6 장

프로그램 분석

프로그램이 과연 우리가 바라는 대로 실행될 것인가? 이 질문에 대한 답를 자동으로 해 주는 소프트웨어는 가능한가? 즉, 프로그램이 우리가 기획한 데로 실행될 것인지를 미리 검증하는 기술은 가능한가? 이러한 기술이 소프트웨어 기술의 중요축으로 발전하여 왔고, 프로그램 분석 기술이 그에 대한 답으로 나온 것이다.

프로그램 분석(*static program analysis*)은 프로그램이 실행중에 가지는 성질을 실행전에 자동으로 안전하게 어림잡는 일반적인 방법이다. 정적 분석(*static analysis*)이라고도 한다.

- "실행전"은 프로그램을 실행시키지 않고 분석한다는 뜻이다.
- "자동으로"는 프로그램이 분석을 해 준다는 뜻이다, 사람이 손으로 하는 분석이 아니라.
- "안전하게"는 프로그램이 실행중에 가지는 모든 상황을 빠뜨림없이 고려한다는 뜻이다. 예를 들어, 프로그램 식 "`x+1`"가 가질 수 있는 값들을 안전하게 예측하려면, 변수 `x`가 가질 수 있는 모든 값들을 고려해야 알 수 있다. 하나라도 놓치면 안된다.

  어떤 프로그램식 e는 실제 1이나 2를 계산한다고 하자. 어림잡는 과정을 통해서 분석한 결과, 그 식은 "0이상"인 값을 계산한다고 결론내린다고

하자. 이 결론은 대강이지만 안전하다. 실제 계산되는 값들이 "0이상"이라고 어림잡은 결과에 모두 포섭되므로.

- "어림잡는"은 정확하게 할 수 없으므로 대략 어림잡는다는 뜻이다. 실제를 모두 포섭하도록 헐렁하게 어림잡게 된다. 그러다 보니, 실제 이외의 것들이 어림잡는 데 들어오기도 한다.

  이것은 어쩔 수 없다. 어림잡지 않고는 불가능하다. 정확하게 해 내는 분석기가 가능하다면, 불가능한 일을 할 수 있기 때문이다. 그러한 분석기를 가지고 끝나요-문제(*the halting problem*)를 푸는 프로그램을 만들 수 있기 때문이다(어떻게?).

- "일반적"이라는 뜻은, 분석 대상 프로그램의 소스언어 레벨에 제한이 없으며, 분석할 성질에도 제한이 없다는 뜻이다. 분석 대상 프로그램의 소스언어의 의미구조가 명확히 정의되어 있기만 하면 된다. 기계어, 어셈블리어, C, Java, ML등 상관없다. 분석할 성질에 대한 제약도 없다.

프로그램 분석은 "static analysis", "abstract interpretation", "type system", "model checking", "theorem proving", "data-flow analysis" 등의 다양한 이름들로 다양한 수준에서 다양한 필요에 맞추어 연구되어 왔던 기술이다.

6.1 요약 해석

요약해석(*abstract interpretation*)은 말 그대로, 프로그램을 요약해서 실행해보는 것이다. 즉, 분석할 프로그램의 실제 실행(프로그램의 의미)의 요약본을 계산하는 것이다.

요약해석(*abstract interpretation*)은 프로그램분석을 바라보는 우리들의 눈을 뜨게 한 간단하면서 강력한 틀(framework)이다.

- "틀"이라고 한 것은, 그 안에 재료를 붓기만 하면 우리가 바라는 벽돌이 나오기 때문이다. 요약해석의 틀을 따라 프로그램 분석을 디자인하면 결과로는 항상 안전한 분석기가 나온다.

- "강력한"이유는, 거의 모든 프로그램 분석이 이 틀에서 디자인 될 수 있다는 주장이 설득력 있기 때문이다[CC95b, CC93, CC95a, Cou97]. 이 틀을 모르고 지금까지 고안된 거의 모든 프로그램 분석들이 모두 이 틀로 만들어 낼 수 있다고 증명되었다. 이런 과거로 보아 짐작컨데 앞으로 우리가 고안하게 될 프로그램 분석들은 대부분 이 틀에 넣어 만들어 낼 수 있을 것이라고 믿게된 것이다.

- "간단"한 이유는, 그 틀을 사용하는 방법이 간단하기 때문이다. 생각하고 체크할 것이 몇개되지 않는다.

