数论与组合模型

浙江大学 谈之奕

NIM游戏

数论

数学建模 *MATH T*

- 数论 (number theory)
    - 研究整数性质的数学分支
        - 数论问题的表述大多是算术的，但绝大多数问题用初等方法根本无法讨论。对数论的研究常常综合应用几何、代数和分析方法
        - 数论在计算机科学、信息科学、密码学、管理科学等领域获得广泛应用
        - 数论在中国古代有着悠久光辉的研究历史和成就，也是中国近代数学最早开拓并取得瞩目成就的数学研究领域之一

Die Mathematik hielt Gauss um seine eigenen Worte zu gebrauchen, für die Königin der Wissenschaften und die Arithmetik für die Königin der Mathematik. Diese lasse sich dann öfter herab

Von Waltershausen WS, *Gauss: zum Gedächtnis*, 1856

复数 (complex number) $\mathbb{C}$

实数 (real number) $\mathbb{R}$

有理数 (rational number) $\mathbb{Q}$

整数 (integer) $\mathbb{Z}$

自然数 $\mathbb{N}$ (natural number)

费马大定理 (Fermat's Last Theorem)

哥德巴赫猜想 (Goldbach Conjecture)

孪生素数猜想 (Twin Prime Conjecture)

黎曼猜想 (Riemann Hypothesis)

NIM游戏

- NIM游戏
  - 现有 n 堆硬币，每堆数量一定
  - 两人轮流取硬币，每次只能从其中一堆中取，每次取至少一枚
  - 取到最后一枚硬币的一方获胜

如何才能取胜

是否一定能胜

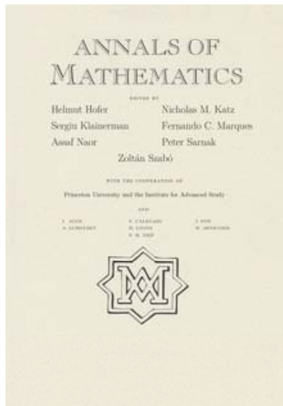
必胜 策略

nehmen: vt. 拿，取，拿起

nimm：nehmen的命令式

Charles Leonard Bouton
（1869-1922）
美国哈佛大学数学系副教授，1898年于德国莱比锡大学取得博士学位

Bouton CL. Nim, a game with a complete mathematical theory. *Annals of Mathematics*, 3: 35-39, 1901.



Annals of Mathematics，1884年创办于弗吉尼亚大学，现由普林斯顿大学数学系和高等研究院编辑出版，是目前最有影响的纯粹数学学术期刊之一

NIM游戏

数学建模

MATH T

- NIM游戏

后手必胜 $\begin{array}{c}1\\1\end{array} \to \begin{array}{c}1\\0\end{array} \to \begin{array}{c}0\\0\end{array}$

先手必胜 $\begin{array}{cc}2 & k\\1 & 1\end{array} \to \begin{array}{c}1\\1\end{array}$

后手必胜 $\begin{array}{c}k\\k\end{array} \to \begin{cases}\begin{array}{c}k\\0\end{array} \to \begin{array}{c}0\\0\end{array}\\[2ex] \begin{array}{c}k\\l\end{array} \to \begin{array}{c}l\\l\end{array}\end{cases}$

先手必胜 $\begin{array}{c}k\\l\end{array} \to \begin{array}{c}l\\l\end{array}$

先手必胜 $\begin{array}{c}1\\1\\1\end{array} \to \begin{array}{c}1\\1\\0\end{array}$

先手必胜 $\begin{array}{c}k\\k\\l\end{array} \to \begin{array}{c}k\\k\\0\end{array}$

后手必胜 $\begin{array}{c}3\\2\\1\end{array} \to \begin{array}{cccccc}0 & 1 & 2 & 3 & 3 & 3\\2 & 2 & 2 & 0 & 1 & 2\\1 & 1 & 1 & 1 & 1 & 0\end{array}$

先手必胜 $\begin{array}{c}4\\2\\1\end{array} \to \begin{array}{c}3\\2\\1\end{array}$

$\begin{array}{c}4\\2\\1\end{array} \to \begin{array}{cccccc}2 & 1 & 0 & 4 & 4 & 4\\2 & 2 & \cancel{2} & \cancel{1} & 0 & 2\\1 & 1 & 1 & 1 & 1 & 0\end{array}$

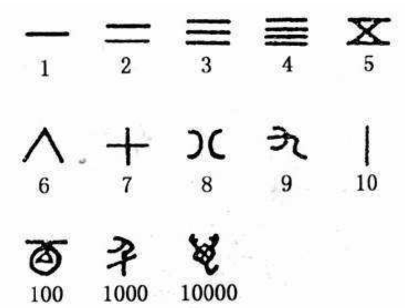
数学建模
MATH T

记数法

- 数（number）
  - 人类认识、分析和描述世界的基本手段之一。数的抽象是数学的开端
- 记数法（number system）
  - 记录或标志数目的方法
- 位值制记数法（positional numeral system）
  - 用一组有顺序的数字来表示一个数。每个数字所表示的大小，既取决于它本身的数值，又取决于它所在的位置

$$239 = 2\cdot 10^2 + 3\cdot 10 + 9$$

$$2 = \left\lfloor \frac{239}{10^2} \right\rfloor,\ 3 = \left\lfloor \frac{239 - 2\times 10^2}{10} \right\rfloor,\ 9 = \left\lfloor \frac{239 - 2\times 10^2 - 3\times 10}{1} \right\rfloor$$



