CS 441 Discrete Mathematics for CS
Lecture 15

Mathematical induction & Recursion

Milos Hauskrecht
milos@cs.pitt.edu
5329 Sennott Square

Proofs

Basic proof methods:

- Direct, Indirect, Contradiction, By Cases, Equivalences

Proof of quantified statements:

- **There exists x with some property P(x).**
  - It is sufficient to find one element for which the property holds.
- **For all x some property P(x) holds.**
  - Proofs of 'For all x some property P(x) holds' must cover all x and can be harder.
- **Mathematical induction** is a technique that can be applied to prove the universal statements for sets of positive integers or their associated sequences.

Mathematical induction

- Used to prove statements of the form $\forall x\, P(x)$ where $x \in Z^+$

Mathematical induction proofs consists of two steps:

1) **Basis:** The proposition P(1) is true.
2) **Inductive Step:** The implication
   $P(n) \rightarrow P(n+1)$, is true for all positive n.

- Therefore we conclude $\forall x\, P(x)$.

- **Based on the well-ordering property:** Every nonempty set of nonnegative integers has a **least element**.

Mathematical induction

Example: Prove the sum of first n odd integers is n^2 .

i.e. $1 + 3 + 5 + 7 + ... + (2n - 1) = n^2$ for all positive integers.

Proof:

- What is P(n)? $P(n):\ 1 + 3 + 5 + 7 + ... + (2n - 1) = n^2$

Basis Step Show P(1) is true

- Trivial: $1 = 1^2$

Inductive Step Show if P(n) is true then P(n+1) is true for all n.

- Suppose P(n) is true, that is $1 + 3 + 5 + 7 + ... + (2n - 1) = n^2$
- Show P(n+1): $1 + 3 + 5 + 7 + ... + (2n - 1) + (2n + 1) = (n+1)^2$ follows:
- $\underbrace{1 + 3 + 5 + 7 + ... + (2n - 1)}_{n^2} + (2n + 1) =$
  $n^2 + (2n+1) = (n+1)^2$

Correctness of the mathematical induction

Suppose **P(1) is true** and **P(n) $\rightarrow$ P(n+1) is true** for all positive integers n. Want to show **$\forall$x P(x).**

Assume there is at least one n such that P(n) is false. Let S be the set of nonnegative integers where P(n) is false. Thus S $\neq \emptyset$.

Well-Ordering Property: Every nonempty set of nonnegative integers has a least element.

By the Well-Ordering Property, S has a least member, say k. k > 1, since P(1) is true. This implies k - 1 > 0 and P(k-1) is true (since k is the smallest integer where P(k) is false).

Now: P(k-1) $\rightarrow$ P(k) is true

thus, P(k) must be true (a contradiction).

- **Therefore $\forall$x P(x).**

Mathematical induction

Example: Prove $n < 2^n$ for all positive integers n.

- P(n): $n < 2^n$

Basis Step: $1 < 2^1$ (obvious)

Inductive Step: If P(n) is true then P(n+1) is true for each n.

- Suppose P(n): $n < 2^n$ is true
- Show P(n+1): $n+1 < 2^{n+1}$ is true.

$$\begin{aligned} n + 1 &< 2^n + 1 \\ &< 2^n + 2^n \\ &= 2^n(1 + 1) \\ &= 2^n(2) \\ &= 2^{n+1} \end{aligned}$$

Mathematical induction

Example: Prove $n^3 - n$ is divisible by 3 for all positive integers.

- P(n): $n^3 - n$ is divisible by 3

Basis Step: P(1): $1^3 - 1 = 0$ is divisible by 3 (obvious)

Inductive Step: If P(n) is true then P(n+1) is true for each positive integer.

- Suppose P(n): $n^3 - n$ is divisible by 3 is true.
- Show P(n+1): $(n+1)^3 - (n+1)$ is divisible by 3.

$$(n+1)^3 - (n+1) = n^3 + 3n^2 + 3n + 1 - n - 1$$
$$= (n^3 - n) + 3n^2 + 3n$$
$$= (n^3 - n) + 3(n^2 + n)$$

↗ ↖

divisible by 3 divisible by 3

Strong induction

- **The regular induction:**
  - uses the basic step **P(1)** and
  - inductive step **P(n-1) → P(n)**
- **Strong induction uses:**
  - Uses the basis step **P(1)** and
  - inductive step **P(1) and P(2) … P(n-1) → P(n)**

Example: Show that a positive integer greater than 1 can be written as a product of primes.

Strong induction

Example: Show that a positive integer greater than 1 can be written as a product of primes.

Assume P(n): an integer n can be written as a product of primes.

