Proof Methods

Section 1.7-1.8

Proofs of Mathematical Statements

- A *proof* is a valid argument that establishes the truth of a statement.
- Proofs can be used to prove mathematical theorems.
- Proofs have many practical applications:
  - verification that computer programs are correct
  - establishing that operating systems are secure
  - enabling programs to make inferences in artificial intelligence
  - showing that system specifications are consistent

Forms of Theorems

- Theorem is a statement that can be shown to be true.
- Many theorems have the form:

$$p \rightarrow q$$

$$\forall x(P(x) \rightarrow Q(x))$$

- To prove them, we show that where *c* is an arbitrary element of the domain

$$P(c) \rightarrow Q(c)$$

- $p \leftrightarrow q$, $\exists x\, P(x)$, $\forall x\, P(x)$……

Proof methods 1,2

- *Trivial Proof*: If we know q is true, then $p \to q$ is true as well.

  "If it is raining then $1=1$."

- *Vacuous Proof*: If we know p is false then $p \to q$ is true as well.

  "If $2 + 2 = 5$then orange is purple ."

[Even though these examples seem silly, both trivial and vacuous proofs are used in the following chapters]

Discrete Mathematics

Proof method 3

- *Direct Proof*: Assume that p is true. Use rules of inference, logical equivalences, axioms and definitions to show that *q* must also be true.

Example: Give a direct proof of the theorem "If n is an odd integer, then n^2 is odd."

Definition: The integer n is even if there exists an integer k such that $n = 2k$, and n is odd if there exists an integer k, such that $n = 2k + 1$. Note that every integer is either even or odd and no integer is both even and odd.

Even and Odd Integers

Solution: Assume that n is odd. Then $n = 2k + 1$ for an integer k. Squaring both sides of the equation, we get:

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2r + 1,$$

where $r = 2k^2 + 2k$, an integer.

We have proved that if n is an odd integer, then n^2 is an odd integer.

Proving Conditional Statements: $p \to q$

Definition: The real number *r* is *rational* if there exist integers *p* and *q* where $q \neq 0$ such that *r* = *p*/*q*

Example: Prove that the sum of two rational numbers is rational.

Solution: Assume *r* and *s* are two rational numbers. Then there must be integers *p, q* and also *t, u* such that

$$r = p/q, \quad s = t/u, \quad u \neq 0, \quad q \neq 0$$

$$r + s = \frac{p}{q} + \frac{t}{u} = \frac{pu + qt}{qu} = \frac{v}{w}$$

where $v = pu + qt$

$w = \mathrm{qu} \neq 0$

◀

Thus the sum is rational.

Proof methods 4

– *Proof by Contraposition*: Assume $\neg q$ and show $\neg p$ is true also. This is sometimes called an *indirect proof* method. If we give a direct proof of $\neg q \rightarrow \neg p$ then we have a proof of $p \rightarrow q$.

Why does this work?

Example: Prove that if n is an integer and $3n + 2$ is odd, then n is odd.

Solution: Assume n is even. So, $n = 2k$ for some integer k. Thus

$$3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1) = 2j \text{ for } j = 3k + 1$$

Therefore $3n + 2$ is even. Since we have shown $\neg q \rightarrow \neg p$, $p \rightarrow q$ must hold as well. If n is an integer and $3n + 2$ is odd (not even) , then n is odd (not even).

Proof methods 5

- *Proof by Contradiction*:

To prove p, assume $\neg p$ and derive a contradiction such as $p \wedge \neg p$. (an indirect form of proof). Since we have shown that $\neg p \rightarrow \mathbf{F}$ is true , it follows that the contrapositive $\mathbf{T} \rightarrow p$ also holds.

Example

- **Example**: Use a proof by contradiction to give a proof that √2 is irrational.

Solution: Suppose √2 is rational. Then there exists integers *a* and *b* with √2 = *a*/*b*, where *b* ≠ 0 and *a* and *b* have no common factors (see Chapter 4). Then

$$2 = \frac{a^2}{b^2} \qquad 2b^2 = a^2$$

Therefore a^2 must be even. If a^2 is even then *a* must be even (an exercise). Since *a* is even, $a = 2c$ for some integer *c*. Thus,

$$2b^2 = 4c^2 \qquad b^2 = 2c^2$$

Therefore b^2 is even. Again then *b* must be even as well.

But then 2 must divide both *a* and *b*. This contradicts our assumption that *a* and *b* have no common factors. We have proved by contradiction that our initial assumption must be false and therefore √2 is irrational.

Example

前提：$\neg(p\wedge q)\vee r$，$r\to s$，$\neg s$，p

结论：$\neg q$

① q	P	
② $r\to s$	P	
③ $\neg s$	P	
④ $\neg r$	②③	MT
⑤ $\neg(p\wedge q)\vee r$	P	
⑥ $\neg(p\wedge q)$	④⑤	DS
⑦ $\neg p\vee\neg q$	⑥	DM
⑧ $\neg p$	①⑦	DS
⑨ p	P	
⑩ $\neg p\wedge p$	⑧⑨	Conjunction

Proof method 6

Proof by cases:

$(P1 \vee P2 \vee \ldots \vee Pn) \rightarrow Q$

$\Leftrightarrow \neg P1 \wedge \neg P2 \wedge \ldots \wedge \neg Pn \vee Q$

$\Leftrightarrow (\neg P1 \vee Q) \wedge (\neg P2 \vee Q) \wedge \ldots \wedge (\neg Pn \vee Q)$

$\Leftrightarrow (P1 \rightarrow Q) \wedge (P2 \rightarrow Q) \wedge \ldots \wedge (Pn \rightarrow Q)$

This statement can be proved by proving each of the n conditional statement. For i, $P_i \rightarrow Q$

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: $a \geq b \geq c$

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

Hence $(a @ b) @ c = a = a @ (b @ c)$

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.

