Some Notes on Structural Induction

Michael Erdmann*

Spring 2019

These notes provide a brief introduction to structural induction for proving properties of SML programs. We assume that the reader is already familiar with SML and the notes on evaluation and natural number induction for pure SML programs.

Structural inductions in SML often arise as inductions over the structure of values defined by \texttt{datatype} declarations. Most \texttt{datatype} declarations give rise to an induction principle which may be used to prove properties of recursive functions with arguments of the given type.

\textbf{Notation Reminder:} We write $e \xrightarrow{k} e'$ (or $e \Rightarrow^k e'$) for a computation of $k$ steps, $e \Rightarrow e'$ (or $e \Rightarrow^* e'$) for a computation of any number of steps (including 0), $e \hookrightarrow v$ for a complete computation of $e$ to a value $v$, and $n = m$ or $e = e'$ for mathematical equality.

We say that two expressions $e$ and $e'$ are \textit{extensionally equivalent}, and write $e \equiv e'$, whenever one of the following is true: (i) evaluation of $e$ produces the same value as does evaluation of $e'$, or (ii) evaluation of $e$ raises the same exception as does evaluation of $e'$, or (iii) evaluation of $e$ and evaluation of $e'$ both loop forever. In other words, evaluation of $e$ appears to behave just as does evaluation of $e'$. We say that an expression \textit{has no value} if its evaluation either raises an exception or loops forever.

Observe: If $e_1 \Rightarrow e$ and $e_2 \Rightarrow e$, then $e_1 \equiv e_2$. In other words, “reduction implies equivalence”. CAUTION: The opposite implication need not hold: two expressions can be equivalent without one reducing to the other. For instance, $(1 + 9) \equiv (2 * 5)$, but neither expression reduces to the other.

In proofs that establish equivalences, we frequently justify an equivalence $e_1 \equiv e_2$ by writing something like \texttt{[step, 2nd clause of f]}. This means that either $e_1 \Rightarrow e_2$ or $e_2 \Rightarrow e_1$, as established by the function clause being cited. (Observe that such a reduction does indeed imply $e_1 \equiv e_2$, by the previous paragraph.)

*Modified from a draft by Frank Pfenning.
1 Proof By Cases

A very simple form of “structural induction” arises if the datatype declaration is not recursive, but provides a finite number of data constructors. For such datatypes we can prove theorems by cases, which may also be viewed as an induction with only base cases. As an example, consider the declaration

```plaintext
datatype PrimColor = Red | Green | Blue
```

We can now prove properties of all primitive colors by distinguishing the cases of Red, Green, and Blue.

Another form for proof by cases arises for the Booleans, since there is a pervasive definition

```plaintext
datatype bool = true | false
```

For example, it is easy to see that

```plaintext
(if e then e' else e') \neq e'
```

since, for instance, evaluation of e might loop forever, whereas e' could reduce to a value. However, if e reduces to a value, then the two expressions are extensionally equivalent, as we now prove:

**Theorem 1** For every expression e (of type bool) such that e \rightarrow v for some v, and for every e',

```plaintext
(if e then e' else e') \equiv e'
```

**Proof:** By cases on the value of e.

```plaintext
if e then e' else e'
\implies if v then e' else e' [by assumption on e]
```

Now either v = true or v = false by cases on the structure of bool. In either case, the expression above reduces to e'.

2 Structural Induction on Lists

Here is one way to define SML lists that contain integers:

```plaintext
datatype list = nil | :: of int * list
infixr ::
```

Caution: The predefined list type int list in SML is defined slightly differently, but in a way that should not concern us today. In this document we will simply speak of the type list defined above, which is equivalent to SML’s type int list.

