COMP9020

Foundations of Computer Science

Term 3, 2024

Lecture 12: Induction

Outline

Outline

Recursive datatypes

Describe arbitrarily large objects in a finite way

Recursive functions

Define behaviour for these objects in a finite way

Induction

Reason about these objects in a finite way

Example

Recall the recursive program:

Example

Summing the first n natural numbers:

$$\begin{array}{l} \texttt{sum}(n): \\ \quad \texttt{if}(n = 0): 0 \\ \quad \texttt{else}: n + \texttt{sum}(n-1) \end{array}$$

Another attempt:

Example

$$\begin{array}{l} \texttt{sum2}(n): \\ \quad \texttt{return}\; n * (n+1)/2 \end{array}$$

Induction proof **guarantees** that these programs will behave the same.

Inductive Reasoning

Suppose we would like to reach a conclusion of the form

$$P(x) \textit{ for all } x \text{ (of some type)}$$

Inductive reasoning (as understood in philosophy) proceeds from examples.

E.g. From "This swan is white, that swan is white, in fact every swan I have seen so far is white"

Conclude: "Every Swan is white"

Inductive Reasoning

Suppose we would like to reach a conclusion of the form

$$P(x) \textit{ for all } x \text{ (of some type)}$$

Inductive reasoning (as understood in philosophy) proceeds from examples.

E.g. From "This swan is white, that swan is white, in fact every swan I have seen so far is white"

Conclude: "Every Swan is white"

Take Notice

This may be a good way to discover hypotheses.
But it is not a valid principle of reasoning!

Mathematical induction *is a variant that is valid.*

Mathematical Induction

Mathematical Induction is based not just on a set of examples, but also a rule for deriving new cases of $P(x)$ from cases for which P is known to hold.
General structure of reasoning by mathematical induction:

Base Case [B]: $P(a_1), P(a_2), \ldots, P(a_n)$ for some small set of examples $a_1 \ldots a_n$ (often $n = 1$)
Inductive Step [I]: A general rule showing that if $P(x)$ holds for some cases $x = x_1, \ldots, x_k$ then $P(y)$ holds for some new case y, constructed in some way from $x_1, \ldots, x_k$.

Conclusion: Starting with $a_1 \ldots a_n$ and repeatedly applying the construction of y from existing values, we can eventually construct all values in the domain of interest.

Induction proof structure

Let $P(x)$ be the proposition that ...

We will show that $P(x)$ holds for all x by induction on x.

Base case: $x = ...$**:**

- $P(x)$: ...
- ....
- so $P(x)$ holds.

[Repeat for all base cases]

Inductive case: $P(x)$ **implies** $P(y)$

- Assume $P(x)$ holds. That is, ...
- We will show $P(y)$ holds.
- ...
- So $P(x)$ implies $P(y)$.

[Repeat for all inductive cases]

Conclusion

We have shown $P(...)$, and for all x, $P(x)$ implies $P(y)$. Therefore, by induction, $P(x)$ holds for all x.

Outline

Basic induction

Basic induction is the general principle applied to the natural numbers.

Goal: Show $P(n)$ holds for all $n \in \mathbb{N}$.

Approach: Show that:

Base case (B): $P(0)$ holds; and

Inductive case (I): If $P(k)$ holds then $P(k+1)$ holds.

Conclusion (C): $P(n)$ holds for all $n \in \mathbb{N}$.

Example

Recall the recursive program:

Example

Summing the first n natural numbers:

$\texttt{sum}(n)$:
  $\texttt{if}(n = 0)$: 0
  $\texttt{else}$: $n + \texttt{sum}(n-1)$

Another attempt:

Example

$\texttt{sum2}(n)$:
  $\texttt{return}\ n * (n+1)/2$

Induction proof **guarantees** that these programs will behave the same.

Example

Let $P(n)$ be the proposition that: $\sum_{i=0}^{n} i \ = \frac{n(n+1)}{2}$.

We will show that $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Example

Let $P(n)$ be the proposition that: $\sum_{i=0}^{n} i \ = \frac{n(n+1)}{2}$.

