Proof methods and Strategy

Proof methods (review)

$$p \rightarrow q$$

- Direct technique
  - Premise: p
  - Conclusion: q
- Proof by contraposition
  - Premise: $\neg q$
  - Conclusion: $\neg p$
- Proof by contradiction
  - Premise: $p \wedge \neg q$
  - Conclusion: a contradiction

Prove a theorem (review)

How to prove a theorem?

1. Choose a proof method
2. Construct argument steps

Argument:

premises

conclusion

Proof by cases

- Prove a theorem by considering different cases seperately

To prove q it is sufficient to prove

$\mathbf{p_1 \lor p_2 \lor \ldots \lor p_n}$

$\mathbf{p_1 \rightarrow q}$

$\mathbf{p_2 \rightarrow q}$

…

$\mathbf{p_n \rightarrow q}$

Exhaustive proof

- Exhaustive proof
  - Number of possible cases is relatively small.
  - A special type of proof by cases
  - Prove by checking a relatively small number of cases

Exhaustive proof (example)

Show that $n^2 \leq 2^n$ if n is positive integer with n <3.

Proof (exhaustive proof):

- Check possible cases
  - n=1 $1 \leq 2$
  - n=2 $4 \leq 4$

Exhaustive proof (example)

Prove that the only consecutive positive integers not exceeding 50 that are perfect powers are 8 and 9.

Proof (exhaustive proof):

- Check possible cases
  - a=2   1,4,9,16,25,36,49
  - a=3   1,8,27
  - a=4   1,16
  - a=5   1,32
  - a=6   1
- The only consecutive numbers that are perfect powers are 8 and 9.

Definition:
An integer is a perfect power if it equals n^a, where a in an integer greater than 1.

Proof by cases

Proof by cases must cover all possible cases.

Proof by cases (example)

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

Proof (proof by cases):

- Break the theorem into some cases
  1. $n = 0$
  2. $n \geq 1$
  3. $n \leq -1$

Proof by cases (example)

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

Proof (proof by cases):

- Check possible cases
  1. $n = 0$ $\quad 0^2 \geq 0$
  2. $n \geq 1$
     $n.n \geq 1.n \quad n^2 \geq n$
  3. $n \leq -1$
     $n^2 \geq 0 \quad n^2 \geq n$
- $n^2 \geq n$ holds in all three cases, we can conclude that if n is an integer, then $n^2 \geq n$.

Proof by cases (example)

Prove that |xy|=|x||y|, where x and y are real numbers.

Definition:
The absolute value of a, |a|, equals a when a≥0 and equals -a when a<0.

Proof (proof by cases):

- Break the theorem into some cases
  1. x and y both nonnegative
  2. x nonnegative and y is negative
  3. x negative and y nonnegative
  4. x and y both negative

Proof by cases (example)

Prove that $|xy|=|x||y|$, where x and y are real numbers.

Definition:
The absolute value of a, $|a|$, equals a when $a \geq 0$ and equals $-a$ when $a<0$.

Proof (proof by cases):

- Check possible cases
  1. x and y both nonnegative

     $|xy| = xy$ $\quad$ $|x|=x$ $\quad$ $|y|=y$ $\quad$ $|x||y| = xy$

     $|xy| = |x||y|$

  2. x nonnegative and y is negative

     $|-xy| = xy$ $\quad$ $|x|=x$ $\quad$ $|-y| = y$ $\quad$ $|x||y| = xy$

     $|xy| = |x||y|$

Proof by cases (example)

Prove that $|xy|=|x||y|$, where x and y are real numbers.

Definition:
The absolute value of a, $|a|$, equals a when $a\geq 0$ and equals $-a$ when $a<0$

Proof (proof by cases):

- Check possible cases
  3. x negative and y nonnegative

     $|-xy| = xy$ $\quad |-x|=x \quad |y| = y$ $\quad |-x||y| = xy$

     $|xy| = |x||y|$
  4. x and y both negative

     $|-x.-y| = xy$ $\quad |-x|=x \quad |-y| = y$ $\quad |-x||-y| = xy$

     $|xy| = |x||y|$
- It is true for all four cases, so $|xy|=|x||y|$, where x and y are real numbers.

Proof by cases (example)

Prove that $x^2 + 3y^2 = 8$ is false where x and y are integers.

