Consider a simple language with unit and sum types.

**Statics**

- \( \Gamma \vdash () : \text{unit} \) (unit-1)
- \( \Gamma \vdash \text{inl}[\tau_1;\tau_2](e) : \tau_1 + \tau_2 \) (+-I1)
- \( \Gamma \vdash \text{inr}[\tau_1;\tau_2](e) : \tau_1 + \tau_2 \) (+-I2)
- \( \Gamma \vdash e : \tau_1 + \tau_2 \)
- \( \Gamma, x_1 : \tau_1 \vdash e_1 : \tau \)
- \( \Gamma, x_2 : \tau_2 \vdash e_2 : \tau \)
- \( \Gamma \vdash \text{case}(e; x_1.e_1; x_2.e_2) : \tau \) (+-E)

**Dynamics**

- \( e \text{val} \)
  - \( \text{inl}[\tau_1;\tau_2](e) \text{val} \) (inl1)
- \( e \mapsto e' \)
  - \( \text{inl}[\tau_1;\tau_2](e) \mapsto \text{inl}[\tau_1;\tau_2](e') \) (inl2)
- \( e \text{val} \)
  - \( \text{inr}[\tau_1;\tau_2](e) \text{val} \) (inr1)
- \( e \mapsto e' \)
  - \( \text{inr}[\tau_1;\tau_2](e) \mapsto \text{inr}[\tau_1;\tau_2](e') \) (inr2)
  - \( \text{case}(\text{inl}[\tau_1;\tau_2](e); x_1.e_1; x_2.e_2) \mapsto [e/x_1]e_1 \) (case1)
  - \( \text{case}(\text{inr}[\tau_1;\tau_2](e); x_1.e_1; x_2.e_2) \mapsto [e/x_2]e_2 \) (case2)
- \( e \mapsto e' \)
  - \( \text{case}(e; x_1.e_1; x_2.e_2) \mapsto \text{case}(e'; x_1.e_1; x_2.e_2) \) (case3)

**Find the bug!** Here are some incorrect proofs about this language. Can you find the problems?

**Broken Preservation Proof**

**Theorem 1** (Substitution). If \( \Gamma \vdash e : \tau \) and \( \Gamma, x : \tau \vdash e' : \rho \), then \( \Gamma \vdash [e/x]e' : \rho \).

**Theorem 2** (Preservation). If \( \emptyset \vdash e : \tau \) and \( e \mapsto e' \) then \( \emptyset \vdash e' : \tau \).

**Proof.** We proceed by rule induction on the dynamics of the language, letting \( P(e_1 \mapsto e_2) = \text{“for all } \tau, \text{if } \emptyset \vdash e_1 : \tau \text{ then } \emptyset \vdash e_2 : \tau.\text{”} \)

... 

**Case (case1):** We must show that for all \( e, e \text{ val} \) implies \( P(\text{case}(\text{inl}[\tau_1;\tau_2](e); x_1.e_1; x_2.e_2) \mapsto [e/x_1]e_1) \).

1) \( e \text{ val} \) by induction principle
2) \( \emptyset \vdash \text{inl}[\tau_1;\tau_2](e) : \tau_1 + \tau_2 \) by induction principle
3) \( \emptyset, x_1 : \tau_1 \vdash e_1 : \tau \) by induction principle
**To show:** \( \emptyset \vdash [e/x_1]e_1 : \tau \)
4) \( \emptyset \vdash e : \tau_1 \) by inversion on (2)
5) \( \emptyset \vdash [e/x_1]e_1 : \tau \) by Substitution on (4) and (3)

...
Fixed Preservation Proof

**Theorem 3** (Substitution). If \( \Gamma \vdash e : \tau \) and \( \Gamma, x : \tau \vdash e' : \rho \), then \( \Gamma \vdash [e/x]e' : \rho \).

**Theorem 4** (Preservation). If \( \emptyset \vdash e : \tau \) and \( e \mapsto \rightarrow e' \) then \( \emptyset \vdash e' : \tau \).