We will show that $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

[B] Base case: $n = 0$:

[I] Inductive case: $P(k) \Rightarrow P(k+1)$:

[C] Conclusion:

Example

Let $P(n)$ be the proposition that: $\sum_{i=0}^{n} i \; = \frac{n(n+1)}{2}$.

We will show that $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.
[B] Base case: $n = 0$:

$$\left(\sum_{i=0}^{0} i\right) = 0 \; = \frac{0(0+1)}{2}.$$

So $P(0)$ holds.

[I] Inductive case: $P(k) \Rightarrow P(k+1)$:

[C] Conclusion:

Example

Let $P(n)$ be the proposition that: $\sum_{i=0}^{n} i \ = \frac{n(n+1)}{2}$.

We will show that $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

[B] Base case: $n = 0$:

$$\left(\sum_{i=0}^{0} i\right) = 0 \ = \frac{0(0+1)}{2}.$$

So $P(0)$ holds.

[I] Inductive case: $P(k) \Rightarrow P(k+1)$:

That is,

$$\sum_{i=0}^{k} i \ = \frac{k(k+1)}{2} \ \Rightarrow \ \sum_{i=0}^{k+1} i \ = \frac{(k+1)(k+2)}{2}$$

(proof?)

[C] Conclusion:

Example

Let $P(n)$ be the proposition that: $\sum_{i=0}^{n} i \ = \frac{n(n+1)}{2}$.

We will show that $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.
[B] Base case: $n = 0$:

$$\left(\sum_{i=0}^{0} i \right) = 0 \ = \frac{0(0+1)}{2}.$$

So $P(0)$ holds.

[I] Inductive case: $P(k) \Rightarrow P(k+1)$:
That is,

$$\sum_{i=0}^{k} i \ = \frac{k(k+1)}{2} \ \Rightarrow \ \sum_{i=0}^{k+1} i \ = \frac{(k+1)(k+2)}{2}$$

(proof?)

[C] Conclusion: We have $P(0)$ is true, and $P(k)$ implies $P(k+1)$.
Therefore, by induction, $P(n)$ holds for all $n \in \mathbb{N}$.

Proof of inductive step.

Assume $P(k)$ holds. That is:

$$\left(\sum_{i=0}^{k} i\right) = \frac{k(k+1)}{2} + (k+1). \qquad \text{(IH)}$$

Then:

$$\begin{aligned}
\sum_{i=0}^{k+1} i &= \left(\sum_{i=0}^{k} i\right) + (k+1) \\
&= \frac{k(k+1)}{2} + (k+1) \qquad \text{(by the inductive hypothesis)} \\
&= \frac{k(k+1) + 2(k+1)}{2} \\
&= \frac{(k+1)(k+2)}{2}
\end{aligned}$$

Therefore $P(k)$ implies $P(k+1)$. □

Outline

Variations

There are many variants of basic induction that may be more useful in certain circumstances. For example:

1. Induction from m upwards
2. Induction steps > 1
3. Strong induction
4. Backward induction
5. Forward-backward induction
6. Structural induction

Induction From m Upwards

If

[B] $P(m)$

[I] $\forall k\,(\geq)\,m, P(k) \rightarrow P(k+1)$

then

[C] $\forall n\,(\geq)\,m, P(n)$

Example

Theorem. For all $n \geq 1$, the number $8^n - 2^n$ is divisible by 6.

[B] $8^1 - 2^1$ is divisible by 6
[I] if $8^k - 2^k$ is divisible by 6, then so is $8^{k+1} - 2^{k+1}$, for all $k \geq 1$

Prove [I] using the "trick" to rewrite 8^{k+1} as $8 \cdot (8^k - 2^k + 2^k)$ which allows you to apply the IH on $8^k - 2^k$.

$$
\begin{aligned}
8^{k+1} - 2^{k+1} &= 8 \cdot (8^k - 2^k + 2^k) - 2 \cdot 2^k \\
&= 8 \cdot (8^k - 2^k) + 8 \cdot 2^k - 2 \cdot 2^k \\
&= 8 \cdot (8^k - 2^k) + 6 \cdot 2^k
\end{aligned}
$$

