CS311H: Discrete Mathematics

Mathematical Induction

Işıl Dillig

Review: Induction and Strong Induction

- How does one prove something by induction?
- What is the inductive hypothesis?
- What is the difference between regular and strong induction?
- Is strong induction more powerful than standard induction?

Example

- For $n \geq 1$, prove there exist natural numbers a, b such that:

$$5^n = a^2 + b^2$$

- Hint: $5^{n+1} = 5^2 \cdot 5^{n-1}$

Matchstick Example

- The Matchstick game: There are two piles with same number of matches initially
- Two players take turns removing any positive number of matches from one of the two piles
- Player who removes the last match wins the game
- Prove: Second player always has a winning strategy.

Matchstick Proof

- $P(n)$: Player 2 has winning strategy if initially n matches in each pile
- Base case:
- Induction: Assume $\forall j. 1 \leq j \leq k \rightarrow P(j)$; show $P(k+1)$
- Inductive hypothesis:
- Prove Player 2 wins if each pile contains $k+1$ matches

Matchstick Proof, cont.

- Case 1: Player 1 takes $k+1$ matches from one of the piles.
- What is winning strategy for player 2?
- Case 2: Player 1 takes r matches from one pile, where $1 \leq r \leq k$
-
-

Recursive Definitions

- Should be familiar with recursive functions from programming:

```
public int fact(int n) {
   if(n <= 1) return 1;
   return  n * fact(n - 1);
}
```

- Recursive definitions are also used in math for defining sets, functions, sequences etc.

Recursive Definitions in Math

- Consider the following sequence:

$$1, 3, 9, 27, 81, \ldots$$

- This sequence can be defined recursively as follows:

$$\begin{aligned} a_0 &= 1 \\ a_n &= 3 \cdot a_{n-1} \end{aligned}$$

- First part called base case; second part called recursive step

Recursively Defined Functions

- Just like sequences, functions can also be defined recursively
- Example:

$$\begin{aligned} f(0) &= 3 \\ f(n+1) &= 2f(n) + 3 \quad (n \geq 1) \end{aligned}$$

- What is $f(1)$?
- What is $f(2)$?
- What is $f(3)$?

Recursive Definition Examples

- Consider $f(n) = 2n + 1$ where n is non-negative integer
- What's a recursive definition for f?
- Consider the sequence $1, 4, 9, 16, \ldots$
- What is a recursive definition for this sequence?
- Recursive definition of function defined as $f(n) = \sum_{i=1}^{n} i$?

Recursive Definitions of Important Functions

- Some important functions/sequences defined recursively
- Factorial function:

$$\begin{aligned} f(1) &= 1 \\ f(n) &= n \cdot f(n-1) \quad (n \geq 2) \end{aligned}$$

- Fibonacci numbers: $1, 1, 2, 3, 5, 8, 13, 21, \ldots$

$$\begin{aligned} a_1 &= 1 \\ a_2 &= 1 \\ a_n &= a_{n-1} + a_{n-2} \quad (n \geq 3) \end{aligned}$$

- Just like there can be multiple bases cases in inductive proofs, there can be multiple base cases in recursive definitions

Inductive Proofs for Recursively Defined Structures

- Recursive definitions and inductive proofs are very similar
- Natural to use induction to prove properties about recursively defined structures (sequences, functions etc.)
- Consider the recursive definition:

$$\begin{aligned} f(0) &= 1 \\ f(n) &= f(n-1) + 2 \end{aligned}$$

- Prove that $f(n) = 2n + 1$

Example

- Let f_n denote the n'th element of the Fibonacci sequence
- Prove: For $n \geq 3$, $f_n > \alpha^{n-2}$ where $\alpha = \frac{1+\sqrt{5}}{2}$
- Proof is by strong induction on n with two base cases
- Intuition 1: Definition of f_n has two base cases
- Intuition 2: Recursive step uses f_{n-1}, f_{n-2} $\Rightarrow$ strong induction
- Base case 1 (n=3): $f_3 = 2$, and $\alpha < 2$, thus $f_3 > \alpha$
- Base case 2 (n=4): $f_4 = 3$ and $\alpha^2 = \frac{(3+\sqrt{5})}{2} < 3$

Example, cont.

Prove: For $n \geq 3$, $f_n > \alpha^{n-2}$ where $\alpha = \frac{1+\sqrt{5}}{2}$

- Inductive step: Assuming property holds for f_i where $3 \leq i \leq k$, need to show $f_{k+1} > \alpha^{k-1}$
- First, rewrite α^{k-1} as $\alpha^2 \alpha^{k-3}$
- α^2 is equal to $1 + \alpha$ because:

$$\alpha^2 = \left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{\sqrt{5}+3}{2} = \alpha + 1$$

- Thus, $\alpha^{k-1} = (\alpha + 1)(\alpha^{k-3}) = \alpha^{k-2} + \alpha^{k-3}$

Example, cont.

