

機率圖靈機與隨機複雜度類

完整教材 (依據 5CCS2FC2 Foundations of Computing II 第九週內容編寫)

機率與期望值、機率圖靈機、BPP 與 ZPP

整理自 Dr. Christopher Hampson(King's College London) 之投影片
並參考補充文獻擴充編寫

2026 年 7 月

本週學習目標

1. 複習機率空間、事件、隨機變數與機率質量函數 (p.m.f.)。
2. 掌握期望值與其線性性質、馬可夫不等式、變異數與標準差。
3. 理解機率圖靈機 (PTM): 機率轉移函數、計算樹、分支機率與接受機率。
4. 掌握隨機複雜度類 BPP(有界錯誤) 與 ZPP(零錯誤), 及其對應的蒙地卡羅與拉斯維加斯演算法。
5. 理解定理 $ZPP \subseteq BPP$ 的完整證明 (馬可夫不等式的應用)。
6. 認識擴充後的複雜度階層, 以及 BPP 與 NP、P 之間的未解問題。

Contents

1	機率、事件與隨機變數 (複習)	3
1.1	機率空間	3
1.2	隨機變數	3
2	期望值與變異數	4
2.1	期望值	4
2.2	變異數與標準差	4
3	機率圖靈機 (Probabilistic Turing Machines)	5
3.1	定義	5
3.2	組態、計算樹與分支機率	5
3.3	接受準則	6
3.4	PTM 的量測值都是隨機變數	6
4	隨機複雜度類: BPP 與 ZPP	6
4.1	BPP: 有界錯誤機率多項式時間	6
4.2	ZPP: 零錯誤機率多項式時間	6
4.3	蒙地卡羅 vs. 拉斯維加斯	7

5	定理: $ZPP \subseteq BPP$	7
6	補充:RP、co-RP 與 ZPP 的刻劃	8
7	擴充的複雜度階層	9
8	本週重點整理	10
9	練習題 (附解答)	10
	參考資料	11

1 機率、事件與隨機變數 (複習)

1.1 機率空間

定義 1.1 (樣本空間與機率測度). **樣本空間**是某個隨機過程所有可能結果的集合

$$S = \{\text{所有可能的結果}\} = \{s_1, s_2, \dots, s_n\}.$$

S 上的**機率測度**是一個函數 $\text{Prob} : S \rightarrow [0, 1]$, 滿足 $\sum_{s \in S} \text{Prob}(s) = 1$ 。

定義 1.2 (事件). **事件**是樣本空間的任意子集 $E \subseteq S$ (即 $E \in \mathcal{P}(S)$)。機率測度可延伸到事件上, $\text{Prob} : \mathcal{P}(S) \rightarrow [0, 1]$:

$$\text{Prob}(E) = \sum_{s \in E} \text{Prob}(s).$$

例 1.3 (擲兩顆公平骰子). $S = \{(i, j) : 1 \leq i, j \leq 6\}$, 共 36 個結果, 每個機率 $1/36$ 。事件「點數和為 7」 $= \{(1, 6), (2, 5), (3, 4), (4, 3), (5, 2), (6, 1)\}$, 機率 $= 6/36 = 1/6$ 。

1.2 隨機變數

定義 1.4 (隨機變數). S 上的**隨機變數**是對隨機結果 $s \in S$ 的一種「量測」, 即函數

$$X : S \rightarrow \mathbb{R}.$$

隨機變數 X 取值 $k \in \mathbb{R}$ 的機率為

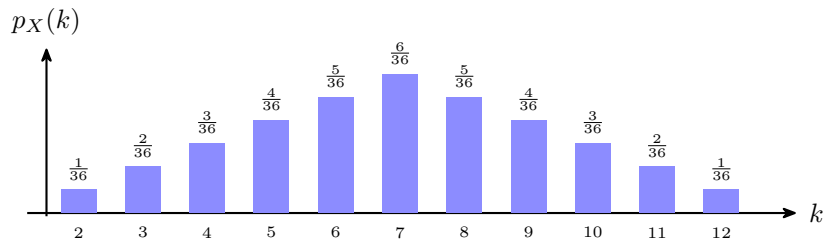
$$\text{Prob}(X = k) = \text{Prob}(\{s \in S : X(s) = k\}),$$

