



# 第三章 鸽巢原理

3.1 鸽巢原理的简单形式

3.2 鸽巢原理的加强形式

3.3 Ramsey定理

# 组合数学

- 存在性问题

- 鸽巢原理

- 计数问题

- 排列组合

- 容斥原理

- 生成函数、递推关系

- Pólya计数

- 组合设计

- 组合优化



# 第三章 鸽巢原理

3.1 鸽巢原理的简单形式

3.2 鸽巢原理的加强形式

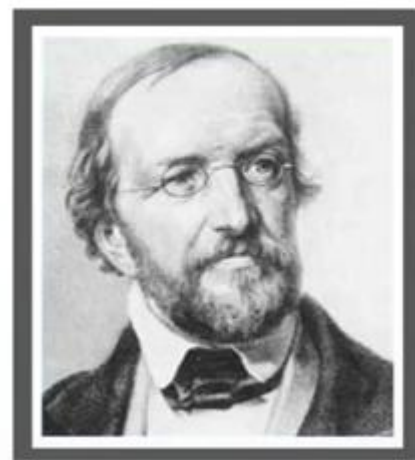
3.3 Ramsey定理

# 鸽巢原理

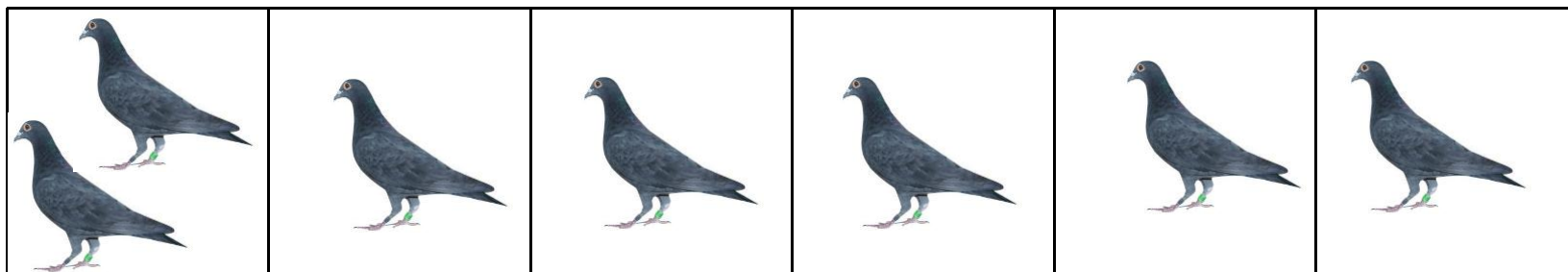
- 十九世纪德国数学家狄里克雷于1834年提出  
**鸽巢原理**，当时命名为**抽屉原理**

(Schubfachprinzip, drawer principle)

- **7个鸽子飞进6个巢里，一定有一个巢至少有2只鸽子**



Dirichlet,  
1805—1859



- 利用抽屉原理来建立有理数的理论，以后逐渐地应用到引数论、集合论、组合论等数学分支中，所以抽屉原理又称为**狄里克雷原理**

## ■ 两桃杀三士

□ 《晏子春秋·内篇谏下·第二十四》



齐景公



公孙接、田开疆、古冶子



晏子

## ■ 宋代费衎的《梁溪漫志》中，就曾运用抽屉原理来批驳“算命”一类迷信活动的谬论

“近世士大夫多喜谭命，往往自能推步。予尝见人言曰者阅人命，盖未始见年、月、日、时同者；纵有一二，必倡言于人以为异。尝略计之，若生时无同者，则一时生一人，一日生十二人，以岁记之，则有四千三百二十人；以一甲子计之，止（只）有二十五万九千二百人而已。今只从一大郡计，其户口之数尚不减数十万，况举天下之大，自五公大人以至小民何啻亿兆？虽明于数者有不能历算，则生时同者必不为少矣。其间五公大人始生之时则必有庶民同时而生者，又何贵贱贫富之不同也？”

- 把一个人出生的年、月、日、时（八字）作算命的根据，把“八字”作为“抽屉”，不同的抽屉只有 $12 \times 360 \times 60 = 259200$ 个。以天下之人为“物品”，其数“何啻亿兆”，进入同一抽屉的人必然千千万万，因而结论是“生时同者必不为少矣”。既然“八字”相同，“又何贵贱贫富之不同也？”

# 举例

- 13个同学，肯定至少有两个人出生在同一个月份。
- 假设有5对已婚夫妇，从中随机挑出6人，一定会挑出一对夫妇。
- 10位同学，每位同学至少认识其余9位同学中的一位，则至少有两位认识的人数相等。
- 在任意6个人中，或者有3个人两两互相认识，或者有3个人两两互相不认识（Ramsey定理）
- 月黑风高穿袜子：蓝色、黄色、红色袜子各3双，请问最少取多少只袜子，一定可以凑成一双？4只

# 知识点

数论问题

几何图形  
类问题

连续时间  
问题

棋盘着色

中国剩余  
定理

满足条件的  
最小物体  
数

**存在性  
问题**

完全图的一  
种着色

**Ramsey  
定理**

**鸽巢原理**

简单形式

加强形式

$n+1$  个

$n$  个

$n$  个

$m$  个

物体

鸽子

盒子

巢

$$K_p \rightarrow K_{n_1}, K_{n_2}, \dots, K_{n_l}$$

$$K_p \rightarrow K_m, K_n$$

**Ramsey数**



# 鸽巢原理

定理3.1.1 如果把 $n+1$ 个物体放进 $n$ 个盒子，那么至少有一个盒子包含两个或更多的物体。（反证法）

**注意：** 鸽巢原理只能用于证明某种现象的存在性。



## ■ 当 $X$ , $Y$ 为有限集时

- 如果 $X$ 的元素多于 $Y$ 的元素 ( $|X| > |Y|$ )，则 $f$ 不是单射
- 如果 $|X| = |Y|$ ，且 $f$ 是满射，则 $f$ 是单射  
(如果没有一个盒子为空，则每个盒子恰好有一个物体)

- 如果 $|X| = |Y|$ ，且 $f$ 是单射，则 $f$ 是满射

(如果没有盒子被放入多于一个物体，则每个盒子里有一个物体)

# 鸽巢原理→其他形式

定理3.1.1 如果把 $n+1$ 个物体放进 $n$ 个盒子，那么至少有一个盒子包含两个或更多的物体。（反证法）

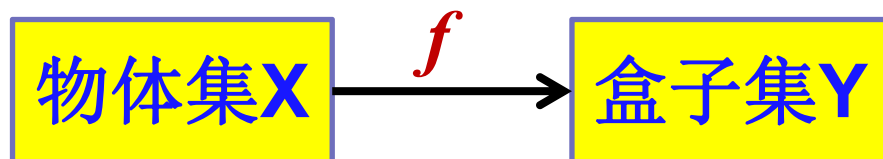
**注意：** 鸽巢原理只能用于证明某种现象的存在性。

## ■ 鸽巢原理的其他形式

- $n$  个物体放入  $n$  个盒子且没有一个盒子是空的, 那么, 每个盒子正好包含一个物体.
- $n$  个物体放入  $n$  个盒子且没有盒子被放入多于一个物体, 那么, 每个盒子有一个物体.

# 鸽巢原理→其他形式

定理3.1.1 如果把 $n+1$ 个物体放进 $n$ 个盒子，那么至少有一个盒子包含两个或者更多的物体。



- $n$ 个物体放入 $n$ 个盒子且没有一个空的, 那么, 每个盒子正好包含一个物体.
- $n$ 个物体放入 $n$ 个盒子且没有盒子被放入多于一个物体, 那么, 每个盒子有一个物体.

例：如果有 $n+1$ 个整数，而这些整数是小于或等于 $2n$ ，是否一定会有一对数是互素的？为什么？

（匈牙利大数学家厄杜斯(Paul Erdős, 1913 - 1996) 向当年年仅11岁的波萨 (Louis Pósa) 提出这个问题，而小波萨思考了不足半分钟便能给出正确的答案。）

$n$ 个盒子：  $\boxed{1, 2}$   $\boxed{3, 4}$   $\boxed{5, 6}$  ...  $\boxed{\begin{smallmatrix} 2n-1, \\ 2n \end{smallmatrix}}$

从 $n$ 个盒子中取出 $n+1$ 个数，一定会有一个盒子中的两个数同时被取出，即一对互素数。

例：证明，如果从 $\{1, 2, \dots, 2n\}$ 中选择 $n+1$ 个整数，那么存在两个整数，它们之间差为1。

例：如果从 $\{1, 2, \dots, 2n\}$ 中选择 $n+1$ 个不同的整数，证明一定存在两个整数，它们之间差为1。

$n$ 个盒子：  $\boxed{1, 2}$     $\boxed{3, 4}$     $\boxed{5, 6}$     $\dots$     $\boxed{\begin{smallmatrix} 2n-1, \\ 2n \end{smallmatrix}}$

证明：把集合  $\{1, 2, \dots, 2n\}$  划分成 $n$ 个子集

$$S_1, S_2, \dots, S_n,$$

其中，  $S_i = \{2i-1, 2i\}, i=1, 2, \dots, n$ 。

由鸽巢原理知，从 $\{1, 2, \dots, 2n\}$ 中取出 $n+1$ 个数，一定会有一个子集中的整数同时被取出，且这两个整数之间差为1。

例：如果有  $n+1$  个不同的正整数，且这些正整数是小于或等于  $2n$ ，是否一定会有一对数是互素的？为什么？

匈牙利大数学家厄杜斯 (Paul Erdős, 1913 - 1996) 向当年年仅11岁的路易·波萨 (Louis Pósa) 提出这个问题，而小波萨思考了不足半分钟便给出了正确的答案。

$n$  个盒子：  $\boxed{1, 2}$   $\boxed{3, 4}$   $\boxed{5, 6}$  ...  $\boxed{\begin{matrix} 2n-1, \\ 2n \end{matrix}}$

例：如果从 $\{1, 2, \dots, 2n\}$ 中选择  $n+1$  个不同的整数，证明一定存在两个整数，它们之间差为1。

证明：设选择的  $n+1$  个整数为  $a_1 < a_2 < \dots < a_{n+1}$ 。

令  $b_1 = a_1 + 1, b_2 = a_2 + 1, \dots, b_{n+1} = a_{n+1} + 1$ ，则

$$1 < b_1 < b_2 < \dots < b_{n+1} \leq 2n+1。$$

现有  $2n+2$  个数：

$$a_1, a_2, \dots, a_{n+1}, b_1, b_2, \dots, b_{n+1},$$

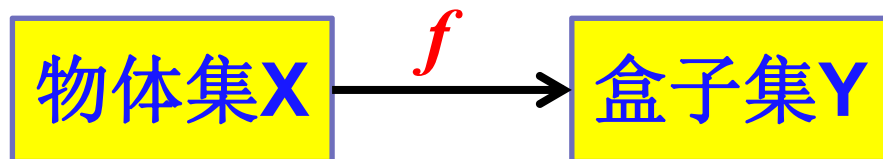
且每个数均属于  $\{1, 2, \dots, 2n+1\}$ 。

由鸽巢原理知，这  $2n+2$  个数中至少有一对数相等。

由于  $a_1, \dots, a_{n+1}$  互不相等，且  $b_1, \dots, b_{n+1}$  互不相等，

因此存在一对  $b_j = a_j + 1$  与  $a_k$  ( $j \neq k$ ) 相等，得  $a_k$  和  $a_j$  只相差1。

# 鸽巢原理的集合语言表述



令  $X$  和  $Y$  是两个有限集,  $f: X \rightarrow Y$  是一个由  $X$  到  $Y$  的函数。

- 如果  $X$  与  $Y$  含有相同个数的元素, 且  $f$  是映上(满射)的, 那么  $f$  是一对一的
- 如果  $X$  与  $Y$  含有相同个数的元素, 且  $f$  是一对一的, 那么  $f$  是映上的(满射)
- 如果  $X$  的元素多于  $Y$  的元素, 那么  $f$  就不是一对一的



# 鸽巢原理：数论中的应用

例. 证明：在 $m$ 个正整数  $a_1, a_2, \dots, a_m$  中, 存在  $0 \leq k < l \leq m$ , 使得  $a_{k+1} + a_{k+2} + \dots + a_l$  能够被  $m$  整除。

证：考虑 $m$ 个和：

$$s_1 = a_1, s_2 = a_1 + a_2, s_3 = a_1 + a_2 + a_3, \dots, s_m = a_1 + a_2 + \dots + a_m$$

- (1) 若以上和中有一个能被  $m$  整除，则结论成立；
- (2) 否则，设  $r_1, r_2, \dots, r_m$  是  $s_1, s_2, \dots, s_m$  除以  $m$  的非零余数，则  $1 \leq r_i \leq m-1, i=1, \dots, m$ 。

由鸽巢原理知，存在  $r_l = r_k, l > k$ ，则

$$a_{k+1} + a_{k+2} + \dots + a_l = s_l - s_k \text{ 能被 } m \text{ 整除。}$$

例. 从整数 $1, 2, \dots, 200$ 中选取**101**个不同的整数。证明所选的数中存在两个整数，使得**其中一个**是**另一个的因子**。

分析：

- 任何整数可分解为一些**素数的乘积**，如对任何整数 $n$ ,  $n = 2^k \times a$ ，其中， **$a$ 为奇数**， **$k \geq 0$** 。
- 整数 $1, 2, \dots, 200$ 只能有**100个不同奇数**，故可对101个数运用鸽巢原理。

例. 从整数 $1, 2, \dots, 200$ 中选取**101**个不同的整数。证明所选的数中存在两个整数，使得**其中一个是另一个的因子**。

证：对于1到200间的整数 $n$ ， $n$ 可写作以下形式：

$$n = 2^k \times a \quad (1)$$

其中  $a$  是  $1, 2, \dots, 200$  内的奇数。

由于要选取 101 个整数，而 200 内只有 100 个奇数，由鸽巢原理知**必存在两个整数  $n_1$  与  $n_2$  写作 (1) 式形式后，两个奇数相等**。

假设 $n_1=2^{k_1} \times b$ ,  $n_2=2^{k_2} \times b$ ，其中  $b$  是 $1, 2, \dots, 200$ 内的奇数，显然，当 $k_1 > k_2$ 时， $n_2$  整除 $n_1$ ；否则 $n_1$ 整除 $n_2$ 。

例：对于任意给定的52个非负整数，证明：其中必存在两个非负整数，要么两者的和能被100整除，要么两者的差能被100整除。

证：对于任意一个非负整数，其整除100的余数可能为 $\{0, 1, 2, \dots, 99\}$ 中之一。

对这100个余数进行分组，构造如下51个集合：

$\{0\}, \{1, 99\}, \{2, 98\}, \{3, 97\}, \dots, \{49, 51\}, \{50\}.$

两种情况：

- (1) 52个非负整数中存在两个数除以100的余数相同，显然它们的差能被100整除；
- (2) 若52个非负整数除以100的余数各不相同，则必存在两个数的余数恰好构成上述两元集合中一个；此时它们的和能被100整除。

