2.2 More Methods of Proof 更多的证明方法

- **Proof by Contradiction 反证法**
- **Proof by Contrapositive 逆否证明法**
- **Proof by Cases 分情况证明法**
- **Proofs of Equivalence 等价证明法**
- **Existence Proofs 存在性证明法**

Proof by Contradiction 反证法

A **proof by contraction** establishes $p \to q$ by assuming that the hypothesis p is true and that the conclusion q is false and then, **using p and $\neg q$** as well as other axioms, definitions, previously derived theorems, and rules of inference, derives a contradiction.

Proof by Contradiction 反证法

A **proof by contraction** establishes $p \to q$ by assuming that the hypothesis p is true and that the conclusion q is false and then, **using p and $\neg q$** as well as other axioms, definitions, previously derived theorems, and rules of inference, derives a contradiction.

A proof by contradiction is sometimes called an **indirect proof** （间接证明）.

Proof by Contradiction 反证法

A **proof by contraction** establishes $p \to q$ by assuming that the hypothesis p is true and that the conclusion q is false and then, **using p and $\neg q$** as well as other axioms, definitions, previously derived theorems, and rules of inference, derives a contradiction.

The method of **proof by contradiction** of a theorem $p \to q$ consists of the following steps:

1. Assume p is true and q is false
2. Show that $\neg p$ is also true.
3. Then we have that $p \wedge \neg p$ is true.
4. But this is impossible, since the statement $p \wedge \neg p$ is always false. There is a contradiction!
5. So, q cannot be false and therefore it is true.

Proof by Contradiction 反证法

Example 2.2.1 Give a proof by contradiction of the following statement:

For every $n \in \mathbf{Z}$, if n^2 is even, then n is even.

Proof by Contradiction 反证法

Example 2.2.1 Give a proof by contradiction of the following statement:

For every $n \in \mathbf{Z}$, if n^2 is even, then n is even.

The method of **proof by contradiction** of a theorem $p \to q$ consists of the following steps:

1. Assume p is true and q is false
2. Show that $\neg p$ is also true.
3. Then we have that $p \wedge \neg p$ is true.
4. But this is impossible, since the statement $p \wedge \neg p$ is always false. There is a contradiction!
5. So, q cannot be false and therefore it is true.

Proof by Contradiction 反证法

Example 2.2.1 Give a proof by contradiction of the following statement:

For every $n \in \mathbf{Z}$, if n^2 is even, then n is even.

Proof We give a proof by contradiction. Thus we assume the hypothsis n^2 is even and that the conclustion is false n is odd. Since n is odd, there exists an integer k such $n = 2k + 1$. Now

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Thus n^2 is odd, which contradicts the hypothesis n^2 is even.
The proof by contradiction is complete. We have proved that For every $n \in \mathbf{Z}$, if n^2 is even, then n is even.

The method of **proof by contradiction** of a theorem $p \rightarrow q$ consists of the following steps:

1. Assume p is true and q is false
2. Show that $\neg p$ is also true.
3. Then we have that $p \wedge \neg p$ is true.
4. But this is impossible, since the statement $p \wedge \neg p$ is always false. There is a contradiction!
5. So, q cannot be false and therefore it is true.

Proof by Contradiction 反证法

Example 2.2.1 Give a proof by contradiction of the following statement:

For all real numbers x and y, if $x + y \geq 2$, then either $x \geq 1$ or $y \geq 1$.

The method of **proof by contradiction** of a theorem $p \to q$ consists of the following steps:

1. Assume p is true and q is false
2. Show that $\neg p$ is also true.
3. Then we have that $p \land \neg p$ is true.
4. But this is impossible, since the statement $p \land \neg p$ is always false. There is a contradiction!
5. So, q cannot be false and therefore it is true.

Proof by Contrapositive 逆否证明法

Suppose that we give a proof by contradiction of $p \rightarrow q$ in which, as in Examples 2.2.1and 2.2.2, we deduce $\neg p$. In effect, we have proved $\neg q \rightarrow \neg p$.

