PROOFS

Lecture 5

Proofs of Mathematical Statements

- A proof is a valid argument that establishes the truth of a statement.
- In math, CS, and other disciplines, informal proofs which are generally shorter, are generally used.
  - More than one rule of inference is often used in a step.
  - Steps may be skipped.
  - The rules of inference used are not explicitly stated.
  - Easier to understand and to explain to people.
  - But it is also easier to introduce errors.
- Proofs have many practical applications:
  - verification that computer programs are correct
  - establishing that operating systems are secure
  - enabling programs to make inferences in artificial intelligence
  - showing that system specifications are consistent.

Terminologies

- A theorem is a statement that can be shown to be true with a proof
  - definitions
  - other theorems
  - axioms (statements assumed to be true)
  - rules of inference
- A lemma is a ‘helping theorem’ or a result which is needed to prove a theorem.
- A corollary is a result which follows directly from a theorem.
- A conjecture is a statement that is being proposed to be true. Once a proof of a conjecture is found, it becomes a theorem. It may turn out to be false.

Understanding how theorems are stated

- Many theorems asserts that a property holds for all elements in a domain, such as the integer or real number.
- Although the precise statement of such theorem should include a universal quantifier, the standard convention in math is to omit it.

For example, the statement:

“If $x > y$, where x and y are positive real numbers, then $x^2 > y^2$ ”

really means

“For all positive real numbers x and y, if $x > y$, then $x^2 > y^2$.”

Proving Theorems

- Theorem's form: $\forall x(P(x) \rightarrow Q(x))$

- To prove them, we show that where c is an arbitrary element of the domain,

$$P(c) \rightarrow Q(c)$$

- By universal generalization, the truth of the original formula follows.
- So, we must prove something of the form: $p \longrightarrow q$

Proving Theorems

- Trivial Proof: If we know q is true, then $p \rightarrow q$ is true as well.
- Vacuous Proof: If we know p is false, then $p \rightarrow q$ is true as well.
- Direct Proof: Assume that p is true and use rules of inference, axioms, and logical equivalences to show that q must also be true.
- Proof by Contraposition: Assume $\neg q$ and show $\neg p$ is true also. This is sometimes called an indirect proof method. If we give a direct proof of $\neg q \rightarrow \neg p$ then we have a proof of $p \rightarrow q$.
- Proof by Contradiction: (AKA reductio ad absurdum): To prove p, assume $\neg p$ and derive a contradiction such as $p \wedge \neg p$. (an indirect form of proof). Since we have shown that $\neg p \rightarrow F$ is true , it follows that the contrapositive $T \rightarrow p$ also holds.

Direct Proofs:

Example Theorem 1:

An <u>even integer</u> plus an <u>odd integer</u> is an <u>odd integer</u>

Example 1

- To prove directly that an even integer plus an odd integer is another odd integer, we will use the definitions of even and odd integers and algebraic manipulation.
- An even integer is any integer that can be expressed as $2k$, where k is an integer. An odd integer is any integer that can be expressed as $2n+1$, where n is also an integer.
- Let's let e represent the even integer and o represent the odd integer. Then we have: $e=2k$ for some integer k and $o=2n+1$ for some integer n. Adding e and o together, we get: $e+o=2k+(2n+1)$.
  Simplifying this, we get: $e+o=2k+2n+1$.
  $e+o=2(k+n)+1$.
- Since k and n are both integers, their sum $(k+n)$ is also an integer. Let's call this sum m, so $m=k+n$. Now we can express the sum of e and o as: $e+o=2m+1$.
- This is the form of an odd integer because it is an even number $(2m)$ plus 1. Thus, we have shown directly that adding an even integer to an odd integer yields another odd integer.

Direct Proofs:

Example Theorem 2:

If n is an odd integer, then n^2 is odd.

Direct Proofs:

Let n be an odd integer. An odd integer can be written as $2k+1$, where k is an integer.

Now square n: $n^2 = (2k+1)^2$

Expanding the square, we have:

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

$n^2 = 4k^2 + 4k + 1$

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

$2k^2 + 2k$ is an even integer because the sum of two even integers are even integers. Let's denote this integer as m, where $m = 2k^2 + 2k$.

Thus, we have: $n^2 = 2m + 1$

The expression $2m+1$ fits the definition of an odd integer (an integer that is two times an integer plus one).

Proof by Contraposition:

Example Theorem:

Prove that if n is an integer and $7n + 9$ is even, then n is odd.

Example

- The contrapositive of the statement "if n is an integer and 7n+9 is even, then n is odd" is "if n is not odd then 7n+9 is not even". Rewriting this gives "if n is even then 7n+9 is odd".
- We will start by assuming n is even and then prove that 7n+9 is odd. An even number can be expressed as 2k for some integer k.
- So, let n=2k.
- Now let's plug this into the expression 7n+9: 7n+9=7(2k)+9
  7n+9=14k+9
  7n+9=14k+8+1
  7n+9=2(7k+4)+1
- The term 2(7k+4) is clearly even because it is a multiple of 2. By adding 1 to an even number, the result is odd. Therefore, 7n+9 is odd.
- Since the contrapositive is proven true, the original statement is also true. Therefore, if n is an integer and 7n+9 is even, then n must be odd.

Proof by Contradiction

Example Theorem:

There are no integer x and y such that $x^2 = 4y + 2$

Example

- To prove the statement "There are no integer x and y such that $x^2=4y+2$," we can use a proof by contradiction.
- Suppose, for the sake of contradiction, that there exist integers x and y such that $x^2 = 4y+2$.
- The square of any integer x is either even or odd:
  - If x is even, then $x=2k$ for some integer k, and $x^2 = (2k)^2 = 4k^2$ which is divisible by 4.
  - If x is odd, then $x=2k+1$ for some integer k, and $x^2 = (2k+1)^2 = 4k^2 + 4k+1 = 4(k^2 + k)+1$, which is of the form $4n+1$ for some integer n.
- The square of an integer x is either of the form 4m (if x is even) or 4n+1 (if x is odd). It is never of the form 4y+2, since that would imply x^2 is 2 more than a multiple of 4, which is not possible as shown above.
- The assumption that there exist integers x and y such that $x^2 = 4y+2$ leads to a contradiction. Therefore, there are no integers x and y for which $x^2 = 4y+2$.

“Proof” that 1 = 2

Step	**Reason**
1. $a = b$	Premise
2. $a^2 = a \times b$	Multiply both sides of (1) by a
3. $a^2 - b^2 = a \times b - b^2$	Subtract b^2 from both sides of (2)
4. $(a - b)(a + b) = b(a - b)$	Algebra on (3)
5. $a + b = b$	Divide both sides by $a - b$
6. $2b = b$	Replace a by b in (5) because $a = b$
7. $2 = 1$	Divide both sides of (6) by b

What is wrong with this?

Looking Ahead

- If direct methods of proof do not work:
  - We may need a clever use of a proof by contraposition.
  - Or a proof by contradiction.