數學傳播　46卷1期, pp. 21-32

Alon 的組合零點定理

張鎮華

1. 從 Hilbert 的零點定理談起

本文主要在介紹 Noga Alon (以色列數學家, 1956 年 2 月 17 日生) 利用多項式解決組合問題的工作。這要從 David Hilbert (德國數學家, 1862 年 2 月 23 日 $\sim$ 1943 年 2 月 14 日) 的零點定理 (Nullstellensatz) 說起, 它是代數幾何的一個基礎, 請參見 van der Waerden 的書 [29]。

考慮以某個體 (field) $\mathbb{F}$ 爲係數的所有 n 個變數的多項式 $f = f(x_1, x_2, \ldots, x_n)$ 所成的集合, 其元素可做加、減、乘、除 (除法會產生商式和餘式), 是一個環 (ring), 稱之爲多項式環 $\mathbb{F}[x_1, x_2, \ldots, x_n]$。當 $c \neq 0$ 的時候, f 的某一項 $cx_1^{d_1}x_2^{d_2}\ldots x_n^{d_n}$ 的度數 (degree) $\deg(cx_1^{d_1}x_2^{d_2}\ldots x_n^{d_n})$ 定義成 $d_1+d_2+\cdots+d_n$, 而 f 的度數則定義成 f 當中度數最高的項的度數。舉例來說, 在兩個變數的實係數多項式環 $\mathbb{R}[x, y]$ 中, $x^4+2x^2y^3+3y^2$ 及其各項的度數爲 $\deg(x^4) = 4$、$\deg(2x^2y^3) = 5$、$\deg(3y^2) = 2$、$\deg(x^4+2x^2y^3+3y^2) = \max\{4, 5, 2\} = 5$。

一個體 $\mathbb{F}$ 稱爲代數封閉 (algebraically closed) 的意思是說, $\mathbb{F}$ 中的任意不是常數的多項式一定有 $\mathbb{F}$ 中的根。舉例來說, $\mathbb{R}$ 就不是代數封閉, 因爲多項式 $x^2 + 1$ 沒有實數根。但是 $\mathbb{C}$ 就是代數封閉, 因爲根據代數基本定理, 任意不是常數的複係數多項式一定有一個複數根。

以下就是 Hilbert 的零點定理。

定理 1.1 (**零點定理**)**.** 假設 $\mathbb{F}$ 是一個代數封閉體, $f, g_1, g_2, \ldots, g_m$ 是多項式環 $\mathbb{F}[x_1, x_2, \ldots, x_n]$ 中的一些多項式。如果 $g_1, g_2, \ldots, g_m$ 的共同根也是 f 的根, 則存在一個正整數 k 及 $\mathbb{F}[x_1, x_2, \ldots, x_n]$ 中的一些多項式 $h_1, h_2, \ldots, h_m$, 使得 $f^k = h_1g_1 + h_2g_2 + \cdots + h_mg_m$。

對於 $m = n$ 而且各個 g_i 是單變數多項式 $\prod_{a_i\in S_i}(x_i - a_i)$ 的特殊情況 (其中 S_i 是 $\mathbb{F}$ 的有限非空子集), 有下面這個更強的定理。值得注意的是, 這一次並不需要假設 $\mathbb{F}$ 有代數封閉的條件。

定理 1.2. 假設 $\mathbb{F}$ 是一個體, $f = (x_1, x_2, \ldots, x_n)$ 是 $\mathbb{F}[x_1, x_2, \ldots, x_n]$ 中的一個多項式。如果 $S_1, S_2, \ldots, S_n$ 是 $\mathbb{F}$ 的有限非空子集, 定義 $g_i(x_i) = \prod_{a_i\in S_i}(x_i - a_i)$。如果 $g_1, g_2, \ldots, g_m$

的共同根也是 f 的根 (即對所有 $a_1 \in S_1$、$a_2 \in S_2$、…、$a_n \in S_n$ 都有 $f(a_1, a_2, \ldots, a_n) = 0$), 則存在滿足 $\deg(h_i) \le \deg(f) - \deg(g_i)$ 的多項式 $h_1, h_2, \ldots, h_n$ 使得 $f = h_1 g_1 + h_2 g_2 + \cdots + h_n g_n$。更進一步來說, 當 R 是 $\mathbb{F}$ 的子環, 而且 $f, g_1, g_2, \ldots, g_n$ 都在 $R[x_1, x_2, \ldots, x_n]$ 時, 前述的 h_i 也都在 $R[x_1, x_2, \ldots, x_n]$ 內。

Alon [1] 利用定理 1.2 發展出來的組合零點定理 (Combinatorial Nullstellensatz), 提供了一個靈活的技巧, 可以廣泛地應用在各種組合學的問題上, 尤其在圖論方面的各種應用更是最近幾年的熱門主題之一。

定理 1.3 (組合零點定理). 假設某個體 $\mathbb{F}$ 中有 n 個子集 $S_1, S_2, \ldots, S_n$, 每一個都滿足 $|S_i| > d_i$; 而且 f 是 $\mathbb{F}[x_1, x_2, \ldots, x_n]$ 中的一個多項式。如果 f 的度數爲 $d_1 + d_2 + \cdots + d_n$, 而且它有某個非零項 $cx_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}$, 則存在 $a_1 \in S_1$、$a_2 \in S_2$、…、$a_n \in S_n$ 使得 $f(a_1, a_2, \ldots, a_n) \neq 0$。

對於組合零點定理的證明, Alon [1] 用了一個比較迂迴的論述。他先證明了一個比較弱的性質 (姑且稱之爲弱組合零點定理), 也就是將組合零點定理中的假設

(C1) f 的度數爲 $d_1 + d_2 + \cdots + d_n$, 而且它有某個非零項 $cx_1^{d_1} x_2^{d_2} \ldots x_n^{d_n}$,