## 思考题：

1. 证明：在 $n+2$ 个任选的正整数中，存在两个数，或者其差能被  $2n$  整除，或者其和能被  $2n$  整除。

2. 一间房屋内有10个人，他们当中没有人超过 60 岁（年龄只能以整数给出），但又至少不低于 1 岁。

证明：总能找出两组人（两组人中不含相同的人），使得年龄和相同。题中的10能换成更小的数吗？

3. 证明：对任意正整数 $n$ ，必存在由 0 和 3 组成的正整数能被  $n$  整除。

# 鸽巢原理：几何图形类应用

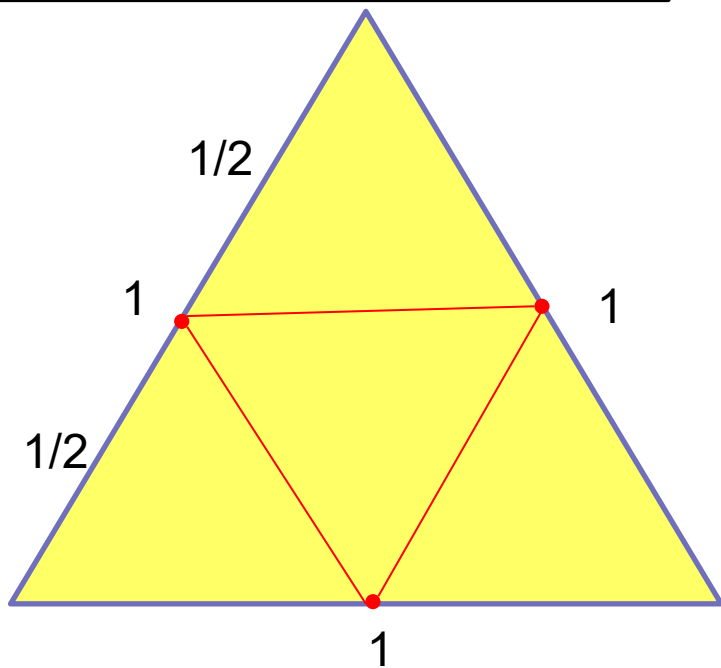
例5. 在边长为1的等边三角形内任意选择5个点。

证明：一定存在2个点，其距离至多为 $1/2$ 。

证明：如图所示，将等边三角形依每边中点分成四部分。

显然落在任意一个部分中的两点之间的距离至多为 $1/2$ 。

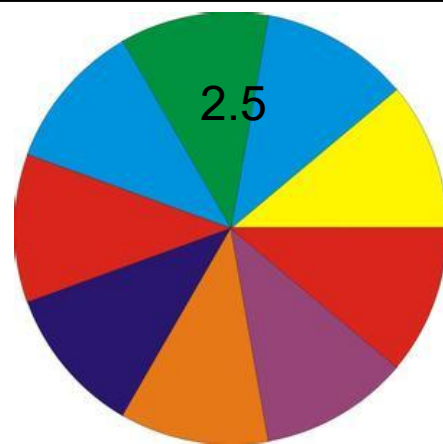
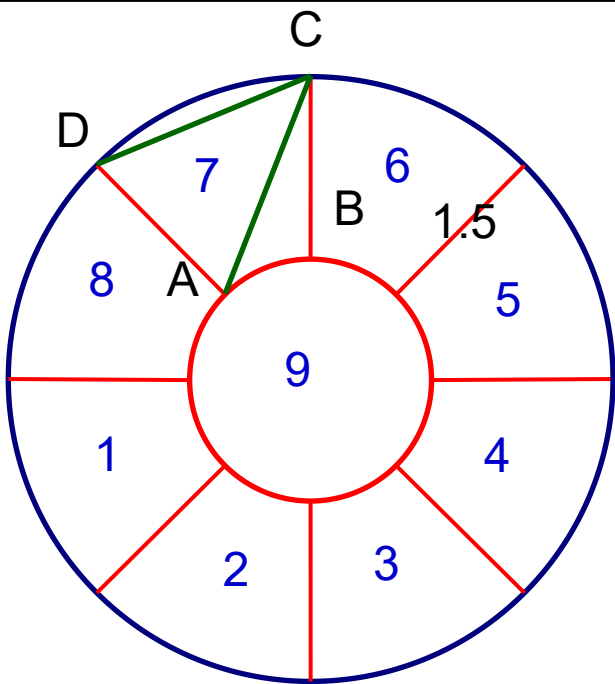
根据鸽巢原理，任意选择5个点，肯定有两个点落在同一个部分，因此这两点距离至多为 $1/2$ 。



思考：

1. 证明在边长为1的等边三角形中任意选择10个点，一定存在两个点，其距离至多为 $1/3$ 。
2. 确定一个整数 $n_k$ ，使得如果在边长为1的等边三角形中任意选择 $n_k$ 个点，一定存在2个点，其距离至多为 $1/k$ 。
3. 在直径为5的圆内任意给定10个点，证明存在两点，它们之间的距离小于2。

例：在直径为5的圆内任意给定10个点，  
证明存在两点，它们之间的距离小于2。



用一个与已知圆同心，半径为1的小圆，再把圆环部分等分成8个部分，构成9个抽屉。

$$|CD| = \sqrt{2 - \sqrt{2}}R = \sqrt{2 - \sqrt{2}} \cdot 5 < 1.92 < 2$$

$$|AC| = \sqrt{R^2 + r^2 - 2Rr \cos \frac{\pi}{4}}$$
$$= \sqrt{2.5^2 + 1^2 - 2 \times 2.5 \times 1 \times \frac{\sqrt{2}}{2}} < 1.93 < 2$$



证明：无论怎么样涂色，其中必有一个由单元格构成的矩形的4个角上的格子被涂上同一种颜色。

[illegible]

例：将一个矩形分成4行19列的网格，每个单元格涂1种颜色，有3种颜色可以选择，

证明：无论怎么样涂色，其中必有一个由单元格构成的矩形的4个角上的格子被涂上同一种颜色。

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

证：每一列有4行，但只有3个颜色，则由鸽巢原理知，必有两个单元格的顏色相同，其不同位置的组合有 $C(4, 2)=6$ 种，

例：将一个矩形分成**4行19列**的网格，每个单元格涂1种颜色，有**3种颜色**可以选择，

证明：无论怎么样涂色，其中**必有一个由单元格构成的矩形的4个角上的格子被涂上同一种颜色**。

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

证：每一列有4行，但只有3个颜色，则由鸽巢原理知，**必有两个单元格的**颜色相同，其不同位置的组合有 **$C(4, 2)=6$** 种，

例：将一个矩形分成4行19列的网格，每个单元格涂1种颜色，有3种颜色可以选择，

证明：无论怎么样涂色，其中必有一个由单元格构成的矩形的4个角上的格子被涂上同一种颜色。

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

证：每一列有4行，但只有3个颜色，则由鸽巢原理知，必有  
两个单元格的顏色相同，其不同位置的组合有 $C(4, 2)=6$ 种，

例：将一个矩形分成**4行19列**的网格，每个单元格涂1种颜色，有**3种颜色**可以选择，

证明：无论怎么样涂色，其中**必有一个由单元格构成的矩形的4个角上的格子被涂上同一种颜色**。

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
				黄	黄	黄				红	红	红				绿	绿	绿
		黄	黄			黄		红	红			红		绿	绿			绿
	黄		黄		黄		红		红		红		绿		绿		绿	
	黄	黄		黄			红	红		红			绿	绿		绿		

证：每一列有4行，但只有3个颜色，则由鸽巢原理知，**必有两个单元格的**颜色相同，其不同位置的组合有 **$C(4, 2)=6$** 种，

例：将一个矩形分成**4行19列**的网格，每个单元格涂1种颜色，有**3种颜色**可以选择，

证明：无论怎么样涂色，其中**必有一个由单元格构成的矩形的4个角上的格子被涂上同一种颜色**。

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
				黄	黄	黄				红	红	红				绿	绿	绿
		黄	黄			黄		红	红			红		绿	绿			绿
	黄		黄		黄		红		红		红		绿		绿		绿	
	黄	黄		黄			红	红		红			绿	绿		绿		

证：每一列有4行，但只有3个颜色，则由鸽巢原理知，**必有两个单元格的**颜色相同，其不同位置的组合有 **$C(4, 2)=6$** 种，则3种颜色下，一列中两个同色单元格的位置组合共有**18种**，而现在有**19列**。

因此，由鸽巢原理，**必有两列的两个同色单元格位置相等且颜色相同**。

例：将一个矩形分成4行19列的网格，每个单元格涂1种颜色，有3种颜色可以选择，

证明：无论怎么样涂色，其中必有一个由单元格构成的矩形的4个角上的格子被涂上同一种颜色。

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
红	白	白	白	黄	黄	黄	白	白	白	红	红	红	白	白	白	绿	绿	绿
白	白	黄	黄	白	白	黄	白	红	红	白	白	红	白	绿	绿	白	白	绿
白	黄	白	黄	白	黄	白	红	白	红	白	红	白	绿	白	绿	白	绿	白
红	黄	黄	白	黄	白	白	红	红	白	红	白	白	绿	绿	白	绿	白	白

证：每一列有4行，但只有3个颜色，则由鸽巢原理知，必有两个单元格的**颜色相同**，其不同位置的组合有 $C(4, 2)=6$ 种，则3种颜色下，一列中两个同色单元格的位置组合共有**18种**，而现在有**19列**。

因此，由鸽巢原理，必有两列的两个同色单元格位置相等且**颜色相同**。

显然，这两列构成的矩形的4个角上的格子的颜色相同。证毕。

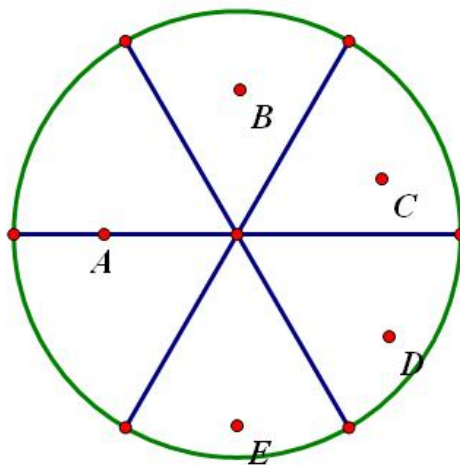
思考：随意地把一个3行9列棋盘的每个方格涂成红色或蓝色，求证：必有两列方格的涂色方式是一样的。

1	2	3	4	5	6	7	8	9



思考：

（英国数学奥林匹克1975年的问题）在一个半径为1单位的圆板上钉7个钉，使得两个钉的距离是大于或等于1，那么这7个钉一定会有一个位置恰好是在圆心上。



# 鸽巢原理：连续时间问题

例：某厂在五年期间的每一个月里至少试制一种新产品，  
每年最多试制19种新产品。

试证明：一定存在连续几个月，恰好试制24种新产品。

证：设五年间每个月新产品数分别为  $a_1, a_2, \dots, a_{59}, a_{60}$ 。

构造出数列  $a_n$  的前  $n$  项和的数列  $s_1, s_2, \dots, s_{59}, s_{60}$ ,

则有： $1 \leq a_1 = s_1 < s_2 < \dots < s_{59} < s_{60} \leq 19 \times 5 = 95$ ,

而序列  $s_1+24, s_2+24, \dots, s_{59}+24, s_{60}+24$  也是一个严格递增序列：

$$25 \leq s_1+24 < s_2+24 < \dots < s_{59}+24 < s_{60}+24 \leq 95+24 = 119。$$

于是，这120个数  $s_1, s_2, \dots, s_{59}, s_{60}$  和  $s_1+24, s_2+24, \dots, s_{59}+24, s_{60}+24$  都在区间  $[1, 119]$  内。

根据鸽巢原理，必定存在两个数相等。

# 鸽巢原理：连续时间问题

例：某厂在五年期间的每一个月里至少试制一种新产品，  
每年最多试制19种新产品。

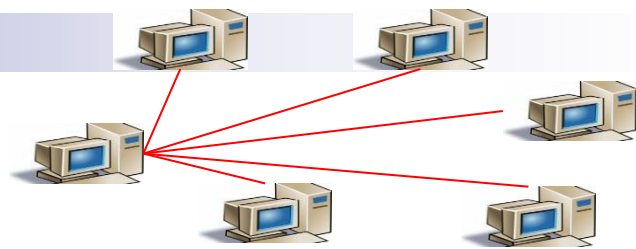
试证明：一定存在连续几个月，恰好试制24种新产品。

证：(续)：由于 $s_1, s_2, \dots, s_{59}, s_{60}$  与  $s_1+24, s_2+24, \dots, s_{59}+24, s_{60}+24$  均为严格单调的，因此必然存在一个  $i$  和  $j$ ，使得

$$s_i = s_j + 24。$$

因此该厂在从第  $j+1$  个月起到第  $i$  个月的这几个月时间里，  
恰好试制了24种新产品。

# 应用-计算机网络



**例.** 假设有一个由**6台**计算机组成的网络，证明在这样网络中**至少存在两台计算机直接连接数量相同的其他计算机。**

**证：** 每台计算机的直接连接数**大于等于0,小于等于5**，  
**且0和5不能同时出现。**

(1) 若一个计算机的直接连接数为**0**，此时其他计算机最大连接数为**4**

(2) 若一个计算机的直接连接数为**5**，则其他计算机的最小直接连接数为**1**

因此，计算机的直接连接数最多只能有**5**个数。由鸽巢原理，  
6台计算机中至少有两台的直接连接数相同。

# 中国剩余定理

- 韩信点兵传说：韩信带1500名兵士打仗，战死四五百人。命令士兵

- ✓ 3人一排，多出2名；
- ✓ 5人一排，多出3名；
- ✓ 7人一排，多出2名。

- ✓ 韩信马上说出人数：1073人。

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

- 《孙子算经》：“今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？”

- 宋朝数学家秦九韶于1247年《数书九章》卷一、二《大衍类》对“物不知数”问题做出完整系统的解答。

- 明朝数学家程大位编成了歌诀：  
三人同行七十稀，五树梅花廿一枝，  
七子团圆正半月，除百零五便得知。



例6 (中国剩余定理) 令  $m, n$  是互素的正整数,  $a$  和  $b$  分别是小于  $m$  和  $n$  的非负整数。那么, 存在正整数  $x$ , 使得  $x$  除以  $m$  余数为  $a$ , 且除以  $n$  余数为  $b$ , 即

$$x = pm + a, \quad x = qn + b。$$

分析:

1) 首先构造足够多 “除以  $m$  余数为  $a$ ” 的整数

2) 证明在这些数中存在 “除以  $n$  余数为  $b$ ” 的整数。

需要多少这样的数?

