

離散數學

Discrete Mathematics

TZU-CHUN HSU¹

¹vm3y3rmp40719@gmail.com

¹Department of Computer Science, Zhejiang University



2021 年 1 月 28 日
Version 4.0

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](#)。

MIT License

Copyright (c) 2020 TZU-CHUN HSU

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

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。

2 Summary

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

2. **Theorem (1.60)** (質數) 若 p 為質數, $a \in \mathbb{Z}$, 則 $a^{-1} \equiv a \pmod{p}$ 即 $a^2 \equiv 1 \pmod{p} \iff a \equiv \pm 1 \pmod{p}$ 。

3. **Theorem (1.61, 1.62)** (質數)

- Wilson's theorem: 若 p 為質數, 則

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

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

$$m^{p-1} \equiv 1 \pmod{p} \quad (2)$$

4. **Theorem (1.65, 1.66)** (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, $m \in \mathbb{Z}$, 且 $\gcd(m, p) = 1$, 則 $m^{-1} \equiv m^{p-2} \pmod{p}$

5. **Theorem (1.74)** (質數) If $2^n - 1$ is prime, then n is prime.

6. **Theorem (.14)** 證明 \mathbb{Z}^+ 中質數個數為 ∞ 。

Proof. 若質數個數為有限個, 令

$$P_1, P_2, \dots, P_k \quad (3)$$

為所有質數。取

$$E = P_1 P_2 \cdots P_k + 1 \quad (4)$$

所以 E 為 composite, 則

$$\exists P_j \quad \text{s.t. } P_j | E \quad (5)$$

又

$$\begin{aligned} P_j &| P_1 P_2 \cdots P_k \\ \Rightarrow P_j &| (E - P_1 P_2 \cdots P_k) \\ \Rightarrow P_j &| 1 \end{aligned} \quad (6)$$

但質數 P_j 不可能整除 1，矛盾，因此 $P_j = 1$ ， E 為質數。得證， \mathbb{Z}^+ 中質數個數為 ∞ 。

7. **Theorem (2.101)** 證明 $(0, 1)$ 為不可數集。

Proof. $f : \mathbb{Z}^+ \rightarrow (0, 1)$ is bijective, 令 $f(i) = r_i, \forall i = 1, 2, 3, \dots$ 其中

$$\begin{cases} r_1 = 0.r_{11}r_{12}\cdots \\ r_2 = 0.r_{21}r_{22}\cdots \\ \vdots \\ r_i = 0.r_{i1}r_{i2}\cdots \end{cases} \quad (7)$$

取

$$s = 0.s_1s_2\cdots, s_i = \begin{cases} 4, & r_{ii} \neq 4 \\ 5, & r_{ii} = 4 \end{cases} \quad (8)$$

$s_i \in (0, 1)$ 但 $\nexists i \in \mathbb{Z}^+$ s.t. $f(i) = s$, 因此 $(0, 1)$ 為不可數集。

8. **Theorem (.53)**

$$A = \{1, 2, \dots, 2n\} \quad (9)$$

在 A 取 $N + 1$ 個數，

$$\exists a, b \text{ s.t. } a|b \vee b|a \quad (10)$$

Proof.

$$\forall x \in A, x = 2^k \times y, k \in \mathbb{Z}, y = 2l + 1, l \in \mathbb{Z} \quad (11)$$

又 A 中只有 n 個奇數，則取 $n + 1$ 個數時，

$$\begin{aligned} \exists a, b \text{ s.t. } a = 2^{k_1} \times y, b = 2^{k_2} \times y \\ a|b \vee b|a \end{aligned} \quad (12)$$

9. **Theorem (3.56)**

- 若 A 為一集合，且 $|A| = m$ ， A 上等價關係的個數，即相異分割數。

$$\sum_{i=1}^m S(m, i) \quad (13)$$

- m 相異物放入 n 相同箱可空箱的方法。

$$\sum_{i=1}^n S(m, i) \quad (14)$$

10. **Theorem ((5-35)5.56)** Ordered sum of positive integers, where each summand is ≥ 2 :

$$\begin{cases} a_n = a_{n-1} + a_{n-2} & , n \geq 2 \\ a_1 = 0, a_2 = 1 \end{cases} \quad (15)$$

11. **Theorem (6.35)** 若 G 與 \overline{G} 同構, 且 $|V| = n$, 則 $n = 4k \vee n = 4k + 1$ 。

