# Mat 2345
# Week 3-ish

Secs 1.6 – 1.7

Fall 2013

# Student Responsibilities — Week 3



- **Reading**: Textbook, Section 1.7
- **Assignments**: Worksheets & more — See web site
- **Attendance**: Laboriously Encouraged

## Week 3 Overview

- 1.6 Introduction to Proofs, review
- 1.7 Proof Methods and Strategy

# Mathematical Proofs



- Proofs in mathematics are **valid arguments** that establish the truth of mathematical statements.

- **Argument** : a sequence of statements that ends with a conclusion.

- **Valid** : the conclusion or final statement of the argument must follow from the truth of the preceding statements, or **premises**, of the argument.

- An argument is valid if and only if it is impossible for all the premises to be true and the conclusion to be false.

# Formal Proofs

To prove an argument is valid or the conclusion follows logically from the hypotheses:

- **Assume** the hypotheses are true
- Use the rules of inference and logical equivalences to determine that the conclusion is true.

# Methods of Proof



- **Trivial Proof**: if $q$ is true, then $p \rightarrow q$ is true
- **Vacuous Proof**: if one or more hypotheses are false
- **Direct Proof**: assume hypotheses true, show conclusion true
- **Indirect Proof**: assume conclusion false, show hypotheses is false
- **Proof** by **Contradiction**: assume conclusion false, derive contradiction (yielding $\neg q \rightarrow \mathit{False}$, so $q$ must be true)
- **Proof** by **Cases**: break hypotheses into equivalent disjunctive implications, prove case by case

# A Guide to Writing Proofs



Based on supplement to the text by
Ron Morash, University of Michigan–Dearborn

Deducing conclusions having the form:
"For every $x$, if $P(x)$, then $Q(x)$"
$(\forall x[P(x) \rightarrow Q(x)])$

- Direct proof
- Indirect proof
  - Proof by contraposition
  - Proof by contradiction
  - Deriving conclusions of the form "$q$ or $r$"
- Proof by mathematical induction

# $\forall x[P(x) \to Q(x)]$



- Many defining properties in math have the form $\forall x[P(x) \to Q(x)]$, representing the idea "All P's are Q's".

- Many math propositions that students are asked to prove have as their conclusion a statement involving a definition of this form.

  For example,

  "Prove that for all sets $A$ and $B$, $A \subseteq A \cup B$"

  or

  "Prove that for all primes $p$ and $q$ greater than 2, $pq + 1$ is not prime."

# $\forall x[P(x) \rightarrow Q(x)]$, Cont.



- Note that the desired conclusion in such propositions is a statement involving a **definition**.

- Further, many propositions have a *hypothesis*, a statement we are allowed to assume true, and whose assumed truth, presumably, will play a role in deriving the conclusion.

# Direct Proof



- **Direct proof**: an argument in which a proposition in its originally-stated form is proven
- Direct proofs of propositions with no hypothesis tends to be simpler than for those in the form $\forall x, P(x) \rightarrow Q(x)$.
- Usually, a definition is used to facilitate the proof.

# Sets, a Quick Intro



- **Set**: an **unordered** collection or group of objects, which are said to be **elements**, or **members** of the set

- **Subset**: Let $A$ and $B$ be sets. Then
$$A \subseteq B \Leftrightarrow \forall x \ [\, x \in A \rightarrow x \in B \,]$$

- **Complement** of $A$, denoted $\overline{A}$, is the set
$$\{x \mid \neg(x \in A)\} = \{x \mid x \notin A\}$$

- **Union** of $A$ and $B$, denoted $A \cup B$, is the set
$$\{x \mid x \in A \vee x \in B\}$$

- **Intersection** of $A$ and $B$, denoted $A \cap B$, is the set
$$\{x \mid x \in A \wedge x \in B\}$$

If the intersection is void, $A$ and $B$ are said to be **disjoint**

# Direct Proof, Example 1

**Theorem** For all sets $A$ and $B$, $A \subseteq A \cup B$

**Discussion** Let $A$ and $B$ be arbitrary sets, and let $x$ be an arbitrary element of $A$ (Assume $x \in A$). We must prove $x \in A \cup B$