同理 $\text{Prob}(X \leq k) = \text{Prob}(\{s \in S : X(s) \leq k\})$ 。

定義 1.5 (機率質量函數 p.m.f.). 隨機變數 X 的**機率質量函數**描述每個值出現的可能性:

$$p_X(k) = \text{Prob}(X = k).$$

例 1.6 (兩骰點數和的 p.m.f.). 令 $X((i, j)) = i + j$, 其 p.m.f. 呈三角形分布, $k = 7$ 時最大 ($p_X(7) = 6/36$):



2 期望值與變異數

2.1 期望值

定義 2.1 (期望值). 隨機變數 X 的**期望值** (平均) 是其可能值的加權平均:

$$\mathbb{E}[X] = \sum_k k \cdot p_X(k).$$

例 2.2 (灌鉛骰子). 一顆不公平的骰子, 其 p.m.f. 與期望值計算如下:

k	1	2	3	4	5	6	合計
$p_X(k)$	0.15	0.3	0.15	0.1	0.05	0.25	1
$k \cdot p_X(k)$	0.15	0.6	0.45	0.4	0.25	1.5	3.35

故 $\mathbb{E}[X] = 3.35$ (公平骰子則為 3.5)。

定理 2.3 (期望值的線性). 設 X, Y 為任意兩個隨機變數, $a, b \in \mathbb{R}$ 。則:

$$(i) \mathbb{E}[aX + b] = a \mathbb{E}[X] + b;$$

$$(ii) \mathbb{E}[X + Y] = \mathbb{E}[X] + \mathbb{E}[Y].$$

備註 2.4. 性質 (ii) 對任意 X, Y 成立——**不需要獨立性!** 這使它成為分析隨機演算法最有力的工具 (把複雜的隨機量拆成簡單指示變數之和)。

定理 2.5 (馬可夫不等式). 設 X 為非負隨機變數, 期望值為 $\mathbb{E}[X]$ 。則對任何 $a > 0$:

$$\text{Prob}(X \geq a \cdot \mathbb{E}[X]) \leq \frac{1}{a}.$$

Proof. 設 $\mu = \mathbb{E}[X]$ 。由定義

$$\mu = \sum_k k \cdot p_X(k) \geq \sum_{k \geq a\mu} k \cdot p_X(k) \geq a\mu \sum_{k \geq a\mu} p_X(k) = a\mu \cdot \text{Prob}(X \geq a\mu),$$

兩邊除以 $a\mu$ 即得。(第一個不等號丟掉 $k < a\mu$ 的非負項; 第二個把 k 下修為 $a\mu$ 。) □

備註 2.6. 直觀: 「隨機變數超過平均 a 倍的機率, 最多 $1/a$ 」。例如至多 $1/3$ 的機率會超過期望值的 3 倍——這正是第 5 節證明 $\mathbf{ZPP} \subseteq \mathbf{BPP}$ 的關鍵。

2.2 變異數與標準差

變異數要量測「 X 偏離平均 $\mu = \mathbb{E}[X]$ 的程度」。

兩次嘗試

嘗試 1: $\text{Var}[X] \stackrel{?}{=} \mathbb{E}[X - \mu]$? 失敗——由線性, $\mathbb{E}[X - \mu] = \mathbb{E}[X] - \mu = 0$, **恆為零** (正負偏差互相抵消)。

嘗試 2: $\text{Var}[X] \stackrel{?}{=} \mathbb{E}[(X - \mu)^2]$? 成功——平方使所有偏差變正, 是良好的離散程度量測。

定義 2.7 (變異數與標準差). $\text{Var}[X] = \mathbb{E}[(X - \mu)^2]$, 其中 $\mu = \mathbb{E}[X]$ 。標準差為 $\sigma_X = \sqrt{\text{Var}[X]}$ (單位與 X 相同)。

定理 2.8. $\text{Var}[X] = \mathbb{E}[X^2] - \mathbb{E}[X]^2$ 。

Proof. 展開平方並利用線性 (μ 是常數):

$$\mathbb{E}[(X - \mu)^2] = \mathbb{E}[X^2 - 2\mu X + \mu^2] = \mathbb{E}[X^2] - 2\mu \mathbb{E}[X] + \mu^2 = \mathbb{E}[X^2] - 2\mu^2 + \mu^2 = \mathbb{E}[X^2] - \mu^2.$$

□

3 機率圖靈機 (Probabilistic Turing Machines)

3.1 定義

定義 3.1 (機率圖靈機 PTM). 機率圖靈機 $M = \langle \Sigma, Q, q_{\text{init}}, q_{\text{accept}}, q_{\text{reject}}, \delta \rangle$, 其中:

