Harvard School of Engineering and Applied Sciences — CS 152: Programming Languages

Simply-typed lambda calculus (Lecture 11)
Section and Practice Problems

Week 6: Tue Feb 28–Fri Mar 3, 2023

---

1 Simply-typed lambda calculus

(a) Add appropriate type annotations to the following expressions, and state the type of the expression.

(i) $\lambda a.\, a + 4$

Answer: *With minimal annotations:*

$$\lambda a : \textbf{\textit{int}}.\, a + 4$$

and the expression has type $\textbf{\textit{int}} \to \textbf{\textit{int}}$.

(ii) $\lambda f.\, 3 + f\ ()$

Answer: *With minimal annotations:*

$$\lambda f : \textbf{\textit{unit}} \to \textbf{\textit{int}}.\, 3 + f\ ()$$

and the expression has type $(\textbf{\textit{unit}} \to \textbf{\textit{int}}) \to \textbf{\textit{int}}$.

(iii) $(\lambda x.\, x)\ (\lambda f.\, f\ (f\ 42))$

Answer: *With minimal annotations:*

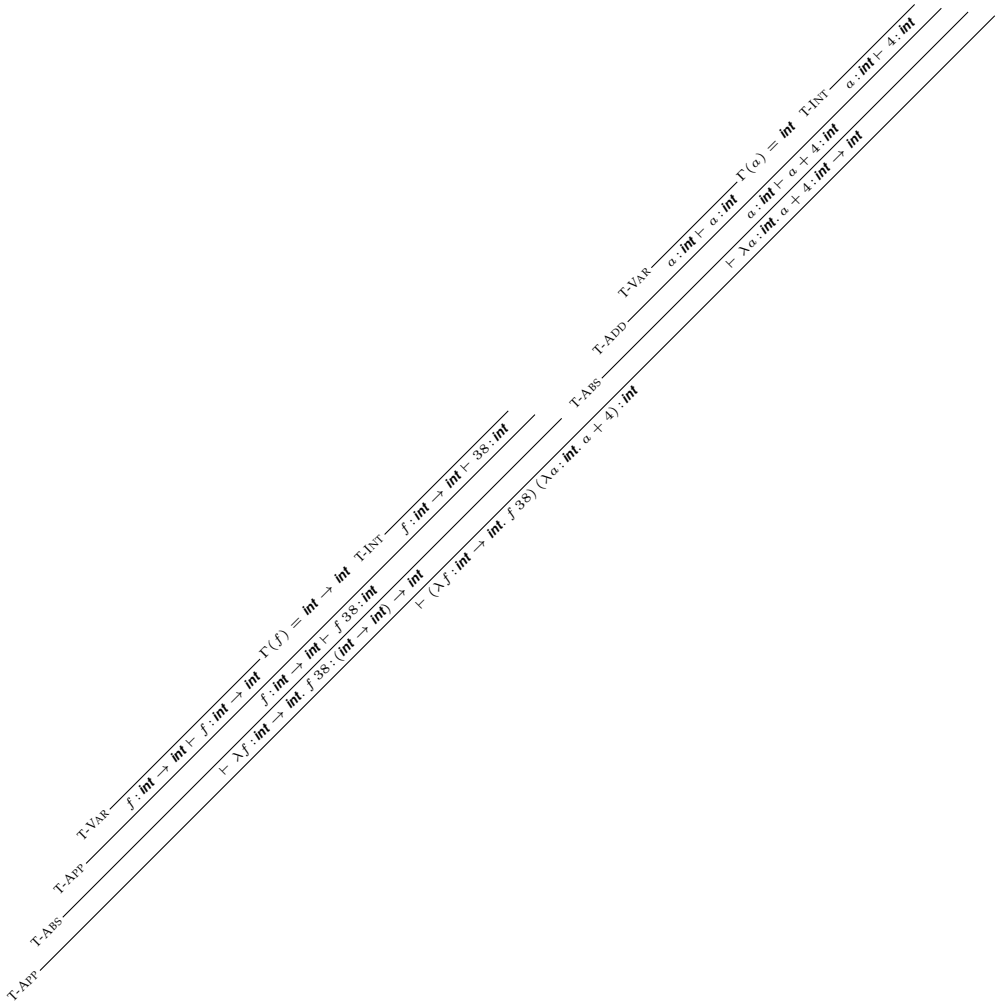
$$(\lambda x : (\textbf{\textit{int}} \to \textbf{\textit{int}}) \to \textbf{\textit{int}}.\, x)\ (\lambda f : \textbf{\textit{int}} \to \textbf{\textit{int}}.\, f\ (f\ 42)).$$