Proof (proof by cases):

- Find possible cases
  - $x = -2, -1, 0, 1, 2$
  - $y = -1, 0, 1$
- Check possible cases
  - $x^2 = 0, 1, 4$
  - $3y^2 = 0, 3$
  - Largest sum of x^2 and $3y^2$ is 7.
- So, $x^2 + 3y^2 = 8$ is false where x and y are integers.

Without loss of generality

- How to shorten the proof by cases.
  - If same argument is used in different cases.
    - Proof theses cases together, **without loss of generality (WLOG).**
  - Incorrect use of this principle can lead to errors.

Without loss of generality (example)

Prove that $|xy|=|x||y|$, where x and y are real numbers.

Proof (proof by cases):

- Check possible cases
  1. x and y both nonnegative
  2. x nonnegative and y is negative
  3. x negative and y nonnegative
  4. x and y both negative

Without loss of generality (example)

Prove that $|xy|=|x||y|$, where x and y are real numbers.

Proof (proof by cases):

- Check possible cases
  1. x and y both nonnegative
  2. x nonnegative and y is negative

     $|xy| = -xy$ $\quad$ $|x|=x \quad |y| = -y$ $\quad$ $|x||y| = -xy$

     $|xy| = |x||y|$
  3. x negative and y nonnegative

     we can complete this case using the same argument as we used for case 2.
  4. x and y both negative

Without loss of generality (example)

Show that $(x+y)^r < x^r + y^r$ where x and y are positive real numbers and r is a real number with $0 < r < 1$.

Proof:

- Without loss of generality assume $x+y = 1$.

  $x + y = t$

  $(x/t) + (y/t) = 1$

  $((x/t)+(y/t))^r < (x/t)^r + (y/t)^r$

  $t^r ((x/t)+(y/t))^r < t^r (x/t)^r + t^r (y/t)^r$

  $(x+y)^r < x^r + y^r$

  So, the inequality $(x+y)^r < x^r + y^r$ is the same when $(x+y=1)$ and $(x+y=t)$.

Without loss of generality (example)

Show that $(x+y)^r < x^r + y^r$ where x and y are positive real numbers and r is a real number with $0 < r < 1$.

Proof:

- We assume $x+y = 1$.
- Since x and y are positive, $0< x < 1$ and $0< y < 1$.
- $0 < r < 1$ $\quad$ $0 < 1-r < 1$
- $x^{1-r} < 1$ $\quad$ $y^{1-r} < 1$
- $x / x^r < 1$ $\quad$ $y / y^r < 1$
- $x^r > x$ $\quad$ $y^r > y$
- $x^r + y^r > x+y=1$
- $x^r + y^r > (x+y)^r = 1$

Errors in proofs (example)

If x is a real number, then x^2 is a positive real number.

Proof:

Case 1: x is positive

x^2 is the product of two positive numbers, so x^2 is positive.

Case2: x is negative

x^2 is the product of two negative numbers, so x^2 is positive.

- **Case x=0 is missed.**
  - **Case 3: x=0**

    $x^2 = 0$, so x^2 is not positive
  - Thus the theorem is false.

Errors in proofs (example)

Show that 1 = 2.

Proof:

Assume a and b are two equal positive integers.

1. $a=b$
2. $a^2 = ab$
3. $a^2 - b^2 = ab - b^2$
4. $(a - b)(a + b) = b(a - b)$
5. $a + b = b$
6. $2b = b$
7. $1 = 2$

- Step 5: $a - b = 0$, so dividing both sides of the equation by $a-b$ is wrong.

Existence proofs

- A proof of a proposition of the form $\exists x\, P(x)$ is called an existence proof.
- Existence proof
  - Constructive proof
    - Finding an element a that P(a) is true.
  - Nonconstructive proof
    - Prove $\exists x\, P(x)$ is true in some other way.
    - Prove by contradiction
      - $\neg \exists x\, P(x)$ ($\equiv \forall x\, \neg P(x)$) implies a contradiction.

Constructive proof (example)

There is a positive integer that can be written as the sum of squares of two positive integers.

