《离散数学》复习

Chapter 1: Logic and Proofs

一、Propositional Logic

1. 命题 proposition

   ① 可真可假 ② 一定为陈述句 (statement)

2. 逻辑运算符

   ① Negation: $\neg$ ② Conjunction (合取,与): $\wedge$

   ③ Disjunction (析取,或): $\vee$

   ④ Implication (蕴含): $\rightarrow$

   $p \rightarrow q$: {p: Hypothesis; q: Conclusion}

p	q	$p\rightarrow q$
T	T	1
T	F	0
F	T	1
F	F	1

   称法: I. if p then q   II. p is sufficient for q

   III. p implies q   IV. p only if q

   V. q is necessary for p   VI. if q whenever p

   Eg: F → everything, everything → T

   难点: p、q 前后顺序判断

   ⑤ Biconditional (等价) $\leftrightarrow$

p	q	$p\leftrightarrow q$
T	T	1
T	F	0
F	T	0
F	F	1

3. 优先级: $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$

4. 命题公式 Propositional Formula

   ① Tautology: 永真式 ② Contradiction: 永假式

   ③ Contingence: 或真或假式

二、命题的等价性

1. Converse (逆命题) $p\to q$, $q\to p$ 互逆

Contrapositive (逆否命题) $p\to q$, $\neg q\to\neg p$

原命题与逆否命题等价

2. 变换规则

① Commutative (交换律)

② Associative (结合律)

③ Distributive (分配律)

④ Excluded Middle (排中律): $p\wedge\neg p\Leftrightarrow F$. $p\vee\neg p\Leftrightarrow T$

⑤ Absorption : $p\wedge(p\vee q)\Leftrightarrow p$

$p\vee(p\wedge q)\Leftrightarrow p$

3. "$\to$"与"$\leftrightarrow$"的命题转化

① $p\to q \Leftrightarrow \neg p\vee q$

② $p\leftrightarrow q \Leftrightarrow (\neg p\vee q)\wedge(\neg q\vee p)$

4. 命题的规范形式 Propositional Normal Forms

① 两种规范形式

I. 析取范式 (DNF) : 形如 $A_1A_2A_3+B_1B_2B_3B_4+\cdots$

II. 合取范式: (CNF) :

② 全析取范式 (Full Disjunctive Form, 即 Sum of Minterm)

5. 推理规则

① Modus Ponens: $\left.\begin{matrix} p\to q \\ p \end{matrix}\right\} \Rightarrow q$

② Modus Tollens: $\left.\begin{matrix} p\to q \\ \neg q \end{matrix}\right\} \Rightarrow \neg p$

③ Rule of Addition: $p \Rightarrow p\vee q$

④ Rule of Simplification: $p\wedge q \Rightarrow p$

⑤ Rule of Conjunction: $\left.\begin{matrix} p \\ q \end{matrix}\right\} \Rightarrow p\wedge q$

⑥ Rule of Hypothetical Syllogism: $\left.\begin{matrix} p\to q \\ q\to r \end{matrix}\right\} p\to r$

⑦ Rule of Disjunctive Syllogism: $\left.\begin{matrix} p\vee q \\ \neg p \end{matrix}\right\} \Rightarrow q$

6. 三条推理技巧

① 若结论形如($p\to q$),则可用下式:

$$(p_1\wedge p_2\wedge\cdots\wedge p_n)\to(p\to q) \Leftrightarrow (p_1\wedge\cdots\wedge p_n\wedge p)\to q$$

② 使用反证法.

若要证明 $p\to q$,则假设 p 为 T,q 为 F,导出 $\neg p$ 也为 T,

产生矛盾,从而假设不成立.

③ 归结原理 Resolution

$$(p\vee q)\wedge(\neg p\vee r)\to(q\vee r)$$

三.谓词和量词 Predicates & Quantifiers

1. 基本概念

① 谓词(Predicates):又称"命题函数",它是含有变量的命题,命题的真假取决于变量的取值,记作 $P(x)$

② 量词(Quantifiers):包括全称量词(Universal Quantifier)和存在量词(Existential Quantifier)

③ 若让命题函数转化成命题,需进行量词化 e.g. $P(x) \xrightarrow[\text{化}]{\text{量词}} \forall x\, P(x)$

④ Universe of Discourse：论域

⑤ 对于包含量词的命题，量词的优先级最高

⑥ 在命题函数中，所有变量都经过量词化，才能视为命题

e.g. $\forall x P(x) \longrightarrow \exists y R(x,y)$ 不是命题

只是重名而已

e.g. 用命题表示"每个人恰有一个朋友"

