普通高校本科计算机专业特色教材精选·数理基础

# 离散数学及其应用

杨振启 杨云雪 张克军 主编

清华大学出版社

普通高校本科计算机专业特色教材精选·数理基础

# 离散数学及其应用

杨振启 杨云雪 张克军 主 编

聂盼红 吕俊斌 朱节中 副主编

清华大学出版社

北京

## 内 容 简 介

本书介绍离散数学的知识和应用。全书共 7 章，分别介绍命题逻辑、谓词逻辑、集合论、二元关系、图论、初等数论和代数系统，并介绍相关的应用。其中，第 6 章讨论了数论在公钥密码系统 ElGamal 加密解密、数字签名解决方案和计算机大整数加法中的应用；第 7 章利用群的知识给出了著名的 RSA 公钥密码解决方案，在域的内容中给出了通信中的线性码和循环码的编码与纠错理论，还对信息的加密解密算法和编码效率进行了讨论。书中的应用都有详细的背景知识介绍，应用理论涉及的结论和定理也都有详细的证明过程。

本书适合信息与计算科学专业、计算机科学与技术专业、信息安全专业以及电子通信等专业的学生使用，也可供相关领域的科研人员和工程技术人员参考。



图书在版编目（CIP）数据

离散数学及其应用/杨振启，杨云雪，张克军主编. —北京：清华大学出版社，2018
(普通高校本科计算机专业特色教材精选 · 数理基础)
ISBN 978-7-302-48807-1

Ⅰ. ①离… Ⅱ. ①杨… ②杨… ③张… Ⅲ. ①离散数学-高等学校-教材 Ⅳ. ①O158

中国版本图书馆 CIP 数据核字(2017)第 272853 号

责任编辑：袁勤勇　战晓雷
封面设计：傅瑞学
责任校对：梁　毅
责任印制：杨　艳
出版发行：清华大学出版社
网　　址：http://www.tup.com.cn, http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969, c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015, zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn,010-62795954
印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　印　张：17.75　　字　数：428 千字
版　　次：2018 年 1 月第 1 版　　印　次：2018 年 1 月第 1 次印刷
印　　数：1～1500
定　　价：39.00 元

产品编号：075970-01

# 前　言

离散数学是现代数学的一个分支, 是计算机科学中基础理论的核心课程. 是研究离散量的数学结构、性质及关系的基础. 它一方面充分描述了计算机科学离散性的特点, 为学习算法与数据结构、程序设计语言、操作系统、编译原理、电路设计、数据库与信息检索系统等专业课程打下良好的数学基础; 另一方面, 通过学习离散数学, 既可以获得离散数学建模、离散数学理论、计算机求解方法的一般知识, 还可以培养和提高抽象思维能力和严密的推理能力. 离散数学所体现的现代数学思想对于加强学生的素质教育也有着不可替代的作用.

离散数学主要面向高等院校的信息科学、计算机科学以及通信专业的学生, 是为非数学专业学生开设的一门专业基础课程. 我们认为非数学专业的学生学习离散数学课程的主要目的还是在于数学知识的应用, 这才能体现该课程的价值. 目前市面上已有的同类教材中很少见到在应用方面的介绍, 学生不容易取得好的学习效果.

本书的编写充分注意到了上述问题. 全书分为 7 章. 分别是命题逻辑、谓词逻辑、集合论、二元关系、图论、初等数论和代数系统, 这些都是目前离散数学中的常见内容. 除此之外, 本书内容还包含了相关知识的应用. 具体应用主要有公钥密码系统、电子签名、计算机大整数加法、编码与纠错等, 在介绍这些应用之前, 先详细介绍了信息安全和编码与纠错理论的背景知识.

本书层次结构清晰, 每个概念后都给出了较多的例题, 这对理解一些抽象的概念具有很好的帮助. 要比较好地掌握离散数学知识, 应该有较好的理解和分析问题的能力, 所以本书在定理的推导方面, 特别是关于应用中定理的推导, 如公钥密码系统算法正确性的证明、编码理论及编码效率等涉及的每个结论, 都给出了详尽的证明过程, 非常方便读者阅读.

本书适合信息与计算科学专业、计算机科学与技术专业、信息安全专业以及通信专业等专业的学生使用, 也可供相关领域的科研人员和工程技术人员参考.