**例6 (中国剩余定理)** 令 $m, n$ 是互素的正整数,  $a$ 和 $b$ 分别是小于 $m$ 和 $n$ 的非负整数。那么, 存在正整数 $x$ , 使得 $x$ 除以 $m$ 余数为 $a$ , 且除以 $n$ 余数为 $b$ , 即  $x=pm+a$ ,  $x=qn+b$ 。

证: 考虑  $n$  个除以 $m$ 余数为 $a$  的整数:

$$a, m+a, \dots, (n-1)m+a$$

假设存在两个数  $im+a$  和  $jm+a$  ( $0 \leq i < j \leq n-1$ ) 除以 $n$ 的余数都为 $r$ , 即存在非负整数  $k$  和  $l$  使得

$$im+a = kn + r, \quad jm+a = ln + r$$

上两式相减得  $(j-i)m=(l-k)n$ 。由于 $m, n$ 互素, 因此  $n$  是  $j-i$  的因子。

又由于  $0 \leq j-i \leq n-1$ , 矛盾。

故上述  $n$  个整数除以  $n$  的余数各不相同。

由鸽巢原理,  $n$  个数  $0, 1, 2, \dots, n-1$  中都出现在这些余数集之中, 因此  $b$  也出现。

设对应除以  $n$  余数为  $b$  的数为  $x = pm + a$  ( $0 \leq p \leq n-1$ ), 同时  $x = qn + b$  ( $0 \leq q \leq n-1$ ), 结论成立。

# 中国剩余定理一般形式

- 设 $m_1, m_2, \dots, m_k$ 是 $k$ 个两两互素的正整数,  $0 \leq a_i < m_i$  ( $i=1, \dots, k$ ), 则存在 $x$ , 使得 $x$ 除以 $m_i$ 的余数为 $a_i$ , 即 $x \equiv a_i \pmod{m_i}$  ( $i=1, \dots, k$ )。

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$



# 解决实际问题中的意义

## ■ 密码问题

- 可以选取5个两两互素的整数 $m_i (i=1,2,\dots,5)$ ，每个股东秘密保存 $b_i$ ，那么存在唯一的 $x$ 使得 $x$ 除以 $m_i$ 的余数为 $b_i$ ，用 $x$ 作为密钥加密机密文件。
- **注意：** 鸽巢原理仅提供了存在性证明，还需要设计求 $x$ 的有效算法，这需要我们学习更多数学才能解决。

# 知识点

数论问题

几何图形  
类问题

连续时间  
问题

棋盘着色

中国剩余  
定理

满足条件的  
最小物体  
数

**存在性  
问题**

完全图的一  
种着色

**Ramsey  
定理**

**鸽巢原理**

简单形式

加强形式

$n+1$  个

$n$  个

$n$  个

$m$  个

物体

鸽子

盒子

巢

$$K_p \rightarrow K_{n_1}, K_{n_2}, \dots, K_{n_l}$$

$$K_p \rightarrow K_m, K_n$$

**Ramsey数**

# 非对称密码体制

- 非对称密码体制提供的安全性取决于难以解决的数学问题，例如，将大整数因式分解成质数。
- 公钥系统使用这样两个密钥，一个是公钥，用来加密文本，另一个是安全持有的私钥，只能用此私钥来解密。也可以使用私钥加密某些信息，然后用公钥来解密，而公钥是大家都可以知道的，这样拿此公钥能够解密的人就知道此消息是来自持有私钥的人，从而达到了认证作用。

# Diffie-Hellman 算法描述 (1976)

1. Alice 与 Bob 确定两个大素数  $n$  和  $g$ , 这两个整数不保密, Alice 与 Bob 可以使用不安全信道确定这两个数.
2. Alice 选择另一个大随机数  $x$ , 并计算  $A$  如下:
  1.  $A = g^x \bmod n$
3. Alice 将  $A$  发给 Bob
4. Bob 选择另一个大随机数  $y$ , 并计算  $B$  如下:
  1.  $B = g^y \bmod n$
5. Bob 将  $B$  发给 Alice
6. 计算秘密密钥  $K_1$  如下:
  1.  $K_1 = B^x \bmod n$
7. 计算秘密密钥  $K_2$  如下:
  1.  $K_2 = A^y \bmod n$
8.  $K_1 = K_2$

# RSA 算法 (1977)

- 1977 年，即，Diffie-Hellman 的论文发表一年后，MIT 的三名研究人员根据这一想法开发了一种实用方法。这就是 RSA，它是以三位开发人员 — Ron Rivest、Adi Shamir 和 Leonard Adelman — 姓的首字母大写命名的，而且 RSA 可能是使用最广泛的公钥密码体制。
- 是一种块加密算法。
- 应用最广泛的公钥密码算法
- 只在美国申请专利，且已于2000年9月到期

# 小结

- 鸽巢原理用于证明某种结构的存在性。
- 运用鸽巢原理通常需要将问题转化。

# 作业

- 3.4练习题

- 5, 8, 10

1. 证明：在 $n+2$ 个任选的正整数中，存在两个数，或者其差能被 $2n$ 整除，或者其和能被 $2n$ 整除。

证明：已知所有正整数除以 $2n$ 的余数的取值只能为 $0, 1, 2, \dots, 2n-1$ 。

把以上余数构造以下 $n+1$ 个子集：

$\{1, 2n-1\}, \{2, 2n-2\}, \dots, \{n-1, n+1\}, \{n, n\}, \{0, 0\}$ 。

任选 $n+2$ 个正整数，由鸽巢原理知，一定存两个数，其除以 $2n$ 的余数来自同一个子集，设为 $A$ 。

(1)若 $A$ 是前 $n-2$ 个子集中一个，则这两个数的和能被 $2n$ 整除；

(2)若 $A$ 是最后2个子集中一个，则这两个数的差能被 $2n$ 整除。



9. 一间房屋内有10个人，他们当中没有人超过60岁（年龄只能以整数给出），但又至少不低于1岁。

证明：总能找出两组人（两组人中不含相同的人），使得年龄和相同。题中的10能换成更小的数吗？

证明：(1) 10个人构成的子集一共是 $2^{10}=1024$ 个，去除掉空集与全集，一共1022个子集可以是找出的两组人中的一组。

由于这些子集的年龄和最小为1岁，且不超过  $60 \times 9 = 540$  岁。因此，由鸽巢原理知，至少有两组人的年龄和相同，去除这两组人的相同人后，所得的两组人满足题目要求。

9. 一间房屋内有10个人，他们当中没有人超过60岁（年龄只能以整数给出），但又至少不低于1岁。

证明：总能找出两组人（两组人中不含相同的人），使得年龄和相同。题中的10能换成更小的数吗？

证明：(2) 当考虑9个人时，9个人构成的子集一共是 $2^9=512$ 个，去除掉空集与全集，一共510个子集可以是找出的两组人中的一组。

又这些子集的年龄和最小为1，最大为 $60*8=480$ 。

因此，由鸽巢原理知，至少有两组人的年龄和相同，去除这两组人的相同人后，所得的两组人满足题目要求。

例. 证明: 对任意正整数  $n$ , 必存在由0和3组成的正整数能被  $n$  整除。

证明: 设有  $n+1$  个数  $a_1, a_2, \dots, a_{n+1}$ , 其中  $a_i = 33\dots3$ , 由  $i$  个 3 构成 ( $i=1, \dots, n+1$ )。

由于任何正整数除以  $n$  的余数有  $0, 1, \dots, n-1$ , 共  $n$  种情况。由鸽巢原理知, 一定存在两个数除以  $n$  后的余数相同。

假设这两个数为  $a_i, a_j$ , 且  $a_i > a_j$ , 则

$$a_i - a_j = 3\dots30\dots0 \quad (j \text{ 个 } 0, i-j \text{ 个 } 3)$$

能被  $n$  整除, 且是由0和3组成的正整数。



# 第三章 鸽巢原理

3.1 鸽巢原理的简单形式

3.2 鸽巢原理的加强形式

3.3 Ramsey定理

# 知识点

数论问题

几何图形  
类问题

连续时间  
问题

棋盘着色

中国剩余  
定理

满足条件的  
最小物体  
数

**存在性  
问题**

完全图的一  
种着色

**Ramsey  
定理**

**鸽巢原理**

**简单形式**

**加强形式**

$$K_p \rightarrow K_{n_1}, K_{n_2}, \dots, K_{n_l}$$

$$K_p \rightarrow K_m, K_n$$

**Ramsey数**

$n+1$  个

$n$  个

$n$  个

$m$  个

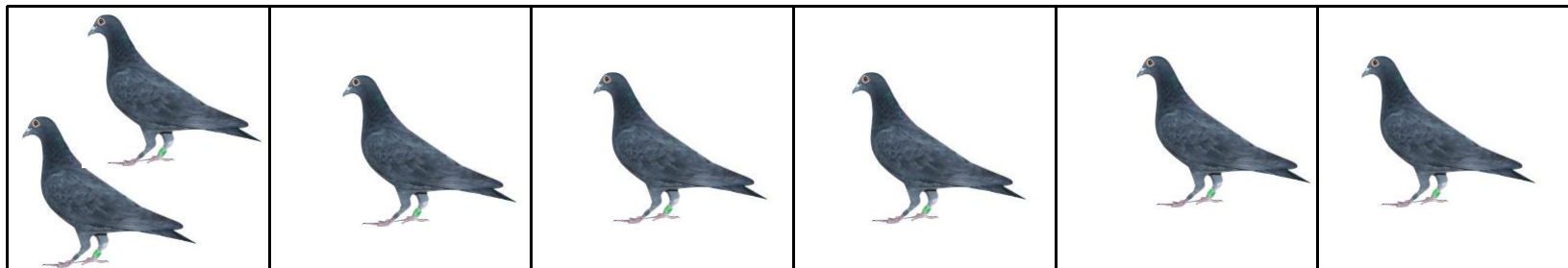
物体

鸽子

盒子

巢

# 回顾：鸽巢原理的简单形式



**定理3.1.1** 如果把  $n+1$  个物体放进  $n$  个盒子，那么至少有一个盒子包含两个或者更多的物体。

# 鸽巢原理：加强形式(1)——实例

定理3.2.1 令 $q_1, q_2, \dots, q_n$ 为正整数。若将

$$q_1 + q_2 + \dots + q_n - n + 1$$

个物体被放进 $n$ 个盒子内，那么，

- 或者第1个盒子至少含有 $q_1$ 个物体，
- 或者第2个盒子至少含有 $q_2$ 个物体，...
- 或者第 $n$ 个盒子至少含有 $q_n$ 个物体。

例： 5个盒子， $3+4+1+7+2-5+1=13$ 个物品，

则不会出现：第1个盒子少于3个物品

第2个盒子少于4个物品

第3个盒子少于1个物品

第4个盒子少于7个物品

第5个盒子少于2个物品

?

## 鸽巢原理：加强形式(2)——特例

定理3.2.1 令 $q_1, q_2, \dots, q_n$ 为正整数。如果将

$$q_1 + q_2 + \dots + q_n - n + 1$$

个物体被放进 $n$ 个盒子内，那么，

- 或者第1个盒子至少含有 $q_1$ 个物体，
- 或者第2个盒子至少含有 $q_2$ 个物体，...
- 或者第 $n$ 个盒子至少含有 $q_n$ 个物体。

简单形式：

当 $q_1 = q_2 = \dots = q_n = 2$ ，有

$$q_1 + q_2 + \dots + q_n - n + 1 = n + 1.$$



## 鸽巢原理：加强形式(3)——证明

定理3.2.1 令 $q_1, q_2, \dots, q_n$ 为正整数。如果将

$$q_1 + q_2 + \dots + q_n - n + 1$$

个物体被放进 $n$ 个盒子内，那么，

- 或者第1个盒子至少含有 $q_1$ 个物体，
- 或者第2个盒子至少含有 $q_2$ 个物体，...
- 或者第 $n$ 个盒子至少含有 $q_n$ 个物体。

证：(反证法) 假设对任意  $i=1, \dots, n$ ，第  $i$  个盒子中物体都少于  $q_i$ ，那么物体总数少于或等于

$$(q_1 - 1) + (q_2 - 1) + \dots + (q_n - 1) = q_1 + q_2 + \dots + q_n - n,$$

矛盾。因此，至少存在一个  $i=1, \dots, n$ ，使得第  $i$  个盒里至少有  $q_i$  个物体。

## 鸽巢原理：加强形式(4)–推论

定理3.2.1 令  $q_1, q_2, \dots, q_n$  为正整数。如果将

$$q_1 + q_2 + \dots + q_n - n + 1$$

个物体被放进  $n$  个盒子内，那么，

- 或者第1个盒子至少含有  $q_1$  个物体，
- 或者第2个盒子至少含有  $q_2$  个物体，...
- 或者第  $n$  个盒子至少含有  $q_n$  个物体。

特殊形式：  $q_1 = q_2 = \dots = q_n = r$  时，

$$q_1 + q_2 + \dots + q_n - n + 1 = n(r-1) + 1$$

推论3.2.2 设  $n$  和  $r$  都是正整数。如果  $n(r-1)+1$  个物体放入  $n$  个盒子，则至少有一个盒子含有至少  $r$  个物体。

## 鸽巢原理：加强形式(5)-推论

推论3.2.2 设  $n$  和  $r$  都是正整数。如果  $n(r-1)+1$  个物体放入  $n$  个盒子，则至少有一个盒子含有至少  $r$  个物体。

假设第  $i$  个盒子里放入的物品数为  $m_i$ ，即

$$m_1 + m_2 + \dots + m_n = n(r-1) + 1,$$

有  $(m_1 + m_2 + \dots + m_n)/n = (n(r-1) + 1)/n = r-1 + 1/n > r-1$ ,

因此，至少有一个  $m_i \geq r$ 。

平均原理：如果  $n$  个非负整数  $m_1, m_2, \dots, m_n$  的平均数大于  $r-1$ ，即  $(m_1 + m_2 + \dots + m_n)/n > r-1$ ，则至少有一个整数大于或等于  $r$ 。

设  $m$  和  $n$  都是正整数。如果  $m$  个物体放入  $n$  个盒子，则至少有一个盒子含有  $\lceil m/n \rceil$  个或更多的物体。

# 课堂练习

例: (1) 在100个人当中至少有多少人生在同一个月?

(2) 从一幅标准的52张牌中随意选出26张牌, 则至少有几张牌是同一个花色?

(3) 从一幅标准的52张牌中要随意选出 7 张是同样的花色, 必须至少选出多少张牌?

解: (1) 至少有  $\lceil 100/12 \rceil = 9$  个人生在同一个月。

(2) 至少有  $\lceil 26/4 \rceil = 7$  张牌是同一个花色。

(3) 由鸽巢原理, 任意选出25 张牌, 必存在  $\lceil 25/4 \rceil = 7$  张牌是一个花色。

当选出24张牌时, 有可能出现每个花色都是6张牌。

因此, 必须至少选出 25张牌。

例. 一篮水果装有苹果、梨和桔子。为了保证或者至少8个苹果，或者至少6个梨 或者 至少9个桔子，则放入篮子中的水果的最少件数是多少？

解：由鸽巢原理的加强形式，放入篮子中的水果为 $8 + 6 + 9 - 3 + 1 = 21$  件时，无论如何选择，都将满足题目要求。

但当放入篮子中的水果数为20时，可能出现7个苹果，5个香蕉和8个桔子的情形，不满足题目要求。

因此放入篮子中的水果的最少件数是 21。

(用于判断满足条件的最小物品总数)

例. 证明：从任意给出的5个正整数中必能选出3个数，它们的和能被3整除。

分析：任意正整数除以3的余数只能为0，1或2。

设A为任意给出的5个正整数的集合。

A中三个数能被3整除，只有四种情况：

- (1) 三个数的余数分别为：0，1，2
- (2) 三个数的余数全为0
- (3) 三个数的余数全为1
- (4) 三个数的余数全为2

例. 证明：从任意给出的5个正整数中必能选出3个数，它们的和能被3整除。

证明：任意正整数除以3的余数只能为0，1或2。

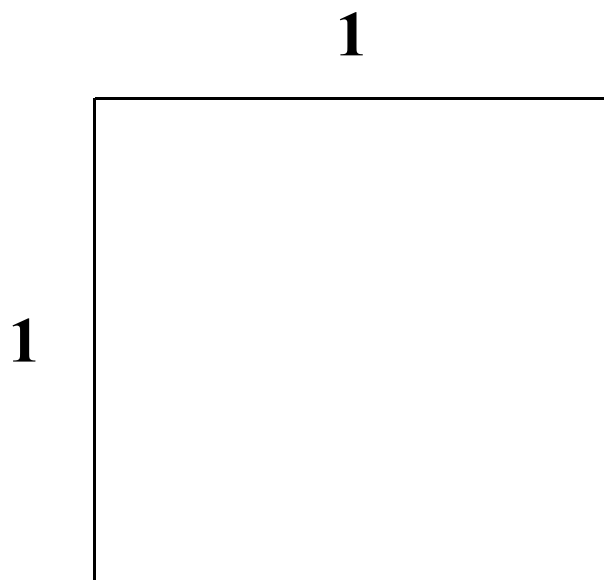
设A为任意给出的5个正整数的集合。

设 $t_0$ ， $t_1$ ， $t_2$ 为A中除以3余数分别为0，1，2的数的个数。

- (1) 若 $t_0$ ， $t_1$ ， $t_2$ 均不为0，则一定有三个数除以3的余数分别为0，1，2，则这三个数的和能被3整除。
- (2) 若 $t_0$ ， $t_1$ ， $t_2$ 中至少有一个为0，不妨设 $t_0=0$ ，则 $t_1+t_2=5$ 。

