

Discrete

Mathematics - P17

递增/递减

对于定义域X和陪域Y，~~两者~~都是实数集R的子集的函数 $f: X \rightarrow Y$

如果对定义域中的 $x_1, x_2, \forall x_1, x_2 \in X (x_1 < x_2 \rightarrow f(x_1) \leq f(x_2))$, 称 f 为递增的

(~~对于~~ $x_1 < x_2 \rightarrow f(x_1) < f(x_2)$)，称 f 为严格递增的

$\forall x_1, x_2 \in X (x_1 < x_2 \rightarrow f(x_1) > f(x_2))$, 称 f 为递减的

(~~对于~~ $x_1 < x_2 \rightarrow f(x_1) > f(x_2)$)，称 f 为严格递减的

注意：~~于是~~ 严格递增/严格递减的 \rightarrow 于是是一对一的

而~~于是~~ 递增/递减的，且不是严格递增/严格递减的 \rightarrow 于是不是一对一的

映上函数 (onto function), 或称满射函数(surjection), 即函数陪域中的每个元素都是定义域中某一个元素的像

即~~于是~~ 是满射的(surjective) $\leftrightarrow \forall b \in B \exists a \in A f(a) = b$, 对于函数 $f: A \rightarrow B$

一一对应 (one-to-one correspondence), 或称双射函数(bijection), 即既是一对一又是映上的函数

即~~于是~~ $f: A \rightarrow B$ 是双射的(bijective) $\leftrightarrow (\forall x \in A \forall y \in A (x \neq y \rightarrow f(x) \neq f(y))) \wedge (\forall b \in B \exists a \in A f(a) = b)$

恒等函数

函数 $\iota_A: A \rightarrow A$ (读作 iota) 是恒等函数, 有 $\forall x \in A \iota_A(x) = x$, 即把每个元素指派给其自身

证明 $f: A \rightarrow B$ 是单射的, $\forall x \in A \forall y \in A (x \neq y \rightarrow f(x) \neq f(y))$, 或 $\forall x \in A \forall y \in A (f(x) = f(y) \rightarrow x = y)$

$f: A \rightarrow B$ 不是单射的, $\exists x \in A \exists y \in A (x \neq y \wedge f(x) = f(y))$, 注意不能用 $\exists x \in A \exists y \in A (x = y \wedge f(x) = f(y))$ 因为只能为一个元素指派恰好一个值

$f: A \rightarrow B$ 是满射的, $\forall b \in B \exists a \in A f(a) = b$] 注意: 两个量词的顺序

$f: A \rightarrow B$ 不是满射的, $\exists b \in B \forall a \in A f(a) \neq b$] 对换量词顺序逻辑上是等价的

反函数 (inverse function), 或称函数的逆(inverse), 用 f^{-1} 表示集合A到集合B的 $1-1$ 对应的函数 $f: A \rightarrow B$ 的逆

指派给B中元素 b 的是A中唯一使 $f(a) = b$ 的元素 a , 即 f^{-1} 是集合B到集合A的, 有 $f^{-1}: B \rightarrow A$

有 $\forall a \in A \forall b \in B (f(a) = b \leftrightarrow f^{-1}(b) = a)$

注意 f^{-1} 与 $1/f$ 具有不同的意义, 前者表示函数 f 的反函数 f^{-1}

后者表示 $\forall a \in A \forall b \in B (f(a) = b \rightarrow (1/f)(a) = 1/b)$, 且 $\forall a \in A f(a) \neq 0 \rightarrow (1/f)(a) \neq 0$

可逆的 (invertible), 即 $1-1$ 对应的, 于是可逆的 \leftrightarrow 于是 $1-1$ 对应的, 因为此时 f 有反函数 f^{-1}

如果 f 不是 $1-1$ 对应的, 则称 f 是不可逆的(not invertible)

函数的图象(graph), 对于从集合A到集合B的函数 f , 其图像是序偶集合 $\{(a, b) | a \in A \text{ 且 } b = f(a)\}$

$\{(c, d), (e, f), (g, h)\} \rightarrow \{(1, 2), (3, 4), (5, 6), (7, 8)\} \rightarrow \{(a, b) | a \in A \text{ 且 } b = f(a)\}$

$\{(c, d), (e, f), (g, h)\} \rightarrow \{(1, 2), (3, 4), (5, 6), (7, 8)\} \rightarrow \{(a, b) | a \in A \text{ 且 } b = f(a)\}$

Discrete

Mathematics - P18

函数合成/组合 (composition), 用 $f \circ g$ 表示从集合 A 到集合 C 的函数 $g: A \rightarrow B$ 与从集合 B 到集合 C 的函数 $f: B \rightarrow C$ 的合成

即 $\forall a \in A \quad (f \circ g)(a) = f(g(a))$, 即 $f \circ g$ 指派给 a 的元素是 g 指派给 a 的元素 b 对应于 f 中的元素 $f(b)$

注意 $f \circ g: A \rightarrow C$, 且当 g 的值域 $R_g \subseteq f$ 的定义域 D_f 时, $f \circ g$ 才有定义

