Principles of Programming Languages IV

Wael Aboelsaadat
wael@cs.toronto.edu
http://www.cs.toronto.edu/~wael/324.html

Today

• Administrative
  – Weekly Survey
  – Assignment 2

• Roadmap
  – Continuations
  – High-order Functions
  – Examples
  – Algebraic Proofs
Scheme: higher order func - map

- A higher order function used to apply another function to every element of a list:

  \[(\text{map } \langle \text{func} \rangle \ \langle \text{arg-list} \rangle)\]
  
  - Arguments: a function and arguments lists
  - \langle \text{func} \rangle must be a function taking as many arguments as there are in \langle \text{arg-list} \rangle and returning a single value
  - The dynamic order in which \langle \text{func} \rangle is applied to the elements of the \langle \text{arg-list} \rangle is unspecified.

- Examples:
  \[\text{=> (map + '}( \ 1 2 3 \) '}( \ 4 5 6 \) )\]
  (5 7 9)
  \[\text{=>(map (lambda (x) (+ 1 x)) '}( \ 1 2 3 \) )\]
  (2 3 4)
  \[\text{=>(map abs '}( -1 2 -3 -4 \) )\]
  (1 2 3 4)

Scheme: higher order func - for-each

- Another high order function (map)

- Syntax:

  \[(\text{for-each }\langle \text{func} \rangle \ \langle \text{list} \rangle)\]
  
  - Guaranteed to apply function \langle \text{func} \rangle to each element of a list.
  - Value returned by for-each is unspecified

- Implementation:

  \[
  \begin{align*}
  \text{(define (for-each proc list)} & \\
  & \quad \text{(cond \ ((null? (cdr list)) (proc (car list))) ; one-element list} \\
  & \quad \text{else (proc (car list)) (for-each proc (cdr list))))}
  \end{align*}
  \]

- Example:
  \[\text{=> (for-each display '}(a b c (d e f))\)\]
  abc(d e f)
**Scheme: higher order func - reduce**

- **A high order function (we have already seen map)**

- **Syntax:**
  
  $$(\text{reduce } \text{func} \text{ initial-list})$$
  
  – Reduce a list of values to a single value by repeatedly applying a binary function to the list of values

- **Implementation:**
  
  $$(\text{define}$$
  
  $$(\text{reduce} \text{func} \text{list id})$$
  
  $$(\text{if} (\text{null? list})$$
  
  $$(\text{id})$$
  
  $$(\text{func} \text{(car list)} \text{ (reduce func (cdr list) id)}))$$
  
- **Example:**
  
  $$\Rightarrow (\text{reduce} + \text{ '(1 2 3 4 5) 0}) \; :15$$
  
  $$\Rightarrow (\text{reduce} \times \text{ '(1 2 4 6 8 10) 1}) \; :3840$$
  
  $$\Rightarrow (\text{reduce} \text{ append \text{ '(1 2 3) (4 5 6) (7 8)) ()} \; ) \; :\text{(1 2 3 4 5 6 7 8)}$$
  
  $$\Rightarrow (\text{reduce} \text{ expt \text{ '(2 2 2) 1}) \; :65536$$

**Scheme: vectors**

- **Another compound structure (lists, paris)**
  
  – Similar to lists, it can hold heterogeneous elements

- **What’s the problem with lists?**
  
  – Access time… Vectors are accessed in constant time.

- **Example:**
  
  $$\Rightarrow (\text{make-vector} \text{ 5 0}) \; ;\text{creates a vector of length 5 initialized to 0}$$
  
  $$\Rightarrow \text{#(0 0 0 0 0)} \; ;\text{prefix notation # to do the same thing}$$
  
  $$\Rightarrow (\text{vector-length (make-vector 150)}) \; ;\text{returns 150}$$
  
  $$\Rightarrow (\text{vector-ref \text{ #(a b c) 2}}) \; ;\text{returns the third element c}$$
  