換成一個比較強的假設

(C0) $f \neq 0$, 而且它的任意非零項 $cx_1^{d_1'} x_2^{d_2'} \ldots x_n^{d_n'}$ 均滿足 $d_1' \le d_1, d_2' \le d_2, \ldots, d_n' \le d_n$。

Alon 先證明了弱組合零點定理, 用它來證明定理 1.2, 然後再用定理 1.2 來證明組合零點定理。Tao 和 Vu [26] 給了一個直接的數學歸納法證明組合零點定理, 不過他們的證明分成兩步, 還是有點複雜。Michalek [22] 給了一個更直接的證明。亦請參見本文著者 [13, 14] 的證明。後來 Lasoń [21] 證明了一個比較強的性質 (姑且稱之爲強組合零點定理), 也就是將組合零點定理中的假設 (C1) 換成一個比較弱的假設

(C2) f 有某個非零項 $cx_1^{d_1} x_2^{d_2} \ldots x_n^{d_n}$, 且對 f 中任意非零項 $c' x_1^{d_1'} x_2^{d_2'} \ldots x_n^{d_n'}$, 若所有 $d_i' \ge d_i$ 則所有 $d_i' = d_i$。

顯然 (C0) 可推得 (C1), 而 (C1) 可以推得 (C2), 但是反過來都不成立。例如, 當 $d_1 = 2$、$d_2 = 3$、$d_3 = 4$ 時, $x_1^2 x_2^3 x_3^4 + x_1^2 x_2^2 x_3^5$ 滿足 (C1) 但不滿足 (C0), $x_1^2 x_2^3 x_3^4 + x_1^2 x_2^2 x_3^6$ 滿足 (C2) 但不滿足 (C1)。

證明強組合零點定理: 對 $d := d_1 + d_2 + \cdots + d_n$ 做數學歸納法證明。當 $d = 0$ 的時候 $d_1 = d_2 = \ldots = d_n = 0$, f 爲非零常數多項式, 定理顯然成立。假設 $d \ge 1$, 不妨假設 $d_1 \ge 1$。選取 $a \in S_1$, 利用多項式的長除法, 將 f 除以 $x_1 - a$ 可得

$$f(x_1, x_2, \ldots, x_n) = q(x_1, x_2, \ldots, x_n)(x_1 - a) + r(x_2, x_3, \ldots, x_n),$$

由於 f 滿足條件 (C2), 可知 $q(x_1, x_2, \ldots, x_n)$ 有一項 $cx_1^{d_1-1}x_2^{d_2}\ldots x_n^{d_n}$ 滿足條件 (C2) (但其中的 d_1 換成 $d_1 - 1$)、$r(x_2, x_3, \ldots, x_n)$ 是一個有 $n-1$ 個變數的多項式。根據已知條件, $\mathbb{F}$ 的子集 $S_1\backslash\{a\}, S_2, \ldots, S_n$ 除了 $|S_1\backslash\{a\}| > d_1 - 1$ 外都有 $|S_i| > d_i$; 由歸納法假設, 存在$a_1 \in S_1\backslash\{a\}$、$a_2 \in S_2$、…、$a_n \in S_n$ 使得 $q(a_1, a_2, \ldots, a_n) \neq 0$。如果 $r(a_2, a_3, \ldots, a_n) = 0$, 則 $f(a_1, a_2, \ldots, a_n) = q(a_1, a_2, \ldots, a_n)(a_1 - a) \neq 0$; 如果 $r(a_2, a_3, \ldots, a_n) \neq 0$, 則 $f(a, a_2, \ldots, a_n) = r(a_2, a_3, , \ldots, a_n) \neq 0$。定理得證。 □

接下來我們要利用組合零點定理來解決一些組合問題, 其用法就是設法造出一個多項式 $f(x_1, x_2, \ldots, x_n)$ 來模擬想要證明命題的特性, 使得如果這個多項式存在一個特定的點 $(a_1, a_2, \ldots, a_n)$ 滿足 $f(a_1, a_2, \ldots, a_n) \neq 0$ 的話, $(a_1, a_2, \ldots, a_n)$ 就會對應於想要的東西, 然後再用組合零點定理來證明這樣的 $(a_1, a_2, \ldots, a_n)$ 的確存在。這些及更多的內容請參見 Alon 的文章 [1]。

2. Cauchy-Davenport 定理 — 加性數論

在數論中, 加性數論 (additive number theory) 在研究整數的子集合, 以及其在加法下的特性。更抽象來說, 加性數論的研究包括對於有加法運算的交換群 (abelian group) 以及交換半群 (commutative semigroup)。其中主要研究的二個對象分別是交換群或半交換群 G 中二個子集 A 及 B 的和集 (sumset)

$$A + B = \{a + b : a \in A, b \in B\},$$

以及 A 的 k-重和集 (k-fold sumset)

$$kA = \underbrace{A + A + \cdots + A}_{k}。$$

在這方面的研究, 有一個方向是直接問題, 也就是由 A 的結構來判斷 kA 的結構。例如, 假設 A 是一個固定的子集, 判斷哪些元集可以表示爲 kA 中的和元素 (參見 [23])。這方面有二個經典的問題, 一個是 Goldbach 猜想, 也就是, 當 P 是所有質數所成的集合時, 猜想 $2P$ 包括了所有大於 2 的偶數; 另一個是 Waring 問題, 也就是, 當

$$A_n = \{0^n, 1^n, 2^n, 3^n, \ldots\}$$

時, k 要多大才能確保 kA_n 包括所有正整數。

許多這一類的研究常使用 Hardy-Littlewood 圓法 (circle method) 及篩法 (sieve methods) 當工具。例如 Vinogradov 證明了, 每一個夠大的奇數都可以表示爲三個質數的和, 以及所有夠大的偶數都可以表示爲四個質數的和。Hilbert 證明了, 對於每一個正整數 n, 每一個非

