Proof Strategies

based on How to Prove It (chapter 3)

Few terms

- A proof of a theorem is simply a deductive argument whose **premises are the hypotheses of the theorem** and whose **conclusion is the conclusion of the theorem**.

- We will refer to the statements that are known or assumed to be true at some point in the course of figuring out a proof as <u>givens</u>, and the statement that remains to be proven at that point as the <u>goal</u>.

Proofs Involving Conditionals: $\rightarrow$ 1st strategy

To prove a goal of the form $P \rightarrow Q$: Assume P is true and then prove Q.

Givens: - Goal: $P \rightarrow Q$

transformed into:

Givens: P Goal: Q

Thm 1. Suppose a and b are real numbers. Prove that if $0 < a < b$ then $a^2 < b^2$.

Proofs involving Conditionals : →

- Proof.
- Suppose $0 < a < b$.
- Multiplying the inequality $a < b$ by the positive number a we can conclude that $a^2 < ab$, and similarly multiplying by b we get $ab < b^2$.
- Therefore $a^2 < ab < b^2$, so $a^2 < b^2$, as required.
- Thus, if $0 < a < b$ then $a^2 < b^2$.

Proofs Involving Conditionals : → Second Strategy.

Because any conditional statement $P \to Q$ is equivalent to its contrapositive $\neg Q \to \neg P$, you can prove $P \to Q$ by proving $\neg Q \to \neg P$ instead, using the strategy discussed earlier.

To prove a goal of the form $P \to Q$: Assume Q is false and prove that P is false.

Givens: - Goal: $P \to Q$

transformed into:

Givens: ? Goal: ?

Thm 2. Suppose a, b, and c are real numbers and $a > b$. Prove that if $ac \leq bc$ then $c \leq 0$.

Proofs Involving Conditionals : → Second Strategy.

Proof. We will prove the contrapositive. Suppose $c > 0$. Then we can multiply both sides of the given inequality $a > b$ by c and conclude that $ac > bc$. Therefore, if $ac \leq bc$ then $c \leq 0$.

Thm 3

Suppose that x and y are real numbers and $x \neq 3$.
If $x^2 y = 9y$ then $y = 0$.
Proof. Suppose that $x^2 y = 9y$.
Then $(x^2 - 9) y = 0$.
Since $x \neq 3$, $x^2 \neq 9$, so $x^2 - 9 \neq 0$.
Therefore, we can divide both sides of the equation
$(x^2 - 9) y = 0$ by $x^2 - 9$,
which leads to the conclusion that $y = 0$.
Thus, if $x^2 y = 9y$ then $y = 0$.

a) What's wrong with the proof of the theorem?
b) Show that the theorem is incorrect **by finding a counterexample.**

Incorrect Theorems or Proofs

Theorem. Suppose n is a natural number larger than 2, and n is not a prime number. Then 2n + 13 is not a prime number.

Show that the theorem is incorrect:

find a counterexample: n>2, n-natural, not prime, but 2n + 13 is a prime number.

Section 3.1 Exercise 15

Proofs Involving Negations: ¬

To prove a **goal of the form ¬ P**:

1) If possible, **reexpress the goal** in some other form (**without ¬**) and then use one of the proof strategies for this other goal form.

2) To prove a **goal of the form ¬ P**: **Assume P is true and try to reach a contradiction**. Once you have reached a contradiction, you can conclude that P must be false.

Proofs Involving Negations: ¬

Example 1. Suppose $A \cap C \subseteq B$ and $a \in C$.

Prove that $a \notin A \setminus B$.

Given	Goal
$A \cap C \subseteq B$ $a \in C$	$a \notin A \setminus B$
	$\neg(a \in A \wedge a \notin B)$
	$a \notin A \vee a \in B$

We will look into this proof when we study proofs involving disjunctions (slide 19-21 of this lecture).

Proof by contradiction

Example: Prove that if $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$.

Givens	*Goal*
$x^2 + y = 13$	$x \neq 3$
$y \neq 4$	

Givens	*Goal*
$x^2 + y = 13$	Contradiction
$y \neq 4$	
$x = 3$	

Proofs of set properties

Suppose A and B are sets. Prove that if $A \cap B = A$ then $A \subseteq B$.

