2018~2019 学年离散数学笔记

南京大学数学系孙智伟老师授课
Fiddie 整理

Ver 1.5

March 28, 2025

Contents

第 1 章　数学基础与一阶逻辑

离散数学 (discrete mathematics) 包括: 数理逻辑、组合数学与图论、初等数论、可计算性理论、格与布尔代数、编码理论、集合论、抽象代数. 离散数学研究离散的数学结构, 与分析相对立, 于 20 世纪 30 年代兴起. Paul Erdos(1913-1996) 对离散数学的发展作出重大贡献. 有人提出了 Erdos Number 来衡量人与 Erdos 的距离. R.L. Graham 和他的夫人 Fan Chung Graham 都作了很大贡献. W.T. Gowers 用 Ramsay 定理解决泛函分析问题.

D.E.Knuth 发明了 LaTeX, 他的《程序设计技巧》(The art of computer programming) 是全 20 世纪最伟大的计算机著作, 与数论有很大关系. **做这份离散数学笔记的语言正是 LaTeX**. 我参与运营的微信公众号“**数学兔的极大理想**”经常分享数学笔记, 欢迎关注!

§ 1.1　集合论的创立与第三次数学危机

1.1.1　Cantor 集合论

集合论的创始人: Georg Cantor(1845-1918), 他生于圣彼得堡, 和 Schwarz 是朋友, 在 1862 年上大学, 1867 成为数论方向博士. 1869 年, Heine 建议 Cantor 证明 Fourier 展式唯一性 (1870 年证出)

$$f(x)=\frac{a_0}{2}+\sum_{n=1}^{\infty}(a_n\cos nx+b_n\sin nx).$$

上式收敛仍可能有间断点, 于是 Cantor 研究这些间断点构成的集合, 又转而研究集合论.

Cantor 对集合的定义: 所谓集合, 就是把我的直观或思维中确定的相互间有明确区别的那些对象 (叫集合的元素) 看作一个整体来考虑.

定义 1.1.1

如果存在集合 X 和 Y 的一一对应, 则称这两个集合是**等势**的 $(X\approx Y)$, 或者说 X 与 Y 有相同的**基数** (cardinality), 即 $|X|=|Y|$. 如果 $A\approx\mathbb{N}=\{0,1,2,\cdots\}$, 则称 A 是**可数的 (可列的)**.

例 1.1.2: 可数的例子

(1) $\{0,2,4,6,\cdots\}$ 可数, 因为可取 $n\longmapsto 2n,\mathbb{N}\to 2\mathbb{N}$.

(2) 如果 A,B 可数, 则 $A\cup B$ 可数: $\{a_0,b_0,a_1,b_1,\cdots\}$(重复删掉).

(3) 整数集 $\mathbb{Z}$ 可数: $\{0,1,-1,2,-2,3,-3,\cdots\}$.

(4) 有理数集 $\mathbb{Q}$ 可数: 分子 + 分母小的先数, 对 $\frac{p}{q}$, 若 $p+q$ 相同, 分子小的先数. 重复的删掉 (方框部分):

$$\left\{\frac{0}{1},\boxed{\frac{0}{2}},\frac{1}{1},-\frac{1}{1},\boxed{\frac{0}{3}},\frac{1}{2},-\frac{1}{2},\frac{2}{1},-\frac{2}{1},\cdots\right\}$$

名人语录:

(1) 数学的精髓在于自由. ——Cantor

(2) Cantor 的贡献可能是这一时代所能夸耀的最巨大的工作. ——Russell

例 1.1.3: 旅馆问题

有可数个房间且住满人, 若再来一个客人, 可以让 n 号房间的人搬到 $n+1$ 号, 让客人去 0 号房; 若再来可数个客人, 可让 n 号房间的人搬到 $2n$ 号.

定义 1.1.4

所有有理系数非零多项式 $P(x)$ 中, $P(x)$ 的零点叫**代数数**, 非代数数的复数叫**超越数**.

例 1.1.5: 代数数与超越数例子

(1) $r \in \mathbb{Q}$ 是 $x-r=0$ 的根, 所以有理数必为代数数.
(2) 实的超越数是无理数.
(3) 已知 π, e 等少量几个是超越数.
(4) 定义 $P(x)=\sum\limits_{k=1}^{n} a_k x^k$ 的**高** (height) 为:

$$h(p)=n+\sum_{k=0}^{n}|a_k|.$$

则 $h(p)\leq$ 常数 c 的 $\mathbb{Z}[x]$ 只有有限个. $P(x)\in\mathbb{Z}[x]$ 中, 高小的先数, 则 $\mathbb{Z}[x]$ 可数, 它有 n 个根. 如果把它们列一下, 则全体代数数都可数.

Cantor 用集合论证明了超越数比代数数多. 1873 年, Cantor 考虑实数集是否可数.

(1) 小区间与大区间可以一一对应: $[0,1]\approx[a,b]$. 只需让 $f(x)=a+(b-a)x$, 它是单射也是满射.

(2) 开区间与闭区间一一对应: $[0,1]\approx(0,1]\approx[0,1)\approx(0,1)$. 让

$$f(0)=\frac{1}{2}, f\left(\frac{1}{2^n}\right)=\frac{1}{2^{n+1}}(n=1,2,\cdots), 0<x<1.$$

且当 x^{-1} 不为 2 的幂次时 $f(x)=x$. 则 $f(x)$ 是 $[0,1)$ 到 $(0,1)$ 的一一对应.

$$\begin{array}{cccccc} & \frac{1}{2} & \frac{1}{4} & \frac{1}{8} & \cdots & \\ \nearrow & \nearrow & \nearrow & \nearrow & & \\ 0 & \frac{1}{2} & \frac{1}{4} & \frac{1}{8} & \cdots & (\text{其他不动}) \end{array}$$

同理, $[a,b]\approx[a,b)\approx(a,b]\approx(a,b)$.

(3) 无穷区间与有限区间对应:

① $y=\tan x$ 是从 $\left(-\frac{\pi}{2},\frac{\pi}{2}\right)$ 到 $(-\infty,+\infty)$ 的一一对应;

② $f(x)=\dfrac{1}{1-x}, x\in[0,1)$ 是从 $[0,1)$ 到 $[1,+\infty)$ 的一一对应.

定理 1.1.6

实数轴上任意两端区间等势.

证明: 根据前面的 (1)(2)(3) 可得. □

定理 1.1.7. Cantor,1873

实数集 $\mathbb{R}$ 不可数.

证明: 根据上面定理, $\mathbb{R} \approx [0,1]$. 假设 $[0,1]$ 可数, 即 $[0,1] \approx \mathbb{N}$, f 是 $\mathbb{N} \to [0,1]$ 的一一对应, 把 $f(n)$ 写成

$$x_n = 0.x_{n_0}x_{n_1}x_{n_2}\cdots(\text{十进制})$$

其中 $x_{n_i} \in \{0,1,\cdots,9\}$. 则

$$\begin{aligned} x_0 &= 0.x_{00}x_{01}x_{02}x_{03}\cdots \\ x_1 &= 0.x_{10}x_{11}x_{12}x_{13}\cdots \\ x_2 &= 0.x_{20}x_{21}x_{22}x_{23}\cdots \\ x_3 &= 0.x_{30}x_{31}x_{32}x_{33}\cdots \\ &\cdots \end{aligned}$$

取 $a_n \in \{1,2,\cdots,8\}$ 使得 $a_n \neq x_{nn}$ (不取 0 与 9 是防止有两种表示) 考虑 $a = 0.a_0a_1a_2\cdots$(每一位都不是 0 或 9), 则 $a \in [0,1]$, 但是 $a_n \neq x_{nn}, \forall n$, 则 $a \neq x_n$, 这与 $[0,1] = \{x_0, x_1, x_2, \cdots\}$ 矛盾. □

注: 上面的证明方法叫**对角线方法**. 定理表明, 实数集基数比自然数集基数大. 把 $|\mathbb{N}|$ 记为 $\aleph_0$(阿列夫零), 把 $|\mathbb{R}|$ 记为 $\aleph$(阿列夫). Crelle 的杂志上记载了上面论文.

推论 1.1.8

实的超越数不可数.

注: (1) 实的代数数可数.

注: (2) 一条线上的点与 n 维立方体 $[0,1]^n$ 上的点可以一一对应.

Kronecker(Crelle 杂志的编辑) 对集合论很抨击, 后来很多人反对集合论, Cantor 很难发文章. 有数学家反对集合论是因为"信口开河", 没给出一个超越数, 基数的概念是"雾中之雾". 后来 Cantor 进了精神病院.

名人名言: 集合论是一种疾病. ——Poincaré

Cantor 连续统假设: 没有集合 X 使 $\aleph_0 < |X| < \aleph_1$.

定义 1.1.9

如果 A 与 B 的一个子集一一对应, 则说 $A \preccurlyeq B(|A| \leq |B|)$. 如果 $A \preccurlyeq B$ 但 A, B 不一一对应, 则说 $A \prec B(|A| < |B|)$.

1.1.2 算术 (自然数理论) 是否自相矛盾

从集合论可以定义自然数 $0 = \varnothing, 1 = \{0\}, 2 = \{0,1\}$. 1902 年 Russell 发现 Cantor 的朴素 (naive) 集合论自相矛盾. 第三次数学危机与数学根基有关.

Russell 悖论 (Paradox): 如果 $\{\text{集合}x : x \notin X\}$ 是个集合 X, 则 $X \in X \Leftrightarrow X \notin X$, 根据排中律, $X \in X$ 或 $X \notin X$, 无论出现哪种情况都会有矛盾.

Cantor 集合论中概括原理: $\{\text{集合}x : x\text{具有某种性质}\varphi(x)\}$ 是个集合.

定理 1.1.10

不存在基数最大的集合.

证明: Cantor 发现 $X \prec D(X) = \{X\text{的子集}\}$, 如果把所有集合拿来, 基数比原来就会大, 矛盾. □

理发师悖论: 南大仙林校区的理发师给且只给南大仙林校区不自己理发的人理发. 他该不该给自己理发?

说谎悖论：“我在说谎”对不对?

Perry 悖论: 汉字只有有限个 (不超过一百个汉字的句子有有限个), 而自然数有无限个, 故存在不能用不超过一百个汉字的句子描述的自然数, 有“不能用不超过一百个汉字的句子描述的最小的自然数”, 小于一百个汉字描述了那个特定的自然数.

Gödel 不完备定理 (1931) 在一个相容的公理可数的包含算术的公理系统中, 无法证明其相容性, 且此系统有个命题 α, 使得 α 与非 α 在系统中都不可证. (要相容性就没完备性)

1.1.3 关于数学基础形成的三个流派

1. 罗素为代表的逻辑主义（不是很成功）
2. Kronecker, Brouwer 为代表的直觉主义（不接受排中律）
3. Hilbert 为代表的形式主义：集合不应下定义 (最基本的概念没法定义), 他主张建立公理系统, 但最终没建立, 因为要过分追求完美. 好的公理化系统要求: (1) 公理之间独立, 不可互推. (2) 相容性 (不自相矛盾), (3) 完备性 (对的都有证明).

例 1.1.11: 公理化

以 Euclid 平面几何为例.

平行线公理: 过直线外一点可作唯一的一条直线与之平行 (三角形内角和为 180 度用了此公理).

1830 年 Janos Bolyai 设这个公理不成立, 推出了许多古怪定理, 但与前 4 个公理不矛盾.

1813 年 Gauss 考虑过这个问题, 但因害怕被嘲讽而没公开.

Lobachevsky, 大学校长, 俄国人, 要发展一种新的几何, 保留前 4 个公理但第 5 个公理改成: " 过直线外一点, 可作这条直线的至少两条平行线. " 在他的大学校报公开发表, 这种几何叫 Lobachevsky 几何.

1850 年 Riemann 发展了 Riemann 几何, 改为了“过直线外一点, 一条平行线都作不出来”. 这是广义相对论的几何框架.

1866 年证明了非欧几何不矛盾等价于 Euclid 几何不矛盾.

§ 1.2 命题联结词与合式公式

名人名言：逻辑是不可战胜的, 因为要反对逻辑还得使用逻辑. ——R. Boutoux

数学根基在于一阶逻辑之上, 先讲命题验算 (proposition calculus).

定义 1.2.1: 命题

陈述客观世界事情的陈述句叫**命题** (proposition), 其特征性质是可分真假.

命题的“真值”有两种: 真 (true,T,1)、假 (false,F,0), 常用 $p, q, r\cdots$ 表示命题.

由简单命题造复杂命题时常用命题联结词: 如果.. 则.., 如果 (如果 (如果.. 则..) 则..) 则.., 但用文字写很难看, 故用符号 $((p \to q) \to r) \to s$.

命题联结词有下面 5 种.

1. **否定词 (negation)** 命题 p 的否定记为 $\neg p$(非 p).

$$\neg p\text{真} \Leftrightarrow p\text{假}.$$

例如: 若"$2+3=7$" 表示 p, 则 $\neg p$ 表示 $2+3 \neq 7$.

2. **析取词 (disjunction)**: $p \vee q$(p 或 q).

$$p \vee q\text{真} \Leftrightarrow p\text{真或}q\text{真}.$$

例如: p :It's a cat. q :It's a tiger. 则 $p \vee q$:It's either a cat or a tiger or both.

3. **合取词 (junction)**: $p \wedge q$(p 并且 q).

$$p \wedge q\text{真} \Leftrightarrow p, q\text{都真}.$$

例如: p :He can sing songs. q :She can dance well. 则 $p \wedge q$:He can sing songs while she can dance well.

4. **蕴含词 (implication)**$p \to q$(p 蕴涵 q, p only if q).

$$p \to q\text{真} \Leftrightarrow p\text{假, 或}p, q\text{都真}.$$

$p \to q$ 成立时, p 为 q 的充分条件 (sufficient condition), q 为 p 的必要条件 (necessary condition).

5. **等价词 (equivalence, biconditional)**$p \leftrightarrow q$ (当且仅当, 等价, if and only iff, iff).
$p \leftrightarrow q$ 真, 指 p, q 同时真或者同时假, 相当于 $p \to q$(p only if q) 且 $q \to p$(p if q). 此时 p 是 q 的充分必要条件. 例如: p :You can take the flight. q :You buy a ticket. $p \leftrightarrow q$:You can take the flight if and only if you buy a ticket.

1.2.1 命题演算中的合式公式

(1) 命题符号是合式公式.
(2) 如果 α 是合式公式, 则 $\neg\alpha, \alpha \vee \beta, \alpha \wedge \beta, \alpha \to \beta, \alpha \leftrightarrow \beta$ 也是.
(3) 合式公式仅限于上法所得.
省略括号时, 规定否定词级别最高, 如 $(\neg\alpha) \to \beta$ 即 $\neg\alpha \to \beta$.
讨论两个命题的关系不用联结词, 比如 $p \leftrightarrow q \Leftrightarrow (p \to q) \wedge (q \to p)$.
$p \to q$ 的逆命题指的是 $q \to p$, 逆否命题指的是 $\neg q \to \neg p$.

例 1.2.2

p 与 q 恰好有一个成立, 可表示为 $(p \wedge \neg q) \vee (\neg p \wedge q)$.

George Boole(1815-1866) 首先引入了命题联结词, 讨论命题验算. 1854 年《The Law of Thought》是他的成名作, 把命题逻辑代数化.

练习题 1.

将下列语句翻译成命题逻辑表达式. (用 p, q, r 表示命题, 再写好合式公式)

(1)You can access the Internet from campus only if you are in computer science major or you are not a freshman.

(2)You are not a top student, unless you can work out this problem.

§ 1.3 命题的等价与永真公式

定义 1.3.1

设命题 (合式公式)φ 中共有 n 个命题变元 $p_1,\cdots,p_n$, 对 $p_1,\cdots,p_n$ 分别指定真值 $\delta_1,\cdots,\delta_n(\delta_i\in\{0,1\})$, 则称 φ 有个**赋值 (指派)**$(p_1,\cdots,p_n)=(\delta_1,\cdots,\delta_n)$.

如果此赋值使得 φ 真, 则称它为 φ 的**成真赋值**. 如果此赋值使得 φ 假, 则称它为 φ 的**成假赋值**. 如果在任何赋值下 φ 都真, 则称 φ 为**永真公式 (重言式)**. 如果 φ 有成真公式, 则称 φ 为**可满足的**. φ 永真时, 称 φ 为**逻辑规律**.

对于命题公式 α 与 β, 如果在任何赋值之下, α,β 同真假, 则称 α 与 β **等价**, 记为

$$\alpha\equiv\beta,$$

相当于 $\alpha\leftrightarrow\beta$ 永真.

注: $\alpha\equiv\beta$ 表示的是两个命题之间的关系, 而 $\alpha\leftrightarrow\beta$ 只是一个命题.

真值表 (truth table):

	p_1	p_2	$\cdots$	p_n	p
2^n 个 $\left\{\vphantom{\begin{matrix}a\\b\\c\end{matrix}}\right.$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	

例如，最简单的命题联结词的真值表:

p	$\neg p$
0	1
1	0

p	q	$p\vee q$
0	0	0
0	1	1
1	0	1
1	1	1

p	q	$p\wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

p	q	$p\to q$
0	0	1
0	1	1
1	0	0
1	1	1

1.3.1 命题演算的一些基本的逻辑规律

注: 画真值表可以严格证明.

1. 关于否定词:
   (1) $\neg\neg\alpha\equiv\alpha$.
   (2) $\alpha\vee\neg\alpha$.(排中律)
   (3) $\neg(\alpha\wedge\neg\alpha)$.(矛盾律)
   (4) $(\alpha\to\neg\beta)\to(\beta\to\neg\alpha)$.
2. 关于蕴含词:
   (1) $\alpha\to\alpha$.
   (2) $\alpha\to(\alpha\to\beta)\equiv\alpha\to\beta$.
   (3) $(\alpha\to(\beta\to\gamma))\to(\beta\to(\alpha\to\gamma))$.
   (4) $(\alpha\to\beta)\to(\beta\to\gamma)\to(\alpha\to\gamma)$.
3. 关于等价词:
   (1) $\alpha\leftrightarrow\beta\equiv(\alpha\to\beta)\wedge(\beta\to\alpha)\equiv(\alpha\wedge\beta)\vee(\neg\alpha\wedge\neg\beta)$(非常好用).
   (2) $(\alpha\to\beta)\to((\beta\to\alpha)\to(\alpha\leftrightarrow\beta))$.
4. 关于析取词与合取词:
   (1) $\alpha\vee\alpha\equiv\alpha\wedge\alpha\equiv\alpha$.(幂等律)

(2) $\alpha \vee \beta \equiv \beta \vee \alpha, \alpha \wedge \beta \equiv \beta \wedge \alpha$.(交换律)
(3) $(\alpha \vee \beta) \vee \gamma \equiv \alpha \vee (\beta \vee \gamma), (\alpha \wedge \beta) \wedge \gamma \equiv \alpha \wedge (\beta \wedge \gamma)$.(结合律)
(4) $\alpha \vee (\alpha \wedge \beta) \equiv \alpha, \alpha \wedge (\alpha \vee \beta) \equiv \alpha$. (吸收律)
(5) $\alpha \vee (\beta \wedge \gamma) \equiv (\alpha \vee \beta) \wedge (\alpha \vee \gamma), \alpha \wedge (\beta \vee \gamma) \equiv (\alpha \wedge \beta) \vee (\alpha \wedge \beta)$.
(6) $\neg(\alpha \vee \beta) \equiv \neg\alpha \wedge \neg\beta, \neg(\alpha \wedge \beta) \equiv \neg\alpha \vee \neg\beta$.(de Morgan 律) either or 的否定是 neither nor
(7) $\alpha \to \beta \equiv \neg\alpha \vee \beta$. (好用)
(8) $(\alpha \to \beta) \wedge (\alpha \to \gamma) \equiv \alpha \to (\beta \wedge \gamma)$, $(\alpha \to \gamma) \wedge (\beta \to \gamma) \equiv (\alpha \vee \beta) \to \gamma$,
$(\alpha \to \beta) \vee (\alpha \to \gamma) \equiv \alpha \to (\beta \vee \gamma)$, $(\alpha \to \gamma) \vee (\beta \to \gamma) \equiv (\alpha \wedge \beta) \to \gamma$.

例 1.3.2

证明 de Morgan 律.

证明: 只需要注意到:

$$\neg(\alpha \vee \beta) \text{ 真} \Leftrightarrow \alpha \vee \beta \text{ 假} \Leftrightarrow \alpha, \beta \text{ 都假} \Leftrightarrow \neg\alpha, \neg\beta \text{ 都真} \Leftrightarrow \neg\alpha \wedge \neg\beta \text{ 真}.$$
$$\neg(\alpha \wedge \beta) \text{ 假} \Leftrightarrow \alpha \wedge \beta \text{ 真} \Leftrightarrow \alpha, \beta \text{ 都真} \Leftrightarrow \neg\alpha, \neg\beta \text{ 都假} \Leftrightarrow \neg\alpha \vee \neg\beta \text{ 假}.$$

注: 第一行证明完以后, $\alpha \vee \beta \equiv \neg(\neg\alpha \wedge \neg\beta)$, 把 α 换为 $\neg\alpha$,β 换为 $\neg\beta$ 即可证出第二行.

例 1.3.3

证明 $(\alpha \to \gamma) \vee (\beta \to \gamma) \equiv (\alpha \wedge \beta) \to \gamma$.

证明:

$$\begin{aligned}
(\alpha \to \gamma) \vee (\beta \to \gamma) &\equiv (\neg\alpha \vee \gamma) \vee (\neg\beta \vee \gamma) && (\text{用 } 4(7)) \\
&\equiv (\neg\alpha \vee \neg\beta) \vee \gamma && (\text{结合律}) \\
&\equiv \neg(\alpha \wedge \beta) \vee \gamma && (\text{de Morgan}) \\
&\equiv (\alpha \wedge \beta) \to \gamma.\square && (\text{用 } 4(7))
\end{aligned}$$

□

例 1.3.4

证明 $\alpha \to (\beta \to \gamma) \equiv (\alpha \wedge \beta) \to \gamma$.

证明:

$$\begin{aligned}
\alpha \to (\beta \to \gamma) &\equiv \neg\alpha \vee (\neg\beta \vee \gamma) && (\text{用 } 4(7)) \\
&\equiv (\neg\alpha \vee \neg\beta) \vee \gamma && (\text{结合律}) \\
&\equiv \neg(\alpha \wedge \beta) \vee \gamma && (\text{de Morgan}) \\
&\equiv (\alpha \wedge \beta) \to \gamma. && (\text{用 } 4(7))
\end{aligned}$$

□

例 1.3.5

证明 Pierce 律, 即 $((\alpha \to \beta) \to \alpha) \to \alpha$ 永真.

证明: 方法一:

$$\begin{aligned}
((\alpha \to \beta) \to \alpha) \to \alpha &\equiv \neg(\neg(\alpha \to \beta) \vee \alpha) \vee \alpha && (\text{用 2 次 } 4(7)) \\
&\equiv ((\alpha \to \beta) \wedge (\neg\alpha)) \vee \alpha && (\text{de Morgan}) \\
&\equiv ((\neg\alpha \vee \beta) \wedge (\neg\alpha)) \vee \alpha && (\text{用 } 4(7)) \\
&\equiv \neg\alpha \vee \alpha \equiv 1. && (\text{排中律})
\end{aligned}$$

方法二: 反证, 若 $((\alpha \to \beta) \to \alpha) \to \alpha$ 假, 则 $(\alpha \to \beta) \to \alpha$ 真且 α 假, 则 $\alpha \to \beta$ 假且 α 假, 这是不可能发生的. □

注: 对于方法二, 回顾前面的那个真值表.

五个联结词本质上可只采用 $\neg$ 与 $\vee(\wedge, \to)$. 例如

$$\begin{aligned}
\alpha \wedge \beta &\equiv \neg(\neg\alpha \vee \neg\beta) \\
\alpha \vee \beta &\equiv \neg(\neg\alpha \wedge \neg\beta) \\
\alpha \to \beta &\equiv \neg\alpha \vee \beta \\
\alpha \leftrightarrow \beta &\equiv (\alpha \wedge \beta) \vee (\neg\alpha \wedge \neg\beta) \\
\alpha \vee \beta &\equiv \neg\alpha \to \beta.
\end{aligned}$$

练习题 2.

1. **(2022 年)** 判断题: 命题公式 $((p \vee q) \to r) \longleftrightarrow ((p \to r) \vee (q \to r))$ 永真. ( )
2. **(2014 年)** 不用真值表证明 $((\alpha \to \beta) \to \alpha) \to \alpha$ 永真, 其中 α 与 β 为命题公式.
3. 证明如下命题.

$$\begin{aligned}
\alpha &\equiv \neg\alpha \to \alpha \\
(\alpha \to \gamma) \wedge (\beta \to \gamma) &\equiv (\alpha \vee \beta) \to \gamma \\
\alpha \wedge (\beta \vee \gamma) &\equiv (\alpha \wedge \beta) \vee (\alpha \wedge \gamma) \\
\alpha \vee (\alpha \wedge \beta) &\equiv \alpha.
\end{aligned}$$

4. 证明 de Morgan 律的广义形式: (这里省略了括号是因为有交换律与结合律.)

$$\begin{aligned}
\neg(\alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \neg\alpha_n) &\equiv \neg\alpha_1 \vee \neg\alpha_2 \vee \cdots \vee \neg\alpha_n, \\
\neg(\alpha_1 \vee \alpha_2 \vee \cdots \vee \neg\alpha_n) &\equiv \neg\alpha_1 \wedge \neg\alpha_2 \wedge \cdots \wedge \neg\alpha_n.
\end{aligned}$$

§ 1.4 析取范式与合取范式

定义 1.4.1

命题变元或其否定叫**准变元**.

由有限个准变元作析取而得的析取式叫**析基 (或简单析取式)**,

由有限个准变元作合取而得的合取式叫**合基 (或简单合取式)**.

有限个合基的析取式叫**析取范式**. 有限个析基的合取式叫**合取范式**.

注: 按照合 (析) 取范式易知成假 (真) 赋值.

例 1.4.2

$(p \wedge \neg q) \vee (\neg p \wedge \neg q \wedge \neg s) \vee (\neg q \wedge \neg r)$ 是析取范式.

例 1.4.3

$(p \vee \neg q) \wedge (\neg p \vee \neg q \vee \neg s) \wedge (\neg q \vee \neg r)$ 是合取范式.

定理 1.4.4

对任一个命题公式 φ, 都可以找到一个等价于它的析取范式, 也可以找到它的合取范式.

证明: 步骤如下.

Step 1: 利用 $\alpha \leftrightarrow \beta \equiv (\alpha \to \beta) \wedge (\beta \to \alpha) \equiv (\alpha \wedge \beta) \vee (\neg\alpha \wedge \neg\beta)$ 以及 $\alpha \to \beta \equiv \neg\alpha \vee \beta$, 可以去掉 $\leftrightarrow$ 与 $\to$.

Step 2: 否定词往里走, 用 $\neg\neg\alpha \equiv \alpha$ 以及 de Morgan 律. 准否定词深入到命题变元里面.

Step 3: 用分配律求得所要的析取范式与合取范式. □

例 1.4.5

把公式 $\varphi = (p \to q) \leftrightarrow r$ 化成等价于它的析取范式与合取范式.

$$
\begin{aligned}
\varphi &\equiv ((p \to q) \wedge r) \vee (\neg(p \to q) \wedge \neg r) \\
&\equiv ((\neg p \vee q) \wedge r) \vee (\neg(\neg p \vee q) \wedge \neg r) \\
&\equiv (\neg p \wedge r) \vee (q \wedge r) \vee (p \wedge \neg q \wedge \neg r), \\
\varphi &\equiv ((p \to q) \to r) \vee (\neg(p \to q) \to \neg r) \\
&\equiv ((\neg(p \to q) \vee r) \wedge (\neg r \vee (p \to q))) \\
&\equiv (\neg(\neg p \vee q) \vee r) \wedge (\neg r \vee (\neg p \vee q)) \\
&\equiv ((p \wedge \neg q) \vee r) \wedge (\neg p \vee q \vee \neg r) \\
&\equiv (p \vee r) \wedge (\neg q \vee r) \wedge (\neg p \vee q \vee \neg r).
\end{aligned}
$$

定义 1.4.6: k 进制

对大于 1 的整数 g, 自然数 n 可唯一表示成 $\sum\limits_{i=0}^{k} a_i g^i$, 这儿 $a_i \in \{0, 1, \cdots, g-1\}$, 此时说 n 的 g 进制表示为 $a_k \cdots a_2 a_1 a_0$.

例 1.4.7

十进制 $101 = 1\times 10^2 + 0\times 10^1 + 1\times 10^0$, 二进制 $101 = 1\times 2^2 + 0\times 2^1 + 1\times 2^0 = 5_{10进制下}$.

定义 1.4.8

设 $p_1,\cdots,p_n$ 是 n 个不同的命题符号, p_i' 是 p_i 或 $\neg p_i$. 设 $\delta_i = \begin{cases}1, & p_i' 为 p_i\\ 0, & p_i' 为 \neg p_i\end{cases}$, 且 $\delta_i' = 1-\delta_i$.

$m = p_1'\wedge p_2'\wedge\cdots p_n'$ 是一个**极小项**, 它唯一的成真赋值是 $(p_1,\cdots,p_n) = (\delta_1,\cdots,\delta_n)$.

$M = p_1'\vee p_2'\vee\cdots\vee p_n'$ 是一个**极大项**, 它唯一的成假赋值是 $(p_1,\cdots,p_n) = (\delta_1',\cdots,\delta_n')$.

设二进制的 $\delta_1,\cdots,\delta_n$ 表示数 i, 则把上述极小项记为 m_i, 把上述极大项记为 $M_i(0\le i\le 2^n-1)$.

例 1.4.9

$m_4 = p\wedge\neg q\wedge\neg r$ 的成真赋值是 $(1,0,0)$, $M_4 = \neg p\vee q\vee r$ 的成假赋值是 $(1,0,0)$.

根据 de Morgan 律不难知道 $\neg m_i = M_i$. 即 m_i 的成真赋值对应于 M_i 的成假赋值.

定义 1.4.10

合基都为极小项的析取范式叫**主析取范式**, 析基都为极大项的合取范式叫**主合取范式**.

例 1.4.11

$(p\wedge\neg q)\vee(\neg q\wedge r)\vee(p\wedge r)$ 不是主析取范式. $(p\wedge\neg q\wedge r)\vee(\neg p\wedge q\wedge r)\vee(p\wedge q\wedge\neg r)$ 是主析取范式.

由主析取范式可知成真赋值, 由主合取范式可知成假赋值.

例 1.4.12

$(p\vee\neg q\vee r)\wedge(\neg p\vee q\vee r)\wedge(p\vee q\vee\neg r)$ 三个有一个为假即可.

注: 永真公式无主合取范式 (为 1); 永假公式无主析取范式 (为 0).

定理 1.4.13

对任一命题公式 φ, 有唯一的与之等价的主析取范式, 也有唯一与之等价的主合取范式. (有统一办法找到它们).

证明: (1) 先找 φ 的析 (合) 取范式, 再用 $\alpha\vee\alpha = \alpha\wedge\alpha = \alpha$, $\alpha\wedge\neg\alpha = 0, \alpha\vee\neg\alpha = 1$. 如果有项没出现, 用 $\alpha\vee\neg\alpha$ 与 $\alpha\wedge\neg\alpha$. 如

$$\alpha\wedge\beta = \alpha\wedge\beta\wedge(\gamma\vee\neg\gamma) = (\alpha\wedge\beta\wedge\gamma)\vee(\alpha\wedge\beta\wedge\neg\gamma),$$
$$\alpha\vee\beta = \alpha\vee\beta\vee(\gamma\wedge\neg\gamma) = (\alpha\vee\beta\vee\gamma)\wedge(\alpha\wedge\beta\wedge\neg\gamma).$$

从而把析取范式化成主析取范式, 把合取范式化成主合取范式.

(2) 如果有两个不同的主析取范式 φ_1,φ_2, 则 φ_1 的某个极小项在 φ_2 中没出现, 它对应的成真赋值使 φ_1 真但 φ_2 假. 矛盾. (合取同理) □

例 1.4.14

求公式 $\varphi = \neg(r\to p)\vee(q\wedge(p\vee r))$ 的主析取范式.

解:

$$\begin{aligned}\varphi &\equiv \neg(\neg r \vee p) \vee (q \wedge (p \vee r))\\ &\equiv (\neg p \wedge r) \vee (p \wedge q) \vee (q \wedge r)\\ &\equiv (\neg p \wedge r \wedge (\neg q \vee q)) \vee (p \wedge q \wedge (r \vee \neg r)) \vee ((p \vee \neg p) \wedge q \wedge r)\\ &\equiv \cdots (\text{分配律})\\ &\equiv (\neg p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge r) \vee (p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r).(\text{重复的干掉})\end{aligned}$$

或者写 $\varphi = m_1 \vee m_3 \vee m_6 \vee m_7$. 成真赋值是 $(p,q,r) = (0,1,1),(0,0,1),(1,1,1),(1,1,0)$.

例 1.4.15

把 $\varphi = (p \wedge (q \to r)) \to s$ 化为主合取范式, 求成假赋值.

解:

$$\begin{aligned}\varphi &\equiv \neg(p \wedge (\neg q \vee r)) \vee s\\ &\equiv \neg p \vee (q \wedge \neg r) \vee s \ (\text{析取, 不是我们要的})\\ &\equiv (\neg p \vee s) \vee (q \wedge \neg r) \ (\text{交换律})\\ &\equiv (\neg p \vee s \vee q) \wedge (\neg p \vee s \vee \neg r) \ (\text{分配律})\\ &\equiv (\neg p \vee q \vee s \vee (r \wedge \neg r)) \wedge (\neg p \vee \neg r \vee s \vee (q \wedge \neg q)) \equiv \cdots\\ &\equiv (\neg p \vee q \vee r \vee s) \wedge (\neg p \vee q \vee \neg r \vee s) \wedge (\neg p \vee \neg q \vee \neg r \vee s).\end{aligned}$$

或者写成 $\varphi = M_8 \wedge M_{10} \wedge M_{14}$, 成假赋值为 $(p,q,r,s) = (1,0,0,0),(1,0,1,0),(1,1,1,0)$.

