CIS 500

Software Foundations

Fall 2004

27 September

Announcements

- Homework 1 is graded.
  - Pick it up from Cheryl Hickey (Levine 502).
  - We paid careful attention to problems 2 and 4.
  - Solutions to all problems are on the web page.
  - If you have questions or can't read the comments see the TAs during their office hours.
- Homework 2 was due at noon.
- Homework 3 is on the web page.
- Should be already reading TAPL chapter 5.

The Lambda Calculus

The lambda-calculus

- If our previous language of arithmetic expressions was the simplest nontrivial programming language, then the lambda-calculus is the simplest interesting programming language...
  - Turing complete
  - higher order (functions as data)
  - main new feature: variable binding and lexical scope
- The e. coli of programming language research
- The foundation of many real-world programming language designs (including ML, Haskell, Scheme, Lisp, ...)

Intuitions

Suppose we want to describe a function that adds three to any number we pass it. We might write

```
plus3 x   =   succ (succ (succ x))
```

That is, "`plus3 x` is `succ (succ (succ x))`."

Intuitions

Suppose we want to describe a function that adds three to any number we pass it. We might write

```
plus3 x   =   succ (succ (succ x))
```

That is, "`plus3 x` is `succ (succ (succ x))`."

Q: What is `plus3` itself?

Intuitions

Suppose we want to describe a function that adds three to any number we pass it. We might write

```
plus3 x   =   succ (succ (succ x))
```

That is, "`plus3 x` is `succ (succ (succ x))`."

Q: What is `plus3` itself?

A: `plus3` is the function that, given `x`, yields `succ (succ (succ x))`.

Intuitions

Suppose we want to describe a function that adds three to any number we pass it. We might write

```
plus3 x   =   succ (succ (succ x))
```

That is, "`plus3 x` is `succ (succ (succ x))`."

Q: What is `plus3` itself?

A: `plus3` is the function that, given `x`, yields `succ (succ (succ x))`.

```
plus3   =   λx. succ (succ (succ x))
```

This function exists independent of the name `plus3`.

Intuitions

Suppose we want to describe a function that adds three to any number we pass it. We might write

```
plus3 x   =   succ (succ (succ x))
```

That is, "`plus3 x` is `succ (succ (succ x))`."

Q: What is `plus3` itself?

A: `plus3` is the function that, given `x`, yields `succ (succ (succ x))`.

```
plus3   =   λx. succ (succ (succ x))
```

This function exists independent of the name `plus3`.

On this view, `plus3 (succ 0)` is just a convenient shorthand for "the function that, given `x`, yields `succ (succ (succ x))`, applied to `succ 0`."

```
plus3 (succ 0)   =   (λx. succ (succ (succ x))) (succ 0)
```


Essentials

We have introduced two primitive syntactic forms:

- abstraction of a term `t` on some subterm `x`:

  `λx. t`

  "The function that, when applied to a value `v`, yields `t` with `v` in place of `x`."

- application of a function to an argument:

  $\mathtt{t_1}\ \mathtt{t_2}$

  "the function $\mathtt{t_1}$ applied to the argument $\mathtt{t_2}$"

cf. anonymous functions "`fun x` $\rightarrow$ `t`" in OCaml.

Abstractions over Functions

Consider the λ-abstraction

```
g   =   λf. f (f (succ 0))
```

Note that the parameter variable `f` is used in the function position in the body of `g`. Terms like `g` are called higher-order functions.

If we apply `g` to an argument like `plus3`, the "substitution rule" yields a nontrivial computation:

```
g plus3  =   (λf. f (f (succ 0))) (λx. succ (succ (succ x)))
        i.e.  (λx. succ (succ (succ x)))
                ((λx. succ (succ (succ x))) (succ 0))
        i.e.  (λx. succ (succ (succ x)))
                (succ (succ (succ (succ 0))))
        i.e.  succ (succ (succ (succ (succ (succ (succ 0))))))
```


Abstractions Returning Functions

Consider the following variant of `g`:

```
double   =   λf. λy. f (f y)
```

I.e., `double` is the function that, when applied to a function `f`, yields a function that, when applied to an argument `y`, yields `f (f y)`.

