

随机：乱敲键盘能敲出什么

从一串乱码到量子噪声，一个工程师能摸到的偶然

J

费曼式写法 · 由多个 AI 代理撰写与互相审校

导读

从一串乱码到量子噪声，一个工程师能摸到的偶然

这本书的种子，是一串有人在键盘上乱敲出来的字符：

sa de er ge d sa de tu ba

没有主题，没有寓意，连作者都是「手滑」。但它逼出了一个值得写一本书的问题：**随机到底是什么？**是本性的世界，还是我们的无知？是一堆噪声，还是一种可以利用、甚至必须依赖的资源？

先给你两个反直觉的入口：

- 圆周率 π 的小数点后一亿位，看起来比任何乱码都乱——但它一点都不随机，因为一段几十行的程序就能把它完整写出来。「乱」和「随机」是两回事，差在能不能被压缩。
- 赌场的轮盘每一次都不可预测，赌场的利润却比水电费还稳定。单次越不可测，长期越可测——这不是悖论，是随机性最深的脾气。

这本书的路线是这样的：前两章把「随机是无知还是本性」掰开——硬币、拉普拉斯妖、混沌；第三到第五章看随机的统计铁律——为什么洗牌只会越洗越乱、为什么大数必然沉淀、为什么钟形曲线到处都是；第六章调转枪口看人脑，为什么我们总是看错随机；第七到第九章钻进工程——计算机怎么假装随机、真随机从哪里来；最后三章看用途——怎么拿随机算 π 、怎么拿它当密码学的命根子、以及在一个充满运气的世界里怎么做决定。

写法上有个承诺：不用大词。每个专业名词第一次出现，都会当场用大白话讲清楚；能用一个精准类比讲透的，绝不堆定义。你不需要任何概率论基础，只需要一点点「较真」的耐心。

读完全书，希望你能回答那个贯穿始终的问题，并且对两件事产生永久的免疫力：一是看到「太巧了」时的脊背发凉，二是听到「该反转了」时的心动。这两种感觉，都是噪声在给你讲故事。

现在，从那一串乱码开始吧。

第一章 · 一串乱码

这本书是从一串乱码开始的：

sa de er ge d sa de tu ba

这是有人在键盘上随手敲出来的。没有含义，没有出处，看起来什么都不像。可就是这个「什么都不像」，值得停下来问一句：**我们凭什么说它「乱」？**「乱」到底是一种可以定义、可以测量的性质，还是只是「我看不出规律」的另一种说法？

这一章就把这个感觉逼到墙角：随机，到底是个东西，还是只是个借口？

第一直觉：看不出规律

问十个工程师「这串字符随机吗」，九个会说「看起来挺随机的」。追问一句「什么叫看起来」，答案通常是：看不出规律。

这个直觉很好，但有个漏洞：**「看不出」是主观的**。给你两串数：

3 1 4 1 5 9 2 6 5 3 5 8 9 7 9

7 2 9 0 4 6 1 8 3 5 7 2 0 4 9

哪串更随机？多数人会说第二串——第一串开头几个数「太顺了」。但第一串是圆周率 π 的小数部分，从第一位开始，一位不多一位不少，是数学里确定得不能再确定的东西；第二串才是我瞎敲的。看出规律与否，取决于你认不认识那个规律。所以「看不出规律」定义不了随机，它只定义了「你不知道规律」。

换个问法：这串东西能不能被压短

把「有没有规律」换成一个能动手操作的问题：**这串字符能不能用更短的话完整描述出来？**

比如 `abababababababab`，十六个字符，但你不需要记住十六个字符，只要记住「ab 重复八次」——七个字。再比如 `3.1415926535...`，圆周率小数点后一百万位，听起来信息量大得吓人，但一段几十行的程序就能把它全部算出来。它的「描述」很短。

反过来，`sa de er ge d sa de tu ba` 这串，你想向别人完整复述它，除了把每个字符原样报一遍，没有更省事的办法。压不短。

大白话

大白话：一串东西的「规律含量」，可以用「最短的完整描述有多长」来量。描述越短，规律越多；描述跟原串一样长，就是没规律——这就是我们直觉里的「随机」。

这个想法被形式化之后叫 柯尔莫哥洛夫复杂度——大白话讲，就是「能生成这串东西的最短程序的长度」。按这个定义，**随机串就是「最短的程序就是把串本身打印出来」的那种串**。圆周率不随机，因为程序很短；你乱敲的那串很随机，因为没法压缩。

这个定义漂亮极了，还给出了一个反直觉的推论：绝大多数字符串都是随机的。道理是简单的计数——长度能省一位以上的描述，总数就那么些，根本不够分给所有字符串。所以「乱」不是个例，「乱」是常态，「有规律」才是稀有的意外。

泼一盆冷水：这个定义算不出来

别急着高兴。柯尔莫哥洛夫复杂度有个要命的性质：**它是不可计算的**。不存在一个通用程序，你扔给它任意一串字符，它告诉你最短描述有多长。粗略地说，要证明「没有更短的描述了」，你得排除所有可能的压缩方案，而这比把宇宙算一遍还难。

所以现实里我们退而求其次，用的是一堆**统计检验**——大白话讲，就是拿一堆「随机串应该有的样子」去对：0 和 1 是不是大约各一半？连续三位相同的频率是不是在正常范围？有没有藏着的周期？通不过检验的，肯定不随机；全部通过的，也只能说「我们没抓到它的规律」，不能说它真随机。

大白话：证明一串东西随机，基本做不到；证明它**不**随机，只要抓到一个规律就够了。所以随机的「判定」永远是单向的——只能证伪，不能证实。

那串乱码的判决

回到开头那串字符。它压不短（我们想不出比原样复述更省的描述），它也没有什么统计上的可疑之处。按我们能用的所有判据，它是随机的。

但注意第三章会见面的一个事实：这串字符是**人**敲的。人是个糟糕的随机源——手指会下意识交替、会避开同一个键连击、会偏爱键盘中间的位置。真要较真，「人随手敲的乱码」和「掷骰子掷出来的乱码」在统计上是分辨得出来的。人以为自己在制造随机，其实制造的是「自己觉得像随机的东西」。

这带来一个贯穿全书的问题：**随机到底是世界本身的性质，还是我们对世界无知的度量？**硬币落地是哪一面，是「随机的」，还是只是「你算不过来」？下一章，我们从一枚硬币开始，把这个问题掰开。

第二章 · 无知还是本性

抛一枚硬币，正面还是反面？我们脱口而出：随机的，各一半概率。但这一章要较个真：硬币落地之前，答案其实已经写好了吗？

硬币其实是一台机器

把抛硬币放慢一万倍看：手指给它一个初速度和一个翻转的角速度，它在空中转若干圈，落进手心，可能还会弹一下。整个过程没有一步是「碰运气」——空气阻力、重力、弹性碰撞，全是牛顿力学管的事。理论上，只要你知道**每一个**初始条件——速度精确到小数点后无穷位、气流、桌面的硬度——你就能算出结果。