例 1.4.16

某科研所要从 A,B,C 三名骨干中选取 1 至 2 人出国进修, 选派满足:

(1)A 去则 C 去;

(2)B 去则 C 不去;

(3)C 不去则 A 或 B 可去.

问: 如何选派?

解: 让 p,q,r 分别表示 A,B,C, 需要求公式

$$\begin{aligned}\varphi &= (p \to r) \wedge (q \to \neg r) \wedge (\neg r \to (p \vee q))\\ &\equiv (\neg p \vee r) \wedge (\neg q \vee \neg r) \wedge (r \vee p \vee q).\end{aligned}$$

把 $\vee$ 看成 $+$, $\wedge$ 看成 $\times$, $\bar{p}$ 看成 $\neg p$, 用分配律:

$$\begin{aligned}\varphi &= (\bar{p}+r)(\bar{q}+\bar{r})(p+q+r) = \cdots\\ &= \bar{p}\bar{q}r + \bar{p}q\bar{r} + p\bar{q}r + \bar{q}r\\ &= \bar{p}\bar{q}r + \bar{p}q\bar{r} + p\bar{q}r + \bar{q}r(p+\bar{p})\\ &= \cdots\\ &= \bar{p}\bar{q}r + \bar{p}q\bar{r} + p\bar{q}r\\ &= (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge r).\end{aligned}$$

成真赋值是 $(p,q,r) = (0,0,1),(0,1,0),(1,0,1)$. 可以选派 B 去, 或 C 去, 或 AC 都去.

练习题 3.

1. 求下列公式的主析取范式, 并求成真赋值.
   (1) $(\neg p \to q) \to (\neg q \vee p)$
   (2) $(\neg p \to q) \wedge (q \wedge r)$
   (3) $(p \vee (q \wedge r)) \to (p \vee q \vee r)$
   (4) **(2014 年)**$p \to ((p \to \neg q) \wedge \neg(\neg p \vee q))$
   (5) **(2022 年)**$p \to ((p \to q) \wedge \neg(\neg p \vee \neg q))$
2. 求下列公式的主合取范式, 并求成假赋值.
   (1) $\neg(q \to \neg p) \wedge \neg p$
   (2) $(p \wedge q) \vee (\neg p \vee r)$
   (3) $(p \to (p \vee q)) \vee r$
   (4) **(2014 年)**$\neg(p \vee q) \leftrightarrow (p \wedge q)$
3. 在某班班委成员选举中, 已知王小红、李强、丁金生三位同学被选进了班委会. 该班的甲, 乙, 丙三名学生预言:
   甲说：王小红为班长，李强为生活委员.
   乙说：丁金生为班长，王小红为生活委员.
   丙说：李强为班长，王小红为学习委员.
   班委会分工名单公布后发现, 甲、乙、丙三人都恰好猜对了一半. 问王小红、李强、丁金生各任何职 (用等值等演求解)?
4. **【选做】**8 年前 (2011), 孙智伟提出了如下的猜想 (收敛很快). 前 3 个问题每个悬赏 300 美元.
   (1) $\displaystyle\sum_{k=0}^{\infty} \frac{66k+17}{(2^{11}3^3)^k} T_k^3(10, 11^2) = \frac{540\sqrt{2}}{11\pi}$.
   (2) $\displaystyle\sum_{k=0}^{\infty} \frac{126k+31}{(-80)^{3k}} T_k^3(22, 11^2) = \frac{880\sqrt{5}}{21\pi}$.
   (3) $\displaystyle\sum_{k=0}^{\infty} \frac{3990k+1147}{(-288)^{3k}} T_k^3(62, 95^2) = \frac{432}{95\pi}(195\sqrt{14} + 94\sqrt{2})$.
   (4) $\displaystyle\sum_{k=0}^{\infty} \frac{24k+5}{28^{2k}} \binom{2k}{k} T_k^2(4, 9) = \frac{49}{9\pi}(\sqrt{3} + \sqrt{6})$.
   (5) $\displaystyle\sum_{k=0}^{\infty} \frac{2800512k+435257}{434^{2k}} \binom{2k}{k} T_k^2(73, 576) = \frac{10406669}{2\sqrt{6}\pi}$.
   其中, $T_k(b, c)$ 表示 $(x^2 + bx + c)^k$ 展开式中 x^k 项系数.

§ 1.5 公理系统与形式演绎

定义 1.5.1

给了公式集 Γ 及一些推理规则, 若用 Γ 中公式及特定的推理规则可得到 α, 则说从 Γ **可推出** α**. 记为** $\Gamma \vdash \alpha$. 这样公理系统中 Γ 的公式叫**公理 (axiom)**. 对 $\vdash$ 的语法赋上语义, 记为 $\models$, 当 $\Gamma \models \alpha$ 时称 α 为该系统的**定理 (theorem)**.

常用的推理规则为下述**分离规则**:

(1)$\alpha \to \beta$ 则 $\alpha \vdash \beta$.

(2)$\gamma \vdash \alpha \to \beta$ 且 $\gamma \vdash \alpha$, 则 $\gamma \vdash \beta$.

例 1.5.2

利用两个真值联结词 $\to, \vee$, 公理集 γ 由下面四条公理组成:

(a) $(\alpha \vee \alpha) \to \alpha$,

(b) $\alpha \to (\alpha \vee \beta)$,

(c) $(\alpha \vee \beta) \to (\beta \vee \alpha)$,

(d) $(\beta \to \gamma) \to ((\alpha \vee \beta) \to (\alpha \vee \gamma))$.

且推理规则只有分离规则. 证明 $\alpha \to \neg\neg\alpha, \neg\neg\alpha \to \alpha$.

证明: 由公理 (d) 有: (1)$(\beta \to \gamma) \to ((\neg\alpha \vee \beta) \to (\neg\alpha \vee \gamma))$,

即 (1')$(\beta \to \gamma) \to ((\alpha \to \beta) \to (\alpha \to \gamma))$.

由 (1') 得 (2)$((\alpha \vee \alpha) \to \alpha) \to \Big((\alpha \to (\alpha \vee \alpha)) \to (\alpha \to \alpha)\Big)$.

由分离规则分 (2) 为 (a)(3), 其中 (3)$(\alpha \to (\alpha \vee \alpha)) \to (\alpha \to \alpha)$.

由公理 (b) 再分离有 (4)$(\alpha \to \alpha)$, 即 $(\neg\alpha \vee \alpha)$.

由公理 (c) 得 (5)$(\neg\alpha \vee \alpha) \to (\alpha \vee \neg\alpha)$.

分离 (5)(4) 得 (6)$\alpha \vee \neg\alpha$.

由 (6) 得 (7)$\neg(\alpha \vee \neg\alpha) \equiv \alpha \to \neg\neg\alpha$.

由 (7) 得 (8)$\neg\alpha \to \neg\neg\neg\alpha$.

由公理 (d) 得 (9)$((\neg\alpha) \to (\neg\neg\neg\alpha)) \to ((\alpha \vee \neg\alpha) \to (\alpha \vee \neg\neg\neg\alpha))$.

分离 (9)(8) 得 (10)$(\alpha \vee (\neg\alpha)) \to (\alpha \vee \neg\neg\neg\alpha)$.

分离 (10)(6) 得 (11)$\alpha \vee \neg\neg\neg\alpha$,

由公理 (c) 得 (12)$(\alpha \vee \neg\neg\neg\alpha) \to (\neg\neg\neg\alpha \vee \alpha)$.

分离 (12)(11) 得 $\neg\neg\neg\alpha \vee \alpha$, 则 $\varphi : \neg\neg\alpha \to \alpha$. □

定理 1.5.3

上述永真公式公理系统是相容的, 该系统中定理还是可判定的 (有统一办法).

证明: (1) 该系统导出的都是永真公式, 易见公理 (a)-(d) 为永真公式, $\alpha \to \beta, \alpha \vdash \beta, \alpha \to \beta$ 与 α 均为永真公式时, 由分离规则可知 β 为永真公式. 而 α 永真时 $\neg\alpha$ 不永真, 故该系统不能既推出 α 又推出 $\neg\alpha$, 相容性成立.

(2) 对于命题演算公式 φ, 有个可行的办法把 φ 化成等价于它的主合取范式 ψ, 即 $\varphi \leftrightarrow \psi$. (把中间各种律用有限步可以证出来, 再证系统中两个命题等价) 是否为公理, 看有无成假赋值, 把 $\varphi \leftrightarrow \psi$ 化成主合取范式, 最终化为 1, 则它是定理 (φ 永真当且仅当 ψ 为 1, 有统一办法证). □

§ 1.6 一阶逻辑语言

定义 1.6.1

对于 n 元**函词符号** f, 当填入 n 个个体 $a_1,\cdots,a_n$ 后, 得到的 $f(a_1,\cdots,a_n)$ 是个**个体**. 对于 n 元**谓词符号** p, 当填入 n 个个体 $a_1,\cdots,a_n$ 后, 得到的 $p(a_1,\cdots,a_n)$ 是个**命题**.

例如：他打你的妹妹. a 表示他, b 表示你, $f(b)$: b 的妹妹. $p(x,y)$ 指 x 打 y. 则“他打你的妹妹”为 $p(a,f(b))$.

定义 1.6.2

设 p 为一元谓词, $p(a)$ 成立时, 称 a **具有性质** p. 设 R 为 n 元谓词, $R(a_1,\cdots,a_n)$ 成立时, 称个体 $a_1,\cdots,a_n$ **具有** n **元关系** R.

函词符号有三种方法: (1) 前置法: 如 $\sin\dfrac{\pi}{3},\ln x$. (2) 中置法: 如 $x+3,x\times y$. (3) 后置法: 如 $n!$.

采用中置法需要一些辅助括号, 如 $5\div((x+2)\times 3-y)$. 用前置与后置法可不加括号, 顺序不会乱. 比如逆波兰式 $\div 5-\times+x23y$.

下面引入“量词”(quantifier) 的概念.

定义 1.6.3: 存在量词 (existential quantifier)

$\exists x\ \varphi(x)$, 指有个个体 a 使 $\varphi(a)$ 成立. ($\varphi(a)$ 是个公式).

定义 1.6.4: 全称量词 (universal quantifier)

$\forall x\ \varphi(x)$ 指有对个体域中每个个体 a, $\varphi(a)$ 成立.

有下列关系:

$$\begin{aligned}
\neg\exists x\ \varphi(x) &\equiv \forall x\ \neg\varphi(x)\\
\forall x\ \varphi(x) &\equiv \neg\exists x\ \neg\varphi(x)\\
\neg\forall x\ \varphi(x) &\equiv \exists x\ \neg\varphi(x)\\
\exists x\ \varphi(x) &\equiv \neg\forall x\ \neg\varphi(x)
\end{aligned}$$

定义 1.6.5: 项

(1) 个体变元为项; (2) 个体常量为项; (3) f 为 n 元函词符号且 $t_1,\cdots,t_n$ 为项时, $f(t_1,\cdots,t_n)$ 为项. (4) 项仅由上法所得.

定义 1.6.6: 原子公式

(1) t_1,t_2 为项时 $t_1=t_2$ 为原子公式. (2) p 为 n 元谓词符号且 $t_1,\cdots,t_n$ 为项时, $p(t_1,\cdots,t_n)$ 为原子公式. (3) 原子公式仅由上法所得.

定义 1.6.7: 公式

(1) 原子公式是最简单的公式. (2) φ 是公式时, $\forall x\ \varphi(x)$ 与 $\exists x\ \varphi(x)$ 与 $\neg\varphi(x)$ 也是公式. (3) φ,ψ 为公式时, $\varphi\vee\psi,\psi\wedge\varphi,\varphi\to\psi$ 也是公式. (4) 公式仅由上法所得.

例如：$\forall x\exists y(x+y=3y-5)$ 为一个公式.

为方便起见, 约定：在一阶逻辑公式中, 否定词优先级高于量词, 量词的优先级高于 $\vee,\wedge,\to,\leftrightarrow$. 例如: $\neg\forall x\ \varphi(x)\to\underline{(\exists y\ \underline{\psi(y)\wedge\alpha(x,y)})}$.

例 1.6.8

几个例子：

(1) 存在唯一的 x 使 $\varphi(x)$ 成立, 即 $\exists! x\ \varphi(x)$, 相当于 $\exists x(\varphi(x) \wedge \forall y(\varphi(y) \rightarrow y = x))$.

(2)$\exists x \in X\ \varphi(x)$ 指 $\exists x(x \in X \wedge \varphi(x))$.

(3)$\forall x \in X\ \varphi(x)$ 指 $\forall x(x \in X \rightarrow \varphi(x))$.

(4)$\neg\forall x \in X\ \varphi(x)$ 指 $\neg\forall x(\neg(x \in X) \vee \varphi(x)) \equiv \exists x((x \in X) \wedge \neg\varphi(x)) \equiv \exists x \in X \neg\varphi(x)$. (用了 de Morgan 律)

例 1.6.9

更多例子：

(1)$\lim\limits_{x\to a} f(x) = A$ 相当于 $\forall\varepsilon > 0 \exists\delta > 0 \forall x(0 < |x-a| < \delta \rightarrow |f(x) - A| < \varepsilon)$.

(2) 函数 $f(x)$ 在区间 I 上一致连续指 $\forall\varepsilon > 0 \exists\delta > 0 \forall x \in I \forall y \in I(|x-y| < \delta \rightarrow |f(x) - f(y)| < \varepsilon)$.

(3) 函数 $f(x)$ 在区间 I 上不一致连续: (作否定)

$$\begin{aligned}
&\neg\forall\varepsilon > 0 \exists\delta > 0 \forall x \in I \forall y \in I(|x-y| < \delta \rightarrow |f(x) - f(y)| < \varepsilon) \\
\equiv&\exists\varepsilon > 0 \forall\delta > 0 \exists x \in I \exists y \in I \neg(\neg(|x-y| < \delta) \vee |f(x) - f(y)| < \varepsilon) \\
\equiv&\exists\varepsilon > 0 \forall\delta > 0 \exists x \in I \exists y \in I(|x-y| < \delta \wedge |f(x) - f(y)| \geq \varepsilon).
\end{aligned}$$

其中第 2 行的否定词不断后移, 并用了 $p \rightarrow q \equiv \neg p \vee q$, 第 3 行用了 de Morgan 律.

定义 1.6.10

设 ρ 为量词 ($\forall$或$\exists$), $\rho x\ \ \varphi(x)$ 时称变元 $\varphi(x), x$ 受量词 ρ 约束, 叫**约束变元**. 不受约束的叫**自由出现 (自由变元)**.

例 1.6.11

在 $\lim\limits_{x\to a} f(x) = A$ 中, $x, f(x)$ 都是约束出现, a, A 都是自由出现.

例 1.6.12

在 $\forall x(\varphi(x) \wedge x + y = 5) \vee x \neq 3 \vee \exists y(y^2 = y)$ 中, 前三个 x 是约束变元, 第一个 y 是自由变元, 最后的 x 是自由变元, 最后三个 y 是约束变元.

一个变元既有约束又有自由不好, 而约束变元可以改名, 或改成与已有自由变元不同名的新变元. (即: 不改变自由变元的名称, 且不把约束变元的名称改为已有的自由变元的名称)

上一例子可改为

$$\forall t(\varphi(t) \wedge t + y = 5) \vee x \neq 3 \vee \exists u(u^2 = u).$$

再比如, $\displaystyle\int_0^{x^2} f(x)\mathrm{d}x$ 可以改为 $\displaystyle\int_0^{x^2} f(t)\mathrm{d}t$.

注: 一阶逻辑中量词只作用于个体变元上 (而不是量词或谓词).

练习题 4.

1. **(2014 年)** 在一阶逻辑中证明 $\exists x(\alpha(x) \rightarrow \beta(x)) \equiv \forall x\alpha(x) \rightarrow \exists x\beta(x)$.
2. **(2023 年)** 使用一阶逻辑语言叙述：存在恰好两个不同的 x 使得 $\phi(x)$ 成立.

§ 1.7 谓词演算中公式的等价与 Skolem 前束范式

一些基本的等价式如下:

$$\neg\exists x\ \varphi(x) \equiv \forall x\ \neg\varphi(x).$$
$$\neg\forall x\ \varphi(x) \equiv \exists x\ \neg\varphi(x).$$
$$\forall x(\varphi(x) \wedge \psi(x)) \equiv \forall x\ \varphi(x) \wedge \forall x\ \psi(x).(\text{“任意”对应“且”})$$
$$\exists x(\varphi(x) \vee \psi(x)) \equiv \exists x\ \varphi(x) \vee \exists x\ \psi(x).(\text{“存在”对应“或”})$$

注意

$$\exists x(\varphi(x) \wedge \psi(x)) \rightarrow \exists x\ \varphi(x) \wedge \exists x\ \psi(x).(\leftarrow \text{不成立})$$
$$\forall x(\varphi(x) \vee \psi(x)) \leftarrow \forall x\ \varphi(x) \vee \forall x\ \psi(x).(\rightarrow \text{不成立})$$

例如: $\varphi(x) : x$ 为奇数; $\psi(x) : x$ 为偶数.

例 1.7.1

设 $X = \{x_1, \cdots, x_n\}$. 则 $\forall$ 可视为广义析取词, $\exists$ 可视为广义合取词, 即

$$\forall x \in X\ \varphi(x) \equiv \varphi(x_1) \wedge \varphi(x_2) \cdots \wedge \varphi(x_n).$$
$$\exists x \in X\ \varphi(x) \equiv \varphi(x_1) \vee \varphi(x_2) \cdots \vee \varphi(x_n).$$

例 1.7.2

证明 $\exists x(\varphi(x) \rightarrow \psi(x)) \equiv \forall x\ \varphi(x) \rightarrow \exists x\ \psi(x)$.

证明: 左边 $\equiv \exists x(\neg\varphi(x) \vee \psi(x)) \equiv \exists x\ \neg\varphi(x) \vee \exists x\ \psi(x) \equiv \neg\forall x\ \varphi(x) \vee \exists x\ \psi(x) \equiv$ 右边. □

设 x 不在 ψ 中自由出现, 则

$$\forall x(\varphi(x) \vee \psi) \equiv \forall x\ \varphi(x) \vee \psi,$$
$$\exists x(\varphi(x) \wedge \psi) \equiv \exists x\ \varphi(x) \wedge \psi.$$

例 1.7.3

设 x 不在 ψ 中自由出现. 证明 $\forall x(\varphi(x) \rightarrow \psi) \equiv \exists x\ \varphi(x) \rightarrow \psi$, $\forall x(\psi \rightarrow \varphi(x)) \equiv \psi \rightarrow \forall x\ \varphi(x)$.

证明: 注意

$$\forall x(\varphi(x) \rightarrow \psi) \equiv \forall x(\neg\varphi(x) \vee \psi) \equiv \forall x\ \neg\varphi(x) \vee \psi \equiv \neg\exists x\ \varphi(x) \vee \psi \equiv \exists x\ \varphi(x) \rightarrow \psi,$$
$$\forall x(\psi \rightarrow \varphi(x)) \equiv \forall x(\neg\psi \vee \varphi(x)) \equiv \neg\psi \vee \forall x\ \varphi(x) \equiv \psi \rightarrow \forall x\ \varphi(x).$$

Skolem 前束范式形如 $\rho_1 x_1 \rho_2 x_2 \cdots \rho_n x_n \varphi(x_1, \cdots, x_n)$. 这儿 ρ_i 为 $\forall$ 或 $\exists$, 且 $\varphi(x_1, \cdots, x_n)$ 不含量词.

定理 1.7.4

任何一个一阶公式可化为一个等价于它的 Skolem 前束范式.

证明: Step 1. $\alpha \rightarrow \beta \equiv \neg\alpha \vee \beta$, $\alpha \leftrightarrow \beta \equiv (\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha) \equiv (\alpha \wedge \beta) \vee (\neg\alpha \wedge \neg\beta)$.

Step 2. 将否定词深入到原子公式前, 用 $\neg\neg\alpha \equiv \alpha$, $\neg\forall x\ \varphi(x) \equiv \exists x\ \neg\varphi(x)$, $\neg\exists x\ \varphi(x) \equiv \forall x\ \neg\varphi(x)$.

Step 3. 把量词朝外放. $\forall x\ \varphi(x) \wedge \forall x\ \psi(x) \equiv \forall x(\varphi(x) \wedge \psi(x))$, $\exists x\ \varphi(x) \vee \exists x\ \psi(x) \equiv \exists x(\varphi(x) \vee \psi(x))$. 如果 x 不在 ψ 中自由出现, 则用 $\forall x(\varphi(x) \vee \psi) \equiv \forall x\ \varphi(x) \vee \psi$, $\exists x(\varphi(x) \wedge \psi) \equiv \exists x\ \varphi(x) \wedge \psi$. □

例 1.7.5

把 $\forall x\ \varphi(x) \vee \neg\exists x\ \psi(x)$ 化为 Skolem 前束范式.

解:

$$\begin{aligned}
\forall x\ \varphi(x) \vee \neg\exists x\ \psi(x) &\equiv \forall x\ \varphi(x) \vee \forall x\ \neg\psi(x) && \text{(否定词放前面)}\\
&\equiv \forall x\ \varphi(x) \vee \forall y\ \neg\psi(y) && \text{(变为与 } x \text{ 无关)}\\
&\equiv \forall x(\varphi(x) \vee \forall y\ \neg\psi(y)) && (x \text{ 不在后面公式自由出现})\\
&\equiv \forall x\forall y(\varphi(x) \vee \neg\psi(y)).
\end{aligned}$$

例 1.7.6

求 $\forall x\ \varphi(x,y) \to \exists y\ \psi(x,y)$ 的 Skolem 前束范式.

解:

$$\begin{aligned}
\forall x\ \varphi(x,y) \to \exists y\ \psi(x,y) &\equiv \forall u\ \varphi(u,y) \to \exists v\ \psi(x,v) && \text{(改名, 防混)}\\
&\equiv \neg\forall u\ \varphi(u,y) \vee \exists v\ \psi(x,v)\\
&\equiv \exists u\neg\varphi(u,y) \vee \exists v\ \psi(x,v)\\
&\equiv \exists u(\neg\varphi(u,y) \vee \psi(x,u)) && \text{(可以把 v 换成 u)}
\end{aligned}$$

事实上可以写为 $\exists u\exists v(\neg\varphi(u,y) \vee \psi(x,v))$, 但字母能少用就少用.

练习题 5.

1. 将 $\exists x\ \varphi(x) \to \forall x\ \psi(x)$ 化为 Skolem 前束范式.
2. 将 $\exists x(\neg\exists y\ P(x,y)) \to (\exists z\ Q(z) \to R(x))$ 化为 Skolem 前束范式. (P,Q,R 为谓词).
3. **(2014 年)** 将 $\exists x\alpha(x) \to (\forall x\beta(x) \to \neg\gamma(x))$ 化为等价于它的前束范式.

§ 1.8 语义与模型

注: 有自由变元的不好谈真假, 例如 $x+3=5$.

定义 1.8.1: 模型

无自由变元的一阶公式叫**闭公式或断定**. 取定非空集 D 作为个体域. **"解释" I** 把 φ 中常量符号 C 解释为 D 中具体个体 (记为 $C^{\mathcal{U}}$). 把 φ 中 n 元函词符号 f 解释成 $D\times\cdots\times D$(笛卡尔积) 到 D 中函数, 把 φ 中 n 元谓词符号 P 解释成 D 中一个具体的 n 元谓词 ($P^{\mathcal{U}}$). 把 φ 解释成 $\varphi^{\mathcal{U}}$ 后, $\forall x\ \varphi(x)$ 指对每一个 $a\in D$ 有 $\varphi^{\mathcal{U}}(a)$. $\exists x\ \varphi(x)$ 指有一个个体 $a\in D$ 使 $\varphi^{\mathcal{U}}(a)$. $\neg\varphi$ 指 $\varphi^{\mathcal{U}}$ 不成立. ……如上解释后 φ 成真时, $\mathcal{U}=(D,I)$ 称为 φ 的一个**模型** (记为 $\mathcal{U}\vDash\varphi$). 如果 $\mathcal{U}=(D,I)$ 是闭公式集 Σ 中每个 σ 的模型, 则称 $\mathcal{U}$ 为 Σ 的一个**模型 (model)**.

例 1.8.2

在群中, 群的公理 Σ 为: ($\circ$ 为二元函词符号)

$$\forall x\forall y\forall z((x\circ y)\circ z=x\circ(y\circ z)).\qquad\text{(结合律)}$$
$$\forall x(e\circ x=x).\qquad\text{(左单位元)}$$
$$\forall x\exists y(y\circ x=e).\qquad\text{(左逆元)}$$

其中 e 为常量符号.

定义 1.8.3

对于一阶闭公式 φ, 如果任何 $\mathcal{U}=(D,I)$ 为它的模型, 则称 φ **永真**.

例 1.8.4

$\exists x(x=x)$ 永真; $\exists x\exists y(x\neq y)$ 不永真 (当只有一个个体的时候不对); $\exists x\exists y\ \varphi(x,y)\leftrightarrow\exists y\exists x\ \varphi(x,y)$ 永真; $\forall x\exists y\ \varphi(x,y)\leftrightarrow\exists y\forall x\ \varphi(x,y)$ 不永真, 一般不可调序.

模型实际上就是提供例子.

例 1.8.5

在群中, 取 $D=\mathbb{R}\backslash\{0\}$, 赋予下列解释 I: ①把 e 解释为 1; ②把 $\circ$ 解释为实数乘法. 如此 $\mathcal{U}=(D,I)$ 为 Σ 的一个模型.

例 1.8.6

在群中, 取 $D=\mathbb{Z}$, 赋予下列解释 I: ①把 e 解释为整数中零; ②把 $\circ$ 解释为整数加法. 如此 $\mathcal{U}=(D,I)$ 为 Σ 的一个模型.

可选几个一阶公式作为公理, 采用分离规则, 如此公理系统相容, 推出的都永真. ("永真" 的判定要看语义, 与定理 (语法) 不同, 语义和语法要吻合)

Gödel 证明了这样的系统完备, 但不可判定 (无统一的办法证明定理).

§ 1.9 (*) 可计算性理论

1.9.1 可计算函数

定义 1.9.1: 寄存器机

一个**寄存器机 (register machine)** 由如下部分组成:

(1) 一些**寄存器 (register)** $R_1, R_2, \cdots$，每个寄存器都指定一个非负整数.

(2) 一个**程序 (program)**，由有限个**状态 (state)** $S_0, S_1, \cdots, S_n$ 组成，其中

①每个状态 $S_1, \cdots, S_n$ 都与一个指令关联.

② S_1 表示初始状态，程序首先执行 S_1 上的指令.

③ S_0 表示终止状态，到达 S_0 时，程序终止.

(3) 在 S_i 上的**指令 (instruction)**，$1 \leq i \leq n$，是下面两种形式之一:

①对寄存器 R_j 进行加 1，然后移到状态 S_k.

$$S_i \xrightarrow{R_j+1} S_k$$

②如果 $R_j > 0$，对寄存器 R_j 进行减 1，然后移到状态 S_k；否则（如果 $R_j = 0$），移到状态 S_l.

$$\begin{tikzcd} S_i \arrow[r, "R_j-1"] \arrow[dr, dotted] & S_k \\ & S_l \end{tikzcd}$$

下面是寄存器机的一些例子.

例 1.9.2

下面的寄存器机实现了对寄存器 R_1 进行加 1.

$$S_1 \xrightarrow{R_1+1} S_0 \tag{1.1}$$

例 1.9.3

下面的寄存器机实现了对寄存器 R_5 进行加 3.

$$S_1 \xrightarrow{R_5+1} S_2 \xrightarrow{R_5+1} S_3 \xrightarrow{R_5+1} S_0$$

例 1.9.4

下面的寄存器机实现了将寄存器 R_1 赋值为 0.

$$\begin{tikzcd} S_1 \arrow[loop left, "R_1-1"] \arrow[dr, dotted] & \\ & S_0 \end{tikzcd} \tag{1.2}$$

实现方法是对 R_1 重复减 1 直到取 0.

设 $\mathbb{N}_0 = \{0, 1, 2, \cdots\}$ 为非负整数的全体.

定义 1.9.5: 可计算函数

函数 $f:\mathbb{N}_0^k\to\mathbb{N}_0$ 称为**可计算函数 (computable function)**，若存在一个寄存器机，在初始状态下寄存器 $R_1,\cdots,R_k$ 赋值为 $n_1,\cdots,n_k$，其它寄存器赋值为 0，在终止状态 S_0 下寄存器 R_1 赋值为 $f(n_1,\cdots,n_k)$.

注意，可计算函数的输出是寄存器 R_1 的值.

寄存器机有可能不终止，比如下面的寄存器机的初始值 R_1 非零，就会在 S_1 和 S_2 循环；而如果初始值 R_1 为零，那么寄存器机马上终止.

$$\begin{tikzcd} S_1 \arrow[r, bend left, "R_1-1"] \arrow[dr, dotted] & S_2 \arrow[l, bend left, "R_1+1"] \\ & S_0 \end{tikzcd} \tag{1.3}$$

这样子，对于某些“输入值”，我们就说它的函数值未定义. 比如上面的寄存器机是一个映射 $f:\mathbb{N}_0\to\mathbb{N}_0$，将 0 映为 0，但是对正整数未定义.

定义 1.9.6: 偏函数

称 $f:\mathbb{N}_0^k\to\mathbb{N}_0$ 为**偏函数 (partial function)**，若将 f 限制在 $A\subset\mathbb{N}_0^k$ 后，$f|_A:A\to\mathbb{N}_0$ 是一个函数.

例如：

1. 映射 $f:\mathbb{N}_0\to\mathbb{N}_0$，$f(n)=\frac{n}{2}$ 是偏函数，它只对偶数有定义，此时 $A=\{0,2,4,6,8,\cdots\}$.
2. 映射 $f:\mathbb{N}_0\to\mathbb{N}_0$，$f(n)=\sqrt{n}$ 是偏函数，它只对平方数有定义，此时 $A=\{0,1,4,9,16,\cdots\}$.

我们也可以对偏函数定义可计算的概念.

定义 1.9.7: 可计算偏函数

偏函数 $f:\mathbb{N}_0^k\to\mathbb{N}_0$ 称为**可计算偏函数 (computable partial function)**，若存在一个寄存器机，在初始状态下寄存器 $R_1,\cdots,R_k$ 赋值为 $n_1,\cdots,n_k$，其它寄存器赋值为 0，且如果 $f(n_1,\cdots,n_k)$ 有定义，则在终止状态 S_0 下寄存器 R_1 赋值为 $f(n_1,\cdots,n_k)$；如果 $f(n_1,\cdots,n_k)$ 没有定义，则寄存器机不终止.

例如，设偏函数 $f:\mathbb{N}_0\to\mathbb{N}_0$ 满足 $f(0)=0$，而当 m 为正整数时 $f(m)$ 未定义. 根据 (1.3) 所给的寄存器机，f 是可计算偏函数.

下面是一些可计算函数的例子.

例 1.9.8: 清零函数, clearing function

$f:\mathbb{N}_0^k\to\mathbb{N}_0$，$f(n_1,\cdots,n_k)=0$ 是可计算函数，因为 (1.2) 给出了寄存器机的定义方式.

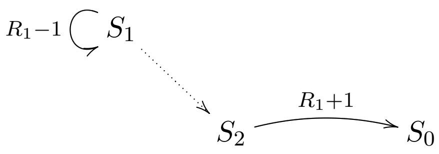
例 1.9.9: 后继函数, successor function

$f:\mathbb{N}_0\to\mathbb{N}_0$，$f(n)=n+1$ 是可计算函数. 因为 (1.1) 给出了寄存器机的定义方式.

例 1.9.10

$f:\mathbb{N}_0\to\mathbb{N}_0$，$f(n)=1$ 是可计算函数.

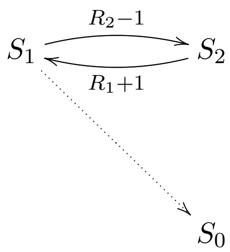
这是因为，寄存器机可定义如下：



例 1.9.11: 加法函数, addition function

$f:\mathbb{N}_0^2\to\mathbb{N}_0$，$f(m,n)=m+n$ 是可计算函数.

这是因为，寄存器机可定义如下：



它循环地将寄存器 R_2 减 1，将寄存器 R_1 加 1，当 $R_2=0$ 时终止，最终输出 R_1 的值为 $m+n$.

例 1.9.12: 投影函数, projection function

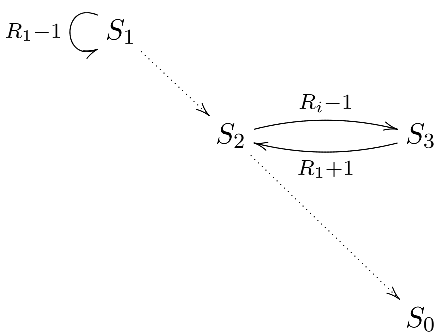
$f:\mathbb{N}_0^k\to\mathbb{N}_0$，$f(n_1,\cdots,n_k)=n_i$，其中 $1\le i\le k$，是可计算函数.

我们分情况讨论. 注意当程序终止时，寄存器 R_1 的值为输出值，故需要分 $i=1$ 与 $i\ne1$ 讨论.

