CS70 – SPRING 2026

LECTURE 2 : JAN. 22

Previous Lecture

- Propositions
- Connectives $\wedge \quad \vee \quad \neg \quad \Rightarrow \quad \Leftrightarrow$
- Truth tables ; logical equivalence $\equiv$
- Implications

$$P \Rightarrow Q \quad \equiv \quad \neg Q \Rightarrow \neg P \qquad \text{(contrapositive)}$$

$$\not\equiv \quad Q \Rightarrow P \qquad \text{(converse)}$$

- Predicates & Quantifiers :

$$\forall x\, P(x) \qquad\qquad \exists x\, P(x)$$

- De Morgan's Laws :

$$\neg \forall x\, P(x) \equiv \exists x\, (\neg P(x)) \qquad \neg \exists x\, P(x) \equiv \forall x\, (\neg P(x))$$

Today : Proofs

Goals:

- Clearly specify our claims (e.g., about behavior of programs or systems)
- Convince ourselves & others that these claims are valid

Q: What is a proof ?

A: A sequence of statements (propositions), each of which follows from the preceding ones by a valid law of reasoning

A proof may also use basic facts we assume without proof (axioms) and other facts we've already proved (lemmas)

Keep in mind:

- Proofs are a "social process" — a contract between the prover and the reader

- Writing good proofs is an art (like writing good code)

Proof Techniques

1. Direct proof
2. Proof by contraposition
3. Proof by contradiction
4. Proof by cases
5. Proof by induction ← next lecture

1. Direct Proof

Goal: Prove $P \Rightarrow Q$

Approach: Assume P

$\vdots$

logical steps / axioms / lemmas

Therefore Q $\square$

Theorem: For any integers a, b, c with $a \neq 0$, if $a \mid b$ and $a \mid c$ then $a \mid (b+c)$

Proof: Let a, b, c be arbitrary integers with $a \neq 0$

Assume $a \mid b$ and $a \mid c$

Then $b = aq_1$ and $c = aq_2$ for integers q_1, q_2

Hence
$$b + c = aq_1 + aq_2 = a(q_1 + q_2)$$

Since $q_1 + q_2$ is an integer, this implies $a \mid (b+c)$ $\square$

Note: Same proof shows that also $a \mid (b-c)$ (Exercise)

Example: Divisibility by 11

E.g.: $23738 \longrightarrow 2373 - 8 = 2365$

$\longrightarrow 236 - 5 = 231$

$\longrightarrow 23 - 1 = 22$

$\longrightarrow 2 - 2 = 0$ ✓

"Delete last digit & subtract it from remaining number"

Denote by reduce(n) the number obtained from n by this rule

Claim: n is divisible by 11 $\iff$ reduce(n) is divisible by 11

Theorem: For any integer $n \geq 10$, $11 \mid n \iff 11 \mid \text{reduce}(n)$

Proof: Need to prove two things:

(i) $\forall n \geq 10, \quad 11 \mid n \implies 11 \mid \text{reduce}(n)$

(ii) $\forall n \geq 10, \quad 11 \mid \text{reduce}(n) \implies 11 \mid n$

Proof of (i): Assume $11 \mid n$

Write n as $\overset{\text{other digits}}{\underbrace{\quad n' \quad}} \ \overset{\text{last digit}}{d}$

$$\text{reduce}(n) = n' - d \qquad ①$$

$$n = 10n' + d \qquad ②$$

Add ① + ②: $\text{reduce}(n) + n = 11n'$

Thus $11 \mid (\text{reduce}(n) + n)$

Since also $11 \mid n$, know that $11 \mid \text{reduce}(n)$

[by previous Theorem, used here as a Lemma]

Theorem: For any integer $n \geq 10$, $11 | n \iff 11 | \text{reduce}(n)$

Proof: Need to prove two things:

(i) $\forall n \geq 10, \quad 11 | n \Rightarrow 11 | \text{reduce}(n)$

(ii) $\forall n \geq 10, \quad 11 | \text{reduce}(n) \Rightarrow 11 | n$

Proof of (ii): Assume $11 | \text{reduce}(n)$

Exactly as before, $11 | (\text{reduce}(n) + n)$

Thus $11 | n$ $\square$

Theorem: For any integer $n \geq 1$, $n^3 - n$ is divisible by 6

Proof: Factorize: $n^3 - n = n(n^2-1) = n(n+1)(n-1)$

Now notice that for any $n \geq 1$, $n-1, n, n+1$ are <u>consecutive</u> non-negative integers.

So they include one multiple of 3 and (at least) one multiple of 2.

Hence their product $n(n+1)(n-1)$ is divisible by 2 and by 3, and hence by 6. $\square$

Examples:
$n=1$: $n^3-n = 0 \times 1 \times 2 = 0$
$n=2$: $n^3-n = 1 \times 2 \times 3 = 6$
$n=3$: $n^3-n = 2 \times 3 \times 4 = 24$ ...etc.

Proof by Contraposition

Goal: Prove $P \Rightarrow Q$

Recall: $P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$

Approach:

Assume $\neg Q$

$\cdot$

$\cdot$

$\cdot$

$\cdot$

logical steps/ axioms/ lemmas

Therefore $\neg P$

Hence $P \Rightarrow Q$ $\square$

Theorem: Let n be an integer. If n^2-4n+7 is even then n is odd.

Proof: By contraposition

Assume n is even & prove that n^2-4n+7 is odd

$$\underbrace{n^2}_{\text{even}} - \underbrace{4n}_{\text{even}} + \underbrace{7}_{\text{odd}} \text{ is odd} \qquad \square$$

Moral: Easier to work "backwards" from n than forwards from n^2-4n+7

Theorem: For a real number x, if $x^3 - x > 0$ then $x > -1$.