  $$\Rightarrow (\text{let} ((v \text{ (vector 'a 'b 'c 'd 'e)})$$
  
  $$(\text{vector-set! v 2 'x)}) \; ;\text{#(a b x d e)}$$
  
  $$\Rightarrow (\text{vector-fill! v y}) \; ;\text{replace each element of v with y}$$
  
  $$\Rightarrow (\text{vector->list \text{ #(a b c)}) \; ;\text{return list (a b c)}$$
  
  $$\Rightarrow (\text{list->vector \text{ '(a b c)}) \; ;\text{return vector #(a b c)}$$
  
  $$\Rightarrow (\text{let} ((v \text{ (make-vector 5)}))$$
  
  $$(\text{for-each (lambda (i)$$
  
  $$(\text{vector-set! v i (* i i)}) \text{ '(0 1 2 3 4)) v})$$
What is a continuation?

- The current continuation at any point in the execution of a program is an abstraction of the rest of the program.
- A continuation of the evaluation of an expression E in a surrounding context C represents the entire future of the computation, which waits for the value of E.

E.g.

<table>
<thead>
<tr>
<th>Context C and expression E</th>
<th>Intuitive continuation of E in C</th>
</tr>
</thead>
<tbody>
<tr>
<td>(+ 5 (* 4 3))</td>
<td>The adding of 5 to the value of E</td>
</tr>
<tr>
<td>(cons 1 (cons 2 (cons 3 '())))</td>
<td>The consing of 3, 2 and 1 to the value of E</td>
</tr>
<tr>
<td>(define x 5) (if (= 0 x) 'undefined (remainder (* (+ x 1) (- x 1)) x))</td>
<td>The multiplication of E by x - 1 followed by a division by x</td>
</tr>
</tbody>
</table>

What is a continuation?

- A more precise notation of the continuation of E.

<table>
<thead>
<tr>
<th>Context C and expression E</th>
<th>Continuation of E in C</th>
</tr>
</thead>
<tbody>
<tr>
<td>(+ 5 (* 4 3))</td>
<td>(lambda (e) (+ 5 e))</td>
</tr>
<tr>
<td>(cons 1 (cons 2 (cons 3 '())))</td>
<td>(lambda (e) (cons 1 (cons 2 (cons 3 e))))</td>
</tr>
<tr>
<td>(define x 5) (if (= 0 x) 'undefined (remainder (* (+ x 1) (- x 1)) x))</td>
<td>(lambda (e) (remainder (* e (- x 1)) x)) c</td>
</tr>
</tbody>
</table>


**Scheme: continuations**

- **Scheme** provides a primitive that captures a continuation of an expression \( E \) in a context \( C \)

- **Syntax**

  \[
  \text{call-with-current-continuation}( \text{func} \ (\text{param}) ) \quad \text{call/cc}( \text{func} \ (\text{param}) )
  \]

  - `call/cc` takes a parameter, which is a receiver function of one parameter.
  - `call/cc` captures its own continuation and passes it to the receiver, i.e., `call/cc` applies the receiver to its own continuation.

<table>
<thead>
<tr>
<th>Context C and expression ( E )</th>
<th>Context C and the capturing</th>
</tr>
</thead>
<tbody>
<tr>
<td>(+ 5 (* 4 3))</td>
<td>(+ 5 (call/cc (lambda (e) (* 4 3) )) )</td>
</tr>
<tr>
<td>(cons 1 (cons 2 (cons 3 '())))</td>
<td>(cons 1 (cons 2 (cons 3 (call/cc (lambda (e) ?)))) )</td>
</tr>
<tr>
<td>(define x 5)</td>
<td>(define x 5)</td>
</tr>
<tr>
<td>(if (= 0 x) 'undefined)</td>
<td>(if (= 0 x) 'undefined</td>
</tr>
<tr>
<td>(remainder (+ (+ x 1) (- x 1)) x)</td>
<td>(remainder (+ (call/cc (lambda (e) (+ x 1))) (- x 1)) x)</td>
</tr>
</tbody>
</table>

---

**Scheme: continuations**

- **Syntax**

  \[
  \text{call/cc}( \text{func} \ (\text{param}) )
  \]

  - `call/cc` takes a parameter, which is a receiver function of one parameter.
  - `call/cc` captures its own continuation and passes it to the receiver, i.e., `call/cc` applies the receiver to its own continuation.

