

積木結構的計算複雜性理論

王則柯

1981 年的《美國數學會通報》(Bull. AMS) 上, 發表了伯克利加州大學教授斯梅爾 (S. Smale) 的論文「代數基本定理與計算複雜性理論」, 討論用牛頓方法計算多項式零點的計算複雜性問題。斯梅爾的結果可以有條件地簡述為: 用牛頓方法為任一 n 階複係數多項式找到一個零點的成本 (以牛頓疊代次數衡量), 隨著多項式階數 n 的增長而增長的速率不超過 n^9/μ^7 , 這裡 μ 是允許論斷失敗的概率, $0 < \mu < 1$ 。

兩年以後, 1983 年 4 月, 筆者應斯梅爾教授的邀請, 在伯克利加州大學報告了下述結果: 用庫恩 (Kuhn) 方法算出任一 n 階複係數多項式一個零點的成本 (以多項式計值次數衡量), 隨著多項式階數 n 的增長而增長的速率不超過 $n^2 \log(n/\varepsilon)$, 這裡 $\varepsilon > 0$ 是零點數值計算的精度要求。

數值計算方法的計算複雜性問題, 是應用數學當今令人矚目的發展。本文以斯梅爾的論文和我們的 $n^2 \log(n/\varepsilon)$ 的工作為主, 介紹計算複雜性討論的若干進展。

代數基本定理與計算複雜性問題

大家知道, 形如 $f(z) = C_n z^n + C_{n-1} z^{n-1} + \dots + C_1 z + C_0$ 的函數, 稱為 n

階複係數多項式, 這裡 n 是自然數, z 是複變量, C_0, \dots, C_n 都是複常數, 並且 $C_n \neq 0$ 。如果一個複數 ξ 使得用 $z = \xi$ 代入這個多項式後多項式的值為 0, 即 $f(\xi) = 0$, 就說 $z = \xi$ 是多項 $f(z)$ 的一個零點, 或一個根。

在尋求零點或計算零點的時後, 我們可以先用 $C_n \neq 0$ 除整個多項式, 所得的多項式 $g(z) = z^n + (C_{n-1}/C_n)z^{n-1} + \dots + (C_1/C_n)z + (C_0/C_n)$ 的零點與原來多項式 $f(z)$ 的零點一致。因此, 今後我們只討論形如

$$f(z) = z^n + a_{n-1}z^{n-1} + \dots + a_1z + a_0$$

的所謂首一多項式 (monic polynomial), 其中 z 是複變量, a_0, \dots, a_{n-1} 都是複常數。自然數 n 仍是多項式的階。

代數基本定理說, 任一 n 階複係數多項式必有一個複零點。或者採用更強的形式: 任一 n 階複係數多項式, 正好有 n 個複零點。數學史上有一些經典的論題, 它們雖然已經被解決, 卻仍然一再喚起人們的熱情, 去從事溫故而創新的工作。代數基本定理就是這樣一個論題。大家知道, 天才的德國數學家高斯, 從 1799 年到 1850 年前後相距達半個世紀

的時間裡，曾經提出代數基本定理的四個證明。更早，還可以追溯到牛頓、麥克勞林、達朗貝爾、歐拉和拉格朗日。但是必須指出，即使是高斯的證明，在嚴格的意義上說來，也是有缺陷的。

近幾十年來，人們致力於代數基本定理的構造性的證明 (constructive proof)，取得了很大的成功。庫恩算法 (見本刊第17卷第3期「多項式方程求根的魔術植物栽培算法」) 就是一個例子。構造性是什麼意思呢？以判斷“有沒有零點”的所謂零點存在性問題為例，構造性的討論方法是：具體 (設計一種方法) 找出零點來，說明它是存在的。非構造性的討論方法則往往是“反證法”：假定零點不存在，然後引出與已知事實的矛盾。打個比方：面對3隻雛雞，閉著眼睛你也可以判斷其中至少有2隻是同性的，否則會與雞只有雌雄兩個性別的事實矛盾。這樣一個判斷過程就是非構造性的。倘若你是一個辨認雛雞性別的行家，實際辨認出其中有2只是雄的，並由此得出存在一對同性雛雞的結論，這樣一個判斷過程就是構造性的。反證法在邏輯上常常非常漂亮，但是帶給人們的信息較少。相反，構造性的工作雖然有時比較繁複，卻不但肯定了“存在”的事實，還指示怎樣把這個“存在”找出來。所以，隨著社會和科學的發展，各方面對數學的要求，越來越傾向於構造性的解決辦法。面對我們的多項式零點問題，構造性的工作就是要提出尋求或計算零點的一種方法或一種算法。