注意 即使 $f \circ g$ 和 $g \circ f$ 都有定义 $f(g(a)) = g(f(a))$ 不一定成立, 即函数复合不满足交换律

例如 $f(x) = 2x+3, g(x) = 3x+2, (f \circ g)(x) = 6x+7, (g \circ f)(x) = 6x+11$

如果函数 f 是可逆的, 则 f^{-1} 也是可逆的, 且 $(f^{-1})^{-1} = f$

由于 $(f \circ f^{-1})(a) = f^{-1}(f(a)) = f^{-1}(b) = a$ 且 $(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a) = b$

即函数与其反函数的合成为恒等函数, 即 $(f \circ f^{-1})(a) = a, (f^{-1} \circ f)(b) = b$

注意 函数合成具有传递性 (对于一一对一, 映上, 一一对应)

若 g 是一一对一的 且 g 是一一对一的 $\rightarrow f \circ g$ 是一一对一的

g 是映上的 且 g 是映上的 $\rightarrow f \circ g$ 是映上的

g 是一一对应的 且 g 是一一对应的 $\rightarrow f \circ g$ 是一一对应的

在 Haskell 中, 函数复合的运算符 \circ 与记号 \circ 等价

即有 $f: A \rightarrow B, g: B \rightarrow C$ 对应于 $f: A \rightarrow C$

$f \circ g: A \rightarrow C$ 对应于 $f \circ g: A \rightarrow C$

下取整函数 (floor function). 将小于或等于实数 x 的最大整数指派给 x , 记为 $\lfloor x \rfloor$

也称最大整数函数, 此时记为 $\lfloor x \rfloor$

上取整函数 (ceiling function). 将大于或等于实数 x 的最小整数指派给 x , 记为 $\lceil x \rceil$

注意: $\forall x \in \mathbb{R} \quad \forall n \in \mathbb{Z} \quad (\lfloor x \rfloor = n \leftrightarrow x-1 < n \leq x < n+1)$

$\forall x \in \mathbb{R} \quad \forall n \in \mathbb{Z} \quad (\lceil x \rceil = n \leftrightarrow n-1 < x \leq n < n+1)$

由此引出与 $\lfloor x \rfloor$ 和 $\lceil x \rceil$ 相关的常用的证明和计算方法:

适用于 $\lfloor x \rfloor$: 令实数 $x = n + \varepsilon$, 其中 $n \in \mathbb{Z}, \varepsilon \in \mathbb{R} \wedge 0 \leq \varepsilon < 1$

适用于 $\lceil x \rceil$: 令实数 $x = n - \varepsilon$, 其中 $n \in \mathbb{Z}, \varepsilon \in \mathbb{R} \wedge 0 \leq \varepsilon < 1$

然后对 ε 进行分情形讨论. 由于 $\lfloor x+n \rfloor = \lfloor x \rfloor + n, \lceil x+n \rceil = \lceil x \rceil + n$.

注意: $\forall x \in \mathbb{R} \quad x-1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x+1$

且有当 $x \in \mathbb{Z}$ 时, $\lfloor x \rfloor = \lceil x \rceil$, 当 $x \notin \mathbb{Z}$ 时, $\lfloor x \rfloor + 1 = \lceil x \rceil$

注意: $\forall x \in \mathbb{R} \quad \lfloor -x \rfloor = -\lceil x \rceil$ 注意当 $0 < \varepsilon < 1$ 的情形, $\lfloor -n+\varepsilon \rfloor = -n + \lfloor -\varepsilon \rfloor = -\lfloor n+\varepsilon \rfloor$

特别注意: 不同的编程语言对 $\lfloor x \rfloor$ 的理解不完全相同, 体现在 float \rightarrow int 时的实现不同

如果对 float 采用截去小数部分, 则有 $x \geq 0$ 时 $\lfloor x \rfloor = \lfloor x \rfloor$, 但 $x < 0$ 时 $\lfloor x \rfloor = \lceil x \rceil$

而如果采用四舍五入方式, 则有 $x \geq 0$ 时 $\lfloor x \rfloor = \lfloor x + \frac{1}{2} \rfloor$, 而 $x < 0$ 时 $\lfloor x \rfloor = \lceil x - \frac{1}{2} \rceil$

Discrete

Mathematics - P19

阶乘函数

$f: N \rightarrow \mathbb{Z}^+$, 定义为 $f(0) = 0! = 1$, $f(n) = n! = 1 \times 2 \times \dots \times (n-1) \times n$

有斯特林公式 $n! \sim \sqrt{2\pi n} (n/e)^n$

渐近于 $f(x) \sim g(x)$ 表示, $f(x)$ 渐近于 $g(x)$, 即 $\lim_{n \rightarrow \infty} f(n)/g(n) = 1$

部分函数 (partial function). 从集合 A 到集合 B 的函数 $f: A \rightarrow B$ 为 A 的子集中的元素 a 指派一个元素 b