Example

```
     double plus3 0
=    (λf. λy. f (f y))
       (λx. succ (succ (succ x)))
       0
i.e. (λy. (λx. succ (succ (succ x)))
             ((λx. succ (succ (succ x))) y))
       0
i.e. (λx. succ (succ (succ x)))
             ((λx. succ (succ (succ x))) 0)
i.e. (λx. succ (succ (succ x)))
             (succ (succ (succ 0)))
i.e. succ (succ (succ (succ (succ (succ 0)))))
```


The Pure Lambda-Calculus

As the preceding examples suggest, once we have λ-abstraction and application, we can throw away all the other language primitives and still have left a rich and powerful programming language.

In this language — the "pure lambda-calculus"— everything is a function.

- Variables always denote functions
- Functions always take other functions as parameters
- The result of a function is always a function

Formalities

Syntax

t ::=		*terms*
	x	*variable*
	λx.t	*abstraction*
	t t	*application*

Terminology:

- terms in the pure λ-calculus are often called λ-terms
- terms of the form λx. t are called λ-abstractions or just abstractions

Syntactic conventions

Since λ-calculus provides only one-argument functions, all multi-argument functions must be written in curried style.

The following conventions make the linear forms of terms easier to read and write:

- Application associates to the left

  E.g., `t u v` means `(t u) v`, not `t (u v)`

- Bodies of λ- abstractions extend as far to the right as possible

  E.g., `λx. λy. x y` means `λx. (λy. x y)`, not `λx. (λy. x) y`

Scope

The λ-abstraction term `λx.t` binds the variable `x`.

The scope of this binding is the body `t`.

Occurrences of `x` inside `t` are said to be bound by the abstraction.

Occurrences of `x` that are not within the scope of an abstraction binding `x` are said to be free.

```
λx. λy. x y z
```


Scope

The λ-abstraction term `λx.t` binds the variable `x`.

The scope of this binding is the body `t`.

Occurrences of `x` inside `t` are said to be bound by the abstraction.

Occurrences of `x` that are not within the scope of an abstraction binding `x` are said to be free.

```
λx. λy. x y z
λx. (λy. z y) y
```


Structural induction

What is the structural induction principle for lambda calculus terms?

Values

$\mathtt{v}$ ::=		*values*
	$\lambda\mathtt{x.t}$	*abstraction value*

Operational Semantics

Computation rule:

$$(\lambda\mathtt{x.t_{12}})\ \mathtt{v_2} \longrightarrow [\mathtt{x} \mapsto \mathtt{v_2}]\mathtt{t_{12}} \qquad \text{(E-AppAbs)}$$

Notation: $[\mathtt{x} \mapsto \mathtt{v_2}]\mathtt{t_{12}}$ is "the term that results from substituting free occurrences of $\mathtt{x}$ in $\mathtt{t_{12}}$ with $\mathtt{v_{12}}$."

Operational Semantics

Computation rule:

$$(\lambda\mathtt{x.t_{12}})\ \mathtt{v_2} \longrightarrow [\mathtt{x} \mapsto \mathtt{v_2}]\mathtt{t_{12}} \qquad \text{(E-AppAbs)}$$

Notation: $[\mathtt{x} \mapsto \mathtt{v_2}]\mathtt{t_{12}}$ is "the term that results from substituting free occurrences of $\mathtt{x}$ in $\mathtt{t_{12}}$ with $\mathtt{v_{12}}$."

Congruence rules:

$$\frac{\mathtt{t_1} \longrightarrow \mathtt{t_1'}}{\mathtt{t_1}\ \mathtt{t_2} \longrightarrow \mathtt{t_1'}\ \mathtt{t_2}} \qquad \text{(E-App1)}$$

$$\frac{\mathtt{t_2} \longrightarrow \mathtt{t_2'}}{\mathtt{v_1}\ \mathtt{t_2} \longrightarrow \mathtt{v_1}\ \mathtt{t_2'}} \qquad \text{(E-App2)}$$

Terminology

A term of the form $(\lambda\mathtt{x.t})\ \mathtt{v}$ — that is, a λ-abstraction applied to a value — is called a redex (short for "reducible expression").

