# 1.7
# Introduction to Proofs

# Section Summary

- Mathematical Proofs
- Forms of Theorems
- Direct Proofs
- Indirect Proofs
  - Proof of the Contrapositive
  - Proof by Contradiction

# Some Terminologies

**Theorem:** A statement that can be shown to be true.
**Proposition:** Less important theorem
**Proof :** A valid argument that establishes the truth of a theorem
**Axioms:** The underlying assumptions about mathematical structures,
or hypotheses of the theorem to be proved,
or previously proved theorems.
**Lemma :** A 'helping theorem' or a result which is needed to prove a theorem.
**Corollary:** A result which follows directly from a theorem.
**Conjecture:** A statement whose truth value is unknown.

# Understanding How Theorems Are Stated

**Some typical examples,**

1. **"if $x>y$, where $x$ and $y$ are positive real numbers, then $x^2>y^2$."**

   **For all positive real number $x$ and $y$, if $x>y$, then $x^2>y^2$.**

2. **"if $n$ is odd, then $n^2$ is odd."**

   **For all natural number $n$, if $n$ is odd, then $n^2$ is odd.**

$$\boxed{\forall n\ (P(n) \rightarrow Q(n))}$$

**How to prove?**

# Method of Proving Theorems

**To prove a theorem of the form $\forall x\ (P(x) \rightarrow Q(x))$**

- **show that $P(c) \rightarrow Q(c)$ is true, where $c$ is an arbitrary element of the domain**
- **apply universal generalization.**

**How to show that a conditional statement $p \rightarrow q$ is true?**

# Direct Proofs

To establish that $p \to q$ is true.

$p$ may be a conjunction of other hypotheses.

- ✓ assumes the hypotheses are true
- ✓ uses the rules of inference, axioms ,definition, previously proven theorems, and any logical equivalences to establish the truth of the conclusion.

**〖Example 1〗 Give a direct proof of the theorem "If $n$ is odd, then $n^2$ is odd."**

*Proof:*

**Assume that the hypothesis of this implication is true, namely, suppose that $n$ is odd.**

**Then $n = 2k + 1$, where $k$ is an integer.**

**It follows that**

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

**Therefore,**

**$n^2$ is odd (it is 1 more than twice an integer).**

# Formal Proofs vs. Informal Proofs

**Formal proof:**

- **All steps were supplied**
- **The rules for each step in the argument were given**

**Informal proof:**

- **More than one rule of inference may be used in each step**
- **Steps may be skipped**
- **The axioms being assumed and the rules of inference used are not explicity stated**

# Proof by Contraposition

Using proof by contraposition (a kind of indirect proof ) to establish that $p \rightarrow q$ is true.

- ✓ assumes the conclusion of $p \rightarrow q$ is false ($\neg q$ is true)
- ✓ uses the rules of inference, axioms ,definition, previously proven theorems, and any logical equivalences to establish the premise $p$ is false.

**Note:**

- **Recall:** $p \rightarrow q \equiv \neg q \rightarrow \neg p$
- **In order to show that a conjunction of hypotheses is false is suffices to show just one of the hypotheses is false.**

**〖Example 2〗Theorem:** ***A perfect number is not a prime.***

**A *perfect* number is one which is the sum of all its divisors except itself.**

**For example, 6 is perfect since 1 + 2 + 3 = 6.**

*Proof:*

**We assume the number *s* is a prime and show it is not perfect.**

**But the only divisors of a prime are 1 and itself.**

**Hence the sum of the divisors less than *s* is 1 which is not equal to *s*.**

**Hence *s* cannot be perfect.**

# Vacuous Proof

Using the method of vacuous proof to establish that $p \to q$ is true.

- ✓ Show that $p$ is false

**Note:**

**If one of the hypotheses in $p$ is false then $p \to q$ is *vacuously* true.**

**〖Example 3〗If Tom is both handsome and ugly then he feels unhappy.**

***Solution:***

**This is of the form $(p \wedge \neg p) \rightarrow q$ .**

**The hypotheses form a contradiction.**

**Hence $q$ follows from the hypotheses vacuously.**

**〖Example 4〗 Show that the proposition $P(0)$ is true, where $P(n)$ is "If $n>1$,then $n^2>n$" and the domain consists of all integers.**

# Trivial proof

Using the method of trivial proof to establish that $p \rightarrow q$ is true.

- ✓ Show that $q$ is true.

