集合中的組合數學

呂彥德

January 25, 2017

0 前言與預備知識

這篇文章主要的預設讀者是喜歡數學的高中生，目的是介紹一些些高等組合數學的內容以啟發大家對數學的熱忱。要注意這篇文章並不能扮演教科書的角色讓讀者有系統且有深度地學習，文中會介紹的內容只是龐大數學理論中的冰山一角，我們邀請有興趣的讀者參考列出的文獻進修。後面三個章節基本上是互相獨立的，讀者可以從依照任意順序去唸，只是筆者在第一章做的註解和說明比較多，所以建議大家從第一章開始可能會學到比較多東西。

文中的習題主要是引導式題型，帶領讀者一步步建立一些結果，而一般來說一開始的習題會較為簡單，之後會有改編自一些論文或是其他出處的題目，就會比較困難。本文除了最後一章的最後一個習題要求讀者會複數之外，其餘的預備知識都會在這一章節作介紹。在文中讀者有時可能會感到挫折：怎麼題目那麼難、命題的描敘都好抽象。這些是正常的，在較深的數學裡基本上沒有人能夠讀一遍理論就懂，都是在不斷練習以及培養對數學的成熟度中才會慢慢學到東西。Albert Einstein 說過：「教育就是當一個人把在學校所學全部忘光之後剩下的東西。」筆者希望讀者在學習完這篇文章後真正學到的東西是了解數學要如何思考、還有碰到一個全新的研究對象時，該問哪些重要的問題？

0.1 集合論初步

集合論是多數人開始學習抽象化數學時第一個會碰到的對象。所謂的集合是由一堆抽象物件構成的整體，這些構成它的物件稱作是這個集合的元素。一般來說我們會以大括號 $\{\}$ 表示一個集合，裡頭的元素將會寫在兩個括號之間，例如 $\{1,2,3\}$ 就是由 $1,2,3$ 這三個物件所組成的集合。此外通常會用大寫字母如 A,B,X,Y 等記集合，而另外小寫字母如 a,b,x,y 等記元素。一個最基礎的符號是 $\in$，表示屬於關係，也就是說判斷一個給定的物件在不在給定的集合中，比方說 $1\in\{1,2,3\}$, $4\notin\{1,2,3\}$。

利用屬於符號可以有效簡化一些寫法，舉例而言寫級數時

$$\sum_{i=1}^{4} i^2 \text{ 可以寫成 } \sum_{i\in\{1,2,3,4\}} i^2.$$

而且在其他許多情況下左邊的寫法會變得很奇怪，假如今天給定一個集合 $\{x,y,z\}$，並且對每個元素都賦一個值，分別為 $f(x),f(y),f(z)$，而我們想把這些元素賦的值加起來時，顯然不能夠寫 $\sum_{i=x}^{z} f(i)$，因為求和範圍非常曖昧，另一方面寫法 $\sum_{i\in\{x,y,z\}} f(i)$ 就沒有什

麼問題了，所以在多數情況下數學家喜歡用後者的這種記法。數列 $(a_n)_{n=1}^{\infty}$ 也可以記成 $(a_n)_{n\in\mathbb{N}}$。另外 $i \in \{x,y,z\}$ 裡面的 i 其實沒什麼意義，我們可以改成 j,k,l 之類的變數也沒關係，只是要注意不要改到 x,y,z 之一。

首先介紹第一種二個集合之間的關係，稱為包含關係：若集合 A 中的所有元素都是集合 B 中的元素，則稱集合 A 為 B 的子集，符號為 $A \subseteq B$。例如 $\{1,2\}$ 是 $\{1,2,3\}$ 的子集，但 $\{1,4\}$ 就不是 $\{1,2,3\}$ 的子集。根據定義，任一個集合必定是自身的子集。另外還有一個很特別的集合記做 $\emptyset$，稱之為空集合，它是唯一沒有任何元素的集合，並且依照規定空集合是任何一個集合的子集。對於集合 A，可以定義它的冪集 $\mathcal{P}(A)$ 為 A 的所有的子集合所形成的集合 (也就是說它是由數個集合所形成的集合)。例如當 $A = \{1,2,3\}$ 時

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}.$$

有時候我們會希望把滿組某種條件的物件放在一起形成一個新的集合，這時候寫出集合裡全部的元素不一定是容易的，好比說如果要描寫奇數集時比較單純的寫法是：$\{1,3,5,\dots\}$，但是這樣的記法有時候會產生歧義，因為我們並沒有列出所有元素，所以可能會有人認為我們在描述的集合是 $\{1,3,5,6,7,8,9,\dots\}$ 或是 $\{1,3,5,100,300,500,\dots\}$ 等等。為了不產生誤會，同時為了節省符號，數學家會用 $|$ 或是 , 來描述集合裡元素的性質，例如奇數集可以寫成 $\{2n+1 \mid n \text{ 為非負整數}\}$ 或是 $\{2n+1,\ n \text{ 為非負整數}\}$，而筆者偏好使用 $|$，在行文中都將用這種寫法。

當有兩個或是多個集合時，我們可以考慮在上面定義一些操作，以下先用兩個集合來說明：

1. 集合 A 和 B 的聯集，記做 $A \cup B$，是指至少在集合 A 或 B 之一出現的元素所構成的集合。例如集合 $\{1,2,3\}$ 和集合 $\{2,3,4\}$ 的聯集為集合 $\{1,2,3,4\}$.

2. 集合 A 和 B 的交集，記做 $A \cap B$，是指同時在集合 A 與 B 中出現的元素所構成的集合。例如集合 $\{1,2,3\}$ 和集合 $\{2,3,4\}$ 的交集為集合 $\{2,3\}$.

3. 集合 A 對 B 的相對差集，記做 $A \setminus B$，是在集合 A 中但不在集合 B 中所出現的的元素所構成的集合，例如集合 $\{1,2,3\}$ 對 $\{2,3,4\}$ 的相對差集為集合 $\{1\}$.

4. 集合 A 和 B 的笛卡兒積，記做 $A \times B$，是由所有可能的有序對 (a,b) 形成的集合，其中第一個物件是 A 的成員，第二個物件是 B 的成員，例如 $\{1,2\}$ 和 $\{\text{貓},\text{狗}\}$ 的笛卡兒積為 $\{(1,\text{貓}),(1,\text{狗}),(2,\text{貓}),(2,\text{狗})\}$。一般可以寫成 $A \times B = \{(a,b) \mid a \in A,\ b \in B\}$。而當集合 A 與集合 B 相等時，可以用 A^2 代替 $A \times B$.

在定義 3. 中，如果 B 是集合 A 的子集，我們會另外稱 $A \setminus B$ 為集合 B 在集合 A 中的補集，並用 B^c 代替 $A \setminus B$，此時 A 又稱為全集。而當上下文描述足夠清楚時，可以不必強

調全集是誰而直接寫出一個集合的補集。類似地可以定義多個集合的聯集 (至少在其中一個集合出現的元素所構成的集合)、交集 (在所有集合都出現的元素所構成的集合)、笛卡兒積。

集合與數對最大的不同點大致有兩點：其一，集合只允許一個元素出現一次，像是 $\{1,1,2,3\} = \{1,2,3\}$，而數對顯然不是如此；其二，集合不記元素出現次序，像是 $\{1,2,3\} = \{2,3,1\}$，而數對則是要考慮順序。但實際上為了方便，數學家也常常會寫出「有序集合」(但每個元素只會出現一次)、「無序數對」(每個元素可以出現好多次) 這些東西。

笛卡兒積的寫法在本文中會常常出現，是為了要更準確地描述語句。比如說陳述「取 a,b,c 為三個正整數」，我們可以改寫成「取 $a,b,c \in \mathbb{N}$」，但筆者偏好「取 $(a,b,c) \in \mathbb{N}^3$」，後者強調了每個物件是由哪些集合中取出來的。

一般常使用的集合有自然數集 $\mathbb{N}$ (在本文中 0 不為自然數) 及其有限子集、整數集 $\mathbb{Z}$、有理數集 $\mathbb{Q}$、實數集 $\mathbb{R}$、複數集 $\mathbb{C}$.

0.2 函數論

函數在數學中為兩集合間的一種對應關係：輸入值集合中的每項元素皆能對應唯一一項輸出值集合中的元素。嚴格一點來寫的話，給定兩個集合 A 與 B，一個從 A 到 B 函數是說對於每個 A 中的元素都找唯一一個 B 中的元素與它對應。當 f 是這樣一個函數時，我們會記做 $f : A \to B$，而以 $f(a)$ 記元素 $a \in A$ 在 B 中對應到的值。此時 A 稱為函數的定義域，B 稱為函數的為到達域。例如由

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^2 \end{aligned}$$

所定義的函數中 $\mathbb{R}$ 是定義域剛好也是到達域，然後有 $f(1) = 1, f(2) = 4$ 等等。注意到符號中有兩種不同的箭頭 $\to$ 和 $\mapsto$，前者是用來描述集合的對應，而後者則是用來描述元素的對應。要特別注意的是 $f(x)$ 不是一個函數，它是一個值，f 才是一個函數，有時候也可以記函數成 $f(\cdot)$。然而偶爾為了方便，數學家還是會直接寫「取函數 $f(x) = \cdots$」而不會寫 $f : x \mapsto \cdots$。

當兩個函數 f,g 的定義域與到達域都一樣，且 $f(x) = g(x)\ \forall x \in$ 定義域 ($\forall$ 代表「對所有」) 時，我們說這兩個函數是相等的，寫作 $f = g$，當然有時候到達域不同但仍有 $f(x) = g(x)\ \forall x \in$ 定義域，由慣例還是可以說這兩個函數相等。根據一個函數的特性它又可以有以下名稱：

1. 單射函數：不同的輸入值映射到不同的函數值。也就是說若 x 和 y 屬於定義域，則僅當 $x = y$ 時有 $f(x) = f(y)$.

2. 滿射函數：其值域 $\{f(a) \mid a \in A\} \subseteq B$ 即為其到達域。也就是對於映射 f 的到達域中之任意 y，都存在至少一個定義域的元素 x 滿足 $f(x) = y$.

3. 雙射函數：既是單射的又是滿射的函數。

另外我們常常會要求證明某某函數良好定義 (well-defined)，意思就是說證明定義域裡的元素被唯一地對應到到達域裡的元素。例如問

$$\begin{array}{rcl} f : \mathbb{R} & \to & \mathbb{R}^{\geq 0} \\ x & \mapsto & \begin{cases} x^2 & , \text{ 如果 } x \geq 0 \\ 2x & , \text{ 如果 } x \leq 0 \end{cases} \end{array}$$

是否良好定義。首先發現 $\{x \mid x \geq 0\} \cap \{x \mid x \leq 0\} = \{0\}$，而此時 $0^2 = 2 \times 0$，所以每個定義域裡的元素都被唯一定義了，可是可以發現 f 必須要把 -1 送到 -2，而後者不在 $\mathbb{R}^{\geq 0}$ 裡，因此這個函數不是良好定義的。而一旦我們將到達域改為 $\mathbb{R}$，這個函數就是良好定義的了。

0.3 進階集合論

第一次接觸以下內容的讀者可能會有理解上的困難，這是合情合理的，如果看不懂可以直接跳過這個小節，在閱讀文章時只要看到什麼無窮集合的大小、偏序集合、選擇公理、Zorn 引理之類的可以全部無視，其實不會錯過太多東西，筆者會將 (有限集合和自然數集) 與 (一般集合) 分開處理。

集合論還有一個重要的觀念叫做基數，也就是一個集合的大小：當 X 是一個有限集 (也就是說元素個數有限) 時，會以 $|X|$ 表示 X 中的元素個數，例如 $|\{1,2,3\}| = 3$。我們可以比較任意兩個有限集的大小，而為了比較兩個任意集合的大小，引入以下定義：對於兩個集合 A 與 B，當存在一個從 A 到 B 的雙射函數時，說 A 與 B 等勢，寫作 $|A| = |B|$。首先這個寫法看上去是有一些問題的：

1. 當 A 或 B 中至少一者為有限集時，我們已經定義 $|\cdot|$ 了，這時候作為整數的相等真的也會有 $|A| = |B|$ 嗎？

2. 式子 $|A| = |B|$ 是一個等式，而我們期待等式會滿足一些性質：

   a) 對所有 x 總有 $x = x$.

   b) 對所有 x, y 當 $x = y$ 時總也有 $y = x$.

   c) 對所有 x, y, z，當 $x = y$ 且 $y = z$ 時也會有 $x = z$.

而這三個關係式在等勢的意義下仍然能夠成立嗎？

這兩個問題的回答都是肯定的，筆者邀請讀者自行驗證第一項，給這裡給出第二項的證明 (讀者可以畫一下圖可能比較好裡解)：

Proof. a) 取 A 為一個集合。考慮恆等函數 $\mathrm{id}_A : A \to A$，定義為 $\mathrm{id}_A(a) = a$ $(\forall a \in A)$，可以發現它是從 A 到 A 的雙射函數，因此在等勢的意義下有 $|A| = |A|$.

b) 取 A, B 為兩個集合且滿足 $|A| = |B|$。由等勢的定義可以取到一個從 A 到 B 的雙射函數 f，現在定義一個從 B 到 A 的函數 f^{-1} 為 $f^{-1}(b) = a$, 如果 $f(a) = b$.

我們先證明這個函數是良好定義的：首先因為 f 是滿射函數，所以對於每個 $b \in B$，都可以找到 $a \in A$ 使得 $f(a) = b$，這表示說 f^{-1} 把每個 B 的元素都對應到 A 裡面的元素。

再來要驗證 f^{-1} 把每個 B 的元素都唯一地對應到 A 裡面的元素。這是因為如果 $f(a_1) = b$ 而 $f(a_2) = b$ 的話，那麼由於 f 單射我們會得到 $a_1 = a_2$，因此每個 $f^{-1}(b)$ 都是唯一確定的。至此得知這個函數是良好定義的。

最後要證明其實這個 f^{-1} 是雙射函數。首先 f^{-1} 是單射的，因為如果 $f^{-1}(b_1) = f^{-1}(b_2)$ 由定義我們會得到 (假設它們 $= a$) $f(a) = b_1 = b_2$。再來 f^{-1} 是滿射的，因為對於所有 $a \in A$ 都會有 $f^{-1}(f(a)) = a$.

由以上，在等勢的意義下有 $|B| = |A|$.

c) 取 A, B, C 為三個集合且滿足 $|A| = |B|$, $|B| = |C|$。由等勢的定義可以取到一個從 A 到 B 的雙射函數 f，以及一個從 B 到 C 的雙射函數 g，現在定義一個從 A 到 C 的函數 h 為 $h(a) = g(f(a))$。

我們同樣先證明這個函數是良好定義的：注意到 f, g 是兩個函數，這代表對於每個 $a \in A$, $f(a)$ 在 B 裡面都是唯一確定的，而 $g(f(a))$ 也因此在 C 裡面唯一確定，換句話說對於每個 $a \in A$, $h(a)$ 都在 C 裡面唯一確定，故 h 良好定義。

再來要驗證其實這個 h 是雙射函數。首先 h 是單射的，因為如果 $h(a_1) = h(a_2)$ 由定義我們會得到 $g(f(a_1)) = g(f(a_2))$，由於 g 單射可以繼續得到 $f(a_1) = f(a_2)$，最後由於 f 也是單射的所以得到 $a_1 = a_2$。再來 h 是滿射的，因為 g 滿射所以對於所有 $c \in C$ 可以找到 $b \in B$ 使得 $g(b) = c$，又 f 滿射所以可以再找到 $a \in A$ 使得 $f(a) = b$，此時 $h(a) = c$。

由以上，在等勢的意義下有 $|A| = |C|$. □

讀者可能有聽過無窮大也有分大小，比方正整數的無窮大 $|\mathbb{N}|$ 就與實數的無窮大 $|\mathbb{R}|$ 不一樣。證明如下：假設存在從 $\mathbb{N}$ 到 $\mathbb{R}$ 的雙射函數 f，那麼我們將每個 $f(n)$ 都用十進制展開 $f(n) = e_n.a_1^{(n)}a_2^{(n)}\cdots$，其中 e_n 是 $f(n)$ 的整數部分，而 $a_i^{(n)}$ 們則是小數點後面

的部分，每個 $a_i^{(n)}$ 都在 0 到 9 之間。現在取一個新的實數 $b = 0.b_1b_2\cdots$ 定義是說 b_1 是隨便一個在 0 到 8 之間不等於 $a_1^{(1)}$ 的整數，而 b_2 是隨便一個在 0 到 8 之間不等於 $a_2^{(2)}$ 的整數，依此類推。注意到這個實數 b 不可能是任何的 $f(n)$，因為 b 的小數點第 n 位和 $f(n)$ 的小數點第 n 位不同，矛盾。

一個問題產生了：有沒有辦法比較無窮集合的大小呢？從有限集合開始，一個直觀的定義是說如果可以把集合 A 放進集合 B 裡面，那麼集合 B 比集合 A 大。我們直接把這個定義推廣到一般集合上：對於兩個集合 A 與 B，當存在一個從 A 到 B 的單射函數時，說 A 比 B 小，寫作 $|A| \leq |B|$。可以驗證當 B 為有限集時比它小的集合 A 也會是有限集，而且作為整數的大小關係也真的有 $|A| \leq |B|$。注意到這種大小關係函會滿足以下性質：

1. 對所有 x 總有 $x \leq x$.
2. 對所有 x, y 當 $x \leq y$ 且 $y \leq x$ 時會有 $x = y$. (這是不顯然的，我們將在第一章的習題三證明)
3. 對所有 x, y, z，當 $x \leq y$ 且 $y \leq z$ 時會有 $x \leq z$.

定義 1 由這樣的想法者以定義所謂的偏序集合：給定集合 A，當 $\preceq$ 是一個滿足

1. 自反性：對所有 $x \in A$ 總有 $x \preceq x$.
2. 反對稱性：對所有 $(x, y) \in A^2$ 當 $x \preceq y$ 且 $y \preceq x$ 時會有 $x = y$.
3. 傳遞性：對所有 $(x, y, z) \in A^3$，當 $x \preceq y$ 且 $y \preceq z$ 時會有 $x \preceq z$.