The declaration infixr :: changes the lexical status of the constructor :: to be a right-associative infix operator. That is, 1::2::3::nil should be read as 1:(2::(3::nil)) which in turn would correspond to ::(1,(::(2,::(3,nil)))) if :: had not been declared infix. SML provides an alternative syntax for lists, as follows:

```plaintext
[] = nil
[e_1, e_2, \ldots, e_n] = e_1 :: (e_2 :: (\ldots (e_n :: nil)))
```
The recursive nature of the declaration of \texttt{list} means that the corresponding induction principle is not just a proof by cases. It reads:

$$\begin{align*}
\text{If:} & \quad 1. \text{ a property holds for the empty list } \texttt{nil} \\
& \quad \quad \quad \quad \text{ and } \\
& \quad 2. \text{ whenever the property holds for a value } l \text{ of type } \texttt{list}, \text{ it also holds for } v :: l \text{ (for any value } v \text{ of type } \texttt{int}), \\
\text{then:} & \quad \text{ the property holds for all values of type } \texttt{list}.
\end{align*}$$

As a very simple example, consider the definition of a function to append two lists:

\begin{verbatim}
(* @ : list * list -> list *)
fun @ (nil, k) = k
  | @ (x::l, k) = x :: @ (l, k)

infixr @
\end{verbatim}

Appending two lists that are values always reduces to a value in SML. While this may seem trivial, it is actually not the case for some other functional languages such as Haskell in which values may be defined recursively.

**Lemma 2** The function \texttt{@} is total. 
In other words, for any values \( l \) and \( k \) of type \texttt{list}, \( l \ @ k \hookrightarrow v \) for some \( v \).

**Proof:** By structural induction on \( l \).

**Base Case:** \( l = \texttt{nil} \).

We need to show that for any list value \( k \), \( \texttt{nil @ k} \hookrightarrow \) for some \( v \).

\[ \texttt{nil @ k} \Rightarrow k \quad \text{[by the first clause of \texttt{@}]} \]

**Induction Step:** \( l = x :: l' \) for some values \( x \) and \( l' \).

Induction hypothesis: Assume \( l' \ @ k \hookrightarrow v' \) for some \( v' \).

We need to show that: \( l \ @ k \hookrightarrow v \) for some \( v \).

Evaluating code, we see that:

\[ (x :: l') @ k \]
\[ \Rightarrow x :: (l' @ k) \quad \text{[by the second clause of \texttt{@}]} \]
\[ \Rightarrow x :: v' \quad \text{[by induction hypothesis on } l'] \]
\[ = v \quad \text{(writing } v \text{ for the value } x :: v') \]

By the structural induction principle for lists, this completes the proof. \( \square \)

One can also prove that \( l \ @ k \) takes \( O(|l|) \) steps, where \( |l| \) is the length of the list \( l \). From this observation one can see that \( (l \ @ k) \ @ m \) takes \( O(2|l| + |k|) \) steps, while \( l \ @ (k \ @ m) \) takes only \( O(|l| + |k|) \) steps. This is the basis for a number of simple efficiency improvements one can make in SML programs. It is formalized in the following lemma.
Lemma 3  For any values $l_1$, $l_2$, and $l_3$ of type list,

$$(l_1 @ l_2) @ l_3 \equiv l_1 @ (l_2 @ l_3)$$

Proof: We reformulate this slightly to simplify the presentation of the proof:

$$(l_1 @ l_2) @ l_3 \equiv l_{12} @ l_3 \equiv l_{123} \quad \text{iff} \quad l_1 @ (l_2 @ l_3) \equiv l_1 @ l_{23} \equiv l_{123}$$

The proof is by structural induction on $l_1$.

Base Case: $l_1 = \text{nil}$.

We need to show that for any pair of list values $l_2$ and $l_3$, $(\text{nil} @ l_2) @ l_3$ is extensionally equivalent to a value $l_{23}$ iff $\text{nil} @ (l_2 @ l_3)$ is extensionally equivalent to the value $l_{23}$. Well,

$$(\text{nil} @ l_2) @ l_3 \equiv l_2 @ l_3 \quad \text{[step, first clause of @]}$$

and

$$\text{nil} @ (l_2 @ l_3) \equiv \text{nil} @ l_{23} \quad \text{[for some value $l_{23}$, by totality of @, i.e., Lemma 2]}$$

Induction Step: $l_1 = x :: l_1'$ for some values $x$ and $l_1'$.