- 字母表 $\Sigma = \{a_1, \dots, a_k\}$ 、有限狀態集 $Q = \{q_1, \dots, q_n\}$ 、初始狀態 $q_{\text{init}} \in Q$ 、接受/拒絕狀態 $q_{\text{accept}}, q_{\text{reject}} \in Q$ ——與一般圖靈機完全相同;
- 唯一的差別是機率轉移函數:

$\delta(\text{目前狀態}, \text{讀到的符號}) \mapsto \text{可能指令上的機率分布},$

其中每條指令屬於 $Q \times (\Sigma \cup \{\sqcup\}) \times \{\leftarrow, \rightarrow\}$ (新狀態、寫入符號、移動方向)。

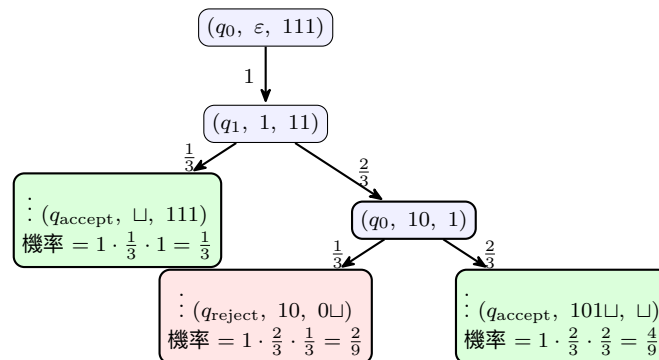
備註 3.2 (與 NDTM 的對照). 非決定性圖靈機 (NDTM) 在分支點「同時探索」所有選項; 機率圖靈機則在分支點擲骰子——依機率分布隨機選一條指令執行。語法上兩者幾乎相同, 差別在接受的語意: NDTM 問「是否存在接受分支」, PTM 問「接受分支的總機率是多少」。等價地, 可把 PTM 想成「多了一條寫滿隨機位元的骰子帶」的決定性圖靈機。

3.2 組態、計算樹與分支機率

PTM 的組態 (configuration) 與一般圖靈機相同, 是機器在某時刻的完整快照:

(目前狀態, 讀寫頭左邊的字串, 讀寫頭所在位置起的右邊字串)。

在輸入 w 上執行 M , 所有可能的組態序列構成一棵計算樹; 每條 (分支) 轉移都帶有機率。一條分支的機率是沿路各轉移機率的乘積。



圖中三片葉的機率 $\frac{1}{3} + \frac{2}{9} + \frac{4}{9} = 1$ (所有分支機率之和恆為 1)。

3.3 接受準則

定義 3.3 (接受機率). PTM M 接受輸入 w 的機率, 是所有通往接受狀態的分支機率之和:

$$\text{Prob}(M(w) = 1) = \text{Prob}(\text{分支}_1 \text{ 或 } \text{分支}_2 \text{ 或 } \dots) = \sum_{\text{所有接受分支}} \text{Prob}(\text{該接受分支}).$$

以上圖為例: $\text{Prob}(M(w) = 1) = \frac{1}{3} + \frac{4}{9} = \frac{7}{9}$, $\text{Prob}(M(w) = 0) = \frac{2}{9}$ 。

3.4 PTM 的量測值都是隨機變數

任何可以附加在單次計算上的數值性質, 都成為一個隨機變數:

- 終止時間 $T(n)$ (走到停機狀態所需步數);
- 使用空間 $S(n)$ (用過的帶格數);
- 進入某特定狀態的次數, 等等。

於是可以討論期望執行時間 $\mathbb{E}[T(n)]$ ——這正是定義 ZPP 所需的觀念。

4 隨機複雜度類: BPP 與 ZPP

4.1 BPP: 有界錯誤機率多項式時間

定義 4.1 (BPP). 語言 L 屬於有界錯誤機率多項式時間 (Bounded-error Probabilistic Polynomial time), 若存在 PTM M 滿足:

- 機率健全 (Sound): 若 $w \notin L$, 則 $\text{Prob}(M(w) = 1) \leq 1/3$;
- 機率完備 (Complete): 若 $w \in L$, 則 $\text{Prob}(M(w) = 1) \geq 2/3$;
- 多項式時間: $T(n) \in O(n^k)$, 對某個 $k > 0$ (最壞情況保證)。