本书由南京信息工程大学、南京航空航天大学、常熟理工学院、徐州工程学院、南京工程学院等高校组织编写, 杨振启、杨云雪、张克军任主编, 聂盼红、吕俊斌、朱节中任副主编, 参加编写工作的还有涂为员、戴磊、孙天凯、张晗和韩磊老师.

作者编写本书时参考了很多书籍和资料, 在此向有关作者表示诚挚的谢意.

由于作者水平有限, 书中难免有不妥之处. 期待读者提出宝贵的批评和建议, 以便作者在修订时参考. 谢谢!

作　者

2017 年 10 月

# 目　录

# 第1章 命题逻辑

使用计算机必须首先学会编程序, 那么什么是程序?

程序 = 算法 + 数据.

算法 = 逻辑 + 控制.

可见“逻辑”对于编程序是多么重要. 要想学好和使用好计算机, 必须学习逻辑. 此外, 通过学习逻辑, 掌握逻辑推理规律和证明方法, 可以培养学生的逻辑思维能力, 提高证明问题的技巧.

逻辑学是一门研究思维形式及思维规律的科学, 也就是研究推理过程的规律的科学. 逻辑规律就是客观事物在人的主观意识中的反映. 思维的形式结构包括了概念、判断和推理之间的结构和联系, 其中概念是思维的基本单位, 通过概念对事物是否具有某种属性进行肯定或否定的回答, 就是判断; 由一个或几个判断推出另一判断, 就是推理. 用数学方法来研究推理的规律称为数理逻辑. 这里所指的数学方法, 就是引进一套符号体系的方法, 在其中表达和研究推理的规律.

最早提出用数学方法来描述和处理逻辑问题的是德国数学家莱布尼茨 (G.W.Leibniz), 从此数理逻辑形成了专门的学科. 数理逻辑作为计算机科学的基础理论之一, 在程序设计、数字电路设计、计算机原理、人工智能等计算机课程中得到了广泛应用. 数理逻辑的主要内容包括逻辑演算、证明论、公理集合论、递归论和模型论, 本书主要介绍其中的命题逻辑和谓词逻辑 (一阶逻辑), 其余部分读者可参考有关专著.

命题逻辑是数理逻辑中最基本、最简单的部分, 但究竟什么是命题? 如何表示命题及进行命题演算? 如何进行推理证明? 本章将讨论这些问题.

## 1.1 命题和联结词

数理逻辑研究的中心问题是推理. 推理的前提和结论都是表达判断的陈述句. 什么是命题? 直观来说, 陈述客观发生的事情的陈述句就叫做命题. 凡陈述的事情发生了, 则此命题为真命题, 反之为假. 也就是说, 一个命题要么为真, 要么为假, 两者必居其一. 当然, 两者也只能居其一, 即不能说一个命题既真又假. 据此, 可以给出命题的如下描述:

### 1.1.1 命题

**定义 1.1** 能判断真假而不是可真可假的陈述句为**命题**.

由作为命题的陈述句所表达的内容得到的判断结果称为命题的**真值**. 真值只取两个: 真与假. 真值为真的命题称为真命题. 真值为假的命题称为假命题. 命题通常用大写英文字母如 $P$、$Q$、$R$ 等表示.

**例 1.1**　判断下列语句是否为命题.

(1) 4 是素数.

(2) 2025 年人类将到达火星.

(3) 今天是星期二.

(4) 2+3=5.

(5) 这朵花真美丽啊!

(6) 离散数学是计算机科学的基础课程.

(7) 严禁随地吐痰!

(8) 她身体好吗?

(9) $x$=3.

(10) 我在说谎.

(11) 如果 $a>b$ 且 $b>c$, 则 $a>c$.

**解:** 其中陈述句 (4)、(6)、(11) 所陈述的内容与事实相符, 是对的, 正确的, 是真命题, 或者称命题的值为“真”, 简记为 T 或数字 1. 陈述句 (1) 是错的, 不正确, 称为假命题, 或称命题的值为“假”, 简记为 F 或数字 0. 陈述句 (2) 是命题, 但命题真值暂时不能确定, 要等到 2025 年才能确定. 陈述句 (3) 是命题, 其真值根据具体情况而定. 语句 (5) 是感叹句, (7) 是祈使句, (8) 是疑问句, 这 3 句都不是陈述句, 当然不是命题. 语句 (9)、(10) 都是陈述句, 但都不是命题, 其中 (9) 没有确定的真值, (10) 是悖论 (可以推导出互相矛盾的结果的陈述句).