Note that $\lambda x : (\textbf{\textit{int}} \to \textbf{\textit{int}}) \to \textbf{\textit{int}}.\, x$ *has type* $((\textbf{\textit{int}} \to \textbf{\textit{int}}) \to \textbf{\textit{int}}) \to ((\textbf{\textit{int}} \to \textbf{\textit{int}}) \to \textbf{\textit{int}})$.
The expression $\lambda f : \textbf{\textit{int}} \to \textbf{\textit{int}}.\, f\ (f\ 42)$ *has type* $(\textbf{\textit{int}} \to \textbf{\textit{int}}) \to \textbf{\textit{int}}$.
The whole expression has type $(\textbf{\textit{int}} \to \textbf{\textit{int}}) \to \textbf{\textit{int}}$.

(b) For each of the following expressions, give a derivation showing that the expression is well typed.

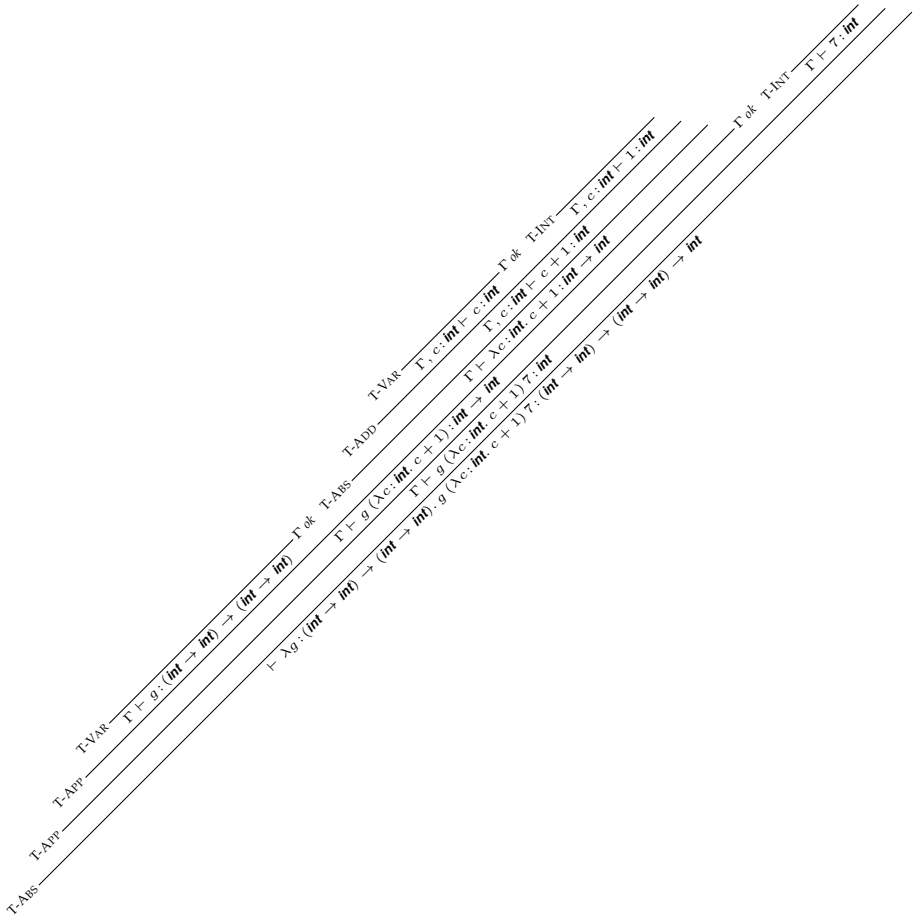
(i) $(\lambda f : \textbf{int} \to \textbf{int}.\, f\ 38)\ (\lambda a : \textbf{int}.\, a + 4)$