甲骨文中的数字

木楼式时刻更钟
[清]乾隆
故宫博物院藏

CCXXXIX　239

两百三十九

罗马数码	I	II	III	IV	V	VI	VII
含义	1	2	3	4	5	6	7
罗马数码	VIII	IX	X	L	C	D	M
含义	8	9	10	50	100	500	1000

记数法

数学建模

MATH T

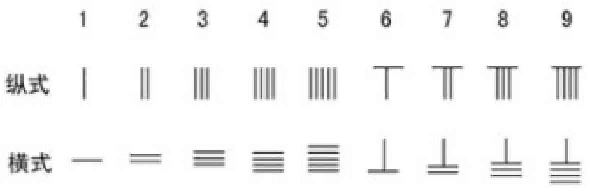
- 位值制记数法
  - 选定进位制的基底 b，给定 $0,1,2,\cdots,b-1$共 b 个数码。任何一个自然数 N， 均可用某个以这些数码为系数的 b 的多项式表示出来

$$N = a_k \cdot b^k + a_{k-1} \cdot b^{k-1} + \cdots + a_1 \cdot b + a_0$$

$$\Rightarrow (a_k a_{k-1} \cdots a_1 a_0)_b, \quad a_0, a_1, \cdots, a_k \in \{0,1,\cdots,b-1\}$$

- 任意数的 b 进制表示是唯一的
- 任意两个不同数的 b 进制表示不同

巴比伦	六十进制
古印度	十进制
中国古代	十进制
玛雅人	二十进制

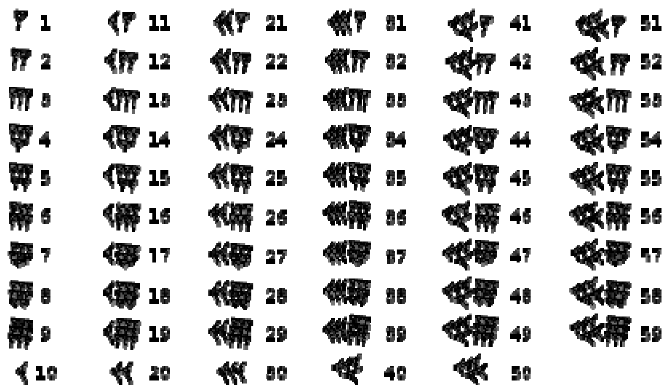


从右到左，纵横相间 

中国算筹计数（约公元前5世纪）

1 2 3 4 5 6 7 8 9 0

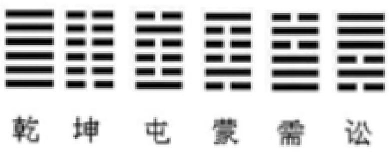
印度-阿拉伯数码，起源于印度，8世纪起传入阿拉伯国家，13世纪传入欧洲，约至16世纪写法固定，是现在的国际通用数码



巴比伦楔形文字（约公元前2000年）

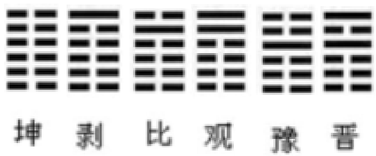
二进制

- 二进制（binary number system）
  - 基底为 2， 用数码 0 和 1 表示的记数法
  - 二进制的运算
    - $0+0=0, 0+1=1, 1+1=10$
  - 二进制的应用
    - 二进制在电子计算机中得到了广泛的应用。计算机由逻辑电路组成，电路中通常只有两个状态：开关接通和断开。两种状态恰好可用 1 和 0 表示



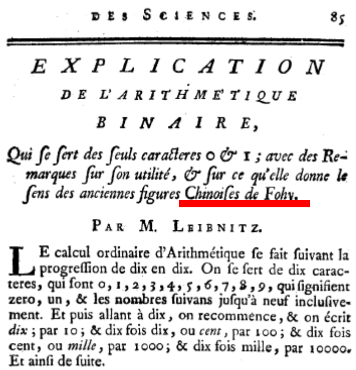
63 0 34 17 58 23

《周易》原书前6卦



0 1 2 3 4 5

北宋哲学家邵雍按自己的理解重排64卦中的前6卦



DES SCIENCES. 85

EXPLICATION
DE L'ARITHMETIQUE
BINAIRE,

Qui ſe ſert des ſeuls caracteres 0 & 1 ; avec des Remarques ſur ſon utilité, & ſur ce qu'elle donne le ſens des anciennes figures Chinoiſes de Fohy.