〖Example 5〗**If the earth is smaller than moon then the void set is a subset of every set .**

***Solution:***

**The assertion is *trivially* true independent of the truth of *p*.**

[ Even though these examples seem silly, both trivial and vacuous proofs are often used in mathematical induction, as we will see in Chapter 5) ]

# Proof by contradiction

Using the method of proof by contradiction to establish the truth of the 'theorem' $p$

- ✓ assumes the conclusion $p$ is false
- ✓ derives a contradiction, usually of the form $q \wedge \neg q$ which establishes $\neg p \rightarrow F$.

## 〖Example 6〗Theorem: There are infinitely many primes.

*Proof:*

**Assume finitely many primes: $p_1, p_2, \ldots\ldots, p_n$**

- **Let $q = p_1 p_2 \cdots p_n + 1$**
- **Either $q$ is prime or by the fundamental theorem of arithmetic it is a product of primes.**
- **But none of the primes $p_j$ divides $q$ since if $p_j \mid q$, then $p_j$ divides**

$$q - p_1 p_2 \cdots p_n = 1 .$$

- **Hence, there is a prime not on the list $p_1, p_2, \ldots\ldots, p_n$. It is either $q$, or if $q$ is composite, it is a prime factor of $q$. This contradicts the assumption that $p_1, p_2, \ldots\ldots, p_n$ are all the primes.**
- **Consequently, there are infinitely many primes.**

**Note:**

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

1) **Assume $p$ is true and $q$ is false**
2) **Show that $\neg p$ is also true.**

   **Since the statement $p \wedge (\neg p)$ is always false.**

   **—Contradiction!**

〖Example 7〗 **Show that $s \vee r$ logically follows from the hypotheses**

$$p \vee q, p \to r, q \to s$$

*solution:*

| Step | Reason |
|---|---|
| 1. $\neg (s \vee r)$ | **Additional hypothesis** |
| 2. $\neg s \wedge \neg r$ | **Step 1 and De morgan** |
| 3. $\neg s$ | **Simplification using step 2** |
| 4. $\neg r$ | **Simplification using step 2** |
| 5. $p \to r$ | **Hypothesis** |
| 6. $\neg p$ | **Modus tollens using steps 4 and 5** |
| 7. $q \to s$ | **Hypothesis** |
| 8. $\neg q$ | **Modus tollens using steps 3 and 7** |
| 9. $\neg p \wedge \neg q$ | **Conjunction using step 6 and 8** |
| 10. $\neg (p \vee q)$ | **Step 9 and De morgan** |
| 11. $p \vee q$ | **Hypothesis** |

# Proof of Equivalence

(1) To prove the proposition "*p* if and only if *q*"

(2) To prove that several propositions $p_1$ , $p_2, \ldots, p_n$ are equivalent

- ✓ establish the implications $p_1 \to p_2, \ldots, p_{n-1} \to p_n, p_n \to p_1$

$$[p_1 \leftrightarrow p_2 \leftrightarrow \ldots \leftrightarrow p_n] \equiv [(p_1 \to p_2) \wedge (p_2 \to p_3) \wedge \ldots \wedge (p_n \to p_1)]$$

# Mistakes in Proofs

**Many mistakes result from the introduction of steps that do not logically follow from those that precede it.**

**Many incorrect arguments are based on a fallacy called *begging the question* (circular reasoning).**

# 1.8
# Proof Methods and Strategy

## Section Summary

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

# Exhaustive Proof and Proof by Cases

Using the method of proof by cases to show that $(p_1 \vee p_2 \vee \ldots \vee p_n) \to q$

✓establish all implications $p_i \to q$

**Note:**

**1)** $(p_1 \vee p_2 \vee \ldots \vee p_n) \to q \equiv (p_1 \to q) \wedge (p_2 \to q) \wedge \ldots \wedge (p_n \to q)$

**Each of the implications $p_i \to q$ is a case.**

**2) An exhaustive proof is a special type of proof by cases where each case involves checking a single example.**

**〖Example 1〗 Prove that if *n* is an integer not divisible by 3, then $n^2 \equiv 1 \pmod 3$.**

*Proof:*

**$P(n)$: $n$ an integer is not divisible by 3**

**$Q(n)$: $n^2 \equiv 1 \pmod 3$**

**Then $p(n)$ is equivalent to $p_1(n) \vee p_2(n)$ , where $p_1(n)$ is "$n \equiv 1 \pmod 3$" and $p_2(n)$ is "$n \equiv 2 \pmod 3$".**

**Hence, to show that $p(n) \rightarrow q(n)$ it can be shown that $p_1(n) \rightarrow q(n)$ and $p_2(n) \rightarrow q(n)$.**

**It is easy to give direct proves of those two implications.**

# Existence Proofs

Using constructive existence proof to establish the truth of $\exists x P(x)$.