**说明**　命题是陈述句, 而不能是疑问句、祈使句、感叹句等. 判断结果不唯一确定的陈述句不是命题 (有时需根据论及该命题的时间、空间来确定). 陈述句中的悖论不是命题.

以下是关于命题的几个概念.

**原子命题**或**简单命题**　不能分解成更简单的语句的命题.

**复合命题**　多个原子命题由联结词和圆括号联结起来构成的命题. 复合命题的真假值只与原子命题的真假值有关.

**命题常项**或**命题常元**　已知真假值的命题. 可以用字母表示, 也可以直接用 T、F 表示.

**命题变项**或**命题变元**　真值可以变化的陈述句为命题变项或命题变元. 命题变项不是命题.

命题逻辑中, $P$、$Q$、$R$ 等既可以表示命题常项, 也可以表示命题变项. 在使用中, 需要由上下文确定它们表示的是常项还是变项.

在例 1.1 中, 语句 (1)、(2)、(3)、(4)、(6) 都是原子命题, 语句 (11) 是复合命题.

## 1.1.2　命题联结词

自然语言中, 常使用“或”“与”“如果……, 那么……”等连接词, 这些在数理逻辑中称为联结词. 联结词是复合命题的重要组成部分, 为了便于书写和推理, 必须对联结词作出明确规定和符号化. 数理逻辑研究方法的主要特征是将论述或推理中的各种要素都符号化. 即构造各种符号语言来代替自然语言. 将联结词符号化, 消除其二义性, 对其进行严格定义.

在命题逻辑中有以下几种基本的联结词: $\neg$、$\wedge$、$\vee$、$\rightarrow$、$\leftrightarrow$.

**定义 1.2** 给定命题 $P$, 命题 $R$ 当且仅当 $P$ 为假时为真, 则称 $R$ 为 $P$ 的**否定或非** $P$, 记为 $\neg P$. 符号 $\neg$ 称作否定联结词. 其定义可用表 1.1 所示的真值表表示.

**表 1.1 $\neg P$ 的真值表**

| $P$ | $\neg P$ |
|---|---|
| 0 | 1 |
| 1 | 0 |

**注** 真值表是表示逻辑陈述真假性的一种方法. 在一个命题的真值表中列出它所包含的所有原子命题的真值的可能值, 就可以计算出相对于每种组合的该命题的真值.

**例 1.2** 命题符号化.

今天不下雨.

**解**: 用 $P$ 表示今天下雨, 则原命题为 $\neg P$.

**定义 1.3** 给定两个命题 $P$、$Q$, 若命题 $R$ 当且仅当 $P$、$Q$ 同时为真时为真, 则称 $R$ 为 $P$、$Q$ 的**合取**, 记为 $P \wedge Q$ . 其定义可用如表 1.2 所示的真值表表示.

**表 1.2 $P \wedge Q$ 的真值表**

| $P$ | $Q$ | $P \wedge Q$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

**例 1.3** 将下列命题符号化.

(1) 张三和李四都是三好学生.

(2) 王芳不仅用功而且聪明.

(3) 王芳虽然聪明, 但不用功.

(4) 我们去看电影并且房间里有 10 张桌子.

**解**: 第 (1) 个命题设 $P$: 张三是三好学生, $Q$: 李四是三好学生. 则原命题符号化为 $P \wedge Q$. 第 (2) 个命题设 $P$: 王芳用功, $Q$: 王芳聪明. 则原命题符号化为 $P \wedge Q$. 第 (3) 个命题设 $P$: 王芳用功, $Q$: 王芳聪明. 则原命题符号化为 $Q \wedge \neg P$. 第 (4) 个命题设 $P$: 我们去看电影, $Q$: 房间里有 10 张桌子. 则原命题符号化为 $P \wedge Q$.

**说明** 自然语言中的“既……又……”“不但……而且……”“虽然……但是……”“一面……一面……”等联结词都可以符号化为 $\wedge$; 并非所有的“和”都表示合取. 例如, “王五和赵六是兄弟.”这句是原子命题, 表示为 $P$ 或 $Q$ 即可, 当命题描述的是对象之间的关系时不能用合取; 在数理逻辑中, 关心的只是复合命题与构成复合命题的各原子命题之间的真值关系, 即抽象的逻辑关系, 并不关心各语句的具体内容.

