First (half) week...

Almost Done! Yaay!

I hope you are getting into the flow.

Waitlist/concurrent enrollment.

Waitlist: in the past have gotten people in.
Can’t promise.

Concurrent Enrollment: not always accomodated.
New scheme this year makes it easier.

Keep up, send email to fa17@eecs.org to get enrolled in gradescope, etc.
Last Time: The Language of Proofs.

Propositions: Statements that are true or false.

\[ 3 > 2. \]

Propositional Forms.

\[ P \lor Q, \ P \land Q, \ \neg P, \ P \implies Q \]

Truth Tables/Logical Equivalence.

\[ \neg P \lor Q \equiv P \implies Q. \]
\[ \neg Q \implies \neg P \equiv P \implies Q. \]

Predicates:

Statements with free variables whose values determine truth.

\[ P(x) = 'x > 2. \]

Quantifiers:

\[ \forall x \in \mathbb{N}, x > 2. \]
\[ \exists x \in \mathbb{N}, x > 2. \]

Universe:


\[ \mathbb{N}, \mathbb{Z}, \mathbb{R}, \ldots \]
Back to: Wason’s experiment: 1

Theory: “If a person travels to Chicago, he/she flies.”

Suppose you see that Alice went to Baltimore, Bob drove, Charlie went to Chicago, and Donna flew.

Which cards do you need to flip to test the theory?

\[
P(x) = \text{“Person } x \text{ went to Chicago.”} \quad Q(x) = \text{“Person } x \text{ flew”}
\]

Statement/theory: \( \forall x \in \{A, B, C, D\}, P(x) \implies Q(x) \)

\( P(A) = \text{False} \). Do we care about \( Q(A) \)?

No. \( P(A) \implies Q(A) \), when \( P(A) \) is False , \( Q(A) \) can be anything.

\( Q(B) = \text{False} \). Do we care about \( P(B) \)?

Yes. \( P(B) \implies Q(B) \equiv \neg Q(B) \implies \neg P(B) \).

So \( P(Bob) \) must be False .

\( P(C) = \text{True} \). Do we care about \( Q(C) \)?

Yes. \( P(C) \implies Q(C) \) means \( Q(C) \) must be true.

\( Q(D) = \text{True} \). Do we care about \( P(D) \)?

No. \( P(D) \implies Q(D) \) holds whatever \( P(D) \) is when \( Q(D) \) is true.

Only have to turn over cards for Bob and Charlie.
More for all quantifiers examples.

- “doubling a number always makes it larger”
  
  \[(\forall x \in \mathbb{N}) (2x > x) \quad \text{False} \quad \text{Consider} \quad x = 0\]

  Can fix statement...

  \[(\forall x \in \mathbb{N}) (2x \geq x) \quad \text{True}\]

- “Square of any natural number greater than 5 is greater than 25.”

  \[(\forall x \in \mathbb{N})(x > 5 \implies x^2 > 25)\]

  Idea alert: Restrict domain using implication.

  Note that we may omit universe if clear from context.
Quantifiers... not commutative.

➤ In English: “there is a natural number that is the square of every natural number”.

\[(\exists y \in N) (\forall x \in N) (y = x^2)\] False

➤ In English: “the square of every natural number is a natural number.”

\[(\forall x \in N) (\exists y \in N) (y = x^2)\] True
Consider

\(\neg (\forall x \in S)(P(x))\),

English: there is an \(x\) in \(S\) where \(P(x)\) does not hold.

That is,

\[\neg (\forall x \in S)(P(x)) \iff \exists (x \in S)(\neg P(x)).\]

What we do in this course! We consider claims.

**Claim:** \((\forall x) P(x)\) “For all inputs \(x\) the program works.”

For **False**, find \(x\), where \(\neg P(x)\).

Counterexample.

Bad input.

Case that illustrates bug.

For **True**: prove claim! What we do in this course!
Consider

\(\neg(\exists x \in S)(P(x))\)

English: means that for all \(x\) in \(S\), \(P(x)\) does not hold.

That is,

\(\neg(\exists x \in S)(P(x)) \iff \forall(x \in S)\neg P(x)\).
Which Theorem?

Theorem: $(\forall n \in \mathbb{N}) \neg((\exists a, b, c \in \mathbb{N}) (n \geq 3 \implies a^n + b^n = c^n))$

Which Theorem?

Fermat’s Last Theorem!

Remember Special Triangles:
for $n = 2$, we have 3,4,5 and 5,7, 12 and ...

1637: Proof doesn’t fit in the margins.

1993: Wiles ...(based in part on Ribet’s Theorem)

Movie – “Nova: The Proof.”