这个子集称为 f 的定义域 (domain of definition), 当定义域与 A 相等时, 称为全函数 (total function)

字母在 A 中但不在函数 f 的定义域中的元素无定义 (undefined)

序列

(sequence). 是一个从整数集的子集 (通常是 \mathbb{N} 或者 \mathbb{Z}) 到一个集合 S 的函数

用记号 $\{a_n\}$ 描述序列, 即 a_n 表示整数 n 的像, 称为序列的一个项 (term)

几何级数 (geometric progression) 指形如 $a, ar, ar^2, \dots, ar^n, \dots$ 的序列, 其中 a 和 r 都是实数

称 a 为初始项, r 为公比, 且几何级数是指数函数 $f(x) = ar^x$ 的离散的对应体

算术级数 (arithmetic progression), 指形如 $a, a+d, a+2d, \dots, a+nd, \dots$ 的序列, 其中 a 和 d 都是实数

称 a 为初始项, d 为公差, 且算术级数是线性函数 $f(x) = a+dx$ 的离散的对应体

串

(string) 指有穷序列. 即形如 a_1, a_2, \dots, a_n , 有时也表示为 $a_1 a_2 \dots a_n$.

如位串和字符串通常表示为 $a_1 a_2 \dots a_n$ 的形式

空串

(empty string) 即没有任何项的串, 通常记作 λ , 空串的长度 (串的项数) 为 0

递推关系

(recurrence relation) 递归地定义了一个序列, 即 $\forall n > n_0$, a_n 可以表示为 a_0, \dots, a_{n-1} 中若干项的表达式

n_0 是一个非负整数, a_0, \dots, a_{n_0} 需要特别地定义, 即基础地定义

或者说递归定义的初始条件指定了在递推关系定义的首项 (a_{n_0+1}) 前的那些项 (a_0, \dots, a_{n_0})

斐波那契数列 (Fibonacci Sequence), 初始条件 $f_0 = 0, f_1 = 1$, 递推关系 $\forall n > 1, f_n = f_{n-1} + f_{n-2}$

闭公式

(closed formula), 指序列的项的一个显式公式, 也即解决了所有初始条件的递推关系

如 Fibonacci 数列有闭公式 $f_n = (\varphi^n - (-\varphi)^{-n}) / \sqrt{5}$, 其中 $\varphi = (1 + \sqrt{5})/2$, $n \in \mathbb{N}$

Lucas 序列

有 $L_1 = 1, L_2 = 3$, $\forall n > 2, L_n = L_{n-1} + L_{n-2}$, 与 Fibonacci 数列的关系在于初始条件不同

另外, 令 $f_{-1} = 0$. 则 $\forall n \in \mathbb{Z}^+, L_n = f_n + f_{n-2}$, 同时 $L_{n-1} + L_{n-2} = f_{n-1} + f_{n-3} + f_{n-2} + f_{n-4}$

$= f_n + f_{n-2} = L_n$

Discrete

Mathematics - P₂₀

迭代

(Iteration), 通常利用数学归纳法找到序列的递推公式, 之后迭代或重复利用递推关系

正向替换: 从初始条件 a_0 出发找到连续的项, 直到 a_n 为止

反向替换: 从 a_n 开始表示为序列之前的项直到可以用初始条件 a_0 来表示为止

复合利率

(Compound Interest), 可以解释为一个递推关系, 对初始资产 S_0 和利率 r , 第 n 期资产 $S_n = (1+r)S_{n-1}$

求和记号 (summation notation), 用 $\sum_{i=1}^n a_i$ 表示 $a_1 + a_2 + \dots + a_n$ 的求和, 称为求和下标

可以扩展为 $\sum_{i \in S} a_i$ 表示对所有在集合 S 中的元素 i , a_i 的求和

求和记号符合分配律和结合律, 即 $\sum_{i=1}^n (ax_i + by_i) = a\sum_{i=1}^n x_i + b\sum_{i=1}^n y_i$

注意部分常用求和公式: $\sum_{i=0}^k ar^i (r \neq 1) = a + ar + \dots + ar^k = (a - ar^{k+1}) / (1-r)$

$$\sum_{k=1}^{\infty} k = n(n+1)/2, \quad \sum_{k=1}^{\infty} k^2 = n(n+1)(2n+1)/6, \quad \sum_{k=1}^{\infty} k^3 = n^2(n+1)^2/4$$

当 $|x| < 1$ 时 $\sum_{k=0}^{\infty} x^k = 1 + x + x^2 + \dots + x^n + \dots = 1/(1-x)$

当 $|x| < 1$ 时 $\sum_{k=1}^{\infty} kx^{k-1} = 1 + 2x + 3x^2 + \dots + nx^{n-1} + \dots = 1/(1-x)^2$

证明方法: 令 $S = 1 + x + x^2 + \dots$, 则 $x \cdot S = x + x^2 + \dots = S - 1$

$$\text{又 } |x| < 1, \quad (1-x)S = 1, \quad \text{即 } \sum_{k=0}^{\infty} x^k = 1/(1-x)$$

