i^\sharp\}_i$이 유한하다는 것과 $\forall i \in \mathbb{N} : F^{\sharp i}(\bot^\sharp) \sqsubseteq X_i^\sharp$임을 보이면 된다.

- $\{F^\sharp(X_i^\sharp)\}_i$가 증가하는 체인이면, 체인 $\{X_i^\sharp\}_i$은 (5)의 조건을 만족하므로 유한하게 된다. $\{F^\sharp(X_i^\sharp)\}_i$가 증가하는 체인인가? 그렇다. 왜냐면, (6)에 의해서 $F^\sharp(X_{i+1}^\sharp)$는 $F^\sharp(X_i^\sharp)$ 이거나 $F^\sharp(X_i^\sharp \bigtriangledown F^\sharp(X_i^\sharp))$ 이다. 조건 (4)으로 $X_i^\sharp \sqsubseteq X_i^\sharp \bigtriangledown F^\sharp(X_i^\sharp)$ 이고 $F^\sharp$는 단조(*monotonic*) 함수이므로, 항상 $F^\sharp(X_i^\sharp) \sqsubseteq F^\sharp(X_{i+1}^\sharp)$이다.
- 이제 $\forall i \in \mathbb{N} : F^{\sharp i}(\bot^\sharp) \sqsubseteq X_i^\sharp$을 보이자. 기초는 당연하다 $F^{\sharp 0}(\bot^\sharp) = \bot^\sharp \sqsubseteq X_0^\sharp$. $F^{\sharp i}(\bot^\sharp) \sqsubseteq X_i^\sharp$라고 하자. $F^\sharp$가 단조(*monotonic*) 함수 이므로 $F^{\sharp i+1}(\bot^\sharp) \sqsubseteq F^\sharp(X_i^\sharp)$이다.
  (6)에 의해 $X_{i+1}^\sharp$는 두 경우가 있다. $F^\sharp(X_i^\sharp) \sqsubseteq X_i^\sharp$일 때는 $X_{i+1}^\sharp = X_i^\sharp$이므로, 이때는 $F^\sharp(X_i^\sharp) \sqsubseteq X_{i+1}^\sharp$, 따라서 $F^{\sharp i+1}(\bot^\sharp) \sqsubseteq X_{i+1}^\sharp$이다.
  $F^\sharp(X_i^\sharp) \not\sqsubseteq X_i^\sharp$일 때는 $X_{i+1}^\sharp = X_i^\sharp \bigtriangledown F^\sharp(X_i^\sharp)$이므로, 이때도 $\bigtriangledown$의 조건에 의해 $F^\sharp(X_i^\sharp) \sqsubseteq X_i^\sharp \bigtriangledown F^\sharp(X_i^\sharp) = X_{i+1}^\sharp$.
  모든 경우 $F^\sharp(X_i^\sharp) \sqsubseteq X_{i+1}^\sharp$이므로, 귀납가정 $F^{\sharp i+1}(\bot^\sharp) \sqsubseteq F^\sharp(X_i^\sharp)$에 의해, $F^{\sharp i+1}(\bot^\sharp) \sqsubseteq X_{i+1}^\sharp$이다. □

Narrowing Theorem

좁히기 $\triangle$의 조건:

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

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:

$$\begin{aligned} Y_0^\sharp &= \mathcal{A}^\sharp \\ Y_{i+1}^\sharp &= Y_i^\sharp \triangle F^\sharp(Y_i^\sharp) \end{aligned} \tag{9}$$

Theorem (narrow's safety)

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

좁히기 $\triangle$의 조건:

$$\forall a, b \in D^\sharp : a \sqsupseteq b \Rightarrow a \sqsupseteq (a \triangle b) \sqsupseteq b \tag{10}$$

이고

$$\forall \text{감소하는 체인} \{a_i\}_i : \text{체인 } y_0 = a_0, y_{i+1} = y_i \triangle a_{i+1} \text{ 는 유한} \tag{11}$$

좁히기로 정의하는 체인:

$$\begin{aligned} Y_0^\sharp &= \mathcal{A}^\sharp \\ Y_{i+1}^\sharp &= Y_i^\sharp \triangle F^\sharp(Y_i^\sharp) \end{aligned} \tag{12}$$

Proof. 체인 $\{Y_i^\sharp\}_i$이 유한하다는 것과 $\forall i \in \mathbb{N} : F^{\sharp i}(\bot^\sharp) \sqsubseteq Y_i^\sharp$임을 보이면 된다.