Induction hypothesis: Assume

$$(l_1' @ l_2) @ l_3 \equiv l_{12}' @ l_3 \equiv l_{123}' \quad \text{iff} \quad l_1' @ (l_2 @ l_3) \equiv l_1' @ l_{23} \equiv l_{123}'$$

We need to show that:

$$(l_1 @ l_2) @ l_3 \equiv l_{12} @ l_3 \equiv l_{123} \quad \text{iff} \quad l_1 @ (l_2 @ l_3) \equiv l_1 @ l_{23} \equiv l_{123}$$

Evaluating code, for the left expression we obtain:

$$(x :: l_1') @ l_2 @ l_3 \equiv (x :: (l_1' @ l_2)) @ l_3 \quad \text{[step, second clause of @]}$$

and

$$(x :: (l_1' @ l_2)) @ l_3 \equiv x :: (l_1' @ l_3) \quad \text{[for some value $l_{12}$, by totality of @]}$$

We need to show that:

$$(x :: (l_1' @ l_3)) \equiv x :: (l_1' @ l_{23}) \quad \text{[step, second clause of @]}$$

For the right expression we obtain:

$$(x :: l_1') @ l_2 @ l_3 \equiv (x :: l_1') @ l_{23} \quad \text{[for some value $l_{23}$, by totality of @]}$$

By the structural induction principle for lists, this completes the proof. \(\Box\)
We actually have the stronger and often useful result that $\oplus$ is associative even for expressions which are not necessarily values, assuming sequential code evaluation. This holds even under extensions by arbitrary effects, since in $e_1 \oplus (e_2 \oplus e_3)$ and $(e_1 \oplus e_2) \oplus e_3$, the expressions $e_1$, $e_2$ and $e_3$ are evaluated in the same order, with all $\oplus$ computations in between reducing to values whenever the arguments are values.

**Lemma 4** For arbitrary expressions $e_1$, $e_2$ and $e_3$ of type list,

$$(e_1 \oplus e_2) \oplus e_3 \equiv e_1 \oplus (e_2 \oplus e_3)$$

**Proof:** By straightforward computation and Lemma 3:

$$(e_1 \oplus e_2) \oplus e_3$$

$\Rightarrow$ $(l_1 \oplus e_2) \oplus e_3$ or $e_1$ has no value

$\Rightarrow$ $(l_1 \oplus l_2) \oplus e_3$ or $e_2$ has no value

$\Rightarrow$ $l_{12} \oplus e_3$ [by totality of $\oplus$]

$\Rightarrow$ $l_{12} \oplus l_3$ or $e_3$ has no value

$\Rightarrow$ $l_{123}$ [by totality of $\oplus$]

For the right-hand side we compute:

$$e_1 \oplus (e_2 \oplus e_3)$$

$\Rightarrow$ $l_1 \oplus (e_2 \oplus e_3)$ or $e_1$ has no value

$\Rightarrow$ $l_1 \oplus (l_2 \oplus e_3)$ or $e_2$ has no value

$\Rightarrow$ $l_1 \oplus (l_2 \oplus l_3)$ or $e_3$ has no value

$\Rightarrow$ $l_1 \oplus l_{23}$ [by totality of $\oplus$]

$\Rightarrow$ $l'_{123}$ [by totality of $\oplus$]

$\cong$ $l_{123}$ [by proof of Lemma 3]
3 Structural Induction on Other Types

As an example for structural induction over other types we use binary trees in which the leaves carry integer data:

```plaintext
datatype tree = Leaf of int | Node of tree * tree
```

The structural induction principle for these types of trees then reads:

```
If:
1. a property holds for every leaf \( \text{Leaf}(x) \), with \( x \) a value of type \( \text{int} \),
   and
2. whenever the property holds for values \( t_1 \) and \( t_2 \) of type \( \text{tree} \),
   it also holds for \( \text{Node}(t_1, t_2) \),
then: the property holds for all values of type \( \text{tree} \).
```

The following function is inefficient, since the elements of `flatten t1` may end up being copied many times when the result lists are appended.

```plaintext
(* flatten : tree -> list
  REQUIRES: true
  ENSURES: flatten(t) computes the inorder traversal of the leaf values.
*)
fun flatten (Leaf(x)) = [x]
| flatten (Node(t1,t2)) = flatten t1 @ flatten t2
```