<table>
<thead>
<tr>
<th>Context C and expression ( E )</th>
<th>Value of ( C )</th>
<th>Application of call/cc</th>
<th>Value</th>
</tr>
</thead>
</table>
| (+ 5 (call/cc (lambda (e)
  (set! cont-remember e) (* 4 3))))
  (define x 5)
  (if (= 0 x) 'undefined
  (remainder (* (+ x 1) (- x 1)) x)) | 17 | (cont-remember 3) | 8 |
| (cons 1 (cons 2 (cons 3 (call/cc (lambda (e)
  (set! cont-remember e) ?()))))) | (1 2 3) | (cont-remember '(7 8)) | (1 2 3 7 8) |
| (define x 5)
  (if (= 0 x) 'undefined
  (remainder (* (call/cc (lambda (e) (+ x 1))) (- x 1)) x)) | 4 | (cont-remember 3) | 2 |
### Scheme: continuations

- **How to use call/cc to change continuation?**
  Consider (func n) in (+ (func n) 3)
  1. We make (func n) the body of a function
  2. Let us have one argument passed to that function
  3. Let us call this argument “return”
     (lambda (return) (func n))
  4. Use call/cc
     (call/cc (lambda (return) (func n)))
  The above step will bind the current continuation to return and executes (func n)

- **Primary usage:**
  - Exception handling
  - Backtracking

### Scheme: continuations

- **E.g.**
  ```scheme
  => (define aFuture ')
  => (display (+ 2 (call/cc (lambda (cont)
     (set! aFuture cont) 8))))
  10
  => (display aFuture)
  #continuation 1
  => (display aFuture)
  #continuation 1
  => (display (+ 2 (call/cc (lambda (cont)
     (set! aFuture cont) 8))))
  10
  => (display aFuture)
  #continuation 2
  ```

- **E.g.**
  ```scheme
  => (define error ')
  => (call/cc (lambda (cont)
     (set! error cont) (even? 9)))
  ()
  => (display error)
  #continuation 3
  ```
Scheme: continuations

- **E.g.**

  ```scheme
  => (define some-flag #t)
  => (define (my-abortable-proc escape-proc)
      (display " in my-abortable-proc ")
      (if some-flag
          (escape-proc "ABORTED")
          (display " still in my-abortable-proc ")

  " NOT ABORTED ")
  => (my-abortable-proc display)
  in my-abortable-proc ABORTED still in my-abortable-proc NOT ABORTED
  => (define (my-resumable-proc)
      (display " in my-resumable-proc 1 ")
      (display (call-with-current-continuation my-abortable-proc))
      (display " in my-resumable-proc 2 "))
  => (my-resumable-proc)
  in my-resumable-proc 1 in my-abortable-proc ABORTED in my-resumable-proc 2
  => (set! some-flag #f)
  ```

Scheme: sequencing

- **Another control structure (we have already seen cond and if)**

- **Syntax:**

  ```scheme
  (begin exp₀ exp₁ ... expₙ)
  ```

  - expressions are evaluated from left to right
  - The value of the rightmost expression is the value of the entire expression. Other expressions are for side-effects only

- **Example:**

  ```scheme
  => (define x 3)
  => (begin
      (set! x (+ x 1))
      (+ x x) ) ; returns 8
  ```
**Scheme: assoc function**

- **assoc** does lookup in a list

- **Eg:**
  ```scheme
  => (define NAMES '( (Smith Pat Q)
                   (Jones Chris J)
                   (Walker Kelly T)
                   (Thompson Shelly P)))
  => (assoc 'Smith NAMES)
      (Smith Pat Q)
  => (assoc 'Walker NAMES)
      (Walker Kelly T)
  ```

- **assoc** returns the first sublist if more than one sublist with the same key exist.