的關係時，稱 $\preceq$ 為**偏序關係**，而 $(A, \preceq)$ 是一個**偏序集合**。一些常見的例子有：

1. 一般的實數比大小。$(\mathbb{R}, \leq)$ 是一個偏序集合。
2. 正整數的整除關係。$(\mathbb{N}, \mid)$ 是一個偏序集合 ($a \mid b$ 的定義是說 a 整除 b)。
3. 集合的包含關係。任給一個集合 A，則 $(\mathcal{P}(A), \subseteq)$ 是一個偏序集合。
4. 數列的優超關係。給定兩個由正實數組成且只有有限項非零的數列 $(a_n)_{n\mathbb{N}}, (b_n)_{n\in\mathbb{N}}$，首先假設他們都是遞減的，那麼當他們滿足
$$\sum_{i=1}^{n} a_i \geq \sum_{i=1}^{n} b_i \ \forall n \in \mathbb{N} \quad \text{且} \quad \sum_{i=1}^{\infty} a_i = \sum_{i=1}^{\infty} b_i$$
時 (注意兩個數列都只有有限項非零，所以 $\sum_{i=1}^{\infty}$ 其實只有有限項相加)，說 (a_n) 優超 (b_n)，寫作 $(a_n) \succ_M (b_n)$，那麼 $(\{\text{由正實數組成且只有有限項非零的遞減數列}\}, \prec_M)$ 是一個偏序集合。更一般地，當一個只有有限項非零的數列不是遞減的時候，可以依照裡面元素的大小重新排這個數列，由此可以定義兩個由正實數組成且只有有限項非零的數列之間的優超關係 (試問這個定義良好嗎？)。

注意到這些關係也有些許的不同，譬如說第一個例子裡隨便兩個實數都可以比大小，但是第二個例子中並不是隨便兩個正整數都可以比大小，像是有 $2 \nmid 3$ 且 $3 \nmid 2$。當在一個偏序集合 $(A, \preceq)$ 中有 $a \in A$ 使得對所有 $b \in A$ 都有 $b \preceq a$，我們說 a 是最大元素，注意到最大元素如果存在則最多只能有一個；而當有 $a \in A$ 使得沒有 $b \neq a$ 滿足 $a \preceq b$ 時 (也就是說沒有人比它大)，我們說 a 是極大元素。注意到極大元素可以有好多個，例如在

$$A = \{\emptyset, \{1\}, \{1,2\}, \{2,3\}\}$$

中用集合的包含關係定義偏序關係時，會發現這個偏序集合裡沒有最大元素，卻有兩個極大元素 $\{1,2\}, \{2,3\}$.

公理化集合論裡面最最重要的公理之一是選擇公理：如果有任意多個非空集合，那麼可以從每個集合中選出一個元素。這個敘述看起來很顯然，但是有許多數學家不願意承認 (事實上他們在不使用該公理的情況下重新研究所有數學體系，也得到了一整片結論)，原因是這個公理會導致許多不直覺的事情發生，一個有名的例子是 Banach-Tarski 定理：可以將 3 維空間的實心球分成 5 塊[19]，藉由旋轉及平移拼成兩個跟原本球一模一樣的球 (想像你可以把一張小朋友剪成 5 小片然後拼出兩張後到銀行重新換錢 $\cdots$)。在這裡我們不打算進一步地探討這些東西，只是簡單的給出一個應用：如果承認選擇公理，便可以證明出 Zorn 引理 (事實上兩者等價)，後者在非常多數學領域上扮演舉足輕重的角色。

引理 (Zorn 引理) 假設 $(A, \preceq)$ 是一個偏序集，對於它的一個子集 T，如果對所有 $(s,t) \in T^2$ 都有 $s \preceq t$ 或是 $t \preceq s$ 則稱為 T 是一個全序子集。而如果 A 中存在一個元素 a 使得 $\forall t \in T,\ t \preceq a$ 則稱 T 是有上界的 (注意 a 可以不在 T 裡面)。

那麼在任何一非空的偏序集中，若任何鏈（即全序子集）都有上界，則此偏序集內必然存在至少一個極大元素。

0.4 其他

在以下章節中我們會看到一些與圖論以及矩陣相關的命題，因此在這一小節先做簡單的介紹。

給定一個圖，那麼有什麼簡易的表示方法呢？一個直觀想法是說可以把它的頂點和頂點之間的連線關係都寫出來，例如說畫一個三角形，我們知道它有三個頂點，假設將他們依序標號寫成 $1,2,3$，那麼三角形的邊就可以寫成 $(1,2),(2,3),(1,3)$ (注意這裡的數對是不考慮元素次序的，也就是說 $(1,2) = (2,1)$)，可以看出這些資訊完整了描述了圖的結構。由這樣的想法出發，定義所謂的一個圖是指用 (V,E) 所表示的集合對，其中 V 是這個圖的頂點集，而 E 是他的邊集，邊集裡面的元素是長成 (v_1, v_2) 的形式，其中 v_1, v_2 是兩個 (不相同) 的頂點。在上面的例子裡三角形的圖就是 $\triangle = (\{1,2,3\}, \{(1,2),(2,3),(1,3)\})$；

另外一個例子是說正方形的圖

$$\square = (\{1,2,3,4\}, \{(1,2),(2,3),(3,4),(4,1)\}).$$

一個邊所含的兩個點稱為這個邊的頂點，例如邊 (v_1, v_2) 的頂點就是 v_1, v_2。而當兩個點之間有一條邊將他們相連之則稱這兩個點相鄰，或是說他們是鄰居。假設說今天有個圖寫成 $(\{a,b,c\}, \{(a,b),(b,c),(c,a)\})$，顯然我們會覺得它和上述 123 所表示的三角形是同一張圖，可是有一個問題出現了：作為集合，並不會有 $\{1,2,3\} = \{a,b,c\}$，所以從 (V,E) 的這種定義出發並不能直接說這兩個是同一張圖 (因為 $(\{1,\dots\}, \{(1,2),\dots\}) \neq (\{a,\dots\}, \{(a,b),\dots\})$)，有什麼好的解決辦法呢？

回到較根本的問題：為什麼我們會覺得從 abc 定義的圖會和從 123 所定義的圖一樣呢？仔細想想會發現是因為如果將頂點之間做對應 $1 \leftrightarrow a, 2 \leftrightarrow b, 3 \leftrightarrow c$，那麼邊之間也會有同樣的對應關係 $(1,2) \leftrightarrow (a,b), \dots$，所以我們才會覺得兩張圖是一樣的。從這樣的想法出發，便可以定義圖之間的同構關係：給定兩張圖 $(V,E), (V',E')$，當存在 V 和 V' 之間的對射函數 f 使得 $(v_1,v_2) \in E \Leftrightarrow (f(v_1), f(v_2)) \in E'$ 時稱這兩張圖同構。在這樣的意義下上述的 123 三角形和 abc 三角形就可以視作相等的。

還有一種特別的圖叫做二分圖，是指說可以將這個圖的頂點集 V 分成兩個不相交的子集 A 與 B，使得圖裡面的所有邊的兩個頂點分別在 A 和 B 裡。用數學點的語言來說就是可以寫出 $V = A \cup B$ 使得 $A \cap B = \emptyset$ (兩個子集不相交)，並且 $E \subseteq A \times B$ (所有邊都是某個 A 的點連到某個 B 的點)，在本文中會特別以 (A,B,E) 記這樣的圖。

最後要介紹矩陣。所謂的一個 $n \times m$ 矩陣就是一個具有 m 直行以及 n 橫列元素所排成的矩形，例如

$$\begin{bmatrix} \text{橘貓} & \text{斯芬克斯貓} \\ \text{什麼貓} & \text{黑貓} \\ \text{俄羅斯藍貓} & \text{白貓} \end{bmatrix}$$

就是一個 3×2 的貓形矩陣，它很可愛。特別地 $n \times 1$ 的矩陣又被稱作 (行) 向量。

給定矩陣 A，它的轉置矩陣 $A^\top$ 是指把 A 的行跟列全都倒過來後得到的矩陣，例如上面貓形矩陣的轉置就是

$$\begin{bmatrix} \text{橘貓} & \text{什麼貓} & \text{俄羅斯藍貓} \\ \text{斯芬克斯貓} & \text{黑貓} & \text{白貓} \end{bmatrix}.$$

一個矩陣通常會用 $(a_{ij})_{i \le n, j \le m}$ 的形式表示，其中 a_{ij} 是第 j 行第 i 列的元素，像是貓形矩陣 $_{32} =$ 白貓。可以看出轉置矩陣的寫法是 $(a_{ij})^\top_{i \le n, j \le m} = (a_{ji})_{j \le m, i \le n}$。我們還可以定義兩個矩陣的乘法為：假設 $(a_{ij})_{i \le n, j \le m}, (b_{jk})_{j \le m, k \le l}$ 是兩個分別為 $n \times m$ 和 $m \times l$ 的矩陣，那麼定義 $(a_{ij}) \times (b_{jk}) = (c_{ik})_{i \le n, k \le l}$，其中

$$c_{ik} = \sum_{j=1}^{m} a_{ij} b_{jk}.$$

注意乘法只在第一個矩陣的行數等於第二個矩陣的列數時有定義。

■ **習題 1.** 集合論的練習

這個習題裡所有大寫英文字母都表示集合。現實生活中我們常被要求證明兩個集合的相等 $A = B$，一般人寫的會像是「在 A 的元素滿足某某性質，然後因為 ...，所以我們可以發現 B 中元素也恰好是滿足這些性質的元素，所以兩個集合一樣。」的中文論述，這樣的證明當然可以是正確的，只是在很多情況下兩個集合很複雜，不一定能看出裡面元素所滿足的性質到底是不是一樣的。一般而言數學家會藉由分別證明 $A \subseteq B$ 且 $A \supseteq B$ 來說明兩個集合相等。舉例來說，我們想要證明 $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$：

Proof. 先證明左邊 $\subseteq$ 右邊：取元素 $x \in (A \cup B) \cap C$，那麼根據定義它同時在 $A \cup B$ 和 C 裡面。第一個推論 $x \in A \cup B$ 又告訴我們說它至少在 A 或 B 其中一者裡，不妨假設它在 A 中，那麼我們將得到 $x \in A \cap C$，故 $x \in (A \cap C) \cup (B \cap C)$。由於元素 x 是任取的，因此必然有左邊 $\subseteq$ 右邊。

再來要證明左邊 $\supseteq$ 右邊：取元素 $x \in (A \cap C) \cup (B \cap C)$，那麼根據定義它至少在 $A \cap C$ 或 $B \cap C$ 其中一者裡，不妨假設它在 $A \cap C$ 中，這蘊含了它同時在 A 和 C 中，可以看出 $x \in (A \cup B) \cap C$。由於元素 x 是任取的，因此必然有左邊 $\supseteq$ 右邊。綜上得證。 □

試利用這樣的論述形式做以下習題。

1. 假設 m 是正整數。證明
$$\left(\bigcup_{j=1}^{m} A_j \right) \cap B = \bigcap_{j=1}^{m} (A_j \cup B) .$$
2. 假設 m 是正整數。證明
$$\left(\bigcup_{j=1}^{m} A_j \right) \cap (B \cup C) = \left(\bigcap_{j=1}^{m} (A_j \cup B) \right) \cap \left(\bigcap_{j=1}^{m} (A_j \cup C) \right) .$$
3. 假設 m 是正整數。證明
$$\bigcup_{j=1}^{m} (B \setminus A_j) = B \setminus \left(\bigcap_{j=1}^{m} A_j \right) .$$
4. 證明在上述三小題中把 $\cup$ 和 $\cap$ 做互換等式仍成立。

■ **習題 2.** 函數的像與逆像

這個習題裡 A 和 B 表示兩個集合，$A_1, A_2, \ldots$ 是 A 的子集，而 $B_1, B_2, \ldots$ 是 B 的子集，最後 f 是從 A 到 B 的一個函數。

當 A' 是 A 的子集時，我們說 A' 在 f 之下的像為

$$f(A') = \{b \in B \mid \text{存在} a' \in A' \text{使得} f(a') = b\}.$$

它顯然是 B 的子集合。而當 B' 是 B 的子集時，我們說 B' 在 f 之下的逆像為

$$f^{-1}(B') = \{a \in A \mid f(a) \in B'\}.$$

注意這和我們在進階集合論小節裡 f 為對射函數時所引入的逆函數 f^{-1} 不一樣。

1. 先給讀者一個簡單的例子：考慮 $A = \{1,2\}, B = \{a,b,c\}, f(1) = a, f(2) = c$。試說明

$$f(\{1\}) = \{a\},\ f^{-1}(\{a,b\}) = \{1\},\ f^{-1}(\{b\}) = \emptyset.$$

2. 假設 m 是正整數。證明

$$f\left(\bigcup_{j=1}^{m} A_j\right) = \bigcup_{j=1}^{m} f\left(A_j\right).$$

3. 假設 m 是正整數。證明

$$f^{-1}\left(\bigcup_{j=1}^{m} B_j\right) = \bigcup_{j=1}^{m} f^{-1}\left(B_j\right).$$

4. 證明在上述兩小題中把 $\cup$ 和 $\cap$ 做互換等式仍成立。

5. 有沒有關於相對差集的類似性質？

■ 習題 3. 動物界的主宰關係

文獻[12] 是經濟學的一篇經典論文，這個習題的前半部分靈感即是來自這篇文章，希望讀者做完後可以多多少少學習到碰到一個新的問題時要如何思考。

假設某片大草原上有 n 種動物，每兩種動物之間都有捕食和被捕食的關係。在一般的情況下這個關係並沒有傳遞性，也就是說可能會有動物甲捕食動物乙，動物乙捕食動物丙，然而動物丙卻捕食動物甲的這種情況發生。一個重要的問題是研究動物之間的捕食關係，但正如先前所說，捕食關係並沒有傳遞性，所以不一定存在一種動物可以吃掉其他所有動物。所以我們退一步想，是否有一種動物可以「傳遞性」地吃掉其他其他所有動物呢？

一個直觀的定義是說，對於動物 a 和動物 b，當存在一串動物鏈 $a_0 = a, a_1, \ldots, a_k = b$ 使得對所有 $i \leq k-1$ 都有動物 a_i 捕食動物 a_{i+1} 時，則稱動物 a 可傳遞地捕食動物 b。當某種動物可傳遞地捕食其他所有動物，我們稱牠是一個主宰動物。

1. 考慮 $n = 2,3,4$ 所對應出的所有捕食關係，試問是否總是有某種動物可傳遞地捕食其他所有動物呢？

2. 由上面的例子可以看出總有主宰動物，然而當 n 繼續變大顯然要討論所有情況是不可能的，於是我們考慮直接證明這件事是對的。首先一個自然的想法是說，能夠直接捕食最多種動物的那種動物就是一隻主宰動物。試證明這個想法是對的。

3. 現在已知總有某種動物可傳遞地捕食其他所有動物，於是另一個可以問的問題是：它可以多快地傳遞性捕食其他所有動物呢？

   更具體來說，對於動物 a 和動物 b，如果存在一串動物鏈 $a_0 = a, a_1, \ldots, a_k = b$ 使得對所有 $i \leq k-1$ 都有動物 a_i 捕食動物 a_{i+1} 時，則稱動物 a 可以 k-傳遞地捕食動物 b。顯然會有主宰動物可以 $(n-1)$-傳遞地捕食其他動物，問題是 $n-1$ 可以再縮小嗎？

   再次藉由考慮能夠直接捕食最多種動物的那種動物，證明牠可以 2-傳遞地捕食其他動物。

4. 主宰動物一定只有一隻嗎？

可以問的問題仍然很多，比方有 n 種動物時共有幾種可能的捕食關係？然而「主宰動物」的研究看起來已經做完了，因為已經探討過牠的存在性以及唯一性 (主宰動物不唯一) 了，於是這個問題就這樣結束了嗎？當然不是。既然前文介紹了這麼多集合論的內容，我們何不試著用這些較抽象的理論重新描寫一次研究問題呢？

首先有 n 種動物，可以寫出動物集 $A = \{1, \ldots, n\}$，於是動物間的捕食關係可以想成是一個函數 f，他的定義域是所有由 A 中兩個不同元素所形成的集合的集合，簡記為 $\mathcal{P}_2(A)$ $(= \{\{1,2\}, \{1,3\}, \ldots\})$，而他的到達域是動物集 A，定義是 $f(\{a,b\})$ 為 a, b 之中為捕食者的那個。這個函數有一個很重要的性質就是 $\forall B \in \mathcal{P}_2(A)$，總有 $f(B) \in B$ (因為 $f(B)$ 是 B 裡的捕食者)。

從集合論的語言來描述問題馬上可以看出一個可行的推廣：令 $A = \{1, \ldots, n\}$，對於正整數 $l \leq n$，以 $\mathcal{P}_l(A)$ 記所有由 A 中 l 個不同元素所形成的集合的集合，假設 f 是滿足「$\forall B \in \mathcal{P}_l(A)$，總有 $f(B) \in B$」的一個從 $\mathcal{P}_l(A)$ 到 A 的函數 (稱為捕食函數)。那麼定義廣義的捕食關係為：對於動物 a 和動物 b，當存在一個 $B \in \mathcal{P}_l(A)$ 使得 $(a,b) \in B^2$，且 $f(B) = a$ 時，則說動物 a 捕食動物 b (事實上 a 捕食其他所有 B 裡面的動物)。而傳遞性捕食關係定義照抄，對於動物 a 和動物 b，當存在一串動物鏈 $a_0 = a, a_1, \ldots, a_k = b$ 使得對所有 $i \leq k-1$ 都有動物 a_i 捕食動物 a_{i+1} 時，則稱動物 a 可以 (k-) 傳遞地捕食動物 b。

我們再次詢問：主宰動物總是存在嗎？而牠又可以多快地傳遞性捕食完其他動物呢？

5. 藉由對 l 進行數學歸納法，證明主宰動物總是存在。(可以先想想如何從 $l = 2$ 推到 $l = 3$)

6. 證明必有某種動物可以 l-傳遞地捕食其他動物。

推廣形式並不是唯一的，例如讀者也可以考慮 f 的到達域是 $\mathcal{P}_2(A)$ (也就是說每群動物裡會有兩個捕食者) 之類的變形，有非常多非常多可能性。而這裡考慮的算是較簡單的推廣，但也足以讓我們做出其他很有趣的結果了，例如說：

