Chapter 1 预备知识

目录

1 集合, 关系, 函数

1.1 集合

定义 1 *康托尔集合论(朴素集合论):*

1. *集合可由任何有区别的对象组成;*
2. *集合由其组成对象整体唯一确定;*
3. *任何性质都确定一个具有该性质的对象的集合.*

朴素集合论因其定义的不严格性受到攻击, 此即第三次数学危机. 第三次数学危机以公理化集合论(ZFC公理集合论系统, 详见附录)的提出得到解决. 在组合数学中, 我们通常并不关心那些引起悖论的"集合"(如所有集合的集合等). 一定程度上我们可以接受集合的"朴素"的定义.

定义 2 *多重集是元素可重复出现的集合. 某个元素a_i出现的次数n_i称为该元素的重数.常将k个元素的多重集记作*

$$\{n_1 \cdot a_1, \ldots, n_k \cdot a_k\}$$

定义 3 *若存在集合X到集合Y的双射(见下文), 则称集合X与Y等势. 由此得到的关系为等价关系. 所有与某集合X等势的集合确定一个等价类, 称为X的基数类, 记为$cardX$.*

关于集合基数类的相关结论,可先阅读第二节了解函数和关系的相关内容后阅读.

对于有限集X, 设其有n个元素, 则$cardX = n$. 若$X \sim N_0$, 则记$cardX = \aleph_0$; 若$X \sim R$, 则记$cardX = \aleph$.

若集合X与集合Y的某个子集等势, 则说集合X的基数类不大于集合Y的基数类, 记为$cardX \leq cardY$.

$$(cardX \leq cardY) := (\exists Z \subset Y \mid cardX = cardZ)\,.$$

集合与自身的一部分等势是无穷集的特征. 戴德金曾以此为无穷集的定义.

上述不等关系可证明有以下性质:

1. $(cardX \leq cardY) \wedge (cardY \leq cardZ) \Rightarrow (cardX \leq cardZ)$(显然);

2. $(cardX \leq cardY) \wedge (cardY \leq cardx) \Rightarrow (cardX = cardY)$(施罗德-伯恩斯坦定理);

3. $\forall X \forall Y\,(cardX \leq cardY) \vee (cardY \leq cardX)$(康托尔定理).

故基数类是线性有序的(见下文). 施罗德-伯恩斯坦定理的证明:

证明 1 先证明一个引理:

引理 1 *(集合在映射下的分解定理):若有映射$f : X \to Y, g : Y \to X$, 则存在分解*

$$X = A \cup \tilde{A}, Y = B \cup \tilde{B}, \text{其中} f(A) = B, g\left(\tilde{B}\right) = \tilde{A}, A \cap \tilde{A} = \varnothing, B \cap \tilde{B} = \varnothing$$

引理的证明 1 设$M = \{E \subset X \mid E \cap g(Y \setminus f(E)) = \varnothing\}$, 易知$\varnothing \in M$. 令$A = \cup_{E \in M}$, 先证$A \in M$. 事实上$\forall E \in M\,(E \subseteq A)$, 故由 $E \cap g(Y \setminus f(E)) = \varnothing$ 可知 $E \cap g(Y \setminus f(A)) = \varnothing$ 故

$$A \cap g(Y \setminus f(A)) = (\cup_{E \in M} \cap g(Y \setminus f(A))) = \cup_{E \in M}(E \cap g(Y \setminus f(A))) = \varnothing$$

从而$A \in M$且为M中关于包含关系的最大元. 令$f(A) = B, \tilde{B} = Y \setminus B, \tilde{A} = g\left(\tilde{B}\right)$, 此时$A \cap \tilde{A} = A \cap g\left(\tilde{B}\right) = A \cap g(Y \setminus B) = A \cap g(Y \setminus f(A))\varnothing$.

下证$A \cup \tilde{A} = X$. 否则$\exists x_0 \in X\left(x_0 \notin A \cup \tilde{A}\right)$. 设$A_0 = A \cup \{x_0\}$, 则$\tilde{B} = Y \setminus f(A) \supseteq Y \setminus f(A_0)$. 故$\tilde{A} = g\left(\tilde{B}\right) \supseteq g(Y \setminus f(A_0))$.

$$\varnothing = A \cap \tilde{A} \supseteq A \cap g(Y \setminus f(A_0)) \Rightarrow A \cap g(Y \setminus f(A_0)).$$

$x_0 \notin \tilde{A} \Rightarrow x_0 \notin g(Y \setminus f(A_0)) \Rightarrow A_0 \cap g(Y \setminus f(A_0)) = (A \cup \{x_0\}) \cap g(Y \setminus f(A_0) = \varnothing)$

故$A_0 \in M$. 这与A是M中关于包含关系的最大元矛盾. 从而引理证毕.