(1) 若 $i=1$，则 R_1 就是最终的结果. 所以，我们只需对任意一个除了 R_1 之外的其它寄存器进行变动，比如：

$$S_1 \xrightarrow{R_2+1} S_0$$

(2) 若 $i\ne1$，首先需要将 R_1 清空为 0，然后将 R_i 的值赋值到 R_1. 我们可以将例 1.9.8 和例 1.9.11 结合在一起. 寄存器机可定义如下：



所以 f 是可计算函数. □

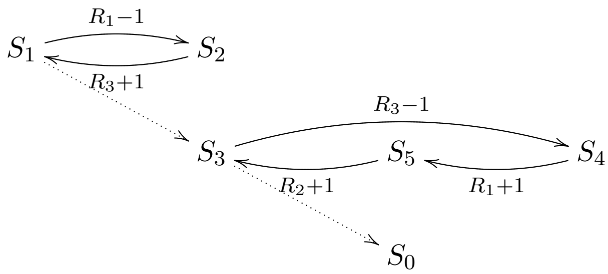
我们可以用上面的可计算函数构造出许多其它的可计算函数.

例 1.9.13

将寄存器 R_1 的值复制到 R_2.

进行复制操作需要引入额外的一个寄存器 R_3. 首先要将 R_1 的值“移动”到 R_3，然后再将 R_3

的值“移动”到 R_1 和 R_2.



类似地，通过函数的复合，可以构造很多可计算函数．比如，例 1.9.10 中的函数 $f:\mathbb{N}_0\to\mathbb{N}_0$，$f(n)=1$，实际上是由两个可计算函数复合而成：$g:\mathbb{N}_0\to\mathbb{N}_0$，$g(n)=0$ 和 $h:\mathbb{N}_0\to\mathbb{N}_0$，$h(n)=n+1$，于是 $f=h\circ g$.

定理 1.9.14

可计算偏函数的复合是可计算偏函数.

下面用加法来定义乘法．对于函数 $h:\mathbb{N}_0^2\to\mathbb{N}_0$，$h(m,n)=mn$，我们可以用加法来进行递归定义．首先对任意 $m\in\mathbb{M}_0$，$h(m,0)=0$．为了“达到”$h(m,n)=mn$，需要对寄存器 R_1（初始值为 m）进行重复加 n 次的操作，所以函数 h 可以递归定义 (recursively define) 如下：

$$h(m,0)=0,\qquad h(m,k+1)=h(m,k)+m,\qquad k\in\mathbb{N}_0.$$

接下来，也可以定义阶乘函数 $h:\mathbb{N}_0\to\mathbb{N}_0$，$h(n)=n!$．递归地使用前面所定义的乘法，如下：

$$h(0)=1,\qquad h(k+1)=(k+1)h(k).$$

一般地，这种形式的递归叫做**原始递归 (primitive recursion)**.

定理 1.9.15

对可计算偏函数进行原始递归，得到的函数也是可计算偏函数.

下面考虑函数的“极小化”(minimalisation)，它是将 f 的输入值中的最小值映射为 0 的操作．函数 g 的“极小化”是 $f:\mathbb{N}_0\to\mathbb{N}_0$，定义为：如果存在 n 使得 $g(m,n)=0$，并且对任意 $k<n$，$g(m,k)$ 有定义且 $g(m,k)>0$，则定义 $f(m)=n$；否则，如果这样的 n 不存在，则 $f(m)$ 未定义.

例 1.9.16

考虑加法函数 $g:\mathbb{N}_0^2\to\mathbb{N}_0$，$g(m,n)=m+n$，在其上定义极小化函数.

如果 $m=0$，我们需要寻找 n 使得 $g(0,n)=0$．即 $0+n=0$，得 $n=0$．而“对任意 $k<n$，$g(m,k)$ 有定义且 $g(m,k)>0$”是自动成立的．所以 $f(0)=0$.

如果 $m>0$，我们需要寻找 n 使得 $g(m,n)=0$，即 $m+n=0$．但是，这样的 n 并不存在，所以 $f(m)$ 未定义.

于是，g 的极小化函数是一个偏函数 $f:\mathbb{N}_0\to\mathbb{N}_0$，$f(0)=0$，且当 $m>0$ 时，$f(m)$ 未定义．前面已经验证了，f 是可计算偏函数.

一般地，有如下定理.

定理 1.9.17

一个可计算偏函数的极小化是一个可计算偏函数.

1.9.2 递归函数

定义 1.9.18

递归函数 (primitive recursive function，原始递归函数) 构成的集合 I 由如下函数构成：

(1) 零函数 $f:\mathbb{N}_0^k\to\mathbb{N}_0$，$f(n_1,\cdots,n_k)=0$ 属于 I；

(2) 后继函数 $f:\mathbb{N}_0\to\mathbb{N}_0$，$f(n)=n+1$ 属于 I；

(3) 投影函数 $f:\mathbb{N}_0^k\to\mathbb{N}_0$，$f(n_1,\cdots,n_k)=n_i$，其中 $1\le i\le k$，属于 I；

(4) I 中两个函数的复合属于 I；

(5) 对 I 中的函数使用原始递归，得到的函数属于 I，即：如果有 I 中的两个函数 $f:\mathbb{N}_0^{k+1}\to\mathbb{N}_0$ 和 $g:\mathbb{N}_0^{k-1}\to\mathbb{N}_0$，函数 $h:\mathbb{N}_0^k\to\mathbb{N}$ 定义为

$$
\begin{aligned}
h(0,n_2,\cdots,n_k)&=g(n_2,\cdots,n_k),\\
h(n+1,n_2,\cdots,n_k)&=f(n,h(n,n_2,\cdots,n_k),n_2,\cdots,n_k)
\end{aligned}
$$

则 $h\in I$.

在递归函数的基础上，如果还满足下面的条件，则称为递归偏函数 (recursive partial function，或叫部分递归函数).

(6) 对 I 中的函数使用极小化，得到的函数属于 I.

递归函数的例子：

1. 常值函数 $f_1:\mathbb{N}_0^k\to\mathbb{N}_0$，$f_1(n_1,\cdots,n_k)=n$.
2. 加法函数 $f_2:\mathbb{N}_0^2\to\mathbb{N}_0$，$f_2(m,n)=m+n$. 它可以用投影函数和后继函数如下递归定义：
   ① $f_2(m,0)=m$，可以用投影函数得到.
   ② $f_2(m,k+1)=f_2(m,k)+1$，可以用后继函数得到.
3. 乘法函数 $f_3:\mathbb{N}_0^2\to\mathbb{N}_0$，$f_3(m,n)=mn$. 它可以如下递归定义：
   ① $f_3(m,0)=0$，可以用零函数或投影函数得到.
   ② $f_3(m,k+1)=f_3(m,k)+m$. 这里加法可以用 f_2 来得到，即 $f_3(m,k+1)=f_2(f_3(m,k),m)$.
4. 乘方函数 $f_4:\mathbb{N}_0^2\to\mathbb{N}_0$，$f_4(m,n)=m^n$. 它可以如下递归定义：
   ① $f_4(m,0)=1$，可以用后继函数与投影函数的复合得到；
   ② $f_4(m,k+1)=mf_4(m,k)$. 这里乘法可以用 f_3 来得到，即 $f_4(m,k+1)=f_3(m,f_4(m,k))$.
5. 示性函数 $f_5:\mathbb{N}_0\to\mathbb{N}_0$，$f_5(n)=\begin{cases}0, & n=0,\\ 1, & n\ne 0.\end{cases}$ 可以如下递归定义：
   ① $f_5(0)=0$，用零函数或投影函数得到.
   ② $f_5(k+1)=1$，用零函数与后继函数的复合得到.
6. $f_6:\mathbb{N}_0\to\mathbb{N}_0$，$f_6(n)=\begin{cases}0, & n=0,\\ n-1, & n\ne 0.\end{cases}$ 可以如下递归定义：
   ① $f_6(0)=0$，用零函数或投影函数得到.
   ② $f_6(k+1)=f_6(k)+f_5(k)$，用加法函数 f_2 得到. 即 $f_6(k+1)=f_2(f_6(k),f_5(k))$.
7. 减法函数 $f_7:\mathbb{N}_0^2\to\mathbb{N}_0$，$f_7(m,n)=\begin{cases}m-n, & m\ge n,\\ 0, & m<n.\end{cases}$ 可以如下递归定义：
   ① $f_7(m,0)=m$. 用投影函数得到.
   ② $f_7(m,k+1)=f_6(f_7(m,k))$.

定理 1.9.19

$f:\mathbb{N}_0^k\to\mathbb{N}_0$ 是递归偏函数当且仅当它是可计算偏函数.

1.9.3 编码

因为可计算函数可以写成程序的形式，而每个程序都可以用自然数来表示，故可计算函数的全体是可数的．根据定理 1.9.19，全体递归偏函数是可数的．将自然数 n 对应的程序定义为 f_n，于是得到一个排列：

$$f_1, f_2, \cdots.$$

注意，有可能两个不同的函数对应了同一个递归偏函数，所以存在 $i, j \in \mathbb{N}_0$，$i \neq j$ 使得 $f_i = f_j$.

定理 1.9.20

函数 $g : \mathbb{N}_0 \to \mathbb{N}_0$，$g(n) = \begin{cases} f_n(n) + 1, & f_n(n)\text{有定义}, \\ 0, & f_n(n)\text{无定义}, \end{cases}$ 不是递归函数.

证明: 用反证法．若 g 是递归函数，则它是 $f_1, f_2, \cdots$ 中的其中一个，记 $g = f_k$，$k \in \mathbb{N}$．根据 g 处处由定义可知 f_k 处处有定义.

但是，根据 g 的定义，$g(k) = f_k(k) + 1$，所以 $g(k) \neq f_k(k)$，所以 g 和 f_k 在点 k 处不相同，故不可能有 $g = f_k$，导出矛盾．因此，g 不是递归函数. □

练习题 6.

1. 用画图的方式说明下面的函数是可计算函数.
   (1) $f_1 : \mathbb{N}_0 \to \mathbb{N}_0$, $f_1(m) = 3$;
   (2) $f_2 : \mathbb{N}_0 \to \mathbb{N}_0$, $f_2(m) = m + 3$;
   (3) $f_3 : \mathbb{N}_0^2 \to \mathbb{N}_0$, $f_3(m, n) = m + n + 3$;
   (4) $f_4 : \mathbb{N}_0 \to \mathbb{N}_0$, $f_4(m) = 5m$;
   (5) $f_5 : \mathbb{N}_0 \to \mathbb{N}_0$, $f_5(m) = 5m + 3$;
   (6) $f_6 : \mathbb{N}_0^2 \to \mathbb{N}_0$, $f_6(m, n) = m + 5n$;
   (7) $f_7 : \mathbb{N}_0^2 \to \mathbb{N}_0$, $f_7(m, n) = 2m + 5n$.
2. 证明下面的函数是递归函数.
   (1) $g_1 : \mathbb{N}_0 \to \mathbb{N}_0$, $g_1(m) = 3$;
   (2) $g_2 : \mathbb{N}_0 \to \mathbb{N}_0$, $g_2(m) = m + 3$;
   (3) $g_3 : \mathbb{N}_0^2 \to \mathbb{N}_0$, $g_3(m, n) = m + n + 3$;
   (4) $g_4 : \mathbb{N}_0^2 \to \mathbb{N}_0$, $g_4(m, n) = m + 3n$;
   (5) $g_5 : \mathbb{N}_0^2 \to \mathbb{N}_0$, $g_5(m, n) = mn + m$;
   (6) $g_6 : \mathbb{N}_0^2 \to \mathbb{N}_0$, $g_6(m, n) = mn + 3$;
   (7) $g_7 : \mathbb{N}_0^2 \to \mathbb{N}_0$, $g_7(m, n) = 9mn$;
   (8) $g_8 : \mathbb{N}_0 \to \mathbb{N}_0$, $g_8(m) = 9m^2 + 2$.

第 2 章　图论初步

§ 2.1　图论的起源与基本概念

图论 (graph theory) 属于组合数学, 目前 (2019) 南大做图论的有陈耀俊、周国飞 (张高飞的学生)、张运清 (陈的老婆) 他们都比孙智伟小, 许多人都在做图论. 最好的杂志为 J. Combine Theory Ser. A(组合), J. Combine Theory Ser. B(图论).

定义 2.1.1

设 V 是个有限非空集, 集合 E 与 V 不相交, 且有一个关联函数 $\psi : E \to \{\{x, y\} : x, y \in V\}$(无序对) 或 $\{\langle x, y\rangle : x, y \in V\}$(有序对). 则称 $G = \langle V, E\rangle$ 是个**图 (graph)**, 把 V 中元素叫**顶点 (vertex)**, E 中元素叫**边 (edge)**. 如果 $e \in E$ 且 $\psi(e) = \{x, y\}$ 或 $\langle x, y\rangle$, 则说 x, y 是 e 的**端点**, e 关联顶点 x, y(或说边 e 连接顶点 x, y).

通常把 V 中元用平面上的点表示, 边 e 连接点 x, y 时, 用一条 x 到 y 的连线表示这样的边, $\psi(e)$ 为有序对 $\langle x, y\rangle$ 时, 用从 x 指向 y 的连线表示这样的边 e(叫**有向边/弧**).

注: 边的曲直与长度不重要, 重要的是关系.

定义 2.1.2

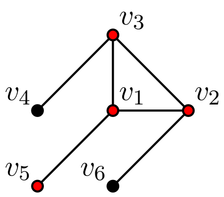
没有方向的边叫**无向边**, 各边都是无向边的图叫**无向图 (undirected graph)**, 各边均为有向边的图叫**有向图 (directed graph)**. 图 G 中, 两个端点重合的边叫**环**. 连接两点 x, y 的边不止一条时, 称它们为**平行边或多重边**. 有平行边的图叫**多重图**, 既无环又无平行边的无向图叫**简单图 (simple graph)**. 图 G 中有边 e 连接顶点 x, y 时, 称 x, y **相邻 (adjacent)**, 无向图中有公共顶点的两条边叫**相邻的边**, 有向图中边 e_1 的终点与边 e_2 的起点相同时称 e_1, e_2 **相邻 (adjacent)**.

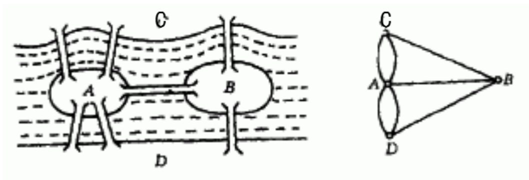
注: 这里的“环”与抽象代数是两码事.

定义 2.1.3

对于图 G, 用 $V(G)$ 表示 G 的顶点集, 用 $E(G)$ 表示 G 的边集. 把 $v \in V(G)$ 的**邻域**定义为 $N_G(v) = \{u \in V(G) \setminus \{v\} : u$ 与 v 相邻$\}$. 把 $N_G(v) \cup \{v\}$ 叫 v 的**闭邻域**.

下图中, $N_G(v_1) = \{v_2, v_3, v_5\}$.





Euler 考虑哥尼斯堡 (Königsberg) 七桥问题: 能否从图中某一地出发, 经过每座桥各一次又回到原来的陆地如果把每块陆地用平面上的点表示, 边代表桥, 则它无解.

四色猜想: (de Morgan 的学生 Francis Guthrie 在 1852/10/23 提出) 在一张平面地图上, 不论有多少个国家, 也不论它们如何分布, 只用四种颜色画图, 就可使不同相邻国家颜色不同. de Morgan 不会做, 给了 Hamilton, 但他对这个问题不感兴趣. 问 Cayley(1878) 也没做出来, (还写了篇文章说难在哪里). Einstein 的老师 Minkowski 说不难, 是因为没一流的数学家研究, 后来他也没做出来. 1879 年 Kempe 宣布做了出来, 发表文章在 Amer. I. Math 得到很多荣誉 (包括英国皇家), 但 1890 年 P. J. Heawood 发现了漏洞（只能证 5 种颜色的情况）. 1976 年 Appel 与 Haken 用计算机证明四色猜想 (用了穷举方法, 运行几个月), 到目前无人工可解决的证明.

定义 2.1.4

设 $G_1,\cdots,G_n$ 为图, 顶点集 $V(G_1),\cdots,V(G_n)$ 两两不交. 则称

$$G=\langle\bigcup_{i=1}^{n}V(G_i),\bigcup_{i=1}^{n}E(G_i)\rangle$$

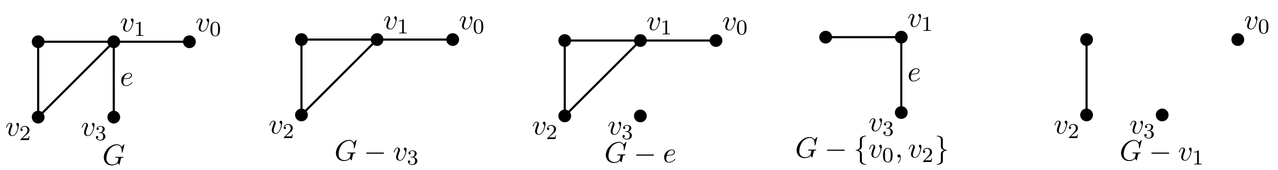
为 $G_1,\cdots,G_n$ 的**并**.

定义 2.1.5

设 G 为图. $V_0\subseteq V(G), E_0\subseteq E(G)$. 从 G 中删去属于 V_0 的顶点及其关联的边后所得的图记为 $G-V_0$. 当 $V_0=\{v_0\}$ 时也写 $G-v_0$. 从 G 中删去属于 E_0 的边所得的图为 $G-E_0$, 当 $E_0=\{e\}$ 时也写 $G-e_0$. 如果在 G 上添加上两个端点属于 $V(G)$ 的新边 $e_1,\cdots,e_n$ 后所得的图记为 $G+e_1+\cdots+e_n$.

例 2.1.6

如下图.

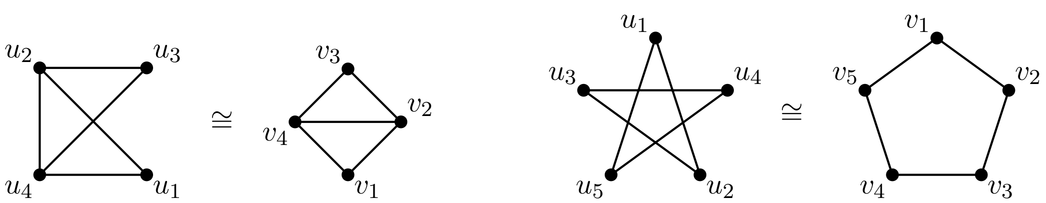


定义 2.1.7

设 G 与 H 是两个图, 如果存在 $V(G)$ 与 $V(H)$ 的一一对应 f 以及 $E(G)$ 到 $E(H)$ 的一一对应 g, 使得 G 中边 e 连接顶点 $u,v\Leftrightarrow H$ 中 $g(e)$ 连接 $f(u),f(v)$, 则称 G 与 H **同构**, 记为 $G\cong H$(G is isomorphic to H).

例 2.1.8

两个同构的例子, 其中 u_i 与 v_i 一一对应.



Ulam 同构猜想: 假设 G 与 H 都是具有 $p\geq 3$ 个顶点的无向图, $V(G)=\{u_1,\cdots,u_p\}$, $V(H)=\{v_1,\cdots,v_p\}$. 如果对 $i=1,\cdots,p$ 都有 $G-u_i\cong H-v_i$, 则 $G\cong H$. (现在 (2019 年) 还没解决)

§ 2.2 子图、补图、完全图与二部图

定义 2.2.1: 子图

设 G, H 为图, 如果 $V(H) \subseteq V(G), E(H) \subseteq E(G)$, 则称 H 是 G 的**子图**. 如果 $V(H) = V(G), E(H) \subseteq E(G)$, 则称 H 是 G 的**生成子图 (支撑子图)**.

注: $V_0 \subseteq V(G)$ 时, $G - V_0$ 是 G 的子图; $E_0 \subseteq E(G)$ 时, $G - E_0$ 是 G 的生成子图.

定义 2.2.2: 导出子图

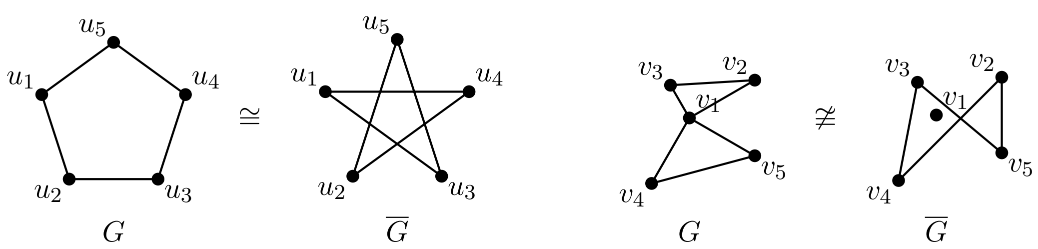
设 G 为图, $V_0 \subseteq V(G)$, 以 V_0 为顶点集, 以端点全为 V_0 中的边的全体为边的集合的图叫 V_0 在 G 中的**导出子图** ($G[V_0]$), 也叫 G 在 V_0 上的**限制**. $E_0 \subseteq E(G)$, 以 E_0 为边集, 以 E_0 中边的端点作为顶点集的图叫 E_0 在 G 中的**边导出子图** ($G[E_0]$), 也叫 G 在 E_0 上的**限制**.

定义 2.2.3: 补图

对于简单图 G, 它的**补图 (complement)**$\overline{G}$ 顶点集仍为 $V(G)$. 对不同的 $u, v \in V(G) = V(\overline{G})$, G 中有边连接 $u, v \Leftrightarrow \overline{G}$ 中无边连接 u, v. 如果 $G \cong \overline{G}$, 则称 G 为**自补图**.

例 2.2.4

自补图与非自补图的例子. 注意第 2 个图的 $\overline{G}$ 有个孤立点, 故不是自补图.



定义 2.2.5: 完全图

恰有 n 个顶点的图叫 n **阶图**, 边数最多的 n 阶简单图 K_n 叫 n **阶完全图**.

由于 n 阶完全图中任意两个不同顶点都恰好有一条边, 则

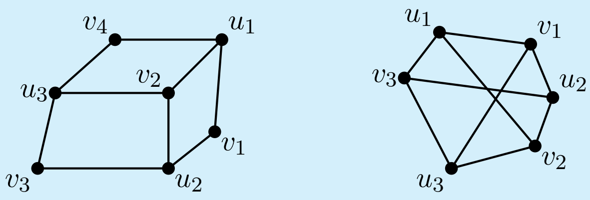
$$|E(K_n)| = \binom{n}{2} = \frac{n(n-1)}{2}.$$

定义 2.2.6: 二部图

设 G 为无向图, 若 $V(G) = V_1 \cup V_2$, V_1, V_2 非空但 $V_1 \cap V_2 = \varnothing$, 且每条边 $e \in E(G)$ 的两个端点中一个在 V_1 中, 另一个在 V_2 中, 则称 G 为具有**二分类** (V_1, V_2) **的二部图**.

例 2.2.7

二部图例子. 这里 u, v 分开.



定义 2.2.8: 完全二部图

设 G 为具有二分类 (V_1, V_2) 的二部图. 如果对 $u \in V_1, v \in V_2$, G 中恰有一条边连接 u, v, 则称 G 为**完全二部图**. 若 $|V_1| = m, |V_2| = n$ 时, 这样的完全二部图记为 $K_{m,n}$, 它有 mn 条边.

例 2.2.9

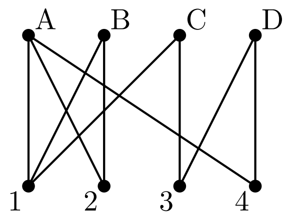
今有 A, B, C, D 四个老师, 欲安排他们上数分、组合、近代、数论四门课, 每个老师上一门他胜任的课程. 已知: A 能教数分、组合、数论, B 能教数分、组合, C 能教数分、近代, D 能教近代、数论. 怎么安排他们上课?

解: 用 1,2,3,4 分别表示数分、组合、近代、数论, 要在二部图中找四条不相邻的边.

(1) $A_1 \Rightarrow B_2 \Rightarrow C_3 \Rightarrow D_4$;

(2) $A_2 \Rightarrow B_1 \Rightarrow C_3 \Rightarrow D_4$;

(3) $A_4 \Rightarrow D_3 \Rightarrow C_1 \Rightarrow B_2$, 共 3 种方案.



练习题 7.

1. **(2014 年)** 设 G 是具有二分类 (V_1, V_2) 的正则二部图, 则必有 $|V_1| = |V_2|$. ( )
2. 设 G 是二部图, 证明: $|E(G)| \le \dfrac{|V(G)|^2}{4}$.
3. 设 $2 \le r \le s$, 问完全二部图 $K_{r,s}$ 中,
   (1) 含多少种非同构的圈?
   (2) 至多有多少个顶点彼此不相邻?
   (3) 至多有多少条边彼此不相邻?
   (4) 点连通度 κ 为几? 边连通度 λ 为几?

§ 2.3 迹、路、圈

定义 2.3.1

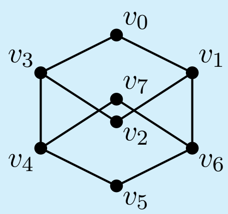
设 G 为无向图, 边 e_i 连接 $v_{i-1}, v_i (i = 1, 2, \cdots, n)$. 则称 $v_0 e_1 v_1 e_2 v_2 \cdots v_{n-1} e_n v_n$ 为一条 v_0 到 v_n 的**途径**. 当 $e_1, \cdots, e_n$ 不是环也不是多条边时, 简记此途径为 $v_0 v_1 \cdots v_n$. 所含边数 n 叫**途径长度**. 一条 $v_0 - v_n$ 途径所含边各不相同时, 称之为 $\mathbf{v_0 - v_n}$ **迹 (trace)**. 一条 $v_0 - v_n$ 的迹经过的点 $v_0, \cdots, v_n$ 两两不同时, 称之为 $\mathbf{v_0 - v_n}$ **路 (path)**. 如果 $v_0 - v_n$ 迹中 $v_0 = v_n$ 但 $v_0, v_1, \cdots, v_{n-1}$ 两两不同, 则称它为一个 **n− 圈 (circle)**. 用 C_n 表示有 n 个顶点的圈. (它们是同构的)

定义 2.3.2: 距离

设 G 为无向图, $u, v \in V(G)$. 如果 $u = v$, 则说 u, v 的**距离** $d(u, v) = 0$. (有时用 $d_G(u, v)$). $u \neq v$ 时, 如果存在 $u - v$ 路, 则最短 $u - v$ 路的长度叫 u, v 之间的距离 $d(u, v)$. 如果没有 $u - v$ 路, 则 $d(u, v) = \infty$.

例 2.3.3

考虑下图.



该图中,

(1) $v_0 v_1 v_2 v_1 v_6$ 是长为 4 的路径.

(2) $v_0 v_3 v_4 v_5 v_6 v_7 v_4$ 是长为 6 的 $v_0 - v_4$ 迹. (边不一样, 点有重复)

(3) $v_0 v_1 v_2 v_3 v_4 v_5 v_6 v_7$ 是长为 7 的路.

(4) $v_4 v_5 v_6 v_7 v_4$ 是长为 4 的圈 (4-圈).

(5) $v_1 v_2 v_3 v_4 v_5 v_6 v_1$ 是长为 6 的圈 (6-圈).

(6) $d(v_0, v_5) = 3$.

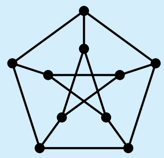
定义 2.3.4: 围长

设 G 是没有环的无向图, G 含圈时, G 所含圈的长度最小值叫 G 的**围长 (girth)**.

注: G 不含圈的时候称 G 的 $g(G)$ 为 $+\infty$.

例 2.3.5: Petersen 图,1898

该图在图论中很重要, 常被用来举例子和反例.



不难发现 Petersen 图 G 中 $g(G) = 5$.

例 2.3.6

设 G 为简单图, 每个顶点至少关联 $k(\geq 1)$ 条边, 则 G 必含长为 k 的路.

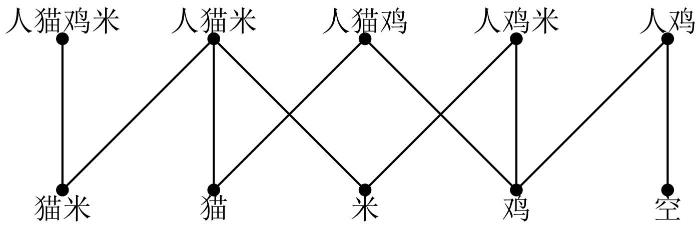
证明: 设 $p = v_1v_2\cdots v_nv_{n+1}$ 是 G 中具有最大长度的路. 只需证 $n \geq k$. 如果 $n \geq k$, 则 G 有长为 k 的路 $v_1v_2\cdots v_kv_{k+1}$.

(反证) 假如 $n < k$, 则 v_1 必与 $v_2, \cdots, v_{n+1}$ 之外某个顶点 v_0 相连. 于是 $v_0v_1\cdots v_{n+1}$ 是比 P 更长的路, 矛盾. □

例 2.3.7

一个人带着猫、鸡、米, 欲从河的左岸到右岸, 每次只能带一件东西过河. 猫与鸡、鸡与米不能在无人看管的情况下放在一起. 问：至少需要多少次渡河才能把这些全带到对岸？

解: 用线表示过河, 点表示左岸剩余物品. 共有 2 种方案.



练习题 8.

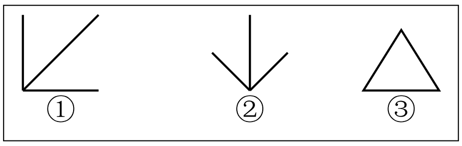
1. **(2014 年)** 设 G 为简单图且 $\delta(G) \geq 2$, 则 G 中含有长大于 $\delta(G)$ 的圈. ( )
2. **(2022 年)** 填空题: 设 m, n 为正整数且 $m \leq n$, 则 $K_{m,n}$ 含 l-圈当且仅当 $l \in \{$________________$\}$.
3. 设 G 是 n 阶自补图, 证明 $n = 4k$ 或 $n = 4k+1$, 其中 k 为正整数.
4. 设 G 是 6 阶无向简单图. 证明 G 或它的补图 $\overline{G}$ 中存在 3 个顶点彼此相邻.
5. **(2022 年)** 证明围长为 5 的 k-正则图 G 至少有 k^2+1 个顶点. (注: G 的围长指 G 中最短圈的长度, k-正则图指各顶点的次数为 k.)

§ 2.4 图的连通性

定义 2.4.1

无向图 G **连通 (connected)** 指对任一对不同顶点 $u, v \in V(G)$, G 中有 $u-v$ 路. 在无向图 G 中, 如果对 $u, v \in V(G)$ 有 $u=v$ 或 G 含 $u-v$ 路, 则说 $u \sim v$.

易见 $\sim$ 是 $V(G)$ 上等价关系.(自反、对称、传递性) 把相互等价的归入一类叫**等价类**, 不同的等价类无公共顶点. 比如: 下图①②③中的点是三个等价类.



G(不连通)

定义 2.4.2: 连通分支

每个这样的一个等价类中顶点导出的子图叫 G 的一个**连通分支** (也叫**极大连通子图**). 用 $\omega(G)$ 表示 G 的**连通分支数**. 对于有向图 G, 如果把边的方向去掉后的无向图连通, 则称 G 是**弱连通图**. 如果对有向图 G 中任一对不同顶点 u, v, G 中有 $u-v$ 路或 $v-u$ 路, 则称 G 为**单向连通图**. 双向连通图叫**强连通图**. 注意有向图的 $u-v$ 路是从 u 指向 v.

定义 2.4.3

设 G 为无向图, $e \in E(G)$. 如果 $\omega(G-e) > \omega(G)$, 则称 e 是个**桥**或**割边**.

由于 $\omega(G) = \omega((G-e)+e) \geq \omega(G-e) - 1$, 则 e 为割边时, $\omega(G-e) = \omega(G) + 1$.

定义 2.4.4

设 $G = \langle V, E \rangle$ 为无向图. 如果 $\varnothing \neq E_0 \subseteq E, \omega(G-E_0) > \omega(G)$, 但 $E_1 \subset E_0$ 时 $\omega(G-E_1) = \omega(G)$, 则称 E_0 为 G 的**边割集**. 把 G 为边割集基数最小的记为 $\lambda(G)$, 这叫 G 的**边连通度**.

当 $\lambda(G) \geq r$ 时, 称 G 为 $r-$ 边连通图 (割小于 r 条边不改变连通分支数). 当 G 不连通时, 约定 $\lambda(G) = 0$.

根据定义, 边 e 为 G 的割边等价于 $E_0 = \{e\}$ 为 G 的边割集.

定义 2.4.5

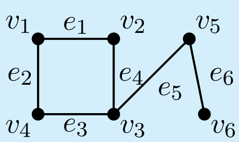
设 $G = \langle V, E \rangle$ 为无向图, 若 $\varnothing \neq V_0 \subseteq V, \omega(G-V_0) > \omega(G)$, 但 $V_1 \subset V_0$ 时 $\omega(G-V_1) = \omega(G)$, 则称 V_0 为 G 的**点割集**. $V_0 = \{v\}$ 为点割集时称 v 为**割点**. 记**连通度** $\kappa(G)$ 为 G 中点割集基数最小者.

$\kappa(G) \geq k$ 时称 G 为 $k-$(点) 连通图. 当 G 不连通时记 $\kappa(G) = 0$. 约定 $\kappa(K_n) = n-1$.

注: 接下来会证明 $\kappa(G) \leq \lambda(G) \leq \delta(G)$. 定义在后面.

例 2.4.6

下图中 e_5, e_6 为割边, $\{e_2, e_3\}$ 为边割集; e_5 为割边; $\{v_2, v_4\}$ 为点割集. 注意 $\{v_3, v_5\}$ 不是点割集.



定理 2.4.7

设 G 是无向图, $e \in E(G)$. 则 e 为 G 的割边 $\Leftrightarrow e$ 不在所有圈上.