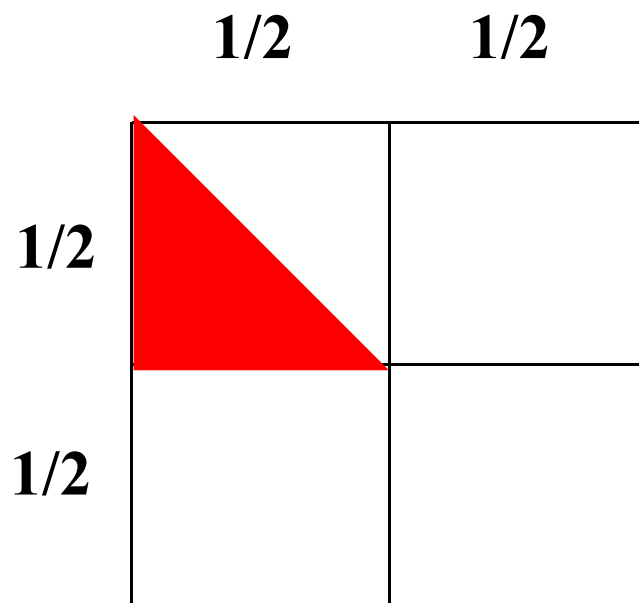
由平均原理知，至少有 $\lceil 5/2 \rceil = 3$ 个数除以3的余数相同（全为1或全为2），则这三个数的和能被3整除。

例. 在一个边长为1的正方形内任取 9 个点，证明以这些点为顶点的各个三角形中，至少有一个三角形的面积不大于  $1/8$ 。





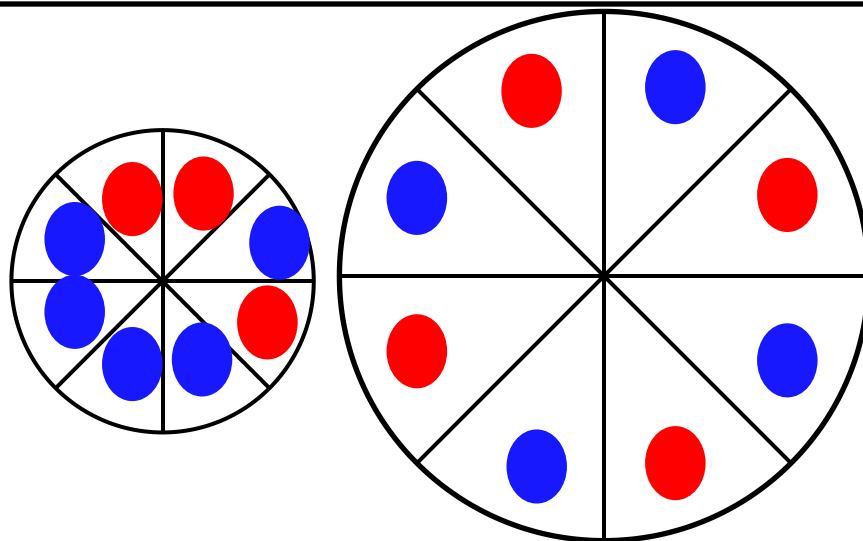
例. 在一个边长为1的正方形内任取 9 个点，证明以这些点为顶点的各个三角形中，至少有一个三角形的面积不大于  $1/8$ 。

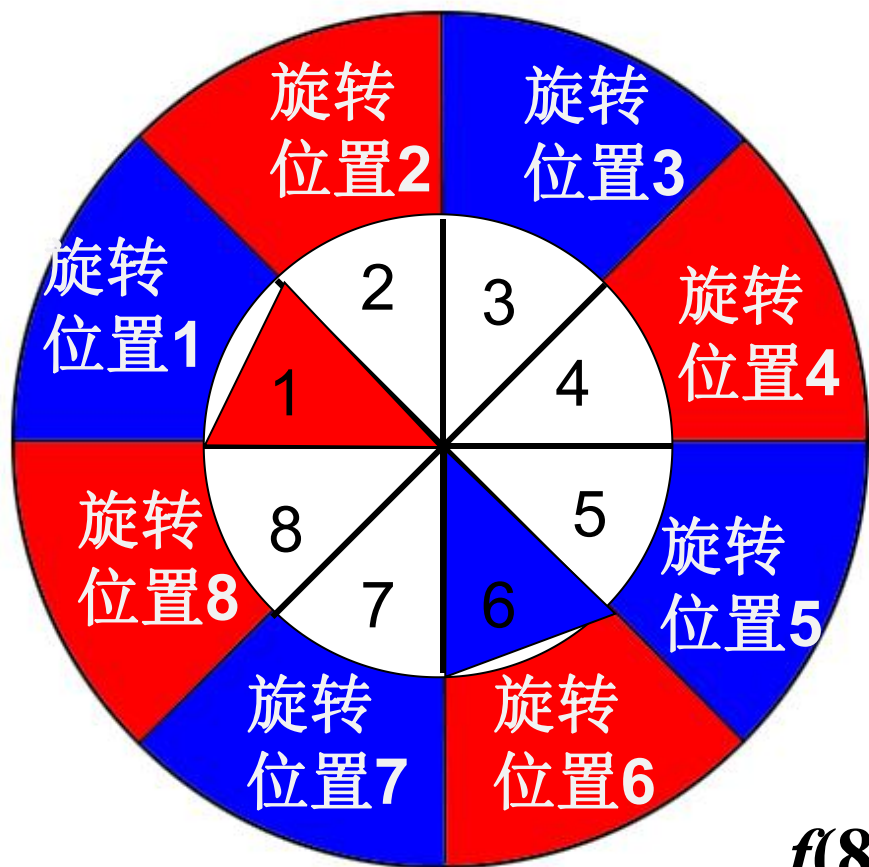


例：两个大小不一的碟子，均被分成200个相等扇形。

- ✓ 在大碟子中任选100个扇形涂成红色，其余的涂成蓝色。
- ✓ 小碟子中，每一个扇形随机地涂成红色或者蓝色，数目无限制。
- ✓ 将小碟子与大碟子中心重合。

试证能够通过适合旋转，存在两个碟子相同颜色重合的扇形数至少是100个的情形。





分析：大碟子不动，转动小碟子，转完一圈，回到原位，每个扇形与所有旋转位置颜色重合次数均为4。

$$f(8,1)=1, f(1,1)=0$$

定义函数：

$$f(i,j) = \begin{cases} 0, & \text{在旋转位置 } i, j \text{ 扇区与大碟颜色不同} \\ 1, & \text{在旋转位置 } i, j \text{ 扇区与大碟颜色相同} \end{cases}$$

## 小碟子扇形区编号

旋转  
位置

1

2

3

...

200

$S_1$

$f(1,1)$

$f(1,2)$

$f(1,3)$

...

$f(1,200)$

$S_2$

$f(2,1)$

$f(2,2)$

$f(2,3)$

...

$f(2,200)$

$S_3$

$f(3,1)$

$f(3,2)$

$f(3,3)$

...

$f(3,200)$

...

...

...

...

...

...

$S_{200}$

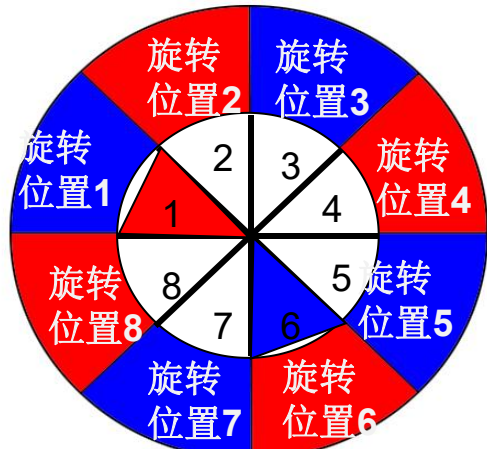
$f(200,1)$

$f(200,2)$

$f(200,3)$

...

$f(200,200)$



当配色确定时，通过旋转小碟，共有 **200** 种可能的对应方式，因此平均颜色重合数为  $20000/200=100$ 。

由鸽巢原理的加强形式知，肯定存在一种方式，其颜色重合数至少为100。

对任意的  $k$ ,  $\sum_{i=1}^{100} f(i, k) = 100$ , (每列)  
即转动一圈，第  $k$  个扇区与所有位置上的颜色重合数为100。

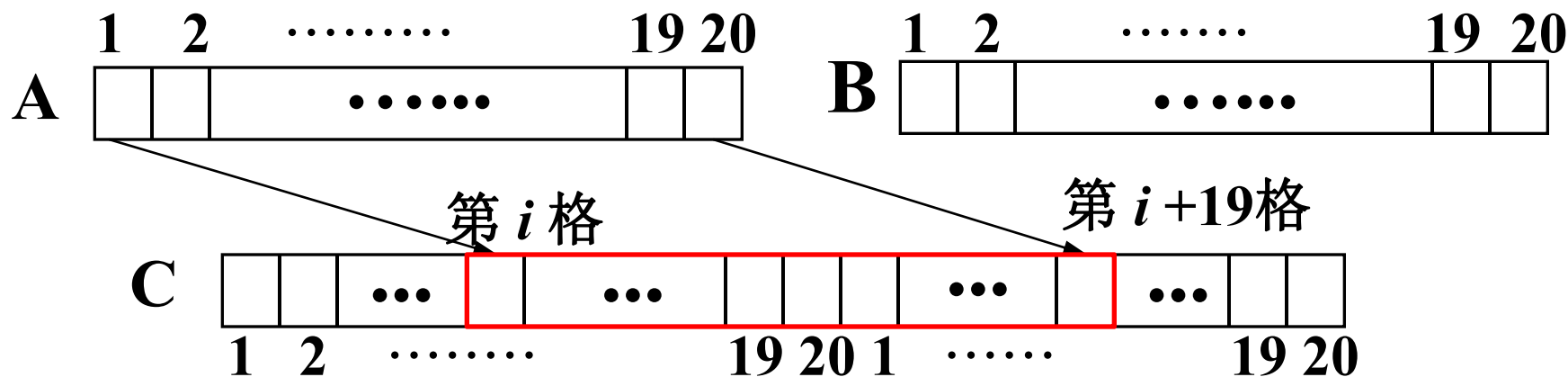
因此，所有扇区在所有位置上，颜色重合的总数为：

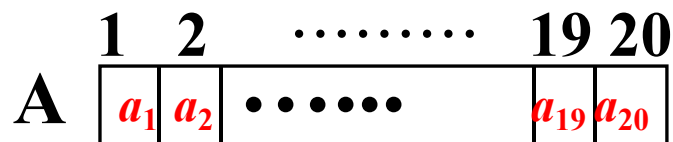
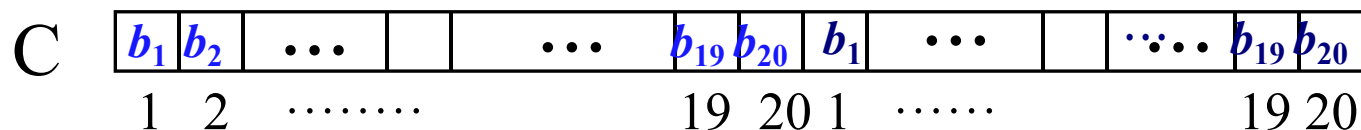
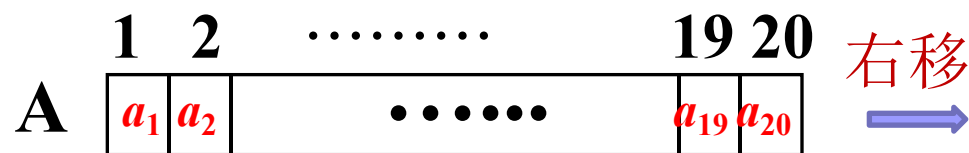
$$\sum_{i,j=1}^{200} f(i, k) = 200 \times 100 = 20000$$

思考：设  $A = a_1 a_2 \cdots a_{20}$  是 10 个 0 和 10 个 1 组成的 20 位 2 进制数。 $B = b_1 b_2 \cdots b_{20}$  是任意的 20 位 2 进制数。

令  $C = b_1 b_2 \cdots b_{20} b_1 b_2 \cdots b_{20} = c_1 c_2 \cdots c_{40}$ 。

则存在某个  $i$ ,  $1 \leq i \leq 21$ , 使得  $c_i c_{i+1} \cdots c_{i+19}$  与  $a_1 a_2 \cdots a_{20}$  至少有 10 位对应数字相同。





1、假想着 A 如图所示从左向右一格一格移动。

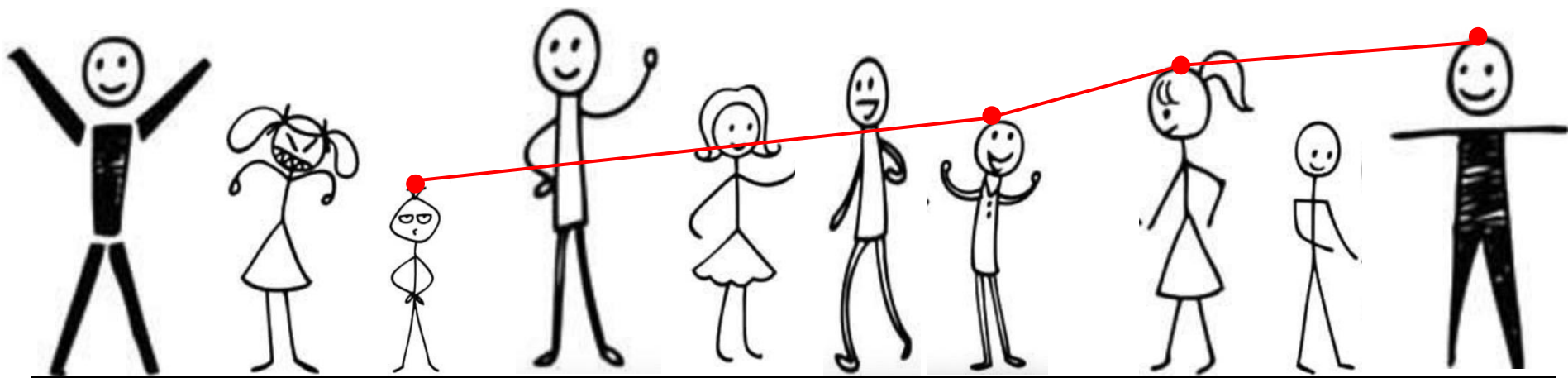
2、在移动到最后一格时，C中每对 $b_j$ 一共遍历所有 $a_1, a_2, \dots, a_{20}$ 。  
因为A中有10个0和10个1，每一对 $b_j$ 都有10位次对应相等。

3、在20次的移动过程中共有 $10 \times 20 = 200$ 位次对应相等。

4、因此必有一次移动，满足相同数字的格数至少为  
 $200/20=10$ 位

例：设 $n^2+1$ 个人并肩排成一条直线，是否一定能选出 $n+1$ 个人向前迈出一大步，使得从左至右他们的身高是递增的或递减的。

$n=3$



例：证明每个由  $n^2+1$  个实数构成的序列  $a_1, a_2, \dots, a_{n^2+1}$  或者含有长度为  $n+1$  的递增序列，或者含有长度为  $n+1$  的递减子序列。

□ 子序列：

设  $b_1, b_2, \dots, b_n$  是一个序列，则  $b_{i_1}, b_{i_2}, \dots, b_{i_k}$  是一个子序列，其中  $1 \leq i_1 < i_2 < \dots < i_k \leq n$ 。

- 递增子序列：若子序列  $b_{i_1}, b_{i_2}, \dots, b_{i_k}$  满足  
(非递减)  $b_{i_1} \leq b_{i_2} \leq \dots \leq b_{i_k}$
- 递减子序列：若子序列  $b_{i_1}, b_{i_2}, \dots, b_{i_k}$  满足  
(非递增)  $b_{i_1} \geq b_{i_2} \geq \dots \geq b_{i_k}$



