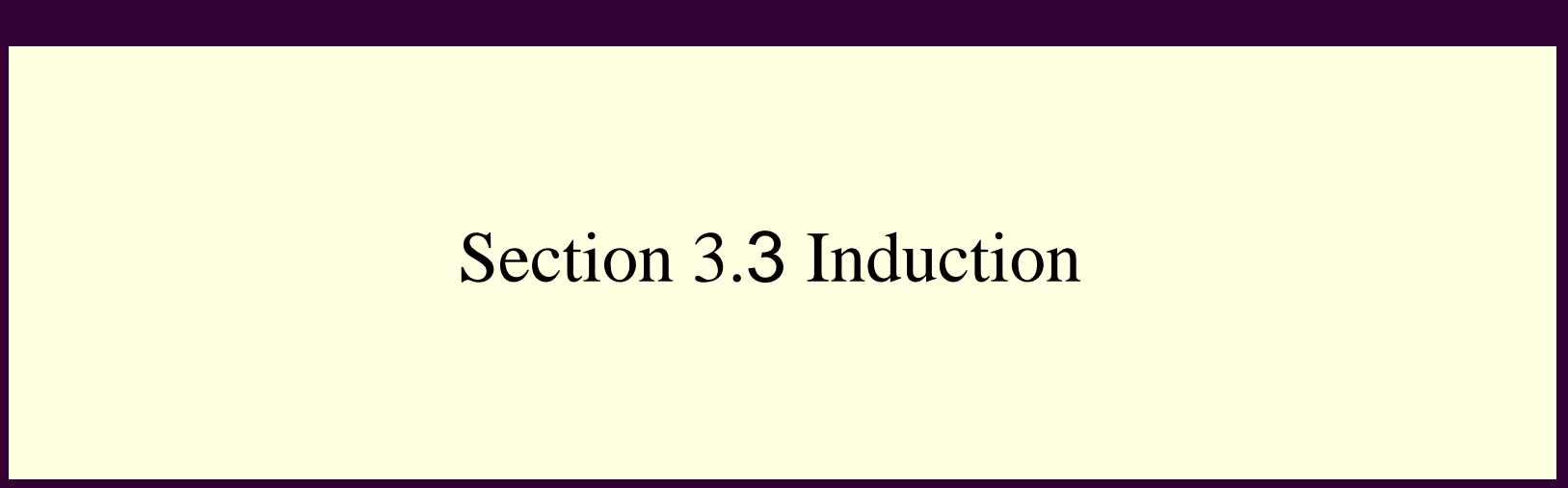




# Proof Methods



## Section 3.3 Induction

# Definitions

---

- **Definition:** A set  $S$  is *well ordered* if every subset has a least element.
- Let  $P(x)$  be a predicate over a well ordered set  $S$ . The problem is to prove

$$\forall xP(x) .$$

- The rule of inference called *The (first) principle of Mathematical Induction* can sometimes be used to establish the universally quantified assertion.

# Some Background

---

- From modus ponens:

$p$

$p \rightarrow q$

$\therefore q$  conclusion

- We can easily derive “double modus ponens”:

$p(0)$

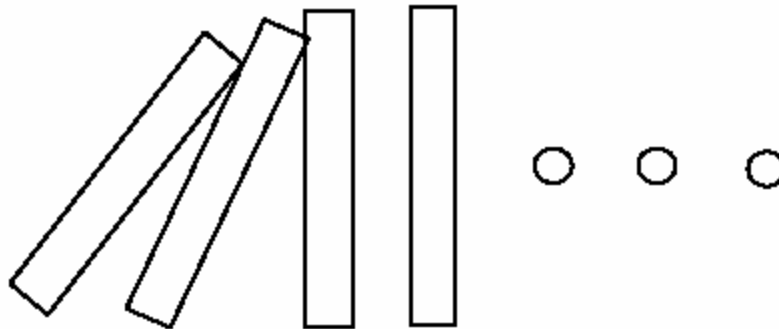
$p(0) \rightarrow p(1)$

$p(1) \rightarrow p(2)$

$\therefore p(2)$  conclusion

# Some Background

- We might also derive triple modus ponens, quadruple modus ponens, and so on. Thus, we have no trouble proving assertions about arbitrarily large integers.
- A classic example:
  - For instance, the initial domino falls.  
If any of the first 999 dominoes falls, then so does its successor.  
Therefore, the first 1000 dominoes all fall down.



# Mathematical Induction

- The (first) principle of Mathematical Induction  
The problem is to prove:  $\forall xP(x)$
- In the case that  $x \in \mathbb{N}$  ( $S=\mathbb{N}$ , the natural numbers), the principle has the following form:

$$P(0)$$

$$P(n) \rightarrow P(n+1)$$

$$\therefore \forall xP(x)$$

- 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*

# Mathematical Induction

---

- We first prove that the predicate is true for the smallest element of the set  $S$  (0 if  $S = \mathbb{N}$ ).
- We then show if it is true for an element  $x$  ( $n$  if  $S = \mathbb{N}$ ) implies it is true for the “next” element in the set ( $n + 1$  if  $S = \mathbb{N}$ ). 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!!

# Mathematical Induction: Summary

---

- Summary: two steps involved in a induction proof
  - *Basis Step* H1:  $P(k)$  ( $k = 0$  for natural number)
  - *Induction Step*:  $P(n) \rightarrow P(n + 1)$  for arbitrary  $n$ .
- To prove  $P(k)$ , merely a verification/substitution is needed.
- To prove H2 we normally use a Direct Proof.

# Example

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

Solution:

- Step 0: Identifying  $P(n)$ :

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

- Step 1: *The Basis Step* (H1), we need to prove

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

# Example (Cont.)

- *Step 2: The Induction (Inductive) Step (H2):* using a direct proof.

- State the Induction Hypotheses: Assume  $P(n)$  is true for  $n$  arbitrary
- 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.)

# Example (Cont.)

## ■ Step 2 (cont.)

- 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.

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

Use the assumption  $P(n)$  to substitute

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

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

# Example (Cont.)

- Step 2 (cont.)

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

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

Q.E.D.

# Mathematical Induction

---

We can use the Principle to prove more general assertions because  $\mathbb{N}$  is well ordered.

Suppose we wish to prove for some specific integer  $k$

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

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

# Example

---

Prove: the sum of first  $n$  odd positive integers is  $n^2$  ( $n \geq 1$ )

# Example

---

Prove

$2^n < n!$  for positive integers  $n \geq 4$ .

# Example

---

- Example: prove that  $2^{2n} - 1$  ( $n \geq 1$ ) is divisible by 3.