CS 2050 Discrete Mathematics January 18th 2024

Lecture 6: More on Proof

Lecturer: Abrahim Ladha

1 Universes of Discourse

Without defining what a set is, we implement some common notation for the universes of discourse.

- The Naturals $\mathbb{N} = 0, 1, 2, 3, ...$
- The Integers $\mathbb{Z} = ..., -2, -1, 0, 1, 2, ...$
- The Rationals $\mathbb{Q} = a/b$ where a, b are any integer but b isn't zero.
- The Irrationals $\mathbb{I}$ any quantity which isn't rational
- The Reals $\mathbb{R} =$ any number with any decimal expansion. Every real is either rational or irrational.
- The Complex Numbers $\mathbb{C} = a + bi$ where a, b are any reals and $i^2 = -1$.

2 Exhaustive Proof

Suppose we want to prove a statement of the form $\forall x P(x)$. If we are lucky enough that the universe of discourse of x is finite, then we may simply prove it for each x. If x can only be one of a, b, c, d, then $\forall x P(x) = P(a) \wedge P(b) \wedge P(c) \wedge P(d)$ Lets do a simple example

Theorem 1. If n is a number between two and four, then $n^2 > n$

Proof. We confirm that $2^2 = 4 > 2$ and $3^2 = 9 > 3$ and $4^2 = 16 > 4$. □

This obviously doesn't work in the case that the universe of discourse is infinite. You are not allowed to have an infinitely long proof. A proof of $\forall x P(x)$ must itself be of finite length, but assert something which is true for infinitely many values of x.

3 Proof by Cases

A theorem may require a trickier proof, in that it may need to be decomposed into *cases*. If you wish to prove a statement of the form $(p_1 \vee ... \vee p_k) \implies q$, it is equivalent to prove $(p_1 \implies q) \wedge ... \wedge (p_k \implies q)$. For example, if you wish to prove a statement about all numbers, you may do it into cases, one case with the assumption that your number is even, and another case with the assumption that your number is odd.

Theorem 2. If n is any number, then $n^2 + n$ is even.

Proof. Let n be any number. Then we have two cases.

Case 1: If n is even, then $n = 2k$ for some k. Then $n^2 + n = 4k^2 + 2k = 2(2k^2 + 1)$ which is even.

Case 2: If n is odd, then $n = 2k + 1$ for some k. Then $n^2 + n = 4k^2 + 4k + 1 + 2k + 1 = 2(2k^2 + 3k + 1)$ which is even. □

Note that when you break your problem into cases, they must cover the entire universe of discourse. If you wish to prove something is true for any integer of $\mathbb{Z}$, it is not sufficient to prove it in the cases that $x > 0$ and $x < 0$, since you have not covered the case that $x = 0$. Famously, the four color theorem was proved by checking nearly two thousand cases. Along with a proof of each case, they have to provide a proof that the those were the only cases.

4 Without Loss of Generality

Sometimes, a theorem doesn't need multiple cases if the cases are all the same. For example, suppose you were to prove "If x, y have opposite parity then xy is even". You don't need to split this into the two cases that x even y odd and x odd y even. Since $xy = yx$, you may simply say "by loss of generality, suppose x is even and y is odd". Each case is simply a relabeling of the other where you swap what x and y are called.

5 Infinitely Many Primes

This is a cool proof, couldn't figure out where else to show it so its goes here

Theorem 3 (Euclid's Theorem)**.** There are infinitely many primes.

Proof. Assume to the contrary there are only finitely many prime numbers. Then there are only finitely many primes $p_1, p_2, ..., p_k$ where p_i denotes the ith prime number. Consider the number

$$n = (p_1 \cdot p_2 \cdot ... \cdot p_k) + 1$$

Note that n is not equal to any of the finitely many primes, so by assumption, it must not be prime, but be composite. Then it has a prime divisor p, which must be one of $p_1, ..., p_k$. But then p divides $P = p_1 \cdot ... \cdot p_k$ and p divides $n = (p_1 \cdot p_2 \cdot ... \cdot p_k) + 1$. So p divides $n - P = (p_1 \cdot p_2 \cdot ... \cdot p_k) + 1 - (p_1 \cdot p_2 \cdot ... \cdot p_k) = 1$. But no prime number divides 1, a contradiction. □

6 Non-constructive Proof

Suppose we want to prove a statement of the form $\exists x P(x)$. We may simply find a value x from its universe of discourse which satisfies the predicate P. As it turns out, this is not necessary. You can prove something to exist *without knowing what it is.* Again, we witness the power of proof.

Theorem 4. Some digit of $\pi = 3.14...$ appears infinitely often.

Proof. Suppose not. Then every digit of π appears only finitely many times. Then the decimal expansion of π must terminate, which would imply that π is a rational, contradiction. □

Observe how we used the fact that decimal numbers which terminate must be rational. Any terminating decimal of the form 1.23 may be written as $1 + \frac{23}{100}$. Next, note that this proof established that a digit of π does appear infinitely often. It didn't establish which digit, or how often, or where it appears. It simply established exactly and only what it stated. It didn't give us any method to even determine what digit appears infinitely often. This is why we may denote the proof as *non-constructive.*

Theorem 5. There exists rational numbers a, b such that a^b is rational.

This result should surprise you. If a, b are irrationals, it turns out, you would be wrong to expect that a^b is also irrational.

The proof should surprise you even more. It doesn't won't tell us for which irrational numbers a, b is the theorem true, or even one example. But it does simply assert such a pair of irrationals must exist.

Proof. Consider $\sqrt{2}^{\sqrt{2}}$. We have two cases, whether or not that $\sqrt{2}^{\sqrt{2}}$ is rational or irrational.

- Case 1: If $\sqrt{2}^{\sqrt{2}}$ is rational, then $a = b = \sqrt{2}$ and we are done.
- If $\sqrt{2}^{\sqrt{2}}$ is irrational, then $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$

$$a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2}\sqrt{2}} = (\sqrt{2})^2 = 2$$

In either case, we have asserted that there exist irrational a, b such that a^b is rational. □

For the proof, we don't even know if $\sqrt{2}^{\sqrt{2}}$ is rational or irrational! Yet in either case, we may assert the existence of irrationals a, b with the property that a^b is rational. One of the pairs $a, b = \sqrt{2}, \sqrt{2}$ or $a, b = \sqrt{2}^{\sqrt{2}}, \sqrt{2}$ must work. We don't know which, but we know it must be one of them!