**Scheme: I/O**

- **Input/output**
  - (read …) : reads and returns an expression
  - (read-char …) : reads and returns a character
  - (peek-char …) : returns next available character w/o updating
  - (char-ready? …) : returns #t if char has been entered
  - (write-char …) : outputs a single character
  - (write OBJECT …) : outputs the object (strings are in quotes, )
  - (display OBJECT… ) : outputs the object in a more readable form
  - (newline) : outputs end-of-line

- **Reading/writing files**
  - (open-input-file)
  - (open-output-file)

- **Example:**
  ```scheme
  > (display "hello world")
  > (define r (read))
  > (display r)
  ```
**Scheme: I/O - cont’d**

- **Reading an input file**

  (define (echo filename)
  (let ((p (open-input-file filename)))
    (let loop ((obj (read p)))
      (if (eof-object? obj) #t
        (begin
          (write obj)
          (newline)
          (loop (read p)))))))

**Scheme: tree example**

- **Constructing a tree:**

  J> (define TREE
  "'(dog
    (bird (aardvark () ()) (cat () ()) )
    (possum (frog () ()) (wolf () ()) )))

- **Simple tree functions: (empty?, root, left-subtree, right-subtree)**

  J> (define empty?
  (lambda (tree)
    (null? tree)))

  J> (define root
  (lambda (tree)
    (if (empty? tree)
      'Error
      (car tree))))

  J> (define left-subtree
  (lambda (tree)
    (if (empty? tree)
      'Error
      (cadr tree))))

  J> (define right-subtree
  (lambda (tree)
    (if (empty? tree)
      'Error
      (caddr tree))))

  ; (car (cdr (cadr tree)))
Scheme: tree example - cont’d

• Tree searching:
  ```scheme
  => (define contains?
      (lambda (tree sym)
        (cond ((empty? tree) #f)
              ((equal? (root tree) sym) #t)
              (else (or (contains? (left-subtree tree))
                        (contains? (right-subtree tree))))))
  ```

• Alternate tree searching:
  ```scheme
  => (define bst-contains?
      (lambda (bstree sym)
        (cond ((empty? tree) #f)
              ((= (root tree) sym) #t)
              ((> (root tree) sym) (bst-contains? (left-subtree tree) sym))
              (else (bst-contains? (right-subtree tree) sym))))
  ```

Scheme: tree example - cont’d

• Tree traversal:
  ```scheme
  => (define pre-order
      (lambda (tree)
        (if (null? tree) '()
            (append (list (car tree))
                    (pre-order (cadr tree))
                    (pre-order (caddr tree))))))
  ```
  (dog bird aardvark cat possum frog wolf)

  ```scheme
  => (define in-order
      (lambda (tree)
        (if (null? tree) '()
            (append (in-order (cadr tree))
                    (list (car tree))
                    (in-order (caddr tree))))))
  ```
  (aardvark cat bird frog possum dog)

  ```scheme
  => (define post-order
      (lambda (tree)
        (if (null? tree) '()
            (append (post-order (cadr tree))
                    (post-order (caddr tree))
                    (list (car tree))))))
  ```
  (aardvark cat bird frog wolf possum dog)
Scheme: tree example - cont’d

- Backtracking:
  - It is an approach to find a target path in a tree, e.g. just a path, all paths, the shortest path

- E.g. find the path that sums to 94
  - 27, 15, 4 (46 \rightarrow \text{then go 1 step up. Visit remaining children else go up})
  - 27, 15, 22 (64 \rightarrow \text{then go 1 step up. Visit remaining children else go up})
  - 27, 33, 32 (92 \rightarrow \text{then go 1 step up. Visit remaining children else go up})
  - 27, 33, 34 (94)