負整數都是某一個固定數目 k 的 n 次方數的和, 也就是 kA_n 包含了所有正整數; 例如 $n=2$ 時, 每一個非負整數都是 4 個 2 次方數的和, 也就是 $4A_2$ 包含了所有正整數。

一般來說, 對於某個非負整數的子集 A, 若可以讓 kA 包括所有的正整數, A 就稱爲 k 階的基底 (basis of order k); 若 kA 包括所有夠大的整數, A 就稱爲 k 階漸近基底 (asymptotic basis of order k)。最近有許多研究是關於有限階漸近基底的一般特性, 例如, 若集合 A 是 k 階漸近基底, 但集合 A 的真子集都不是 k 階漸近基底, 則集合 A 稱爲 k 階的最小漸近基底 (minimal asymptotic basis of order k)。目前已經證明了, 對於任意 k, 總是存在 k 階的最小漸近基底, 但是也存在不包含k 階的最小漸近基底的k 階漸近基底。另一個問題是, 一個 n 最少可以表示成某個最小漸進基底中多少個元素的和。著名的 Erdős-Turán 猜想也是有關漸近基底的問題。

另一個方向關注的是反問題 (最近此研究方向常稱爲加性組合學), 假設已經知道和集 $A+B$ 的資訊, 目的是要找到個別集合 A 和 B 的資訊 (參見 [24])。和上述有關基底的問題不同, 這個方向處理的多半是有限子集而不是無限子集。典型的問題是 $|A+B|$ 相對於 $|A|$ 和 $|B|$ 很小時, 這兩個子集有什麼樣的結構。在整數的例子中, 經典的 Freiman 問題用多維算術級數提供了有力的部分答案。另一個典型的問題是要以 $|A|$ 和 $|B|$ 來表示 $|A+B|$ 的下限。這類問題的例子有 Cauchy-Davenport 定理及限制和集 (restricted sumset) 的 Erdős-Heilbronn 猜想。用來解決這類問題的方式來自各數學領域, 例如組合學、遍歷理論、分析、圖論、群論、線性代數及多項式法。

下面來介紹 Cauchy-Davenport 定理。先介紹一些更基礎的內容。

假設 A 和 B 是兩個正整數的有限非空子集, 令 $|A|=n$ 而 $|B|=m$。第一個問題是, $|A+B|$ 可能會多大?

當 $A=\{1,2,\ldots,n\}$ 而 $B=\{n,2n,\ldots,mn\}$ 時, $A+B=\{n+1,n+2,\ldots,n+mn\}$, 此時 $|A+B|=mn=|A||B|$, 相對比較大。事實上, 這已經是最大可能了, 因爲容易看出來, 一般來說都有

$$|A+B|\le |A||B|。$$

另一方面, 當 $A=\{1,2,\ldots,n\}$ 而 $B=\{1,2,\ldots,m\}$ 時, $A+B=\{2,3,\ldots,n+m\}$, 此時 $|A+B|=n+m-1=|A|+|B|-1$, 相對比較小。事實上, 這是最小可能了, 一般來說, 假設

$$A=\{a_1<a_2<\cdots<a_n\}、\quad B=\{b_1<b_2<\cdots<b_m\},$$

則下面這個遞增數列包含了 $A+B$ 中的 $n+m-1$ 個數,

$$a_1+b_1<a_1+b_2<a_1+b_3<\cdots<a_1+b_{m-1}<a_1+b_m<a_2+b_m<\cdots<a_{n-1}+b_m<a_n+b_m。$$

反過來, 我們可以問, 如果 $|A+B|=|A|+|B|-1$, 那麼 A 和 B 會長成甚麼樣子? 當 A 或 B 只有一個元素時, 不管另一個集合長相如何, 顯然會有 $|A+B|=|A|+|B|-1$。所

以假設 $|A| = n \geq 2$ 且 $|B| = m \geq 2$。當 $|A+B| = n+m-1$ 時, 再考慮下面這個遞增數列, 它也包含了 $A+B$ 中的 $n+m-1$ 個數,

$$a_1+b_1<a_2+b_1<a_2+b_2<\cdots<a_2+b_{m-2}<a_2+b_{m-1}<a_3+b_{m-1}<\cdots<a_n+b_{m-1}<a_n+b_m。$$

因爲 $|A+B| = n+m-1$, 前述的兩個數列, $A+B$ 的所有元素恰好都出現在數列中一次, 所以這兩個數列的各對應項相等, 而有

$$a_1 + b_j = a_2 + b_{j-1}\ (2 \leq j \leq m)、a_i + b_m = a_{i+1} + b_{m-1}\ (1 \leq i \leq n-1),$$

也就是

$$a_2 - a_1 = b_j - b_{j-1}\ (2 \leq j \leq m)、a_{i+1} - a_i = b_m - b_{m-1}\ (1 \leq i \leq n-1),$$

因此, A 和 B 是兩個有共同非零公差 d 的等差級數所成的集合。當然, 具有這樣性質的 A 和 B 也會有 $|A+B| = |A|+|B|-1$。

綜合來說, 有如下的性質。

命題 2.4. 若 A 和 B 是 $\mathbb{Z}$ 的有限非空子集, 則 $|A+B| \geq |A|+|B|-1$。更進一步來說, $|A+B| = |A|+|B|-1$ 若且唯若 $|A| = 1$ 或 $|B| = 1$, 或是存在某個 $d > 0$ 使得

$$A = \{a, a+d, a+2d, \ldots, a+(|A|-1)d\}、B = \{b, b+d, b+2d, \ldots, b+(|B|-1)d\}。$$