回到题目. $\exists f : X \to Y, g : Y \to X$均为单射, 由引理,存在这样的分解 $X = A \cup \tilde{A}, Y = B \cup \tilde{B}, f(A) = B, g\left(\tilde{B}\right) = \tilde{A}$. 此时$f : A \to B, g : B \to A$均为双射.此时可作双射$F : X \to Y$, 其满足

$$x \to F(x) = \begin{cases} f(x), & x \in A; \\ g^{-1}(x), & x \in \tilde{A}. \end{cases}$$

从而$X \sim Y$. 原命题证毕.

定义

$$(cardX < cardY) := (cardX \leq cardY) \wedge (cardX \neq cardY).$$

定理 1

$$cardX < card\mathcal{P}(X)$$

证明 2 该结论对空集$\varnothing$显然成立.下考虑$X \neq \varnothing$. 因为$\mathcal{P}(X)$有X的所有单元素子集, 故$cardX \leq card\mathcal{P}(X)$. 下证$cardX \neq card\mathcal{P}(X)$.

否则存在$f : X \to \mathcal{P}(X)$, 考虑由不属于对应集合$f(x) \in \mathcal{P}(X)$的元素$x \in X$所组成的集合$A = \{x \in X \mid x \notin f(x)\}$. 由$A \in \mathcal{P}(X)$知$\exists a \in X(f(a) = A)$, 对这样的$a$,有$a \notin A \wedge a \in A$, 矛盾.

定义 4 **图**是一个有序二元组,通常记作$G = (V, E)$, 其中V是顶点的集合,也称为点集, E是V的所有2-子集(无序对,元素可重复)所组成集合的一个子集, 称为边集. **有向图**的定义类似, 只是E改为有序对集的子集.

关于图论的内容将在后续进行介绍.

1.2 关系, 函数

定义 5 设A, B为两个集合, 其**笛卡尔积*(Cartesion product)***定义为:

$$A \times B = \{(a, b) \mid a \in A, b \in B\} \tag{1}$$

当$|A| = m, |B| = n$时,易知$|A \times B| = mn$.

定义 6 一个从A到B的**二元关系**R, 记为$R : A \to B$, 定义为$A \times B$的一个子集.

若有$A \subseteq A', B \subseteq B'$, 则$R \subseteq A \times B \subseteq A' \times B'$. 同一个关系可以作为不同集合的子集给出.

包含某关系的定义域的集合称为该关系的出发域, 包含某关系值域的集合称为该关系的的到达域. $(x, y) \in R$常写为xRy, 称为x与y的关系为R.

定义 7 $\mathcal{R}^{-1} = \{(b, a) \mid (a, b) \in \mathcal{R}\}$称为关系$\mathcal{R}$的逆关系.

定义 8 如果关系$\mathcal{R}_1 : X \to Y, \mathcal{R}_2 : Y \to Z$中$\mathcal{R}_\in$定义于$R_1$的值域,则可构造一个新的关系$\mathcal{R}_1 \circ \mathcal{R}_2 : X \to Z$, 其满足

$$x\mathcal{R}_1 \circ \mathcal{R}_2 z \Leftrightarrow ((x \in X) \wedge (z \in Z) \wedge \exists y \in Y(x\mathcal{R}_1 y \wedge y\mathcal{R}_2 z))$$

该关系称为关系$\mathcal{R}_1$与$\mathcal{R}_2$的复合.

对于有限集X, Y上的关系$\mathcal{R} \subseteq X \times Y$, 我们可以用关系图, 关系矩阵等方式表示.

关系图一般用于描述一个集合X上的关系

定义 9 设集合X上有关系$\mathcal{R}$, 则有向图$G = (X, V)$称为集合X上的**关系图**, 其中对于有向边$\left(x_i, x_j\right)$, $\forall x_i, x_j \in X$,

$$\begin{cases} \left(x_i, x_j\right) \in V, & x_i \mathcal{R} x_j; \\ \left(x_i, x_j\right) \notin V, & \neg x_i \mathcal{R} x_j. \end{cases}$$

定义 10 设集合X, Y上有关系$\mathcal{R}, cardX = m, cardY = n$, 则矩阵$A = \left(a_{ij}\right)_{m \times n}$称为关系$\mathcal{R}$的关系矩阵, 若其满足

$$a_{ij} = \begin{cases} 1, & x_i \mathcal{R} y_j; \\ 0, & \neg x_i \mathcal{R} y_j. \end{cases}$$

定义 11 对于一个关系$\mathcal{R}$, 若其满足以下性质:

- $a\mathcal{R}a$(自反性);
- $a\mathcal{R}b \Rightarrow b\mathcal{R}a$(对称性);
- $(a\mathcal{R}b) \wedge (b\mathcal{R}c) \Rightarrow a\mathcal{R}c$(传递性)

则关系$\mathcal{R}$为等价关系. $a\mathcal{R}b$可记为$a \sim b$.相互等价的元素的全体构成等价类.

常见的等价关系: 相等关系; 模同余关系; 集合的等势关系; 同余关系(代数);函数局部相等关系(此时等价类为在某点的函数芽).

