

# Discrete

## Mathematics - P131

麦卡锡91函数 (McCarthy 91 function) 是计算机科学中用于形式验证的一个测试案例

a test case for formal verification within computer science

递归地定义函数  $M(n)$ , 其中  $n \in \mathbb{Z}^+$

$$M(n) = \begin{cases} n-10 & n > 100 \\ M(M(n+1)), & n \leq 100 \end{cases}$$

$\text{McCarthy} :: \text{Int} \rightarrow \text{Int}$

$\text{McCarthy } n$

$$\quad | n > 100 = n - 10$$

$$| \text{otherwise} = \text{McCarthy} (\text{McCarthy} (n+1))$$

麦卡锡91函数  $M(n)$  是从正整数集合到正整数集合的良定义函数

对于  $n > 100$ ,  $M(n) = n - 10$ , 于是  $M: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$  在  $n > 100$  时是良定义的

对于  $1 \leq n \leq 100$ , 首先考虑  $90 \leq n < 101$  的部分

$$\begin{aligned} \text{有 } M(90) &= M(M(90+1)) = M(M(91)) = M(101-10) \\ &= M(91) = M(M(91+1)) = M(M(92)) = M(102-10) \\ &= M(92) = \dots = M(100) = M(M(100+1)) = M(M(101)) = M(111-10) \end{aligned}$$

$$= M(100) = M(M(100+1)) = M(M(101)) = M(111-10)$$

$= M(101) = 91$ , 即对任意  $90 \leq n < 101$ , 有  $M(n) = 91$

基础步骤: 以  $M(90) = M(91) = \dots = M(100) = 91$

递归步驟: 假设对于任意  $n \in \mathbb{Z}^+$ ,  $M(n+1) = M(n+2) = \dots = M(100) = 91$ , 其中  $n < 90$

则  $M(n) = M(M(n+1))$ , 又  $n+1 < n+11 \leq 100$

根据归纳假设,  $M(n+1) = 91$ ,

则有  $M(n) = M(91) = 91$

根据强归纳法, 对于任意正整数  $1 \leq n \leq 100$ , 有  $M(n) = 91$

于是可知  $M: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$  是良定义的

形式验证 (formal verification), 指使用形式化的数学方法证明或反驳

系统相对于某个正式规范或属性的预期算法的正确性

the act of proving or disproving the correctness of intended algorithm  
underlying a system with respect to a certain formal specification  
or property, using formal method or mathematical

可以分为模型检查 (model checking) 和 演绎验证 (deductive verification)

或是 等价性检查 (equivalence checking)

形式模型检查 (formal model checking), 又称特性检查

定理证明 (theory prover)

# Discrete

## Mathematics - P132

自生成序列 (self-generating sequence), 用简单的递归关系或规则产生的不寻常序列

如在《Gödel, Escher, Bach》中 selfGenGEB :: Int → Int

递归地定义序列  $\{a(n)\}$ , 其中  $n \in \mathbb{N}$  selfGenGEB 0 = 0

$a(n) = \begin{cases} 0 & n=0 \\ n - \lfloor a(n-1) \rfloor & n>0 \end{cases}$  selfGenGEB n = n - selfGenGEB (n-1)

如 map selfGenGEB [0..10] → [0, 1, 1, 2, 3, 3, 4, 4, 5, 6, 6]

令  $\mu = \frac{\sqrt{5}-1}{2}$ , 则有  $a(n) = \lfloor (n+1)\mu \rfloor$

证明过程有:  $\mu = \frac{\sqrt{5}-1}{2}$ , 则有  $\mu^2 + \mu - 1 = 0$ , 即  $\mu^2 = 1 - \mu$ ,  $\mu^2 + \mu = 1$

对于任意  $n > 0$ ,  $(\mu n - \lfloor \mu n \rfloor) + (\mu^2 n - \lfloor \mu^2 n \rfloor)$

$$= (\mu + \mu^2)n - \lfloor \mu n \rfloor - \lfloor (1-\mu)n \rfloor = n - \lfloor \mu n \rfloor - (n + \lfloor \mu n \rfloor) \\ = - \lfloor \mu n \rfloor - \lfloor \mu n \rfloor$$

令  $\mu n = m + \xi$ , 其中  $m \in \mathbb{Z}^+$ ,  $0 < \xi < 1$

则  $\lfloor \mu n \rfloor = m$ ,  $- \lfloor \mu n \rfloor = -(m+1)$

$$\text{即 } (\mu n - \lfloor \mu n \rfloor) + (\mu^2 n - \lfloor \mu^2 n \rfloor) = - \lfloor \mu n \rfloor - \lfloor \mu n \rfloor = -m + (m+1) = 1$$

令实数  $0 \leq \alpha < 1$  且  $\alpha \neq 1 - \mu$ , 则考虑  $\lfloor (1+\mu)(1-\alpha) \rfloor + \lfloor \alpha + \mu \rfloor = 1$

当  $0 \leq \alpha < 1 - \mu$  时,  $1 - \alpha > \mu$ ,  $\alpha + \mu \in (0, 1)$

