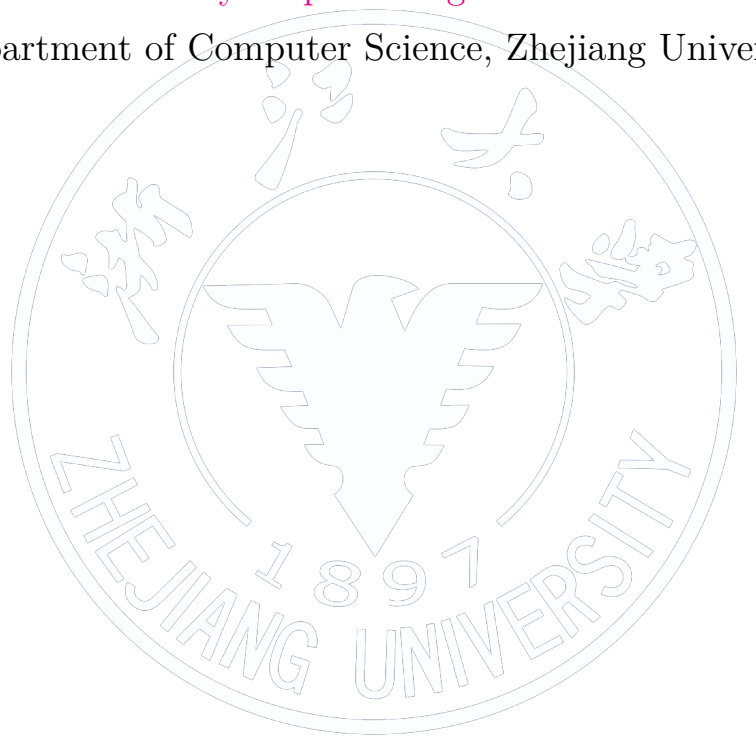
離散數學

Discrete Mathematics

TZU-CHUN HSU[1]

[1]vm3y3rmp40719@gmail.com

[1]Department of Computer Science, Zhejiang University



2020 年 11 月 25 日

Version 2.0

Disclaimer

本文「離散數學」為台灣研究所考試入學的「離散數學」考科使用，內容主要參考黃子嘉先生的三本離散數學參考書 [1][2][3]，以及 wjungle 網友在 PTT 論壇上提供的離散數學筆記 [4]。

本文作者為 TZU-CHUN HSU，本文及其 LaTeX 相關程式碼採用 **MIT 協議**，更多內容請訪問作者之 GitHub 分頁Oscarshu0719。

1 Overview

1. 本文頁碼標記依照實體書 [1][2][3] 的頁碼。
2. TKB 筆記 [4] 章節頁碼：

Chapter	Page No.
1	1
2	26
3	60
4	78
5	92
6	118
7	152
8	168
9	176
10	207
11	223
12	×
13	227

3. 1.2 考很重，2.5 少考，4.2 考不多，4.3 不是很重要。前 7 章佔 70%，第 9, 10, 13 章各 10%。
4. 第 9, 10, 11, 13 章暫時略過。
5. 必考：（參考 TKB 筆記 [4] 中頁碼）
   (a) 6
   (b) 11
   (c) 14
   (d) 31
   (e) 32
   (f) 41
   (g) 43
   (h) 53
   (i) 54
   (j) 74

(k) 89

(l) 107

(m) 111

(n) 127

(o) 134

(p) 136

(q) 137

(r) 143

(s) 144

(t) 154

(u) 157

(v) 170

6. 證明：（參考 TKB 筆記 [4] 中頁碼）

(a) 6

(b) 56

(c) 58

(d) 76

(e) 129

(f) 152

7. 三角函數：

- 和角公式：

$$\sin(\alpha+\beta) = \sin\alpha\cos\beta + \cos\alpha\sin\beta \tag{1a}$$

$$\sin(\alpha-\beta) = \sin\alpha\cos\beta - \cos\alpha\sin\beta \tag{1b}$$

$$\cos(\alpha+\beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta \tag{1c}$$