**Proof**

- By **definition of union**, we must show $x \in A$ or $x \in B$
- Since we assumed $x \in A$, the desired conclusion, $x \in A$ or $x \in B$ follows immediately
- Thus, $x \in A \cup B$, and the proof is complete

# Direct Proof, Example 2



**Theorem** For all sets $X$ and $Y$, $X \cap (Y \cup \overline{X}) \subseteq Y$

**Discussion** Let $X$ and $Y$ be arbitrary sets. To prove $X \cap (Y \cup \overline{X}) \subseteq Y$, let $a$ be an arbitrarily chosen element of $X \cap (Y \cup \overline{X})$, and prove $a \in Y$

**Proof**

- By the assumption (and **definition** of intersection), $a \in X$ and $a \in Y \cup \overline{X}$
- From this, we know $a \in X$ AND either $a \in Y$ or $a \in \overline{X}$
- Thus, either $a \in Y$ or $a \notin X$
- But we also know $a \in X$, so $a \notin X$ is false
- Hence, we conclude $a \in Y$, and the proof is complete

# Propositions With One Or More Hypotheses



The tools we can use:

- the assumption(s) we're entitled to make at the outset, in setting up the proof
- assumed axioms and previously–proved theorems (if any)
- rules of inference from logic
- in addition, most propositions contain one or more *hypotheses* — statements which are assumed to be true (and will likely be used in the proof)

# Direct Proof, Example 3

**Theorem** For all sets $X$, $Y$, and $Z$, **if** $X \subseteq Y$, **then** $X \cap Z \subseteq Y \cap Z$.

**Discussion** Let $X$ and $Y$ be sets, such that $X \subseteq Y$. To prove $X \cap Z \subseteq Y \cap Z$, assume $b \in X \cap Z$ and show $b \in Y \cap Z$. To do this, we'll have to prove that $b \in Y$ and $b \in Z$. Notice we are focusing on the **conclusion**.

**Proof**

- What do we know or assume is true? $b \in X \cap Z$, which means (by definition of $\cap$) that $b \in X$ and $b \in Z$ — $\surd$
- Now we just have to prove $b \in Y$
- Since $b \in X$ and $X \subseteq Y$, by definition of $\subseteq$, we can conclude $b \in Y$ — $\surd$
- Thus, we have proven **if** $X \subseteq Y$, **then** $X \cap Z \subseteq Y \cap Z$

# Direct Proof, Example 4

**Theorem** Every non–constant linear function $f(x) = Mx + B, M \neq 0$, is one–to–one.

**Discussion** Let $M$ be a nonzero real number. Let $x_1$ and $x_2$ be real numbers and assume that $f(x_1) = f(x_2)$. We must prove that $x_1 = x_2$ (since that is the definition of one–to–one).

**Proof**

- Since $f(x_1) = Mx_1 + B$ and $f(x_2) = Mx_2 + B$, we have $Mx_1 + B = Mx_2 + B$
- By a rule of elementary algebra, if $Mx_1 + B = Mx_2 + B$, then $Mx_1 = Mx_2$
- Since $Mx_1 = Mx_2$ and $M \neq 0$ (by hypothesis), we conclude by another rule of elementary algebra that $x_1 = x_2$, as desired.

# Disproving False Propositions Having Conclusions of the Form $\forall x[P(x) \to Q(x)]$



- Sometimes we are faced with a proposition that must either be "proved or disproved," and are not told in advance if the proposition is true.

- If it is false, then it will be impossible to write a correct proof of the proposition

- Trying to do so may provide insight, but will not lead to a valid proof.

# Example 5



Prove or disprove:

**Theorem** For all sets $X$, $Y$, and $Z$, **if** $X \cap Z \subseteq Y \cap Z$, **then** $X \subseteq Y$.

**Discussion** Suppose we attempt to prove this proposition. Let $X$, $Y$, and $Z$ be arbitrary sets such that $X \cap Z \subseteq Y \cap Z$. To prove $X \subseteq Y$, let $w \in X$; we must prove $w \in Y$.

At this point, we run into a problem: $w \in X$ doesn't mean $w \in X \cap Z$, unless we know $w \in Z$ (which we do not). So either there is another proof method, or the proposition is false.