7. 對於一個平面點集 A，稱由所有離 A 的至少一個點的距離 $\leq \epsilon$ 的點所形成的集合為 A 的 ϵ-鄰居。假設 $A_1, A_2, \ldots, A_n$ 是一些平面上的點集，已知對於任意三個集合 A_i, A_j, A_k 都可以找到其中兩個 (例如 A_i, A_j) 使得 $A_i \cup A_j$ 的 ϵ-鄰居包含 A_k。試證明其中存在兩個集合 A_u, A_v 使得 $A_u \cup A_v$ 的 2ϵ-鄰居包含其他所有點集。

附註

- 如果讀者曾看過選擇公理的數學描述，那應該會看出這裡的捕食函數是一個選擇函數。
- 選擇函數在邏輯理論，也因此在某部分資訊理論 (跟數學比較有接軌的那塊) 中是很重要的。習題 1. 裡面的等式又被稱為 de Morgan 定律，是很重要的性質，如果讀者會法文並且很想練習與此相關的題目，可以在這裡下載 Informatique A 的考題 (http://www.ens.fr/admission/concours-sciences/rapports-et-sujets-43/annee-2016-194/article/rapports-et-sujets-2016-mpi?lang=fr)，內容是 Boolean 可滿足性問題的相關題目。

1 Hall 婚姻定理

近年來臺灣以及國外都有不少相親的節目。假設你是一個婚姻介紹所的負責人，負責將女方介紹給男方。看完由女方提供的的相片及個人簡介後，來到介紹所的男性們都選出了幾位各自心儀的對象，那麼你是否有辦法把女士們分配給男士，使得每位男士都滿意呢？Hall 婚姻定理是數學家 Philip Hall 在 1935 年證明的，內容給出了上述分配法存在的充要條件。事實上在 1931 年 D. König 以及 E. Egervary 就已用不同的敘述 (所謂的 (0,1)-矩陣及二分圖網)，得到相同的結果；甚至 K. Menger 在 1927 年研究圖網的連通性時，就證明出了更一般化的定理，將前三者的結果視為特殊情況。

以數學語言來說，婚姻問題就變成了：給定一組集合 $A = (A_1, \ldots, A_n)$ (A_i 是第 i 個男生心儀的女生集合)，是否有辦法在每個集合 A_i 中都取出一個元素 a_i，使得 $a_1, \ldots, a_n$ 兩兩相異 (一個女生不可以嫁給兩個男生)？如果這樣的取法存在，那麼我們說 $a = (a_1, \ldots, a_n)$ 是 A 的一組相異代表系。顯然地，如果相異代表系存在的話，那麼對於所有 $\{1, \ldots, n\}$ 的子集合 I，都要有 $|\cup_{i\in I} A_i| \geq |I|$，否則會有一些男生搶人數比他們還要少的女生。神奇的是，這個條件也是充分條件。

定理 1 (Hall 婚姻定理)　給定任一集合 S，以及一組集合 $A = (A_i)_{i\in S}$，當對所有 S 的子集合 I，都有 $|\cup_{i\in I} A_i| \geq |I|$ 時，我們說 A 滿足 Hall 條件。

現給定任一集合 S，以及一組集合 $A = (A_i)_{i\in S}$，如果每個 A_i 都是有限集，那麼存在 A 的一組相異代表系當且僅當 A 滿足 Hall 條件。

附註　對於第一次接觸這樣數學描述的讀者而言，筆者相信「給定任一集合 S，以及一組集合 $A = (A_i)_{i\in S}$, ...」這句話不是很好懂。我們可以用 $S = \{1, 2, 3\}$ 來做說明：命題的敘述其實是現在有一組集合 $A = (A_1, A_2, A_3)$，而且他們滿足 $|A_1| \geq 1, |A_2 \cup A_3| \geq 2, \ldots$。那麼為什麼要用這麼難懂的寫法呢？為什麼不直接寫 $A = (A_1, A_2, \ldots)$？一個最主要的原因就是當我們用這種數列的寫法時，其實隱含著集合的個數最多只有 $|\mathbb{N}|$ 個，而預備知識一章告訴我們說還有很多更大的可能性，所以為了將定理描述到最一般的形式這裡就採用這種寫法。以後大家走數學相關領域也會常常看到這種描述。

Proof. 顯然 Hall 條件是存在相異代表系的必要條件，我們只須證明他也是充分條件。首先考慮一個特殊情形：所有 A_i 都只包含一個元素。這時 Hall 條件告訴我們所有 A_i 中的元素是兩兩相異的，因此定理成立。

接下來對於一般的情況，我們的策略是想辦法歸結到上述的特例。以下暫時考慮 S 是有限集的情況，可以假設 $S = \{1, \dots, n\}$：如果 A 不是上述特例，那麼至少存在一個 $s \in S$ 使得 A_s 裡面有兩個元素，不失一般性可以假設 $s = 1$，並從中取出 x 和 y 是相異元素。宣稱

引理 令 $A' = (A_1 \setminus \{x\}, A_2, \dots, A_n)$, $A'' = (A_1 \setminus \{y\}, A_2, \dots, A_n)$，那麼 A' 與 A'' 當中至少一個會滿足 Hall 條件。

Proof. 簡記 $S' = S \setminus \{1\}$。使用歸謬法，假設兩組集合都不滿足 Hall 條件，那麼將會存在 S' 的兩個子集合 I_1, I_2 使得

$$|(A_1 \setminus \{x\}) \cup \bigcup_{i \in I_1} A_i| \le |I_1|, \quad |(A_1 \setminus \{y\}) \cup \bigcup_{i \in I_2} A_i| \le |I_2|.$$

所以得到

$$\begin{aligned} |I_1| + |I_2| &\ge |(A_1 \setminus \{x\}) \cup \bigcup_{i \in I_1} A_i| + |(A_1 \setminus \{y\}) \cup \bigcup_{i \in I_2} A_i| \\ &\ge |A_1 \cup \bigcup_{i \in I_1 \cup I_2} A_i| + |\bigcup_{i \in I_1 \cap I_2} A_i| \qquad (*) \\ &\ge (|I_1 \cup I_2| + 1) + |I_1 \cap I_2| \\ &= |I_1| + |I_2| + 1, \text{ 矛盾。} \end{aligned}$$

其中 $(*)$ 式是由 $|A| + |B| = |A \cup B| + |A \cap B|$ 而來。 □

由此，只需將引理重複用在 A 上我們就會回到最開始的特例，因此此時 Hall 定理也成立。

最後是 S 為任意集合的情況，這時用上述方法無法回到最開始的特例，因此必須另外處理。考慮以下集合

$$\Omega = \{(B_i)_{i \in S} \text{ 滿足 Hall 條件} \mid \forall i \in S, B_i \subseteq A_i\}.$$

並在 Ω 上定義一個偏序關係：如果 $B = (B_i) \in \Omega$, $B' = (B'_i) \in \Omega$，那麼

$$B \preceq B' \iff \forall i \in S, B_i \subseteq B'_i.$$

可以由 A_i 們的有限性證明 Zorn 引理在 $(\Omega, \preceq)$ 成立，因此有極小元素 $B \in \Omega$。又，引理 1. 可以直接推廣成 S 任意集的情況，因此可看出所有 B_i 都只包含一個元素，Hall 定理證畢。 □

■ **習題 1.** Hall 定理的各種形式

1. 將定理最後一段的證明補齊。也就是說證明 $\preceq$ 是一個偏序關係，且可以在 $(\Omega, \preceq)$ 上使用 Zorn 引理，還有引理 1. 可以直接推廣成 S 任意集的情況。

2. 當 S 為自然數集時我們並不需要使用 Zorn 引理，可以考慮以下的對角化過程：令 $A^{(0)} = (A_1, A_2, A_3 \dots)$，由引理 1. 知道存在 $a_1 \in A_1$ 使得 $(\{a_1\}, A_2, A_3, \dots)$ 滿足 Hall 條件，因此令 $A^{(1)} = (\{a_1\}, A_2, A_3, \dots)$，再知道存在 $a_2 \in A_2$ 使得 $(\{a_1\}, \{a_2\}, A_3, \dots)$ 滿足 Hall 條件，因此令 $A^{(2)} = (\{a_1\}, \{a_2\}, A_3, \dots)$，依此類推，對每個 $n \in \mathbb{N}$ 都可以定義出一個 $a_n \in A_n$。證明 $(\{a_1\}, \{a_2\}, \dots)$ 滿足 Hall 條件並推出 Hall 定理。

3. 證明在 Hall 條件中，如果把 I 改為有限子集合，那麼 Hall 定理仍然成立。

另外在定理中，我們考慮的是 S 為任意集合而 A_i 們有限的情況，因此一個合理的推廣形式是不對集合 A_i 的大小做限制。

4. 證明 S 為有限集時，對任一組集合 $A = (A_i)_{i \in S}$ 都有：存在 A 的一組相異代表系當且僅當 A 滿足 Hall 條件。也就是說此時不需要 A_i 們的有限性。

5. 當 S 為任意集合且至少有一個 A_i 為無限集時，Hall 定理是錯的，試給出一個簡單的反例。

6. (Hall 定理強化) 給定任一集合 S，一組集合 $A = (A_i)_{i \in S}$，以及正整數序列 $(p_i)_{i \in S}$。證明存在 $X_i \subseteq A_i$ $(i \in S)$ 使得 X_i 們兩兩不相交，還有 $|X_i| = p_i$ $(i \in S)$ 當且僅當對所有 $I \subseteq S$ 都有
$$|\bigcup_{i \in I} A_i| \geq \sum_{i \in I} p_i.$$

7. (Marshall Hall 定理) 令 S 是有限集，k 是正整數，假設在 Hall 定理中每個 $|A_i|$ 都至少是 k，試證明至少有 $k!/(n-k)!$ 個 A 的相異代表系 (當 $m \leq 0$ 時我們取 $m! = 1$)。這個結果可以推廣到 $S = \mathbb{N}$ 甚至是 S 任意集嗎？

■ **習題 2.** Hall 定理的應用

1. 假設某個國小一年級有 30 個班級，每班的課表都是相同的：週一至週五每天早上都是四堂課，總共六堂國語，兩堂英文，四堂數學，兩堂體育，兩堂音樂，兩堂生活，還有兩堂班會課。假設一個老師最多只能教一種課，試問這個年級各科至少要雇用多少老師？

2. (拉丁方陣) 所謂的 $n \times n$ 拉丁方陣指的是在這個 $n \times n$ 的方陣中恰有 n 種不同的元素，每一種不同的元素在同一行或同一列裡恰出現一次。而如果 $n \geq k$，那麼 $n \times k$

拉丁矩陣指的是在這個 $n \times k$ 的矩陣中恰有 n 種不同的元素，每一種不同的元素在同一行裡恰出現一次，並且在同一列裡最多出現一次。例如

$$\begin{bmatrix} 1 & 2 \\ 3 & 1 \\ 2 & 3 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}$$

分別是 3×2 的拉丁矩陣以及 3×3 的拉丁方陣，並且拉丁方陣被拉丁矩陣所生成。

a) 證明 $n \times k$ 拉丁矩陣一定可以生成 $n \times n$ 拉丁方陣。

b) 證明至少有 $n!(n-1)! \cdots (n-k+1)!$ 個 $n \times k$ 拉丁矩陣。

3. (Sperner 引理) 假設 S 是由某些集合所形成的集合，如果對於所有 $(A, B) \in S^2$, $A \neq B$ 都有 $A \not\subseteq B$ 且 $B \not\subseteq A$，則稱 S 是一組 Sperner 系統。假設 n 是正整數且 S 是由 $\{1, \ldots, n\}$ 的子集合所組成的 Sperner 系統，目的是要證明總有

$$|S| \leq \binom{n}{\lfloor n/2 \rfloor}.$$

a) 令 $A_1, \ldots, A_m$ 是不同的 $\{1, \ldots, n\}$ 的子集合，每一個都包含 k 個元素，其中 $k \geq \lfloor n/2 \rfloor + 1$。令 $\mathcal{B}_i = \{B \subset A_i \mid |B| = k-1\}$ $(1 \leq i \leq m)$，證明 $(\mathcal{B}_1, \ldots, \mathcal{B}_m)$ 存在一組相異代表系。

b) 令 $l_S = \max\{|A| \mid A \in S\}$。假設 $l_S \geq \lfloor n/2 \rfloor + 1$，證明由上述可以得到另一個 Sperner 系統 S' 使得 $|S| = |S'|$ 且 $l'_S < l_S$.

c) 證明如果 S 是 Sperner 系統，那麼 $\overline{S} = \{A^c \mid A \in S\}$ 也是。由此總結。

4. (Birkhoff-von Neumann 定理) 所謂的雙機率矩陣指的是每個行和列求和均為 1 的非負實數方陣，而置換矩陣指的是一個每個係數都為 0 或 1 的雙機率矩陣。目的是要證明所有雙機率矩陣都是置換矩陣的非負線性組合。假設 $P = (P_{i,j})_{1 \leq i,j \leq n}$ 是一個雙機率矩陣。

a) 定義 $A_i = \{j \mid P_{i,j} > 0\}$ $(1 \leq i \leq n)$。證明 $(A_1, \ldots, A_n)$ 存在相異代表系。

b) 證明定理。

5. 一個 $n \times n$ 的表格種每格都填上了 0 或 1，使得任意不同行不同列的 n 個格子中一定至少有一格填上了 1。證明可以選出 i 行與 j 列使得這些行列的交點都填上了 1，並且 $i + j \geq n + 1$.

6. (2012 Putnam B3) 有 $2n$ 個隊伍打循環賽，賽程共歷時 $2n-1$ 天。每一天每一隊都會和另一隊比賽，其中不會有平手。在循環賽中任意兩隊都恰好舉行過一次比賽。是問是否一定能從每一天選出該日勝利的某一隊使得沒有一隊被選到兩次？

7. 在一個 $2n \times 2n$ 的西洋棋盤中，每一行每一列都包含 n 個城堡。證明可以從中選出 $2n$ 個城堡使得每一行每一列都包含這 $2n$ 個城堡中的 1 個。

8. (2010 ISL C3) 在一個星球上總共有 2^N 個國家 ($N \geq 3$)。每一個國家都有一面國旗，國旗都是由 N 個 1×1 的格子組成的 $N \times 1$ 長方形，其中每個格子都被塗上藍色或黃色。沒有兩個不同的國家擁有一樣的國旗。如果對於一組 N 個國旗，他們可以被排列成一個 $N \times N$ 的方陣使得主對角線上的格子都是同色的，那麼稱這組國旗是多樣的。是求出最小的正整數 M，使得任意 M 個國其中必定有一組國旗是多樣的。

9. (2006 ARO finals) 已知在一個夏令營裡每個人的朋友數都至少是 50 位且不超過 100 位，證明可以將 1331 種不同的 T 恤分發給所有人，使得每個人都有 20 位朋友他們拿到的 T 恤是不同的。

■ **習題 3.** 二分圖問題

假設 $G = (A, B, E)$ 是一個二分圖。當存在一些不相交的邊使得所有 A (或是 B) 中的頂點都在邊上時，我們說 G 存在一個左 (或是右) 匹配；而當存在一些不相交的邊使得所有頂點都在邊上時，我們說 G 存在一個完美匹配。當 C 是 A 的一個子集時，我們可以定義他的鄰居集：

$$\mathcal{N}_R(C) = \{b \in B \mid (c, b) \in E,\ \forall c \in C\}.$$

類似地當 D 是 B 的一個子集時，可以定義鄰居集 $\mathcal{N}_L(D)$，這兩個對應為 Galois 連接。則 Hall 定理宣稱了對一個局部有限 (就是說每個頂點連到的邊都是有限的) 二分圖，如果對所有 $C \subseteq A$ 都有 $|\mathcal{N}_R(C)| \geq C$ 那麼這個圖有左匹配。

1. 證明一個局部有限二分圖如果有左匹配也有右匹配，那麼就有完美匹配。

2. (Cantor–Bernstein 定理) 由此推出如果兩個集合滿足 $|X| \leq |Y|$ 且 $|Y| \leq |X|$ 那麼 $|X| = |Y|$.

3. (Hall-Harem 定理) 設 $G = (A, B, E)$ 是一個二分圖，k 是正整數。當存在一些邊使得所有 A 中的頂點都恰好在 k 條邊上，且 B 中所有頂點都恰好在 1 條邊上時，我們說 G 存在一個完美 $(1, k)$ 匹配。

   令 $G = (A, B, E)$ 是一個二分圖。當對所有 A 的有限子集合 C，B 的有限子集合 D 都有

   $$|\mathcal{N}_R(C)| \geq k|C|,\ |\mathcal{N}_L(D)| \geq \frac{1}{k}|D|.$$

   時，我們說 G 滿足 Hall-Harem 條件。證明當 $G = (A, B, E)$ 是一個局部有限二分圖時，G 存在完美 $(1, k)$ 匹配當且僅當他滿足 Hall-Harem 條件。

以下幾個小題我們將要研究兩個二分圖的同構問題[1]。首先對於兩個圖，當存在一個兩個頂點集之間的雙射函數，使得在同一頂點集的兩個頂點相鄰若且唯若他們在這個函數的像也是相鄰的，那麼說這兩個圖是同構的，並以 $\cong$ 記這個關係。現在給定兩個二分圖 $G=(A,B,E)$ 和 $H=(C,D,F)$，當存在兩個單射函數 $\phi: A\to C$, $\psi: B\to D$ 使得 $(x,y)\in E \Rightarrow (\phi x, \psi y)\in F$ 時我們說 G 是 H 的子圖，記做 $G\leq H$.