備註 4.2 (1/3 與 2/3 有什麼特別?). 沒有! 任何「與 1/2 隔開一段固定距離」的門檻都定義出同一個類。把演算法獨立重複 t 次取多數決, 由 Chernoff 界, 錯誤機率隨 t 指數下降: 重複 $O(1)$ 次即可把錯誤壓到 2^{-100} 以下——比硬體故障的機率還低。這個技巧稱為機率放大 (amplification)。

4.2 ZPP: 零錯誤機率多項式時間

定義 4.3 (ZPP). 語言 L 屬於零錯誤機率多項式時間 (Zero-error Probabilistic Polynomial time), 若存在 PTM M 滿足:

- 健全: 若 $w \notin L$, 則 $\text{Prob}(M(w) = 1) = 0$;
- 完備: 若 $w \in L$, 則 $\text{Prob}(M(w) = 1) = 1$;
- 期望多項式時間: $\mathbb{E}[T(n)] \in O(n^k)$, 對某個 $k > 0$ 。

注意兩個定義中「放寬的位置」剛好互換: BPP 放寬正確性、堅持最壞時間; ZPP 堅持正確性、放寬時間 (只要求平均多項式)。

4.3 蒙地卡羅 vs. 拉斯維加斯

蒙地卡羅演算法 (Monte Carlo)	拉斯維加斯演算法 (Las Vegas)
執行時間 固定 (決定性上界)	執行時間是 隨機變數
答案可能 出錯 (機率有界)	答案 永遠正確
例: Miller–Rabin 質數測試、Karger 最小割	例: 隨機化快速排序、隨機化選擇
$\text{BPP} = \left\{ \begin{array}{l} \text{可用多項式時間蒙地卡羅} \\ \text{演算法求解的問題} \end{array} \right\}$	$\text{ZPP} = \left\{ \begin{array}{l} \text{可用期望多項式時間拉斯維加斯} \\ \text{演算法求解的問題} \end{array} \right\}$

實際例子

- **Miller–Rabin 質數測試 (蒙地卡羅)**: 每回合用一個隨機底數檢驗; 若 n 是合數, 單回合誤判「質數」的機率 $\leq 1/4$; 重複 t 回合後誤判機率 $\leq 4^{-t}$ 。時間固定、答案可能錯——典型 BPP 風格 (實際上是 one-sided error, 屬於 co-RP)。
- **隨機化快速排序 (拉斯維加斯)**: 隨機選樞軸, 輸出永遠是正確排序; 只有執行時間隨機, 期望 $O(n \log n)$, 最壞 (極低機率) $O(n^2)$ ——典型 ZPP 風格。

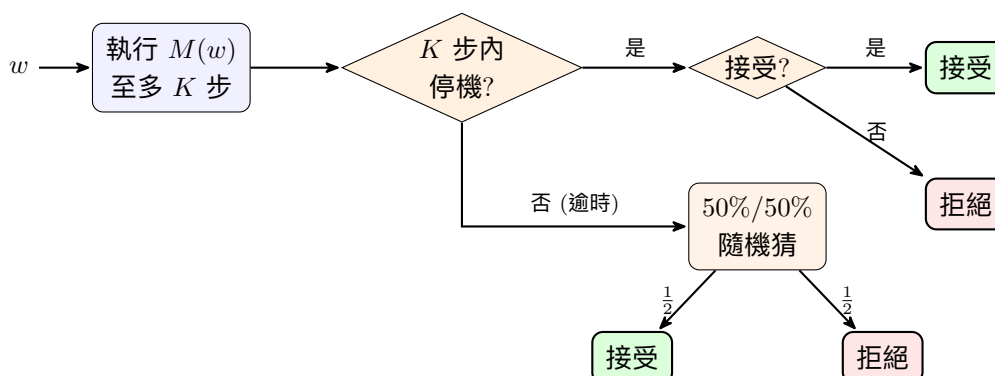
5 定理: $\text{ZPP} \subseteq \text{BPP}$

定理 5.1. $\text{ZPP} \subseteq \text{BPP}$ 。

Proof. **步驟 1.** 設 $L \in \text{ZPP}$, 則存在對 L 健全且完備的 PTM M , 期望執行時間為多項式:

$$\mathbb{E}[T(n)] < c \cdot n^k \quad \text{對某些 } c, k > 0.$$

步驟 2(建構 M'). 令 $K = 3 \cdot \mathbb{E}[T(n)]$, 建構新的 PTM M' :