Recall that $p \rightarrow q$ and $\neg q \rightarrow \neg p$ are equivalent. This special case of proof by contradiction is called **proof by contrapositive**.

Example 2.2.4 Give a proof by contrapositive to prove that
for all $x \in \mathbf{R}$, if x^2 is irrational, then x is irrational.

Proof by Contrapositive 逆否证明法

Suppose that we give a proof by contradiction of $p \to q$ in which, as in Examples 2.2.1and 2.2.2, we deduce $\neg p$. In effect, we have proved $\neg q \to \neg p$.

Recall that $p \to q$ and $\neg q \to \neg p$ are equivalent. This special case of proof by contradiction is called **proof by contrapositive**.

Example 2.2.4 Give a proof by contrapositive to prove that

for all $x \in \mathbf{R}$, if x^2 is irrational, then x is irrational.

if x is not irrational, then x^2 is not irrational

$\Leftrightarrow$ if x is rational, then x^2 is rational

Proof by Contrapositive 逆否证明法

Suppose that we give a proof by contradiction of $p \to q$ in which, as in Examples 2.2.1and 2.2.2, we deduce $\neg p$. In effect, we have proved $\neg q \to \neg p$.

Recall that $p \to q$ and $\neg q \to \neg p$ are equivalent. This special case of proof by contradiction is called **proof by contrapositive**.

Example 2.2.4 Give a proof by contrapositive to prove that

for all $x \in \mathbf{R}$, if x^2 is irrational, then x is irrational.

Proof We begin by letting x be an arbitrary real number. We prove the contrapositive of the given statement, which is
if x is not irrational, then x^2 is not irrational
or, equivalently,
if x is rational, then x^2 is rational.
So suppose that x is rational. Then $x = p/q$ for some integers p and q.
Now $x^2 = p^2/q^2$.Since x^2 is the quotient of integers, x^2 is rational. The proof is complete.

Proof by Contrapositive 逆否证明法

Suppose that we give a proof by contradiction of $p \to q$ in which, as in Examples 2.2.1and 2.2.2, we deduce $\neg p$. In effect, we have proved $\neg q \to \neg p$.

Recall that $p \to q$ and $\neg q \to \neg p$ are equivalent. This special case of proof by contradiction is called **proof by contrapositive**.

Exercise1 Give a proof by contrapositive to prove that

If $3n + 2$ is odd, then n is odd.

Proof by Contrapositive 逆否证明法

Suppose that we give a proof by contradiction of $p \rightarrow q$ in which, as in Examples 2.2.1and 2.2.2, we deduce $\neg p$. In effect, we have proved $\neg q \rightarrow \neg p$.

Recall that $p \rightarrow q$ and $\neg q \rightarrow \neg p$ are equivalent. This special case of proof by contradiction is called **proof by contrapositive**.

Example 2.2.1 For every $n \in \mathbf{Z}$, if n^2 is even, then n is even.

Exercise2 For every $n \in \mathbf{Z}$, if n is even, then n^2 is even.

Proof by Contrapositive 逆否证明法

Exercise2 For every $n \in \mathbf{Z}$, if n is even, then n^2 is even.

Proof by Contrapositive 逆否证明法

Exercise2 For every $n \in \mathbf{Z}$, if n is even, then n^2 is even.

1. Suppose n^2 is not even.
2. So n^2 is odd.
3. $\exists k \;\; n^2 = 2k + 1$
4. $\exists k \;\; n^2 - 1 = 2k$
5. $\exists k \;\; (n - 1)(n + 1) = 2k$
6. $2 \mid (n - 1)(n + 1)$
7. $2 \mid (n - 1) \;\vee\; 2 \mid (n + 1)$ since 2 is prime
8. $\exists a \;\; n - 1 = 2a \;\vee\; \exists b \;\; n+1 = 2b$
9. $\exists a \;\; n = 2a + 1 \vee \; \exists b \;\; n = 2b - 1$
10. In both cases n is odd
11. So n is not even

Proof by Cases 分情况证明法

Proof by cases is used when the original hypothesis naturally divides itself into various cases.

