离散数学考前复习

第一部分 逻辑

命题逻辑的定义

命题是一个或真或假的陈述句，但不能既真又假

逻辑连接词(逻辑运算符)，真值表

逻辑连接词

- 否定词 NOT Negation $\neg$
- 合取词 AND Conjunction $\wedge$
- 析取词 OR Disjunction $\vee$
- 异或词 XOR Exclusive or $\oplus$
- 蕴含词 if-then Implication $\rightarrow$
- 等价词 if and only if Biconditional $\leftrightarrow$

运算优先级：$\neg > \wedge > \vee > \rightarrow > \leftrightarrow$

真值表

蕴含：只有真->假为假

等价：同真同假时为真

命题逻辑等价，基本逻辑等价式，逻辑等价的证明

命题逻辑等价

$$p \leftrightarrow q$$

是永真式，称命题p和q是等价的

基本逻辑等价式

几个难记忆的基本逻辑等价式

$$\text{吸收律}$$
$$p \vee (p \wedge q) \Leftrightarrow p$$
$$p \wedge (p \vee q) \Leftrightarrow p$$

$$\text{其他}$$
$$(p \to q) \wedge (p \to r) \Leftrightarrow p \to (q \wedge r)$$
$$(p \to r) \wedge (q \to r) \Leftrightarrow (p \vee q) \to r$$
$$(p \to q) \vee (p \to r) \Leftrightarrow p \to (q \vee r)$$
$$(p \to r) \vee (q \to r) \Leftrightarrow (p \wedge q) \to r$$

逻辑等价的证明

两种方式：

1. 画真值表
2. 通过已知的逻辑等价式，证明$p \leftrightarrow q$是永真式

命题逻辑推理:推理法则，形式化推理证明

逻辑蕴含

如果p->q是永真式，则命题p蕴含q

有效的论证

若每当所有的前提都为真时，结论也为真，则这样的论证称为有效的。也就是等价于下列蕴含式为真。

$$p_1 \wedge p_2 \wedge \ldots \wedge p_n \to q$$
$$is\ tautology$$

推理法则

附加	$p \to (p \vee q)$
化简	$(p \wedge q) \to p$
合取	$((p) \wedge (q)) \to (p \wedge q)$
假言推理	$(p \wedge (p \to q)) \to q$
取拒式	$(\neg q \wedge (p \to q)) \to \neg p$
假言三段论	$((p \to q) \wedge (q \to r)) \to (p \to r)$
析取三段论	$((p \vee q) \wedge (\neg p)) \to q$
构造两难性	$(((p \to r) \wedge (q \to r)) \wedge (p \vee q)) \to r$
消解	$((p \vee q) \wedge (\neg p \vee r)) \to (q \vee r)$

形式化论证 Formal Proofs

假定假设是正确的，用一些推论和逻辑等价式来确定结论的正确

如果有这样p→q的结论形式，我们就能把原问题转换成为下面这个式子：

$$p_1 \wedge p_2 \wedge \ldots \wedge p_n \wedge p \Rightarrow q$$

因为

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

是永真式

归谬法：

使用归谬法证明p->q的步骤：

1. 假设p为真，q为假
2. 证明$\neg p$ 也为真->矛盾！

谬误 Fallacies

1. 断定结论的谬误

$((p \to q) \land q) \to p$把此式当作重言式的不正确的论证

2. 否定假设的谬误

$$((p \to q) \land \neg p) \to \neg q$$

谓词和量词

谓词

一般来说，形为$P(x_1, x_2, ..., x_n)$的语句是命题函数P在n元组$(x_1, x_2, .., x_n)$的值，P也称为谓词。

量词

全称量词 ∀

∀ x P(x)对论域中任意一个x而言， P(x)的真值都为真。

$$\forall x P(x) \Leftrightarrow P(x_1) \land P(x_2) \land ... \land P(x_n)$$

存在量词 ∃

∃ x P(x) 在论域中存在一个x使P(x) 的真值为真

$$\exists x P(x) \Leftrightarrow P(x_1) \lor P(x_2) \lor ... \lor P(x_n)$$

量词的否定

$$\neg \forall x P(x) \Leftrightarrow \exists x \neg P(x)$$
$$\neg \exists x P(x) \Leftrightarrow \forall x \neg P(x)$$

