21世纪高等学校规划教材 | 计算机科学与技术

离散数学基础

（第二版）

谢胜利 虞铭财 黄月华 高丽丽 编著

清华大学出版社

离散数学基础

（第二版）

谢胜利 虞铭财 黄月华 高丽丽 编著

清华大学出版社
北京

内 容 简 介

本书对计算机类专业在本科阶段最需要掌握的离散数学基础知识做了系统介绍，力求概念清晰，注重实际应用。全书共7章，包括准备知识(集合、整数、序列、矩阵)、数理逻辑、组合数学(计数)、二元关系、布尔代数、图论(图、树、图和树的有关算法)等，并含有较多的与计算机类专业相关的例题和习题。

本书叙述简洁、深入浅出、注重实践和应用，主要面向地方院校和独立学院计算机类专业的本科学生，也可以作为大学非计算机专业学生的选修课教材和计算机应用技术人员的自学参考书。

图书在版编目(CIP)数据

离散数学基础/谢胜利等编著. --2版. --北京：清华大学出版社，2016
21世纪高等学校规划教材·计算机科学与技术
ISBN 978-7-302-42085-9

Ⅰ. ①离… Ⅱ. ①谢… 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(2015)第264102号

责任编辑：黄　芝
封面设计：傅瑞学
责任校对：时翠兰
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 装 者：北京密云胶印厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：12.5　　**字　　数**：302千字
版　　次：2012年1月第1版　2016年2月第2版　　**印　　次**：2016年2月第1次印刷
印　　数：1～2000
定　　价：29.00元

产品编号：066806-01

出版说明

随着我国改革开放的进一步深化，高等教育也得到了快速发展，各地高校紧密结合地方经济建设发展需要，科学运用市场调节机制，加大了使用信息科学等现代科学技术提升、改造传统学科专业的投入力度，通过教育改革合理调整和配置了教育资源，优化了传统学科专业，积极为地方经济建设输送人才，为我国经济社会的快速、健康和可持续发展以及高等教育自身的改革发展做出了巨大贡献。但是，高等教育质量还需要进一步提高以适应经济社会发展的需要，不少高校的专业设置和结构不尽合理，教师队伍整体素质亟待提高，人才培养模式、教学内容和方法需要进一步转变，学生的实践能力和创新精神亟待加强。

教育部一直十分重视高等教育质量工作。2007 年 1 月，教育部下发了《关于实施高等学校本科教学质量与教学改革工程的意见》，计划实施“高等学校本科教学质量与教学改革工程”（简称“质量工程”），通过专业结构调整、课程教材建设、实践教学改革、教学团队建设等多项内容，进一步深化高等学校教学改革，提高人才培养的能力和水平，更好地满足经济社会发展对高素质人才的需要。在贯彻和落实教育部“质量工程”的过程中，各地高校发挥师资力量强、办学经验丰富、教学资源充裕等优势，对其特色专业及特色课程（群）加以规划、整理和总结，更新教学内容、改革课程体系，建设了一大批内容新、体系新、方法新、手段新的特色课程。在此基础上，经教育部相关教学指导委员会专家的指导和建议，清华大学出版社在多个领域精选各高校的特色课程，分别规划出版系列教材，以配合“质量工程”的实施，满足各高校教学质量和教学改革的需要。

为了深入贯彻落实教育部《关于加强高等学校本科教学工作，提高教学质量的若干意见》精神，紧密配合教育部已经启动的“高等学校教学质量与教学改革工程精品课程建设工作”，在有关专家、教授的倡议和有关部门的大力支持下，我们组织并成立了“清华大学出版社教材编审委员会”（以下简称“编委会”），旨在配合教育部制定精品课程教材的出版规划，讨论并实施精品课程教材的编写与出版工作。“编委会”成员皆来自全国各类高等学校教学与科研第一线的骨干教师，其中许多教师为各校相关院、系主管教学的院长或系主任。

按照教育部的要求，“编委会”一致认为，精品课程的建设工作从开始就要坚持高标准、严要求，处于一个比较高的起点上。精品课程教材应该能够反映各高校教学改革与课程建设的需要，要有特色风格、有创新性（新体系、新内容、新手段、新思路，教材的内容体系有较高的科学创新、技术创新和理念创新的含量）、先进性（对原有的学科体系有实质性的改革和发展，顺应并符合 21 世纪教学发展的规律，代表并引领课程发展的趋势和方向）、示范性（教材所体现的课程体系具有较广泛的辐射性和示范性）和一定的前瞻性。教材由个人申报或各校推荐（通过所在高校的“编委会”成员推荐），经“编委会”认真评审，最后由清华大学出版