Induction principle

What is the induction principle for the small-step evaluation relation?

Induction principle

What is the induction principle for the small-step evaluation relation?

We can show a property P is true for all derivations of $\mathtt{t} \rightarrow \mathtt{t}'$, when

- P holds for all derivations that use the rule E-AppAbs.
- P holds for all derivations that end with a use of E-App1 assuming that P holds for all subderivations.
- P holds for all derivations that end with a use of E-App2 assuming that P holds for all subderivations.

Alternative evaluation strategies

Strictly speaking, the language we have defined is called the pure, call-by-value lambda-calculus.

The evaluation strategy we have chosen — call by value — reflects standard conventions found in most mainstream languages.

Some other common ones:

- Call by name (cf. Haskell)
- Normal order (leftmost/outermost)
- Full (non-deterministic) beta-reduction

Programming in the Lambda-Calculus

Multiple arguments

Above, we wrote a function `double` that returns a function as an argument.

```
double   =   λf. λy. f (f y)
```

This idiom — a λ-abstraction that does nothing but immediately yield another abstraction — is very common in the λ-calculus.

In general, `λx. λy. t` is a function that, given a value `v` for `x`, yields a function that, given a value `u` for `y`, yields `t` with `v` in place of `x` and `u` in place of `y`.

That is, `λx. λy. t` is a two-argument function.

(This is how two argument functions work in OCaml.)

The "Church Booleans"

```
tru  =  λt. λf. t
fls  =  λt. λf. f
```

$$
\begin{array}{lll}
 & \texttt{tru v w} & \\
= & \underline{\texttt{(λt.λf.t) v}}\ \texttt{w} & \text{by definition} \\
\longrightarrow & \underline{\texttt{(λf. v) w}} & \text{reducing the underlined redex} \\
\longrightarrow & \texttt{v} & \text{reducing the underlined redex}
\end{array}
$$

$$
\begin{array}{lll}
 & \texttt{fls v w} & \\
= & \underline{\texttt{(λt.λf.f) v}}\ \texttt{w} & \text{by definition} \\
\longrightarrow & \underline{\texttt{(λf. f) w}} & \text{reducing the underlined redex} \\
\longrightarrow & \texttt{w} & \text{reducing the underlined redex}
\end{array}
$$

Functions on Booleans

```
not   =   λb. b fls tru
```

That is, `not` is a function that, given a boolean value `v`, returns `fls` if `v` is `tru` and `tru` if `v` is `fls`.

Functions on Booleans

```
and   =   λb. λc. b c fls
```

That is, `and` is a function that, given two boolean values `v` and `w`, returns `w` if `v` is `tru` and `fls` if `v` is `fls`

Thus `and v w` yields `tru` if both `v` and `w` are `tru` and `fls` if either `v` or `w` is `fls`.

Pairs

```
pair = λf.λs.λb. b f s
fst = λp. p tru
snd = λp. p fls
```

That is, `pair v w` is a function that, when applied to a boolean value `b`, applies `b` to `v` and `w`.

By the definition of booleans, this application yields `v` if `b` is `tru` and `w` if `b` is `fls`, so the first and second projection functions `fst` and `snd` can be implemented simply by supplying the appropriate boolean.

Example

	$\texttt{fst (pair v w)}$	
$=$	$\texttt{fst (}\underline{\texttt{(λf. λs. λb. b f s) v w}}\texttt{)}$	by definition
$\longrightarrow$	$\texttt{fst (}\underline{\texttt{(λs. λb. b v s) w}}\texttt{)}$	reducing the underlined redex
$\longrightarrow$	$\texttt{fst (λb. b v w)}$	reducing the underlined redex
$=$	$\underline{\texttt{(λp. p tru) (λb. b v w)}}$	by definition
$\longrightarrow$	$\underline{\texttt{(λb. b v w) tru}}$	reducing the underlined redex
$\longrightarrow$	$\texttt{tru v w}$	reducing the underlined redex
$\longrightarrow^*$	$\texttt{v}$	as before.