有人真干过这事。数学家 Persi Diaconis（他同时是职业魔术师，靠手熟能控制硬币翻转次数）带团队造了台抛硬币机，用机器固定初始条件抛硬币，结果硬币每次都落在同一面。他们还发现人手抛的硬币有个约 51% 的小偏差：更可能落在抛起时朝上的那一面——因为「空中翻转」和「落下时朝哪面」之间有微妙的力学耦合。

大白话

大白话：硬币不掷骰子。它每一次的结果都被初速度、角度、气流算死了。我们说它「随机」，只是因为我们的手控制不了那么精确、眼睛也算不了那么快。

拉普拉斯妖：把「无知」推到极致

1814 年，拉普拉斯把这个想法推到了头：想象一个智力无边的存在（后人叫它 拉普拉斯妖——大白话讲，就是一个知道宇宙中每个粒子此刻的位置和速度、并且算力无限的超级大脑）。对它来说，上一章那串乱码不随机，硬币不随机，明天上海的天气不随机——**一切都已经写好，它只需要往前算**。在这个图景里，随机性根本不存在于世界中，只存在于「算不过来」的生物的脑子里。

这就是第一章那个问题的第一种答案：**随机 = 无知的度量**。概率论在经典世界里不是关于世界的学问，是关于「我们缺多少信息」的学问。我们说「正面概率 1/2」，翻译过来是「在

我掌握的信息下，我没有理由偏向任何一面」。

混沌：给无知加了个放大器

如果故事到此为止，那随机就只是个工程学问题——只要测量更准、算得更快，无知总能缩小。但二十世纪发现的混沌给这条路判了死刑。大白话讲，混沌系统是「误差会指数放大的系统」：初始条件差一丁点，结果差出去十万八千里。

气象学家洛伦兹 1961 年意外撞见了它：他把天气模拟的一个中间值从 0.506127 四舍五入成 0.506 重新跑，结果天气走向了完全不同的剧本。差在小数点后第四位，几周后的模拟里就是晴天和风暴的区别。这就是后来叫「蝴蝶效应」的东西。

关键在数学上：混沌系统的误差按 e 的 λt 次方 增长， λ 是正的。这意味着**测量精度每提高十倍，你能预测的时间只延长固定的一小段**。想预测明年的天气？你需要的初值精度超过原子的尺度——而量子力学（第九章见）从根本上不许你测那么准。所以混沌不是「我们还不够努力」，而是「努力也没用」：初始条件里藏着的那点不确定，会被系统本身放大成宏观的不可预测。

所以硬币到底随不随机

现在可以给硬币一个诚实的判决了：

- **本体上**：经典力学里，硬币是确定的。结果在离手那一刻已注定。
- **实践上**：由于混沌放大，任何物理上可行的测量精度都撑不起长期预测。骰子、轮盘、洗牌同理——它们都是小型混沌系统，这就是为什么赌场敢靠它们吃饭。
- **认识上**：「概率 1/2」是我们对信息缺口的诚实记账，不是世界的内在属性。

注意这个结论的形状：第一章问「随机是本性的还是我们的无知」，经典物理给出的答案是「无知——但是一种**原则上也消除不掉**的无知」。混沌像一台放大器，把任何微小的不确定放大成现实的随机。至于世界在底层（量子层面）是不是真的掷骰子，先卖个关子，第九章专门讲。

下一章换个角度：不看单次，看整体。为什么一副新牌洗着洗着就乱了、却永远不会自己洗回去？那里藏着随机最深刻的统计规律。

第三章 · 洗着洗着就乱了

一副新牌，出厂时是按花色和点数排好的：黑桃 A 到 K，红桃 A 到 K……你拿去洗，洗一次，乱一点；洗七次，基本全乱。然后你接着洗，洗到天荒地老——它永远不会自己洗回出厂顺序。为什么？洗牌这个动作又不认识「出厂顺序」，它凭什么只往乱的方向走？

答案藏在一次计数里，这次计数是整个统计物理的地基。

乱不是被吸引的，乱是多数

52 张牌的全排列有多少种？ $52!$ ，约等于 8 后面跟 67 个零。这是一个大到没有直觉意义的数——打个比方，宇宙诞生至今的秒数，才 10 的 18 次方量级。

现在问：这么多种排列里，「有序的」占多少？看你标准多宽：出厂顺序算 1 种；把四种花色顺序换一换，撑死几十种；就算你把「看起来挺整齐」的标准放到极宽，有序排列的数量跟 10 的 67 次方比起来，仍然是零——不是比喻，是数学上趋于零的比例。

大白话

大白话：洗牌不「喜欢」乱。洗牌只是瞎换。但瞎换几乎必然落进「乱」的阵营，因为乱的排列占了几乎全部名额。不是乱被吸引了过去，是有序的地盘小到根本踩不中。

这就是熵的直觉——大白话讲，熵就是「这个宏观样子背后，对应多少种微观排法」；对应得越多，熵越高。一副全乱的牌，「全乱」这个宏观描述背后对应着天文数字种具体排法，熵高；出厂顺序只对应一种，熵最低。热力学第二定律说「孤立系统的熵不减少」，翻译成人话就是：**系统瞎走的时候，几乎必然走向微观排法多的状态——因为那边地方大。**

为什么不可逆：不是不能，是等不起

严格说，洗牌洗回出厂顺序的概率不是零，是 $1/52!$ 量级——每洗一次大约千亿亿亿亿亿亿亿亿亿分之一。你要等它发生一次，需要的洗牌次数比宇宙年龄按秒算还多几十个数量级。所以「永远不会」是「在宇宙的时间尺度内永远不会」，这在实践上和绝对的「永远不」没有区别。

这个「计数解释」回答了物理学里一个很深的困惑：微观力学（牛顿方程、薛定谔方程）全是时间可逆的——倒着放，每个碰撞都合法。那宏观的不可逆从哪来？答案就是：不是定律不许倒放，是倒放要踩中的那个状态占的比例太小。牛奶溶进咖啡的每一种分子路径都合法，牛奶自己聚回去的路径也合法，但前者的「合法走法」比后者多了无法想象的数量级。**时间的箭头不是定律画出来的，是计数数出来的。**

洗几次才算乱：七次

顺便解决一个工程问题：要洗几次，牌才算「够乱」？Persi Diaconis（对，就是第二章那位造抛币机的魔术师数学家）和 Dave Bayer 在 1992 年把这个问题算死了。他们给最常见的 riffle shuffle（把牌分两半、交错插入）建了数学模型，然后度量「洗了 k 次之后，牌序分布离完全均匀还差多远」。

答案是个漂亮的阶跃：52 张牌，洗 5 次还明显留着原序的痕迹，洗 6 次差口气，**洗 7 次之后突然接近均匀**，再多洗改善很小。乱度不是渐变，是在第七次附近「相变」式地到位的。牌手之间流传的「新牌要洗七遍」原来不是玄学，背后真有定理撑腰。

反过来的推论更好玩：你只洗三四次就上手的牌局，牌序里还残留着上一局的结构——这解释了为什么休闲牌局里「同花扎堆」「大牌连坐」的感觉比真随机多。那不是错觉，是数学。

