

Discrete

Mathematics - P120

推论规则 (consequence rule)

推论规则 (consequence rule), 用于强化前置条件, 弱化后置条件的霍尔规则

to strengthen the precondition and/or to weaken the postcondition

即记为 $P_1 \rightarrow P_2, \{P_1\} S \{Q_2\}, Q_2 \rightarrow Q_1$, 或者写作 $P_1 \rightarrow P_2, P_2 \{S\} Q_2, Q_2 \rightarrow Q_1$

$\{P_1\} S \{Q_1\}$

其中 P_1 为一个对于初始断言 P_2 , 使蕴含式 $P_1 \rightarrow P_2$ 始终为真的断言

Q_1 为一个对于终结断言 Q_2 , 使蕴含式 $Q_2 \rightarrow Q_1$ 始终为真的断言

则可以通过替换使 $\{P_2\} S \{Q_2\}$ 成为 $\{P_1\} S \{Q_1\}$

循环不变量 (loop invariant), 在循环的每次执行期间都保持为真的性质

在证明一个循环的正确性时, 需要分三个阶段证明循环不变量为真

初始化: 在循环的第一次迭代 (iteration) 开始前, 断言为真

保持: 如果在循环的某一次迭代开始前断言, 则循环的下一次迭代开始前断言为真

终止: 在循环终止时, 断言为真, 并且作为一个有用的性质用于证明包含循环的算法

注意, 这里可以看作应用了推论规则, 证明一个弱于循环不变量的后置条件

while 规则 (while rule), 应用霍尔规则于程序中的循环结构, 如 for, while, do-while

由于不同的循环结构在逻辑上是等价的, 这里考虑形如 while B do S done 的语句块

对于断言 P 作为循环不变量, B 作为循环条件 (condition), S 为循环体的语句块

则记为 $\{P \wedge B\} S \{P\}$ 或者写作 $(P \wedge \text{condition}) \{S\} P$

$\{P\} \text{while } B \text{ do } S \text{ done} \{\neg B \wedge P\} P \{ \text{while condition } S \} (\neg \text{condition} \wedge P)$

注意与条件规则类似, 循环条件断言 B 不能有副作用, 且 B 为假时终止循环

注意, 条件结构可以用一次循环结构 (one-time loop construct) 表示, 令 b 为循环条件

即 $b := \text{true}; \text{while } B \wedge b \text{ do } S; b := \text{false} \text{ done}; b := \text{true}; \text{while } \neg B \wedge b \text{ do } T; b := \text{false} \text{ done}$

如果 B 为真, 则执行 S, 并且强制终止循环。如果 B 为假, 则执行 T, 并且强制结束循环。

则此语句块与 if B then S else T endif 是等价的

注意上述一般 while rule 还需证明循环终止, 以证明全局正确性 (total correctness)

记为 $\langle \text{is a well-founded ordering on the set } D, \{P \wedge B \wedge t = z\} S \{P \wedge t \in D \wedge t < z\}$

$\{P \wedge t \in D\} \text{while } B \text{ do } S \text{ done} \{\neg B \wedge P \wedge t \in D\}$

对于集合 D, 偏序集 $(D, <)$ 是良基的, 即不存在元素的无限递减序列。

infinite length

即保证了循环变量 (loop variant) t 不能无限下降, 而存在 strictly decreasing chain with

注意, 循环条件 B 必须蕴含 t 不是集合 D 中的最小元素。

Discrete

Mathematics - P121

对于正整数 n , 令 f_n 为第 n 个斐波那契数, 另外对 $n=0$, $f_0=0$

对于任意非负整数 n, k , 有 $f_k f_n + f_{k+1} f_{n+1} = f_{n+k+1}$

基础步骤聚: 当 $k=0$ 时, 对于任意非负整数 n , 当 $k=1$ 时, $f_1 f_n + f_2 f_{n+1} = f_n + f_{n+1}$

$$f_0 f_n + f_1 f_{n+1} = 0 \times f_n + 1 \times f_{n+1} = f_{n+1} = f_{n+k+1} = f_{n+2} = f_{n+k+1}$$

递归步聚: 假设对任意 $k \in \mathbb{Z}^+$ 有对于任意 $n \in \mathbb{N}$, $P(n, 0) \wedge P(n, 1) \wedge \dots \wedge P(n, k)$ 为真

$$\text{则对于 } P(n, k+1), f_{k+1} f_n + f_{k+2} f_{n+1} = (f_k + f_{k+1}) f_n + (f_k + f_{k+1}) f_{n+1}$$

$$= (f_k f_n + f_{k+1} f_{n+1}) + (f_{k+1} f_n + f_k f_{n+1})$$

$$\text{根据归纳假设 } P(n, k), P(n, k-1) \stackrel{(IH)}{=} f_{n+k+1} + f_{n+k} = f_{n+k+2} = f_{n+(k+1)+1}$$

于是根据扩展归纳法, 有对于任意 $n, k \in \mathbb{N}$, 有 $f_k f_n + f_{k+1} f_{n+1} = f_{n+k+1}$

卢卡斯数 (Lucas number), 为定义在非负整数上的序列 L_n , 其中 $n=0, 1, 2, \dots$

递归地定义序列的第 n 项 L_n , $n \in \mathbb{N}$

$$L_n = \begin{cases} 2 & n=0 \\ 1 & n=1 \\ L_{n-1} + L_{n-2} & n>1 \end{cases}$$

对于正整数 n , 有 $f_n + f_{n+2} = L_{n+1}$

基础步聚: 当 $n=1$ 时, $f_1 + f_3 = 1 + 2 = 3 = L_0 + L_1 = L_2$

递归步聚: 假设对任意 $n \in \mathbb{Z}^+$, $P(n) \wedge \dots \wedge P(n)$ 为真, 则考虑 $P(n+1)$

$$f_{n+1} + f_{n+3} = (f_{n-1} + f_n) + (f_{n+1} + f_{n+2})$$

$$= (f_{n-1} + f_{n+1}) + (f_n + f_{n+2})$$

特别地有, 当 $n=1$ 时, $f_{n-1} + f_{n+1} = f_0 + f_2 = 1 = L_1$

$$\text{于是 } f_{n+1} + f_{n+3} \stackrel{(IH)}{=} L_n + L_{n+1} = L_{n+2} = L_{(n+1)+1}$$