例：证明每个由  $n^2+1$  个实数构成的序列  $a_1, a_2, \dots, a_{n^2+1}$  或者含有长度为  $n+1$  的递增序列，或者含有长度为  $n+1$  的递减子序列。

证：假设不存在长度为  $n+1$  的递增子序列，只需构造一个长度为  $n+1$  的递减子序列。

设  $l_k$  是以  $a_k$  为起始的最长递增子序列长度， $k=1, 2, \dots, n^2+1$ ，则对  $\forall k$  有  $1 \leq l_k \leq n$ 。

对序列  $l_1, l_2, \dots, l_{n^2+1}$ ，运用鸽巢原理加强形式，一定存在  $\lceil (n^2+1)/n \rceil = n+1$  个  $l_i$  相等。

设  $l_{k_1} = l_{k_2} = \dots = l_{k_{n+1}}$ ，其中  $1 \leq k_1 < k_2 < \dots < k_{n+1} \leq n^2+1$ 。

下面证明  $a_{k_1}, a_{k_2}, \dots, a_{k_{n+1}}$  是长度为  $n+1$  的递减序列。

例：证明每个由  $n^2+1$  个实数构成的序列  $a_1, a_2, \dots, a_{n^2+1}$  或者含有长度为  $n+1$  的递增序列，或者含有长度为  $n+1$  的递减子序列。

证(续)：

下面证明  $a_{k_1}, a_{k_2}, \dots, a_{k_{n+1}}$  是长度为  $n+1$  的递减序列。

(反证法) 假设存在  $k_i, k_{i+1}$ , 使得  $a_{k_i} < a_{k_{i+1}}$ ,

把  $a_{k_i}$  加到以  $a_{k_{i+1}}$  开始的最长递增子序列，则构成了以  $a_{k_i}$  开始的递增子序列，得  $l_{k_i} > l_{k_{i+1}}$ , 与  $l_{k_i} = l_{k_{i+1}}$  矛盾。

因此  $a_{k_1} \geq a_{k_2} \geq \dots \geq a_{k_{n+1}}$  构成了一条长度为  $n+1$  的递减序列。

证毕。

**思考题.** 设军乐队的 $mn$ 个人按以下方式站成  $m$ 行  $n$  列的方队：  
在每一行中每个人都比他或她左边的人高。  
假设指挥将每一列的人按身高从前至后增加的顺序重排。证明：各行仍然是按身高从左至右增加的序列排列。

前

23	24	37	40	48
2	7	8	44	46
5	6	38	46	60



2	6	8	40	46
5	7	37	44	48
23	24	38	46	60

左

**思考题.** 设军乐队的 $mn$ 个人按以下方式站成  $m$ 行  $n$  列的方队：  
在每一行中每个人都比他或她左边的人高。  
假设指挥将每一列的人按身高从前至后增加的顺序重排。证明：各行仍然是按身高从左至右增加的序列排列。

证明：假设  $mn$  个人构成的方阵记为矩阵  $A=(a_{ij})$ ，其中  $a_{ij}$  为位于第  $i$  行第  $j$  列的人的身高，则对任意第  $i$  行，

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

假设重排后的方阵记为  $B=(b_{ij})$ ，满足则对任意第  $j$  列，

$$b_{1j} \leq b_{2j} \leq \dots \leq b_{mj} .$$

只需对任意第  $i$  行的第  $j-1$  与第  $j$  列元素  $b_{i,j-1}$  与  $b_{ij}$ ，证明

$$b_{i,j-1} < b_{ij} .$$

**思考题.** 设军乐队的 $mn$ 个人按以下方式站成  $m$ 行  $n$  列的方队：在每一行中每个人都比他或她左边的人高。

假设指挥将每一列的人按身高从前至后增加的顺序重排。证明：各行仍然是按身高从左至右增加的序列排列。

$b_{11}$	$b_{12}$	...	$b_{1,j-1}$	$b_{1,j}$	$b_{1,j+1}$	...	$b_{1,n}$
$b_{21}$	$b_{22}$	...	$b_{2,j-1}$	$b_{2,j}$	$b_{2,j+1}$	...	$b_{2,n}$
...	...	...	...	...	...	...	...
$b_{i-1,1}$	$b_{i-1,2}$	...	$b_{i-1,j-1}$	$b_{i-1,j}$	$b_{i-1,j+1}$	...	$b_{i-1,n}$
$b_{i1}$	$b_{i2}$	...	$b_{i,j-1}$	$b_{i,j}$	$b_{i,j+1}$	...	$b_{i,n}$
$b_{i+1,1}$	$b_{i+1,2}$	...	$b_{i+1,j-1}$	$b_{i+1,j}$	$b_{i+1,j+1}$	...	$b_{i+1,n}$
...	...	...	...	...	...	...	...
$b_{m1}$	$b_{m2}$	...	$b_{m,j-1}$	$b_{m,j}$	$b_{m,j+1}$	...	$b_{m,n}$

假设  $b_{i,j-1} \geq b_{ij}$ .

**思考题.** 设军乐队的 $mn$ 个人按以下方式站成  $m$ 行  $n$  列的方队：在每一行中每个人都比他或她左边的人高。  
 假设指挥将每一列的人按身高从前至后增加的顺序重排。证明：各行仍然是按身高从左至右增加的序列排列。

$b_{11}$	$b_{12}$	...	$b_{1,j-1}$	$b_{1,j}$	$b_{1,j+1}$	...	$b_{1,n}$
$b_{21}$	$b_{22}$	...	$b_{2,j-1}$	$b_{2,j}$	$b_{2,j+1}$	...	$b_{2,n}$
...	...	...	...	...	...	...	...
$b_{i-1,1}$	$b_{i-1,2}$	...	$b_{i-1,j-1}$	$b_{i-1,j}$	$b_{i-1,j+1}$	...	$b_{i-1,n}$
$b_{i1}$	$b_{i2}$	...	$b_{i,j-1} \geq$	$b_{i,j}$	$b_{i,j+1}$	...	$b_{i,n}$
$b_{i+1,1}$	$b_{i+1,2}$	...	$b_{i+1,j-1}$	$b_{i+1,j}$	$b_{i+1,j+1}$	...	$b_{i+1,n}$
...	...	...	...	...	...	...	...
$b_{m1}$	$b_{m2}$	...	$b_{m,j-1}$	$b_{m,j}$	$b_{m,j+1}$	...	$b_{m,n}$

假设  $b_{i,j-1} \geq b_{ij}$ .

因此，在 $A$ 中只有  $i-1$ 个人  $b_{k,j-1}$  ( $1 \leq k \leq i-1$ ) 可能在  $i$  个人  $b_{k,j}$  ( $1 \leq k \leq i$ ) 的相邻左侧，  
 与鸽巢原理矛盾，  
 因此，假设不成立。

**思考题.** 设军乐队的 $mn$ 个人按以下方式站成  $m$ 行  $n$  列的方队：在每一行中每个人都比他或她左边的人高。  
假设指挥将每一列的人按身高从前至后增加的顺序重排。证明：各行仍然是按身高从左至右增加的序列排列。

证明：（反证法）假设  $b_{i,j-1} \geq b_{ij}$  . (1)

考虑 $B$ 的第 $j-1$ 列，有  $b_{k,j-1} \geq b_{i,j-1}$ ,  $k = i, i+1, \dots, m$ . (2)

考虑 $B$ 的第 $j$ 列，有  $b_{k,j} \leq b_{i,j}$ ,  $k = 1, 2, \dots, i$ . (3)

由(1)-(3)得

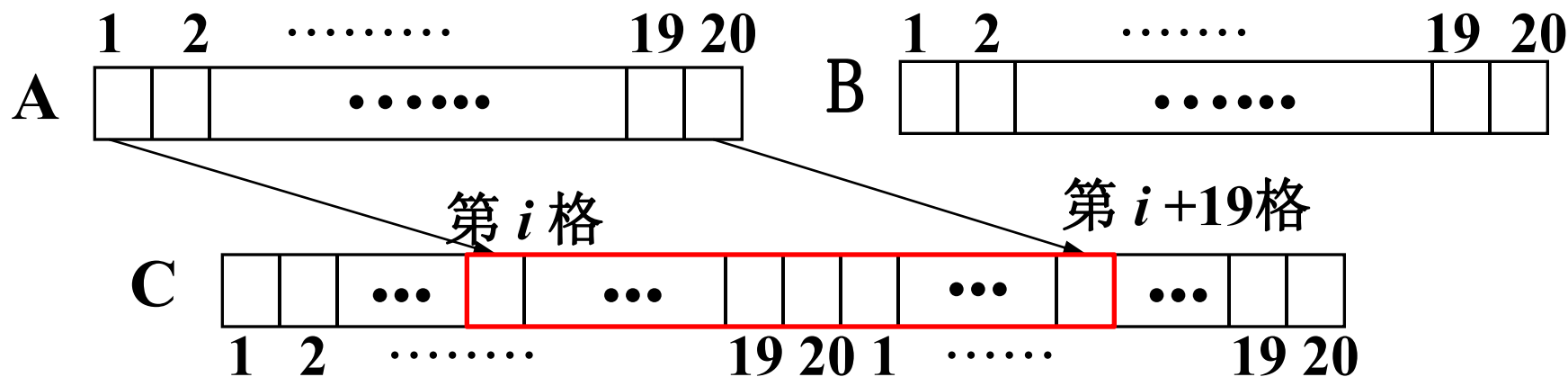
$$b_{1,j} \leq b_{2,j} \leq \dots \leq b_{i,j} \leq b_{i,j-1} \leq b_{i+1,j-1} \leq \dots \leq b_{m,j-1}.$$

因此，在 $A$ 中只有 $i-1$ 个人  $b_{k,j-1}$  ( $1 \leq k \leq i-1$ ) 可能在  $i$  个人  $b_{k,j}$  ( $1 \leq k \leq i$ ) 的相邻左侧，与鸽巢原理矛盾，因此，假设不成立。证毕。

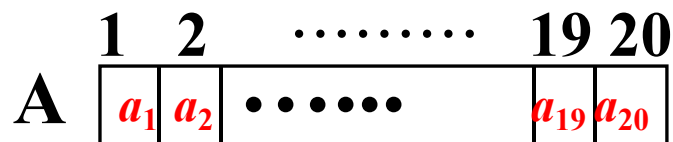
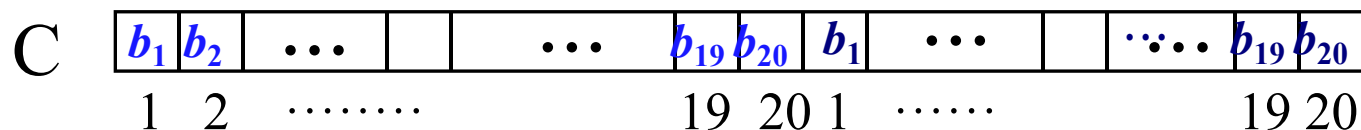
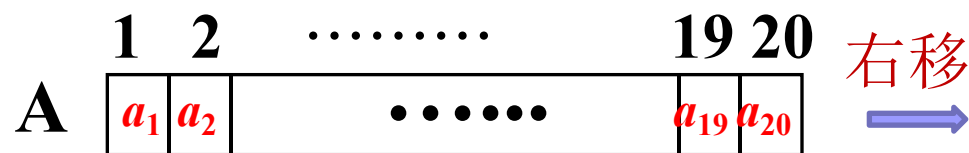
例. 设  $A = a_1 a_2 \cdots a_{20}$  是 10 个 0 和 10 个 1 组成的 20 位 2 进制数。 $B = b_1 b_2 \cdots b_{20}$  是任意的 20 位 2 进制数。令

$$C = b_1 b_2 \cdots b_{20} b_1 b_2 \cdots b_{20} = c_1 c_2 \cdots c_{40}.$$

则存在某个  $i$ ,  $1 \leq i \leq 21$ , 使得  $c_i c_{i+1} \cdots c_{i+19}$  与  $a_1 a_2 \cdots a_{20}$  至少有 10 位对应数字相同。







1、假想着 A 如图所示从左向右一格一格移动。

2、在移动到最后时,  $C$  中每对  $b_j$  一共遍历所有  $a_1, a_2, \dots, a_{20}$ 。  
因为  $A$  中有 10 个 0 和 10 个 1, 每一对  $b_j$  都有 10 位次对应相等。

3、在 20 次的移动过程中共有  $10 \times 20 = 200$  位次对应相等。

4、因此必有一次移动, 满足相同数字的格数至少为  
 $200/20=10$  位

# 回顾

定理3.1.1 如果把 $n+1$ 个物体放进  $n$  个盒子，那么至少有一个盒子包含两个或更多的物体。

定理3.2.1 令  $q_1, q_2, \dots, q_n$  为正整数。若将

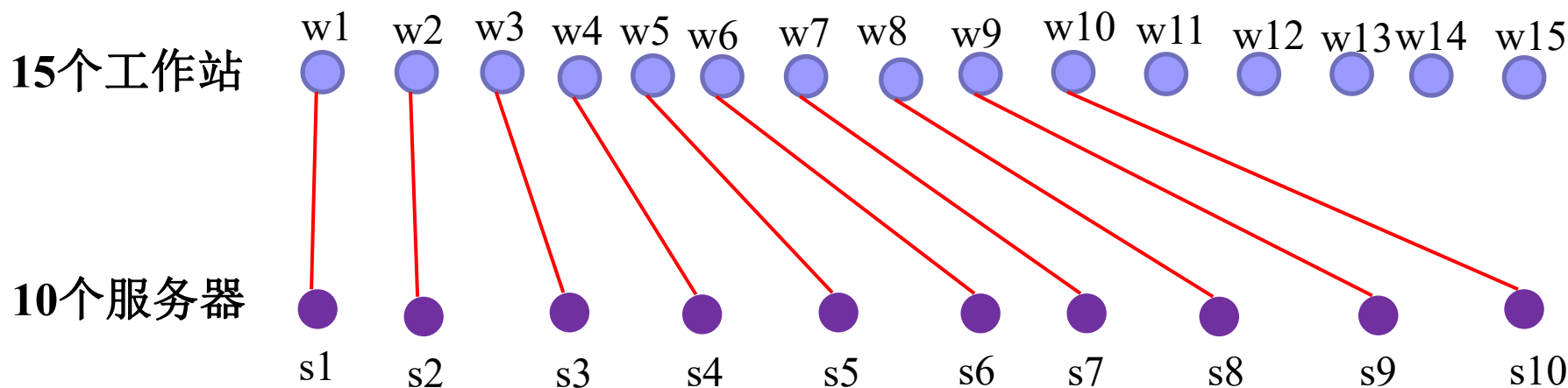
$$q_1 + q_2 + \dots + q_n - n + 1$$

个物体被放进  $n$  个盒子内，那么，

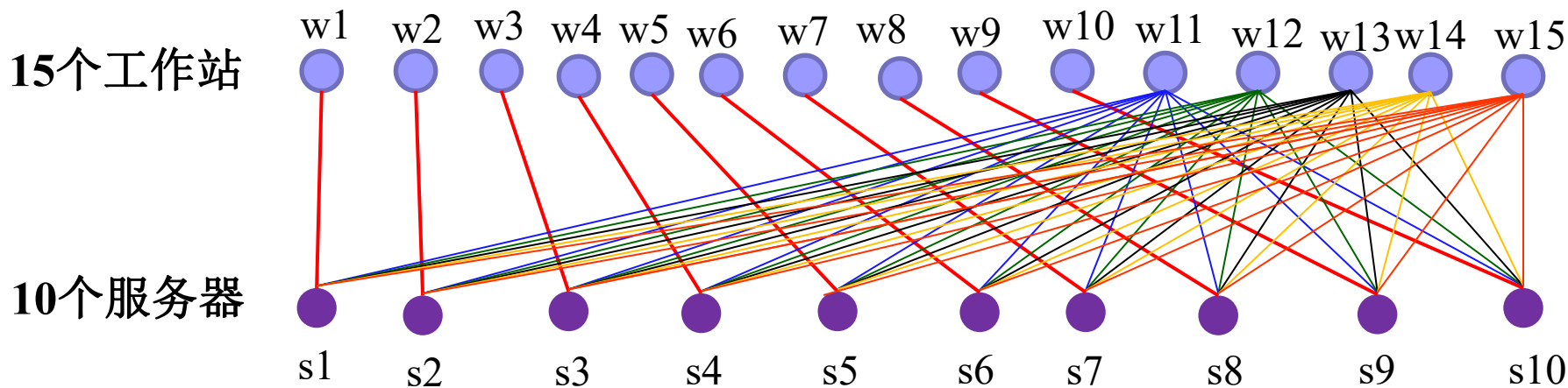
- 或者第1个盒子至少含有  $q_1$  个物体，
- 或者第2个盒子至少含有  $q_2$  个物体，...
- 或者第  $n$  个盒子至少含有  $q_n$  个物体。

