SC 612: Discrete Mathematics (MSc(IT)-Autumn 2023)

Lecture 5: Introduction to Proofs

Instructor: Gopinath Panda *August 14, 2023*

Definition 0.1

- *Theorem: a statement that can be shown to be true.*
- *A theorem may be the universal quantification of a conditional statement with one or more premises and a conclusion.*
- *A theorem is true with a proof.*
- *Proposition: Less important theorems*
- *Proof: a valid argument that establishes the truth of a theorem.*
- *Axiom or postulate: Statements assume to be true.*
- *Lemma: A less important theorem that is helpful in the proof of other results*
- *Conjecture: is a 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.*

1 Direct Proof

Direct proofs always assume a hypothesis is true and then logically deduces a conclusion. A proof that $p \to q$ is true that proceeds by showing that q must be true when p is true

- A direct proof of a conditional statement $p \to q$ is constructed when
  - the first step is the assumption that p is true;
  - subsequent steps are constructed using rules of inference, with
  - the final step showing that q must also be true.

Example. *Prove that the square of an odd integer is odd.*

Solution: To show, "If n is an odd integer, then n^2 is odd."
Let $P(n)$: "n is an odd integer" and $Q(n)$: " n^2 is odd."
This theorem states $\forall n P((n) \to Q(n))$. We will not explicitly use universal instantiation.
Assume that the hypothesis of this conditional statement is true, namely, n is odd.
Therefore, $n = 2k + 1$, where k is some integer. To show that n^2 is also odd.
Squaring both sides of $n = 2k+1$, we get $n^2 = (2k+1)^2 = 4k^2+4k+1 = 2\,(2k^2 + 2k)+1$.
Therefore, n^2 is an odd integer (it is one more than twice an integer).

Example. *Prove that the product of perfect squares is perfect.(An integer a is a perfect square if there is an integer b such that $a = b^2$.)*

Solution: To show, if m and n are both perfect squares, then nm is also a perfect square.
Assume that the hypothesis is true, namely, m and n are both perfect squares.
By definition, there are integers s and t such that $m = s^2$ and $n = t^2$. To show that mn is a perfect square. $mn = s^2t^2$. Hence, $mn = s^2t^2 = (st)^2$. Thus, mn is also a perfect square.

2 Indirect Proof

Direct proofs begin with the premises, continue with a sequence of deductions, and end with the conclusion.
Indirect proofs
- do not start with the premises and end with the conclusion.
- start by assuming the denial of the conclusion.

An indirect proof has two forms:
- Proof By Contraposition.
- Proof By Contradiction.

For both of these scenarios, we assume the negation of the conclusion and set out to prove either the hypothesis's negation or a contradictory statement.

2.1 Proof by contraposition

A proof that $p \to q$ is true that proceeds by showing that p must be false when q is false
- Proofs by contraposition make use of the fact that

$$p \to q \equiv \neg q \to \neg p$$

- Thus, $p \to q$ can be proved by showing that $\neg\, q \to \neg\, p$, is true.
- In a proof by contraposition of $p \to q$, 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.

Example. *Prove that if n is an integer and 3n + 2 is odd, then n is odd.*

Direct proof: Assume that $3n + 2$ is an odd integer
$\implies 3n + 2 = 2k + 1$ for some integer k.
$\implies n = \frac{2k-1}{3}$ it is difficult to say n is odd
Proof by contraposition: Assume that the conclusion of the conditional statement "If 3n + 2 is odd, then n is odd" is false;
Assume that n is even $\implies n = 2k$ for some integer k.
$\implies 3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$.
$\implies 3n + 2$ is even. Therefore not odd.
This is the negation of the premise of the theorem.
Because the negation of the conclusion implies that the hypothesis is false, the original conditional statement is true.
Hence, "If 3n + 2 is odd, then n is odd."

2.2 Proof by Contradiction

Suppose we want to prove that a statement p is true.
- Suppose that we can find a contradiction q such that $\neg\, p \to q$ is true.
- Since q is false, but $\neg\, p \to q$ is true $\implies$ $\neg\, p$ is false $\implies$ p is true.

3 Vacuous Proof

A proof that $p \to q$ is true based on the fact that p is false
- 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):= "If $n > 1$, then $n^2 > n$" and the domain consists of all integers.*
Solution: Note that P(0):= "If $0 > 1$, then $0^2 > 0$." We can show P(0) using a vacuous proof. Indeed, the hypothesis $0 > 1$ is false $\implies$ P(0) is automatically true.

