# SNU 4541.664A Program Analysis, Spring 2011

# Final Exam

06/08/2011(수), 11:00-14:00

**Problem 1** **[10 × (1pts, -1pts)]** O/X로 답하라.

1. 분석하고자 하는 프로그램의 소스 언어에 따라서 정적 프로그램 분석이 완벽(sound and complete)할 수 있다.
2. 분석하고자 하는 프로그램의 성질에 따라서 정적 프로그램 분석이 완벽(sound and complete)할 수 있다.
3. 요약 해석(abstract interpretation)에서 요약 공간(abstract domain)이 무한하도록 정의될 수 있다.
4. 타입 시스템에 기초한 프로그램 분석은 주어진 증명규칙으로 프로그램에 대한 어떤 성질을 증명해 내는 것이다.
5. 타입 시스템에 기초한 프로그램 분석은 모두 요약해석 틀 안에서 정의될 수 있다.
6. 다음의 조건을 만족하도록 프로그램 분석을 디자인하면 그 분석은 실제상황을 모두 포섭한다:
   - 주어진 프로그램의 실제 의미는 연속함수 $F : 2^S \to 2^S$의 최소고정점으로 정의한다. ($2^S$의 원소들 사이의 순서는 집합포함순: $x \sqsubseteq y = x \subseteq y$)
   - 주어진 프로그램의 요약된 의미는 단조함수 $\hat{F} : \hat{S} \to \hat{S}$의 최소 고정점으로 정의한다.
   - $2^S$와 $\hat{S}$는 갈로아 연결
     $$2^S \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \hat{S}$$
     되어있다.
7. $A, B$는 집합이고 $2^B$와 $\hat{B}$사이는 갈로아 연결되어 있다. 그러면 다음 두 CPO사이에 갈로아 연결이 가능하다:
   $$2^{A \overset{\text{fin}}{\to} 2^B} \to 2^B \underset{\alpha?}{\overset{\gamma?}{\leftrightarrows}} (A \overset{\text{fin}}{\to} \hat{B}) \to \hat{B}$$
8. $A$는 집합이고 $A^\omega$는 길이가 무한 할 수도 있는 $A$원소들의 리스트들의 집합이다. $2^A$와 $\hat{A}$사이는 갈로아 연결되어 있다. $A$의 각 원소를 유한한 인덱스 집합 $I$의 한 원소로 맺어주는 함수가 존재한다. 이때 다음 두 CPO사이에 갈로아 연결이 가능하다:
   $$2^{A^\omega} \underset{\alpha?}{\overset{\gamma?}{\leftrightarrows}} I \to \hat{A}$$
9. "$\{n \mid n \in \mathbb{Z}, n \bmod 2 = 1\}$"은 모든 홀수들의 집합을 안전(sound)하고 유한하게 요약한 것이다.

10. 타입 시스템의 안전성을 증명할 때 "Preservation Lemma"를 증명하는데, 그 내용은 프로그램 식이 실행될 때 그 식의 타입은 유지된다는 것이다.

**Problem 2 [6pts]** 정수집합은 그 집합의 최소, 최대의 쌍으로 요약가능하다.

$$2^{\mathbb{Z}} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \hat{A} = \{\bot\} \cup \{[a,b] \mid a,b \in \mathbb{Z} \cup \{-\infty,\infty\}, a \leq b\}$$

1. (3pts) $2^{\mathbb{Z}}$와 $\hat{A}$에서 원소들 사이의 순서($\sqsubseteq$)를 정의하라.
2. (3pts) 갈로아 연결 $\alpha$와 $\gamma$를 정의하고 왜 갈로아 연결인지 보이라.

**Problem 3 [14pts]** 위의 요약 공간 $\hat{A}$ 에 대해서

1. (7pts) 다음의 $\triangledown$ 연산자를 축지법(widening)으로 사용할 수 있는가? 가부 이유를 축지법의 조건에 맞추어 논하라.

$$\begin{array}{rcl} \bot \triangledown X & = & X \\ X \triangledown \bot & = & X \\ [a,b] \triangledown [a',b'] & = & [(\min(a,a')\text{<-100 ? } -\infty : \min(a,a')), (\max(b,b')\text{>100 ? } \infty : \max(b,b'))] \end{array}$$

2. (7pts) 다음의 $\triangle$ 연산자를 좁히기(narrowing)로 사용할 수 있는가? 가부 이유를 좁히기의 조건에 맞추어 논하라.

$$\begin{array}{rcl} \bot \triangle X & = & X \\ X \triangle \bot & = & X \\ [a,b] \triangle [a',b'] & = & [(\min(a,a')\text{<-100 ? } a' : a), (\max(b,b')\text{>100 ? } b' : b)] \end{array}$$

**Problem 4 [10pts]** $D$는 CPO, $f : D \to D$는 연속함수, $\hat{D}$는 $D$와 갈로아 연결 $D \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \hat{D}$ 된 요약 공간이다. $\alpha \circ f \sqsubseteq \hat{g} \circ \alpha$ 를 만족하는 $\hat{g} : \hat{D} \to \hat{D}$중에서 제일 작은 것은 $\alpha \circ f \circ \gamma$임을 보여라.