证明: e 为环时, 左右两边都不成立. 下设 e 不为环, u, v 为它的两个端点. 则

$$\begin{aligned} e \text{ 为割边} &\Leftrightarrow G - e \text{ 中 } u, v \text{ 处于不同连通分支} \\ &\Leftrightarrow G - e \text{ 中无 } u - v \text{ 路}, u, v \text{ 不等价} \\ &\Leftrightarrow e \text{ 不在圈上}. \end{aligned}$$

这就完成了证明. □

注: 最后一步中, u, v 不等价 $\Rightarrow e$ 不在圈上显然, 反过来, 如果 $G - e$ 中有 $u - v$ 路, 则该 $u - v$ 路加上边 e 就得到了一个圈.

下面定义 $e(G) = |E(G)|$ 为 G 的**边数**.

定理 2.4.8

连通分支数为 k 的 p 阶简单图的边数最大者为

$$\binom{p-k+1}{2} = \frac{(p-k)(p-k+1)}{2}.$$

证明: 对于一个由 $p-k+1$ 阶完全图 K_{p-k+1} 与 $k-1$ 个孤立点组成的图 G, 有

$$e(G) = \frac{(p-k)(p-k+1)}{2}.$$

任给一个有 k 个连通分支的 p 阶简单图 G, 设 $G_1, \cdots, G_k$ 为 G 的 k 个连通分支, 记 $n_i = |V(G_i)|$. 则

$$\boxed{e(G) = \sum_{i=1}^{k} e(G_i) \le \sum_{i=1}^{k} \binom{|V(G_i)|}{2} = \sum_{i=1}^{k} \frac{n_i(n_i-1)}{2} = \frac{1}{2}\sum_{i=1}^{k} n_i^2 - \frac{1}{2}p.}$$

其中用到了 $n_1 + n_2 + \cdots + n_k = p$. 记 $x_i = n_i - 1 \ge 0$. 则 $x_1 + \cdots + x_k = p + k - 1$, 且

$$\sum_{i=1}^{k} n_i^2 = \sum_{i=1}^{k} (x_i+1)^2 \le (x_1 + \cdots + x_k + 1)^2 + k - 1.$$

故

$$e(G) \le \frac{(p-k+1)^2 + k - 1 - p}{2} = \frac{(p-k+1)(p-k)}{2}.$$ □

注: 最后用到了下面的引理.

引理 2.4.9

对非负实数 $x_1, \cdots, x_k$, $(x_1+1)^2 + \cdots + (x_k+1)^2 \le (x_1 + \cdots + x_k + 1)^2 + k - 1$.

证明: 用数学归纳法, $k = 1$ 显然. $k = 2$ 易证. 假如 k 的情况成立, 看 $k+1$ 的情况, 结合 $k = 2$ 的情况以及 k 的情况立证. □

推论 2.4.10

设 G 是 p 阶简单图, 如果 $e(G) > \binom{p-1}{2} = \frac{(p-1)(p-2)}{2}$, 则 G 必连通.

证明: G 连通等价于 G 的连通分支数为 1. 假如 G 的连通分支数 $k \geq 2$, 根据上述引理,

$$e(G) \leq \frac{(p-k)(p-k+1)}{2} \leq \frac{(p-2)(p-2+1)}{2},$$

矛盾. □

练习题 9.

1. **(2014 年)** 判断题: $n(n \geq 2)$ 阶简单连通图 G 中至少有两个顶点不是割点. ( )
2. **(2014 年)** p 阶连通图边数最小值为__________.
3. 设 $e=(u,v)$ 为无向图 G 中的割边, 证明: u 是割点当且仅当 u 不是悬挂顶点.
4. 若 G 为 $k \geq 2$ 的 k-正则二部图, 则 G 没有割边.
5. 设 r-正则图 G 满足 $\kappa(G)=1$. 若 $r>1$, 证明: $\lambda(G) \leq \dfrac{r}{2}$.

§ 2.5 二部图的判别条件

定义 2.5.1

n 为奇数时, $n-$ 圈叫奇圈. n 为偶数时, $n-$ 圈叫偶圈.

引理 2.5.2

G 为二部图 $\Leftrightarrow$ 每个连通分支为二部图.

证明: "$\Rightarrow$": 设 G 具二分类 (V_1, V_2), 则 G 的每个连通分支 G_i 是具二分类 $(V(G_i)\cap V_1, V(G_i)\cap V_2)$ 的二部图.

"$\Leftarrow$": 设 G 有 k 个连通分支 $G_1, \cdots, G_k$. G_i 是具有二分类 $(V_i^{(1)}, V_i^{(2)})$ 的二部图.
则 G 是具有二分类 $\left(\bigcup\limits_{i=1}^{k} V_i^{(1)}, \bigcup\limits_{i=1}^{k} V_i^{(2)}\right)$ 的二部图. □

定理 2.5.3

无向图 G 为二部图 $\Leftrightarrow$ G 不含奇圈.

证明: 根据前面引理, 只需证连通的情况. 不妨设 G 连通.

"$\Rightarrow$" 设 G 为具二分类 (V_1, V_2) 的连通二部图. 若 G 含 n-圈 $v_1v_2\cdots v_nv_1$, 则 $v_1, v_3, \cdots$ 同属 V_1 或 V_2; $v_2, v_4, \cdots$ 同属 V_2 或 V_1. 如果 n 是奇数, 则 v_n 与 v_1 同属 V_1 或 V_2, 与二部图定义矛盾. (二部图每个分类中顶点彼此不相邻)

"$\Leftarrow$" 设连通图 G 不含奇圈, 我们来说 G 是二部图. 由于 G 不含奇圈, G 无环, 任取 $v \in V(G)$, 让

$$V_0 = \{u \in V(G) : 2|d(u,v)\},$$
$$V_1 = \{u \in V(G) : 2 \nmid d(u,v)\}.$$

下证 G 是具二分类 (V_0, V_1) 的二部图. 对不同于 v 的两个顶点 u, u'(任取), 设 P 是 v 到 u 的最短路, P' 是 v 到 u' 的最短路, w 是 P 与 P' 最后一个公共顶点, 则 P 与 P' 中 $v-w$ 路都为最短, 且长度相同.

如果 u, u' 同属 V_0 或 V_1, 则 P 与 P' 长度的奇偶性相同, 从而 P 中 $w-u$ 路与 P' 中 $w-u'$ 路长度的奇偶性相同.

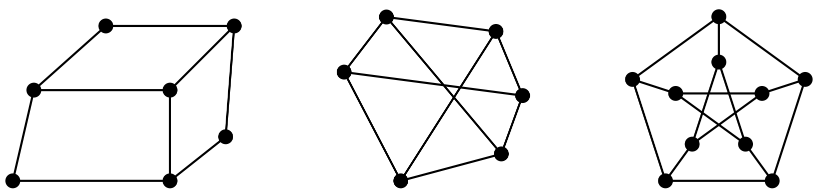
如果 uu' 为边, 则此边与 $w-u$ 路以及 $w-u'$ 路构成奇圈. 因 G 不含奇圈, 则无边连接 u 与 u'. (要注意 u, u' 任取).

由上, G 为有二分类 (V_0, V_1) 的二部图. □

注: $u = v \neq u'$ 时, 如果 uu' 为边, 则 $u \in V_0, u' \in V_1$, 不可能 u, u' 同属 V_0 或 V_1.

例 2.5.4

下面的图中, 前 2 个图没有奇圈, 是二部图; 最后一个图叫 **Peterson 图**, 它有奇圈, 不是二部图.



§ 2.6 图的顶点次数

定义 2.6.1

设 G 为无向图, $v \in V(G)$, $d_G(v)$ 指 v 关联的边的条数, 又称 v **的次数/度**.

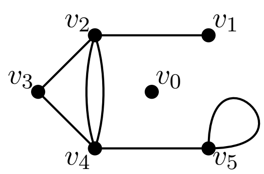
注: 与 v 关联的边为环时算两次.

当 $d_G(v) = n$ 时称 v 为 n 次点, 0 次点又叫**孤立点**. 1 次点叫**悬挂点**.

把 $\Delta(G) = \max\limits_{v \in V(G)} d_G(v)$ 叫 G 的**最大次数**, $\delta(G) = \min\limits_{v \in V(G)} d_G(v)$ 叫 G 的**最小次数**.

如果所有 $d_G(v)(v \in V(G))$ 为同一个值 k, 则 G 叫 $k-$ **正则图**.

例如: 下图中 $d(v_0) = 0, d(v_1) = 1, d(v_2) = 4, d(v_3) = 2, d(v_4) = 4, d(v_5) = 3, \Delta(G) = 4, \delta(G) = 0$.



下面看一个“朋友问题”.

例 2.6.2

在 $p \geq 2$ 个人的人群中必有两个人在本群中朋友个数相同.

证明: 用平面上 p 个点 $v_1, \cdots, v_p$ 表示 p 个人. 如果第 i 个人与第 j 个人是朋友, 则作一条边连接 v_i 与 v_j. $d_G(v_i)$ 表示第 i 个人的朋友个数. 下面证 $d(v_1), \cdots, d(v_p)$ 中必有 2 个相同.

(反证) 假如它们两两不等, 则由正整数性质, $\{d(v_1), \cdots, d(v_p)\}$ 中最大的数比 $p-1$ 大, 即 $\Delta(G) \geq p-1$. 但由于 $\Delta(G) \leq p-1$, 则有一个顶点 v_s 次数恰好为 $p-1$. 从而第 s 个人与其他人都是朋友. 从而 $d(v_1), \cdots, d(v_p)$ 都大于 0. 由于它们两两不同, 又由正整数性质, $\Delta(G) \geq p$, 与 $\Delta(G) \leq p-1$ 矛盾. □

定理 2.6.3. Euler,1736

设 G 为无向图, 则

$$\sum_{v \in V(G)} d_G(v) = 2e(G).$$

证明: 设 $V(G) = \{v_1, \cdots, v_p\}, E(G) = \{e_1, \cdots, e_q\}$. 让

$$N(v_i, e_j) = \begin{cases} 0, & v_i\text{不是}e_j\text{的端点}. \\ 1, & v_i\text{是}e_j\text{的端点, 而}e_j\text{不是环}. \\ 2, & v_i\text{是环}e_j\text{的端点}. \end{cases}$$

则

$$\begin{aligned} \sum_{i=1}^{p} d_G(v_i) &= \sum_{i=1}^{p}\sum_{j=1}^{q} N(v_i, e_j) = \sum_{j=1}^{q}\sum_{i=1}^{p} N(v_i, e_j) \\ &= \sum_{j=1}^{q} 2 = 2q = 2e(G). \end{aligned}$$ □

注: 该定理又称" **握手定理**".

推论 2.6.4

无向图 G 有偶数个奇次点.

证明: 根据上个定理, 把所有奇次点选出来, 有 (注意一个数加偶数不改变奇偶性)

$$\sum_{v\in V(G),2\nmid d_G(v)} d_G(v) \equiv 0(\mod 2).$$

上述 $d_G(v)$ 都是奇数! 而需要有偶数个奇数加起来才为偶数, 故 G 有偶数个奇次点. □

定义 2.6.5

对于具有 p 个顶点 $v_1,\cdots,v_p$ 的无向图 G, $\{d_G(v_p)\}_{i=1}^p$ 叫 G 的一个**度序列**.

定理 2.6.6

设 $d_1,\cdots,d_p\in\mathbb{N}=\{0,1,2,\cdots\}$, 则 $\{d_i\}_{i=1}^p$ 为一个无向图度序列的充分必要条件是

$$d_1+\cdots+d_p\equiv 0(\mod 2).$$

证明: "$\Rightarrow$" 即定理 2.6.3(trivial!)

"$\Leftarrow$" 设 $d_1,\cdots,d_p\in\mathbb{N}$, 且 $d_1+\cdots+d_p$ 为偶数, 则 $d_1,\cdots,d_p$ 中是奇数的有偶数个. 设其中的 $d_{i_1},d_{i_2},\cdots,d_{i_{2k}}$ 为奇数 $(1\le i_1<i_2<\cdots<i_{2k}\le p)$, 取不同顶点 $v_1,\cdots,v_p,1\le i\le p$, 以 v_i 为端点作 $\left\lfloor\frac{d_i}{2}\right\rfloor$ 个环. (也就是说 d_i 为奇数时少了一条边) 当 $j\ne i_1,\cdots,i_{2k}$ 时, $2\left\lfloor\frac{d_j}{2}\right\rfloor=d_j$. 作边 $v_{i_1}v_{i_2}$, $v_{i_3}v_{i_4},\cdots,v_{2k-1}v_{2k}$. (刚刚作环时少了个 degree, 这里连一下就凑够 degree) 由此便作出了一个度序列为 $\{d_i\}_{i=1}^p$ 的无向图. □

注: 作出来的图是这样子的:

定理 2.6.7

设 G 为 p 阶简单图, 顶点次数依次为 $d_1,\cdots,d_p$. 则 $d_1+\cdots+d_p\equiv 0(\mod 2)$ 且当 $1\le k\le p$ 时,

$$\sum_{i=1}^k d_i\le k(k-1)+\sum_{k\le i\le p}\min\{d_i,k\}.$$

证明: (1) 前面定理已证.

(2) 把 p 个点分成两部分: $V_1=\{v_1,\cdots,v_k\}$, $V_2=\{v_{k+1},\cdots,v_p\}$. 在 V_1 内, 最多连 $k(k-1)$ 条边. 而 V_2 中的点往 V_1 连, 最多只能连 k 条. 且由于顶点次数的限制, 最多只能连 d_i 条. 所以 V_2 中的点最多连 $\min\{d_i,k\}$ 条. □

注: 1960 年 Erdös 与 T. Gallai 证明了上面的逆命题成立. 即如果

$$\sum_{i=1}^k d_i\le k(k-1)+\sum_{k\le i\le p}\min\{d_i,k\}.$$

则自然数序列 $\{d_i\}_{i=1}^p$ 也是个简单图度序列.

例 2.6.8

判断 $(6,6,5,4,3,3,1)$ 是不是某个简单图的度序列.

解法一: 假如有个 7 阶简单图 G 使其顶点 $v_1,\cdots,v_7$ 次数依次为 6,6,5,4,3,3,1, 由 $d(v_1)=d(v_2)=6$ 知 v_1,v_2 与其他顶点都连, 从而 v_1v_7,v_2v_7 都为边. 然而 $d(v_7)=1$, 矛盾. 所以它不是一个简单图度序列.

解法二: 用定理 2.6.7, 6+6+5+4+3+3+1 是个偶数, 但

$$21=6+6+5+4\not\leq 4(4-1)+\min\{3,4\}+\min\{3,4\}+\min\{1,4\}=19,$$

不满足定理 2.6.7, 故不是一个简单图度序列. □

练习题 10.

1. 判断题:
   (1) **(2022 年)** 序列 $6,6,6,5,4,3,2$ 是某个 (无向) 简单图的度序列. (　)
   (2) **(2012 年)** 序列 $6,6,6,4,3,3,2$ 是某个 (无向) 简单图的度序列. (　)
2. 一次舞会上有 7 对男女参加, 且舞体互为异性, 会后统计出各人跳舞次数为:
   $$6,6,6,6,6,6,6,6,5,3,3,3,3,3.$$
   证明统计必有错误.
3. **(2022 年)** 一次舞会上有 7 对男女参加, 且舞体互为异性, 会后统计出各人跳舞次数为:
   $$6,6,6,6,6,6,6,6,7,3,3,3,3,3.$$
   证明统计必有错误.
4. 设 G 是 n 阶无向图, $n\geq 3$ 为奇数. 证明 G 与 $\overline{G}$ 中奇度顶点个数相等.
5. 设 G 是 n 阶 m 条边的无向连通图, 证明 $m\geq n-1$.
6. 设 n 阶图 G 中有 m 条边, 证明: $\delta(G)\leq\dfrac{2m}{n}\leq\Delta(G)$.
7. 设 9 阶无向图 G 中, 每个顶点的度数不是 5 就是 6. 证明 G 中至少有 5 个 6 度顶点或至少有 6 个 5 度顶点.
8. 设 G 是 n 阶无向简单图, $n\geq 3$ 为奇数, 证明 G 与 $\overline{G}$ 中奇度顶点个数相等.
9. 设 G 是 n 阶 $n+1$ 条边的无向图, 证明 G 中存在顶点 v, 使得 $d(v)\geq 3$.
10. 若无向图 G 中恰有两个奇度顶点, 证明这两个奇度顶点必连通.
11. **(2014 年)** 设 $v_1,\cdots,v_n$ 为平面上 n 个不同的点, 任两点的距离 (通俗的距离) 至少是 1. 证明至多有 $3n$ 对这样的点使每对点距离恰好为 1.

§ 2.7 树、生成树与赋权图的最小树

定义 2.7.1: 树

无圈的连通无向图叫**树** (**tree**). 只有一个顶点的树叫**平凡树**, 树中 1 次点叫**树叶** (**leaf**).

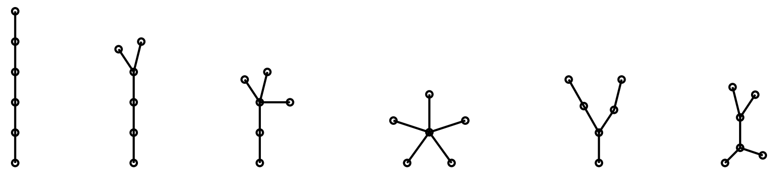
注: 显然, 树必定为简单图.

定义 2.7.2

把每个连通分支都为树的图叫**森林**.

例 2.7.3

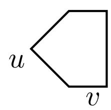
互不同构的 6 阶树共 6 种.



定理 2.7.4

设 G 为简单图, 则: G 为树 $\Leftrightarrow$ 对任何不同的 $u, v \in V(G)$, G 有唯一的 $u-v$ 路.

证明: "$\Leftarrow$" 由条件知 G 必连通. 因为 G 为简单图, G 无环, 若 G 含圈 C, 则 C 上至少有两个不同顶点至少有两条路连接它们 (如右图, u, v 都在圈上, 它们之间至少有两条路连接), 这与只有唯一的 $u-v$ 路矛盾. 故 G 为树.



"$\Rightarrow$" 设 G 为树, u, v 为 G 中不同顶点. 因为 G 连通, 则必有 $u-v$ 路. 假如有两条不同的 $u-v$ 路 P_1 与 P_2, 而 $E(P_1) \neq E(P_2)$, 不妨设 $e \in E(P_1)$ 但 $e \notin E(P_2)$. 则 $(P_1 \cup P_2) - \{e\}$ 连通. 记 v_1, v_2 是 e 的两个端点, 则 $(P_1 \cup P_2) - \{e\}$ 中必有 $v_1 - v_2$ 路. 此路加上边 e 便构成 G 中圈, 与树 G 不含圈矛盾. □

推论 2.7.5

设 u, v 是树 T 的两个不相邻的点, 则 $T + uv$ 恰有一个圈.

注: 这里 uv 表示边.

证明: 树 T 无圈, 则 $T + uv$ 的圈必含边 uv. 由前面的定理，T 中 $u-v$ 路唯一, 故这样的圈唯一. □

定理 2.7.6

若 T 为树, 则

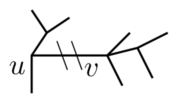
$$e(T) = |V(T)| - 1.$$

证明: 对 $p = |V(T)|$ 进行归纳. $p = 1$ 时, T 只有一个点, 无边. 则 $e(T) = 0 = |V(T)| - 1$.

假设 $p \leq n$ 结论正确, 下证 $p = n+1$ 时结论正确. 由于 $p + 1 \geq 2$ 且 T 连通, T 必有边.

设 uv 为 T 的一条边, 则 uv 是 T 中唯一的 $u-v$ 路. 所以$(T - uv)$ 中无 $u-v$ 路.

设 $T - uv$ 中含 u 的连通分支为 T_u, 含 v 的连通分支为 T_v. 下面证明只有 2 个连通分支: 假如顶点 w 不在 T_u 与 T_v 中, 则 $T - uv$ 中无 $w - u$ 路也无 $w - v$ 路. 从而 T 中无 $w - u$ 路也无 $w - v$ 路 (w 与 uv 边无关, 把 uv 边加上不改变 w 的连通性质), 这与 T 连通矛盾. 因而每个顶点只能在 T_u 或 T_v 里, $T - uv$ 只有 2 个连通分支.



下面证明 T_u 与 T_v 都为树: 由于 T_u, T_v 都是连通分支, 当然连通. 而 T 不含圈, 则 T_u, T_v 都不含圈, 故 T_u, T_v 均为树. 所以 $|V(T_u)|$ 与 $|V(T_v)|$ 都比 $n+1$ 小. 根据归纳假设, $e(T_u) = |V(T_u)| - 1, e(T_v) = |V(T_v)| - 1$. 于是 $e(T) = e(T_u) + e(T_v) + 1 = |V(T_u)| + |V(T_v)| - 1 = |V(T)| - 1$. □

注: 连通图 T 为树 $\Leftrightarrow T$ 的每条边不在圈上 $\Leftrightarrow T$ 每条边都为割边.

定理 2.7.7

非平凡树 T 至少有两片树叶.

证明: 设 T 有 p 个顶点, $v_1, \cdots, v_p$ 恰有 r 片树叶, 则

$$2(p-1) = 2e(T) = \sum_{i=1}^{p} d(v_i) = r + \sum_{v_i\text{不是树叶}} d(v_i) \geq r + 2(p-r) = 2p - r,$$

则 $2(p-1) \geq 2p - r, \Leftrightarrow r \geq 2$. □

例 2.7.8

今有 n 个乒乓球选手, 参加单打淘汰赛, 要决出冠军, 需打多少场比赛?

解: 两个选手间有比赛就连条边, 它不会有圈, 可形成树, 共打 $n-1$ 场. (一个树加上一个点与连这个点的一条边仍然为树). □

定义 2.7.9: 生成树

如果无向图 G 的一个生成子图为树 T, 则称 T 为 G 的一个生成树（支撑树）.

定理 2.7.10

无向图 G 有生成树 $\Leftrightarrow G$ 连通.

证明: "$\Rightarrow$" 设 G 有生成树 T, 对不同的 $u, v \in V(G) = V(T)$, T 中有唯一的 $u-v$ 路, 从而 G 中有 $u-v$ 路, G 连通.

"$\Leftarrow$" 设 G 是 p 阶连通图, 如果 G 本身是树, 则 G 为 G 的生成树.

假如 G 不是树, 但 G 连通, 则 G 有圈 C_1, C_1 上的边 e_1 不是割边, 则 $\omega(G-e_1) = \omega(G) = 1$. 如果 $G-e_1$ 是树, 则 $G-e_1$ 是 G 的生成树. 如果 $G-e_1$ 不是树, 它仍连通, 它包含圈 C_2, C_2 上边 e_2 不是割边, 则 $G-e_1-e_2$ 仍连通, 同样方法进行下去, 如果有边 $e_1, \cdots, e_k$ 使 $G-\{e_1, \cdots, e_k\}$ 为树, 这就是 G 的生成树. □

注: 该过程不可以无限进行下去, 因为边数有限，一定会终止.

推论 2.7.11

设 G 是 p 阶连通图, 则 $e(G) \geq p-1$ 且：$e(G) = p-1 \Leftrightarrow G$ 为树.

证明: G 为树时, $e(G) = |V(G)| - 1 = p - 1$.

G 不为树时, 则 G 有圈, 适当割去 $k \geq 1$ 条边 $e_1, \cdots, e_k$ 后, $T = G - \{e_1, \cdots, e_k\}$ 为生成树. 所以

$$e(T) = |V(T)| - 1 = p - 1$$

所以

$$e(G) = e(T) + k > e(T) = p - 1.$$ □

定义 2.7.12

对于无向连通图 G, 对各边 $e \in E(G)$ 赋以权 $w(e) > 0$, 所得图叫**赋权图**, 把

$$w(G) \triangleq \sum_{e \in E(G)} w(e)$$

叫 G 的**权** (**weight**).

定义 2.7.13: 最小生成树

实际问题中, 往往找赋权图 G 的一个权最小的连通生成子图 T, 这样的 T 必为树, 叫 G 的**最小生成树**.

注: 若这样的 T 不是树, 它有生成树 T', $w(T') < w(T)$, 当然 T' 也是 G 的生成树 (连通生成子图), 这与 T 的选取矛盾.

注: 把最小生成树比作"城市间通高铁"即可.

2.7.1 找赋权连通图的最小树的两个算法

算法 1 (Kruskal 避圈法) 招工, 先找要价低的工人, 小团体 (平行边) 中赶剩一个.

先取 G 中权最小的一条边 e_1, 再在 $G - e_1$ 找权尽可能小的边 e_2, 使 e_1, e_2 不构成圈. 一般地, 选好 $e_1, \cdots, e_k$ 后, 再在 $G - \{e_1, \cdots, e_k\}$ 找权尽可能小的边 e_{k+1}, 使得 $\{e_1, \cdots, e_{k+1}\}$ 的边导出子图中不含圈, 如此进行下去, 最后可以找到边 $e_1, \cdots, e_{p-1}$, 使得这 $p-1$ 条边连同 G 全部 p 个顶点构成的子图 T 为最小树.

T 无圈, 它的每个连通分支都为树. 当

$$p - 1 = e(T) = p - \omega(T) \Rightarrow \omega(T) = 1,$$

则 T 连通. 而当 $k < p - 1$ 时, $e_1, \cdots, e_k$ 与 p 个顶点构成图 T_k 满足

$$k = e(T_k) = p - \omega(T_k) \Rightarrow \omega(T_k) = p - k > 1.$$

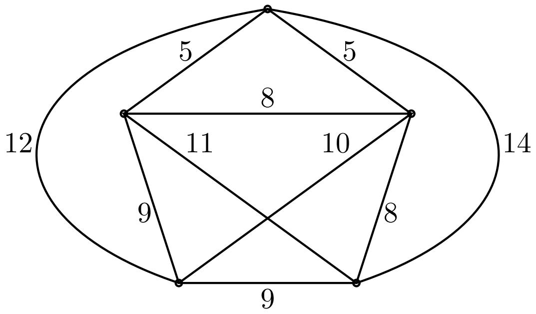
此时 T_k 不连通. 所以 T_k 的两个连通分支间在 G 中有路相连, 可从 G 中找一条边连接两个连通分支, 从而可找 e_{k+1} 使得 $\{e_1, \cdots, e_{k+1}\}$ 的边导出子图不含圈.

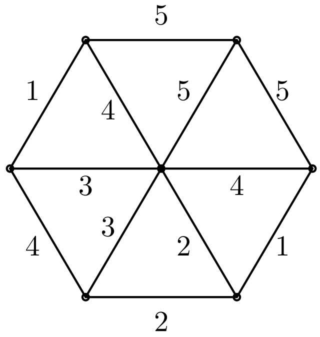
算法 2 (求最小树的破圈法) 招工, 把人全部放进来, 再把要价高的请出去.

若 G 不含圈, 则 G 为最小树. 若 G 含圈, 任取圈 C, 把权最大的边割掉, 仍连通. 如果 $G - e$ 为树, 则它为最小树. 如果 $G - e$ 有圈 C', 再取 C' 权最大的边割掉 (它仍连通). 同样方法进行下去, 最后得最小树 T.

练习题 11.

1. **(2022 年)** 判断题: 至少有两个顶点的树是条路当且仅当它恰有两片树叶. ( )
2. 求下图中两个带权图的最小生成树.





3. 设 G 是树.
   (1) 若 $v \in V(G)$, $d_G(v) = k(k \geq 2)$, 证明 $G \setminus \{v\}$ 至少有 k 个连通分支.
   (2) 若 $\Delta(G) \geq k$, 证明 G 至少有 k 个顶点的度为 1.(等价叙述: G 至少有 k 片树叶.)
4. 设 T 是 $k+1$ 阶无向树, $k \geq 1$. G 是无向简单图, 已知 $\delta(G) \geq k$, 证明 G 中存在与 T 同构的子图.
5. 设 G 为 $n(n \geq 5)$ 阶简单图, 证明 G 或 $\overline{G}$ 中必含圈.
6. **(2014 年)** 设树 T 恰有 r 个一次点, 证明 $r \geq \Delta(T) = \max\limits_{v \in V(T)} d_T(v)$.
7. **(2023 年)** 在一个 n 阶树 $(n \geq 3)$ 里, 若任意两片叶子都没有公共邻点, 求证这个图中至少有一个二度点.
8. **(2022 年)** 设 $d_1, \cdots, d_n$ 为正整数, 且 $\sum\limits_{i=1}^{n} d_i = 2(n-1)$. 又设 G 是以 $d_1, \cdots, d_n$ 为度序列的无向图中连通分支最少的一个图.
   (1) 假如 G 不连通, 证明 G 中某个连通分支含圈.
   (2) 利用 (1) 说明 G 不连通时可通过修改图 G 构造出一个度序列仍为 $d_1, \cdots, d_n$ 的无向图 G' 使得 $\omega(G') < \omega(G)$.
   (3) 利用 (1) 和 (2) 证明 G 必为树.
9. **【选做】优美树猜想:** 设 T 是 n 阶树, 可把这 n 个顶点适当标号为 $1, \cdots, n$, 使得割边标号两两不同 (即跑遍 $1, \cdots, n-1$). 边 ij 的标号指 $|i-j|$.
10. **【选做】1-2-3 猜想:** 对不含孤立边的无向图, 可把每条边适当赋一个属于 $\{1,2,3\}$ 的权使得 u, v 为相邻顶点时, 加权的 $d_G(u)$ 与 $d_G(v)$ 不等. (目前已经解决了 $\{1,2,3,4,5\}$ 的情况.)
11. **【选做】猜想 (孙,2013):** 任给 n 个不同实数 $a_1, \cdots, a_n$, 可把它重新排列为 $b_1, \cdots, b_n$ 但使 $a_1 = b_1$, 使得 $|b_1 - b_2|, |b_2 - b_3|, \cdots, |b_{n-1} - b_n|$ 两两不同. (当 a_1 为最小/最大已证; 米兰的一个博士生证明了 $a_1, \cdots, a_n$ 成等差数列的情况)

§ 2.8 Euler 图与 Hamilton 图

2.8.1 Euler 图

定义 2.8.1

设 G 是有边的无向连通图, 如果存在一个起点与终点相同且经过所有边的迹各一次 (该迹叫**闭 Euler 迹**), 则称 G 为 **Euler 图**.

显然 Euler 图无孤立点.

定理 2.8.2. Euler

设 G 是个非平凡的连通图, 则: G 为 Euler 图 $\Leftrightarrow$ G 的每个顶点都是偶次点.

证明: "$\Rightarrow$" 设 w 为 G 中一条闭 Euler 迹. 由于 G 中每个点至少关联一条边, w 经过 G 每个顶点, 如果顶点 v 在 w 中出现 k 次, 则 $d_G(v) = 2k$.

"$\Leftarrow$" 设 G 各顶点均为偶次点, G 不可能是树. (因为树有至少 2 个 1 次点) 而 G 连通, 则 G 必含圈. 设 C_1 为 G 的一个圈, 则 $G - E(C_1)$ 中各个顶点仍为偶次点 (全部圈上的点都少 2 度, 奇偶性不变). 若 $G - E(C_1)$ 还有边, 则 $G - E(C_1)$ 各边连通分支都不是树, 则它还有圈 C_2. $G - E(C_1) - E(C_2)$ 中各顶点仍为偶次点. 如此下去可知 G 是若干个边不相交的圈的并 (对圈的个数归纳), 从而有闭 Euler 迹. □

注: 非平凡指的是不止一个顶点.

定义 2.8.3

对连通图 G, 起点与终点不同且经过所有边各一次的迹叫**开 Euler 迹**.

注: 闭 Euler 迹与开 Euler 迹经过的点是可以重复的.

注意连通图 G 含 u 到 v 的开 Euler 迹 $\Leftrightarrow$ $G + uv$ 为 Euler 图 $\Leftrightarrow$ G 中仅有 u, v 为奇次点, 其他点为偶次点. 故有:

定理 2.8.4

连通图 G 有开 Euler 迹 $\Leftrightarrow$ G 中恰有两个奇次点.

定义 2.8.5

含开或闭 Euler 迹的连通图叫**一笔画图**.

2.8.2 Hamilton 图

1859 年, Hamilton 发明了个游戏: 正十二面体有 20 个顶点 (视为城市), 要求从某个城市出发, 经过所有其它城市各一次又回到原来的城市.

定义 2.8.6

设 G 为无向图, G 的包含所有顶点的圈叫 **Hamilton 圈**, 含 Hamilton 圈的图叫 **Hamilton 图**.

到目前为止没有一个令人满意的判断 Hamilton 图的充分必要条件.

定理 2.8.7

设 G 是 Hamilton 图, 则当 $\varnothing \neq S \subseteq V(G)$ 时, $\omega(G - S) \leq |S|$.

证明: 设 C 为 G 的 Hamilton 圈. 则 $C-S$ 是 $G-S$ 的生成子图 (顶点没少, 少了些边). $G-S$ 是由 $C-S$ 加上端点属于 $V(C-S)$ 的一些边构成, 故 $\omega(G-S)\le\omega(C-S)$. (当加上一条边后, 连通分支可能会少 1 条或不变!)

只需要证 $\omega(C-S)\le|S|$. 设 $V(G)=V(C)=\{v_1,\cdots,v_r\}$, 则

$$\omega(C-v_1)=1=\{v_1\}.$$

对删去顶点个数归纳. 假设 $\omega(C-v_1-v_2-\cdots-v_s)\le s$ 对, 则

$$\omega(C-v_1-v_2-\cdots-v_s-v_{s+1})\le\omega(C-v_1-\cdots-v_s)+1\le s+1.$$

(删去原本在圈中的一个点, 连通分支数多 0 或 1) □

例 2.8.8

在 4×4 棋盘中跳马.

v_1			v_2
	v_5	v_6	
	v_7	v_8	
v_4			v_3

视小方格为顶点, 如果马可以从一小方格跳到另一个小方格, 则在相应顶点图连条边. 如此可得一个简单图 G. 下面看 G 是否为 Hamilton 图:

让 $S=\{v_5,v_6,v_7,v_8\}$, 在 G 中把 S 拿掉后 v_1,v_2,v_3,v_4 变为孤立点,

$$|V(G-S)|=12,\qquad\omega(G-S)\ge5>|S|=4.$$

违背了定理 2.8.7的必要条件. 故 G 不是 Hamilton 图, 故不可以跳满棋盘.

