Announcements

• Quiz 1 is today
• Homework 2 is due on Thursday
• Review first Chapter.

Collaboration Policy

• Homework assignments are to be completed by yourself
  – Do not discuss homework solutions with anyone other than a TA or the instructor (Piazza is encouraged for homework questions)
  – Students caught collaborating on homework solutions are in violation of the academic integrity policy

• Feel free to collaborate with others on the quiz problems
Topics

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

Proof Techniques

Suppose I said prove “if n is an integer, then n^2 >= n”
- p: n is an integer
- q: n^2 >= n

What if proving the case for p as an int is too difficult?
- What could I do?
- Break it up into cases?
  - p_1 = n is an int > 0
  - p_2 = n is an int < 0
  - p_3 = n is an int = 0

Proof by Cases
Proof Techniques - proof by cases

Suppose we want to prove a theorem of the form: \((p_1 \lor p_2 \lor \ldots \lor p_n) \rightarrow q\)

We can prove it in pieces corresponding to the cases, but which must be true?

A: \((p_1 \rightarrow q) \lor (p_2 \rightarrow q) \lor \ldots \lor (p_n \rightarrow q)\)

B: \((p_1 \rightarrow q) \land (p_2 \rightarrow q) \land \ldots \land (p_n \rightarrow q)\)

Ask the class

Suppose we want to prove a theorem of the form: \(p_1 \lor p_2 \lor \ldots \lor p_n \rightarrow q\)

We can prove it in pieces corresponding to the cases, but which must be true?

A: \((p_1 \rightarrow q) \lor (p_2 \rightarrow q) \lor \ldots \lor (p_n \rightarrow q)\)

B: \((p_1 \rightarrow q) \land (p_2 \rightarrow q) \land \ldots \land (p_n \rightarrow q)\)

C: This class is not fun AND difficult. 😞
Proof Techniques - proof by cases

Proof for $n=2$:

$(p_1 \lor p_2) \rightarrow q \equiv \neg (p_1 \lor p_2) \lor q$  
Defn of $\rightarrow$

$\equiv (\neg p_1 \land \neg p_2) \lor q$  
DeMorgan’s

$\equiv (\neg p_1 \lor q) \land (\neg p_2 \lor q)$  
Distributivity

$\equiv (p_1 \rightarrow q) \land (p_2 \rightarrow q)$  
Defn of $\rightarrow$

Proofs - something for everyone

“if $x$ is a perfect square, and $x$ is even, then $x$ is divisible by 4.”

Formally: $(p \land q) \rightarrow r$

Contrapositive: $\neg r \rightarrow \neg (p \land q) \equiv \neg r \rightarrow (\neg p \lor \neg q)$

Suppose $x$ is not divisible by 4. How many cases needed?

Then $x = 4k + 1$, or $x = 4k + 2$, or $x = 4k + 3$.

Now structure looks like $(u_1 \lor u_2 \lor u_3) \rightarrow (\neg p \lor \neg q)$

Case 1 ($&3$): $x = 4k + 1$, odd, corresponds to $\neg q$

Case 2: $x = 4k + 2$, even, so we need to prove it is not a perfect square.
“if \( x \) is a perfect square, and \( x \) is even, then \( x \) is divisible by 4.”

- Subgoal, prove Case 2:
- Case 2: \( x = 4k + 2 \), even (so we have to show not square).
  - But \( x = 4k + 2 = 2(2k + 1) \)
  - \( x \) is the product of 2 and an odd number.
- So, \( x \) is not a perfect square.

Existence Proofs

Two ways of proving \( \exists x \ P(x) \).

Either build one, or show one can be built.

- Constructive
- Non-constructive

Two examples, both involving \( n! \)

For the examples, think of \( n! \) as a list of factors.
Quantifiers: Existence Proofs

Example: Prove that for all positive integers \( n \), there exist \( n \) consecutive composite integers.

\( \forall n \text{ (positive integers)}, \exists x \text{ so that } x, x+1, x+2, \ldots, x+n-1 \text{ are all composite.} \)

Proof: Let \( n \) be an arbitrary integer.

\[(n + 1)! + 2 \text{ is divisible by } 2, \therefore \text{ composite.}\]
\[(n + 1)! + 3 \text{ is divisible by } 3, \therefore \text{ composite.}\]
\[\vdots\]
\[(n + 1)! + (n + 1) \text{ is divisible by } n + 1, \therefore \text{ composite.}\]

Quantifiers: Existence Proofs

Example: Prove that for all integers \( n \), there exists a prime \( p \) so that \( p > n \).

\( \forall n \text{ (integer)}, \exists p \text{ so that } p \text{ is prime, and } p > n. \)

Proof: Let \( n \) be an arbitrary integer, and consider \( n! + 1. \) If \( (n! + 1) \) is prime, we are done since \( (n! + 1) > n. \) But what if \( (n! + 1) \) is composite?

If \( (n! + 1) \) is composite then it has a prime factorization, \( p_1p_2\ldots p_n = (n! + 1) \)

Consider the smallest \( p_\text{min} \) how small can it be?
Quantifiers: Existence Proofs

\( \forall n \text{ (integers)}, \exists p \text{ so that } p \text{ is prime, and } p > n. \)

Proof: Let \( n \) be an arbitrary integer, and consider \( n! + 1 \). If \( (n! + 1) \) is prime, we are done since \( (n! + 1) > n \). But what if \( (n! + 1) \) is composite?

- If \( (n! + 1) \) is composite then it has a prime factorization, \( p_1 p_2 \ldots p_n = (n! + 1) \)
- Consider the smallest \( p_i \), and call it \( p \). How small can it be?
- So, \( p > n \), and we are done. BUT WE DON’T KNOW WHAT \( p \) IS!!!

Another Example - Largest Prime Number

**Prove by contradiction:** There is no largest prime number; that is, there are infinitely many prime numbers.

Proof:
Suppose the given conclusion is false; that is, there is a largest prime number \( p \). So the prime numbers we have are \( 2, 3, 5, \ldots, p \); assume there are \( k \) such primes, \( p_1, p_2, \ldots, p_k \).

Let \( x \) denote the product of all of these prime numbers plus one:
\[ x = (2 \times 3 \times 5 \ldots \times p) + 1. \]
Clearly, \( x > p \).

When \( x \) is divided by each of the primes \( 2, 3, 5, \ldots, p \), we get 1 as the remainder. So \( x \) is not divisible by any of the primes. Hence either \( x \) must be a prime, or if \( x \) is composite then it is divisible by a prime \( q \neq p \). In either case, there are more than \( k \) primes.

But this contradicts the assumption that there are \( k \) primes, so our assumption is false. In other words, there is no largest prime number.

From Discrete Mathematics with Applications, by Thomas Koshy
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 1 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.
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.

Tilings

Example 3: Can we tile a board obtained by removing both the upper left and the lower right squares of a standard checkerboard?

Nonstandard Checkerboard

Dominoes
**Tilings**

Solution?:
- There are 62 squares in this board.
- To tile it we need 31 dominos.
- *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

https://www.youtube.com/watch?v=BQG9McMC59U
### 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:

\[
T(13) = 3 \cdot 13 + 1 = 40, T(40) = 40/2 = 20, T(20) = 20/2 = 10,
\]

\[
T(10) = 10/2 = 5, T(5) = 3 \cdot 5 + 1 = 16, T(16) = 16/2 = 8,
\]

\[
T(8) = 8/2 = 4, T(4) = 4/2 = 2, T(2) = 2/2 = 1
\]

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.
Quiz 1