즉, 두가지를 보인다:

1. (5pts) $\alpha \circ f \sqsubseteq (\alpha \circ f \circ \gamma) \circ \alpha$ 이다.
2. (5pts) $\alpha \circ f \sqsubseteq \hat{g} \circ \alpha$인 임의의 $\hat{g}$은 $\alpha \circ f \circ \gamma \sqsubseteq \hat{g}$ 이다.

**Problem 5 [10pts]** 다음의 정수식 프로그래밍 언어를 타겟으로 하는 분석기를 정의하려고 한다.

$$\begin{array}{rcll} e & ::= & n & (n \in \mathbb{Z}) \\ & | & e\,\texttt{+-} & \\ & | & e\,\texttt{mod}\,e & \end{array}$$

$e\,\texttt{mod}\,0$ 는 $e$의 값과 상관없이 임의의 양수가되고, $n$+-는 $n+1$과 $n-1$중에서 임의로 선택된다.

요약공간을 만드는 갈로아 연결

$$2^{\mathbb{Z}} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \{\bot, 0, >0, <0, \geq 0, \leq 0, \top\}$$

을

$$\begin{array}{rrcll} & \alpha\emptyset & = & \bot & \\ \text{else} & \alpha\{0\} & = & 0 & \\ \text{else} & \alpha X & = & >0 & \text{if } \forall x \in X. x > 0 \\ \text{else} & \alpha X & = & \geq 0 & \text{if } \forall x \in X. x \geq 0 \\ \text{else} & \alpha X & = & <0 & \text{if } \forall x \in X. x < 0 \\ \text{else} & \alpha X & = & \leq 0 & \text{if } \forall x \in X. x \leq 0 \\ \text{else} & \alpha X & = & \top & \text{otherwise} \end{array}$$

로 정의했다. 안전한 $\hat{\texttt{+-}}$와 $\hat{\texttt{mod}}$를 가장 정확하게 정의하라.

**Problem 6 [20pts]** 수업시간에 다룬 명령형 언어의 조립식 요약해석 정의를 가지고 프로그램을 분석하는 예를 서술하라.

언어는

$$\begin{array}{rcl} C & \to & \texttt{skip} \mid x \texttt{ := } E \mid C \texttt{ ; } C \\ & \mid & \texttt{if } B\ C\ C \\ & \mid & \texttt{while } B \texttt{ do } C \\ E & \to & n \quad (n \in \mathbb{Z}) \mid x \\ & \mid & E \texttt{ + } E \mid B \quad \text{(boolean expr)} \end{array}$$

모듬 의미공간은

$$\begin{array}{rcl} \mathcal{C}\,C & \in & 2^{Memory} \to 2^{Memory} \\ \mathcal{V}\,E & \in & 2^{Memory} \to 2^{Value} \\ \mathcal{B}\,B & \in & 2^{Memory} \to 2^{Memory} \\ Memory & = & Loc \xrightarrow{\text{fin}} Value \\ Value & = & \mathbb{Z} + \mathbb{B} \\ Loc & = & Var \\ \mathbb{B} & = & \{T, F\} \end{array}$$

원소 표기법은

$$m \in Memory \qquad M \in 2^{Memory}$$

요약 의미공간은

$$\begin{array}{rcl} \hat{\mathcal{C}}\,C & \in & \hat{Memory} \to \hat{Memory} \\ \hat{\mathcal{V}}\,E & \in & \hat{Memory} \to \hat{Value} \\ \hat{\mathcal{B}}\,B & \in & \hat{Memory} \to \hat{Memory} \end{array}$$

갈로아 연결 된 요약공간은

$$2^{Memory} \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \hat{Memory} \qquad 2^{Value} \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \hat{Value}$$

요약된 정수공간은 "interval domain"

$$\hat{\mathbb{Z}} = \{\bot\} \cup \{[a, b] \mid a, b \in \mathbb{Z} \cup \{-\infty, \infty\}, a \leq b\}$$