4. 證明如果 G,H 是兩個有限二分圖 (即頂點數有限的二分圖)，那麼 $G\leq H$ 且 $H\leq G$ 蘊含 $G\cong H$。說明為何這在局部有限二分圖上不正確。

5. 以下僅考慮有限二分圖。證明 $G\leq H$ 當且僅當存在單射函數 $\phi: A\to C$ 使得

$$|\bigcup_{I\in\gamma}\mathcal{N}_R(A)|\leq|\bigcup_{I\in\gamma}\mathcal{N}_R(\phi(A))|,\ \ \forall\gamma\subseteq\mathcal{P}(A).$$

6. 由此證明 $G\cong H$ 當且僅當存在雙射函數 $\phi: A\to C$ 使得

$$|\mathcal{N}_R(I)|=|\mathcal{N}_R(\phi(I))|,\ \ \forall I\subseteq A.$$

7. 最後推出 $G\cong H$ 當且僅當存在雙射函數 $\phi: A\to C$ 使得

$$|\bigcup_{x\in I}\mathcal{N}_R(x)|=|\bigcup_{x\in I}\mathcal{N}_R(\phi(x))|,\ \ \forall I\subseteq A.$$

8. (一般圖同構) 給定圖 $G'=(V',E')$，可以考慮二分圖 $B(G')=(V',E',F')$，其中 $(v,e)\in F'\Leftrightarrow v\in e$。證明 $G'\cong H'$ 當且僅當 $B(G')\cong B(H')$.

附註

- Hall 定理可以運用在二分圖匹配。由這樣的想法出發，Hall 定理可以用於許多跟矩陣相關的問題上。
- 可以想見計算獨立代表系的個數也是相當重要的問題，習題中的 Marshall Hall 定理是一個初步估計。
- 由證明可以看出 Hall 定理跟選擇公理是邏輯等價的，事實上很多組合理論當中的定理也會跟 Hall 定理的有限版本邏輯等價，讀者可以參考這篇文章【http://robertborgersen.info/Presentations/GS-05R-1.pdf】。我們以下也會看到幾個例子。
- 在 Hall 定理所宣稱的等價關係中，正向蘊含幾乎是顯然的，而反過來卻困難許多，其中有一部分的原因可以想成因為定理的證明是非構造性的，也就是說我們實際上並沒有給出一個具體的配對，甚至也沒有給出一種好的演算法來做匹配。數學家 T. Gowers 在他的部落格裡寫了一篇小品【https://gowers.wordpress.com/2008/12/28/how-can-one-equivalent-statement-be-stronger-than-another/】，讀者可以看看他的想法以及底下其他人的回應。

我們在一開始說過，Hall 並不是第一個發現這個性質的數學家，那麼為什麼要在定理冠上他的名字呢？原因是他簡單的描述讓許多不明顯的性質逐一浮現，從 1930 年代到 1950 年代之間是相異代表系的起步時期，一直到 1960 年代，這套理論和擬陣理論相結合，更大展異彩，其中 R. Rado 是功不可沒的。

現在假設有 n 個人比循環賽，也就是說任意兩個人之間都恰好比一場賽，而且沒有平手的賽局。我們可以給出最後的積分表 $(w_1,\dots,w_n)$，其中 w_i 是第 i 個人的總勝場數，不妨假設 $w_1 \geq \cdots \geq w_n$，顯然有 $(w_1,w_2,\dots,w_n) \succ_M (n-1,n-2,\dots,0)$ (這裡提醒讀者 $\succ_M$ 表示數列的優超關係。對於跳過預備知識 0.3 小節進階集合論的讀者，可以直接看第 6 頁的定義 1，該定義並不需要集合論的知識)。問題是，這是否也是一個充分條件呢？也就是說，給定一個非負整數數列 $(w_1,\dots,w_n)$，如果 $(w_1,w_2,\dots,w_n) \succ_M (n-1,n-2,\dots,0)$，是不是一定存在一種循環賽使得第 i 個人恰好贏了 w_i 場？

這個命題與 Hall 定理有異曲同工之妙，他們的本質都在於，給定一個由某些物件所形成的集合以及某個性質，在不違反這個性質的條件之下我們可以從這個集合裡拿出多少物件？比方 Hall 定理就是要依序從 $A_1,A_2,\dots$ 中取出元素，使得每次拿出的元素都與之前的不同；而循環賽問題可以想像成，從 $i=1,\dots,n$ 依序列出 w_i 場比賽 (第 i 個人打贏的那些比賽)，使得每次列出的比賽都與之前的不同 (否則會有 i 贏 j，而 j 也贏 i)。

為了讓這個想法再清楚些，我們再給一個例子：現給定由 $\mathbb{R}^3$ 裡向量組成的集合 A_1,A_2,A_3，假設對其中任意的 $m \leq 3$ 個集合的聯集 $A_{i_1} \cup \cdots \cup A_{i_m}$，裡面的的向量都至少張成一個 m 維空間，是否能取出 $(a_1,a_2,a_3) \in A_1 \times A_2 \times A_3$ 使得 a_1,a_2,a_3 線性獨立？對於這個問題，則是可以考慮成要依序取出 a_1,a_2,a_3 使得每次取出的元素都不在之前張成的空間裡。以上三者是我們稱為組合最優化的課題，對於一般的討論，文獻[4,15,22] 是非常好的教科書，特別是 Alexander Schrijver 被譽為經典的那三冊書。以下我們要介紹擬陣理論來處理這幾個問題。

定義 2 假設 E 是一個有限集 (稱之為基礎集)，而 $\mathcal{I}$ 是由一些 E 的子集合 (稱之為獨立集) 所形成的集合，並滿足

1. $\emptyset \in \mathcal{I}$.
2. 如果 $A \in \mathcal{I}$ 且 $A' \subseteq A$，那麼 $A' \in \mathcal{I}$.
3. 如果 $(A_1,A_2) \in \mathcal{I}^2$ 且 $|A_1| < |A_2|$，那麼存在 $x \in A_2 \setminus A_1$ 使得 $A_1 \cup \{x\} \in \mathcal{I}$.

那麼 $M=(E,\mathcal{I})$ 稱之為一個擬陣。

■ **習題 4.** 擬陣的性質

1. 證明 $(\{1,2,3\},\{\emptyset,\{1\},\{2\},\{3\}\})$ 是擬陣。

2. 對任意有限集 E，證明 $(E, \mathcal{P}(E))$ 是擬陣。

3. 給出最小的集合 $\mathcal{I}$ 使得 $(\{1,2,3,4\}, \mathcal{I})$ 是擬陣，並且 $\{1,2\}, \{2,3,4\}$ 都在 $\mathcal{I}$ 中。

4. (子擬陣) 假設 $M = (E, \mathcal{I})$ 是一個擬陣，且 A 是 E 的子集。定義 $\mathcal{I}_A = \mathcal{P}(A) \cap \mathcal{I}$，證明 $M_A = (A, \mathcal{I}_A)$ 是一個擬陣，稱為在 M 上由 A 導出的子擬陣。例如

   $M = (\{1,2,3\}, \{\{1\}, \{2\}, \{3\}, \{1,2\}\})$, $A = \{1,2\}$, 則 $M_A = (\{1,2\}, \{\{1\}, \{2\}, \{1,2\}\})$.

5. (直和擬陣) 假設 $M = (E, \mathcal{I})$, $N = (F, \mathcal{J})$ 是兩個擬陣。定義

   $$M \oplus N = (E \times \{0\} \cup F \times \{1\}, \{I \times \{0\} \cup J \times \{1\} \mid I \in \mathcal{I},\ J \in \mathcal{J}\}).$$

   證明 $M \oplus N$ 也是擬陣，這稱為 M 和 N 的直和擬陣。

6. 事實上擬陣理論是由線性代數衍生出來的：給定 E 是有限個 3 維空間的向量所形成的集合，令 $\mathcal{I} = \{\{e_1, \ldots, e_n\} \in \mathcal{P}(E) \mid e_1, \ldots, e_n \text{ 線性獨立}\}$，證明 $(E, \mathcal{I})$ 是擬陣。

7. (極大獨立集，極小相依集) 設 $M = (E, \mathcal{I})$ 是一個擬陣。

   a) 如果 $I \in \mathcal{I}$，並且對所有 $e \in E \setminus I$ 都有 $I \cup \{e\} \notin \mathcal{I}$，我們稱 I 是一組極大獨立集 (就是說沒有獨立集可以包含他)，或是 I 為一組基底。證明所有基底的集合大小都是一樣的，這個值又記做 $r(M)$，稱為 M 的秩。

   b) 一個在 $\mathcal{P}(E)$ 中卻不在 $\mathcal{I}$ 中的集合叫做相依集。如果 I 是相依集，並且對所有 $e \in I$ 都有 $I \setminus \{e\} \in \mathcal{I}$，我們稱 I 是一組極小相依集。證明所有極小相依集的集合大小都是一樣的，並且這個值為 M 的秩加 1。

8. (秩函數) 設 $M = (E, \mathcal{I})$ 是一個擬陣。

   a) 設 A 是 E 的子集。考慮 M_A 為在 M 上由 A 導出的子擬陣，我們可以定義出 $r_M(M_A)$，而這個值會取決於 M，也就是說即使對於同一個集合 A，當 M 不同時 $r(M_A)$ 也會不同。例如 $E = \{1,2,3\}$, $A = \{1,2\}$,

   $$M_1 = (\{1,2,3\}, \{\{1\}, \{2\}, \{3\}, \{1,2\}\}),\ M_2 = (\{1,2,3\}, \{\{1\}, \{2\}, \{3\}\}).$$

   則 $r((M_1)_A) = 2 \neq 1 = r((M_2)_A)$.
   當 M 已經固定時 $r(M_A)$ 也唯一確定了，我們可以 $r(A)$ 簡記 $r(M_A)$ (或是記 $r_M(A)$)。特別地，有 $r(E) = r(M_E) = r(M)$.

   b) 證明恆有 $0 \leq r(A) \leq |A|$.

   c) 證明對所有 $A \subseteq B \subseteq E$ 總有 $r(A) \leq r(B) \leq r(E)$.

d) 證明對任意兩個 E 的子集 A, B 恆有 $r(A\cup B)+r(A\cap B)\le r(A)+r(B)$. (提示：取 $\{a_1,\dots,a_l,b_1,\dots,b_m,c_1,\dots,c_n\}$ 為 $A\cup B$ 的一組基底，其中 $a_i\in A\setminus B$, $b_i\in B\setminus A$, $c_i\in A\cap B$，證明 $\{c_1,\dots,c_n\}$ 是 $A\cap B$ 的一組基底。)

e) 證明對任意 E 的子集 A 和 E 的元素 e，都有 $r(A)\le r(A\cup\{e\})\le r(A)+1$.

f) 證明兩個擬陣直和的秩為兩個擬陣的秩相加。

9. (擬陣交集定理) 有時候估計兩個擬陣共同的獨立集大小是很重要的問題 (讀者可以先往下看理解擬陣理論中獨立集的意義後再回來做這道題目，會較能理解為何我們需要這樣的估計)。給定兩個有共同基礎集的擬陣 $M_1=(E,\mathcal{I}_1), M_2=(E,\mathcal{I}_2)$，我們的目的是要證明

$$\max_{J\in\mathcal{I}_1\cap\mathcal{I}_2}|J|=\min_{A\subseteq E}(r_1(A)+r_2(E\setminus A)).$$

a) 證明左式 $\le$ 右式是顯然的。

b) 我們要對 $|E|$ 做數學歸納法證明左式 $\ge$ 右式。證明當 $\mathcal{I}_1\cap\mathcal{I}_2=\emptyset$ 時兩式相等。

c) 以下假設 $\mathcal{I}_1\cap\mathcal{I}_2\neq\emptyset$。任取 $\{e\}\in\mathcal{I}_1\cap\mathcal{I}_2$，藉由考慮 M_1/e 以及 M_2/e 證明兩式相等。

d) 敘述中我們僅考慮兩個擬陣的交集。試寫出任意有限交集所對應到的定理，並證明之。

附註

- 可以看出估計 $r(M)$ 是重要的問題。
- 定義擬陣有許多等價的方法，上面是以獨立集來考慮。另外還可以從所謂的基底、閉集、迴路等等出發去定義。文獻[13,25] 是不錯的入門書。
- 最後一小題提到的擬陣交集定理中我們有一個形如 max = min 的等式，其實有一大串組合定理都寫成這樣的形式，他們又被稱作 minimax 定理，這是 20 世紀組合數學研究的主流，下一章將會更深入探討這個關係。

數學上常常被問的一個問題是：為什麼數學要那麼抽象？而回答總是這樣的：它讓我們能夠理解性質背後共同的結構，並且針對這個核心概念去做更深更廣的探索。例如在天才數學家 Galois 提出高次方程的可解性研究之後，近代代數學就不只是普通的加減乘除運算還有方程式根的算法，而是去研究群、環、體、模等等不一樣的結構，並試著在更高的觀點下解決初等敘述的問題。很多數學的分支就是像這樣，人們先去意識到一些現象的共通本質，然後加以抽象化之後進而發展出一整套的理論。

包含上述提到的三個問題，有很多的研究都會與所謂「獨立」的概念有關。在 1935 年，Whitney 在研究平面圖與代數觀點的圖論時最早意識到這當中的抽象概念，而隨後

MacLane 在研究幾何格子論時也涉及到同樣的觀點，此外代數學家 van der Waerden 在研究向量空間的線性獨立性質時也有類似的抽象化思考。最後以這些人的研究作為源頭，就出現了擬陣的這樣一種抽象化的理論體系。在 1942 年 Richard Rado 成功地將 Hall 定理推廣到擬陣上面，而基本上我們可以說這一章習題中絕大多數出現過的定理 (當然不只) 都是這個定理的直接推論。

定理 2 (Hall-Rado 定理)　給定一個擬陣 $M = (E, \mathcal{I})$，以及一組集合 $A = (A_1, \ldots, A_n) \in \mathcal{P}(E)^n$，那麼存在 $\{a_1, \ldots, a_n\}$ 使得

1. $(a_1, \ldots, a_n)$ 為 A 的一組相異代表系。
2. $\{a_1, \ldots, a_n\}$ 為獨立集。

當且僅當對所有 $\{1, \ldots, n\}$ 的子集合 I，都有 $r(\cup_{i \in I} A_i) \geq |I|$，其中不等式稱為 Hall-Rado 條件。

■ **習題 5.** Hall-Rado 定理

1. 模仿 Hall 定理，證明 Hall-Rado 定理。
2. (缺碼) 給定一個擬陣 $M = (E, \mathcal{I})$，以及一組集合 $A = (A_1, \ldots, A_n) \in \mathcal{P}(E)^n$，證明可以從其中 $n - d$ 個集合各取出一個元素，使得取出來的元素兩兩不同且構成一個獨立集若且唯若對所有 $\{1, \ldots, n\}$ 的子集合 I，都有 $r(\cup_{i \in I} A_i) \geq |I| - d$。

■ **習題 6.** Hall-Rado 定理的應用

1. (Hall 定理) 證明當 S 為有限集時，Hall 定理可以由 Hall-Rado 定理在擬陣 $M = (S, \mathcal{P}(S))$ 上推得。
2. (線性代數) 給定由 $\mathbb{R}^3$ 裡向量組成的集合 A_1, A_2, A_3，假設對其中任意的 $m \leq 3$ 個集合的聯集 $A_{i_1} \cup \cdots \cup A_{i_m}$，裡面的的向量都至少張成一個 m 維空間，證明能取出 $(a_1, a_2, a_3) \in A_1 \times A_2 \times A_3$ 使得 a_1, a_2, a_3 線性獨立。

   附註　讀者在做完這兩道小題後應該可以看出獨立集的取法了。在 Hall 定理中我們要求依序取出的元素要是不同的，也就是說一群元素會形成獨立集當且僅當他們兩兩相異，因此所有 S 的子集合都要是獨立集。在第 2. 小題中我們想要依序取出 a_1, a_2, a_3，使每次取出的元素都不在之前張成的空間裡，也就是說獨立集應該要是所有 $A_1 \cup A_2 \cup A_3$ 中線性獨立的子集。
3. (Gale-Ryser 定理) 現在有一個 $m \times n$ 且所有係數都為 0 或 1 的矩陣 ($(0,1)$-矩陣)，可以寫出 $R = (R_1, \ldots, R_m)$ 以及 $C = (C_1, \ldots, C_n)$ 分別是列合序列以及行合序列，也就是說 R_i 是第 i 列的係數總和，而 C_j 是第 j 行的係數總和。

a) 定義 $R^* = (R_1^*, R_2^*, \dots)$ 為 $R_k^* = |\{i \mid R_i \geq k\}|$。證明 $C \prec_M R^*$.

b) 我們要證明逆命題也是成立的，也就是說如果 $R = (R_1, \dots, R_m)$ 以及 $C = (C_1, \dots, C_n)$ 是兩個非負整數序列，並且 $C \prec_M R^*$，那麼存在一個 $(0,1)$-矩陣以 R 和 C 為列合序列以及行合序列。考慮以下過程：令 E_k 是所有由行和為 C_k 的 $m \times 1$ 矩陣 (且為 $(0,1)$ 矩陣) 所形成的集合，我們的目的就是要依序選出 $e_i \in E_i$ $(1 \leq k \leq n)$ 去拼出一個 $m \times n$ 的矩陣，而且依次拼出來的 $m \times k$ 矩陣第 i 列和都小於等於對應到的 R_i $(1 \leq i \leq m)$.

i. 令 $E = \{(i,j) \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ 是矩陣裡所有位置所形成的集合，記 $X_i = \{(i,k) \mid 1 \leq k \leq n\}$ 為第 i 列的位置集合 $(1 \leq i \leq m)$。我們說 $I \in \mathcal{P}(E)$ 是一個獨立集當且僅當對所有 $1 \leq i \leq m$ 都有 $|I \cap X_i| \leq R_i$，也就是說 I 不能包含第 i 列多於 R_i 個位置。證明這定義出一個擬陣。

ii. 證明秩函數為 $r(A) = \sum_{k=1}^{m} \min\{|A \cap X_i|, R_i\}$.

iii. 證明逆命題。

4. (Landau 定理) 目的是證明給定一個非負整數數列 $(w_1, \dots, w_n)$，則存在一種循環賽使得第 i 個人恰好贏了 w_i 場當且僅當 $(w_1, w_2, \dots, w_n) \succ_M (n-1, n-2, \dots, 0)$。其中正向蘊含是顯然的，現在要證明反向蘊含。假設有一場循環賽，我們可以考慮對應到的矩陣 $P = (P_{i,j})_{1 \leq i,j \leq n}$，其中 $P_{i,j} = 1$ 如果 i 打贏了 j，否則 $= 0$，且 $P_{i,i} = 0$。利用這樣的對應關係以及之前所做的分析證明反向蘊含。

■ 習題 7. 加性數論

加性數論這個領域的一個分支主要在估計集合 $A + B = \{a + b \mid a \in A, b \in B\}$ 中的元素個數，其中 A, B 可能是兩個正整數的子集，或者是兩個 $\mathbb{Z}/p\mathbb{Z}$ 的子集，甚至是兩個某個交換群的子集。當然更一般的情況是討論 $A + B + C$, $A - B$, $2A = A + A$, nA 等等集合的大小。在這個習題中我們研究文獻[10] [21]。其實這個習題是擬陣的直接應用，和 Hall-Rado 沒有關係，只是筆者希望在讀者熟悉獨立集的意義後再來做這道題目。

對正整數 n，藉由考慮一個整數除以 n 的餘數可以在集合 $\{0, \dots, n-1\}$ 上定義加法減法以及乘法，之後將以 $\mathbb{Z}/n\mathbb{Z}$ 記這個集合以及對應到的運算。例如在 $\mathbb{Z}/3\mathbb{Z}$ 中我們可以寫出等式 $2 + 2 = 1, 2 \times 2 = 1$ 等等。在研究 $G = \mathbb{Z}/p\mathbb{Z}$ 中的算術關係時，Cauchy-Davenport 定理是最根本的結果之一：如果 A, B 是兩個 G 的子集，那麼 $|A + B| \geq \min\{p, |A| + |B| - 1\}$。以下承認這個定理。

給定 $M = (E, \mathcal{I})$ 是一個擬陣，以及一個函數 $w : M \to G = \mathbb{Z}/p\mathbb{Z}$，稱之為加權函數。對所有 $X \subseteq E$，定義 $X^w = \sum_{x \in X} w(x)$，而 $M^w = \{B^w \mid B \text{ 為一組基底}\}$。

1. 對 $A \subseteq E$，可以定義 A 的閉集

$$\mathrm{cl}(A) = \{e \in E \mid r(A) = r(A \cup \{e\})\}.$$

證明對所有 $A \subseteq E$，總有 $\mathrm{cl}(\mathrm{cl}(A)) = \mathrm{cl}(A)$.

