詳細解答

STEP III 2015，第 12 題

概率與統計 • 概率生成函數

> **STEP III 2015，第 12 題**
>
> 繼續閱讀之前，請先看題目（原題為英文）。題目載於 STEP Support Programme 的試題資料庫：
>
> step.maths.org/questions/15-s3-q12

關鍵思路

除以 m 的餘數（remainder）只取決於指數模 m 的值，所以在餘數的生成函數（generating function）中，凡是出現 x^m 的地方都可以換成 1。把獨立（independent）的投擲結果相加，相當於把生成函數相乘，之後再把 x 的冪次約簡一次。有了這條規則，整個計算就變成簡單的多項式代數，其中 $x \cdot y$ 和 y^2 都會化為 y 的倍數。

解答

全文中，設 $X_1, X_2, \ldots$ 為各次投擲的結果，它們互相獨立，且各自在 $\{1, \ldots, 6\}$ 上服從均勻分佈（uniform）。

約簡規則。 設 m 為正整數。若 U 與 V 互相獨立，且取值於 $\{0, 1, \ldots, m-1\}$，則 $U+V$ 的概率生成函數（probability generating function, pgf）是 $G_U(x)G_V(x)$，這是一個多項式，其中 x^k 項的係數就是 $U+V=k$ 的概率。$U+V$ 除以 m 的餘數等於 j，當且僅當 $U+V$ 等於 j 或 $j+m$。因此，只要對 $k \geq m$ 把每個 x^k 換成 x^{k-m}，換言之令 $x^m = 1$，便得到該餘數的 pgf。由於 S_n 的餘數就是（S_{n-1} 的餘數）+（X_n 的餘數）的餘數，而這兩者互相獨立，所以每個餘數的 pgf 都可由前一個相乘再令 $x^m = 1$ 得到。我們以 $\equiv$ 表示「在使用 $x^m = 1$ 後相等」。

第 (i) 部分

擲出 $1,\ldots,5$ 的餘數分別是 $1,\ldots,5$，而擲出 6 的餘數是 0。每種情況的概率都是 $\frac{1}{6}$，所以

$$\mathrm{G}(x) = \tfrac{1}{6}\left(1+x+x^2+x^3+x^4+x^5\right) = \tfrac{1}{6}z, \qquad \text{其中} z = 1+x+\cdots+x^5.$$

在 $x^6 = 1$ 之下，把 z 乘以 x 只是把每一項往前轉一格：$xz = x+x^2+\cdots+x^5+x^6 \equiv z$。因此對每個 k 都有 $x^k z \equiv z$，而且

$$z^2 = \sum_{k=0}^{5} x^k z \equiv 6z.$$

所以 R_2 的 pgf 是

$$\tfrac{1}{36}z^2 \equiv \tfrac{1}{36}\cdot 6z = \tfrac{1}{6}z = \mathrm{G}(x),$$

正如所求。

同樣的步驟在每一步都適用：若 R_{n-1} 的 pgf 是 $\mathrm{G}(x)$，則 R_n 的 pgf 是 $\mathrm{G}(x)^2 \equiv \mathrm{G}(x)$。由歸納法（induction），每個 R_n 的 pgf 都是 $\mathrm{G}(x) = \frac{1}{6}z$。$6 \mid S_n$ 的概率就是 $\mathrm{P}(R_n = 0)$，即 $\mathrm{G}(x)$ 的常數項（constant term）：

$$\mathrm{P}(S_n \text{ 可被整除，除數為} 6) = \tfrac{1}{6}.$$

第 (ii) 部分

現在 $m = 5$。擲出 $1,2,3,4$ 的餘數是 $1,2,3,4$；擲出 5 的餘數是 0；擲出 6 的餘數是 1。所以餘數為 1 的概率是 $\frac{2}{6}$，其餘各為 $\frac{1}{6}$：

$$\mathrm{G}_1(x) = \tfrac{1}{6}\left(1+2x+x^2+x^3+x^4\right) = \tfrac{1}{6}(x+y), \qquad y = 1+x+x^2+x^3+x^4.$$

與第 (i) 部分完全一樣，在 $x^5 = 1$ 之下有 $xy \equiv y$，所以對所有 k 都有 $x^k y \equiv y$，而且

$$y^2 = \sum_{k=0}^{4} x^k y \equiv 5y.$$

因此

$$\begin{aligned}\mathrm{G}_2(x) &\equiv \tfrac{1}{36}(x+y)^2 = \tfrac{1}{36}\left(x^2+2xy+y^2\right)\\ &\equiv \tfrac{1}{36}\left(x^2+2y+5y\right) = \tfrac{1}{36}\left(x^2+7y\right),\end{aligned}$$

