Overview

- HW#1 Due Now & Pick up HW2 handout!
- Last lecture: Sets Completed (keep coming back...)
  - Proof by cases, Proof by using existing rules
  - Basic counting theorems
  - Principle of inclusion and exclusion
- Today's lecture: General Proof Techniques
  - Proof Techniques
  - Proof by Exhaustion
  - Proof by Counter Example
  - Proof by Contraposition
  - Proof by Contradiction

Chapter 1.2 : Proof Techniques
### Review some set proof templates

- \( x \in A \): show that \( x \) has all membership properties of \( A \)
- \( A \subseteq B \): show that every element of \( A \) is also in \( B \).
- \( A \subset B \): show \( A \subseteq B \) and also some element \( x \) of \( B \) is not in \( A \)
- \( A = B \): show that \( A \subseteq B \) and \( B \subseteq A \)
- \( A \not= B \): show that \( A \not\subseteq B \) or \( B \not\subseteq A \) by showing some element \( x \) of \( A \) or \( B \) is not in \( B \) or \( A \)
- \( A \rightarrow B \): suppose \( A \) is true then derive \( B \): “if \( A \), then \( B \)”
- \( A \leftrightarrow B \): show that \( A \rightarrow B \) and \( B \rightarrow A \)
- **Proof by Cases: Make Membership Tables**
- **Proof by Using Existing Rules: Deductive Proof with Set Identities**

### Six general proof techniques

1) **Exhaustive Proof**: (to prove \( P \) is true),
   - Show that all possible cases for \( P \) are true, (only for finite cases)
2) **Direct Proof**: to prove \( P \rightarrow Q \) is true (if \( P \) is true, then \( Q \) is true),
   - Show that, suppose \( P \) is true, then **deduce** \( Q \). (deductive)
3) **Contraposition**: to prove \( P \rightarrow Q \) is true
   - Show \( Q' \rightarrow P' \) (not \( Q \) implies not \( P \)) (indirect proof)
4) **Contradiction**: to prove \( P \rightarrow Q \) is true,
   - Show \( P \) and \( Q' \rightarrow \) (contradiction):
     - Assume both the hypothesis (\( P \)) and the negation of the conclusion (not \( Q \)) are true, then try to deduce some contradiction from this assumption.
5) **Counterexample**: to disprove something

6) **Induction**: to prove that $P(n)$ is true for all $n$,

Use the principle of mathematical induction:

- **Base case**: $P(1)$ or $P(0)$ is true
- **For all $k$**, $[P(k) \text{ true } \rightarrow P(k+1) \text{ true}]$
- **Conclusion**: $P(n)$ true, $\forall n$

---

**Proof by Exhaustion**: "Proof by case"

**Example**: Show that $n! < 2^n$ for $n \in \{1, 2, 3\}$ any positive integer $n \leq 3$ (U?)

**Proof**:

List all possible cases:

- $n=1$, $1! < 2^1 \rightarrow 1 < 2$ (true)
- $n=2$, $2! < 2^2 \rightarrow 2 < 4$ (true)
- $n=3$, $3! < 2^3 \rightarrow 6 < 8$ (true) $\blacksquare$ Q.E.D.
Example: if an integer between 5 and 15 is divisible by 6, then it is also divisible by 3.

Proof:

List all possible cases:
- \( n = 6 \) is divisible by 6 and is divisible by 3.
- \( n = 12 \) is divisible by 6 and is divisible by 3.
- All other \( n \) values are not divisible by 6.

Note: If the above problem is for all integers, then we cannot use exhaustive proof.

Direct Proof: (deductive)

Example: For all \( x \), if \( x \) is divisible by 6 then \( x \) is divisible by 3.

Proof:

if \( x \) is divisible by 6
\[ \rightarrow x = k \times 6, \text{ for some integer } k \]
\[ \rightarrow x = k \times 2 \times 3 \]
\[ \rightarrow x = (k \times 2) \times 3 \]
\[ \rightarrow x = k' \times 3, \text{ where } k' = k \times 2 \]
since \( k' \) is integer, \( x \) is divisible by 3.
Example: Show that the product of two even integers is even. 

Proof: Let \( x = 2m \), \( y = 2n \) for some integer \( m \), \( n \) then \( xy = (2m)(2n) = 2(2mn) \), which is even.

\[ \therefore 2mn \text{ is integer.} \]

Example: Show that the sum of two odd integers is even

Proof: Let \( x = 2m+1 \), \( y = 2n+1 \) for some integer \( m \), \( n \) then \( x + y = 2m + 2n + 2 = 2(m+n+1) \), where \( m+n+1 \) is an integer

\[ \therefore x+y \text{ is even.} \]

**Proof by Counterexample:**

Proving \( P \) to be false (disproof) is much easier than proving \( P \) to be true (proof)!

**PROOF:** must show all cases are true

**DISPROOF:** showing only one case that is not true suffices!

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>A ( \cap ) C</th>
<th>A ( \cup ) (B ( \cap ) C)</th>
<th>A ( \cup ) B</th>
<th>(A ( \cup ) B) ( \cap ) (A ( \cup ) C)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
**Proof by Counterexample:**

Proving P to be false (disproof) is much easier than proving P to be true (proof)!

