Logic & Proofs
(Lecture – 6)

Dr. Nirnay Ghosh

Introduction to Proofs

- A proof is a valid argument that establishes the truth of a mathematical statement.
- The methods of proof are important not only for proving mathematics statements but also used in many computer science applications.
  - Verifying the correctness of computer programs, establishing that operating systems are secure, making inferences in artificial intelligence, showing that system specifications are consistent, and so on.
- Consequently, understanding the techniques used in proofs is essential both in mathematics and in computer science.

Terminologies

- **Theorem:** It is a statement that can be shown to be true.
  - Example: It may be universal quantification of a conditional statement with one or more premises and a conclusion or some other type of logical statements.
- **Proof:** A proof is a valid argument that establishes the truth of a theorem.
  - The statements used in a proof can include **axioms** (or postulates), which are statements we assume to be true, the premises, if any, of the theorem, and previously proven theorems.
  - Rules of inference, together with definitions of terms, are used to draw conclusions from other assertions, tying together the steps of a proof. In practice, the final step of a proof is usually just the conclusion of the theorem.

Terminologies

- **Lemma:** A less important theorem that is helpful in proving other results.
- **Corollary:** It is a theorem that can be established directly from a theorem that has been proved.
- **Conjecture**: It is statement that is being proposed to be a true statement, usually on the basis of some partial evidence, a heuristic argument, or the intuition of an expert.
  - When a proof of a conjecture is found, the conjecture becomes a theorem. Many times conjectures are shown to be false, so they are not theorems.

Methods of Proving Theorems: Direct Proofs

- To prove: conditional statement $p \rightarrow q$ is true
- Approach:
  - Assumption: p is true
  - Subsequent steps are constructed using rules of inference, axioms, definitions, previously proven theorems to show that q must also be true.
- Direct proofs of many results are quite straightforward, with a fairly obvious sequence of steps leading from the hypothesis to the conclusion.
- However, direct proofs sometimes require particular insights and can be quite tricky.

The integer n is *even* if there exists an integer k such that $n = 2k$, and n is *odd* if there exists an integer k such that $n = 2k + 1$. (Note that every integer is either even or odd, and no integer is both even and odd.) Two integers have the *same parity* when both are even or both are odd; they have *opposite parity* when one is even and the other is odd.

Methods of Proving Theorems: Proof by Contraposition

- Direct proofs often reach dead ends while proving theorems of the form $\forall x(P(x) \rightarrow Q(x))$.
- Need for other proof techniques: **indirect proof**
  - They do not start with the premises and end with the conclusion
- **Proofs by contraposition** make use of the fact that the conditional statement $p \rightarrow q$ is equivalent to its contrapositive, $\neg q \rightarrow \neg p$.
  - The conditional statement $p \rightarrow q$ can be proved by showing that its contrapositive, $\neg q \rightarrow \neg p$, is true.
  - We take $\neg q$ as a premise, and using axioms, definitions, and previously proven theorems, together with rules of inference, we show that $\neg p$ must follow

The real number r is *rational* if there exist integers p and q with $q \neq 0$ such that $r = p/q$. A real number that is not rational is called *irrational*.

Vacuous Proof

- We can quickly prove that a conditional statement $\boldsymbol{p} \rightarrow \boldsymbol{q}$ is true when we know that p is false.
- Consequently, if we can show that p is false, then we refer that proof, as a **vacuous proof** of the conditional statement $\boldsymbol{p} \rightarrow \boldsymbol{q}$.
- Vacuous proofs are often used to establish special cases of theorems that state that a conditional statement is true for all positive integers
  - **Example**: Show that the proposition $P(0)$ is true, where $P(n)$ is "If $n > 1$, then $n^2 > n$" and the domain consists of all integers.
  - **Solution**: Note that P(0) is "If $0 > 1$, then $0^2 > 0$." We can show P(0) using a vacuous proof. Indeed, the hypothesis $0 > 1$ is false. This tells us that P(0) is automatically true.

Trivial Proof

- We can also quickly prove a conditional statement $\boldsymbol{p \rightarrow q}$ if we know that the conclusion q is true.
- By showing that q is true, it follows that $\boldsymbol{p \rightarrow q}$ must also be true. A proof of $\boldsymbol{p \rightarrow q}$ that uses the fact that q is true is called a **trivial proof**.
- Trivial proofs are often important when special cases of theorems are proved.
  - **Example**: Let $P(n)$ be "If a and b are positive integers with $a \geq b$, then $a^n \geq b^n$," where the domain consists of all nonnegative integers. Show that $P(0)$ is true..
  - **Solution**: The proposition P(0) is "If $a \geq b$, then $a^0 \geq b^0$." Because $a^0 = b^0 = 1$, the conclusion of the conditional statement "If $a \geq b$, then $a^0 \geq b^0$" is true. Hence, this conditional statement, which is $P(0)$, is true. This is an example of a trivial proof. Note that the hypothesis, which is the statement "$a \geq b$," was not needed in this proof.

Methods of Proving Theorems: Proof by Contradiction

- Suppose we want to prove that a statement p is true. Furthermore, suppose that we can find a contradiction q such that $\neg \boldsymbol{p} \rightarrow \boldsymbol{q}$ is true. Because q is false, but $\neg \boldsymbol{p} \rightarrow \boldsymbol{q}$ is true, we can conclude that $\neg p$ is false, which means that p is true.
  - How can we find a contradiction q that might help us prove that p is true in this way?
- The statement $\boldsymbol{r} \wedge \neg \boldsymbol{r}$ is a contradiction whenever r is a proposition.
- We can prove that p is true if we can show that $\neg \boldsymbol{p} \rightarrow (\boldsymbol{r} \wedge \neg \boldsymbol{r})$ is true for some proposition r.
- Proof of this type are called **proof by contradiction**.
  - Because a proof by contradiction does not prove a result directly, it is another type of indirect proof.