

## Theorem Problem

SNU 4541.664A Program Analysis

Spring 2006

Note 15

Prof. Kwangkeun Yi

## 단순 타입 시스템 Simple Type System

타입 추론 규칙

추론 규칙의 안전성 증명

## 대상 프로그램

다음의 언어를 생각하자:

$e \rightarrow n$	정수
$x$	변수
$e + e$	덧셈
$\lambda x.e$	함수
$e e$	적용

식  $e$ 는 실행이 끝나면 정수나 함수를 내놓는다. 따라서, 실행 결과 값은

$$v \rightarrow n \mid \lambda x.e \mid x$$

프로그램 실행은 다음의 기본적인 다시쓰기 과정의 반복:

$$n + n' \rightarrow (n + n') \quad (\lambda x.e) v \rightarrow \{v/x\}e$$

어디를 다시 쓸지는 다음의 실행문맥이 결정:

$$\begin{array}{l} K \rightarrow [] \\ | \quad K + e \mid v + K \\ | \quad K e \mid v K \end{array}$$

프로그램의 실행 규칙은

$$\frac{e \rightarrow e'}{K[e] \rightarrow K[e']}$$

- **에러상태** =  $e$ 가 값도 아닌데 진행( $\rightarrow$ ) 할 수 없으면
- $e$ 가 “문제없이 실행” =  $e$ 가 에러상태가 되지 않음

## 타입 시스템 = 형식 논리

- 논리식 생김새 “ $e : \tau$ ”
- 논리식 의미  $\llbracket e : \tau \rrbracket = \text{true}$   
iff “ $e$  가 문제없이 실행되며, 끝난다면 그 결과는  $\tau$  타입이다”
- 예:
  - $1 + 2 : \iota$
  - $(\lambda x.x) 3 : \iota$
  - $\lambda x.3 : \tau \rightarrow \iota$ , 임의의  $\tau$ .
- 추론규칙(*inference rules*)은 “ $\Gamma \vdash e : \tau$ ” 꼴을 유추 하는 규칙들
- 가정들  $\Gamma$ 
  - 변수들의 타입들에 대한 가정
  - $x + 1 : \iota$ , 가정  $x : \iota$  아래서.
  - $x 2 : \iota$ , 가정  $x : \iota \rightarrow \iota$  아래서.

$\Gamma \vdash e : \tau$ 를 추론하는 규칙

$$\overline{\Gamma \vdash n : \iota} \quad \overline{\Gamma \vdash x : \tau} \quad x : \tau \in \Gamma$$

$$\frac{\Gamma \vdash e_1 : \iota \quad \Gamma \vdash e_2 : \iota}{\Gamma \vdash e_1 + e_2 : \iota}$$

$$\frac{\Gamma \vdash e_1 : \tau' \rightarrow \tau \quad \Gamma \vdash e_2 : \tau'}{\Gamma \vdash e_1 e_2 : \tau}$$

$$\frac{\Gamma + x : \tau \vdash e : \tau'}{\Gamma \vdash \lambda x. e : \tau \rightarrow \tau'}$$

표기법  $\Gamma + x : \tau \stackrel{\text{def}}{=} \{y : \tau' \mid y \neq x, y : \tau' \in \Gamma\} \cup \{x : \tau\}$

계획:  $\emptyset \vdash \text{pgm} : \tau$  이면  $\llbracket \text{pgm} : \tau \rrbracket = \text{true}$

## 추론의 예: 증명 나무

$$\frac{\frac{\frac{\overline{\{x:\iota\} \vdash x:\iota} \quad x:\iota \in \{x:\iota\}}{\{x:\iota\} \vdash x+1:\iota}}{\emptyset \vdash \lambda x.x+1:\iota \rightarrow \iota} \quad \overline{\emptyset \vdash 2:\iota}}{\emptyset \vdash (\lambda x.x+1) 2:\iota}$$

# 계획대로 되었는가? 올바른 추론 규칙인가?

임의의 프로그램  $e$ 에 대해서

$$\vdash e : \tau$$

이면

$$\llbracket e : \tau \rrbracket = \text{true}$$

인가? 즉,

- $e$  가 문제없이 실행되며
- 끝난다면 그 결과는  $\tau$  타입

인가?



# 증명 방법

- Progress Lemma: 값이 나올 때 까지 문제없이 진행한다.  
 $\vdash e : \tau$  이고  $e$ 가 값이 아니면 반드시  $e \rightarrow e'$ .
- Subject Reduction Lemma: 진행은 타입을 보존한다.  
 $\vdash e : \tau$  이고  $e \rightarrow e'$  이면  $\vdash e' : \tau$ .

## 증명 방법 II

- $e \rightarrow error$  를 정의
- Subject Reduction Lemma:  
 $\vdash e : \tau$  이고  $e \rightarrow e'$  이면  $\vdash e' : \tau$ .