Proof by Cases 分情况证明法

Proof by cases is used when the original hypothesis naturally divides itself into various cases.

Suppose that the task is to prove $p \to q$ and that p is equivalent to $p_1 \lor p_2 \lor \ldots p_n$ (p_1, ..., p_n are the cases).
Instead of proving

$$(p_1 \lor p_2 \lor \ldots p_n) \to q,$$

we prove

Proof by Cases 分情况证明法

Proof by cases is used when the original hypothesis naturally divides itself into various cases.

Suppose that the task is to prove $p \rightarrow q$ and that p is equivalent to $p_1 \lor p_2 \lor \ldots p_n$ (p_1, ..., p_n are the cases).
Instead of proving

$$(p_1 \lor p_2 \lor \ldots p_n) \rightarrow q,$$

we prove

$$(p_1 \rightarrow q) \land (p_2 \rightarrow q) \land \ldots \land (p_n \rightarrow q).$$

Proof by Cases 分情况证明法

Proof by cases is used when the original hypothesis naturally divides itself into various cases.

Suppose that the task is to prove $p \to q$ and that p is equivalent to $p_1 \vee p_2 \vee \ldots p_n$ (p_1, ..., p_n are the cases).
Instead of proving

$$(p_1 \vee p_2 \vee \ldots p_n) \to q,$$

we prove

$$(p_1 \to q) \wedge (p_2 \to q) \wedge \ldots \wedge (p_n \to q).$$

Sometimes the number of cases to prove is finite and not too large, so we can check them all one by one. We call this type of proof **exhaustive proof** **（穷举证明）**.

Proof by Cases 分情况证明法

Example 2.2.6 Prove that $2m^2 + 3n^2 = 40$ has no solution in positive integers, that is, that $2m^2 + 3n^2 = 40$ is false for all positive integers m and n.

Proof by Cases 分情况证明法

Example 2.2.6 Prove that $2m^2 + 3n^2 = 40$ has no solution in positive integers, that is, that $2m^2 + 3n^2 = 40$ is false for all positive integers m and n.

Proof If $2m^2 + 3n^2 = 40$, we must have $2m^2 \leq 40$. Thus $m^2 \leq 20$ and $m \leq 4$. Similarly, we must have $3n^2 \leq 40$. Thus $n^2 \leq 40/3$ and $n \leq 3$. Therefore it suffices to chech the cases $m = 1, 2, 3, 4$ and $n = 1, 2, 3$.

The entries in the table give the value of $2m^2 + 3n^2$ for the indicated values of m and n.

		m = 1	2	3	4
n	1	5	11	21	35
	2	14	20	30	44
	3	29	35	45	59

Since $2m^2 + 3n^2 \neq 40$ for $m = 1, 2, 3, 4$ and $n = 1, 2, 3$, and $2m^2 + 3n^2 > 40$ for $m > 4$ or $n > 3$, we conclude that $2m^2 + 3n^2 = 40$ has no solution in positive integers.

Proof by Cases 分情况证明法

Example 2.2.7 We prove that for every real number x, $x \leq |x|$.

Proof of Equivalence 等价证明法

Some theorems are of the form p if and only if q. Such theorems are proved by using the equivalence

$$p \leftrightarrow q \equiv (p \longrightarrow q) \land (q \longrightarrow p)$$

that is, to prove "p if and only if q", prove "if p then q" and "if q then p".

Proof of Equivalence 等价证明法

Some theorems are of the form p if and only if q. Such theorems are proved by using the equivalence

$$p \leftrightarrow q \equiv (p \longrightarrow q) \wedge (q \longrightarrow p)$$

that is, to prove “p if and only if q”, prove “if p then q” and “if q then p”.