Induction Steps $\ell > 1$

If

[B] $P(m)$

[I] $P(k) \rightarrow P(k + \ell)$ for all $k \geq m$

then

[C] $P(n)$ for every ℓ'th $n \geq m$

Example

The Fibonacci numbers can be defined by the recurrence relation

$$F_1 = 1, F_2 = 1$$

and

$$F_n = F_{n-1} + F_{n-2}, \text{ for } n > 2$$

The first 12 Fibonacci numbers F_n are:

$$1, \quad 1, \quad 2, \quad 3, \quad 5, \quad 8, \quad 13, \quad 21, \quad 34, \quad 55, \quad 89, \quad 144$$

Every 4th Fibonacci number is divisible by 3.

[B] $F_4 = 3$ is divisible by 3
[I] if $3 \mid F_k$, then $3 \mid F_{k+4}$, for all $k \geq 4$

Prove [I] by rewriting F_{k+4} in such a way that you can apply the IH on F_k

Example

$$
\begin{aligned}
F_{k+4} &= F_{k+3} + F_{k+2} \\
&= (F_{k+2} + F_{k+1}) + (F_{k+1} + F_k) \\
&= (F_{k+1} + F_k) + 2(F_k + F_{k-1}) + F_k \\
&= (F_k + F_{k-1}) + 4F_k + 2F_{k-1} \\
&= 5F_k + 3F_{k-1}
\end{aligned}
$$

Strong Induction

This is a version in which the inductive hypothesis is stronger. Rather than using the fact that $P(k)$ holds for a single value, we use *all* values up to k.

If

[B] $P(m)$

[I] $[P(m) \wedge P(m+1) \wedge \ldots \wedge P(k)] \rightarrow P(k+1)$ for all $k \geq m$

then

[C] $P(n)$, for all $n \geq m$

Example

Claim: All integers ≥ 2 can be written as a product of primes.

[B] 2 is a product of primes
[I] If all x with $2 \leq x \leq k$ can be written as a product of primes, then $k+1$ can be written as a product of primes, for all $k \geq 2$

Proof for [I]?

Example

Proof.

- Case 1: $k+1$ is prime.
  If $k+1$ is a prime number, then it is already a product of primes (since a prime number can be considered a product of itself).
- Case 2: $k+1$ is composite.
  If $k+1$ is composite, then it can be written as a product of smaller integers. Assume $k+1 = a \times b$, where $2 \leq a, b < k+1$. By the inductive hypothesis, since a and b are less than $k+1$ and greater than or equal to 2, they can each be written as a product of primes. Thus, $k+1$ can also be written as a product of primes.

$\square$

Negative Integers, Backward Induction

Take Notice

Induction can be conducted over any subset of $\mathbb{Z}$ *with least element. Thus* m *can be negative; eg. base case* $m = -10^6$.

Take Notice

One can apply induction in the 'opposite' direction $p(m) \to p(m-1)$. *It means considering the integers with the opposite ordering where the next number after* n *is* $n-1$. *Such induction would be used to prove some* $p(n)$ *for all* $n \leq m$.

Take Notice

Sometimes one needs to reason about all integers $\mathbb{Z}$. *This requires two separate simple induction proofs: one for* $\mathbb{N}$, *another for* $-\mathbb{N}$. *They both would start form some initial values, which could be the same, e.g. zero. Then the first proof would proceed through positive integers; the second proof through negative integers.*

Forward-Backward Induction

Idea

To prove $P(n)$ *for all* $n \geq k_0$

- *verify* $P(k_0)$
- *prove* $P(k_i)$ *for infinitely many* $k_0 < k_1 < k_2 < k_3 < \dots$
- *fill the gaps*
  $P(k_1) \to P(k_1 - 1) \to P(k_1 - 2) \to \dots \to P(k_0 + 1)$
  $P(k_2) \to P(k_2 - 1) \to P(k_2 - 2) \to \dots \to P(k_1 + 1)$
  $\dots\dots\dots$

Take Notice

This form of induction is extremely important for the analysis of algorithms.

