Proof Methods and Strategy

Section 1.8

Section Summary

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

Proof by Cases

- It is not always the case that you can prove a theorem using a single argument that holds for all possible cases.
- To Prove that a conditional statement $p \rightarrow q$ is true, it is convenient to use a disjunction $p1 \vee p2 \vee \cdots \vee pn$ instead of p as the hypothesis of the conditional statement, where p and $p1 \vee p2 \vee \cdots \vee pn$ are equivalent.

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, i=1…n* .
- Prove each case.

Proof by Cases

Ex: Show that for all real numbers a, b, c

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

[taking the maximum of two numbers 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: $a \geq b \geq c$

$\max(a, b) = a \qquad \max(a, c) = a \qquad \max(b, c) = b$

Hence $\max(\max(a, b), c) = a = \max(a, \max(b, c))$

Therefore the equality holds for the first case.

Case 2: $a \geq c \geq b$

...

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.

Proof by Cases

- EX: Prove that if n is an integer, then $n^2 \geq n$.

Solution: We can prove that $n^2 \geq n$ for every integer by considering three cases, when $n = 0$, when $n \geq 1$, and when $n \leq -1$. We split the proof into three cases because it is straightforward to prove the result by considering zero, positive integers, and negative integers separately.

Case (i): When $n = 0$, because $0^2 = 0$, we see that $0^2 \geq 0$. It follows that $n^2 \geq n$ is true in this case.

Case (ii): When $n \geq 1$, when we multiply both sides of the inequality $n \geq 1$ by the positive integer n, we obtain $n \cdot n \geq n \cdot 1$. This implies that $n^2 \geq n$ for $n \geq 1$.

Case (iii): In this case $n \leq -1$. However, $n^2 \geq 0$. It follows that $n^2 \geq n$.

Because the inequality $n^2 \geq n$ holds in all three cases, we can conclude that if n is an integer, then $n^2 \geq n$. ◀

Without Loss of Generality

- Without loss of generality (often abbreviated to WOLOG, WLOG or w.l.o.g.)
- Is used before an assumption in a proof which narrows the premise to some special case; it implies that the proof for that case can be easily applied to all others, or that all other cases are equivalent or similar.

Wikipedia

Without Loss of Generality

Ex: 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.

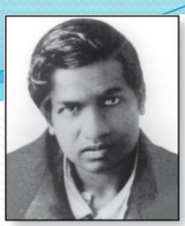
Suppose x and y are not both even. Then, one or both are odd. Without loss of generality, assume that x is odd. Then $x = 2m + 1$ for some integer m.

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 phrase *without loss of generality* (WLOG) indicates this.



Existence Proofs

Srinivasa Ramanujan
(1887-1920)

- Proof of theorems of the form $\exists x P(x)$.
- There are two ways to prove a theorem of this type.
  - Constructive
  - Nonconstructive
- 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).

Ex: 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

$$1729 = 10^3 + 9^3 = 12^3 + 1^3$$ ◀

Godfrey Harold Hardy
(1877-1947)

Nonconstructive Existence Proofs

- In a nonconstructive existence proof, we assume no c exists which makes $P(c)$ true and derive a contradiction.

Ex: Show that there exist irrational numbers x and y such that x^y is rational.

Proof: We know that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$. If it is rational, we have two irrational numbers x and y with x^y rational, namely $x = \sqrt{2}$ and $y = \sqrt{2}$. But if $\sqrt{2}^{\sqrt{2}}$ is irrational, then we can let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$ so that $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\sqrt{2})} = \sqrt{2}^2 = 2$. ◀

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 $\forall x P(x)$.

Ex: "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.

Ex: 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.
  1. First try a direct method of proof.
  2. 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.
  1. 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 $\neg p$.
  2. 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

Ex: 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 $\forall x P(x)$.

Ex: 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 integer 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.

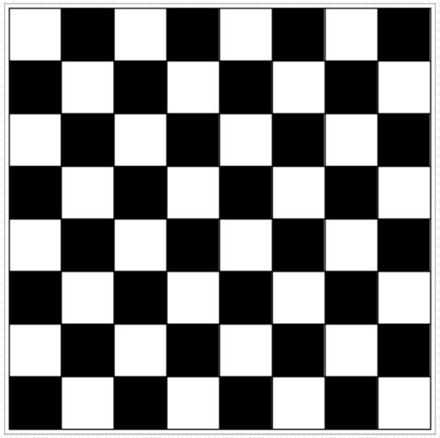
Since x was arbitrary, the result follows by UG.

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

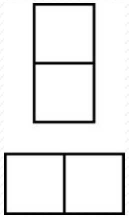
Proof and Disproof: Tilings

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

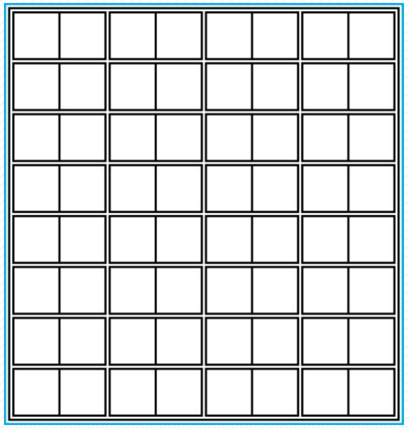
Solution: Yes! One example provides a constructive existence proof.



The Standard Checkerboard



Two Dominoes



One Possible Solution

Proof and Disproof: Tilings

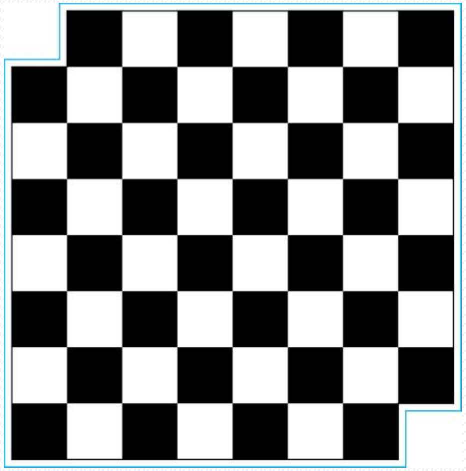
Ex 2: Can we tile a checkerboard obtained by removing one of the four corner squares of a standard checkerboard?

Solution:

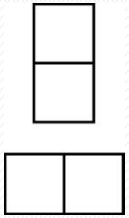
- Our checkerboard has $64 - 1 = 63$ squares.
- Since each domino has two squares, a board with a tiling must have an even number of squares.
- The number 63 is not even.
- We have a contradiction. ◄

Proof and Disproof: Tilings

Ex 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 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.

An Open Problem

Collatz Conjecture:
If you pick any positive integer n and apply the following rules,
1) if n is even then n/2
2) if n is odd then 3n+1
you will eventually reach the integer 1.

For example, starting with $x = 13$:

$13 = 3 \cdot 13 + 1 = 40$
$40 = 40/2 = 20$
$20 = 20/2 = 10$
$10 = 10/2 = 5$

$5 = 3 \cdot 5 + 1 = 16$
$16 = 16/2 = 8$
$8 = 8/2 = 4$
$4 = 4/2 = 2$
$2 = 2/2 = 1$

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.
- Combinatorial proofs use counting arguments.