2. 對於每個 $x \in M$，可以定義 $M/x = (E \setminus \{x\}, \{I \subseteq E \setminus \{x\} \mid I \cup \{x\} \in \mathcal{I}\})$。證明當 $\{x\} \in \mathcal{I}$ 時 (此時說 $\{x\}$ 不是迴圈)，M/x 是一個擬陣。

3. 取 $x \in M$ 使得 $\{x\}$ 不是迴圈。證明對所有 $X \subseteq E \setminus \{x\}$ 都有 $r_{M/x}(X) = r_M(X \cup \{x\}) - 1$.

4. 利用第 1. 小題證明當 $x \in M$ 使得 $\{x\}$ 不是迴圈時，一定有

$$(M/x)^w + G_x \subseteq M^w.$$

其中 $G_x = \{g \in G \mid x \in \mathrm{cl}(w^{-1}(g))\}$.

5. (Schrijver-Seymour 定理) 利用前述兩小題，對 $r(M)$ 做數學歸納法證明

$$|M^w| \geq \min\{p, \sum_{g \in G} |r_M(w^{-1}(g))| - r(M) + 1\}.$$

6. (Erdős-Ginzburg-Ziv 定理) 證明在 G 中任取 $2p-1$ 個元素其中一定有 p 個元素和為 0。(提示：令 $x_1, \ldots, x_{2p-1} \in G$，取 $M = (\{1, \ldots, 2p-1\}, \{I \mid |I| \leq p\}), w(i) = x_i$.)

7. 利用幾個例子思考 Cauchy-Davenport 定理的意義，並找出定理中等號成立的充要條件。

2 組合對偶

所謂的線性規劃指得是在某些線性不等式被滿足的條件下，要求出另一個線性方程的最大值，這是組合最優化問題中的一個重要領域。許多現實生活的問題都可以用線性規劃來處理，例如：網路流、多商品流量等問題，都被認為非常重要。目前已有大量針對線性規劃演算法的研究。很多最優化問題算法都可以分解為線性規劃子問題，然後逐一求解。在微觀經濟學和商業管理領域中，線性規劃亦被大量應用於例如降低生產過程的成本等手段，最終提升產值與營收。

以下是維基百科上線性規劃的一個例子：假設一個農夫有一塊面積為 A 平方公里的農地，打算種植小麥或大麥，或是兩者依某一比例 (x_1, x_2) 混合種植。該農夫只可以使用有限數量的肥料 F 和農藥 P，而單位面積的小麥和大麥都需要不同數量的肥料和農藥，小麥以 (F_1, P_1) 表示，大麥以 (F_2, P_2) 表示。設小麥和大麥的每單位的售價分別為 S_1 和 S_2，則小麥與大麥的種植面積問題可以表示為以下的線性規劃問題：

$$\max \quad Z = S_1 x_1 + S_2 x_2 \quad \text{(最大化利潤 − 目標函數)}$$

$$\text{要求} \begin{cases} x_1 + x_2 \leq A & \text{(種植面積的限制)} \\ F_1 x_1 + F_2 x_2 \leq F & \text{(肥料數量的限制)} \\ P_1 x_1 + P_2 x_2 \leq P & \text{(農藥數量的限制)} \\ x_1 \geq 0 & \text{(不可以栽種負數的面積)} \\ x_2 \geq 0 & \text{(不可以栽種負數的面積)} \end{cases}$$

我們可以在 (x_1, x_2) 平面上畫出要求條件的那些直線，最後會包圍出一塊區域，而目的就是在這塊區域中找到使得 $Z = S_1 x_1 + S_2 x_2$ 最大的點 (或是值)。

最早解線性不等式組的研究可以追朔到法國數學家 Joseph Fourier，他在 1827 年提出一種演算法求解，這個方法現今被稱為 Fourier–Motzkin elimination。之後一直要到 1939 年，前蘇聯數學以及經濟學家 Leonid Kantorovich 才將一般的敘述用現今熟知的語言描寫出。第二次世界大戰時，各國都絞盡腦汁想找出一種策略使得能有效節省購買軍備的花費，並同時使敵國賠上越多的軍債，而他的研究就是建立在此之上而發展出來的。在大約同一時期，荷蘭裔美國籍的數學以及經濟學家 T. C. Koopmans 利用線性規劃的語言重新公式化一些經典的經濟學問題，後來這兩人都於 1975 年拿到了諾貝爾經濟學獎。

在 1946-1947 年之間，美國數學家 George B. Dantzig 獨立地發展了一般線性規劃的概念，這有效促使了博弈論之父 John von Neumann 在他賽局上的研究，事實上這類命題的對偶與他的問題是等價的。

我們可以考慮上述農夫的對偶問題：假如有另一個農夫缺少肥料和農藥，他希望同先前這個農夫購買，兩人於是談判付肥料和農藥的價格。如何構造一個數學模型來研究如何既使得原先的農夫覺得有利可圖肯把肥料和農藥的資源賣給他，同時使得自己支付的金額最少？問題可以表述如下：假設 y_1, y_2 分別表示每單位肥料和農藥的價格，則所支付租金最小的目標函數可以表示為

$$\min \quad E = Fy_1 + Py_2 \quad (\text{最小化成本} - \text{目標函數})$$

$$\text{要求} \begin{cases} F_1y_1 + P_1y_2 \leq S_1 & (\text{控制肥料與農藥的價格，使得農夫覺得比起拿那些肥料和農藥去種植小麥，賣給園主更有利可圖}) \\ F_2y_1 + P_2y_2 \leq S_2 & (\text{與上相似，但改為大麥}) \\ y_1 \geq 0 & (\text{不可用負數單位金額購買}) \\ y_2 \geq 0 & (\text{不可用負數單位金額購買}) \end{cases}$$

我們可以想像總會有 $E \geq Z$，否則第一個農夫賣出肥料和農藥只會賠錢。

用矩陣的形式來寫的話，會有如下的問題：

原始問題	對偶問題
最大化 $\mathbf{c}^\top\mathbf{x}$	最小化 $\mathbf{y}^\top\mathbf{b}$
要求 $\mathbf{Ax} \leq \mathbf{b}, \mathbf{x} \geq 0$	要求 $\mathbf{y}^\top\mathbf{A} \geq \mathbf{c}^\top, \mathbf{y} \geq 0$

其中 $\mathbf{A}, \mathbf{b}, \mathbf{c}$ 給定，而 $\mathbf{x}, \mathbf{y}$ 是未知行向量。

定義 3 由要求的不等式所限制出來的區域稱為可行區域，當一個行向量 $\mathbf{x}'$ 在可行區域中時，我們稱它為可行解，如果它進一步滿足 $\mathbf{Ax}' \leq \mathbf{b}, \mathbf{x}' \geq 0$ 且

$$\mathbf{c}^\top\mathbf{x}' = \max\{\mathbf{c}^\top\mathbf{x} \mid \mathbf{Ax} \leq \mathbf{b}, \mathbf{x} \geq 0\}$$

時，我們說他是原始問題的最佳解。類似地，可以定義對偶問題的最佳解。

定理 3 (線性規劃對偶定理) 對於所有線性規劃，原始問題有最佳解當且僅當對偶問題有最佳解。並且此時

$$\max\{\mathbf{c}^\top\mathbf{x} \mid \mathbf{Ax} \leq \mathbf{b}, \mathbf{x} \geq 0\} = \min\{\mathbf{y}^\top\mathbf{b} \mid \mathbf{y}^\top\mathbf{A} \leq \mathbf{c}^\top, \mathbf{y} \geq 0\}$$

附註

- 是否有最佳解並不是一個很容易直接驗證的性質，但如果我們認識一些拓撲性質，其實可以發現可行區域的有界性蘊含最佳解的存在性，證明如下：比方取原始問題，注意到 $\mathbf{Ax} \leq \mathbf{b}, \mathbf{x} \geq 0$ 會定義出一個 $\mathbb{R}^{\text{某維度}}$ 的閉集 (因為線性函數是連續的)，如果這個集合又有界，那麼它是緊緻的，所以連續函數 $\mathbf{x} \mapsto \mathbf{c}^\top \mathbf{x}$ 將在上面取到最大值。尚未學過拓撲的讀者可以直接承認這個性質。

- 原始問題的最佳解如果存在那它一定在可行區域的邊界上，否則當它在可行區域的內部時，我們將這個最佳解 $\mathbf{x}'$ 往 $\mathbf{c}$ 的方向移動一點點 (即是說考慮 $\mathbf{x}' + t\mathbf{c}$)，它仍然在可行區域內但卻讓 $\mathbf{c}^\top \mathbf{x}$ 變得更大。同理對偶問題的最佳解如果存在那它一定在可行區域的邊界上。

- 這篇講義不會證明這個定理，因為筆者沒找到喜歡的證法。

■ **習題 1.** 最大流最小割定理

以下內容取材自維基百科。考慮一個現實生活上的問題：某個城市裡有一種水管分布，每條水管都有一特定的寬度，因此只可以保持一特定的水流量。當任何水管匯合，流入匯流點的總水量必須等於流出的水量，否則我們會很快地缺水，或者是會有水的屯積。這個水流的分布網有一個作為源點的入水口，和一個作為匯點的出水口。一道流便是一條由源點到匯點而使從出水口流出的總水量一致的可能路徑。直觀地，一個網路的總流量是水從出口流出的速率，於是產生一個很重要的民生問題——這個分布網一次最多可以允許多少流量的水？

在圖論中，網路流是指在一個每條邊都有容量的有向圖分配流，使一條邊的流量不會超過它的容量。一道流必須符合每一個頂點 (在這裡又稱為節點) 的進出的流量相同的限制，除非這是一個源點——有較多向外的流，或是一個匯點——有較多向內的流。

嚴謹一點的定義是，假設 $G = (V, E)$ 是一個有限的有向圖 (即是說邊是有固定方向的，所以 邊 $(a, b) \neq$ 邊 (b, a))，它的每條有向邊 $(u, v) \in E$ 都有一個非負值實數的容量 $c(u, v)$，而如果 $(u, v) \notin E$，我們假設 $c(u, v) = 0$。另外區別兩個頂點：一個源點 s 和一個匯點 t。一道網路流是一個對於所有結點 u 和 v 都有以下特性的實數函式 $f : V \times V \to \mathbb{R}$：

- 容量限制：$f(u, v) \leq c(u, v)$。一條邊的流不能超過它的容量。

- 斜對稱：$f(u, v) = -f(v, u)$。由 u 到 v 的淨流必須是由 v 到 u 的淨流的相反。

- 流量守恆：除非 $u = s$ 或 $u = t$，否則 $\sum_{w \in V} f(u, w) = 0$。所有結點的淨流是零，除了「製造」流的源點和「消耗」流的匯點。

可以看出流量守恆又會寫成以下形式：

$$\forall v \in V \setminus \{s,t\},\quad \sum_{u:(u,v)\in E} f(u,v) = \sum_{u:(v,u)\in E} f(v,u).$$

流的流量的定義是

$$|f| = \sum_{v\in V} f(s,v).$$

s 為源點，代表著從源點流向目標點的流量。於是上述的水流問題即是要求流量的最大值。以下給定一個網路 $(G=(V,E),s,t,c)$。

—第一部分—

1. 證明任意網路流的總流量是零，也就是說

$$|f| = \sum_{v\in V} f(s,v) = \sum_{v\in V} f(v,t).$$

為了研究最大流問題，定義一個 $s-t$ 割 $C=(S,T)$ 是一種使得 $s\in S, t\in T$ 的將 V 分成兩個不相交子集的劃分。C 的割集是集合 $\{(u,v)\in E \mid u\in S, v\in T\}$。注意如果 C 的割集中的邊被移除了，那必定有 $|f|=0$。一個 $s-t$ 割的容量定義是

$$c(S,T) = \sum_{(u,v)\in E\cap S\times T} c(u,v).$$

而最小 $s-t$ 割問題是要計算 $c(S,T)$ 的最小值，即找到 S 和 T 使 $s-t$ 割的容量達到它的最小值。

2. 證明總有最小割 $\geq$ 最大流。即

$$\min_{(S,T)\text{是一個}s-t\text{割}} c(S,T) \geq \max_{f\text{是一個網路流}} |f|.$$

3. 以下要證明最小割 $=$ 最大流，這個結果又被稱作最大流最小割定理。令 P 是蒐集所有由 s 到 t 的簡單路徑 (也就是說每條邊最多只會走一次) 所形成的集合，對所有簡單路徑 $p\in P$，都引入變數 x_p，表示這條路徑上的總流量。證明最大流問題可以寫成

$$\begin{cases} \text{最大化} & \sum_{p\in P} x_p & & \\ \text{要求} & \sum_{e\in p} x_p & \leq c(e) & \forall e\in E \\ & x_p & \geq 0 & \forall p\in P \end{cases}$$

4. 試寫出他的對偶問題 (假設對偶問題的未知行向量是 $\mathbf{y}$)，給出解釋。證明最小割 $\geq$ 對偶問題的最佳解。

難5. 由上可知使用對偶還不能證明最大流最小割定理，必須要再證明最小割 = 對偶問題的最佳解。我們邀請讀者參考維基百科的這個頁面 (https://zh.wikipedia.org/wiki/戴克斯特拉算法)，並用此找出依據權重 $y_{(u,v)}$ 所定義出的從 s 到 v 的距離，記為 $d(v)$.

難6. 證明最小割 $\leq$ 對偶問題的最佳解。由此最大流最小割定理得證。

—第二部分—

這裡要給出最大流最小割定裡的一些應用，這個部分的題目相對而言較困難。

1. 證明 Hall 婚姻定理。

2. (Menger 定理) 令 $G = (V, E)$ 是一張圖而 s, t 是兩個頂點。證明彼此間不相交從 s 到 t 的簡單路徑數的最大值等於從 G 中拿掉邊後使得 s 和 t 無法被路徑連通的拿掉邊數最小值。

3. (König 定理) 給定一張無向的二分圖 $G = (U, V, E)$，所謂的一個匹配集指的是由某些不相交的邊 (即沒有任何頂典蓉時在兩條邊上) 所形成的集合。而一個頂點覆蓋集指的是圖上每條邊至少包含該集合的一個點。那麼

$$\max_{M\text{為匹配集}} |M| = \min_{S\text{為頂點覆蓋集}} |S|.$$

4. (Dilworth 定理) 給定一個偏序集。我們稱一個任意兩個元素都不能比大小的集合為一個反鏈，而任意兩個元素都能比大小的集合為一個鏈。證明在任意有限偏序集裡反鏈中元素個數的最大值等於將這個偏序集分成許多鏈的聯集的鏈個數最小值。(提示：考慮上一題。)

5. (Mirsky 定理) 這是上題的對偶。證明在任意有限偏序集裡鏈中元素個數的最大值等於將這個偏序集分成許多反鏈的聯集的反鏈個數最小值。

6. (零和遊戲) 對於想多了解一些博弈理論的讀者筆者建議參考維基百科的這個頁面 (https://zh.wikipedia.org/wiki/零和博弈)。對於正整數 n，以 e_n 表示所有係數均為 1 的 n 維行向量，證明對任意正整數 n, m 以及 $n \times m$ 的矩陣 P 總有

$$\max_{\{x\in\mathbb{R}^n | e_n^\top x=1, x\geq 0\}} \min_{\{y\in\mathbb{R}^m | e_m^\top y=1, y\geq 0\}} y^\top P x = \min_{\{y\in\mathbb{R}^m | e_m^\top y=1, y\geq 0\}} \max_{\{x\in\mathbb{R}^n | e_n^\top x=1, x\geq 0\}} y^\top P x.$$

附註

- Dilworth 定理有幾個有趣的應用，例如 Erdős–Szekeres 定理：給定 $nm+1$ 個兩兩不等的實數，那麼一定可以找出其中 $n+1$ 個呈遞增數列，或是可以找出其中 $m+1$ 個呈遞減數列。讀者可以用整數的整除關係編出其他題目嗎？