令 $B(x,y)$：y 是 x 的朋友

$\forall x \exists y \forall z \, (B(x,y) \land ((z \neq y) \rightarrow \neg B(x,z)))$

2. 含有量词的等价变换规律

① 交换律：$\forall x \forall y \, P(x,y) \Leftrightarrow \forall y \forall x \, P(x,y)$

$\exists x \exists y \, P(x,y) \Leftrightarrow \exists y \exists x \, P(x,y)$

注：$\forall$ 和 $\exists$ 不能随意交换

② De Mogan's：

$\neg \forall x \, p(x) \Leftrightarrow \exists x \neg p(x)$

$\neg \exists x \, p(x) \Leftrightarrow \forall x \neg p(x)$

③ 有条件的分配律：

$\forall x [p(x) \land q(x)] \Leftrightarrow \forall x \, p(x) \land \forall x \, q(x)$

$\exists x [p(x) \lor q(x)] \Leftrightarrow \exists x \, p(x) \lor \exists x \, q(x)$

3. 前束范式 Prenex Normal Forms

① 前束范式是命题的一种标准形式，它把所有的量词移到最前面，形如 $Q_1 x_1 Q_2 x_2 \cdots Q_n x_n B$

（其中 Q_i 为 $\forall$ 或 $\exists$，B 是一个不含量词的公式）

② 将命题转化为前束范式

Ⅰ. 消除所有 '→'、'↔'.

Ⅱ. 将所有 '¬' 向内移动, 使得 '¬' 只出现在文字中.

Ⅲ. 若有必要, 对同名但不相关的变量进行重命名

Ⅳ. 将所有量词移到公式最前面

4. 含有量词的命题推理规则

① Universal Instantiation (UI) $\left.\begin{matrix}\forall x\in D,\ P(x)\\ d\in D\end{matrix}\right\}\Rightarrow P(d)$

② Universal Generalization (UG) $P(d)$ for any $d\in D \Rightarrow \forall x\in D, P(x)$

③ Existential Instantiation (EI) $\left.\begin{matrix}\exists x\in D\\ P(x)\end{matrix}\right\}\Rightarrow P(d)$ for some $d\in D$

④ Existential Generalization (EG) $P(d)$ for some $d\in D \Rightarrow \exists x P(x)$

Chapter 2: Sets and Functions

一、Sets 集合

1. 集合的性质: 无序性, 可重复性, 确定性

2. 子集 $\begin{cases}\text{子集}: \subseteq \\ \text{真子集 (proper subset)}: \subset\end{cases}$

3. 无限集和有限集

① 集合 S 的基数 (Cardinality) 记作 $|S|$, 用于刻画集合的大小

② 任何集合都有基数, 有限集的基数是其元素个数.

③ 有限集都是可数集 (denumerable / countable set)

无限可数集: N, Z, Q, N^2, 无限不可数集: R …

注: 在证明与集合相关的等式时, 需证左右两侧的集合相互包含

具体地, 要证 $A\subseteq B$, 从 A 中任取 x 然后证 $x\in B$

二、集合的运算

1. 并 Union ($\cup$)

2. 交 Intersection ($\cap$)　　注: disjoint (不相交)

3. 差 Difference $A-B=\{x \mid x\in A \wedge x\notin B\}$, $A-B=A\cap\overline{B}$

4. 反 Complement $\overline{A}=U-A$

5. 异或 Symmetric Difference : $A\oplus B=(A-B)\cup(B-A)$

(仅在A或B一个集合中出现)

e.g. Prove : $A\oplus B=A\oplus C \Rightarrow B=C$

证: $B=\phi\oplus B$

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

$=A\oplus(A\oplus C)=(A\oplus A)\oplus C=\phi\oplus C=C$

6. 幂集 Power Set

集合S的所有子集组成的集合称为S的幂集. 记作$P(S)$或2^S

$P(S)=\{T \mid T\subseteq S\}$

7. Cartesian Product

① $A_1\times A_2\times\cdots\times A_n=\{(a_1,a_2,\cdots,a_n) \mid a_i\in A_i\}$

$A^n=A\times A\times\cdots\times A$ (n次)

② 运算规律 (通常情况下)

I. $A\times B\neq B\times A$　　II. $(A\times B)\times C\neq A\times(B\times C)$

III. $A\times(B\cup C)=A\times B\cup A\times C$

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

e.g. 反例 a. $A\times B\subseteq C\times D$, 不一定有 $A\subseteq C$、$B\subseteq D$, 反例是$A=D=\phi$, $B=C=\{1\}$

b. $(A\cup B)\times(C\cup D)=(A\times C)\cup(B\times D)$ 不成立, 用上述规律III展开可证

三、集合的基数

1. 有限集的基数

① Principle of Inclusion-Exclusion:

$$|A\cup B| = |A| + |B| - |A\cap B|$$

2. 无限集的基数

① 两集合基数相等 $\Leftrightarrow$ 两集合间能构成双射.