平均原理：设  $m$  和  $n$  都是正整数。如果  $m$  个物体放入  $n$  个盒子，则至少有一个盒子含有  $\lceil m/n \rceil$  个或更多的物体。

思考：假设有**15台**工作站和**10台**服务器。可以用一条电缆直接把工作站连接到服务器。**同一时刻只有一条到服务器的直接连接是有效的**。如果想保证在**任何时刻任何一组不超过10台工作站**可以通过直接连接同时访问不同的服务器，所需的**最少直接连线**的数目是多少？



例：假设有**15台**工作站和**10台**服务器。可以用一条电缆直接把工作站连接到服务器。**同一时刻只有一条到服务器的直接连接是有效的**。如果想保证在任何时刻任何一组**不超过10台工作站**可以通过直接连接同时访问不同的服务器，所需的**最少直接连线**的数目是多少？



解：设工作站集合为 $\{w_1, \dots, w_{15}\}$ ，服务器集合为 $\{s_1, \dots, s_{10}\}$ ，

(1) 当 $i=1, \dots, 10$ 时，把 $w_i$ 与 $s_i$ 直接相连；

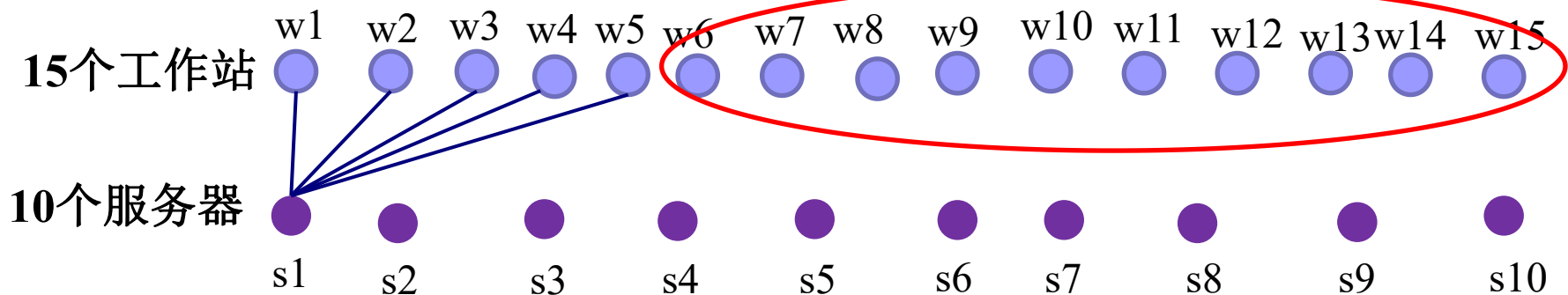
(2) 当 $i=11, \dots, 15$ 时，把 $w_i$ 与所有的服务器相连，一共有60条直接连接。(试证此时满足题目要求)

例：假设有**15台**工作站和**10台**服务器。可以用一条电缆直接把工作站连接到服务器。**同一时刻只有一条到服务器的直接连接是有效的**。如果想保证在任何时刻任何一组**不超过10台工作站**可以通过直接连接同时访问不同的服务器，所需的**最少直接连线**的数目是多少？

解(续)：下面证明**60**是满足条件的最小直接连线数目。

假设直接连线数目只有**59**条，此时，**必有一个服务器最多连接5台工作站**，否则直接连线数目超过**59**。

那么剩下的**9台服务器**和**10台工作站**无法满足需求（补充）。



# 作业

## ■ 3.4 练习题

□ 27, 28

## 思考题：

1. 一个圆周被分成 36 段，在 36 段上按任意方式分配数字  $1, 2, \dots, 36$ ，证明存在三个相邻段，使得分配给他们的数字之和至少是 56

定理3.1.1 如果把  $n+1$  个物体放进  $n$  个盒子，那么至少有一个盒子包含两个或者更多的物体。

定理3.2.1 令  $q_1, q_2, \dots, q_n$  为正整数。如果将

$$q_1 + q_2 + \dots + q_n - n + 1$$

个物体被放进  $n$  个盒子内，那么，

- 或者第1个盒子至少含有  $q_1$  个物体，
- 或者第2个盒子至少含有  $q_2$  个物体，...
- 或者第  $n$  个盒子至少含有  $q_n$  个物体。

设  $m$  和  $n$  都是正整数。如果  $m$  个物体放入  $n$  个盒子，则至少有一个盒子含有  $\lceil m/n \rceil$  个或更多的物体。





## 第三章 鸽巢原理

3.1 鸽巢原理的简单形式

3.2 鸽巢原理的加强形式

3.3 Ramsey定理

# Ramsey定理：一个简单形式

通俗实例：在6个人中，

- 或者有3个人，他们中每两个人都互相认识；
- 或者有3个人，他们中的每两个人都彼此不认识。



Frank Plumpton Ramsey  
(1903-1930)  
1930年发表“On a  
Problem in Formal Logic”  
证明了 $R(3,3)=6$

- 传播很广的数学竞赛题，曾刊登在《美国数学月刊》上（1958年6/7月号）。
- Ramsey定理是组合论中一个重要的存在性定理，推动了组合论等数理科学的发展，形成了一个方向。
- 在计算机科学中的应用
  - 姚其智利用Ramsey定理证明了在信息检索中，二分搜索是最好的检索策略。
  - Ramsey 数对分组交换网络设计中通信设施数量选择等问题具有指导意义。

# Ramsey定理：一个简单形式

通俗实例：在6个人中，

- 或者有3个人，他们中每两个人都互相认识；
- 或者有3个人，他们中的每两个人都彼此不认识。



Frank Plumpton Ramsey  
(1903-1930)  
1930年发表“On a  
Problem in Formal Logic”  
证明了 $R(3,3)=6$

- 英国数学家、哲学家、逻辑学家、经济学家，在他短促的一生中对许多领域做出开拓性的贡献。
- 出生在剑桥，剑桥大学三一学院学习数学。
- 他和查尔斯·凯·奥格顿聊天时，说他想学德语。奥格顿便给他一本文法书、字典和一篇深奥的心理学论文并告诉他：使用那本文法书和字典，告诉我们你的想法。约一星期后，他不止学会了德语，还对语法书中一些理论提出了反对意见。

# Ramsey定理：一个简单形式

通俗实例：在6个人中，

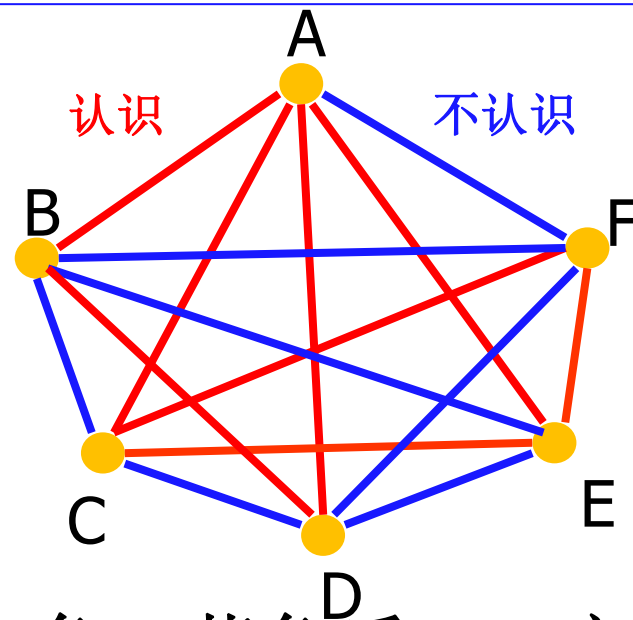
- 或者有3个人，他们中每两个人都互相认识；
- 或者有3个人，他们中的每两个人都彼此不认识。

图形式：(6个顶点的完全图 $K_6$ )

□ 顶点：每个人

边：两个人的认识关系

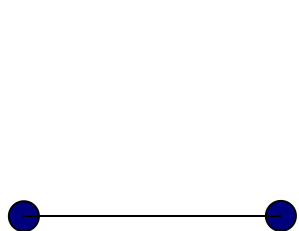
□ 边着色：红边表示认识，  
蓝边表示不认识



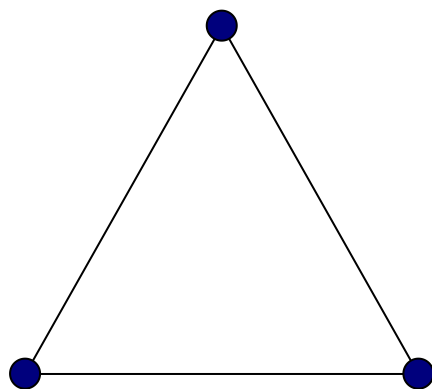
问题转化为：给图 $K_6$ 的边任意着红色、蓝色后，一定存在一个红色三角形或蓝色三角形

# 回顾：n阶完全图

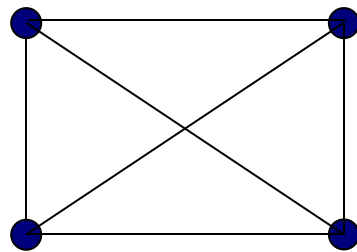
用 $K_n$ 表示平面上没有3点共线的 $n$ 个顶点构成的一个完全图 ( $n$ 阶完全图)。



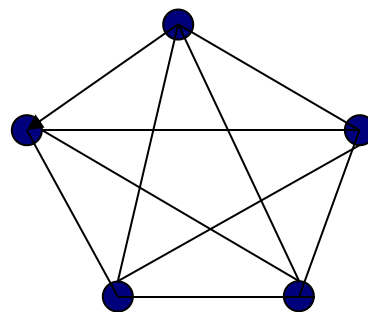
$K_2$



$K_3$

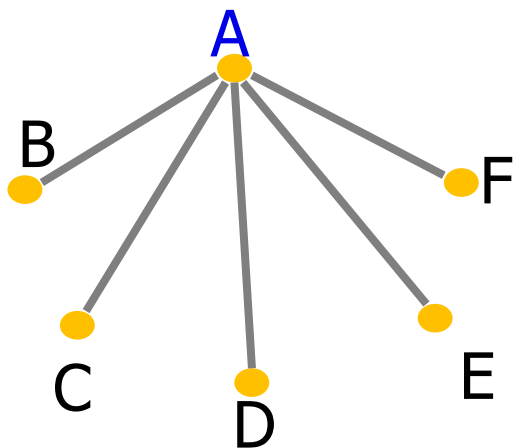


$K_4$



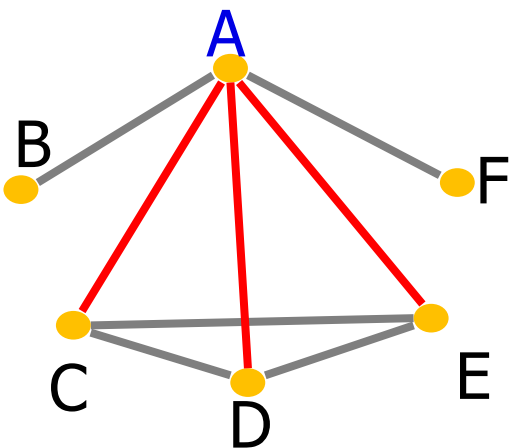
$K_5$

证明：给图 $K_6$ 的边任意着红色、蓝色，一定存在一个红色  $K_3$  或 蓝色  $K_3$ ，记为 $K_6 \rightarrow K_3, K_3$



- ✓  $K_6$ 中任意一个结点A连接了5条边，由鸽巢原理的加强形式，至少有 $[5/2] = 3$ 条边是同一个颜色；假设以上3条边均为红色，且这三条红边连向点C, D, E。

证明：给图 $K_6$ 的边任意着红色、蓝色，一定存在一个红色  $K_3$  或 蓝色  $K_3$ ，记为  $K_6 \rightarrow K_3, K_3$



✓  $K_6$ 中任意一个结点A连接了5条边，  
由鸽巢原理的加强形式，至少有  
 $[5/2] = 3$  条边是同一个颜色；  
假设以上3条边均为红色，且这三条红  
边连向点C, D, E。

- (1) 若C, D, E两两相连的边中存在一条红边，则与上述三条红边构成红色  $K_3$ ；
  - (2) 否则，C, D, E 两两相连的边均为蓝色，构成蓝色  $K_3$ 。
- 证毕。

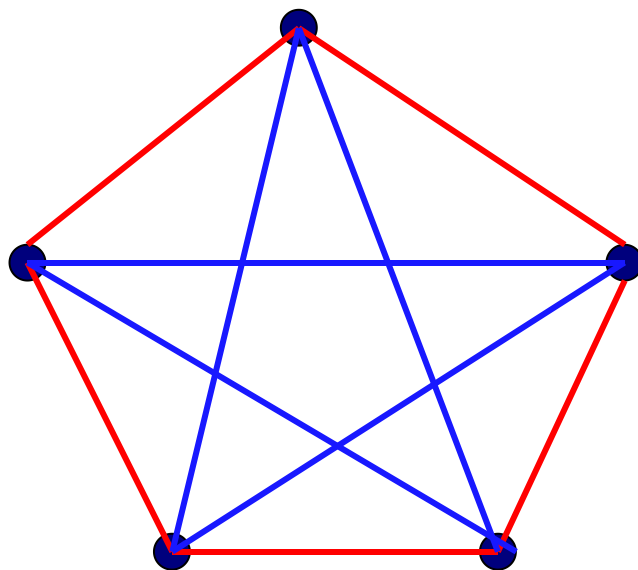
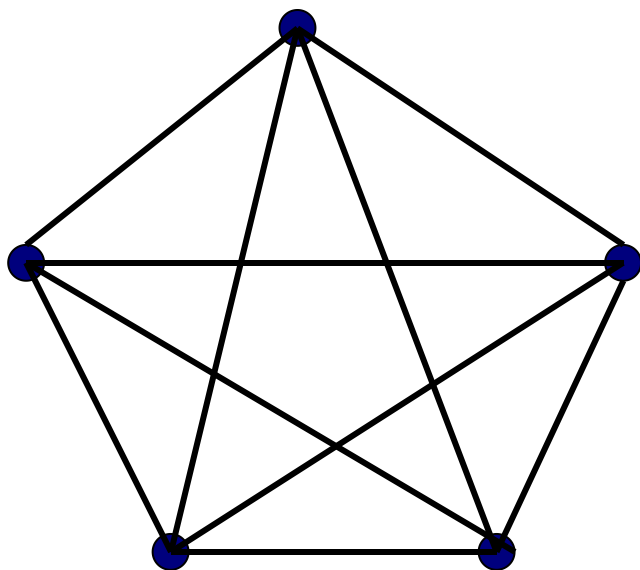
■ 结论:  $K_6 \rightarrow K_3, K_3$