PAR M. LEIBNITZ.

LE calcul ordinaire d'Arithmétique ſe fait ſuivant la progreſſion de dix en dix. On ſe ſert de dix caracteres, qui ſont 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, qui ſignifient zero, un, & les nombres ſuivans juſqu'à neuf incluſivement. Et puis allant à dix, on recommence, & on écrit *dix* ; par 10 ; & dix fois dix, ou *cent*, par 100 ; & dix fois cent, ou *mille*, par 1000 ; & dix fois mille, par 10000. Et ainſi de ſuite.

Gottfried Wilhelm Leibniz （1646-1716）
德国哲学家、数学家

Leibniz G, Explanation of binary arithmetic, which uses only the characters 1 and 0, with some remarks on its usefulness, and on the light it throws on the ancient Chinese figures of Fu Xi, *Memoires de mathématique et de physique de l'Académie royale des sciences, Académie royale des sciences*, 1703

《周易》，中国儒家典籍，六经之一，成书于周。全书由64卦组成。每卦由6个“爻”排列而成。每个爻为阳爻“——”或阴爻“— —”两种符号之一。《周易》虽属占书，但在其神秘的形式中蕴含着较深刻的理论思维和辩证观念

安全状态与不安全状态

- 对己方取后形成的某个状态
  - 若无论对方如何取均不会获胜，状态（对己方）为安全的
    - 至少有两堆硬币的状态是安全的
  - 若对方至少存在一种获胜的取法，状态（对己方）为不安全的
    - 只有一堆硬币的状态是不安全的
  - 若无论对方如何取，己方下一次取后均可变为一个安全状态的状态也是安全的
  - 若对方至少存在一种取法，己方下一次取无法变为一个安全状态的状态也是不安全的
- NIM游戏的必胜策略
  - 取硬币方寻找一种取法，使取后状态对己方是安全的

3		2		2
2	→	2	→	2
1		1		0
安全				安全

2		2		2
2	→	2	→	0
1		0		0
不安全				不安全

NIM游戏与二进制

- 二进制与位和
  - 将每堆硬币数表示为二进制。将所有二进制数的每一位数字分别求和，其尾数称为位和
    - 只有一堆硬币时，位和不可能全为0
    - 每次从某一堆中取若干枚硬币，该堆硬币的二进制数发生变化，至少有一位位和发生变化
- 位和与安全性
  - 若所有位和均为 0，则当前状态为安全的，否则为不安全
  - 若当前状态安全，对任意取法，状态变为不安全
  - 若当前状态不安全，存在一种取法，状态变为安全
    - 按自左至右的顺序确定第一个数字之和不为0的位，寻找该位数字为1的堆，从该堆中取走若干枚使得状态变为安全

2	1 0
12	1 1 0 0
13	1 1 0 1
21	1 0 1 0 1
	1 0 1 1 0

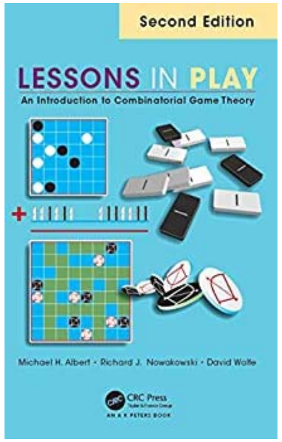
2	1 0
12	1 1 0 0
13	1 1 0 1
3	1 1
	0 0 0 0

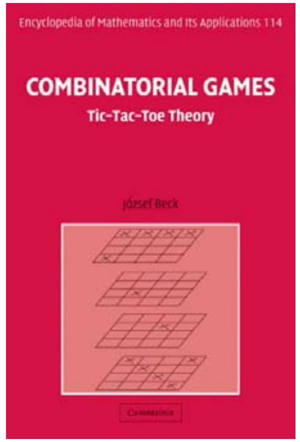
2	1 0
9	1 0 0 1
8	1 0 0 0
3	1 1
	0 0 0 0

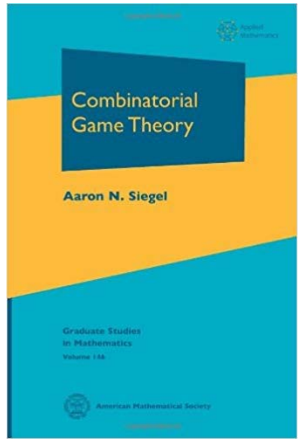
2	1 0
9	1 0 0 1
13	1 1 0 1
3	1 1
	0 1 0 1

NIM游戏

- NIM游戏
  - 若初始状态不安全，先手必胜。若初始状态安全，后手必胜
  - 必胜一方选择适当的取法，使取后状态对己方是安全的
- NIM的变形
  - **Misère NIM**：取到最后一枚硬币的一方落败
  - **NIM k**：每次只能从一堆硬币中至多取 k 枚
  - **Greedy NIM**：每次只能硬币数量最多的堆中取
  - **N-person NIM**