性質 2.4 的證明主要用到整數可以比較大小, 所以將其中的整數集 $\mathbb{Z}$ 換成實數集 $\mathbb{R}$, 性質還會成立。但是如果將整數集 $\mathbb{Z}$ 換成複數集 $\mathbb{C}$, 情況會是如何呢? 一般常說, 複數集是「不能定義」大小關係的; 這樣的說法其實不夠精確, 更精確來說, 應該是, 如果在複數集定義大小關係, 則不能滿足一般大小關係習慣有的一些性質, 例如

(P1) 三個關係 $a < b$、$a = b$、$b < a$ 恰有一個成立;

(P2) 關係 $0 < a$ 等價於 $-a < 0$;

(P3) 若 $a < b$ 且 $b < c$, 則 $a < c$;

(P4) 若 $a < b$, 則 $a + c < b + c$;

(P5) 若 $a < b$ 且 $0 < c$, 則 $ac < bc$。

如果複數中可以定義滿足前述五個性質的大小關係, 則會產生矛盾, 說明如下。

先來看 $\sqrt{-1}$。因爲 $0 \neq \sqrt{-1}$, 則由 (P1) 可知 $0 < \sqrt{-1}$ 或 $\sqrt{-1} < 0$。當 $0 < \sqrt{-1}$ 時, 由 (P5) 就會得到 $0\sqrt{-1} < \sqrt{-1}\sqrt{-1}$, 也就是 $0 < -1$。當 $\sqrt{-1} < 0$ 時, 由 (P2) 就有 $0 < -\sqrt{-1}$, 再由 (P5) 就會得到 $0(-\sqrt{-1}) < (-\sqrt{-1})(-\sqrt{-1})$, 也就是 $0 < -1$。所以總是有 $0 < -1$, 再一次利用 (P5) 得到 $0(-1) < (-1)(-1)$, 也就是 $0 < 1$, 再由 (P2) 就有 $-1 < 0$, 這和 $0 < -1$ 違反 (P1) 而產生矛盾。

不過, 複數中卻可以定義大小關係爲

「對於實數 a, b, a', b', 若 $a < a'$、或者 $a = a'$ 但是 $b < b'$, 則稱 $a + b\sqrt{-1} < a' + b'\sqrt{-1}$。」

此時雖然性質 (P5) 不成立, 但是 (P1)、(P2)、(P3)、(P4) 都成立。前面證明性質 2.4 時, 其實並不會用到乘法, 只需有性質 (P1)、(P2)、(P3)、(P4) 就夠了。所以性質 2.4 中的 $\mathbb{Z}$ 換成 $\mathbb{C}$ 後還是成立。

這樣來說, 是不是對任何加法系統都會有 $|A+B| \geq |A| + |B| - 1$ 的不等式? 答案是不會。

考慮模環 $\mathbb{Z}_r$, 也就是 $\mathbb{Z}_r = \{0, 1, 2, \ldots, r-1\}$, 其中的加法、乘法是整數的加法、乘法後取 $\bmod r$。例如, 在 $\mathbb{Z}_9$ 中, $3 + 3 = 6$、$6 + 6 = (12 \bmod 9) = 3$、$2 \times 2 = 4$、$4 \times 4 = (16 \bmod 9) = 7$。

要注意的是, 爲了討論性質 2.4 並不需要考慮乘法。其次, $\mathbb{Z}_r$ 中並無法定義大小關係使得性質 (P1)、(P3)、(P4) 都成立, 說明如下。如果 $0 < 1$, 則連續使用 (P4) 就會得到 $1 < 2$、$2 < 3$、$\ldots$、$n-1 < (n-1) + 1 = 0$, 再連續使用 (P3) 就會得到 $0 < 0$, 和 (P1) 矛盾; 如果 $1 < 0$, 則連續使用 (P4) 就會得到 $2 < 1$、$3 < 2$、$\ldots$、$0 = (n-1) + 1 < n - 1$, 再連續使用 (P3) 就會得到 $0 < 0$, 和 (P1) 矛盾。

事實上, 考慮 $\mathbb{Z}_9$ 的部分集合 $A = B = \{0, 3, 6\}$ 時, $A + B = \{0, 3, 6\}$, 所以 $|A + B| = |A| = |B| = 3$, 此時 $|A + B| \geq |A| + |B| - 1$ 並不成立。

不過在特殊情況, 當 r 是質數時, 只要 $|A + B|$ 不超過 r, 確實會有 $|A + B| \geq |A| + |B| - 1$, 這就是著名的 Cauchy-Davenport 定理。

定理 2.5 (Cauchy-Davenport 定理). 若 p 爲質數, A 和 B 爲 $\mathbb{Z}_p$ 的兩個非空子集 , 則 $|A + B| \geq \min\{p, |A| + |B| - 1\}$。

Augustin-Louis Cauchy (法國數學家, 1789 年 8 月 21 日 $\sim$ 1857 年 5 月 23 日) 在 1813 年證明了這個定理, 利用它重新證明了 Joseph-Louis Lagrange (義大利數學家, 1736 年 2 月 25 日 $\sim$ 1813 年 4 月 10 日) 在 1770 年得到的結果, 任意正整數是 4 個平方數的和。後來 Davenport 將此定理敘述爲 Khintchine 的一個關於兩個整數列和的 Schnirelman 密度的猜想 (後來被 H. Mann 證明了) 的離散相似版本, 這個結果有若干推廣, 例如可參見 [24]。Cauchy 和 Davenport 對於定理 2.5 的證明用了相同的組合概念, 都是在 $|B|$ 上做數學歸納法。[9, 10] 最近提供了不同的代數證法, 其優點是可以輕易地推廣到若干相關結果。Alon [1] 利用組合零點定理提供 Cauchy-Davenport 定理的如下的簡單證明, 其中, 當 p 是質數時, $\mathbb{Z}_p$ 是一個體。