- ✓ Establish $P(c)$ is true for some $c$ in the domain.
- ✓ Then $\exists x P(x)$ is true by Existential Generalization (EG).

**〖Example 2〗 Show that there are *n* consecutive composite positive integers for every positive integer *n*.**

*Proof:*

$\forall n \exists x (x + i \text{ is composite for } i = 1, 2, \ldots, n)$.

**Let $x = (n + 1)! + 1$.**

**Consider the integers $x + 1, x + 2, \ldots, x + n$.**

**Note that $i + 1$ divides $x + i = (n + 1)! + (i + 1)$ for $i = 1, 2, \ldots, n$.**

**Hence, *n* consecutive composite positive integers have been given.**

**Note that in the solution a number $x$ such that $x + i$ is composite for $i = 1, 2, \ldots, n$ has been produced.**

**Hence, this is an example of constructive existence proof.**

# Existence Proofs

Using nonconstructive existence proof to establish the truth of $\exists x P(x)$.

✓ Assume no $c$ exists which makes $P(c)$ true and derive a contradiction

〖Example 3〗*Theorem:There exists an irrational number.*

*Proof:*

**Assume there doesn’t exist an irrational number. Then all numbers must be rational.**

**Then the set of all numbers must be countable.**

**Then the real numbers in the interval [0, 1] is a countable set.**

**But we have already shown this set is not countable.**

**Hence, we have a contradiction (The set [0,1] is countable and not countable).**

**Therefore, there must exist an irrational number.**

# Uniqueness Proofs

To show that a theorem assert the existence of a unique element with a particular property.

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

- ✓ Existence: We show that an element $x$ with the desired property exists.
- ✓ uniqueness : We show that if $y \neq x$, then $y$ does not have the desired property. Or, we can show that if $x$ and $y$ both have the desired property ,then $x=y$.

# Disproof by Counterexample

Using the method of disproof by counterexample to establish that $\neg \forall x P(x)$ is true.

-To construct a $c$ such that $P(c)$ is false.

**Recall:** $\neg \forall x P(x) \Leftrightarrow \exists x \neg P(x)$

# Nonexistence Proofs

To establish that $\neg \exists x P(x)$ is true .

- ✓ Use a proof by contradiction by assuming there is a $c$ which makes $P(c)$ true .

**Recall:** $\neg \exists x\, P(x) \Leftrightarrow \forall x \neg P(x)$

# Universally Quantified Assertions

To establish the truth of $\forall x P(x)$.

- ✓ We assume that $x$ is an arbitrary member of the universe and show $P(x)$ must be true.
- ✓ Using UG it follows that $\forall x P(x)$.

**〖Example 4〗*Theorem: For the universe of integers, x is even iff $x^2$ is even.***

*Proof:*

**$\forall x[x$ is even $\leftrightarrow x^2$ is even] .**

**Recall that $p \leftrightarrow q$ is equivalent to $(p \rightarrow q) \wedge (q \rightarrow p)$.**

**Case 1. *sufficiency***

**Show that if $x$ is even then $x^2$ is even using a direct proof .**

**Case 2. *necessity***

**We use an indirect proof.**

**Assume $x$ is not even and show $x^2$ is not even.**

# Proof Strategies

***Forward reasoning:*** **Using premises, together with axioms and known theorems to lead to the conclusion.**

***Backward reasoning:*** **To reason backward to prove a statement $q$, we find a statement $p$ that we can prove with the property that $p \to q$.**

# Proof Strategy in Action

**Mathematics text formally present theorems and their proofs.**

- **as if mathematical facts were carved in stone**
- **Don’t convey the discovery process in mathematics**

***The discovery process in mathematics:***

**Begin with exploring concepts and examples, asking questions, formulating conjectures, and attempting to settle these conjecture either by proof or by counterexample.**

# 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.
  - ✓ Cantor diagonalization is used to prove results about the size of infinite sets.
  - ✓ Combinatorial proofs use counting arguments.

**Homework:**

SE：P.91 37;  P.108 15

EE：P.96 39;  P.114 17