步驟 3(時間). 依設計, M' 必定在 $K = 3\mathbb{E}[T(n)] \in O(n^k)$ 步內停機——最壞情況多項式時間。

步驟 4(機率健全). 要證: $w \notin L \Rightarrow \text{Prob}(M'(w) = 1) \leq 1/3$ 。
 設 $w \notin L$ 。由 M 健全, M 的任何分支都不會接受 w , 故 M' 錯誤接受的唯一可能是「逾時後亂

猜」。由馬可夫不等式 (定理 2.5, 取 $a = 3$):

$$\text{Prob}(M'(w) = 1) \leq \text{Prob}(T(n) > 3 \cdot \mathbb{E}[T(n)]) \leq \frac{1}{3}.$$

(嚴格說, 逾時機率 $\leq 1/3$ 、猜錯方向機率 $1/2$, 故錯誤接受機率 $\leq 1/6 \leq 1/3$ 。)

步驟 5(機率完備). 要證: $w \in L \Rightarrow \text{Prob}(M'(w) = 1) \geq 2/3$ 。

設 $w \in L$ 。由 M 完備, 只要 M 在 K 步內停機就必定接受; M' 錯誤拒絕的唯一可能同樣是逾時後亂猜:

$$\text{Prob}(M'(w) = 1) \geq 1 - \text{Prob}(T(n) > 3 \cdot \mathbb{E}[T(n)]) \geq 1 - \frac{1}{3} = \frac{2}{3}.$$

步驟 6. M' 是多項式時間的蒙地卡羅演算法, 滿足 BPP 的三個條件, 故 $L \in \text{BPP}$ 。 □

備註 5.2 (證明的本質). 「期望時間多項式」透過馬可夫不等式轉成「大機率在 3 倍期望時間內停機」; 把長尾截斷、用擲硬幣補上答案, 就把時間的不確定性轉換成答案的不確定性——正是 ZPP 與 BPP 兩種放寬方式之間的橋樑。

6 補充: RP、co-RP 與 ZPP 的刻劃

介於「零錯誤」與「雙邊錯誤」之間, 還有單邊錯誤的類:

定義 6.1 (RP 與 co-RP). 語言 $L \in \text{RP}$ (Randomized Polynomial time), 若存在多項式時間 PTM M :

- 若 $w \notin L$: $\text{Prob}(M(w) = 1) = 0$ (說「是」絕不出錯);
- 若 $w \in L$: $\text{Prob}(M(w) = 1) \geq 1/2$ (說「否」可能出錯)。

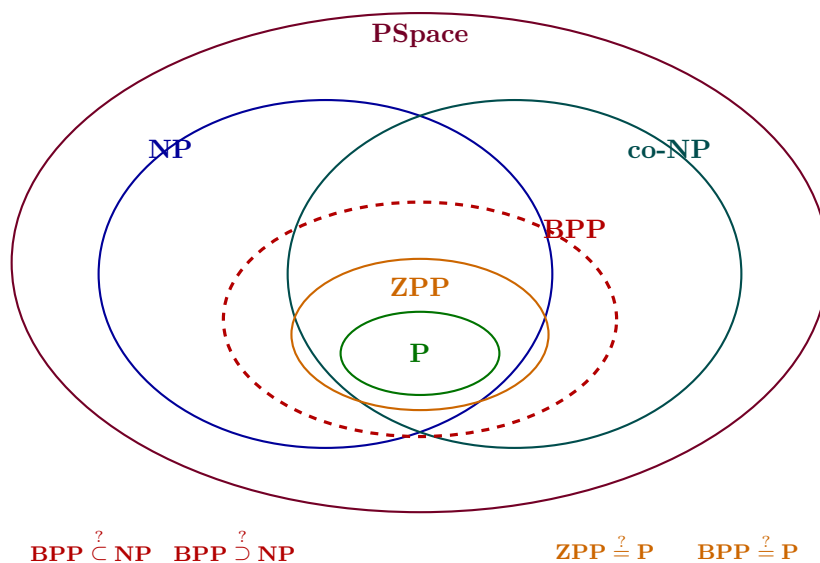
co-RP 則相反: $w \in L$ 時必答「是」; $w \notin L$ 時以機率 $\geq 1/2$ 答「否」。