證明 Cauchy-Davenport 定理: 如果 $|A + B| \geq p$, 定理顯然成立, 所以只需考慮 $|A + B| \leq p - 1$ 的情況。假設定理不成立, 也就是 $|A + B| \leq |A| + |B| - 2$。令 $S_1 = A$ 且

$S_2 = B$, 則可選取非負整數 d_1 和 d_2 使得 $|A+B| = d_1 + d_2$、$|S_1| > d_1$、$|S_2| > d_2$。考慮 $\mathbb{Z}_p[x, y]$ 中的多項式

$$f(x, y) = \prod_{c \in A+B} (x + y - c),$$

其度數爲 $|A+B| = d_1+d_2$, 而且它有一個項 $\binom{d_1+d_2}{d_1} x^{d_1} y^{d_2}$。因爲 $d_1+d_2 < p$, 所以 $\binom{d_1+d_2}{d_1}$ 當作整數不是 p 的倍數, 當作 $\mathbb{Z}_p$ 的元素不爲 0, 所以根據組合零點定理, 存在 $a \in A$、$b \in B$ 使得 $f(a, b) \neq 0$。因爲 $a + b \in A + B$, 由 $f(x, y)$ 的定義得知 $f(a, b) = 0$, 矛盾。 □

一些涉及限制和集的類似結果如下所述。

定理 2.6 (**Dias da Silva-Hamidoune [15]**). 若 p 爲質數, A 爲 $\mathbb{Z}_p$ 的一個非空子集 , 則 $|\{a + a' : a, a' \in A, a \neq a'\}| \geq \min\{p, 2|A| - 3\}$。

定理 2.7 (**Alon-Nathanson-Ruzsa [9]**). 若 p 爲質數, A 和 B 爲 $\mathbb{Z}_p$ 的兩個非空子集 , 則 $|\{a + b : a \in A, b \in B, ab \neq 1\}| \geq \min\{p, |A| + |B| - 3\}$。

3. 利用組合零點定理證明圖論中的三個定理

圖論這門學問有將近三百年的歷史, 經由各方學者的研究, 已經有很完整的發展, 不但在數學上有其深度, 在其他領域上也有很多應用。很少有一個數學的分支可以說是哪一年誕生的, 而現在大家公認, Euler 在 1736 年解決 Königsberg 七橋問題的文章 [18] 是圖論的起源。

從 1736 年到 1936 年這整整兩百年, 可以說是圖論的春秋戰國時代, 不同領域的人們在他們各自的崗位上, 用不同的名稱、不同的內容, 探索和 Euler 發現的圖一樣的概念 (參見 Biggs、Lloyd 和 Wilson 的書 [11])。一直到 1936 年, Kőnig 寫出圖論的第一本著作《有限和無限圖的理論》[20], 正式宣告圖論這門學問誕生。這以後的八十多年來, 各式各樣的圖論書籍, 呈幾何級數的速度產生。

這一節利用組合零點定理來證明一些圖論上的定理。我們討論的圖都是簡單圖 (simple graph), 也就是, 只有有限多個點、沒有重邊 (multiple edges)、沒有迴邊 (loops); 如果要討論有有限多個點、允許重邊、沒有迴邊的圖, 會稱之爲重圖 (multi-graph) 以便區別。

正則子圖的存在性

Berge 和 Sauer 曾猜想任何 4-正則圖都一定包含一個 3-正則子圖 (參見 Bondy 和 Murty 的書 [12] 第 246 頁), 這個猜想後來被 Taśkinov [27] 證明。不過很容易看出這個猜想對於重圖是不會成立的 (考慮 C_3 把每條邊複製成兩條重邊就是一個反例)。但是可以證明, 一個 4-正則重圖只要再加入一條邊, 就會保證裡面有 3-正則子重圖。而這個結果是下面這個定理的特例, Alon [1] 利用組合零點定理證明如下。

定理 3.1 (**Alon-Friedland-Kalai [3, 4]**). 如果 p 是質數[1], 而且 G 是一個最大度數 $\Delta(G) = 2p-1$ 且平均度數大於 $2p-2$ 的重圖, 則 G 包含一個 p-正則子重圖。

證明: 假設 G 有 n 點及 m 邊。每一條邊 e 定義一個變數 x_e, 然後考慮在有限體 $\mathbb{Z}_p$ 上的多項式

$$f(\vec{x}) = \prod_{v\in V(G)} \left(1 - \Big(\sum_{e\ni v} x_e\Big)^{p-1}\right) - \prod_{e\in E(G)} (1-x_e)\,。$$

這個多項式第一個乘積是把 n 個度數是 $p-1$ 的多項式乘起來, 而因爲 G 的平均度數大於 $2p-2$, 知道有 $n(p-1) < m$; 又因爲它的第二個乘積的度數是 m, 於是知道 $f(\vec{x})$ 的度數是 m, 其中 $\prod_{e\in E(G)} x_e$ 這項的係數是 $(-1)^{m+1}$, 所以不等於 0。對於這項來說每個 d_e 都是 1, 所以若對所有 $e \in E$ 都取 $S_e = \{0,1\}$, 則根據組合零點定理, 存在某個 $\vec{a} = (a_e : e \in E(G)) \in \prod_{e\in E(G)} S_e$ 使得 $f(\vec{a}) \neq 0$。