既然我們強調構造性工作的實際應用價值，那麼，算法的效率如何，就是一個十分重

要問題。如果有人提出一種算法，並且在數學上證明了按照這種算法一定可以找到問題的解，但是可能要在最新的電子計算機上花費 10^{10} 年的時間，你對這種樣子的算法，有什麼感覺呢？說不定會啼笑皆非。

時間就是成本。所以算法效率的討論，也就是計算成本的討論。一種算法，通常是對於某種類型的問題提出來的。問題的規模有大有小。問題的規模越大，解決問題的成本一般也越高。按照計算複雜性理論 (computational complexity theory)，如果計算成本隨著問題規模的增長而增長的關係是多項式的 (exponentially)，這種算法就被認為是實際上難以接受的。如果計算成本隨著問題規模的增長的關係是多項式的，這種算法將被認為是實際可行的，並被稱作多項式時間算法 (algorithm of polynomial time)。以當前世界上電子計算機對付得最多的線性規畫 (linear programming) 問題為例，單純形方法 (simplex method) 是一種人們樂於採用的方法。但是有人舉出例子，說明在最壞的情況下，單純形方法的計算成本是指數式增長的。1978年，蘇聯數學家哈奇安 (Khachian) 提出線性規劃問題的一種多項式時間算法，一時成為「紐約時報」的頭版新聞。不久，斯梅爾教授宣布，概率地說 (probabilistically)，即除去一部分最壞的和很壞的情形以外，單純形方法的計算成本隨問題規模增長而增長的關係是線性的。大家知道，線性關係，是最好的一類多項式關係。又過了不久，旅美印度數學家卡馬卡 (Karmarkar) 提出在許多情況下會比單純形方法優越的內

點算法。這些都是計算複雜性理論方面令人驚嘆的進展。

牛頓方法與逼近零點

牛頓方法 (Newton method) 是一種廣泛使用的零點計算方法。對於複平面上函數 $f(z)$ 的零點計算問題, 牛頓方法可以很簡單地表述為: 在複數平面上取定一點 z_0 , 歸納地定義

$$z_{k+1} = z_k - f(z_k)/f'(z_k), k = 0, 1, 2, \dots$$

每算一個 z_{k+1} , 就叫做一次牛頓疊代 (Newton iteration), 而原來的 z_0 , 叫做牛頓方法的初值。

面對零點的數值計算, 人們常常首先想到是否可以用牛頓方法, 這至少有兩個原因: 第一, 牛頓方法已經有三百年的歷史, 似已在數學家 and 數值計算專家的頭腦中生根。人們對牛頓方法有過大量研究, 雖然情況至今未能說完全令人滿意。人們在使用牛頓方法方面積累了豐富經驗, 雖然失敗還是常常會發生。第二, 牛頓方法的表述特別簡單, 入門也就顯得特別容易。只要懂得一點一元函數微分學的概念, 一個從未接觸過牛頓方法的人, 也可以馬上用牛頓方法取得他的第一批計算結果。

牛頓方法的表述固然簡單, 但它的計算收斂性 (convergence) 討論卻相當麻煩。例如, 算到某一步, 得到的 z_k 使 $f'(z_k) = 0$, 疊代就做不下去了。至於初值 z_0 的選取, 更是一個嚴重的問題。初值選得好, 計算就收斂得快。初值選得不好, 收斂就慢, 甚至根本不

收斂。所以, 牛頓方法又是一種難以把握的方法。

重要的是找到一個足夠好的初值。什麼叫足夠好的初值? 斯梅爾提出了逼近零點 (approximate zero) 的概念: 如果 z_0 使得牛頓疊代對所有 $k = 0, 1, 2, \dots$, 都有意義, z_0, z_1, z_2, \dots 收斂到 $f(z)$ 的一個零點, 並且對所有 k 都成立 $|f(z_{k+1})/f(z_k)| < 1/2$, 就稱 z_0 是 $f(z)$ 的一個逼近零點。換言之, 逼近零點的意思是, 從這點開始牛頓疊代收斂到函數的一個零點, 並且每次疊代使函數值的絕對值衰減一半以上。可見, 逼近零點真是比較好的初值。當用牛頓方法進行零點計算的時候, 一旦找到了逼近零點, 剩下的工作就不多了。

概念明確了, 接下去就要確立達到逼近零點的條件, 並設計首先把逼近零點找到的方法。

拿多項式來說, 使得多項式 $f(z)$ 的導函數 $f'(z)$ 的值為零的點, 稱作多項式的臨界點 (critical point), 這點的多項式值, 稱作多項式的臨界值 (critical value)。把 n 階多項式的所有 $n - 1$ 個臨界值的絕對值按大小排列起來, 取最小的一個, 記作 $\rho = \rho(f)$, 不妨稱作多項式 $f(z)$ 的表徵值。運用單複變函數中與比勃巴赫-德布蘭傑 (Bieberbach-De Branges) 定理有關的結果, 斯梅爾證明了:

如果 $|f(z_0)| < \rho(f)/13$, z_0 就是多項式 $f(z)$ 的一個逼近零點。

這就給出了判別逼近零點的一個充分條件。這個條件要能起作用, 必須 $\rho(f) > 0$ 。

根據 $\rho(f)$ 的定義, $\rho(f) > 0$ 是多項式沒有重零點 (重根) 的特徵。另一方面, 如果某點多項式值為 0, 這點就已經是多項式的零點了。對於一個沒有重零點的多項式 $f(z)$, 從複數 z 到複數 w 平面的變換 $w = f(z)$, 在每個零點附近都是近似線性的。所以 w 平面上由 $|w| < \rho(f)/13$ 確定的圓域的原像, 是 z 平面上以多項式 $f(z)$ 的 n 個零點為中心的 n 個小的近似圓域。由此可見, 斯梅爾的充分條件, 是在 z 平面上確定以多項式零點為中心的 n 個近似圓形的快速收斂區, 見圖 1。一旦進入了快速收斂區, 牛頓方法的收斂速度就會很快。



圖 1. 快速收斂區

斯梅爾的主要結果

現在考慮如何具體把逼近零點找出來。

設想把牛頓疊代的步長適當縮小, 變得精細一些, 可望有所幫助。斯梅爾在牛頓疊代公式中引入一個步長參數 $h, 0 < h \leq 1$ 。從複平面的一點 $z(0)$ 開始, 歸納地定義

$$z(k+1) = z(k) - h \cdot \frac{f(z(k))}{f'(z(k))}, k = 0, 1, 2, \dots$$

希望因為適當選取步長參數 h , 經過從 $z(0)$ 開始的若干步參數 h 的牛頓疊代, 可以到達多項式的一個逼近零點。

這樣一來, $z(0)$ 又是一種初始點。 $z(0)$ 選得好, 可以較快找到逼近零點, 即可以較快

進入快速收斂區。 $z(0)$ 選得不好, 說不定一直找不到逼近零點。怎樣表徵初始點 $z(0)$ 與多項式 $f(z)$ 的關係的好壞呢? 斯梅爾引進參數 \mathcal{K} , 在個別次要的技術限制之下, 定義 \mathcal{K} 為各個臨界值與初始點多項式值 $f(z(0))$ 之比的幅角的最小絕對值。這個 \mathcal{K} 當然是同時依賴於 $f(z)$ 和 $z(0)$ 的, 即 $\mathcal{K} = \mathcal{K}(f, z(0))$ 。我們將要知道, 如果 $\rho(f)$ 和 $\mathcal{K}(f, z(0))$ 都大於 0, 初始點 $z(0)$ 對於多項式 $f(z)$ 來說, 就是不錯的。事實上, 斯梅爾在進一步引進參數 $\zeta = \zeta(f, z(0)) = 13|f(z(0))|/\rho(f)$ 之後, 證明了

定理: 若多項式 $f(z)$ 和初始點 $z(0)$ 符合 $\rho(f) > 0$ 和 $\mathcal{K}(f, z(0)) > 0$ 的條件, 則取

$$h = \frac{\sin(\mathcal{K}/2)}{4(3 \sin(\mathcal{K}/2) + \log \zeta)},$$

從 $z(0)$ 開始的以 h 為步長參數的參數牛頓疊代都有意義, 並且在

$$s = 4\left(3 + \frac{\log \zeta}{\sin(\mathcal{K}/2)}\right)^2$$

步之內到達多項式 $f(z)$ 的一個逼近零點。

面對一個業已確定的多項式, 可以討論某個初始點取得好還是不好。反過來, 面對一個業已固定的初始點, 可以討論某個多項式 (與這個給定的初始點匹配得) 好還是不好。上面講過, 我們只須討論首一式多項式。一個形如 $f(z) = z^n + a_{n-1}z^{n-1} + \dots + a_1z + a_0$ 的首一多項式被 n 個複常數 a_0, a_1, \dots, a_{n-1} 完全確定。反過來也一樣。因此我們可以把由所有 n 階首一多項式組成的空間, 與複 n 維歐氏空間 C^n 等同看