把视角抬高一格

回头看，这一章回答的是「整体层面的随机」：单次洗牌不可预测（第二章的混沌），但洗很多次之后的**分布**却精确可算——第七次后每种排列等概率。这透露了随机性的一个深层性格：**单次越不可捉摸，大数目的统计规律反而越铁。**

下一章我们就顺着这个性格走：为什么保险公司敢给你的车定价、赌场敢开门营业？他们赌的不是单次结果，是一个叫大数定律的东西。

第四章 · 单次不可测，长期可预测

赌场的轮盘，每一转的结果都不可预测——第二章说了，它是个混沌系统，物理上就没法预测。可拉斯维加斯的财报里，博彩收入稳定得像水电费。保险公司更极端：你的车明年撞不撞，天知道；但一千万辆车的总赔付，精算师能算到小数点后两位。

单次最不可预测的东西，加总起来为什么反而最好预测？这就是大数定律，随机世界里最赚钱的定律。

先立一个直觉：平均会「沉淀」

抛硬币 10 次，正面上占 7 成毫不稀奇；抛 1000 次，正面比例落在 45%-55% 之外就已经很少见；抛 100 万次，比例几乎一定贴在 50% 附近，偏差不超过零点几个百分点。**次数越多，正面比例越「沉淀」到 1/2 上。**这就是大数定律——大白话讲：同一个随机实验独立重复足够多次，平均值几乎必然收敛到期望值。

注意它没说什么。它没说「前面正面多了，后面反面会追上来补」——硬币没有记忆（第六章专门拆这个错觉）。它是靠「稀释」起作用的：前 10 次多出来的 2 个正面，在 100 万次里被稀释到可以忽略，不是被「纠正」掉的。这个区别看着咬文嚼字，其实是赌徒破产和赌场赚钱的分水岭。

期望值：给每次随机定个「平均价」

要把大数定律变成生意，还需要一个概念：期望值——大白话讲，就是「每种结果 × 它的概率，全加起来」，也就是长期平均下来每次能拿多少。

拿美式轮盘的单注举例：押一个数字，押中赔 35 倍。轮盘有 38 个格子（1-36 加 0 和 00），押中概率 1/38。期望收益是 $35 \times (1/38) + (-1) \times (37/38) \approx -0.053$ ，即每押 1 块钱，平均亏 5.3 美分。这 5.3% 叫 庄家优势——大白话讲，就是赌场在每局里抽的「隐形税」。

单个赌客的一晚，是方差的天下：可能翻倍，可能清零，什么都可能发生。但赌场面对的不是一个人，是每年几千万次下注。大数定律保证：几千万次下注的平均收益，几乎必然贴着

-5.3%。赌客在赌博，**赌场不在赌博——赌场在收税**。它把不可预测的单次，批发成了稳定的现金流。

保险公司：同一个定律，更体面的用法

保险的生意模型和赌场一字不差，只是站的方向不同。你的车明年出险概率假设是 5%，平均赔付 2 万，期望成本就是 1000 块。保险公司收你 1300 块保费——多出的 300 是它的「庄家优势」。

单看你一个人，保险公司是在赌：赌你今年不撞。但它同时承保一千万人，大数定律上场：一千万人的总赔付几乎必然落在「期望 × 一千万」附近很窄的区间里。它不怕某个人出险，它怕的是**算错期望**——所以精算师才是保险公司的核心资产。

大白话

大白话：赌场和保险公司干的是同一件事——把「单次不可预测」的随机事件大量批发，让大数定律把平均值压成确定收入。区别只在于：赌场的优势来自规则设计，保险公司的优势来自对真实概率的了解比你深。

大数定律的两个使用条件

这个定律不是万金油，它有两个前提，忽略任何一个都会翻车：

- **独立**。每次实验互不影响。轮盘满足；但 2008 年金融危机里，大量房贷被假设「违约相互独立」，结果房价一跌全国一起违约——相关性一来，大数定律当场失效，「分散风险」变成「集中陪葬」。
- **期望存在且有限**。有些赌局的期望是无穷大或不存在的（比如著名的「圣彼得堡悖论」：奖金翻倍直到出正面，期望无穷大，但没人真愿意为它付无穷块钱）。这时候「平均会沉淀」根本不成立。

这两条在第八章讲伪随机、第十章讲蒙特卡洛时还会回来——用计算机模拟随机时，「独立性是假的」正是最大的坑。

平均会沉淀，但围绕平均怎么晃？

大数定律说平均值会贴住期望，但没说你离期望多远、以什么方式晃。抛 100 次硬币，正面次数在 50 附近晃动的形状是什么样的？非常具体的形状：一座钟。而且惊人地，不管你抛的是硬币、骰子，还是任何乱七八糟分布的东西，加总起来都是那座钟。

为什么？下一章讲概率论里最不可思议的结果：中心极限定理。

第五章 · 为什么钟形曲线到处都是

身高、考试分数、测量误差、城市某天的用电量、一批零件的直径——这些东西的来源天差地别，画成直方图却都长成同一座钟：中间高、两边对称地低下去。为什么？凭什么管零件直径的规律和管考试成绩的规律是同一个？

答案是概率论里最不可思议的一条定理：中心极限定理。先别管公式，我们先用一块钉子板把它「看」出来。

高尔顿钉板：一座钟的机械制造

想象一块竖直的板子，上面钉满交错排列的钉子，像弹珠台。从正上方放下一颗小球，它撞到第一颗钉子，随机向左或向右滚；撞到下一排钉子，再随机向左或向右……滚过十几排钉子后，落进底部的一排槽里。

放一颗球，落哪完全没法猜。放一万颗球，奇迹出现：槽里堆出来的轮廓**每次**都是那座钟。中间槽最高，向两边对称衰减。这个装置叫高尔顿钉板——大白话讲，就是一台「把大量小随机加起来」的机器：每颗钉子的左右是一次小随机，小球的最终位置是十几步随机的总和。

机器里藏着的逻辑只有一句话：**落到正中间，需要「左右差不多各半」——这种组合有无数种走法；落到最边上，需要「步步都朝同一边」——只有一条走法**。中间位置的「走法数量」碾压边缘位置，和第三章「乱是多数」是同一个计数逻辑。钟形曲线不是被谁设计出来的，是组合数堆出来的。

定理本身：加什么都行，加多了就是它

高尔顿钉板里每步是「向左或向右」——一个非常特殊的分布。中心极限定理说的比这猛得多：**不管单个小随机服从什么分布**（均匀、偏斜、离散、长得再奇怪），**只要它们相互独立、单个的晃动有限，把足够多个加起来，和的分布就趋向同一座钟**（正态分布）。

大白话：钟形曲线是「加法」的 attractor（吸子）。随机量只要是被「许多互不相干的小因素加总」出来的，它几乎必然呈钟形——至于小因素各自长什么样，加多了之后全被磨平。