Answer:



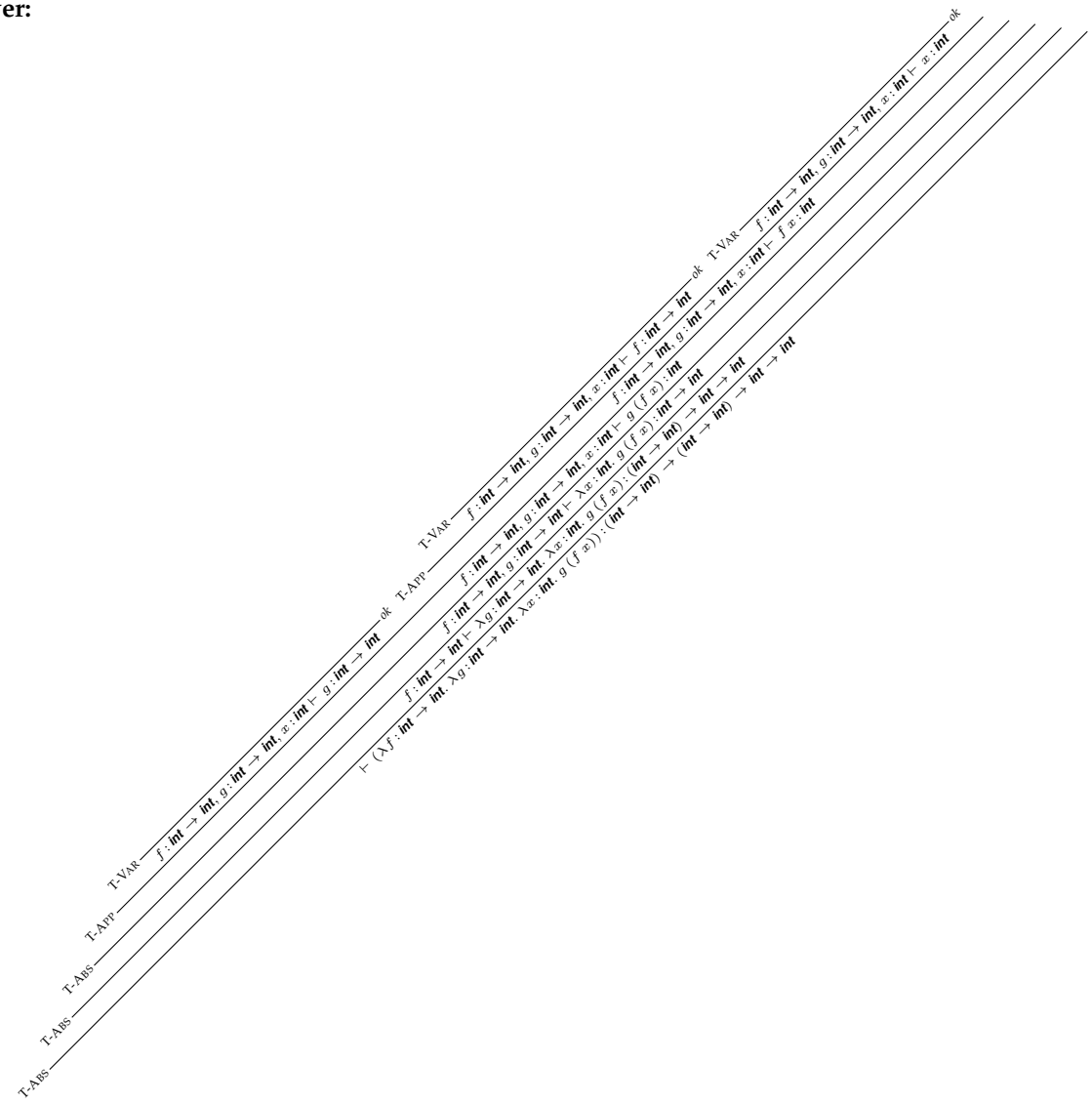
(ii) $\lambda g : (\textsf{int} \to \textsf{int}) \to (\textsf{int} \to \textsf{int}).\ g\ (\lambda c : \textsf{int}.\ c + 1)\ 7$