社审定出版。

目前,针对计算机类和电子信息类相关专业成立了两个“编委会”,即“清华大学出版社计算机教材编审委员会”和“清华大学出版社电子信息教材编审委员会”。推出的特色精品教材包括:

(1) 21 世纪高等学校规划教材·计算机应用——高等学校各类专业,特别是非计算机专业的计算机应用类教材。

(2) 21 世纪高等学校规划教材·计算机科学与技术——高等学校计算机相关专业的教材。

(3) 21 世纪高等学校规划教材·电子信息——高等学校电子信息相关专业的教材。

(4) 21 世纪高等学校规划教材·软件工程——高等学校软件工程相关专业的教材。

(5) 21 世纪高等学校规划教材·信息管理与信息系统。

(6) 21 世纪高等学校规划教材·财经管理与应用。

(7) 21 世纪高等学校规划教材·电子商务。

(8) 21 世纪高等学校规划教材·物联网。

清华大学出版社经过三十多年的努力,在教材尤其是计算机和电子信息类专业教材出版方面树立了权威品牌,为我国的高等教育事业做出了重要贡献。清华版教材形成了技术准确、内容严谨的独特风格,这种风格将延续并反映在特色精品教材的建设中。

清华大学出版社教材编审委员会

联系人:魏江江

E-mail:weijj@tup.tsinghua.edu.cn

前言

本书以第1版为基础，在听取广大读者的意见和建议的基础上修改而成。本版主要对第1版中一些描述错误和印刷错误进行订正，增加第4.8节的函数等内容。

离散数学是计算机类专业的一门重要的专业基础课，属于现代数学的范畴，是随着计算机科学的发展而逐步形成的一门新兴的工具性学科，它在计算机类专业的许多后续课程中有着广泛的应用，为计算机科学与技术提供数学基础。国内出版的离散数学教材不少，但特别适合地方院校和独立学院计算机类专业使用的不多，主要问题是理论性太强，大都是从纯数学的角度讨论问题，缺乏与计算机相关专业联系。本教材的写作目的是从离散数学教学的实际现状出发，克服目前国内教材普遍存在着重理论、忽视应用的问题，本着突出离散数学的实用性，按实用够用的原则精选教学内容，突破传统的离散数学的四大模块内容，删除部分大学阶段用不到的内容，增加基础知识、组合数学和布尔代数等内容，使教学内容更加实用易学。

本教材第1章主要介绍本书所需的准备知识，包括集合及在计算机中的表示、数论初步、序列和递推关系、一般矩阵和布尔矩阵的运算。第2章主要介绍数理逻辑的基础知识，包括命题逻辑和谓词逻辑的基本概念、演算及推理理论。第3章主要介绍组合数学中的计数理论和方法，包括计数法则、生成函数、鸽巢原理和容斥原理。第4章主要介绍二元关系理论，包括二元关系基本概念和运算、等价关系和划分、偏序关系和拓扑排序、n元关系及应用、函数等。第5章主要介绍布尔代数的基本理论和应用，包括布尔运算、布尔表达式和布尔函数、积之和展开式(析取范式)、逻辑门电路表示和卡诺图。第6章主要介绍图的基本理论和应用，包括图论基础、图的矩阵表示、连通性理论、几种特殊的图、带权图的最短路径算法(Dijkstra算法和Floyd算法)。第7章主要介绍树及其应用，包括树的定义、树的应用(决策树、前缀码等)、树的遍历算法、表达式表示、生成树和最小生成树算法(Prim和Kruskal算法)。

本教材有以下特点。

(1) 简单易学：只要求学生学过高等数学，不需要更多的预备知识，写作风格深入浅出，理论适中，实例丰富，便于自学。

(2) 实用性强：注重离散数学作为计算机科学专业的数学基础，强调与本专业后续课程的关系，所举例子尽量与专业相关。

(3) 定位明确：适合地方二本院校和独立学院学生使用。

本教材教学课时数为72～90学时。教师可根据学时数、专业和学生的实际情况对教材内容进行选讲。

本书由谢胜利、虞铭财、黄月华、高丽丽编写。其中第1章由虞铭财编写，第3章由黄月华编写，第5章由高丽丽编写，其余章节由谢胜利编写。全书由谢胜利统稿。

因为作者水平有限，难免存在错误，恳请读者赐教指正。

编　者

2015年9月

目 录

第1章 准备知识

1.1 集合

1.1.1 集合的基本概念

集合是一个基本的数学概念，它是不能精确定义的。一般认为一个集合指的是一些可确定且可分辨的对象或概念构成的整体。通常一个集合中的对象都具有相同(类似)的性质，当然也可以将完全无关的对象放在一个集合中。集合中的对象称为集合的元素。