모듬의미와 요약의미의 조립식정의는

$$\begin{array}{rcl} \mathcal{C}\,\texttt{skip}\,M & = & M \\ \mathcal{C}\,x \texttt{ := } E\,M & = & \{m\{x \mapsto v\} \mid m \in M, v \in \mathcal{V}\,E\,M\} \\ \mathcal{C}\,C_1 \texttt{ ; } C_2\,M & = & \mathcal{C}\,C_2\,(\mathcal{C}\,C_1\,M) \\ \mathcal{C}\,\texttt{if } B\,C_1\,C_2\,M & = & \mathcal{C}\,C_1\,(\mathcal{B}\,B\,M) \cup \mathcal{C}\,C_2\,(\mathcal{B}\,\neg B\,M) \\ \mathcal{C}\,\texttt{while } B \texttt{ do } C\,M & = & \mathcal{B}\,\neg B\,(fix\lambda X.M \cup \mathcal{C}\,C\,(\mathcal{B}\,B\,X)) \\ \mathcal{V}\,n\,M & = & \{n\} \\ \mathcal{V}\,x\,M & = & \{m\,x \mid m \in M\} \\ \mathcal{V}\,E_1 \texttt{ + } E_2\,M & = & \{v_1 + v_2 \mid v_1 \in \mathcal{V}\,E_1\,M, v_2 \in \mathcal{V}\,E_2\,M\} \\ \mathcal{B}\,B\,M & = & \cup\{M' \mid \mathcal{V}\,B\,M' = \{T\}, M' \subseteq M\} \end{array}$$

와

$$
\begin{array}{rcl}
\hat{\mathcal{C}}\ \texttt{skip}\ \hat{m} & = & \hat{m} \\
\hat{\mathcal{C}}\ x\ \texttt{:=}\ E\ \hat{m} & = & \hat{m}\{x \hat{\mapsto} \hat{\mathcal{V}}\ E\ \hat{m})\} \\
\hat{\mathcal{C}}\ C_1\ ;\ C_2\ \hat{m} & = & \hat{\mathcal{C}}\ C_2\ (\hat{\mathcal{C}}\ C_1\ \hat{m}) \\
\hat{\mathcal{C}}\ \texttt{if}\ B\ C_1\ C_2\ \hat{m} & = & \hat{\mathcal{C}}\ C_1\ (\hat{\mathcal{B}}\ B\ \hat{m})\ \sqcup\ \hat{\mathcal{C}}\ C_1\ (\hat{\mathcal{B}}\ \neg B\ \hat{m}) \\
\hat{\mathcal{C}}\ \texttt{while}\ B\ \texttt{do}\ C\ \hat{m} & = & \hat{\mathcal{B}}\ \neg B\ (\mathit{Narrow}(\mathit{Widen}\ (\lambda \hat{x}.\hat{m}\ \sqcup\ \hat{\mathcal{C}}\ C\ (\hat{\mathcal{B}}\ B\ \hat{x}))))) \\
\hat{\mathcal{V}}\ n\ \hat{m} & = & \alpha_2\{n\} \\
\hat{\mathcal{V}}\ x\ \hat{m} & = & \hat{m}\ \hat{at}\ x \\
\hat{\mathcal{V}}\ E_1\ \texttt{+}\ E_2\ m & = & (\hat{\mathcal{V}}\ E_1\ \hat{m})\ \hat{+}\ (\hat{\mathcal{V}}\ E_2\ \hat{m})
\end{array}
$$

다음의 프로그램에 대한 요약의미를 정의하고, 그 값을 계산하는 과정을 보이라. 위의 정의에서 빠진 부분들($\hat{Value}, \hat{Memory}, \hat{at}, \hat{\mapsto}, \hat{+}, \hat{\mathcal{B}}\ B$ 등)을 모두 정의하고 계산과정을 보인다.

```
x := 10;
while x < 20 do x := x + 1
```

**Problem 7 [15pts]** 다음은 실행과정(trace) 요약해석 알고리즘 중 하나이다. 왜 이 알고리즘은 실행과정 요약해석을 올바르게 구현한 것인지를 설득하라.

$T, T' : \Delta \to \hat{State}$;
$W : 2^{\Delta}$; (* worklist *)
**begin**
  $T := T' := \alpha(T_0)$;  $W := \Delta$;
  **repeat**
    $T' := T$;
    $T := \alpha(T_0)\ \sqcup\ ((\wp\sqcup) \circ \hat{\pi})(\bigcup_{i \in W} \hat{next}\ T[i])$;
    $W := \{i \in \Delta \mid T[i] \not\sqsubseteq T'[i]\}$;
  **until**  $W = \{\}$; (* no more increase *)
**return**  $T'$;
**end**

**Problem 8 [15pts]** 수업시간에 다룬 "type-based analysis"예(각 식이 실행중에 호출할 함수들의 집합을 유추하기)에 따라서 아래의 프로그램이 어떻게 분석되는 지, 그 증명나무(proof tree)를 그리라.

$$(\lambda k.(k(\lambda y.1)) + (k(\lambda z.2)))(\lambda x.x10)$$

□ 수고많았습니다. □