Example 2.2.9 Prove that for every integer n, n is odd if and only if $n-1$ is even.

Proof of Equivalence 等价证明法

Some theorems are of the form p if and only if q. Such theorems are proved by using the equivalence

$$p \leftrightarrow q \equiv (p \longrightarrow q) \wedge (q \longrightarrow p)$$

that is, to prove "p if and only if q", prove "if p then q" and "if q then p".

Example 2.2.9 Prove that for every integer n, n is odd if and only if $n-1$ is even.

Proof If n is odd, then $n = 2\mathrm{k} + 1$ for some integer k.
Now $n-1 = (2k+1) - 1 = 2k$. Therefore, $n-1$ is even.
If $n-1$ is even, then $n-1 = 2k$ for some integer k.
Now $n = 2k+1$. Therefore, n is odd. The proof is complete.

Proof of Equivalence 等价证明法

Some theorems are of the form p if and only if q. Such theorems are proved by using the equivalence

$$p \leftrightarrow q \equiv (p \longrightarrow q) \land (q \longrightarrow p)$$

that is, to prove "p if and only if q", prove "if p then q" and "if q then p".

To prove that $p_1, p_2, \ldots, p_n$ are equivalent, the usual method is to prove

$$(p_1 \longrightarrow p_2) \land (p_2 \longrightarrow p_3) \land \ldots \land (p_{n-1} \longrightarrow p_n) \land (p_n \longrightarrow p_1).$$

Proof of Equivalence 等价证明法

Example 2.2.11

Let A, B, and C be sets. Prove that the following are equivalent:

(a) $A \subseteq B$

(b) $A \cap B = A$

(c) $A \cup B = B$.

Proof of Equivalence 等价证明法

Example 2.2.11

Let A, B, and C be sets. Prove that the following are equivalent:

(a) $A \subseteq B$

(b) $A \cap B = A$

(c) $A \cup B = B$.

(a) $\rightarrow$ (b)

Assume that $A \subseteq B$, and prove that $A \cap B = A$.

Proof of Equivalence 等价证明法

Example 2.2.11

Let A, B, and C be sets. Prove that the following are equivalent:

(a) $A \subseteq B$

(b) $A \cap B = A$

(c) $A \cup B = B$.

(b) $\rightarrow$ (c)

Assume that $A \cap B = A$, and prove that $A \cup B = B$.

Proof of Equivalence 等价证明法

Example 2.2.11

Let A, B, and C be sets. Prove that the following are equivalent:

(a) $A \subseteq B$

(b) $A \cap B = A$

(c) $A \cup B = B$.

(c) $\rightarrow$ (a)

Assume that $A \cup B = B$, and prove that $A \subseteq B$.

Existence Proofs 存在性证明法

A proof of

$$\exists x \, \mathrm{P}(x)$$

is called an **existence proof**. One way to prove it is to exhibit one member a in the domain of discourse that makes $\mathrm{P}(a)$ true.

Example 2.2.12 Let a and b be real numbers with $a < b$. Prove that there exists a real number x satisfying $a < x < b$.

Existence Proofs 存在性证明法

A proof of

$$\exists x \, \mathrm{P}(x)$$

is called an **existence proof**. One way to prove it is to exhibit one member a in the domain of discourse that makes $\mathrm{P}(a)$ true.

Example 2.2.14 Let

$$A = \frac{s_1 + s_2 + \ldots + s_n}{n}$$

be the average of the real numbers $s_1, s_2, \ldots, s_n$. Prove that there exists i such that $s_i \geq A$.

Problem-Solving Tips

- If you are trying to construct a direct proof of a statement of the form $p \to q$ and you seem to be getting stuck, try a proof by contradiction. You then have more to work with: Besides assuming p, you get to assume $\neg q$.
- When writing up a proof by contradiction, alert the reader by stating, "We give a proof by contradiction, thus we assume $\cdots$," where $\cdots$ is the negation of the conclusion. Another common introduction is: Assume by way of contradiction that $\cdots$.