Answer: *We have* $\Gamma = g : (\textbf{\textit{int}} \to \textbf{\textit{int}}) \to (\textbf{\textit{int}} \to \textbf{\textit{int}})$ *for succinctness.*



(iii) $\lambda f : \textbf{int} \to \textbf{int}.\ \lambda g : \textbf{int} \to \textbf{int}.\ \lambda x : \textbf{int}.\ g\ (f\ x)$

Answer:



2 Type soundness

(a) Recall the substitution lemma that we used in the proof of type soundness.

Lemma (Substitution)**.** *If* $x : \tau' \vdash e : \tau$ *and* $\vdash v : \tau'$ *then* $\vdash e\{v/x\} : \tau$.

Using the definition of substitution given in Assignment 2, prove this lemma. You may assume that v does not have any free variables (i.e., $FV(v) = \emptyset$).

Remember to state what set you are performing induction on and what the property is that you are proving for every element in that set. If you are not sure what cases you need to consider, or what you are able to assume in each case of the inductive proof, we strongly suggest that you write down the inductive reasoning principle for the inductively defined set.

Answer: *We recall the definition of substitution, since we will use it in this proof.*

$$y\{e/x\} = \begin{cases} e & \text{if } x = y \\ y & \text{if } x \neq y \end{cases}$$

$$(e_1\ e_2)\{e/x\} = e_1\{e/x\}\ e_2\{e/x\}$$

$$(\lambda y.\, e')\{e/x\} = \begin{cases} \lambda y.\, e' & \text{if } x = y \\ \lambda y.\, (e'\{e/x\}) & \text{if } x \neq y \text{ and } y \notin FV(e) \\ \lambda z.\, ((e'\{z/y\})\{e/x\}) & \text{if } x \neq y \text{ and } y \in FV(e), \text{ where} \\ & \quad z \notin FV(e) \cup FV(e') \cup \{x\} \end{cases}$$

We extend substitution for the new syntactic forms in our language.

$$n\{e/x\} = n$$
$$()\{e/x\} = ()$$
$$e_1 + e_2\{e/x\} = (e_1\{e/x\}) + (e_2\{e/x\})$$

We proceed by structural induction on expressions. That is, we will perform induction on the set of expressions. As an aside, the inductive reasoning principle for the set of expressions for this language is the following:

For any property P,
If

- *$P(n)$ holds*
- *$P(())$ holds*
- *$P(x)$ holds*
- *For all expressions e, if $P(e)$ holds then $P(\lambda x{:}\tau.\, e)$ holds*
- *For all expressions e_1 and e_2, if $P(e_1)$ and $P(e_2)$ holds then $P(e_1\ e_2)$ holds*
- *For all expressions e_1 and e_2, if $P(e_1)$ and $P(e_2)$ holds then $P(e_1 + e_2)$ holds*

then

for all expressions e, $P(e)$ holds.

The property we will prove is actually stronger than the lemma. We will need this stronger property in order to deal with the case for functions. The property is:

$$P(e) = \forall \Gamma, x, \tau, v, \tau'.\ \textit{if } \Gamma[x \mapsto \tau'] \vdash e{:}\tau \textit{ and } \vdash v{:}\tau' \textit{ then } \Gamma \vdash e\{v/x\}{:}\tau$$

We consider the possible cases (which correspond to the 6 bullet points in the inductive reasoning principle above).