定义 1.1 *若对象 a 是集合 A 的元素，记为 $a\in A$，读做 a 属于 A；否则记为 $a\notin A$，读做 a 不属于 A。*

元素与集合之间的“属于关系”是“非常明确”的。对某个集合 A 和元素 a 来说，a 或者属于集合 A，或者不属于集合 A，两者必居其一且仅居其一。界限不分明或含糊不清的情况绝对不允许存在。在离散数学中，仅仅讨论界限清楚、无二义性的集合，而对不清晰的对象构成的集合属于模糊论(Fuzzy Set Theory)的研究范畴，本书将不予研究。例如，著名的理发师问题就是属于模糊论的研究范畴。

集合的表示方法通常有如下两种。

一种是列出集合的所有元素，元素之间用逗号间隔，并用花括号将它们括起来，称为枚举法。如：

$$A=\{a,b,c,d\}$$

$$B=\{1,3,5,7,9\}$$

有时用花括号表示集合但并不列出它的所有元素，先列出集合中的某些元素，然后当元素的一般形式很明显时就用省略号表示。例如：

26 个大写英文字母的集合表示为$\{A,B,C,\cdots,Z\}$；

小于 100 的正整数集合表示为$\{1,2,3,\cdots,99\}$。

另一种是谓词法，即给出作为集合成员的元素所具有的性质，来刻画集合的所有元素。如：$\mathbf{R}=\{x\mid x$ 为实数$\}$，$A=\{x\mid x>3$ 且 $x\in\mathbf{R}\}$。

几个常用的集合符号：

$\varnothing$——空集(不含任何元素的特殊集合)；

$\mathbf{N}$——自然数集合；

Z——整数集合;

$\mathbf{Z}^+$——正整数集合;

Q——有理数集合;

R——实数集合;

C——复数集合。

定义 1.2 设 A,B 为集合,如果集合 A 的每个元素都是集合 B 的元素,则称 A 是 B 的子集,记为 $A\subseteq B$。如果 A 中至少存在一个元素它不是 B 的元素,则称 A 不是 B 的子集,记为 $A\nsubseteq B$。

根据定义有对任意集合 A,都有 $\varnothing\subseteq A, A\subseteq A$。

定义 1.3 设 A,B 为集合,如果 $A\subseteq B$ 且 $B\subseteq A$,则称 A,B 相等,记为 $A=B$。

因此要证明 A,B 相等,只要证明 A 是 B 的子集同时 B 也是 A 的子集。

如果强调 A 是 B 的子集,而 $A\neq B$,则称 A 是 B 的真子集,记为 $A\subset B$。

集合广泛用于计数问题,这类问题要讨论集合的大小。

定义 1.4 若 A 为集合,集合 A 中恰有 n 个不同的元素,n 是非负整数,则 A 为有限集,称 n 是 A 的基数,记为 $|A|=n$。含有 n 个元素的集合为 n 元集。

如:A 为大写英文字母集,则 $|A|=26$,B 为小于 10 的正整数集,则 $|B|=9$。由于空集没有元素,所以 $|\varnothing|=0$。

如果一个集合不是有限的,那么就是无限的。如整数集、实数集都是无限集。

许多问题都要检查一个集合所有可能的组合,看它们是否具有某种性质。为了考虑集合元素所有可能的组合,构造一个新集合,它以这个集合的所有子集作为它的元素。

定义 1.5 设 A 为集合,把 A 的全体子集构成的集合称作 A 的幂集,记为 $P(A)$ 或 2^A,符号化表示为:$P(A)=\{x\mid x\subseteq A\}$。

例 1.1 求 $P(\varnothing)$,$P(\{a\})$,$P(\{a,b\})$,$P(\{a,b,c\})$及其基数。

解:由于$\varnothing$中没有一个元素,故$\varnothing$的子集只有$\varnothing$,则 $P(\varnothing)=\{\varnothing\}$,$|P(\varnothing)|=1$。

