section 8. Methods of proof of $P \rightarrow Q$.

1. Direct $P \rightarrow Q$. ("vacuous" proof, $P = F$ always).

2. Contrapositive $\neg Q \rightarrow \neg P$.
   ("trivial" proof. If $Q = T$ always).

3. Contradiction.
   - Show that $\neg P \rightarrow (r \land mr)$
     Since $\neg P = F$ thus $P = T$.
   - Show $\neg (P \rightarrow Q) \rightarrow (P \land \neg P) \lor (Q \land \neg Q)$.
     $\neg (P \rightarrow Q) \equiv P \land \neg Q$
     Since $\neg (P \rightarrow Q) = F$ thus $P \rightarrow Q = T$.

Assume $P$.

\[ \begin{array}{c}
\forall x \quad \text{all def'n, lemmas, etc associated with } P \text{ and } \neg Q \\
\hline
\vdash (P \land \neg P) \lor (Q \land \neg Q)
\end{array} \]

Sometimes direct proof of $\neg Q \rightarrow \neg P$ is simple.

Sometimes direct proof $P \rightarrow Q$ is simple.
4. Equivalence (iff) \( p \leftrightarrow q \).

Need to show (by some method of proof),
that both \( p \rightarrow q \) and \( q \rightarrow p \).

5. Exhaustive / proof by cases.

show \( p \rightarrow q \) holds for all possible classes
of arguments to \( p \) and \( q \).

e.g. \( n \in \mathbb{Z} \) is either positive, negative, neutral
\( n \in \mathbb{Z} \) is either odd or even
\( n \in \mathbb{R} \) is either rational or irrational
etc.

Aside / memory jog,

Truth table for \( \neg(p \rightarrow q) \equiv p \land \neg q \)

<table>
<thead>
<tr>
<th>P</th>
<th>Q</th>
<th>P \rightarrow Q</th>
<th>\neg(p \rightarrow q)</th>
<th>p \land \neg q</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

logically equivalent
6. Constructive existence proofs of \( \exists x \in U \exists P(x) \).
Find one \( x \in U \) for which \( P(x) = T \).

7. Nonconstructive existence proof of \( \exists x \in U \exists P(x) \).
Show there must exist an \( x \in U \) for which \( P(x) = T \).
(Typically use proof by cases to show \( x \) must exist).

- Example from Lec 7 (next page).
- Proof that the set of prime numbers is infinite.
Example of

#7: Non constructive existence proof.

Show there exists a value, but don’t have to pinpoint it.

Prove that there exists irrational x, y.

s.t. $x^y$ is rational.

Recall rational # $r = \frac{l}{m}$, where $l, m \in \mathbb{Z}$ w. no common factors.

Need an instance where $x, y$ are both irrational

but $x^y$ is rational.

Try $x = \sqrt{2}$ and $y = \sqrt{2}$

consider $x^y = \sqrt{2}^{\sqrt{2}}$

case 1: if $\sqrt{2}^{\sqrt{2}}$ is rational $\rightarrow$ done w/ existence proof.

case 2: if $\sqrt{2}^{\sqrt{2}}$ is irrational

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

$x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2$.

$(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}$ is rational.
Example of nonconstructive existence proof.

Prove the proposition

\[ Q: \text{The set of prime numbers is infinite.} \]

Thus \( \forall n \in \mathbb{Z} \) \( \exists p > n \) where \( p \) is prime and \( n \in \mathbb{Z} \)

**Proof**

Show by direct proof that \( \neg Q = F \). Thus \( Q = T \).

**Q**: There are a finite number of primes.

Let \( n \) denote the largest prime.

Let \( y = n! + 1 \). Recall \( n! = (n)(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1 \).

**Case 1**: \( y \) is prime, \( \neg Q = F \) (since \( y > n \)).

**Case 2**: \( y \) is composite (and has more than 2 factors)

\[ y = \frac{n! + 1}{1} = \frac{n(n-1)(n-2)\cdots 1 + 1}{1} \]

composite w/ factors every integer \( x \leq n \).
Factors of $y = \{1, n! + 1\}$, some additional number of factors which are greater than $n$ and primes.

If $y$ is composite $\exists p > n \implies \neg \phi(y) = \text{F.}$

**Class questions:**
- Why does a factor of $n! + 1$ have to be greater than $n$?
  \[ y' = n! = \underbrace{n \cdot (n-1) \cdot (n-2) \ldots 1}_{n \text{ factors}} \]

  - Why do two consecutive integers not share a common factor (other than 1)?

\[ y = y' + 1 \]

\[ y = y' + 1 \quad \frac{y = y'}{y' \neq \mathbb{Z}} \]

**Ideas discussed**

\[ y' + 1 \]

\[ y' \]

\[ m = n + 1 \]

\[ \frac{y' + 1}{y'} = 1 + \frac{1}{y'} = 1 + \frac{1}{n \cdot (n+1) \cdot (n-2) \ldots 1} \]

... the number theory to show this next lecture...
Proof by contradiction that for all \( x \in \mathbb{R} \),
the mapping \( \sqrt{x^2} \) is not a function.

\[
P := \forall x \in \mathbb{R} \ (\sqrt{x^2} \text{ is not a function})
\]

Recall argument form: \( \forall P \rightarrow (r \land \neg r) \)

Definition of a function:

\[
r = \text{every } a \in A \text{ is mapped onto one } b \in B.
\]

\( b \) does not have to be unique to \( a \).

Assert: \( \forall P \equiv \sqrt{x^2} \text{ is a function for } x \in \mathbb{R} \rightarrow r. \)

\[
\sqrt{x^2} = \pm x \ \text{ for } x \in \mathbb{R}, \rightarrow \neg r
\]

\[\therefore (r \land \neg r)\]
A sequence is an ordered list
\[ S = \{a_0, a_1, a_2, \ldots a_n\} \]

\( a_j \) is the \( j \)th element.

\( a \) is just a variable name.
\[ S' = \{b_0, b_1, b_2, \ldots b_n\} \]

\( b_j \) is the \( j \)th element.

Typically \( j \in \mathbb{N} = \{0, 1, 2, 3, \ldots\} \)

but often \( j \in \mathbb{Z^+} = \{1, 2, 3, \ldots\} \).

A sequence: the order of appearance and repetition of elements matters (unlike a set).

Overload of notation! (curly brackets "context clarifies")

Set, \( T = \{e_1, e_2, \ldots e_n\} \)
where \( e_j \neq e_i \) if \( i \neq j \)

sequence \( S' = \{a_0, a_1, a_2, \ldots\} \)
but \( a_1 \) can be equal to \( a_2 \).