**Finding a Counterexample** — a specific example that contradicts the truth of the proposition.

- First, we must determine the negation of the proposition
- The negation of $\forall x[P(x) \to Q(x)]$ is $\exists x[P(x) \land \neg Q(x)]$
- So the negation of the proposition is: "there exists sets $X$, $Y$, and $Z$ such that $X \cap Z \subseteq Y \cap Z$ but $X$ is not a subset of $Y$."
- Consider: $X = \{4, 7\}$. $Y = \{7, 9\}$, and $Z = \{7, 9, 10\}$. Then $X \cap Z = \{7\}$, $Y \cap Z = \{7, 9\}$, so $X \cap Z \subseteq Y \cap Z$. However, $X \not\subseteq Y$.
- Hence we have a counterexample; the proposition is false.

- **Note**: a **single** counterexample to a general proposition is sufficient to prove that proposition false.

- On the other hand, if we were to try to prove a general proposition true by **example**, we would have to show it holds for **all** elements in the domain – impossible when the domain is infinite.

- In that case, no number of specific cases that affirm a proposition are sufficient to establish its truth in general.

- A general proof is required for a general case with an infinite domain.

# Tactic of Division into Cases



- This method is used as the propositions we wish to prove become more complex.
- It may be that we must consider $p \vee \neg p$, which breaks down into two cases: $p$ and $\neg p$
- Or, there may be a finite number of possibilities to consider, and we may have more than two cases. For example, $x < 0$, $x = 0$, and $x > 0$.

# Example 7, Proof by Cases

**Theorem** For all sets $A$ and $B$, $(A \cap B) \cup (A \cap \overline{B}) \subseteq A$

**Discussion** Let $A$ and $B$ be arbitrary sets. To prove the proposition, assume $x \in (A \cap B) \cup (A \cap \overline{B})$ and prove $x \in A$.

**Proof**

- By definition of $\cup$, we know $x \in (A \cap B)$ or $x \in (A \cap \overline{B})$.
- That is, either $(x \in A \wedge x \in B)$ **or** $(x \in A \wedge x \in \overline{B})$
- We don't know which is the case, but we do know one of them must be true.

- Now the argument can be divided into two exhaustive cases:

Case I $x \in (A \cap B) \equiv x \in A \wedge x \in B$
Then, in particular, $x \in A$ (by definition of $\cap$ and $\wedge$), so the conclusion holds.

Case II $x \in (A \cap \overline{B}) \equiv x \in A \wedge x \in \overline{B}$
Then again, $x \in A$ (by definition of $\cap$ and $\wedge$), so the conclusion holds.

- Under either of the only two possible cases, we have $x \in A$, the desired conclusion.

# Example 8

**Theorem** For all sets $A$ and $B$, $A \subseteq (A \cap B) \cup (A \cap \overline{B})$

**Discussion** Let $A$ and $B$ be arbitrary sets. To prove the proposition, assume $x \in A$ and prove $x \in (A \cap B) \cup (A \cap \overline{B})$. To do this, we must prove either $x \in (A \cap B)$ or $(x \in A \cap \overline{B})$

## Proof

- Thus, either $(x \in A$ and $x \in B)$, or else $(x \in A$ and $x \in \overline{B})$.
- Since we assumed $x \in A$, we need only consider whether $x$ is in $B$ or $\overline{B}$.

- Now the argument can be divided into two exhaustive cases:

Case I $x \in B$
Then, since $x \in A$, we have $x \in A$ and $x \in B$, or $x \in (A \cap B)$

Case II $x \in \overline{B}$
Then since $x \in A$, we have $x \in A$ and $x \in \overline{B}$, or $x \in (A \cap \overline{B})$

- Thus we have shown that $x \in (A \cap B)$ or $x \in (A \cap \overline{B})$, so $x$ must be in their union.