则有  $(1+\mu)(1-\alpha) > (1+\mu)\mu = \mu + \mu^2 = 1$ ,

于是  $\lfloor (1+\mu)(1-\alpha) \rfloor + \lfloor \alpha + \mu \rfloor = 1 + 0 = 1$

当  $1 - \mu < \alpha < 1$  时,  $1 - \alpha < \mu$ ,  $\alpha + \mu \in (1, 2)$

则有  $(1+\mu)(1-\alpha) < (1+\mu)\mu = \mu + \mu^2 = 1$

于是  $\lfloor (1+\mu)(1-\alpha) \rfloor + \lfloor \alpha + \mu \rfloor = 0 + 1 = 1$

基础步骤:  $a(0) = 0 = \lfloor (0+1)\mu \rfloor$

$a(1) = 1 = \lfloor (1+1)\mu \rfloor$

递归步骤: 假设对任意  $n \in \mathbb{N}$ ,  $P(0) \wedge \dots \wedge P(n-1)$  为真, 则考虑  $P(n)$

$a(n) = n - \lfloor a(n-1) \rfloor \stackrel{\text{IH}}{=} n - \lfloor (n-1)\mu \rfloor$ , 又  $0 \leq \lfloor (n-1)\mu \rfloor < n$

$$\text{则 } a(n) \stackrel{\text{IH}}{=} n - \lfloor (n-1)\mu + \lfloor (n-1)\mu \rfloor + 1 \rfloor = \lfloor (n+1)\mu - \lfloor (n-1)\mu \rfloor - 1 \rfloor$$

$$= \lfloor (n+1)\mu - (n-1)\mu - 1 \rfloor = \lfloor (n+1)\mu - n\mu + 1 \rfloor$$

$$= \lfloor (n+1)\mu - n\mu + 1 \rfloor = \lfloor (n+1)\mu - n\mu + 1 \rfloor$$

$$= \lfloor (n+1)\mu - n\mu + 1 \rfloor = \lfloor (n+1)\mu - n\mu + 1 \rfloor$$

$$= \lfloor (n+1)\mu - n\mu + 1 \rfloor = \lfloor (n+1)\mu - n\mu + 1 \rfloor$$

$$= \lfloor (n+1)\mu - n\mu + 1 + (\varepsilon - 1) \rfloor = \lfloor (n+1)\mu - n\mu + 1 + \varepsilon \rfloor$$

$$= \lfloor (n+1)\mu - n\mu + 1 + \varepsilon \rfloor = \lfloor (n+1)\mu - n\mu + 1 + \varepsilon \rfloor$$

$$= \lfloor (n+1)\mu - n\mu + 1 + \varepsilon \rfloor = \lfloor (n+1)\mu - n\mu + 1 + \varepsilon \rfloor$$

# Discrete

## Mathematics - P133

对于自生成序列  $a_{cn} = n - \lfloor a_{c(n-1)} \rfloor$ ,  $a_{c(0)} = 0$ ,  $n \in \mathbb{N}$ ,  $\mu = \frac{\sqrt{5}-1}{2}$

有当  $\mu n - \lfloor \mu n \rfloor < 1 - \mu$  时,  $a_{cn} = a_{c(n-1)}$

当  $\mu n - \lfloor \mu n \rfloor > 1 - \mu$  时,  $a_{cn} = a_{c(n-1)} + 1$

证明过程有, 当  $\mu n - \lfloor \mu n \rfloor < 1 - \mu$  时,  $\mu(n+1) < \lfloor \mu n \rfloor + 1$

$$\text{RP } a_{cn} = \lfloor \mu(n+1) \rfloor = \lfloor \mu n \rfloor = a_{c(n-1)}$$

当  $\mu n - \lfloor \mu n \rfloor > 1 - \mu$  时,  $\mu(n+1) > \lfloor \mu n \rfloor + 1$

$$\text{RP } a_{cn} = \lfloor \mu(n+1) \rfloor = \lfloor \mu n \rfloor + 1 = a_{c(n-1)} + 1$$

哥伦布的自生成序列 (Golomb's self-generating sequence)

唯一的、非减的正整数序列  $a_1, a_2, \dots$  (unique nondecreasing sequence)

对于每个正整数  $k$ , 这个序列包含  $\lfloor k \rfloor$  的  $k$  次出现

so:	$a_1$	$  a_2$	$  a_3$	$  a_4$	$  a_5$	$  a_6$	$  a_7$	$  a_8$	$  a_9$	$  a_{10}$	$  a_{11}$	$  a_{12}$	$  a_{13}$	$  a_{14}$	$  a_{15}$	$  a_{16}$	$\dots$
	1	2	2	3	3	4	4	4	5	5	5	6	6	6	6	7	$\dots$

令函数  $f(n)$  为使  $a_m = n$  的最大整数  $m$ , 其中  $a_m$  是序列的第  $m$  项

则有  $f(n) = \sum_{k=1}^n a_k$ , 且  $f(f(n)) = \sum_{k=1}^m k \cdot a_k$

基础步骤: 当  $n=1$  时,  $f(1) = 1 = \sum_{k=1}^1 a_k = 1$

$f(f(1)) = f(1) = 1 = \sum_{k=1}^1 k \cdot a_k = 1 \times 1$

递归步骤: 假设对于任意  $n \in \mathbb{Z}^+$  且  $n > 1$ ,  $P(1) \wedge \dots \wedge P(n-1)$  为真, 则考虑  $P(n)$