Church numerals

Idea: represent the number n by a function that "repeats some action n times."

$$c_0 = \lambda s.\ \lambda z.\ z$$
$$c_1 = \lambda s.\ \lambda z.\ s\ z$$
$$c_2 = \lambda s.\ \lambda z.\ s\ (s\ z)$$
$$c_3 = \lambda s.\ \lambda z.\ s\ (s\ (s\ z))$$

That is, each number n is represented by a term c_n that takes two arguments, `s` and `z` (for "successor" and "zero"), and applies `s`, n times, to `z`.

Functions on Church Numerals

Successor:

Functions on Church Numerals

Successor:

```
scc = λn. λs. λz. s (n s z)
```


Functions on Church Numerals

Successor:

```
scc = λn. λs. λz. s (n s z)
```

Addition:

Functions on Church Numerals

Successor:

```
scc = λn. λs. λz. s (n s z)
```

Addition:

```
plus = λm. λn. λs. λz. m s (n s z)
```


Functions on Church Numerals

Successor:

```
scc = λn. λs. λz. s (n s z)
```

Addition:

```
plus = λm. λn. λs. λz. m s (n s z)
```

Multiplication:

Functions on Church Numerals

Successor:

```
scc = λn. λs. λz. s (n s z)
```

Addition:

```
plus = λm. λn. λs. λz. m s (n s z)
```

Multiplication:

```
times = λm. λn. m (plus n) c₀
```


Functions on Church Numerals

Successor:

```
scc = λn. λs. λz. s (n s z)
```

Addition:

```
plus = λm. λn. λs. λz. m s (n s z)
```

Multiplication:

```
times = λm. λn. m (plus n) c₀
```

Zero test:

Functions on Church Numerals

Successor:

```
scc = λn. λs. λz. s (n s z)
```

Addition:

```
plus = λm. λn. λs. λz. m s (n s z)
```

Multiplication:

```
times = λm. λn. m (plus n) c₀
```

Zero test:

```
iszro = λm. m (λx. fls) tru
```


Functions on Church Numerals

Successor:

```
scc = λn. λs. λz. s (n s z)
```

Addition:

```
plus = λm. λn. λs. λz. m s (n s z)
```

Multiplication:

```
times = λm. λn. m (plus n) c₀
```

Zero test:

```
iszro = λm. m (λx. fls) tru
```

What about predecessor?

Predecessor

```
zz = pair c0 c0

ss = λp. pair (snd p) (scc (snd p))
```


Predecessor

```
zz = pair c0 c0

ss = λp. pair (snd p) (scc (snd p))

prd = λm. fst (m ss zz)
```


Normal forms

Recall:

- A normal form is a term that cannot take an evaluation step.
- A stuck term is a normal form that is not a value.

Are there any stuck terms in the pure λ-calculus?

Prove it.

Normal forms

Recall:

- A normal form is a term that cannot take an evaluation step.
- A stuck term is a normal form that is not a value.

Are there any stuck terms in the pure λ-calculus?

Prove it.

Does every term evaluate to a normal form?

Prove it.

Divergence

```
omega   =   (λx. x x) (λx. x x)
```

Note that `omega` evaluates in one step to itself!

So evaluation of `omega` never reaches a normal form: it diverges.

Divergence

```
omega   =   (λx. x x) (λx. x x)
```

Note that `omega` evaluates in one step to itself!

So evaluation of `omega` never reaches a normal form: it diverges.

Being able to write a divergent computation does not seem very useful in itself.
However, there are variants of `omega` that are very useful...