- $e = n$
  Assume that $\Gamma[x \mapsto \tau'] \vdash e{:}\tau$ and $\vdash v{:}\tau'$.
  Since $e = n$, we have $e\{v/x\} = e$. Thus, $\Gamma \vdash e\{v/x\}{:}\tau$ holds trivially.
- $e = ()$
  Assume that $\Gamma[x \mapsto \tau'] \vdash e{:}\tau$ and $\vdash v{:}\tau'$.
  Since $e = ()$, we have $e\{v/x\} = e$. Thus, $\Gamma \vdash e\{v/x\}{:}\tau$ holds trivially.
- $e = y$
  Assume that $\Gamma[x \mapsto \tau'] \vdash e{:}\tau$ and $\vdash v{:}\tau'$.
  We consider two subcases, where x and y are the same variable, and where they are different variables.

  - x *and* y *are the same variable.*
    In this case, we have $\tau = \tau'$ *(since* $e = x$ *and* $\Gamma[x \mapsto \tau'] \vdash e : \tau$ *means that, by inversion using rule* T-VAR, $\tau = \tau'$ *). Also, we have* $e\{v/x\} = v$*. From* $\vdash v : \tau'$ *we can derive* $\Gamma \vdash v : \tau'$*, and so* $\Gamma \vdash e\{v/x\} : \tau$ *holds.*
  - x *and* y *are different variables.*
    In this case, we have $e\{v/x\} = e$*. Thus,* $\Gamma \vdash e\{v/x\} : \tau$ *holds trivially.*

- $e = \lambda y : \tau_y . e'$

  Assume that $\Gamma[x \mapsto \tau'] \vdash e : \tau$ *and* $\vdash v : \tau'$*. Also assume that the property holds for* e' *(i.e., the inductive hypothesis).*

  We consider three subcases, corresponding to the three possible cases for substitution of $\lambda y : \tau_y . e'$*.*

  - x *and* y *are the same variable.*
    In this case, we have $e\{v/x\} = e$*. Thus,* $\Gamma \vdash e\{v/x\} : \tau$ *holds trivially.*
  - x *and* y *are different variables and* $y \notin FV(v)$*.*
    In this case, we have $e\{v/x\} = \lambda y : \tau_y . (e'\{v/x\})$*.*
    By inversion on $\Gamma[x \mapsto \tau'] \vdash e : \tau$*, we have* $\Gamma[x \mapsto \tau'][y \mapsto \tau_y] \vdash e' : \tau''$ *for some* τ'' *where* $\tau = \tau_y \to \tau''$*.*
    Since x *and* y *are different variables, note that* $\Gamma[x \mapsto \tau'][y \mapsto \tau_y]$ *is equal to* $\Gamma'[x \mapsto \tau']$ *where* $\Gamma' = \Gamma[y \mapsto \tau_y]$*. Because the inductive hypothesis holds for expression* e'*, and* $\Gamma'[x \mapsto \tau'] \vdash e' : \tau''$*, we have* $\Gamma' \vdash (e'\{v/x\}) : \tau''$*.*
    Using typing rule T-ABS*, we have that* $\Gamma \vdash \lambda y : \tau_y . (e'\{v/x\}) : \tau_y \to \tau''$*. That is, we have* $\Gamma \vdash e\{v/x\} : \tau$*, as required.*
  - x *and* y *are different variables and* $y \in FV(v)$*.*
    This case is actually impossible. Since v *is a value,* v *can not have any free variables.*

- $e = e_1\ e_2$

  Assume that $\Gamma[x \mapsto \tau'] \vdash e : \tau$ *and* $\vdash v : \tau'$*. Also assume that the property holds for* e_1 *and for* e_2 *(i.e., the inductive hypothesis).*

