Slide 1

Administrivia

- Reminder: Homework 2 due today (5pm).
- Quiz solutions will be online, usually shortly after the quiz.
- Quiz 2 next Tuesday. Predicate logic.

Slide 2

Example Revisited

- Section 1.3 problem 11 again . . .

Slide 3

Proof Techniques

- In chapter 1 we worked up a formal system for proving "meaningless" formulas — which can prove "meaningful" formulas as special cases.
- Most of the time, though, we want to prove something is valid in a particular context, and the procedure is less formal and makes use of context-specific additional info (e.g., definitions of terms such as "even integer").
- *But* keep in mind that less-formal proofs could be done in the millimeter-by-millimeter style of chapter 1.
- (Why are we doing this anyway? In part because CS majors almost surely will see theorems/proofs in CS theory classes, in part to help with that "mathematical maturity" goal . . . Goal is to recognize what makes a valid proof.)

Slide 4

Proof Techniques, Continued

- Suppose you have a "conjecture" (e.g., "all odd numbers greater than 1 are prime"). How to (try to) prove it?
- Well, first must sometimes decide *whether* to prove it. Do you think it's true?
- If it's a statement about all integers, etc., often helpful to start with "inductive reasoning" — try some examples and see what happens.
- If one doesn't work? "Counterexample" that shows conjecture false.
- If all succeed? Just means you didn't find a counterexample. So, turn to "deductive reasoning" to prove — subject of first part of chapter 2.
- Lots of examples/problems will be simple stuff about integers. Why? Something where we supposedly all know the "context".

What Do We Mean By "Proof"?

Slide 5

- By "proof" we mean informal version, sometimes relying on context, of formal "this follows from that" arguments of chapter 1.
- Goal is to convince human reader. Sometimes a sequence of formulas will do. Other times some prose is needed to explain what they mean. (Ask yourself: Would this make sense to you?)

Exhaustive Proof / Proof By Cases

Slide 6

- Idea here is to prove by considering each "case" separately. Only works if there are finitely many. (Recall result from propositional logic that allows this.)
- Simple example: To show that for all integers x with $0 \leq x \leq 4$, $x^2 < 20$, five cases to consider.
- Slightly more complex example: To show something for all integers, can consider two cases, odd integers and even integers.

  (Aside: How shall we define "even"? Is zero even?)
- Much more complex example: Computer-assisted proof of 4-color map theorem (1976, used almost 2000 separate cases).

Slide 7

Direct Proof

- Idea here is to show $P \rightarrow Q$ like we've been doing — assume P and derive Q — but less formally.
- Example: Show that for integers p and m, if p is even and m is positive, p^m is even.

Slide 8

Proof by Contraposition

- Idea is based on a derived rule from propositional logic: If $Q' \rightarrow P'$, then $P \rightarrow Q$.

  So if proving $P \rightarrow Q$ is difficult, we can try proving $Q' \rightarrow P'$ instead.
- Example: Show that if m and n are integers and $m + n$ is even, either m and n are both even or m and n are both odd.

Slide 9

Proof By Contradiction

- Idea is based on another rule we could prove using propositional logic: If $(P \wedge Q') \rightarrow false$, then $P \rightarrow Q$.

  So if proving $P \rightarrow Q$ is difficult, we can try assuming $P \wedge Q'$ and "deriving a contradiction".

  Note that sometimes P is just $true$.
- Example: Show that $\sqrt{2}$ is irrational.

Slide 10

Minute Essay

- Find a counterexample for the following conjecture: "If x is an integer, $\sqrt{x}$ is an integer."
- To show that there is no largest prime, we could assume P and derive a contradiction. What is P? (You don't have to show there's no largest prime, just say what P is.)

Minute Essay Answer

- Find a counterexample for the following conjecture: "If x is an integer, $\sqrt{x}$ is an integer."

  $x = 2$

- To show that there is no largest prime, we could assume P and derive a contradiction. What is P? (You don't have to show there's no largest prime, just say what P is.)

  "There is a largest prime."