- 文獻[22] 裡可以找到更多線性規劃在數學上的應用。另外文獻[5] 是最近發表的論文，旨在探討正則圖的獨立集性質，也是關於線性規劃在組合數學上的一個有趣應用，讀者有興趣可以先看[26] 裡面的解釋。

■ 習題 2. 數論：篩法

國中時大家都學過 Eratosthenes 的質數篩法：寫出 $1 \sim n$ 的所有正整數，首先從 2 開始，篩除掉所有 2 的倍數，接著從剩下的數中挑出最小的那個 (所以是 3)，並再次篩除掉所有這個的倍數，依此類推，而最後剩下來的數就是 $1 \sim n$ 中的所有質數了。如果用稍微抽象一點的描述，我們可以想像所謂的篩法指的是這樣的一個過程：先給定一個正整數子集 A，接著對每個質數 p 都給出一個集合 A_p，裡面的元素滿足某種特定的性質，而目的是估計出 $A \setminus (\cup A_p)$ 的大小。例如 Eratosthenes 質數篩法就是取 $A = \mathbb{N}$, $A_p = \{n \mid p \text{ 整除 } n\}$。

這個習題靈感來自於 Terence Tao 的這篇部落格【https://terrytao.wordpress.com/2015/01/21/254a-notes-4-some-sieve-theory】，只是這裡研究的組合篩法有點太一般化，讀者在書上或其他地方較常看到的會是以下的內容：給定正整數子集 $\mathcal{A}$，以及質數子集 $\mathcal{P}$，還有某個正實數 y，目的是要估計集合 $\mathcal{A}$ 中有多少元素不被小於等於 y 而且在 $\mathcal{P}$ 中的質數所整除，也就是說要估計集合 $\mathcal{S}(\mathcal{A}, \mathcal{P}, y) = \{a \in \mathcal{A} \mid p \in \mathcal{P}, \gcd(a, p) > 1 \Rightarrow p > y\}$ 的大小。為了達成這個目標，對每個正整數 d，都定義如下的集合：$\mathcal{A}_d = \{a \in \mathcal{A} \mid d \text{ 整除 } a\}$，如果集合 $\mathcal{A}$ 裡的數在自然數中分布的夠均勻，那麼可以期待 $|\mathcal{A}_d| = |\mathcal{A}|/d$，但這並不總是如此，所以我們會寫成

$$|\mathcal{A}_d| = |\mathcal{A}| \cdot \frac{\rho(d)}{d} + R_d.$$

其中 $\rho(d)/d$ 表示取到集合 $\mathcal{A}_d$ 裡元素的機率，而 R_d 是誤差項。一般來說會要求 ρ 是個積性函數 (也就是說當 m, n 是兩個互質的正整數時會有 $\rho(mn) = \rho(m)\rho(n)$)，因為當 m, n 互質時一個 $\mathcal{A}$ 裡的數能被正整數 m 整除和被正整數 n 整除應為兩個獨立事件。

總體來說估計 $|\mathcal{A}_d|$ 是相對容易的，事實上由此出發推敲 $|\mathcal{S}(\mathcal{A}, \mathcal{P}, y)|$ 的值也是可行的，因為可以合理的猜測大約會有

$$|\mathcal{S}(\mathcal{A}, \mathcal{P}, y)| \approx |\mathcal{A}| \cdot \prod_{p \in \mathcal{P},\, p \le y} \left(1 - \frac{\rho(p)}{p}\right).$$

這是一個粗略的估計。由此想法出發可以有 Brun 組合篩法、Selberg 篩法、大篩法、小篩法等等，以及他們的各種形式。中國解析數論學家陳景潤在 1966 年證明了大偶數必可表為一個質數及一個不超過二個質數的乘積之和，又於 1978 年證明了存在無窮多個不超過二個質數乘積的正整數，減掉 2 後會是一個質數，這些都是篩法的重大里程碑。

以下正式進入習題，考慮以下形式的篩法問題 (理想篩法)：令 P 是一個無平方因數的正整數。對 P 的每一個質因數 p，都給定一個正整數子集 E_p，並且由此對所有 $d \mid P$

定義 $A_d = \bigcap_{p|d} A_p$，最後設 $A_1 = \mathbb{Z}$。除此之外再給定 $(a_n)_{n\in\mathbb{Z}}$ 是一個只有有限項非零的非負實數數列。假設說對某些 $d \mid P$ 我們知道 $X_d = \sum_{n\in A_d} a_n$ 的值 (把這些 d 收集起來構成集合 $\mathcal{D}$)，那麼是否能給出

$$\sum_{n\notin\bigcup_{p|P} A_p} a_n$$

的一組上下界？

以下用一道小題目來說明 (對應到上述 $P = 6$ 而 $A_p = \{n \mid p \text{ 整除 } n\}, \mathcal{D} = \{1,2,3\}$)：假設 $(a_n)_{n\in\mathbb{Z}}$ 是一個只有有限項非零的非負實數數列，已知

$$\sum_{n\in\mathbb{Z}} a_n = 100, \quad \sum_{n\in\mathbb{Z},2|n} a_n = 20, \quad \sum_{n\in\mathbb{Z},3|n} a_n = 30.$$

意圖求出 $S = \sum_{n\in\mathbb{Z},(6,n)=1} a_n$ 的值。

藉由注意到 $X_1 = S + X_2 + X_3 - X_6$ 且 $0 \le X_6 \le \min\{X_2, X_3\}$，不難說明

$$50 \le \sum_{n\in\mathbb{Z},(6,n)=1} a_n \le 70.$$

這個例子是簡單的。

1. 考慮以下定義：

   定義 4 所謂的上界篩指的是滿足以下條件的一個 $\nu^+ : \mathbb{Z} \to \mathbb{R}$ 函數：

   a) 可以找到某些實數 $\lambda_d^+ \in \mathbb{R}$ 使得 $\nu^+ = \sum_{d\in\mathcal{D}} \lambda_d^+ 1_{A_d}$.

   b) 對所有整數 n 都有 $\nu^+(n) \ge 1 - 1_{\bigcup_{p|P} A_p}(n)$.

   類似地可以定義下界篩是滿足以下條件的一個 $\nu^- : \mathbb{Z} \to \mathbb{R}$ 函數：

   a) 可以找到某些實數 $\lambda_d^- \in \mathbb{R}$ 使得 $\nu^- = \sum_{d\in\mathcal{D}} \lambda_d^- 1_{A_d}$.

   b) 對所有整數 n 都有 $\nu^-(n) \le 1 - 1_{\bigcup_{p|P} A_p}(n)$.

   利用對偶證明

   $$\max_{(a_n)_{n\in\mathbb{Z}}\text{是滿足理想篩法的條件的數列}} \sum_{n\notin\bigcup_{p|P} A_p} a_n = \min_{\text{對應到的}\nu^+\text{是上界篩}} \sum_{d\in\mathcal{D}} \lambda_d^+ X_d.$$

2. 利用對偶證明

   $$\min_{(a_n)_{n\in\mathbb{Z}}\text{是滿足理想篩法的條件的數列}} \sum_{n\notin\bigcup_{p|P} A_p} a_n = \max_{\text{對應到的}\nu^-\text{是下界篩}} \sum_{d\in\mathcal{D}} \lambda_d^- X_d.$$

以下考慮理想篩法的一個簡略應用。我們的目的是要概算出在 $1^2+1, 2^2+1, \ldots, n^2+1$ 中有多少正整數不被任何一個 $1 \sim x$ 中的質數所整除。以下承認一個數論性質：同餘方程式 $f(X) = X^2 + 1 \equiv 0 \pmod{p}$ 在 p 除以 4 餘 1 時有兩組解，而在 p 除以 4 餘 3 時無解。

3. 定義一個整數數列 $(a_n)_{n\in\mathbb{Z}}$ 為 $a_{f(i)} = 1$ $(i = 1, \ldots, n)$，而其餘的 a_j 則 $= 0$，並取 P 是所有小於等於 x 的質數的乘積。證明 $\lambda_d^+ = (-1)^{\omega(d)}$ 對應到一個上界篩 (其中 $\omega(d)$ 表示正整數 d 的質因數個數)。

4. 證明 $1^2+1, 2^2+1, \ldots, n^2+1$ 中不被任何一個 $1 \sim x$ 中的質數所整除的正整數個數

$$\geq \frac{n}{2} \prod_{\substack{p\leq x \\ p\equiv 1 \pmod 4}} \left(1 - \frac{2}{p}\right) - 3^{\pi(x)}.$$

   其中 $\pi(x)$ 是不超過 x 的質數個數。

當 n 足夠大使得右式 > 0 時，我們知道 $(1^2+1)\cdots(n^2+1)$ 會有一個 $> x$ 的質因數，但要求出這樣的 n 的下界需要一些解析數論的預備知識，所以習題就此打住，而筆者宣稱可以取 n 為 $3^x \log x$ 的某個固定常數倍，由此可以反過來說明 $(1^2+1)\cdots(n^2+1)$ 總會有一個大於 $\log n$ 某個固定常數倍的質因數。同樣的想法告訴我們當有一個整係數多項式 f 時，如果能知道同餘方程式 $f(X) \equiv 0 \pmod p$ 的解數，就能夠在一定程度上估算乘積 $f(1)\cdots f(n)$ 的最大質因數。另一個類似的命題則是希望直接估計 $f(n)$ 的最大質因數，可以看出這是更難而且需要更強大的方法才能下手的問題，這兩者是數論中在 1950 年代後占有重要地位的課題。

5. 利用上述給出以下命題的一種篩法證明：對一個正整數數列 $(u_n)_{n\in\mathbb{N}}$，以 $\mathbb{P}((u_n))$ 記他的質因數集，也就是說 $\mathbb{P}((u_n)) = \{p \text{ 為質數} \mid \text{存在 } n \in \mathbb{N} \text{ 使得 } p \text{ 整除 } a_n\}$。試證明對於一個整係數多項式 f，$\mathbb{P}(f(n))$ 總是無窮集。讀者認識其他初等的證明方法嗎？

3 Ramsey 理論

1928 年，英國數學家、哲學家兼經濟學家 F. P. Ramsey 在倫敦數學會上宣讀了一篇題為《On a problem of formal logic》的論文。他在這一篇談論型式邏輯的文章中證明了組合數學歷史上最為經典的一個結果，這個定理經常被人用通俗的語言描述如下：只要總人數夠多，就必定能從中找到所求數目的人、使得這些人彼此互相都認識或者互相都不認識。在 1930 年前後，各國數學家獨立地發現了好幾個形式各異的數學定理，他們的本質都是相同的，這些定理構成了現在稱為 Ramsey 理論的基礎。

Ramsey 本人在他提出了這個定理的不久之後就因病在 26 歲便英年早逝了，無法繼續做更進一步的研究，幸好這一系列的工作得以被 Erdős 等人繼承下去，而現在為了紀念他，我們便將這類的理論通稱為 Ramsey 理論，其基本精神都是在於研究當一個充分大的組合結構在做分解時的現象，其最典型的結論常常是型如「只要物件夠多，必定可以在其中找到任意想要的結構。」R. L. Graham 曾在 1983 年國際數學家大會上說過：「數學常被稱為是關於秩序的科學，Ramsey 理論的中心思想也許可以用一句格言來做最好的詮釋—不可能有完全的無序。」

定理 4 (Ramsey 定理)　給定某些至少都為 2 的正整數 $c, n_1, \ldots, n_c$，那麼存在正整數 $R(n_1, \ldots, n_c)$ 使得當我們任意地把一個頂點數 (至少) 為 $R(n_1, \ldots, n_c)$ 的完全圖的邊染上 c 種顏色時，總可以找到 $i \in \{1, \ldots, c\}$ 使得圖中有頂點數為 n_i 且所有邊都是色 i 的子圖。

Proof. 從一個多數讀者可能看過的例子開始：如果把一個頂點數為 6 的完全圖的邊染上兩種顏色，那一定有一個同色三角形 (對應到 $c = 2, n_1 = n_2 = 3$)。證明如下：假設說兩種顏色是紅色跟藍色。任取一個頂點，他會連出去 5 條邊，由鴿籠原理至少有 3 條邊是同一種顏色的，可以假設是紅色。現在進一步考慮連到的這三個頂點，如果有兩個頂點連的邊是紅色的，證明就結束了，否則任兩個頂點連的邊是藍色的，此時也有藍色三角形，所求結論仍然成立。

我們將模仿上述先證明 Ramsey 定理 $c = 2$ 的情況。

引理 1　當 n_1, n_2 都 ≥ 2 時 $R(n_1, n_2)$ 存在，且 $R(n_1, n_2) \leq R(n_1 - 1, n_2) + R(n_1, n_2 - 1)$.

Proof. 以下對 $n_1 + n_2$ 進行數學歸納法證明命題。當 $n_1 = 2$ 或 $n_2 = 2$ 時顯然 $R(n_1, n_2)$ 是存在的。現在假設 $n_1, n_2 \geq 3$，任意對一個頂點數為 $R(n_1 - 1, n_2) + R(n_1, n_2 - 1)$ 的完

全圖做邊的 2-染色。隨意取一頂點，由鴿籠原理知道以下敘述至少一者為真：

1. 有 $R(n_1-1,n_2)$ 條染上色 1 的邊。
2. 有 $R(n_1,n_2-1)$ 條染上色 2 的邊。

不妨假設第一個敘述為真，那麼取出這些染上色 1 的邊所對應到的頂點，由假設可知他們所形成的完全圖有頂點數為 n_1-1 的且所有邊都是色 1 的子圖或是有頂點數為 n_2 的且所有邊都是色 2 的子圖，因此引理成立。 □

再來對染色數 c 進行數學歸納法，由上知 $c=2$ 時定理成立。

引理 2 當 $c>2$ 時 $R(n_1,\ldots,n_{c-1},n_c)\le R(n_1,\ldots,R(n_{c-1},n_c))$.

Proof. 任意對一個頂點數為 $R(n_1,\ldots,R(n_{c-1},n_c))$ 的完全圖做邊的 c-染色，並暫時將色 $c-1$ 和色 c 看作是同一種顏色。由歸納假設由以下敘述至少一者為真：

1. 對某個 $i\in\{1,\ldots,c-2\}$，圖中有頂點數為 n_i 且所有邊都是色 i 的子圖。
2. 有頂點數為 $R(n_{c-1},n_c)$ 且所有邊都是色 $c-1$ 或色 c 的子圖。

容易驗證無論在何種情況引理總成立。 □

至此 Ramsey 定理得證。 □

■ **習題 1.** Ramsey 定理的應用

以下為方便，對於正整數 m 將以 $[m]$ 簡記集合 $\{1,\ldots,m\}$。而當我們說對於某些物件進行染色時，其實是指以下的一個過程：對於集合 E，在 E 上的 n-染色指的是一個函數 $\chi:E\to[n]$，其中 $\chi(e)$ 是元素 $e\in E$ 所染到的顏色，這個函數又被稱作染色函數。

1. 對於實數數列 $a_1,a_2,\ldots$，當對所有 $i\ge 2$ 都有 $a_i<\frac{1}{2}(a_{i-1}+a_{i+1})$ 時我們說它是嚴格凸的；而當對所有 $i\ge 2$ 都有 $a_i>\frac{1}{2}(a_{i-1}+a_{i+1})$ 時則說它是嚴格凹的。證明所有由兩兩不等的實數所構成的數列中，一定有嚴格凸的子數列或是嚴格凹的子數列。
2. 證明對任意圖 H_1,H_2 總存在圖 $G=G(H_1,H_2)$，使得當我們將 G 的頂點集進行 2-染色後一定可以找到色 1 的 H_1 子圖或色 2 的 H_2 子圖。
3. 將實數集 $\mathbb{R}$ 進行 2-染色，證明對所有正整數對 (m,n)，總存在同色實數 $x<y<z$ 滿足 $m(z-y)=n(y-x)$.
4. (Schur 定理) 欲研究方程式 $a+b=c$ 的同色解 (a,b,c)。

a) 給定正整數 n，證明存在正整數 $S(n)$ 使得對於 $[S(n)]$ 的任一個 n-染色，方程式 $a+b=c$ 總有同色解。(提示：考慮頂點集為 $\mathbb{N}$ 完全圖 G，將邊 (i,j) 染上 $|i-j|$ 的顏色。)

b) 承認以下數論性質：對任意質數 p，總有正整數 g 使得 $g^1,\dots,g^{p-1}$ 模 p 後恰好為 $1,\dots,p-1$ 的某個排列。證明 Fermat 最後猜想的變形：對所有正整數 n，總存在 P 使得對所有質數 $p \geq P$，方程式 $x^n+y^n \equiv z^n \pmod{p}$ 有解。

5. 試問能否將正整數集進行有限染色，使得存在函數 $f:\mathbb{N}\to\mathbb{N}$ 滿足：對所有 $(x,y)\in\mathbb{N}^2$ 正整數 $x+f(y)$ 和 $y+f(x)$ 都是不同色的?