e.g. $(0,1)$之间所有实数组成的集合与 R 基数相等

双射: $f(x) = \tan[\pi(x-\frac{1}{2})]$

② 某集合是无限集 $\Leftrightarrow$ 存在一个真子集,与它有相同的基数

③ 所有的无限可数集具有相同的基数,记作 $\aleph_0$, 无限不可数集的基数 $> \aleph_0$

④ 幂集的基数大于原集合的基数: $|2^A| > |A|$

⑤ 有限个/可数个可数集的并是可数集

e.g. 证明 R 是不可数集.

I. 证明 $(0,1)$ 范围内的实数集是不可数的

若 $(0,1)$ 内实数可数,则可列出:

$0.a_{00}a_{01}a_{02}\cdots$

$0.a_{10}a_{11}a_{12}\cdots$

$0.a_{20}a_{21}a_{22}\cdots$ 其中 $a_{ij}\in\{0,1,2,\cdots,9\}$

构建一个新的数

$b=0.b_0b_1b_2\cdots$, 其中 $b_i=\begin{cases}2 & ,\text{若 } a_{ii}=1\\ 1 & ,\text{若 } a_{ii}\neq 1\end{cases}$

于是 b 不同于上面列出的任何一数,从而 $(0,1)$ 内实数不可数

II.

四、函数 Functions

1. 定义

$f: A \to B$ | $f(a)=b$

① A: Domain ② B: Codomain（上域） | ① b是a的 image

③ Range: 值域（是上域的子集） | ② a是b的 pre-image

2. 单射、满射、双射

① 单射 One-to-one function (Injective)

$\forall a,b \in A \wedge a \neq b \Rightarrow f(a) \neq f(b)$

② 满射 Onto function (Surjective)

③ 双射 One-to-one Correspondence (Bijection)

注：双射是可逆（Invertible）的，具有反函数（Inverse Function）

3. 复合函数 Composition $(f \circ g)(a) = f(g(a))$

4. 向上/下取整函数

① Floor: $\lfloor x \rfloor$ e.g. $\lfloor -24.5 \rfloor = -25$, $\lceil -24.5 \rceil = -24$

② Ceiling: $\lceil x \rceil$

5. 函数的增长性

① $f(x)=O(g(x))$: ∃常数 c, k，在 $x>k$ 时，$|f(x)| \leq C|g(x)|$

e.g. Prove $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$, $f(x)=O(x^n)$

由三角不等式，$x>1$ 时

$$|f(x)| \leq |a_n|x^n+|a_{n-1}|x^{n-1}+\cdots+|a_0|$$

$$= x^n\left(|a_n|+\frac{|a_{n-1}|}{x}+\cdots+\frac{|a_0|}{x^n}\right)$$

$$\leq x^n\left(|a_n|+|a_{n-1}|+\cdots+|a_0|\right)$$ 得证

② $f(x)=\Omega(g(x))$: ∃常数 c, k，在 $x>k$ 时，$|f(x)| \geq C|g(x)|$

 ③ $f(x)=\Theta(g(x))$: $f(x)=O(g(x))$ 且 $f(x)=\Theta(g(x))$ 称 f 与 g 同阶 (of order)

Chapter 3: Algorithm

1. 复杂度比较表

$$O(1) < O(\log n) < O(n) < O(n\log n) < O(n^b) < O(b^n) < O(n!)$$

$b>1$

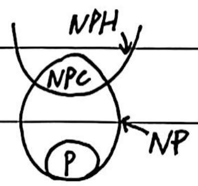
2. NP问题

① P: 能在多项式时间解决

② NP: 能在多项式时间验证

③ NPH: 所有NP问题都能以多项式时间归约到该问题.