由于对 $\forall k \in \mathbb{N}$ x^k 都是可导的, 所以 $d(\sum_{k=0}^{\infty} x^k) = \sum_{k=0}^{\infty} d(x^k)$

$$\text{又 } k=0 \text{ 时 } d(1)=0, \quad \sum_{k=1}^{\infty} kx^{k-1} = \sum_{k=0}^{\infty} d(x^k) = d(\sum_{k=0}^{\infty} x^k) = d(1/(1-x)) = 1/(1-x)^2$$

另外类似地有用 $\prod_{i=1}^n a_i$ 表示 $a_1 \times a_2 \times \dots \times a_n$, 称为求积记号

可以扩展为 $\prod_{i \in S} a_i$ 表示对所有集合 S 中的元素 i , a_i 的乘积

$a_n = \lfloor \sqrt{2n} + \frac{1}{2} \rfloor$ 用于构造序列包含整数 k 恰好 k 次, 即形如 1, 2, 2, 3, 3, 3, 4, 4, 4, 4, ...

$a_n = n + \lceil \sqrt{n} \rceil$ 用于构造序列, 其中 a_n 是第 n 个不是完全平方数的整数, $\{x\}$ 表示最接近于实数 x 的整数
即形如 2, 3, 5, 6, 7, 8, 10, 11, ...

迭进 (telescoping) 表示形如 $\sum_{k=1}^n (a_k - a_{k-1})$ 的求和, 结果为 $a_n - a_0$, 其中 a_0, a_1, \dots, a_n 都是实数

有 $|A| = |B| \iff \exists f: A \rightarrow B$ 是一一对应的, 或者说存在一个从 A 到 B 的一一对应

特别的有 $\exists f: A \rightarrow B$ 是一对一的 $\iff |A| \leq |B|$, 即 A 的基数小于等于 B 的基数

$\exists f: A \rightarrow B$ 是映射的 $\iff |A| \geq |B|$, 即 A 的基数大于等于 B 的基数

但是特别注意不能直接推出 $|A| = |B| \iff \exists f: A \rightarrow B$ 是一一对应的, 因为必须证明存在一个映射

因为必须证明存在的 $f: A \rightarrow B$ 一一对应的且是同一个映射

Discrete

Mathematics - P21

可数集

countable

(countable set) 指集合或者是有限集，或者与自然数集具有相同的基数

即对于集合 S , $|S| = |\mathbb{N}| \leftrightarrow \exists f: \mathbb{N} \rightarrow S$ 是一一对应的

不可数集

(uncountable set) 指如果集合不是可数的，集合首先是无限集

再有集合 S 不可数 $\leftrightarrow \nexists f: \mathbb{N} \rightarrow S$ 是一一对应的 $\leftrightarrow \forall f: \mathbb{N} \rightarrow S$ 不是一一对应的

阿里夫零 (aleph null), 用 \aleph_0 表示可数集合 S 的基数，即 $|S| = \aleph_0$ 。也称 S 有基数“阿里夫零”
或者说 \aleph_0 是自然数集的基数（或是正整数集）有 $|\mathbb{N}| = |\mathbb{Z}^+| = \aleph_0$ 。

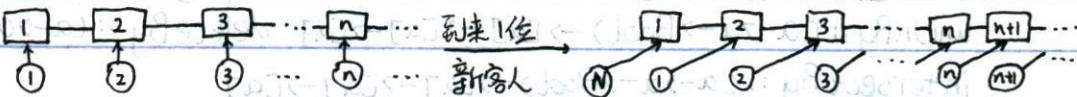
另外 \aleph_0 是希伯来语的第一个字母 阿里夫, aleph

希尔伯特大饭店 由大卫·希尔伯特提出的一个悖论，证明对有限集为假定的性质可能对可数无限集为真

如对于一个有可数无限多个房间的大饭店，每间房都有客人

而当一位新客人到来时，大饭店可以在不赶走现有客人的情况下容纳新客人

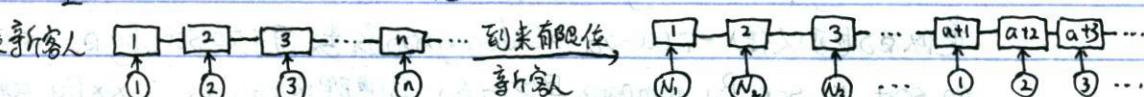
即有



当有一位新客人到来时，每位原客人都移到下一房间，新客人住入 1 号房间

基于 $f(x) = x + 1$ 在 $x \in \mathbb{Z}^+$ 上是一一对应的函数

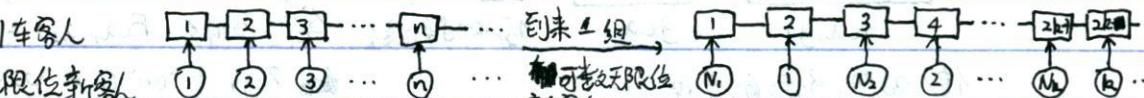
扩展为有限位新客人



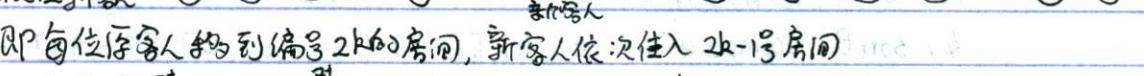
当有有限位新客人到来时，每位原客人都到 $n+a$ 房间，新客人依次住入 $1-a$ 房间