DeMorgan Restatement:
Theorem: $\neg((\exists n \in \mathbb{N}) (\exists a, b, c \in \mathbb{N}) (n \geq 3 \implies a^n + b^n = c^n)$
Summary.

Propositions are statements that are true or false.

Propositional forms use $\land, \lor, \neg$.

Propositional forms correspond to truth tables.

Logical equivalence of forms means same truth tables.

Implication: $P \implies Q \iff \neg P \lor Q$.

Contrapositive: $\neg Q \implies \neg P$

Converse: $Q \implies P$

Predicates: Statements with “free” variables.

Quantifiers: $\forall x \ P(x), \exists y \ Q(y)$

Now can state theorems! And disprove false ones!

DeMorgans Laws: “Flip and Distribute negation”

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

$\neg \forall x \ P(x) \iff \exists x \ \neg P(x)$.

A bit dry...

Why?
From the language of Proofs...

to
Proofs.
And now: 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
Quick Background and Notation.

Integers closed under addition.
\[ a, b \in \mathbb{Z} \implies a + b \in \mathbb{Z} \]

\( a \mid b \) 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: \( a \mid b \iff \exists q \in \mathbb{Z} \text{ where } b = aq \).

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.
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 \(a|c\)

\[ b = aq \quad \text{and} \quad c = aq' \quad \text{where} \quad q, q' \in \mathbb{Z} \]

\[ b - c = aq - aq' = a(q - q') \quad \text{Done?} \]

\(b - c = a(q - q')\) and \((q - q')\) 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:** \(P \implies Q\)

**Assume** \(P\).

\[
\ldots
\]

**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 $11|n$.

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

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.  $\implies 11|n$.  $\square$

Direct proof of $P \implies Q$:
Assumed $P$: $11|a - b + c$. Proved $Q$: $11|n$. 
The Converse

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

Is converse a theorem?
$\forall n \in D_3, (11|n) \implies (11|\text{alt. sum of digits of } n)$

Yes? No?
Another Direct Proof.

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

Proof: Assume \( 11|n \).

\[
\begin{align*}
\quad n &= 100a + 10b + c = 11k \implies \\
99a + 11b + (a - b + c) &= 11k \implies \\
a - b + c &= 11k - 99a - 11b \implies \\
a - b + c &= 11(k - 9a - b) \implies \\
a - b + c &= 11\ell \quad \text{where } \ell = (k - 9a - b) \in \mathbb{Z}
\end{align*}
\]

That is \( 11|\text{alternating sum of digits} \).

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

Often works with arithmetic properties ...

...not when multiplying by 0.

We have.

Theorem: \( \forall n \in N', (11|\text{alt. sum of digits of } n) \iff (11|n) \)
Proof by Contraposition

Thm: For $n \in \mathbb{Z}^+$ and $d|n$. If $n$ is odd then $d$ is odd.

$n = 2k + 1$ what do we know about $d$?

What to do? Is it even true?

Hey, that rhymes ...and there is a pun ... colored blue.

Anyway, what to do?

Goal: Prove $P \implies Q$.

Assume $\neg Q$

...and prove $\neg P$.

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

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

$d|n$ so we have

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

$n$ is even. $\neg P$
Another Contraposition...

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

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

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

\( P = 'n^2 \) is even.’ ............ \( \neg P = 'n^2 \) is odd’

\( Q = 'n \) is even’ ............ \( \neg Q = 'n \) 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 ...
Theorem: $\sqrt{2}$ is irrational.
Must show: For every $a, b \in \mathbb{Z}$, $(\frac{a}{b})^2 \neq 2$.

A simple property (equality) should always “not” hold.

Proof by contradiction:

**Theorem:** $P$.

$\neg P \implies P_1 \cdots \implies R$

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

$\neg P \implies R \land \neg R \equiv \text{False}$

$\neg P \implies \text{False}$

Contrapositive: True $\implies P$. Theorem $P$ is proven.
Theorem: $\sqrt{2}$ is irrational.

Assume $\neg P$: $\sqrt{2} = a/b$ 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.

$a = 2k$ 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 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 $p$ (“$p > 1$” = $R$) which is one of $p_i$.
- $p$ divides both $x = p_1 \cdot p_2 \cdots p_k$ and $q$, and divides $x - q$,

  $\implies p | x - q \implies p \leq x - q = 1$. or $p|1$.

- so $p \leq 1$. (Contradicts $R$.)

The original assumption that “the theorem is false” is false, thus the theorem is proven. \qed
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 \textit{in between} 13 and \( q = 30031 \) that divides \( q \).
- Proof assumed no primes \textit{in between} \( p_k \) and \( q \).
And...

Happy Friday!
Enjoy your weekend...
...and take care.