Section 4.1 - Mathematical Induction
and
Section 4.2 - Strong Induction and Well-Ordering

A very special rule of inference!

Definition: A set S is *well ordered* if every subset has a least element.

Note: [0, 1] is not well ordered since (0,1] does not have a least element.

Examples:

- N is well ordered (under the ≤ relation)

- Any coutably infinite set can be well ordered

The least element in a subset is determined by a bijection (list) which exists from N to the countably infinite set.

- Z can be well ordered but it is not well ordered under the ≤ relation (Z has no smallest element).

- The set of finite strings over an alphabet using lexicographic ordering is well ordered.

Let P(x) be a predicate over a well ordered set S.

The problem is to prove

$$xP(x).$$

The rule of inference called

The (first) principle of Mathematical Induction

can sometimes be used to establish the universally quantified assertion.

In the case that S = N, the natural numbers, the principle has the following form.

$$P(0)$$
$$P(n) \rightarrow P(n+1)$$
$$xP(x)$$

The hypotheses are

H1: $P(0)$

and

H2: $P(n) \rightarrow P(n+1)$ for n arbitrary.

- H1 is called *The Basis Step*.
- H2 is called *The Induction* (*Inductive*) *Step*

- We first prove that the predicate is true for the smallest element of the set S (0 if S = N).

- We then show if it is true for an element x (n if S = N) implies it is true for the “next” element in the set (n + 1 if S = N).

Then

• knowing it is true for the first element means it must be true for the element following the first or the second element

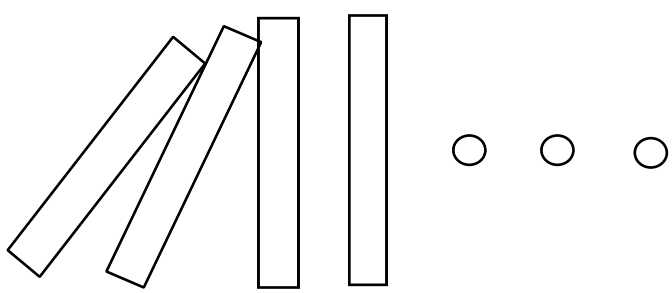
• knowing it is true for the second element implies it is true for the third

and so forth.

Therefore, induction is equivalent to *modus ponens* applied an countable number of times!!

It is like a row of dominos:

If the nth domino falls over the (n+1)st must fall over so pushing the first one down means all must fall down.



• To prove H2 we normally use a Direct Proof.

• Assuming *P(n)* to be true for arbitrary n is called the *Induction* (*Inductive*) *Hypothesis*.

Example: (a classic)

Prove:

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

In logical notation we wish to show

$$n[\sum_{i=0}^{n} i = \frac{n(n+1)}{2}]$$

Hence, the predicate *P(n)* is

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

<u>Note: Identifying P(x) is often the hardest part!</u>

- We first prove H1: *P(0):* $0 = \sum_{i=0}^{0} i = \frac{0(0+1)}{2}$
- Now establish H2 using a direct proof:
- <u>State the Induction Hypotheses</u> :
- Assume *P(n)* is true for n arbitrary

(this looks as if you are assuming the truth of what is to be proved and hence we have a circular argument. This is <u>not</u> the case.)

- Now use this and anything else you know to establish that *P(n + 1)* must be true.

P(n + 1) is the assertion

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

(Note: Write down the assertion *P(n+1)*! Don't make it hard for yourself because you don't know what it is you are to prove.)

But,

$$\sum_{i=0}^{n+1} i = \sum_{i=1}^{n} i + (n+1)$$

using the property of summations.

Now apply the induction hypothesis.

Note: you must manipulate the assertion *P(n+1)* so that you can apply the induction hypothesis *P(n)*. If you do not apply the induction hypothesis somewhere, it is not a valid induction proof.

Use the assumption *P(n)* to substitute

$$\frac{n(n+1)}{2} \text{ for } \sum_{i=0}^{n} i$$

to get

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

and we manipulate the right side to get

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

which is exactly *P(n+1).*

Hence, we have established H2.

We now say by the Principle of Mathematical Induction it follows that *P(n)* is true for all n *or*

$$n[\sum_{i=0}^{n} i = \frac{n(n+1)}{2}]$$

Q.E.D.

We can use the Principle to prove more general assertions because N is well ordered.

Suppose we wish to prove for some specific integer k

$$x[n \geq k \rightarrow P(x)]$$

Now we merely change the basis step to *P(k)* and continue.

Example:

Show

3n + 5 is O(n^2).

Proof:

We must find C and k such that

$$3n + 5 \leq Cn^2$$

whenever n ≥ k (or n > k-1).

If we try C = 1, then the assertion is not true until k = 5.

Hence we prove by induction that $3n + 5 \leq n^2$ for all n ≥ 5.

The assertion becomes

$$n[n \geq 5 \rightarrow 3n + 5 \leq n^2]$$

and the predicate *P(n)* is $3n + 5 \leq n^2$

- Basis step: *P(*5): 3x5 + 5 = 20 ≤ $(5)^2$ which establishes the basis step.

- The induction hypothesis: assume *P(n)*: $3n + 5 \leq n^2$ is true for n arbitrary.

- Use this and any other clever things you know to show *P(n+1)*.

<u>Write down the assertion *P(n+1)*!</u>

$$P(n+1)\text{: } 3(n+1) + 5 \leq (n+1)^2$$

Now put it in a form which will allow you to apply the induction hypothesis.

We rewrite the left side as $(3n+5)+3$ and apply the induction hypothesis to (3n+5) which we assume is less than n^2.

Now we must show that

$$n^2 + 3 \leq (n + 1)^2 = n^2 + 2n + 1$$

which is true iff

$$3 \leq 2n + 1$$

which is true iff

$$n \geq 1.$$

But we have already restricted $n \geq 5$ so $n \geq 1$ must hold.

Hence we have established the induction step and the assertion must be true for all n:

$$n[n \geq 5 \rightarrow 3n + 5 \leq n^2]$$

Q.E.D.

Note: in doubly quantified assertions of the form

$$m \quad n[P(m,n)]$$

we often assume m (or n) is arbitrary to eliminate a quantifier and prove the remaining result using induction.

Another Example:

All horses are the same color.

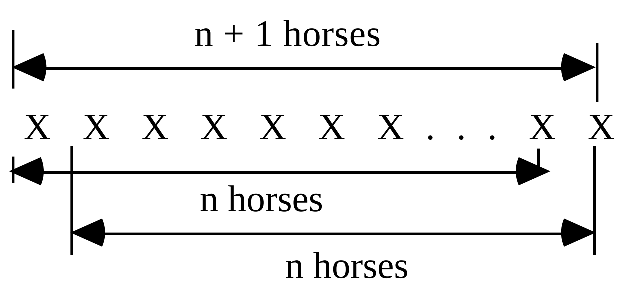
Proof: We do induction on the size of sets of horses of the same color.

• Basis step: The assertion is obviously true for all sets of 0 horses (and all sets with 1 horse).

• Induction step: The induction hypothesis becomes 'Assume the assertion is true for all sets with n horses.'

Now show it must be true for all sets of n+1 horses.

But every set of n+1 horses has an overlap of horses which are the same color.



Hence the set of n+1 horses must have the same color.

Therefore, all horses have the same color.

What's wrong?

The Second Principle of Mathematical Induction

The rule of inference becomes:

H1: $P(0)$

H2: $P(0) \quad P(1) \; ... \quad P(n) \rightarrow P(n+1)$

$xP(x)$

The two rules are equivalent but sometimes the second is easier to apply. See your text for the classic examples.