定理 6.2. $\text{ZPP} = \text{RP} \cap \text{co-RP}$ 。

證明概要. ($\subseteq$) 與定理 5.1 同法: 把 ZPP 機器截斷在 3 倍期望時間; 逾時一律「拒絕」得 RP 機器, 一律「接受」得 co-RP 機器。

($\supseteq$) 設 L 同時有 RP 機器 M_1 與 co-RP 機器 M_2 。交替執行: 若 M_1 接受, 答案確定是「 $w \in L$ 」(RP 說「是」不會錯); 若 M_2 拒絕, 確定「 $w \notin L$ 」。兩者都沒給確定答案就重來。每一輪得到確定答案的機率 $\geq 1/2$, 期望輪數 ≤ 2 , 故期望時間多項式且永不出錯——即 ZPP (拉斯維加斯) 機器。 □

7 擴充的複雜度階層



已知的包含關係 (未知是否嚴格):

$$P \subseteq ZPP = RP \cap co-RP \subseteq RP \cup co-RP \subseteq BPP \subseteq PSpace.$$

未解問題與現代觀點

- **BPP 與 NP 的關係完全未知:** 不知道 $BPP \subseteq NP$ 、 $NP \subseteq BPP$, 或兩者皆非。若 $NP \subseteq BPP$, 則 NP-complete 問題有實用的隨機演算法——被認為極不可能。
- **主流猜想:** $P = BPP$ (隨機性沒有本質幫助)。若存在夠強的偽隨機數產生器, 即可用決定性方式模擬所有隨機演算法 (去隨機化, derandomization); Impagliazzo–Wigderson (1997) 證明: 若某些指數時間問題需要指數大小電路, 則 $P = BPP$ 。
- **歷史例證:** 質數測試曾長期只有隨機演算法 (Miller–Rabin $\in co-RP$), 直到 AKS (2002) 給出決定性多項式演算法, 證明 $PRIMES \in P$ ——隨機性「先行、決定性追上」的經典案例。
- 另外已知 $BPP \subseteq P/poly$, 且 $BPP \subseteq \Sigma_2 \cap \Pi_2$ (多項式階層第二層)。

8 本週重點整理

主題	重點
機率空間	樣本空間 S 、 $\text{Prob} : S \rightarrow [0, 1]$; 事件 $E \subseteq S, \text{Prob}(E) = \sum_{s \in E} \text{Prob}(s)$
隨機變數	$X : S \rightarrow \mathbb{R}$; p.m.f. $p_X(k) = \text{Prob}(X = k)$
期望值	$\mathbb{E}[X] = \sum_k k p_X(k)$; 線性: $\mathbb{E}[aX + b] = a\mathbb{E}[X] + b$ 、 $\mathbb{E}[X + Y] = \mathbb{E}[X] + \mathbb{E}[Y]$ (不需獨立)
馬可夫不等式	$\text{Prob}(X \geq a \mathbb{E}[X]) \leq 1/a$ (非負 X)
變異數	$\text{Var}[X] = \mathbb{E}[(X - \mu)^2] = \mathbb{E}[X^2] - \mathbb{E}[X]^2$; $\sigma_X = \sqrt{\text{Var}[X]}$
PTM	轉移函數給出指令的機率分布; 分支機率 = 沿路乘積; $\text{Prob}(M(w) = 1) = \sum$ 接受分支機率
BPP	錯誤機率 $\leq 1/3$ (雙邊)、最壞時間多項式; 蒙地卡羅; 可放大到任意小錯誤
ZPP	永不出錯、期望時間多項式; 拉斯維加斯; $\text{ZPP} = \text{RP} \cap \text{co-RP}$
$\text{ZPP} \subseteq \text{BPP}$	截斷在 $3\mathbb{E}[T]$ 步 + 逾時擲硬幣; 馬可夫不等式給出 $\leq 1/3$ 錯誤
階層	$\text{P} \subseteq \text{ZPP} \subseteq \text{BPP} \subseteq \text{PSPACE}$; 猜想 $\text{P} = \text{BPP}$; BPP vs NP 未知

9 練習題 (附解答)

練習 1. 擲一顆公平骰子, 令 X 為點數。求 $\mathbb{E}[X]$ 、 $\mathbb{E}[X^2]$ 與 $\text{Var}[X]$ 。

解答

$$\mathbb{E}[X] = \frac{1+2+\dots+6}{6} = 3.5; \mathbb{E}[X^2] = \frac{1+4+9+16+25+36}{6} = \frac{91}{6} \approx 15.17; \text{Var}[X] = \mathbb{E}[X^2] - \mathbb{E}[X]^2 = \frac{91}{6} - 12.25 = \frac{35}{12} \approx 2.92。$$

練習 2. 某拉斯維加斯演算法的期望執行時間為 $100n^2$ 步。用馬可夫不等式估計: 執行超過 $10^4 n^2$ 步的機率至多是多少?