由于序列是唯一的且非减的,

则  $f(n) - f(n-1)$  为序列中  $n$  出现的次数, 即  $f(n) - f(n-1) = a_n$

于是  $f(n) = f(n-1) + a_n \stackrel{IH}{=} \sum_{k=1}^{n-1} a_k + a_n = \sum_{k=1}^n a_k$

令  $f(n-1) = i$ , 则  $f(n) = f(n-1) + a_n = i + a_n$

又  $a_{i+1}, a_{i+2}, \dots, a_{i+a_n}$  此  $a_n$  项均等于  $n$

则  $f(i+a_n) = f(i+a_n-1) + a_{i+a_n} = f(i+a_n-1) + n$

$= \dots = f(i) + a_n \cdot n$

则  $f(f(n)) = f(\sum_{k=1}^n a_k) = f(i) + n \cdot a_n = f(f(n-1)) + n \cdot a_n$   
 $\stackrel{IH}{=} \sum_{k=1}^{n-1} k \cdot a_k + n \cdot a_n = \sum_{k=1}^n k \cdot a_k$

于是依据数学归纳法, 对于任意  $n \in \mathbb{Z}^+$ ,  $f(n) = \sum_{k=1}^n a_k$  且  $f(f(n)) = \sum_{k=1}^n k \cdot a_k$

SelfGenGolomb 1 = 1  
 SelfGenGolomb 2 = 2  
 $\text{SelfGenGolomb } n = \text{let func } k \text{ acc}$

$| \text{acc} <= 0 \Rightarrow (\text{acc} = k-1) \text{ 但是不黑心}$   
 $| \text{otherwise } = \text{func } (k+1) (\text{acc} - \text{SelfGenGolomb } k)$

# Discrete

## Mathematics - P134

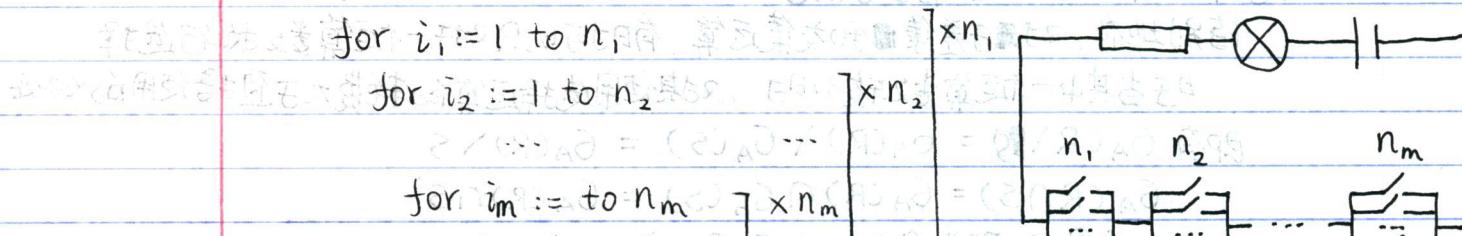
通过良序性证明 $\sqrt{2}$ 是无理数 (using well-ordering principle to prove  $\sqrt{2}$  is irrational)

正明过程有，假设 $\sqrt{2}$ 是有理数，则 $\sqrt{2}$ 可以被表示为即约分数的形式  
即存在正整数  $p, q$ , 使得  $\gcd(p, q) = 1$  且  $p/q = \sqrt{2}$   
则可知  $p = \sqrt{2}q$ , 且对于所有形如  $\sqrt{2}a$  ( $a \in \mathbb{Z}^+$ ) 的正整数  
 $p$  是其中最小的一个正整数。  
即  $p$  是集合  $\{\sqrt{2}a | a \in \mathbb{Z}^+\}$  中最小的元素  
又  $1 < \sqrt{2} < 2$ , 则有  $q < p = \sqrt{2}q < 2q$   
又  $\sqrt{2}p - p = \sqrt{2}p - \sqrt{2}q = \sqrt{2}(p - q)$   
 $p - q > 0$  且  $p - q$  为正整数  
又  $p - q < q$ , 即  $(p - q)\sqrt{2} < \sqrt{2}q$   
所以  $\sqrt{2}(p - q)$  是形如  $\sqrt{2}a$  的正整数, 但比  $\sqrt{2}q$  小  
与前提  $\sqrt{2}q$  是最小元素相矛盾，  
于是有  $\sqrt{2}$  是无理数

计数的乘积法则 (product rule for counting), 指当一个过程由两个子任务  $n_1, n_2$  构成时  
则完成过程的方式数为完成第一个任务的方式数  
和完成第一个任务后再做第二个任务的方式数之积  
即如有  $n_1$  种方式完成第一个任务, 完成后有  $n_2$  种方式完成第二个任务  
则完成全过程有  $n_1 \times n_2$  种方式

