学科与专题介绍

随机性与伪随机性

Avi Wigderson

随机性的概念激起了千年来人们的好奇心，如像 “机会”,“运气” 等概念在日常生活与公众文化中起着重要作用. 在这篇文章里，我试图弄清楚关于随机性的含义和用途. 第 1 部分，我将描述各种可以认定为 *完全的* 随机性的应用，读者无疑熟悉其中的一些. 第 2 部分，我将描述 *伪* 随机性，即研究在非随机性 (或弱随机性) 结构中的具随机外形 (random-looking) 的现象以及它们的应用.

1. 完全随机性及其应用

设想完全随机性的最佳途径为一个 (任意长的) 硬币投掷序列，其中每个硬币是 *公平的*: 它有 50:50 出现头像 (H) 或背面 (T) 的机会. 而且每一次投掷都 *独立* 于其它的投掷. 因此 20 次硬币投掷结果的下面两个序列恰好有相同的概率 $(1/2)^{20}$:

HHHTHTTTHTTHHTTTTTHT 与 **HHHHHHHHHHHHHHHHHHHH**

应用上述硬币投掷的二元序列，我们可以用一个更大的 “字母表” 来生成其它的随机物，如投掷一个六面骰子，旋转一个赌盘，或一副 52 张纸牌的完全洗牌. 他们都是至今仍很流行的应用古典随机性进行赌博的方式之一. 当我们 (或赌场) 计算各种赌局中的胜负时，都隐含地假定了 (为什么？) 投掷 / 旋转 / 洗牌是完全随机的. 它们是这样的吗？现在让我们来观察随机性的另一些应用，并且对于每一种应用，你应该问问自己 (我将提醒你) 完全随机性从何而来.

a. 统计

假定全体美国人民 (超过 3 亿) 要在红与蓝中做出一种选择. 如果我们想要知道选择红的 *确切* 人数，则我们必须询问每一个人. 但是如果我们仅满足于知道一个 *近似值*, 例如允许 3% 的误差，则可像下面这样 (远为省钱的方法) 进行. *随机* 取一个 2000 人的样本，并只询问他们的选择. 一条称为 “大数律” 的数学定理保证了样本集合中选择红色的比例与整个人民中选择红色的比例相差不超过 3% 的概率为 99%. 值得注意的是，保证了 99% 的 *置信度* 及 3% 的 *误差* 参数的 2000 人的样本量完全不依赖于人口总量！

如果全世界人民 (超过 60 亿) 进行选择，甚至整个宇宙的原子来进行选择，同样的样本量也就够了. 定理的关键是 2000 个样本在整个选择人群中是完全随机的. 思考：许多测量和选择，以及医学和科学实验的总体里运用的这种抽样，它们的完全随机性的出处是什么？

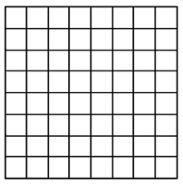

图 1

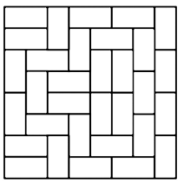

图 2

b. 物理与化学

考虑下面的问题：给你一个如图 1 的区域. 这个区域的一个多米诺骨牌式的贴砖将该区域分割为 2×1 的许多长方形 —— 图 2 给出了一个这种分割的例子. 问题：一个给定的区域有多少种不同的多米诺贴砖分割？更重要的是计算部分分割 (容许有一些空洞) 的个数. 除了令人感兴趣的表象外，这样的一些计数问题则是物理与化学探索事物性质基本问题的核心. 这个问题被称为 "单体 – 二聚物 (monomer-dimer) 问题", 并与晶体表面的双原子分子 (diatomic molecules) 的组织有关. 一个区域的长方形贴砖分割的个数决定了这种形状的晶体的一些热动力学性质. 但是即便对于小区域，这种计数问题亦非平凡，而对于感兴趣的大区域，欲检查所有可能性，即使最快的计算机也永远算不到头. 然而再一次地，如果你只要一个估计 (对科学家来说，它常常已经足够了), 则可以通过所谓的 "蒙特卡罗方法" 得到这样一个有高置信度的估计. 蒙特卡罗方法是由 Nicholas Metropolis (米特罗波利斯), Stanislaw Ulam (乌拉姆) 与 John von Neumann (冯·诺依曼) 发展起来的. 这是一个聪明的概率算法，它在所有可能的长方形贴砖的地方进行 "随机游走", 但仅仅走过它们中的少数几个. 它关键性地依赖于完全随机选择. 这个方法 (及许多其它概率算法) 的众多应用中，随机性取自何处？