定义 12 对于一个关系$\mathcal{R}$, 若其满足以下性质:

- $a\mathcal{R}a$(自反性);
- $(a\mathcal{R}b) \wedge (b\mathcal{R}a) \Rightarrow a = b$(反对称性);
- $(a\mathcal{R}b) \wedge (b\mathcal{R}c) \Rightarrow a\mathcal{R}c$(传递性)

则关系$\mathcal{R}$为偏序关系.$a\mathcal{R}b$可记为$a \preceq b$. 若也有

$$\forall a \forall b \left((a\mathcal{R}b) \vee (b\mathcal{R}a)\right)$$

即X中任意两元素可比, 则$\mathcal{R}$称为序关系, 定义序关系的集合X称为线性序集

常见的偏序关系:集合的包含关系, 数的不小(大)于关系; 整数的整除关系, 线性空间的包含关系.

定义 13 若关系$\mathcal{R}$满足

$$(x\mathcal{R}y_1) \wedge (x\mathcal{R}y_2) \Rightarrow (y_1 = y_2)$$

则其称为函数关系.常用符号f表示函数, 用记号$y = f(x)$或$x \overset{f}{\mapsto} y$. 此时X称为函数的定义域, x为函数的自变量, Y称为函数的值域, y为函数的函数值.

若两个函数f_1, f_2具有相同的定义域, 且在每个$x \in X$上$f_1(x) = f_2(x)$, 则两个函数相同.

定义 14 函数也称为映射.若$\forall x_1, x_2 \in X(f(x_1) \neq f(x_2))$,则$f$为单射; 若$f(X) = Y$, 则$f$为满射.若$f$既为单射也为满射, 则称$f$为双射.

2 偏序集

定义 15 设X是一个非空集合, P是定义在X上的偏序关系, 则称$\mathbf{P} = (X, P)$为一个偏序集*(Partial ordered set)*. 不引起混淆的情况下,有时也直接称X为一个偏序集.

例 1 设$\mathbb{Z}^+$为全体正整数集合,对于$a, b \in \mathbb{Z}^+$, 规定$a \preceq b$当且仅当$a|b$. 此时易验证$\mathbb{Z}^+$为偏序集.

例 2 设S为一集合,$\mathcal{P}(S)$为其子集之集, 规定$a \preceq b$当且仅当$A \subseteq B$, 此时易验证$\mathcal{P}(S)$为偏序集. 当S为无限集时, 考虑其有限子集之集有类似的性质.

偏序集的关系图称为Hasse图. 其图示特性为:若$a \preceq b$, 则a在b下方,且连接以一条线.

2.1 链, 反链

定义 16 给定偏序集$\mathbf{P} = (X, P)$, 若对X中任意两元素x, y, $x \preceq y \vee y \preceq q$, 则称$\mathbf{P}$为一全序集或线性序集,也称为**链**. 若$\neg(x \preceq y) \wedge \neg(y \preceq x)$, 则称$\mathbf{P}$为**反链**.

应注意到链与反链的定义并不是完全对称的. 在下文Dilworth定理中我们可以看到这样的区别.

定义 17 给定偏序集$\mathbf{P} = (X, P)$, 若X'是X的子集, 则易验证P在X上的限制也是一个偏序集. 称$\mathbf{P}' = (X', P)$为$\mathbf{P}$的**子偏序集**. 偏序集(X, P)的最长子链的长度称为这个偏序集的**高度**, 最长子反链的长度称为这个偏序集的**宽度**.

例 3 考虑偏序集$(\mathbb{Z}^+, |)$, 易知其一子偏序集$\left(\left\{m \mid m = 2^k, k \in \mathbb{N}\right\}, |\right)$是其一子链, 另一子偏序集$\left(\left\{p \mid p\text{为素数}\right\}, |\right)$是其一子反链. 我们易知它有无穷大的高度和宽度.

我们易知对一偏序集$\mathbf{P}$的一个子链A和一个子反链B, $card\,(A \cap B) \leq 1$. 其证明留给读者.

定义 18 偏序集X的极小元是X中的一个元素a,满足$x \neq a \Rightarrow (\neg x \leq a)$; 偏序集$X$的极大元是$X$中的一个元素$b$,满足$x \neq b \Rightarrow (\neg b \leq x)$;

定义 19 偏序集X的最小元是X中的一个元素a, 使得$\forall x \in X\,(a \leq x)$; 偏序集$X$的最大元是$X$中的一个元素$b$, 使得$\forall x \in X\,(x \leq b)$;

2.2 Dilworth定理, 反链分解算法

定理 2 设偏序集$(X, \leq)$的高度为n, 则存在划分$X = \bigcup_{i=1}^{n} A_i$, 使得每个$A_i$都是反链.

证明 3 首先注意不可能将X划分为更少的链. 下面对n归纳.

当$n = 1$时,结论显然. 假设结论对$n-1$成立, 下面考虑n的情形. 设A_1为X的所有极大元素组成的集合, 则A_1为一个反链. 若$X \setminus A_1$中有长度为n的链,则此链的最后一个元素为X中的极大元, 其属于A_1, 矛盾. 因此$X \setminus A_1$高度为$n-1$. 由归纳假设其可划分为$n-1$个反链, 从而X可划分为n个反链.证毕.