Proof:

- Find an example
  - $5 = 2^2 + 1^2$

Nonconstructive proof (example)

There exist irrational numbers x and y such that x^y is rational

Proof:

- By previous example
  - $\sqrt{2}$ is irrational.
- $(\sqrt{2})^{\sqrt{2}}$
- Case 1: If $(\sqrt{2})^{\sqrt{2}}$ is rational
  - Thus, theorem is proved
- Case 2: If $(\sqrt{2})^{\sqrt{2}}$ is irrational
  - $((\sqrt{2})^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2} \cdot \sqrt{2}} = (\sqrt{2})^2 = 2$
  - 2 (=2/1) is rational.
  - Thus, theorem is proved.

Definition:
The real number r is rational if r=p/q, ∃ integers p and q that $q \neq 0$.

Uniqueness proofs

- Theorem assert the existence of a unique element.
  - Unique element:
    - There is exactly one element with a particular property.
  - What we need to show?
    - There is an element x with this property. **(Existence)**
    - No other element y has this property.

      If y has this property too, then x = y. **(Uniqueness)**

Uniqueness proofs

- Proof of *"there is an element with unique property P(x)"*:

$$\exists x\ (P(x) \wedge \forall y\ (y \neq x \rightarrow \neg P(x)))$$

Uniqueness proofs (example)

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

Proof: (uniqueness proof)

- Existence proof
  - $r = - b/a$
  - $a(-b/a) + b = -b + b = 0$

Uniqueness proofs (example)

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

Proof: (uniqueness proof)

- uniqueness proof
  - Assume s is a real number such that $as + b = 0$.

    $as + b = ar + b$

    $as = ar$

    $s = r \qquad (a \neq 0)$
  - So, if $s \neq r$, then $as+b \neq 0$.

Proof strategies

- Finding proofs can be challenging.
  - Replace terms by their definitions
  - Carefully analyze hypotheses and conclusion
  - Choose a proof technique
  - Attempt to prove the theorem
  - If it fails try different proof methods

Forward and backward reasoning

$$\mathbf{p \rightarrow q}$$

- Forward reasoning
  - Assume premises are true.
  - Using premises, axioms, other theorems, construct a sequence of steps that leads to the conclusion.
- Backward reasoning
  - Work on the conclusion
  - Find a statement r that you can prove $\mathbf{r \rightarrow q}$.

Backward reasoning (example)

Prove that arithmetic mean of two positive real numbers is more than their geometric mean.

Proof: (backward reasoning)

$(x+y)/2 > \sqrt{xy}$

$(x+y)^2/4 > xy$

$(x+y)^2 > 4xy$

$x^2 + 2xy + y^2 > 4xy$

$x^2 - 2xy + y^2 > 0$

$(x-y)^2 > 0$

We can easily reverse the steps to construct a proof using forward reasoning.

Arithmetic mean of x and y:
$(x+y)/2$
Geometric mean of x and y:
$\sqrt{xy}$

Backward reasoning (example)

Prove that arithmetic mean of two positive real numbers is more than their geometric mean.

Proof: (backward reasoning)

$(x-y)^2 > 0$

$x^2 - 2xy + y^2 > 0$

$x^2 + 2xy + y^2 > 4xy$

$(x+y)^2 > 4xy$

$(x+y)^2/4 > xy$

$(x+y)/2 > \sqrt{xy}$

Arithmetic mean of x and y:
$(x+y)/2$
Geometric mean of x and y:
$\sqrt{xy}$

Backward reasoning (example)

Game:

- There are 15 stones on a pile
- Two players takes turn to remove stones from the pile.
- A player can remove one, two or three stones at a time from the pile.
- The player who removes the last stone wins the game.

Show that player 1 can win the game no matter what player 2 does.

Backward reasoning (example)

Proof: (backward reasoning)

Find a strategy for player 1 that player 1 always wins.

(backward reasoning)

- Player 1 wins.
- At last step, 1,2 or 3 stones are left on the pile.

  (How can player 1 make player 2 leave 1, 2 or 3 stones on the pile?)
- Player 1 leaves 4 stones on the pile.

  (How many stones should be left on the pile for player 1?)
- 5, 6 or 7 stones are left on the pile for player 1.

  (How can player 1 make player 2 leave 5, 6 or 7 stones on the pile?)

Backward reasoning (example)

Proof: (backward reasoning)

- Player 1 leaves 8 stones on the pile.