c. 网络拥塞

设想一个拥有上百万个节点与链接的大网络：它可以是道路、电话线路、或符合于我们目的的最佳对象 —— 互联网. 当有一个很大的交通流量 (汽车 / 通话 / 电子邮件) 时，大量交通流经的节点以及链接就会产生拥塞. 确定使拥塞达到极小的最佳方案是什么？这个问题的主要困难为汽车 / 通话 / 发电子邮件到何处的决定是个人的，无通盘安排的. 不难看出 (在适当的网络中), 如果许多出发点 – 终点这种偶对是随机的，则几乎可以确定，在 *每一个* 节点拥塞是很小的. 然而，我们往往不是随机地选择我们的走向，或随机地打电话：我打给我的朋友，你打给你的朋友，在这种情形下高度拥塞肯定会产生. 为了改进这个问题, Leslie Valiant (瓦林特) 提出了如下在实际应用中的天才想法. 每当 A 要给 B 发送电子邮件时，她将选取一个随机的中间人 C, 而将电子邮件发给 C, 并要求 C 将电子邮件转发给 B (忘掉隐私及意愿，它们与此无关). 尽管电子邮件的数目加倍了，但瓦林特证明了 (在适当的网络中) 拥塞度以很高的概率降低了一个大因子. 再次表明，对于这个解决办法是否有效而言，完全随机性和不同抉择的独立性是本质的.

d. 对策论

有时不仅对于某些工作 (如前述诸例) 的效率改进需要有完全随机性，而且对一些基本概念的深入了解亦然. 这种概念之一是作为经济学与决策论基础的 "合理行为". 设想有一个由各个集团 (例如某人群，公司，国家等等) 组成的集合，进行着策略交互作用 (例如交通、价格竞争、冷战), 其中任何集团都影响每个集团的结局. 每个集团都有一个可供选择的策略集合，并且每一个策略的选择将决定对于每一个集团的 (正或负) 值. 所有集团都有这个信息 —— 什么行为的集合将构成对他们全体都是合理的行为？John Nash (约翰·纳什) 60 年前就表述了他的 (赢得诺贝尔奖的) 概念 "纳什平衡", 它今天已被广泛

认同. 对于一个策略集合 (每个集团一个策略), 如果没有一个集团可以用转换其策略为另一策略，在其他所有集团的已给定策略的条件下而改进其值 (否则这对该集团改换策略将是合理的了！), 则这个策略集合就被称为纳什平衡. 尽管这是一个自然的稳定性概念，但首先要问的问题是：哪些对策 (如上述策略情况) 具有这样一个合理平衡解？纳什证明了，只要诸集团能够投掷硬币 (即用随机的方式来作决策 —— 校注), 则不论有多少集团，每个集团有多少策略，以及每个集团给出他们的策略选择后得到什么值 . . . *每一个* 策略都有纳什平衡！即，容许 *混合* 策略，集团可以 (明智地) 从他们可选的策略中随机地选取一个，这样使这个概念一般化，使它可用于每个对策之中！在这里又要问：在所有这些情况下，集团需要做他们的硬币投掷吗？

e. 密码学

作为今天计算机安全与 e–贸易理论基础的这一领域，或许能最好地表明在我们的生活中随机性是如何不可或缺的. 首先，在密码情形中，有一些 *秘密* 某些人是知道的，而另一些人是不知道的. 这是什么意思？ “秘密” 是另一个基本概念，它的定义本身就需要随机性. 这样的一个定义是由 Claude Shannon (香农), 这位信息理论之父给出的，他用另一个基本概念 *熵* 来量化不确定性 (即我们 *不知道* 的程度), 而熵则需要所处理的对象是随机的.