在伪代码中, 乘积法则可被描述为多层循环结构

$$k := 0 \quad \text{for } i_1 := 1 \text{ to } n_1 \quad \dots \quad \rightarrow k = n_1 \times n_2 \times \dots \times n_m$$



有穷集  $S$  的不同子集数是  $2^{|S|}$

由于  $S$  的子集与长度为  $|S|$  的位串之间存在一个一一对应的映射

根据乘积法则, 位串有  $2^{|S|}$  个, 即  $S$  的子集也有  $2^{|S|}$  个

即  $S$  的幂集  $P(S)$  有  $|P(S)| = 2^{|S|}$

有时幂集也写作  $2^S$ , 其中  $S$  表示一个集合

# Discrete

## Mathematics - P 135

集合的乘积法则 (product rule for sets), 指有限集合的笛卡尔积的大小是各个集合大小的乘积  
对于有穷集  $A_1, A_2, \dots, A_m$ , 笛卡尔积为  $A_1 \times A_2 \times \dots \times A_m$

其笛卡尔积中的元素为  $m$  元组, 即  $\{(a_1, a_2, \dots, a_m) \mid a_i \in A_i, a_i \in A_2, \dots, a_m \in A_m\}$

从中选取一个元素  $(a_1, a_2, \dots, a_m)$  的过程可描述为  $m$  个子任务

即从  $A_1$  中选取一个元素, 从  $A_2$  中选取一个元素, …, 从  $A_m$  中选取一个元素

于是有  $|A_1 \times A_2 \times \dots \times A_m| = |A_1| \times |A_2| \times \dots \times |A_m|$

计数的求和法则 (sum rule for counting), 如果一个过程由两个不重合的分支构成时

则完成这个过程的方式数为完成第一个分支的方式数

与完成第二个分支的方式数之和

即如果有  $n_1$  种方式完成第一个分支, 有  $n_2$  种方式完成第二个分支

则完成全过程有  $n_1 + n_2$  种方式

在伪代码中, 求和法则可描述为多个循环语句相连

$k := 0$   $\rightarrow k = n_1 + n_2 + \dots + n_m$

for  $i_1 := 1$  to  $n_1$   $\] + n_1$

$k := k + 1$   $\] + n_1 \dots + n_m$

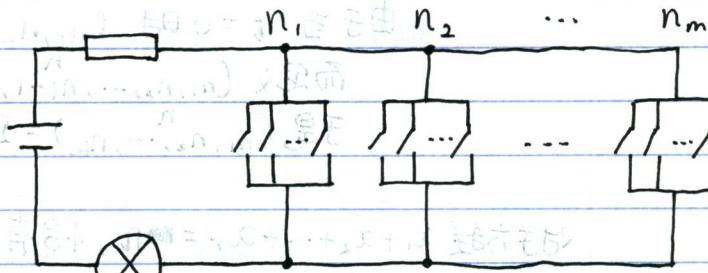
for  $i_2 := 1$  to  $n_2$   $\] + n_2 \dots + n_m$

$k := k + 1$   $\] + n_2 \dots + n_m$

...

for  $i_m := 1$  to  $n_m$   $\] + n_m \dots + n_m$

$k := k + 1$



集合的求和法则 (sum rule for sets), 指两个互斥的集合的并集的大小是各个集合大小之和

对于有穷集  $A_1, A_2, \dots, A_m$ , 且对于任意  $1 \leq i < j \leq m$ ,  $A_i \cap A_j = \emptyset$

则对于有穷集的并集  $A_1 \cup A_2 \cup \dots \cup A_m$

其元素为单个元素, 即  $\{x \mid x \in A_1 \cup A_2 \cup \dots \cup A_m\}$

从中选取一个元素  $x$  的过程可描述为  $m$  个不重合的分支

即从  $A_1$  中选取一个元素, 或从  $A_2$  中选取一个元素, …, 或从  $A_m$  中选取一个元素

于是有  $|A_1 \cup A_2 \cup \dots \cup A_m| = |A_1| + |A_2| + \dots + |A_m|$

注意这里必须要求任意两个有穷集的交集为空集.

并且注意要求比  $A_1 \cap A_2 \cap \dots \cap A_m$  为空集更严格

# Discrete Mathematics - P136

计数的减法法则 (subtraction rule for counting), 也称容斥原理 (inclusion-exclusion for counting)