■ **習題 2.** 緊緻性定理

1. (Ramsey 定理—有限形式) 這是 Ramsey 定理的另一個形式。給定正整數 n,k,m，總存在正整數 $R^{(k)}(n,m)$ 使得對於 $[R^{(k)}(n,m)]^{(k)}$ 的任一個 n-染色，都可以找到一個有 m 個元素的子集 A 使得 $A^{(k)}$ 是單色的。

2. (Ramsey 定理—無窮形式) 給定正整數 n,k 以及一個可數無窮集 X，那麼對於 $X^{(k)}$ 的任一個 n-染色，總存在一個無窮子集 A 使得 $A^{(k)}$ 是單色的。(提示：對 $k\geq 2$ 使用數學歸納法，證明存在某個 $x_1\in X$，和某個無窮子集 $X_1\subseteq X$ 使得 $x_1\in X_1$ 且 X_1 中所有包含 x_1 的 k 元子集都是單色的。)

   附註 讀者可以看出無窮形式和有限形式的定理是不一樣的，從有限形式的定理我們最多只能證明對於 $X^{(k)}$ 的任一個 n-染色，可找到任意大的有限子集 A 使得 $A^{(k)}$ 是單色的；而從無窮形式出發，也看起來無法推回任何跟有限形式相關的結論。以下我們要較深入地探討這個關係。

3. (緊緻性定理) 緊緻性定理是符號邏輯和模型論中的基本事實，用白話點的語言來說它斷言一個邏輯式對於一個集合是成立的若且唯若這個邏輯式對它的所有有限子集都是成立的。

   以下我們將證明圖論形式的 Erdős-de Bruijn 緊緻性定理：令 G 是一張無窮超圖，任一條超邊都是有限集，若其所有有限子圖都可以被 k-點著色 (即是說可把點著 k 色，使得沒有兩個相鄰的點著同色)，那麼 G 也可以。

   a) 假設 G 的頂點只有可數無窮多個。以 H_n 表示 $V'=\{1,2,\dots,n\}$ 的導出子圖，由於 G 的所有有限子圖都可以被 k-點著色，這代表對所有 n，存在染色函數 $\chi_n:\{1,2,\dots,n\}\to\{1,2,\dots,k\}$，使得 χ_n 作用在 H_n 上是 k-點著色。
   現考察無窮數列 $(\chi_n(1))_{n\in\mathbb{N}}$，由鴿籠原理知道存在顏色 c_1 以及無窮集 $S_1\subseteq\mathbb{N}$ 使得 $\chi_n(1)=c_1$ $(\forall n\in S_1)$。再考察無窮數列 $(\chi_n(2))_{n\in S_1}$，同理存在無窮集

$S_2 \subseteq S_1$ 使得 $\chi_n(2) = c_2$。可以根據這個過程歸納地定義出染色函數 $\chi^*(i) = c_i$ $(\forall i \in \mathbb{N})$。證明這是 G 的 k-點著色。

b) 當 G 的頂點不只有可數無窮多個時上述的證明便不可行了。利用 Zorn 引理證明一般狀況。

4. 利用緊緻性定理證明無窮形式的 Ramsey 定理蘊含有限形式。

5. 試在一個頂點集為 $\mathbb{R}$ 的完全圖上進行邊的 2-染色，使得沒有任何頂點集序數為 $|\mathbb{R}|$ 的單色子圖。因此 Ramsey 定理只對可數無窮集成立。

小時候大家都一定玩過井字遊戲，而多數讀者可能都知道當兩個夠聰明的玩家在 3×3 的方格玩時結果一定是平手，沒有任何一方有必勝策略。於是新的問題產生了：如果在一個 $3 \times 3 \times 3$ 的立方體玩，是否仍然會平手呢？後者的答案較不明顯，因為 3 維空間比 2 維空間多了很多條可以連成一直線的方格，所以兩個玩家可行的策略看起來更多了。在這個例子中，其實稍微暴力一下便可以發現在 $3 \times 3 \times 3$ 的井字遊戲中先手必勝，但這個方法不夠好，因為當我們問多人玩家在 $n \times \cdots \times n$ 中玩時是否無人有必勝策略時暴力法顯然是不可行的。

1963 年 A. W. Hales 和 R. I. Jewett 回答了上述問題。他們的 Hales–Jewett 定理是當今許多深刻研究的基石，更重要的，它完全顯示出 Ramsey 理論的本質，因此曾有數學家說，“Without this result, Ramsey theory would more properly be called Ramseyan theorems.” 我們從一些基本定義開始。

定義 5 假設 A 是一個有 t 個元素的字母表 (alphabet)，記做 $A = \{0, 1, \ldots, t-1\}$。而 $*$ 是一個不在字母表裡的符號。

- 單字是由一串子母組成的有序數列。
- 根是由一串子母以及至少一個 $*$ 組成的有序數列。
- 對於 $(A \cup \{*\})^n$ 中的一個根 τ 以及某個字母 a，以 $\tau(a)$ 記為 τ 中的 $*$ 全部以 a 取代後所得到的單字。
- 一條由根 τ 所定義出來的線是指

$$L_\tau = \{\tau(0), \tau(1), \ldots, \tau(t-1)\}.$$

- 設 a, b 為兩個單字或根，那麼 ab 記為把 b 接在 a 後組成的有序數列。
- 設 a, b 為不全為單字的兩個單字或根，那麼簡記線 L_{ab} 為 $L_a L_b$。

例如當 $A = \{0, 1, 2, 3\}$ 時，$a = (1, 2, 3)$ 是一個單字，而 $b = (1, *, 2)$ 是一個根，由這個根所對應到的線為 $L_b = \{(1, 0, 2), (1, 1, 2), (1, 2, 2), (1, 3, 2)\}$，最後 $ab = (1, 2, 3, 1, *, 2)$.

定理 5 (Hales-Jewett 定理) 給定正整數 n,k，以及一個有 k 個字母的字母表 A，總存在正整數 $HJ(n,k)$ 使得對於 $A^{HJ(n,k)}$ 的任一個 n-染色，存在一條單色線。

Proof. 我們進行雙重歸納法。首先對 $k=1$ 命題是顯然的，現在要從 $k-1$ 推到 k。我們再考慮以下引理：

引理 給定正整數 n,k,l，其中 $l \leq k$，以及一個有 k 個字母的字母表 A，總存在正整數 $HJ(n,k,l)$ 使得對於 $A^{HJ(n,k,l)}$ 的任一個 n-染色，存在一條單色線，或是存在 l 條共用某個點的線，而且除去這個頂點後每條都是單色線 (這些線稱為偽單色線，而共用的頂點稱為焦點)。

假如引理證完，那麼在引理中取 $l=k$，知道要嘛有一條單色線，要嘛有 k 條偽單色線。若是後者，考慮那些線共用的頂點，就知道其中一定有一條長為 k 的單色線，代表 $HJ(n,k)$ 存在，就證完 HJ 定理。

而證明這個引理，我們要用到 $HJ(n,k-1)$ 的存在性，然後對 l 進行數學歸納法：$l=1$ 是顯然的，因為取 $HJ(n,k,1)=HJ(n,k-1)$ 即可。現在要從 $l-1$ 推到 l，我們宣稱一件事：可以取 $HJ(n,k,l)=s_1+s_2$ $(s_1=HJ(n,k,l-1), s_2=HJ(((k+1)^{s_1}n)^{l-1},k)$.

Proof. 對於任一 $A^{s_1+s_2}$ 裡面的點，我們可以把它寫成 $[x,y]$ 的形式，其中 $x\in A^{s_1}, y\in A^{s_2}$。現在我們先固定某個 $y\in A^{s_2}$，然後考慮新的塗色方式 χ_y：它讓 $x\in A^{s_1}$ 塗上 $[x,y]$ 的顏色 (就是說 $\chi_y(x)=\chi([x,y])$，其中 χ 為原本塗色方式)。這樣做的時候，我們等於是把 A^{s_1} 的點作 n-染色，根據 s_1 的定義，裡面會有 $l-1$ 條偽單色線 (若有一條單色線就直接得證)，把這些線叫作 $L_{y,1}, L_{y,2}, \ldots, L_{y,l-1}$，對應的顏色為 $\chi_{y,1}, \chi_{y,2}, \ldots, \chi_{y,l-1}$。這些偽單色線及其顏色可以看做是 A^{s_2} 裡頭的點 y 所擁有的一種特質，因此定義一個函數 f 為 $f(y)=\{(L_{y,1},\chi_{y,1}),\ldots,(L_{y,l-1},\chi_{y,l-1})\}$。

現在我們來看要怎麼用 s_2。首先我們考慮上面定義的函數 f 它的值域為何：假設現在任給一個集合 $\{(L_{y,1},\chi_{y,1}),\ldots,(L_{y,l-1},\chi_{y,l-1})\}$，將所有元素視為獨立 (這樣估計的值域會大一點)，那顯然 $\chi_{y,i}$ 最多有 n 種取法，$L_{y,i}$ 有 $(k+1)^{s_1}-k^{s_1}<(k+1)^{s_1}$ 種取法，因此 f 的值域最多有 $((k+1)^{s_1}n)^{l-1}$ 個元素。現在把這些元素一個一個賦值到 $1,\ldots,((k+1)^{s_1}n)^{l-1}$，稱賦值函數為 ϕ。然後把所有 $y\in A^{s_2}$ 作一種新的染色方式：y 塗上 $\phi(f(y))$ 的顏色。這樣做等於是把 A^{s_2} 的點作 $((k+1)^{s_1}n)^{l-1}$-染色，根據 s_2 的定義，裡面會有一條單色線 L。那麼對於任意點 $y'\in L$，這些 y' 是單色的，並考慮這些 y' 所對到的 $f(y')$，比方說我們知道 $=\chi([x_{y',1},y'])=\chi([x_{y',2},y'])=\cdots$ (對所有 $x_{y',i}\in L_i$)，因此得到 $l-1$ 條偽單色線 L_iL。最後設 $L_{y',i}$ 這些線的焦點是 A，那 AL 會和上述 $l-1$ 條偽單色線構成 l 偽單色線。 □

至此，HJ 定理得證。 □

雖然筆者已經盡力寫詳細了，不過相信還是有許多人看不懂這到底在做什麼，這邊舉一個例子讓大家比較好理解 (以下數列記法中我們可能會把括號以及逗點拿掉，例如 $(0,1,2)$ 和 012 是一樣的)：取 $A=\{0,1,2,3,4\}$，假設在引理中要從 $r=2$ 條偽單色線推到 3 條偽單色線，並設我們算出來的 $s_1=4, s_2=5$。那麼考慮的就是形如 $([\cdot,\cdot,\cdot,\cdot],[\cdot,\cdot,\cdot,\cdot,\cdot])$ 這樣的座標。比方說先固定 $y=(0,1,2,2,2)$，那麼再來就是看 $(\cdot,\cdot,\cdot,\cdot)$ 這樣的點 (為方便直接把 y 拿掉)。現在把這種點拿來染色，定義為 $\chi_y(x)=\chi([x,y])$，比方 $(1,2,3,4)$ 就是染成跟原來 $(1,2,3,4,[y])=(1,2,3,4,0,1,2,2,2)$ 相同的顏色。所以我們在 A^{s_1} 上做了一個 4-染色，由 s_1 的定義會有 2 條偽單色線。

現在把所有 $y\in A^{s_2}$ 作一種新的染色方式：y 塗上 $\phi(f(y))$ 的顏色，簡單來說我們就是要根據點 y 在上一段找的偽單色線及其顏色來做區分，比方 $y_1=(0,0,0,0,0)$ 找到的兩條偽單色線的根分別是 $\tau_1=(1,*,2,*), \tau_2=(1,4,2,*)$，偽單色線的顏色為 c_1,c_2，那麼當且僅當另一個點 y_2 找到的兩條偽單色線的根也是 $\tau_1=(1,*,2,*), \tau_2=(1,4,2,*)$ 且顏色還分別為 c_1,c_2 時，我們把點 y_1 和 y_2 染同個顏色。這樣做等於是把 A^{s_2} 的點作染色，而根據 s_2 的定義，這裡頭有一條單色線，不妨假設是由 $\tau=(1,2,*,*,4)$ 所定義出來的線。

這代表說 $12004, 12114, 12224, 12334, 12444$ 是同色的，現在由染色函數 ϕ 的定義，這 5 個點所對應到的 2 條偽單色線及其顏色都是完全相同的。假設兩條偽單色線的根分別是 $\tau_1=(1,*,2,*), \tau_2=(1,4,2,*)$，而偽單色線的顏色為 c_1,c_2，也就是說 $1020, 1121, 1222, 1323$ 這四點染上 c_1，但根據定義在最原本的 χ 染色下 1020 和 102012004 同色，所以 102012004 染上 c_1；同樣地 1121 和 112112114 同色，所以 112112114 染上 c_1，...，這樣就得到一條偽單色線 $(1,*,2,*,1,2,*,*,4)$ 了。同理 $(1,4,2,*,1,2,*,*,4)$ 也定義出偽單色線，最後 $(1,4,2,4,1,2,*,*,4)$ 也會是條偽單色線，這三線共點。 □

附註

- HJ 定理和 Ramsey 定理有本質上的不同，在 HJ 定理中我們要求有同色線的存在，也就是說不僅要求某些點是同色的，還要求這些點在同一條線上。然而這些組合線本身就已經有一定的結構了，而在 Ramsey 定理中邊和邊之間卻是完全獨立的。我們可以說在某種觀點下 HJ 定理比 Ramsey 定理使用兩次還要強。

- HJ 定理和 Ramsey 定理中宣稱了有夠大的某個東西就可以找到某種要求的結構，卻沒有告訴我們要多大的集合才會有這種性質。具體來說，假設在習題 2. 中的 Ramsey 有限形式我們改將正整數塗上任意多種顏色，而已知有「足夠多」的數都被塗上某種顏色，那麼最後能否取到被塗上這種顏色的單色集呢？類似地，如果在 HJ 定理中顏色數量也不是有限的，但已知有「足夠多」的點都被塗上某種顏色，那麼最後能否取到被塗上這種顏色的單色線呢？

這些問題又被稱作密度問題，有興趣的讀者可以參考維基百科或是文獻[14,16]。我們在下面的習題會看到一個例子。

■ **習題 3.** 高維 HJ 定理

假設 A 是一個有 t 個元素的字母表，而 $*_1,\ldots,*_d$ 是 d 個不在字母表裡的符號。可以類似的定義單字及根。對於 $(A\cup\{*_1,\ldots,*_d\})^n$ 中的一個根 τ 以及某些字母 $a_1,\ldots,a_d$，以 $\tau(a_1,\ldots,a_d)$ 記為 τ 中的 $*_i$ 全部以 a_i 取代後所得到的單字。一個由根 τ 所定義出來的 d 維空間是指 $S_\tau=\{\tau(a_1,\ldots,a_d)\mid(a_1,\ldots,a_d)\in A^d\}$.

定理 6 (Hales-Jewett 定理) 給定正整數 n,k,d，以及一個有 k 個字母的字母表 A，總存在正整數 $HJ(n,k,d)$ 使得對於 $A^{HJ(n,k,d)}$ 的任一個 n-染色，存在一個單色 d 維空間。

1. 對於尚未充分理解 HJ 定理證明的讀者，試著模仿上述證明 $H(n,k+1,d)\leq H(n,1,d)+H(n,k,d^n)^{H(n,1,d)}$ 且 $H(n+1,1,d+1)\leq H(n,H(n+1,1,d),d+1)$，由此高維 HJ 定理成立。

   而對於以理解 HJ 定理證明的讀者，試著直接證明 $HJ(n,k,d)\leq dHJ(n^d,k)$.

2. (Gallai 定理) 令 $S\subseteq\mathbb{N}^d$ 是個有限集。S 的相似集指的是型如 $a+\lambda S$ 的集合，其中 $a\in\mathbb{N}^d,\lambda\in\mathbb{N}$。比方在 $\mathbb{N}^1$ 中，$\{1,2,\ldots,m\}$ 的相似集就是等差數列。

   證明對任意有限集 $S\subseteq\mathbb{N}^d$，以及任意 $\mathbb{N}^d$ 的 k-染色，一定存在 S 的單色相似集。(提示：設 $S=\{s_1,\ldots,s_m\}$，考慮由下定義的 $S^{HJ(k,m)}$ 的 k-染色：$\chi'(\mathbf{x})=\chi(x_1+\cdots+x_{HJ(k,m)})$, $\mathbf{x}=(x_1,\ldots,x_{HJ(k,m)})$.)

■ **習題 4.** Roth 定理

在前一個習題的 Gallai 定理中如果取 $d=1$ 和 $S=\{1,2,\ldots,m\}$ 將得到 Van der Waerdern 定理：將正整數集有限染色後，可以找到任意長的等差數列。當然和 Ramsey 和 HJ 一樣，我們可以考慮他的密度問題 (Szemerédi 定理)：將正整數集染色後，如果有「足夠多」的正整數都被塗上某種顏色，是否可以找到任意長且被塗上這種顏色的單色等差數列？這個習題改編自[6,7,20]，將帶領讀者證明上述問題的一個較弱版本：

定理 7 對所有 $\delta>0$，當 $n>\exp\exp(1200/\delta)$ 時，只要 $A\subseteq[n]$ 包含至少 δn 個元素，那麼 A 中就有長度為 3 的等差數列 (即 3 個數成等差數列)。

—預備知識—

離散 Fourier 分析是現今加性數論的主流方法，這是由數學家 Timothy Gowers 在 1998 年重新證明 Szemerédi 定理時所引入的，我們以下將介紹這個工具。

提醒讀者對正整數 n，藉由考慮一個整數除以 n 的餘數可以在集合 $\{0,\dots,n-1\}$ 上定義加法減法以及乘法，之後將以 $\mathbb{Z}/n\mathbb{Z}$ 記這個集合以及對應到的運算。例如在 $\mathbb{Z}/3\mathbb{Z}$ 中我們可以寫出等式 $2+2=1, 2\times 2=1$ 等等。

以下為了節省符號，如非特別說明則所有的函數都是指從 $\mathbb{Z}/n\mathbb{Z}$ 到 $\mathbb{C}$ 的函數，並引入 X_n 是 $\mathbb{Z}/n\mathbb{Z}$ 上的均勻隨機變數，並以 $\mathbb{E}$ 表示期望值。對於不熟悉機率的讀者，可以把這些東西就當成一種縮寫，而他們的意義就是說當 f 是一個從 $\mathbb{Z}/n\mathbb{Z}$ 到 $\mathbb{C}$ 的函數時

$$\mathbb{E}[f(X_n)] = \frac{1}{n}\sum_{x\in\mathbb{Z}/n\mathbb{Z}} f(x).$$

最後我們以 $e_n(\cdot)$ 記從 $\mathbb{Z}/n\mathbb{Z}$ 到 $\mathbb{C}$ 的函數

$$e_n(x) = \exp\left(2i\pi\frac{x}{n}\right) = \cos\left(\frac{x}{n}\right) + i\sin\left(\frac{x}{n}\right).$$

1. 證明當 $r\in\mathbb{Z}/n\mathbb{Z}\setminus\{0\}$ 時 $\mathbb{E}[e_n(rX_n)]=0$，否則 $=n$.

