Lecture 7 Feb 4, 14

- Sections 1.7 and 1.8
- Some problems from Sec 1.8

Section Summary

- Proof by Cases
- Existence Proofs
  - Constructive
  - Nonconstructive
- Disproof by Counterexample
- Nonexistence Proofs
- Uniqueness Proofs
- Proof Strategies
- Proving Universally Quantified Assertions

Proof by Cases

- To prove a conditional statement of the form:

$$(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q$$

- Use the tautology

$$[(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q] \leftrightarrow$$
$$[(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)]$$

- Each of the implications $p_i \rightarrow q$ is a *case*.

Proof by Cases

Example: Let $a \,@\, b = \max\{a, b\} = a$ if $a \geq b$, otherwise $a \,@\, b = \max\{a, b\} = b$.

Show that for all real numbers a, b, c

$$(a \,@ b) \,@\, c = a \,@\, (b \,@\, c)$$

(This means the operation @ is associative.)

Proof: Let a, b, and c be arbitrary real numbers.

Then one of the following 6 cases must hold.

1. $a \geq b \geq c$
2. $a \geq c \geq b$
3. $b \geq a \geq c$
4. $b \geq c \geq a$
5. $c \geq a \geq b$
6. $c \geq b \geq a$

Continued on next slide →

Proof by Cases

Case 1: $a \geq b \geq c$

$(a \mathbin{@} b) = a$, $a \mathbin{@} c = a$, $b \mathbin{@} c = b$

Hence $(a \mathbin{@} b) \mathbin{@} c = a = a \mathbin{@} (b \mathbin{@} c)$

Therefore the equality holds for the first case.

A complete proof requires that the equality be shown to hold for all 6 cases. But the proofs of the remaining cases are similar. Try them.

Without Loss of Generality

Example: Show that if x and y are integers and both $x \cdot y$ *and* $x+y$ are even, then both x and y are even.

Proof: Use a proof by contraposition. Suppose x and y are not both even. Then, one or both are odd. Without loss of generality, assume that x is odd. Then $x = 2m + 1$ for some integer k.

Case 1: y is even. Then $y = 2n$ for some integer n, so $x + y = (2m + 1) + 2n = 2(m + n) + 1$ is odd.

Case 2: y is odd. Then $y = 2n + 1$ for some integer n, so $x \cdot y = (2m + 1)\,(2n + 1) = 2(2m \cdot n + m + n) + 1$ is odd.

We only cover the case where x is odd because the case where y is odd is similar. The use phrase *without loss of generality* (WLOG) indicates this. ◀

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
- $1729 = 10^3 + 9^3 = 12^3 + 1^3$ ◀

- How did we know to choose the number 1729? Is there a smaller number that works? Do you know how to search the next number that can be written as a sum of two cubes in two ways using a computer?
- if we replace cube by square, we can find a number more easily. How would you find it?

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.

Showing that 7 is a counterexample

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

How to show that 7 can't be written as a sum of 3 squares?

Proof: If $7 = a^2 + b^2 + c^2$, then $0 <= a, b, c <= 2$. Why?

Now we can consider all possible cases. There are 27 cases to consider for (a, b, c): (0, 0, 0), (0, 0, 1), …, (2, 2, 2). In all the cases, we can check that $a^2 + b^2 + c^2 \neq 7$

Uniqueness Proofs

- Some theorems asset 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 p 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.

Universally Quantified Assertions

- To prove theorems of the form $\forall x P(x)$,assume *x* is an arbitrary member of the domain and show that *P*(*x*) must be true. Using UG it follows that $\forall x P(x)$.

  Example: An integer *x* is even if and only if x^2 is even.

  Solution: The quantified assertion is

  $\forall x$ [*x* is even $\leftrightarrow$ x^2 is even]

  We assume *x* is arbitrary.

  Recall that $p \leftrightarrow q$ is equivalent to $(p \rightarrow q) \wedge (q \rightarrow p)$

  So, we have two cases to consider. These are considered in turn.

Continued on next slide →

Universally Quantified Assertions

Case 1. We show that if x is even then x^2 *is* even using a direct proof (the *only if* part or *necessity*).

If x is even then $x = 2k$ for some integer k.

Hence $x^2 = 4k^2 = 2(2k^2)$ which is even since it is an integer divisible by 2.

This completes the proof of case 1.

Case 2 on next slide →

Universally Quantified Assertions

Case 2. We show that if x^2 is even then x must be even (the *if* part or *sufficiency*). We use a proof by contraposition.

Assume x is not even and then show that 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 hence not even. This completes the proof of case 2.

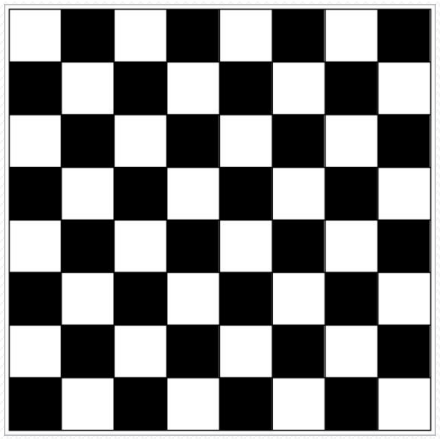
Since x was arbitrary, the result follows by UG.