Albert MH, Nowakowski RJ, Wolfe D, *Lessons in Play: An Introduction to Combinatorial Game Theory*. CRC, 2019

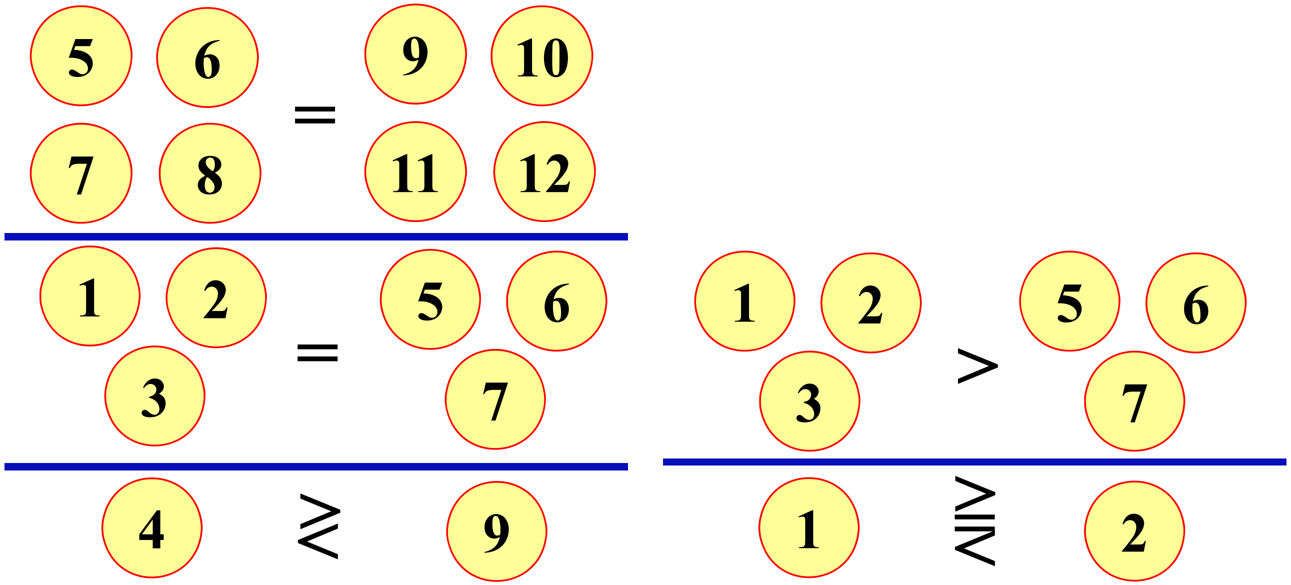
Siegel AN. *Combinatorial Game Theory*. American Mathematical Society, 2013

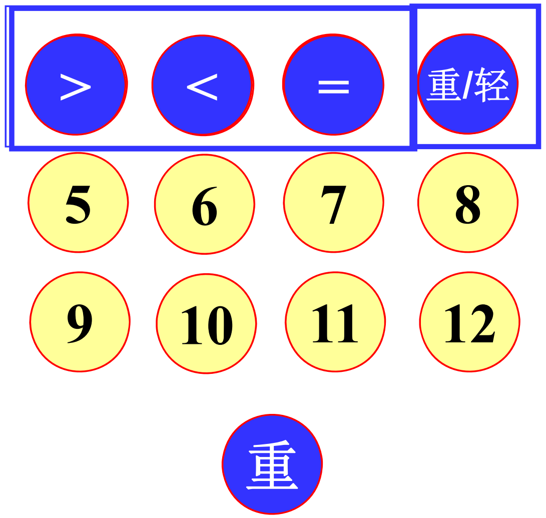
Beck J. *Combinatorial Games: Tic-tac-toe Theory*. Cambridge University Press, 2008.