$$\cos(\alpha-\beta) = \cos\alpha\cos\beta + \sin\alpha\sin\beta \tag{1d}$$

- 和差化積：

$$\sin\alpha+\sin\beta=2\sin\frac{\alpha+\beta}{2}\cos\frac{\alpha-\beta}{2} \tag{2a}$$

$$\sin\alpha-\sin\beta=2\cos\frac{\alpha+\beta}{2}\sin\frac{\alpha-\beta}{2} \tag{2b}$$

$$\cos\alpha+\cos\beta=2\cos\frac{\alpha+\beta}{2}\cos\frac{\alpha-\beta}{2} \tag{2c}$$

$$\cos\alpha-\cos\beta=-2\sin\frac{\alpha+\beta}{2}\sin\frac{\alpha-\beta}{2} \tag{2d}$$

- 積化和差：

$$2\sin\alpha\cos\beta=\sin(\alpha+\beta)+\sin(\alpha-\beta) \tag{3a}$$

$$2\cos\alpha\sin\beta=\sin(\alpha+\beta)-\sin(\alpha-\beta) \tag{3b}$$

$$2\cos\alpha\cos\beta=\cos(\alpha+\beta)+\cos(\alpha-\beta) \tag{3c}$$

$$2\sin\alpha\sin\beta=\cos(\alpha+\beta)-\cos(\alpha-\beta) \tag{3d}$$

2 Summary

1. **Theorem (1.16)**

$$P(A \cup B) \neq P(A) \cup P(B) \tag{4a}$$
$$P(A \cap B) = P(A) \cap P(B) \tag{4b}$$

2. **Theorem (1-42)1.92** $2^{mn} \pmod{2^m - 1} = 1$。

3. **Theorem (1.58, 1.60)**（質數）

   - 若 $a \in \mathbb{Z}, n \in \mathbb{Z}^+$，且 $\gcd(a, n) = 1$，則 $a^{-1} \pmod{n}$ 存在。
   - 若 p 為質數，$a \in \mathbb{Z}$，則 $a^{-1} \equiv a \pmod{p}$ 即 $a^2 \equiv 1 \pmod{p} \iff a \equiv \pm 1 \pmod{p}$。

4. **Theorem (1.61, 1.62)**（質數）

   - Wilson's theorem：若 p 為質數，則

$$(p-1)! \equiv -1 \pmod{p} \tag{5}$$

   - Fermat's little theorem：若 p 為質數，$m \in Z$，且 $\gcd(m, p) = 1$，則

$$m^{p-1} \equiv 1 \pmod{p} \tag{6}$$

5. **Theorem (1.64, 1.65, 1.66)**（質數）

   - 若 $p \in \mathbb{Z}^+$，則 $\phi(p) = p - 1 \iff p$ 為質數。
   - 若 $m \in \mathbb{Z}, n \in \mathbb{Z}^+$，且 $\gcd(m, n) = 1$，則 $m^{\phi(n)} \equiv 1 \pmod{n}$。
   - 若 p 為質數，$m \in Z$，且 $\gcd(m, p) = 1$，則 $m^{-1} \equiv m^{p-2} \pmod{p}$

6. **Theorem (1.71)** RSA 公鑰密碼系統（RSA public key cryptosystem）：

   - 訊息：M。
   - 加密鑰（encryption key）：

$$n = pq,\ e \tag{7}$$

   其中 p, q 為質數，且 $\gcd(e, \phi(n)) = 1,\ \phi(n) = (p-1)(q-1)$。

- 加密訊息：

$$C = M^e \pmod{n} \tag{8}$$

- 解密鑰（decryption key）：

$$d \equiv e^{-1} \pmod{\phi(n)} \tag{9}$$

- 解密訊息：

$$C^d \equiv M \pmod{n} \tag{10}$$

7. **Theorem (2.18, 2.25)**

- 若 A 為集合，$R \subseteq A \times A$ 為一關係，則 R 具遞移性 $\iff R^n \subseteq R,\ \forall n \in \mathbb{Z}^+$。
- 若 A 為集合，$R, S \subseteq A \times A$ 為二關係，則
  - 若 R, S 具反身性，則 $R \cap S$ 與 $R \cup S$ 亦具反身性。
  - 若 R, S 具對稱性，則 $R \cap S$ 與 $R \cup S$ 亦具對稱性。
  - 若 R, S 具遞移性，則 $R \cap S$ 亦具遞移性。