这就解释了开头的清单。身高 = 遗传里成百上千个基因位点的小效应 + 营养的许多小波动，加出来的；测量误差 = 仪器热噪声、读数视差、环境振动的加总；考试成绩 $\approx$ 每道题得分的加总。凡是你看到的钟形，背后都是同一台「加法机器」在干活。

反过来，这个定理也给你一个侦探工具：**看到钟形，去找「独立小因素的加总」；看不到钟形，说明假设里有哪条断了。**断法主要有两种——

钟形不管用的两个世界

断法一：因素不是相加，是相乘。城市人口、个人财富、一本书的销量，都是「富者愈富」的过程：现在的体量决定下一步的增长幅度，因素是**乘**上去的。乘法的产物取对数才变成加法——所以这些量取对数后才呈钟形（对数正态），原始分布则是拖着长尾巴的偏态。把乘出来的分布当钟形用，会系统性低估「巨富」「巨城」出现的概率。

断法二：单步的晃动没有上限，或者不独立。股价日收益率的分布，尾部比钟形预言的胖得多——1987 年 10 月 19 日美股单日跌 22.6%，若按正态分布和当时的波动率估算，这种跌幅的概率小到宇宙年龄里都该遇不上一次，但它就是发生了。原因正是定理前提的塌方：市场参与者的恐慌会互相传染（不独立），而且价格跳跃的幅度没有「有限晃动」的保证（肥尾）。塔勒布靠骂「拿钟形曲线管金融风险」出了一整个系列的书，骂的就是这个。

钟的宽度：顺带记住根号 n

中心极限定理还附赠一个定量结论： n 个独立小随机**加起来**，总晃动（标准差）按 $\sqrt{n}$ 增长；所以**平均**起来，晃动按 $\sqrt{n}/n = 1/\sqrt{n}$ 缩小。这就是为什么实验重复 4 次，精度只提高 2 倍；想提高 10 倍精度，得重复 100 次。这个「 $\sqrt{n}$ 税」是实验科学一切成本的来源，也是第七章随机游走的骨架。

到这里，随机的「统计规律」讲完了：单次不可测（第二章），大数平均可测（第四章），加总必呈钟形（第五章）。规律这么铁，人脑却照样天天看错——下一章讲我们自己：为什么

人脑是一台「在噪声里强行找规律」的机器，以及赌徒们为此交的学费。

第六章 · 赌徒的错觉

1913 年 8 月 18 日，蒙特卡洛赌场的一张轮盘桌上，球连续落在了黑色上。第 5 次、第 10 次、第 15 次……赌客们疯了：「出了这么多黑，红色该来了！」他们疯狂押红，越押越重。黑色一直出到第 26 次才停。那一晚，赌场从「相信红该来了」的人们身上赚了几百万法郎。

这一章不讲随机本身，讲我们这台「随机解读机」为什么出厂就有 bug。

错觉一：该来了——独立事件没有记忆

轮盘每一次旋转都是独立的：球不记得上次落在哪，轮子也不记。连续 26 次黑色之后，下一次红色的概率还是 $18/37$ ，一丝没变。觉得「该红了」，等于假设轮盘有一本账，会主动「找平」——但第四章说过，大数定律靠的是稀释，不是补偿。前面出的 26 个黑，在无限长的未来里被稀释掉，而不是被「补回来」。

这个错觉叫赌徒谬误——大白话讲，就是把「长期会平均」错当成「短期会找平」。它不只坑赌徒：产房门口「前面连生三个男孩，这胎该是女孩了」、招聘官「前面几个都不行，下一个该行了」、投资人「连跌五天了，该反弹了」——全是同一个 bug 换皮肤。

有意思的是它的镜像版本也存在：篮球里的「热手」迷信——觉得连进三球的人「手感来了」，下一球更可能进。心理学家 Gilovich、Vallone 和 Tversky 在 1985 年把 NBA 的投篮数据翻了个底朝天：排除站位、防守压力之后，连进之后的命中率并没有显著高于平时。赌徒觉得「该反转了」，球迷觉得「会延续下去」——方向相反，病根相同：**都不肯接受「这只是一段随机噪声」**。

错觉二：扎堆就是有问题——随机比你想的更「不均匀」

二战时伦敦人发现德军 V-1 飞弹的落点在地图上明显「扎堆」，纷纷猜测德军在精确瞄准某些街区。统计学家 R.D. Clarke 把地图打上格子一算：落点分布和「完全随机」应有的样子（泊松分布）吻合得严丝合缝。扎堆是随机的**正常长相**，不是瞄准的证据。

这叫聚类错觉——大白话讲：真正的随机序列里，「挤在一起」和「连成一串」出现的频率远高于直觉。直觉以为随机是「均匀撒开」，其实均匀撒开恰恰是最不随机的样子。给你个亲手验证的机会：让朋友「假装随机」地写 100 个正反面，再拿 100 次真抛硬币对比——人编的那组几乎从不出现 5 连正，真的那组里 5 连、6 连比比皆是。第一章说「人是糟糕的随机源」，这就是原因：人以为的随机是「交替」，真的随机是「连串」。Apple 当年就栽在这：iPod 的随机播放真随机，用户却投诉「怎么老连放同一个歌手」，最后只好把算法改成「更不随机、但更均匀」，用户反而觉得「这才随机」。

病根：人脑是台过度灵敏的规律探测器

为什么人人都带这两个 bug？进化给的解释很朴素：在草原上，「草丛动了 → 可能有狮子」这个判断，误报（白紧张）的成本低，漏报（被吃掉）的成本是命。自然选择于是把我们调成一台**宁错杀不放过的规律探测器**——宁可在一万次噪声里看出一千个假规律，也不能放过一个真信号。这套配置在草原上是保命的，在轮盘、K 线和体检报告面前就是灾难。

大白话

大白话：人脑对「随机」的出厂设置是错的。我们觉得随机应该「均匀、交替、不扎堆」，真随机偏偏「连串、扎堆、不均匀」。所以面对真随机，人总觉得「有鬼」；面对人编的假随机，反而觉得「这才对」。

能修吗？

可以打两个补丁。一是**先问基准率**：看到「扎堆」，先算「纯随机时这种扎堆该多常见」，多半答案就是「就该这么常见」。二是**把样本量问出来**：任何「连 X 次」的说法，先问总共多少次。连进 3 球听着神，放在 82 场常规赛的数千次出手里，随机都能批发一箩筐。

但老实说，补丁只能减量，无法根治——这是硬件问题。认清这一点本身就是解药：下次你心里冒出「这也太巧了吧」，先停半秒，问问自己是不是又在给噪声写故事。

下一章回到数学。我们看看随机累积起来的轨迹长什么样——一个醉汉从路灯下出发，跌跌撞撞，他会走出多远？答案里的 $\sqrt{n}$ 已经在上一章等着我们了。

第七章 · 醉汉的脚步

1827 年，植物学家布朗把花粉颗粒泡在水里，放在显微镜下看——花粉在水里永不停歇地乱抖，轨迹毫无章法。不是水流，不是生命，换无机物（墨粉、石粉）也照抖不误。这个「乱抖」困扰了学界近八十年，直到 1905 年，一个专利局小职员把它算明白了：那是水分子从四面八方撞出来的。这个职员叫爱因斯坦，他给出的模型，就是本章的主角：随机游走——大白话讲，每一步都随机选方向、一直走下去的轨迹。