這時候, 根據各個 a_e 是 0 或 1, 可以決定出 G 的一個子重圖 H, 其中 $e \in E(H)$ 若且唯若 $a_e = 1$。這個子重圖 H 至少有一條邊, 因爲 $f(\vec{0}) = 0$。既然 H 有邊, 那麼在 $f(\vec{a})$ 的定義當中第二個乘積就會是 0。這時候, 如果對於某個 v 來說 $\sum_{e\ni v} a_e$ 在 $\mathbb{Z}_p$ 當中不是 0, 那麼根據 Fermat 小定理就有

$$1 - \Big(\sum_{e\ni v} a_e\Big)^{p-1} \equiv 0 \pmod{p},$$

所以 $f(\vec{a})$ 的定義當中的第一個乘積也是 0, 這跟 $f(\vec{a}) \neq 0$ 矛盾; 這就表示對於每個點 v 來說都要有 $\deg_H(v) = \sum_{e\ni v} a_e \equiv 0 \pmod{p}$, 但問題是 $\Delta(G) = 2p-1$, 所以 $\deg_H(v)$ 若不是 0 就是恰好等於 p, 所以 H 去掉那些孤立點以後就是 G 的一個 p-正則子重圖。 □

和 *d*-點團集相交的集合的數目

下面是組合零點定理的另一個應用, 其內容看起來有一點不自然, 但展示了組合零點定理的多功能性。

定理 3.2. 如果 p 是質數, 而 $G = (V, E)$ 的點數 $|V| > d(p-1)$, 則存在一個非空的點集 $U \subseteq V$, 使得和 U 相交的 d-點團的數目是 p 的倍數。

證明: 每一個點 v 定義一個變數 x_v, 然後考慮在有限體 $\mathbb{Z}_p$ 上的多項式

$$f(\vec{x}) = \prod_{v\in V}(1-x_v) - 1 + g(\vec{x})^{p-1}, \text{ 其中 } g(\vec{x}) = \sum_{\emptyset\neq I\subseteq V} (-1)^{|I|+1} K(I) \prod_{v\in I} x_v,$$

[1] 其實他們證明了這個結論對於 p 是質數次方的情況也是對的, 但這裡只證明比較簡單的, 當 p 是質數的情況。另外, 這個定理是不是對於任何自然數 p 都成立, 是一個還沒有被解決的問題。

$K(I)$ 表示包含 I 的 d-點團的數目。因爲只有在 $|I| \le d$ 的時候 $K(I) \neq 0$, 所以 $g(\vec{x})$ 的次數最多是 d; 又因爲 $|V| > d(p-1)$, 所以 $f(\vec{x})$ 的次數是 $|V|$, 其中 $\prod_{v\in V} x_v$ 這項的係數是 $(-1)^{|V|}$, 所以不等於 0。對於這項來說每個 d_v 都是 1, 所以如果對所有 $v \in V$ 都取 $S_v = \{0,1\}$, 則根據組合零點定理, 存在某個 $\vec{a} = (a_v : v \in V) \in \prod_{v\in V} S_v$ 使得 $f(\vec{a}) \neq 0$。

令 $U = \{v \in V : a_v = 1\}$, 因爲 $f(\vec{0}) = 0$, 所以 $U \neq \emptyset$。既然 $U \neq \emptyset$, 那麼在 $f(\vec{a})$ 的定義當中第一個乘積就會是 0。這時候, $g(\vec{a})^{p-1} \neq 1$, 那麼根據 Fermat 小定理就有 $g(\vec{a}) = 0 \in \mathbb{Z}_p$, 因爲 $\prod_{v\in I} a_v$ 只有在 $I \subseteq U$ 的時候不是 0, 其實等於 1, 所以 $g(\vec{a}) = \sum_{\emptyset\neq I\subseteq U}(-1)^{|I|+1}K(I)$, 根據排容原理, 這就是和 U 相交的 d-點團的個數, 在 $\mathbb{Z}_p$ 是 0, 當作整數是 p 的倍數。 □

上面這個結果也可以推廣到 p 是某個質數的次方的情況, 一些相關的結果請參見 [2, 8]。

圖著色問題

圖的著色問題可追溯到 1850 年英國有一位學生 Francis Guthrie 提出來的四色問題。這個問題經過一百多年, 最後才在 1976 年, 由 Appel, Haken 與 Koch [6, 7] 藉著電腦的幫助, 透過放電論證法 (discharging method), 證明成爲四色定理, 他們的證明後來被 Robertson, Sanders, Seymour 與 Thomas [25] 簡化, 不過還是不能避免利用到電腦來證明。

四色問題可以說是圖論當中, 除了七橋問題以外最有名的問題, 其所衍生出來的許多著色問題, 引發了許多精彩的理論。著色問題除了歷史性的挑戰以外, 在現今的許多實際應用問題如: 排時、排序、時間表、頻道分配、資源分配、實驗設計等議題上都十分有用。圖著色與圖論的其他部分、數學的其他分支, 甚至其他科學也有很深而不可分離的關係。一百多年來的發展, 已經產生了許多深刻的結果與工具, 並且造就了許多具挑戰性的未解問題。

一個圖 G 的 k-著色 (k-coloring) 是指一個函數 $f : V(G) \to \{1, 2, \ldots, k\}$, 而一個正常 k-著色 (proper k-coloring) 則是指使得 $f(x) \neq f(y)$ 對相鄰兩點 x 和 y 都成立的 k-著色。圖 G 的著色數 (chromatic number)$\chi(G)$ 是指使得 G 存在正常 k-著色的最小 k。如果 $\chi(G) \le k$, 也會說 G 可以被 k-著色 (k-colorable)。在這個定義之下, 四色定理的內容就是「任意平面圖 G 都可以被四著色」。

列表著色是點著色的一種推廣, 在這種著色方式當中仍舊是要給每一點著上一種顏色, 不過每個點各自可以使用的顏色集合可能各不相同, 有別於先前的著色模式中每個點可用的顏色集合都是 $\{1, 2, \ldots, k\}$。這種著色概念由 Vizing [28] 及 Erdős、Rubin 與 Taylor [17] 獨立介紹出來。