伪币辨识

群试问题

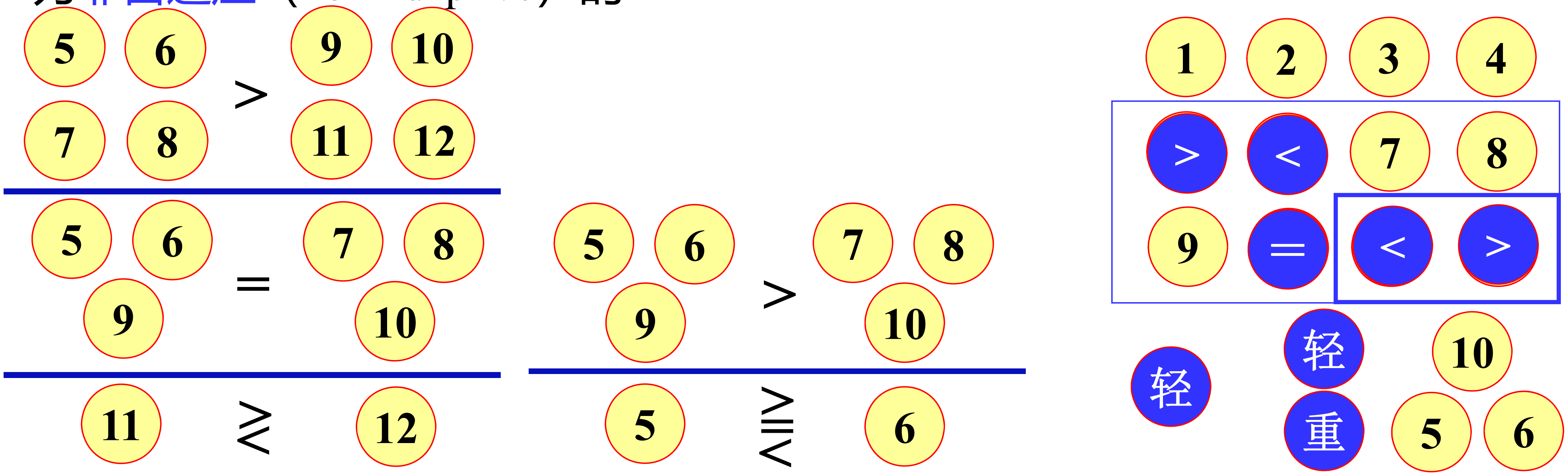
- 伪币辨识
  - 12枚外观相同的硬币中有一枚是伪币，伪币质量与真币不同
  - 天平一次称量只能比较两端质量大小，不能读出质量数值
  - 能否用天平称量三次找出伪币，并说明伪币相对真币偏轻或偏重





群试问题

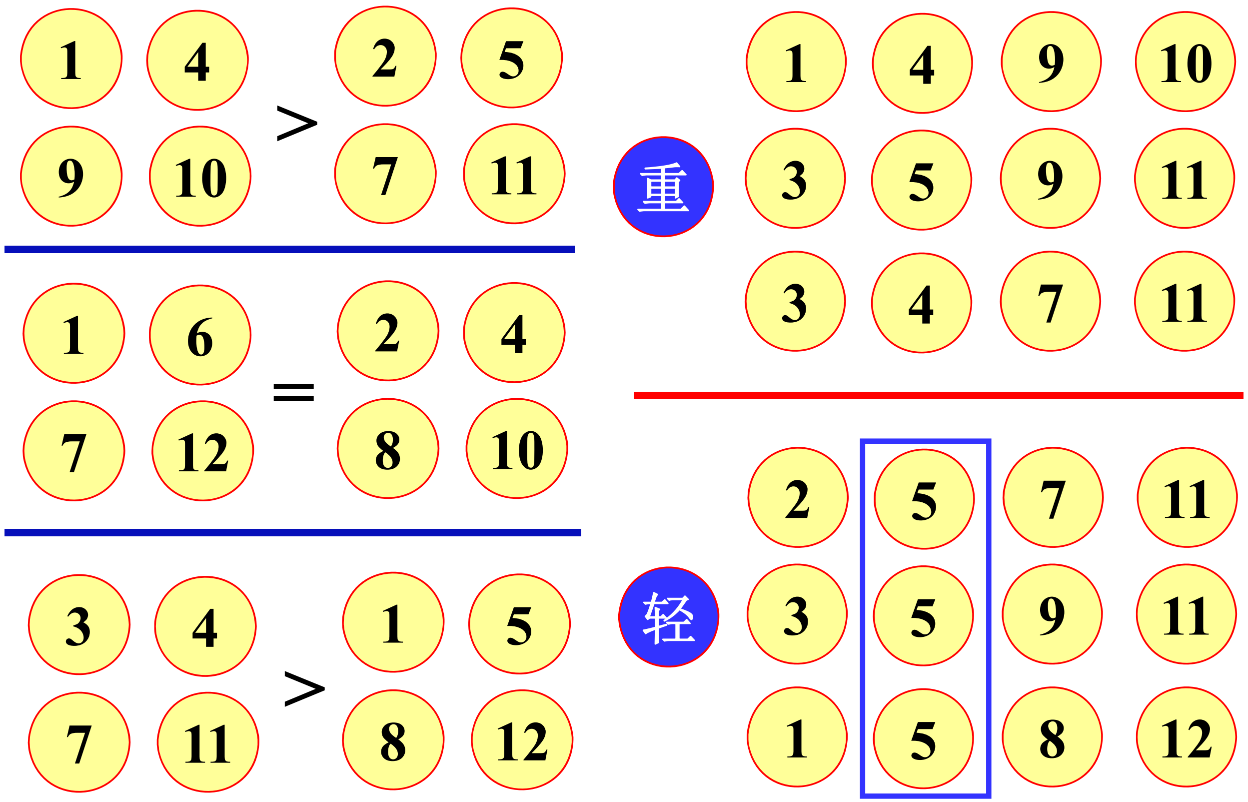
- 伪币辨识
  - 硬币真伪的可能性共有 $12\times 2=24$ 种。每一种称量结果对应一种可能性，不同称量结果对应的可能性各不相同
  - 后一次称量依赖于之前称量结果的方案为自适应（adaptive）的，否则称为非自适应（non-adaptive）的