Problem-Solving Tips

- Proof by cases is useful if the hypotheses naturally break down into parts. For example, if the statement to prove involves the absolute value of x, you may want to consider the cases $x \geq 0$ and $x < 0$ because $|x|$ is itself defined by the cases $x \geq 0$ and $x < 0$. If the number of cases to prove is finite and not too large, the cases can be directly checked one by one.

  In writing up a proof by cases, it is sometimes helpful to the reader to indicate the cases, for example,

  [Case I: $x \geq 0$.] Proof of this case goes here.

  [Case II: $x < 0$.] Proof of this case goes here.

- To prove p if and only if q, you must prove two statements: (1) if p then q and (2) if q then p. It helps the reader if you state clearly what you are proving. You can write up the proof of (1) by beginning a new paragraph with a sentence that indicates that you are about to prove "if p then q." You would then follow with a proof of (2) by beginning a new paragraph with a sentence that indicates that you are about to prove "if q then p." Another common technique is to write

  [$p \rightarrow q$.] Proof of $p \rightarrow q$ goes here.

  [$q \rightarrow p$.] Proof of $q \rightarrow p$ goes here.

Problem-Solving Tips

- To prove that several statements, say $p_1, \ldots, p_n$, are equivalent, prove $p_1 \rightarrow p_2$, $p_2 \rightarrow p_3, \ldots, p_{n-1} \rightarrow p_n, p_n \rightarrow p_1$. The statements can be ordered in any way and the proofs may be easier to construct for one ordering than another. For example, you could swap p_2 and p_3 and prove $p_1 \rightarrow p_3, p_3 \rightarrow p_2, p_2 \rightarrow p_4, p_4 \rightarrow p_5, \ldots,$ $p_{n-1} \rightarrow p_n, p_n \rightarrow p_1$. You should indicate clearly what you are about to prove. One common form is

  [$p_1 \rightarrow p_2$.] Proof of $p_1 \rightarrow p_2$ goes here.

  [$p_2 \rightarrow p_3$.] Proof of $p_2 \rightarrow p_3$ goes here.

  And so forth.

- If the statement is existentially quantified (i.e., there exists $x \ldots$), the proof, called an existence proof, consists of showing that there exists at least one x in the domain of discourse that makes the statement true. One type of existence proof exhibits a value of x that makes the statement true (and proves that the statement is indeed true for the specific x). Another type of existence proof indirectly proves (e.g., using proof by contradiction) that a value of x exists that makes the statement true without specifying any particular value of x for which the statement is true.

2.3 Resolution Proofs 消解证明 / 归结证明

Due to J. A. Robinson (1965)

If $p \lor q$ and $\neg p \lor r$ are both true, then $q \lor r$ is true.

2.3 Resolution Proofs 消解证明 / 归结证明

Due to J. A. Robinson (1965)

If $p \vee q$ and $\neg p \vee r$ are both true, then $q \vee r$ is true.

Example 2.3.4 Prove the following using resolution：

$$\begin{array}{ll} 1, & a \vee b \\ 2, & \neg a \vee c \\ 3, & \neg c \vee d \\ \hline \therefore & b \vee d \end{array}$$

2.3 Resolution Proofs 消解证明 / 归结证明

Due to J. A. Robinson (1965)

If $p \vee q$ and $\neg p \vee r$ are both true, then $q \vee r$ is true.

Special Case of Rule

If $p \vee q$ and $\neg p$ are both true, then q is true.
If $\neg p \vee q$ and p are both true, then q is true.

2.3 Resolution Proofs 消解证明 / 归结证明

Due to J. A. Robinson (1965)

If $p \vee q$ and $\neg p \vee r$ are both true, then $q \vee r$ is true.

Example 2.3.5 Prove the following using resolution：

$$\begin{array}{ll} 1, & a \\ 2, & \neg a \vee c \\ 3, & \neg c \vee d \\ \hline \therefore & d \end{array}$$