④ NPC: 属于NP的NPH问题



Chapter 4: Induction and Recursion

一、归纳法

1. Well-Ordering Property (良序性质): 任何非负整数的集合必有最小元素.

二、递归

1. 递归定义集合

e.g. 定义能被3整除的整数集 : $3\in S$, $x+y\in S$, 若$x\in S \wedge y\in S$

2. 递归算法

e.g. Euclid's GCD 计算两个非负整数的最大公约数 (Greatest Divisor)

```
gcd (a,b: a<b)
if a=0 then gcd(a,b):=b
else gcd(a,b):=gcd(b%a, a)
```

3. 使用递归研究字符串

① Alphabet：Σ（字母表），包含字符（Symbol）

② Σ 上的字符串是 Σ 上的字符组成的有限序列

③ 字符串 a 与 b 的连接（Concatenation）记作 ab

④ Σ 上所有字符串组成的集合记作 Σ^*，递归定义如下：

I. λ 为空字符串，$\lambda \in \Sigma^*$

II. 若 $w \in \Sigma^*$，$x \in \Sigma$，则 $wx \in \Sigma^*$

⑤ 字符串 w 的長度记作 $l(w)$，递归定义如下：

I. $l(\lambda) = 0$

II. 若 $w \in \Sigma^*$，$x \in \Sigma$，则 $l(wx) = l(w) + 1$

《离散数学》复习

Chapter 5: Counting

一、加法法则与乘法法则

1. 加法法则 The Sum Rule
2. 乘法法则 The Product Rule

eg. ① 从m个元素的集合到n个元素的集合,有多少个one-to-one function(单射):

答: $m>n$时,没有 $m\leq n$时,有 $n(n-1)\cdots(n-m+1)$ 个

② 从m个元素的集合到n个元素的集合,有多少个二元关系

$2^{m\times n}$

二、鸽巢原理 Pigeonhole Principle

1. 定义

① 基本: 若$(k+1)$或更多物体放到k个箱子中,则至少有一个箱子有至少2个物体

② 广义: 若N个物体放入k个箱子中,则至少有一个箱子有至少$\lceil \frac{N}{k} \rceil$个物体

2. 定理: 任意不超过2n的$(n+1)$个正整数中,必存在一个整数能整除另一个整数

证明: 把$(n+1)$个整数$a_1,\cdots,a_{n+1}$表示为$a_j=2^k\times q_j$的形式.(其中k为常数,q_j为奇数.

不超过2n的奇数只有n个,而上式定义的奇数q_j有$(n+1)$个.

故至少有2个整数$a_j.a_i$对应的奇数

3. 定义（子序列）

①子序列（Subsequence）是通过按原始顺序包含原始序列的某些项而从原始序列中获得的序列

②为序列定义严格单增/单减（Strictly Increasing/Decreasing）

4. 定理：每个长为(n^2+1)的，由不同的实数组成的序列，都包含长为$(n+1)$的或者严格单增，或者严格单减的子序列

证明：1° 记i_k、d_k分别是以元素a_k作为起始，可构建的最长的单增、单减子序列的长度

2° 先证：$a_k \leftrightarrow (i_k, d_k)$

假设$\exists a_s$, s.t. $i_s=i_k, d_s=d_k$, $s<k$

由于$a_k \neq a_s$，所以

若$a_s<a_k$，则一定有$i_s \geq i_k+1$

若$a_s>a_k$，则一定有$d_s \geq d_k+1$

故此假设不成立，$a_k \leftrightarrow (i_k, d_k)$成立

3° 假设题述序列不包含长为$(n+1)$的严格单增/单减子序列。

则$1 \leq i_k, d_k \leq n$，即(i_k, d_k)共有n^2种取法

而题述序列长为(n^2+1)，由鸽洞原理，

$\exists i,j$, s.t. $i_i=i_j, d_i=d_j, i\neq j$

这与2°的结论矛盾，故假设不成立，得证

5.定理：设 $x_1,\cdots,x_n$ 是長度为 n 的整数序列，则存在某个连续(Consecutive)子序列，其和能被 n 整除

证明：1° 定义前缀和 $A_i=\sum_{j=0}^{i} x_j$，特别地，$A_0=0$，由此定义 n 个前缀和：$A_1,\cdots,A_n$

2° 若某个 A_i 能被 n 整除，则直接满足条件.

3° 若所有 A_i 都不能被 n 整除，则这 n 个前缀和除以 n 的余数只有 $(n-1)$ 种情况 $(1,2,\cdots,n-1)$

于是，根据鸽洞原理，至少有两个前缀和 A_i,A_j 的余数相同，于是 $x_{i+1},\cdots,x_j$ 之和能被 n 整除

6.定理：设 $a_1,a_2,\cdots,a_N$ 是长 $N=2^n$ 的序列，由 n 个不同的负整数组成，则存在某个连续子序列，其乘积是完全平方数 (Perfect Square)