醉汉问题：走 n 步，离家多远？

把随机游走简化成最纯粹的版本：一个醉汉站在路灯下，每秒随机向左或向右迈一步，各 50% 概率。走了一万步，他在哪？

期望值上说，他还在路灯下——向左向右对称，平均位移是零。但这个「平均还在原地」极具误导性：**他几乎肯定不在原地**。正确的问法是「平均离原地多远」，答案是 $\sqrt{n}$ ：走 100 步，典型离家 10 步；走 10000 步，典型离家 100 步。

为什么是多一步的「 $\sqrt{}$ 」？第五章已经埋了伏笔： n 步的总位移就是 n 个独立 ± 1 的和，和的晃动按 $\sqrt{n}$ 长。你也可以这么建立直觉：每一步都像往「位移账户」里随机存 $+1$ 或 -1 ，存得越多，账户的「余额波动」越大，但波动只按平方根的速度长——因为大部分存取会互相抵消，净效果只剩零头的量级。

大白话

大白话：随机游走不是「不走」，是「走得很没效率」。想离家远 2 倍，要走 4 倍的路；想远 10 倍，要走 100 倍。随机方向的脚步大量自相抵消，净位移只剩 $\sqrt{n}$ 。

这个 $\sqrt{n}$ 到处都是：香水味在房间里扩散，靠的是分子随机游走，所以香味铺满房间要等很久——扩散距离按时间的平方根长，急不得；芯片里的掺杂、焊点的老化、耳机的线为什么总能缠死，背后都是它。

爱因斯坦的关键一跃：乱抖证明原子存在

1905 年，「原子」还只是个有争议的假说——不少大物理学家（比如马赫）拒绝相信看不见的东西存在。爱因斯坦的论文做了一件绝事：他**反过来**用随机游走算了一笔账——假设水由分子构成、分子按温度乱撞，那么花粉颗粒的随机游走应该走多远？算出来： $\sqrt{n}$ 关系成立，且具体数值能被显微镜测量。佩兰随后真的去数了花粉的位移，数据和爱因斯坦的公式严丝合缝，还顺手测出了阿伏伽德罗常数。原子的存在由此钉死——**看不见的原子，是通过它撞出来的随机性被「看见」的**。这是随机性第一次被当成精密的物理测量工具。

醉汉会回家吗？看维度

数学家波利亚在 1921 年问了一个可爱的问题：醉汉无限走下去，回到起点的概率是多少？答案分维度，而且出乎意料：

- **一维、二维**（线上、平面上）：回家的概率是 1。醉汉无限走下去，几乎必然回到路灯下——而且回来无穷多次。
- **三维**：回家的概率只有约 34%。数学家角谷静夫有句名言：「喝醉了的人总能找到回家的路，喝醉了的鸟可能一去不返。」空间多了一维，「岔路」就多到回不来。

这个「维度决定命运」的结果不止可爱：高分子链的构象、神经网络里的信号扩散、网页之间的随机跳转（PageRank 的数学骨架就是个三维以上「带重启的随机游走」），都在用同一套语言。

股价：一场被围观的随机游走

1900 年，比爱因斯坦还早五年，法国数学家巴舍利耶在博士论文里就用同样的数学描述了巴黎证券交易所的价格波动——他才是随机游走模型的第一个正式使用者，可惜论文被埋了半个世纪。后来被重新发现，长成了现代金融数学的基石：股价的短期变动近似随机游走，对数收益率近似钟形（第五章提醒过：尾部比钟形胖，这个近似在极端行情里会死人）。

「近似随机游走」有个扎心的推论，叫有效市场假说的弱形式——大白话讲：如果价格已经反映了所有公开信息，那下一步涨跌只由「新信息」驱动，而新信息按定义是不可预测的，所以**短期走势原则上不可预测**。这就是为什么猴子掷飞镖选股有时能赢基金经理——不是猴子聪明，是「短期预测」这件事本身的可操作空间，比基金宣传册上写的小得多。

收个尾

随机游走给我们的是第三种看随机的角度：第一章看「一串」，第三章看「一池」，这章看「一条轨迹」。轨迹的脾气是 $\sqrt{n}$ ——缓慢、低效、无处不在，从花粉到股价共用一套骨架。

但到目前为止，我们用的随机都来自物理世界。可你每天打交道最多的随机数是计算机产的。问题来了：计算机是一台彻底确定的机器，它拿什么产生随机？下一章揭这个底——你会发现它一直在「假装」。

第八章 · 计算机怎么假装随机

冯·诺依曼——现代计算机架构的设计者——1951 年留下一句名言：「任何以为用算术方法能产生随机数字的人，当然是生活在罪恶之中。」他不是在骂谁，是在陈述一个结构性事实：**计算机是一台彻底的确定性机器。同一个程序、同一个输入，永远给同一个输出。让它产生「随机」，等于让它做自己最做不到的事。**

但你的代码里 `random()` 每天都在跑。它在干什么？答案是：假装。

线性同余：一个除余数的轮回

最经典的假装方案叫线性同余发生器（LCG）——大白话讲，就是一条递推式：

$$\text{下一个数} = (a \times \text{当前数} + c) \bmod m$$

从某个「种子」（初始值）出发，反复套这条式子：乘一乘、加一加、除一除取余数。余数的序列看起来忽大忽小、毫无规律——拿它当随机数用。所谓 `random()`，多数时候就是这么一条式子在空转。

注意三个直接推论：

- **种子决定一切**。同一个种子，序列一模一样，分毫不差。所以调试模拟程序时固定种子，bug 就能复现；两个玩家用同一个种子，就能生成同一张游戏地图（《我的世界》的世界种子就是这么来的）。
- **必然循环**。状态只有 m 种取值，最多走 m 步必然撞回旧值，然后整个序列原样重播。这个长度叫周期——大白话讲，这盒「随机磁带」有多长，播完就倒带。
- **它不是随机，是「像」**。序列从头到尾被三个常数和种子钉死。第一章的压缩语言说：它的柯尔莫哥洛夫复杂度极低——整条「随机」长河，用一行式子就能完整描述。

假装会露馅：RANDU 的灾难

「看起来像」和「经得起看」之间隔着深渊。1960 年代，IBM 在大型机上标配了一个 LCG 叫 RANDU，参数没选好，留下了计算机史上最著名的随机数事故：把 RANDU 连续生成的三个数当成三维坐标画点，所有点竟然整整齐齐躺在 **15 个平面**上——三维空间里本该均匀撒开的点，实际是一摞平行的薄片。

后果很实际：当年大量用 RANDU 做的蒙特卡洛模拟（第十章会讲这种方法），结果都有系统性偏差——你以为你在整个空间里均匀采样，其实只采了 15 片「夹层」。无数论文的结论建立在这种「假均匀」上。Marsaglia 后来那句刻薄的总结成了行规：「随机数发生器不该是随便选的参数凑出来的。」