  From $\Gamma[x \mapsto \tau'] \vdash e : \tau$*, by inversion, we have that* $\Gamma[x \mapsto \tau'] \vdash e_1 : \tau'' \to \tau$ *and* $\Gamma[x \mapsto \tau'] \vdash e_2 : \tau''$ *for some type* τ''*. (That is, rule* T-APP *is the only typing rule that has a conclusion that matches* $\Gamma[x \mapsto \tau'] \vdash e : \tau$*, and so it must be the case that the premises of* T-APP *are true.)*

  From the inductive hypothesis, we have that $\Gamma[x \mapsto \tau'] \vdash e_1\{v/x\} : \tau'' \to \tau$ *and* $\Gamma[x \mapsto \tau'] \vdash e_2\{v/x\} : \tau''$*.*

  From the definition of substitution, we have that $e\{v/x\} = (e_1\{v/x\})\ (e_2\{v/x\})$*.*

  Thus, using the typing rule T-APP*, we have that* $\Gamma \vdash e\{v/x\} : \tau$*, as required.*

- $e = e_1 + e_2$

  Assume that $\Gamma[x \mapsto \tau'] \vdash e : \tau$ *and* $\vdash v : \tau'$*. Also assume that the property holds for* e_1 *and for* e_2 *(i.e., the inductive hypothesis).*

  From $\Gamma[x \mapsto \tau'] \vdash e : \tau$*, by inversion, we have that* $\Gamma[x \mapsto \tau'] \vdash e_1 :$ ***int*** *and* $\Gamma[x \mapsto \tau'] \vdash e_2 :$ ***int****, and* $\tau =$ ***int****. (That is, rule* T-ADD *is the only typing rule that has a conclusion that matches* $\Gamma[x \mapsto \tau'] \vdash e : \tau$*, and so it must be the case that the premises of* T-ADD *are true.)*

  From the inductive hypothesis, we have that $\Gamma[x \mapsto \tau'] \vdash e_1\{v/x\} :$ ***int*** *and* $\Gamma[x \mapsto \tau'] \vdash e_2\{v/x\} :$ ***int***.

  From the definition of substitution, we have that $e\{v/x\} = (e_1\{v/x\}) + (e_2\{v/x\})$*.*

  Thus, using the typing rule T-ADD*, we have that* $\Gamma \vdash e\{v/x\} : \tau$*, as required.*

(b) Recall the context lemma that we used in the proof of type soundness.

Lemma (Context). *If* $\vdash E[e_0] : \tau$ *and* $\vdash e_0 : \tau'$ *and* $\vdash e_1 : \tau'$ *then* $\vdash E[e_1] : \tau$.

Prove this lemma.

Remember to state what set you are performing induction on and what the property is that you are proving for every element in that set. If you are not sure what cases you need to consider, or what you are able to assume in each case of the inductive proof, we strongly suggest that you write down the inductive reasoning principle for the inductively defined set.

Answer: *We proceed by structural induction on contexts* E*. That is, we are doing induction on the set of contexts, which is inductively defined by the grammar:*

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

As an aside, the inductive reasoning principle for the set of contexts is the following:

For any property P*,*
If

- $P([\cdot])$ *holds*
- *For all contexts* E*, if* $P(E)$ *holds then* $P(E\ e)$ *holds*
- *For all contexts* E*, if* $P(E)$ *holds then* $P(v\ E)$ *holds*
- *For all contexts* E*, if* $P(E)$ *holds then* $P(E + e)$ *holds*
- *For all contexts* E*, if* $P(E)$ *holds then* $P(v + E)$ *holds*

then

for all contexts E*,* $P(E)$ *holds.*

So, the property we are proving is:

$$P(E) = \forall e_0, e_1, \tau, \tau'.\ \textit{if } \vdash E[e_0] : \tau \textit{ and } \vdash e_0 : \tau' \textit{ and } \vdash e_1 : \tau' \textit{ then } \vdash E[e_1] : \tau$$

We consider the possible cases (which correspond to the 5 bullet points in the inductive reasoning principle above).