$P(\{a\})=\{\varnothing,\{a\}\}$,$|P(\{a\})|=2$

$P(\{a,b\})=\{\varnothing,\{a\},\{b\},\{a,b\}\}$,$|P(\{a,b\})|=4$

$P(\{a,b,c\})=\{\varnothing,\{a\},\{b\},\{c\},\{a,b\},\{a,c\},\{b,c\},\{a,b,c\}\}$,$|P(\{a,b,c\})|=8$

不难看出,若 A 是 n 元集,则 $P(A)$有 2^n 个元素。

定义 1.6 在一个具体的问题中,如果所涉及的集合都是某个集合的子集,则称这个集合为全集,记做 E 或 U。

全集是一个相对的概念,由于研究的问题不同,所取的全集也不同。例如,在研究平面解析几何的问题时可把整个坐标平面取做全集。在研究整数的问题时,可以把整数集 **Z** 取做全集。

1.1.2 集合的基本运算和性质

两个集合可以以许多不同的方式结合在一起。例如,从爱好文学的学生集合和爱好体育的学生集合入手,可以构成爱好文学或爱好体育的学生集合,既爱好文学又爱好体育的学生集合,不爱好文学的学生集合等。

定义 1.7 设 A,B 是两个集合,则 A 与 B 的并集(Union)是由 A 与 B 中的所有元素构

成的集合。

$$A \cup B = \{x \mid (x \in A) \text{或} (x \in B)\}$$

例 1.2 并运算。

$$\{1,2,3,4\} \cup \{3,4,5,6\} = \{1,2,3,4,5,6\}$$
$$\{a,b,c\} \cup \{a,d,e\} = \{a,b,c,d,e\}$$
$$\{a,b,c,d\} \cup \varnothing = \{a,b,c,d\}$$
$$\mathbf{Q} \cup \mathbf{N} = \mathbf{Q}$$

上述集合的并运算可以说是初等数学中“加法”运算的一个扩充。

定义 1.8 设 A,B 是两个集合，则 A 与 B 的交集(Intersection)是由 A 与 B 中的共同元素构成的集合。

$$A \cap B = \{x \mid (x \in A) \text{并且} (x \in B)\}$$

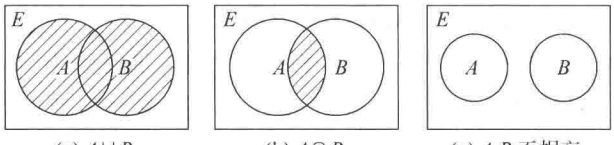
例 1.3 交运算。

$$\{1,2,3,4\} \cap \{3,4,5,6\} = \{3,4\}$$
$$\{a,b,c\} \cap \{a,d,e\} = \{a\}$$
$$\{a,b,c,d\} \cap \varnothing = \varnothing$$
$$\mathbf{Q} \cap \mathbf{N} = \mathbf{N}$$

上述集合的交运算可以说是初等数学中“乘法”运算的一个扩充。

如果两个集合的交集为空集，就说两个集合不相交。

集合之间运算和相互关系可以用文氏图(JohnVenn)来刻画，图 1.1 分别表示 A,B 的并集、交集、两集合不相交。



(a) $A \cup B$ (b) $A \cap B$ (c) A,B 不相交

图 1.1 集合 A,B 的并集、交集、两集合不相交

定义 1.9 设 A,B 是两个集合，则 A 与 B 的差集(Difference)是只属于 A 而不属于 B 的所有元素构成的集合。A 与 B 的差集也称为 B 相对于 A 的补集。

$$A - B = \{x \mid (x \in A) \text{并且} (x \notin B)\}$$

例 1.4 差运算。

$$\{1,2,3,4\} - \{3,4,5,6\} = \{1,2\}$$
$$\{a,b,c\} - \{a,d,e\} = \{b,c\}$$
$$\{a,b,c,d\} - \varnothing = \{a,b,c,d\}$$
$$\varnothing - \{a,b,c,d\} = \varnothing$$