  (How many stones should be left on the pile for player 1?)
- 9, 10 or 11 stones are left on the pile for player 1.

  (How can player 1 make player 2 leave 9, 10 or 11 stones on the pile?)
- Player 1 leaves 12 stones on the pile.

Backward reasoning (example)

Proof: (backward reasoning)

- Strategy for player 1
  - Turn 1: leave 12 stones on the pile for player 2
  - Turn 2: player 2
  - Turn 3: leave 8 stones on the pile for player 2
  - Turn 4: player 2
  - Turn 5: leave 4 stones on the pile for player 2
  - Turn 6: player 2
  - Turn 7: removes all stones

Player 1 wins.

Adapting existing proofs

Often an existing proof can be adapted to prove a new result.

Some of the ideas in existing proofs may be helpful.

Adapting existing proofs (example)

If 3 is a factor of n^2, then 3 is a factor of n.

Proof (proof by contradiction):

Assume 3 is a factor of n^2 and 3 is not a factor of n.

$\exists a \quad n^2 = 3a$

$\exists b \quad n = 3b+1 \qquad$ or $\qquad n=3b+2$

Case 1: $n=3b+1$

$n^2 = (3b+1)^2 = 9b^2 + 6b + 1 = 3\,(3b^2 + 2b) + 1$

Let $k = 3b^2 + 2b$.

$n^2 = 3k + 1 \qquad$ So, 3 is not a factor of n^2.

(**Contradiction**)

Adapting existing proofs (example)

If 3 is a factor of n^2, then 3 is a factor of n.

Proof (proof by contradiction):

Assume 3 is a factor of n^2 and 3 is not a factor of n.

$\exists a \quad n^2 = 3a$

$\exists b \quad n = 3b+1 \qquad$ or $\qquad n=3b+2$

Case 2: $n=3b+2$

$n^2 = (3b+2)^2 = 9b^2 + 12b + 4 = 3\,(3b^2 + 4b + 1) + 1$

Let $k = 3b^2 + 4b + 1$.

$n^2 = 3k + 1 \qquad$ So, 3 is not a factor of n^2.

(**Contradiction**)

So, if 3 is a factor of n^2, then 3 is a factor of n.

Adapting existing proofs (example)

Prove that $\sqrt{3}$ is irrational.

Definition:
The real number r is rational if r=p/q, ∃ integers p and q that $q \neq 0$.

Proof (proof by contradiction):

Assume $\sqrt{3}$ is rational.

$\exists a,b \quad \sqrt{3} = a/b \quad b \neq 0$

If a and b have common factor, remove it by dividing a and b by it.

$\sqrt{3} = a/b$

$3 = a^2 / b^2$

$3b^2 = a^2$

So, 3 is factor of $a^2$and by previous theorem, 3 is factor of n.

Adapting existing proofs (example)

Prove that $\sqrt{3}$ is irrational.

Definition:
The real number r is rational if r=p/q, ∃ integers p and q that $q \neq 0$.

Proof (proof by contradiction):

$3b^2 = a^2$

$\exists k \quad a = 3k.$

$3b^2 = 9k^2$

$b^2 = 3k^2$

So, 3 is factor of b^2 and by previous theorem, 3 is factor of b.

$\exists m \qquad b = 3m.$

So, a and b have common factor 3 which contradicts the Assumption.

Looking for counterexample

- Theorem proof
  - You might first try to prove theorem.
  - If your attempts are unsuccessful, try to find counterexample.

Looking for counterexample (example)

Every positive integer is the sum of the squares of three integers.

Proof:

- Try to find a counterexample

$$1 = 0^2 + 0^2 + 1^2$$
$$2 = 0^2 + 1^2 + 1^2$$
$$3 = 1^2 + 1^2 + 1^2$$
$$4 = 0^2 + 0^2 + 2^2$$
$$5 = 0^2 + 1^2 + 2^2$$
$$6 = 1^2 + 1^2 + 2^2$$
$$7 = ?$$

Looking for counterexample (example)

Every positive integer is the sum of the squares of three integers.

Proof:

- Try to find a counterexample

  7 is a counterexample.

  Since squares less than 7 are 0, 1 and 4, 7 cannot be written as a sum of three of these numbers.