**定义 1.4** 给定两个命题 $P$、$Q$, 若命题 $R$ 当且仅当 $P$、$Q$ 同时为假时为真, 则称 $R$ 为 $P$、$Q$ 的**析取**, 记为 $P \vee Q$. 其定义可用如表 1.3 所示的真值表表示.

联结词“析取”与汉语中的“或”几乎一致, 但要注意, 它们之间也有细微的区别.

**例 1.4** 将下列命题符号化.

(1) 郑莉爱跳舞或爱听音乐.

(2) 夏群只能挑选 202 或 203 房间.

(3) 他今天做了 10 或 20 道习题.

**表 1.3　$P \vee Q$ 的真值表**

| $P$ | $Q$ | $P \vee Q$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 1 |

**解：** 第 (1) 个命题设 $P$: 郑莉爱跳舞, $Q$: 郑莉爱听音乐. 则原命题符号化为 $P \vee Q$. $P$ 和 $Q$ 允许同时为真, 是一种相容或. 第 (2) 个命题设 $P$: 夏群挑选 202 房间, $Q$: 夏群挑选 203 房间. 因为夏群只能挑选其中的一个房间, 这里的“或”表达的是排斥或, 所以原命题不能表示为 $P \vee Q$, 应表示为 $(P \wedge \neg Q) \vee (\neg P \wedge Q)$ 或 $(P \vee Q) \wedge \neg (P \wedge Q)$. 第 (3) 个命题是原子命题, 因为“或”只表示了习题的近似数目, 该命题用 $P$ 表示.

**说明**　自然语言中的“或”具有二义性, 用它联结的命题有时具有相容性, 有时具有排斥性, 对应的联结词分别称为相容或和排斥或 (排异或).

**定义 1.5**　给定两个命题 $P$、$Q$, 复合命题“如果 $P$ 则 $Q$”称作 $P$ 与 $Q$ 的**蕴涵式**, 记作 $P \rightarrow Q$, 并称 $P$ 是蕴涵式的前件, $Q$ 为蕴涵式的后件, $\rightarrow$ 称作蕴涵联结词, 并规定 $P \rightarrow Q$ 为假当且仅当 $P$ 为真且 $Q$ 为假. 其定义可用如表 1.4 所示的真值表表示.

**表 1.4　$P \rightarrow Q$ 的真值表**

| $P$ | $Q$ | $P \rightarrow Q$ |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 1 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

**注**　$P \rightarrow Q$ 的逻辑关系表示 $Q$ 是 $P$ 的必要条件, 或 $P$ 是 $Q$ 的充分条件. $Q$ 是 $P$ 的必要条件有许多不同的叙述方式, 如: “只要 $P$ 就 $Q$”“因为 $P$ 所以 $Q$”“$P$ 仅当 $Q$”“只有 $Q$ 才 $P$”“除非 $Q$ 才 $P$”等.

**例 1.5**　将下列命题符号化, 并求出其真值.

(1) 如果 2 加 3 等于 5, 则天是蓝的.

(2) 2 加 3 等于 5 仅当天是蓝的.

(3) 除非天是蓝的, 2 加 3 才等于 5.

(4) 只有天是蓝的, 2 加 3 才等于 5.

(5) 只要 2 加 3 不等于 5, 则天是蓝的.

(6) 如果我有车, 那么我去接你.

**解：** 对于 (1) ~(5) 的命题, 设 $P$: 2 加 3 等于 5, $P$ 的真值为 1; $Q$: 天是蓝的, $Q$ 的真值为 1. (1) ~(4) 的命题符号化均为 $P \rightarrow Q$, 真值均为 1. 第 (5) 个命题符号化为 $\neg P \rightarrow Q$, 真值

为 1. 第 (6) 个命题中, 设 $P$: 我有车, $Q$: 我去接你, 命题符号化为 $P\rightarrow Q$, 真值依具体情况而定 (当我有车时, 若我去接了你, 这时 $P\rightarrow Q$ 为真; 若我没去接你, 则 $P\rightarrow Q$ 假. 当我没有车时, 我无论去或不去接你均未食言, 此时认定 $P\rightarrow Q$ 为真是适当的).

**说明** 作为一种规定, 当 $P$ 为假时, 无论 $Q$ 是真是假, $P\rightarrow Q$ 均为真. 也就是说, 只有 $P$ 为真 $Q$ 为假这一种情况使得复合命题 $P\rightarrow Q$ 为假. 称为实质蕴含.