待, 稱為 n 階複係數多項式空間 (space of monic polynomials of degree n)。斯梅爾取定 $z(0) = 0$, 即老是以原點為初始點, 然後利用代數幾何和積分幾何的知識, 給對於這個初始點來說是最壞的和較壞的多項式, 在整個多項式空間中所佔的體積作一個估計。全空間的體積無窮, 比較難以把握。但是由 $|a_0| < R, |a_1| < R, \dots, |a_{n-1}| < R$ 所確定的複 n 維圓柱 $P(R)$ 的體積是一個有限數 $(\pi R^2)^n$, 就容易把握得多。這個 n 維圓柱由所有係數的絕對值都小於 R 的一切多項式組成。把最壞的和較壞的多項式從所考慮的空間 (複 n 維圓柱) 中挖去。最壞的當然要挖去。較壞的多項式挖去越多, 剩下的多項式就越好, 這樣從 $z(0) = 0$ 開始的參數牛頓疊代就可以越快進入快速收斂區, 即可以越快到達一個逼近零點 (圖 2)。若挖去部分的體積與全空間 (複 n 維圓柱) 的體積之比為 $\mu, 0 < \mu < 1$, 那麼如果對剩餘的部分得到一個一致的結論 \mathcal{A} , 我們也可以說結論 \mathcal{A} 對空間中任一多項式成立的概率 (probability) 為 $1 - \mu$ 。正是這樣的考慮, 引導斯梅爾得到他的主要結果:

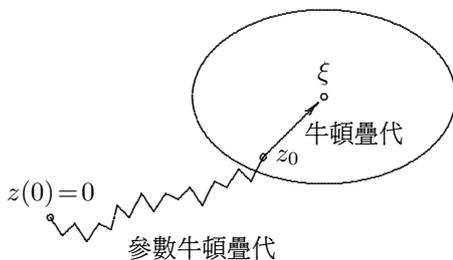


圖 2. 斯梅爾方案

定理: 給定 n 及 $0 < \mu < 1$ 。取

$\sigma = (\mu/150)^{3/2}/(n+2)^2$ 。對複 n 維圓柱 $P(R)$ 中的任一多項式 $f(z)$, 以下事實成立的概率至少是 $1 - \mu$: 只要適當選取步長參數 h , 就可以保證從 $z(0)$ 開始的參數牛頓疊代在

$$s = 4 \left(3 + \frac{\log(15/\sigma)8R}{\sigma^2} \right)^2$$

步之內達到 $f(z)$ 的一個逼近零點。

定理中的 s 的表達式頗為複雜。對 $R = 1$ 情況作耐心的換算, 可以得到 $s = (100(n+2))^9/\mu^7$ 的結果, 即: 給定 n 和 $0 < \mu < 1$, 對於係數 a_0, a_1, \dots, a_{n-1} 的絕對值小於 1 的 n 階首一多項式, 從 $z(0) = 0$ 開始的步長適當的參數牛頓疊代在 $s = (100(n+2))^9/\mu^7$ 步內進入多項式的快速收斂區的概率至少是 $1 - \mu$ 。這就是本文開始時以簡要形式介紹的斯梅爾的結果。

斯梅爾曾因微分拓樸學方面證明高維的邦加萊猜測而在 1966 年獲得國際數學界的最高榮譽菲爾茲獎。隨後, 他和其他學者一起開創動力系統 (dynamical systems) 的研究。近年來, 他從微分拓樸和動力系統的高度, 最初是基於數理經濟學 (mathematical economics) 問題的背景, 致力於計算方法和計算複雜性理論的研究, 連續發表了一系列引起純粹數學界、應用數學界和數理經濟學界注意的論文。上述「代數基本定理與複雜性理論」, 是其中很有份量的一篇。

庫恩多項式零點算法

庫恩多項式零點算法, 只有二十年的歷史。鑒於本刊十七卷三期已有詳盡介紹, 現在

我們只作簡單的複述。算法的敘述，由以下三部分組成：

1. 半空間 $C[-1, +\infty)$ 的一種單純剖分

記 C 為複數平面, $C_k = C \times \{k\}$, $k = -1, 0, 1, 2, \dots$ 。記 $z = x + iy$, 而 \mathbb{Z} 為整數集。用四族平行直線

$$\{z \in C : x = p, p \in \mathbb{Z}\}$$

$$\{z \in C : y = p, p \in \mathbb{Z}\}$$

和 $\{z \in C : y = (2p + 1) \pm x, p \in \mathbb{Z}\}$

分割 C_{-1} 平面, 而對 $k = 0, 1, 2, \dots$, 用四族平行直線

$$\{z \in C : x = 2^{-k}p, p \in \mathbb{Z}\}$$

$$\{z \in C : y = 2^{-k}p, p \in \mathbb{Z}\}$$

和 $\{z \in C : y = 2^{1-k}p \pm x, p \in \mathbb{Z}\}$

分割 C_k 平面。在這個基礎上, 將每兩層平面之間的空間, 分割成一個個四面體。

C_{-1} 的方格和 C_0 的方格上下相對, 它們所界定的方塊被分成 5 個四面體。對於 $k = 0, 1, 2, \dots, C_k$ 的一個方格和 C_{k+1} 的 4 個方格上下相對, 它們所界定的方塊被分成 14 個四面體。這些方塊將稱為基本方體。