非自适应方案

- 单伪币最优方案
  - 对任意整数 $w \ge 2$
    - 若 $3 \le n \le (3^w - 3)/2$，存在一非适应的称量方案，使用 w 次称量可从 n 枚硬币中辨别伪币并确定轻重
    - 若 $n > (3^w - 3)/2$，不存在自适应的称量方案，用 w 次称量即可从 n 枚硬币中辨别伪币并确定轻重

Freeman John Dyson
(1923-2020)
英裔美籍物理学家、数学家
英国皇家学会会员
1981年Wolf奖得主



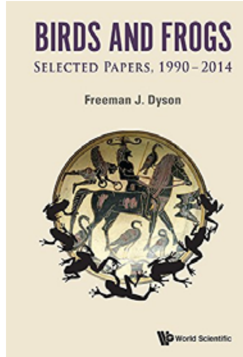
Dyson FJ. The Problem of the Pennies. ***The Mathematical Gazette*****, 30, 231-234, 1946.**

数学建模 MATH T

数学
建模
MATH T

科学家与作家

- 飞鸟与青蛙
  - 有些数学家是鸟，其他的则是青蛙
    - 鸟翱翔在高高的天空，俯瞰延伸至遥远地平线的广袤的数学远景。他们喜欢那些统一我们思想、并将不同领域的诸多问题整合起来的概念
    - 青蛙生活在天空下的泥地里，只看到周围生长的花儿。他们乐于探索特定问题的细节，一次只解决一个问题
  - 数学的世界既辽阔又深刻，需要鸟们和青蛙们协同努力来探索
    - 数学丰富又美丽，因为鸟赋予它辽阔壮观的远景，青蛙则澄清了它错综复杂的细节
    - 数学既是伟大的艺术，也是重要的科学，因为它将普遍的概念与深邃的结构融合在一起
    - 如果声称鸟比青蛙更好，因为它们看得更遥远，或者青蛙比鸟更好，因为它们更加深刻，那么这些都是愚蠢的见解



Dyson FJ, *Birds and Frogs: Selected Papers of Freeman Dyson, 1990–2014*, World Scientific, 2015

Dyson FJ. Birds and frogs. *Notices of the AMS*, 56(2), 212-223, 2009.（王丹红译稿）

科学家与作家

数学
建模
MATH T

René Descartes
(1596-1650)
法国哲学家、数学家

David Hilbert
(1862-1943)
德国数学家

Erwin Rudolf Josef
Alexander Schrödinger
(1887-1961)
奥地利物理学家

Bourbaki group（布尔巴基学派）

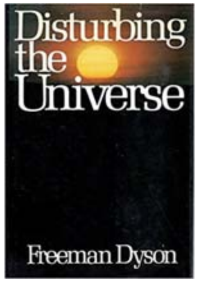
Hermann Klaus Hugo Weyl
(1885-1955)
德国数学家、物理学家

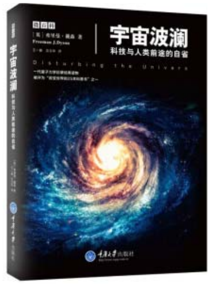
杨振宁
(1922-　)
中国物理学家

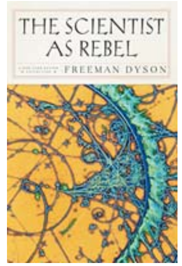
Yuri Ivanovitch Manin
(1937-　)
俄罗斯数学家

Francis Bacon
(1561-1626)
英国哲学家

Abram Samoilovitch
Besicovitch
(1891-1970)
俄罗斯数学家







Dyson FJ, *Disturbing the Universe*, Harper & Row, 1979.（中译本：宇宙波澜，邱显正译，三联书店**1998**年版，王一操、左立华译，重庆大学出版社**2015**年版）

Dyson FJ, *The Scientist as Rebel*, New York Review Books, 2006.（中译本：反叛的科学家，肖明波、杨光松译，浙江大学出版社，**2013**）

1996年第4届Lewis Thomas 奖得主

林开亮. 弗里曼· 戴森: 科学家与作家的一生. 科学文化评论, 10(3), 82-101, 2013.