**定义 1.6** 给定两个命题 $P$、$Q$, 复合命题"$P$ 当且仅当 $Q$"称作 $P$ 与 $Q$ 的**等价式**, 记作 $P\leftrightarrow Q$, $\leftrightarrow$ 称作等价联结词, 并规定 $P\leftrightarrow Q$ 为真当且仅当 $P$ 与 $Q$ 同时为真或同时为假. 其定义可用如表 1.5 所示的真值表表示.

**表 1.5 $P\leftrightarrow Q$ 的真值表**

| $P$ | $Q$ | $P\leftrightarrow Q$ |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

**例 1.6** 将下列命题符号化, 并求出其真值.

(1) π 是无理数当且仅当加拿大位于亚洲.

(2) 2 加 3 等于 5 的充要条件是 π 是无理数.

(3) 若两圆 A、B 的面积相等, 则它们的半径相等; 反之亦然.

(4) 当王小红心情愉快时, 她就唱歌; 反之, 当她唱歌时, 一定心情愉快.

**解:** 第 (1) 个命题, 设 $P$: π 是无理数, $Q$: 加拿大位于亚洲, 符号化为 $P\leftrightarrow Q$, 真值为 0. 第 (2) 个命题, 设 $P$: 2 加 3 等于 5, $Q$: π 是无理数, 符号化为 $P\leftrightarrow Q$, 真值为 1. 第 (3) 个命题, 设 $P$: 两圆 A、B 的面积相等, $Q$: 两圆 A、B 的半径相等, 符号化为 $P\leftrightarrow Q$, 真值为 1. 第 (4) 个命题, 设 $P$: 王小红心情愉快, $Q$: 王小红唱歌, 符号化为 $P\leftrightarrow Q$, 真值依具体情况而定.

**说明** $P\leftrightarrow Q$ 的逻辑关系为 $P$ 与 $Q$ 互为充分必要条件;$(P\rightarrow Q)\wedge(Q\rightarrow P)$ 与 $P\leftrightarrow Q$ 的逻辑关系完全一致.

以上介绍的 5 种联结词是命题逻辑中最常用、最重要的联结词, 它们共同组成了一个联结词集 $\{\neg,\wedge,\vee,\rightarrow,\leftrightarrow\}$, 其中 $\neg$ 为一元联结词, 其余的为二元联结词. 多次使用联结词集中的联结词, 可以组成更为复杂的复合命题. 求复杂的复合命题的真值时, 需要规定联结词的优先顺序, 将括号也考虑在内. 本书规定的联结词优先顺序为 ( )、$\neg$、$\wedge$、$\vee$、$\rightarrow$、$\leftrightarrow$, 对于同一优先级的联结词, 先出现者先运算.

### 1.1.3 命题表达式

通过前面的内容可以看出, 命题常项和命题变项利用联结词和圆括号通过有限步可以构造出新的复合命题. 在这些复合命题中, $P$、$Q$、$R$ 等不仅可以代表命题常项, 也可以代表命题变项, 这样组成的复合命题形式称为**命题表达式**或**命题公式**. 这些命题表达式的构成必须符合一定的规则. 为此, 给出下面的定义.

**定义 1.7 合式公式.**

(1) 单个命题常项和变项是合式公式, 并称为原子命题公式.

(2) 若 $A$ 是合式公式, 则 $(\neg A)$ 也是合式公式.

(3) 若 $A$、$B$ 是合式公式, 则 $(A \wedge B)$、$(A \vee B)$、$(A \rightarrow B)$、$(A \leftrightarrow B)$ 也是合式公式.

(4) 只有有限次地应用 (1) ~(3) 形式的符号串才是合式公式.

在命题逻辑中, 合式公式又称为**命题公式**, 简称为**公式**.

**注意**　这个定义是递归的. (1) 是递归的基础, 由 (1) 开始, 使用 (2)、(3) 规则, 可以得到任意的合式公式; 在公式的定义中, $A$、$B$ 等符号代表任意的命题公式, 以下定义均有类似用法; $(\neg A)$、$(A \wedge B)$ 等公式单独出现时, 外层括号可以省去, 写成 $\neg A$、$A \wedge B$ 等, 公式中不影响运算次序的括号也可以省去, 如公式 $(P \vee Q) \vee (\neg R)$ 可以写成 $P \vee Q \vee \neg R$.