4 Trivial Proof

A proof that $p \to q$ is true based on the fact that q is true
- Trivial proofs are often important when special cases of theorems are proved.

Example. *Let P(n):= "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):= "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, P(0) is true.

5 Proof of Equivalence

To prove a theorem that is a biconditional statement $p \iff q$
- Show that $p \to q$ and $q \to p$ are both true.
- The validity of this approach is based on the tautology

$$(p \iff q) \iff (p \to q) \wedge (q \to p)$$

6 Counterexample:

To show that a statement of the form $\forall\, xP(x)$ is false we need only an element x such that P(x) is false.

Example. *"Every positive integer is the sum of the squares of two integers".*

Solution: $P(x) := x = a^2 + b^2, x > 0, a, b$ are all integers.
$1 = 1^2 + 0^2, \quad 2 = 1^2 + 1^2, \quad 3 = 1^2 + 1^2 + 1^2$ x=3 is a counter example to $\forall\, xP(x)$.

7 Exhaustive proof:

A proof that establishes a result by checking a list of all possible cases

Example. *Prove that $(n+1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$.*

Solution: Using proof by exhaustion, only need verify the inequality $(n+1)^3 \geq 3^n$ when n = 1, 2, 3, and 4.
- For n = 1, we have $(n+1)^3 = 23 = 8$ and $3^n = 3^1 = 3$;
- For n = 2, we have $(n+1)^3 = 33 = 27$ and $3^n = 3^2 = 9$;
- For n = 3, we have $(n+1)^3 = 43 = 64$ and $3^n = 3^3 = 27$;
- For n = 4, we have $(n+1)^3 = 53 = 125$ and $3^n = 3^4 = 81$.

In each of these four cases, we see that $(n+1)^3 \geq 3^n$.
Hence, $(n+1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$.

8 Proof by cases:

A proof broken into separate cases, where these cases cover all possibilities

Example. *Prove that if n is an integer, then $n^2 \geq n$.*

Solution: We can prove that $n^2 \geq n$ for every integer n by considering three cases, when n = 0, when $n \geq 1$, and when $n \leq -1$.
• Case (i): When n = 0, because $0^2 = 0$, we see that $0^2 \geq 0$. It follows that $n^2 \geq n$ is true in this case.
• Case (ii): When $n \geq 1$, multiplying both sides by the positive integer n, we obtain $n \times n \geq n \times 1 \implies n^2 \geq n$ for $n \geq 1$.
• Case (iii): When $n \leq -1$. However, $n^2 \geq 0 \implies n^2 \geq n$.
Because the inequality $n^2 \geq n$ holds in all three cases, we can conclude that if n is an integer, then $n^2 \geq n$.

Without Loss Of Generality (WLOG): an assumption in a proof that makes it possible to prove a theorem by reducing the number of cases to consider in the proof

Example. *Show that if x and y are integers and both xy and $x + y$ are even, then both x and y are even.*

Solution: We will use proof by contraposition, the notion of WLOG, and proof by cases. First, suppose that x and y are not both even. That is, assume that x is odd or that y is odd (or both).
• WLOG, we assume that x is odd, so that x = 2m + 1 for some integer k.
To show xy is odd or x + y is odd. Consider two cases:
• (i) y even, y = 2n for some integer n, so that x + y = (2m + 1) + 2n = 2(m + n) + 1 is odd.
• (ii) y odd, y = 2n + 1 for some integer n, so that xy = (2m + 1)(2n + 1) = 4mn + 2m + 2n + 1 = 2(2mn + m + n) + 1 is odd. This completes the proof by contraposition. (WLOG is justified because the proof when y is odd can be obtained by simply interchanging the roles of x and y.)

9 Existence proof

A proof of a proposition of the form $\exists\, xP(x)$.
• Constructive existence proof: a proof that an element with a specified property exists that explicitly finds such an element
• An existence proof of $\exists\, xP(x)$ can be given by finding an element a, called a witness, such that P(a) is true.
• Nonconstructive existence proof: A proof that an element with a specified property exists that does not explicitly find such an element.
• that is, we do not find an element a such that P(a) is true, but rather prove that $\exists\, xP(x)$ is true in some other way(contradiction)

10 Uniqueness Proof

Some theorems assert that there is exactly one element with this property.
• The two parts of a uniqueness proof are:
Existence: an element x with the desired property exists.
Uniqueness: if y= x, then y does not have the desired property.