University of Florida
Dept. of Computer & Information Science & Engineering

COT 3100

Applications of Discrete Structures

Dr. Michael P. Frank

Slides for a Course Based on the Text
Discrete Mathematics & Its Applications
(5th Edition)
by Kenneth H. Rosen

Module #13:
Inductive Proofs

Rosen 5th ed., §3.3
~11 slides, ~1 lecture

§3.3: Mathematical Induction

- A powerful, rigorous technique for proving that a predicate $P(n)$ is true for *every* natural number n, no matter how large.
- Essentially a "domino effect" principle.
- Based on a predicate-logic inference rule:

$$\frac{\begin{array}{l} P(0) \\ \forall n \geq 0\ (P(n) \rightarrow P(n+1)) \end{array}}{\therefore \forall n \geq 0\ P(n)}$$

"The First Principle of Mathematical Induction"

Validity of Induction

Proof that $\forall k \geq 0\ P(k)$ is a valid consequent:

Given any $k \geq 0$, $\forall n \geq 0\ (P(n) \rightarrow P(n+1))$ (antecedent 2) trivially implies $\forall n \geq 0\ (n<k) \rightarrow (P(n) \rightarrow P(n+1))$, or $(P(0) \rightarrow P(1)) \wedge (P(1) \rightarrow P(2)) \wedge \ldots \wedge (P(k-1) \rightarrow P(k))$. Repeatedly applying the hypothetical syllogism rule to adjacent implications k-1 times then gives $P(0) \rightarrow P(k)$; which with $P(0)$ (antecedent #1) and *modus ponens* gives $P(k)$. Thus $\forall k \geq 0\ P(k)$.

The Well-Ordering Property

- The validity of the inductive inference rule can also be proved using the *well-ordering property*, which says:
  - Every non-empty set of non-negative integers has a minimum (smallest) element.
  - $\forall\ \emptyset \subset S \subseteq \mathbf{N} : \exists m \in S : \forall n \in S : m \leq n$
- Implies $\{n | \neg P(n)\}$ has a min. element m, but then $P(m\text{-}1) \rightarrow P((m\text{-}1)+1)$ contradicted.

Outline of an Inductive Proof

- Want to prove $\forall n\, P(n)$…
- *Base case* (or *basis step*): Prove $P(0)$.
- *Inductive step*: Prove $\forall n\, P(n) \rightarrow P(n+1)$.
  - *E.g.* use a direct proof:
  - Let $n \in \mathbf{N}$, assume $P(n)$. (*inductive hypothesis*)
  - Under this assumption, prove $P(n+1)$.
- Inductive inference rule then gives $\forall n\, P(n)$.

Generalizing Induction

- Can also be used to prove $\forall n \geq c\ P(n)$ for a given constant $c \in \mathbf{Z}$, where maybe $c \neq 0$.
  - In this circumstance, the base case is to prove $P(c)$ rather than $P(0)$, and the inductive step is to prove $\forall n \geq c\ (P(n) \rightarrow P(n+1))$.
- Induction can also be used to prove $\forall n \geq c\ P(a_n)$ for an arbitrary series $\{a_n\}$.
- Can reduce these to the form already shown.

Second Principle of Induction

- Characterized by another inference rule:

$$\frac{\begin{array}{l} P(0) \\ \forall n \geq 0 \colon \overbrace{(\forall 0 \leq k \leq n\ P(k))}^{P \text{ is true in } all \text{ previous cases}} \rightarrow P(n+1) \end{array}}{\therefore \forall n \geq 0 \colon P(n)}$$

- Difference with 1st principle is that the inductive step uses the fact that $P(k)$ is true for *all* smaller $k<n+1$, not just for $k=n$.

Induction Example (1st princ.)

- Prove that the sum of the first *n* odd positive integers is n^2. That is, prove:

$$\forall n \geq 1: \underbrace{\sum_{i=1}^{n}(2i-1) = n^2}_{P(n)}$$

- Proof by induction.
  - Base case: Let n=1. The sum of the first 1 odd positive integer is 1 which equals 1^2. (Cont…)

Example cont.

- Inductive step: Prove $\forall n \geq 1$: $P(n) \rightarrow P(n+1)$.
  - Let $n \geq 1$, assume $P(n)$, and prove $P(n+1)$.

$$\sum_{i=1}^{n+1}(2i-1) = \left(\sum_{i=1}^{n}(2i-1)\right) + (2(n+1)-1)$$

$$= n^2 + 2n + 1$$

$$= (n+1)^2$$

By inductive hypothesis P(n)

Another Induction Example

- Prove that $\forall n>0, n<2^n$. Let $P(n)=(n<2^n)$
  - Base case: $P(1)=(1<2^1)=(1<2)=\mathbf{T}$.
  - Inductive step: For $n>0$, prove $P(n)\rightarrow P(n+1)$.
    - Assuming $n<2^n$, prove $n+1 < 2^{n+1}$.
    - Note $n + 1 < 2^n + 1$ (by inductive hypothesis)
      $< 2^n + 2^n$ (because $1<2=2\cdot 2^0\leq 2\cdot 2^{n-1}= 2^n$)
      $= 2^{n+1}$
    - So $n + 1 < 2^{n+1}$, and we're done.

Example of Second Principle

- Show that every $n>1$ can be written as a product $p_1p_2\ldots p_s$ of some series of s prime numbers. Let $P(n)$="n has that property"
- Base case: $n=2$, let $s=1$, $p_1=2$.
- Inductive step: Let $n\geq 2$. Assume $\forall 2\leq k\leq n$: $P(k)$. Consider $n+1$. If prime, let $s=1$, $p_1=n+1$. Else $n+1=ab$, where $1<a\leq n$ and $1<b\leq n$. Then $a=p_1p_2\ldots p_t$ and $b=q_1q_2\ldots q_u$. Then $n+1= p_1p_2\ldots p_t\, q_1q_2\ldots q_u$, a product of $s=t+u$ primes.

Another 2nd Principle Example

- Prove that every amount of postage of 12 cents or more can be formed using just 4-cent and 5-cent stamps.
- Base case: 12=3(4), 13=2(4)+1(5), 14=1(4)+2(5), 15=3(5), so $\forall 12 \leq n \leq 15, P(n)$.
- Inductive step: Let $n \geq 15$, assume $\forall 12 \leq k \leq n$ $P(k)$. Note $12 \leq n-3 \leq n$, so $P(n-3)$, so add a 4-cent stamp to get postage for $n+1$.