大白话

大白话：伪随机数的可怕之处不是它假，而是它**假得很有结构**——肉眼看是噪声，放进正确的维度里看，是整齐的栅栏。用它做模拟，等于在一把弯尺上量布。

现代的假装：又好又长的磁带

今天的默认选择（Python 的 `random`、Excel 的 `RAND`）是梅森旋转（Mersenne Twister）——大白话讲，一个把内部状态搅得极其充分的伪随机发生器。它的周期是 $2^{19937} - 1$ ，长到把宇宙里每个原子每纳秒取一个数、取到宇宙热寂也播不完；统计性质通过了几乎所有常规检验；而且快。

但它依然是「磁带」：知道种子就能重播全部，观察到足够多的输出（624 个连续输出）就能反推出内部状态、预测未来所有输出。所以它从头到尾都在文档里印着警告：**不可用于密码学**。模拟、游戏、洗牌尽管用；密钥、令牌、抽奖——碰都别碰。这个分水岭第十一章会正式接管。

假装也是一种美德

别急着瞧不起伪随机。「确定地假」恰恰是它的核心价值：

- **可复现**：科学模拟里，「同样的种子，同样的结果」是别人能验证你工作的前提。真随机反而没法写论文。

- **可测试**：软件测试里，固定种子的伪随机让「随机输入的测试」也能稳定复现 bug。
- **可共享**：一个 64 位种子顶一部世界的说明书——分布式系统不用传输整张地图，传一个种子就够。

伪随机的定位想清楚了其实很优雅：**它提供的不是随机性，是「按方抓药的复杂性」**——一种低成本、可复现、统计上足够好的「乱」。它欠的那一味药——真正的不可预测——得去物理世界里找。下一章，我们去看看真随机从哪里来，以及怎么验货。

第九章 · 真随机从哪里来

上一章结论很直白：计算机自己造不出真随机，只会放磁带。那真随机从哪里来？答案分两层：经典世界里的「噪声」，和量子世界里的「本性」。这一章也把第二章卖的那个关子结了：世界到底掷不掷骰子？

经典噪声：把「测不准」榨成随机数

硬件世界充满了原则上可测、实际上测不准的微小波动。把它们放大、数字化，就是真随机数的原料：

- **热噪声**：电阻里的电子被热搅得乱撞（第七章的布朗运动在电路里的样子），两端电压有微小随机起伏。Intel 从 Ivy Bridge 开始把「放大热噪声」的电路直接做进了 CPU，就是 `RDRAND` 指令。
- **时钟抖动**：两个独立振荡器的相位差永远有微小漂移，采它当随机源。
- **系统噪声杂烩**：Linux 的 `/dev/urandom` 靠「熵池」——把键盘敲击的精确时刻、鼠标移动、硬盘寻道时间、网络包到达间隔这些「测不准的小数」统统攒进一个池子，再用哈希充分搅拌。

这类随机源的本质还是第二章那句话：**它是「无知」，不是「本性」**——混沌放大的测量极限。理论上，拉普拉斯妖盯着你的 CPU，这些数全是可预测的。但对任何现实的攻击者，这已经够用。不过「理论上可预测」让密码学家如鲠在喉——他们想要的是物理定律担保的不可预测。

量子：世界真的掷骰子

第二章的问题在这里终审。量子力学给出的答案是：**有些事件的结果，在发生之前不存在**。不是我们算不出来，是宇宙中根本没有「算出来」所需的信息。

最干净的例子：让一个光子射向半透半反镜，50% 透过、50% 反射，两条路上各放一个探测器。哪个探测器响？哥本哈根诠释说：测量之前，光子处在「两条路都走」的叠加态；测

量那一刻，结果才「坍缩」成一个。单次结果不可预测——不是因为镜子复杂，而是按量子力学的数学结构，**单次结果没有隐藏的剧本**。

「没有隐藏剧本」不是哲学口号，1964 年贝尔把它变成了可检验的不等式：如果世界底层藏着「局域的隐藏变量」（预先写好的答案），实验统计必须满足某个上限；如果量子力学对，可以突破它。从 1982 年阿斯佩实验到 2015 年三个「无漏洞」贝尔实验，结果一致：**上限被突破，隐藏剧本不存在**。爱因斯坦不信的那句「上帝不掷骰子」，实验站队了玻尔——而且玻尔赢得很彻底：骰子不但掷，还掷得没有任何地方写着底稿。

大白话

大白话：经典的随机是「你看不到答案」，量子的随机是「没有答案可看」。贝尔实验把两者的区别变成了实验室里能测的数。商用量子随机数发生器（QRNG）卖的就是这个：物理定律签名的不可预测性。

从噪声到比特：还得过两道加工

物理噪声到手不等于能用，还要两道工序：

1. **去偏**。真实噪声源总是偏的（0 比 1 多一点、电压阈值有漂移）。冯·诺依曼给过一个优雅的去偏法：把比特两两分组，01 记作 0，10 记作 1，00 和 11 丢弃——不管原始偏差多大，出来的序列严格五五开。
2. **搅拌**。把多个来源的噪声用密码学哈希充分混合，让任何单一路的缺陷都被稀释。Linux 熵池干的就是这个。

怎么验货：只能证伪，不能证实

买回来的随机数发生器是真随机吗？这里第一章的判词回来了：**随机性无法证实，只能证伪**。业界做法是拿统计检验套件（NIST STS、Dieharder）去轰：频率、连串、压缩率、自相关系数……十五项、上百项检查全过，结论也只是「没抓到毛病」。

所以工程上的信任链是分层的：量子原理保证「源头无剧本」，统计检验保证「没被抓到结构」，多源搅拌保证「单点失效不致命」。三层叠起来，就是现代密码系统的地基。

一个浪漫的收尾：既然真随机这么金贵，有人干脆把它做成了公共服务。NIST 有个「随机数灯塔」，每分钟广播一串由量子物理过程产生、带时间戳和前序哈希链的随机数，任何人都可以引用；Cloudflare 则用一面墙的熔岩灯——镜头拍着一百盏灯里蜡块的翻滚——给全球相当比例的互联网流量提供加密种子。物理世界的混乱，被打包成了全互联网的公共品。

有了真随机和伪随机两味药，下一章看它们怎么干活：一种叫蒙特卡洛的方法，拿随机数当算盘，硬算那些公式算不动的东西。

第十章 · 把随机当工具

1946 年，洛斯阿拉莫斯。数学家乌拉姆在病中玩纸牌接龙消磨时间，忽然琢磨：这局能接通的概率是多少？组合数学算起来是个天文数字的分支树，根本算不动。他换了个思路：何必算？**摆一百局、一千局，数赢了几局不就行了。**他把这想法告诉了冯·诺依曼，两人立刻意识到这不只是纸牌技巧——刚造出来的电子计算机，正好能干「重复一千局」这种事。