這就是所求的結果。（作為合理性檢查，代入 $x = 1$ 得 $\frac{1}{36}(1+35) = 1$。）

一般的 pgf。 由約簡規則，$G_n(x) \equiv G_1(x)^n = \frac{1}{6^n}(x+y)^n$。用二項式定理（binomial theorem）展開：

$$(x+y)^n = x^n + \sum_{k=1}^{n} \binom{n}{k} x^{n-k} y^k.$$

對 $k \geq 1$，利用 $y^k \equiv 5^{k-1} y$（由 $y^2 \equiv 5y$ 用歸納法得出），再利用 $x^{n-k} y \equiv y$，得

$$x^{n-k} y^k \equiv 5^{k-1} y.$$

所以

$$(x+y)^n \equiv x^n + y \sum_{k=1}^{n} \binom{n}{k} 5^{k-1} = x^n + \frac{y}{5}\left[(1+5)^n - 1\right] = x^n + \frac{6^n - 1}{5} y.$$

? **想一想** $(6^n - 1)/5$ 是從哪裏來的？

由二項式定理，和 $\sum_{k=0}^{n} \binom{n}{k} 5^k$ 等於 $(1+5)^n = 6^n$；我們少了 $k = 0$ 那一項（其值為 1），又多了一個因子 $\frac{1}{5}$。因此

$$G_n(x) = \frac{1}{6^n}\left(x^r + \frac{6^n - 1}{5} y\right),$$

其中 r 是 n 除以 5 的餘數（因為 $x^n \equiv x^r$）。所以每個餘數的概率都是 $\dfrac{6^n - 1}{5 \cdot 6^n}$，唯獨餘數 r 額外多了 $\frac{1}{6^n}$。

被 5 整除。 我們需要 $P(T_n = 0)$，即 $G_n(x)$ 的常數項。y 的常數項是 1。

- 若 $5 \nmid n$，則 $r \neq 0$，x^r 對常數項沒有貢獻，所以

$$P(S_n \text{ 可被整除，除數為5}) = \frac{6^n - 1}{5 \cdot 6^n} = \frac{1}{5}\left(1 - \frac{1}{6^n}\right),$$

  正如所求。

- 若 $5 \mid n$，則 $r = 0$，$x^r = 1$ 會加上 $\frac{1}{6^n}$：

$$P(S_n \text{ 可被整除，除數為5}) = \frac{6^n - 1}{5 \cdot 6^n} + \frac{1}{6^n} = \frac{6^n + 4}{5 \cdot 6^n} = \frac{1}{5}\left(1 + \frac{4}{6^n}\right).$$

驗算

- $n = 1$：公式給出 $\frac{1}{5} \cdot \frac{5}{6} = \frac{1}{6}$，而事實上只有擲出 5 才能被 5 整除。
- $n = 2$：公式給出 $\frac{1}{5} \cdot \frac{35}{36} = \frac{7}{36}$。直接計算，和為 5（四種方法）及 10（三種方法）共得 $\frac{7}{36}$，與 $\frac{1}{36}(x^2 + 7y)$ 的常數項吻合。

- $n = 5$：答案是 $\frac{6^5+4}{5\cdot 6^5} = \frac{389}{1944} \approx 0.2001$，略高於 $\frac{1}{5}$。用電腦對 $n \le 8$ 窮舉全部 6^n 種結果，證實了整個 pgf $G_n(x)$ 以及兩種情況。
- 當 $n \to \infty$ 時，兩個答案都趨向 $\frac{1}{5}$：餘數變成均勻分佈。

常見錯誤

- 忘記擲出 6 除以 5 的餘數是 1，因此 G_1 中 x 的係數是 $\frac{2}{6}$。
- 對所有 n 都把 x^n 約簡為 x^0：其實 x^n 約簡為 x^r，其中 r 是 n 的餘數，這正是 $5 \mid n$ 的情況與別不同的原因。
- 用「=」寫出 $G_n(x) = G_1(x)^n$，然後沒有按 $x^5 = 1$ 約簡就直接讀取係數。

STEP 之外

令 $x^m = 1$ 相當於在模 $x^m - 1$ 的多項式環（ring）中運算，即 m 階循環羣（cyclic group）的羣代數（group algebra）。一個等價的工具是單位根濾波（roots-of-unity filter）：$P(m \mid S_n) = \frac{1}{m}\sum_{\omega^m=1} G_S(\omega)$，這正是離散傅立葉變換（discrete Fourier transform）在發揮作用。這個觀點亦解釋了為何循環上隨機步的總和會趨於均勻分佈，而這正是馬爾可夫鏈（Markov chains）與羣上隨機漫步（random walks）理論的起點。Grimmett 與 Welsh 的 *Probability: An Introduction*（《概率導論》）以合適的程度介紹了生成函數與隨機漫步。

Beyond STEP 詳細解答：https://beyondstep.keithmcnulty.org/zh-hant/。解答文字採用 CC0 1.0；題目本身版權屬 Cambridge University Press & Assessment 所有（©），本文件不予轉載。由機器從英文翻譯而成；尚未經審閱。