注: Petersen 图满足定理 2.8.7的必要条件, 但不是 Hamilton 图. (图参见前几节)

定理 2.8.9. Ore,1960

设 G 为 $p\ge3$ 阶简单图. 且对 G 的任一对不相邻顶点 u,v, 有 $d_G(u)+d_G(v)\ge p$. 则 G 为 Hamilton 图.

证明: 先证 G 连通. 若不然, 则有两个不同顶点 u,v 使 G 无 $u-v$ 路. 特别地, u,v 不相邻. 假如 u 所在连通分支为 G_1, v 所在连通分支为 G_2, 则

$$d_G(u)+d_G(v)\le|V(G_1)|-1+|V(G_2)|-1\le|V(G)|-2<p.$$

这与 $d_G(u)+d_G(v)\ge p$ 矛盾, 故 G 连通.

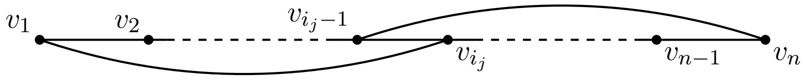
设 $P=v_1v_2\cdots v_n$ 是 G 中一条最长路, 则 $n\le p$. v_1 的相邻顶点只能在 $v_2,\cdots,v_n$ 中, 否则可以延长. 同样v_n 的相邻顶点只能在 $v_1,\cdots,v_{n-1}$ 中. 下证: P 全部 n 个顶点 $v_1,\cdots,v_n$ 是个 n-圈的所有顶点. (该圈不一定每个 v_{i-1} 连着 v_i)

如果 v_1 与 v_n 相邻, 则 $v_1\cdots v_nv_1$ 是个 n-圈.

如果 v_1 与 v_n 不相邻, 设 v_1 的相邻的点是 $v_{i_1},v_{i_2},\cdots,v_{i_k}(2\le i_1<i_2<\cdots<i_k\le n)$. 若 v_{i_1-1}, $v_{i_2-1},\cdots,v_{i_k-1}$ 都不是 v_n 的相邻点, 则

$$d_G(v_1)+d_G(v_n)\le k+(n-1-k)<n\le p,$$

与条件矛盾. 故有 $1 \le j \le k$ 使 v_{i_j-1} 与 v_n 相邻. 如此, $v_1v_2\cdots v_{i_j-1}v_nv_{n-1}\cdots v_{i_j}v_1$ 是个 n-圈, $v_1, \cdots, v_n$ 是它的全部顶点. 该圈上每个点可看做最长路的起点.



下证 $n = p$: 当 $1 \le i \le n$ 时, v_i 的相邻点都在 C 上. 如果 $n \le p$(即 $n < p$), 则有个顶点 u 不在圈上. 但 v_i 的相邻点都在 C 上, 不与 z 连. (否则如果与 u 连, 由 $v_1, \cdots, v_n$ 构成的路不是最长) 但由连通性, u 与圈上的点之间有路, 矛盾. 故 C 为 G 的 Hamilton 圈, G 是 Hamilton 图. □

推论 2.8.10. Dirac,1952

设 G 为 $p \ge 3$ 阶简单图, 若 $\forall v \in V(G)(d_G(v) \ge \frac{p}{2})$, 则 G 为 Hamilton 图.

证明: 对一对不相邻顶点 u, v,

$$d_G(u) + d_G(v) \ge \frac{p}{2} + \frac{p}{2} = p.$$

由 Ore 定理, G 为 Hamilton 图. □

注: 范更毕于 1984 年推广了 Ore 定理. 他对 Hamilton 图研究很深.

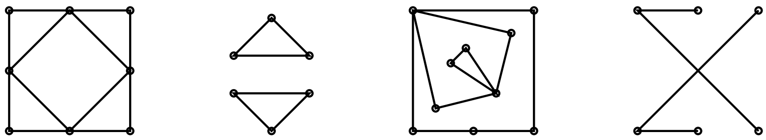
例 2.8.11

一国王要召集他的 $2n(n \ge 2)$ 个大臣议事. 每位大臣与另外的 $2n-1$ 个大臣中至多 $n-1$ 个不和. 能否安排这 $2n$ 个大臣围绕圆桌而坐, 使得不和的大臣不坐在一起（不相邻)?

解: 把大臣记为顶点, 和谐的大臣间连条边. 如此得一个 $2n$ 阶简单图 G. 对于顶点 v, $d_G(v) \ge n = \frac{2n}{2}$. 由上述推论, G 为 Hamilton 图. 可安排这些大臣依 Hamilton 图上顶点顺序坐下.

练习题 12.

1. 判断下图中哪些是 Euler 图, 对不是 Euler 图的至少加多少条边才能成为 Euler 图?



2. 说明 $n(\ge 2)$ 阶无向树不是 Euler 图, 也不是 Hamilton 图; 任意无向树 T 都是二部图.
3. 设 G 是无向简单图, 证明: 若 G 中有割边或割点, 则 G 不是 Hamilton 图.
4. 完全图 $K_n(n \ge 3)$ 都是 Hamilton 图吗?
5. Petersen 图既不是 Euler 图又不是 Hamilton 图, 至少加几条新边才会成为 Euler 图? 至少加几条新边才会成为 Hamilton 图?
6. 设 G 是具有二分类 (V_1, V_2) 的二部图, $|V_1| \ne |V_2|$, 证明: G 不是 Hamilton 图.
7. 设 G 为 $n(n \ge 3)$ 阶无向简单图, $e(G) = \frac{1}{2}(n-1)(n-2)+2$.
   (1) 证明: $\delta(G) \ge 2$.
   (2) 证明: G 是 Hamilton 图.
8. **(2014 年)** 设 G 为 $n(n \ge 3)$ 阶无向简单图,
   (1) 如果 G 有一对不同顶点 u, v 适合 $d_G(u) + d_G(v) < n$, 试证 $e(G) \le \frac{(n-1)(n-2)}{2} + 1$.
   (2) 利用 (1) 证明: $e(G) \ge \frac{1}{2}(n-1)(n-2)+2$ 时, G 是 Hamilton 图.
9. **(2022 年)** 设 G 是恰有 $n(n > 1)$ 个顶点的无向简单图, 而且对 G 的任一对不相邻顶点 u 与 v, 都有 $d_G(u) + d_G(v) \ge n-1$. 利用 Ore 定理证明 G 必有 Hamilton 路.

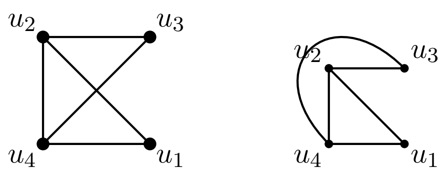
§ 2.9 平面图

定义 2.9.1

设 G 为无向图. 若可把 G 画在平面上使得任两边不在顶点之外的地方相交, 则称 G 为 **(可) 平面图**. 这种画法叫 G 的一个**平面嵌入**.

例 2.9.2

平面图的例子: 左边可以变为右边, 把一条边拉出来, 所以是平面图.



例 2.9.3

二部图 $K_{2,n}$ 是平面图, 其中 n 是正整数. 设二部图有二分类 (V_1, V_2), $|V_1| = 2$, 把 V_1 的点拉到 V_2 两端即可.

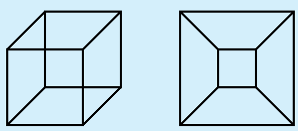
由于用 LaTeX 画图太辛苦太麻烦, 这次就不画图了.

定理 2.9.4. 剥橘子

一个无向图为平面图 $\Leftrightarrow$ 可把此图画到球面上, 使得任意两边 (球面弧) 不在端点以外的地方相交.

例 2.9.5

凸多面体. 以凸多面体的顶点为图的顶点, 多面体的棱作为图的边. 把多面体包在球里, 以多面体内部任一点作为光源, 投射到球面上, 所得图的弧不相交, 则多面体是平面图. 下图是六面体 (左边变为右边):

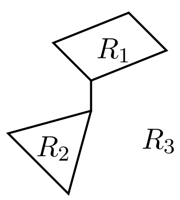


定义 2.9.6

平面图 G 的边把平面分成若干个区域, 每个这样的区域叫一个**面 (face)**. 面积无限的面叫**外面**, 面积有限的面 (封闭区域) 叫**内部面**. 包围每个面的所有边组成的叫该面的**边界**. 面 R 的**次数** $\deg(R)$ 指它边界上边的条数. 如果一个边的两侧是同一个面 R, 则计算 $\deg(R)$ 时此边算两次.

例 2.9.7

下图中 $\deg(R_1) = 4, \deg(R_2) = 3, \deg(R_3) = 9.$



注: 类似于握手定理, 对于平面图 G, 有如下定理:

定理 2.9.8

$$\sum_{R\text{为}G\text{的面}} \deg(R) = 2e(G).$$

定理 2.9.9. Euler

设连通平面图 G 恰有 p 个顶点, q 条边, r 个面, 则 $p - q + r = 2$.

证明: 通过割去圈上边可得 G 的生成树 T(构造没有圈的图), 割去圈上一条边时, 边数少 1, 面数小 1. (两个面被打通了) 边数与面数之差不变, 故 $q - r = e(T) - T$ 的面数 $= p - 1 - 1 = p - 2$. □

注: 易知树 T 的面数都是 1. 另外定理 2.7.6表明 $e(T) = p - 1$.

推论 2.9.10. Euler 多面体公式

设一凸多面体顶点数为 V, 棱数为 E, 面数为 F, 则 $V - E + F = 2$.

定理 2.9.11

设 G 为 p 阶平面图, 每个面次数至少为 $n(\geq 3)$, 则

$$q = e(G) \leq \frac{n}{n-2}(p-2).$$

证明: 先设 G 连通, G 恰有 r 个面 $R_1, \cdots, R_r$, 则

$$2q = \sum_{i=1}^{r} \deg(R_i) \geq rn.$$

由 Euler 公式, $p - q + r = 2$, 则

$$2q \geq (2 + q - p)n \Leftrightarrow q \leq \frac{n}{n-2}(p-2).$$

当 G 每个面的次数都为 n 时取等号.

假如 G 不连通, $G_1, \cdots, G_k$ 为所有连通分支, 作边 e_i 连接 G_i 中一个顶点与 G_{i+1} 中一个顶点, 所得的图 G' 连通, 由刚才所证, $q = e(G) \leq e(G') \leq \dfrac{n}{n-2}(p-2)$. □

推论 2.9.12

$K_{3,3}$ 与 K_5 不是平面图.

证明: 对 $G = K_{3,3}$, 顶点数 $p = 6$, 边数 $q = 9$. G 为奇圈, 假如 G 是可平面图, 每个面次数至少为 4. (至少 4 条边才能围成一个圈) 然而 $9 \nleq \dfrac{4}{4-2}(6-2) = 8$, 与上面定理矛盾.

对 $G = K_5$, 顶点数 $p = 5$, 边数 $q = 10$. 假如 K_5 为平面图, 则每个面的次数至少为 3. (至少 3 边才能围成一个圈) 而 $q = 10 \nleq \dfrac{3}{3-2}(5-2) = 9$, 与上面定理矛盾. □

注: 平面图的子图仍然是平面图, 所以当 $m \geq 3$ 且 $n \geq 3$ 时, $K_{m,n}$ 不是平面图; 当 $n \geq 5$ 时, K_n 不是平面图.

定义 2.9.13

把 uv 边去掉, 引入 w 连接 u,v, 称此操作为**插入二度点** w. 设 w 只和 u,v 相连, 删去点 w, 引入 uv 边, 则称此操作为**消去二度点** w. 如果经过若干次插入或消去二度点可由图 G 得到图 H, 则称 G 与 H **同胚**.

波兰人 Kuratowski 在 1930 年得到如下定理来判别平面图: (比较难证)

定理 2.9.14. Kuratowski

G 为平面图 $\Leftrightarrow$ G 不含同胚于 $K_{3,3}$ 的子图, 也不含同胚于 K_5 的子图.

例 2.9.15: Euler

正多面体只有 5 种.

证明: 把正多面体对应到平面图. 设一个正多面体的顶点数为 p, 棱数为 q, 面数为 r, 根据 Euler 公式有 $p-q+r=2$. 设每个面为正 $n\geq 3$ 边形, 每个顶点恰好在 $k\geq 3$ 个棱上. 则

$$\boxed{\begin{array}{ll} \dfrac{n}{n-2}(p-2)=q=\dfrac{1}{2}kp & (\text{定理 } 2.7.6) \\ 2q=rn & (\text{定理 } 2.9.8). \end{array}}$$

解得

$$p=\frac{4n}{2k-(k-2)n}, q=\frac{2kn}{2k-(k-2)n}, r=q+2-p=\frac{4k}{2k-(k-2)n}.$$

由于 $p>0$, 则 $2k>(k-2)n\Rightarrow 3\leq n<\dfrac{2k}{k-2}\Rightarrow 3k-6<2k\Rightarrow k\leq 5$.

1° 当 $k=3$ 时, $3\leq n<6$, n 可取 $3,4,5$.

① $n=3$ 时, $p=4,q=6,r=4$.

② $n=4$ 时, $p=8,q=12,r=6$.

③ $n=5$ 时, $p=20,q=30,r=12$. (Hamilton 设计的游戏)

2° 当 $k=4$ 时, $3\leq n<4\Rightarrow n=3,p=6,q=12,r=8$.

3° 当 $k=5$ 时, $3\leq n<\dfrac{10}{3}\Rightarrow n=3,p=12,q=30,r=20$. □

2.9.1 其他拓展

下面定理与二部图的匹配问题有关：如果有 n 个男生、n 个女生, A_k 为第 k 个男生喜欢的女生的集合. Hall 定理表明, 对于 $\varnothing\neq I\subseteq\{1,\cdots,n\}$, 有: 任取若干男生, 把他们喜欢的女生放在一起, 女生的个数都多于选取的男生个数 $\Leftrightarrow$ 每个男生可找到自己喜欢的女生做老婆.

定义 2.9.16

设 $A_1,\cdots,A_n$ 为集合, 若 $a_1\in A_1,\cdot,a_n\in A_n$, 则称 $\{a_i\}_{i=1}^n$ 为 $\{A_i\}_{i=1}^n$ 的一个**代表系**, 若 $a_1,\cdots,a_n$ 两两不同, 则称 $\{a_i\}_{i=1}^n$ 为 $\{A_i\}_{i=1}^n$ 的一个**相异代表系**, 简称 **SDR(system of distinct representatives)**.

定理 2.9.17. Hall, 1935

集列 $\{A_i\}_{i=1}^n$ 有 SDR 的充分必要条件是

$$\left|\bigcup_{i\in I}A_i\right|\geq|I|,\forall I\subseteq\{1,\cdots,n\}$$

证明: "⇒" 设 $\{a_i\}_{i=1}^n$ 为 $\{A_i\}_{i=1}^n$ 的一个 SDR, 则 $I\subseteq\{1,\cdots,n\}$ 时,

$$\bigcup_{i\in I}A_i\supseteq\{a_i:i\in I\}\Rightarrow\left|\bigcup_{i\in I}A_i\right|\geq|\{a_i:i\in I\}|=|I|.$$

"⇐": 可由下面定理推出.

定理 2.9.18. 孙, Proc AMS, 129(2001)p3129-3131

设 $A_1,\cdots,A_n(n\geq 1)$ 为 X 的子集, 且 $\{a_i\}_{i=1}^n$ 为 $\{A_i\}_{i=1}^n$ 的一个 SDR, 则有 $J\subseteq\{1,\cdots,n\}$ 使得 $n\in J$, 并且

$$\Big|\Big\{a\in X:\text{由 } a \text{ 与 } a_1,\cdots,a_{n-1} \text{ 适当排序后形成 } \{A_i\}_{i=1}^n \text{ 的 SDR}$$
$$\text{且 } i\notin J \text{ 时 } A_i \text{ 的代表元为 } a_i\Big\}\Big|=\left|\bigcup_{j\in J}A_j\right|-|J|+1.$$

根据上面定理, 由 $n-1$ 的情况推 n 的情况 (加元素并排序) 就证出来了, 从而可以直接归纳证明 Hall 定理.

证明: 【出自 Fiddie 的《组合数学》笔记】

(1) 考虑一个连通图 G, 顶点是 $1,\cdots,n$, 且 i,j 之间有边当且仅当 $i\neq n$ 且 $a_i\in A_j$. 记

$$J=\{1\leq j\leq n:\text{存在 } G \text{ 中 } j \text{ 到 } n \text{ 的通路}\}.$$

(路经过的顶点都不同) 并记 $A=\bigcup_{j\in J}A_j$. 对任意 $i=1,2,\cdots,n-1$, 有:

$$\begin{aligned}a_i\in A&\Leftrightarrow a_i\in A_j,\text{对某个}j\in J\\&\Leftrightarrow \text{存在 } G \text{ 中从 } i \text{ 到某个 } j\in J \text{ 的边}\\&\Leftrightarrow G \text{ 包含一个从 } i \text{ 到 } n \text{ 的路}\Leftrightarrow i\in J.\end{aligned}$$

所以 $\{1\leq i<n:a_i\in A\}=J\setminus\{n\}$.

记集合 $B=A\setminus\{a_i:i\in J\setminus\{n\}\}$, 则 $|B|=|A|-|J|+1$, 且 $B\cup\{a_1,\cdots,a_{n-1}\}=\varnothing$. ($a_i\in B\Rightarrow a_i\in A\Rightarrow i\in J\setminus\{n\}\Rightarrow a_i\notin B$, 矛盾).

(2) 接下来证明 "$a,a_1,\cdots,a_{n-1}$ 可以组合成 $\{A_i\}_{i=1}^n$ 的 SDR, 且 $i\notin J$ 时用 a_i 代表 A_i" ⇔ "$a\in B$".

让 $a\in X$, 如果 a 和 $a_1,\cdots,a_{n-1}$ 可以重新排列组成 $\{A_i\}_{i=1}^n$ 的 SDR, 其中 a_i 是 A_i 的代表元 ($i\notin J$), 则由于 a 是某个 A_j 的代表元 ($j\in J$), 则 $a\in B$.

反过来, 如果 $a\in B$, 则对某个 $j\in J$ 有 $a\in A_j$.

若 $j=n$, 则 $a_n=a\in A_n$, 故 $(a_1,\cdots,a_n)$ 是 $(A_1,\cdots,A_n)$ 的 SDR, 且当 $i\notin J$ 时, A_i 的代表元是 a_i.

若 $j\neq n$, 则 G 包含从 j 到 n 的路 $j_0j_1\cdots j_l$, 其中 $j_0=j,j_l=n$. 注意 $I=\{j_0,\cdots,j_l\}\subseteq J$. 令 $b_{j_0}=a,b_{j_1}=a_{j_0},\cdots,b_{j_l}=a_{j_{l-1}}$, 则当 $i\in I$ 时, $b_i\in A_i$. 这里如果 $i\notin I$, 我们记 $b_i=a_i$, 用原来的代表元 a_i 来代表 A_i, 所以 $\{b_i\}_{i=1}^n$ 是 $\{A_i\}_{i=1}^n$ 的 SDR. (需要验证一下各个 a_i 两两不同)

由上, $a\in X$ 可以与 $a_1,\cdots,a_{n-1}$ 组合成 $\{A_i\}_{i=1}^n$ 的 SDR, 使得 $i\notin I$ 时, 仍用 a_i 代表 $A_i\Leftrightarrow a\in B$. 而且 $|B|=|A|-|J|+1$. □

下面定理与组合数学密切相关：

定理 2.9.19. Ramsey

设 $q_1,\cdots,q_t\geq r\geq 1$ 为整数. 一定存在一个 N (把最小的这样的数记为 $R_r(q_1,\cdots,q_t)$——Ramsey 数), 使得对任给基数至少为 N 的集合 S, 把 S 的所有 r 元子集随意分到 t 个抽屉中, 则有 $1\leq i\leq t$, 使 S 有个 q_i 元子集, 其所有 r 元子集均在第 i 个抽屉中.

注: 例如：$R_2(3,3)=6$, 6 个人里必有 3 个人要么互相是朋友, 要么互相不是朋友. (看前面习题)

练习题 13.

1. 判断题.
   (1) **(2022 年)** 设 G 是恰有 k 个连通分支的平面图, 其顶点数为 p, 边数为 q, 面数为 r, 则 $p-q+r=k+1$. (　　)
   (2) **(2022 年)**Petersen 图 G 是可平面图. (　　)
2. **(2022 年)** 填空题: 完全图 K_n 为可平面图当且仅当 n 满足__________.
3. 设 G 是 $n(\geq 12)$ 阶无向简单图, 证明 G 或 $\overline{G}$ 必为非平面图.
4. 设 G 是简单平面图, 面数 $r<12,\delta(G)\geq 3$. 证明 G 中存在次数小于或等于 4 的面.
5. 设 G 是 n 阶 m 条边的简单平面图, 已知 $m<30$, 证明 $\delta(G)\leq 4$.

第 3 章　ZFC 公理集合论

§ 3.1　ZFC 公理集合论的诞生

1874-1875 年 Cantor 创立集合论.

1902 年 Russell 悖论: 设由具有性质 $x \notin x$(自己不属于自己) 的集合 x 构成集合 X, 则 $X \in X \Leftrightarrow X \notin X$, 依排中律, $X \in X$ 或 $X \notin X$, 总是矛盾.

集合论是绝大部分数学的基础, Cantor 这种原始的集合论叫朴素 (naive) 集合论.

1908 年意大利数学家 Zermelo 提出对集合不加定义, 只用公理来刻画, 把集合不看做什么整体, 而视为满足一些公理的对象.

名人名言: "这些原理应足够地狭窄, 以排除掉所有悖论, 同时又要足够地宽广, 以保留集合论中有价值的东西." ——Zermelo

Zermelo 提出了集合论的 7 条公理.

1922-1923 年德国 Fraenkel 改进 Zermelo 公理系统, 又用了一条公理, 这八条公理构成 ZF 集合论系统, 若再加上**选择公理 (Axiom of Choice)**, 叫 ZFC 公理系统.

选择公理: 由一组两两不相交的集合中各取一个代表元, 可以构成一个新的集合.

ZFC 公理系统采用带相等词 "=" 的一阶逻辑语言, 个体变元为集合变元, 个体域非空 (要有个集合), $x \in X$ 时称 x 为 X 的元素 (element), 叫 x **属于** X. 这里 x 与 X 均为集合.

§ 3.2　外延性公理、对偶公理及有序对

公理 3.1: 外延性公理 (Axiom of extensionality)

$$\forall A \forall B(\forall x(x \in A \leftrightarrow x \in B) \to A = B).$$

为了方便, 可写为 (省略 $\forall A \forall B$)

$$\forall x(x \in A \leftrightarrow x \in B) \to A = B.$$

对集合而言, 只要外延相同便认为集合相等而不必管内涵. 比如

$$\{\text{大于 } 2 \text{ 的偶素数}\} = \{\text{小于 } 0 \text{ 的自然数}\}$$

定义 3.2.1

如果 $\forall x(x \in A \to x \in B)$, 则说 A 为 B 的**子集 (subset)**, 记为 $A \subseteq B$. 也说 A 被 B 所**包含**. 如果 $A \subseteq B \wedge A \neq B$, 则写 $A \subset B$, 称为 A 被 B **真包含**, A 是 B 的**真子集 (proper subset)**.

$$\begin{aligned}
\forall x(x \in A \leftrightarrow x \in B) &\equiv \forall x((x \in A \to x \in B) \wedge (x \in B \to x \in A)) \\
&\equiv \forall x(x \in A \to x \in B) \wedge \forall x(x \in B \to x \in A) \\
&\equiv A \subseteq B \wedge B \subseteq A.
\end{aligned}$$

注: 外延性公理相当于

$$A \subseteq B \wedge B \subseteq A \Rightarrow A = B.$$

公理 3.2: 对偶公理 (pairing axiom)

$$\forall a \forall b \exists X \forall x (x \in X \leftrightarrow (x = a \vee x = b)).$$

注意这里 a, b 为集合.

假如 $\forall x (x \in X \leftrightarrow (x = a \vee x = b)$ 且 $\forall x (x \in Y \leftrightarrow (x = a \vee x = b)$, 则 $\forall x (x \in X \leftrightarrow x \in Y)$. 根据外延性公理, $X = Y$. 因此给定集合 a, b 以后, 上述公理中 X 存在且唯一, 记之为 $\{a, b\}$.

$\{a, b\} = \{b, a\}$, 这是因为

$$x \in \{a, b\} \Leftrightarrow x = a \vee x = b \Leftrightarrow x = b \vee x = a \Leftrightarrow x \in \{b, a\}.$$

这样, 我们把 $\{a, b\} = \{b, a\}$ 叫**无序对**.

把 $\{a, a\}$ 简记为 $\{a\}$, 叫**独点集**.

$$x \in \{a\} \Leftrightarrow x \in \{a, a\} \Leftrightarrow x = a \vee x = a \Leftrightarrow x = a.$$

如何定义有序对? 有序对的特征是 $\langle x, y \rangle = \langle u, v \rangle x = u \wedge y = v$.

定义 3.2.2: 有序对

把有序对 $\langle x, y \rangle$ 定义为 $\{\{x\}, \{x, y\}\}$.

定理 3.2.3. K. Kuratowsky, 1921

在上述定义下, $\langle x, y \rangle = \langle u, v \rangle \Leftrightarrow (x = u) \wedge (y = v)$.

证明: "$\Leftarrow$" 显然. "$\Rightarrow$" : 设 $\langle x, y \rangle = \langle u, v \rangle$, 即 $\{\{x\}, \{x, y\}\} = \{\{u\}, \{u, v\}\}$.

- 如果 $\{u\} = \{x, y\}$, 则 $u = x = y$, 则

$$\{u, v\} \in \langle u, v \rangle = \langle x, y \rangle = \{\{x\}, \{x, y\}\} = \{\{x\}, \{x\}\},$$

从而 $\{u, v\} = \{x\}$, $u = v = x$, 从而 $u = x, v = y$ 成立.

- 如果 $\{x\} = \{u, v\}$, 则 $x = u = v$, 则

$$\{x, y\} \in \langle x, y \rangle = \langle u, v \rangle = \{\{u\}, \{u, v\}\} = \{\{u\}, \{u\}\},$$

从而 $\{x, y\} = \{u\}$, $x = y = u$, 从而 $u = x, v = y$ 成立.

- 下设 $\{u\} \neq \{x, y\}$ 且 $\{x\} \neq \{u, v\}$. 此时

$$\{u\} \in \{\{u\}, \{u, v\}\} = \langle u, v \rangle = \langle x, y \rangle = \{\{x\}, \{x, y\}\}.$$

而 $\{u\} \neq \{x, y\}$, 必有 $\{u\} = \{x\}$, $u = x$.

$$\{u, v\} \in \{\{u\}, \{u, v\}\} = \langle u, v \rangle = \langle x, y \rangle = \{\{x\}, \{x, y\}\},$$

而 $\{u, v\} \neq \{x\}$, 必有 $\{u, v\} = \{x, y\}$, $v \in \{x, y\}$. 若 $v \neq y$, 则 $v = x = u$, 与 $\{x\} \neq \{u, v\}$ 矛盾, 故 $v = y$. □

注: 推广到多维: $\langle x, y, z\rangle \triangleq \langle\langle x, y\rangle, z\rangle$,

$$\begin{aligned}\langle x_1, y_1, z_1\rangle = \langle x_2, y_2, z_2\rangle &\Leftrightarrow \langle\langle x_1, y_1\rangle, z_1\rangle = \langle\langle x_2, y_2\rangle, z_2\rangle \\ &\Leftrightarrow \langle x_1, y_1\rangle = \langle x_2, y_2\rangle \wedge z_1 = z_2 \\ &\Leftrightarrow x_1 = x_2 \wedge y_1 = y_2 \wedge z_1 = z_2.\end{aligned}$$

设 $\langle x_1, \cdots, x_{n-1}\rangle$ 有定义, 则 $\langle x_1, \cdots, x_{n-1}, x_n\rangle$ 定义为 $\langle\langle x_1, \cdots, x_{n-1}\rangle, x_n\rangle$, 这样

$$\langle x_1, \cdots, x_{n-1}, x_n\rangle = \langle y_1, \cdots, y_{n-1}, y_n\rangle \Leftrightarrow \langle\langle x_1, \cdots, x_{n-1}\rangle, x_n\rangle = \langle\langle y_1, \cdots, y_{n-1}\rangle, y_n\rangle.$$

对 n 归纳易得

$$\langle x_1, \cdots, x_{n-1}, x_n\rangle = \langle y_1, \cdots, y_{n-1}, y_n\rangle \Leftrightarrow x_1 = y_1 \wedge \cdots \wedge x_n = y_n.$$

把 $\langle\langle x_1, \cdots, x_{n-1}\rangle, x_n\rangle$ 叫由 $x_1, \cdots, x_n$ 构成的**有序 n 元组**或 **n 元矢量**.

§ 3.3 联集公理、分出公理与集合代数

公理 3.3: 联集公理 (Axiom of union)

任给集合 X,

$$\exists Y \forall y(y \in Y \leftrightarrow \exists x(y \in x) \wedge x \in X).$$

(x 是 X 儿子, y 是 X 孙子)

根据外延性公理, 这样的 Y 存在唯一, 记为 $\bigcup X$(X 的联集).

$$y \in \bigcup X \Leftrightarrow \exists x \in X(y \in x).$$

对于集合 A, B, $\bigcup\{A, B\}$ 记为 $A \cup B$(A 与 B 的并集). 注意

$$x \in A \cup B \Leftrightarrow x \in \bigcup\{A, B\} \Leftrightarrow x \in A \vee x \in B.$$

定义 $\{x_1, x_2, x_3\} \triangleq \{x_1, x_2\} \cup \{x_3\}$, 则

$$x \in \{x_1, x_2, x_3\} \Leftrightarrow x = x_1 \vee x = x_2 \vee x = x_3,$$

定义 $\{x_1, \cdots, x_n\} = \{x_1, \cdots, x_{n-1}\} \cup \{x_n\}$, 由归纳,

$$x \in \{x_1, \cdots, x_n\} \Leftrightarrow x = x_1 \vee \cdots \vee x = x_n.$$

$\bigcup X$ 常记为 $\bigcup\limits_{i \in I} X_i$. (如果 $A = \{A_1, \cdots, A_n\}$, 则 $\bigcup A = A_1 \cup A_2 \cup \cdots \cup A_n$).

$$x \in \bigcup_{i \in I} X_i \Leftrightarrow \exists i \in I(x \in X_i).$$

$$x \in \bigcup_{i=1}^{n} X_i \Leftrightarrow x \in X_1 \vee x \in X_2 \vee \cdots \vee x \in X_n.$$

Cantor 朴素集合论中**概括原理**: 设 φ 为二阶公式, 则存在集合 X, 使对任何集合 x 都有 $x \in X \Leftrightarrow \varphi(x)$.

公理 3.4: 分出公理 (Axiom of separation)

设 $\varphi(x)$ 是不以 Y 为自由变元的公式, 则

$$\exists Y \forall x(x \in Y \leftrightarrow (x \in X \wedge \varphi(x))).$$

注: 分出公理表明, 允许构造出一种带 $\varphi(x)$ 性质的集合.

根据外延性公理, 这样的 Y 存在唯一, 记之为 $\{x \in X : \varphi(x)\}$.

$$y \in \{x \in X : \varphi(x)\} \Leftrightarrow y \in X \wedge \varphi(y).$$

设 X 是个集合, 根据分出公理, $\{x \in X : x \neq x\}$ 也是个集合, 记为 $\varnothing$. 显然 $\forall x(x \notin \varnothing)$, $\varnothing$ 中没有元素, 叫做**空集 (empty set)**.

定义 3.3.1

对集合 X, 让

$$\bigcap X = \{y \in \bigcup X : \forall x \in X(y \in x)\}$$

表示交 (intersection),

把 $\bigcap\{A, B\}$ 记为 $A \cap B$. 当然 $\bigcap \varnothing = \{y \in \bigcup \varnothing : \forall x \in \varnothing(y \in x)\} = \varnothing$.

把 $\bigcap\{X\}$ 记为 $\bigcap\limits_{x \in X} x$. 当 $X = \{X_i : i \in I\}$ 时, $\bigcap X$ 常记为 $\bigcap\limits_{i \in I} X_i$.

$$X \cap Y = \{x \in X : x \in Y\} = \bigcap\{X, Y\},$$

把 $X \setminus Y = \{x \in X : x \notin Y\}$ 叫集合 X 与 Y 的**差**. $Y \subseteq X$ 时, $X \setminus Y$ 也记为 $X - Y$.

定义 3.3.2: 对称差

$X \oplus Y = (X \setminus Y) \cup (Y \setminus X)$.

例 3.3.3

$X \oplus Y = (X \cup Y) \setminus (X \cap Y)$.