Metropolis 给这个方法起了个风骚的名字：蒙特卡洛——因为乌拉姆有个叔叔爱去蒙特卡洛赌场。它的第一个正经任务，是算原子弹里的中子扩散。

思路一句话就能说完：**算不出的答案，只要它能写成「某个随机事件的平均值」，就用大量随机采样去逼近它。**这一章看这台「随机算盘」怎么打。

第一笔账：往圆里扔飞镖算 π

画一个边长 2 的正方形，里面内切一个半径 1 的圆。闭眼往里扔飞镖（均匀随机地扔）：落在圆里的概率 = 圆面积 / 正方形面积 = $\pi/4$ 。扔一万镖，数圆里的比例，乘以 4，就是 π 的估计值。扔得越多越准——第四章的大数定律在给你打工。

注意这里发生了什么魔术： π 是一个**确定**的数，跟随机八竿子打不着；我们却用随机的方法把它算了出来。这就是蒙特卡洛的灵魂——**把确定的问题改写成随机变量的期望，然后采样。**面积、体积、积分，全是「期望」的马甲。

为什么不用尺子量：维数灾难与免费通行证

算面积有更「正常」的办法：把正方形切成一亿个小格子，数圆盖住了几格。二维时这很好。但现代工程里的「面积」常常长在几百维的空间里——一个期权的价格取决于几十上百个随机因子，一个蛋白质的形状是几千个坐标。网格法在 d 维里要 N^d 个点，维度一高，格子数爆炸到宇宙原子都不够填。这叫「维数灾难」。

蒙特卡洛在这里拿到了一张免费通行证：它的误差只取决于**采样次数**，跟维度无关——不管几维，误差永远按 $1/\sqrt{n}$ 缩小（第五章的 $\sqrt{n}$ 税，老朋友了）。扔一百万个点，误差大约千分之一，二维如此，一千维也如此。网格法在高维里指数爆炸，蒙特卡洛在高维里闲庭信

步。这就是现代金融定价、核反应堆设计、图形渲染全押注蒙特卡洛的原因：**不是它多优雅，是高维世界里只有它还走得动。**

大白话

大白话：维数灾难是「地毯式搜查」在高维的破产——房间太多，警察不够用。蒙特卡洛改成「随机抽查」：不管房间多少，抽查一千间的把握都一样。牺牲精度换可行性，是高维世界里唯一的活路。

随机算盘打到了哪

今天的蒙特卡洛无处不在，举三个不同量级的：

- **核物理与医学**：中子在反应堆里的每一次碰撞、散射、吸收都是带概率的事件——直接模拟亿万条「随机游走轨迹」（第七章），统计出链式反应的全貌。放疗剂量计算同理：光子在你身体里的散射路径也是模拟出来的。
- **金融**：一个复杂衍生品的价格 = 「在成千上万条可能的未来市场路径上的平均收益」。于是每晚，投行让随机数在假想市场里跑几十万条平行未来，取平均。
- **人工智能**：AlphaGo 的决策核心是「蒙特卡洛树搜索」——棋盘上算不动的局面，就随机模拟几千盘「下完这步之后随便走」的棋，数哪步赢得多。当年它赢李世石的那几步「神之一手」，相当一部分是随机模拟数出来的。

还有个进阶版值得一提：当「均匀抽查」效率太低时（比如要在天文数字的分子构象里找低能量的那些），就用 MCMC（马尔可夫链蒙特卡洛）——大白话讲，让采样点做一场「偏好低处」的随机游走，在重要的区域多待、不重要的少来。贝叶斯统计、大模型的许多训练技巧、乃至选举预测模型，跑的都是它。

两条行规

蒙特卡洛用多了，会记住两条行规。一，**结果是估计，带误差棒**：报蒙特卡洛的结果必须报「±多少」，误差按 $1/\sqrt{n}$ 缩——想把误差砍十倍，采样量加一百倍，没有捷径。二，**伪随机要验货**：第八章 RANDU 的 15 个平面就是蒙特卡洛史上最大的事故——随机源有结构，模拟就把结构当物理。

到这里，随机从「麻烦」彻底变成了「资产」。下一章看它最金贵的用途：密码学。在那里，随机不只是工具，是命根子——密钥的全部强度，就是随机数发生器的强度。

第十一章 · 把随机当武器

密码学有个不太好意思说出口的秘密：所有精巧的数学——椭圆曲线、大数分解、格——最后都挂在一个朴素的东西上：**一个谁也猜不着的随机数**。算法是公开的，流程是公开的，整个系统的全部秘密都浓缩在密钥里（这叫柯克霍夫原则：保密靠密钥，不靠算法）。而密钥的全部强度，就是产生它那个随机数发生器的强度。随机数猜得着，数学再漂亮也是纸糊的。

这一章看三件事：随机性在密码学里能达到的理论极限、它一旦掺水会发生什么、以及工程上怎么伺候好它。

理论极限：一次一密，香农盖过章的「绝对安全」

想象最笨的加密：明文每个字母，和密钥里对应字母「相加」（模 26），密钥是一串**真随机**字母。香农 1949 年证明了一个惊人的定理：只要密钥（1）真随机、（2）和明文一样长、（3）只用一次、（4）不泄露，那么截获的密文**不包含明文的任何信息**——不是「很难破」，是数学上「无可破」：任何一段同样长度的明文都能配出某个密钥产生这段密文，破译者面对无限多等可能的解，连「猜对了」都无法确认。这叫一次一密——大白话讲，用真随机噪声把明文完全淹没，密文里除了噪声什么都不剩。

完美保密的代价全在「密钥管理」上：密钥要用真随机（第九章的物理源）、要和明文一样长、见一次面就得换新的、还得安全地送到对方手里。这四条少一条，天就塌了。苏联在 1940 年代的间谍网里把「只用一次」破成了「偶尔重用」——美国的维诺纳计划抓住重用的密钥对密文做差分，噪声相消，明文浮出，一点一点抠出了几千页苏联密电。一次一密仍是「绝对安全」的，前提是那个随机真的「只随机一次」。

大白话

大白话：一次一密是密码学的光速——理论上碰不得的完美，实践上伺候不起的娇贵。它真正的遗产是那个证明：**足够的真随机，可以让信息彻底消失。**

掺水的随机：三起真实事故

现实系统不用一次一密，用 AES、RSA 这些实用算法——但密钥、随机数填充、临时数，样样要从随机数发生器里出。发生器一掺水，算法直接架空。三起教科书级事故：

- **1995 年，网景浏览器**：SSL 密钥的种子是「当前时间 + 进程号」。加州大学两个学生（Ian Goldberg 和 David Wagner）一算：时间能猜、进程号范围小，整个密钥空间几分钟就能穷举完。「安全浏览器」的锁，钥匙孔比钥匙大。
- **2008 年，Debian 的 OpenSSL**：一位开发者为了消除编译器警告，删掉了一行「往随机池里搅入未初始化内存」的代码——连带把真正搅入熵的那行也废了。此后近两年里，Debian 系系统产生的所有密钥，种子只剩进程号：32767 种可能。全球几万台服务器的「随机密钥」，其实每人只有三万分之一的秘密。
- **2010 年，索尼 PS3**：签名算法 ECDSA 要求每次签名用一个全新随机数（叫临时数）。索尼把它写死成了一个固定值。两个签名一相减，私钥直接解出来——和维诺纳是同一个错误：噪声被「重用」之后就不再是噪声。黑客当众演示算出索尼的根密钥，整个主机防线清零。