Dyson集

数学
建模
MATH T

- Dyson集
  - 满足以下条件的 w 元向量子集 $S \subseteq \{-1,0,1\}^w$ 称为Dyson集
    - $\sum_{\mathbf{v}\in S} \mathbf{v} = \mathbf{0}$ 天平两端硬币数相等，结果由伪币位置决定
    - 若 $\mathbf{v} \in S$，则 $-\mathbf{v} \notin S$

      结果确定伪币及其轻重
  - 若存在含 n 个 w 元向量的Dyson集，则可用非自适应称量方案经 w 次称量从 n 枚硬币中辨别伪币并确定轻重
    - 每个向量代表一枚硬币在各次称量中的位置。称量结果必与伪币所在位置相对应

$(1,\ 1,\ -1)$	1	左	左	右
$(-1,\ -1,\ 0)$	2	右	右	
$(0,\ 0,\ 1)$	3			左
$(1,\ -1,\ 1)$	4	左	右	左
$(-1,\ 0,\ -1)$	5	右		右
$(0,\ 1,\ 0)$	6		左	
$(-1,\ 1,\ 1)$	7	右	左	左
$(0,\ -1,\ -1)$	8		右	右
$(1,\ 0,\ 0)$	9	左		
$(1,\ -1,\ 0)$	10	左	右	
$(-1,\ 0,\ 1)$	11	右		左
$(0,\ 1,\ -1)$	12		左	右
$(1,\ 0,\ 1)$		重	平	重

1 4 9 10 > 2 5 7 11

1 6 7 12 = 2 4 8 10

3 4 7 11 > 1 5 8 12

Dyson集

- Dyson集的构造
  - 令 $f:\{-1,0,1\}\to\{-1,0,1\}$，$f(-1)=0,\ f(0)=1,\ f(1)=-1$
    - $x+f(x)+f(f(x))=0$，$f(f(x))=x$
    - $f(-x)=-f(f(x))$，$f(-f(x))=-x$，$f(-f(f(x)))=-f(x)$
  - 令 $\mathbf{f}:\{-1,0,1\}^w\to\{-1,0,1\}^w$，$\mathbf{f}(\mathbf{x})=(f(x_1),\cdots,f(x_w))$
  - 记 $S(\mathbf{x})=\{\mathbf{x},\mathbf{f}(\mathbf{x}),\mathbf{f}(\mathbf{f}(\mathbf{x})),-\mathbf{x},-\mathbf{f}(\mathbf{x}),-\mathbf{f}(\mathbf{f}(\mathbf{x}))\}$
    - $S(\mathbf{x})$ 中向量两两不同
    - 对任意 $\mathbf{v}\in S(\mathbf{x})$，$\mathbf{f}(\mathbf{v})\in S(\mathbf{x})$
  - 记 $S^{+}(\mathbf{x})=\{\mathbf{x},\mathbf{f}(\mathbf{x}),\mathbf{f}(\mathbf{f}(\mathbf{x}))\}$
    - $\mathbf{x}+\mathbf{f}(\mathbf{x})+\mathbf{f}(\mathbf{f}(\mathbf{x}))=\mathbf{0}$，$\mathbf{v}$ 与 $-\mathbf{v}$ 在 $S^{+}(\mathbf{x})$ 中至多出现一次

x	-1	0	1
$f(x)$	0	1	-1
$f(f(x))$	1	-1	0
$f(f(f(x)))$	-1	0	1

$-x$	1	0	-1
$-f(f(x))=f(-x)$	-1	1	0
$-x=f(-f(x))$	1	0	-1
$-f(x)=f(-f(f(x)))$	0	-1	1

$$3\le n\le\frac{3^w-3}{2}\qquad \left|\{-1,0,1\}^w\right|=3^w$$

$$\mathbf{-1}=(-1,\cdots,-1)$$
$$\mathbf{1}=(1,\cdots,1)$$
$$\mathbf{0}=(0,\cdots,0)$$

如何在 $\mathbf{v}$ 与 $-\mathbf{v}$ 恰取一个的情况下保证 $\sum_{\mathbf{v}\in S}\mathbf{v}=\mathbf{0}$

$$\mathbf{v}_1+\mathbf{v}_2+\mathbf{v}_3=0$$

$(1,-1,0)\quad(-1,1,1)$

$(-1,0,1)\quad(0,-1,-1)$

$(0,1,-1)\quad(1,0,0)$

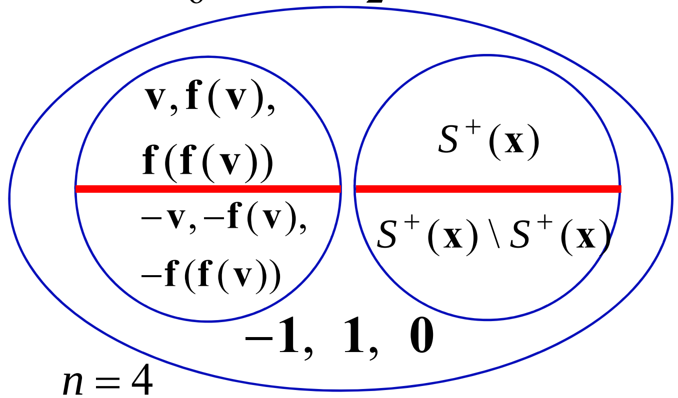
如何保证 $\mathbf{v}$ 与 $-\mathbf{v}$ 在不同的子集中不被重复选取