基于 $f(x) = x + a$ 在 $x \in \mathbb{Z}^+$ 上是一一对应的函数 ($a \in \mathbb{Z}^+$)

扩展为到来 1 车客人



车上有可能无限位新客人



即每位原客人都到编号 $2k+1$ 的房间，新客人依次住入 $2k+1$ 房间

有当 $f: \mathbb{Z}^+ \rightarrow \text{原有}$, $g: \mathbb{Z}^+ \rightarrow \text{新来}$ 都是一一对应的函数时

$$h(n) = \begin{cases} f(cn/2), & n=2k \\ g((cn+1)/2), & n=2k-1 \end{cases}, k \in \mathbb{Z}^+, \text{也是} \rightarrow \text{一一对应的函数}$$

再扩展为到来有限车新客人，每辆车上有可数无限位客人，



第 k 辆车: $\boxed{1} \rightarrow \boxed{2} \rightarrow \boxed{3} \rightarrow \dots \rightarrow \boxed{n} \rightarrow \dots$

即当 $f: \mathbb{Z}^+ \rightarrow \text{原有}$, $g_1: \mathbb{Z}^+ \rightarrow \text{第 } 1 \text{ 辆车}, \dots, g_k: \mathbb{Z}^+ \rightarrow \text{第 } k \text{ 辆车}$ 时

$$h(n) = \begin{cases} g_1(m), & n = (m-1)l + 1 \\ \dots & \dots \\ g_k(m), & n = (m-1)l + k \end{cases}$$

其中, $m \in \mathbb{Z}^+$, $k \in \mathbb{Z}^+$

$$f(m), \quad n = m(l+1)$$

第 k 辆车: $\boxed{1} \rightarrow \boxed{2} \rightarrow \boxed{3} \rightarrow \dots \rightarrow \boxed{n} \rightarrow \dots$

一一对应的

$$g_k(m), \quad n = (m-1)l + k$$

$$f(m), \quad n = m(l+1)$$

Discrete

Mathematics - P 22

可数证明 可以通过列举一个集合的元素来证明无限集是可数的。

即通过某种顺序排列一个无限集中的元素，使之可以表示成一个序列。

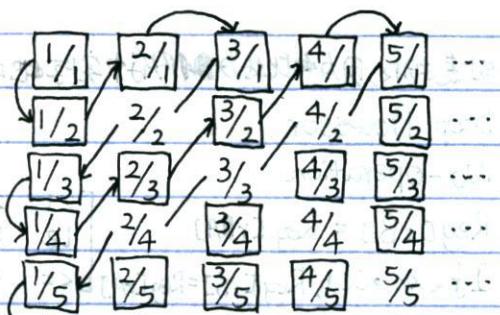
即找到了一个从自然数集 \mathbb{N} 或正整数集 \mathbb{Z}^+ 到无限集 S 的一一对应函数 $f: \mathbb{N}(\mathbb{Z}^+) \rightarrow S$

如对于整数集 $\{\dots, -2, -1, 0, 1, 2, \dots\}$ ，定义序列 $\{a_n\} = \begin{cases} -k, & n=2k-1 \\ k, & n=2k \end{cases}$ 其中 $n \in \mathbb{Z}^+$ 。
有序列 $\{0, -1, 1, -2, 2, \dots\}$

如对于正有理数集 \mathbb{Q}^+ ，可知每个正有理数 q 都可以表示为即约分数的形式 $\frac{\text{irreducible numerator}}{\text{denominator}}$ 。

即 $\forall q \in \mathbb{Q}^+ \exists n \in \mathbb{Z}^+, d \in \mathbb{Z}^+ (\gcd(n, d) = 1 \wedge q = n/d)$ 。

按顺序列举正有理数，注意剔除非即约分數，可得序列 $\{\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{3}{1}, \frac{1}{3}, \frac{1}{4}, \dots\}$



编号 1 2 3 4 5 ...

原有客人 (0) : (0,1) (0,2) (0,3) (0,4) (0,5) ...

第1辆车 : (1,1) (1,2) (1,3) (1,4) (1,5) ...

第2辆车 : (2,1) (2,2) (2,3) (2,4) (2,5) ...

第3辆车 : (3,1) (3,2) (3,3) (3,4) (3,5) ...

第4辆车 : (4,1) (4,2) (4,3) (4,4) (4,5) ...

注意这个方法也可以用于扩展希尔伯特大饭店到新来可数无限辆车，每辆车上有可数无限新客人
可得入住序列 $\{(0,1), (1,1), (0,2), (0,3), (1,2), (2,1), (3,1), (2,2), \dots\}$

group k : 1 2 3 4 5 ...