Scheme: quasi object oriented

- Stack implementation:

```scheme
]=> (define (stack)
  (let ((s '()))
    (lambda (op . args)
      (cond
        ((equal? op 'push!)
          (set! s (cons args s)))
        ((equal? op 'pop!)
          (if (null? s) #f
            (let ((top (car s)))
              (set! s (cdr s))
              top))
          (else #f))
        ((equal? op 'empty?)
          (null? s))
        (else #f))))

]=>(define stk (stack))
]=>(stk 'push! 1) ; 1 , s = (1)
]=>(stk 'push! 3) ; 3 , s = (3 1)
]=>(stk 'push! 'x) ; x , s = (x 3 1)
=>(stk 'pop!) ; x , s = (3 1)
=>(stk 'empty?) ; #f, s = (3 1)
=>(stk 'dump) ; #f, s = (3 1)
```
Software Verification

- Software crisis
  - Quality of software?

- Enforce roles/responsibilities
  - QA test the program on many different inputs
  - However, subtle bugs may remain undiscovered, only to appear at random, inconvenient or dangerous moments.

- Implement quality processes (e.g. CMM, ISO…)
  - However, bugs may remain undiscovered

- Use Algebraic proofs
  - Especially useful for safety-critical software (e.g. Air control, …)

Software Verification: proving properties of programs

- Example:

  (define (append X Y)
   (if (null? X) Y
       (cons (car X) (append (cdr X) Y ))))

  (define (length X)
   (if (null? X) 0
       (+ 1 (length (cdr X)))))

  - **Prove the following:**

    Theorem: \( (\text{length} (\text{append} X Y)) = (\text{length} X) + (\text{length} Y) \)
    for all lists \( X \) and \( Y \)
Software Verification: prove outline

- Use mathematical induction on the length of X
  - A two-part method of proving a theorem involving an integral parameter.
    - First the theorem is verified for the smallest admissible value of the integer.
    - Then it is proven that if the theorem is true for any value of the integer, it is true for the next greater value. The final proof contains the two parts.

- First, prove that the theorem is true for lists of length 0 [Basis]

- Then, prove that if the theorem is true for lists of length N, then it is also true for lists of length N+1 [Inductive Step]

- This implies that the theorem is true for lists of any length (i.e. for any list)

Software Verification: structural induction

- Actually, we will use a variation of induction that emphasizes the structure of lists, not their length.

- First, prove that the theorem is true for X = ' () i.e. when X has length 0 [Basis]

- Then, prove that if the theorem is true for X = L, then it is also true for X = (cons E L) [Inductive Step]
  - Note: if L has length N, then (cons E L) has length N + 1
Software Verification: preliminaries

- Before using induction (or any other technique) to prove a complex property of a program, write down the basis properties that can be trivially verified by inspecting the program code.

- The inductive proof should only use these properties of the code.

- The code itself plays no other role in a proof of correctness and can be henceforth ignored.

- Note: If the basic properties are wrong, then the entire proof is wrong. So be sure to get them right!!

Software Verification: basic properties of append

- Code:

\[
\begin{align*}
\text{(define (append X Y)} & \\
& \text{(if (null? X ) Y} \\
& \text{\quad (cons (car X) (append (cdr X) Y )))}
\end{align*}
\]

- Using \( X = ' () \)

\[
\text{(append ' () Y )} = Y
\]  \[1\]

- Using \( X = (\text{cons E L}) \)

\[
\text{(append (cons E L) Y )} = (\text{cons E (append L Y)})
\]  \[2\]

- Note:
  - if \( X = (\text{cons E L}) \), then \( (\text{car X}) = E, (\text{cdr X}) = L \)
Software Verification: basic properties of length

- **Code:**
  ```lisp
  (define (length X)
    (if (null? X) 0
      (+ 1 (length (cdr X)))))
  ```

- **Using** $X = ' ()$
  
  $(\text{length } ' () ) = 0$ \[3\]

- **Using** $X = (\text{cons } E \ L)$
  
  $(\text{length } (\text{cons } E \ L)) = 1 + (\text{length } L)$ \[4\]

