Announcements

• Quiz 1 is today

• Homework 2 is due on Thursday

• Review first Chapter.
Topics

- Existence Proofs
  - Constructive
  - Nonconstructive
- Disprove by Counterexample
- Nonexistence Proofs
- Uniqueness Proofs
- Proof Strategies
- Proving Universally Quantified Assertions
- Open Problems
Existence Proofs

- Proof of theorems of the form $\exists x P(x)$
- Constructive existence proof:
  - Find an explicit value of $c$, for which $P(c)$ is true.
  - Then $\exists x P(x)$ is true by Existential Generalization (EG).

Example: Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways:
Proof: $1729$ is such a number since
\[1729 = 10^3 + 9^3 = 12^3 + 1^3\]
Counterexamples

• Recall \( \exists x \neg P(x) \equiv \neg \forall x P(x) \)

• To establish that \( \neg \forall x P(x) \) is true (or \( \forall x P(x) \) is false) find a \( c \) such that \( \neg P(c) \) is true or \( P(c) \) is false.

• In this case \( c \) is called a counterexample to the assertion \( \forall x P(x) \).

Example: “Every positive integer is the sum of the squares of 3 integers.” The integer 7 is a counterexample. So the claim is false.
Uniqueness Proofs

• Some theorems assert the existence of a unique element with a particular property, $\exists! x \ P(x)$. The two parts of a uniqueness proof are

  - **Existence**: We show that an element $x$ with the property exists.
  - **Uniqueness**: We show that if $y \neq x$, then $y$ does not have the property.

Example: Show that if $a$ and $b$ are real numbers and $a \neq 0$, then there is a unique real number $r$ such that $ar + b = 0$.

Solution:
  - Existence: The real number $r = -b/a$ is a solution of $ar + b = 0$ because $a(-b/a) + b = -b + b = 0$.
  - Uniqueness: Suppose that $s$ is a real number such that $as + b = 0$. Then $ar + b = as + b$, where $r = -b/a$. Subtracting $b$ from both sides and dividing by $a$ shows that $r = s$. 

Proof Strategies for proving $p \rightarrow q$

• Choose a method
  – First try a direct method of proof
  – If this does not work, try an indirect method (e.g., try to prove the contrapositive)

• For whichever method you are trying, choose a strategy
  – First try forward reasoning. Start with the axioms and known theorems and construct a sequence of steps that end in the conclusion. Start with $p$ and prove $q$, or start with $\neg q$ and prove $\neg p$.
  – If this doesn’t work, try backward reasoning. When trying to prove $q$, find a statement $r$ that we can prove with the property $p \rightarrow q$. 
Backward Reasoning

Example: Suppose that two people play a game taking turns removing, 1, 2, or 3 stones at a time from a pile that begins with 15 stones. The person who removes the last stone wins the game. Show that the first player can win the game no matter what the second player does.

Proof: Let \( n \) be the last step of the game.

Step \( n \): Player\(_1\) can win if the pile contains 1, 2, or 3 stones.
Step \( n-1 \): Player\(_2\) will have to leave such a pile if the pile that he/she is faced with has 4 stones.
Step \( n-2 \): Player\(_1\) can leave 4 stones when there are 5, 6, or 7 stones left at the beginning of his/her turn.
Step \( n-3 \): Player\(_2\) must leave such a pile, if there are 8 stones.
Step \( n-4 \): Player\(_1\) has to have a pile with 9, 10, or 11 stones to ensure that there are 8 left.
Step \( n-5 \): Player\(_2\) needs to be faced with 12 stones to be forced to leave 9, 10, or 11.
Step \( n-6 \): Player\(_1\) can leave 12 stones by removing 3 stones.

Now reasoning forward, the first player can ensure a win by removing 3 stones and leaving 12.
Proof and Disproof: Tilings

Example 1: Can we tile the standard checkerboard using dominos?
Solution: Yes! One example provides a constructive existence proof.

The Standard Checkerboard

Two Dominoes

One Possible Solution
Tilings

Example 2: Can we tile a checkerboard obtained by removing one of the four corner squares of a standard checkerboard?

Solution:

• Our checkerboard has $64 - 1 = 63$ squares.
• Since each domino has two squares, a board with a tiling must have an even number of squares.
• The number 63 is not even.
• We have a contradiction.
Example 3: Can we tile a board obtained by removing both the upper left and the lower right squares of a standard checkerboard?
Tilings

Solution?:

• There are 62 squares in this board.
• To tile it we need 31 dominoes.
• Key fact: Each domino covers one black and one white square.
• Therefore the tiling covers 31 black squares and 31 white squares.
• Our board has either 30 black squares and 32 white squares or 32 black squares and 30 white squares.
• Contradiction!
The Role of Open Problems

- Unsolved problems have motivated much work in mathematics. Fermat’s Last Theorem was conjectured more than 300 years ago. It has only recently been finally solved.