注意这个方法可以用于编程时的 Iterator 的定义，即可以将可数集视为一个可列举序列来生成

康托尔对角线法 (Cantor diagonalization argument)，通过证明 $(0,1)$ 的实数不可列举，进而证明实数集不可数

假设 $(0,1)$ 的实数可以按某种顺序列出

即存在一个序列 $\{r_1, r_2, r_3, \dots\}$

且 $\forall i \in \mathbb{Z}^+ r_i$ 可以表示为 $0.d_{i1}d_{i2}d_{i3}\dots$

其中 $d_{ij} \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

构造一个新的实数 $r = 0.d_1d_2d_3d_4\dots$

使 $d_{ii} = \begin{cases} 4 & \text{如果 } d_{ii} \neq 4 \\ 5 & \text{如果 } d_{ii} = 4 \end{cases}$

则可知 $\forall i \in \mathbb{Z}^+ d_i \neq d_{ii}$ 其 $r = 0.d_1d_2d_3d_4d_5\dots$

也就是说 $\forall i \in \mathbb{Z}^+ r_i$ 与 r 在小数点后的第 i 位不相等，即 $r_i \neq r$

于是有一个实数 $r \in (0,1)$ 但不在序列 $\{r_1, r_2, r_3, \dots\}$ 中，与假设矛盾，进而证明 $\{r | r \in (0,1), r \in \mathbb{R}\}$ 不可数。

注意： \forall 集合 $A, B (A \subseteq B \wedge A$ 是不可数的 $\rightarrow B$ 是不可数的)

可用于证明某一集合是不可数的，通过证明集合的一个子集不可数。

\forall 集合 $B (A \subseteq B \wedge A$ 是不可数的 $\rightarrow B$ 是不可数的)

注意：如果集合A和集合B是可数集合，则 $A \cup B$ 也是可数集合

扩展可得对可数无限个集合 A_i ，($\bigwedge_{i \in I} A_i$ 是可数无限的) $\rightarrow (\bigcup_{i \in I} A_i$ 是可数无限的)

Schröder - 如果集合A和集合B有 $|A| \leq |B|$ 且 $|B| \leq |A|$ ，则有 $|A| = |B|$

Bernstein定理 或者说如果存在函数 $f: A \rightarrow B$ 和 $g: B \rightarrow A$ 都是-对一的，则存在 $A \rightarrow B$ 的-对应函数

常用于证明不可数集合的基数相等，如 $|R \times R| = |R|$

令有集合 $A = (0, 1) \times (0, 1)$ 和集合 $B = (0, 1)$ ，集合A与集合B的元素均为实数

可取 $f: (0, 1) \rightarrow (0, 1) \times (0, 1)$ 为 $f(x) = (x, x)$ 。可知 $f(x)$ 是一对一的

对于 $g: (0, 1) \times (0, 1) \rightarrow (0, 1)$ ，则对于 $(x, y), x, y \in (0, 1)$

利用十进制展开式 $x = 0.c_1c_2c_3\ldots, y = 0.d_1d_2d_3\ldots, c_i, d_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}, i \in \mathbb{Z}^+$

取 $r = 0.c_1d_1c_2d_2c_3d_3\ldots$ ，可知 $r \in (0, 1)$ 是一对一的

且对于任意不相同的实数对 (x, y) ， r 均不相同，即 $g: (0, 1) \times (0, 1) \rightarrow (0, 1)$

进而由 $|(0, 1)| = |R|$ ，证明 $|R \times R| = |R|$

可计算函数 (computable function) 指存在用某种编程语言写的计算机程序可以计算其值的函数

否则即为不可计算函数 (uncomputable function)

注意这里隐含地表明计算机程序的结果集合是可数无限的 (对于可数无限的输入)

或者说对于某一个程序的可能输出，总是可能构造一个 Iterator

使得 Iterator 产生的序列集合等于程序的可能输出

连续统假设 (continuum hypothesis)，命题阐述了不存在介于 \aleph_0 和 c (实数集 R 的基数) 之间的基数 χ ，

即不存在集合 A ，使得 $\aleph_0 < |A| < c = |R|$

可以证明最大的无限集的基数形成一个无限序列 $\aleph_0 < \aleph_1 < \aleph_2 < \dots$

注意其中有 $\aleph_0 = |\mathbb{N}|$ ，而根据假设， $c = \aleph_0$ ，但是基数最小的不可数集

也无法证伪

康托尔定理 对于集合 S ，不存在从集合 S 到 S 的幂集 $P(S)$ 的映上函数，即 $\forall S, |S| < |P(S)|$

于是有 $|\mathbb{Z}^+| < |P(\mathbb{Z}^+)|$ ，即可重写为 $\aleph_0 < 2^{\aleph_0}$

另外有 $|\mathbb{C}| = |\mathbb{R}| = |\mathbb{R}^2| = |\mathbb{R}^3| = |\mathbb{R}^n| = |\mathbb{R}^{\omega}| = |\mathbb{R}^{\mathbb{N}}| = |\mathbb{R}^{\mathbb{Z}^+}| = |\mathbb{R}^{\mathbb{Z}}|$

