12.9 用不公平的硬币作公平的决定

工作纸

题目

STEP I 2019，第 11 题

继续阅读之前，请先看题目（原题为英文）。题目载于 OCR 提供下载的 2019 年 STEP 试卷（zip 文件）内的 STEP I 试卷：

www.ocr.org.uk/Images/696590-2019-past-papers.zip

提示

请先自行尝试解题。如果遇到困难，请逐一阅读提示，每读完一个便回到题目再试。标有停一停，试一试的提示是关键步骤。每个提示之后均留有空位供你演算。

> **想一想** 在一轮之中，作出决定的概率是多少？没有决定的概率又是多少？$2pq$ 最大可以取甚么值？

阶段 1 在第 n 轮作出决定

涵盖：第 (i) 部分，第 n 轮

> **想一想** 在一轮之中，各枚硬币结果一致的概率（probability）是多少？要在第 n 轮作出决定，须先有 $n-1$ 次不一致，然后出现一次一致。

阶段 2 在第 n 轮或之前作出决定

涵盖：第 (i) 部分，第 n 轮或之前

> **停一停，试一试** 首 n 轮都未能作出决定的概率是多少？$pq = p(1-p)$ 最大可以是多少？

阶段 3 三个人

涵盖：第 (ii) 部分

想一想 若三枚硬币结果全部一致，第一轮便能作出决定。否则，如果多数是正面，便把结果不同的那枚硬币翻成正面：这时第二轮需要出现甚么结果？如果多数是反面，又如何？

停一停，试一试 利用 $p+q=1$ 及 $p^3+q^3=(p+q)^3-3pq(p+q)$，把所有式子用 $s=pq$ 表示。

背后的数学

冯纽曼的妙计

题目中的程序很快，但有偏差。冯纽曼的程序则是公平的：掷两次，出现 HT 或 TH 就作决定，出现 HH 或 TT 就重复。每次尝试成功的概率是 $2pq$，所以平均需要 $\frac{1}{2pq}$ 次尝试；当硬币偏差很大时，这会很慢（图 12.9.1）。题目的程序每轮作出决定的概率是 $p^2+q^2\geq\frac{1}{2}$，但当 $p>\frac{1}{2}$ 时，它的结果偏向酒店。

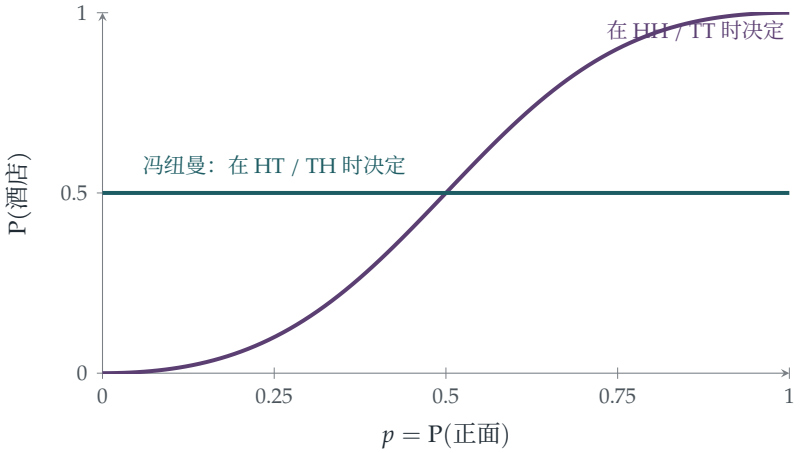


图 12.9.1 选中酒店的概率，对应硬币的偏差。在两枚硬币结果相同时作决定（紫红色）很快，但偏向较可能出现的一面。冯纽曼的程序（蓝绿色）对每一个 p 都完全公平，代价是当硬币偏差很大时需时较长。

提取随机性

冯纽曼的妙计是第一个*随机性提取器*（randomness extractor）：一种把不完美的随机性变成完美随机性的程序。它浪费很多（每两次投掷最多只得到一个公平的位元，而且往往一个也得不到）；更好的方法会把被弃掉的 HH 和 TT 重新利用，从而提取硬币所含的几乎全部随机性，而这随机性的多少是用硬币的*熵*（entropy）来量度的，即每次投掷 $-p\log_2 p - q\log_2 q$ 个位元。提取器用于电脑的硬件随机数产生器：这些产生器收集不可预测但有偏差的物理杂讯，并必须把它变成无偏差的位元，供密码学（cryptography）使用。

冯纽曼与随机数

冯纽曼在 1951 年的论文“Various techniques used in connection with random digits”中描述了这个妙计。当时他和同事正在为设计核武器而进行一些最早期的电脑模拟（即“蒙地卡罗方法”（Monte Carlo method））。在同一篇论文中，他就用算术方法产生随机数说了一句名言：“任何人若考虑用算术方法来产生随机数字，当然就是身处罪恶之中。”

延伸练习

1 **轮数的期望值。**求第 (i) 部分的程序所需轮数的期望值（expected number），以及冯纽曼的程序所需轮数的期望值。对哪些 p 而言，冯纽曼的程序较慢?

2 **公平的三选一。**利用一枚有偏差的硬币，设计一个程序，从三个选项中选出一个，使每个选项的概率都恰好是 $\frac{1}{3}$。

3 **用公平硬币造出有偏差的骰子。**利用一枚公平的硬币，设计一个程序，模拟一枚掷出正面的概率恰好是 $\frac{1}{3}$ 的硬币。所需投掷次数的期望值是多少？

4 **再看三个人。**在第 (ii) 部分中，他们去酒店的概率是多少？请以 p 的函数表示。当 $p = \frac{1}{2}$ 时，这个程序公平吗？

延伸阅读

- **John von Neumann，“Various techniques used in connection with random digits”**，*National Bureau of Standards Applied Mathematics Series* 12 (1951)。篇幅短小而著名。
- **Donald Knuth，*The Art of Computer Programming*, Vol. 2**（Addison-Wesley），第 3 章，论随机数。
- **Michael Mitzenmacher & Eli Upfal，*Probability and Computing***（Cambridge University Press），论提取随机性与熵。

完整的引导式解答见第 12.9 节：

https://beyondstep.keithmcnulty.org/zh-hans/ch12/von-neumann.html

每星期一道 STEP 题目，完整讲解：The STEP Up，以电子邮件免费发送，订阅网址：keithmcnulty.substack.com