Example: AM-GM Inequality

Theorem. For all $n \geq 1$,

$$\frac{a_1 + a_2 + \ldots + a_n}{n} \geq (a_1 \times a_2 \times \ldots \times a_n)^{\frac{1}{n}}$$

[B]	$P(2)$
[Forward Induction]	$P(k) \implies P(2k)$
[Backward Induction]	$P(k) \implies P(k-1)$

Example: AM-GM Inequality

Base Case P(2)

The AM-GM inequality for two numbers is $\frac{a_1+a_2}{2} \geq (a1 \cdot a_2)^{\frac{1}{2}}$.
This is equivalent to proving $\left(\frac{a_1+a_2}{2}\right)^2 \geq a1 \cdot a_2$.
Expanding the left-hand side:

$$\left(\frac{a_1 + a_2}{2}\right)^2 = \frac{a_1^2 + 2a_1a_2 + a_2^2}{4}$$

Thus, we need to show

$$\frac{a_1^2 + 2a_1a_2 + a_2^2}{4} \geq a_1a_2$$

Multiplying both sides by 4, we get $a_1^2 + 2a_1a_2 + a_2^2 \geq 4a_1a_2$, which simplifies to

$$(a_1 - a_2)^2 \geq 0,$$

which is always true. Therefore, the base case holds.

Example: AM-GM Inequality

Forward Induction $P(k) \implies P(2k)$
Assume that the inequality holds for some $n = k$, i.e., for any non-negative real numbers $a_1, a_2, \cdots, a_k$, we have:

$$\frac{a_1 + a_2 + \cdots + a_k}{k} \geq (a_1 \times a_2 \times \cdots \times a_k)^{\frac{1}{k}}$$

We now need to prove that the inequality holds for $2k$ numbers:

$$\frac{a_1 + a_2 + \cdots + a_{2k}}{2k} \geq (a_1 \times a_2 \times \cdots \times a_{2k})^{\frac{1}{2k}}$$

Example: AM-GM Inequality

Proof:

Divide the $2k$ numbers into two groups of k numbers each:

$$G_1 = \{a_1, a_2, \cdots, a_k\}, \quad G_2 = \{a_{k+1}, a_{K+2}, \cdots, a_{2k}\}$$

By the inductive hypothesis P(k), the AM-GM inequality holds for each group:

$$\frac{a_1 + a_2 + \cdots + a_k}{k} \geq (a_1 \times a_2 \times \cdots \times a_k)^{\frac{1}{k}}$$

and

$$\frac{a_{k+1} + a_{k+2+} \cdots + a_{2k}}{k} \geq (a_{k+1} \times a_{k+2} \times \cdots \times a_{2k})^{\frac{1}{k}}$$

Add these two inequalities:

$$\frac{a_1 + a_2 + \cdots + a_{2k}}{k} \geq (a_1 \times a_2 \times \cdots \times a_k)^{\frac{1}{k}} + (a_{k+1} \times a_{k+2} \times \cdots \times a_{2k})^{\frac{1}{k}}$$

Example: AM-GM Inequality

Proof cont'd

Multiply both sides by $\frac{1}{2}$

$$\frac{a_1 + a_2 + \cdots + a_{2k}}{2k} \geq \frac{(a_1 \times \cdots \times a_k)^{\frac{1}{k}} + (a_{k+1} \times \cdots \times a_{2k})^{\frac{1}{k}}}{2}$$

By the AM-GM inequality for two numbers (the case $n = 2$), we know that:

$$\frac{(a_1 \times \cdots \times a_k)^{\frac{1}{k}} + (a_{k+1} \times \cdots \times a_{2k})^{\frac{1}{k}}}{2} \geq (a_1 \times a_2 \times \cdots \times a_{2k})^{\frac{1}{2k}}$$

Thus, we conclude that:

$$\frac{a_1 + a_2 + \cdots + a_{2k}}{2k} \geq (a_1 \times a_2 \times \cdots \times a_{2k})^{\frac{1}{2k}}$$

Hence, $P(2k)$ is true.

