Discrete Mathematics 27/7/2018

Lecture 3: Proof Techniques

Instructor: Sourav Chakraborty *Scribe: Arpan Kumar Bag*

1 Proof Techniques

The proof techniques that we are going to use in this course are

- Constructive proof
- Contrapositive
- Contradiction
- Induction
- Counter example

Constructive Proof can be further categorized into two type.

- Direct Proof
- Case studies

Now let we have to prove $A \implies B$ given $B = C \wedge D$. Then

$$(A \implies C \wedge D) \equiv (A \implies C) \wedge (A \implies D).$$

So we can split the problem into smaller parts then we can solve the problem by solving the smaller parts. We can also ignore the redundant assumptions.Let $A = C \wedge D; C \implies B$.Then we get

$$(C \wedge D \implies B) \equiv (A \implies B).$$

Example: If b is an odd prime then prove that $2b^2 \geq (b+1)^2$ and $b^2 \equiv 1 \bmod 4$.

Solution: To prove the 1st part of the problem notice that if $b \geq 3$ then the statement holds true. Here we do not need b to be prime or odd.

$$b \geq 3 \implies b - 1 \geq 2 \implies (b-1)^2 \geq 4.$$

$$b^2 - 2b + 1 \geq 2 \implies b^2 \geq 2b + 1 \implies 2b^2 \geq b^2 + 2b + 1$$

$$2b^2 \geq 2b + 1.$$

It is not always easy to see the redundant assumptions. So one can also use backward steps to see this. So we start with the statement that we have to prove and get a easier version of that problem. For this problem

$$2b^2 \geq (b+1)^2 \implies 2b^2 \geq b^2 + 2b + 1 \implies b^2 \geq 2b + 1.$$

$$b^2 - 2b + 1 \geq 2 \implies (b-1)^2 \geq 2 \implies (b-1)^2 \geq 4$$

$$b - 1 \geq 2 \implies b \geq 3$$

For 2nd part of the problem b need not to be an odd prime for this result. If b is odd then the result follows because if b is odd then both $b-1$ and $b+1$ is divisible by 2.

1.1 Constructive Proof

Constructive proof is a technique where we use some known facts or results to prove the statement. There are two types of constructive proof.

1.1.1 Direct proof

As the name suggests,in this method we directly prove the statement by some results or known facts.

1.1.2 Case studies

In this type we break the statement into smaller parts and prove the statement by proving the smaller parts.
Example: If p is prime ≥ 5 then prove that $p^2 \equiv 1 \bmod 6$

Solution: Here we can divide the problem into 6 subcases.

$$p \equiv i \bmod 6 \ \ where\, i = 0, 1, 2, 3, 4, 5$$

For $i = 0, 2, 3, 4$ p is composite because for $i = 0$, p is divisible by 6, for $i = 2, p$ can be written as $6k+2$ for some natural number k. Similarly for $i = 3, 4$ p is not prime. So we just have to consider the cases for $i = 1, 5$. For $i = 1$ we can write p as $6k + 1$ for some natural number k. Then

$$p^2 = 36k^2 + 12k + 1 \implies p^2 \equiv 1 \bmod 6.$$

Similarly we can prove for $i = 5$. Hence the statement follows.

1.2 Contrapositive

In this method we try to prove the negation of the actual statement.We know that

$$A \implies B \equiv \neg B \implies \neg A$$

.If $B = C \vee D$ then

$$\neg B = \neg C \wedge \neg D.$$

So we can prove for $\neg C$ and $\neg D$ and ultimately prove the statement.

1.3 Contradiction

In this form of proof we start by assuming that the opposite of the statement is true and then we try to show that the assumption leads to a contradiction. In the following example we are using both the contrapositive and contradiction method.

Example: If a, b is rational then prove that either $a\ and\ b$ are both rational or both irrational.

Solution: The contapositive of this statement is if a is rational and b is irrational then ab is not rational. Now we are going to use contradiction method. Let ab be rational.Since $a\ and\ ab$ are rational we can take $a = \frac{p}{q}\ and\ ab = \frac{r}{s}$ where p, q, r, s are some integers. Now

$$a = \frac{p}{q}\ and\ ab = \frac{r}{s} \implies b = \frac{qr}{ps}$$

a contradiction to our assumption that b is irrational. Hence the contrapositive statement follows and so our main statement also follows.
Now we are going to give another example of the Contradiction method.

Example: Prove that real numbers are uncountable.

Solution: Let $\mathbb{R}$ is countable . Then there exist a bijective function $f : \mathbb{R} \to S$ where $S \subseteq \mathbb{N}$. Since $\mathbb{N}$ is a well ordered set then any subset of $\mathbb{N}$ will have a minimum element. Let r_1 be $f^{-1}(min(S))$. Similarly let r_2=$f^{-1}(min(S - f(r_1)))$ and so on. So we have the relation $f(r_1) < f(r_2) < f(r_3)$..... Now we are going to prove that $\mathbb{R} \cap (0, 1)$ is uncountable. Let

$$r_1 = 0.r_{11}r_{12}r_{13}....$$

$$r_2 = 0.r_{21}r_{22}r_{23}....$$

$$r_3 = 0.r_{31}r_{32}r_{33}....$$

$$.... \quad .... \quad ....$$

Where $0 \leq r_{ij} \leq 9$
By our assumption every real no. in $(0, 1)$ have a place in the enumeration. r_1, r_2, r_3.....Now let us consider the real number $p = 0.p_1p_2p_3$..... such that

$$p_k = (r_{kk} + 1) \bmod 9.$$

Now p is different from each r_i in the ith decimal place. Therefore p does not belong to r_1, r_2....., a contradiction. There $(0, 1)$ is uncountable. Therefore $\mathbb{R}$ is uncountable.

Note: The above process is called the Cantor's Diagonal method.