定理 3 ***Dilworth*定理**: 设有限偏序集$(X, \leq)$的宽度为m, 则存在划分$X = \bigcup_{i=1}^{m} C_i$, 使得每个$C_i$都是链.

证明 4 易知X不可能被划分为更少的链. 对$cardX$归纳.

当$cardX = 1$时结论显然. 假设结论对$cardX < K$成立, 考虑$cardX = K$的情况. 设C_1为X的一个极大链(即X中无其他的链真包含C_1),考虑偏序集$X \setminus C_1$, 若其宽度为$m-1$, 则归纳可知结论成立.

若$X \setminus C_1$的宽度为m, 设$\{a_1, \ldots, a_m\}$为$X \setminus C_1$的一条反链. 定义$S^- = \{x \in X \mid \exists i\,(x \leq a_i)\}, S^+ = \{x \in X \mid \exists i\,(x \leq a_i)\}$, 因为$(X, \leq)$的宽度为$m$, 可知

$$X = S^- \cup S^+, S^- \cap S^+ = \{a_1, \ldots, a_m\}$$

C_1为极大链, 故其最大元不在S^-中. 由归纳假设知, S^-可被划分为m个链$S_1^-, \ldots, S_m^-$. 易验证a_i为S_i^-的最大元. 事实上, 若$x \in S_i^+ \wedge x > a_i$, 由$x \in S^-$知存在$j$使得$x \leq a_j$. 故$a_i \leq x \leq a_j$. 矛盾. 同理可将$S^+$分解为$m$个链$S_1^+, \ldots, S_m^+$, 且$a_i$为$S_i^+$的最小元. 对任一$1 \leq i \leq m$把$S_i^-$和$S_i^+$通过$a_i$连接起来, 就把$X$划分为$m$个链.

思考:为什么上述两定理对偏序集的要求不同.

由上述定理我们可以通过抽屉原理/鸽巢原理自然地得到下述结论:

定理 4 在任一含mn+1个元素的偏序集**P**中, 或有一长度至少为m+1的链(即**P**的高度$\geq m+1$), 或有一宽度至少为$n+1$的反链(即**P**的宽度$\geq n+1$).

由**定理2**的证明过程我们可以得到有限偏序集的反链分解算法. 其为一递归算法.

算法 1 反链分解算法:
输入:偏序集A;
输出:偏序集中的反链$B_1, \ldots, B_n$, 其中n为A的宽度. *Step 1:* $i = 1$;
Step 2: B_i为A_i中极大元的集合(其为一反链);
Step 3: $A = A \setminus B_i$(其宽度-1);
Step 4: if $A \neq \varnothing$ $i++$, 转向2; *else end.*

3 初等计数方法

初等技术方法的计数原理是加法原理与乘法原理,两者分别对应不同情形和独立步骤.

3.1 排列组合与多重排列组合

定义 20 排列数即

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

其计数的是在n个元素中取出r个排成一排的方案数. 我们特别地规定当$r > n$时$P(n,r) = 0$.

定义 21 组合数即

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

读作"n选取r",计数的是从n个元素中选取r个的方案数.我们特别地规定当$r > n$时$C(n,r) = 0$.

定义 22 参数为$n, r_1, \ldots, r_k$的**多重选取数**即

$$\binom{n}{r_1, \ldots, r_k} = \frac{n!}{r_1! \ldots r_k!}$$

其中$\sum_{i=1}^{k} r_i = n$.

事实上,其组合意义可由组合数公式和乘法原理得到.

定义 23 从n个不同元素中取出r个排成一个圆环的方法数称为环排列数/圆排列数,其为

$$\frac{n!}{(n-r)!} \cdot \frac{1}{r}$$

这是因为任一排列有其他$r-1$个排列与其生成的环排列相同.

例 4 把集合$[n] = \{1, 2, \ldots, n\}$划分为$b_i$个$i$-子集, $i = 1, \ldots, k$, 满足$\sum_{i=1}^{k} ib_i = n$, 求分解方法数.

解 1 n个元素的全排列有$n!$种, 对于每个划分, b_i个i子集没有顺序, 每个集合的元素也没有顺序, 故每个划分对应着$b_1! \ldots b_k! (1!)^{b_1} \ldots (k!)^{b_k}$个不同的$n$-排列,故方法数为

$$\frac{n!}{b_1! \ldots b_k! (1!)^{b_1} \ldots (k!)^{b_k}}$$

或根据多重选取数考虑,为

$$\frac{\binom{n}{1,\ldots,1,\ldots,k,\ldots,k}}{b_1! \ldots b_k!}$$

其中多重选取数中有b_i个i. 上述两结果是相等的.

例 5 集合$[n] = \{1, 2, \ldots, n\}$到自身的双射(即$n$元置换)在映射合成下构成一群$S_n$, 任意置换$\sigma$可表示为$S_n$中互不相交的轮换之积, 这种表示方式在不考虑轮换次序的意义下唯一, 称为σ的轮换分解. $l_i(\sigma)$表示σ的轮换分解中长度为i的轮换个数, 则$(l_1(\sigma), \ldots, l_n(\sigma))$称为$\sigma$的**轮换型号**. 对$1 \cdot l_1 + \ldots + n \cdot l_n = n$, 轮换型号为$(l_1, \ldots, l_n)$的置换有多少个?