解答

$$10^4 n^2 = 100 \cdot (100n^2) = 100 \cdot \mathbb{E}[T], \text{ 取 } a = 100: \text{Prob}(T \geq 100 \mathbb{E}[T]) \leq \frac{1}{100}。$$

練習 3. 在計算樹範例中, 若把分支機率 $\frac{1}{3}/\frac{2}{3}$ 改為 $\frac{1}{2}/\frac{1}{2}$ (兩處皆改), 接受機率變為多少?

解答

$$\text{三片葉的機率變為: 接受 } \frac{1}{2} \text{、拒絕 } \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} \text{、接受 } \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}。 \text{ 故 } \text{Prob}(M(w) = 1) = \frac{1}{2} + \frac{1}{4} = \frac{3}{4}。$$

練習 4. 為什麼 BPP 定義中的 $(1/3, 2/3)$ 可以換成 $(0.49, 0.51)$ 甚至 $(1/2 - 1/n^c, 1/2 + 1/n^c)$ 而不改變這個類?

解答

用機率放大: 獨立重複 t 次取多數決。只要單次正確機率與 $1/2$ 有間隔 ε , Chernoff 界給出多數決出錯機率 $\leq e^{-2\varepsilon^2 t}$ 。取 t 為適當多項式 (如 $\varepsilon = 1/n^c$ 時取 $t = O(n^{2c+1})$), 即可把錯誤壓回 $1/3$ 以下, 總時間仍是多項式。故所有這些門檻定義同一個類。

練習 5. 在 $ZPP \subseteq BPP$ 的證明中, 為什麼截斷步數取 $K = 3\mathbb{E}[T(n)]$ 而不是 $\mathbb{E}[T(n)]$?

解答

若只跑 $\mathbb{E}[T(n)]$ 步, 馬可夫不等式 ($a = 1$) 只給出逾時機率 ≤ 1 ——毫無用處。取 $a = 3$ 才能保證逾時機率 $\leq 1/3$, 使錯誤機率落在 BPP 要求的界內。(任何 $a > 2$ 皆可, 取 3 恰好對齊 $1/3$ 、 $2/3$ 門檻。)

練習 6 (思考題). 把 Miller–Rabin(合數時誤判機率 $\leq 1/4$ 、質數時必答「質數」) 歸類: 它證明 PRIMES 屬於 RP、co-RP 還是 BPP?

解答

以 $L = \text{PRIMES}$ 來看: $w \in L$ (質數) 時必答「是」; $w \notin L$ (合數) 時答「是」的機率 $\leq 1/4 \leq 1/2$ 。「說『否』絕不出錯」= co-RP 的定義 (對 L 而言單邊錯誤在「是」端), 故 $\text{PRIMES} \in \text{co-RP}$ (等價地 $\text{COMPOSITES} \in \text{RP}$); 又 $\text{co-RP} \subseteq \text{BPP}$, 故也在 BPP。2002 年 AKS 更證明了 $\text{PRIMES} \in \text{P}$ 。

參考資料

1. C. Hampson, *5CCS2FC2 Foundations of Computing II, Week 9* 投影片 (probability / PTM / BPPvsZPP), King's College London.
2. S. Arora, B. Barak, *Computational Complexity: A Modern Approach*, Cambridge Univ. Press, 2009.(第 7 章: Randomized Computation)
3. M. Sipser, *Introduction to the Theory of Computation*, 3rd ed., Cengage, 2013. (§10.2 機率演算法)
4. R. Motwani, P. Raghavan, *Randomized Algorithms*, Cambridge Univ. Press, 1995.
5. R. Impagliazzo, A. Wigderson, "P = BPP if E requires exponential circuits," *STOC*, 1997.
6. M. Agrawal, N. Kayal, N. Saxena, "PRIMES is in P," *Annals of Mathematics*, 160:781–793, 2004.
7. Wikipedia: *BPP (complexity)*; *ZPP (complexity)*; *RP (complexity)*; *Probabilistic Turing machine*; *Monte Carlo algorithm*; *Las Vegas algorithm*.