例如，若我从长度为 10 的所有十进制数中完全随机地抽取一个作为密码，则你猜出它的机会正好是 $1/10^{10}$. 但如果我从我的朋友的电话号码 (亦是一些十位数) 集合中随机选取密码，那么你的不确定性就大为减小了：猜出我的秘密的概率就加大了，即

$$1/\text{我的朋友的人数}$$

(是的，密码学假定除了我投掷硬币的结果外，我的对手知道我的每件事). 然而秘密刚开始：*所有的* 密码协议，如公钥加密、数字签名、电子货币、零知识证明等等，皆完全依赖于随机性，因而没有在确定性世界里的安全类似物. 当你联机登录、发送电子邮件、网络购物等，你需要在日常生活里用到这样的协议. 由于这些协议的要求，你的计算机怎样投掷硬币？

2. 伪随机性

a. 随机性的一个计算观点

欲回答上面反复提出的问题，我们必须仔细研究一下随处可见的随机事物：硬币投掷. 它是随机的吗？理论计算机科学的一个关键理解是，这个答案依赖于谁 (或哪一种应用) 使用它！为了阐明这个道理，我们将进行几个 (心智的) 实验. 设想我的手中握有一个 (合格的) 硬币，在我将它向空中高高抛掷的一秒钟后，假设要你 (你正在看着我) 猜当它落到地板上时的结果，那么你的猜测为正确的概率是多少？你说 50:50? 我同意！现在考虑同一个实验的另一种形式，其中仅有的差别是你可以用一台便携式电脑来帮助你. 那么此时你猜对的概率是多少？我确信你会再说 50:50, 我会再次赞同. 便携式电脑如何能帮上忙？如果你将它联接到一个超级计算机上，而该计算机又与一些录像机以及房间周围的一些传感器相联接，又将如何呢？现在你的猜测正确的机会是多少？事实上，它

应该是百分之百．这个装置在一秒钟内算出所需要的所有信息是轻而易举的：硬币的速度、方向、角动量、我的手到地板的距离、空气的湿度等等，并将正确的答案提给你．

在所有 3 种实验中，都是投掷硬币，但观察者改变了，结果的不确定性依赖于观察者．随机性是在旁观者眼里，或更精确地说，是在计算的能力之中．如果我们投掷多个硬币，情况亦然：对一个已知的观察者 / 应用程序来说，结果有多大的不确定性依赖于他们如何处理它．因此，一个现象 (自然的或人为的), 如果我们所关心的观察者 / 应用程序的群体不能把它从随机中区分出来，那么就可以认为它是 “足够随机” 或 伪随机 的！由 Manuel Blum (布鲁姆), Shafi Goldwasser (戈德瓦塞尔), Silvio Micali (米凯利), 以及 Andrew Yao (姚期智) 在 1980 年代早期发展起来的这个观点标志着与较老的观念的显著分离，并导致密码学成为计算机科学中有重大突破的唯一领域．另一方面，像 “蒙特卡罗方法” 那样，导致了对概率算法中随机性的能力有了一个非常好的理解．它们是真的需要随机性，还是需要对于求解单体二聚物问题及其许多姊妹问题有着等同效率的确定性的方法？令人惊奇的是，对于后者我们现在有了很强的证据，指出在这样一些算法框架中随机性的不足．Russel Impagliazzo (因帕利亚佐) 与 Wigderson (威格森) 的一条定理证明了，假定 任何 普通的计算问题是难处理的 (广为相信的以及与 P$\neq$ NP 猜想有关的一些东西), 则随机性没有能力提升算法效率！每一个概率算法都可以被换成一个有类似效率的确定性算法．证明的关键在于伪随机生成元的构建，而这些生成元所产生的序列是不能用这些算法把它们与随机性区分开来的．

b. 确定性过程与结构的类随机 (random-like) 行为

一个聪明的观察者会如何去分辨随机与非随机事物？一个最自然的答案是，寻找在随机事物中极其可能具有的那些 “模式” 和性质，并看看是否所给事物中含有它们．上面提到的定理允许观察者去检验 任何 一个这种性质，只要这个检验是有效的．但是对于许多实际目的来说，仅需事物有 一些 有用和有兴趣的这种性质就足够了．数学和计算机科学中有大量的例子．这里是一个例子：随机网络的一个性质是，要想切断它 (将它分拆为两个或多个大块), 我们就必须切断它的许多链接．这个性质在通讯网络中是极为期待的，并要使它们能够容错．我们能否确定性与有效性地构造出具有这样一个类随机性质的事物？