8. **Theorem (2.53, 2.55)**

- $t(s(r(R)))$ **未必**等於 $t(R) \cup r(R) \cup r(R)$。
- 若 R_1, R_2 為二等價關係，其分割分別為 π_1 與 π_2，則
  - $R_1 \cap R_2$ 為等價關係，且分割為 $\pi_1 \cdot \pi_2$。
  - $R_1 \cup R_2$ **未必**為等價關係，因為 $R_1 \cup R_2$ **未必**具遞移性，而 $t(R_1 \cup R_2)$ 為等價關係，且分割為 $\pi_1 + \pi_2$。

9. **Theorem (2.63, 2.66, 2.67, 2.69, 2.70, 2.71, 2.74)**

- 若 $f:\ A \to B$，$A_1, A_2 \subseteq A$，則
  - 若 $A_1 \subseteq A_2$，則 $f(A_1) \subseteq f(A_2)$。
  - $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$。
  - $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$。
  - f 為一對一 $\iff f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$
- 若 $f:\ A \to B, g:\ B \to C$，則
  - 若 f, g 為一對一，則 $g \circ f$ 亦是一對一，反之不然。
  - 若 f, g 為映成，則 $g \circ f$ 亦是映成，反之不然。
  - 若 f, g 可逆，則 $g \circ f$ 亦可逆，反之不然。

  - 若 $g \circ f$ 為一對一，則 f 亦是一對一。
  - 若 $g \circ f$ 為映成，則 g 亦是映成。
- 若 $f : A \to B$，$B_1, B_2 \subseteq B$，則
  - 若 $B_1 \subseteq B_2$，則 $f^{-1}(B_1) \subseteq f^{-1}(B_2)$。
  - $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$。
  - $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$。

10. **Theorem (2.96, 2.99, 2.100, 2.101, 2.102)**

- 若 $\{A_i\}_{i \in \mathbb{Z}^+}$ 為可數集，則 $\bigcup_{i \in \mathbb{Z}^+} A_i$ 為可數集。
- $\mathbb{Q}^+, \mathbb{Q}, \mathbb{Z}^+ \times \mathbb{Z}^+$ 皆為可數集。
- $(0,1) \sim \mathbb{R}, \mathbb{R}, \overline{\mathbb{Q}}, \mathbb{C} \sim \mathbb{R}$ 皆為不可數集。
- $|\mathbb{Z}| = |\mathbb{Z}^+| = |\mathbb{Q}| < |\overline{Q}| = |\mathbb{R}| = |\mathbb{C}|$

11. **Theorem (3.23, 3.24)**

- $$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r} \tag{11}$$
- Vandermonde's convolution：
$$\sum_{k=0}^{n} \binom{r}{k} \binom{s}{n-k} = \binom{r+s}{n} \tag{12}$$

12. **Theorem (3.50, 3.56, 3.57, 3.59, 3.60)**

- m 個相異物放入 n 個相同箱（不允許空箱）：
$$\mathrm{S}(m,n) = \frac{\mathrm{onto}(m,n)}{n!} = \frac{\sum_{i=0}^{n} (-1)^i \binom{n}{i} (n-i)^m}{n!}, \ \forall m \geq n \geq 1 \in \mathbb{Z}^+ \tag{13}$$
- – m 個相異物放入 n 個相同箱（允許空箱）。
  – 若 A 為一集合，且 $|A| = m$，則 A 上等價關係的個數，即相異分割數。
$$\sum_{i=1}^{n} \mathrm{S}(m,i) \tag{14}$$
- $$\mathrm{S}(m+1,n) = \mathrm{S}(m,n-1) + n\mathrm{S}(m,n), \ \forall m \geq n \geq 2 \in \mathbb{Z}^+ \tag{15}$$