對於圖 G 中的每一點 v, 令 $L(v)$ 是可供 v 選擇的顏色集。一個正常列表著色 (proper list coloring)f 是使得每一點 v 都有 $f(v) \in L(v)$ 的正常著色。如果無論 $L(v)$ 如何給定, 只要 $|L(v)| \ge k$ 的話 G 都有正常列表著色, 就說 G 可被列表 k-著色 (list k-colorable) 或

k-可選擇的 (k-choosable), 而 G 的列表著色數 (list chromatic number 或 choice number 或 choosability) $\chi_\ell(G)$ 就是使 G 可被列表 k-著色的最小 k。

Alon [1] 利用組合零點定理證明 Alon 和 Tarsi [5] 的一個結果。

對於有 n 個點的圖 $G=(V,E)$, 不妨假設 $V=\{1,2,\ldots,n\}$, 點 i 對應到變數 x_i, 考慮 n 個變數的 $|E|$ 次多項式

$$f_G(x_1,x_2,\ldots,x_n)=\prod\{(x_i-x_j):i<j,\{i,j\}\in E\}。$$

說一個有向圖 D 是一個循環 (circulation), 如果 $\deg_D^+(v)=\deg_D^-(v)$ 對於每個點 v 都成立的話。一個循環的奇偶性是根據它邊數的奇偶性來界定的。用 $\mathrm{CE}(D)$ 和 $\mathrm{CO}(D)$ 分別表示, 有向圖 D 的子圖是偶循環和奇循環的集合。

定理 3.3 (**Alon-Tarsi [5]**)**.** 令 $D=(V,E)$ 是點集 $V=\{1,2,\ldots,n\}$ 的圖 G 的一個定向, 它滿足 $|\mathrm{CE}(D)|\neq|\mathrm{CO}(D)|$。如果 $g:V\to\mathbb{Z}$ 定義成 $g(i)=d_i+1$, 其中 $d_i=\deg_D^+(i)$, 則 G 是 g-可選擇的。

證明: 對 $1\le i\le n$, 令 $S_i\subseteq\mathbb{Z}$ 含 d_i+1 個整數, 要由 S_i 中取一個顏色 a_i 著點 i 構成 G 的著色, 等同於要滿足 $f_G(a_1,a_2,\ldots,a_n)\neq 0$。因爲 $f_G(x_1,x_2,\ldots,x_n)$ 的度數是 $\sum_{i=1}^n d_i$, 由組合零點定理, 只要驗證 $\prod_{i=1}^n x_i^{d_i}$ 在 f_G 的係數不是 0 就可以。

把 $f_G(x_1,x_2,\ldots,x_n)$ 的 $|E|$ 個相乘項 x_i-x_j 展開, 得到 $2^{|E|}$ 項 $(-1)^r\prod_{i=1}^n x_i^{d'_i}$, 這種單項多項式對應到 G 的一個定向 D': 從 $|E|-r$ 項 x_i-x_j 中取 x_i 相乘、這對應到有向邊 ij, 從 r 項 x_i-x_j 中取 $-x_j$ 相乘, 這對應到有向邊 ji。這時候, 對所有 i 會有 $d'_i=\deg_{D'}^+(i)$。用 $\mathrm{DE}(d'_1,d'_2,\ldots,d'_n)$ 和 $\mathrm{DO}(d'_1,d'_2,\ldots,d'_n)$ 分別表示 G 的定向 D' 出度序列是 $d'_1,d'_2,\ldots,d'_n$ 而 r (也就是 $j>i$ 的邊 ji 的個數) 是偶數和奇數的集合, 則

$$f_G(x_1,x_2,\ldots,x_n)=\sum_{d'_1,d'_2,\ldots,d'_n\ge 0}\left(|\mathrm{DE}(d'_1,d'_2,\ldots,d'_n)|-|\mathrm{DO}(d'_1,d'_2,\ldots,d'_n)|\right)\prod_{i=1}^n x_i^{d'_i}。$$

對給定的 D, 它的度序列是 $d_1,d_2,\ldots,d_n$。對任意 $D'\in\mathrm{DE}(d_1,d_2,\ldots,d_n)\cup\mathrm{DO}(d_1,d_2,\ldots,d_n)$, 考慮 D 中在 D' 中是反向的所有邊的集合所構成的有向圖 D''。因爲 D 和 D' 有相同的出度序列, 所以 D'' 是 D 的循環子圖。對應 $D'\longrightarrow D''$ 顯然是 $\mathrm{DE}(d_1,d_2,\ldots,d_n)\cup\mathrm{DO}(d_1,d_2,\ldots,d_n)$ 到 $\mathrm{CE}(D)\cup\mathrm{CO}(D)$ 的 1-1 映成函數, 而且當 $D\in\mathrm{DE}(d_1,d_2,\ldots,d_n)$ 的時候 $D'\in\mathrm{DE}(d_1,d_2,\ldots,d_n)$ 若且唯若 $D''\in\mathrm{CE}(D)$, 當 $D\in\mathrm{DO}(d_1,d_2,\ldots,d_n)$ 的時候 $D'\in\mathrm{DE}(d_1,d_2,\ldots,d_n)$ 若且唯若 $D''\in\mathrm{CO}(D)$, 所以

$$\left||\mathrm{DE}(d_1,d_2,\ldots,d_n)|-|\mathrm{DO}(d_1,d_2,\ldots,d_n)|\right|=\left||\mathrm{CE}(D)|-|\mathrm{CO}(D)|\right|,$$