2. 整數標號法

對於 $k = 0, 1, 2, \dots, C_k$ 上的格點 z 的整數標號 $l(z)$ 由

$$l(z) = \begin{cases} 1, & \text{若 } f(z) = 0 \text{ 或} \\ & -\frac{\pi}{3} \leq \arg f(z) \leq \frac{\pi}{3}, \\ 2, & \text{若 } \frac{\pi}{3} < \arg f(z) \leq \pi, \\ 3, & \text{若 } -\pi < \arg f(z) < -\pi/3, \end{cases}$$

確定, 這裡, 非 0 複數幅角取值範圍規定為 $(-\pi, \pi]$ 。對於 C_{-1} 上的格點, 用 z^n 代替 $f(z)$ 按上式標號。

3. 同標號頂替算法

取 m 為不小於 $3(1 + \sqrt{2})n/4\pi$ 的最小整數。在 C_{-1} 平面上以原點為中心的邊長 $2m$ 的方塊 Q_n 的邊 ∂Q 上, 按照逆時針方向, 正好有 n 條稜其端點標號由 1 到 2。從這 n 條 (1,2) 稜出發, 向方塊 Q_n 裡面走, 按照遇到 (1,2) 稜就穿過去的規則, 可以找到 n 個頂點標號為 (1,2,3) 的完全標號三角形。

從 C_{-1} 上這 n 個完全標號三角形出發, 計算同處於四面體的第四個頂點的標號, 算出是什麼標號, 就用它頂替同標號的那個頂點。這樣計算下去, 就可以找到多項式 $f(z)$ 的全部 n 個零點。算法敘述可看本刊十七卷三期的圖, 那裡還給出證明大意。

如果說庫恩算法的敘述不像牛頓方法那麼簡單, 它的使用卻方便得多。不管需要計算零點的首一多項式是怎樣的, 只要把多項式的階數 n 和複係數組 a_0, a_1, \dots, a_{n-1} 以及零點計算的精度要求 ε 輸入機器, 算法就可以按照精度要求把多項式的 n 個零點逐一算出來。

積木結構的成本估計

算法效率的討論, 不是事後的計算成本核算, 而是在算題之前, 預先估計計算成本是多少。

牛頓方法的效率, 用所需的牛頓疊代的次數來衡量。庫恩算法的效率, 可以用所需的同標號頂替的次數衡量。每次頂替, 算一次

$f(z)$ 。因此，也可以說是用多項式 $f(z)$ 計值次數為尺度，討論庫恩算法的效率。這裡要注意，每次牛頓疊代，包含 $f(z)$ 和 $f'(z)$ 兩個多項式計值。

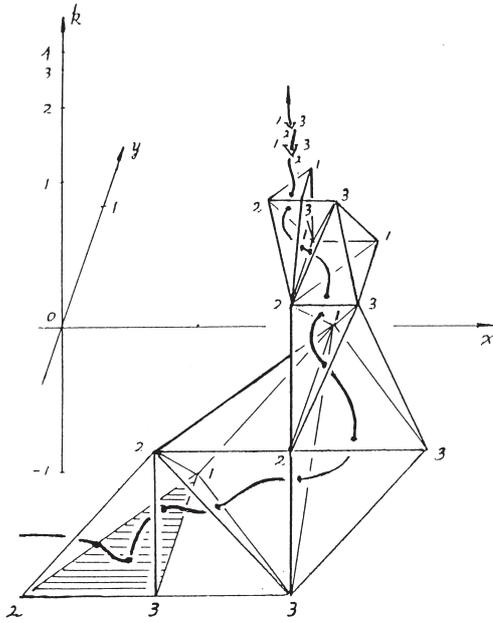


圖 3. 計算一個零點的四面體塔

從 ∂Q 的 (1,2) 稜開始的庫恩算法計算，在方塊 Q_n 內平面搜索到完全標號三角形後，就向“空中”發展，在四面體中穿行，每穿過一個四面體，就要計一次 $f(z)$ ，做一次同標號頂替。我們知道，每個四面體只允許計算路徑通過一次。所以，計算的進行，可以看作是四面體的不斷堆砌。(圖3) 如果是成本核算，那麼只要數一下這 n 座四面體體塔由多少四面體組成。但是現在要做的是成本估計，那麼可以先把計算可能走到的範圍確定下來，然後數一下在這個範圍之內，四面體的數目。這是成本討論的指導思想。

按照上述思想，庫恩證明了

引理 1. 記 $a = \max\{|a_0|, |a_1|, \dots, |a_{n-1}|\}$ ，記 $r = \max\{3\sqrt{2}(2+\pi)n/4\pi, 1+na/(n-1)\}$ ，再令 $R = r + \sqrt{2}$ ，那麼完全標號三角形和原點軸 $\{0\} \times [-1, +\infty)$ 的距離都小於 R 。

