Lecture 3

8/30

Last time: Type system to reject programs like
|"Hello" ^ "World"|

Type safety: "Well-typed programs can't go wrong"
-Robin Milner

2 components:

Progress: If e is well-typed, it's a value or can take a step.

Preservation: If a well-typed exp. takes a step, still well-typed w/ the same type.

$$\overset{:\tau}{e_1} \mapsto \overset{:\tau}{e_2} \mapsto \overset{:\tau}{e_3} \mapsto \dots \mapsto v$$

Preservation: If $e:\tau$ and $e \mapsto e'$ then $e':\tau$

Pf: By induction on the derivation of $e \mapsto e'$

S-1 By inversion on T-3, $\tau = int$.
By T-1, $\overline{n_1+n_2}$: int.

S-2 By inversion on T-4, $\tau = string$. By T-2, "$s_1 s_2$":string.

S-3 By inversion on T-5, $\tau = int$. By T-1, $\overline{|s|}$: int.

S-4 By inversion on T-3, $\tau = int$, $e_1:int$, $e_2:int$
By IH, $e_1':int$.
By T-3, $e_1'+e_2:int$.

S-5. By inversion on T-3, $\tau = int$, $e_2:int$. $\overline{n_1}:int$
By IH, $e_2':int$.
By T-3, $\overline{n_1}+e_2':int$.

S-6, S-7, S-8 similar to above. □

Lemma: Canonical Forms

1. If e val and $e : \text{int}$, then $e = \overline{n}$ for some n.
2. If e val and $e : \text{string}$, then $e = \text{"}s\text{"}$ for some s.

Pf: The only rules that can derive e val are V-1 and V-2.

If V-1, then $e = \overline{n}$ and $e : \text{int}$.

If V-2, then $e = \text{"}s\text{"}$ and $e : \text{string}$. □

Progress: If $e : \tau$, then e val or there exists e' s.t. $e \mapsto e'$.

Pf: By induction on the derivation of $e : \tau$.

T-1 $\overline{n}$ val by V-1

T-2 "s" val by V-2

T-3 Then $\tau = \text{int}$, $e = e_1 + e_2$, $e_1 : \text{int}$, and $e_2 : \text{int}$.

By IH, e_1 val or $e_1 \mapsto e_1'$.

- e_1 val. By CF, $e_1 = \overline{n_1}$ for some n_1.
  By IH, e_2 val or $e_2 \mapsto e_2'$.
  - e_2 val. By CF, $e_2 = \overline{n_2}$ for some n_2.
    By S-1, $\overline{n_1} + \overline{n_2} \mapsto \overline{n_1 + n_2}$.
  - $e_2 \mapsto e_2'$. By S-5, $\overline{n_1} + e_2 \mapsto \overline{n_1} + e_2'$.
- $e_1 \mapsto e_1'$. By S-4, $e_1 + e_2 \mapsto e_1' + e_2$.

T-4, T-5 similar to above. □