证明: 任给集合 x, 由外延性公理以及

$$\begin{aligned}
& x \in X \oplus Y \\
\Leftrightarrow & x \in X \setminus Y \vee x \in Y \setminus X \\
\Leftrightarrow & (x \in X \wedge x \notin Y) \vee (x \in Y \wedge x \notin X) \\
\Leftrightarrow & (x \in X \vee x \in Y) \wedge \underline{(x \in X \vee x \notin X)} \wedge \underline{(x \notin Y \vee x \in Y)} \wedge (x \notin Y \vee x \notin X) \\
\Leftrightarrow & (x \in X \cup Y) \wedge \neg(x \in X \cap Y).
\end{aligned}$$

于是 $X \oplus Y = (X \cup Y) \setminus (X \cap Y)$. □

关于对称差, 有如下性质:

$$\begin{aligned}
& A \oplus B = B \oplus A \\
& (A \oplus B) \oplus C = A \oplus (B \oplus C) \\
& \varnothing \oplus A = A \oplus \varnothing = A \\
& A \oplus A = \varnothing.
\end{aligned}$$

例 3.3.4

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

证明: 用外延性公理以及

$$\begin{aligned}
& x \in A \cup (B \setminus A) \\
\Leftrightarrow & x \in A \vee (x \in B \wedge x \notin A) \\
\Leftrightarrow & (x \in A \vee x \in B) \wedge \underline{(x \in A \vee x \notin A)} \\
\Leftrightarrow & x \in A \vee x \in B \\
\Leftrightarrow & x \in A \cup B.
\end{aligned}$$

所以 $A \cup (B \setminus A) = A \cup B$. □

基数: $A \cap B = \varnothing$ 时, $|A| + |B| \triangleq |A \cup B|$. 此外

$$|A \cup B| = |A \cup (B \setminus A)| = |A| + |B \setminus A| \leq |A| + |B|.$$

(注意 $B = (B \setminus A) \cup (A \cap B)$)

当 A, B 有穷时, $|B \setminus A| = |B| - |A \cap B|$, 则 $|A \cup B| = |A| + |B| - |A \cap B|$.

当 A, B, C 有穷时, $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.

定理 3.3.5. 容斥原理 (Inclusion-Exclusive Principle)

设 $S_1, \cdots, S_n$ 是有穷集, 则

$$\begin{aligned}
\left|\bigcup_{i=1}^{n} S_i\right| = & \sum_{i=1}^{n} |S_i| - \sum_{1 \leq i < j \leq n} |S_i \cap S_j| + \sum_{1 \leq i < j < k \leq n} |S_i \cap S_j \cap S_k| \\
& - \cdots + (-1)^{n-1} |S_1 \cap S_2 \cap \cdots \cap S_n|.
\end{aligned}$$

关于集合 $\cup, \cap, \setminus$ 的集合代数中基本规律:

幂等律: $A \cup A = A, A \cap A = A$.

交换律: $A \cup B = B \cup A, A \cap B = B \cap A$.

结合律: $(A \cup B) \cup C = A \cup (B \cup C), (A \cap B) \cap C = A \cap (B \cap C)$.

分配律: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C), A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

证明: 用外延性公理以及

$$\begin{aligned}
x \in A \cap (B \cup C) & \Leftrightarrow x \in A \wedge (x \in B \vee x \in C) \\
& \Leftrightarrow (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \\
& \Leftrightarrow x \in (A \cap B) \cup (A \cap C).
\end{aligned}$$

吸收律: $A \cup (A \cap B) = A, A \cap (A \cup B) = A$.

de Morgan 律: $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B), X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$.

分配律也可以推广为 $A \cap \bigcup_{i \in I} B_i = \bigcup_{i \in I} (A \cap B_i), A \cup \bigcap_{i \in I} B_i = \bigcap_{i \in I} (A \cup B_i)$.

当 $A \subseteq X$ 时, 称 $X \setminus A$ 为 A 的**补集 (complement)**, 有时记为 $\overline{A}$.

$$B = A \cup B \Leftrightarrow A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \setminus B = \varnothing.$$

练习题 14.

1. 已知 $\langle x, y\rangle = z$, 求 x, y. (把 x, y 用 z 以及 $\cup, \cap, \setminus$ 等运算表达.) 注意不需要分类讨论, 要具有一般性. (如果 $\{x\} = y$, 则 $x = \bigcap y = \bigcup y$).
2. 证明容斥原理. 提示: 对 n 归纳证明, 考虑

$$\left|\bigcup_{i=1}^{n} S_i\right| = \left|S_n \cup \bigcup_{i=1}^{n-1} S_i\right|.$$

3. 证明 de Morgan 律推广形式:

$$X \setminus \bigcap_{i\in I} X_i = \bigcup_{i\in I} X \setminus X_i, X \setminus \bigcup_{i\in I} X_i = \bigcap_{i\in I} X \setminus X_i,$$

§ 3.4 幂集公理与笛卡尔积

公理 3.5: 幂集公理 (Power set axiom)

任给集合 X,

$$\exists Y \forall y (y \in Y \leftrightarrow y \subseteq X).$$

由外延性公理, 这样的 Y 存在唯一, 记为 $\mathcal{P}(X)$(X 的**幂集 (power set)**). 当 $|X| = n$ 时, $|\mathcal{P}(X)| = 2^n$.

定理 3.4.1

不存在集合 X 使得 $\forall x(x \in X)$.

证明: 假如存在这样的 X, 则依分出公理, $Y = \{x \in X : x \notin x\}$ 是个集合, 则

$$Y \in Y \Leftrightarrow Y \in X \wedge Y \notin Y \Leftrightarrow Y \notin Y,$$

导致矛盾. □

$\{$集合$x\}$ 不是集合, 而叫**类 (class)**, 是 class 而不是 set 的叫**真类 (proper class)**.

$\mathcal{P}(X)$ 由 X 的所有子集构成, $A \approx B$ 指存在 A 到 B 的一一对应 f, $A \preccurlyeq B$ 指 $|A| \leq |B|$, 存在 $B_0 \subseteq B$ 使得 $A \approx B$. $A \prec B$ 指 $A \preccurlyeq B$ 但不成立 $A \approx B$, 相当于 $|A| < |B|$.

定理 3.4.2

对任何集合 X, $X \prec \mathcal{P}(X)$, 即 $|X| < |\mathcal{P}(X)|$.

证明: X 中 x 对应 $\mathcal{P}$ 中 $\{x\}$, 则

$$X \approx \{\{x\} : x \in X\} \subseteq \mathcal{P}(X).$$

所以 $|X| \leq |\mathcal{P}(X)|$, 这里 $\{\{x\} : x \in X\}$ 是个集合是因为由分出公理,

$$\{y \in \mathcal{P}(X) : y \neq \varnothing \wedge \forall u \forall v (u \in y \wedge v \in y \to u = v)\}$$

是个集合.

下面证 $X \approx \mathcal{P}(X)$ 不成立.(反证) 若 f 是 X 到 $\mathcal{P}(X)$ 的一一对应, 则由分出公理,

$$Y = \{y \in X : y \notin f(y)\}$$

是个集合, $Y \subseteq X$, 故 $Y \in \mathcal{P}(X)$, 则有一个 $x \in X$, 使得 $f(x) = Y$. 从而

$$x \in f(x) \Leftrightarrow x \in Y \Leftrightarrow x \in X \wedge x \notin f(x) \Leftrightarrow x \notin f(x).$$

矛盾, 因此 $X \preccurlyeq \mathcal{P}(X)$ 但 $X \approx \mathcal{P}(X)$ 不成立, 即 $X \prec \mathcal{P}(X)$. □

下面定义笛卡尔积, 想让 $X \times Y$ 指 $\{\langle x, y\rangle : x \in X \wedge y \in Y\}$. 当 $x \in X$ 且 $y \in Y$ 时,

$$\begin{aligned}
\{x\}, \{x, y\} \subseteq X \cup Y &\Rightarrow \{x\}, \{x, y\} \in \mathcal{P}(X \cup Y) \\
&\Rightarrow \langle x, y\rangle = \{\{x\}, \{x, y\}\} \subseteq \mathcal{P}(X \cup Y) \\
&\Rightarrow \langle x, y\rangle \in \mathcal{P}\mathcal{P}(X \cup Y).
\end{aligned}$$

定义 3.4.3

X, Y 为集合时, $\{z \in \mathcal{P}\mathcal{P}(X \cup Y) : \exists x \in X \exists y \in Y(\langle x, y \rangle = z)\}$ 也是个集合, 记为 $X \times Y$, 叫集合 X 与 Y 的**笛卡尔积 (Decartesian product)**. $X \times Y$ 中的元素为**有序对**.

$$\langle x, y \rangle \in X \times Y \Leftrightarrow x \in X \wedge y \in Y.$$

注: $\exists x \in X \exists y \in Y(\langle x, y \rangle = z)$ 成立时, $z \in \mathcal{P}\mathcal{P}(X \cup Y)$ 自动成立, 上面是为了用分出公理说明 $X \times Y$ 是个集合.

集合 $X_1, X_2, \cdots, X_n$ 的笛卡尔积为

$$X_1 \times X_2 \times \cdots \times X_n = \{\langle x_1, \cdots, x_n \rangle : x_1 \in X_1 \wedge \cdots \wedge x_n \in X_n\}.$$

练习题 15.

1. 证明 $\mathcal{P}(X) = \mathcal{P}(Y) \Leftrightarrow X = Y$.
2. 设 $X_1, X_2, \cdots, X_n$ 是集合, 则有集合 X 使 X 中元为 n 元矢量 $\langle x_1, \cdots, x_n \rangle$, 且

$$\langle x_1, \cdots, x_n \rangle \in X \Leftrightarrow x_1 \in X_1 \wedge \cdots \wedge x_n \in X_n.$$

3. **(2012 年)** 列出集合 $X = \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}$ 的幂集 $\mathcal{P}(X)$ 中的所有元素: ____________________________________.
4. **(2012 年)** 是否有集合 X 使得 $\forall x(x \in X \longleftrightarrow \forall y(y \notin x \vee x \notin y))$? 请说明理由.
5. **(2022 年)**(不用正规公理) 用反证法证明没有集合 X 满足 $\forall x(x \notin X \longleftrightarrow \exists y(y \in x \wedge x \in y))$.

§ 3.5 关系与映射

定义 3.5.1

集合 R 为**关系 (relation)** 指

$$\forall z(z \in R \to \exists x \exists y(\langle x, y\rangle = z))$$

的有序对构成的集合, 对于关系 R, $\langle x, y\rangle \in R$ 也写 xRy, 此时说 x 与 y 有关系 R.

$\langle x, y\rangle \in R$ 时, 第一个分量是否构成集合? $\{\{x\},\{x,y\}\} \in R \Rightarrow \{x\},\{x,y\} \in \bigcup R \Rightarrow x, y \in \bigcup\bigcup R$. 对于关系 R, 依分出公理, $\{x \in \bigcup\bigcup R : \exists y(xRy)\}$ 是个集合, 叫做 R 的**定义域 (domain)**, 记为 $Dom(R)$. $x \in Dom(R) \Leftrightarrow \exists y(xRy)$. 把 $\{y \in \bigcup\bigcup R : \exists x(xRy)\}$ 叫 R 的**值域 (range of R)**, 或叫**像集 (image of R)**, 记为 $Ran(R)$ 或 $Im(R)$. $y \in Dom(R) \Leftrightarrow \exists x(xRy)$. 如果 $R \subseteq A \times A$, 则称 R 为 A 上**关系**, 对于关系 R, 让 $A = Dom(R) \cup Ran(R)$, 则 $R \subseteq A \times A$(R 为 A 上关系).

设 R 为关系, R 在 A 上**限制**指

$$R\lceil A = R \cap (A \times Ran(R)) = \{\langle x, y\rangle \in R; x \in A\}.$$

R 之下 A 的**像集**指

$$R\lceil A] = Im(R\lceil A) = \{y \in Ran(R) : \exists x \in A(xRy)\}.$$

下面给出一些基本性质.

定理 3.5.2

我们有

(1)$Dom(R_1 \cup R_2) = Dom(R_1) \cup Dom(R_2)$

(2)$Im(R_1 \cup R_2) = Im(R_1) \cup Im(R_2)$

(3)$Dom(R_1 \cap R_2) \subseteq Dom(R_1) \cap Dom(R_2)$ （交出来可能为空）

(4)$Im(R_1 \cap R_2) \subseteq Im(R_1) \cap Im(R_2)$

(5)$Dom(R_1) \setminus Dom(R_2) \subseteq Dom(R_1 \setminus R_2)$

(6)$Im(R_1) \setminus Im(R_2) \subseteq Im(R_1 \setminus R_2)$

(7) 像集: $R\lceil A \cup B] = R\lceil A] \cup R\lceil B]$

(8) 像集: $R\lceil A \cap B] \subset R\lceil A] \cap R\lceil B]$

(9) 限制: $R\lceil(A \cup B) = R\lceil A \cup R\lceil B$

证明: 以 (1) 为例, 用外延性公理即可,

$$\begin{aligned} x \in Dom(R_1 \cup R_2) &\Leftrightarrow \exists y(\langle x, y\rangle \in R_1 \vee \langle x, y\rangle \in R_2) \\ &\Leftrightarrow \exists y(\langle x, y\rangle \in R_1) \vee \exists y(\langle x, y\rangle \in R_2) \\ &\Leftrightarrow x \in Dom(R_1) \vee x \in Dom(R_2) \Leftrightarrow x \in Dom(R_1) \cup Dom(R_2). \end{aligned}$$

其他类似. □

定义 3.5.3: 逆关系

$R^{-1} = \{\langle y, x\rangle \in Ran(R) \times Dom(R) : xRy\}$.

当 R 为关系时, $xRy \Leftrightarrow yR^{-1}x$, $(R^{-1})^{-1} = R$, $(A \times B)^{-1} = B \times A$, $Dom(R^{-1}) = Ran(R)$, $Ran(R^{-1}) = Dom(R)$, $(R_1 \cup R_2)^{-1} = R_1^{-1} \cup R_2^{-1}$, $(R_1 \cap R_2)^{-1} = R_1^{-1} \cap R_2^{-1}$, $(R_1 \setminus R_2)^{-1} = R_1^{-1} \setminus R_2^{-1}$.

定义 3.5.4: 复合

$R \times S = \{\langle x, z\rangle \in Dom(S) \times \mathrm{Im}(R) : \exists y(xSy \wedge yRz)\}$.

根据分出公理, 这是个集合,

$$\langle x, z\rangle \in R \circ S \Leftrightarrow \exists y(\langle x, y\rangle \in S \wedge \langle y, z\rangle \in R).$$

注: 类比在函数中, $f \circ g(x) = f(y) = z, y = g(x)$. 叔侄关系 $=$ 父子关系 $\circ$ 兄弟关系, 爷孙关系 $=$ 父子关系 $\circ$ 父子关系.

当 R, S 为关系时,

$$Dom(R \circ S) = \{x \in Dom(S) : \exists y \in Dom(R)(xSy)\}$$
$$Ran(R \circ S) = \{z \in Ran(R) : \exists y \in Ran(S)(yRz)\}.$$

定理 3.5.5

设 R, S, T 为关系, 则

$$(R \circ S)^{-1} = S^{-1} \circ R^{-1}, (R \circ S) \circ T = R \circ (S \circ T).$$

证明: 用外延性公理来证. (1) 两边元素都是有序对, 则

$$\langle x, y\rangle \in (R \circ S)^{-1} \Leftrightarrow \langle y, x\rangle \in (R \circ S) \Leftrightarrow \exists z(ySz \wedge zRx) \Leftrightarrow \exists z(zS^{-1}y \wedge xR^{-1}z) \Leftrightarrow \langle x, y\rangle = S^{-1} \circ R^{-1}.$$

(2) 同理

$$\begin{aligned}
\langle x, z\rangle \in (R \circ S) \circ T &\Leftrightarrow \exists y(xTy \wedge \langle y, z\rangle \in (R \circ S) \\
&\Leftrightarrow \exists y(xTy \wedge \exists w(ySw \wedge wRz)) \\
&\Leftrightarrow \exists y \exists w(xTy \wedge ySw \wedge wRz) \\
&\Leftrightarrow \exists w(\exists y(xTy \wedge ySw) \wedge wRz) \\
&\Leftrightarrow \exists w(\langle x, w\rangle \in S \circ T \wedge wRz) \\
&\Leftrightarrow \langle x, z\rangle \in R \circ (S \circ T).
\end{aligned}$$

3.5.1 映射或函数

定义 3.5.6

F 为**映射** (mapping) 或**函数** (function), 指 F 为关系, 且对 $x \in Dom(F)$, $\exists! y(xFy)$.

注: $\exists! x\varphi(x)$ 指 $\exists x(\varphi(x) \wedge \forall y(\varphi(y) \to y = x))$.

$x \in Dom(F)$ 且 $\langle x, y\rangle \in F$ 时, 把这唯一的 y 记为 $F(x)$, 叫函数 F 在 x 处的值. 当 $x \notin Dom(F)$ 时, 称 F 在 x 处无定义.

当 F 为函数时, $F(x) = \bigcup F[\{x\}]$.

例 3.5.7

$F = \{\langle 0, 1\rangle, \langle 1, 3\rangle, \langle 2, 1\rangle\}$ 为函数. $Dom(F) = \{0, 1, 2\}, F(0) = 1, F(1) = 3, F(2) = 1$.

当 f 与 g 为函数时, $\langle x, z\rangle \in f \circ g \Leftrightarrow \exists y(\langle x, y\rangle \in g \wedge \langle y, z\rangle \in f)$.

由于 $Dom(f\circ g)=\{x\in Dom(g):g(x)\in Dom(f)\}$, 则 $f\circ g$ 也是函数, 且 $x\in Dom(f\circ g)$ 时, $f\circ g(x)=f(g(x))$.

当 f,g 为映射时, $f\cap g$ 也是, 但 $f\cup g$ 不一定是. 但是当 $Dom(f)\cap Dom(g)=\varnothing$ 时, $f\cup g$ 也是函数.

定义 3.5.8

设 X,Y 为集合, 若 f 为映射, 且 $Dom(f)=X, Ran(f)\subseteq Y$, 则说 f **是 X 到 Y 中映射**, 记 $f:X\to Y$. 对于 $f:X\to Y$, 若

$$x_1\neq x_2\Rightarrow f(x_1)\neq f(x_2),$$

则称 f 是 X 到 Y 的**单射 (injective mapping)**, 如果 $Ran(f)=Y$, 即

$$\forall y\in Y\exists x\in X(f(x)=y),$$

则说 f 是 X 到 Y 的**满射 (surjective mapping)**. 若 $f:X\to Y$ 既是单射又是满射, 则说 f 是 X 到 Y 的**双射 (bijective)** 或**一一对应 (one to one correspondence)**.

$A\approx B(|A|=|B|)$ 指存在 A 到 B 的一一对应 f, $A\preccurlyeq B(|A|\leq|B|)$ 指存在 A 到 B 的单射.

定理 3.5.9

设 $A\approx C, B\approx D, A\cap B=C\cap D=\varnothing$, 则 $A\cup B\approx C\cup D$.

注: $A\cap B=\varnothing$ 时, $|A\cup B|$ 只依赖于 $|A|$ 与 $|B|$, 与 A,B 的选取无关. $|A\cup B|=|A|+|B|$. (选取无关指的是换与 A,B 等势的 C,D, $|\cdot|$ 不变.

当 $A\cap B\neq\varnothing$ 时, $\{0\}\times A\approx A, \{1\}\times B\approx B$, 则 $\{0\}\times A\cap\{1\}\times B=\varnothing$, 从而 $|A|+|B|=|\{0\}\times A\cup\{1\}\times B|$.

定理 3.5.10. 集合乘法

$A\approx C$, $B\approx D$, 则 $A\times B\approx C\times D$.

证明: 记 $f:A\to C, g:B\to D$, 定义 $h(\langle a,b\rangle)\triangleq\langle f(a),g(b)\rangle$ 即可.

注: 定理表明 $|A\times B|$ 只与 $|A|$ 与 $|B|$ 有关, 与 A,B 的选取无关. $|A|\cdot|B|\triangleq|A\times B|$. (基数的乘法). 若 $|A|=m, |B|=n$, 则 $|A\times B|=mn$.

定义 3.5.11: 集合乘方

定义 $B^A\triangleq\{f:A\to B\}=\{f\in\mathcal{P}(A\times B):f\text{为映射}\wedge Dom(f)=A\}$.

$f:A\to B\Rightarrow f\subseteq A\times B\Rightarrow f\in\mathcal{P}(A\times B)$. 用分出公理, B^A 是集合. $|A|=m, |B|=n$, 则 $|B^A|=n^m$.

定理 3.5.12

$A\approx C, B\approx D\Rightarrow B^A\approx D^C$.

证明: 设 $F:A\to C, G:B\to D$ 为一一映射, 要定义 $f\in B^A\longrightarrow\varphi(f)\in D^C$. 对 $f\in B^A$ 及 $c\in C, F^{-1}(c)\in A, f(F^{-1}(c))\in B, G(f(F^{-1}(c)))\in D$,

定义 $\varphi(f):C\to D$ 为 $\varphi(f)(c)=G\circ f\circ F^{-1}(c)$. 当 $f\in B^A$ 时, $\varphi(f)\in D^C$, 所以 φ 是从 B^A 到 D^C 的映射.

下证 φ 是单射. 若 $\varphi(f)=\varphi(f')$, $f,f'\in B^A$, 下证 $f=f'$. 当 $c\in C$ 时,

$$\begin{aligned}\varphi(f)(c)=\varphi(f')(c) &\Leftrightarrow G\circ f\circ F^{-1}(c)=G\circ f'\circ F^{-1}(c)\\ &\Rightarrow G\circ f\circ F^{-1}=G\circ f'\circ F^{-1}\\ &\Rightarrow G\circ f\circ F^{-1}\circ F=G\circ f'\circ F^{-1}\circ F\\ &\Rightarrow G\circ f=G\circ f'\\ &\Rightarrow G^{-1}\circ G\circ f=G^{-1}\circ G\circ f'\Rightarrow f'=f.\end{aligned}$$

下证 φ 是满射. 任给 $g\in D^C$, 要找 $f\in B^A$ 使得 $\varphi(f)=g$. 而 $G\circ f\circ F^{-1}=g\Rightarrow f=G^{-1}\circ g\circ F$, 若 $a\in A$, 则

$$F(a)\in C\Rightarrow g(F(a))\in D\Rightarrow G^{-1}(g(F(a)))\in B.$$

所以 $f:A\to B$. $\square$

注: $|B^A|$ 只依赖于 $|A|$ 与 $|B|$ 的选取, 与 A,B 的选取无关. $|B|^{|A|}\triangleq|B^A|$.

$\varnothing$ 是个函数 (空函数).

定理 3.5.13

下面命题成立:

(1)$A^{\varnothing}=\{\varnothing\}$;

(2)$A\neq\varnothing\Rightarrow\varnothing^A=\varnothing$;

(3)$A^B=\varnothing\Leftrightarrow A=\varnothing\wedge B\neq\varnothing$;

(4)$A^{\{x\}}=\{\{\langle x,y\rangle\}:y\in A\}$;

(5)$A\subseteq B\Rightarrow A^C\subseteq B^C$.

练习题 16.

1. 判断题:
   (1) **(2008 年)** 对任意集合 A,B,C 都有 $(A\times B)^C\approx A^C\times B^C$. ( )
   (2) **(2008 年)** 集合的等势 $\approx$ 是个等价关系. ( )
   (3) **(2012 年)** 如果 f,g 为映射, 则 $f\cap g$ 与 $f\cup g$ 都是映射. ( )
   (4) **(2022 年)**$A^{\varnothing}=\varnothing$. ( )
   (5) **(2022 年)**$\varnothing^{\varnothing}=\varnothing$. ( )
2. $B\cap C=\varnothing$ 时, $A^{B\cup C}\approx A^B\times A^C$.
3. **(2022 年)** 设 A,B,C 为集合. 对 $f\in(A^B)^C$, 让 $\sigma(f):B\times C\to A$ 如下给出:

$$\sigma(f)(\langle b,c\rangle)=f(c)(b).(b\in B,c\in C).$$

   (1) σ 是 $(A^B)^C$ 到 $A^{B\times C}$ 的单射.
   (2) σ 是 $(A^B)^C$ 到 $A^{B\times C}$ 的满射.
4. **(2022 年)** 设 R 为关系, 在 ZF 集合论中用分出公理证明有集合 A(叫 R 的值域), 使得

$$y\in A\Leftrightarrow\exists x(xRy).$$

§ 3.6 等价关系与序结构

定义 3.6.1: 自反

对 A 上关系 R, 称 R 在 A 上**自反 (reflective)**, 指 $\forall x \in A(xRx)$, 等价于 $I_A = \{\langle x, x\rangle : x \in A\} \subseteq R$. R 自反指 R 在 $A = Dom(R) \cup Ran(R)$ 上自反.

注: 当 R 自反时, $xRx, xRx \Rightarrow xR \circ Rx$, 故 $R \subseteq R \circ R$.

定义 3.6.2: 对称

对 A 上关系 R, 称 R 在 A 上**对称 (symmetric)**, 指 $\forall x \in A \forall y \in A(xRy \to yRx)$, R 对称指

$$\forall x \forall y(xRy \to yRx).$$

注: 当 R 自反时, 等价于 $R = R^{-1}$.

定义 3.6.3: 传递

对 A 上关系 R, 称 R 在 A 上**传递 (transitive)**, 指 $\forall x \in A \forall y \in A \forall z \in A((xRy \wedge yRz) \to xRz)$, R 传递指

$$\forall x \forall y \forall z((xRy \wedge yRz) \to xRz).$$

注: 当 R 传递时, 等价于 $R \circ R \subseteq R$.

定义 3.6.4: 反对称

R 反对称指 $\forall x \forall y((xRy \wedge yRx) \to x = y)$, 相当于 $x \neq y$ 时, xRy 与 yRx 不同时成立.

注: 当 R 反对称时, 等价于 $R \cap R^{-1} \subseteq I_A$. I_A 指 A 上的恒等映射.

定理 3.6.5

设诸 $R_i(i \in I)$ 均自反（对称、传递）, 则它们的交 $\bigcap\limits_{i\in I} R_i$ 也自反（对称、传递）, 即 $\bigcap\{R_i : i \in I\}$ 自反（对称、传递）.

证明: 设 $x \in Dom\left(\bigcap\limits_{i\in I} R_i\right)$, 则 $i \in I$ 时, $x \in Dom(R_i)$. 如果每个 R_i 自反, 则 xR_ix, 则 $\langle x, x\rangle \in R_i \Rightarrow \langle x, x\rangle \in \bigcap\limits_{i\in I} R_i$. 类似地 $Ran\left(\bigcap\limits_{i\in I} R_i\right)$ 的验证同理.

设诸 $R_i(i \in I)$ 对称, $\langle x, y\rangle \in \bigcap\limits_{i\in I} R_i$, 则当 $i \in I$ 时, $\langle x, y\rangle \in R_i \Rightarrow \langle y, x\rangle \in R_i$. 则 $\langle y, x\rangle \in \bigcap\limits_{i\in I} R_i$.

设诸 $R_i(i \in I)$ 传递, $\langle x, y\rangle, \langle y, z\rangle \in \bigcap\limits_{i\in I} R_i$, 则 $i \in I$ 时, xR_iy 且 yR_iz, 由传递性可知 xR_iz, 则 $\langle x, z\rangle \in \bigcap\limits_{i\in I} R_i$. □

定义 3.6.6

设 R 为 A 上关系, 则

$$r(R) = \bigcap_{R \subseteq R' \subseteq A\times A, \text{且 } R' \text{ 在 } A \text{ 上自反}} R'$$

是包含 R 的最小的 A 上的自反关系, 叫 R 在 A 上的**自反闭包**.

$$s(R) = \bigcap_{R \subseteq R' \subseteq A\times A, \text{且 } R' \text{ 在 } A \text{ 上对称}} R'$$

是包含 R 的最小的 A 上的对称关系, 叫 R 在 A 上的**对称闭包**.

$$t(R) = \bigcap_{R \subseteq R' \subseteq A\times A, \text{且 } R' \text{ 在 } A \text{ 上传递}} R'$$

是包含 R 的最小的 A 上的传递关系, 叫 R 在 A 上的**传递闭包**.

事实上, $s(R) = R \cup R^{-1}$, $t(R) = \bigcup\limits_{n=1}^{\infty} R^n$. 对于第二条的证明, 若 $R \subseteq t(R)$, 则 $R^2 = R \circ R \subseteq t(R) \circ t(R) \subseteq t(R)$, 这样下去可推出

$$\bigcup_{n=1}^{\infty} R_n \subseteq t(R).$$

只需再证 $\bigcup\limits_{n=1}^{\infty} R_n$ 有传递性: 设 $\langle x, y\rangle \in \bigcup\limits_{n=1}^{\infty} R_n$, $\langle y, z\rangle \in \bigcup\limits_{n=1}^{\infty} R_n$, 则有 $m, n \in \mathbb{N}^+$, 使得 $\langle x, y\rangle \in R^m$, $\langle y, z\rangle \in R^n$. 于是

$$\langle x, z\rangle \in R^n \circ R^m = R^{n+m} \subseteq \bigcup_{n=1}^{\infty} R_n.$$

定义 3.6.7

设 R 为 A 上关系, R 是 A 上**等价关系**指 (1)R 自反、(2)R 对称、(3)R 传递. R 为等价关系指 R 是 $A = Dom(R) \cup Ran(R)$ 上的等价关系.

定义 3.6.8

π 为集合 X 上的一个**分类 (partition)**, 指 $\pi \subseteq \mathcal{P}(X)$, 且满足

(1)$\forall A \in \pi(A \neq \varnothing)$, 即每块非空;

(2)$\forall A \in \pi \forall B \in \pi(A \neq B \to A \cap B = \varnothing)$, 即不同两块之间不交.

(3)$\bigcup \pi = \bigcup\limits_{A\in\pi} A = X$, 即这些块拼起来为整体.

注: 等价关系很重要, 它与分类一一对应, 见下面定理.

定理 3.6.9

设 X 为非空集, 则 $\{X \text{ 上分类 }\} \approx \{X \text{ 上等价关系 }\}$.

证明: (1) 设 π 为 X 上一个分类, 对 $x, y \in X$, 让 xRy 指 $\exists A \in \pi(x \in A \wedge y \in A)$. 证它为等价关系. 记 $R = \{\langle x, y\rangle \in X \times X : \exists A \in \pi(x \in A \wedge y \in A)\}$.

当 $x \in X$ 时, 有 $A \in \pi$ 使得 $x \in A$, 而 $x \in A \wedge y \in A \Rightarrow xRx$, 故 R 自反.

设 xRy, 则有 $A \in \pi$ 使得 $x, y \in A$, 从而 $y, x \in A$, 从而 yRx, 故 R 对称.

设 $xRy \wedge yRz$, 则有 $A \in \pi$ 使得 $x, y \in A$, 有 $B \in \pi$ 使得 $y, z \in B$. 从而 $y \in A$ 且 $y \in B$. 但是由分类的定义, 不同的集合无公共元素, 则 $A = B$, 从而 $x, z \in A, xRz$. 故 R 传递.

(2) 设 R 为 X 上等价关系, 对 $x \in X$, 记 $[x]_R = \{y \in X : xRy\}$ 为 x 所在的 R 的等价类. 下证 $\pi_R = \{[x]_R : x \in X\}$ 是 X 的一个分类 (重复的只算一次), 设 $x \in [x]_R$, 由于 xRx, 则

$$\bigcup_{x \in X} [x]_R \supseteq X = \bigcup_{x \in X} \{x\}.$$

故 $\bigcup\limits_{x \in X} [x]_R = X$. (验证了分类定义中的 (1)(3))

下证不同两块之间没有共同元素. 设 $z \in [x]_R \cap [y]_R$, 则 xRz 且 yRz. 由对称性, $xRz \wedge zRy$, 由传递性, xRy. 任给 $w \in X$, 当 xRw 时, $yRx \wedge xRw \Rightarrow yRw$, 而 yRw 时 $xRy \wedge yRw \Rightarrow xRw$, 故 $xRw \Leftrightarrow yRw$. 因此 $[x]_R = \{w \in X : xRw\} = \{w \in X : yRw\} = [y]_R$, 即 xRy 时 $[x]_R = [y]_R$. 故若 $[x]_R \neq [y]_R$, 就有 $[x]_R \cap [y]_R = \varnothing$.

由上, $\pi_R = \{[x]_R : x \in X\}$ 是 X 的一个分类. □

例 3.6.10

矩阵相似是等价关系. $A \sim B$ 指 $\exists P$ 可逆, $PAP^{-1} = B$.

例 3.6.11

$\mathbb{Z}$ 上模 m 同余关系为等价关系. $a \equiv b(\mod m)$ 即 $\exists q \in \mathbb{Z}(a - b = mq)$.

定义 3.6.12

设 $\leq$ 是集合 A 上二元关系, 若它满足

(1) 自反性: $\forall x \in A(x \leq x)$;

(2) 反对称: $\forall x \in A \forall y \in A((x \leq y \wedge y \leq x) \to x = y)$;

(3) 传递性: $\forall x \in A \forall y \in A \forall z \in A(x \leq y \leq z \to x \leq z)$.

则称 $\leq$ 为 A 上**半序**或**偏序 (partial order)**. 也说 A 按 $\leq$ 构成一个**半序结构**.

定义 3.6.13

如果 $\leq$ 为 A 上半序且还满足可比性, 即 $\forall x \in A \forall y \in A(x \leq y \vee y \leq x$, 则称 $\leq$ 为 A 上**全序**或**线性序 (linear ordering)**.

当 $\leq$ 为 A 上半序时, $x < y$ 指 $x \leq y \wedge x \neq y$, 它有如下性质:

(1)$\forall x \in A(x \not< x)$.

(2)$\forall x \in A \forall y \in A(x < y \to y \not< x)$.

(3)$\forall x \in A \forall y \in A \forall z \in A(x < y < z \to x < z)$.

例 3.6.14

设 X 为集合, $\mathcal{P}(X) = \{A : A \subseteq X\}$, 则被包含关系 $\subseteq$ 为集合 $\mathcal{P}(X)$ 上的半序.

若 $X = \{0, 1, 2, \cdots\}$, 则 $A_1 = \{0, 1\}$ 与 $A_2 = \{1, 2\}$ 不能互相被包含.

例 3.6.15

$\mathbb{N} = \{0, 1, 2\}$ 上 $\leq$（小于或等于）是个全序. $\mathbb{N}$ 上整除关系是个半序.