Example: AM-GM Inequality

Backward Induction $P(k) \implies P(k-1)$
Assume that the inequality holds for some $n = k$, i.e., for any non-negative real numbers $a_1, a_2, \cdots, a_k$, we have:

$$\frac{a_1 + a_2 + \cdots + a_k}{k} \geq (a_1 \times a_2 \times \cdots \times a_k)^{\frac{1}{k}}$$

We now need to prove that the inequality holds for $k-1$ numbers, i.e., for any non-negative real number $b_1, b_2, \cdots, b_{k-1}$, we need to prove:

$$\frac{b_1 + b_2 + \cdots + b_{k-1}}{k-1} \geq (b_1 \times b_2 \times \cdots \times b_{k-1})^{\frac{1}{k-1}}$$

Example: AM-GM Inequality

Proof: Let $b_k = \frac{b_1+b_2+\cdots+b_{k-1}}{k-1}$, by the indctive hypothesis, the AM-GM inequality holds for this set of k numbers:

$$\frac{b_1 + b_2 + \cdots + b_{k-1} + b_k}{k} \geq (b_1 \times b_2 \times \cdots \times b_{k-1} \times b_k)^{\frac{1}{k}}$$

Substitute $b_k = \frac{b_1+b_2+\cdots+b_{k-1}}{k-1}$ into these expression, we obtain:

$$\frac{b_1 + b_2 + \cdots + b_{k-1}}{k-1} \geq (b_1 \times b_2 \times \cdots \times b_{k-1} \times \frac{b_1 + b_2 + \cdots + b_{k-1}}{k-1})^{\frac{1}{k}}$$

This is equivalent to

$$(\frac{b_1 + b_2 + \cdots + b_{k-1}}{k-1})^{\frac{k-1}{k}} \geq (b_1 \times b_2 \times \cdots \times b_{k-1})^{\frac{1}{k}}$$

Therefore, we have

$$\frac{b_1 + b_2 + \cdots + b_{k-1}}{k-1} \geq (b_1 \times b_2 \times \cdots \times b_{k-1})^{\frac{1}{k-1}}$$

Hence, $P(k-1)$ is true.

Outline

Structural Induction

Basic induction allows us to assert properties over **all natural numbers**. The induction scheme (layout) uses the recursive definition of $\mathbb{N}$.

The induction scheme can be applied not only to natural numbers (and integers) but to any partially ordered set in general – especially those defined recursively.

The basic approach is always the same — we need to verify that

- **[B]** the property holds for all minimal objects — objects that have no predecessors; they are usually very simple objects allowing immediate verification
- **[I]** for any given object, if the property in question holds for *all* its predecessors ('smaller' objects) then it holds for the object itself

Example: Induction on Σ^*

Recall definition of Σ^*:

$\lambda \in \Sigma^*$

If $w \in \Sigma^*$ then $aw \in \Sigma^*$ for all $a \in \Sigma$

Structural induction on Σ^*:

Goal: Show $P(w)$ holds for all $w \in \Sigma^*$.

Approach: Show that:

Base case (B): $P(\lambda)$ holds; and

Inductive case (I): If $P(w)$ holds then $P(aw)$ holds for all $a \in \Sigma$.

Example: Induction on Σ^*

Recall:

Formal definition of Σ^*:

$$\lambda \in \Sigma^*$$

If $w \in \Sigma^*$ then $aw \in \Sigma^*$ for all $a \in \Sigma$

Formal definition of concatenation:

(concat.B) $\lambda v = v$

(concat.I) $(aw)v = a(wv)$

Formal definition of length:

(length.B) $\text{length}(\lambda) = 0$

(length.I) $\text{length}(aw) = 1 + \text{length}(w)$

Example: Induction on Σ^*

Recall:

Formal definition of Σ^*:

$$\lambda \in \Sigma^*$$
$$\text{If } w \in \Sigma^* \text{ then } aw \in \Sigma^* \text{ for all } a \in \Sigma$$