13. **Theorem (6.6, 6.7, 6.8, 6.9, 6.10, 6.11, 6.12, 6.16, 6.18)**

- 若 $G = (V, E)$, $|V| = n$，則

$$|E| \geq \binom{n-1}{2} + 1 \tag{16}$$

時，G 為連通圖。

14. **Theorem (6.44, 6.47, 6.55)**

- 一簡單無向圖，若所有點的度數至數為 k，則圖上必含一個長度至少為 $k+1$ 的環路（cycle）。
- 若 A 為一鄰接矩陣，則 $\frac{1}{6}\operatorname{tr}(A^3)$ 為圖上三角形個數。

15. **Theorem (6.57, 6.59, 6.60, 6.62)**

- 圖中有尤拉迴路 $\iff$ 為連接圖且所有點的度數為偶數。
- K_n 有尤拉迴路 $\iff$ n 為奇數。
- $K_{m,n}$ 有尤拉迴路 $\iff$ m, n 為偶數。
- 圖中有尤拉路線 $\iff$ 為連通圖且圖中恰含 0 個或 2 個點度數為奇數。
- 圖中有尤拉迴路 $\iff$ 為強連通圖且所有點的出度數與入度數相同。

16. **Theorem (6.64, 6.68, 6.71, 6.72, 6.73, 6.74, 6.84)**

- 有向完全圖必有有向漢米爾頓**路徑**。
- 若 $G = (V, E)$, $|V| = n \geq 3$ 為一無迴圈無向圖，
  - 若

$$\begin{aligned} &\deg(x) + \deg(y) \geq n-1,\ \forall x, y \in V, x \neq y \vee \\ &\deg(v) \geq \frac{n-1}{2},\ \forall v \in V \end{aligned} \tag{17}$$

    ，則 G 有漢米爾頓**路徑**。
  - 若

$$\begin{aligned} &\deg(x) + \deg(y) \geq n,\ \forall x, y \in V, x, y \text{ 不相鄰} \vee \\ &\deg(v) \geq \frac{n}{2},\ \forall v \in V \end{aligned} \tag{18}$$

    ，則 G 有漢米爾頓**環路**。
- $K_n, n \geq 3$ 必有漢米爾頓**環路**。

- 若一圖有漢米爾頓環路，則該圖中任兩點至少有兩條路徑相連。
- 一連通雙分圖，若圖中有漢米爾頓**環路**，則兩邊的頂點數相同。
- 一連通雙分圖，若圖中有漢米爾頓**路徑**，則兩邊的頂點數相差 ≤ 1。
- K_n 有 $\frac{(n-1)!}{2}$ 個相異漢米爾頓環路。
- K_n，n 為奇數，有 $\leq \frac{n-1}{2}$ 個**不共邊**的漢米爾頓環路。
- $K_{n,n}$ 有 $\frac{1}{2}n!(n-1)!$ 個相異漢米爾頓環路。
- 若 $G=(V,E)$, $|V|=n$，則

$$|E| \geq \binom{n-1}{2} + 2 \tag{19}$$

時，G 有漢米爾頓**環路**。

17. **Theorem (6.88, 6.90, 6.93, 6.94, 6.97, 6.98)**

- Euler formula：若 $G=(V,E), |V|=v, |E|=e, r$為區域個數, M為分量圖數，且 G 為平面圖，則 $v-e+r=1+M$。
- 若 $G=(V,E), |V|=v, |E|=e \geq 2, r$為區域個數，且 G 為無迴圈簡單**連通**平面圖，則
  - $$\frac{3}{2}r \leq e \leq 3v-6 \tag{20}$$
  - 若 G **不含任何三角形**，則
  $$e \leq 2v-4 \tag{21}$$
  - 若每個環路 $\geq k \geq 3$ 邊組成，則
  $$e \leq \frac{k}{k-2}(v-2) \tag{22}$$
- 雙分圖不含三角形。
- 一無迴圈簡單平面圖必含一個度數 ≤ 5 的頂點。

18. **Theorem (6.109, 6.110, 6.113, 6.114, 6.115, 6.116)**

- $\chi(K_n)=n$，$\chi(W_n)=1+\chi(C_n)$，$\chi(C_n)=\begin{cases}2, & n=2k\\ 3, & n=2k+1\end{cases}$。