- $\{F^\sharp(Y_i^\sharp)\}_i$가 감소하는 체인이면, 체인 $\{Y_i^\sharp\}_i$은 (11)의 조건을 만족하므로 유한하게 된다. $\{F^\sharp(Y_i^\sharp)\}_i$가 감소하는 체인인가? 그렇다, 다음이 사실이라면:

$$\forall i \in \mathbb{N} : Y_i^\sharp \sqsupseteq F^\sharp(Y_i^\sharp). \tag{13}$$

  왜냐면, $Y_i^\sharp \sqsupseteq F^\sharp(Y_i^\sharp)$ 이라면 조건 (10)에 의해서 $Y_i^\sharp \sqsupseteq Y_i^\sharp \triangle F^\sharp(Y_i^\sharp) \sqsupseteq F^\sharp(Y_i^\sharp)$. $F^\sharp$는 단조(*monotonic*) 함수이므로 $F^\sharp(Y_i^\sharp) \sqsupseteq F^\sharp(Y_i^\sharp \triangle F^\sharp(Y_i^\sharp)) = F^\sharp(Y_{i+1}^\sharp)$ 이다.
  위의 (13)은 사실인가? 그렇다. 기초 경우, 정의 (12)와 조건 $\mathcal{A}^\sharp \sqsupseteq \mathcal{F}^\sharp(\mathcal{A}^\sharp)$에 의해서 $Y_0^\sharp \sqsupseteq F^\sharp(Y_0^\sharp)$. 귀납 경우: $Y_i^\sharp \sqsupseteq F^\sharp(Y_i^\sharp)$라고 하자. 조건 (10)에 의해서, $Y_i^\sharp \sqsupseteq Y_i^\sharp \triangle F^\sharp(Y_i^\sharp) \sqsupseteq F^\sharp(Y_i^\sharp)$. 정의 (12)에 의해 다시 쓰면, $Y_i^\sharp \sqsupseteq Y_{i+1}^\sharp \sqsupseteq F^\sharp(Y_i^\sharp)$. 여기에, $F^\sharp$는 단조(*monotonic*) 함수 이므로, 왼편 두개로 부터 $F^\sharp(Y_i^\sharp) \sqsupseteq F^\sharp(Y_{i+1}^\sharp)$이고, 오른쪽에 연결하면 $Y_{i+1}^\sharp \sqsupseteq F^\sharp(Y_{i+1}^\sharp)$.
- 체인 $\{Y_i^\sharp\}_i$이 유한하다는 것은 보였고, $\forall i \in \mathbb{N} : F^{\sharp i}(\bot^\sharp) \sqsubseteq Y_i^\sharp$임을 보이자. 기초 경우, $F^{\sharp 0}(\bot^\sharp) = \bot^\sharp$이므로 당연하다. 귀납 경우: $F^{\sharp i}(\bot^\sharp) \sqsubseteq Y_i^\sharp$라고 하자. $F^\sharp$는 단조(*monotonic*) 함수이므로, $F^{\sharp i+1}(\bot^\sharp) \sqsubseteq F^\sharp(Y_i^\sharp)$. 항상 $Y_i^\sharp \sqsupseteq F^\sharp(Y_i^\sharp)$이므로(13) 조건 (10)에 의해서 $Y_i^\sharp \triangle F^\sharp(Y_i^\sharp) \sqsupseteq F^\sharp(Y_i^\sharp)$이므로, $F^{\sharp i+1}(\bot^\sharp) \sqsubseteq F^\sharp(Y_i^\sharp) \sqsubseteq Y_i^\sharp \triangle F^\sharp(Y_i^\sharp) = Y_{i+1}^\sharp$. □