即如果一个任务可以划分为两个有重合部分的分支

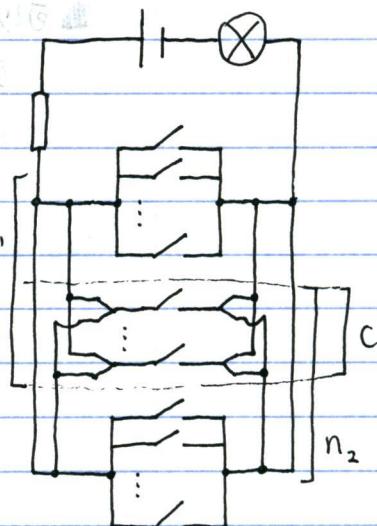
则完成任务的方法数为

完成第一个分支的方法数与完成第二个分支的方法数之和

减去两个分支中相同的方法数

即如果完成第一个分支有  $n_1$  种方式, 完成第二个分支有  $n_2$  种方式

且其中有  $C$  种方式相同, 则完成全过程有  $n_1 + n_2 - C$  种方式



集合的减法法则 (subtraction rule for set), 即对于两个集合  $A, B$

其并集的大小等于两个集合大小之和减去交集的大小

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

计数的除法法则 (division rule for counting), 如果一个任务可由一个有  $n$  种方式完成的过程实现

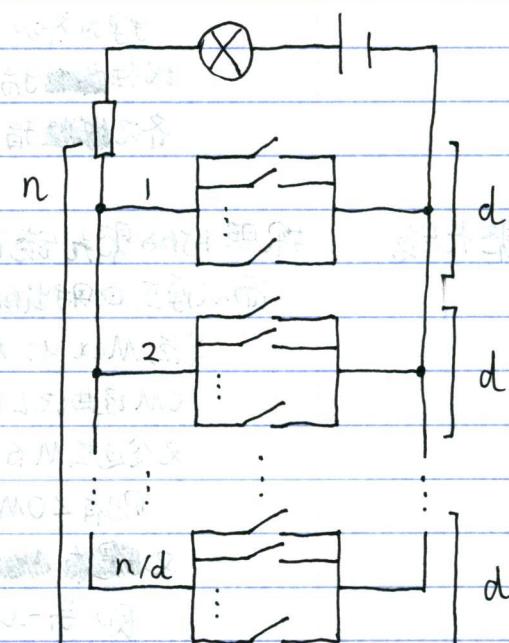
而  $n$  种方式可以划分为不相重合的  $d$  分支, 每个分支有  $d$  种方式

则以分支数考虑完成任务的不同方式数为  $n/d$

或者说, 对于一个问题可以用  $n$  种方法解决,

而每  $d$  种方法对应于一种模型

则用于解决问题的不同模型数为  $n/d$



集合的除法法则 (division rule for set), 对于一个有限集  $A$

如果  $A$  由  $n$  个互异的  $d$  个元素集合的并集组成

则有  $n = |A|/d$

或者描述为 对于有限集  $A$  和  $B$

有从  $A$  到  $B$  的函数  $f: A \rightarrow B$

且对于任意  $y \in B$ , 正好存在  $d$  个  $x \in A$  使得  $f(x) = y$

使得  $f(x_i) = y, i=1, 2, \dots, d$

则有  $f: A \rightarrow B$  是映射的

且  $|B| = |A|/d$

$$\frac{n}{d} = \frac{|A|}{d}$$

网际协议版本4

0 1 2 3 4 8 16 24 31

(Internet Protocol version 4, IPv4)

A类	0	网络号 (netid)				主机号 (hostid)		
B类	1 0	网络号 (netid)				主机号 (hostid)		
C类	1 1 0	网络号 (netid)				主机号 (hostid)		
D类	1 1 1 0	组播地址 (multicast address)				地址 (address)		
E类	1 1 1 1 0	地址 (address)				地址 (address)		