一旦指定了全集 U，就可以定义集合的补集。

定义 1.10 令 U 是全集，则集合 A 的补集 $\overline{A}$(Complement)就是 $U-A$。

$$\overline{A} = \{x \mid x \notin A\}$$

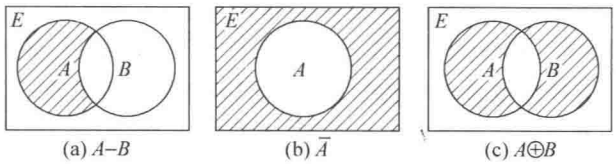
定义 1.11 设 A,B 是两个集合，则 A 与 B 的对称差是：

$$A \oplus B = (A - B) \cup (B - A)$$

例 1.5 对称差运算。

$$\{1,2,3,4\}\oplus\{3,4,5,6\}=\{1,2,5,6\}$$
$$\{a,b,c\}\oplus\{a,d,e\}=\{b,c,d,e\}$$
$$\{a,b,c,d\}\oplus\varnothing=\{a,b,c,d\}$$

$A-B$,$\overline{A}$,$A\oplus B$ 可以用图 1.2 所示的文氏图表示。



(a) $A-B$　(b) $\overline{A}$　(c) $A\oplus B$

图 1.2　$A-B$,$\overline{A}$,$A\oplus B$ 的文氏图

任何代数运算都遵循一定的算律,下面的恒等式给出了集合运算的主要算律,其中 A,B,C 代表任意集合。

幂等律　$A\cup A=A$　(1.1)

$A\cap A=A$　(1.2)

结合律　$(A\cup B)\cup C=A\cup(B\cup C)$　(1.3)

$(A\cap B)\cap C=A\cap(B\cap C)$　(1.4)

交换律　$A\cup B=B\cup A$　(1.5)

$A\cap B=B\cap A$　(1.6)

分配律　$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$　(1.7)

$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$　(1.8)

同一律　$A\cup\varnothing=A$　(1.9)

$A\cap U=A$　(1.10)

零律　$A\cup U=U$　(1.11)

$A\cap\varnothing=\varnothing$　(1.12)

排中律　$A\cup\overline{A}=U$　(1.13)

矛盾律　$A\cap\overline{A}=\varnothing$　(1.14)

吸收律　$A\cup(A\cap B)=A$　(1.15)

$A\cap(A\cup B)=A$　(1.16)

德摩根律　$A-(B\cup C)=(A-B)\cap(A-C)$　(1.17)

$A-(B\cap C)=(A-B)\cup(A-C)$　(1.18)

$\overline{A\cup B}=\overline{A}\cap\overline{B}$　(1.19)

$\overline{A\cap B}=\overline{A}\cup\overline{B}$　(1.20)

$\overline{\varnothing}=U$　(1.21)

$\overline{U}=\varnothing$　(1.22)

双重否定律　$\overline{\overline{A}}=A$　(1.23)

例 1.6 令 A,B,C 为任意集合,证明:

$$\overline{A\cup(B\cap C)}=(\overline{C}\cup\overline{B})\cap\overline{A}$$

证明：我们有$\overline{A\cup(B\cap C)}=\overline{A}\cap\overline{B\cap C}$

$$=\overline{A}\cap(\overline{B}\cup\overline{C})$$
$$=\overline{A}\cap(\overline{C}\cup\overline{B})$$
$$=(\overline{C}\cup\overline{B})\cap\overline{A}$$

1.1.3 集合的笛卡儿积

笛卡儿积在后面讨论关系和图论时都有重要应用。

首先引入有序对和无序对的概念。

定义 1.12 由两个元素 x 和 y(允许 $x=y$)按一定顺序排列成的二元组叫作一个有序对或序偶，记作$\langle x,y\rangle$，其中 x 是它的第一元素，y 是它的第二元素。若两个元素 x 和 y 之间无排列次序，则该二元组叫作无序对，记做(x,y)。

有序对$\langle x,y\rangle$具有以下性质。

(1) 当 $x\neq y$ 时，$\langle x,y\rangle\neq\langle y,x\rangle$。

(2) $\langle x,y\rangle=\langle u,v\rangle$的充分必要条件是 $x=u$ 且 $y=v$。

这些性质是无序对(x,y)所不具备的。例如当 $x\neq y$ 时有$(x,y)=(y,x)$。原因在于有序对中的元素是有序的，而无序对中的元素是无序的。

例 1.7 已知$\langle x+2,4\rangle=\langle 5,2x+y\rangle$，求 x 和 y。

解：由有序对相等的充要条件有

$$x+2=5$$
$$2x+y=4$$

解得 $x=3,y=-2$。

定义 1.13 设 A,B 为集合，用 A 中元素为第一元素，B 中元素为第二元素构成有序对。所有这样的有序对组成的集合叫作 A 和 B 的笛卡儿积，记做 $A\times B$。笛卡儿积的符号化表示为 $A\times B=\{\langle x,y\rangle\mid x\in A\wedge y\in B\}$。

