CS 113
DISCRETE STRUCTURES

Chapter 1: Logic and Proof

PROOF

- We are about to enter the formal world of proof
- We take these formal ideas for granted when proving things
  - They are useful in all areas of mathematics
  - They are useful in several areas of computer science
- For starters, there are
  - Axioms-Things we assume to be true
  - Definitions-Things we define based on other things we know
  - Undefined terms-These are things that we take for granted
- You can’t define everything—you need some starting points

TYPES OF PROVEN STATEMENTS

- So, everything else has to be proven
- There are names for proven statements
  - A general proven statement is called a theorem
  - A lemma is a minor statement, often one whose only use is to prove a theorem
  - A corollary is a statement that is either
    - A simple consequence of a theorem, or
    - Follows almost directly from a theorem
- Notice that all these are proven statements

GENERAL METHODS OF PROOF

- There are several ways to prove something true
- The first is <u>direct proof</u>
  - This is the type of proof you find most often
  - You just start at the beginning and progress to the end
- Often, direct proof is too hard
  - Then we resort to other methods

ANOTHER METHOD OF PROOF

- The second method of proof is indirect proof
- This is when we assume the result is false
- We then derive a contradiction
- This method is also called proof by contradiction

STILL ANOTHER METHOD OF PROOF

- The third method of proof is called proof by contrapositive
- You prove the contrapositive
- Recall that a statement and its contrapositive have the same truth value

PROVING A STATEMENT TRUE- MODUS PONENS

- To prove something, we use the rules of inference:
- Here are the rules
  1. Modus ponens
     - Suppose $p \to q$. Also suppose p is true
     - Then q must be true
- This rule probably seems obvious

PROVING A STATEMENT TRUE- MODUS TOLENS

1. Rule 2: Modus tolens
   - Suppose $p \to q$. Also suppose $-q$ is true
   - Then p must be false

PROVING A STATEMENT TRUE- MORE METHODS

- Addition
  - If p is true, then $p \vee q$ is true too
- Simplification
  - If $p \wedge q$ is true , then p is true too
- Conjunction
  - If p and q are each true, then $p \wedge q$ is true too
- Hypothetical syllogism
  - If $p \rightarrow q$ and $q \rightarrow r$ are each true, then $p \rightarrow r$ is true too
- Disjunctive syllogism
  - If $p \vee q$ and $\overline{p}$ are each true, then q must be true too

PROVING A STATEMENT TRUE- RESOLUTION

- If $p \vee q$ and $\overline{p} \vee r$ are each true, then $q \vee r$ is true too
- Resolution only allows the use of $\vee$ in the reasoning
- The letters (or their negations) are called clauses
- Resolution is popular in programs that prove theorems
- The reason is that it is correct
  - This means that it will only arrive at a contradiction if the clauses are inconsistent
- It is also refutation complete
  - This means if the clauses are inconsistent it will arrive at a contradiction

PRACTICE PROBLEMS

- p. 35, #11-14, 16-20, 21-24, 28-37

INSTANTIATION

- You can also make a statement specific
- Suppose the statement “All dogs like bones” is true
- And, suppose Fido is a dog
- You can then say
- “Fido likes bones”
- The reverse is also true

MATHEMATICAL INDUCTION

- Induction is like a row of dominos
- You knock over the first one
- The first one (all by itself) knocks over the second one
- The second one (all by itself) knocks over the third one
- This continues until they all fall over
- This is the idea behind mathematical induction

USING MATHEMATICAL INDUCTION

- To use it, you show
  - P(1) (This is like knocking over the first domino.)
  - This is called the base step.
- You then show
  - P(n) implies P(n+1) This is like each domino knocking over the next.)
  - This is called the inductive step.
  - Notice that, to use this step, you assume that P(n) is true.
- You then can conclude that P(x) is true for all integers

AN EXAMPLE OF INDUCTION

- **Let's try to prove that the sum of the first n odd numbers is n^2 using induction.**

- **That statement is P(n). Here is the proof.**
- **First, check the base step, which is P(1).**
  - **So, here, n=1.**
- **This means you have to show that the sum of the first 1 odd numbers is 1^2.**
  - **Well, the fist 1 odd number is 1. Adding it up (What?) give the sum to be 1.**
  - **Also, 1^2 is also 1.**
  - **So, this is true**
- **We have completed the base step.**

THE INDUCTIVE STEP

- **We now have to show that P(n) implies P(n+1)**
- **We get to assume that P(n) is true.**
  - **This means that we can assume that the sum of the first n odd integers is n^2**
  - **Let's try to find a formula for that**
  - **$1 + 3 + 5 + \ldots + 2n-1 = n^2$**
  - **We get to assume this. (This is really P(n).)**
- **We have to show that P(n+1) is true.**
  - **That means substituting n+1 for n into the formula above.**
  - **So, we have to show that $1 + 3 + 5 + \ldots + 2(n+1)-1 = (n+1)^2$**
  - **The proof is on the next slide**

PROVING THAT THE FORMULA HOLDS

- $1 + 3 + 5 + \ldots + 2(n+1)-1$
- $= 1 + 3 + 5 + \ldots + 2n-1 + 2(n+1)-1$ Inserting the previous number
- $= 1 + 3 + 5 + \ldots + 2n-1 + 2n + 2 -1$ Distributing
- $= n^2 + 2n + 1$ Using the inductive hypothesis
- $= (n+1)^2$
- We have shown what we need to show. The proof is complete.

- Can we prove that $2^0 + 2^1 + 2^2 + \ldots + 2^n = 2^{n+1}-1$ using induction?

TWO FORMS OF MATHEMATICAL INDUCTION

- **There are actually two forms of induction**
- **The weak form uses P(n) to prove P(n+1)**
  - **The previous problem used the weak form**
- **The strong form usesP(1), P(2), …, P(n) to prove P(n+1)**
- **Let's do Problem 26 on p. 47**

The Base Step

- **We have to show P(24), that is, we have to show how to get 24 using 5s an7s**
- **We can do that using 2 of each**
- **Then we do the inductive step**
- **We assume we can**

Questions?

- Are there any questions?