Week02 proof

Reading

- Secton1.8
- section 5.1
- section 5.2

direct proof and indirect proof

If a proof leads from the premises of a theorem to the conclusion, then it is a direct proof, otherwise, it is an indirect proof.

A **direct proof** shows that a conditional statement p ! q is true by showing that

if p is true, then q must also be true

exercise

‘If n is an odd integer, then n2 is odd’.

proof:

Suppose n is an odd integer. Then there exists an integer k such that n = 2k + 1. n2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k2 + 2k) + 1. Since 2(k^2 + 2k) is an integer, n2 is odd.

Proof by Contraposition (indirect proof)

$$if\ p \to q\ then$$
$$\neg q \to \neg p$$

exercise

Prove that **if n is an integer and 3n + 2 is odd, then n is odd.**

proof:

p : 3n+2 is odd;

q : n is odd

it is the same meaning that:

if n is even then proof 3n+2 is even

let n=2k, 3n+2 = 6k+2 = 2(3k+1)

because 3k+1 is integer

6k+2 is even

Q.E.D.

Proof by Contradiction (indirect proof)

Because the statement

$$r \wedge \neg r$$

is a contradiction whenever r is a proposition, we can prove that p is true if we can show that

$$\neg p \rightarrow (r \wedge \neg r)$$

is true for some proposition r.

Exercise

Prove that

$$\sqrt{2}\ is\ irrational$$

Proof.

Suppose $\sqrt{2}$ is rational. Then there exist integers p and q with $q \neq 0$ such that $\sqrt{2} = p/q$ and p and q do not have any common factor. Thus, $2 = p^2/q^2$. $p^2 = 2q^2$. Thus, p^2 is even. Since if n is odd, then n^2 is odd (proved in previous slides), p is even. Hence there exists an integer k such that $p = 2k$. Then $p^2 = (2k)^2 = 2q^2$. $q^2 = 2k^2$. Thus q^2 is even, hence q is even. Thus, p and q are both even, which contradicts the fact that p and q do not have any common factor. $\square$

Proof of Equivalence

To prove a theorem that is a biconditional statement or a bi-implication,
that is, a statement of the form

$$p \leftrightarrow q$$

we show that

$$p \rightarrow q$$

and

$$q \rightarrow p$$

are both true.

so:

This shows that if the n conditional statements $p_1 \rightarrow p_2$, $p_2 \rightarrow p_3$,..., $p_n \rightarrow p_1$ can be shown to be true, then the propositions p_1, p_2,..., p_n are all equivalent.

$$[p_1 \leftrightarrow p_2 \leftrightarrow \ldots \leftrightarrow p_n] \leftrightarrow [(p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \ldots \wedge (p_n \rightarrow p_1)].$$

Counterexamples

To show that a statement of the form $\forall x\, P(x)$ is false, we need only find a counterexample, that is, an example x for which $P(x)$ is false.

exercise

Show that the statement **'Every positive integer is the sum of the squares of two integers'** is false

proof:

3 is not include

Proof by Cases

- Sometimes we cannot prove a theorem using a single argument that holds for all possible cases.
- Need to consider different cases separately.
- **Rationale:** To prove a conditional statement of the form

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

the tautology

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

can be used as a rule of inference.

exercise

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

Proof.

Let us prove by cases.

- If $n = 0$, then $0^2 \geq 0$.
- If $n \geq 1$, we multiply both sides of the inequality $n \geq 1$ by the positive integer n, then we have $n^2 \geq n$.
- If $n \leq -1$, $n^2 \geq n$ holds, since $n^2 \geq 0$.

Thus, in each case, $n^2 \geq n$. □

Mathematical Induction (数学归纳法)

Basis Step: We show that the statement holds for the positive integer 1 (i.e. P(1) is true).
Inductive Step We show that if the statement holds for a positive integer then it must also hold for the next larger integer (i.e. for all positive integers k, if P(k) is true, then P(k + 1) is true).

$$\begin{array}{l} P(1) \\ \forall k\,(P(k) \rightarrow P(k+1)) \\ \hline \therefore \forall n\, P(n) \end{array}$$

Strong Induction

Basis Step We verify that the proposition $P(1)$ is true.

Inductive Step We show that the conditional statement $[P(1) \land P(2) \land \ldots \land P(k)] \rightarrow P(k+1)$ is true for all positive integers k.