Proof strategy: **Take arbitrary** x ∈A and prove that x ∈B, using $A \cap B = A$

Givens	*Goal*
$A \cap B = A$	$\forall x(x \in A \rightarrow x \in B)$

Givens	*Goal*
$A \cap B = A$ $x \in A$	$x \in B$

Proofs Involving Quantifiers: ∃, ∀

Example 3.3.3. Prove that for every real number x, if $x > 0$ then there is a real number y such that $y(y + 1) = x$.

We need to prove the property for every x.
Let x be arbitrary positive real number.

Givens	*Goal*
$x > 0$	$\exists y[y(y+1) = x]$

$$y(y+1) = x \quad \Rightarrow \quad y^2 + y - x = 0 \quad \Rightarrow \quad y = \frac{-1 \pm \sqrt{1+4x}}{2}.$$

Proofs involving Conjunctions: ∧

- To use a **given** of the form **P ∧ Q**: treat this given as two separate givens: P, and Q.
- To prove a **goal** of the form **P ∧ Q**: prove P, and Q separately.

- Example: Suppose A and C are disjoint and $A \subseteq B$,
- Prove that $A \subseteq B \setminus C$

Givens	*Goal*
$A \subseteq B$	$A \subseteq B \setminus C$
$A \cap C = \varnothing$	

Givens	*Goals*
$A \subseteq B$	$x \in B$
$A \cap C = \varnothing$	$x \notin C$
$x \in A$	

Next, prove that each goal is following from givens.

Proofs involving Disjunctions: ∨

- To use **a given in the form** $P \vee Q$**:**
- Break your proof into cases.
- For case 1, assume that P is true and use this assumption to prove the goal.
- For case 2, assume Q is true and give another proof of the goal.

Proofs involving Disjunctions: ∨

- **Example.** Suppose that A, B, and C are sets. Prove that if $A \subseteq C$ and $B \subseteq C$ then $A \cup B \subseteq C$.

Givens	*Goal*
$A \subseteq C$	$\forall x(x \in A \cup B \to x \in C)$
$B \subseteq C$	

Givens	*Goal*
$A \subseteq C$	$x \in C$
$B \subseteq C$	
$x \in A \vee x \in B$	

- Case 1: from $A \subseteq C$, $B \subseteq C$, and $x \in A$ prove that $x \in C$.
- Case 2: from $A \subseteq C$, $B \subseteq C$, and $x \in B$ prove that $x \in C$.

Proofs involving Disjunctions: ∨

- To prove **a goal of the form P ∨ Q**: Break your domain (described by givens) into cases. In each case, either prove P or prove Q.

- **Example 3.5.3**. Prove that for every integer x, the remainder when x^2 is divided by 4 is either 0 or 1.

Givens	*Goal*
$x \in \mathbb{Z}$	$(x^2 \div 4 \text{ has remainder } 0) \vee (x^2 \div 4 \text{ has remainder } 1)$

x	x^2	quotient of $x^2 \div 4$	remainder of $x^2 \div 4$
1	1	0	1
2	4	1	0
3	9	2	1
4	16	4	0
5	25	6	1
6	36	9	0

Let's break into 2 cases: x is even and x is odd;
then prove each part of the original goal involving disjunction.

Givens	*Goal*
$x \in \mathbb{Z}$	$x^2 \div 4$ has remainder 0
$\exists k \in \mathbb{Z}(x = 2k)$	

Givens	*Goal*
$x \in \mathbb{Z}$	$x^2 \div 4$ has remainder 1
$\exists k \in \mathbb{Z}(x = 2k + 1)$	

Proofs involving Disjunctions: ∨

To prove **a goal of the form P ∨ Q:**

- If P is true and does not contradicts to the givens, then of course P ∨ Q is true.
- Next, suppose P is false and prove Q.
- Thus, P ∨ Q is true.

Proofs involving Disjunctions: ∨

Before using strategy:

Givens	*Goal*
—	$P \vee Q$
—	

After using strategy:

Givens	*Goal*
—	Q
—	
$\neg P$	

Proofs Involving Disjunctions: $\vee$

- **Example.** Prove that for every real number x, if $x^2 \geq x$ then either $x \leq 0$ or $x \geq 1$.

Givens	*Goal*
$x^2 \geq x$	$x \geq 1$
$x > 0$	

- Proof. Suppose $x^2 \geq x$. It is true that $x \leq 0$ or $x > 0$.
- If $x \leq 0$, then it does not contradict to $x^2 \geq x$, and $x \leq 0$ or $x \geq 1$ is true.
- Now suppose $x > 0$. Then we can divide both sides of the inequality $x^2 \geq x$ by x to conclude that $x \geq 1$.
- Thus, either $x \leq 0$ or $x \geq 1$.