- "눈을 뜨게한"이란, 고안한 프로그램 분석이 무슨 일을 하는 것인지를 깨닫게 해주기 때문이다. 궁리해낸 프로그램 분석을 그 틀 안에서 바라보면 결국은 그 분석이 무엇을 하는 것인지를 알게된다. 내가 만든 분석이 무엇을 어떻게 요약해서 프로그램을 실행해 보는 격이구나, 를 깨닫게 해준다.

  이러한 이해가 왜 필요한가? 우리가 고안한 분석, 그 이상의 것을 고안할 수 있는 지평을 열어주기 때문이다. 예를 들면 마치 이런것이다. 피켜스케이팅 선수가 한 지점에서 점점 빨리 뱅뱅 돈다. 어느 누군가가 폈던 팔을 우연히 차렷자세로 했더니 도는 속도가 증가하는 것을 겪었던 것이다. 그것을 보고 뉴튼역학을 이해하고 있는 사람이 알려준다. 그 현상은 같은 회전 에너지가 회전 반경이 줄어드는 것을 회전 속도로 상쇄시키는 것이라고. 그런거였구나, 그렇다면 이런 안무도 가능하겠구나. 달려오는 여자 파트너의 팔을 될 수 있으면 짧게 잡아서 회전시켜라, 그러면 그 파트너의 회전이 민첩해 질것이다. 늦은 음악에 맞게 천천히 회전시키고 싶으면 팔을 길게 펴고 달려오는 파트너의 팔도 길게 잡고, 몸도 회전반경이 최대한 길어지도록 쭉 펴라.

요약해석에서 프로그램 분석은 실제 실행을 요약해서 해 보는 것이다. 분석할 프로그램의 실제 실행은 그 소스언어의 의미구조(*semantics*)에 의해 정의된다. 그 요약본은 소스언어의 의미구조를 요약해서 정의된다. 이 때 요약본은

안전해야 한다. 요약본으로 프로그램을 해석한 결과가 실제 실행한 결과를 모두 포섭해야 한다.

그런데, 왜 요약이 필요한 것일까? 요약없이 그대로 실행해 보면(simulation) 되는 것 아닐까? 그럴 수 없다. 실제 실행을 모두 미리 계산해 보는 것은 일반적으로 불가능하다. 실제 실행중에 일어나는 일이 무한히 많기 때문이다. 프로그램의 실행이 끊나지 않는 경우도 있고, 외부의 입력이 무한히 많을 수 도 있다. 이런 모든 상황을 모두 미리 계산해 낼 방법은 없다. 그러한 계산은 무한한 시간을 필요로한다. 프로그램 분석은 항상 끝나야 한다. 그것도 가능한한 빨리. 요약은 유한한 세계에서 프로그램을 돌리는 데 필요하다. 그래야 그 분석이 항상 끝날 수 있다.

유의할 것은, 요약은 생략이 아니라는 것이다. 그 요약은 간단하게 표현하는 것이지만, 그 표현이 의미하는 바는 모든 실제 상황을 포함해야 한다. 예를 들어, 실제가 $\{2, 4, 6, 8, \cdots\}$라고 하자. "정수"라는 이름의 요약은 그 것을 안전하게 요약하는 것이 된다. "정수"가 요약하고 있는 집합 $\{\cdots, -2, -1, 0, 1, 2, \cdots\}$는 위의 실제를 빠뜨리지 않고 포함하고 있으므로. 그런데, "4의배수"라는 요약은 안전치 않다. 2나 6등을 빼뜨린 요약이기 때문이다. 한편, "짝수"라는 요약은 안전하면서 "정수"보다는 더 정확한 요약이다. "짝수"는 실제만을 정확히 요약하고 있고 그 이외의 군더더기가 없는 요약이다.

6.1.1 요약 해석 틀: 원리

다음의 틀에따라 프로그램 분석을 구성하면 그 분석이 올바르다는 것이 보장되고 그 구현 방안도 드러난다. 다음의 과정이 그 틀이다. 요약해석의 주요 논문들[CC77, CC79, CC92a, CC92b]의 총정리라고 할 수 있다.