Recursion in the Lambda Calculus

Iterated Application

Suppose `f` is some λ-abstraction, and consider the following term:

$$Y_f \quad = \quad (\lambda x.\ f\ (x\ x))\ (\lambda x.\ f\ (x\ x))$$

Iterated Application

Suppose `f` is some λ-abstraction, and consider the following term:

$$\texttt{Y}_\texttt{f} \quad = \quad (\lambda\texttt{x. f (x x)) (}\lambda\texttt{x. f (x x))}$$

Now the "pattern of divergence" becomes more interesting:

$$\begin{array}{c}
\texttt{Y}_\texttt{f} \\
= \\
\underline{(\lambda\texttt{x. f (x x)) (}\lambda\texttt{x. f (x x))}} \\
\longrightarrow \\
\texttt{f (}\underline{(\lambda\texttt{x. f (x x)) (}\lambda\texttt{x. f (x x))}}\texttt{)} \\
\longrightarrow \\
\texttt{f (f (}\underline{(\lambda\texttt{x. f (x x)) (}\lambda\texttt{x. f (x x))}}\texttt{))} \\
\longrightarrow \\
\texttt{f (f (f (}\underline{(\lambda\texttt{x. f (x x)) (}\lambda\texttt{x. f (x x))}}\texttt{)))} \\
\longrightarrow \\
\ldots
\end{array}$$

$\texttt{Y}_\texttt{f}$ is still not very useful, since (like `omega`), all it does is diverge.

Is there any way we could "slow it down"?

Delaying Divergence

$$\texttt{poisonpill} \quad = \quad \lambda\texttt{y. omega}$$

Note that `poisonpill` is a value — it it will only diverge when we actually apply it to an argument. This means that we can safely pass it as an argument to other functions, return it as a result from functions, etc.

$$\begin{array}{c}
\underline{(\lambda\texttt{p. fst (pair p fls) tru) poisonpill}} \\
\longrightarrow \\
\texttt{fst (pair poisonpill fls) tru} \\
\longrightarrow^* \\
\underline{\texttt{poisonpill tru}} \\
\longrightarrow \\
\texttt{omega} \\
\longrightarrow \\
\ldots
\end{array}$$

A delayed variant of `omega`

Here is a variant of `omega` in which the delay and divergence are a bit more tightly intertwined:

$$\texttt{omegav} \quad = \quad \lambda\texttt{y. (}\lambda\texttt{x. (}\lambda\texttt{y. x x y)) (}\lambda\texttt{x. (}\lambda\texttt{y. x x y)) y}$$

Note that `omegav` is a normal form. However, if we apply it to any argument `v`, it diverges:

$$\begin{array}{c}
\texttt{omegav v} \\
= \\
\underline{\lambda\texttt{y. (}\lambda\texttt{x. (}\lambda\texttt{y. x x y)) (}\lambda\texttt{x. (}\lambda\texttt{y. x x y)) y) v}} \\
\longrightarrow \\
\underline{(\lambda\texttt{x. (}\lambda\texttt{y. x x y)) (}\lambda\texttt{x. (}\lambda\texttt{y. x x y))}}\texttt{ v} \\
\longrightarrow \\
(\lambda\texttt{y. (}\lambda\texttt{x. (}\lambda\texttt{y. x x y)) (}\lambda\texttt{x. (}\lambda\texttt{y. x x y)) y) v} \\
= \\
\texttt{omegav v}
\end{array}$$

Another delayed variant

Suppose `f` is a function. Define

$$Z_f \;=\; \lambda y.\ (\lambda x.\ f\ (\lambda y.\ x\ x\ y))\ (\lambda x.\ f\ (\lambda y.\ x\ x\ y))\ y$$

This term combines the "added `f`" from Y_f with the "delayed divergence" of `omegav`.