按照上述思想，我們證明了

引理 2: $k \geq 0$ 時， C_k 平面上完全標號三角形任一頂點與多項式某個零點的距離不超過

$$-\sqrt{2}(1 + 3n/4)/2^k.$$

因為計算經過的四面體都由兩個完全標號三角形張成，所以依照上述兩個引理，計算可能經過的四面體，全在一個半徑為 R 的底座圓台和 n 座圓台階梯 (可以相重) 之內，每一節圓台階梯的半徑是 $\sqrt{2}(1 + 3n/4)/2^k$ 。 n 座四面體塔都在這個由一個底座圓台和 n 座圓台階梯所組成的算法的可能區域內。

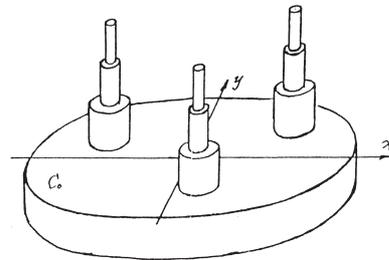


圖 4. 算法的可能區域

做到現在，剩下只須把算法可能區域中的四面體 (不管計算是否經過) 的數目算出來就可以了。

底座圓台的體積是 πR^2 ，頂多包含 πR^2 個 C_{-1} 和 C_0 之間的基本方體，而每個基本方體被分割成 5 個四面體，所以底座圓台所包含的四面體的數目不超過 $5\pi R^2$ 。

在 C_k 和 C_{k+1} 之間的一節階梯圓台的體積是 $\pi(\sqrt{2}(1+3n/4)2^{-k})^2$, 相應層次的基本方體的體積是 2^{-2k} , 而每個方體被分割成14個四面體, 所以每節圓台包含的四面體的數目是 $14\pi(\sqrt{2}(1+3n/4)2^{-k})^2/2^{-2k} = 28\pi(1+3n/4)^2$. 這裡 k 消失了, 是因為階梯圓台越少, 基本方體和四面體也越小, 比例完全一樣。

ε 是零點計算的精度要求, 那麼按照引理2, 記 $K = \lceil \log_2(\sqrt{2}(1+3n/4)/\varepsilon) \rceil$ 為不小於 $\log_2(\sqrt{2}(1+3n/4)/\varepsilon)$ 的最小整數, 知道圓台階梯在平面 C_k 截斷即可。這時算得的完全標號三角形的任一頂點與多項式的零點的距離在

$$\sqrt{2}(1+3n/4)/(\sqrt{2}(1+3n/4)/\varepsilon) = \varepsilon$$

之內, 已經達到精度要求。這樣, n 座高為 K 的圓台階梯所包含的四面體的數目不超過

$$n28\pi(1+3n/4)^2 \lceil \log_2(\sqrt{2}(1+3n/4)/\varepsilon) \rceil。$$

總結以上, 我們得到

定理: 用庫恩算法按精度要求 ε 算出 n 階首一多項式 $f(z)$ 全部 n 個零點所需要的多項式 $f(z)$ 計值次數不超過

$$\pi[5R^2 + 28n(1+3n/4)^2$$

$$\lceil \log_2(\sqrt{2}(1+3n/4)/\varepsilon) \rceil]。$$

如果問算出一個零點的平均成本, 那麼上式應當除以 n 。當 $R = 1$ 即 $|a_0|, |a_1|, \dots, |a_{n-1}|$ 都不超過1時, 上式可以換算成 $63(n+1)^2 \lceil \log_2(n/\varepsilon) \rceil$ 。這就是本文開頭說的 $n^2 \log(n/\varepsilon)$ 。

引理的初等證明

上述兩個引理的證明極其初等, 值得向非專門家介紹。首先, 注意複數的幅角關係, 畫圖就可證明:

命題: 規定複數幅角取值範圍為 $(-\pi, \pi]$ 。那麼, 若複數 w 符合 $|w| < 1$, 就必有 $|\arg(1+w)| \leq (\pi/2)|w|$ 。

引理1的證明: 因為三角形稜長不超過 $\sqrt{2}$, 所以有一頂點與原點距離超過 R 的三角形, 三頂點與原點的距離都要超過 r 。下面只須證明這樣的三角形不是完全標號三角形。我們不討論 $n = 1$ 的平凡情形。

頂點均可表成 (z, k) , k 是不小於 -1 的整數。設 $(z_1, k_1), (z_2, k_2)$ 是上述三角形的兩個頂點。若 $k_1, k_2 > -1$, 兩點都由 $w = f(z)$ 計算標號。改寫

$$f(z) = z^n(1 + \frac{a_{n-1}}{z} + \dots + \frac{a_1}{z^{n-1}} + \frac{a_0}{z^n}) = z^n(1 + g(z))。$$