# Discrete

## Mathematics - P137

树图

(tree diagram) 指由根, 从根出发的分支及从分支的某些端点, 出发的其他分支构成的图

用内点表示每个可能的选择产生的分支, 用树叶表示可能的结果

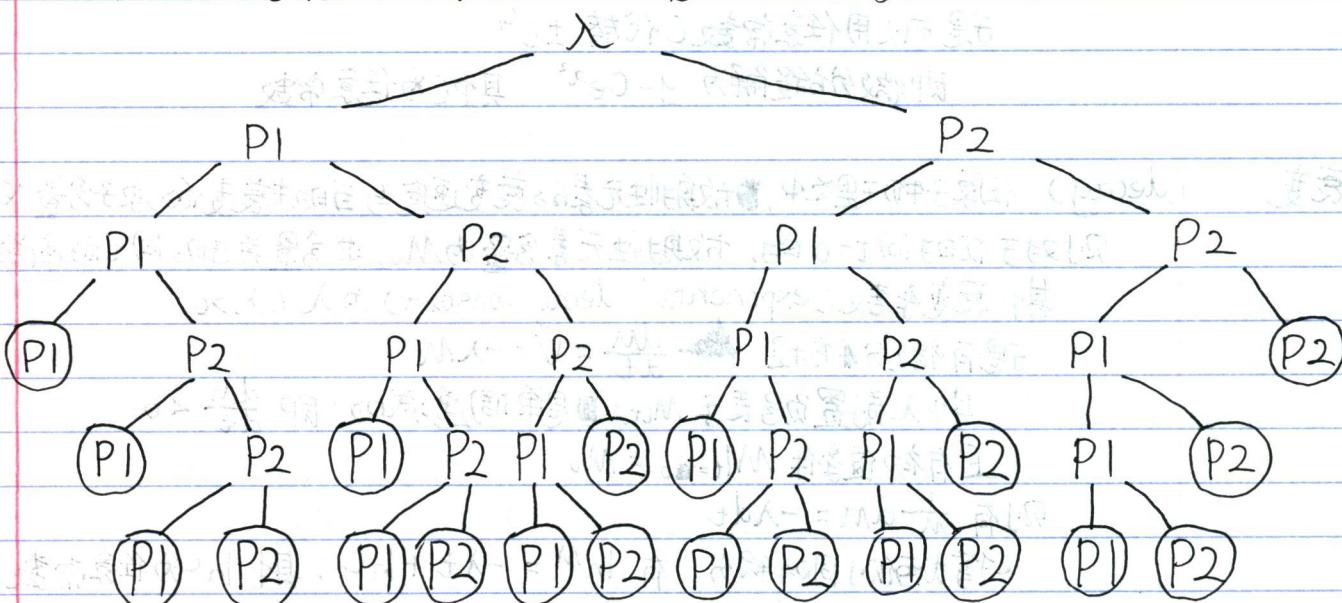
于是可以用树叶的个数来表示不同的选择的数量

注意与树不同, 在组合中应用树图,

通常更关心树生成方式的正确性以及树叶的数量

(Best of 5)

如用树图表示在两个玩家间 B05 比赛的不同过程数



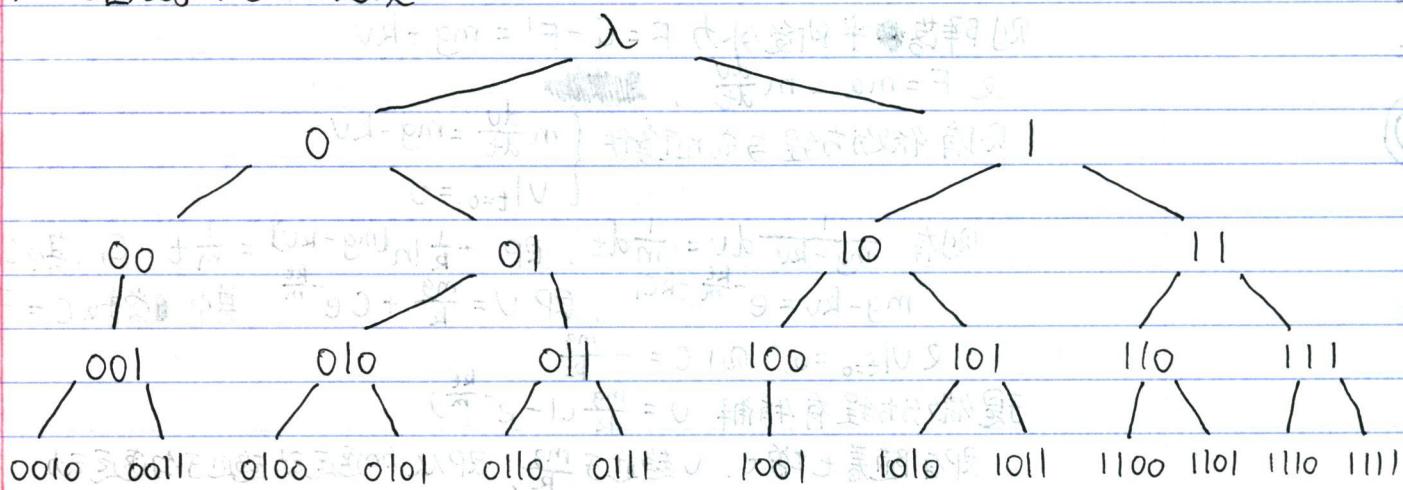
对于  $n$  个命题的命题, 存在  $2^n$  个不同的真值表

证明过程有, 对于有  $n$  个命题组成的复合命题, 每个命题有 T, F 两种可能且相互独立

则真值表共有  $2^n$  行, 又对于真值表的每一行有 T, F 两种真值指派

则共有  $2^{2^n}$  种不同的真值表

用树图表示不含 3 位连续的 0 的 4 位位串的个数



# Discrete

## Mathematics - P138

鸽巢原理 (pigeonhole principle), 又称为狄利克雷抽屉原理 (Dirichlet's drawer principle)

当  $k+1$  个物体放入  $k$  个盒子时，则至少有一个盒子包含至少 2 个物体

$(x_1, x_2, \dots, x_{k+1}) = (x_1, x_2, \dots, x_k, x_{k+1})$  为  $(x_1, x_2, \dots, x_k)$  的一个元素

推论 如果函数  $f$  是从至多  $k+1$  个元素的集合到  $k$  个元素的集合的，则函数  $f$  不是一对一的

即对于函数  $f: X \rightarrow Y$ , 如果  $|X| \geq k+1$  且  $|Y| = k$ .

