CS70: Proofs Today!!!

Woohoo!!

Propositional Logic Identities.

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

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

$$\neg (P \land Q) \equiv \neg P \lor \neg Q$$

$$\neg (P \land Q) \equiv \neg P \lor \neg Q$$

$$P \Rightarrow Q \equiv \neg P \Rightarrow \neg Q$$

contrapositive.

$$P \Rightarrow Q \equiv \neg P \lor Q$$

P is antecedent or assumption.

Q is consequent or conclusion.

CS70: Lecture 2. Outline.

Today: Proofs!!!

1. By Example.
2. Direct. (Prove $$P \Rightarrow Q$$.)
3. by Contraposition (Prove $$P \Rightarrow Q$$)
4. by Contradiction (Prove $$P$$)
5. by Cases
If time: discuss induction.

Direct Proof.

Theorem: For any $$a, b, c \in \mathbb{Z}$$, if $$a | b$$ and $$a | c$$ then $$a | (b - c)$$.

Proof: Assume $$a | b$$ and $$a | c$$

$$b = aq$$ and $$c = aq'$$ where $$q, q' \in \mathbb{Z}$$

$$b - c = aq - aq' = a(q - q')$$ Done?

$$a | (b - c)$$ is an integer so

$$a | (b - c)$$

Works for $$\forall a, b, c$$?

Argument applies to every $$a, b, c \in \mathbb{Z}$$.

Direct Proof Form:

Goal: $$P \Rightarrow Q$$

Assume $$P$$.

... Therefore $$Q$$.

Quick Background and Notation.

Integers closed under addition.

$$a, b \in \mathbb{Z} \Rightarrow a + b \in \mathbb{Z}$$

$$a | b$$ means “$$a$$ divides $$b$$”.

2|4? Yes! Since for $$q = 2, 4 = (2)(2)$$.

7|23? No! No q where true.

4|2? No!

Formally: $$a | b \iff \exists q \in \mathbb{Z}$$ where $$b = aq$$.

3|15 since for $$q = 5, 15 = 3(5)$$.

A natural number $$p > 1$$, is prime if it is divisible only by 1 and itself.

Review puzzle

Theory: If you drink alcohol you must be at least 18.

Which cards do you turn over?

Write implication and contraposition:

Drink $$= \Rightarrow " \geq 18"$$

"< 18" $$= \Rightarrow$$ Don't Drink.

It's easier now. At least for me.
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Thm: For $n \in D_3$, if alternating sum of digits of $n$ divisible by 11, then $11 \mid n$.

\[
\forall n \in D_3, \ (11 \mid \text{alt. sum of digits of } n) \implies 11 \mid n
\]

Examples:

- $n = 121$ Alt Sum: $1 - 2 + 1 = 0$. Divis. by 11. As is 121.
- $n = 605$ Alt Sum: $6 - 0 + 5 = 11$ Divis. by 11. As is 605 $= 11(55)$

Proof: For $n \in D_3$, $n = 100a + 10b + c$, for some $a, b, c$.

Assume: Alt. sum: $a - b + c = 11k$ for some integer $k$.

Add $99a + 11b$ to both sides.

$100a + 10b + c = 11k + 99a + 11b = 11(k + 9a + b)$

Left hand side is $n$, $k + 9a + b$ is integer. $\implies 11 \mid n$.

Direct proof of $P \implies Q$.

Assumed $P$: $11(a - b + c)$. Proved $Q$: $11 \mid n$.

---

The Converse

Another direct proof.

Theorem: $\forall n \in D_3, (11 \mid \text{alt. sum of digits of } n) \implies 11 \mid n$

Is converse a theorem?

$\forall n \in D_3, (11 \mid n) \implies (11 \mid \text{alt. sum of digits of } n)$

Yes? No?

---

Another Contraposition...

Lemma: For every $n$ in $N$, $n^2$ is even $\implies n$ is even. ($P \implies Q$)

$n^2$ is even, $n^2 = 2k, \ldots \sqrt{2k}$ even?

Proof by contraposition: ($P \implies Q$) $\equiv (\neg Q \implies \neg P)$

$P = 'n^2$ is even.' and $\neg P = 'n^2$ is odd'

$Q = 'n$ is even' and $\neg Q = 'n$ is odd'

Prove $\neg Q \implies \neg P$: $n$ is odd $\implies n^2$ is odd.

$n = 2k + 1$

$n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

$n^2 = 2l + 1$ where $l$ is a natural number.

... and $n^2$ is odd!

$\neg Q \implies \neg P$ so $P \implies Q$ and ...

---

Proof by contradiction:form

Theorem: $\sqrt{2}$ is irrational.

Must show: For every $a, b \in Z$, $(\frac{a}{b})^2 \neq 2$.

A simple property (equality) should always "not" hold.

Proof by contradiction:

Theorem: $P$.

$\neg P \implies P_1 \implies R$

$\neg P \implies Q_1 \implies \neg R$

$\neg P \implies R \land \neg R \equiv False$

or $\neg P \equiv False$

Contrapositive of $\neg P \equiv False$ is $True \implies P$.

Theorem $P$ is proven.
**Theorem:** \( \sqrt{2} \) is irrational.

Assume \(-P:\ \sqrt{2} = a/b \) for \( a,b \in \mathbb{Z} \).

Reduced form: \( a \) and \( b \) have no common factors.

\[ \sqrt{2}b = a \]

\[ 2b^2 = a^2 = 4k^2 \]

\( a^2 \) is even \( \implies a \) is even.

\[ a = 2k \text{ for some integer } k \]

\[ b^2 = 2k^2 \]

\( b^2 \) is even \( \implies b \) is even.