解 2 类似地,结果为

$$\frac{n!}{b_1! \ldots b_n! (1!)^{b_1} \ldots (n!)^{b_n}} \cdot \prod_{i=1}^{n} ((i-1)!)^{l_i} = \frac{n!}{b_1! \ldots b_n! 1^{b_1} \ldots n^{b_n}}$$

定理 5 从n个不同元素中取r个元素作允许重复的组合(即允许组合$\{a_1,\ldots,a_r\}$中$i\neq j\wedge a_i=a_j$), 其方案数为$\binom{n+r-1}{r}$.

只需要通过$b_i=a_i+i-1$进行对应即可. 证明过程留做习题.

定理 6 从n个线序不同元素中取r个作不相邻组合, 其组合数为$\binom{n-r+1}{r}$

证明类似.留做习题.

例 6 线性方程$x_1+\ldots+x_n=b$的非负整数解数为$\binom{n+b-1}{b}$

证明 5 方程的每个非负整数解$(\xi_1,\ldots,\xi_n)$对应一个将b个无区别的球放入n个有标志的盒子的情况, 其数目等于从1到n中取b个作可重组合,其组合数为

$$\binom{n+b-1}{b}$$

事实上也可以通过插空法证明.

3.2 十二重计数方法

对于一般的将n个球放入m个篮子的方法数问题, 其用映射的严格数学语言描述如下:

例 7 设集合A的基数为n, 集合B的基数为m, 有多少从A到B的满足一定条件的映射$f:A\to B$?

根据A,B的元素是否可区分以及f为单射,满射或不加限制,共有12种情况. 其中f为单射说明每个"篮子"至多放一个球, 满射说明每个"篮子"均不能空.

其中$(m)_n$表示$m(m-1)\ldots(m-n+1)$, $S(n,i)$, $p_i(n)$分别为第二类Stirling数和分拆数,

$$\sigma(n\leq m)=\begin{cases}1, & n\leq m;\\ 0, & otherwise\end{cases}$$

集合A中的元素(基数为n)	集合B中的元素(基数为m)	映射f	f的个数
各自不同	各自不同	不加限制	m^n
各自不同	各自不同	单射	$(m)_n$
各自不同	各自不同	满射	$m!S(n,m)$
各自不同	全部相同	不加限制	$\sum_{i=1}^{m} S(n,i)$
各自不同	全部相同	单射	$\sigma(n \le m)$
各自不同	全部相同	满射	$S(n,m)$
全部相同	各自不同	不加限制	$\binom{n+m-1}{n}$
全部相同	各自不同	单射	$\binom{m}{n}$
全部相同	各自不同	满射	$\binom{n-1}{m-1}$
全部相同	全部相同	不加限制	$\sum_{i=1}^{m} p_i(n)$
全部相同	全部相同	单射	$\sigma(n \le m)$
全部相同	全部相同	满射	$p_m(n)$

3.3 排列和组合的生成算法

3.3.1 排列:递增进制序法

排列生成的递增进制序法基于以下事实.

定理 7 对$n \in \mathbb{N}, \forall 0 \le m \le n! - 1, \exists a_1, \ldots, a_{n-1}, 0 \le a_i \le i,$ 使得

$$m = \sum_{i=1}^{n-1} a_i \cdot i!$$

且这样的表示是唯一的.

证明 6 设

$$m_i = \begin{cases} m, & i = 1; \\ \frac{m_{i-1} - a'_{i-1}}{i}, & 2 \le i \le n-1; \end{cases}, \text{其中} a'_i \equiv m_i (mod i+1), 0 \le a'_i \le i$$

我们易知a'_i即为所求得a_i, 且这样的a'_i是唯一的.

由此,我们建立了一个非负整数$0 \le m \le n! - 1$与序列$(a_{n-1}, \ldots, a_1)$的一一对应. 下面我们建立序列与全排列的一一映射. 此时数m称为排列的**序数**, 这样的序列称为排列的**中介数**.

取a_i表示数$i+1$在此排列中的位置的右方比数$i+1$小的数的个数,$i = n - 1, \ldots, 1$. 此时生成排列的方法为递增进制序法.

例 8 对于数$1,2,3,4$的一个排列4213, 4右方比它小的数的个数为3, 故$a_3 = 3$; 类似地,有$a_2 = 0, a_1 = 1$, 故此排列的中介数为(301), 其序数$m = 3 \cdot 3! + 0 \cdot 2! + 1 \cdot 1! = 19$.

考虑这样的中介数实质上是一个变进制数, 我们可以基于变进制数的运算法则通过一个中介数得到其下一中介数(即满足序数+1的中介数).

3.3.2 排列:递减进制序法

排列生成的递减进制序法基于以下事实.