Therefore we have shown that x is even if and only if x^2 is even. ◀

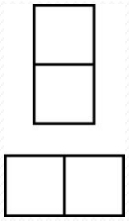
Proof and Disproof: Tilings

Example 1: Can we tile the standard checkerboard using dominos?

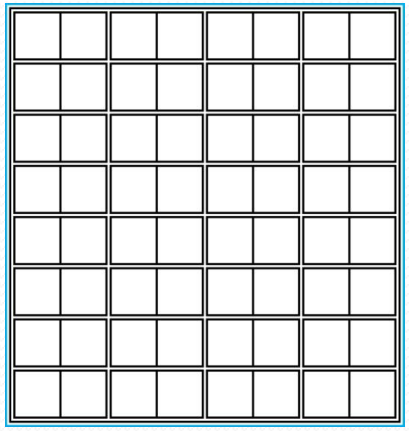
Solution: Yes! One example provides a constructive existence proof.



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?

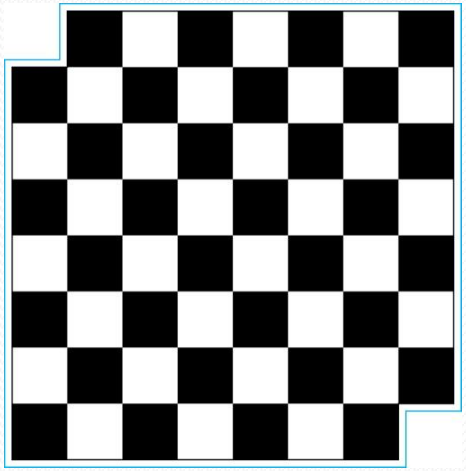
Solution:

- 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.

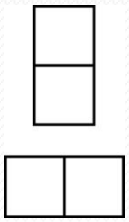
◀

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

Continued on next slide →

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!

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.

Some problems from Sec 1.8

- Problem 2: Prove that there are no positive perfect cubes less than 1000 that are the sum of the cubes of two positive integers.

Create a table in which each row is a perfect cube between 1 and 1000, and each column is a perfect cube between 1 and 1000. Fill the table with all possible ways of adding a row value and a column value. Check that the table (that has 100 entries) does not have 1000 in it.

In the next slide, we will show we can automate this process by writing a program in Python that will search for two numbers p and q such that $p > 0$, $q > 0$ and $p^3 + q^3 = K$ for a given value K.

Program for problem 2, Sec 1.8

```
def search(k):
    # seachers for a and b such that a^3 + b^3 = k
    # finds all solutions
    # if it can't find it, it prints "No solution"
    count = 0
    for a in range(1,k):
        for b in range(1,k):
            if (a*a*a + b*b*b == k):
                print("Solution: a = ", a, "b = ", b)
                count = count + 1
    if count == 0:
        print("No solution")
```

```
>>> search(1000)
No solution
>>> search(1729)
Solution: a =  1 b =  12
Solution: a =  9 b =  10
Solution: a =  10 b =  9
Solution: a =  12 b =  1
```

Problem 9, Sec 1.8

Prove that there are 100 consecutive positive integers that are not perfect squares. Is your proof constructive or nonconstructive?

Proof: Consider $100^2 = 10{,}000$. What is the next perfect square? It must be $101^2 = 10201$. How many numbers are between 10,000 and 10201?

This is a constructive proof since we explicitly constructed two perfect squares and showed that they are separated by more than 100 numbers and none of the intervening numbers can be perfect squares.

Problem 10, Sec 1.8

Prove that either $A = 2 \cdot 10^{500} + 15$ or $B = 2 \cdot 10^{500} + 16$ is not a perfect square. Is your proof constructive or nonconstructive?

Proof: (i) To prove such results, you should look for a property that perfect squares have, and then show that A or B does not have that property.

Note how we are using modus tollens here:

- Ax (x is a perfect square → P(x))
- The number A does not have property p, i.e., ~P(A)

From these two, we use existential instantiation and modus tollens, and conclude that A is not a perfect square.

What property can we use here? One that works is:
P(x): if x is odd → x leaves remainder 1 when divided by 4.

The details will be presented in class.

Problem 26, Sec 1.8

Suppose that five ones and four zeros are arranged around a circle. Between any two equal bits you insert a 0 and between any two unequal bits you insert a 1 to produce nine new bits. Then you erase the nine original bits. Show that when you iterate this procedure, you can never get nine zeros. [*Hint:* Work backward, assuming that you did end up with nine zeros.]

Proof: You can try to construct a proof using the hint.

We will give an equally easy, direct proof (using forward reasoning).

Claim (aka Lemma): A pattern P with at least one 0 and one 1 will always generate a new pattern with at least one 0 and one 1.

Proof sketch: In any circular string of 0's and 1's with at least one 0 and at least one 1, there will be two adjacent bits that are different, and also two adjacent bits that are the same.

From the lemma, the claim easily follows.