又 $|\mathbb{C}| = |\mathbb{R}|$ 则以 d_i 表示正整数是否在 \mathbb{Z}^+ 的一个子集 S 中，

所以有 $|\mathbb{R}| = |\mathbb{P}(\mathbb{Z}^+)| = c$ 即有一个从 \mathbb{C} 到 $\mathbb{P}(\mathbb{Z}^+)$ 的-对应。

同时有 $\aleph_0 = 2^{\aleph_0}$ (如果连续统假设为真) 于是有 $|\mathbb{C}| = |\mathbb{P}(\mathbb{Z}^+)| = c$

假设为真)

Discrete

Mathematics - P24

矩阵 (matrix), 指矩形的数组, $m \times n$ 行列的矩阵称为 $m \times n$ 矩阵。

特别的有行数和列数相等的矩阵称为方阵 (square), $n \times n$ 矩阵也称 n 阶矩阵 / 方阵。

令 $m, n \in \mathbb{Z}^+$,

并有 $A = [a_{ij}]$ 为一个 $m \times n$ 矩阵

则 A 的第 i 行 $[a_{i1} a_{i2} \dots a_{in}]$ 为 $1 \times n$ 矩阵

$a_{i1} a_{i2} \dots a_{in}$

A 的第 j 列 $[a_{1j} a_{2j} \dots a_{nj}]^T$ 为 $m \times 1$ 矩阵

$a_{1j} a_{2j} \dots a_{nj}$

元素 (element) 或称项 (entry), 用 a_{ij} 表示矩阵 A 的第 (i, j) 元素

$a_{m1} a_{m2} \dots a_{mn}$

即矩阵 A 在第 i 行第 j 列位置上的数。

有时简写为 $A = [a_{ij}]$, 表示第 (i, j) 元素为 a_{ij} 的矩阵 A 。

矩阵相等: 如果两个矩阵有同样数量的行和列, 且每个位置的对应项都相等, 则两个矩阵是相等的。

即有对矩阵 A 和 B , $A = B \iff (A$ 和 B 都是 $m \times n$ 矩阵 $\wedge \forall i \in m \forall j \in n a_{ij} = b_{ij})$, 其中 $m, n, i, j \in \mathbb{Z}^+$

矩阵加法 (matrix addition) 用 $A + B$ 表示矩阵 A 和 B 的和, 即其第 (i, j) 元素等于 $a_{ij} + b_{ij}$ 的矩阵。

即令 $A = [a_{ij}]$ 和 $B = [b_{ij}]$ 是 $m \times n$ 矩阵, 则 $A + B$ 是 $m \times n$ 矩阵且 $A + B = [a_{ij} + b_{ij}]$

矩阵乘法 (matrix multiplication) 用 AB 表示矩阵 AB 的乘积, 即其第 (i, j) 元素等于 A 的第 i 行和 B 的第 j 列的乘积之和。

即令 $A = [a_{ij}]$ 是 $m \times k$ 矩阵, $B = [b_{ij}]$ 是 $k \times n$ 矩阵, 则 AB 是 $m \times n$ 矩阵

且 $AB = [c_{ij}]$, $c_{ij} = \sum_{x=1}^k a_{ix} b_{xj}$, 其中 $m, n, i, j \in \mathbb{Z}^+, 1 \leq i \leq m, 1 \leq j \leq n$

注意如果 A 的列数与 B 的行数不相等, 则 AB 无定义。

特别注意: 矩阵乘法不服从交换律, 即 $AB \neq BA$ 不一定相等。

如 $A = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$, $AB = \begin{bmatrix} 3 & 2 \\ 5 & 3 \end{bmatrix}$, $BA = \begin{bmatrix} 4 & 3 \\ 3 & 2 \end{bmatrix}$. 可见此时 $AB \neq BA$

但是注意, 如果 AB 与 BA 均有定义且具有相同大小, 则 A 和 B 必定是方阵且具有相同大小。

如 $A = m \times n$, $B = n \times m$, 则 $AB = m \times m$, $BA = n \times n$

n 阶单位矩阵 (identity matrix of order n) 为 $n \times n$ 矩阵, 主对角线上元素为 1, 其他位置元素为 0。

即 $n \times n$ 矩阵 $I_n = [s_{ij}]$. 有 $I_n = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$

其中 $s_{ij} = \begin{cases} 1, & i=j \\ 0, & i \neq j \end{cases}$

注意: 矩阵乘以合适的单位矩阵不会改变该矩阵。

如对于 $m \times n$ 矩阵 A , 有 $I_m A = A I_n = A$

方阵的幂次

定义方阵的幂次如: 对于 $n \times n$ 矩阵 A , 则 $A^0 = I_n$, $A^{r+r} = \underbrace{AA \cdots A}_{r+1 \text{ 个 } A}$, $= A^{r-1} A$. 其中 $r \in \mathbb{Z}^+$