定理 8 对$n \in \mathbb{N}, \forall 0 \leq m \leq n! - 1, \exists a_2, \ldots, a_n, 0 \leq a_i \leq i$, 使得

$$m = \sum_{i=2}^{n} \frac{a_i \cdot n!}{i!}$$

且这样的表示是唯一的.

证明留做习题.

取a_i表示为数i在此排列中的位置的右方比数i小的数的个数,$i = 2, \ldots, n$, 此时生成排列的方法为递减进制序法. 数m为称为排列的序数, 序列$(a_2, \ldots, a_n)$称为排列的中介数.

采用递减进制序法的好处在于, 通过中介数得到新的排列时进位次数较少.

3.3.3 排列:字典序法

排列生成的字典序法基于线性序集中序关系的传递性. 对一n元线性序集, 我们易知其同构于集合$[n] = \{1, \ldots, n\}$. 我们只需要考虑$[n]$的排列即可.

对$[1]$, 其排列是唯一的. 对集合$[n]$, 我们依次取序关系中的最小元至最大元(此时为1至n)作为排列的第一个元素. 对取$x \in [n]$的情况, 我们考虑线性序集$[n] \setminus \{x\}$生成的排列, 它们作为排列的后续元素.

例 9 对于$[3]$, 我们依次取元素$1,2,3$作为排列的第一个元素. 取1时$[3] \setminus \{1\} = \{2,3\}$. 对此集合依次取元素$2,3$作为排列的第二个元素, 得到的集合分别为$\{3\}, \{2\}$. 故生成的排列依次为$123, 132$. 类似地得到排列$213, 231, 312, 321$.

字典序法中, 我们从一个排列得到它的下一个排列时, 需要考虑我们对上述递归过程已进行到哪一步. 这意味着我们需要找到我们已遍历过哪些

子集的排列.事实上我们只需要从末位出发向前找到最大单调增序列, 即对排列$P_1 \dots P_n$, 寻找最小的k, 使得排列$P_k \dots P_n$是严格递减的. 这说明我们已经遍历过集合$\{P_k, \dots, P_n\}$的排列. 若$k = 1$, 则我们已经遍历$[n]$所有的排列; 对$k \geq 2$, 我们考虑集合$\{P_{k-1}, P_k, \dots, P_n\}$.

设在给定序关系下P_{k-1}的后继为x, 则由我们已考虑所有以$\{P_{k-1}, P_k, \dots, P_n\} \ni p \leq x \wedge p \neq x$为原排列第$k-1$位的排列, 且未考虑所有以$x \leq q \in \{P_{k-1}, P_k, \dots, P_n\}$的$q$作为原排列的第$k-1$个元素的排列, 知我们应开始考虑以$x$为原排列第$k-1$位的排列, 即对原排列的下一排列$P'_1 \dots P'_n$, 有$P'_{k-1} = x$. 易知$P'_k, \dots, P'_n$为$\{P_{k-1}, P_k, \dots, P_n\} \setminus \{x\}$ 中元素的递增排列. 我们用一个直观的例子来理解.

例 10 字典序下$[4]$的一排列为2431, 我们可知此时431为满足上述条件的子排列. 这说明当2为排列的第1位时我们已经遍历了线性序集$\{1, 3, 4\}$的排列. 我们接下来只需要考虑集合$\{1, 2, 3, 4\}$中2的后继, 即3, 作为排列的第1位时的情况. 对于集合$\{1, 2, 3, 4\} \setminus \{3\} = \{1, 2, 4\}$, 其递增排列为124. 故其下一排列为3124.

基于上述给出的排列的顺序关系, 我们可以得到字典序法的排列的序数和中介数. 我们易知给定前i位时排列有$(n-i)!$种, 而第i位有$(n-i+1)$种取法. 我们因而可以给出递增进制的中介数$(a_1 \dots a_{n-1}), 0 \leq a_i \leq n-i$. 其对应序数为$m = \sum_{i=1}^{n-1} a_i (n-i)!$. 其中$a_i$表示排列中$P_i$右边比$P_i$小的数的个数.

3.3.4 排列:换位法

排列生成的换位法基于排列的奇偶性

定义 24 排列$P = P_1 \dots P_n$中若$1 \leq i < j \leq n \wedge P_i > P_j$, 则$P_i, P_j$构成一组逆序. 排列中逆序的对数称为排列的逆序数. 若排列的逆序数为奇数, 则排列称为奇排列; 若为偶数, 则称为偶排列.

记s_i为P_i右侧比P_i小的数的个数, 则逆序数为$\sum_{i=1}^{n-1} s_i$.

定义 25 换位法中数的方向:对排列$P = P_1 \dots P_n$, 数$k \geq 2$的方向为左当且仅当排列中$1, \dots, k-1$的排列为偶, 方向为右当且仅当排列中$1, \dots, k-1$的排列为奇. 数$k = 1$的方向为左.

值得注意的是,$k = 2$时排列1恒为偶排列, 故2的方向恒为左.