则  $X$  中至少有两个元素被指派了  $Y$  中的同一个元素。

即  $\exists x_1, x_2 \in X, y \in Y (f(x_1) = y \wedge f(x_2) = y \wedge x_1 \neq x_2)$

对于任意正整数  $n$ , 存在一个  $n$  的倍数，使得其十进制表示中只有 0 和 1

证明过程有：考虑  $1, 11, 111, \dots, \overbrace{11\dots1}^{n+1}$  共  $n+1$  个正整数

则取  $1 \bmod n, 11 \bmod n, \dots, \overbrace{11\dots1}^{n+1} \bmod n$  共有  $n+1$  个余数  
而整数模  $n$  的余数只有  $n$  种可能。

即存在正整数  $1 \leq a < b \leq n+1$

使得  $\overbrace{11\dots1}^a \bmod n = \overbrace{11\dots1}^b \bmod n$

于是取两者的差

$\overbrace{11\dots1}^b - \overbrace{11\dots1}^a = \overbrace{100\dots0}^{b-a} \bmod n = 0$

于是对任意正整数  $n$ , 存在一个  $n$  的倍数，使得其十进制表示中只有 0 和 1

广义鸽巢原理 (generalized pigeonhole principle), 对于正整数  $N$  和  $k$

指如果  $N$  个物体放入  $k$  个盒子，则至少有一个盒子包含至少  $\lceil N/k \rceil$  个物体

证明过程有：假设  $N$  个物体放入  $k$  个盒子后，没有盒子包含至少  $\lceil N/k \rceil$  个物体

则  $k$  个盒子皆有至多  $\lceil N/k \rceil - 1$  个物体

于是至多有  $k(\lceil N/k \rceil - 1)$  个物体

又  $k(\lceil N/k \rceil - 1) < k[(N/k) + 1] - 1 = N$ , 与前矛盾

于是有  $N$  个物体放入  $k$  个盒子，其中  $N, k \in \mathbb{Z}^+$

则至少有一个盒子包含至少  $\lceil N/k \rceil$  个物体

推论 如果  $N$  个物体放入  $k$  个盒子，而保证至少有一个盒子包含至少  $r$  个物体，则  $N \geq k(r-1) + 1$

证明过程有： $N$  个物体放入  $k$  个盒子，则保证至少一个盒子包含  $\lceil N/k \rceil$  个物体

如果这个盒子至少有  $r$  个物体，则应保证有  $\lceil N/k \rceil \geq r$ , 即  $\lceil N/k \rceil \geq r-1$

又  $N, k, r$  均为正整数

则有  $N > k(r-1)$ , 即  $N \geq k(r-1) + 1$

# Discrete

289 - multipole

## Mathematics - P139

对于实数序列  $a_1, a_2, \dots, a_N, N \in \mathbb{Z}^+$ , 子序列指从初始序列按照原始顺序选取部分项组成的序列

即  $a_{i_1}, a_{i_2}, \dots, a_{i_m}$ , 其中  $1 \leq i_1 < i_2 < \dots < i_m \leq N$

如果序列的每一项都大于其前一项，则称为严格递增的

如果序列的每一项都小于其前边的项，则称为严格递减的

对于  $n^2+1$  个不同实数构成的序列，都包含一个长为  $n+1$  的递增序列或递减序列

即对于  $a_1, a_2, \dots, a_{n^2+1}$ , 其中  $a_i$  为不相同的实数,  $n \in \mathbb{N}$

则或者存在  $a_{i_1}, a_{i_2}, \dots, a_{i_{n+1}}$  为严格递增的

或者存在  $a_{d_1}, a_{d_2}, \dots, a_{d_{n+1}}$  为严格递减的

证明过程有：对于不同实数构成的序列  $a_1, a_2, \dots, a_{n^2+1}$

可以对每一项  $a_k$  指派一个序偶  $(i_k, d_k)$ .

使得认为以  $a_k$  为 首项的最长严格递增子序列长度

$d_k$  为以  $a_k$  为 首项的最长严格递减子序列长度

假设不存在  $n+1$  的严格递增序列和严格递减序列

则对于任意  $1 \leq k \leq n^2+1$ ,  $1 \leq i_k \leq n$ ,  $1 \leq d_k \leq n$

则序偶  $(i_k, d_k)$  存在  $n^2$  种不同的取值

于是在  $n^2+1$  个序偶中至少有 2 个相同的序偶

即对于元素  $a_h, a_j$ , 有  $i_h = i_j$  且  $d_h = d_j$ , 假设  $h < j$

如果  $a_h > a_j$ , 则可以将  $a_h$  置于  $a_j$  的递减序列之前

从而得到  $d_j+1$  的递减序列, 即与  $d_j = d_h$  矛盾

如果  $a_h < a_j$ , 则可以将  $a_h$  置于  $a_j$  的递增序列之前

从而得到  $i_j+1$  的递增序列, 即与  $i_j = i_h$  矛盾

于是有存在  $n+1$  的严格递增子序列或严格递减子序列

拉姆齐定理 (Ramsey theory), 又称拉姆齐二染色定理

对于正整数  $r, s$ , 存在一个最小的正整数  $R(r, s)$

使得在完全图  $K_{R(r, s)}$  中的每一条边着色为红色或蓝色

则或者存在一个  $K_r$  的子图每一条边都是红色

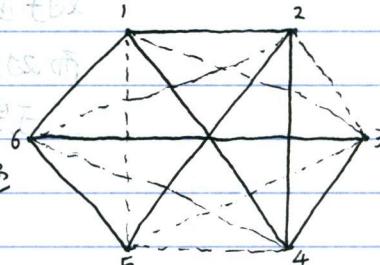
或者存在一个  $K_s$  的子图每一条边都是蓝色

称  $R(r, s)$  为拉姆齐数 (Ramsey number),

如  $R(3, 3) = 6$

对于给定的正整数  $r, s$ ,

$R(r, s)$  是唯一的且是有限的.