Proofs Involving Disjunctions: V

Example. Suppose $A \cap C \subseteq B$ and $a \in C$.

Prove that $a \notin A \setminus B$.

Givens	Goal
$A \cap C \subseteq B$ $a \in C$	$a \notin A \setminus B$
	$\neg(a \in A \wedge a \notin B)$
	$a \notin A \vee a \in B$

Givens	Goal
$A \cap C \subseteq B$ $a \in C$	$a \in B$
$a \in A$	

Proofs Involving Biconditionals: $\leftrightarrow$

- $P \leftrightarrow Q$ is equivalent to $(P \rightarrow Q) \wedge (Q \rightarrow P)$.
- According to our strategies a given or goal of the form $P \leftrightarrow Q$ should be treated as two separate givens or goals: $P \rightarrow Q$, and $Q \rightarrow P$.
- To prove a goal of the form $P \leftrightarrow Q$:
  - Prove $P \rightarrow Q$ and $Q \rightarrow P$ separately.
- To use a given of the form $P \leftrightarrow Q$:
  - Treat this as two separate givens: $P \rightarrow Q$, and $Q \rightarrow P$.

Proofs Involving Biconditionals: $\leftrightarrow$

Example 3.4.2. Suppose x is an integer. Prove that x is even iff x^2 is even.

- The goal is (x is even) $\leftrightarrow$ (x^2 is even), so we prove the two goals separately:
  1. (x is even) $\rightarrow$ (x^2 is even)
  2. (x^2 is even) $\rightarrow$ (x is even)

Proofs Involving Biconditionals:↔

Example 3.4.4. Suppose A, B, and C are sets.

Prove that $A \cap (B \setminus C) = (A \cap B) \setminus C$.

$$x \in A \cap (B \setminus C) \text{ iff } x \in A \wedge x \in B \setminus C \text{ iff } x \in A \wedge x \in B \wedge x \notin C;$$

$$x \in (A \cap B) \setminus C \text{ iff } x \in A \cap B \wedge x \notin C \text{ iff } x \in A \wedge x \in B \wedge x \notin C.$$

Proofs Involving Biconditionals: $\leftrightarrow$

Theorem 3.4.6. For every integer n, 6|n iff 2|n and 3|n.

Proof. Let n be an arbitrary integer.

- ($\rightarrow$) Suppose 6|n.
  - Then we can choose an integer k such that 6k = n. Therefore n = 6k = 2(3k), so 2|n, and similarly n = 6k = 3(2k), so 3 | n.
- ($\leftarrow$) Suppose 2|n and 3|n.
  - Then we can choose integers j and k such that n = 2 j and n = 3k.
  - 6(j − k) = 6j − 6k = 3(2j) −2(3k) = 3n − 2n = n, so 6|n.

Proofs of Existence and Uniqueness

- **To prove a goal of the form $\exists!\, x\, P(x)$:**
  - **Prove existence: $\exists\, x\, P(x)$**
  - **Prove uniqueness: $\forall y(P(y) \rightarrow (y = x))$**

- **Theorem.** For every real number x, if $x \neq 2$ then there is a unique real number y such that $2y/(y + 1) = x$.
- **Proof.** Let x be an arbitrary real number, and suppose $x \neq 2$. Let $y = x/(2 - x)$, which is defined since $x \neq 2$. Then

$$\frac{2y}{y+1} = \frac{\frac{2x}{2-x}}{\frac{x}{2-x}+1} = \frac{\frac{2x}{2-x}}{\frac{2}{2-x}} = \frac{2x}{2} = x.$$

- To see that this solution is unique, suppose $2z/(z + 1) = x$. Then $2z = x(z + 1)$, so $z(2 - x) = x$. Since $x \neq 2$ we can divide both sides by $2 - x$ to get $z = x/(2 - x) = y$.

Proofs of Existence and Uniqueness

- **Theorem.** There is a unique set A such that **for every set** B, $A \cup B = B$.
- **Proof.**
- **Existence:**
- Clearly $\forall B(\emptyset \cup B = B)$, so $\emptyset$ has the required property.
- **Uniqueness:**
- Suppose $\forall B(C \cup B = B)$ and $\forall B(D \cup B = B)$. Applying the first of these assumptions to D we see that $C \cup D = D$, and applying the second to C we get $D \cup C = C$. But clearly $C \cup D = D \cup C$, so $C = D$.