例 11 考虑排列15243, 易知1, 2方向为左. 排列1, 2为偶排列, 故3方向为左; 排列1, 2, 3为偶排列, 故4方向为左; 排列1243为奇排列, 故5方向为右. 因此,此排列方向为

$$\overleftarrow{1}\ \overrightarrow{5}\ \overleftarrow{2}\ \overleftarrow{4}\ \overleftarrow{3}$$

换位法的中介数由递减进制数$a_2 \dots a_n$给出, 序数为$m = \sum_{i=2}^{n} \frac{a_i \cdot n!}{i!}$. 其中$a_i$在$i$上箭头朝左时表示$i$右边比$i$小的数的个数, 在$i$箭头朝右时表示$i$左边比$i$小的数的个数.

对于换位法得到的排列$P = P_1 \dots P_n$, 其下一排列的生成方法如下: 设$P_i = n$.

- 若n方向朝左且$i \neq 1$, 则下一排列$P' = P_1 \dots P_{i-2} P_i P_{i-1} P_{i+1} \dots P_n$;
- 若n方向朝左且$i = 1$, 则对排列$P_2 \dots P_n$递归调用此算法;
- 若n方向朝右, 类似上述, 只是方向由左变右, 由判断$i = 1$变为判断$i = n$.

4 组合恒等式

4.1 二项式定理

定理 9 二项式定理:设n为正整数, 则

$$(x+y)^n = \sum_{i=1}^{n} \binom{n}{k} x^k y^{n-k}$$

可通过数学归纳法或组合意义证明. 二项式定理有许多平凡推论. 下特别提出其中一条, 并给出其组合证明:

定理 10 设$n \geq 1$, 则

$$\sum_{k\text{为奇数}} \binom{n}{k} = \sum_{k\text{为偶数}} \binom{n}{k}$$

证明 7 设$X = \{1, \dots, n\}$, $A = \left\{S \subseteq X \mid card\ S \text{为偶数} \wedge 1 \in S\right\}$, $B = \left\{S \subseteq X \mid card\ S \text{为奇数} \wedge 1 \in S\right\}$, $C = \left\{S \subseteq X \mid card\ S \text{为偶数} \wedge 1 \notin S\right\}$, $D = \left\{S \subseteq X \mid card\ S \text{为奇数} \wedge 1 \notin S\right\}$.

考虑映射$f : A \to D$为$f(S) = S \setminus \{1\}$, 易知其为双射. 故$card\ A = card\ D$.

同理$card\ B = card\ D$.故

$$LHS = card\ B + card\ D = card\ A + card\ C = RHS$$

证毕.

4.2 比较系数法, 组合恒等式

比较系数法为比较同一多项式或级数的两种不同表示方法的某项系数得到等式, 为富比尼原理(又称算二次原理)的一种特例.

定理 11 *Vandermonde*恒等式*:* 设$n, m, k \geq 0$, 则

$$\binom{m+n}{k} = \sum_{i=0}^{k} \binom{m}{i}\binom{n}{k-i}$$

证明 8 比较等式$(x+1)^{m+n} = (x+1)^m (x+1)^n$两侧$x^k$的系数.

左式中系数为*LHS*, 右式中系数为*RHS*. 从而证毕.

推论 1 在*Vandermonde*恒等式中令$m = n = k$,则有

$$\binom{2n}{n} = \sum_{i=0}^{n} \binom{n}{i}^2$$

推论 2 *Pascal*恒等式*:* 在*Vandermonde*恒等式中令$m = 1$, 则有

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$

Pascal恒等式即为杨辉三角中某数等于两肩上数之和.

定理 12 朱世杰恒等式*:* 设$n, m \geq 0$, 则

$$\binom{m+n+1}{n+1} = \sum_{i=0}^{m} \binom{n+i}{n}$$

证明 9 比较等式$(x+1)^{m+n+1} = (x+1)\ldots(x+1)$两端$x^{n+1}$的系数.

左式中系数为*LHS*, 右式中x^{n+1}项系数可看作从$m+n+1$项中选取$n+1$项利用其x的方法数. 第一个x从第i个式子中选取时, 剩余$m+n+1-i$项中选取其他n个x, 此时有$\binom{m+n+1-i}{n}$种选取方式. 从而右式种x^{n+1}系数为

$$\sum_{i=1}^{m+1} \binom{m+n+1-i}{n} = \sum_{i=0}^{m} \binom{n+i}{n}$$

证毕.