定义 3.6.16: 界

设 $\leq$ 为 A 上半序, $B \subseteq A$, $a \in A$. 如果 $\forall b \in B(b \leq a)$, 则称 a 为 B 的**上界**, 如果 $\forall b \in B(a \leq b)$, 则称 a 为 B 的**下界**. 如果 $a \in B$ 且 a 为 B 的上（下）界, 则称 a 是 B 的**最大（小）元**. 如果 $a \in B$ 且 $\forall b \in B(a \not< b)$, 则称 a 是 B 的**极大元**. 如果 $a \in B$ 且 $\forall b \in B(b \not< a)$, 则称 a 是 B 的**极小元**.

注: 若 B 有最大 (小) 元, 则最大 (小) 元唯一.
注: 若 a, b 都是 B 的最大元, 则 $a \leq b, b \leq a$. 由对称性, $a = b$.

定义 3.6.17: 确界

如果 a 为 B 的上界, 且当 a' 为 B 的上界时, $a \leq a'$, 则称 a 为 B 的**上确界**（最小的上界）, 记为 $\sup B$.

如果 a 为 B 的下界, 且当 a' 为 B 的下界时, $a' \leq a$, 则称 a 为 B 的**下确界**（最大的下界）, 记为 $\sup B$.

定义 3.6.18: Hasse 示意图

设 $\leq$ 是有限集 X 上的半序. 把 X 中元画成平面上的点, $x < y$ 时把 y 画到 x 的上方, 且画条 x 到 y 的连线. 当 $x < y < z$ 时, 不画 y 到 z 的连线. 这样所得的图叫做 **Hasse 示意图**.

(下面两个例子中请自行画 Hasse 示意图)

例 3.6.19

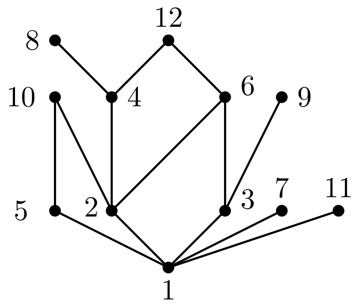
$X = \{0, 1, 2\}$ 时, $\mathcal{P}(X)$ 依 $\subseteq$ 构成半序集.

$\varnothing$ 是 X 的最小元, $\{0, 1, 2\}$ 是 X 的最大元; $\varnothing$ 是 X 的下确界, $\{0, 1, 2\}$ 是 X 的上确界.

例 3.6.20

$X = \{1, 2, \cdots, 12\}$ 依整除关系构成半序集.

7,8,9,10,11,12 是极大元, 1 为极小元也是最小元.



定义 3.6.21: 良序

设 $\leq$ 是非空集 X 上半序, 若 X 的每个非空子集有关于序 $\leq$ 的最小元, 则称 $\leq$ 为 X 上的**良序 (well ordering)**.

注: 良序必为线性序. 因为 $x, y \in X$ 时, $\{x, y\}$ 有最小元, 则 $x \leq y$ 或 $y \leq x$. $\leq$(实数下) 是线性序, 但不是良序.

定理 3.6.22. Zorn 引理

设 X 为非空半序集, 若 X 的每个全序子集（称为**链** (chain)）在 X 中有上确界, 则 X 必有极大元.

设 $\mathscr{A}$ 为集合, 且对每个依被包含关系的链 $\mathscr{B} \subseteq \mathscr{A}$, 都有 $\bigcup \mathscr{B} \in \mathscr{A}$, 则 $\mathscr{A}$ 中有依被包含关系的极大元 M.

练习题 17.

1. 判断题:
   (1) **(2022 年)** 集合间比较势大小的 $\preccurlyeq$ 是半序. ( )
   (2) **(2010 年)** 集合的等势 $\approx$ 是个等价关系. ( )
   (3) **(2022 年)** 设 R 为关系. 则 R是等价关系 $\Leftrightarrow R^{-1} \circ R = R$. ( )
   (4) **(2022 年)** 有理数集 $\mathbb{Q}$ 上 $\leq$(小于或等于) 是良序. ( )
   (5) **(2008 年)** 实数集 $\mathbb{R}$ 上 $\leq$(小于或等于) 是良序. ( )
2. 如果 $\leq$ 为集合 W 上的良序, 证明不存在序列 $\{a_n\}_{n\in\mathbb{N}} \subset W$ 使得 $a_0 > a_1 > a_2 > \cdots$.
3. **(2012 年)** 设 $\leq$ 为非空集合 A 上线性序, 且对任何一阶公式 $\varphi(x)$ 都有

$$\forall a \in A(\forall x \in A(x < a \to \varphi(x)) \to \varphi(a)) \to \forall x \in A(\varphi(x)).$$

   证明 A 的每个非空子集必有最小元.

§ 3.7 集合的等势、选择公理与连续统假设

$X \approx Y$ 指有 X 到 Y 的双射 f.

既然 $X \approx_{Id} X$, 且 $X \approx_f Y \approx_g Z \Rightarrow X \approx_{g \circ f} Z$, 且 $X \approx_f Y \Rightarrow Y \approx_{f^{-1}} X$. 但如果 $\approx$ 是个关系, 则 $\langle x, x\rangle \in \approx$. 从而每个集合在 $\approx$ 的定义域里, 从而 $\approx$ 由所有集合构成. 但所有集合不构成集合, 故 $\approx$ **不是关系**, 自然不是等价关系. (关系是个集合!!)

$X \leq Y$ 指存在 X 到 Y 的单射 f, $|X| \leq |Y|$. 这相当于 X 与 Y 的一个子集等势.

$\preccurlyeq$ **不是关系, 也不是半序**. 但是满足:

(1)$X \preccurlyeq X$(显然)

(2)$X \preccurlyeq Y \preccurlyeq Z \Rightarrow X \preccurlyeq Z$(显然)

(3) 是否有 $A \preccurlyeq B \preccurlyeq A \Rightarrow A \approx B$? Cantor 提出了猜想, 后来 Schröder 与 Bernstein 在 1890 年代同时独立证明.

定理 3.7.1. Schröder-Bernstein

$A \preccurlyeq B \preccurlyeq A \Rightarrow A \approx B$.

证明: (Fraenkel, 1954) 设 $A \approx_f B_0 \subseteq B, B \approx_g A_0 \subseteq A$. 令

$$\mathscr{C} = \{C \subseteq A : C \cup g\lceil B \setminus f\lceil C]] = \varnothing\}.$$

当 $C \in \mathscr{C}$ 时,

$$\begin{aligned} C \subseteq \bigcup \mathscr{C} \subseteq A \Rightarrow & f\lceil C] \subseteq f\lceil \bigcup \mathscr{C}] \\ \Rightarrow & B \setminus f\lceil C] \supseteq B \setminus f\lceil \bigcup \mathscr{C}] \\ \Rightarrow & g\lceil B \setminus f\lceil C]] \supseteq g\lceil B \setminus f\lceil \bigcup \mathscr{C}]]. \end{aligned}$$

因为 $C \cap g\lceil B \setminus f\lceil C]] = \varnothing$, 则 $C \cap g\lceil B \setminus f\lceil \bigcup C]] = \varnothing$. 则 $C \subseteq A \setminus g\lceil B \setminus f\lceil \bigcup C]] = \varnothing \triangleq D$. 这样,

$$\begin{aligned} \text{①} \quad \bigcup_{c \in \mathscr{C}} C = \bigcup \mathscr{C} \subseteq D \Rightarrow & f\lceil \bigcup \mathscr{C}] \subseteq f\lceil D] \\ \Rightarrow & B \setminus f\lceil \bigcup \mathscr{C}] \supseteq B \setminus f\lceil D] \\ \Rightarrow & g\lceil B \setminus f\lceil \bigcup \mathscr{C}]] \supseteq g\lceil B \setminus f\lceil D]]. \end{aligned}$$

即

$$A \setminus D \supseteq g\lceil B \setminus f\lceil D]] \Rightarrow g\lceil B \setminus f\lceil D]] \cap D = \varnothing \Rightarrow D \in \mathscr{C} \Rightarrow D \subseteq \bigcup \mathscr{C}. \quad \text{②}$$

由①②, $D = \bigcup \mathscr{C}$, 则 $\mathscr{C}$ 中依被包含关系中 D 为最大元. 则 $A \setminus D = g\lceil B \setminus f\lceil D]]$, 把 A 分为两块. 让 $h = (f\lceil D) \cup (g\lceil (A \setminus D))$, 则定义域没有相同元, $A \approx_h b$. □

记 $0 = \varnothing, 1 = \{0\}, 2 = \{0, 1\}$.

定理 3.7.2

$\mathcal{P}(X) \approx 2^X$, 从而 $|\mathcal{P}(X)| = 2^{|X|}$.

证明: $2^X = \{\text{映射} f : X \to 2 = \{0, 1\}\}$. 对于 $A \in \mathcal{P}(X)$, 让 $\chi_A(x) = \begin{cases} 1, & x \in A, \\ 0, & x \notin A. \end{cases}$ 为 A 的特征函数, 定义 $\chi : \mathcal{P}(X) \to 2^X$ 如下: $\chi(A) = \chi_A$.

验证 χ 为单射: 若 $A, B \in \mathcal{P}(X)$, 则

$$\chi(A)=\chi(B) \Rightarrow \chi_A=\chi_B \Rightarrow A=\{x\in X:\chi_A(x)=1\}=\{x\in X:\chi_B(x)=1\}=B.$$

验证 χ 为满射: 任给 $f\in 2^X$, f 是 X 到 $2=\{0,1\}$ 的映射. 让 $A=\{x\in X: f(x)=1\}$. 则 $x\in X$ 时, $f(x)=1 \Leftrightarrow x\in A \Leftrightarrow \chi_A(x)=1$. 故 $f:\chi_A=\chi(A)\in Ran(\chi)$. 则 χ 是 $\mathcal{P}(X)$ 到 2^X 的满射.

从而 χ 是双射, $|\mathcal{P}(X)|=2^{|X|}$. □

定理 3.7.3

$\mathbb{R}\approx\mathcal{P}(\mathbb{N})\approx 2^{\mathbb{N}}$. 从而 $\aleph=2^{\aleph_0}$.

证明: $\mathbb{R}\approx[0,1)$, 而 $x\in[0,1)$ 可唯一表成二进制形式:

$$0.x_0x_1x_2\cdots, x_i\in\{0,1\}$$

且没有 N 使 $x_N=x_{N+1}=\cdots=1$. (为了唯一起见, 后面不可以全为 1, 如 $0.100111\cdots=0.101$)

下证 $[0,1)\approx 2^{\mathbb{N}}\backslash$ 可数集. (某项以后全是 1 的数可数!) 取 $f\in 2^{\mathbb{N}}, f:\mathbb{N}\to\{0,1\}$. 则 $\mathbb{R}\approx\mathbb{R}\cup$ 可数集 $\approx 2^{\mathbb{N}}$. □

注: (1)$\mathbb{N}\times\mathbb{N}$ 可数, 相当于可数个可数集并起来还是可数.

数法: 横坐标 + 纵坐标小的先数, 故 $\aleph_0\cdot\aleph_0=\aleph_0$. 而 $\aleph=|\mathbb{R}|=2^{\aleph_0}>\aleph_0$.

注: (2)$\aleph_0^{\aleph_0}=\aleph$, 这是因为由前一个注以及上面定理有: $2^{\aleph_0}\le\aleph_0^{\aleph_0}\le(2^{\aleph_0})^{\aleph_0}=2^{\aleph_0}$,

Cantor 连续统假设: 无集合 X 使得 $\mathbb{N}\prec X\prec\mathbb{R}$, 即 $\aleph_0<|X|<\aleph$.

广义连续统假设任给无穷集 A, 无集合 X 使 $A\prec X\prec\mathcal{P}(A)$, 即 $|A|<|X|<|\mathcal{P}(A)|=2^{|A|}$.

公理 3.6: 选择公理 (axiom of choice)

$$(X\neq\varnothing\wedge\forall x(x\neq\varnothing)\wedge\forall x\in X\forall y\in X(x\neq y\to x\cap y=\varnothing)\to(\exists Y\subseteq\bigcup X\forall x\in X\exists! y\in x(y\in Y)).$$

即, 有一个定义域为 X 的函数 $f(x)$ 使得 $\forall x\in X(f(x)\in x)$. $f=\{\langle x,y\rangle: x\in X\}, f(x)=y\in x$.

例 3.7.4

设 R 为关系, $Dom(R)=X, Ran(R)\subseteq Y$, 用选择公理证明: 存在映射 $F:X\to Y$ 使得 $F\subseteq R$.

证明: 对每个 $x\in X, Y_x=\{y\in Y: xRy\}\neq\varnothing$. 则 $\{\{x\}\times Y_x: x\in X\}$ 都两两不交, 即 $\{x\}\times Y_x\cap\{x'\}\times Y_{x'}\neq\varnothing\Rightarrow x=x'$. 对集合 $\{\{x\}\times Y_x: x\in X\}$ 用选择公理, $F=\{\langle x,y_x\rangle: x\in X\}$ 为函数, 则 $F\subseteq R(y_x\in Y_x)$. □

注: 任一无穷集合都有可数子集.

选择公理的等价形式:

(1)(Zermelo) 任一非空集都有个良序.

(2)Zorn 引理

(3)(三分律) 任给集合 A, B, 则 $A\prec B$ 或 $B\prec A$ 或 $A\approx B$.

(4) 群的真子群必包含于一个极大真子群中.

(5) 环的真理想必包含于一个极大真理想中.

进一步发展:

1924 年, Banach, Tarski 提出分球怪论.

1935 年, Gödel 证明了 ZF 相容 $\Rightarrow$ ZF+AC 相容, 且证明了 ZF 相容 $\Rightarrow$ ZF+GCH 相容.

1963 年, Cohen(拿了 2004Fields 奖) ZF 相容 $\Rightarrow$ ZF+$\neg$AC 相容, 且证明了 ZF 相容 $\Rightarrow$ZF+$\neg$GCH 相容.

1988 年, Laczkovich $\cdots$

练习题 18.

1. 判断题:
   (1) **(2022 年)** 集合 X 为无穷集当且仅当它有个与之等势的真子集. (　)
   (2) **(2012 年)** 由全体从实数集 $\mathbb{R}$ 到 $\mathbb{R}$ 的连续函数构成的集合的基数为 $\aleph$. (　)
   (3) **(2022 年)** 自然数集 $\mathbb{N}$ 到 $\mathbb{N}$ 的映射共有 $\aleph_0$ 个. (　)
2. 设映射 $f : X \to Y, g : Y \to X$ 满足 $g \circ f = I_X, f \circ g = I_Y$. 证明 f 是 X 到 Y 的双射, 且 $f^{-1} = g$.
3. **(2012 年)** 对集合 X 证明 $|X| < |\mathcal{P}(X)|$, 其中 $\mathcal{P}(X)$ 为 X 的幂集.
4. **(2012 年)** 集合 S 由所有从有理数集 $\mathbb{Q}$ 到自身的映射构成, 求 S 的基数.
5. 对于集合 X, 证明幂集 $\mathcal{P}(X)$ 与 $2^X = \{\text{映射} f : X \to \{0,1\}\}$ 等势.

§ 3.8 无穷公理与自然数系统

定义 3.8.1

对集合 x, x 的**后继 (successor)** 指 $x' = x \cup \{x\}$. 集合 A 为**归纳集**指

$$0 = \varnothing \in A \wedge \forall x \in A(x' \in A).$$

公理 3.7: 无穷公理

存在一个归纳集. 即

$$\exists A(0 \in A \wedge \forall a \in A(a' \in A)).$$

定义 3.8.2

属于每个归纳集的集合叫**自然数**. 设 X 为归纳集, 则

$$\{x \in X : \forall A(A\text{为归纳集} \to x \in A)\} = \mathbb{N}.$$

定理 3.8.3

自然数集 $\mathbb{N}$ 是最小的归纳集.

证明: 根据分出公理, $A = \{n \in \mathbb{N} : \varphi(n)\}$ 是个集合 (定义). 故 $\mathbb{N} \subseteq A$. 再证 $\mathbb{N}$ 为归纳集. 0 属于每个归纳集, 故 $0 \in \mathbb{N}$. 若 $n \in \mathbb{N}$, 则对任何归纳集 $A, n \in A$. 从而 $n' \in A$, 从而 $n' \in \mathbb{N}$. 因此 $\mathbb{N}$ 为归纳集. □

定理 3.8.4. 数学归纳法

设 $\varphi(0)$ 成立, $\forall n \in \mathbb{N}(\varphi(n) \to \varphi(n'))$, 则 $\forall n \in \mathbb{N}\varphi(n)$ 对. 这儿 φ 为一阶公式.

证明: 依分出公理, $A = \{n \in \mathbb{N} : \varphi(n)\}$ 是个集合, $A \subseteq \mathbb{N}$, 因为 $\varphi(0)$ 成立, $0 \in A$, 若 $n \in A$, 则 $n \in \mathbb{N}$ 且 $\varphi(n)$ 成立, 从而 $\varphi(n')$ 成立. 而 $n' \in \mathbb{N}$, 则 $n' \in A$, 故 A 为归纳集. 根据定理 3.8.3, A 包含自然数集, 则 $\mathbb{N} \subseteq A \subseteq \mathbb{N}$, 故 $A = \mathbb{N}$. 即 $\forall n \in \mathbb{N}, \varphi(n)$ 成立. □

定理 3.8.5

$\forall n \in \mathbb{N}(n \neq 0 \to \exists m \in \mathbb{N}(m' = n))$. (若 $n \neq 0$, 它是某元素的后继)

证明: 让 $\varphi(n)$ 表示 $n \neq 0 \to \exists m \in \mathbb{N}(m' = n)$, 则 $\varphi(0)$ 成立. 若 $n \in \mathbb{N}$ 且 $\varphi(n)$ 成立, 则 $\varphi(n')$ 也对. (n' 为 n 的后继, 取上面的 $m = n$ 即可) 根据定理 3.8.4(数学归纳法), $\forall n \in \mathbb{N}\varphi(n)$ 也对. □

注: $0 = \varnothing, 1 = 0' = 0 \cup \{0\}, 2 = 1' = 1 \cup \{1\} = \{0, 1\}, 3 = 2' = 2 \cup \{2\} = \{0, 1, 2\}$.

用 $\underline{\in}$ 表示属于或等于.

定理 3.8.6

对 $m, n \in \mathbb{N}$, $m \underline{\in} n \Leftrightarrow m \subseteq n$.

证明: "$\Rightarrow$" 先对 n 归纳. $m \underline{\in} 0 \Rightarrow m = 0 \subseteq m \subseteq 0$.

设已经有 $m \underline{\in} n \Rightarrow m \subseteq n$, 今设 $m \underline{\in} n' = n \cup \{n\}$, 如果 $m \in n' = n \cup \{n\}$, 则 $m = n$ 或 $m \in n$, 即 $m \underline{\in} n$, 根据归纳假设, $m \subseteq n \subseteq n'$. 如果 $m = n'$, 则 $m \subseteq n'$. 用数学归纳法证完.

"$\Leftarrow$" 对 n 归纳. $m \subseteq 0 \Rightarrow m = 0 \Rightarrow m \underline{\in} 0$.

设已有 $m \subseteq n \Rightarrow m \underline{\in} n$, 现在设 $m \subseteq n' = n \cup \{n\}$, 如果 $m \subseteq n$, 由归纳假设,

$$m \underline{\in} n \Rightarrow m \in \{n\} \cup n = n'.$$

下设 $m \nsubseteq n$, 则 m 有个元素在 $\{n\}$ 里, 则 $n \in m$. 由"$\Rightarrow$"方向可知, $n \underline{\in} m \Rightarrow n \subseteq m$. 于是 $n' = n \cup \{n\} \subseteq m \subseteq n'$, 故 $m = n'$, 故 $m \underline{\in} n'$. □

推论 3.8.7

$\forall n \in \mathbb{N}(n \notin n)$, 即 $\forall n \in \mathbb{N}(n \neq n')$.

证明: 对 n 归纳证 $n \neq n'$. $0' = 0 \cup \{0\} = \{0\} \neq \varnothing = 0$. 设 $n \neq n'$, 下证 $n' \neq n''$.

(反证) 若 $n' = n'' = n' \cup \{n'\}$, 则 $n' \in n' = n \cup \{n\}$. 而 $n' \neq n$, 故 $n' \in n$.

根据定理 3.8.6, $n' \subseteq n \subseteq n' = n \cup \{n\}$. 故 $n = n'$, 与归纳假设矛盾. □

注: "即"后面是因为 $n' = n \subseteq \{n\} = n \Leftrightarrow n \in n$.

定理 3.8.8

对 $m, n \in \mathbb{N}$, $m' = n' \Rightarrow m = n$.

证明: 设 $m' = n'$ 但 $m \neq n$, 则 $m \in m'(= m \cup \{m\}) = n' = n \cup \{n\}$. 根据定理 3.8.6, 从而有 $m \subseteq n$.

类似地, $n \in n' = m' = m \cup \{m\} \Rightarrow n \in m$. 根据定理 3.8.6, $n \subseteq m$, 因而 $m = n$. 矛盾. □

定理 3.8.9

任给 $m, n \in \mathbb{N}$, 下述三者中恰有一个成立: $m \in n, m = n, n \in m$.

证明: 根据定理 3.8.7, $n \notin n$, 则 $m \in n$ 与 $m = n$ 不同时成立, 且 $n \in m$ 与 $n = m$ 不同时成立.

如果 $m \in n$ 且 $n \in m$, 由定理 3.8.6得 $m \subseteq n \subseteq m$, 从而 $m = n$, 与 $n \notin n$ 矛盾. (从而三者至多只有一个成立)

下证恰有一个成立. 对 m 归纳证 $m \in n \vee m = n \vee n \in m$. 由 $0 \subseteq n$, 则 $0 \in n$ 或 $0 = n$.

记 $\varphi(m) \triangleq \forall n \in \mathbb{N}(m \in n \vee m = n \vee n \in m)$.

若 $\varphi(m)$ 成立, 下证 $\varphi(m')$ 成立, 即 $\forall n \in \mathbb{N}(n \in m' \vee n = m' \vee m' \in n)$.

根据定理 3.8.6, $0 \subseteq m' \Rightarrow 0 \underline{\in} m'$ 成立. 由定理 3.8.5(非 0 自然数形如 n'), 若 $m = n$, 则 $m' = n'$.

若 $m \in n$, 则 $m \subseteq n \subseteq n'$, $\{m\} \subseteq n \subseteq n'$, 则 $m' = \{m\} \cup m \subseteq n'$.

若 $n \in m$, 则 $n \subseteq m \subseteq m'$, $\{n\} \subseteq m \subseteq m'$, 则 $n' \subseteq m'$. 由归纳假设, $\varphi(m)$ 成立. □

定理 3.8.10

$\underline{\in}$（$\subseteq$）是 $\mathbb{N}$ 上良序.

证明: 由定理 3.8.9(可比性), 以及 $\subseteq$(等价于 $\underline{\in}$, 定理 3.8.6) 是 $\mathbb{N}$ 上半序. 所以 $\underline{\in}$ 是 $\mathbb{N}$ 上良序. 再证 $\mathbb{N}$ 的每个非空子集 A 必有最小元. 对 n 归纳. 设 A 无最小元, 则 $0 \notin A$, 不然 0 为 A 最小元. 让 $\varphi(n)$ 表示 $\forall m \leq n(m \notin A)$, 则 $\varphi(0)$ 对.

(反证) 设 $\varphi(n)$ 成立但 $\varphi(n')$ 不成立, 则 $n' \in A$. 而 A 无最小元, 则 n' 不是最小元, 必有更小的 $m \in A$ 使得 $m < n'$, 于是 $m \in n \cup \{n\} \Leftrightarrow m \underline{\in} n$, 即 $m \leq n$. 由归纳假设 $m \notin A$. 因 $\varphi(n)$ 成立, 则 $m \notin A$, 矛盾.

故对每个 $n \in \mathbb{N}$ 都有 $\forall m \leq n(m \notin A)$. 特别地 $n \notin A$ 与 $A \neq \varnothing$ 矛盾. □

3.8.1 Peano 算术公理系统

1889 年, Peano 把算术公理化（摆开集合论）, 得到 Peano 算术公理系统.

(1) 有个特殊的自然数 0;

(2)n 是自然数 $\Rightarrow n'$(n 的后继) 也是自然数.

(3)$0 \neq n'$. (0 非后继)

(4)$m \neq n \Rightarrow m' \neq n'$. (后继映射是单射)

(5)(数学归纳法) 若 $\varphi(0)$ 成立且 $\varphi(n) \to \varphi(n')$, 则对所有 $n \in \mathbb{N}$, 有 $\varphi(n)$.

ZF 系统中定义的自然数 $0 = \varnothing, n' = n \cup \{n\}$ 满足 Peano 的 5 条公理. （数论是集合论的一部分）

下面可用 Peano 5 条公理发展算术. 在 Peano 算术中定义加、乘、乘方如下:

(1)$m + 0 = m, m + n' = (m+n)'$,

(2)$m0 = 0, mn' = mn + m$,

(3)$m^0 = 1, m^{n'} = m^n m$.

定理 3.8.11

对 $k, m, n \in \mathbb{N}$, 有

(1) 加法结合律: $(k+m)+n = k+(m+n)$;

(2) 加法交换律: $m+n = n+m$;

(3) 乘法分配律: $k(m+n) = km+kn$;

(4) 乘法交换律: $mn = nm$;

(5) 乘法结合律: $(km)n = k(mn)$;

(6) 消去律: $k+m = k+n \Rightarrow m = n; km = kn \Rightarrow k = 0 \vee (m = n)$.

证明: (1) 对 n 归纳. $(k+m)+0 = k+m = k+(m+0)$. 假设 $(k+m)+n = k+(m+n)$, 则 $(k+m)+n' = ((k+m)+n)'$(加法定义). 由归纳假设, $(k+(m+n))' = k+(m+n)' = k+(m+n')$.

(2)-(6) 留作习题 (**作业**). 注意要证 $0+m = m$. □

Peano 算术中 $\leq$ 如下定义: $m \leq n$ 指 $\exists d \in \mathbb{N}(m+d = n)$.

定理 3.8.12

Peano 算术中 $\leq$ 为 $\mathbb{N}$ 上的半序.

证明: (1) 自反性: $n+0 = n$, 故 $n \leq n$.

(2) 反称性:

$$\begin{aligned} & m \leq n \wedge n \leq m \\ \Rightarrow & \exists d_1, d_2 \in \mathbb{N}(m+d_1 = n, n+d_2 = m) \\ \Rightarrow & m+(d_1+d_2) = (m+d_1)+d_2 = n+d_2 = m = m+0 \\ \Rightarrow & d_1+d_2 = 0.(\text{消去律}) \end{aligned}$$

如果 $d_2 \neq 0$, 则有 $d \in \mathbb{N}$ 使得 $d_2 = d'$(**重要处理方法**!!!!!!!!) 于是 $d_1+d_2 = d_1+d' = (d_1+d)' \neq 0$, 与 $d_1+d_2 = 0$ 矛盾. 故 $d_2 = 0$, $d_1+0 = 0+0 \Rightarrow d_1 = 0$(消去律), 则 $m = n$.

(3) 传递性: 设 $k \leq m \leq n$, 则有 $d_1, d_2 \in \mathbb{N}$, 使得 $k+d_1 = m, m+d_2 = n$. 于是 $k+(d_1+d_2) = (k+d_1)+d_2 = m+d_2 = n$, 则 $k \leq n$. □

定理 3.8.13

在 ZF 集合论中, 对 $m, n \in \mathbb{N}$ 有 $m \leq n \Leftrightarrow m \underline{\in} n \Leftrightarrow m \subseteq n$.

证明: 只需证第一个 $\Leftrightarrow$.(第二个已证).

(1) 对 n 归纳证 $m\underline{\in} \Leftrightarrow m \leq n$. 当 $n=0$ 时, $m\underline{\in}0 \Rightarrow m=\varnothing=0 \leq n$. (在作业中已经证 $0+n=n$)

设 $m\underline{\in}n \Rightarrow m \leq n$ 成立, 则 $m=n' \Rightarrow m \leq n'$ ①, 且 $m \in n' \Rightarrow m \in n \cup \{n\} \Rightarrow m\underline{\in}n$. 由归纳假设, $m \leq n \leq n'$ ②. 由①②可知 $m \leq n'$, 归纳证完.

(2) 下证 $m \leq n \Rightarrow m\underline{\in}n$, (反证) 设 $m \leq n$ 但 $m\underline{\notin}n$, 从而由定理 3.8.9, $n \in m$. 由 (1), $n \leq m$. 利用 $\leq$ 反对称性可知 $m=n$, 与 $n \notin n$ 矛盾. □

注: $\underline{\in}$ 是个良序, 则定理表明 $\leq$ 也是个良序.

练习题 19.

1. **(2022 年)** 判断题: ZF 集合论中任何自然数都不属于它自己. ( )
2. **(2022 年)** 在 Peano 算术 (撇开 ZF 集合论中对自然数的定义) 中对 $m, n \in \mathbb{N}$, $m \leq n$ 指 $\exists d \in \mathbb{N}(m+d=n)$, 证明 $k, m, n \in \mathbb{N}$ 时总有 $k+m \leq k+n \Leftrightarrow m \leq n$.

§ 3.9 整数、有理数、实数、复数的构造

3.9.1 用加法定义减法

在 $\mathbb{N}\times\mathbb{N}$ 上定义**差等价** $\sim$ 如下: $\langle k,l\rangle\sim\langle m,n\rangle$ 指 $k+n=l+m$. 下面验证这是个等价关系.

(1) 自反性: 由加法交换律可得 $\langle m,n\rangle\sim\langle m,n\rangle$.

(2) 对称性: $\langle k,l\rangle\sim\langle m,n\rangle$ 即 $k+n=l+m$, 由加法交换律, $m+l=n+k$, 所以 $\langle m,n\rangle\sim\langle k,l\rangle$.

(3) 传递性: $\langle k,l\rangle\sim\langle m,n\rangle\sim\langle p,q\rangle$, 则 $k+n=l+m, m+q=n+p$, 则 $k+n+m+q=l+m+n+p$, 由交换律、结合律、消去律可得 $k+q=l+p$, 即 $\langle k,l\rangle\sim\langle p,q\rangle$.

3.9.2 整数

$\langle m,n\rangle$ 所在的等价类记为 $[\langle m,n\rangle]$, 把它叫做**整数**. $\mathbb{Z}=\{[\langle m,n\rangle]:m,n\in\mathbb{N}\}=\mathbb{N}\times\mathbb{N}/\sim$. (这个符号表示 $\mathbb{N}\times\mathbb{N}$ 关于差等价 $\sim$ 构成的集合)

在 $\mathbb{Z}$ 上定义加乘法如下:

$$[\langle k,l\rangle]+[\langle m,n\rangle]\triangleq[\langle k+m,l+n\rangle]$$
$$[\langle k,l\rangle]\cdot[\langle m,n\rangle]\triangleq[\langle km+ln,kn+lm\rangle]$$

该定义合理 (指换不同的代表元也一样), 证明留作习题.

$n\in\mathbb{N}$ 对应于 $n_{\mathbb{Z}}=[\langle n,0\rangle]$, 所以 $\mathbb{N}\subseteq\mathbb{Z}$.

让 $-n_{\mathbb{Z}}=[\langle 0,n\rangle]$, 则

$$n_{\mathbb{Z}}+(-n_{\mathbb{Z}})=[\langle n,n\rangle]=[\langle 0,0\rangle]=0_{\mathbb{Z}}$$
$$n+[\langle k,l\rangle]\triangleq[\langle n,0\rangle]+[\langle k,l\rangle]=[\langle n+k,l\rangle],$$

当 $m,n\in\mathbb{N}$ 时, $m_{\mathbb{Z}}+(-n_{\mathbb{Z}})=[\langle m,0\rangle]+[\langle 0,n\rangle]=[\langle m,n\rangle]$.

3.9.3 有理数

让 $\mathbb{Z}^*=\mathbb{Z}\setminus\{0\}$, 在 $\mathbb{Z}\times\mathbb{Z}^*$ 上定义**商等价** $\sim$ 如下: $\langle a,b\rangle\sim\langle c,d\rangle$ 指 $ad=bc$. 可以证 $\sim$ 是 $\mathbb{Z}\times\mathbb{Z}^*$ 上的等价关系.

把 $\langle a,b\rangle$ 所在的等价类记为 $\dfrac{a}{b}$, 叫**有理数**. $\dfrac{a}{b}=\dfrac{c}{d}\Leftrightarrow\langle a,b\rangle\sim\langle c,d\rangle$. 定义

$$\mathbb{Q}=\mathbb{Z}\times\mathbb{Z}^*/\sim=\left\{\frac{a}{b}:a\in\mathbb{Z},b\in\mathbb{Z}^*\right\}.$$

定义 $\dfrac{a}{b}+\dfrac{c}{d}=\dfrac{ad+bc}{bd},\dfrac{a}{b}\cdot\dfrac{c}{d}=\dfrac{ac}{bd}$, 易证它们定义合理（换代表元仍一样）.

由于整数 a 对应于有理数 $\dfrac{a}{1}$, 所以 $\mathbb{Z}\subseteq\mathbb{Q}$. 当 $a,b\in\mathbb{Z}^*$ 时, 有逆元: $\dfrac{a}{b}\cdot\dfrac{b}{a}=\dfrac{ab}{ba}=\dfrac{1}{1}=1_{\mathbb{Q}}$.

3.9.4 实数

(1)Cantor 构造方法：实数相当于收敛有理数列的极限. 有理数列 $x_0,x_1,x_2,\cdots$ 相当于函数 $s(n)=x_n, s:\mathbb{N}\to\mathbb{Q}$.

函数 $s(n)=x_n$ 为 Cauchy 列, 指

$$\forall\varepsilon\in\mathbb{Q}\exists N\in\mathbb{N}\forall m\geq N\forall n\geq N(|s(m)-s(n)|<\varepsilon).$$

Cauchy 列 r 与 s 等价, 指

$$\forall\varepsilon\in\mathbb{Q}\exists N\in\mathbb{N}\forall n\geq N(|r(n)-s(n)|<\varepsilon).$$

Cauchy 列 s 所在的等价类记为 $\lim\limits_{n\to\infty}s(n)$, 叫**实数**. $r\sim s\Rightarrow\lim\limits_{n\to\infty}r(n)=\lim\limits_{n\to\infty}s(n)$.