由定义可知, $(P \rightarrow Q) \wedge (Q \leftrightarrow R)$、$(P \wedge Q) \wedge \neg R$、$P \wedge (Q \wedge \neg R)$ 等都是合式公式, 而 $PQ \leftrightarrow R$、$(P \rightarrow Q) \rightarrow (\wedge Q)$ 等都不是合式公式.

### 1.1.4　真值表的构造

一个含有命题变项的命题公式的真值是不确定的, 对它的每个命题变项用指定的命题常项代替后, 命题公式就变成了真值确定的命题了. 对于命题公式, 若对其中出现的每个命题变元都指定一个真值 1 或者 0, 就对命题公式 $A$ 进行了一种**真值指派**或一个**解释**, 而在该指派下会求出公式 $A$ 的一个真值. 若指定的一组值使 $A$ 为 1, 则称这组值为 $A$ 的**成真赋值**; 若使 $A$ 为 0, 则称这组值为 $A$ 的**成假赋值**.

**例 1.7**　设公式 $A$ 为 $(\neg P \vee Q) \rightarrow R$, 若将 $P$、$Q$、$R$ 分别用 (0, 0, 0) 替换, 得到公式 $A$ 的一种解释, 在这种解释下, $A$ 的真值为假, 是它的成假赋值. 同理还可用 (0, 0, 1)、(0, 1, 0)、(0, 1, 1)、(1, 0, 0)、(1, 0, 1)、(1, 1, 0)、(1, 1, 1) 这 7 种不同的真值指派来对公式进行解释.

容易看出, 含 $n(n \geqslant 1)$ 个命题变项的公式共有 $2^n$ 个不同的赋值.

将 $A$ 的所有可能的真值指派以及在每一个真值指派下的取值列成一个表, 就得到命题公式 $A$ 的**真值表**. 真值表可以更好地反映命题公式的真值情况.

由于对每个命题变项可以有两个真值 (T,F) 被指派, 所以有 $n$ 个命题变项的命题公式 $A(P_1, P_2, \cdots, P_n)$ 的真值表有 $2^n$ 行. 为有序地列出 $A(P_1, P_2, \cdots, P_n)$ 的真值表, 可将 F 看成 0, T 看成 1, 按二进制数次序列表.

构造真值表的具体步骤如下:

(1) 命题变项按英文字母字典序进行排列, 如 $A$, $B$, $C$, $\cdots$; 带有下标的命题变元则按下标由小到大的数序排列, 如 $P_1$, $P_2$, $P_3$, $\cdots$.

(2) 对公式的每种解释以二进制从小到大或从大到小的顺序列出.

(3) 若公式较为复杂, 求值遵循从简单到复杂, 由括号里面到外面逐步求值的原则.

**例 1.8**　求下列公式的真值表, 并求成真赋值和成假赋值.

(1) $\neg(P \rightarrow Q) \wedge Q$.

(2) $(Q \rightarrow P) \wedge Q \rightarrow P$.

(3) $(\neg P \vee Q) \rightarrow R$.

**解:**　公式 1 的真值表如表 1.6 所示, 从表可知, 公式 1 的赋值都是成假赋值, 没有成真赋值. 公式 2 的真值表如表 1.7 所示, 从表可知, 公式 2 的赋值都是成真赋值, 没有成假赋值.

公式 3 的真值表如表 1.8 所示, 从表可知, 公式 3 的成假赋值是 000、010、110, 其余的均是成真赋值.

**表 1.6 $\neg(P \to Q) \wedge Q$ 的真值表**

| $P$ | $Q$ | $P \to Q$ | $\neg(P \to Q)$ | $\neg(P \to Q) \wedge Q$ |
|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 0 |
| 0 | 1 | 1 | 0 | 0 |
| 1 | 0 | 0 | 1 | 0 |
| 1 | 1 | 1 | 0 | 0 |

**表 1.7 $(Q \to P) \wedge Q \to P$ 的真值表**

| $P$ | $Q$ | $Q \to P$ | $(Q \to P) \wedge Q$ | $(Q \to P) \wedge Q \to P$ |
|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 1 |
| 0 | 1 | 0 | 0 | 1 |
| 1 | 0 | 1 | 0 | 1 |
| 1 | 1 | 1 | 1 | 1 |

