CS70: Lecture 2. Outline.

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

Review.

Theory: If you drink alcohol you must be at least 18.
Which cards do you turn over?

Drink Alcohol $\implies \geq 18$
“< 18” $\implies$ Don’t Drink Alcohol. Contrapositive.

(A) (B) (C) and/or (D)?

Propositional Forms: $\land, \lor, \neg, P \iff Q = \neg (P \lor Q)$.
Truth Table. Putting together identities. (E.g., cases, substitution.)
Predicates, $P(x)$, and quantifiers. $\forall x, P(x)$.

DeMorgan’s: $\neg (P \land Q) = \neg P \land \neg Q$. $\neg \forall x, P(x) = \exists x, \neg P(x)$.

Quick Background and Notation.

Integers closed under addition.

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

$a | b$ means “a divides b”.

2|4? Yes! Since for $q = 2, 4 = (2)2$.
7|23? No! No $q$ where true.
4|2? No!
2|−4? Yes! Since for $q = 2, −4 = (−2)2$.

Formally: for $a, b \in \mathbb{Z}, a | b \iff \exists q \in \mathbb{Z}$ 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.

A number $x$ is even if and only if $2 | x$, or $x = 2k$ for $x, k \in \mathbb{Z}$.
A number $x$ is odd if and only if $x = 2k + 1$

Correct: (B) and (E).

Last time: Existential statement.

How to prove existential statement?
Give an example. (Sometimes called “proof by example.”)

Theorem: $\exists x \in \mathbb{N}(x = x^2)$

Proof: $0 = 0^2 = 0$

Often used to disprove claim.

Homework.

Divides.

$a | b$ means
(A) There exists $k \in \mathbb{Z}$, with $a = kb$.
(B) There exists $k \in \mathbb{Z}$, with $b = ka$.
(C) There exists $k \in \mathbb{N}$, with $b = ka$.
(D) There exists $k \in \mathbb{Z}$, with $k = ab$.
(E) $a$ divides $b$

Incorrect: (C) sufficient not necessary. (A) Wrong way. (D) the product is an integer.

Correct: (B) and (E).

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 $q, q' \in \mathbb{Z}$

$b – c = a(q – q')$ (and $(q – q')$ is an integer so by definition of divides $a | (b – c)$)

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

Argument applies to every $a, b, c \in \mathbb{Z}$.
Used distributive property and definition of divides.

Direct Proof Form:

Goal: $P \implies Q$

Assume $P$.

Therefore $Q$. 
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of $n$ is divisible by 11, then 11divides $n$.

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

Examples:

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

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|n.

Another Direct Proof.

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

Is converse a theorem?

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

Yes? No?

Proof by Contraposition

Thm: For every $n$ in $Z^+$ and $d \mid n$. If $n$ is odd then $d$ is odd.

$n = kd$ and $n = 2k' + 1$ for integers $k, k'$.

What do we know about $d$?

Goal: Prove $P \implies Q$.

Assume $\neg Q$.

...and prove $\neg P$.

Conclusion: $Q \implies \neg P$ equivalent to $P \implies Q$.

Proof: Assume $\neg Q$. $d$ is even. $\neg d = 2k$.

$d \mid n$ so we have

$n = qd = q(2k) = 2(kq)$

$n$ is even. \(\neg P\)

Another Contraosition...

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

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

Proof by contraposition: \(P \implies Q\) \(\iff\) \(\neg Q \implies \neg P\)

$P$ = \(\neg P\) is even. \(\implies \neg P\) is odd

$Q$ = \(\neg P\) is even. \(\implies \neg P\) is odd

Proof - $\neg P$ = $\neg Q$: $n$ 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!

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

Another Contraosition...

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

Proof: Assume 11|n.

$n = 100a + 10b + c = 11k$ \(\implies\) 99a + 11b + (a - b + c) = 11k

\(-a - b + c = 11(k - 9a - b) \implies a - b + c = 11l\) where \(l = (k - 9a - b) \in Z\)

That is 11 alternating sum of digits.

Note: similar proof to other. In this case every \(\implies\) is \(\iff\)

Often works with arithmetic properties ...

\(\neg P = \neg Q\) when multiplying by 0.

We have.

Theorem: \(\forall n \in N^+, (11 \text{alt. sum of digits of } n) \iff (11|n)\)

Proof by contradiction: form

\[ \sqrt{2} \text{ is irrational.} \]

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:** $P.$

$\neg P = P_1 \implies R$

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

$\neg P = R \land \neg R = False$

or $\neg P \implies False$

Contraosition of $\neg P \implies False$ is True $\implies P.$

Theorem $P$ is true. And proven.
**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 \( p \) (\( p > 1 \Rightarrow R \)) which is one of \( p_i \).
- \( p \) divides both \( x = p_1 \times p_2 \times \cdots p_k \) and \( q \), and divides \( q - x \),
  
  \[ \Rightarrow p \mid (q - x) \Rightarrow p \leq (q - x) = 1. \]

- \( \therefore p \leq 1 \). (Contradicts \( R \))

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

**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.

**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:** \( a, b \) odd: \( -ab^4 \) is odd, \( a^5 \) is odd \( \implies a = b = 1 \). \( \therefore a = b = 1 \), \( \therefore a/b \) is a rational.