逻辑等价

量词相关逻辑等价式 PPT或课本

嵌套量词

- 嵌套量词->出现在其他量词作用域内的量词

- 量词的顺序是重要的
- 嵌套量词的否定

量词有关推理法则

- 全称量词消去
- 全称量词引入
- 存在量词消去
- 存在量词引入

第二部分 集合论+函数

集合的基本概念及表示方法

一组对象形成集合，集合中的对象也叫做集合中的元素或成员

集合用大写字母表示，元素用小写字母表示

集合的描述：

- 花括号表示
- 集合构造符号 U Q Z S={x|P(x)}
- 文氏图

集合之间的关系

- 子集
- 集合相等
- 真子集

集合的势(基数)：集合中不同元素的多少

集合的幂集：集合S所有子集的集合

笛卡尔积

集合运算及运算性质

并、交、差、补集、对称差

重要运算性质

$$A - B = A \cap \bar{B}$$

集合恒等式

函数

函数的定义

一个从集合A到集合B的函数f：A->B

$$\forall a(a \in A \rightarrow \exists b(b \in B \wedge f(a) = b))$$

A叫做定义域，B叫做伴域

如果f(a)=b，那么a叫做b的原像，b叫做a的像

函数的类型

一对一函数　injective one to one

函数f称为一对一的或单射的，当且仅当对于f定义域中的所有的x,y,f(x)=f(y)蕴含x=y

也就是说，原像是唯一的

映上函数　onto surjective满射

从A到B的函数f叫做映上的或满射，当且仅当对每个b∈B,有元素a∈A使得f(a)=b

一一对应函数

一一对应函数，或双射函数，指的是又是射又是满射的函数

逆映射 one to one correspondence

令f为从集合A到集合B的一一对应，f的反函数是这样的函数，它指派给B中元素y的是A中使得f(x) = y唯一元素x。f的反函数用f^{-1}表示，于是在f(x) = y时$f^{-1}(y) = x$ ）

只有函数是双射函数时才有反函数

函数的复合

函数本质上是二元关系,所以可以象二元关系的复合那样来定义函数的复合.

定理: 设f: A->B，g:B->C，则

若f,g是满射，则g•f是满射。

若f,g是单射，则g•f是单射。

若f,g是一一映射，则g•f是一一映射。

集合的基数 Cardinality

有限集的基数就是有限集中元素的个数

集合等势

设A、B为任意两个集合，如果存在从A到B的双射，则称A与B等势

无限集可以与其真子集等势

定理：

- 等势关系是一个等价关系
- 无限集必与它的一个真子集等势（有限集与无限集的根本区别）

等势关系是一个等价关系，对每个等价类给出一个标志，该标志就是集合的势

与自然数集N的集合等势的集合势为$\aleph_0$

与(0,1)等势的集合的势为$\aleph$

A x B

设A，B是两个集合，若A B且A与B的某子集等势，则称A的势小于B的势，记为 |A|＜|B|.

用 |A|≤|B| 表示“ |A| 小于或等于 |B| ”

定理：

- |A|≤|B| ⇔ 存在A到B的单射
- 设A，B，C为任意集合，则

  1)|A|≤|A|

  2)|A|≤|B|，|B|≤|C| ⇒ |A|≤|C|

  3)|A|≤|B|，|B|≤|A| ⇒ |A| = |B|
- (三歧定理) 对任意集合A与B，|A|＜|B|，|B|＜|A|，|A| = |B|中恰有一个成立
- 对任意集合A，必有|A|＜|2^A|

第三部分 关系

关系的基本概念，表示方法

关系的基本概念

设A、B为任 意两个集合，称笛卡儿积A×B的子集R为集合A到B的一个二元关系。若(x, y)∈R， 则称x与y有关系R，记为xRy

- 关系R是一个集合

- $R \subseteq A \times B$

$$R = \{(a,b)|a \in A, b \in B, aRb\}$$

关系的表示方法

- 列出所有有序对
- 集合表示语言
- 二维表格
- 关系矩阵
- 有向图

关系的性质

自反、反自反、对称、反对称、传递

对称+传递->自反

关系的运算

关系是AXB的子集，可以按照两个集合组合的方式来组合两个A到B的关系

集合运算

交、并、补、差、对称差

通过关系矩阵运算

关系的合成

$$R = \{(a,b)|a \in A, b \in B, aRb\}$$
$$S = \{(b,c)|b \in B, c \in C, bSc\}$$
$$SoR = \{(a,c)|a \in A, c \in C, \exists b(b \in B \wedge aRb \wedge bSc)\}$$
$$SoR \neq RoS$$

如何计算？

- 定义
- 关系矩阵相乘

关系的幂

$$R^n = \begin{cases} R & \text{if n=1} \\ R^{n-1}oR & \text{if n>1} \end{cases}$$