- 若 K_n 為一圖 G 的子圖，則 $\chi(G) \geq n$。
- 若 $G = (V, E)$ 為無向圖，λ 為顏色數，則稱 $P(G, \lambda)$ 為著色多項式，表示至多使用 λ 種顏色著色的不同方法數，且 $\chi(G) = \min\{\lambda | P(G, \lambda) > 0\}$。
  - $P(G, \lambda)$ 常數項為 0。
  - $P(G, \lambda)$ 係數和為 0。
  - $P(G, \lambda)$ 最高次項係數為 1。

19. **Theorem (7.5, 7.9, 7.15, 7.16, 7.18, 7.20, 7.22, 7.24, 7.28)**

- 樹：$|E| = |V| - 1$。
- 森林：$|E| = |V| - \kappa(G)$，其中 $\kappa(G)$ 表示樹的個數。
- – 滿（full）二叉樹：非樹葉節點都有二個兒子。
  - 完全（complete）二叉樹：所有樹葉節點的階層皆與樹高相同。
  - 平衡（balanced）二叉樹：若樹高為 h，則所有樹葉節點的階層皆為 h 或 $h-1$。
- 若 $T = (V, E), |V| = n$ 為 m-元樹，其中 i, l 分別表示內部節點與樹葉個數，則
  -
  $$n \leq mi + 1 \tag{23}$$
  -
  $$l \leq (m-1)i + 1 \tag{24}$$

  當 T 為**滿** m-元樹時，等號成立。
- 若 $T = (V, E), |V| = n$ 為**滿** m-元樹，其中 l, h 分別表示樹葉個數與樹高，則

$$(m-1)(h-1) + m \leq l \leq m^h$$
$$mh + 1 \leq n \leq \frac{m^{h+1} - 1}{m - 1} \tag{25}$$
$$h \geq \lceil log_m l \rceil \quad T\text{為平衡樹時，等號成立}$$

- 一滿 m-元樹，i 為內部節點個數，I, E 分別表示內部及外部路徑長，則

$$E = (m-1)I + mi \tag{26}$$

20. **Theorem (7.30, 7.33, 7.34, 7.35, 7.37, 7.44, 7.46, 7.49)**

- 若 G 為無向圖，則 G 為連通圖 $\iff$ G 有生成樹。

- K_n 相異生成樹個數為 n^{n-2}。
- $K_{m,n}$ 相異生成樹個數為 $m^{n-1}n^{m-1}$。
- 若 $G=(V,E)$ 為無向圖，且 $e=\{a,b\}\in E$，$N(G)$ 為 G 的相異生成樹個數，則

$$N(G)=N(G-e)+N(G\cdot e) \tag{27}$$

- 生成樹的任一邊稱分枝（branch），是原圖的邊但不為生成樹的邊稱弦（chord）。若 $G=(V,E),|V|=v,|E|=e$，則
  - 生成樹必含 $v-1$ 分支與 $e-v+1$ 弦。
  - 若將任意弦加入生成樹，則新圖必含一環路，稱該環路為基本環路（fundamental cycle）。
  - 若生成樹切除任意分支，則新圖變不連通，稱 G 中該切集為基本切集（fundamental cut set）。
- 一無向連通圖，其任意切集與環路必含**偶數**個共同邊。

21. **Theorem (8.43)** 若 n 為奇數時，K_n **不**具完美配對；若 n 為偶數時，K_n 具完美配對。

References

[1] 黃子嘉. 離散數學（上）. 鼎茂圖書出版股份有限公司, 5 edition, 2010.

[2] 黃子嘉. 離散數學（下）. 鼎茂圖書出版股份有限公司, 5 edition, 2010.

[3] 黃子嘉. 離散數學（習題詳解）. 鼎茂圖書出版股份有限公司, 6 edition, 2019.

[4] wjungle@ptt. 離散數學 @tkb 筆記. https://drive.google.com/file/d/0B8-2o6L73Q2VVXFqS3liaXpjLTQ/view?usp=sharing, 2017.