例 1.8 设 $A=\{a,b\}$，$B=\{0,1,2\}$，则

$$A\times B=\{\langle a,0\rangle,\langle a,1\rangle,\langle a,2\rangle,\langle b,0\rangle,\langle b,1\rangle,\langle b,2\rangle\}$$
$$B\times A=\{\langle 0,a\rangle,\langle 0,b\rangle,\langle 1,a\rangle,\langle 1,b\rangle,\langle 2,a\rangle,\langle 2,b\rangle\}$$

从本例可以看出，$A\times B\neq B\times A$，除非 $A=B$。即笛卡儿积不满足交换律。

虽然笛卡儿积不满足交换律，也不满足结合律，但笛卡儿积对$\cap$，$\cup$，$-$，$\oplus$都满足分配律。

(1) $A\times(B\cup C)=(A\times B)\cup(A\times C)$。

(2) $(B\cap C)\times A=(B\times A)\cap(C\times A)$。

(3) $(B-C)\times A=(B\times A)-(C\times A)$。

(4) $(B\oplus C)\times A=(B\times A)\oplus(C\times A)$。

由排列组合的知识不难证明，如果$|A|=m$，$|B|=n$，则$|A\times B|=mn$。

1.1.4 集合的计算机表示

要在计算机中实现集合的各种运算，必须首先确定集合在计算机中的表示方法。计算

机中表示集合的方式有各种各样。首先想到的是将集合用数组来表示,将集合的元素依次放在数组中,这样在求集合的交、并、差等运算时会非常浪费时间,因为这些运算涉及大量的元素查找和移动。

我们将要介绍一种利用全集元素的一个任意排序存放元素以表示集合的方法。集合的这种表示法使我们很容易计算集合的各种组合。

假定全集 U 是有限的(而且大小合适,使 U 的元素个数不超过计算机能使用的内存量)。首先为 U 中的元素任意规定一个顺序,例如 $a_1, a_2, \cdots, a_n$。于是可用长度为 n 的二进制位串表示 U 的子集 A:如果 $a_i \in A$,则位串中第 i 位为 1,如果 $a_i \notin A$,则位串中第 i 位为 0。

例 1.9 若 $U=\{a,b,c,d,e,f,g,h\}$,则 $A=\{b,d,f,g\}$,$B=\{a,d,e,f\}$,$\varnothing$,U 对应的二进制位串是什么?

解:将 U 中元素按字典顺序排列,即 a 对应第 1 位、b 对应第 2 位、……、h 对应第 8 位。则

集合 A 对应的 8 位二进制串为 0101 0110。

集合 B 对应的 8 位二进制串为 1001 1100。

集合 $\varnothing$ 对应的 8 位二进制串为 0000 0000。

集合 U 对应的 8 位二进制串为 1111 1111。

用位串表示的集合便于计算集合的补、交、并、对称差。只要对表示集合的位串按位做各种布尔运算。集合的补、交、并、对称差运算对应位串的布尔反、与、或和异或运算。

例 1.10 若 $U=\{a,b,c,d,e,f,g,h\}$,$A=\{b,d,f,g\}$,$B=\{a,d,e,f\}$,求 $\overline{A}$,$A \cap B$,$A \cup B$,$A \oplus B$。

解:A 对应的 8 位二进制串为 0101 0110,对该二进制串的各位求反,得到 $\overline{A}$ 对应的 8 位二进制串 1010 1001。

将 A,B 对应的二进制位串按位求与(bitwise AND):

0101 0110 $\wedge$ 1001 1100 = 0001 0100,则 $A \cap B$ 对应的二进制串为 0001 0100。

将 A,B 对应的二进制位串按位求或(bitwise OR):

0101 0110 $\vee$ 1001 1100 = 1101 1110,则 $A \cup B$ 对应的二进制串为 1101 1110。

将 A,B 对应的二进制位串按位求异或(bitwise XOR):