定理

集合A上的关系R是传递的，当 且仅当对n=1，2，3…有

$$R^n \subseteq R$$

关系的逆

$$R = \{(a,b)|a \in A, b \in B, aRb\}$$
$$R^{-1}(R^c) = (b,a)|(a,b) \in R, a \in A, b \in B$$

几个有关的运算律

$$(SoT)^{-1} = T^{-1}oS^{-1}$$

关系的闭包

自反闭包 Reflexive Closure

R是A上的关系，R的自反闭包，记作r(R)

$$r(R) = R \cup I_A$$

如何计算自反闭包? 主对角线上全改为1

$$R\text{是自反关系} \iff R = R \cup I_A$$

对称闭包Symmetric Closure

R是A上的关系，R的对称闭包，记作s(R)

$$s(R) = R \cup R^{-1}$$

$$R\text{是对称关系} \iff R = R \cup R^{-1}$$

传递闭包Transive Closure

R的传递闭包是包含R的最小的具有传递性的关系

如何计算？

A为有限集，|A|=n，则

$$t(R) = \cup_{i=1}^{n} R_i$$

定理：R是集合A上的关系，则

- 若R是自反的，则s(R)和t(R)都是自反的
- 若R是对称的，则r(R)和t(R)都是对称的
- 若R是传递的，则r(R)是传递的

t(R)= R. 关系R的传递闭包等于连通性关系R.

传递闭包的计算->沃舍尔算法

等价关系，等价类，划分

等价关系

满足下列三个条件的关系，称为等价关系

- 自反的
- 对称的
- 传递的

一些术语

a和b等价

$$(a, b) \in R, R\text{是一个等价关系}$$

x关于R的等价类

R为集合A上的等价关系，对于每个$x \in A$，作集合

$$[x]_R = \{y \in A | xRy\}$$

等价类

R是A上的等价关系，$a \in A$，一切与a等价的元素构成的A的子集，叫做a的R-等价类，记作$[a]_R$或$[a]$

a称为$[a]_R$的代表元

等价关系才有等价类！！！

R是A上的等价关系，R的所有等价类构成的集合叫做A对R的商集，记作A/R

定理

1. 如果R1,R2是A上的等价 关系，那么R1∩R2也是A上的等价关系
2. 如果R1,R2是A上的等价关系，则R1∪R2在A上有自反和对称的关系
3. 如果R1,R2是A上的等价关系，则(R1∪R2)*是A上的等价关系
4. R是集合上的等价关系，则

$$aRb \iff [a] = [b] \iff [a] \cap [b] \neq \emptyset$$

划分

{A1,A2,..,An}是集合A的子集集合，该集合构成A的划分，当且仅当

- Ai $\neq \emptyset$
- $A_i \cap A_j = \emptyset$,when i != j
- A中的任意元素a，存在i使得a∈Ai

R为集合A上的等价关系，R的等价类构成S的划分

给定S的划分，存在等价关系R，以集合Ai，i=1，2，... 作为它的等价类

n元素的集合上有多少个不同的等价关系

$$B(0) = B(1) = 1$$

$$B(n+1) = \sum_{k=0}^{n} C_n^k B(k), n >= 1$$

偏序关系及偏序集

偏序关系

一个关系R是集合S上的偏序关系，则它满足：

- 自反的
- 反对称的
- 传递的

(S,R)叫做偏序集 poset或partial Ordering

可比与不可比

在偏序集(S,R)中，若元素a，b存在aRb或bRa，则称a,b可比

否则称a,b不可比

若偏序集中每一对元素都是可比的，那么S叫做全序集或线序集，R叫做全序或线序，一个全序也叫做链

字典序

词典排序是在两个偏序集的笛卡尔乘积上定义的偏序集。

哈塞图 Hasse Diagrams

用于描述偏序关系的一种方式

如何构造？

- 构造偏序关系的有向图
- 去掉所有的环
- 去掉冗余的边
- 一走所有有向边上的箭头

链和反链

偏序关系(A,≤)，$B \subseteq A$,如果(B,≤)是一个全序集，则B叫做(A,≤)的链

链的长度=|B|

B⊆A，对于B中任意不同的两个元素a,b ,(a,b),(b,a)都不属于关系≤，则B叫做(A,≤)的反链

极大(Maximum)元和极小(Minimal)元

a在偏序集(A,≤)中是极大(小)的，当不存在b∈A，使得a≤b(b≤a)