12. **Theorem (6.44, 6.55)**

- 一簡單無向圖, 若所有點的度數 $\geq k$, 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
 - $\frac{1}{6} \text{tr}(A^3)$ 為圖上三角形個數。
 -

$$\sum_{i=1}^n \sum_{j=1}^n A^2[i, j] = \sum_{i=1}^n \deg(v_i)^2 \quad (16)$$

13. **Theorem ((6-30)6.48)**

- Maximum length of a **trail** of K_n is $\binom{2n}{2} - (n - 1)$.
- Maximum length of a **circuit** of K_n is $\binom{2n}{2} - n$.

14. **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。
- 若圖中有尤拉迴路, 則有尤拉路線。

15. **Theorem (6.68, 6.71, 6.72, 6.73, 6.74, 6.84, (6-51)6.81)**

- K_n^* 必定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

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

，則 G 有漢米爾頓路徑。

- 若

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

，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

$$|E| \geq \binom{n-1}{2} + 2 \quad (19)$$

時， G 有漢米爾頓環路。

16. Theorem (6.93, 6.94, 6.97, 6.98, (6-51)6.81)

- 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, M 為分量圖數, 且 G 為無迴圈簡單連通平面圖, 則

$$\frac{3}{2}r \leq e \leq 3v - 6 \quad (20)$$

– 若 G 不含任何三角形，則

$$e \leq 2v - 4 \quad (21)$$

– 若每個環路 $\geq k \geq 3$ 邊組成，則

$$e \leq \frac{k}{k-2}(v - 2M) \quad (22)$$

- 一無迴圈簡單平面圖必含一個度數 ≤ 5 的頂點。

17. Theorem (6.115)

- 若 $P(G, \lambda)$ 為著色多項式，則
 - $P(G, \lambda)$ 常數項為 0。
 - $P(G, \lambda)$ 係數和為 0。
 - $P(G, \lambda)$ 最高次項係數為 1。

18. Theorem ((6-63)6.98, (6-65)6.99) Edge-coloring:

$$\begin{aligned} \chi'(K_n) &= \begin{cases} n-1, & n=2k \\ n, & n=2k+1 \end{cases} \\ \chi'(C_n) &= \begin{cases} 2, & n=2k \\ 3, & n=2k+1 \end{cases} \\ \chi'(K_{n,n}) &= n \end{aligned} \quad (23)$$

19. Theorem (.129) 若 $G = (V, E)$ is connected, 則

$$|E| \geq |V| - 1 \quad (24)$$

Proof. 用數學歸納法證明：

當 $|V| = 1$ 時，成立。

設 $|V| < n$ 時成立。考慮 $|V| = n$ 時， $\forall v, \deg(v) = m$ ，則 $G - v$ 形成 k 個 components，有

$$G_1 = (V_1, E_1), G_2 = (V_2, E_2), \dots, G_k = (V_k, E_k) \quad (25)$$

又 $G_i, 1 \leq k \leq m$ is connected, 且 $|V_i| < n$ 。根據數學歸納法，

$$|E_i| \geq |V_i| - 1, \forall i = 1, \dots, k \quad (26)$$

則

$$\begin{aligned}
|E| &= |E_1| + \cdots + |E_k| + m \\
&\geq (|V_1| - 1) + \cdots + (|V_k| - 1) + m \\
&= (|V_1| + \cdots + |V_k|) + (m - k) \\
&= |V| - 1 + (m - k) \\
&\geq |V| - 1
\end{aligned} \tag{27}$$

20. Theorem (7.16, 7.24)

- 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

$$n \leq mi + 1 \tag{28}$$

$$l \leq (m - 1)i + 1 \tag{29}$$

當 T 為滿 m -元樹時，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

$$E = (m - 1)I + mi \tag{30}$$

21. Theorem (7.33, 7.34, 7.37)

- 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

$$N(G) = N(G - e) + N(G \cdot e) \tag{31}$$

- 一無向連通圖，其任意切集與環路必含偶數個共同邊。

22. Theorem ()

- $\exists x (P(x) \wedge Q(x)) \neq \exists x P(x) \wedge \exists x Q(x)$
- $(|A| = |B|)$ A : The set of all programs that terminate. B : The set of all programs that do NOT terminate.

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.