于是根据强归纳法, 有对于任意 $n \in \mathbb{Z}^+$, $f_n + f_{n+2} = L_{n+1}$

另外推广至对于任意 $n \in \mathbb{N}$, $f_n + f_{n+2} = L_{n+1}$ 也成立

高阶数列的和: $L_0^2 + L_1^2 + \dots + L_n^2 = L_n L_{n+1} + 2$

对于非负整数 n , 有 $L_0^2 + L_1^2 + \dots + L_n^2 = L_n L_{n+1} + 2$

基础步聚: 当 $n=0$ 时, $L_0^2 = 4 = 2 \times 1 + 2 = L_0 L_1 + 2 = m$

递归步聚: 假设对任意 $n \in \mathbb{N}$, $P(n)$ 为真, 则考虑 $P(n+1)$

$$L_0^2 + L_1^2 + \dots + L_n^2 + L_{n+1}^2 \stackrel{(IH)}{=} L_n L_{n+1} + 2 + L_{n+1}^2 =$$

$$= (L_n + L_{n+1}) L_{n+1} + 2 = 1$$

$$= L_{n+1} L_{n+2} + 2 = m + 1$$

于是依据数学归纳法, 有对于任意 $n \in \mathbb{N}$, 有 $L_0^2 + L_1^2 + \dots + L_n^2 = L_n L_{n+1} + 2$

对比斐波那契数, 有对于任意 $n \in \mathbb{Z}^+$, $f_1^2 + f_2^2 + \dots + f_n^2 = f_n f_{n+1}$

由于 $f_0=0$, 推广至对任意 $n \in \mathbb{N}$, $f_0^2 + f_1^2 + \dots + f_n^2 = f_n f_{n+1}$ 也成立

Discrete

Mathematics - P122

Binet's formula

def - step

对于非负整数 n , 令 L_n 为卢卡斯数的第 n 项, 其中 $\phi = \frac{1+\sqrt{5}}{2}$, $\hat{\phi} = \frac{1-\sqrt{5}}{2}$

对于任意 $n \in \mathbb{N}$, 有 $L_n = \phi^n + \hat{\phi}^n$, 其中 ϕ 为黄金分割率 $\frac{1+\sqrt{5}}{2}$, $\hat{\phi}$ 为 ϕ 的共轭 $\frac{1-\sqrt{5}}{2}$

基础步骤: 当 $n=0$ 时, $\phi^0 + \hat{\phi}^0 = 2 = L_0$

当 $n=1$ 时, $\phi^1 + \hat{\phi}^1 = 1 = L_1$

由于对任意 $n \in \mathbb{Z}^+$ 且 $n > 1$, 有 $L_n = L_{n-1} + L_{n-2}$

则考虑等比数列 $(L_n + \alpha L_{n-1}) = \beta(L_{n-1} + \alpha L_{n-2})$, 其中 $\alpha, \beta \in \mathbb{R}$

则 $L_n = (\beta - \alpha)L_{n-1} + (\beta\alpha)L_{n-2}$, 于是有方程组 $\begin{cases} \beta - \alpha = 1 \\ \beta\alpha = 1 \end{cases}$

解方程组有 $\alpha = \frac{\sqrt{5}-1}{2}$, $\beta = \frac{\sqrt{5}+1}{2}$

又 等比数列的第一项 $L_1 + \alpha L_0 = 1 + 2\alpha = \alpha + \beta$

于是 $(L_{n+1} + \alpha L_n) = \beta^n(L_1 + \alpha L_0) = \alpha\beta^n + \beta^{n+1}$

又 $\beta \neq 0$, 则 $\frac{\beta^{n+1}}{\beta^{n+1}} + \frac{\alpha}{\beta} \cdot \frac{\beta^n}{\beta^n} = \frac{\alpha}{\beta} + 1$, 取 数列 $\{b_n\}$, 其中 $b_n = \frac{L_n}{\beta^n}$

则有 $b_{n+1} + \frac{\alpha}{\beta} \cdot b_n = \frac{\alpha}{\beta} + 1$, 则有 $b_{n+1} - 1 = -\frac{\alpha}{\beta}(b_n - 1)$

于是可知数列 $\{b_n - 1\}$ 是等比数列

即 $b_n - 1 = \left(\frac{-\alpha}{\beta}\right)^n(b_0 - 1)$, 且有 $b_0 = \frac{2}{\beta}$, 则 $b_0 - 1 = 1$

于是有 $L_n/\beta^n - 1 = \left(\frac{-\alpha}{\beta}\right)^n$, 即 $L_n = \beta^n + (-\alpha)^n$

又 $\beta = \phi$, $\alpha = \frac{\sqrt{5}-1}{2} = -\hat{\phi}$, 即 $L_n = \phi^n + \hat{\phi}^n$, $n > 1$

于是可知对任意 $n \in \mathbb{N}$, 有 $L_n = \phi^n + \hat{\phi}^n$

对于正整数 $n > 1$, $L_n = \lfloor \phi^n + \frac{1}{2} \rfloor$, 即 L_n 是距离 ϕ^n 最近的整数

证明过程有, 已知 $L_n = \phi^n + \hat{\phi}^n$. 且 L_n 为整数,

$\hat{\phi} = \frac{1-\sqrt{5}}{2}$, 即 $|\hat{\phi}| < 1$, 即 对于任意 $n \in \mathbb{Z}^+$ $|\hat{\phi}^n| = |\hat{\phi}|^n < 1$

又 $|\phi|^2 = \frac{3-\sqrt{5}}{2} < \frac{1}{2}$, 即 对于任意 $n > 2$, $|\phi|^n = |\phi|^2 \cdot |\phi^{n-2}| < \frac{1}{2} \cdot 1 = \frac{1}{2}$

又 L_n 为整数, 所以 $L_n < L_n + 1$, 令 $\phi^n = k_1 + \xi$, $\hat{\phi}^n = k_2 - \xi$, 其中 $k_1, k_2 \in \mathbb{Z}$,

又 $|\hat{\phi}^n| < \frac{1}{2}$, 当 $n > 1$ 时,

于是可知当 $0 \leq \xi < \frac{1}{2}$ 时, $\hat{\phi}^n = -\xi$, $\phi^n + \frac{1}{2} = L_n - \hat{\phi}^n + \frac{1}{2} = L_n + (\frac{1}{2} + \xi) < L_n + 1$