三起事故同一个模式：**没有人破解数学，他们只是不再猜随机数——因为随机数已经不值得猜了。**

工程答案：CSPRNG 与它的红线

于是有了密码学专用的随机数发生器（CSPRNG）——大白话讲，就是第八章的「磁带机」加固版：内部状态用密码学原语搅拌，让「观察到输出」反推不出状态、「预测下一个数」在计算上不可行。但红线依然是第八章那条：梅森旋转统计再好也不许进密码学——它的输出能反推状态。CSPRNG 的标准是更狠的一条：**不但看起来乱，连「知道全部过去的输出」都不许对「下一个比特」给出任何优势。**

还有一层阴影值得一提：2013 年斯诺登文件披露，美国 NSA 推动成为 NIST 标准的随机数发生器 Dual_EC_DRBG 被指留有后门——特定常数让知道秘密参数的人能从输出反推状态。这提醒了最后一课：**随机数发生器的「随机」，你不光要它乱，还要知道它为什么乱、谁挑的参数。**这也是第九章熔岩灯和量子灯塔存在的意义——把「信任」尽量换成「可审计的物理」。

从武器回到生活

密码学把随机性的地位推到了顶点：足够的真随机能让信息消失，掺水的随机能让堡垒自塌。到此为止，本书讲了随机的定义（第一章）、来源（二、九）、统计脾气（三到七）、人造与使用（八到十一）。

最后一章回到我们自己。离开了赌场和机房，随机性还统治着一件事：人生。运气和本事怎么分？成功故事里有多少是噪声？在一个随机的世界里，怎样做决定才算聪明？

第十二章 · 与随机共处

这本书从一串乱码出发，走到了量子噪声和密码学。最后一章，回到最贴身的问题：你自己的人生，也在被随机性搅动——成功、失败、运气、本事，怎么分？分不清楚，就会把噪声当成能力，把运气当成规律。

看不见的弹孔：幸存者偏差

二战时，美军统计返航轰炸机的弹孔分布：机翼和机身上密密麻麻，发动机和驾驶舱附近很少。军官们的直觉是：给弹孔多的地方加厚装甲。统计学家沃德（Abraham Wald）说不：**恰恰相反，要加固的是弹孔少的地方**。因为你统计的是「活着回来的飞机」——发动机中弹的飞机根本没回来，它们的弹孔你看不见。

这叫幸存者偏差——大白话讲：你只看得见「留下来的样本」，而「留下来」本身就是被筛选过的，拿它总结规律，必然失真。它的现代版本遍地都是：

- 研究「成功企业家的共同特质」，忘了问「有同样特质但破产的人」有多少——敢冒险、辍过学、每天工作十六小时，破产者身上也全是这些。
- 「这个基金十年年化 20%」——同一年发行的另外三百只基金里，亏光的早就清盘了，你看到的排行榜是筛剩下的尾巴。
- 「我爷爷抽烟活到九十九」——没活到的爷爷们不会出现在饭桌上。

大白话

大白话：凡是「从结果往回找原因」的叙事，先问一句：输家在哪？找不到输家的成功学，大多是给噪声写的传记。

运气和本事：一个光谱，不是开关

别从一个极端跳到另一个极端——「全是运气」和「全是本事」一样错。真实世界里，结果 = 本事 + 运气，只是不同领域里两者的配比不同。下围棋，配比压倒性偏向本事；掷硬币猜正反面，全是运气；投资、创业、升职、写书卖不卖得动，落在中间偏运气的位置。

判断配比有个粗糙但好用的指标：**「能不能故意输」**。能故意输的活动（故意输一盘围棋很容易）里本事占大头；连故意输都做不到的活动（猜硬币想错都难超过 50% 太久）里运气占大头。配比不同，策略完全不同：本事主导的领域，苦练有效、向第一名学习有效；运气主导的领域，向第一名学习的收益急剧缩水——他更可能只是幸存者里嗓门最大的。

还有一个统计现象专门惩罚「把运气当本事」：**均值回归**——大白话讲，极端好的表现之后，下一次往往回落到平均水平，因为那次极端里运气占了一大块，而运气不续费。所以「年度基金经理」次年大概率平庸，「封面运动员魔咒」、新官上任的「蜜月期」都是它的化身。不是他们退步了，是运气到期了。

把「决定」和「结果」拆开

随机世界里最害人的思维习惯，是拿结果评判决定——赢了就是英明，输了就是愚蠢。扑克牌手管这叫「resulting」。它的荒谬用极端例子就看得清：拿全部家当去赌 99% 概率赢的一局，赢了——这是蠢决定，好结果；拒绝一场 99% 赢面的局，可能错过——这是好决定，坏结果。**决定的质量只能按「当时已知信息下的期望值」来评，不能按后来的结果来评**——因为结果里掺的那部分运气，在决定的时刻原则上不可知（第二章的混沌、第九章的量子都在担保这一点）。

拆开之后，行动准则就清晰了：

- **在期望值高的地方反复下注**。单次结果交给大数定律，别押身家在一局上——第四章说了，平均沉淀的前提是「活得足够长、次数足够多」。
- **盯住过程，审计过程**。结果可以被运气污染，过程不能。复盘时间「当时的判断逻辑对不对」，不问「这单赚了没」。
- **给运气留位置**。做计划时假设波动存在：留冗余、留现金、留退路——第九章的工程们管这叫「熵池」，人生的版本叫安全边际。
- **对故事保持警惕**。第六章已经证明，人脑是台强行找规律的机器；一切「所以他成功了」的叙事，都默认剔除了没成功的对照组。

回答那个问题

现在可以回答第一章留下的贯穿问题了：**随机到底是世界的本性，还是我们的无知？**

这本书给出的答案是分层的，而且每层都有实验或定理撑腰：

- 宏观世界里，随机主要是**无知**——但混沌把消除无知的成本抬到了物理上付不起的高度，所以它是「原则上消除不掉的无知」（第二章）；
- 微观世界里，随机是**本性**——贝尔实验证明，事件的单次结果在发生前不存在剧本（第九章）；
- 而无论哪一层，随机的**统计规律**都铁得像任何物理定律：熵增、大数、钟形、 $\sqrt{n}$ （第三、四、五、七章）。单次是自由的，整体是被统治的。

所以「乱敲键盘能敲出什么」？能敲出一本这样的书——一串几乎必然无规律的字符（第一章的计数保证了「无规律」是常态），却照样能被我们读出结构、讲出因果、甚至提炼出行动准则。这大概就是人与随机共处的最终姿势：**承认单次不可知，利用整体可测，对故事免疫，对过程较真。**

那串字符 `sa de er ge d sa de tu ba` 没有意义。但追问「它为什么没有意义」，是有意义的。愿你在下一个「太巧了」面前，先想起这本书。

随机：乱敲键盘能敲出什么 · 1