2. 當 f 是一個函數時，定義 $\widehat{f}$ 如 $\widehat{f}(r) = n\mathbb{E}[f(X_n)e_n(-rX_n)]$ 是一個從 $\mathbb{Z}/n\mathbb{Z}$ 到 $\mathbb{C}$ 的函數，這個過程稱為 Fourier 變換。證明 Fourier 反演：

$$f(x) = \sum_{r\in\mathbb{Z}/n\mathbb{Z}} \widehat{f}(r)e_n(rx),\ \forall\, x\in\mathbb{Z}/n\mathbb{Z}.$$

3. 證明 Parseval 恆等式

$$\sum_{r\in\mathbb{Z}/n\mathbb{Z}} |\widehat{f}(r)|^2 = n\sum_{r\in\mathbb{Z}/n\mathbb{Z}} |f(r)|^2.$$

4. 當 f,g 為兩個函數時，可以定義卷積 $f*g$ 為 $(f*g)(r) = n\mathbb{E}[f(X_n)g(r-X_n)]$ 仍然是一個從 $\mathbb{Z}/n\mathbb{Z}$ 到 $\mathbb{C}$ 的函數。取三個函數 f,g,h，證明

   a) $f*g = g*f$, $(f*g)*h = f*(g*h)$.

   b) $f*(g+h) = f*g + f*h$.

   c) $\widehat{f*g} = \widehat{f}\cdot\widehat{g}$.

   d) $\mathbb{E}[(f*g)(X_n)] = \mathbb{E}[f(X_n)]\mathbb{E}[g(X_n)]$.

   利用 (c) 證明對於 $\mathbb{Z}/n\mathbb{Z}$ 的任意子集 A 總有

$$\sum_{(x,d)\in(\mathbb{Z}/n\mathbb{Z})^2} 1_A(x)1_A(x+d)1_A(x+2d) = \frac{1}{n}\sum_{x\in\mathbb{Z}/n\mathbb{Z}} \widehat{1_A}(x)^2\widehat{1_A}(-2x).$$

5. 證明

$$f*g(r) = \sum_{y\in\mathbb{Z}/n\mathbb{Z}^2} f(y)e_n(-yr)\sum_{x\in\mathbb{Z}/n\mathbb{Z}^2} g(x-y)e_n(-(x-y)r)$$

6. 對於 $\mathbb{Z}/n\mathbb{Z}$ 的兩個子集 A, B，記得定義 $A+B=\{a+b \mid a\in A, b\in B\}$。試找出 $A+B$ 和 $1_A * 1_B$ 的關係。

—第一部分—

給定 $\mathbb{Z}/n\mathbb{Z}$ 的一個有序子集 P，當它可以被看作是在 $\mathbb{Z}$ 上的等差數列時，我們說 P 是 $\mathbb{Z}$-等差的。例如說在 $\mathbb{Z}/7\mathbb{Z}$ 中，有序子集 $\{5,1,4\}$ 是一個等差數列，因為 $1-5=3=4-1$，然而它並不是 $\mathbb{Z}$-等差的。另一方面有序子集 $\{2,4,6\}$ 就同時是等差數列和 $\mathbb{Z}$-等差的。我們要證明以下性質：

宣稱 1 假設 $1\geq\delta>0$ 且 $n\geq 50/\delta^2$，那麼對所有包含至少 δn 個元素的 $A\subseteq\mathbb{Z}/n\mathbb{Z}$，只要對於所有 $r\in\mathbb{Z}/n\mathbb{Z}\setminus\{0\}$ 都有 $|\widehat{1_A}(r)|\leq\delta^2 n/100$，那麼以下敘述有至少一者為真。

(i) 在 A 中有長度為 3 的 $\mathbb{Z}$-等差數列。

(ii) 存在一個 $\mathbb{Z}$-等差數列 $P\in\mathbb{Z}/n\mathbb{Z}$，它的長度 $\geq\lfloor n/3\rfloor$，且滿足 $|A\cap P|\geq(\delta+\delta/6)|P|$.

1. 把 $\mathbb{Z}/n\mathbb{Z}$ 不相交地分成 3 個子集合 $I_1=\{0,\ldots,\lfloor n/3\rfloor-1\}, I_2=\{\lfloor n/3\rfloor,\ldots,\lfloor 2n/3\rfloor-1\}, I_3=\{\lfloor 2n/3\rfloor,\ldots,n-1\}$，並令 $B=A\cap I_2$。以下假設條件 (ii) 不為真，證明有 $|B|\geq\delta n/5$.

2. 令 $N(A)$ 為 $y-x\equiv z-y \pmod n$ $(x,y,z)\in A\times B\times B$ 的解數。證明 $N(A)$ 只會算到 $\mathbb{Z}$-等差數列。

3. 由於在 $N(A)$ 的定義中沒有規定不能有 $x=y=z$，所以會把退化的 $\mathbb{Z}$-等差數列也算進去。我們可以用一個很粗略的估計：A 中至少有 $N(A)-|B|\geq N(A)-n$ 個長度為 3 的的 $\mathbb{Z}$-等差數列，因此為了證明條件 (i) 為真，只須證明 $N(A)>n$.

   寫出

$$\begin{aligned}N(A)&=\frac{1}{n}\sum_{r\in\mathbb{Z}/n\mathbb{Z}}\sum_{x\in A}\sum_{y\in B}\sum_{z\in B}e_n((2y-x-z)r)\\&=\frac{1}{n}\sum_{r\in\mathbb{Z}/n\mathbb{Z}}\widehat{1_A}(r)\cdot\widehat{1_B}(-2r)\cdot\widehat{1_B}(r).\end{aligned}$$

4. 由 Cauchy 不等式證明

$$N(A)\geq\frac{1}{n}|A||B|^2-\frac{1}{n}\max_{r\neq 0}|\widehat{1_A}(r)|\cdot\left(\sum_{r\neq 0}|\widehat{1_B}(-2r)|^2\right)^{1/2}\cdot\left(\sum_{r\neq 0}|\widehat{1_B}(r)|^2\right)^{1/2}.$$

5. 注意到當 s 固定時 $s\equiv -2r \pmod n$ 至多只有兩個解 r，證明 $\sum_{r\neq 0}|\widehat{1_B}(-2r)|^2\leq 2\sum_{r\neq 0}|\widehat{1_B}(r)|^2$。並由宣稱中的敘述得到

$$N(A)\geq\frac{|A||B|^2}{n}-\frac{\delta^2}{50\sqrt{2}}\sum_{r\neq 0}|\widehat{1_B}(r)|^2.$$

6. 利用 Parseval 恆等式證明條件 (i) 為真。

—第二部分—

宣稱 2 如果 $n \geq 50$ 且 $\delta > 0$，那麼對所有包含至少 δn 個元素的 $A \subseteq \mathbb{Z}/n\mathbb{Z}$，以下敘述至少一者為真。

(i) 對所有 $r \in \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$，有 $|\widehat{1_A}(r)| \leq \delta^2 n/100$.

(ii) 在 $\mathbb{Z}/n\mathbb{Z}$ 中存在一個至少有 $\delta^2\sqrt{n}/5000$ 個元素的一個 $\mathbb{Z}$-等差有序子集 P，使得 $|A \cap P| \geq (\delta + \delta^2/800)|P|$.

給定 $n \geq 50$，並取一個包含至少 δn 個元素的 $A \subseteq \mathbb{Z}/n\mathbb{Z}$，假設敘述 (i) 是不成立的，那麼我們要敘述 (ii) 成立。由假設取某個 $r \in \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$ 使得 $|\widehat{1_A}(r)| > \delta^2 n/100$.

1. 令 m 是小於等於 $n/(6\lceil\sqrt{n}\rceil)$ 的最大正整數，首先要找到 $\mathbb{Z}/n\mathbb{Z}$ 中一個長度為 $2m+1$ 且有夠好性質的等差數列。

   考慮數 $jr \pmod n$ $(j = 0, \ldots, \lceil\sqrt{n}\rceil)$，由鴿籠原理證明存在正整數 λ 使得

   $$\lambda \leq \lceil\sqrt{n}\rceil, \quad |\lambda r \,(\mathrm{mod}\, n)| \leq \lceil\sqrt{n}\rceil.$$

2. 藉由考慮集合 $\{-m\lambda, -(m-1)\lambda, \ldots, -\lambda, 0, \lambda, \ldots, (m-1)\lambda, m\lambda\}$ 證明 $\mathbb{Z}/n\mathbb{Z}$ 中有一個長度為 $2m+1$ 的等差數列。令這個集合為 Q.

3. 證明對這個集合 Q，有 $\widehat{1_Q}(r) > |Q|/2$.

4. 令 f_A 是由 $f_A(x) = 1_A(x) - |A|/n$ 給出的函數，而 $h_{A,Q} = f_A * 1_Q$。證明

   $$\mathbb{E}[|h_{A,Q}(X_n)|] \geq \frac{1}{n}|\widehat{f_A}(r)||\widehat{1_Q}(r)|, \quad \mathbb{E}[h_{A,Q}(X_n)] = 0.$$

5. 由前述證明

   $$\mathbb{E}[h_{A,Q}(X_n) + |h_{A,Q}(X_n)|] \geq \frac{\delta^2}{200}|Q|.$$

   因此可取到 $x \in \mathbb{Z}/n\mathbb{Z}$ 使得 $h_{A,Q}(x) \geq \frac{\delta^2}{400}|Q|$.

6. 藉由考慮除以 n 的餘數，可以把 $Q_x = \{x - q \mid q \in Q\}$ 當成是 $\mathbb{Z}/n\mathbb{Z}$ 的子集。由定義證明

   $$h_{A,Q}(x) = |A \cap Q_x| - \frac{|A|}{n}|Q_x|.$$

7. 注意到 $|Q_x| = |Q|$，由上述證明

   $$|A \cap Q_x| \geq \left(\delta + \frac{\delta^2}{400}\right)|Q|.$$

8. 藉由寫成
$$Q = \{-m\lambda \,(\mathrm{mod}\, n), \ldots, 0 \,(\mathrm{mod}\, n), \ldots, m\lambda \,(\mathrm{mod}\, n)\}$$
證明 Q 可以寫成兩個 $\mathbb{Z}$-等差數列的聯集；類似地證明 Q_x 可以寫成兩個 $\mathbb{Z}$-等差數列的聯集，並假設這兩個 $\mathbb{Z}$-等差數列叫做 P 和 P'.

9. 證明當 P 和 P' 其中一個集合只包含 $< \delta^2|Q_x|/800$ 個元素時，另一個集合將會滿足條件 (ii).

10. 我們於是假設 P 和 P' 都包含 $\geq \delta^2|Q_x|/800$ 個元素。證明對其中一者，比方說 P，會有
$$\frac{|A \cap P|}{|P|} \geq \frac{|A \cap Q_x|}{|Q_x|} \geq \delta + \frac{\delta^2}{400}.$$
利用 $n \geq 50$ 證明這個集合會滿足條件 (ii)。至此宣稱證畢。

—第三部分—

現在用上述兩個宣稱證明定理 7。對 $\delta > 0$，以 $H(\delta)$ 記命題「當 $n > \exp\exp(1200/\delta)$ 時，只要 $A \subseteq [n]$ 包含至少 δn 個元素，那麼 A 中就有長度為 3 的等差數列。」以下將使用的方法叫做 density increment argument，這個論述的想法是說，首先 $\delta \geq 1$ 時命題是顯然為真的，而如果進一步存在某個函數 f 使得有蘊含式 $H(f(\delta)) \Rightarrow H(\delta)$，並且對所有 $\delta > 0$ 將 f 迭代夠多次之後總會有 $f(\delta) \geq 1$ 時，那麼命題總是成立的！

在以上的兩個宣稱中，我們觀察到下列重要性質

- 總會把 A 放進某個 $\mathbb{Z}$-等差數列 P 中，使得 $A \cap P$ 在 P 中的密度變得更大 (也就是說 $|A \cap P|/|P| \geq |A|/n$)。
- 如果說可以在 $A \cap P$ 中取出一個「對於 P 為 $\mathbb{Z}$-等差數列」的 $\mathbb{Z}$-等差數列，那麼這個 $\mathbb{Z}$-等差數列對於 $\mathbb{Z}/n\mathbb{Z}$ 仍為一個 $\mathbb{Z}$-等差數列。

在定理 7 中我們要求 $A \subseteq [n]$，但其實可以考慮 $A_0 = \{a - 1 \mid a \in A\} \in \mathbb{Z}/n\mathbb{Z}$。試利用以上觀察到的兩個性質以及 density increment argument 證明定理 7。

附註 以上的兩個宣稱說明的是一個集合的 Fourier 係數與這個集合表現得像不像等差數列之間的關係，可以定義所謂的 Fourier 權重 $\|A\|_u$ 為
$$\|A\|_u = \max_{r \neq 0} |\widehat{1_A}(r)|.$$
會有許多 Fourier 權重和等差數列之間的關係式，另外預備知識的第 4,6 小題告訴我們可以用這樣的方法來計算和集 $A + B$ 中等差數列的數量。

對於想多了解離散 Fourier 分析在加性數論上應用的讀者，可以參考這篇課程講義 (http://math.rice.edu/~kk43/cmcthesis.pdf)，另外對於較一般的討論可以閱讀文獻[23] 和另一篇講義 (https://www.math.cmu.edu/~af1p/Teaching/AdditiveCombinatorics/Tao.pdf).

4 討論與未來展望

在這篇講義中有許多部份因為受到筆者能力的限制，或者有時候是要求的預備知識起點太高，所以有許多點並沒有更深入地去介紹，也因此才在許多地方附上參考資料，希望有動力的讀者能夠自主地去學習。

依筆者淺見，文章中有許多理論、問題都很適合拿來做科展，甚至是更進一步的研究。比方說一些大方向的問題像是能否將 Ramsey 理論和擬陣擬論做結合？而 minimax 定理與數學歸納法與 Ramsey 理論又有何種關聯 (讀者可以上維基百科看 Dilworth 定理的數學歸納法證明想想)？當然我們也可以問一些小小的改良像是定理 7 中能不能改進下界 $n > \exp\exp(1200/\delta)$？或是第一章 Landau 問題中如果循環賽的定義是任意 k 個人之間都恰好比一場賽，而每一次賽局都恰有一個人勝出，那麼怎樣的數列可以是積分表？等等，類似的想法都可能是非常好的研究題材。

更高等的純組合數學有時會用到拓撲學，例如說 Hall 婚姻定理其實和 Tychonoff 是等價的，而 Hales-Jewett 可以在整數集上定義一個拓撲再用超濾子證出。所以如果讀者想要做這方面的科展研究，必須要有足夠的邏輯學與拓撲學預備知識。

最後可能有一些讀者希望走競賽，那麼網站 (http://www.artofproblemsolving.com/community/c13_contests) 是不可或缺的，裡面可以找到世界各國各年度大大小小的競賽題目。筆者在第一章曾經放過幾道競賽題，但後面懶得繼續找所以留給讀者自行做這些功課了。

Bibliography

[1] J. L. Arocha. A Generization of the Ph. Hall's theorem. Uni. Nac. Auto. de Mexico, 81 (1985).

[2] T. C. Brown, A proof of Sperner's lemma via Hall's theorem, Proc. Camb. Philos. Soc. 78 (1975).

[3] T. Ceccherini-Silberstein & M. Coornaert. Cellular Automata and Groups. Springer, 2010 edition.

[4] L. Eugene. Combinatorial Optimization: Networks and Matroids. Dover Publications (2001).

[5] D. Ewan & J. Matthew & P. Will & R. Barnaby. Independent Sets, Matchings, and Occupancy Fractions. arXiv:1508.04675 (2015).

[6] W. T. Gowers. Fourier analysis and Szemerédi's theorem. In Proceedings of the International Congress of Mathematicians, Vol. I (Berlin, 1998), number Extra Vol. I, pages 617–629 (electronic) (1998).

[7] W. T. Gowers. A new proof of Szemerédi's theorem. Geom. Funct. Anal. 11 (3): 465–588. doi:10.1007/s00039-001-0332-9. MR 1844079 (2001).

[8] A. W. Hales & R. I. Jewett. Regularity and positional games. Trans. Amer. Math. Soc. 106: 222–229 (1963).

[9] M. Hall. Distinct representatives of subsets. Bull. Amer. Math. Soc., 54 (1948), pp. 922–926.

[10] Y. O. Hamidoune & I. P. da Silva. Distinct Matroid Base Weights and Additive Theory. eprint arXiv:0903.0642 (2009).

[11] D. Jungnickel. Graphs, Networks and Algorithms. Springer, 3rd ed. 2008 edition.

[12] H. G. Landau. On dominance relations and the structure of animal societies: I. Effect of inherent characteristics. Bulletin of Mathematical Biophysics 13: 1 (1951).

[13] J. Oxley. Matroid Theory. Oxford University Press; 2 edition (2011).

[14] D. Pandelis & K. Vassilis & T. Konstantinos. A simple proof of the density Hales-Jewett theorem. Inter. Math. Res. Not. 12, 3340-3352 (2014).

[15] C. H. Papadimitriou & K. Steiglitz Combinatorial Optimization: Algorithms and Complexity. Dover Publications (1998).

[16] D. H. J. Polymath. A new proof of the density Hales–Jewett theorem. Annals of Mathematics. 175 (3): 1283–1327 (2012).

[17] R. Rado, A theorem on independence relations, Quart. J. Math. Oxford 13 (1942), pp. 83–89.

[18] R. Rado. Note on the transfinite case of Hall's theorem on representatives. J. London Math. Soc., 42 (1967), pp. 321–324.

[19] R. M. Robinson, On the Decomposition of Spheres, Fund. Math. 34:246–260.

[20] K. F. Roth. On certain sets of integers. J. London Math. Soc., 28:104–109 (1953).

[21] A. Schrijver & P.D. Seymour. Spanning trees of different weights. Polyhedral combinatorics (Morristown, NJ, 1989), 281–288, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., 1, Amer. Math. Soc., Providence, RI (1990).

[22] A. Schrijver. Combinatorial Optimization: Polyhedra and Efficiency. Algorithms and Combinatorics. 24. Springer (2003).

[23] T. Terence & V. Van. Additive Combinatorics. Cambridge Studies in Advanced Mathematics. 105. Cambridge University Press (2006).

[24] D. J. A. Welsh. Generalized versions of Hall's theorem. J. Combinatorial Theory Ser. B 10 (1971), 95–101.

[25] D. J. A. Welsh. Matroid Theory. Dover Publications (2010).

[26] Z. Yufei. Extremal regular graphs: independent sets and graph homomorphisms. arXiv:1610.09210 (2016).