□ 当  $n > 6$  时,  $K_n \rightarrow K_3, K_3$  一定成立

□  $K_5 \rightarrow K_3, K_3$  是否成立? 不成立

□ 使得  $K_n \rightarrow K_3, K_3$  成立的最小正整数  $n=6$

Ramsey数  
 $r(3, 3)=6$





**定理 3.3.1 (Ramsey定理)** 如果 $m \geq 2$ 及 $n \geq 2$ 是两个整数，则一定存在正整数 $p$ ，使得

$$K_p \rightarrow K_m, K_n$$

当把 $K_p$ 的边着成红色或蓝色时，

- 或者存在一个红色 $K_m$ ，
- 或者存在一个蓝色 $K_n$ 。

**定义 (Ramsey数)** Ramsey数 $r(m, n)$ 是使 $K_p \rightarrow K_m, K_n$ 成立的最小整数 $p$ 。

- $r(m, n)$ 一定存在 ( $m \geq 2$ 及 $n \geq 2$ 是整数)
- $r(m, n) = r(n, m)$

**定理 3.3.1 (Ramsey定理)** 如果 $m \geq 2$ 及 $n \geq 2$ 是两个整数, 则一定存在正整数 $p$ , 使得

$$K_p \rightarrow K_m, K_n$$

平凡的Ramsey数: 对于 整数  $m, n \geq 2$ ,

- $r(2, n) = n$

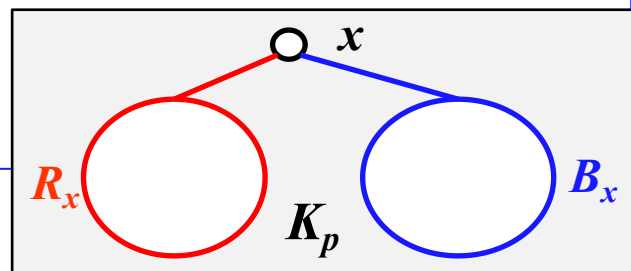
- $r(m, 2) = m$

或者存在一条边是红色,  
或者所有边都是蓝色

定理3.3.1 可通过对 $m, n$ 进行双重归纳证明。

**定理 3.3.1 (Ramsey定理)** 如果 $m \geq 2$ 及 $n \geq 2$ 是两个整数，则一定存在正整数 $p$ ，使得

$$K_p \rightarrow K_m, K_n$$



**证明：**对 $m, n$ 进行如下双重归纳：

- (1) 易证：当 $m=2$ 时， $r(2, n)=n$ ；当 $n=2$ 时， $r(m, 2)=m$ 。
- (2) 假设当 $m \geq 3, n \geq 3$ 时， $r(m-1, n)$ 与 $r(m, n-1)$ 存在，  
 设 $p = r(m-1, n) + r(m, n-1)$ ，下面证明

$$K_p \rightarrow K_m, K_n$$

- (3) 假设 $K_p$ 的边已用一种方式着成红色或蓝色。

考虑 $K_p$ 中一个点 $x$ ，设 $R_x$ 为通过红边与 $x$ 相连的点的集合， $B_x$ 为通过蓝边与 $x$ 相连的点的集合，

则  $|R_x| + |B_x| = p-1 = r(m-1, n) + r(m, n-1) - 1$ ，

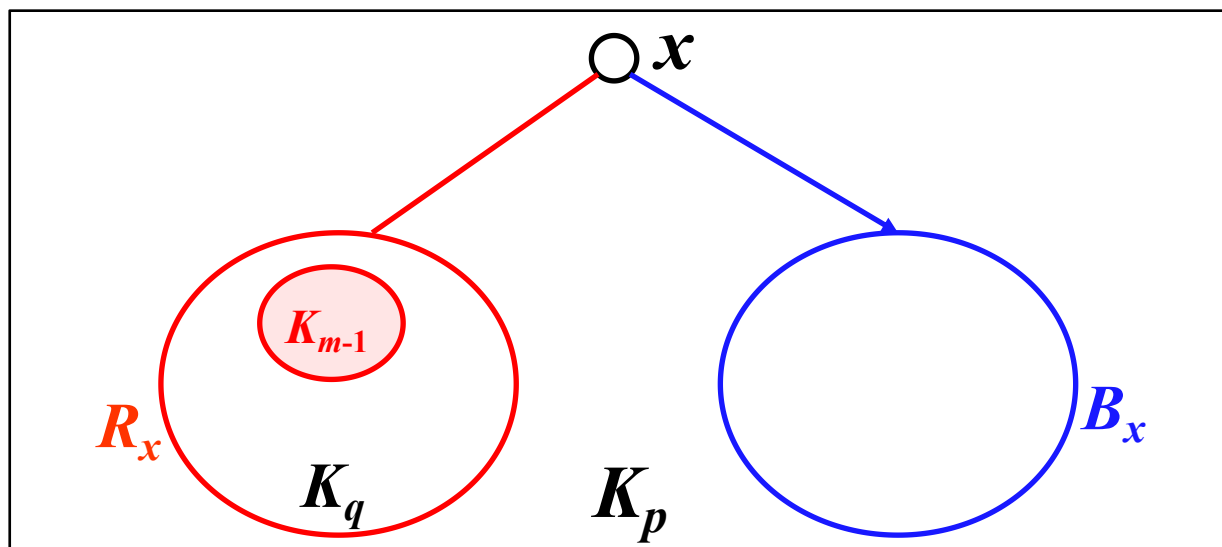
得：  $|R_x| \geq r(m-1, n)$  或者  $|B_x| \geq r(m, n-1)$ 。

证明（续）：  $|R_x| \geq r(m-1, n)$  或者  $|B_x| \geq r(m, n-1)$

(1) 当  $|R_x| \geq r(m-1, n)$  成立时，令  $q = |R_x|$ ，考虑  $K_q$ ，

则有  $K_q \rightarrow K_{m-1}, K_n$ ，即一定存在一个红色  $K_{m-1}$  或蓝色  $K_n$ 。

a) 若存在一个红色  $K_{m-1}$ ，

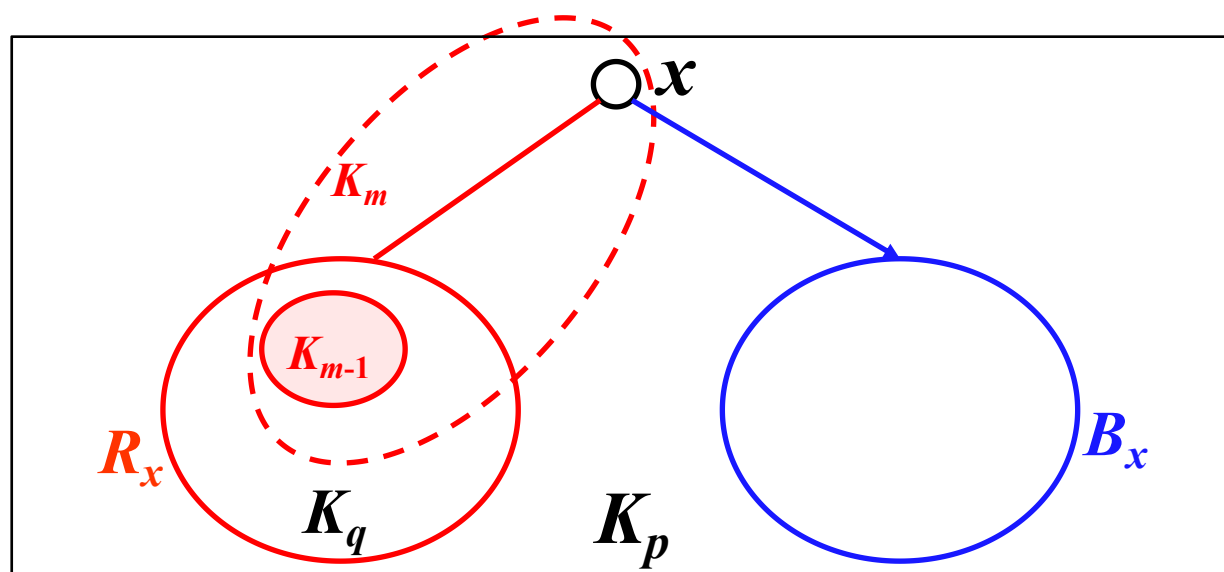


证明（续）：  $|R_x| \geq r(m-1, n)$  或者  $|B_x| \geq r(m, n-1)$

(1) 当  $|R_x| \geq r(m-1, n)$  成立时，令  $q = |R_x|$ ，考虑  $K_q$ ，

则有  $K_q \rightarrow K_{m-1}, K_n$ ，即一定存在一个红色  $K_{m-1}$  或蓝色  $K_n$ 。

a) 若存在一个红色  $K_{m-1}$ ，

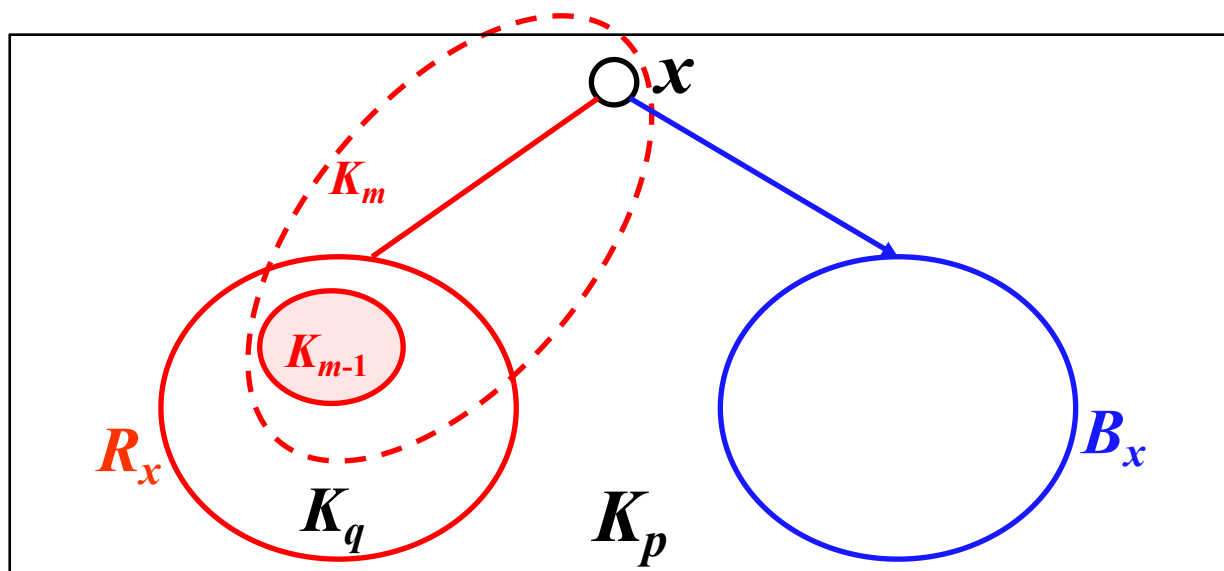


证明（续）：  $|R_x| \geq r(m-1, n)$  或者  $|B_x| \geq r(m, n-1)$

(1) 当  $|R_x| \geq r(m-1, n)$  成立时，令  $q = |R_x|$ ，考虑  $K_q$ ，

则有  $K_q \rightarrow K_{m-1}, K_n$ ，即一定存在一个红色  $K_{m-1}$  或蓝色  $K_n$ 。

a) 若存在一个红色  $K_{m-1}$ ，则增加点  $x$  后，构成红色  $K_m$ ，  
此时有  $K_p \rightarrow K_m, K_n$ 。



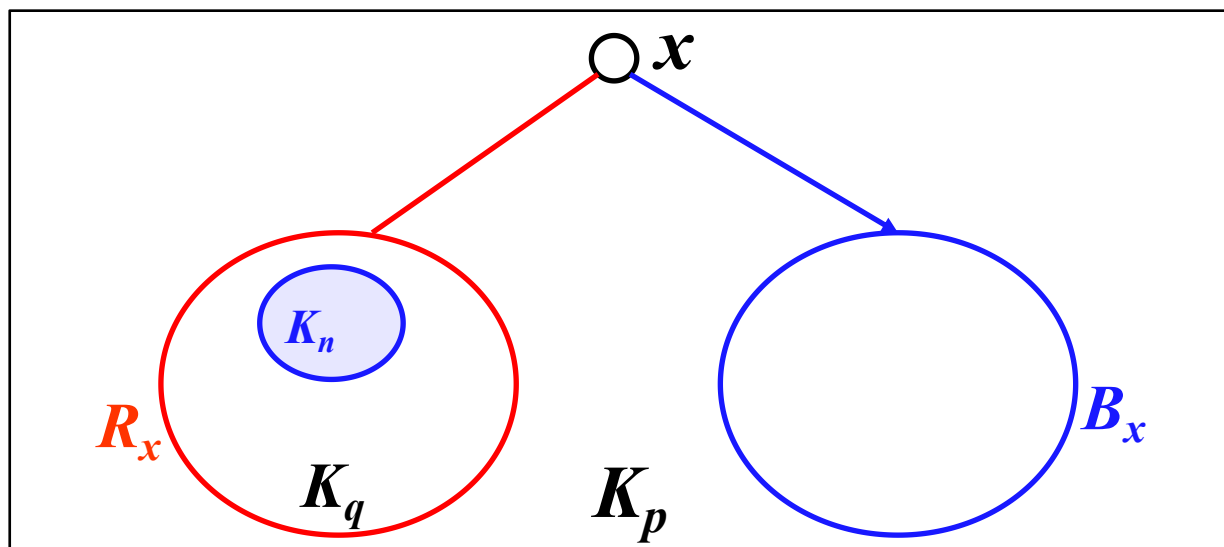
证明（续）：  $|R_x| \geq r(m-1, n)$  或者  $|B_x| \geq r(m, n-1)$

(1) 当  $|R_x| \geq r(m-1, n)$  成立时，令  $q = |R_x|$ ，考虑  $K_q$ ，

则有  $K_q \rightarrow K_{m-1}, K_n$ ，即一定存在一个红色  $K_{m-1}$  或蓝色  $K_n$ 。

a) 若存在一个红色  $K_{m-1}$ ，则增加点  $x$  后，构成红色  $K_m$ ，  
此时有  $K_p \rightarrow K_m, K_n$ 。

b) 若存在一个蓝色  $K_n$ ， $K_p \rightarrow K_m, K_n$  成立。



证明（续）： $|R_x| \geq r(m-1, n)$  或者  $|B_x| \geq r(m, n-1)$

(1) 当 $|R_x| \geq r(m-1, n)$ 成立时，令 $q = |R_x|$ ，考虑  $K_q$ ，

则有 $K_q \rightarrow K_{m-1}, K_n$ ，即一定存在一个红色  $K_{m-1}$  或蓝色  $K_n$ 。

a) 若存在一个红色  $K_{m-1}$ ，则增加点  $x$  后，构成红色  $K_m$ ，  
此时有  $K_p \rightarrow K_m, K_n$ 。

b) 若存在一个蓝色  $K_n$ ， $K_p \rightarrow K_m, K_n$  成立。

(2) 同理可证当  $|B_x| \geq r(m, n-1)$  时， $K_p \rightarrow K_m, K_n$  成立。

由归纳法得，对于所有整数  $m \geq 2$  及  $n \geq 2$ ，存在正整数  $p$ ，  
使得  $K_p \rightarrow K_m, K_n$  成立。

证毕。



**定理 3.3.1 (Ramsey定理)** 如果 $m \geq 2$ 及 $n \geq 2$ 是两个整数，则存在正整数 $p$ ，使得

$$K_p \rightarrow K_m, K_n$$

归纳证明中：

设  $p = r(m-1, n) + r(m, n-1)$ ，从而证明

$$K_p \rightarrow K_m, K_n$$

推论：  $r(m, n) \leq r(m-1, n) + r(m, n-1)$ ，  $m, n \geq 3$ 。

例：试证  $r(3, 4) \leq 10$ ，即把  $K_{10}$  的边任意着红色或蓝色，则一定或者存在一个红色 $K_3$ ，或者存在一个蓝色 $K_4$ 。

$$r(3, 4) \leq r(2, 4) + r(3, 3) = 4 + 6 = 10 \quad r(3, 4) \leq 9?$$

推论：  $r(m, n) \leq r(m-1, n) + r(m, n-1)$ 。

例：试证  $r(3, 4) \leq 10$ ，即把  $K_{10}$  的边任意着红色或蓝色，则一定或者存在一个红色  $K_3$ ，或者存在一个蓝色  $K_4$ 。