Dyson集

- Dyson集的构造
  - 寻找 $\{-1,0,1\}^w$ 中 $m=\frac{1}{6}(3^w-3)$ 个向量 $\mathbf{v}_1,\mathbf{v}_2,\cdots,\mathbf{v}_m$，使得

    $$\{-1,0,1\}^w = S(\mathbf{v}_1)\cup S(\mathbf{v}_2)\cup\cdots\cup S(\mathbf{v}_m)\cup\{\mathbf{-1},\ \mathbf{1},\ \mathbf{0}\}$$
  - 不同 n 值时的Dyson集
    - $n=3k, 1\le k\le m$： $S^+(\mathbf{v}_1)\cup S^+(\mathbf{v}_2)\cup\cdots\cup S^+(\mathbf{v}_k)$

$$\frac{3^w-3}{6}\times 3=\frac{3^w-3}{2}$$



$n=3k+2, 1\le k<m$

$$\begin{array}{ll}
(\ \ 1,\ \ 1,\ \ 1,\ \ 1,\cdots,\ \ 1) & \\
(\ \ 1,-1,\ \ 0,\ \ 0,\cdots,\ \ 0) & \mathbf{v}_1\\
(\ \ 0,-1,\ \ 1,\ \ 1,\cdots,\ \ 1) & -\mathbf{f}(\mathbf{f}(\mathbf{v}_1))\\
(-1,\ \ 1,-1,-1,\cdots,-1) & \mathbf{v}_2\\
(-1,\ \ 0,-1,-1,\cdots,-1) & -\mathbf{f}(\mathbf{f}(\mathbf{v}_2))
\end{array}$$

$S^+(\mathbf{v}_3), S^+(\mathbf{v}_4),\cdots,S^+(\mathbf{v}_{k+1})$

$$3(k-1)+5=3k+2$$

$n=3k+1, 2\le k<m$

$$\begin{array}{ll}
(\ \ 1,\ \ 1,\ \ 1,\ \ 1,\cdots,\ \ 1) & \\
(-1,-1,\ \ 1,\ \ 1,\cdots,\ \ 1) & \mathbf{v}_1\\
(-1,-1,\ \ 0,\ \ 0,\cdots,\ \ 0) & -\mathbf{f}(\mathbf{f}(\mathbf{v}_1))\\
(\ \ 0,\ \ 0,-1,-1,\cdots,-1) & \mathbf{f}(\mathbf{v}_1)\\
(-1,\ \ 1,\ \ 0,\ \ 0,\cdots,\ \ 0) & \mathbf{v}_2\\
(\ \ 1,\ \ 0,-1,-1,\cdots,-1) & \mathbf{f}(\mathbf{f}(\mathbf{v}_2))\\
(\ \ 1,\ \ 0,\ \ 0,\ \ 0,\cdots,\ \ 0) & \mathbf{v}_3
\end{array}$$

$S^+(\mathbf{v}_4), S^+(\mathbf{v}_5),\cdots,S^+(\mathbf{v}_{k+1})$

$$3(k-2)+7=3k+1$$

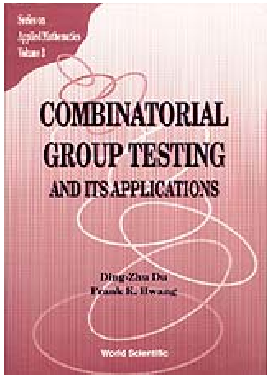
$n=4$

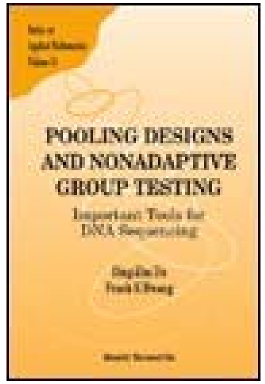
$$\begin{array}{l}
(\ \ 1,\ \ 1,\ \ 1,\cdots,\ \ 1)\\
(-1,\ \ 0,\ \ 0,\cdots,\ \ 0)\\
(\ \ 0,-1,\ \ 0,\cdots,\ \ 0)\\
(\ \ 0,\ \ 0,-1,\cdots,-1)
\end{array}$$

群试

数学建模 MATH T

- 群试（Group testing）
  - 组合群试
    - 假定 n 枚硬币中恰有 k 枚是伪币，如何用尽可能少的检测次数（在任何情况下）找出全部的伪币
  - 概率群试
    - 假定 n 枚硬币相互独立地以概率 p 可能是伪币，如何找出全部的伪币，使平均检测次数尽可能少





Du DZ, Hwang FK, *Combinatorial Group Testing and Its Applications*, World Scientific, 2000.
Du DZ, Hwang FK, *Pooling Designs and Nonadaptive Group Testing: Important Tools For DNA Sequencing*. World Scientific, 2006.

Dorfman R, The detection of defective members of large populations, *The Annals of Mathematical Statistics*, 14, 436–440, 1943

Robert Dorfman
（1916-2002）
美国经济学家


谢　谢