1. 프로그램의 실제 실행을 정의한다. 실제실행은 의미공간(*semantic domain*) D위에 정의된 함수

$$F : D \to D$$

를 이용해서 정의한다. 다음의 조건을 만족하도록 한다:

- 의미공간(*semantic domain*) D는 CPO(*complete partial order*):

$$\begin{array}{ll} \exists \text{부분순서(}\textit{partial order}\text{)} \sqsubseteq & \text{이고} \\ \exists \text{최소원소} \perp \in D & \text{이고} \\ \forall \text{체인} S \subseteq D : \exists(\bigsqcup S) \in D & \end{array}$$

  이어야 한다.

- 실행함수(*semantic function*) F는 연속 함수(*continuous function*):

$$\forall \text{체인} S \subseteq D : F(\bigsqcup_{x \in S} x) = \bigsqcup_{x \in S} F(x)$$

  이어야 한다.

- 프로그램의 실제 실행은 그러한 함수 F의 최소 고정점(*least fixed point*) $lfpF$

$$lfpF = \bigsqcup_{i \in \mathbb{N}} F^i(\perp)$$

  으로 정의한다. ($f^0 = id, f^{i+1} = f \circ f^i$.)

2. 프로그램의 요약된 실행을 정의한다. 이것은 의미공간 D에 대응하는 요약된 의미공간(*abstract domain*) $\hat{D}$을 정의하고, 그 위에 요약된 실행함수(*abstract semantic function*)

$$\hat{F} : \hat{D} \to \hat{D}$$

   를 정의하는 것이다. 다음의 조건을 만족하도록 한다:

   - $\hat{D}$는 CPO(*complete partial order*) 이어야 한다.
   - D와 $\hat{D}$은 갈로아 연결(*Galois connection*)

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

이 되있어야 한다. 즉,

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

$\hat{D}$에서 큰 원소일수록 보다 많은 것을 뜻하게 된다.

α는 실제를 요약하고(*abstraction function*), γ는 요약한 원소가 뜻하는 바를 구체화한다(*concretization function*). α는 실제 세계의 원소에 해당하는 요약이 무엇인지 알려주고, γ는 요약된 세계의 원소가 뜻하는 실제가 무엇인지 알려준다.

- 요약된 실행함수 $\hat{F}$는 단조(*monotonic*) 함수이어야 한다:

$$\forall \hat{x}, \hat{y} : x \sqsubseteq y \Rightarrow \hat{F}(x) \sqsubseteq \hat{F}(y)$$

- 실제 실행함수 F와 요약된 실행함수 $\hat{F}$ 사이는

$$\alpha \circ F \sqsubseteq \hat{F} \circ \alpha, \quad \text{다시 말해,} \quad F \circ \gamma \sqsubseteq \gamma \circ \hat{F} \tag{6.1}$$

관계가 있어야 하거나, 혹은

- 실제 실행함수 F와 요약된 실행함수 $\hat{F}$ 사이는

$$\alpha(f) \sqsubseteq \hat{f} \text{ 이면 } \alpha(F\ f) \sqsubseteq \hat{F}\ \hat{f} \tag{6.2}$$

이어야 한다.

3. 요약 분석은

$$\bigsqcup_{i \in \mathbb{N}} \hat{F}^i(\hat{\bot}) \tag{6.3}$$

의 윗뚜껑(*upper bound*)을 유한시간내에 계산해 내는 것이다. (6.3는 존재한다. $\{\hat{F}^i(\hat{\bot})\}_i$는 체인이므로.)

그러한 윗뚜껑(*upper bound*) $\hat{\mathcal{A}}$는 항상

$$\begin{array}{l}\alpha(lfpF) \sqsubseteq \hat{\mathcal{A}}, \quad \text{다시 말해} \\ lfpF \sqsubseteq \gamma\hat{\mathcal{A}}\end{array}$$

를 만족한다 (Theorem 2 혹은 Theorem 4). 즉, 분석결과 $\hat{\mathcal{A}}$가 실제실행 $lfpF$을 "포섭한다."

4. 요약된 의미공간(*abstract semantic domain*) $\hat{D}$의 높이가 유한하다면, 식 (6.3)을 그대로 계산하면 된다.

5. 요약된 의미공간(*abstract semantic domain*) $\hat{D}$의 높이가 무한하다면, 식 (6.3)의 계산은 끝나지 않는다.