这个问题已由数学家和计算机科学家在设法解决，他们的工作极其相似，然而具有不同的成功构造，例如在数学方面有 Gregory Margulis (马古利斯), Alexander Lubotzky (鲁波茨基), Ralph Philips (菲利普) 和 Peter Sarnak (萨纳克), 而在计算机科学方面则有 Omer Reingold (莱因戈尔德), Salil Vadhan (伐德汗) 与威格森．一个更为基本的容错事物是一个 纠错码—— 一个发码者可以在受到一些噪音影响下发出密码信息，而收码者可以成功地清除错误从而确定出原始讯息的方法．香农定义了这些重要的对象，并证明了一个随机码是纠错码．但是很明显，对于应用，我们需要有效地构造出一个纠错码！另外，今天已经知道了许多不同的确定性构造，而如果没有它们，则从人造卫星到手机到 CD 与 DVD 播放机等我们每天依赖的大量应用，都完全不存在！

数学家与计算机科学家通常从不同途径证明确定性系统与结构具有类随机性质. 在数学方面, 过程和结构与由数论, 代数, 几何等产生的领域有着有机的关联, 证明它们有类随机的性质部分出于对它们如何理解. 在计算机科学方面, 人们通常从一些性质 (它们在实际中是有用的) 出发, 并试图有效地构造出它们所具有的确定性结构. 这些分析与综合的方法常常会汇合并相互提升 (正如我们将在下一节举例说明的). 旨在在伪随机性研究中探索和统一这种联系的一项国家科学基金最近授予了高等研究院数学学院的 Jean Bourgain (布尔甘), 萨纳克, 因帕利亚佐和威格森 (见封页的介绍 [1]).

c. 随机性净化

回到对 *所有* (而非特殊) 应用规定完全随机性的问题, 现在我们对于观察者的计算能力不加限制. 由于真正的随机性不能被确定性地生成, 于是人们不得不假定一些可能不完全的源自随机硬币投掷的东西. 人们能够确定性地和有效地将一个不完全的随机源转换到一个完全的随机源吗? 我们应该如何构建不完全随机性的模型呢?

自然的经验提供了一些线索. 不用进入关于宇宙是确定性的还是概率的 (有趣的) 哲学讨论, 我们常见的许多现象似乎至少是部分地 *不可预测的*. 这些现象包括天气、股市的波动、太阳黑子、放射性衰减等. 因此, 我们可以假设, 任何的这种现象, 它们的一系列结果都含有某种熵 (但该熵存在何处我们没有线索). 抽象地, 你可设想一个对手在做一系列硬币投掷, 但却总可以用任何方式选取每次投掷的偏倚 —— 头像的概率可以设定为 $1/2, 1/3, 0.99$. 或者甚至 $1/\pi$, 但不能是 0 或 1 (这将导致 0 熵). 进而言之, 这些概率可以任意地相关 —— 对手可以视过去的投掷来相应地决定下一次的投掷的偏倚. 我们可以有效地使用这样一个随机性的不完全源去生成一个完全的随机性吗? 正如 20 年前 Miklos Santha (桑沙) 和 Umesh Vazirani 所证明的这个 (非平凡的) 答案是否定的, 他们定义了这些源, 推广了冯·诺依曼的一个简单模型. 尽管在一个方向上希望破灭, 但在另一个方向他们又给出了希望: 证明了如果你有 *两个* (或更多) 这种相互独立的源, 则 *原则上* 人们可以利用它们一同去确定性地生成完全随机性. 举例来说, 倘若天气、股市、太阳黑子互不影响, 我们就能希望将他们的行为联合到一个硬币投掷的完全系列中去. 所缺失的是这样一部随机性净化器 (或计算机科学行话中的 *析取器* (*extractor*)) 的有效构建.