**PROOF:** must show all cases are true

**DISPROOF:** showing only one case that is not true suffices!

There are two (three) types of questions in proof

1) Prove/disprove a statement P.
2) Is a statement P true?
3) Prove/disprove a statement P by using X technique

The second question requires you to see if the statement P is true or not. So you must consider both cases of P is true and P is false.

---

**Examples for Proof by Counterexample:**

Example: Disprove that every integer less than 10 is bigger than 5.

To disprove (or prove the statement is not true), find a counterexample,

Let \( n = 4 \ < 10 \), but \( n \) is not \( > 5 \).

Example: Is the sum of any three consecutive integers even?

Proof or Disproof?

To disprove the statement,

give a counterexample: \( 2+3+4=9 \)
Proof by Contraposition:

Example: Prove that: If the square of an integer is odd, then the integer must be odd.

\[ P \rightarrow Q \iff Q' \rightarrow P' \]

Proof: if \( n^2 \) is odd, then \( n \) is odd (initial statement)

Proof: if \( n \) is not odd, then \( n^2 \) is not odd (contraposition)

i.e. Prove: \( n \) is even \( \rightarrow \) \( n^2 \) is even

Let \( n = 2m \) for some integer \( m \)

\[ n^2 = n \times n = 2m \times 2m = 2(2m^2) \]

\[ \rightarrow \text{since } 2m^2 \text{ is integer, } n^2 \text{ is even.} \]

Example: Show that \( xy \) is odd if and only if both \( x \) and \( y \) are odd.

Proof:

\[ P \iff Q = Q \Rightarrow P \text{ and } P \Rightarrow Q \]

\( (\iff) \) if \( x \) and \( y \) are odd, then \( xy \) is odd.

By direct proof:

Let \( x = 2m + 1, y = 2n + 1 \) for some \( m, n \in \text{integers} \)

\[ xy = (2m+1)(2n+1) = 4mn + 2m + 2n + 1 = 2(2mn+m+n) + 1 \]

\[ \rightarrow \text{since } 2mn + m + n \text{ is an integer, } xy \text{ is odd.} \]
(⇒) if \( xy \) is odd then \( x \) and \( y \) are odd.

By contraposition: if \( x \) is not odd or \( y \) is not odd, then \( xy \) is not odd

i.e. if \( x \) even or \( y \) even, then \( xy \) even

\textbf{case1} \( x \) even, \( y \) odd: Let \( x = 2m, y = 2n+1 \)
\[
xy = 2(2mn + m), \text{ which is even } \therefore 2mn+m \in \mathbb{Z}
\]

\textbf{case2} \( x \) odd, \( y \) even: similar to case1.

\textbf{case3} \( x \) even, \( y \) even: Let \( x = 2m, y = 2n \)
\[
xy = 2(2mn), \text{ which is even } \therefore 2mn \in \mathbb{Z}
\]

\textbf{Proof by Contradiction}

• Prove/Show \( P \rightarrow Q \) by contradiction method

• Is equivalent to show that \( (P \land Q') \) deduces to a contradiction (violation of assumption)

• Logical proof of contradiction:
  
  – Let \( x' = (P \rightarrow Q)' = P \land Q' \), we assume \( x' \) and derive a contradiction \( y' \), i.e. \( x' \rightarrow y' \)
  
  – Where \( y' \) is false, i.e. \( y \) is true (or axiom)
  
  – By \textit{modus tollens}: \( (x' \rightarrow y') \land y \) → \( x \)
  
  – Therefore, conclude \( x = P \rightarrow Q \) is true
Proof by Contradiction:

Example: If a number added to itself gives itself, then the number is 0, i.e. if \( x + x = x \), then \( x = 0 \)

Proof:

Assume \( x + x = x \) and \( x \neq 0 \)

\[ \rightarrow 2x = x \] and \( x \neq 0 \)

\[ \rightarrow 2 = 1 \], which is a contradiction

\( \therefore \) the assumption must be wrong

\( \therefore \) if \( x + x = x \), then \( x = 0 \)

Example: Prove that if \( x^2 + 2x - 3 = 0 \), then \( x \neq 2 \)

1. by contradiction: \( P \) and \( Q' \) \( \rightarrow \) Contradiction

Suppose \( x^2 + 2x - 3 = 0 \) and \( x = 2 \),

\[ \rightarrow 4 + 4 - 3 = 0 \text{ or } 5 = 0 \], which is a contradiction.

2. by direct proof: \( P \implies P' \implies Q \)

if \( x^2 + 2x - 3 = 0 \implies (x + 3)(x - 1) = 0 \)

\[ \rightarrow x = -3 \text{ or } x = 1 \rightarrow x \neq 2 \]

3. by contraposition: \( Q' \implies \rightarrow \rightarrow P' \)

show that if \( x = 2 \), then \( x^2 + 2x - 3 \neq 0 \)

\[ \rightarrow x^2 + 2x - 3 = 5 \neq 0 \]
In class exercises

Show that if $3n+2$ is odd, then $n$ is odd.

a) Proof by contradiction

b) Proof by contraposition

c) Direct proof