12.9 用不公平的硬幣作公平的決定

工作紙

題目

STEP I 2019，第 11 題

繼續閱讀之前，請先看題目（原題為英文）。題目載於 OCR 提供下載的 2019 年 STEP 試卷（zip 檔案）內的 STEP I 試卷：

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

提示

請先自行嘗試解題。如果遇到困難，請逐一閱讀提示，每讀完一個便回到題目再試。標有停一停，試一試的提示是關鍵步驟。每個提示之後均留有空位供你演算。

> **想一想**　在一輪之中，作出決定的概率是多少？沒有決定的概率又是多少？$2pq$ 最大可以取甚麼值？

階段 1　在第 n 輪作出決定

涵蓋：第 (i) 部分，第 n 輪

> **想一想**　在一輪之中，各枚硬幣結果一致的概率（probability）是多少？要在第 n 輪作出決定，須先有 $n-1$ 次不一致，然後出現一次一致。

階段 2 在第 n 輪或之前作出決定

涵蓋：第 (i) 部分，第 n 輪或之前

> **停一停，試一試** 首 n 輪都未能作出決定的概率是多少？$pq = p(1-p)$ 最大可以是多少？

階段 3　三個人

涵蓋：第 (ii) 部分

想一想　若三枚硬幣結果全部一致，第一輪便能作出決定。否則，如果多數是正面，便把結果不同的那枚硬幣翻成正面：這時第二輪需要出現甚麼結果？如果多數是反面，又如何？

停一停，試一試　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。

背後的數學

馮紐曼的妙計

題目中的程序很快，但有偏差。馮紐曼的程序則是公平的：擲兩次，出現 HT 或 TH 就作決定，出現 HH 或 TT 就重複。每次嘗試成功的概率是 $2pq$，所以平均需要 $\frac{1}{2pq}$ 次嘗試；當硬幣偏差很大時，這會很慢（圖 12.9.1）。題目的程序每輪作出決定的概率是 $p^2+q^2\geq\frac{1}{2}$，但當 $p>\frac{1}{2}$ 時，它的結果偏向酒店。

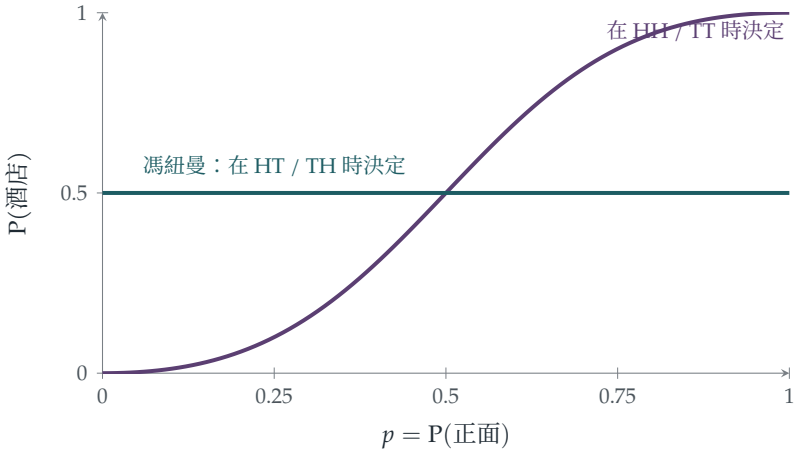

圖 12.9.1 選中酒店的概率，對應硬幣的偏差。在兩枚硬幣結果相同時作決定（紫紅色）很快，但偏向較可能出現的一面。馮紐曼的程序（藍綠色）對每一個 p 都完全公平，代價是當硬幣偏差很大時需時較長。

提取隨機性

馮紐曼的妙計是第一個隨機性提取器（randomness extractor）：一種把不完美的隨機性變成完美隨機性的程序。它浪費很多（每兩次投擲最多只得到一個公平的位元，而且往往一個也得不到）；更好的方法會把被棄掉的 HH 和 TT 重新利用，從而提取硬幣所含的幾乎全部隨機性，而這隨機性的多少是用硬幣的熵（entropy）來量度的，即每次投擲 $-p\log_2 p - q\log_2 q$ 個位元。提取器用於電腦的硬件隨機數產生器：這些產生器收集不可預測但有偏差的物理雜訊，並必須把它變成無偏差的位元，供密碼學（cryptography）使用。

馮紐曼與隨機數

馮紐曼在 1951 年的論文「Various techniques used in connection with random digits」中描述了這個妙計。當時他和同事正在為設計核武器而進行一些最早期的電腦模擬（即「蒙地卡羅方法」（Monte Carlo method））。在同一篇論文中，他就用算術方法產生隨機數說了一句名言：「任何人若考慮用算術方法來產生隨機數字，當然就是身處罪惡之中。」

延伸練習

1 **輪數的期望值。**求第 (i) 部分的程序所需輪數的期望值（expected number），以及馮紐曼的程序所需輪數的期望值。對哪些 p 而言，馮紐曼的程序較慢？

2 **公平的三選一。**利用一枚有偏差的硬幣，設計一個程序，從三個選項中選出一個，使每個選項的概率都恰好是 $\frac{1}{3}$。

3 **用公平硬幣造出有偏差的骰子。**利用一枚公平的硬幣，設計一個程序，模擬一枚擲出正面的概率恰好是 $\frac{1}{3}$ 的硬幣。所需投擲次數的期望值是多少？

4 **再看三個人。**在第 (ii) 部分中，他們去酒店的概率是多少？請以 p 的函數表示。當 $p = \frac{1}{2}$ 時，這個程序公平嗎？

延伸閱讀

- **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，論隨機數。
- **Michael Mitzenmacher & Eli Upfal，*Probability and Computing***（Cambridge University Press），論提取隨機性與熵。

完整的引導式解答見第 12.9 節：

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

每星期一道 STEP 題目，完整講解：The STEP Up，以電郵免費發送，訂閱網址：keithmcnulty.substack.com