## CS 4110

# Programming Languages & Logics

Lecture 19 Proving Type Soundness

#### Syntax

```
expressions e := x | \lambda x : \tau . e | e_1 e_2 | n | e_1 + e_2 | ()
```

values  $v := \lambda x : \tau . e \mid n \mid ()$ 

types  $\tau ::= \text{int} \mid \text{unit} \mid \tau_1 \rightarrow \tau_2$ 

#### Syntax

```
expressions e := x | \lambda x : \tau. e | e_1 e_2 | n | e_1 + e_2 | ()
```

values  $v := \lambda x : \tau . e \mid n \mid ()$ 

types  $\tau ::= \text{int} \mid \text{unit} \mid \tau_1 \rightarrow \tau_2$ 

#### **Dynamic Semantics**

$$E ::= [\cdot] | E e | v E | E + e | v + E$$

$$\frac{e \to e'}{E[e] \to E[e']} \qquad \frac{n = n_1 + n_2}{(\lambda x : \tau. e) \ v \to e\{v/x\}} \qquad \frac{n = n_1 + n_2}{n_1 + n_2 \to n}$$

**Static Semantics** 

#### **Static Semantics**

 $\frac{}{\Gamma \vdash n : \mathbf{int}} \mathsf{T-INT}$ 

#### **Static Semantics**

 $\frac{}{\Gamma \vdash n : \mathbf{int}}$  T-INT  $\frac{}{\Gamma \vdash () : \mathbf{unit}}$  T-UNIT

#### **Static Semantics**

$$\frac{\Gamma \vdash n \colon \mathbf{int}}{\Gamma \vdash n \colon \mathbf{int}} \xrightarrow{\mathsf{T-INT}} \frac{\Gamma \vdash () \colon \mathbf{unit}}{\Gamma \vdash e_1 \colon \mathbf{int}} \xrightarrow{\mathsf{T-ADD}} \frac{\Gamma \vdash e_1 \colon \mathbf{int}}{\Gamma \vdash e_1 + e_2 \colon \mathbf{int}} \xrightarrow{\mathsf{T-ADD}}$$

#### **Static Semantics**

$$\frac{\Gamma \vdash n : \mathbf{int}}{\Gamma \vdash n : \mathbf{int}} \xrightarrow{\mathsf{T-INT}} \frac{\Gamma \vdash () : \mathbf{unit}}{\Gamma \vdash () : \mathbf{unit}} \xrightarrow{\mathsf{T-UNIT}} \frac{\Gamma \vdash e_1 : \mathbf{int}}{\Gamma \vdash e_1 + e_2 : \mathbf{int}} \xrightarrow{\mathsf{T-ADD}} \frac{\Gamma(x) = \tau}{\Gamma \vdash x : \tau} \xrightarrow{\mathsf{T-VAR}} \mathsf{T-VAR}$$

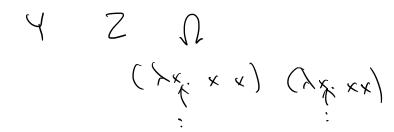
#### **Static Semantics**

#### **Static Semantics**

## **Properties**

### Theorem (Type soundness)

If  $\vdash$  e: $\tau$  and e  $\rightarrow^*$  e' and e'  $\not\rightarrow$  then e' is a value and  $\vdash$  e': $\tau$ .



## **Properties**

### Theorem (Type soundness)

If  $\vdash$  e: $\tau$  and e  $\rightarrow$ \* e' and e'  $\nrightarrow$  then e' is a value and  $\vdash$  e': $\tau$ .

### Lemma (Preservation)

If  $\vdash e : \tau$  and  $e \rightarrow e'$  then  $\vdash e' : \tau$ .

## **Properties**

### Theorem (Type soundness)

If  $\vdash$  e: $\tau$  and e  $\rightarrow^*$  e' and e'  $\not\rightarrow$  then e' is a value and  $\vdash$  e': $\tau$ .

### Lemma (Preservation)

*If*  $\vdash$  *e* :  $\tau$  *and e*  $\rightarrow$  *e' then*  $\vdash$  *e'* :  $\tau$ .

### Lemma (Progress)

If  $\vdash$  e: $\tau$  then either e is a value or there exists an e' such that e  $\rightarrow$  e'.

### Extra Lemmas for Preservation

#### Lemma (Substitution)

If  $x : \tau' \vdash e : \tau$  and  $\vdash v : \tau'$  then  $\vdash e\{v/x\} : \tau$ .

#### Lemma (Context)

If  $\vdash$  E[e]:  $\tau$  and  $\vdash$  e:  $\tau'$  and  $\vdash$  e':  $\tau'$  then  $\vdash$  E[e']:  $\tau$ .

## Extra Lemma for Progress

### Lemma (Canonical Forms)

*If*  $\vdash$  v: $\tau$ , then

- **1**. If  $\tau$  is **int**, then v is a constant, i.e., some c.
- 2. If  $\tau$  is  $\tau_1 \to \tau_2$ , then v is an abstraction, i.e.,  $\lambda x : \tau_1$ . e for some x and e.