- **Note:**
  
  - if $X = (\text{cons } E \ L)$, then $(\text{cdr } X) = L$

Software Verification: summary of basic properties

- $(\text{append } ' () \ Y ) = Y$ \[1\]

- $(\text{append } (\text{cons } E \ L) \ Y ) = (\text{cons } E (\text{append } L \ Y))$ \[2\]

- $(\text{length } ' () ) = 0$ \[3\]

- $(\text{length } (\text{cons } E \ L) ) = 1 + (\text{length } L )$ \[4\]

- **Using these basic properties, we shall prove (by induction) a more complex property:**
  
  **Theorem:** $(\text{length } (\text{append } X Y)) = (\text{length } X) + (\text{length } Y)$
Software Verification: basis proof

• Using induction on the structure of X

• Basis: when X = ' ()

\[
\begin{align*}
\text{(length (append X Y))} \\
= \text{(length (append '() Y))} \\
= \text{(length Y)} & \quad \text{[by 1]} \\
= 0 + \text{(length Y)} \\
= \text{(length '()) + (length Y)} & \quad \text{[by 3]} \\
= \text{(length X) + (length Y)}
\end{align*}
\]

Therefore, the theorem is true when X = ' ()

Software Verification: inductive step

• Suppose that the theorem holds for X = L, i.e. suppose that

\[
\text{(length (append L Y)) = (length L) + (length Y)}
\]

{Inductive hypothesis}

• Now, prove that the theorem holds for X = (cons E L)
Software Verification: proof of inductive step

- If $X = (\text{cons } E \ L)$ then

\[
\begin{align*}
    & (\text{length}\ (\text{append}\ X\ \ Y)) \\
    = & \quad (\text{length}\ \ (\text{append}\ (\text{cons}\ E\ \ L)\ Y)) \\
    = & \quad (\text{length}\ \ (\text{cons}\ E\ (\text{append}\ L\ Y))) \quad \text{[by 2]} \\
    = & \quad 1 + (\text{length}\ (\text{append}\ L\ Y)) \quad \text{[by 4]} \\
    = & \quad 1 + (\text{length}\ L) + (\text{length}\ Y) \quad \text{[by inductive hypothesis]} \\
    = & \quad (\text{length}\ (\text{cons}\ E\ L)) + (\text{length}\ Y) \quad \text{[by 4]} \\
    = & \quad (\text{length}\ X) + (\text{length}\ Y)
\end{align*}
\]

Software Verification: summary of proof of theorem

- For any List, $Y$,
  
  **Basis:** the theorem holds for $X = '()$

  **Inductive Step:** if the theorem holds for $X = L$, then it holds for $X = (\text{cons } E\ L)$

- By the principle of structural induction, the theorem holds for any lists $X$ and $Y$

- **Theorem:**

\[
    \text{length}\ (\text{append}\ X\ \ Y)) = (\text{length}\ X) + (\text{length}\ Y)
\]
Software Verification: proving properties of programs

- Example 2:

```scheme
(define (member A X)
  (cond ((null? X) #f)
        ((equal? A (car X)) #t)
        (else (member A (cdr X)))))
```

- Prove the following:
  
  Theorem: If (member A X) then
  (member A (append X Y))
  for any A, and any lists X and Y.

Software Verification: outline of proof

- As before, we will use structural induction on X

- First, prove that the theorem is true for X=’ () [basis]

- Then, prove that if the theorem is true for X = L, then it is true for X = (cons E L) [inductive step]

- However, this time proof will be more complex, because the program can terminate its recursion in two ways.
Software Verification: basic properties of member

- **Code:**
  
  (define (member A X)
    (cond  ((null? X) #f)
           ((equal? A (car X)) #t)
           (else (member A (cdr X))))
  
  - **Using** X = ' ()
    
    (member A ' ()) = #f  \[5\]
  
  - **Using** X = (cons A L)
    
    (member A (cons A L)) = #t  \[6\]
  