- $\alpha^{k-1} = \alpha^{k-2} + \alpha^{k-3}$
- By recursive definition, we know $f_{k+1} = f_k + f_{k-1}$
- Furthermore, by inductive hypothesis:

$$f_k > \alpha^{k-2} \qquad f_{k-1} > \alpha^{k-3}$$

- Therefore, $f_{k+1} > \alpha^{k-2} + \alpha^{k-3} = \alpha^{k-1}$

$\square$

Recursively Defined Sets and Structures

- We can also define sets and other data structures recursively
- Example: Consider the set S defined as:

$$3 \in S$$
$$\text{If } x \in S \text{ and } y \in S, \text{ then } x + y \in S$$

- What is the set S defined as above?
- Give a recursive definition of the set E of all even integers:
  - Base case:
  - Recursive step:

Strings and Alphabets

- Recursive definitions play important role in study of strings
- Strings are defined over an alphabet Σ
  - Example: $\Sigma_1 = \{a, b\}$
- Set of all strings formed from Σ forms language called Σ^*
  - Σ_1^*: $\{\epsilon, a, b, aa, ab, ba, bb, \ldots\}$

Recursive Definition of Strings

- The language Σ^* has natural recursive definition:
  - Base case: $\epsilon \in \Sigma^*$ (empty string)
  - Recursive step: $\text{If } w \in \Sigma^* \text{ and } x \in \Sigma, \text{ then } wx \in \Sigma^*$
- Since ϵ is the empty string, $\epsilon s = s$
- Consider the alphabet $\Sigma = \{0, 1\}$
- How is the string "1" formed according to this definition?
- How is "10" formed?

Recursive Definitions of String Operations

- Many operations on strings can be defined recursively.
- Consider function $l(w)$ which yields length of string w
- Example: Give recursive definition of $l(w)$
  - Base case:
  - Recursive step:

Another Example

- The reverse of a string s is s written backwards.
- Example: Reverse of "abc" is "bca"
- Give a recursive definition of the $\text{reverse}(s)$ operation
  - Base case:
  - Recursive step:

Palindromes

- A palindrome is a string that reads the same forwards and backwards
- Examples: "mom", "dad", "abba", "Madam I'm Adam", ...
- Give a recursive definition of the set P of all palindromes over the alphabet $\Sigma = \{a, b\}$
- Base cases:
- Recursive step:

Structural Induction

- How do we prove properties about recursively defined structures?
- Stuctural induction is a technique that allows us to apply induction on recursive definitions even if there is no integer
- Structural induction is also no more powerful than regular induction, but can make proofs much easier

Structural Induction Overview

- Suppose we have:
  - a recursively defined structure S
  - a property P we'd like to prove about S
- Structural induction works as follows:
  1. Base case: Prove P about base case in recursive definition
  2. Inductive step: Assuming P holds for sub-structures used in the recursive step of the definition, show that P holds for the recursively constructed structure.

Example 1

- Consider the following recursively defined set S:
  1. $a \in S$
  2. If $x \in S$, then $(x) \in S$
- Prove by structural induction that every element in S contains an equal number of right and left parantheses.
- Base case: a has 0 left and 0 right parantheses
- Inductive step: By the inductive hypothesis, x has equal number, say n, of right and left parantheses.
- Thus, (x) has $n + 1$ left and $n + 1$ right parantheses.

Example 2

- Consider the set S defined recursively as follows:
  - Base case: $3 \in S$
  - Recursive step: If $x \in S$ and $y \in S$, then $x + y \in S$
- Prove S is set of all positive integers that are multiples of 3
- Let A be the set of all positive integers divisble by 3
- We want to show that $A = S$
- To do this, we need to prove $S \subseteq A$ and $A \subseteq S$

Proof, Part I

Consider the set S defined recursively as follows: $3 \in S$ and if $x \in S$ and $y \in S$, then $x + y \in S$

- Let's first prove $S \subseteq A$, i.e., any element in S is divisible by 3
- For this, we'll use structural induction
- Base case:
- Inductive step:

Proof, Part II

- We showed that all integers in S are multiples of 3, but still need to show S includes all positive multiples of 3
- Therefore, need to prove that $3n \in S$ for all $n \geq 1$
- We'll prove this by strong induction on n:
  - Base case (n=1):
  - Inductive hypothesis:
  - Need to show:
  -
  -