提有, 当 $0 \leq \xi < \frac{1}{2}$ 时, $L_n = \lfloor \phi^n + \frac{1}{2} \rfloor$

而当 $\frac{1}{2} < \xi < 1$ 时, $\hat{\phi}^n = 1 - \xi$, $\phi^n + \frac{1}{2} = L_n - \hat{\phi}^n + \frac{1}{2} = L_n + (1 - \xi - \frac{1}{2}) < L_n + 1$

提有当 $\frac{1}{2} < \xi < 1$ 时, $L_n = \lfloor \phi^n + \frac{1}{2} \rfloor$

即有对于任意正整数 $n > 1$, 有 $L_n = \lfloor \phi^n + \frac{1}{2} \rfloor$

即对于任意正整数 $n > 1$, 有 L_n 为最接近 ϕ^n 的整数

又根据 Binet's formula, 有 $f_n = \frac{\phi^n - \hat{\phi}^n}{\sqrt{5}}$

于是有 $\phi^n = (L_n + \sqrt{5} \cdot f_n)/2$, 其中 $n \in \mathbb{N}$

Discrete

Mathematics - P123

5.29 - Solution

对于非负整数 n , f_n 是斐波那契序列的第 n 项, L_n 是卢卡斯数的第 n 项

对于任意非负整数 n , 有 $L_n^2 = 5f_n^2 + 4(-1)^n$

证明过程有, 已知 $L_n = \phi^n + \hat{\phi}^n$, $f_n = (\phi^n - \hat{\phi}^n)/\sqrt{5}$, 其中 $\phi = \frac{1+\sqrt{5}}{2}$, $\hat{\phi} = \frac{1-\sqrt{5}}{2}$

又 $\phi \cdot \hat{\phi} = -1$, 即 $\phi^n \cdot \hat{\phi}^n = (\phi \cdot \hat{\phi})^n = (-1)^n$, 对于 $n \in \mathbb{N}$ 成立

于是有 $L_n^2 = (\phi^n + \hat{\phi}^n)^2 = (\phi^n - \hat{\phi}^n)^2 + 4(\phi^n \hat{\phi}^n)$

$= 5[(\phi^n - \hat{\phi}^n)/\sqrt{5}]^2 + 4(-1)^n$

是有对任意 $n \in \mathbb{N}$, 有 $L_n^2 = 5f_n^2 + 4(-1)^n$

又 L_n 和 f_n 均为正整数, 且当 $n \rightarrow +\infty$ 时, 有 $f_n \rightarrow +\infty$

于是有 $L_n^2/f_n^2 = 5 + 4(-1)^n/f_n^2$

则极限 $\lim_{n \rightarrow +\infty} L_n^2/f_n^2 = 5 + \lim_{n \rightarrow +\infty} 4(-1)^n/f_n^2 = 5 + 0 = 5$

于是有 $\lim_{n \rightarrow +\infty} \frac{L_n}{f_n} = \sqrt{5}$

对于任意正整数 n , 任意连续 n 个正整数之积只能被 $n!$ 整除

令对于 $m, n \in \mathbb{Z}^+$, 命题 $P(m, n)$ 为 $n! \mid m(m+1) \dots (m+n-1)$

基础步骤: 当 $n=1$ 时, 对任意 $m \in \mathbb{Z}^+$, $1 \mid m$ 平凡地成立

当 $m=1$ 时, 对任意 $n \in \mathbb{Z}^+$, 有 $m(m+1) \dots (m+n-1) = n!$ 平凡地成立

递归步骤: 假设对于正整数 $m > 1, n > 1$, 对任意字典序小于 (m, n) 的正整数序偶 (m', n')

即 $m' \in \mathbb{Z}^+, n' \in \mathbb{Z}^+$ 且 $(m', n') < (m, n)$, 有 $P(m', n')$ 为真, 则考虑 $P(m, n)$

$$m(m+1) \dots (m+n-1)/n! = (m+n-1)!/n!(m-1)!$$

$$\begin{aligned} &= (m+n-1)!/(m-1)! = \binom{m+n-1}{m-1} = \binom{m+n-2}{m-1} + \binom{m+n-2}{m-2}, \text{ 其中 } m > 1, n > 1 \\ &= \frac{(m+n-2)!}{(m-2)! n!} + \frac{(m+n-2)!}{m(m-1)! (n-1)!} \end{aligned}$$

$$= (m-1)m \dots (m+n-2)/n! + m(m+1) \dots (m+n-2)/(n-1)!$$

根据归纳假设 $P(m-1, n), P(m, n-1)$ 为真, 则存在 $t \in \mathbb{Z}^+$, 使得 $s = (m-1)m \dots (m+n-2)/n!$

$$\text{于是 } m(m+1) \dots (m+n-1)/n! = s+t \in \mathbb{Z}^+, \text{ 即 } n! \mid m(m+1) \dots (m+n-1)$$

于是根据强归纳法, 对于任意 $n \in \mathbb{Z}^+$, 任意连续 n 个正整数之积只能被 $n!$ 整除

对于任意正整数 n , $(\cos x + i \sin x)^n = \cos nx + i \sin nx$ 于是依据数学归纳法

基础步骤: 当 $n=1$ 时, $(\cos x + i \sin x)^1 = \cos x + i \sin x$, 对于任意 $n \in \mathbb{Z}^+$ 有

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

$$(\cos x + i \sin x)^{n+1} \stackrel{(IH)}{=} (\cos nx + i \sin nx)(\cos x + i \sin x)$$

$$= (\cos nx \cos x - \sin nx \sin x) + i(\sin nx \cos x + \cos nx \sin x) = \cos(n+1)x + i \sin(n+1)x, \text{ 即 } P(n+1) \text{ 为真}$$

Discrete

Mathematics - P124

基础证明

对于任意正整数 n , 且有 $\sin(x/2) \neq 0$, 则有 $\sum_{j=1}^n \cos jx = \cos[(n+1)x/2] \sin(nx/2) / \sin(x/2)$

基础步骤：当 $n=1$ 时, $\sum_{j=1}^1 \cos jx = \cos x = \cos[2x/2] \cdot \sin(x/2) / \sin(x/2)$

递归步骤：假设对任意 $n \in \mathbb{Z}^+$, $P(n)$ 为真, 则考虑 $P(n+1)$

$$\sum_{j=1}^{n+1} \cos jx \stackrel{(IH)}{=} (\cos[(n+1)x/2] \sin(nx/2) / \sin(x/2)) + \cos[(n+1)x]$$

$$= [\cos \frac{(n+1)x}{2} \sin \frac{nx}{2} + \cos \frac{(2n+2)x}{2} \sin \frac{x}{2}] / \sin \frac{x}{2}$$