Formal definition of concatenation:

(concat.B) $\lambda v = v$

(concat.I) $(aw)v = a(wv)$

Formal definition of length:

(length.B) $\text{length}(\lambda) = 0$

(length.I) $\text{length}(aw) = 1 + \text{length}(w)$

Prove:

$$\text{length}(wv) = \text{length}(w) + \text{length}(v)$$

Example: Induction on Σ^*

Let $P(w)$ be the proposition that, for all $v \in \Sigma^*$:

$$\text{length}(wv) = \text{length}(w) + \text{length}(v).$$

We will show that $P(w)$ holds for all $w \in \Sigma^*$ by **structural induction on w.**

Proof:

Example: Induction on Σ^*

Let $P(w)$ be the proposition that, for all $v \in \Sigma^*$:

$$\text{length}(wv) = \text{length}(w) + \text{length}(v).$$

We will show that $P(w)$ holds for all $w \in \Sigma^*$ by **structural induction on** w**.**

Proof:
Base case ($w = \lambda$**):**

$$\text{length}(\lambda v) \quad =$$

Example: Induction on Σ^*

Let $P(w)$ be the proposition that, for all $v \in \Sigma^*$:

$$\text{length}(wv) = \text{length}(w) + \text{length}(v).$$

We will show that $P(w)$ holds for all $w \in \Sigma^*$ by **structural induction on w.**

Proof:
Base case ($w = \lambda$):

$$\text{length}(\lambda v) = \text{length}(v) \qquad \text{(concat.B)}$$

Example: Induction on Σ^*

Let $P(w)$ be the proposition that, for all $v \in \Sigma^*$:

$$\text{length}(wv) = \text{length}(w) + \text{length}(v).$$

We will show that $P(w)$ holds for all $w \in \Sigma^*$ by **structural induction on w.**

Proof:
Base case ($w = \lambda$):

$$\begin{aligned} \text{length}(\lambda v) &= \text{length}(v) && \text{(concat.B)} \\ &= 0 + \text{length}(v) \end{aligned}$$

Example: Induction on Σ^*

Let $P(w)$ be the proposition that, for all $v \in \Sigma^*$:

$$\text{length}(wv) = \text{length}(w) + \text{length}(v).$$

We will show that $P(w)$ holds for all $w \in \Sigma^*$ by **structural induction on w.**

Proof:
Base case ($w = \lambda$):

$$\begin{aligned}
\text{length}(\lambda v) &= \text{length}(v) && \text{(concat.B)} \\
&= 0 + \text{length}(v) \\
&= \text{length}(w) + \text{length}(v) && \text{(length.B)}
\end{aligned}$$

Example: Induction on Σ^*

Proof cont'd:
Inductive case ($w = aw'$): Assume that $P(w')$ holds. That is, for all $v \in \Sigma^*$:

$$\text{(IH):} \qquad \text{length}(w'v) = \text{length}(w') + \text{length}(v).$$

Then, for all $a \in \Sigma$, we have:

$$\text{length}((aw')v) \quad =$$

Example: Induction on Σ^*

Proof cont'd:

Inductive case ($w = aw'$): Assume that $P(w')$ holds. That is, for all $v \in \Sigma^*$:

$$\text{(IH)}: \qquad \text{length}(w'v) = \text{length}(w') + \text{length}(v).$$

Then, for all $a \in \Sigma$, we have:

$$\text{length}((aw')v) \;=\; \text{length}(a(w'v)) \qquad \text{(concat.I)}$$

Example: Induction on Σ^*

Proof cont'd:

Inductive case ($w = aw'$): Assume that $P(w')$ holds. That is, for all $v \in \Sigma^*$:

$$\text{(IH)}: \qquad \mathsf{length}(w'v) = \mathsf{length}(w') + \mathsf{length}(v).$$

Then, for all $a \in \Sigma$, we have:

$$\begin{aligned} \mathsf{length}((aw')v) &= \mathsf{length}(a(w'v)) && \text{(concat.I)} \\ &= 1 + \mathsf{length}(w'v) && \text{(length.I)} \end{aligned}$$