因為 $|z_1| > r, |z_2| > r$, 就有

$$\begin{aligned} & |g(z_2)| \\ & \leq |a_{n-1}|/r + \dots + |a_1|/r^{n-1} + |a_0|/r^n \\ & \leq a(1/r + \dots + 1/r^{n-1} + 1/r^n) \\ & < a/(r-1) \leq (n-1)/n, \\ & |g(z_1) - g(z_2)| \\ & \leq |a_{n-1}| |1/z_1 - 1/z_2| + \dots \\ & \quad + |a_0| |1/z_1^n - 1/z_2^n| \\ & \leq a|z_1 - z_2|(1/r^2 + 2/r^3 + \dots + n/r^{n+1}) \\ & < \sqrt{2}a/(r-1)^2 \\ & \leq \sqrt{2}(n-1)/n(r-1) \\ & \leq \sqrt{2}(n-1)4\pi/3n\sqrt{2}(2+\pi)(n-1) \\ & = 4\pi/3(2+\pi)n, \end{aligned}$$

$$\begin{aligned} \left| \frac{g(z_1) - g(z_2)}{1 + g(z_2)} \right| &\leq \frac{4\pi}{3(2+\pi)n} / \left(1 - \frac{n-1}{n}\right) \\ &= \frac{4\pi}{3(2+\pi)} < 1. \end{aligned}$$

於是，記 $w_1 = f(z_1)$, $w_2 = f(z_2)$ ，由命題得

$$\begin{aligned} \left| \arg \frac{w_1}{w_2} \right| &= \left| \arg \frac{f(z_1)}{f(z_2)} \right| \\ &= \left| \arg \frac{z_1^n(1+g(z_1))}{z_2^n(1+g(z_2))} \right| \\ &\leq \left| \arg \frac{z_1^n}{z_2^n} \right| + \left| \arg \left(1 + \frac{g(z_1) - g(z_2)}{1 + g(z_2)}\right) \right| \\ &\leq n \left| \arg \frac{z_1}{z_2} \right| + \frac{\pi}{2} \left| \frac{g(z_1) - g(z_2)}{1 + g(z_2)} \right| \\ &\leq \frac{n\sqrt{2}}{3\sqrt{2}(2+\pi)n/4\pi} + \frac{\pi}{2} \cdot \frac{4\pi}{3(2+\pi)} = \frac{2\pi}{3}. \end{aligned}$$

當 k_1 和 k_2 有一個或兩個都是 -1 時，更容易得 $\left| \arg(w_1/w_2) \right| < 2\pi/3$ ，這是因為可以用 $w = z^n$ 代替 $w = f(z)$ 。

既然三頂點在 w 平面的像，兩兩之間對原點的張角小於 $2\pi/3$ ，那麼依標號法，三角形不是完全標號三角形。

引理 2 的證明：因為 C_k 平面上三角形任兩頂點的距離不超過 $\sqrt{2}/2^k$ ，我們只須證明完全標號三角形必有一頂點與多項式某零點的距離不超過 $3n\delta/4$ ，這裡 δ 就是等腰直角三角形的斜邊長， $\delta = \sqrt{2}/2^k$ 。

亦只討論 $n > 1$ 的情形。改寫

$$f(z) = (z - \xi_1) \cdot (z - \xi_2) \cdots (z - \xi_n),$$

這裡 $\xi_1, \xi_2, \dots, \xi_n$ 是由代數基本定理保證的 n 個零點。

設 C_k 平面上某三角形 $\{z_1, z_2, z_3\}$ 三頂點與多項式所有零點的距離都大於

$3n\pi/4$ ，那麼對 $j = 1, \dots, n$ ，有

$$\left| \frac{z_2 - z_1}{z_1 - \xi_j} \right| < \frac{\delta}{3n\pi/4} = \frac{4}{3n} < 1.$$

於是按照前述命題，記 $w_i = f(z_i)$ ， $i = 1, 2, 3$ ，就有

$$\begin{aligned} \left| \arg \frac{w_2}{w_1} \right| &= \left| \arg \frac{f(z_2)}{f(z_1)} \right| \\ &= \left| \arg \frac{(z_2 - \xi_1) \cdots (z_2 - \xi_n)}{(z_1 - \xi_1) \cdots (z_1 - \xi_n)} \right| \\ &\leq \left| \arg \frac{z_2 - \xi_1}{z_1 - \xi_1} \right| + \dots + \left| \arg \frac{z_2 - \xi_n}{z_1 - \xi_n} \right| \\ &= \left| \arg \left(1 + \frac{z_2 - z_1}{z_1 - \xi_1}\right) \right| + \dots \\ &\quad + \left| \arg \left(1 + \frac{z_2 - z_1}{z_1 - \xi_n}\right) \right| \\ &\leq \frac{\pi}{2} \left| \frac{z_2 - z_1}{z_1 - \xi_1} \right| + \dots + \frac{\pi}{2} \left| \frac{z_2 - z_1}{z_1 - \xi_n} \right| \\ &< n \frac{\pi}{2} \frac{4}{3n} = \frac{2\pi}{3}. \end{aligned}$$