由於 $|\mathrm{CE}(D)|\neq|\mathrm{CO}(D)|$, 得知 $|\mathrm{DE}(d_1,d_2,\ldots,d_n)|-|\mathrm{DO}(d_1,d_2,\ldots,d_n)|\neq 0$, 也就是 $\prod_{i=1}^n x_i^{d_i}$ 在 f_G 的係數不是 0。 □

最後來討論這個定理的一個有趣的應用。堵丁柱、許得標、黃光明 [16] 曾考慮下面的問題, 一個有 $3n$ 點的圖 G 有 Hamilton 圈, 它的點任意分成 n 組, 每組 3 點、連成一個三角形。這是一個 4-正則圖, 滿足

$$3n/\chi(G) \le \alpha(G) \le \theta(G) = n \text{ 以及 } 3 = \omega(G) \le \chi(G)。$$

堵-許-黃 猜想 $\alpha(G) = n$, Erdős 把它加強猜想 $\chi(G) = 3$。利用前面的定理, Fleischner 和 Stiebitz [19] 證明 G 是 3-可選擇的。

其他一些相關結果亦請參見 [1]。

參考文獻

1. N. Alon, Combinatorial Nullstellensatz, *Combin. Probab. Comput.*, 8 (1999), 7-29.
2. N. Alon and Y. Caro, On three zero-sum Ramsey-type problems, *J. Graph Theory*, 17 (1993), 177-192.
3. N. Alon, S. Friedland and G. Kalai, Regular subgraphs of almost regular graphs, *J. Combin. Theory, Ser. B*, 37 (1984), 79-91.
4. N. Alon, S. Friedland and G. Kalai, Every 4-regular graph plus an edge contains a 3-regular subgraph, *J. Combin. Theory, Ser. B*, 37 (1984), 92-93.
5. N. Alon and M. Tarsi, Colorings and orientations of graphs, *Combinatorica*, 12 (1992), 125-134.
6. K. Appel, W. Haken, Every planar map is four colorable, I: discharging, *Illinois J. Math.*, 21 (1977), 429-490.
7. K. Appel, W. Haken and J. Koch, Every planar map is four colorable, II: reducibility, *Illinois J. Math.*, 21 (1977): 491-567.
8. N. Alon, D. Kleitman, R. Lipton, R. Meshulam, M. Rabin and J. Spencer, Set systems with no union of cardinality 0 modulo m, *Graphs Combin.*, 7 (1991), 97-99.
9. N. Alon, M. B. Nathanson and I. Z. Ruzsa, Adding distinct congruence classes modulo a prime, *Amer. Math. Monthly*, 102 (1995), 250-255.
10. N. Alon, M. B. Nathanson and I. Z. Ruzsa, The polynomial method and restricted sums of congruence classes, *J. Number Theory*, 56 (1996), 404-417.
11. N. L. Biggs, E. K. Lloyd and R. J. Wilson, *Graph Theory* 1736-1936, Clarendon Press, Oxford, 1998.
12. J. A. Bondy and U. S. R. Murty, *Graph Theory with Applications*, American Elsevier, New York, 1976.
13. 張鎮華。《演算法觀點的圖論》。臺大出版中心, 2017。
14. 張鎮華、蔡牧村。《演算法觀點的圖論》, 修訂版。臺大出版中心, 2020。
15. J. A. Dias da Silva and Y. O. Hamidoune, Cyclic spaces for Grassmann derivatives and additive theory, *Bull. London Math. Soc.*, 26 (1994), 140-146.
16. D. Z. Du, D. F. Hsu and F. K. Hwang, The Hamiltonian property of consecutive-d digraphs, *Math. Comput. Modelling*, 17 (1993), 61-63.
17. P. Erdős, A. L. Rubin and H. Taylor, Choosability in graphs, *Proc. West Coast Conf.*

Combin., Graph Theory and Comput., Arcata, Congr. Num., 26 (1979), 125-157.
18. L. Euler, Soluto problematics ad geometriam situs pertinentis, *Commentaii Academiae Scientiarum Impericalis Petropolictanae*, 8 (1736), 128-140.
19. H. Fleischner and M. Stiebitz, A solution to a coloring problem of P. Erdős, *Discrete Math.* 101 (1992), 39-48.
20. D. Kőnig, *Theory of Finite and Infinite Graphs*, translated by R. Mcloart with commentary by W. T. Tutte, Birkhäuser, Boston, 1990. (Originally published as *Theorie der Endlichen und Unendlichen Graphen*, Akademische Verlagsgesellschaft Leipzig 1936. German Edition 1986.)
21. M. Lasoń, A generalization of Combinatorial Nullstellenstaz, *Elec. J. Combin.*, 17 (2010), N32.
22. M. Michalek, A short proof of Combinatorial Nullstellenstaz, *Amer. Math. Monthly*, 117 (2010), 821-823.
23. M. B. Nathanson, *Additive Number Theory: The Classical Bases*, Graduate Texts in Math. 164, Springer-Verlag, 1996.
24. M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Graduate Texts in Math. 165, Springer-Verlag, 1996.
25. N. Robertson, D. Sanders, P. Seymour and R. Thomas, The four-colour theorem, *J. Combin. Theory, Ser. B*, 70 (1997), 2-44.
26. T. Tao and V. Vu, *Additive Combinatorics*, Cambridge University Press, Cambridge, 2006.
27. V. A. Taśkinov, Regular subgraphs of regular graphs, *Soviet Math. Dokl.*, 26 (1982), 37-38.
28. V. G. Vizing, Vertex colorings with given colors (in Russian), *Metody Diskret. Analiz.*, 29 (1976), 3-10.
29. B. L. van der Waerden, *Modern Algebra*, Julius Springer, Berlin, 1931.

—本文作者任台灣大學數學系, 名譽教授—