# Indirect Proof



- Sometimes it's convenient, or even necessary, to prove a form of a proposition that is different from the original, but logically equivalent to it.
- Whenever we write a proof in such a form, it's called an **indirect proof**.
- Three common forms of indirect proof, based on three logical equivalences of pairs of propositions:

  1. **Proof by Contraposition**: $\neg q \to \neg p$ is equivalent to $p \to q$
  2. **Proof by Contradiction**: $\neg p \to (q \wedge \neg q)$ is equivalent to $p$
  3. For conclusions having the form "either $q$ or $r$: $(p \wedge \neg q) \to r$ is equivalent to $p \to (q \vee r)$"

# Proof by Contraposition



- **Proof by Contraposition**: $\neg q \to \neg p$ is equivalent to $p \to q$
- Sometimes it's difficult to see how to prove a proposition of the form $\forall x[P(x) \to Q(x)]$ by starting with the assumption that $P(x)$ is true.
- So, what can we do if we cannot see how to deduce the conclusion, $Q(x)$, from the hypotheses?
- In some proofs, assuming $\neg Q(x)$, the negation of the conclusion, provides a better match with known facts and the other given hypotheses (if any), and may lead more readily to $\neg P(x)$, the negation of the original assumption.

# Proof by Contradiction



- **Proof by Contradiction**: $\neg p \to (q \land \neg q)$ is equivalent to $p$
- In this method, we may prove a conclusion $p$ by showing that the denial of $p$ leads to a contradiction.
- Proof by contraposition is actually a form of proof by contradiction: in a proof of $p \to q$, we assume the truth of $p$ and then use $\neg q$ to derive $\neg p$, we obtain the contradiction $p \land \neg p$.
- Another instance in which proof by contradiction is the standard approach is any proof of a theorem in set theory in which the conclusion asserts that some set equals the empty set.

# Deriving Conclusions of the Form $q \vee r$

- For conclusions having the form "either $q$ or $r$: $(p \wedge \neg q) \rightarrow r$ is equivalent to $p \rightarrow (q \vee r)$"

- Strategy: assume the negation of all but one of the alternative conclusions and, on that basis, try to prove that the remaining conclusion must be true.

- This equivalence becomes relevant when we must derive a conclusion involving alternatives — $q \vee r$

- There may be no circumstance under which we can be sure which of the alternatives is true — only that at least one of them must be true under every circumstance in which the hypothesis is true.

- Because of this, we are unable to determine whether to set up a direct proof based on the conclusion $q$ or on the conclusion $r$.

- The solution is to replace the original problem by the problem of showing that $r$ follows $p \wedge \neg q$ (or equivalently, that $q$ follows from $p \wedge \neg r$)

# $(p \wedge \neg q) \to r$



**Theorem** For all real numbers $x$ and $y$, if $xy = 0$, then $x = 0$ or $y = 0$.

**Discussion** Let $x$ and $y$ be real numbers such that $xy = 0$. Now we have a dilemma: there is no evident way of proceeding toward the conclusion — that one or the other of $x$ or $y$ must be 0.

**Proof**

- Thus, we make the additional assumption that $x \neq 0$ and show that therefore $y$ must be 0.
- Since $x \neq 0$, its reciprocal, $\frac{1}{x}$, must exist.
- Then $y = 1y = [\frac{1}{x}x]y = \frac{1}{x}xy = \frac{1}{x}0 = 0$, so $y = 0$ as desired.

# Another Such Proof

**Theorem** For all sets $A$ and $B$, $A \subseteq B \cup (A \cap \overline{B})$.

**Discussion** Let $A$ and $B$ be arbitrary sets, and assume that $x \in A$. We need to prove that $x \in B \cup (A \cap \overline{B})$; that is, either $x \in B$ **or** $x \in A \cap \overline{B}$.

**Proof**

- Assume $x \notin B$, and we will show that $x$ must then be in $A \cap \overline{B}$, or equivalently, $x \in A \wedge x \in \overline{B}$.
- We already know that $x \in A$ by our initial assumption.
- Since $x \notin B$, we also know $x \in \overline{B}$.
- Thus, $x \in A \wedge x \in \overline{B}$, which we wished to show.

# Proof by Mathematical Induction



- This method will be studied in depth later in the course.

- It is used to prove propositions of the form $\forall n P(n)$, where the universe of discourse is the set of positive integers.

- Examples: $\forall n \geq 1, 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ **or**
  $\forall n \geq 1, n \leq 2^n$.