A more efficient alternative introduces an accumulator argument.

```plaintext
(* flatten2 : tree * list -> list
  REQUIRES: true
  ENSURES: flatten2 (t, acc) \( \equiv \) flatten (t) @ acc
*)
fun flatten2 (Leaf(x), acc) = x::acc
| flatten2 (Node(t1,t2), acc) = 
  flatten2 (t1, flatten2 (t2, acc))

(* flatten’ : tree -> list *)
fun flatten’ (t) = flatten2 (t, nil)
```

We would like to prove that `flatten` and `flatten’` define the same function. In order to do that, we need to prove a lemma about `flatten2`, which requires a generalization of the induction hypothesis: We cannot prove directly by induction that `flatten2(t, nil) \( \equiv \) flatten(t)` since recursive calls in `flatten2` have a more general structure. The case of a leaf provides a clue about the proper generalization.

**Lemma 5** For any values \( t \) of type \( \text{tree} \) and \( \text{acc} \) of type \( \text{list} \),

\[ \text{flatten2}(t, \text{acc}) \equiv \text{flatten}(t) \odot \text{acc} \]
**Proof:** By structural induction on $t$.

**Base Case:** $t = \text{Leaf}(x)$, for some value $x : \text{int}$.

We need to show that, for all values $acc$ of type $\text{list}$,
\[
\text{flatten2}(\text{Leaf}(x), \ acc) \equiv \text{flatten}(\text{Leaf}(x)) \ @ \ acc.
\]

Showing:
\[
\begin{align*}
\text{flatten2}(\text{Leaf}(x), \ acc) & \equiv x :: acc \\
& \equiv x :: (\text{nil} \ @ \ acc) \\
& \equiv (x :: \text{nil}) \ @ acc \\
& = [x] \ @ acc \\
& \equiv \text{flatten}(\text{Leaf}(x)) \ @ acc
\end{align*}
\]

**Induction Step:** $t = \text{Node}(t_1, t_2)$ for some values $t_1$ and $t_2$, both of type $\text{tree}$.

Induction hypothesis: Assume that
for any value $acc$ of type $\text{list}$, $\text{flatten2}(t_1, \ acc) \equiv \text{flatten}(t_1) \ @ \ acc$ and
for any value $acc$ of type $\text{list}$, $\text{flatten2}(t_2, \ acc) \equiv \text{flatten}(t_2) \ @ \ acc$.

We need to show that for any value $acc$ of type $\text{list}$,
\[
\text{flatten2}(t, \ acc) \equiv \text{flatten}(t) \ @ acc.
\]

Showing:
\[
\begin{align*}
\text{flatten2}(\text{Node}(t_1, t_2), \ acc) & \equiv \text{flatten2}(t_1, \text{flatten2}(t_2, \ acc)) \\
& \equiv \text{flatten2}(t_1, \text{flatten}(t_2) \ @ acc) \\
& \equiv \text{flatten}(t_1) \ @ (\text{flatten}(t_2) \ @ acc) \\
& \equiv (\text{flatten}(t_1) \ @ \text{flatten}(t_2)) \ @ acc \\
& \equiv \text{flatten}(\text{Node}(t_1, t_2)) \ @ acc
\end{align*}
\]

By the structural induction principle for trees, this completes the proof. $\square$

Comment: We used totality of $\text{flatten}$ in the proof above. Imagine how you might prove that.

The following theorem now follows directly:

**Theorem 6** For any value $t$ of type $\text{tree}$,
\[
\text{flatten}'(t) \equiv \text{flatten}(t).
\]

**Proof:** We compute directly:
\[
\begin{align*}
\text{flatten}'(t) & \equiv \text{flatten2}(t, \text{nil}) \\
& \equiv \text{flatten}(t) \ @ \text{nil} \\
& \equiv \text{flatten}(t)
\end{align*}
\]

Where the last equivalence holds by a property of $\ @$ which is left as an exercise. $\square$

There are also variants of structural induction analogous to strong induction, where we need to apply the induction hypothesis to some subexpression of the given value. We will not go into further details here.