根据积化和差公式: $\cos \alpha \sin \beta = \frac{1}{2} \sin(\alpha+\beta) - \frac{1}{2} \sin(\alpha-\beta)$

$$\begin{aligned} \text{于是 } \sum_{j=1}^{n+1} \cos jx &= [\frac{1}{2} \sin \frac{(2n+1)x}{2} - \frac{1}{2} \sin \frac{x}{2} + \frac{1}{2} \sin \frac{(2n+3)x}{2} - \frac{1}{2} \sin \frac{(2n+1)x}{2}] / \sin \frac{x}{2} \\ &= [\frac{1}{2} \sin \frac{(2n+3)x}{2} - \frac{1}{2} \sin \frac{x}{2}] / \sin \frac{x}{2} \\ &= \cos \frac{(2n+4)x}{4} \sin \frac{(2n+2)x}{4} / \sin \frac{x}{2} \end{aligned}$$

$$\text{因此 } \sum_{j=1}^{n+1} \cos jx = \cos[(n+1+1)x/2] \sin[(n+1)x/2] / \sin(x/2)$$

于是根据数学归纳法, 有对任意 $n \in \mathbb{N}^+$, 且 $\sin(x/2) \neq 0$

$$\sum_{j=1}^n \cos jx = \cos[(n+1)x/2] \sin(nx/2) / \sin(x/2)$$

对于任意非负整数 n , 对于平面坐标系中 $x \geq 0, y \geq 0, x+y \leq n$ 的格点

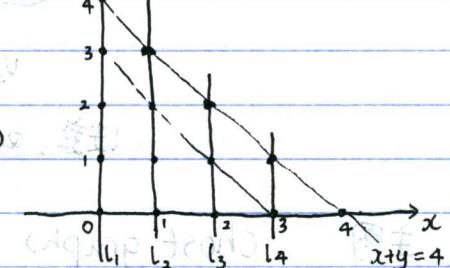
需要至少 $n+1$ 条直线, 才能确保每一个点至少位于其中一条直线上

基础步骤: 当 $n=0$ 时, 需要至少 1 条直线经过 $(0, 0)$

当 $n=1$ 时, 需要至少 2 条直线经过 $(0, 0), (0, 1), (1, 0)$

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

$\forall x \in \mathbb{R}$ 中某一点 x , 可将 $P(n+1)$ 划分为 $x+y < n+1$ 和 $x+y = n+1$ 两部分



其中 $x \geq 0, y \geq 0, x+y < n+1$ 的部分满足 $P(n)$, 即存在 $n+1$ 条直线满足要求 $\{l_1, l_2, \dots, l_{n+1}\}$

由于 $x \geq 0, y \geq 0, x+y=n+1$ 共有 $n+2$ 个格点, 且全部位于直线 $l: x+y=n+1$ 上,

又 $l \notin \{l_1, l_2, \dots, l_{n+1}\}$, 所以 $\forall l_i \in \{l_1, l_2, \dots, l_{n+1}\}, l_i$ 与 l 仅有一个交点,

而 $\{l_1, l_2, \dots, l_{n+1}, l\}$ 满足 $P(n+1)$ 的要求.

于是根据数学归纳法, 有对任意 $n \in \mathbb{N}$, 对于平面坐标系中 $x \geq 0, y \geq 0, x+y \leq n$ 的格点,

需要至少 $n+1$ 条直线, 才能确保每一个格点至少位于其中一条直线上

基础证明: 基本证明

对于函数 $f_1(x), f_2(x), \dots, f_n(x)$ 都不为 0 且可导, 则有 $\frac{[f_1(x)f_2(x)\dots f_n(x)]'}{f_1(x)f_2(x)\dots f_n(x)} = \frac{f'_1(x)}{f_1(x)} + \frac{f'_2(x)}{f_2(x)} + \dots + \frac{f'_n(x)}{f_n(x)}$

基础步骤: 当 $n=1$ 时, $f'_1(x)/f_1(x) = f'_1(x)/f_1(x)$ 平凡地成立

递归步骤: 假设对任意 $n \in \mathbb{Z}^+$, $P(n)$ 为真, 则考虑 $P(n+1)$

$$\begin{aligned} \frac{[f_1(x)\dots f_n(x)f_{n+1}(x)]'}{f_1(x)\dots f_n(x)f_{n+1}(x)} &= \frac{[f_1(x)\dots f_n(x)f_{n+1}(x)]' + [f_1(x)\dots f_n(x)]f'_{n+1}(x)}{f_1(x)\dots f_n(x)f_{n+1}(x)} = \frac{[f_1(x)\dots f_n(x)]'}{f_1(x)\dots f_n(x)} + \frac{f'_{n+1}(x)}{f_{n+1}(x)} \\ &\stackrel{(IH)}{=} \frac{f'_1(x)}{f_1(x)} + \dots + \frac{f'_n(x)}{f_n(x)} + \frac{f'_{n+1}(x)}{f_{n+1}(x)} \end{aligned}$$

于是依据数学归纳法, 对于任意 $n \in \mathbb{Z}^+$, 函数 $f_1(x), f_2(x), \dots, f_n(x)$ 不等于 0 且可导

$$\text{则有 } [f_1(x)f_2(x)\dots f_n(x)]'/f_1(x)f_2(x)\dots f_n(x) = f'_1(x)/f_1(x) + f'_2(x)/f_2(x) + \dots + f'_n(x)/f_n(x)$$

Discrete

Mathematics - P125

St 8/10/2017

对于正实数 x_1, x_2, \dots, x_n , 其中 $n \geq 2$, 有 $(x_1 + \frac{1}{x_1})(x_2 + \frac{1}{x_2}) \cdots (x_n + \frac{1}{x_n}) \geq (x_1 + \frac{1}{x_2})(x_2 + \frac{1}{x_3}) \cdots (x_n + \frac{1}{x_1})$

$$\text{基础步骤聚: 当 } n=2 \text{ 时, } (x_1 + \frac{1}{x_1})(x_2 + \frac{1}{x_2}) = \frac{x_1^2 x_2^2 + x_1^2 + x_2^2 + 1}{x_1 x_2}$$

$$(x_1 + \frac{1}{x_2})(x_2 + \frac{1}{x_1}) = \frac{x_1^2 x_2^2 + 2x_1 x_2 + 1}{x_1 x_2}$$