   이 경우에는 다음을 만족하는

$$\bigsqcup_{i\in\mathbb{N}}(\hat{F}^i(\hat{\bot})) \sqsubseteq \lim_{i\in\mathbb{N}}(\hat{X}_i) \tag{6.4}$$

   유한한 체인 $\{\hat{X}_i\}_i$를 찾는다.

   - $\hat{F}$가 단조(*monotonic*) 함수이면, 그러한 체인 $\{\hat{X}_i\}_i$은 $\hat{F}$에 축지법(*widening operator*) $\triangledown$를 적용하여 다음과 같이 계산하면 되고

$$\begin{array}{rcll}\hat{X}_0 & = & \hat{\bot} & \\ \hat{X}_{i+1} & = & \hat{X}_i & \hat{F}(\hat{X}_i) \sqsubseteq \hat{X}_i \text{ 이면} \\ & = & \hat{X}_i \triangledown \hat{F}(\hat{X}_i) & \text{아니면,}\end{array} \tag{6.5}$$

     이 때 축지법 $\triangledown$의 조건은

$$\forall a, b \in \hat{D} : (a \sqsubseteq a \triangledown b) \ \wedge \ (b \sqsubseteq a \triangledown b) \tag{6.6}$$

이고

$$\forall \text{증가하는 체인} \{x_i\}_i : \text{체인 } y_0 = x_0, y_{i+1} = y_i \bigtriangledown x_{i+1} \text{ 는 유한} \quad (6.7)$$

해야 한다.

그렇게 정의된 체인 $\{\hat{X}_i\}_i$은 유한하고 (유한번째에 더 이상 증가하지 않고), 그 끝($\hat{F}(\hat{X}) \sqsubseteq \hat{X}$인 $\hat{X}$ (why?))은 식 (6.4)을 만족하는 안전한 분석결과가 된다 (Theorem 5).

- $\hat{F}$가 단조(*monotonic*) 함수라면, 축지법을 써서 계산된 $\hat{\mathcal{A}} \stackrel{\text{let}}{=} \lim_{i\in\mathbb{N}}(\hat{X}_i)$를 좁히기(*narrowing operator*) $\bigtriangleup$을 써서 정교하게 다듬을 수 있다. 다음의 체인 $\{\hat{Y}_i\}_i$을 계산하면 되고

$$\begin{aligned} \hat{Y}_0 &= \hat{\mathcal{A}} \\ \hat{Y}_{i+1} &= \hat{Y}_i \bigtriangleup \mathcal{F}(\hat{Y}_i) \end{aligned} \quad (6.8)$$

이 때 좁히기 $\bigtriangleup$의 조건은

$$\forall a, b \in \hat{D} : x \sqsupseteq y \Rightarrow x \sqsupseteq (x \bigtriangleup y) \sqsupseteq y \quad (6.9)$$

이고

$$\forall \text{감소하는 체인} \{x_i\}_i : \text{체인 } y_0 = x_0, y_{i+1} = y_i \bigtriangleup x_{i+1} \text{ 는 유한} \quad (6.10)$$

해야 한다.

그렇게 정의된 체인 $\{\hat{Y}_i\}_i$은 유한하고 (유한번째에 더 이상 감소하지 않고), 그 끝은 식 (6.4)을 만족하는 안전한 분석결과가 된다 (Theorem 6).

왜 위와 같이만 하면 올바른 분석이 되는가? 위에서 인용한 아래 네개의 정리들(Theorem 2,4,5,6) 때문이다. 우선, 정리들에서 사용할 갈로아 연결 α와

γ의 성질들을 밝히고 가자.

Fact 1 *두 CPO D와 $\hat{D}$를 갈로아 연결 $D \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \hat{D}$ 시키는 α와 γ는 다음 여섯가지 성질을 가지고 있다.*

갈로아 연결된 $D \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \hat{D}$의 정의를 다시쓰면:

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

- α*는 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* $\gamma(\hat{x}) \sqsubseteq \gamma(\hat{y})$.

