

單元 2: 仿隨機數的生成

(課本 §3.1)

定義 1. 隨機數 (random number, 亂數) 乃在 $(0, 1)$ 上均勻分布的隨機變數的值, 亦即, 若隨機變數

$$X \sim \text{unif}(0, 1)$$

則

X 的值 $\stackrel{\text{def}}{=}$ 一隨機數

定義 2. 仿 (擬) 隨機數 (pseudorandom numbers) 乃一序列 (串) 的值, 可作為獨立且均為 $\text{unif}(0, 1)$ 分布的隨機變數 $X_1, X_2, \dots, X_n, \dots$ 的值的近似值. 可由一初始值 (initial value) S_0 (又稱作種子, seed) 開始, 經由電腦程式 (乃一種決定公式, 確定公式, 命定公式, deterministic formula) 所產生.

註 1. 由於電腦程式是根據一事先決定 (確定, 命定) 的公式寫成的, 故所產生的值是可預測的, 亦即, 前面的值可決定後面要產生的值, 不符合隨機數 (random numbers) 的獨立性. 但在適當地設計下, 由電腦程式所產生的數與觀念上的, 真正的隨機數在統計意義上並無

差異，所以可被接納為隨機數的近似值，並稱為仿隨機數 (pseudorandom numbers)，以茲區別。

註 2. 一般採用的方法是一種稱作 congruential method 的迭代公式，如下述：

給定種子 S_0

$$S_n = (aS_{n-1} + b) \bmod m$$

$$R_n = S_n/m \text{ (第 } n \text{ 個仿隨機數)}$$

其中 a, b 與 m 需適當地選取以滿足

- (1) 產生的仿隨機數 $R_1, R_2, \dots, R_n, \dots$ 在統計意義上與真正的隨機數無異。
- (2) 在電腦執行上是可行的（例如，避免 overflow 的問題），並是有效率的。

註 3. 大多數的程式語言，數學與統計軟體均附有隨機數生成器，但需驗證其好壞，以免影響模擬的品質。本課程採用自行以 C++ 寫成的隨機數生成器 (generator) `urnd()`。（參考生成器程式檔：`urnd.cpp` 及其用法程式檔：`pseudornd.cpp`）

註 4. 在給定相同的種子 S_0 下, 可得到相同的仿隨機數 (pseudorandom numbers). (以利驗證之用)