Basis step: P(2) is true

Inductive step: Assume true for P(2),P(3), … P(n)

Show that P(n+1) is true as well.

2 Cases:

- If n+1 is a prime then P(n+1) is trivially true
- If n+1 is a composite then it can be written as a product of two integers (n+1) = a*b such that 1< a ,b < n+1
- From the assumption P(a) and P(b) holds.
- Thus, n+1 can be written as a product of primes
- **End of proof**

Recursive Definitions

- Sometimes it is possible to define an object (function, sequence, algorithm, structure) in terms of itself. This process is called **recursion.**

Examples:

- Recursive definition of an **arithmetic sequence**:
  - $\mathbf{a_n}$= a+nd
  - $\mathbf{a_n} = \mathbf{a_{n-1}}$+d , $\mathbf{a_0}$= a
- Recursive definition of **a geometric sequence:**
  - $\mathbf{x_n = ar^n}$
  - $\mathbf{x_n = rx_{n-1}}$, $\mathbf{x_0 = a}$

Recursive Definitions

- In some instances recursive definitions **of objects may be much easier to write**

Examples:

- **Algorithm for computing the gcd:**
  - gcd(79, 35) = gcd(35, 9)
  - More general:
    gcd(a, b) = gcd(b, a mod b)
- **Factorial function:**
  - **n! = n (n-1)!   and 0!=1**

Recursively Defined Functions

To define a function on the set of nonnegative integers

- 1. Specify the value of the function at 0
- 2. Give a rule for finding the function's value at n+1 in terms of the function's value at integers i ≤ n.

Example: **factorial function definition**

- **0! = 1**
- **n! = n (n-1)!**
- **recursive or inductive definition of a function on nonnegative integers**

Recursively defined functions

Example: Assume a recursive function on positive integers:

- f(0) = 3
- f(n+1) = 2f(n) + 3

- **What is the value of f(0) ?** 3
- f(1) = 2f(0) + 3 = 2(3) + 3 = 6 + 3 = 9
- f(2) = f(1 + 1) = 2f(1) + 3 = 2(9) + 3 = 18 + 3 = 21
- f(3) = f(2 + 1) = 2f(2) + 3 = 2(21) = 42 + 3 = 45
- f(4) = f(3 + 1) = 2f(3) + 3 = 2(45) + 3 = 90 + 3 = 93

Recursive definitions

- **Example:**
  Define the function:
  f(n) = 2n + 1 n = 0, 1, 2, ...
  recursively.

- f(0) = 1
- f(n+1) = f(n) + 2

Recursive definitions

- **Example:**
  Define the sequence:
  $a_n = n^2$ for n = 1,2,3, ...
  recursively.

- $a_1 = 1$
- $a_{n+1} = a_n^2 + (2n + 1), \quad n \geq 1$

Recursive definitions

- **Example:**
  Define a recursive definition of the sum of the first n positive integers:

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

- $F(1) = 1$
- $F(n+1) = F(n) + (n+1), \quad n \geq 1$

Recursive definitions

Some important functions or sequences in mathematics are defined recursively

Factorials

- n! = 1 if n=1
- n! = n.(n-1)! if $n \geq 1$

Fibonacci numbers:

- F(0)=0, F(1) =1 and
- F(n) =F(n-1) + F(n-2) for n=2,3, …

Recursive definitions

Methods (algorithms)

- **Greatest common divisor**

  gcd(a,b) = b if b | a

  = gcd(b, a mod b)

- **Pseudorandom number generators:**
  - $x_{n+1} = (ax_n + c) \bmod m$

Recursive definitions

- **Assume the alphabet Σ**
  - Example: $\Sigma = \{a,b,c,d\}$
- **A set of all strings containing symbols in Σ: Σ^***
  - Example: $\Sigma^* = \{$"",a,aa,aaa,aaa…, ab, …b,bb, bbb, …$\}$

Recursive definition of Σ^*

- **Basis step:**
  - empty string $\lambda \in \Sigma^*$
- **Recursive step:**
  - If $w \in \Sigma^*$ and $x \in \Sigma$ then $wx \in \Sigma^*$

Length of a String

Example:
Give a recursive definition of $l(w)$, the length of the string w.
Solution:
The length of a string can be recursively defined by:
$l('') = 0$; the length of the empty string
$l(wx) = l(w) + 1$ if $w \in \Sigma^*$ and $x \in \Sigma$.

Recursive definitions

- **Data structures**
  - **Example: Rooted tree**
- **A basis step:**
  - a single node (vertex) is a rooted tree
- **Recursive step:**
  - Assume T1, T2, … Tk are rooted trees, then the graph with a root r connected to T1, T2, … Tk is a rooted tree