# Discrete

## Mathematics - P140

组合数学 (combinatorics)

组合数学 (combinatorics), 指研究物体安排的科学

枚举 (enumeration), 指物体安排的计数

排列 (permutation), 指集合中不同的元素的一种有序的安排

r-排列 (r-permutation), 指集合中 r 个元素的有序排列

记  $P(n, r)$  为具有 n 个不同元素的集合的 r 排列数

$$P(n, r) = n(n-1)(n-2) \dots (n-r+1) = \prod_{i=0}^{r-1} (n-i)$$

如果整数  $0 \leq r \leq n$ , 则 n 个元素的 r 排列数为

$$P(n, r) = n! / (n-r)!$$

注意这里定义  $0! = 1$

r 组合 (r-combination), 指从 n 集合中无序地选取 r 个元素

集合的 r 组合即集合的一个 r 个元素的子集

记  $C(n, r)$  为具有 n 个不同元素的 r 组合数

也记为  $\binom{n}{r}$ , 称为二项式系数 (binomial coefficient)

如果整数  $0 \leq r \leq n$ , 则 n 个元素的 r 组合数为

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

证明过程如下: 集合的 r 排列可以分成两部分

首先从 n 个集合中选取 r 个元素, 有  $C(n, r)$  种选择方法,

然后对 r 个元素进行排列, 有  $P(r, r)$  种排列方法,

则有  $P(n, r) = C(n, r) \cdot P(r, r)$

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

推论 对于非负整数  $r \leq n$ ,  $C(n, r) = C(n, n-r)$

组合证明 (combinatorial proof), 恒等式的组合证明过程中使用计数的论述而不使用其他方法证明定理

或证明 基于等式两边的对称集合存在一个双射函数来证明

分别称为双计数证明 和 双射证明

如对于  $C(n, r) = C(n, n-r)$  的证明

可以说明从 n 个元素中选取 r 个和从 n 个元素中选取  $n-r$  个的方法是一一对应的

# Discrete

## Mathematics - P141

二项式定理 (binomial theorem), 对于变量  $x, y$ , 非负整数  $n$

$$\text{有 } (x+y)^n = \sum_{j=0}^n \binom{n}{j} x^{n-j} y^j = \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \dots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n$$

推论 对于非负整数  $n$ ,  $\sum_{k=0}^n \binom{n}{k} = 2^n$

证明有, 取  $x=1, y=1$ , 则有  $2^n = (x+y)^n$

$$\text{则 } 2^n = (x+y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k = \sum_{k=0}^n \binom{n}{k}$$

或者用组合方式证明, 对于有  $n$  个元素的集合  $N$

则考虑其子集中元素的个数, 有  $k=0, 1, \dots, n$

而有  $k$  个元素的子集个数为  $\binom{n}{k}$

于是  $\boxed{\text{集合 } N \text{ 的子集个数为 } \sum_{k=0}^n \binom{n}{k}}$

$$\text{又 } |P(N)| = 2^{|N|} = 2^n, \text{ 且 } P(N) \text{ 表示 } N \text{ 的所有子集}$$

于是有  $2^n = |P(N)| = \sum_{k=0}^n \binom{n}{k}$

推论 对于非负整数  $n$ ,  $\sum_{k=0}^n (-1)^k \binom{n}{k} = 0$

证明过程有,  $\sum_{k=0}^n (-1)^k \binom{n}{k} = \sum_{k=0}^n \binom{n}{k} (-1)^k (1)^{n-k}$

$$= (1-1)^n = 0$$

进一步扩展可得  $\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \dots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \dots$

即可描述为 二项式奇数项系数之和与偶数项系数之和相等

推论 对于非负整数  $n$ ,  $\sum_{k=0}^n 2^k \binom{n}{k} = 3^n$

证明过程有,  $\sum_{k=0}^n 2^k \binom{n}{k} = \sum_{k=0}^n \binom{n}{k} 2^k (1)^{n-k}$

$$= (1+2)^n = 3^n$$

帕斯卡恒等式 (Pascal's identity), 对于正整数  $n \geq k$ , 有  $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$

证明过程有,  $\binom{n+1}{k}$  可描述为从  $n+1$  个元素的集合  $T$  中选取  $k$  个元素

令  $a$  为  $T$  中的一个元素, 而  $n$  个元素的集合  $S = T - \{a\}$

则  $\binom{n+1}{k}$  种选择方法可分解为 两种情形

选取了元素  $a$ , 并从  $S$  中选取  $k-1$  个元素, 即  $\binom{n}{k-1}$

不选取元素  $a$ , 并从  $S$  中选取  $k$  个元素, 即  $\binom{n}{k}$

于是合并可知  $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$

采用代数方法的证明:  $\binom{n}{k-1} + \binom{n}{k} = \frac{n!}{(k-1)! (n-k)!} + \frac{n!}{k! (n-k)!}$

$$= \frac{k \cdot n! + (n-k) \cdot n!}{k! (n-k)!}$$

$$= (n+1) n! / k! (n+1-k)! = \binom{n+1}{k}$$