- The big picture is that we first prove $P(1)$ true, then show we can prove $P(k+1)$ is true if $P(k)$ is true — sort of a bootstrapping process. Once we have a basis and a way to leverage from $P(i)$ to $P(i+1)$, we have an algorithm or method for showing all the $P(n)$ are true.

# Existence Proofs — Constructive

We wish to establish the truth of $\exists x P(x)$.

**Constructive** existence proof:

- Establish P(c) is true for some c in the universe
- Then $\exists x P(x)$ is true by Existential Generalization (EG).
- *note:* c may be specific and unique, or may be arbitrary.

# Example 1



**Theorem**. There exists an integer solution to the equation

$$x^2 + y^2 = z^2$$

**Proof**:

Choose $x = 3$, $y = 4$, and $z = 5$.

# Example 2

**Theorem**. There exists a **bijection** from $A = [0, 1]$ to $B = [0, 2]$

- A bijection is a one-to-one, onto function mapping elements of one set to another.
- Let $a, a_1, a_2 \in A$ and $b \in B$.
- Then **1–1** (injection) means if $f(a_1) = b = f(a_2)$, then $a_1 = a_2$.
- **Onto** (surjection) means $\forall b \in B\ \exists a \in A\ [f(a) = b]$, i.e., $b$ has a pre–image in $A$, $f^{-1}(b) = a \in A$.

**Proof**:

We build two injections and conclude there must be a bijection with out ever exhibiting the bijection.

- Let $f$ be the identity map from $A$ to $B$.
- Then $f$ is an injection (and we conclude that $|A| \leq |B|$).
- Define the function $g$ from $B$ to $A$ as $g(x) = \frac{x}{4}$.
- Then $g$ is an injection.
- Therefore, $|B| \leq |A|$.
- We now apply a theorem which states that:

  if $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.
- Hence, there must be a bijection from $A$ to $B$.
- *Note*: we could have chosen $g(x) = \frac{x}{2}$ and obtained a bijection directly.

Q.E.D.

# Existence Proofs — Non-constructive



Assume no $c$ exists which makes $P(c)$ true, and derive a contradiction.

**Theorem** There exists an irrational number.

**Proof**

- Assume there doesn't exist an irrational number.
- Then all numbers must be rational.
- Then the set of all numbers must be **countable**.
- Then the real numbers in the interval $[0, 1]$ is a countable set.
- But this set is **not countable**.
- Hence, we have a contradiction — the set is both countable and not countable.
- Therefore, there must exist an irrational number. Q.E.D. (And we didn't even have to produce it!)

# Biconditional Proofs



Recall that $P \leftrightarrow Q$ is equivalent to $(P \rightarrow Q) \wedge (Q \rightarrow P)$

When proving a biconditional, we must prove both $P \rightarrow Q$ and $Q \rightarrow P$

**Theorem** For the universe of all integers, $x$ is even if and only if $x^2$ is even.

**Discussion** The quantified assertion is:

$$\forall x[(x \textit{ is even}) \leftrightarrow (x^2 \textit{ is even})]$$

Thus, $\forall x[(x \textit{ is even}) \rightarrow (x^2 \textit{ is even})]$ *and*
$\quad\forall x[(x^2 \textit{ is even}) \rightarrow (x \textit{ is even})]$

Assume $x$ is arbitrary.

**Proof**

Case I Show $\forall x[(x \textit{ is even}) \rightarrow (x^2 \textit{ is even})]$

Case II Show $\forall x[(x^2 \textit{ is even}) \rightarrow (x \textit{ is even})]$

Case I. Show if $x$ is even, then $x^2$ is even — using a direct proof.

- If $x$ is even, then $x = 2k$ for some integer $k$.
- Hence, $x^2 = (2k)^2 = 4k^2 = 2(2k^2)$, which is even since it is an integer which is divisible by 2.
- This completes the proof of Case I.

Case II. Show that if $x^2$ is even, then $x$ must be even — using an indirect proof.

- Assume $x$ is not even, and show $x^2$ is not even.
- If $x$ is not even, then it must be odd.
- So, $x = 2k + 1$ for some $k$.
- Then, $x^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which is odd and therefore not even.
- This completes the proof of Case II.

Thus we have shown that $x$ is even IFF $x^2$ is even. Since $x$ was arbitrary, the result follows by UG.