Proof: By contraposition.

Assume $x \leq -1$ & prove that $x^3 - x \leq 0$

Then $x^3 - x = \underbrace{x}_{<0}\underbrace{(x^2 - 1)}_{\geq 0} \leq 0$ $\square$

Proof by Contradiction "Reductio ad absurdum"

Goal: Prove P

Approach:

Assume $\neg P$

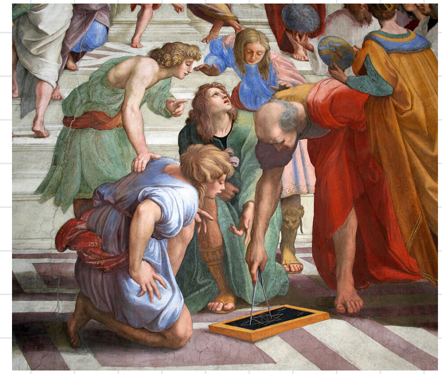
$\vdots \qquad\qquad \vdots$

Therefore $R \qquad$ Therefore $\neg R$

Since $\neg P \Rightarrow (R \land \neg R) \equiv$ False,

P must be True. $\square$

Theorem [Euclid]: There are infinitely many primes.



Proof: By contradiction: Assume there are only finitely many primes.

Call them $p_1, p_2, \ldots, p_k$

Define $q := p_1 p_2 \cdots p_k + 1$

Then q is <u>not</u> prime

R Therefore q has a prime divisor $d > 1$

By our assumption, $d = p_i$ for some $1 \leq i \leq k$

Hence $d \mid (q-1)$ and $d \mid q$

$\neg R$ So $d \mid 1$ i.e. $d = 1$ $\times$

Hence initial assumption was false, i.e., $\exists$ infinitely many primes $\square$

Theorem: $\sqrt{2}$ is irrational

Proof: Assume for ※ that $\sqrt{2}$ is rational.

Then $\sqrt{2} = \frac{a}{b}$ for integers a, b that have no common factors and $b \neq 0$

Lemma: If a^2 is even then a is even

prove by contraposition (Exercise)

Squaring: $2 = \frac{a^2}{b^2}$, hence $2b^2 = a^2$

Hence a^2 is even, so a is even (by Lemma)

So can write $a = 2c$ for integer c

So $a^2 = 2b^2 \Rightarrow 4c^2 = 2b^2$

$\Rightarrow 2c^2 = b^2$

$\Rightarrow b^2$ is even

$\Rightarrow b$ is even (by Lemma)

Hence a, b share common factor 2 ※ $\square$

Proof by Cases

Goal: Prove P

Approach:

Case 1

$\vdots$

P

Case 2

$\vdots$

P

$\vdots$

Case K

$\vdots$

P

P holds in all cases, so P is True $\square$

Theorem: For all real x, $|x+3| - x \geqslant 3$

Proof: **Case (i)** $x \geqslant -3$

$|x+3| - x = x+3-x = 3 \geqslant 3$ ✓

Case (ii) $x < -3$

$x < -3 \Rightarrow 2x < -6$

$\Rightarrow -2x > 6$

$$
\begin{aligned}
|x+3| - x &= -(x+3) - x = -3 - 2x \\
&> -3 + 6 \\
&= 3
\end{aligned}
$$
✓

$\square$

Theorem: There exist irrational numbers x, y s.t. x^y is rational.

Proof: By cases

Case (i): $\sqrt{2}^{\sqrt{2}}$ is rational — DONE by taking $x = y = \sqrt{2}$ ✓

Case (ii): $\sqrt{2}^{\sqrt{2}}$ is irrational

Take $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$

Then $x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = (\sqrt{2})^2 = 2$, rational! ✓

$\square$

Non-constructive Proof: doesn't tell us whether $\sqrt{2}^{\sqrt{2}}$ is rational! (but we don't need to know this for the proof since we've handled both cases)

Note: In fact, $\sqrt{2}^{\sqrt{2}}$ is irrational, but this is much harder to prove!

Proof Fails

Example 1

"Theorem": $2 = 0$

"Proof": Let $x = y = 1$

Since $x = y$, we have $x^2 - y^2 = 0$

Factorizing: $(x+y)(x-y) = 0$

Dividing both sides by $(x-y)$: $x+y = 0$

But $x=y=1$, so we have $2 = 0$ $\square$

$x-y=0$!

Example 2

"Theorem": $2 = 1$

"Proof": Clearly $4 - 6 = 1 - 3$

Add $9/4$ to both sides:

$$4 - 6 + 9/4 = 1 - 3 + 9/4$$

Both sides are perfect squares:

$$(2 - 3/2)^2 = (1 - 3/2)^2$$

Taking square roots:

$$2 - 3/2 = 1 - 3/2$$

Adding $3/2$ to both sides:

$$2 = 1 \qquad \square$$

$a^2 = b^2$

$\Rightarrow |a| = |b|$

$[\not\Rightarrow a = b]$

Example 3

"Theorem": $9 < 4$

$a < b \not\Rightarrow a^2 < b^2$

"Proof": Clearly $-3 < 2$

Squaring both sides:

$9 < 4$ $\square$

Example 4

"Theorem": For any positive real x, $x+\frac{1}{x} \geqslant 4$

"Proof": Assuming $x+\frac{1}{x} \geqslant 4$, since $x>0$ we can multiply both sides by x to get

$$x^2+1 \geqslant 4x$$

Hence $(x-2)^2 \geqslant 0$

This is true for any real x.

Hence $x+\frac{1}{x} \geqslant 4$ for all pos. real x $\square$

Summary

- Proof types:
  - Direct Proof
  - Proof by Contraposition
  - Proof by Contradiction
  - Proof by Cases

- Some common pitfalls

- Next lecture: Proof by Induction