If we now apply Z_f to an argument `v`, something interesting happens:

$$
\begin{array}{c}
Z_f\ v \\
= \\
\underline{(\lambda y.\ (\lambda x.\ f\ (\lambda y.\ x\ x\ y))\ (\lambda x.\ f\ (\lambda y.\ x\ x\ y))\ y)\ v} \\
\longrightarrow \\
\underline{(\lambda x.\ f\ (\lambda y.\ x\ x\ y))\ (\lambda x.\ f\ (\lambda y.\ x\ x\ y))}\ v \\
\longrightarrow \\
f\ (\lambda y.\ (\lambda x.\ f\ (\lambda y.\ x\ x\ y))\ (\lambda x.\ f\ (\lambda y.\ x\ x\ y))\ y)\ v \\
= \\
f\ Z_f\ v
\end{array}
$$

Since Z_f and `v` are both values, the next computation step will be the reduction of $f\ Z_f$ — that is, before we "diverge," `f` gets to do some computation.

Now we are getting somewhere.

Recursion

Let

```
f  =  λfct.
        λn.
          if n=0 then 1
          else n * (fct (pred n))
```

`f` looks just the ordinary factorial function, except that, in place of a recursive call in the last time, it calls the function `fct`, which is passed as a parameter.

N.b.: for brevity, this example uses "real" numbers and booleans, infix syntax, etc. It can easily be translated into the pure lambda-calculus (using Church numerals, etc.).

We can use `Z` to "tie the knot" in the definition of `f` and obtain a real recursive factorial function:

$$
\begin{array}{c}
Z_f\ 3 \\
\longrightarrow^* \\
f\ Z_f\ 3 \\
= \\
(\lambda fct.\ \lambda n.\ \ldots)\ Z_f\ 3 \\
\longrightarrow\ \longrightarrow \\
\text{if } 3{=}0 \text{ then } 1 \text{ else } 3 * (Z_f\ (\text{pred } 3)) \\
\longrightarrow^* \\
3 * (Z_f\ (\text{pred } 3))) \\
\longrightarrow \\
3 * (Z_f\ 2) \\
\longrightarrow^* \\
3 * (f\ Z_f\ 2) \\
\ldots
\end{array}
$$

A Generic Z

If we define

$$\mathtt{Z} \;=\; \lambda\mathtt{f.}\ \mathtt{Z_f}$$

i.e.,

$$\mathtt{Z} \;=\; \lambda\mathtt{f.}\ \lambda\mathtt{y.}\ (\lambda\mathtt{x.}\ \mathtt{f}\ (\lambda\mathtt{y.}\ \mathtt{x\ x\ y}))\ (\lambda\mathtt{x.}\ \mathtt{f}\ (\lambda\mathtt{y.}\ \mathtt{x\ x\ y}))\ \mathtt{y}$$

then we can obtain the behavior of $\mathtt{Z_f}$ for any `f` we like, simply by applying `Z` to `f`.

$$\mathtt{Z\ f} \;\longrightarrow\; \mathtt{Z_f}$$

For example:

```
fact  =  Z ( λfct.
               λn.
                 if n=0 then 1
                 else n * (fct (pred n)) )
```


Technical note:

The term `Z` here is essentially the same as the `fix` discussed the book.

$$\begin{aligned}\mathtt{Z} &= \lambda\mathtt{f.}\ \lambda\mathtt{y.}\ (\lambda\mathtt{x.}\ \mathtt{f}\ (\lambda\mathtt{y.}\ \mathtt{x\ x\ y}))\ (\lambda\mathtt{x.}\ \mathtt{f}\ (\lambda\mathtt{y.}\ \mathtt{x\ x\ y}))\ \mathtt{y}\\ \mathtt{fix} &= \lambda\mathtt{f.}\ (\lambda\mathtt{x.}\ \mathtt{f}\ (\lambda\mathtt{y.}\ \mathtt{x\ x\ y}))\ (\lambda\mathtt{x.}\ \mathtt{f}\ (\lambda\mathtt{y.}\ \mathtt{x\ x\ y}))\end{aligned}$$

`Z` is hopefully slightly easier to understand, since it has the property that $\mathtt{Z\ f\ v} \longrightarrow^{*} \mathtt{f\ (Z\ f)\ v}$, which `fix` does not (quite) share.