这个老问题的解答最近由数学家与计算机科学家结合了分析方法与综合方法而得到. 一些时间前, David Zuckerman (朱克曼) 提出了下面的想法: 假定 A, B 与 C (分别) 表示我们的天气、股市和太阳黑子的样本的输出 (设想他们为整数 [2]). 他猜想算式 $A \times B + C$ 的输出比任何输入有更高的熵 (将更加随机). 如果真是这样, 则迭代 (带有更加独立的弱源的) 这个程序将最终生成一个 (近似的) 完全随机数! 朱克曼证明了这个概念来自一个著名的数学猜想. 尽管这个数学猜想仍未解决, 但最近却在一个完全不同的猜想上由布尔甘, Nets Katz (卡茨) 和 Terence Tao (陶哲轩) 取得了进展 (推广了 Paul Erdős 和 Endre Szemerédi 的工作). 他们研究了随机 *表格* 的性质, 试图在特定的算术表

1) 见本期文 "计算难及性与伪随机性". —— 编注
2) 实际上它们应取自模某个大素数 p 后的数, 而往后的所有算术都应该在 $\bmod p$ 之下进行.—— 原注

格，即熟悉的加法和乘法表格中去寻找这些性质．这里是他们研究这些性质的一个直觉的描述．考虑在一张表格中的一个小窗 (图 3).

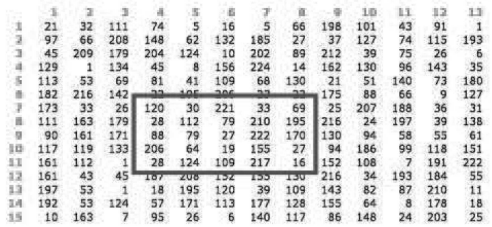

图 3　一张随机表和一个典型的窗口

如果在其中仅有 “很少” 的数出现多于一次，则称这样一个窗口是 *好* 的．不难证明，在一张随机表中，*所有的* 小窗口都是好的．现在看看加法表和乘法表是怎样的呢？非常容易看出每一张表中都有一些坏窗口！[1] 不管怎样，布尔甘，卡茨和陶哲轩证明了，当两张表 *取在一起* 时，则它们在下面的意义下是好的 (图 4): 对于每一个窗口，它或者在乘法表中或者在加法表中 (或在两者中) 是好的！Boaz Barak (巴拉克), 因帕利亚佐，以及威格森给出了这个结果的一个统计学版本，并利用它证明了朱克曼的原始析取器是有效的！

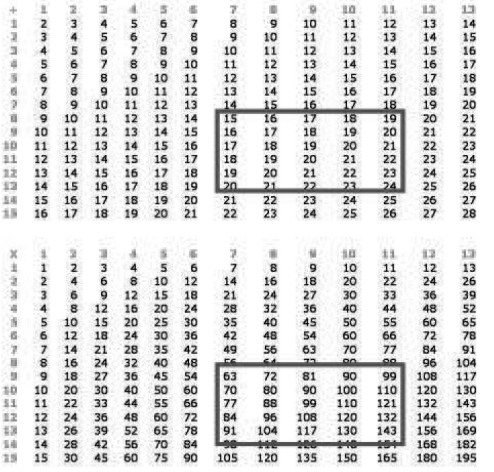

图 4　加法表与乘法表

上面的故事只是一个例子．数论与代数几何中的基本结果，主要是多项式方程的有理解的 “类随机” 行为 (由 André Weil (韦伊), Pierre Deligne (德利涅), Enrico Bombieri (邦别里) 与布尔甘得到的) 最近被大量地用于改造析取器，在各种不同背景中净化了随机性.

d.　伪随机性的百万美元问题

数学与计算机科学中的两个最著名的未决问题，即黎曼猜想与 P 对 NP 问题，都可以被陈述为有关的伪随机性问题．这是 7 个克莱千禧年问题 (Clay Millennium problems) 中的 2 个，每个问题的解答将得到 100 万美元的奖金 (对于这些问题以及挑战言辞的非常好的叙述可见 www.claymath.org/millennium). 尽管随机性完全不是它们通常描述的一部分，但它们却都可以被表现为关于伪随机性的问题．在这 2 种情形，随机结构的具体性质要在特定的结构中去寻找.

关于 P 对 NP 问题，其关联相对容易解释．该问题探索了正常问题的计算难度．容易看出 *随机* 问题[2] (几乎肯定) 很难求解，而 P 对 NP 问题要求对某些 *明确* 的问题，诸如 “流动推销员问题” (即给予一张标有每两个城市间距离的大地图，求恰好通过每个城市一次的最短路径), 去证明同样的事.

现在让我们来仔细讲述黎曼猜想与伪随机性的关联 (在本期封面中解释过 (见 p.4 脚注 —— 编注)). 考虑 3 个字母 L, R, S 的长序列，如

SSRSLLLLLSLRRLSRRRRRSLSLSLL...