定理 13 *Lucas*定理*:*设p是一个素数, 将m, n写为p进制数*:*$m = \sum_{i=0}^{k} a_i p^i, n = \sum_{i=0}^{k} b_i p^i$, 其中$0 \leq a_i, b_i < p, i = 0, \ldots, k$, 则

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{a_i}{b_i} (mod p)$$

证明 10 注意到当$1 \leq j \leq p^i - 1, i \geq 1$时$\binom{p^i}{j} = \frac{p^i}{j}\binom{p^i-1}{j-1}$为正整数, 但此时或$\gcd\left(p^i, j\right) = 1$, 此时$\frac{1}{j}\binom{p^i-1}{j-1}$为正整数, 故$p|p^i\frac{1}{j}\binom{p^i-1}{j-1}$; 或$\frac{p^i}{j} = p^k$, 其中$1 \leq k \leq i$, 此时$p|p^k\binom{p^i-1}{j-1}$. 因此,$p|\frac{p^i}{j}\binom{p^i-1}{j-1}$. 故

$$(1+x)^{p^i} = 1 + x^{p^i} + \sum_{j=1}^{p^i-1}\binom{p^i}{j}x^j \equiv 1 + x^{p^i}(mod p)$$

上式在$i = 0$时依然成立. 故

$$(1+x)^m = (1+x)^{\sum_{i=0}^k a_i p^i} = \prod_{i=0}^k\left((1+x)^{p^i}\right)^{a_i} \equiv \prod_{i=0}^k\left(1+x^{p^i}\right)^{a_i} = \prod_{i=0}^k\left(\sum_{j_i=0}^{a_i}x^{p^i j_i}\binom{a_i}{j_i}\right)(mod p)$$

比较上式两端x^n系数. 左式中系数为LHS. 由n表示为p进制数的唯一性, $n = \sum_{i=0}^k b_i p^i$,可得右式中x^n的系数为

$$\prod_{i=0}^k\binom{a_i}{b_i}(mod p)$$

从而证毕.

尽管$\binom{m}{n}$可能非常大, 应用Lucas定理可以相对容易地求出其模p的余数.

5 习题及参考解答

A 附录:公理化集合论

A.0.1 外延公理

任何集合A与集合B相等,当且仅当它们所具有的各元素是相同的.

$$A = B \Leftrightarrow \forall x\left((x \in A) \Leftrightarrow (x \in B)\right)$$

A.0.2 分离公理

任何集合A和性质P都对应一个集合B, 其元素是且仅是A中具有性质P的各元素.

$$A\text{为一集合} \Rightarrow B\{x \in A \mid P(x)\}\text{为一集合}$$

由分离公理, 任何集合X都有空子集$\varnothing_X = \{x \in X \mid x \neq x\}$, 而由外延公理, 对任意集合$X, Y$, $\varnothing_X = \varnothing_Y$, 即空集是唯一的.

由分离公理, 如果A, B为集合, 则$A \setminus B = \{x \in A \mid x \notin B\}$也是集合.

A.0.3 并集公理

对于集合的任何集合M(集合族 M), 存在一个被成为集合M的并集的集合$\cup M$, 其元素是且仅是M的各元素包含的那些元素.

$$x \in \cup M \Leftrightarrow \exists X ((X \in M) \wedge (x \in X))$$

由并集公理和分离公理, 可以定义集合(族)M的交集为集合

$$\cap M := \{x \in \cup M \mid \forall X ((X \in M) \Rightarrow (x \in X))\}$$

A.0.4 配对公理

对于任何集合X, Y, 存在一个集合Z, 其元素仅为X, Y.

集合Z记为$\{X, Y\}$, 成为集合X, Y的无序偶. 若$X = Y$, 则Z由一个元素组成.

A.0.5 子集之集公理

对于任何集合X, 存在一个集合$\mathcal{P}(X)$, 其元素是且仅是X的各子集.

设$x \in X, y \in Y$, 序偶(x, y)确实构成集合

$$X \times Y := \{p \in \mathcal{P}(\mathcal{P}(X) \cup \mathcal{P}(Y)) \mid p = (x, y) \wedge (x \in X) \wedge (y \in Y)\}$$

上述公理限制了形成新集合的可能性, 例如由康托尔定理 $cardX < card\mathcal{P}(X)$, 故一切集合的集合并不存在.

A.0.6 无穷公理

定义$X^+ = X \cup \{X\}$, 称为集合X的后继集. 若一个集合包含空集以及自身任何一个元素的后继集, 则称该集合为归纳集. 无穷公理:归纳集存在.

可根据上述公理建立自然数集$\mathbb{N}_0$的标准模型(冯·诺伊曼方案). $\mathbb{N}_0$的元素是集合

$$\varnothing, \varnothing^+ = \varnothing \cup \{\varnothing\} = \{\varnothing\}, \{\varnothing\}^+ = \{\varnothing\} \cup \{\{\varnothing\}\}, \ldots$$

我们用符号$0, 1, 2 \ldots$表示它们, 称它们为自然数.

A.0.7 替换公理

设$\mathcal{F}(x, y)$是以下命题(确切地说是一个公式):对于集合X中的任何元素x_0, 存在唯一的对象y_0, 使得$\mathcal{F}(x_0, y_0)$成立. 你们满足以下条件的对象y组成一个集合:存在$x \in X$, 使得$\mathcal{F}(x, y)$成立.

A.0.8 选择公理

对于任何由互不相交非空集合组成的集合族, 存在集合C,使得对于该集合族中的任何集合X, 集合$X \cap C$只由一个元素组成.

前7个公理构成ZF(策梅洛-弗伦克尔)公理系统, 加上选择公理构成ZFC公理系统. 选择公理曾引起激烈讨论.

图 1: 不得已.jpg