Induction in the Lambda Calculus

Two induction principles

Like before, there are two ways to prove properties are true of the untyped lambda calculus.

- Structural induction
- Induction on derivation of $\mathtt{t} \longrightarrow \mathtt{t}'$.

Let's do an example of the latter.

Induction principle

Recall the induction principle for the small-step evaluation relation.

We can show a property P is true for all derivations of $\mathtt{t} \longrightarrow \mathtt{t}'$, when

- P holds for all derivations that use the rule E-AppAbs.
- P holds for all derivations that end with a use of E-App1 assuming that P holds for all subderivations.
- P holds for all derivations that end with a use of E-App2 assuming that P holds for all subderivations.

Free variables, formally

$$\mathbf{FV}(\mathtt{x}) = \{\mathtt{x}\}$$
$$\mathbf{FV}(\lambda\mathtt{x}.\mathtt{t}_1) = \mathbf{FV}(\mathtt{t}_1)/\{\mathtt{x}\}$$
$$\mathbf{FV}(\mathtt{t}_1\ \mathtt{t}_2) = \mathbf{FV}(\mathtt{t}_1) \cup \mathbf{FV}(\mathtt{t}_2)$$

Show that if $\mathtt{t} \longrightarrow \mathtt{t}'$ then $\mathbf{FV}(\mathtt{t}) \supseteq \mathbf{FV}(\mathtt{t}')$.

Induction on derivation

We want to prove, for all derivations of $\mathtt{t} \longrightarrow \mathtt{t}'$, that $\mathbf{FV}(\mathtt{t}) \supseteq \mathbf{FV}(\mathtt{t}')$.

We have three cases.

Induction on derivation

We want to prove, for all derivations of $t \rightarrow t'$, that $FV(t) \supseteq FV(t')$.

We have three cases.

- The derivation of $t \rightarrow t'$ could just be a use of E-AppAbs. In this case, t is $(\lambda x.t')v$ which steps to $[x \mapsto v]t'$.

$$\begin{aligned} FV(t) &= FV(t')/\{x\} \cup FV(v) \\ &\supseteq FV([x \mapsto v]t') \end{aligned}$$

Induction on derivation

We want to prove, for all derivations of $t \rightarrow t'$, that $FV(t) \supseteq FV(t')$.

We have three cases.

- The derivation of $t \rightarrow t'$ could just be a use of E-AppAbs. In this case, t is $(\lambda x.t')v$ which steps to $[x \mapsto v]t'$.

$$\begin{aligned} FV(t) &= FV(t')/\{x\} \cup FV(v) \\ &\supseteq FV([x \mapsto v]t') \end{aligned}$$

- The derivation could end with a use of E-App1. In otherwords, we have a derivation of $t_1 \rightarrow t_1'$ and we use it to show that $t_1\ t_2 \rightarrow t_1'\ t_2$. By induction $FV(t_1) \supseteq FV(t_1')$.

$$\begin{aligned} FV(t_1\ t_2) &= FV(t_1) \cup FV(t_2) \\ &\supseteq FV(t_1') \cup FV(t_2) \\ &= FV(t_1'\ t_2) \end{aligned}$$

- The derivation could end with a use of E-App2. Here, we have a derivation of $t_2 \rightarrow t_2'$ and we use it to show that $t_1\ t_2 \rightarrow t_1\ t_2'$. This case is analogous to the previous case.

- The derivation could end with a use of E-App2. Here, we have a derivation of $t_2 \rightarrow t_2'$ and we use it to show that $t_1\ t_2 \rightarrow t_1\ t_2'$. This case is analogous to the previous case.

- The derivation could end with a use of E-App2. Here, we have a derivation of $\mathtt{t}_2 \longrightarrow \mathtt{t}_2'$ and we use it to show that $\mathtt{t}_1\ \mathtt{t}_2 \longrightarrow \mathtt{t}_1\ \mathtt{t}_2'$. This case is analogous to the previous case.