

MC215: MATHEMATICAL REASONING AND DISCRETE STRUCTURES

□ Friday, 9/12/08

- Theorems and Proofs
- Direct Proofs

□ READING: 2.1

□ EXERCISES:

- pp. 75-76: 7, 12, 13, 18, 19

Theorems

- **What is a theorem?**
 - A declarative statement about objects in a mathematical system that can be proven true.
 - Examples of “mathematical systems” include Euclidean geometry, Real numbers with arithmetic operations, Set theory, ...
- Many theorems have the form
 “If $P(x, y, z, \dots)$ then $Q(x, y, z, \dots)$ ”
- It really means: **“For all $x, y, z, \dots \in \text{domain } D$, if $P(x, y, z, \dots)$ then $Q(x, y, z, \dots)$ ”**
- Shorthand: **“ $P(x, y, z, \dots) \Rightarrow Q(x, y, z, \dots)$ ”**

Examples of If-then Theorems

- **Pythagorean Theorem.** If a and b are the lengths of the legs of a right triangle, and c is the length of the hypotenuse, then $a^2 + b^2 = c^2$.
 - Really means, "For all positive numbers a , b , and, c , if ..."
- **Theorem.** If m and n are perfect squares, then mn is a perfect square.
 - Really means, "For all natural numbers m and n , if ..."
- **Theorem.** The sum of two odd numbers is even.
 - **Can be restated as an if-then:** If m and n are odd numbers, then $m + n$ is even.

Variations on the word “Theorem”

- **Theorem** – usually reserved for a result that is pretty substantive or important
- **Proposition** – like a theorem, but not such an important one
- **Lemma** – a “helper” theorem, i.e., a result that helps in proving some other theorem.
- **Corollary** – a result that follows immediately (or almost immediately) from a preceding theorem

Proofs

□ What is a proof?

- An essay (grammatically correct sequence of sentences) that convincingly shows a theorem to be true.
- It contains arguments based on:
 - **Definitions**
 - **Axioms** (statements agreed upon to be true, at least in a certain setting)
 - **Rules of logic**
 - **Previously proved theorems**

Proving an if-then theorem

- Proving “If $P(x, y, \dots)$ then $Q(x, y, \dots)$ ” ($P \Rightarrow Q$ for short):
 - P is the *hypothesis*, Q is the *conclusion*
 - From the truth table for $p \rightarrow q$, we see the only time $P \Rightarrow Q$ might be false is if P is true and Q is false.
 - So:
 - (1) Assume that P is true.
 - (2) Prove that Q is true.
 - (3) Conclude that $P \Rightarrow Q$ is true.
 - This approach is called **DIRECT PROOF**.

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Preparing a direct proof: working stage

- Working on an if-then proof (e.g., “rough draft”):
 - 1a) Write down the **hypothesis P**.
 - 1b) Write down all the **meanings of terms in P**, using **variable names** (e.g., for “even number” write $n = 2k$).
 - 2a) Write down the **conclusion Q**.
 - 2b) Write down all the **meanings of terms in Q**, using variable names (some of which were introduced in step 1b).
 - 3) (**Hard part!**) Compare the hypothesis ($P =$ what you know) to the conclusion ($Q =$ what you’re proving), and try to find some way to **start with P, say things you know are true, and end up with Q**.

Writing up your proof

- **“Final Draft:”** Remember that you are trying to *convince the reader*, so your writing should be clear and helpful.
(See **“Problem-Solving Tips,”** pp. 73-74).
 - Begin by saying **“Assume that {the conditions of P}.**
 - Next say: **“We must show that {the conditions of Q}.**
 - Compose your argument **clearly**, using **complete sentences**, and **justifying your claims**.
 - End by saying, **“Thus we have proved that {what we wanted to prove}.**

Examples

- **Remember:** If the theorem is not stated as if-then, try first to rephrase it that way.

- **Theorem.** The product of two odd numbers is an odd number.
 - Recall: An integer n is odd if it can be written as $n = 2k + 1$, for some integer k .

- **Theorem.** If A is a subset of B and B is a subset of C , then A is a subset of C .
 - Recall: “ S is a subset of T ” means that $\forall x, x \in S \Rightarrow x \in T$.

Exercise

- **Definition.** If m and n are integers, $m \neq 0$, then we say " m is a divisor of n ," written $m|n$, if there is some integer k such that $n = k m$.
- **Theorem.** If $a|b$ and $b|c$, then $a|c$.

Bad proof #1

- See “**Some Common Errors,**” p. 74.
- **Theorem?** If m and n are even integers, then mn is a perfect square.
- **Proof?**
 - Assume that m and n are even.
 - Thus $m = 2k$, and $n = 2k$.
 - We must show that mn is a perfect square.
 - By our assumptions, $mn = (2k)(2k) = (2k)^2$.
 - Therefore we have shown that mn is a perfect square.
- **What's wrong???** Is the theorem true?

Bad proof #2

- **Theorem?** If m and $m + n$ are both even integers, then n is an even integer.
- **Proof?**
 - Let $m = 2a$ and $n = 2b$.
 - Then $m + n = 2a + 2b$.
 - Now subtract m from both sides to get:
 - $n = 2a + 2b - m = 2a + 2b - 2a = 2b$.
 - Therefore we have shown that n is even.
- **What's wrong???** Is the theorem true?