- 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 $\alpha(\bigsqcup_{x \in S} x) = \bigsqcup_{x \in S} \alpha(x)$. α*가 단조함수 이므로,* $\bigsqcup_{x \in S} \alpha(x) \sqsubseteq \alpha(\bigsqcup_{x \in S} x)$ *이다. 반대 방향도 성립한다. 왜냐하면,* $id \sqsubseteq \alpha \circ \gamma$*이고* γ*가 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.*

□

Theorem 2 *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,*

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

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,

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

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,

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

□

사실, $\hat{F}$는 단조함수가 아니고 팽창(*extensive*) 함수이어도 된다:

$$\forall\hat{x}:x\sqsubseteq\hat{F}(x).$$

이 경우에는 $\alpha\circ\gamma=id$의 조건을 만족해야 한다:

Theorem 3 *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,*

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

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,

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

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,

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

즉,

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

□

Theorem 4 *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,*

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

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

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

이고, 같은 조건때문에 결국은,

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

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

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

α가 연속함수이므로,

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

즉, F가 연속함수이므로,

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

□

Theorem 5 *$\hat{D}$는 CPO 이고, $\hat{F} : \hat{D} \to \hat{D}$는 단조(monotonic) 함수이고, $\triangledown : \hat{D} \times \hat{D} \to \hat{D}$는 조건 (6.6) 과 (6.7)을 만족하면, (6.5)로 정의되는 체인 $\{\hat{X}_i\}_i$ 은*

유한하고 그 끝은 $\lim_{i\in\mathbb{N}} \hat{X}_i \sqsupseteq \bigsqcup_{i\in\mathbb{N}} \hat{F}^i(\hat{\bot})$*이다.*

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 (6.7)의 조건을 만족하므로 유한하게 된다. $\{\hat{F}(\hat{X}_i)\}_i$가 증가하는 체인인가? 그렇다. 왜냐면, (6.5)에 의해서 $\hat{F}(\hat{X}_{i+1})$는 $\hat{F}(\hat{X}_i)$ 이거나 $\hat{F}(\hat{X}_i \bigtriangledown \hat{F}(\hat{X}_i))$ 이다. 조건 (6.6)으로 $\hat{X}_i \sqsubseteq \hat{X}_i \bigtriangledown \hat{F}(\hat{X}_i)$(6.6) 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.

(6.5)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 $\hat{X}_{i+1} = \hat{X}_i \bigtriangledown \hat{F}(\hat{X}_i)$이므로, 이때도, $\hat{F}$는 단조(*monotonic*) 함수이고 조건 (6.6)에 의해 $\hat{F}(\hat{X}_i) \sqsubseteq \hat{X}_i \bigtriangledown \hat{F}(\hat{X}_i) = \hat{X}_{i+1}$, 따라서 $\hat{F}^{i+1}(\hat{\bot}) \sqsubseteq \hat{X}_{i+1}$이다. □

Theorem 6 $\hat{D}$*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 (6.9) 과 (6.10)을 만족하고,* $\hat{F}(\hat{\mathcal{A}}) \sqsubseteq \hat{\mathcal{A}}$ *이면, (6.8)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.*

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 (6.10)의 조건을 만족하므로 유한하게 된다. $\{\hat{F}(\hat{Y}_i)\}_i$가 감소하는 체인인가? 그렇다, 다음이 사실이라면:

$$\forall i \in \mathbb{N} : \hat{Y}_i \sqsupseteq \hat{F}(\hat{Y}_i). \tag{6.11}$$

왜냐면, $\hat{Y}_i \sqsupseteq \hat{F}(\hat{Y}_i)$ 이라면 조건 (6.9)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 (6.11)은 사실인가? 그렇다. 기초 경우, 정의 (6.8)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 (6.9)에 의해서, $\hat{Y}_i \sqsupseteq \hat{Y}_i \triangle \hat{F}(\hat{Y}_i) \sqsupseteq \hat{F}(\hat{Y}_i)$. 정의 (6.8)에 의해 다시 쓰면, $\hat{Y}_i \sqsupseteq \hat{Y}_{i+1} \sqsupseteq \hat{F}(\hat{Y}_i)$. 여기

에, $\hat{F}$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(6.11) 조건 (6.9)에 의해서 $\hat{Y}_i \mathbin{\hat{\triangle}} \hat{F}(\hat{Y}_i) \sqsupseteq \hat{F}(\hat{Y}_i)$이므로, $\hat{F}^{i+1}(\hat{\bot}) \sqsubseteq \hat{F}(\hat{Y}_i) \sqsubseteq \hat{Y}_i \mathbin{\hat{\triangle}} \hat{F}(\hat{Y}_i) = \hat{Y}_{i+1}$. □