**Proof.** We proceed by rule induction on the dynamics of the language, letting \( P(e_1 \mapsto e_2) = "\text{for all } \tau, \text{if } \emptyset \vdash e_1 : \tau \text{ then } \emptyset \vdash e_2 : \tau." \)

\[ \text{...} \]

Case (case\(_1\)): We must show that for all \( e, e \text{ val} \) implies \( P(\text{case}(\text{inl}[\tau_1; \tau_2]((()e); x_1.e_1; x_2.e_2) \mapsto [e/x_1]e_1). \)

1) \( e \text{ val} \) by induction principle

To show: For all \( \tau \), if \( \emptyset \vdash \text{case}(\text{inl}[\tau_1; \tau_2]((()e); x_1.e_1; x_2.e_2) : \tau \) then \( \emptyset \vdash [e/x_1]e_1 : \tau \)

Let \( \tau \) be fixed and arbitrary

2) \( \emptyset \vdash \text{case}(\text{inl}[\tau_1; \tau_2]((()e); x_1.e_1; x_2.e_2) : \tau \) by assumption

To show: \( \emptyset \vdash [e/x_1]e_1 : \tau \)

There exist \( \tau_1 \) and \( \tau_2 \) such that \( \ldots \)

3) \( \emptyset \vdash \text{inl}[\tau_1; \tau_2]((()e); x_1.e_1; x_2.e_2) : \tau \)

4) \( \emptyset, x_1 : \tau_1 \vdash e_1 : \tau \)

5) \( \emptyset, x_2 : \tau_2 \vdash e_2 : \tau \)

6) \( \emptyset \vdash e : \tau_1 \)

7) \( \emptyset \vdash [e/x_1]e_1 : \tau \)

by Substitution on (6) and (3)

\[ \text{...} \]

Broken Unicity of Typing Proof

**Theorem 5** (Unicity of Typing). If \( \Gamma \vdash e : \tau \) then \( \tau \) is unique.

**Proof.** We proceed by rule induction on the derivation of \( \Gamma \vdash e : \tau \).

Case (unit-I):

1) \( \tau = \text{unit} \) by induction principle

2) \( e = () \) by induction principle

3) \( \tau \) is unique because this rule always gives \( \tau = \text{unit} \).

Case (+-I\(_1\)):

1) \( \tau = \tau_1 + \tau_2 \) by induction principle

2) \( e = \text{inl}(e') \) by induction principle

3) \( \tau \) is unique because this rule always gives \( \tau = \tau_1 + \tau_2 \)

Case (+-I\(_2\)):

1) \( \tau = \tau_1 + \tau_2 \) by induction principle

2) \( e = \text{inr}(e') \) by induction principle

3) \( \tau \) is unique because this rule always gives \( \tau = \tau_1 + \tau_2 \)

Case (+-E):

\[ \text{...} \]
Fixed Unicity of Typing Proof  See homework solutions.

Broken Canonical Forms Proof

Theorem 6 (Canonical Forms). If $e \text{ val}$ and $\emptyset \vdash e : \tau$ then

1. If $\tau = \text{unit}$ then $e = \langle \rangle$.

2. If $\tau = \tau_1 + \tau_2$ for some types $\tau_1$ and $\tau_2$ then either $e = \text{inl}[\tau_1; \tau_2](e')$ or $e = \text{inr}[\tau_1; \tau_2](e')$ for some term $e'$.

Proof. We proceed by rule induction on the derivation of $\emptyset \vdash e : \tau$.

Case (unit-I):

1) $\tau = \text{unit}$ by induction principle
To show: $e = \langle \rangle$ since we are in case 1 of the theorem by (1)
2) $e = \langle \rangle$ by induction principle

Case (+-I_1):

1) $\tau = \tau_1 + \tau_2$ by induction principle
To show: $e = \text{inl}[\tau_1; \tau_2](e')$ since we are in case 2 of the theorem by (1)
2) $e = \text{inl}[\tau_1; \tau_2](e')$ by induction principle

Case (+-I_2):

1) $\tau = \tau_1 + \tau_2$ by induction principle
To show: $e = \text{inr}[\tau_1; \tau_2](e')$ since we are in case 2 of the theorem by (1)
2) $e = \text{inr}[\tau_1; \tau_2](e')$ by induction principle

Case (+-E): We have that $e = \text{case}(e; x_1.e_1; x_2.e_2)$ by the induction principle. Is suffices to show that $\text{case}(e; x_1.e_1; x_2.e_2) \text{ val}$ isn’t derivable, as this would give us a contradiction by (1) and $e \text{ val}$.

Proof by inner rule induction on derivation of $e \text{ val}$:

...  

Fixed Canonical Forms Proof  See homework solutions.