证明：  $r(3, 4) \leq r(2, 4) + r(3, 3)$   
 $= 4+6=10$ 。

思考题：试证  $r(3, 4) \leq 9$ ，即给  $K_9$  的边任意着红色或蓝色，则一定或者存在一个红色  $K_3$ ，或者存在一个蓝色  $K_4$ 。

证明：设  $K_9$  的所有边被着成红色或蓝色，则不可能所有的点都正好有3条边相连被着成红色。

否则，9个顶点相连的被着成红色的总边数为  $3 \times 9 = 27$ ，而每条边被两个点相连，因此总边数应为偶数，矛盾。

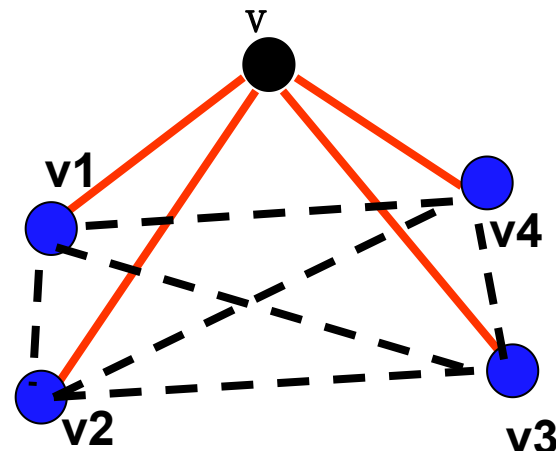
设  $K_9$  的点  $v$  相连的红边个数不为3。

(1) 当与点  $v$  相连的红边个数大于3时，

设  $v$  与点  $v_1, v_2, v_3, v_4$  相连的边为红色，

显然，若不存在红色  $K_3$ ，则  $v_1, v_2, v_3, v_4$

四个点之间的边只能为蓝色，构成蓝色  $K_4$ 。

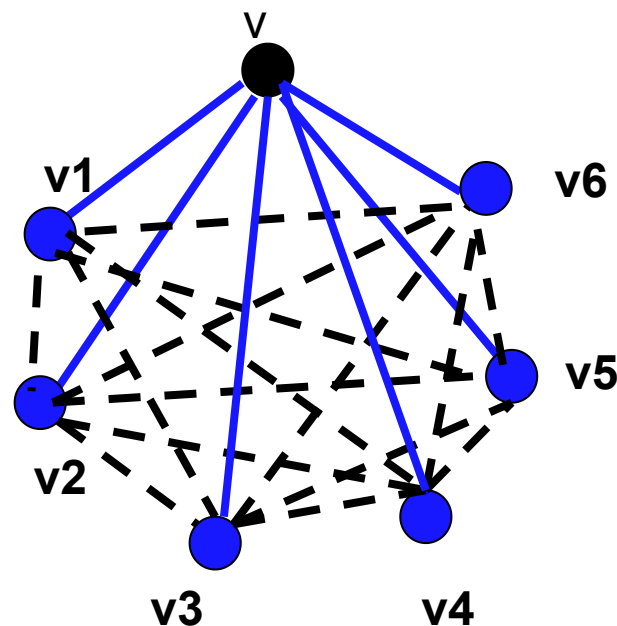


思考题：试证  $r(3, 4) \leq 9$ ，即给  $K_9$  的边任意着红色或蓝色，则一定或者存在一个红色  $K_3$ ，或者存在一个蓝色  $K_4$ 。

证明：(2) 当与点  $v$  相连的红边个数小于3时，与  $v$  相连的蓝边至少为6条。

如图所示，点  $v_1, \dots, v_6$  构成  $K_6$ ，则或者有红色  $K_3$ ，或者有蓝色  $K_3$ 。

若红色  $K_3$  不存在，则必存在蓝色  $K_3$ ，且与点  $v$  构成蓝色  $K_4$ 。



# Ramsey数 $r(m, n)$

m,n	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1
2	1	2	3	4	5	6	7	8	9	10
3	1	3	6	9	14	18	23	28	36	40–43
4	1	4	9	18	25	35–41	49–61	56–84	73–115	92–149
5	1	5	14	25	43–49	58–87	80–143	101–216	125–316	143–442
6	1	6	18	35–41	58–87	102–165	113–298	127–495	169–780	179–1171
7	1	7	23	49–61	80–143	113–298	205–540	216–1031	233–1713	289–2826
8	1	8	28	56–84	101–216	127–495	216–1031	282–1870	317–3583	317–6090
9	1	9	36	73–115	125–316	169–780	233–1713	317–3583	565–6588	580–12677
10	1	10	40–43	92–149	143–442	179–1171	289–2826	317–6090	580–12677	798–23556

# Ramsey定理推广

- Ramsey定理可推广到任意多种颜色的情况。

$l$  种颜色：

如果  $n_1, n_2, \dots, n_l$  都是大于或等于 2 的整数，则一定存在正整数  $p$ ，使得

$$K_p \rightarrow K_{n_1}, K_{n_2}, \dots, K_{n_l}。$$

满足以上条件的最小整数  $p$  称为Ramsey数

$$r(n_1, n_2, \dots, n_l)。$$

例如：  $K_{17} \rightarrow K_3, K_3, K_3$

例：试证  $r(3, 3, 3) \leq 17$

证：设有完全图  $K_{17}$ ，给其边任意着红色、蓝色或绿色。

对任意一个节点A，A连接了16条边。

由鸽巢原理的加强形式知，16条边至少存在  $\lceil 16/3 \rceil = 6$  条边同色，假设为红色，且这6条红边连向点B, C, D, E, F, G。

考虑由结点B, C, D, E, F, G构成的完全图  $K_6$ 。

(1) 若  $K_6$  中有一条边为红色，

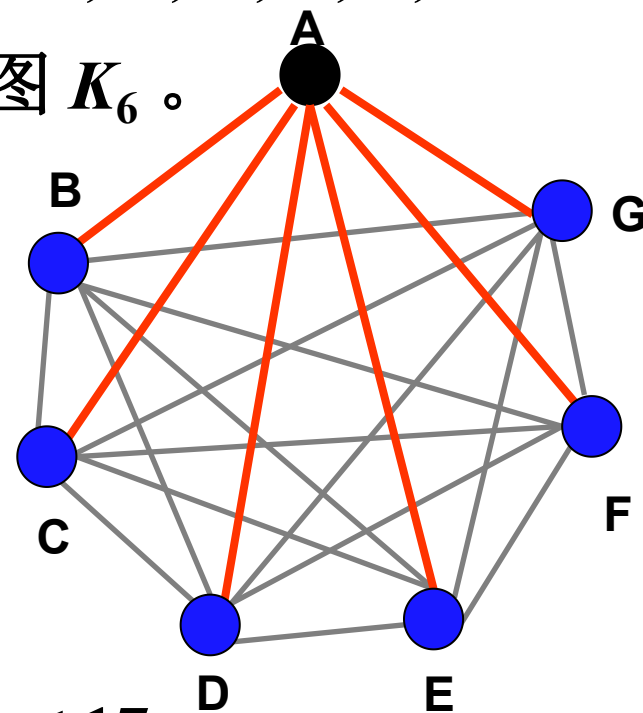
则  $K_{17}$  存在一个红  $K_3$ ；

(2) 若  $K_6$  中无红边，

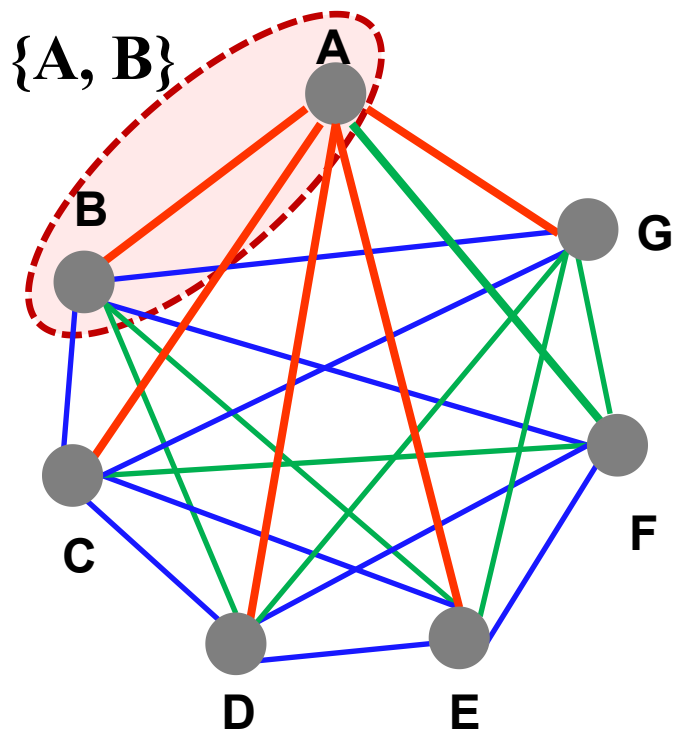
则  $K_6$  仅用蓝黄两色着色。

由  $K_6 \rightarrow K_3, K_3$ ，得  $K_{17}$  一定存在蓝色或绿色  $K_3$ 。

综上，得  $K_{17} \rightarrow K_3, K_3, K_3$ ，从而  $R(3, 3, 3) \leq 17$ 。



# Ramsey定理更一般形式



- 对每条边进行着色
- 一条边是两个顶点的子集

## ■ 扩展:

- 把点对扩展至  $t$  个元素的子集 ( $t \geq 2$ )
- 对每个  $t$  个元素的子集指定颜色



# Ramsey定理更一般形式

给定整数  $t \geq 2$  及整数  $q_1, q_2, \dots, q_k \geq t$ , 则存在一个整数  $p$ , 使得: 如果将  $p$  元素集合中每一个  $t$  元素子集指定为  $k$  种颜色  $c_1, c_2, \dots, c_k$  中一种, 那么

- 或者存在  $q_1$  个元素, 其所有  $t$  子集被指定成颜色  $c_1$ ,
- ... ..,
- 或者存在  $q_k$  个元素, 其所有  $t$  子集被指定成颜色  $c_k$ 。

满足结论的最小整数  $p$  为Ramsey数  $r_t(q_1, q_2, \dots, q_k)$

令  $K_n^t$  表示  $n$  个元素集合中所有  $t$  个元素的子集的集合。

给定整数  $t \geq 2$  及整数  $q_1, q_2, \dots, q_k \geq t$ , 存在一个整数  $p$ , 使得  $K_p^t \rightarrow K_{q_1}^t, K_{q_2}^t, \dots, K_{q_k}^t$ 。

# Ramsey定理是鸽巢原理的加强形式的扩展

给定整数  $t \geq 2$  及整数  $q_1, q_2, \dots, q_k \geq t$ , 存在一个整数  $p$ , 使得  $K_p^t \rightarrow K_{q_1}^t, K_{q_2}^t, \dots, K_{q_k}^t$

$t=1$ 时, 定理描述为:

存在一个整数  $p$ , 使得: 如果  $p$  元素集合的每个元素指定为  $k$  种颜色  $c_1, c_2, \dots, c_k$  中一种, 那么

- 或者存在  $q_1$  个元素被指定为颜色  $c_1, \dots,$
- 或者存在  $q_k$  个元素被指定为颜色  $c_k$ 。

由鸽巢原理的加强形式,

$$r_1(q_1, q_2, \dots, q_k) = q_1 + q_2 + \dots + q_k - k + 1$$

# 总结

定理3.1.1 如果把 $n+1$ 个物体放进  $n$ 个盒子，那么至少有一个盒子包含两个或者更多的物体。

定理3.2.1 令 $q_1, q_2, \dots, q_n$ 为正整数.若将

$q_1 + q_2 + \dots + q_n - n + 1$   
个物体被放进 $n$ 个盒子内，那么，

- 或者第1个盒子至少含有 $q_1$ 个物体，
- 或者第2个盒子至少含有 $q_2$ 个物体，...
- 或者第 $n$ 个盒子至少含有 $q_n$ 个物体。

平均原理：设 $m$ 和 $n$ 都是正整数。如果 $m$ 个物体放入 $n$ 个盒子，则至少有一个盒子包含至少 $\lceil m/n \rceil$ 个物体。

# Ramsey定理的应用

- 信息检索
- 分组交换网络设计

A. C. Yao. Should Tables be sorted? J.acm 28(1981), 615-628

Should Tables Be Sorted? <sup>\*/</sup>

Andrew Chi-Chih Yao

Computer Science Department  
Stanford University  
Stanford, California 94305

## Abstract.

We examine optimality questions in the following information retrieval problem: Given a set  $S$  of  $n$  keys, store them so that queries of the form "Is  $x \in S$ ?" can be answered quickly. It is shown that, in a rather general model including all the commonly-used schemes,  $\lceil \lg(n+1) \rceil$  probes to the table are needed in the worst case, provided the key space is sufficiently large. The effects of smaller key space and arbitrary encoding are also explored.

Key Words and Phrases: Information retrieval, lower bound, optimality, query, Ramsey's theorem, search strategy, sorted table.

CR Categories: 3.74, 4.34, 5.25, 5.31.

<sup>\*/</sup>This research was supported in part by National Science Foundation under grant MCS-77-05313.

# 总结

定理3.1.1 如果把 $n+1$ 个物体放进 $n$ 个盒子，那么至少有一个盒子包含两个或者更多的物体。

平均原理：设 $m$ 和 $n$ 都是正整数。如果 $m$ 个物体放入 $n$ 个盒子，则至少有一个盒子包含至少 $\lceil m/n \rceil$ 个物体。

- 存在性证明往往提供了算法设计思想

例: (1) 从一幅标准的**52张牌**中共随意选出**26张牌**, 则至少有几张牌是同一个花色?  
(2) 从一幅标准的**52张牌**中要随意选出 **7 张是同样的花色**, 必须选出多少张牌?

解: (1) 由鸽巢原理的加强形式知, 至少有  $\lceil 26/4 \rceil = 7$  张牌是同一个花色。

(2) 假设有四个盒子, 每个盒子保存一个花色的牌。由鸽巢原理的加强形式知, 若选择  $N$  张牌, 则一定有一个盒子包含观至少  $\lceil N/4 \rceil$  张牌。

又有满足  $\lceil N/4 \rceil = 7$  的最小整数为  $N=25$ 。因此必须选 25 张牌才能满足需要。

例：如果有5个可能的成绩A, B, C, D, E, F，那么在一个班里最少有多少个学生才能保证至少6个学生得到相同的分数？

解：由鸽巢原理的加强形式知，若有 $N$ 个学生，则一定有一个成绩，使得，得到该成绩的学生个数至少为 $\lceil N/5 \rceil$ 。

由题意知使得 $\lceil N/5 \rceil = 6$ 的最小整数为 $N = 26$ 。

如果学生人数为25，则每个成绩的人数可能出现都为5的情况，不满足题意。

因此最少有26个学生才能保证至少6个学生得到相同的分数

# 知识点

数论问题

几何图形  
类问题

连续时间  
问题

棋盘着色

中国剩余  
定理

满足条件的  
最小物体  
数

**存在性  
问题**

完全图的一  
种着色

**Ramsey  
定理**

**鸽巢原理**

简单形式

加强形式

$n+1$  个

$n$  个

$n$  个

$m$  个

物体

鸽子

盒子

巢

$$K_p \rightarrow K_{n_1}, K_{n_2}, \dots, K_{n_l}$$

$$K_p \rightarrow K_m, K_n$$

**Ramsey数**