Proof method 7

CP rule(演绎定理) Conjunction Premises rules

$$(P_1 \wedge P_2 \wedge \ldots \wedge P_n) \rightarrow (P \rightarrow Q)$$

$$\Leftrightarrow \neg (P1 \wedge P2 \wedge \ldots \wedge Pn) \vee (P \rightarrow Q)$$

$$\Leftrightarrow \neg (P1 \wedge P2 \wedge \ldots \wedge Pn) \vee (\neg P \vee Q)$$

$$\Leftrightarrow \neg P1 \vee \neg P2 \vee \ldots \vee \neg Pn \vee \neg P \vee Q$$

$$\Leftrightarrow (\neg P1 \vee \neg P2 \vee \ldots \vee \neg Pn \vee \neg P) \vee Q$$

$$\Leftrightarrow \neg (P1 \wedge P2 \wedge \ldots \wedge Pn \wedge P) \vee Q$$

$$\Leftrightarrow (P1 \wedge P2 \wedge \ldots \wedge Pn \wedge P) \rightarrow Q$$

P can be regarded as one of premises

Example

Premises: $p\vee q$, $p\rightarrow r$, $r\rightarrow\neg s$

Conclusion: $s\rightarrow q$

①	s	P
②	$p\rightarrow r$	P
③	$r\rightarrow\neg s$	P
④	$p\rightarrow\neg s$	②③HS
⑤	$\neg p$	①④MT
⑥	$p\vee q$	P
⑦	q	⑤⑥DS
⑧	$s\rightarrow q$	CP

Biconditional Statements proof

- To prove a theorem that is a biconditional statement, that is, a statement of the form $p \leftrightarrow q$, we show that $p \rightarrow q$ and $q \rightarrow p$ are both true.

Example: Prove the theorem: "If n is an integer, then n is odd if and only if n^2 is odd."

Solution: We have already shown (previous slides) that both $p \rightarrow q$ and $q \rightarrow p$. Therefore we can conclude $p \leftrightarrow q$.

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

$$1729 = 10^3 + 9^3 = 12^3 + 1^3 \quad \blacktriangleleft$$

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

  $\forall x\, [x \text{ is even} \leftrightarrow x^2 \text{ is even}]$

  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.

◀

Uniqueness Proofs

- Some theorems tell 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 $r = s$.

◀

homework

P57. 23

a): $P(x)$: x is a student;

$Q(x)$: x can speak Hindi

Domain consists of the students.

$$\exists x\, Q(x)$$

Domain consists of all people.

$$\exists x\,(P(x) \land Q(x))$$

b) $R(x)$: x is friendly.

1. $\forall x\, R(x)$

2. $\forall x\,(P(x) \to R(x))$

homework

P84 29.

Solution:

1.	$\exists x \neg P(x)$	P
2.	$\neg P(a)$	1. EI.
3.	$\forall x (P(x) \vee Q(x))$	P
4.	$P(a) \vee Q(a)$	3. UI.
5.	$Q(a)$	2. 4. DS.
6.	$\forall x (\neg Q(x) \vee S(x))$	P
7.	$\neg Q(a) \vee S(a)$	6. UI
8.	$S(a)$	5. 7. DS.
9.	$\forall x (R(x) \rightarrow \neg S(x))$	P
10	$R(a) \rightarrow \neg S(a)$	9. UI
11	$\neg R(a)$	8. 10. MT
12.	$\exists x \neg R(x)$	11. EG

homework

P80 Answer to 28.

proof:

step	statement	Reason
1	$\forall x\,(P(x) \vee Q(x))$	P
2.	$P(a) \vee Q(a)$	UI from (1)
3.	$\forall x((\neg P(x) \wedge Q(x)) \rightarrow R(x))$	P
4.	$\neg P(a) \wedge Q(a) \rightarrow R(a)$	UI from (3)
5.	$P(a) \vee \neg Q(a) \vee R(a)$	Conditional Equivalence from (4)
6	$P(a) \vee R(a) \vee \neg Q(a)$	Commutative law from (5)
7.	$P(a) \vee R(a) \vee P(a)$	Resolution from (2)(6)
8.	$P(a) \vee R(a)$	Idempotent law from (7)
9.	$\neg R(a) \rightarrow P(a)$	Conditional Equivalence from (8)
10	$\forall x(\neg R(x) \rightarrow P(x))$	UG from (9)

homework

- 1.7: P95 8, 20, 28,
- 1.8: P113 6
- Proof the following valid arguments
- $(a \rightarrow b) \wedge (a \rightarrow c), \neg(b \wedge c),\ d \vee a \Rightarrow d$