**表 1.8 $(\neg P \vee Q) \to R$ 的真值表**

| $P$ | $Q$ | $R$ | $\neg P$ | $\neg P \vee Q$ | $(\neg P \vee Q) \to R$ |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 1 | 0 |
| 0 | 0 | 1 | 1 | 1 | 1 |
| 0 | 1 | 0 | 1 | 1 | 0 |
| 0 | 1 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 0 | 1 |
| 1 | 0 | 1 | 0 | 0 | 1 |
| 1 | 1 | 0 | 0 | 1 | 0 |
| 1 | 1 | 1 | 0 | 1 | 1 |

### 1.1.5 命题符号化

有了前面的命题公式概念, 可以进一步研究把自然语言中的有些语句翻译成数理逻辑中的符号形式.

**定义 1.8** 把一个用自然语言叙述的命题写成由命题变项、联结词和圆括号表示的命题公式, 称为**命题符号化**.

命题符号化时应注意: 确定给定句子是否为命题; 确定句子中的联结词是否为命题联结词; 正确地表示原子命题和适当选择命题联结词.

**例 1.9** 将下列命题符号化.

(1) 我和他既是兄弟又是同学.

**解**: 设 $P$: 我和他是兄弟, $Q$: 我和他是同学.

命题可符号化为 $P \wedge Q$.

(2) 张三或李四都可以做这件事.

**解**: 设 $P$: 张三可以做这件事, $Q$: 李四可以做这件事.

命题可符号化为 $P \vee Q$.

(3) 仅当我有时间且天不下雨, 我将去镇上.

**解**: "仅当"实质上是"当"的逆命题. "当 $A$ 则 $B$"是 $A \to B$, 而"仅当 $A$ 则 $B$"是 $B \to A$. 设 $P$: 我有时间, $Q$: 天不下雨, $R$: 我将去镇上.

命题可符号化为 $R \to (P \wedge Q)$.

(4) 张刚总是在图书馆看书, 除非图书馆不开门或张刚生病.

**解**: 对于"除非", 只要记住, "除非"是条件. 设 $P$: 张刚在图书馆看书, $Q$: 图书馆不开门, $R$: 张刚生病.

命题可符号化为 $\neg(Q \vee R) \to P$.

(5) 风雨无阻, 我去上学.

**解**: 可理解为"不管是否刮风, 是否下雨, 我都去上学". 设 $P$: 天刮风, $Q$: 天下雨, $R$: 我去上学.

命题可符号化为 $(P \wedge Q \to R) \wedge (P \wedge \neg Q \to R) \wedge (\neg P \wedge Q \to R) \wedge (\neg P \wedge \neg Q \to R)$ 或 $(P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge R) \vee (\neg P \wedge Q \wedge R) \vee (\neg P \wedge \neg Q \wedge R)$.

**说明**　要准确确定原子命题, 并将其形式化; 要选用恰当的联结词, 尤其要善于识别自然语言中的联结词 (有时它们被省略); 否定词的位置要准确; 必要的括号不能省略, 而可以省略的括号在需要提高公式可读性时亦可不省略; 要注意命题的符号化未必是唯一的.

## 1.2　重　言　式

通过构造命题公式的真值表, 可以发现, 公式在各种赋值下会有不同的取值情况, 而一些形式不同的公式却有着相同的真值表, 为此需要进一步研究公式的分类及不同公式的联系特征及性质等内容.

### 1.2.1　命题公式分类

**定义 1.9**　设 $A$ 为任一命题公式.

(1) 若 $A$ 在它的各种赋值下取值均为真, 则称 $A$ 是**重言式**或**永真式**.

(2) 若 $A$ 在它的各种赋值下取值均为假, 则称 $A$ 是**矛盾式**或**永假式**.

(3) 若 $A$ 不是矛盾式, 则称 $A$ 是**可满足式**.

从定义可以看出以下几点:

(1) 重言式一定是可满足式, 但可满足式不一定是重言式.

(2) 矛盾式一定是不可满足式, 非矛盾式一定是可满足式.

(3) 真值表可用来判断公式的类型:

- 若真值表最后一列全为 1, 则公式为重言式.
- 若真值表最后一列全为 0, 则公式为矛盾式.
- 若真值表最后一列中至少有一个 1, 则公式为可满足式.

**说明**　$n$ 个命题变项共产生 $2^n$ 个不同赋值; 含 $n$ 个命题变项的公式的真值表只有 $2^{2^n}$ 种不同情况.