又 x_1, x_2 为正实数, 则 $x_1^2 + x_2^2 \geq 2x_1 x_2$, 即 $(x_1 + \frac{1}{x_1})(x_2 + \frac{1}{x_2}) \geq (x_1 + \frac{1}{x_2})(x_2 + \frac{1}{x_1})$

递归步聚: 假设对于任意正整数 $2 \leq p < n$, 有 $P(p)$ 成立. 则考虑 $P(n)$

如果存在 $1 \leq i \leq j \leq n$, 使得 $x_i = x_j$.

$$\text{如果 } x_i \text{ 与 } x_j \text{ 相邻, 包括 } i=1, j=n \text{ 时,} \\ \text{则有 } \cdots (x_{\text{pre}(i)} + \frac{1}{x_i})(x_i + \frac{1}{x_j})(x_j + \frac{1}{x_{\text{succ}(j)}}) \cdots$$

$\cdots [(x_{\text{pre}(i)} + \frac{1}{x_j})(x_j + \frac{1}{x_{\text{succ}(j)}}) \cdots] (x_i + \frac{1}{x_i})$

可知前半部分满足 x_1, x_2, \dots, x_n 去掉 x_i 的情形, 即 $P(n-1)$ 为真

$$\text{于是 } (x_1 + \frac{1}{x_2}) \cdots (x_n + \frac{1}{x_1}) = [\cdots (x_{i-1} + \frac{1}{x_j})(x_j + \frac{1}{x_{j+1}}) \cdots] (x_i + \frac{1}{x_i})$$

$$\stackrel{(IH)}{\leq} [(x_1 + \frac{1}{x_2}) \cdots (x_{i-1} + \frac{1}{x_{i-1}})(x_j + \frac{1}{x_j}) \cdots (x_n + \frac{1}{x_1})] \cdot (x_i + \frac{1}{x_i})$$

如果 x_i 与 x_j 不相邻, 则存在两个节点, $x_i \rightarrow x_{i+1} \rightarrow \cdots \rightarrow x_j \rightarrow x_{j+1} \rightarrow \cdots \rightarrow x_n$, 即 $P(n)$ 为真

$$\cdots (x_{i-1} + \frac{1}{x_i})(x_i + \frac{1}{x_{i+1}}) \cdots \text{ 和 } \cdots (x_{j-1} + \frac{1}{x_j})(x_j + \frac{1}{x_{j+1}}) \cdots$$

则替换为 $\cdots (x_{i-1} + \frac{1}{x_i})(x_i + \frac{1}{x_{i+1}}) \cdots (x_j + \frac{1}{x_i})(x_j + \frac{1}{x_{j+1}}) \cdots$

$x_i \leftarrow x_n$ 可知此形成了两个长度为 p 和 q 的回路, 且 $2 \leq p, q < n$, $p+q=n$

$x \in A \cup B$ 且 x_i, x_2, \dots, x_n 分别属于两个回路, 即 $P(p)$ 与 $P(q)$ 为真

$$x_i \leftarrow x_j \rightarrow x_{j+1} \cdots \leftarrow x_{i-1} \text{ 于是有 } (x_1 + \frac{1}{x_2}) \cdots (x_n + \frac{1}{x_1}) = [(x_i + \frac{1}{x_{i+1}}) \cdots (x_{j-1} + \frac{1}{x_j})] [(x_j + \frac{1}{x_{j+1}}) \cdots (x_{n-1} + \frac{1}{x_n})] (x_i + \frac{1}{x_{i+1}}) \cdots (x_{j-1} + \frac{1}{x_j})$$

$$\stackrel{(IH)}{\leq} [(x_1 + \frac{1}{x_2}) \cdots (x_{i-1} + \frac{1}{x_{i-1}})] [(x_j + \frac{1}{x_j}) \cdots (x_{n-1} + \frac{1}{x_n})] (x_i + \frac{1}{x_{i+1}}) \cdots (x_{j-1} + \frac{1}{x_j})$$

$$= (x_1 + \frac{1}{x_2}) \cdots (x_n + \frac{1}{x_1}), \text{ 即 } P(n) \text{ 为真}$$

假设 x_1, x_2, \dots, x_n 两两不相等, 且 $n \geq 4$ 时

则在回路上总能找到两个不相邻的节点 (x_i, x_{i+1}) 和 (x_j, x_{j+1})

基础步聚(+): 使得 $x_i > x_j$ 且 $x_{i+1} < x_j$, 又 $x_i, x_{i+1}, x_j, x_{j+1} > 0$

当 $n=3$ 时

$$(x_1 + \frac{1}{x_1})(x_2 + \frac{1}{x_2})(x_3 + \frac{1}{x_3})$$

$$= \frac{(x_1^2 + 1)(x_2^2 + 1)(x_3^2 + 1)}{x_1 x_2 x_3}$$

$$(x_1 + \frac{1}{x_2})(x_2 + \frac{1}{x_3})(x_3 + \frac{1}{x_1})$$

$$= \frac{(x_1 x_2 + 1)(x_2 x_3 + 1)(x_3 x_1 + 1)}{x_1 x_2 x_3}$$

于是得

$$\frac{[(x_1^2 x_2^2 + x_1^2 + x_2^2 + x_3^2) + (x_2^2 x_3^2 + x_2^2 + x_3^2 + x_1^2) + (x_3^2 x_1^2 + x_3^2 + x_1^2 + x_2^2)]}{x_1 x_2 x_3} / x_1 x_2 x_3$$

$$= [(x_1 x_2 - x_3 x_1)^2 + (x_2 x_3 - x_1 x_2)^2 + (x_3 x_1 - x_2 x_3)^2] / 2x_1 x_2 x_3 \geq 0$$

即 $P(3)$ 为真

提有对正实数 $x_1, x_2, \dots, x_n (n \geq 2)$, $(x_1 + \frac{1}{x_1})(x_2 + \frac{1}{x_2}) \cdots (x_n + \frac{1}{x_n}) \geq (x_1 + \frac{1}{x_2})(x_2 + \frac{1}{x_3}) \cdots (x_n + \frac{1}{x_1})$

Discrete

Mathematics - P126

$\underbrace{a^{\dots^a}}_b \bmod n$

计算迭代幂次的模运算，即对于 a, b, n 为正整数， $(\text{tetration of } a) \bmod n$

$$\text{计算 } a^b \bmod n = (a \uparrow\uparrow b) \bmod n = (a [4] b) \bmod n = (a \rightarrow b \rightarrow 2) \bmod n$$