最大(Greatest)元和最小(Least)元

a是偏序集(A,≤)中的最大元素，当所有的b∈A，有$b \le a$，最小元素类似

最大元，最小元如果存在，则是唯一的

上界和下界

A为S的子集,如果a是S的元素使得对所有元b∈A，有$b \le a$，那么a叫做A的一个上界

下界定义类似

最小上界和最大下界

设〈P，≤〉是偏序集，A ⊆P，若a是A的上界，且对A 的任意上界b，有a≤b，则称a为A的最小上界（上确界），若a 是A的下界，且对A的任意下界b，有b≤a，则称a为A的最大下界 （下确界）

良序集 Well-ordered Sets

偏序集(A, R)，若A的非空子集均有最小元，则称其为良序集

良序集一定是全序集，反之不然。

格Lattices

如果一个偏序集的每对元素都有最小上界和最大下界，就称这个偏序集为格

所有的全序都是格，但并非所有的偏序集都是格

拓扑排序Topological Sorting

从一个偏序构造一个相容的全序叫做拓扑排序

代数系统

运算

设A是一个集合，A×A到A的映射称为A上的二元运算．一般地，A^n到A的映射称为A上的n元运算．

运算的结果

设f是A上的n元运算，对任意的x1 x2，…，xn∈A，f (<x1，x2，…，xn>)称作x1，x2，…，xn在 f 下的运算结果，并简记为f（x1，x2，…，xn）

运算封闭

设 f 是 A 上的n元运算，S ⊆ A，如果对x1，x2，…，xn∈S，恒有f（x1，x2，…，xn）∈S，则称S对运算f是封闭的．运算 f 在 S上是封闭的。

运算表

有限集的运算可以用一个表来表示

运算律

结合律、交换律、左分配律、右分配律、左消去律、右消去律

代数系统

设A是一个非空集合，f1，f2，…，fn是A上的运算（其元数可以不同），我们说A在运算f1，f2，…，fn下构成一个代数系统，记为<A，f1，f2，…，fn>．在不引起混乱的情况下，也可将其简记为A．

子代数系统

设<A，*>是代数系统，S ⊆ A，如果S对 * 封闭，则称<S，*>为<A，*>的子代数．

单位元

掌握概念 左、右单位元，单位元

定理:设代数系统〈A，∘〉中既有左单位元el，又有右单位元er，则 el＝er．

推论：代数系统〈A，∘〉中的单位元如果存在，则必定唯一．

逆元

逆元的概念

定理:设e是代数系统〈A，*〉的单位元， * 满足结合律，如果a∈A的左逆元b及右逆元c均存在，则b＝ c．

推论:设〈A，*〉是有单位元的代数系统， * 满足结合律．如果a∈A的逆元存在，则必定唯一．

幂等元

设〈A，*〉是一个代数系统，如果a∈A满足a * a ＝ a，称a为A的幂等元．

同态和同构

对<A，*>，<B，∘>，f：A→B，如果f保持运算，即：

$$\forall x，y \in A有f（x * y）=f（x）\circ f（y）$$

称f为<A，*>到<B，∘>的同态映射(同态)

同态和同构

设〈A，*〉，〈B，∘〉为两个代数系统，f：A→B 为A到B的同态.

如果f是单射，称f为单同态

如果f为满射，称f为满同态，称B是A在f下的同态象，记为f：A～B

如果f是双射，称f为同构映射（同构），这时称A与B在f映射下同构. 记为f：A ≅ B

定理

f是<A，*>到<B，·>的同态，

g是<B，·>到<C，△>的同态，则

g∘f是<A，*>到<C，△>的同态.

且当f，g均为单同态、满同态、同构时，g∘f也必是单同态、满同态、同构.

满同态保持结合律、交换律、单位元、逆元、幂等元

自同态，自同构

设〈A，*〉为一个代数系统，<A，>到自身的同态称为A的自同态，<A，>到自身的同构称为A的自同构

半群

满足结合律的代数系统叫做半群

半群的运算通常叫做乘法

a^n表示n个a做运算的结果

半群满足指数律

$$a^m a^n = a^{m+n}$$
$$(a^m)^n = a^{mn}$$

可交换半群

满足交换律的半群

可交换半群中有另一指数律：

$$(ab)^n = a^n b^n$$

可交换半群中的运算常用加法记号表示

指数律形式

$$ma + na = (m+n)a$$
$$m(na) = (mn)$$

幺半群

有单位元的半群

用加法记号时，单位元常用0表示，称为零元

幺半群若存在逆元，由于满足结合律，其逆元必唯一

幺半群中，用a^{-1}表示a的唯一逆元

当采用加法记号时，逆元常记作-a，叫做a的负元

子半群

设〈S，∘〉为一半群，若T ⊆ S 在S的运算∘下也构成半群，则称〈T，∘〉为〈S，∘〉的子半群.