Example: Induction on Σ^*

Proof cont'd:
Inductive case ($w = aw'$): Assume that $P(w')$ holds. That is, for all $v \in \Sigma^*$:

$$\text{(IH):} \qquad \text{length}(w'v) = \text{length}(w') + \text{length}(v).$$

Then, for all $a \in \Sigma$, we have:

$$\begin{aligned}
\text{length}((aw')v) &= \text{length}(a(w'v)) && \text{(concat.I)} \\
&= 1 + \text{length}(w'v) && \text{(length.I)} \\
&= 1 + \text{length}(w') + \text{length}(v) && \text{(IH)}
\end{aligned}$$

Example: Induction on Σ^*

Proof cont'd:
Inductive case ($w = aw'$): Assume that $P(w')$ holds. That is, for all $v \in \Sigma^*$:

$$\text{(IH):} \qquad \text{length}(w'v) = \text{length}(w') + \text{length}(v).$$

Then, for all $a \in \Sigma$, we have:

$$\begin{aligned}
\text{length}((aw')v) &= \text{length}(a(w'v)) && \text{(concat.I)} \\
&= 1 + \text{length}(w'v) && \text{(length.I)} \\
&= 1 + \text{length}(w') + \text{length}(v) && \text{(IH)} \\
&= \text{length}(aw') + \text{length}(v) && \text{(length.I)}
\end{aligned}$$

Example: Induction on Σ^*

Proof cont'd:
Inductive case ($w = aw'$): Assume that $P(w')$ holds. That is, for all $v \in \Sigma^*$:

$$\text{(IH):} \qquad \mathrm{length}(w'v) = \mathrm{length}(w') + \mathrm{length}(v).$$

Then, for all $a \in \Sigma$, we have:

$$\begin{aligned}
\mathrm{length}((aw')v) &= \mathrm{length}(a(w'v)) && \text{(concat.I)}\\
&= 1 + \mathrm{length}(w'v) && \text{(length.I)}\\
&= 1 + \mathrm{length}(w') + \mathrm{length}(v) && \text{(IH)}\\
&= \mathrm{length}(aw') + \mathrm{length}(v) && \text{(length.I)}
\end{aligned}$$

So $P(aw')$ holds.

Example: Induction on Σ^*

Proof cont'd:

Inductive case ($w = aw'$): Assume that $P(w')$ holds. That is, for all $v \in \Sigma^*$:

$$\text{(IH)}: \qquad \text{length}(w'v) = \text{length}(w') + \text{length}(v).$$

Then, for all $a \in \Sigma$, we have:

$$\begin{aligned}
\text{length}((aw')v) &= \text{length}(a(w'v)) && \text{(concat.I)} \\
&= 1 + \text{length}(w'v) && \text{(length.I)} \\
&= 1 + \text{length}(w') + \text{length}(v) && \text{(IH)} \\
&= \text{length}(aw') + \text{length}(v) && \text{(length.I)}
\end{aligned}$$

So $P(aw')$ holds.

We have $P(\lambda)$ and for all $w' \in \Sigma^*$ and $a \in \Sigma$: $P(w') \to P(aw')$.
Hence $P(w)$ holds for all $w \in \Sigma^*$.

Example 2: Induction on Σ^*

Recall append : $\Sigma^* \times \Sigma \to \Sigma^*$ defined as:

- $\text{append}(\lambda, x) = x$
- $\text{append}(aw, x) = a\,(\text{append}(w, x))$

Formal definition of append:

(append.B) $\text{append}(\lambda, x) = x$,

(append.I) $\text{append}(aw, x) = a\,(\text{append}(w, x))$

Prove:

For all $w, v \in \Sigma^*$ and $x \in \Sigma$:

$$\text{append}(wv, x) = w(\text{append}(v, x))$$

Example 2: Induction on Σ^*

Theorem

For all $w, v \in \Sigma^*$ *and* $x \in \Sigma$: $append(wv, x) = w(append(v, x))$.

Proof: By induction on w...