同樣， $\left| \arg(f(z_3)/f(z_2)) \right| < 2\pi/3$ ，

$\left| \arg(f(z_1)/f(z_3)) \right| < 2\pi/3$ 。可見， $f(z_1)$ ， $f(z_2)$ ， $f(z_3)$ 在 w 平面上兩兩對原點的張角都小於 $2\pi/3$ ，所以 $\{z_1, z_2, z_3\}$ 不可能是完全標號三角形。

庫恩算法與逼近零點

斯梅爾關於牛頓方法的成本估計是 n^9/μ^7 ，我們關於庫恩算法的成本估計是 $n^2 \log(n/\varepsilon)$ 。美中不足的是參數不完全一致，分別為 n, μ 和 n, ε 。為使參數完全一致，我們令庫恩遷就牛頓，試用庫恩算法為多項式先尋找逼近零點，雖然逼近零點的概念對於庫恩算法原來並無意義，因為庫恩算法是任何情況下一定成功的算法。

逼近零點概念是為牛頓方法而建立的，只對沒有重零點的多項式有效。如果有重零點， $\rho(f) = 0$ ，那麼按照 $|f(z_0)| < \rho(f)/13$ 確定的快速收斂區根本不存在。因此，必須不顧 $\rho(f) = 0$ 和 $\rho(f)$ 太小的情形。對於剩下的 $\rho(f)$ 不太小的多項式，設有常數 $\rho_0 > 0$ 使得 $\rho(f) \geq \rho_0$ 總是成立。按照斯梅爾的充分條件， $|f(z_0)| < \rho(f)/13$ 就是逼近零點了。既然庫恩算法可以任意接近精確零點，何愁在一定時刻之後不會進入快速收斂區？按照這個想法進行從 μ 到 ε 的換算，可以由上述定理推出新的

定理：對於所有係數的絕對值均不超過 1 的 n 階首一多項式，以下事實成立的概率至少是 $1 - \mu$ ：利用庫恩算法，頂多經過

$$200(n+2)^3 \log_2(n/\mu)$$

次多項式計值，就可以為多項式找到一個牛頓算法所需要的良好初值。

現在， $n^3 \log(n/\mu)$ 和 n^9/μ^7 ，就是參數完全一致的比較了。但是，決不能因此而低估斯梅爾的工作的意義。我們討論的是具有良好拓樸幾何結構的庫恩算法，而斯梅爾對付的是難以駕馭的牛頓方法。牛頓方法在壞的情形連收斂性都談不上，更何況成本估計？斯梅爾巧妙地排除壞的和比較壞的情況，得出一個出色的概率估計。這是計算複雜性討論從傳統的最壞情形分析進入到嶄新的概率情形分析的開創性工作。

一定要說有什麼未臻人意的地方的話，那就是斯梅爾設計的用參數牛頓疊代尋找逼近零點的方法，在徹底的意義上不完全是構

造性的。問題在於參數 h 的選取。不錯，斯梅爾給出了 h 的表達式， h 可以由 ζ 和 \mathcal{K} 確定，但是 ζ 和 \mathcal{K} 又依賴於 $\rho(f)$ ，後者要算 $f(z)$ 的臨界值才知道，而 $f(z)$ 的臨界點就是 $f'(z)$ 的零點。這樣，為了構造性地解決尋找 $f(z)$ 零點問題，先要找出另一個多項式 $f'(z)$ 的零點。所以，這種構造性在邏輯上不徹底。

另一方面，對庫恩算法的成本估計，仍大有可以進一步精確化的餘地。在圖 4 的可能性區域內，計算真正走到的，只是很小一個部分。如何利用多項式的特性，進一步改善已有的結果，仍然值得努力。

庫恩算法的優點是保險成功，牛頓方法的長處則是進入快速收斂區後收斂很快。看來，兩種方法配合使用，有可能把二者的長處結合起來。事實上，採用庫恩算法先把零點的位置大致確定，然後改用牛頓方法迅速向精確零點靠近，這在理論分析和實際計算中都是很有希望的方案。

參考文獻

1. Kuhn, H. W., in: Fixed Points: Algorithms and Applications, (ed. Karamradian, S.), Academic Press, 1977, 11-40.
2. Smale, S., Fundamental Theorem of Algebra and Computational Complexity Theory, Bull. AMS, 4(1981), 1-36.
3. 王則柯，計算的複雜性，湖南教育出版社，1993
4. Wang Z. et al., Algebraic Systems and Computational Complexity Theory, Kluwer Acad. Publ., 1994.

—本文作者任教於中國廣州市中山大學數學所—