实际上,只要T ⊆ S对运算∘封闭，则〈T，∘〉即为〈S，∘〉的子半群

〈S，*〉有单位元e，〈S，*〉的子半群未必有单位元，即使有的话，也未必等于e

设S是幺半群，若T是S的子半群，且S的单位元 e∈T，则称T是S的子幺半群.

群

群的相关概念

设〈G，*〉为幺半群，如果∀ a∈G，a的逆元a-1均存在，则称〈G，*〉为群.

一个代数系统<G,*>满足下列条件，则称之为群：

- 结合律成立 (半群)
- G中具有单位元(幺半群)
- G中任意元素a，都存在$a^{-1} \in G$是a的逆元

有限群

当群G中只含有有限个元素时，称其为有限群，否则称其为无限群

有限群G的元素个数称为群G的阶，并规定无限群G的阶为∞. 群G的阶也记为|G|.

交换群

满足交换律的群叫做交换群，也叫做Abel群

群的基本性质

定理1：重点

设〈G，*〉为群，则

（1）G中消去律成立.

（2）单位元e是G中唯一幂等元

定理2：

设〈G，*〉，〈H，◦〉是群，f 是G到H的同态．若e 为G的单位元,则 f（e）为H的单位元，且∀ a∈G，有

$$f(a)^{-1}=f(a^{-1}).$$

定理3：

设〈G，*〉是群，〈H，∘〉是任意代数系统，若存在G到H的满同态, 则<H，∘>必为群.

证明：满同态保持结合律，交换律，单位元，逆元

定理4：

设〈G，*〉是一个半群，且

（1）G中有一左单位元 e，使任意G中元素a

$$ea = a$$

（2）G中任一元素a，均有一“左逆元”

$$a^{-1}a = e$$

逆元的逆元

则G为群

证明：证明左逆元也是右逆元，再证明左单位元也是右单位元

定理5：

设〈G，*〉是半群，如果∀ a，b∈G，方程

$$ax=b$$
$$ya=b$$

在G中总有解，则G是群

定理6：

满足消去律的有限半群必为群

定理7：

有限群的运算表中，每一行(列)都是G中元素的一个全排列

子群与元素的周期

子群的相关概念

设〈G，*〉是一个群，H ⊆ G，如果H在G的运算下也构成群，则称〈H，*〉为〈G，*〉的子群.

任何群G都有两个平凡子群：｛e｝，G，其它子群称为真子群.

子群相关性质

子群保持单位元和逆元

定理1：

设H是群G的子群，则H的单位元 e' 就是G的单位元e. 对a∈H，a在H中的逆元 a' 就是a在G中的逆元a -1.

子群 保持运算，逆元则为群

定理2：

H是群〈G，*〉的非空子集，则H是G的子群 当且仅当

- ∀ a，b∈H 有a * b∈H
- ∀ a∈H ，a在G中的逆元a^{-1} ∈H.

推论：

设〈G，*〉为群，S是G的非空子集，则

S是G的子群 ⇔ ∀ a，b∈S a *b^{-1}∈S.

元素的周期

设G是群，a∈G，若存在正整数n，使$a^n = e$，则将满足该条件的最小正整数n称为a的周期（阶），若这样的n不存在，称a的周期为∞.

表示方法：

用| a|表示a的周期（阶）. 并将周期（阶）为n的元素称为n阶元素

元素周期的性质

定理：

设G是一个群，a∈G，

（1）a的周期等于a生成的循环子群（a）的阶，即

$$|a| = |（a）|$$

（2） 若a的周期为n <∞ ， 则

$$a^m = e \Leftrightarrow n|m.$$

推论：

设G为群，a∈G，若a的周期为n（或等价地说（a）的阶为n），则

$$（a）= \{a0，a1，...，an-1\}$$

循环群

循环群相关概念

设G是一个群，如果存在a∈G，使G ＝（a）＝ $\{a^i \mid i \in Z\}$ ，称G为由a生成的循环群，a称为其生成元.

循环群相关性质

定理1：

设〈G，*〉是一个循环群，若G是无限群，则

$$\langle G, * \rangle \cong \langle Z, + \rangle$$

若G是n阶群，则

$$\langle G, * \rangle \cong \langle Zn, +n \rangle$$

定理2：循环群的子群必为循环群

定理3:设〈G，*〉是n阶循环群，m是正整数且 m | n，则G中存在唯一一个m阶子群.