**Case 2:** \( a, b \) even: \( a^5 \) is even \( \implies p \leq (q - x) = 1 \).

Thus, we have irrational \( a \) and \( b \) with a rational \( x^5 \) (i.e., 2).

One of the cases is true so theorem holds.

**Poll: Odds and evens.**

\( x \) is even, \( y \) is odd.

Even numbers are divisible by 2...

Which are even?

- (A) \( x^3 \)
- (B) \( y^3 \)
- (C) \( x + 5x \)
- (D) \( ay \)
- (E) \( xy \)
- (F) \( x + y \)

A, D, E all contain a factor of 2.

\( x = 2k, \) and \( x^3 = 8k = 2(4k) \) and is even.

\( y^3 \) odd?

\( y = (2k + 1), \) \( y^3 = 8k^3 + 24k^2 + 24k + 1 = 2(4k^3 + 12k^2 + 12k) + 1 \). 

Odd times an odd?

Any power of an odd number? Odd.

Idea: \((2k + 1)^n\) has terms

(a) with the last term being 1

- (b) all other terms having a multiple of \( 2k \).

- (C) \( x + 5x \)

- (D) \( ay \)

- (E) \( xy \)

- (F) \( x + y \)

A, D, E all contain a factor of 2.

\( x = 2k, \) and \( x^3 = 8k = 2(4k) \) and is even.

\( y^3 \) odd?

\( y = (2k + 1), \) \( y^3 = 8k^3 + 24k^2 + 24k + 1 = 2(4k^3 + 12k^2 + 12k) + 1 \). 

Odd times an odd?

Any power of an odd number? Odd.

Idea: \((2k + 1)^n\) has terms

(a) with the last term being 1

**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 \( p_k \) and \( q \).

**Contradiction**

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

Assume \( \sqrt{2} = a/b \) 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 \( \Rightarrow a \) is even.

\( a = 2k \) for some integer \( k \)

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

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

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

**Contradiction**

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

Assume \( \sqrt{2} = a/b \) 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 \( \Rightarrow a \) is even.

\( a = 2k \) for some integer \( k \)

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

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

\( a \) and \( b \) have a common factor. Contradiction.
**Poll: proof review.**

Which of the following are (certainly) true?

(A) $\sqrt{2}$ is irrational.

(B) $\sqrt{2}$ is rational.

(C) $\sqrt{2}^2$ is rational or it isn’t.

(D) $(2^2)^2$ is rational.

(A), (C), (D)

(B) I don’t know.

---

**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!

---

**Poll: What is the problem?**

(A) Assumed what you were proving.

(B) No problem. Its fine.

(C) $x - y$ is zero.

(D) Can’t multiply by zero in a proof.

Dividing by zero is no good. Multiplying by zero is wierdly cool!

Also: Multiplying inequalities by a negative.

**CS70: Note 3. Induction!**

Poll. What’s the biggest number?

(A) 100

(B) 101

(C) $n+1$

(D) infinity.

(E) This is about the “recursive leap of faith.”

---

**Summary: Note 2.**

Direct Proof:

To Prove: $P \implies Q$. Assume $P$. Prove $Q$.

$a|b$ and $a|c \implies a|(b - c)$.

By Contraposition:

To Prove: $P \implies \neg Q$. Assume $\neg Q$. Prove $\neg P$.

$r^2$ is odd $\implies n$ is odd. $n$ is even $\implies r^2$ is even.

By Contradiction:

To Prove: $P \implies \neg Q$. Assume $P$. Prove False.

$\sqrt{2}$ is rational.

$\sqrt{2} = \frac{a}{b}$ with no common factors....

By Cases: informal.

Universal: show that statement holds in all cases.

Existence: used cases where one is true.

Either $\sqrt{2}$ and $\sqrt{2}$ worked.

or $\sqrt{2}$ and $\sqrt{2}^2$ worked.

Careful when proving!

Don’t assume the theorem. Divide by zero. Watch converse. ...

---

**Be really careful!**

**Theorem:** $1 = 2$

**Proof:** For $x = y$, we have

$(x^2 - x^2) = x^2 - y^2$

$x(x - y) = (x + y)(x - y)$

$x = (x + y)$

$x = 1$

$1 = 2$

Poll. What is the problem?

(A) Assumed what you were proving.

(B) No problem. Its fine.

(C) $x - y$ is zero.

(D) Can’t multiply by zero in a proof.

Dividing by zero is no good. Multiplying by zero is wierdly cool!

Also: Multiplying inequalities by a negative.

$P \implies Q$ does not mean $Q \implies P$.

---