这样一个序列可以设想为一个人或机器人在一条直线上游走的一个指令集合 (L 表

1) 若一个窗口的行和列是算术级数，则加法表是坏的．若他们是几何级数，则乘法表是坏的.—— 原注
2) 它须被正式地定义.—— 原注

示向左, R 表示向右, S 表示停留). 每一次，下一个指令指示他向右，向左挪动一个单位长度或停留不动. 如果这样一个序列被 随机地 选取 (有时称为随机游动或醉汉游走 [1]), 则移动体将以高概率停留在与原点的相对近处. 如果序列包含 n 步，则几乎肯定它与起始点的距离接近于 $\sqrt{n}$. 对于黎曼猜想，这个明确的指令序列被称作 Möbius (默比乌斯) 函数，它在每步 t 的定义如下：若 t 被任何素数的大于一次的方幂整除，指令则为停留 (例如 $t = 18$, 它被 3^2 整除), 否则，若 t 被 偶数 个不同素数整除，指令则为向右走一步，而当 t 被 奇数 个不同素数整除时，指令则为向左走一步 (例如，对于 $t = 21 = 3 \times 7$, 向右走；对于 $t = 30 = 2 \times 3 \times 5$, 向左走). 这个由素数决定的明确的指令序列致使一个机器人似醉汉游走，当且仅当黎曼猜想成立. [2]　　(王元　译　　胥鸣伟 陆柱家　校)

****

(上接 29 页) **答**：我们谁能怀疑费马？费马，他是一个非常聪明的人. 这是毫无疑问的.

问：但你真的不相信他给出过证明吗？

答：或许他有过，但他没有能找到足够的地方把它写下来，或者是他后来发现他原来的想法不完全正确. 但我觉得他不像是已经有了证明，因为在那个时期，人们几乎对代数数一无所知. 如果每个代数 (整数) 环都有漂亮的欧几里得算法，那么他还是可能构作出一个证明的，但是事实上存在欧氏算法的环是极少的.

问：我们想以下面的问题来结束对你的采访：依你之见，如何刻画一个罕见的高水平的数学家的特征？

答：想象力，足智多谋，对各种关系和模式的感觉，都是重要因素. 百折不挠加上耐心也很重要. 无须说，你还需要有充沛的精力. 最后，我想有点运气也是不可少的. 是的，有的人能走运多次，有的人只走运一次，而有的人也许从来没走过运. 我的意思是，有时我看到有的人已经有了好想法，甚至是非常棒的想法，但到最后是无果而终. 我也看到过这样的例子：有的人的想法似乎并不好或者说并不令人兴奋，而他却神奇地导出很有趣的结果. 我知道一些人，他们似乎有很多好想法，数学知识也很渊博，但从来没有得到令人兴奋的结果. 我也遇见过一些人，我在跟他们交谈时，并不认为他们特别聪明，他们常会以笨拙和不太漂亮的方式提出一些东西，但最后却导致了特别重要的结果. 所以，我不敢来定义什么是数学才能的本质了. 它涉及的方面太多，包含了太多的变数.

致谢、参考文献　(略)　　(冯绪宁　译　　袁向东　校)

更正启事　本刊 2009 年第 4 期刊出的 “数的主人 Atle Selberg 的生活与数学 (I)” 中，p.357 正文第 3 段中的 “他想到了研究黎曼 Zeta 函数的零点是一个重要题目” 应更正为 “他想到了研究黎曼 Zeta 函数的零点可作为一类矩问题来研究”; 同一段中的 “由此又导出具有正实部的零点必位于临界线上” 应更正为 “由此又导出零点中占有非零比例的一部分位于临界线上”.　　—— 本刊编辑部

1) 见本期文 “计算难及性与伪随机性” 的脚注.—— 编注

2) 记 $\mu(t)$ 为默比乌斯函数，则移动体行走 n 步后，与原点 (出发点) 的距离为 $M(n) = \sum_{t=1}^{n} \mu(t)$. 我们可以类似于素数定理来证明，黎曼猜想成立的充要条件为 $M(n) = O(n^{1/2+\varepsilon})$. 此处的 ε 为给予的正数，而与 O 有关的常数仅依赖于 ε. (参见华罗庚：《指数和的估计及其在数论中的应用》，第 3 章：科学出版社, 1963).—— 译注