Algorithm to reduce power mod calculations

根据欧拉函数(Euler's totient function)的应用

有结论为：对于任意正整数 a, m ，有 m 的欧拉函数值为 $\varphi(m)$

则对于正整数 k ，如果有 $k > \lg m$ ， $a^k \bmod m = a^{\lg m} \bmod m$

$$\text{则有 } a^{k+\varphi(m)} \bmod m = a^k \bmod m.$$

注意这个应用中并不要求 a, m 互素，即 $\gcd(a, m) = 1$

于是可以得到一个递归的计算过程，根据迭代幂次的定义有 $a \uparrow\uparrow b = a \uparrow (a \uparrow\uparrow (b-1))$

于是基础步骤为，当 $(a \uparrow\uparrow (b-1)) < \lg m$ 时，或其他容易计算的情形

$$\text{如 } a \uparrow\uparrow 0 = 1, a \uparrow\uparrow 1 = a, (a \uparrow\uparrow 2) \bmod m = a^a \bmod m$$

则递归步骤可定义为 $(a \uparrow\uparrow b) \bmod m = a^k \bmod m$

$$\text{其中 } k = \min \{ p \mid p \equiv (a \uparrow\uparrow (b-1)) \pmod{\varphi(m)} \mid p > \lg m \}$$

注意在实际应用中这一步可以用 $k = \varphi(m) + (a \uparrow\uparrow (b-1)) \bmod \varphi(m)$ 代替

于是可以递归地定义运算 $T(a, b, n)$ ，其中 $a, n \in \mathbb{Z}^+$

$T(a, b, n) = \begin{cases} 0 & \text{if } b=0, n=1 \\ 1 & \text{if } b=0, n>1 \\ a \bmod n & \text{if } b=1, n>1 \\ a \uparrow\uparrow n & \text{if } b>1, n=1 \\ a^{\varphi(n)+T(a, b-1, \varphi(n))} \bmod n & \text{if } b>1, n>1 \end{cases}$

$$\text{modTetration } a \uparrow\uparrow 2 = a \bmod 2$$

$$\text{modTetration } a \uparrow\uparrow n = a \bmod n$$

$$\text{modTetration } a^{\varphi(n)} = \text{myPowerMod } a \text{ a } n$$

$$\text{modTetration } a^{\varphi(n)+T(a, b-1, \varphi(n))} = \text{let } n' = \text{eulerTotient } n \text{ in myPowerMod } a \text{ (n'+1) } \bmod \text{modTetration } a \text{ (b-1) } n'$$

注意欧拉函数为定义在 $\mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ 上的函数，且对于任意 $x \in \mathbb{Z}^+$ ，有 $0 < \varphi(x) \leq x$

注意到这个等号仅当 $x=1$ 时成立，即 $1 = \varphi(1)$

于是可知欧拉函数的迭代函数(Iterated function)， $\varphi_2^*(x)$ 是良定义的

即 $\varphi_2^* : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ 且有对于足够大的 n ， $\varphi_2^*(n)$ 远小于 n 。

即对于递归定义的函数 $T(a, b, n)$ ，总能在有限步内触及基础步骤。

也就是说，对于任意 a, n ， $\exists k \in \mathbb{N} \forall b \in \mathbb{Z} (b \geq k \rightarrow T(a, b, n) = T(a, k, n))$

取 $a=2$

如对于任意正整数 n ，数列 $2 \bmod n, 2^2 \bmod n, 2^3 \bmod n, \dots$ 最后是一个常数

即从有限个项以后，所有的项都相同

Discrete

Mathematics - P127

对于一个国家的所有城市，在任意两个城市之间有一条直达的单向道路

则存在一个城市，其他每个城市或者可以直达这个城市，或者经由一个其他城市到达这个城市

可以形式化地描述为：关系 R 是定义在城市集合 S 上的，且 $\forall a, b \in S (a \neq b \rightarrow aRb \oplus bRa)$

$\text{则 } \exists x \in S \forall y (x \neq y \rightarrow yRx \vee (\exists z \in S (z \neq x \wedge z \neq y \wedge zRy \wedge zRx)))$

基础步骤聚：当有两个城市，即 $n=2$ 时，有 $\begin{array}{c} v_1 \\ \text{---} \\ v_2 \end{array}$ ，且 v_2 即符合要求。

当有 3 个城市时， $n=3$ ，或者有 $\begin{array}{c} v_1 \\ \text{---} \\ v_2 \\ \text{---} \\ v_3 \end{array}$ ，或者有 $\begin{array}{c} v_1 \\ \text{---} \\ v_2 \\ \text{---} \\ v_3 \end{array}$ 均符合命题要求

形如 $\begin{array}{c} v_1 \\ \text{---} \\ v_2 \\ \text{---} \\ v_3 \end{array}$ 则取 v_3 ， $\begin{array}{c} v_1 \\ \text{---} \\ v_2 \\ \text{---} \\ v_3 \end{array}$ 则取任意一点

递归步骤聚：假设 $\forall n \geq 1 \forall n \geq 3 P(n)$ 为真，则考虑 $P(n+1)$ ，从 S_{n+1} 中任取一个城市 a 。

首先根据归纳假设构造任意 n 个城市的情形， (S_n, R) 其余部分构成 S_n
则可知 S_n 中存在 x 使命题成立。

于是可以对集合 S_n 进行划分，即 $S_n = \{x\} \cup Y_k \cup Z_{n-k-1}$

其中 $X = \{x\}$ 表示 S_n 中满足命题的城市

$Y_k = \{y_1, y_2, \dots, y_k\}$ 表示可以直达城市 x 的城市集合

即 $Y_k = \{y \in S_n \mid yRx\}$ ，且可知 $|Y_k| = k \in [1, n-1]$

$Z_{n-k-1} = \{z_1, z_2, \dots, z_{n-k-1}\}$ 表示经由其他一个城市到达 x 的城市集合

即 $Z_{n-k-1} = \{z \in S_n \mid \exists y \in Y_k zRy \wedge \neg zRx\}, |Z_{n-k-1}| \in [0, n-2]$

再考虑城市 a 与 $\{x\}, Y_k$ 的关系。即 xRz

当 aRx 时，即 a 可以直达 x ，

则有 x 是 S_{n+1} 之中使命题成立的城市

当 $\neg aRx \wedge \exists y \in Y_k aRy$ 时，即 a 不可以直达 x ，但是可以直达 Y_k 中的一个城市时

则有 x 是 S_{n+1} 之中使命题成立的城市

当 $\neg aRx \wedge \forall y \in Y_k \neg aRy$ 时，由于 $\forall y \in S_n aRy \oplus yRa$ 为真