  - **Note:**
    - (car X) = A

Software Verification: basic properties of member – cont’d

- **Code:**
  
  (define (member A X)
    (cond  ((null? X) #f)
           ((equal? A (car X)) #t)
           (else (member A (cdr X))))
  
  - **Using** X = (cons E L) where E != A
    
    (member A (cons E L)) = (member A L)  \[7\]
  
  - **Note:**
    - (car X) = E, (cdr X) = L

19
**Software Verification: summary of basic properties**

- **member Code:**
  - \((\text{member } A \ ' \ ()\) = \#f\) [5]
  - \((\text{member } A \ (\text{cons } A \ L)) = \#t\) [6]
  - \(\text{If } E =\neq A\ \text{then}\)
    \((\text{member } A \ (\text{cons } E \ L)) = (\text{member } A \ L)\) [7]

- **append Code:**
  - \((\text{append } ' \ () \ Y) = Y\) [1]
  - \((\text{append } (\text{cons } E \ L) \ Y) = (\text{cons } E \ (\text{append } L \ Y))\) [2]

**Software Verification: proof of theorem**

- **Theorem:** If \((\text{member } A \ X)\) then \((\text{member } A \ (\text{append } X \ Y))\)

- **Proof:** by induction on \(X\)

- **Basis:** if \(X = ' ()\) then

  \[
  \begin{align*}
  (\text{member } A \ X) \\
  = (\text{member } A \ ' ()) \\
  = \#f \\
  \text{[by 5]}
  \end{align*}
  \]

  *Therefore, the premise of the theorem is false.*

  *Therefore, the theorem is trivially true (for \(X = ' ()\)*
Software Verification: inductive step

• Suppose the theorem is true for $X=L$, i.e.
  
  $\text{if (member A L) then (member A (append L Y))}$
  
  \{ Inductive hypothesis \}

• Now, prove the theorem is true for $X = (\text{cons E L})$

Software Verification: proof of inductive step

• Let $X = (\text{cons E L})$, there are two cases

• Case 1: $E = A$

  \[ \text{Therefore, } X = (\text{cons A L}) \]
  \[ \text{Therefore, } (\text{member A (append X Y))} \]
  \[ = (\text{member A (append (cons A L) Y))} \]
  \[ = (\text{member A (cons A (append L Y)))} \]
  \[ = \#t \] \[\text{[by 2]} \]
  \[ = \#t \] \[\text{[by 6]} \]

  Therefore, the conclusion of the theorem is true
  
  Therefore, the theorem itself is trivially true for $X = (\text{cons A L})$
Software Verification: proof of inductive step – cont’d

- Let $X = (\text{cons } E \ L)$, there are two cases

- Case 2: $X = (\text{cons } E \ L)$ where $E \neq A$

  \[
  \text{if}(\text{member } A \ X) = \#t \ \text{then} \\
  (\text{member } A \ (\text{cons } E \ L)) \\
  = \ ?? \\
  = \ (\text{member } A \ L) \\
  = \ (\text{member } A \ (\text{append } L \ Y)) \quad [\text{by inductive hypothesis}] \\
  = \ (\text{member } A \ (\text{cons } E \ (\text{append } L \ Y))) \quad [\text{by 7}] \\
  = \ (\text{member } A \ (\text{append } (\text{cons } E \ L) \ Y)) \quad [\text{by 2}] \\
  = \ (\text{member } A \ (\text{append } X \ Y))
  \\
  \]

  Therefore, the theorem is true when $X = (\text{cons } E \ L)$ and $E \neq A$

Software Verification: summary of proof of theorem

- For any $A$, and any list $Y$

- Basis
  
  The theorem holds for $X = ' ()$

- Inductive Step:
  
  If the theorem holds for $X = L$, then it holds for $X = (\text{cons } E \ L)$

  Therefore, by the principle of structural induction, the theorem holds for any $A$ and any lists $X$ and $Y$.

- Theorem: If (member $A \ X$) then
  
  (member $A \ (\text{append } X \ Y)$)
Software Verification

- Interested to learn more…
  - CSC465: Formal Methods in Software Design