Fermat’s Last Theorem: The equation $x^n + y^n = z^n$ has no solutions in integers $x$, $y$, and $z$, with $xyz \neq 0$ whenever $n$ is an integer with $n > 2$.

A proof was found by Andrew Wiles in the 1990s

http://www.youtube.com/watch?v=7FnXgprKgSE
An Open Problem

• The 3x + 1 Conjecture: Let T be the transformation that sends an even integer x to x/2 and an odd integer x to 3x + 1. For all positive integers x, when we repeatedly apply the transformation T, we will eventually reach the integer 1.

For example, starting with x = 13:

T(13) = 3\cdot13 + 1 = 40, T(40) = 40/2 = 20, T(20) = 20/2 = 10,  
T(10) = 10/2 = 5, T(5) = 3\cdot5 + 1 = 16, T(16) = 16/2 = 8,  
T(8) = 8/2 = 4, T(4) = 4/2 = 2, T(2) = 2/2 = 1

The conjecture has been verified using computers up to 5.6 \cdot 10^{13}
Additional Proof Methods

• Later we will see many other proof methods:
  – Mathematical induction, which is a useful method for proving statements of the form $\forall n \, P(n)$, where the domain consists of all positive integers.
  – Structural induction, which can be used to prove such results about recursively defined sets.
  – Cantor diagonalization is used to prove results about the size of infinite sets.
  – Combinatorial proofs use counting arguments.
Example Proofs - 1

• Break up into groups of 3 or 4

• Using the definitions of even integer and odd integer, give a proof by contraposition that this statement is true for all integers $n$:
  – If $3n - 5$ is even, then $n$ is odd

• Give a proof by contradiction of:
  – “If $n$ is an even integer, then $3n + 7$ is odd.”
Example Proofs 1 – Solutions

• If $3n - 5$ is even, then $n$ is odd (direct proof)
  – Suppose $n$ is not odd.
  – Therefore $n$ is even and hence $n = 2k$.
  – Therefore $3n - 5 = 3(2k) - 5 = 6k - 5 = 6k - 6 + 1 = 2(3k - 3) + 1$.

• “If $n$ is an even integer, then $3n + 7$ is odd.” (proof by contradiction)
  – Suppose $n$ is even but $3n + 7$ is not odd.
  – Therefore $n = 2k$ and $3n + 7 = 2l$ for some integers $k$ and $l$.
  – Therefore $3(2k) + 7 = 2l$ by substituting $2k$ for $n$.
  – Therefore $6k + 7 = 2l$.
  – Therefore $2l - 6k = 7$.
  – Therefore $2(l - 3k) = 7$.
  – But in this equation the left side is even and the right side is odd, a contradiction.
Example Proofs - 2

• Prove that this statement is true for all integers $n$:
  – $n$ is odd if and only if $5n + 3$ is even.

• Prove or disprove
  – “Every integer is less than its cube”
Example Proofs 2 - Solution

- \( n \) is odd if and only if \( 5n + 3 \) is even.
  - We must prove that two statements are true: \( n \) is odd if \( 5n + 3 \) is even, and \( n \) is odd only if \( 5n + 3 \) is even.
  - (a) If \( 5n + 3 \) is even, then \( n \) is odd, and
  - (b) If \( n \) is odd, then \( 5n + 3 \) is even.

- It is easy to give a proof by contraposition of (a):
  - Suppose \( n \) is not odd, and therefore is even.
  - Therefore \( n = 2k \) for some integer \( k \).
  - Therefore \( 5n + 3 = 5(2k) + 3 = 10k + 3 = 2(5k + 1) + 1 \).
  - Therefore \( 5n + 3 \) is odd.

- It is also easy to give a direct proof of (b):
  - Suppose \( n \) is odd.
  - Therefore \( n = 2k + 1 \) for some integer \( k \).
  - Therefore \( 5n + 3 = 5(2k + 1) + 3 = 10k + 8 = 2(5k + 4) \).
  - Therefore \( 5n + 3 \) is even.
Example Proofs 2 - Solution

- “Every integer is less than its cube”
  False (-2) > (-8)
• **Prove:**
  – if $m$ and $n$ are even integers, then $mn$ is a multiple of 4.

• **Prove by contradiction:**
  – If $n$ is an even integer, then $n + 1$ is odd.
Example Proofs 3 – Solutions

- if $m$ and $n$ are even integers, then $mn$ is a multiple of 4.
  - If $m = 2k$ and $n = 2l$, then $mn = 4kl$. Hence $mn$ is a multiple of 4.

- Prove by contradiction: If $n$ is an even integer, then $n + 1$ is odd.
  - Suppose $n = 2k$ but $n + 1 = 2l$. Therefore $2k + 1 = 2l$ (even = odd), which is a contradiction
Quiz 1