(2)Dedekind 分割构造: 指 $\mathbb{Q}$ 的一个子集 x 满足: ① $\varnothing \neq x \neq \mathbb{Q}$; ②向下封闭, 即 $r < q \in x$ 且 $r \in \mathbb{Q} \Rightarrow r \in x$. ③ x 无最大元. 满足上面三个条件的 x 叫 **Dedekind 分割**.

Dedekind 把 Dedekind 分割看作实数, $\mathbb{R}$ 为实数集. $x \leq_{\mathbb{R}} y$ 指 $x \subseteq y$. 如果 $x = (-\infty, \alpha) \cap \mathbb{Q}, y = (-\infty, \beta) \cap \mathbb{Q}$, 则定义 $x + y \triangleq (-\infty, \alpha + \beta) \cap \mathbb{Q}$, $x +_{\mathbb{R}} y = \{r + s : r \in x, s \in y\}$. 定义 $-x \triangleq \{r \in \mathbb{Q} : \exists s \in \mathbb{Q}(s > r \wedge -s \notin x)\}$(可画图辅助理解). 定义 $|x| \triangleq x \cup -x$.

定理 3.9.1. 上确界原理

实数集的每个有上界的非空子集 A 必在 $\mathbb{R}$ 中有上确界.

只需证 $\bigcap A = \bigcap\limits_{x \in A} x$ 是 Dedekind 分割. $\bigcap A$ 是包含 A 的所有元素的最小子集. 这里 A 在 $\mathbb{R}$ 中为上确界.

3.9.5 复数

$\mathbb{C} = \mathbb{R} \times \mathbb{R}$ 叫**复数集**. 定义

$$\langle a, b\rangle + \langle c, d\rangle = \langle a + b, c + d\rangle;$$

$$\langle a, b\rangle \cdot \langle c, d\rangle = \langle ac - bd, ad + bc\rangle,$$

实数 a 看作复数 $\langle a, 0\rangle$, 故 $\mathbb{R} \subseteq \mathbb{C}$. i 指 $\langle 0, 1\rangle$; $i^2 = \langle 0, 1\rangle \cdot \langle 0, 1\rangle = \langle -1, 0\rangle = -1$.

当 $a, b \in \mathbb{R}$ 时, $a + bi = \langle a, 0\rangle + \langle 0, b\rangle \cdot \langle 0, 1\rangle = \langle 0, b\rangle$.

练习题 20.

1. 证明整数的加乘法定义合理, 即: 设 $k, l, \tilde{k}, \tilde{l}, m, n, \tilde{m}, \tilde{n} \in \mathbb{N}$, 满足 $[\langle k, l\rangle] = [\langle \tilde{k}, \tilde{l}\rangle]$, $[\langle m, n\rangle] = [\langle \tilde{m}, \tilde{n}\rangle]$. 则: $[\langle k + m, l + n\rangle] = [\langle \tilde{k} + \tilde{m}, \tilde{l} + \tilde{n}\rangle]$, 且 $[\langle km + ln, kn + lm\rangle] = [\langle \tilde{k}\tilde{m} + \tilde{l}\tilde{n}, \tilde{k}\tilde{n} + \tilde{l}\tilde{m}\rangle]$.
2. **(2022 年)** 让 $C(\mathbb{R}) = \{$ 实数集 $\mathbb{R}$ 到 $\mathbb{R}$ 的连续函数 $\}$,
   (1) 证明 f, g 为 $C(\mathbb{R})$ 中不同元素时, $f \upharpoonright \mathbb{Q} \neq g \upharpoonright \mathbb{Q}$. ($f \upharpoonright \mathbb{Q}$ 指把 f 的定义域限制到有理数集 $\mathbb{Q}$ 上)
   (2) 用 (1) 证明 $|C(\mathbb{R})| = \aleph$.
3. **(2012 年)**x 为实数指它是一个 Dedekind 分割, 即 x 为有理数集 $\mathbb{Q}$ 的无最大元的非空真子集, 且向下封闭 (即 x 每个元之下的有理数也属于 x), 设 A 为实数集 $\mathbb{R}$ 的有上界的非空子集, 试证 $\bigcup A$ 也是实数 (从而它为 A 在 $\mathbb{R}$ 中上确界).

第 4 章　格与布尔代数

§ 4.1　格的定义与运算的代数特性

定义 4.1.1

设 $\leq$ 是非空集 L 上的半序, 若对任何 $a, b \in L$, $\{a, b\}$ 在 L 中有上确界 $\sup\{a, b\}$, 在 L 中有下确界 $\inf\{a, b\}$, 则说 L 依 $\leq$ 构成一个**格 (lattice)**. $\langle L, \leq\rangle$ 为**格结构**.

对于格 L, 在 L 上定义运算 $\vee$ 与 $\wedge$. $a \vee b$ 指 $\sup\{a, b\}$, $a \wedge b$ 指 $\inf\{a, b\}$.

定理 4.1.2

设 $\langle L, \leq\rangle$ 为格结构, 则

(1)$a \leq b \Leftrightarrow a \wedge b = a \Leftrightarrow a \vee b = b$.

(2) 交换律: $a \vee b = b \vee a, a \wedge b = b \wedge a$.

(3) 结合律: $(a \vee b) \vee c = a \vee (b \vee c), (a \wedge b) \wedge c = a \wedge (b \wedge c)$.

(4) 吸收律: $a \vee (a \wedge b) = a, a \wedge (a \vee b) = a$.

证明: (1)$a \wedge b = a \Leftrightarrow a \leq a$ 且 $a \leq b \Leftrightarrow a \leq b$. 另外一个同理.

(2) 显然.

(3)$a \leq a \vee b \leq (a \vee b) \vee c$ ①, 由

$$\begin{cases} b \leq a \vee b \leq (a \vee b) \vee c \\ c \leq (a \vee b) \vee c \end{cases} \Rightarrow b \vee c \leq (a \vee b) \vee c.②$$

由①②以及序的反对称性可得 $a \vee (b \vee c) \leq (a \vee b) \vee c$. 同理可证 $(a \vee b) \vee c \leq a \vee (b \vee c)$. 所以 $(a \vee b) \vee c = a \vee (b \vee c)$. 类似可证 $(a \wedge b) \wedge c = a \wedge (b \wedge c)$.

(4)$a \vee (a \wedge b) \geq a$ ①, 由 $a \leq a, a \wedge b \leq a$, 所以 $a \vee (a \wedge b) \leq a$ ②, 由①②和序的反对称性立证. 另一个类似. □

定理 4.1.3

设非空集上有两个运算 $\vee, \wedge$. 它们满足交换律、结合律、吸收律. 则对 $a, b \in L$, 有

$$a \vee b = b \Leftrightarrow a \wedge b = a.$$

定义 $a \leq b$ 为 $a \vee b = b$（或 $a \wedge b = a$）, 则 L 按 $\leq$ 形成格, 且

$$\sup\{a, b\} = a \vee b, \inf\{a, b\} = a \wedge b.$$

证明: 根据吸收律, $a \vee b \Rightarrow a \wedge b = a \wedge (a \vee b) = a$. 根据交换律与吸收律, $a \wedge b \Rightarrow a \vee b = (a \wedge b) \vee b = b \vee (b \wedge a) = b$. 故 $a \wedge b = a \Leftrightarrow a \vee b = b$.

让 $a \leq b$ 指 $a \wedge b = a$(等价于 $a \vee b = b$). 先证 $\leq$ 为 L 上半序:

$1°$(自反性)$a \wedge a = a \wedge (a \vee (a \wedge a)) = a$, (用两次吸收律), 故 $a \leq a$.

$2°$(反对称性) 若 $a \leq b \leq a$, 则 $a = a \wedge b = b \wedge a = b$.

$3°$(传递性) 设 $a \leq b \leq c$, 则 $a \wedge b = a$(即 $a \leq b$) 且 $b \wedge c = b$(即 $b \leq c$). 只需证 $a \wedge c = a$(从而 $a \leq c$). 根据结合律, $a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a$, 从而 $a \leq c$.

因此 $\leq$ 为 L 上的半序.

下面证 $\sup\{a,b\}=a\vee b,\inf\{a,b\}=a\wedge b$.

1° 根据交换律与吸收律, $(a\wedge b)\vee a=a\vee(a\wedge b)=a$, 故 $a\wedge b\leq a$. 同样 $a\wedge b=b\wedge a\leq b$, 故 $a\wedge b$ 为 a 与 b 的下界.

2° 设 $c\in L$ 为 $\{a,b\}$ 下界, 则 $c\leq a,c\leq b$. 从而 $c\wedge a=c,c\wedge b=c$. 于是 $(a\wedge b)\wedge c=a\wedge(b\wedge c)=a\wedge c=c$, 则 $c\wedge(a\wedge b)=c$（交换律）. 则 $c\leq a\wedge b$, 从而 $a\wedge b$ 为 $\inf\{a,b\}$.

3° 根据吸收律, $a\wedge(a\vee b)=a$, 故 $a\leq a\vee b$, 同理 $b\leq a\vee b$, 所以 $a\vee b$ 为 $\{a,b\}$ 的上界.

4° 设 $c\in L$ 为 $\{a,b\}$ 上界, 则 $a\leq c,b\leq c$, 即 $a\vee c=c$ 且 $b\vee c=c$. 于是 $(a\vee b)\vee c=a\vee(b\vee c)=a\vee c=c$. 所以 $a\vee b\leq c$. 从而 $a\vee b$ 为 $\sup\{a,b\}$. □

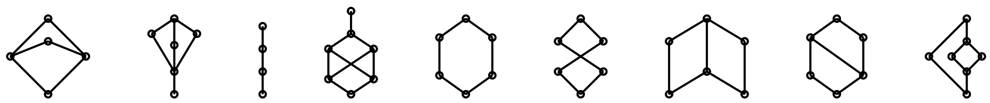
注: 定理表明, 用序或运算规律可定义一个格.

例 4.1.4

$\mathcal{P}(X)=\{A:A\subseteq X\}$ 依 $\subseteq$ 形成格.

练习题 21.

1. 判断下图中哪些是格, 哪些是分配格, 哪些是有补格.



2. 设 L 是格, $a,b,c\in L$ 且 $a\leq b\leq c$. 证明 $a\vee b=b\wedge c$.
3. 设 L 为格, 证明:

$$\forall a_i\in L,a_1\wedge\cdots\wedge a_n=a_1\vee\cdots\vee a_n\Leftrightarrow a_1=a_2=\cdots=a_n.$$

4. 设 $\langle L,\leq\rangle$ 为格结构, $a,b,c,d\in L$ 满足 $a\leq b,c\leq d$. 则 $a\wedge c\leq b\wedge d,a\vee c\leq b\vee d$.

§ 4.2 对偶原理与分配不等式

格一般不成立分配律, 但有分配不等式.

定理 4.2.1. 分配不等式

设 $\langle L, \leq \rangle$ 为格结构, 则 (1)$a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$; (2)$a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$.

证明: (1)$a \leq a \vee b$ 且 $b \wedge c \leq b \leq a \vee b$, 则 $a \vee (b \wedge c) \leq a \vee b$. 类似地, $a \vee (b \wedge c) \leq a \vee c(b, c$ 调位置), 从而 $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$. □

定义 4.2.2: 分配格

若格 L 有分配律

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c), a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c),$$

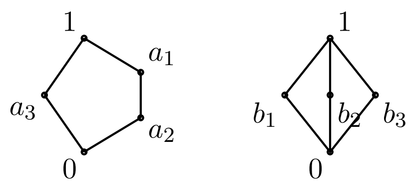
则称 L 为**分配格 (distribute lattice)**.

定义 4.2.3: 有界格

若格 L 有最大元（记为 1）也有最小元（记为 0）, $0 \leq a \leq 1$, 则称格 L 为**有界格**.

例 4.2.4

下面的**五角格**与**钻石格**都不是分配格. 它们的 Hasse 示意图如下:



证明: $a_1 \wedge (a_2 \vee a_3) = a_1 \wedge 1 = a_1$, 但 $(a_1 \wedge a_2) \vee (a_1 \wedge a_3) = a_2 \vee 0 = a_2$.
$b_1 \wedge (b_2 \vee b_3) = b_1 \wedge 1 = b_1$, 但 $(b_1 \wedge b_2) \vee (b_1 \wedge b_3) = 0 \vee 0 = 0$. □

定理 4.2.5. 格的对偶原理

设关于一般格的公式 φ（可能有 $\wedge, \vee, \leq, \geq$）在任何格中成立, 则 φ 的对偶 φ^*（指 φ 中 $\vee$ 与 $\wedge$ 对调, $\leq$ 与 $\geq$ 对调所得）在任何格中成立.

证明: 任给格结构 $\langle L, \leq \rangle$, 则 $\langle L, \geq \rangle$ 也是格. 当 $a, b \in L$ 时, a, b 在 $\langle L, \geq \rangle$ 中的上 (下) 确界与 $\langle L, \leq \rangle$ 中的下 (上) 确界一样. 而 φ 在 $\langle L, \geq \rangle$ 中成立等价于 φ^* 在 $\langle L, \leq \rangle$ 中成立, 根据 $\langle L, \leq \rangle$ 的任意性, φ^* 在任何格中成立. □

例 4.2.6

分配不等式 (1)(2) 中两个命题互为对偶式.

练习题 22.

1. 设 $\leq$ 是非空集 L 上全序, 证明: L 依 $\leq$ 形成分配格.
2. 设 L 为分配格, $a, b, c \in L$, 则 $a \wedge b \leq c \leq a \vee b \Leftrightarrow c = (a \wedge c) \vee (b \wedge c) \vee (a \wedge b)$.
3. 证明 L 是分配格的充要条件是 $\forall x, y, z \in L$, $(x \wedge y) \vee (y \wedge z) \vee (z \wedge x) = (x \vee y) \wedge (y \vee z) \wedge (z \vee x)$.

§ 4.3 格的同态与保序映射

定义 4.3.1: 子格

设 $\langle L, \leq \rangle$ 为格结构, 若 $K \subseteq L$ 且 K 依 $\leq$ 在 K 上限制构成格, 即 $a, b \in K$ 时, $a \vee b \in K, a \wedge b \in K$. 则称 K 为 L 的**子格**.

定义 4.3.2: 同态与同构

设 $\langle L, \leq \rangle$ 和 $\langle \mathscr{L}, \preccurlyeq \rangle$ 为格结构, 若映射 $\sigma : L \to \mathscr{L}$ 满足 $\sigma(a \vee b) = \sigma(a) \vee \sigma(b)$, 则称 σ 是格 L 到 $\mathscr{L}$ 的**同态**. 如果 $\sigma : L \to \mathscr{L}$ 既是双射又是同态, 则称 σ 是 L 到 $\mathscr{L}$ 的**同构映射**.

注: $\sigma(a \vee b) = \sigma(a) \vee \sigma(b)$ 中, 第一个 $\vee$ 是 L 中的上确界, 第二个 $\vee$ 是 $\mathscr{L}$ 中的上确界.

定理 4.3.3. Birkhoff, 1934

格 L 为分配格的充分必要条件是 L 不含五角子格, 也不含钻石子格. （即不含同构于五角格或钻石格的子格）. 【证明比较困难，不作要求. 详见可以看 GTM242 书的对应部分】

定义 4.3.4: 保序映射

设 $\langle L, \leq \rangle$ 和 $\langle \mathscr{L}, \preccurlyeq \rangle$ 为格结构, 若 $\sigma : L \to \mathscr{L}$ 满足

$$x \leq y \Rightarrow \sigma(x) \preccurlyeq \sigma(y), \forall x, y \in L,$$

则称 σ 是**保序映射**.

定理 4.3.5

σ 为格同态 $\Rightarrow \sigma$ 为保序映射.

证明: $x \leq y \Rightarrow x \vee y = y \Rightarrow \sigma(x) \vee \sigma(y) = \sigma(y) \Rightarrow \sigma(x) \preccurlyeq \sigma(y)$. □

练习题 23.

1. **(2008 年)** 判断题: 格的同态映射是保序映射. ( )
2. 设 $\langle L, \leq \rangle$ 是格. 任取 $a \in L$, 令 $S = \{x : x \in L \wedge x \leq a\}$. 证明 $\langle S, \leq \rangle$ 是 L 的子格.
3. **(2022 年)** 设 $\langle L, \leq \rangle$ 与 $\langle L', \leq' \rangle$ 是格结构. σ 是格 L 到 L' 的同态. 证明 σ 是保序映射, 即 $x, y \in L$ 且 $x \leq y$ 时 $\sigma(x) \leq' \sigma(y)$.
4. 若 φ 为格 L 到 L' 之间的双射, 且满足

$$\forall a, b \in L (a \leq b \leftrightarrow \varphi(a) \leq \varphi(b)),$$

则 φ 是格同构.

§4.4 布尔代数

把逻辑变成代数.

定义 4.4.1

设 L 为有界格, 0 为最小元, 1 为最大元. 对于 $a,b\in L$, $a\vee b=1$ 且 $a\wedge b=0$, 则称 a 与 b **互补**, b 为 a 的**补元（余元）**.

0 与 1 互补.

引理 4.4.2

设 L 为分配格, 则 $a,b,c\in L$ 时,

$$\begin{cases} a\vee b=a\vee c \\ a\wedge b=a\wedge c \end{cases} \Rightarrow b=c.$$

证明: $b=b\wedge(a\vee b)=b\wedge(a\vee c)=(b\wedge a)\vee(b\wedge c)=(a\wedge c)\vee(b\wedge c)=(a\vee b)\wedge c=(a\vee c)\wedge c=c.$ 这里用了吸收律、分配律、交换律. □

定理 4.4.3

设 L 为有界分配格.

(1) 如果 $a\in L$ 有补元, 则此补元唯一, 记为 $\overline{a}$.

(2) 如果 $a,b\in L$ 有补元, 则有下面的 de Morgan 律: ① $\overline{a\vee b}=\overline{a}\wedge\overline{b}$, ② $\overline{a\wedge b}=\overline{a}\vee\overline{c}$.

证明: (1) 设 $\overline{a}$ 与 a' 都是 a 的补元, 则 $a\vee a'=a\vee\overline{a}=1$, 且 $a\wedge a'=a\wedge\overline{a}=0$. 根据前面引理, $\overline{a}=a'$. □

(2) 用定义来验证.

$$\begin{aligned}(a\vee b)\vee(\overline{a}\wedge\overline{b})&=(a\vee b\vee\overline{a})\wedge(a\vee b\vee\overline{b})\\&=((a\vee\overline{a})\vee b)\wedge(a\vee(b\vee\overline{b})\\&=(1\vee b)\wedge(a\vee 1)=1\wedge 1=1.\end{aligned}$$

对于第二条式子验证方法也是展开. □

注: 不是分配格时补元可能不唯一, 见后面的习题.

定义 4.4.4

若有界格 L 中每个元都有补格, 则称 L 为**有补格（有余格）**. 有补的分配格叫**布尔代数 (Boolean algebra)**.

例 4.4.5

$B=\{0,1\}$ 按 $\le$（小于或等于）构成布尔代数, 叫电路布尔代数.

例 4.4.6

在命题演算中, 用 0 表示假命题, 1 为真命题, 等价的命题公式视为同一个. 让 $\Gamma=\{$ 命题公式 $\}$, 对 $\alpha,\beta\in\Gamma$, 让 $\alpha\le\beta$ 指 $\alpha\to\beta$ 永真. 则 Γ 为布尔代数.

先验证 $\le$ 是半序, 再验证它形成格, 再验证是否为有界分配格, 最后验证是否为有补格即可.

例 4.4.7

$\mathcal{P}(X)=\{A:A\subseteq X\}$ 依 $\subseteq$ 构成布尔代数.

验证方法同上.

定理 4.4.8. Huntington, 1904

设集合 B 中有两个特殊元 0 与 1, B 上有 $\vee$（加法）与 $\wedge$（乘法）两种运算. 它们满足下面的 Huntington 公理:

(1)$\vee$ 与 $\wedge$ 满足交换律, 且 $\vee$ 对 $\wedge$, $\wedge$ 对 $\vee$ 有分配律.

(2)（同一律）$a \wedge 1 = a, a \vee 0 = a$.

(3)（有补律）对 $a \in B$, 有 $\overline{a} \in B$ 满足 $a \vee \overline{a} = 1, a \wedge \overline{a} = 0$.

则 B 为布尔代数.

证明: Step 1: 证明 $a \vee 1 = 1, a \wedge 0 = 0$. 事实上

$$\begin{aligned}
a \vee 1 = (a \vee 1) \wedge 1 = (a \vee \overline{a}) \wedge (a \vee 1) = a \vee (\overline{a} \wedge 1) = a \vee \overline{a} = 1, \\
a \wedge 0 = (a \wedge 0) \vee 0 = (a \wedge 0) \vee (a \wedge \overline{a}) = a \wedge (0 \vee \overline{a}) = a \wedge \overline{a} = 0.
\end{aligned}$$

Step 2: 证明吸收律.

$$\begin{aligned}
a \vee (a \wedge b) = (a \wedge 1) \vee (a \vee b) = a \wedge (1 \vee b) = a \wedge 1 = a, \\
a \wedge (a \vee b) = (a \vee 0) \wedge (a \vee b) = a \wedge (0 \vee b) = a \vee 0 = a.
\end{aligned}$$

Step 3: 证明 $\begin{cases} a \vee b = a \vee c \\ \overline{a} \vee b = \overline{a} \vee c \end{cases} \Rightarrow b = c.$

$$b = 0 \vee b = (a \wedge \overline{a}) \vee b = (a \vee b) \wedge (\overline{a} \vee b) = (a \vee c) \wedge (\overline{a} \vee c) = (a \wedge \overline{a}) \vee c = 0 \vee c = c.$$

Step 4: 证明结合律. 下证 $a \wedge (b \wedge c) = (a \wedge b) \wedge c$. 让 $L = a \wedge (b \wedge c), M = (a \wedge b) \wedge c$.
下面只需证 $a \vee L = a \vee M, \overline{a} \vee L, \overline{a} \vee M$. 根据 Step 2(吸收律), 有

$$\begin{aligned}
&a \vee L = a \vee (a \wedge (b \wedge c)) = a, \\
&a \vee M = a \vee ((a \wedge b) \wedge c) = (a \vee (a \wedge b)) \wedge (a \vee c) = a \wedge (a \vee c) = a.
\end{aligned}$$

所以 $a \vee L = a \vee M$. 另外

$$\begin{aligned}
\overline{a} \vee L = \overline{a} \vee (a \wedge (b \wedge c)) =& (\overline{a} \vee a) \wedge (\overline{a} \vee (b \wedge c)) \\
=& 1 \wedge (\overline{a} \vee (b \wedge c)) = \overline{a} \vee (b \wedge c), \\
\overline{a} \vee M = \overline{a} \vee ((a \wedge b) \wedge c) =& (\overline{a} \vee (a \wedge b)) \wedge (\overline{a} \vee c) \\
=& ((\overline{a} \vee a) \wedge (\overline{a} \vee b)) \wedge (\overline{a} \vee c) \\
=& (1 \wedge (\overline{a} \vee b)) \wedge (\overline{a} \vee c) \\
=& (\overline{a} \vee b) \wedge (\overline{a} \vee c) \\
=& \overline{a} \vee (b \wedge c).
\end{aligned}$$

所以 $\overline{a} \vee L = \overline{a} \vee M$. 根据 Step 3, 结合律证完.

Step 5: 仿照 Step 3,Step 4 证明 $a \vee (b \vee c) = (a \vee b) \vee c$.

由上, 关于 $\vee$ 与 $\wedge$ 有交换律、结合律、分配律, 故 B 为分配格. $a \leq b$ 相当于 $a \vee b = b$(或 $a \wedge b = a$). 由于 $a \vee 1 = 1, 0 \vee a = a$, 故 $0 \leq a \leq 1$, 故 a 有界. 根据条件 (3), 每个元素都有补元, 则 B 为布尔代数. □

定义 4.4.9: 原子

设 L 为格, 0 为其最小元. 若 $a \in L$ 为 $L \setminus \{0\}$ 中极小元, 即 $0 < b \leq a \Rightarrow b = a$, 则称 a 为 L 中**原子 (atom)**.

引理 4.4.10

设格 L 中有最小元 0, 且 a, b 为不同原子, 则 $a \wedge b = 0$.

证明: $a \wedge b \leq a, a \wedge b \leq b$, 由于 $a \neq b$, 所以 $a \wedge b < a$ 且 $a \wedge b < b$, 所以 $a \wedge b = 0$. (原子下面更小的只有 0). □

引理 4.4.11

设 B 为有限布尔代数, 则 B 中非零元可唯一（不考虑顺序）表示成一些原子之和（上确界）.

证明: 设 $x \in B \setminus \{0\}$. 让 $T(x) = \{a \in B : a \text{ 为原子且 } a \leq x\} = \{a_1, \cdots, a_n\}$. （把 $\leq x$ 的原子都列出来）让 $y = a_1 \vee \cdots \vee a_n$, 下证 $x = y$.

Step 1: 由于 $a_i \leq x (i = 1, 2, \cdots, n)$, 则 x 为诸 a_i 的上界, 故 $y \leq x$ ①.

Step 2: 下证 $y \geq x$. 先证 $x \wedge \overline{y} = 0$. (反证) 假如 $x \wedge \overline{y} \neq 0$, 则断言有个原子 $a \leq x \wedge \overline{y}$. (若 a 不是原子，则可以找更小的, 由于 B 有限, 故必能找到原子)

$a \leq x \wedge \overline{y}$, 则 $a \in \{a_1, \cdots, a_n\}$, 故有 i 使 $a = a_i$. 由于 $a \leq \overline{y}$, 则

$$a = a \wedge \overline{y} = a_i \wedge \overline{a_1 \vee \cdots \vee a_n} = a_i \wedge (\overline{a_1} \wedge \cdots \wedge \overline{a_n}) = (a_i \wedge \overline{a_i}) \wedge (\overline{a_1} \wedge \cdots \wedge \overline{a_{i-1}} \wedge \overline{a_{i+1}} \wedge \cdots \wedge \overline{a_n}) = 0.$$

这与 $a \neq 0$ 矛盾, 故 $x \wedge \overline{y} = 0$. 于是

$$y = y \vee 0 = y \vee (x \wedge \overline{y}) = (y \vee x) \wedge (y \vee \overline{y}) = (x \vee y) \wedge 1 = x \vee y,$$

于是 $x \leq y$ ②. 根据①②可知 $x = y = a_1 \vee \cdots \vee a_n$(原子和).

唯一性的证明: 若有另一组原子 $b_1, \cdots, b_m$ 使 $x = b_1 \vee \cdots \vee b_m$, (反证) 若 $a_i \notin \{b_1, \cdots, b_n\}$, 根据前面引理有:

$$a_i = a_i \wedge x = a_i \wedge (b_1 \vee \cdots \vee b_n) = (a_i \wedge b_1) \vee \cdots \vee (a_i \wedge b_m) = 0 \vee \cdots \vee 0 = 0.$$

矛盾. 故 $a_i \in \{b_1, \cdots, b_m\}, \forall 1 \leq i \leq n$. 则 $\{a_1, \cdots, a_n\} \subseteq \{b_1, \cdots, b_m\}$.

同理可证 $\{b_1, \cdots, b_m\} \subseteq \{a_1, \cdots, a_n\}$. 故 $\{a_1, \cdots, a_n\} = \{b_1, \cdots, b_m\}$. □

定义 4.4.12: 布尔代数同态

设 B_1, B_2 是布尔代数, φ 为 B_1 到 B_2 的映射, 若对任意 $a, b \in B_1$, 有

$$\varphi(a \vee b) = \varphi(a) \vee \varphi(b), \varphi(a \wedge b) = \varphi(a) \wedge \varphi(b), \varphi(\overline{a}) = \overline{\varphi(a)},$$

则称 φ 是 B_1 到 B_2 的**同态**. 若 φ 又是同态又是单射, 则 φ 是 B_1 到 B_2 的**同构映射**. 此时称布尔代数 B_1, B_2 **同构**, 记为 $B_1 \cong B_2$.

定理 4.4.13. 有限布尔代数表示定理

设 B 为有限布尔代数, A 为 B 中原子构成的集合, 则布尔代数 B 同构于幂集代数 $\mathcal{P}(A)$.

证明: 对 $x \in B$, 让 $T(x) = \{B \text{ 中原子 } a (\in A) : a \leq x\} \subseteq A$. 则 $T(x) \in \mathcal{P}(X)$ ①.

(1) 下证 T 是同态: $\forall b \in B, x, y \in B$, 有

$$b \in T(x \wedge y) \Longleftrightarrow b \in A \text{且} b \leq x \wedge y \Longleftrightarrow b \leq x \text{且} b \leq y \Longleftrightarrow b \in T(x) \wedge b \in T(y) \Longleftrightarrow b \in T(x) \cap T(y).$$

故由外延性公理, $T(x \wedge y) = T(x) \cap T(y)$. 另外 $T(0 \vee x) = T(x) = T(x) \cup T(0), T(0) = \varnothing$. 如果 $x, y \in B$ 非零, 设 $T(x) = \{a_1, \cdots, a_n\}, T(y) = \{b_1, \cdots, b_m\}$.

$x \vee y = (a_1 \vee \cdots \vee a_n) \vee (b_1 \vee \cdots \vee b_m)$,

$T(x \vee y) = \{a_1, \cdots, a_n, b_1, \cdots, b_m\} = \{a_1 \cdots, a_n\} \cup \{b_1, \cdots, b_m\}$(前一引理) $= T(x) \cup T(y)$.

对 $x \in B$, 有

$$T(x) \cup T(\overline{x}) = T(x \vee \overline{x}) = T(1) = A.(\leq 1 \text{ 的原子为 } B \text{ 中所有原子})$$

$$T(x) \cap T(\overline{x}) = T(x \wedge \overline{x}) = T(0) = \varnothing.$$

则 $T(x)$ 为 $T(\overline{x})$ 在 A 中的补集. 由上, T 为 B 到 $\mathcal{P}(A)$ 的同态.

(2) 下证 T 为双射. 满射: $\{b_1, \cdots, b_m\} \in \mathcal{P}(A)$, 则 $\{b_1, \cdots, b_m\} \subseteq A$, $(b_1, \cdots, b_m$ 为原子). 让 $x = b_1 \vee \cdots \vee b_m$, 则 $T(x) = \{b_1, \cdots, b_m\}$. 故 T 为满射.

单射: $T(x) = T(y)$ 即 $\{a_1, \cdots, a_n\} = \{b_1, \cdots, b_m\} \Rightarrow x = a_1 \vee \cdots \vee a_n = b_1 \vee \cdots \vee b_m = y$.

根据 (1)(2), T 为同构, 故 $B \cong \mathcal{P}(A)$. □

注: 考试时布尔代数不会做的话就写成幂集代数, 变成并与交的问题, 再推广到一般布尔代数, 把符号换一换即可.

推论 4.4.14

任何有限布尔代数 B_1, B_2, 如果 B_1, B_2 等势, 则 B_1, B_2 同构.

推论 4.4.15

任何有限布尔代数的基数为 $2^n, n \in \mathbb{N}$.

练习题 24.

1. 判断题.
   (1) **(2012 年)** 不存在基数为 36 的布尔代数. ( )
   (2) **(2010 年)** 不存在基数为 48 的布尔代数. ( )
   (3) **(2012 年)** 任两个等势的有限布尔代数是同构的. ( )
   (4) **(2008 年)** 任给正整数 N, N 的全体正因子依整除关系构成布尔代数. ( )
2. 设 B 是布尔代数, $a, b \in B$, 证明

$$a \leq b \Leftrightarrow a \wedge \overline{b} = 0 \Leftrightarrow \overline{a} \vee b = 1.$$

3. 设 B 是布尔代数, $a, b \in B$, 证明: $a \leq b \Leftrightarrow \overline{b} \leq \overline{a}$.
4. 设 B 是布尔代数, 证明下面的模律成立: 即

$$a \leq c \Rightarrow a \vee (b \wedge c) = (a \vee b) \wedge c.$$

5. **(2008 年)** 设 $A = \{1, \cdots, n\}, X = \{x_1, \cdots, x_n\}$ 是 n 元集. 证明布尔代数 $\mathcal{P}(A)$ 同构于布尔代数 $\mathcal{P}(X)$, 这儿 $\mathcal{P}(X)$ 为 X 的幂集.
6. **(2012 年)** 设 B 为布尔代数, $u, v, w, x \in B$ 满足 $w \vee x = u$ 且 $w \wedge x = v$. 试用 u, v, w 以及 B 的运算来表示 x, 并证明表达式的正确性.
7. **(2010 年)** 设 $p_1, \cdots, p_k$ 为不同素数, D 为 $N = p_1 \cdots p_k$ 的所有正因子构成的集合. 证明 D 按照整除这个半序构成布尔代数.
8. **(2022 年)** 设正整数 $N > 1$ 有素数分解式 $p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, 其中 $p_1 < \cdots < p_r$ 为不同素数, $\alpha_1, \cdots, \alpha_r \in \mathbb{Z}^+$. 集合 $D(N) = \{d \in \mathbb{Z}^+ : d | N\}$ 由 N 所有正因子构成.
   (1) 说明 $D(N)$ 依整除这个半序形成有界分配格.
   (2) 刻画使 $D(N)$ 为布尔代数的 N 值.

特别鸣谢

由于本人精力有限, 难免在编辑过程中有笔误, 而南京大学数学系 2018 级的 zst 同学、Vanch 同学与 2019 级的 zyzmoonlight 同学、2020 级的 zjq 同学、天影同学、陈韵雯同学指出了许多处错误, 在此表示衷心的感谢!

习题部分包含了“大家非常喜欢”的那种题, 如果大家后面有一些新的“大家非常喜欢”的题, 欢迎向 Fiddie 反馈, 我将作补充.