证明：1° 定义前缀积 $A_i=\prod_{j=1}^{i} a_j$，特别地 $A_0=1$，由此定义 2^n 个前缀积

将 A_i 分解为质因数的形式：$A_i=x_1^{\alpha_{i1}}x_2^{\alpha_{i2}}\cdots x_n^{\alpha_{in}}$，其中 x_i 代表组成序列 $\{a_n\}$ 的负整数，$\alpha_{ik}\geq 0$

2° 关键点：若 A_i 表达式中所有质因数的幂次 α_{ij} 均为偶数，则 A_i 为完全平方数

3° 若某个 A_i 是完全平方数，则直接满足条件

4° 若所有 A_i 都不是完全平方数，则这 2^n 个前缀积的幂次按奇数或偶数来分，只有 (2^n-1) 种可能（排除掉幂次全为偶数的情况）

根据鸽洞原理，至少有两个前缀积 A_i,A_j 的幂次奇偶完全相同，于是 $\frac{A_j}{A_i}$ 是完全平方数.

7. 球队问题

在30天内，球队每天至少比赛1次，但总比赛次数不超过45。证明存在一段连续的几天中，球队恰好比赛14次

证明：令 a_j 是球队在第j天及之前的比赛场次

于是 $1 \leq a_j \leq 45$

$15 \leq a_j + 14 \leq 59$

Pigeon：$\{a_j\}_{j=1}^{30}$、$\{a_j+14\}_{j=1}^{30}$，共60个Pigeon

Pigeonhole：1~59的整数

$\Rightarrow \exists\ a_i = a_j + 14$

三、排列组合

1. ① 排列 Permutations

$P(n,r)$：在n个元素的集合中排出r个元素，进行有序排列

$P(n,r) = \frac{n!}{(n-r)!}$

② 组合 Combination

$C(n,r)$：无序组合

$C(n,r) = \frac{n!}{(n-r)!\,r!} = \frac{P(n,r)}{r!}$

2. 二项式分解 Binomial Coefficients

I. $(a+b)^n = C_n^0 a^n + C_n^1 a^{n-1} b + \cdots + C_n^n b^n$

II. $C(n+1,k) = C(n,k) + C(n,k-1)$

III. $\sum_{k=0}^{n} C(n,k) = 2^n$

} 可用杨辉三角进行理解

IV. $C(m+n,r) = \sum_{k=0}^{r} C(m,r-k) \cdot C(n,k)$

3. 广义排列组合

① 对于含 n 个元素的集合，允许重复的 r-排列，共有 n^r 种

② 〃 r-组合 $C(n+r-1, r)$

(使用挡板法理解)

e.g.1. 在4种饼干中购买6块，有多少种方法？

解：$n=4$，$r=6$，$C(n+r-1, r) = C(9,6) = 84$

e.g.2. $x_1+x_2+x_3+x_4=29$ 有多少组满足 $x_1>0, x_2>1, x_3>2, x_4\geq 0$ 的整数解？

解：提前为 x_1, x_2, x_3 预留 1,2,3，即 $n=4$，$r=23$

$C(n+r-1, r) = C(26,23) = 2600$

4. 将物品分配到箱子中

① 若物品是不可区分的，则使用上面②的公式

(如：完全相同的球)

② 若物品是可区分的：

将 m 个可区分的物体分配到 k 个可区分的箱子中，使箱子 i 中有 n_i 个物体，总方法数为 $\frac{m!}{n_1!n_2!\cdots n_k!}$ (要求 $\sum n_i = m$)

e.g.1. 52张扑克牌分给四人，每人分5张的方法数：$\frac{52!}{5!\cdot 5!\cdot 5!\cdot 5!\cdot 32!}$

(分剩下的32张牌也要"消序")

四、生成排列 Generating Permutations

1. Lexicographic Order

定义：给定集合 $1,2,\cdots,n$ 的两个排列 $a_1\cdots a_n$，$b_1\cdots b_n$

称 $a_1\cdots a_n$ 先于 (precede) $b_1\cdots b_n$，若存在某个位置 k，使得 $a_1\cdots a_n$、$b_1\cdots b_n$ 的前 $k-1$ 位完全相同，而 $a_k<b_k$

e.g. 23415 先于 23514 先于 23541

2. 生成下一个字典序排列的算法

① 找到排列中最后一对前者小于后者的相邻整数 a_j、a_{j+1}

② 在 a_j 位置放置 $a_{j+1},a_{j+2},\cdots,a_n$ 中大于 a_j 的最小整数

③ 将剩余的整数按升序排列在 $a_{j+1}\sim a_n$ 的位置

e.g. $36\boxed{25}41 \rightarrow 36\boxed{4}\underbrace{125}_{\text{升序}}$

j　j+1　　　　j