则可知 $xRa \wedge \forall y \in Y_k yRa$ 为真，即 $\{x\}, Y_k$ 中的城市可直达 a

而对于 $\forall z \in Z_{n-k-1} \exists y \in Y_k zRy$ ，即 Z_{n-k-1} 中的城市均可经由 Y_k 的一个城市到达 a

则有 a 是 S_{n+1} 之中使命题成立的城市

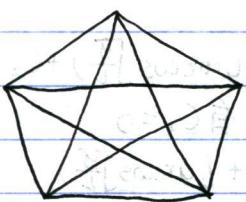
到达这个城市

于是根据类比归纳法，存在一个城市，其他每个城市或者可以直达这个城市，或者可以经由一个其他城市

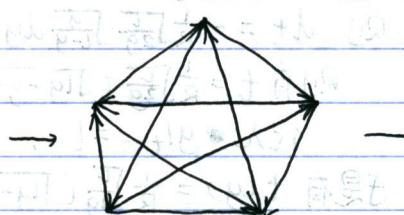
或者可以表述为对于一个完全简单图 K_n 的每条边任意指定方向成为有向图。

则存在一个点，使得其他点到这一点的最短通路长度均不超过 2

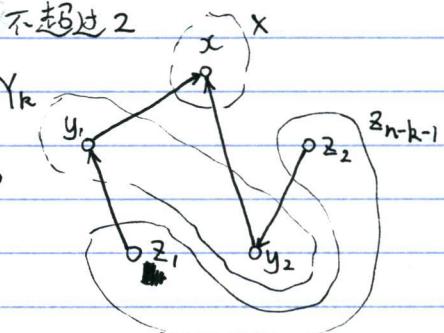
如：



K_5



有向 K_5



z_{n-k-1}

y_2

y_1

x

Discrete

Mathematics - P128

单位分数 (unit fraction), 又称埃及分数 (Egyptian fraction), 指形如 $\frac{1}{n}$ 的分数, 其中 $n \in \mathbb{Z}^+$

则对于任意有理数 $0 < p/q < 1$, 其中 p, q 为正整数, 可被表示为单位分数之和

即存在不相等的正整数 n_1, n_2, \dots, n_k , 使得 $p/q = 1/n_1 + 1/n_2 + \dots + 1/n_k$

贪婪算法为, 从和为0开始, 每一步选择一个最小的正整数 n_i

使得上一步的和加上 $\frac{1}{n_i}$ 不大于 p/q .

如果在某一步计算的和等于 p/q , 则算法终止,

则已选择的 $\{n_1, n_2, \dots, n_k\}$ 即为输出结果, 注意到此只有部分正确性

则证明算法终止, 取命题 $T(p)$ 为, 对于所有满足 $0 < p/q < 1$ 的有理数, 算法终止, 其中 $q \in \mathbb{Z}^+$

于是如果 $T(p)$ 对任意正整数 P 为真, 则可知算法对于任意 $0 < p/q < 1$ 输入终止

基础步骤: 当 $p=1$ 时, 可知 $q \in \mathbb{Z}^+$ 且 $q > 1$, 则取 $n=q$,

即有 $p/q = 1/n$, 算法终止, $T(1)$ 为真

递归步骤: 假设对于 $\forall p \in \mathbb{Z}^+ \wedge p > 1 \wedge T(1) \wedge T(2) \wedge \dots \wedge T(p-1)$ 为真, 则考虑 $T(p)$

对于 $0 < p/q < 1$, 有 $q \in \mathbb{Z}^+$ 且 $q > p$.

当 $p|q$ 时, 存在 $n \in \mathbb{Z}^+$, 使得 $q=np$,

即有 $p/q = 1/n$, 算法终止, 此时 $T(p)$ 为真

当 $\gcd(p, q) \neq 1$ 时, 取 $k = \gcd(p, q)$.

则有 $p/q = (p/k)/(q/k)$, 且 $1 \leq p/k < p$

于是根据归纳假设 $T(p/k)$ 为真, 又对于任意 $\frac{p/k}{q/k} = \frac{p}{kq}$

于是此时算法终止, 有 $T(p)$ 为真

当 $\gcd(p, q) = 1$ 时, 取 $n = \lceil q/p \rceil$

则 $p/q = p'/q' + 1/n$, 即 $p'/q' = (np-q)/nq$

于是令 $p' = np-q$, $q' = nq$.

又 $q > p$, 即 $n = \lceil q/p \rceil \geq 2$, 即 $q' = nq \in \mathbb{Z}^+$

又 $p > 1 \wedge \gcd(p, q) = 1$, 则有 $p \nmid q$, 即 $np-q > 0$ 且 $np-q \in \mathbb{Z}^+$

于是 $0 < np-q < p < nq$, 即根据归纳假设, $T(p')$ 为真

即 p/q 在经过一步选择 n 后, 从 p'/q' 开始算法终止, 则此时 $T(p)$ 为真

于是依据强归纳法, 有对于 $\forall p \in \mathbb{Z}^+ \wedge T(p)$ 为真, 即贪婪算法对于任意 $0 < p/q < 1$ 输入正确终止

Unit Fraction :: Int → Int → Int

unitFraction a₀ b₀ = let d = myGcd a₀ b₀ in

func a b acc

a == 1 = reverse (b : acc)

Unit Fraction 5 7

→ [2, 5, 70]

otherwise = let n = b `div` a + 1

in func (n*a - b) `div` (b*n) (n : acc)

in func (a₀ `div` d) (b₀ `div` d) []