Discrete

11月 - 陈海峰

Mathematics - P 25

转置

(transpose), 用 A^T 表示矩阵 A 的转置, 即交换 A 的行和列得到的矩阵

即有对 $m \times n$ 矩阵 $A = [a_{ij}]$, 则 $A^T = [b_{ij}]$, 且 $b_{ij} = a_{ji}$, 其中 $1 \leq i \leq n, 1 \leq j \leq m, m, n, i, j \in \mathbb{Z}^+$

注意, 转置本身具有性质, 对于 $m \times p$ 矩阵 A 和 $p \times n$ 矩阵 B , $(A^T)^T = A$, $(AB)^T = B^T A^T$

对于 $m \times n$ 矩阵 A 和 B , $(A+B)^T = A^T + B^T$

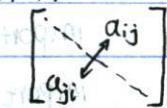
对于 $n \times n$ 矩阵 A , AA^T 是对称的, $A+A^T$ 也是对称的

对称矩阵 (symmetric matrix)

如果一个矩阵与其转置相等, 则该矩阵是对称的, 即 $A = A^T$

即对于 $n \times n$ 矩阵 A , A 是对称的 $\leftrightarrow \forall 1 \leq i \leq n \forall 1 \leq j \leq n a_{ij} = a_{ji}$

或者说矩阵是对称的 \leftrightarrow 矩阵是方阵且相对于主对角线对称



0-1矩阵 (zero-one matrix)

所有元素非0即1, 即 $a_{ij} \in \{0, 1\}$, 0-1矩阵常用于表示各类离散结构

而使用这些结构的算法是基于0-1矩阵的布尔算术运算

布尔算术运算基于布尔运算 \wedge 和 \vee , 通常作用在成对的位上

矩阵的并 (join)

用 AVB 表示 $m \times n$ 的0-1矩阵 A 和 B 的并, 该矩阵也是 $m \times n$ 的0-1矩阵

即对于 $m \times n$ 0-1矩阵 $A = [a_{ij}]$, $B = [b_{ij}]$, $AVB = [c_{ij}]$, 且 $c_{ij} = a_{ij} \vee b_{ij}, 1 \leq i \leq m, 1 \leq j \leq n, m, n, i, j \in \mathbb{Z}^+$

矩阵的交 (meet)

用 $A \wedge B$ 表示 $m \times n$ 的0-1矩阵 A 和 B 的交, 该矩阵也是 $m \times n$ 的0-1矩阵

即对于 $m \times n$ 0-1矩阵 $A = [a_{ij}]$, $B = [b_{ij}]$, $A \wedge B = [c_{ij}]$, 且 $c_{ij} = a_{ij} \wedge b_{ij}, 1 \leq i \leq m, 1 \leq j \leq n, m, n, i, j \in \mathbb{Z}^+$

布尔积

(Boolean product), 用 $A \odot B$ 表示 $m \times k$ 0-1矩阵 A 和 $k \times n$ 0-1矩阵 B 的布尔积

$m \times k$ 矩阵 A 与 $k \times n$ 0-1矩阵 B 的布尔积是 $m \times n$ 0-1矩阵

$1 \leq i \leq m$

即有对于 $A = [a_{ij}]$, $B = [b_{ij}]$, $A \odot B = [c_{ij}]$, 且 $c_{ij} = (a_{i1} \wedge b_{i1}) \vee \dots \vee (a_{ik} \wedge b_{ik}), 1 \leq i \leq m, 1 \leq j \leq n, m, n, k, i, j, k \in \mathbb{Z}^+$

或者可简写为 $A \odot B = [c_{ij}]$, $c_{ij} = \bigvee_{k=1}^k (a_{ik} \wedge b_{kj})$

如果 A 为 0-1 方阵, 且 $r \in \mathbb{Z}^+$, 则定义 A 的 r 次布尔幂是 r 个 A 的布尔积, 记作 $A^{[r]}$

即 $A^{[r]} = A \odot A \odot \dots \odot A (r \uparrow A)$, 且 $A^{[0]} = I_n$

或者如递归地定义, $A^{[0]} = I_n$, $A^{[r]} = A \odot A^{[r-1]}$

注意 布尔积符合结合律, 即对于 $m \times p$ 矩阵 A , $p \times k$ 矩阵 B , $k \times n$ 矩阵 C , $m, p, k, n \in \mathbb{Z}^+$

有 $(A \odot B) \odot C = A \odot (B \odot C)$

另外布尔算术运算 \vee 和 \wedge 符合幂等律, 即 $A \vee A = A$, $A \wedge A = A$

注意在使用此类性质时

交换律, 即 $AVB = BVA$, $A \wedge B = B \wedge A$

应先确认相关计算有

结合律, 即 $(AVB)VC = AV(BVC)$, $(A \wedge B)AC = A \wedge (BAC)$

分配律, 即 $AV(CBA) = (AVB)AC$, $A \wedge (BVC) = (A \wedge B)VC$