Example 2: Induction on Σ^*

Theorem

For all $w, v \in \Sigma^*$ *and* $x \in \Sigma$*:* $\mathit{append}(wv, x) = w(\mathit{append}(v, x))$.

Proof: By induction on w...

$$
\begin{array}{llr@{\;}l l}
\textbf{[B]} & & \text{append}(\lambda v, x) &= \text{append}(v, x) & \text{(concat.B)} \\
\textbf{[I]} & & \text{append}((aw)v, x) &= \text{append}(a(wv), x) & \text{(concat.I)} \\
& & &= a\,\text{append}(wv, x) & \text{(append.I)} \\
& & &= a\,(w\,\text{append}(v, x)) & \text{(IH)} \\
& & &= (aw)\,\text{append}(v, x) & \text{(concat.I)}
\end{array}
$$

Example 3: Induction on Σ^*

Define $\mathsf{rev} : \Sigma^* \to \Sigma^*$:

$$\textbf{(rev.B)}\quad \mathsf{rev}(\lambda) = \lambda,$$

$$\textbf{(rev.I)}\quad \mathsf{rev}(a \cdot w) = \mathsf{append}(\mathsf{rev}(w), a)$$

Example 3: Induction on Σ^*

Theorem

For all $w, v \in \Sigma^*$, $rev(wv) = rev(v) \cdot rev(w)$.

Proof: By induction on w...

Example 3: Induction on Σ^*

Theorem

For all $w, v \in \Sigma^*$, $rev(wv) = rev(v) \cdot rev(w)$.

Proof: By induction on w...

[B]

$$\begin{aligned} \text{rev}(\lambda v) &= \text{rev}(v) && \text{(concat.B)} \\ &= \text{rev}(v)\lambda && \text{(*)} \\ &= \text{rev}(v)\text{rev}(\lambda) && \text{(rev.B)} \end{aligned}$$

[I]

$$\begin{aligned} \text{rev}((aw')v) &= \text{rev}(a(w'v)) && \text{(concat.I)} \\ &= \text{append}(\text{rev}(w'v), a) && \text{(rev.I)} \\ &= \text{append}(\text{rev}(v)\text{rev}(w'), a) && \text{(IH)} \\ &= \text{rev}(v)\text{append}(\text{rev}(w'), a) && \text{(Example 2)} \\ &= \text{rev}(v)\text{rev}(aw') && \text{(rev.I)} \end{aligned}$$

Example 4: Induction on more complex structures

Recall expressions in the Proof assistant:

- (B) $A, B, \ldots, Z, a, b, \ldots z$ are expressions
- (B) $\emptyset$ and $\mathcal{U}$ are expressions
- (R) If E is an expression then so is (E) and E^c
- (R) If E_1 and E_2 are expressions then:
  - $(E_1 \cup E_2)$,
  - $(E_1 \cap E_2)$,
  - $(E_1 \setminus E_2)$, and
  - $(E_1 \oplus E_2)$ are expressions.

Theorem

In any valid expression, the number of $($ *equals the number of* $)$

Proof: By induction on the structure of E...

Exercise

$\boxed{\text{RW: 4.4.2}}$ Define $s_1 = 1$ and $s_{n+1} = \frac{1}{1+s_n}$ for $n \geq 1$

Then $s_1 = 1,\ s_2 = \frac{1}{2},\ s_3 = \frac{2}{3},\ s_4 = \frac{3}{5},\ s_5 = \frac{5}{8},\ s_6 = \frac{8}{13}, \ldots$

The numbers in numerator and denominator remind one of the Fibonacci sequence.

Prove by induction that

$$s_n = \frac{F_n}{F_{n+1}}$$

Proof: By induction on n...

[B] $s_1 = \frac{F_1}{F_2} = \frac{1}{1} = 1$

[I] $s_{n+1} = \frac{1}{1+s_n} = \frac{1}{1+\frac{F_n}{F_{n+1}}} = \frac{F_{n+1}}{F_{n+1}+F_n} = \frac{F_{n+1}}{F_{n+2}}$