Discrete

Mathematics - P129

对于随机分布在环形赛道上的一组汽车，假设没有足够的燃料使其中任意一辆恰好跑完一圈

则不论如何分配燃料，总是存在一辆汽车，

当它沿着赛道前进时可以通过从其他汽车获得加油来完成一圈

首先假设单位路程消耗的燃料为1，即跑过路程为 S 时，消耗 $g = 1 \cdot S$

然后可知，对于任意分布在赛道上的一组汽车 $C_1, C_2, \dots, C_n, n \in \mathbb{N}$ 。

每辆车到下一辆车的距离为 s_1, s_2, \dots, s_{n-1} ，且 s_n 为 C_n 到 C_1 的距离，赛道总长为 S

每辆车获得的燃料分配量为 g_1, g_2, \dots, g_n ，燃料总量 $G = S$

则必然存在至少一辆汽车，其获得的燃料足以跑到下一辆车的位置

假设不存在，则有每一辆汽车可前进距离 $g_i < s_i, i = 1, 2, \dots, n$

则 $\sum g_i < \sum s_i = S = G$ ，与前提矛盾， $S_k^1 = S_k + s_{k+1}$

即 $\exists i, i \leq n, g_i \geq s_i$

基础步骤：当 $n=1$ 时，一辆车获得所有燃料跑完一圈

于是命题平凡地为真， $P(1)$ 为真

当 $n=2$ 时，其中有一辆可以跑到另一辆车的位置，

则可获得所有燃料跑完一圈，即 $P(2)$ 为真

递归步骤：假设 $P(n)$ 为真，则考虑 $P(n+1)$

首先 $n+1$ 辆车中至少有一辆车 C_k ，其燃料 $g_k > s_k$ ，

则其必然可以到达车 C_{k+1} 的位置从而获得 g_{k+1} 。 $S_k^1 = S_k + s_{k+1}$

于是将 C_k 与 C_{k+1} 视为一辆汽车 C_k' ，其燃料为 $g_k + g_{k+1}$ ，到下一辆车距离为

s_{k+2} 。则 $C_1, C_2, \dots, C_k', C_{k+2}, \dots, C_{n-1}, C_n$ 这 n 辆车满足 $P(n)$ 的条件

根据归纳假设，其中存在一辆车使 $P(n)$ 为真

如果这辆车是 C_k' ，则意味着 C_k' 从 C_k 所在的位置开始

以 $g_k + g_{k+1}$ 的燃料起步，可以跑完一圈，即至少可以到达 C_{k+2} 的位置

则在 $P(n+1)$ 中， C_k 以 g_k 的燃料起步，必然可以经过 C_{k+1}

在获得 g_{k+1} 后可到达 C_{k+2} 的位置，其过程与 $P(n)$ 中的 C_k' 一致

于是可知 C_k 使 $P(n+1)$ 为真

如果不是 C_k' ，则假设为某一辆 C_i ，其中 $1 \leq i \leq n$ 且 $i \neq k, k+1$

则 C_i 从其本身位置开始必定可以到达 C_k' 的位置。

获得 g_{k+1} 并进而到达 C_{k+2} 。

在 $P(n+1)$ 中， C_i 可经过与 $P(n)$ 中相同过程到达 C_k ，又 $g_k \geq s_k$

于是 C_i 在获得 g_k 后必定可以到达 C_{k+1} ，进而获得 g_{k+1} 到达 C_{k+2}

于是可知 C_i 使 $P(n+1)$ 为真

于是根据数学归纳法，存在一辆车可以通过从其他汽车加油来跑完一圈

Discrete

Mathematics - P130

对于 n 条直线，任意两条有交点，任意三条没有公共点。

则这些直线将平面划分为 $n(n+1)/2 + 1$ 个区域

基础步骤：当 $n=1$ 时，直线将平面划分为 $2 = 1 \times (1+1)/2 + 1$ 个区域

递归步骤：假设对于任意 $n \in \mathbb{Z}^+$, $P_{(n)}$ 为真，则考虑 $P_{(n+1)}$

向 n 条直线中添加第 $n+1$ 条直线 l_{n+1} ，

则与 l_1, l_2, \dots, l_n 分别交于 P_1, P_2, \dots, P_n ，可知 P_1, \dots, P_n 不重合

于是 l_{n+1} 被 P_1, \dots, P_n 划分为 $n+1$ 段线段或射线 k_1, \dots, k_{n+1}

每一段都将 $P_{(n)}$ 中的唯一一个区域划分为两个新区域

根据归纳假设 $P_{(n)}$ 中有 $n(n+1)/2 + 1$ 个区域，

则 $P_{(n+1)}$ 中有 $n(n+1)/2 + 1 + (n+1) = (n+1)(n+2)/2 + 1$ 个区域

于是依据数学归纳法，可知 n 直线将平面划分为 $n(n+1)/2 + 1$ 个区域

对于 n 个平面，任意三个有公共点，任意四个没有公共点

则这些平面将空间划分成 $(n^3 + 5n + 6)/16$ 个区域

基础步骤：当 $n=1$ 时，一个平面将空间划分为 $2 = (1+5+6)/16$ 个区域

递归步骤：假设对于任意 $n \in \mathbb{Z}^+$, $P_{(n)}$ 为真，则考虑 $P_{(n+1)}$

向有 n 个平面存在的空间加入平面 P_{n+1} ，

则其与 P_1, P_2, \dots, P_n 分别交于直线 l_1, l_2, \dots, l_n

由于平面任意三个有公共点，任意四个没有公共点

则 l_1, l_2, \dots, l_n 将 P_{n+1} 划分成 $n(n+1)/2 + 1$ 个区域

又每个区域将 $P_{(n)}$ 中的一个空间区域划分为两个新区域

则 $P_{(n+1)}$ 中有 $\frac{n^3 + 5n + 6}{6} + \frac{n(n+1)}{2} + 1 = \frac{n^3 + 3n^2 + 8n + 12}{6} = \frac{(n+1)^3 + 5(n+1) + 6}{6}$ 个区域

于是根据数学归纳法，可知 n 个平面将三维空间划分为 $(n^3 + 5n + 6)/16$ 个区域

对于平面上的 n 个圆，任意两个有两个交点，任意三个没有公共点

则这些圆将平面划分为 $n^2 - n + 2$ 个区域

基础步骤：当 $n=1$ 时，一个圆将平面划分为 $2 = 1^2 - 1 + 2$ 个区域

递归步骤：假设对于任意 $n \in \mathbb{Z}^+$, $P_{(n)}$ 为真，则考虑 $P_{(n+1)}$

向有 n 个圆的平面加入圆 C_{n+1} 时，其与 C_1, C_2, \dots, C_n 有 $2n$ 个交点

又 $2n$ 个交点两个不重合，于是划分圆 C_{n+1} 为 $2n$ 段弧

又每段弧将 $P_{(n)}$ 中的唯一一个区域划分为两个新区域

则 $P_{(n+1)}$ 中有 $n^2 - n + 2 + 2n = (n+1)^2 - (n+1) + 2$ 个区域

于是依据数学归纳法，可知 n 个圆将平面划分为 $n^2 - n + 2$ 个区域