- $E = [\cdot]$.

  Assume $\vdash E[e_0] : \tau$ *and* $\vdash e_0 : \tau'$ *and* $\vdash e_1 : \tau'$.

  Since $E[e_0] = e_0$*, we have* $\tau = \tau'$.

  Moreover, since $E[e_1] = e_1$*, from* $\vdash e_1 : \tau'$ *we have* $\vdash E[e_1] : \tau$ *as required.*

- $E = E'\ e$.

  Assume $\vdash E[e_0] : \tau$ *and* $\vdash e_0 : \tau'$ *and* $\vdash e_1 : \tau'$*, and that the property holds for* E'.

  Since $\vdash E'[e_0]\ e : \tau$*, by inversion (i.e., rule* T-App *is the only rule whose conclusion is an application expression), we must have that* $\vdash E'[e_0] : \tau'' \to \tau$ *for some type* τ'' *and* $\vdash e : \tau''$.

  By the inductive hypothesis (i.e., the property holds of E'*), we have that* $E'[e_1]$ *has type* $\tau'' \to \tau$*. Using the typing rule* T-App*, we can conclude that* $\vdash E'[e_1]\ e : \tau$*. That is,* $\vdash E[e_1] : \tau$ *as required.*

- $E = v\ E'$.

  Assume $\vdash E[e_0] : \tau$ *and* $\vdash e_0 : \tau'$ *and* $\vdash e_1 : \tau'$*, and that the property holds for* E'.

  Since $\vdash v\ E'[e_0] : \tau$*, by inversion (i.e., rule* T-App *is the only rule whose conclusion is an application expression), we must have that* $\vdash E'[e_0] : \tau''$ *for some type* τ''*, and* $\vdash v : \tau'' \to \tau$.

  By the inductive hypothesis (i.e., the property holds of E'*), we have that* $E'[e_1]$ *has type* τ''*. Using the typing rule* T-App*, we can conclude that* $\vdash v\ E'[e_1] : \tau$*. That is,* $\vdash E[e_1] : \tau$ *as required.*

- $E = E' + e$.

  Assume $\vdash E[e_0] : \tau$ *and* $\vdash e_0 : \tau'$ *and* $\vdash e_1 : \tau'$, *and that the property holds for* E'.

  Since $\vdash E'[e_0]+e : \tau$, *by inversion (i.e., rule* T-ADD *is the only rule whose conclusion is an addition expression), we must have that* $\vdash E'[e_0] :$ ***int*** *and* $\vdash e :$ ***int***, *and that* $\tau =$ ***int***.

  By the inductive hypothesis (i.e., the property holds of E'*), we have that* $E'[e_1]$ *has type* ***int***. *Using the typing rule* T-ADD, *we can conclude that* $\vdash E'[e_1] + e : \tau$. *That is,* $\vdash E[e_1] : \tau$ *as required.*

- $E = v + E'$.

  Assume $\vdash E[e_0] : \tau$ *and* $\vdash e_0 : \tau'$ *and* $\vdash e_1 : \tau'$, *and that the property holds for* E'.

  Since $\vdash v+E'[e_0] : \tau$, *by inversion (i.e., rule* T-ADD *is the only rule whose conclusion is an addition expression), we must have that* $\vdash E'[e_0] :$ ***int*** *and* $\vdash v :$ ***int***, *and that* $\tau =$ ***int***.

  By the inductive hypothesis (i.e., the property holds of E'*), we have that* $E'[e_1]$ *has type* ***int***. *Using the typing rule* T-ADD, *we can conclude that* $\vdash v + E'[e_1] : \tau$. *That is,* $\vdash E[e_1] : \tau$ *as required.*

Since all these cases go though, using the inductive reasoning principle, we can conclude that the property holds for all contexts. That is exactly the lemma we were trying to prove.