\( a \) and \( b \) have a common factor. Contradiction.

**Proof by cases.**

**Theorem:** \( x^5 - x + 1 = 0 \) has no solution in the rationals.

**Proof:** First a lemma...

**Lemma:** If \( x \) is a solution to \( x^5 - x + 1 = 0 \) and \( x = a/b \) for \( a,b \in \mathbb{Z} \), then both \( a \) and \( b \) are even.

Reduced form \( \frac{a}{b} \): \( a \) and \( b \) can’t both be even! + Lemma \( \implies \) no rational solution.

**Proof of lemma:** Assume a solution of the form \( a/b \).

\[ \left( \frac{a}{b} \right)^5 - \frac{a}{b} + 1 = 0 \]

Multiply by \( b^5 \):

\[ a^5 - ab^4 + b^5 = 0 \]

Case 1: \( a \) odd, \( b \) odd: odd - odd + odd = even. Not possible.

Case 2: \( a \) even, \( b \) odd: even - even + odd = even. Not possible.

Case 3: \( a \) odd, \( b \) even: odd - even + even = even. Not possible.

Case 4: \( a \) even, \( b \) even: even - even + even = even. Possible.

The fourth case is the only one possible, so the lemma follows.

**Proof by contradiction:** example

**Theorem:** There are infinitely many primes.

**Proof:**

- Assume finitely many primes: \( p_1, \ldots, p_k \).
- Consider number

\[ q = (p_1 \times p_2 \times \cdots p_k) + 1. \]

- \( q \) cannot be one of the primes as it is larger than any \( p_i \).
- \( q \) has prime divisor \( p \) (\( p > 1 \equiv R \)) which is one of \( p_i \).
- \( p \) divides both \( x = p_1 \times p_2 \times p_3 \) and \( q \), and divides \( q - x \).

\[ \implies p|q-x \implies p \leq q - x = 1. \]

- \( \implies p \leq 1. \text{ (Contradicts } R) \)

The original assumption that “the theorem is false” is false, thus the theorem is proven.

**Proof by cases.**

**Theorem:** There exist irrational \( x \) and \( y \) such that \( xy \) is rational.

Let \( x = y = \sqrt{2} \).

Case 1: \( xy = \sqrt{2} \cdot \sqrt{2} \) is rational. Done!

Case 2: \( \sqrt{2} \cdot \sqrt{2} \) is irrational.

- New values: \( x = \sqrt{2} \cdot \sqrt{2}, \ y = \sqrt{2} \)

- \( x^2 = (\sqrt{2} \cdot \sqrt{2})^2 = \sqrt{2}^2 \cdot \sqrt{2}^2 = \sqrt{2}^2 \cdot 2 = 2. \)

Thus, we have irrational \( x \) and \( y \) with a rational \( x^2 \) (i.e., 2).

One of the cases is true so theorem holds.

Question: Which case holds? Don’t know!!

**Product of first \( k \) primes.**

**Did we prove?**

- “The product of the first \( k \) primes plus 1 is prime.”
- No.
- The chain of reasoning started with a false statement.

Consider example..

\[ 2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509 \]

- There is a prime in between 13 and \( q = 30031 \) that divides \( q \).
- Proof assumed no primes in between \( p_i \) and \( q \).

**Be careful.**

**Theorem:** \( 3 = 4 \)

**Proof:** Assume \( 3 = 4 \).

Start with \( 12 = 12 \).

Divide one side by 3 and the other by 4 to get \( 4 = 3 \).

By commutativity theorem holds.

Don’t assume what you want to prove!
Be really careful!

Theorem: 1 = 2
Proof: For x = y, we have
(x^2 - xy) = x^2 - y^2
x(x - y) = (x + y)(x - y)
x = 2x
1 = 2
Dividing by zero is no good.

P \implies Q does not mean Q \implies P.
Multiplying both sides of an equation by zero keeps it an equation.
Indeed: multiplying both sides of a wrong equation makes it right.
Also: Multiplying inequalities by a negative.

The natural numbers.

CS70: Note 3. Induction!
1. The natural numbers.
2. 5 year old Gauss.
3. ..and Induction.
4. Simple Proof.

Gauss induction proof.
Theorem: For all natural numbers n, 0 + 1 + 2 + ... + n = \frac{n(n+1)}{2}
Base Case: Does 0 +0 + 1 = \frac{0(0+1)}{2}? Yes.
Induction Step: Show ∀k \geq 0, P(k) \implies P(k+1)
Induction Hypothesis: P(k) = 1 + 2 + ... + k = \frac{k(k+1)}{2}

1 + 2 + ... + k + (k+1) = \frac{k(k+1)}{2} + (k+1)
= (\frac{k}{2} + 1)(k + 1)
= (\frac{k+2}{2})(k + 1)
= \frac{(k+1)(k+2)}{2}

P(k+1)! By principle of induction...
Proof by Induction.

The canonical way of proving statements of the form

\[(\forall k \in \mathbb{N})(P(k))\]

- For all natural numbers \(n, 1 + 2 \cdots + n = \frac{n(n+1)}{2}\).
- For all \(n \in \mathbb{N}, n^2 - n\) is divisible by 3.
- The sum of the first \(n\) odd integers is a perfect square.

The basic form
- Prove \(P(0)\), “Base Case”.
- \(P(k) \implies P(k + 1)\)
  - Assume \(P(k)\), “Induction Hypothesis”
  - Prove \(P(k + 1)\), “Induction Step.”

\(P(n)\) true for all natural numbers \(n\)!!!
Get to use \(P(k)\) to prove \(P(k + 1)\)!!!