0101 0110 $\oplus$ 1001 1100 = 1100 1010,则 $A \oplus B$ 对应的二进制串为 1100 1010。

分别表示的集合为 $\{d,f\}$,$\{a,b,d,e,f,g\}$,$\{a,b,e,g\}$。

1.2 整数

1.2.1 整除

当一个整数除以另一个整数的时候,商可能是整数,也可能不是整数。例如 15/3=5 是整数,而 15/4=3.75 不是整数,我们有下面的定义。

定义 1.14 如果 a,b 是整数,$a \neq 0$,若有整数 c 使得 $b=ac$,就说 a 整除 b。在 a 整除 b 时,a 是 b 的一个因子,b 是 a 的倍数。符号 $a \mid b$ 表示 a 整除 b,当 a 不整除 b,写成 $a \nmid b$。

定理 1.1 如果 a 和 b 是任意两个整数,且 $a>0$,则必有 $b=qa+r$,其中 q,r 是整数,且

$0 \leqslant r < a$。q 称为商(Quotient),r 称为余数(Remainder)。

例 1.11

(1) $a=3, b=16$,则 $16=5\times(3)+1$,即 $q=5, r=1$。

(2) $a=10, b=3$,则 $3=0\times(10)+3$,即 $q=0, r=3$。

(3) $a=5, b=-11$,则 $-11=-3\times(5)+4$,即 $q=-3, r=4$。

定理 1.2 令 a, b 和 c 都是整数,则:

(1) 如果 $a|b$ 且 $a|c$,则 $a|(b+c)$。

(2) 如果 $a|b$ 且 $a|c$,而且 $b>c$,则 $a|(b-c)$。

(3) 如果 $a|b$ 或 $a|c$,则 $a|(bc)$。

(4) 如果 $a|b$ 且 $b|c$,则 $a|c$。

证明:

(1) 如果 $a|b$ 且 $a|c$,则 $b=k_1 a$ 且 $c=k_2 a$(k_1, k_2 是整数),所以,$(b+c)=(k_1+k_2)a$,即 $a|(b+c)$。

(2) 证明完全同(1)中的证明。

(3) 如同(1),有 $b=k_1 a$ 或 $c=k_2 a$(k_1, k_2 是整数),则或者 $bc=k_1 ac$,或者 $bc=k_2 ab$。

所以,在任何情况下都有 $a|bc$。

(4) 如果 $a|b$ 且 $b|c$,有 $b=k_1 a$ 且 $c=k_2 b$(k_1, k_2 是整数),所以,$c=k_2 b=k_2(k_1 a)=(k_2 k_1)a$,因而,$a|c$。

推论 1.1 如果 $a|b$ 且 $a|c$,则 $a|(mb+nc)$,其中 m, n 是整数。

定义 1.15 一个大于 1 的正整数 p 被称为素数或质数(Prime),如果仅有 p 自身和数字 1 能整除 p。大于 1 又不是素数的正整数称为合数。

例 1.12 数 2,3,5,7,11,13 都是素数,而 4,10,16,21 则是合数。

小于 100 的素数有 2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97。

素数是构成正整数的根本,可由下面的算术基本定理揭示。

定理 1.3 (算术基本定理)每一个大于 1 的整数 n 可以唯一地被分解成:$p_1^{k_1} p_1^{k_2} \cdots p_s^{k_s}$(其中:$p_1 < p_2 < \cdots < p_s$ 是整除 n 的不同的素数,k_i 是正整数,该正整数的值是每个素数作为 n 的因子所出现的次数)。

例 1.13

(1) $9=3\times3=3^2$。

(2) $24=8\times3=2\times2\times2\times3=2^3\times3$。

(3) $30=2\times3\times5$。

在密码学中为信息加密的某些地方往往用到大素数。证明一个整数是否是素数很重要。定理 1.4 可以得到证明一个整数为素数的方法。

定理 1.4 如果 n 是合数,那么它必有一个小于或等于$\sqrt{n}$的素因子。

证明: 如果 n 是合数,则它有一个因子 a,使得 $1<a<n$,于是 $n=ab$,其中 a 和 b 是大于 1 的正整数。这样就有 $a \leqslant \sqrt{n}$ 或 $b \leqslant \sqrt{n}$,否则 $ab>\sqrt{n}\cdot\sqrt{n}=n$。所以 n 有一个不大于$\sqrt{n}$的正因子。这个因子或是素数,或根据算术基本定理有素因子。无论哪种情况,n 都有一个小