

用電腦證明組合恆等式

柳柏濂

1998年1月，在美國數學會 (AMS) 第104屆年會上，美國 Temple 大學的 D. Zeilberger 和 Pennsylvania 大學的 H. S. Wilf 共同獲得美國數學會的 Steele 重大貢獻獎。他們的獲獎論文是1990年刊登在「美國數學會雜誌」(J. Am. Math. Soc. 3卷147-158) 上的“有理函數確證組合恆等式”。(Rational functions certify combinatorial identities)。這篇簡短的論文，提供了一個證明組合恆等式的全新方法。從而，開闢了一個機器證明的新天地。

Zeilberger和 Wilf 的方法，被稱為 WZ 方法。要闡述 WZ 方法如何使組合恆等式的證明進入計算機的代數系統中，讓我們先從電腦證明恆等式談起。

一．舉例能代替證明嗎？

這不是一個小學生提出來的問題，而是一個數學家發出的挑戰性的詰問。

的確，從我們在初中開始學習平面幾何證明的那一刻起，數學老師就把那金科玉律般的警句灌入我們的腦中：“舉例不能代替邏輯證明！”

1986年，數學家 and 計算機科學家洪加威先生就在「中國科學」的一篇文章 ([2]) 中，向那種傳統的觀念挑戰，他的論文題目便是：“能用例證來證明幾何定理嗎？”。

計算機的誕生，計算機科學的發展，機器證明理論的深入，使數學研究傳統的模式發生了變化。既然，計算機是一種擅長於數值處理工具，那麼，用量的表達代替形的描述，用數值計算來代替邏輯推理，便自然成為處理數學問題的新思維。

我們從代數恆等式的證明將可以悟出：有時，舉例的確可以代替證明。

為了簡便敘述；我們考察一個簡單的例子。請讀者專注於我們所用的方法，而不要發出“殺雞用牛刀”的責難。

例如：要證明代數恆等式

$$(x + 1)(x^2 - x + 1) = x^3 + 1 \quad (1)$$

我們只須對 x 任意取4個數 (舉例)。例如 $x = -1, 0, 1, 2$ 。先後代入 (1) 式，得

$$0 = 0 \quad (\text{當 } x = -1)$$

$$1 = 1 \quad (\text{當 } x = 0)$$

$$2 = 2 \quad (\text{當 } x = 1)$$

$$9 = 9 \quad (\text{當 } x = 2)$$

於是斷言：(1) 式恆成立。

上述證明是可行的。它的邏輯基礎是：若 (1) 式非恆等式，則方程 $x^3 + 1 - (x + 1)(x^2 - x + 1) = 0$ 是一個3次方程。根據高斯定理 (n 次代數方程至多有 n 個根) 它至多只能有3個不同的根。但由上面舉例證明，它有4個不同的根，矛盾！

這種“舉例”方法，就是用電腦證明代數恆等式的精髓。

我們要證明恆等式

$$f(x) = g(x) \quad (2)$$

其中 $f(x)$ 和 $g(x)$ 都是多項式，且它們的最高次數是 n 。我們只須用 $n + 1$ 個不同的數，算得 $n + 1$ 個等式成立，(舉 $n + 1$ 個例子)，則可證明 (2) 是恆等式。

可能讀者會說：用舉例方法證明恆等式 (2)，方法是簡單，但算起來可不容易。但是，如果我們加入電腦這一武器，算起來也就得心應手了。要知道，計算可是電腦的強項啊！

從“有限”能推斷“無限”，這正是數學的魅力所在。

計算代替 (蘊含) 推理，舉例達到證明。用電腦，我們成功地實現了代數恆等式的證明。

二. 先試用“萬金油”。

我們剛剛為代數恆等式的機器證明歡呼，可是，用上述的賦值法，即使我們有電腦，

也不能證明組合恆等式。因為組合恆等式是包含有二項式係數的恆等式，如果把它看作一個方程的話，我們面對的往往不是一個整式方程。

翻開任一本離散數學，你都會遇到大量的組合恆等式問題，作為一種技巧，數學家會用一種模型方法去證明一些簡單的恆等式。例如，恆等式

$$\sum_{k \geq 0} \binom{n}{k} = 2^n \quad (3)$$

可以用兩種方法去求一個 n 元集的所有子集個數，從而輕易地建立起它們的恆等關係。然而，對於較複雜的大量組合恆等式，數學家採用一種行之有效的代數技巧。H. S. Wilf 把它稱為“Snakeoil”。我們姑且譯之為“萬金油”方法，用數學語言來說，這是生成函數方法。它的基本原理是：不直接用代數變換推導恆等式，而轉去求帶參數的整個族的生成函數，然後，讀出生成函數的係數。

最有幫助的級數 (生成函數) 通常是

$$\sum_{r \geq 0} \binom{n}{r} x^r = (1 + x)^n \quad (4)$$

$$\sum_{r \geq 0} \binom{r}{k} x^r = \frac{x^k}{(1 - x)^{k+1}} \quad (k \geq 0) \quad (5)$$

$$\sum_{n \geq 0} \frac{1}{n+1} \binom{2n}{n} \cdot x^n = \frac{1}{2x} (1 - \sqrt{1 - 4x}) \quad (6)$$

(註 $\binom{n}{r} = 0$, 當 $r < 0$ 或 $r > n$)。

為了說明萬金油方法，我們考察兩個例子。

例1: 求證

$$\sum_{k \geq 0} \binom{k}{n-k} = \frac{1}{\sqrt{5}} \left[\left(\frac{1 + \sqrt{5}}{2} \right)^{n+1} \right]$$

$$-\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}] \quad (n = 0, 1, 2, \dots) \quad (7)$$

證明步驟如下：

(i) 判斷和式依賴的自由變量是 n ，令

$$f(n) = \sum_{k \geq 0} \binom{k}{n-k}$$

(ii) 設 $F(x)$ 是 $f(n)$ 的冪級數生成函數，即令

$$\begin{aligned} F(x) &= \sum_n f(n)x^n \\ &= \sum_n x^n \sum_{k \geq 0} \binom{k}{n-k} \end{aligned}$$

(iii) 交換兩個求和次序，並利用已知的生成函數，把和寫成函數形式。

$$\begin{aligned} F(x) &= \sum_{k \geq 0} \sum_n \binom{k}{n-k} x^n \\ &= \sum_{k \geq 0} x^k \sum_n \binom{k}{n-k} x^{n-k} \\ &\quad (\text{爲了用(4)}) \\ &= \sum_{k \geq 0} x^k (1+x)^k \\ &= \sum_{k \geq 0} (x+x^2)^k \\ &= \frac{1}{1-x-x^2} \end{aligned} \quad (8)$$

(iv) 求出生成函數的係數，便是 $f(n)$ 。

易見，(8) 式是 Fibonacci 數的生成函數。(見「數學傳播」22 卷第 2 期拙作 [3])，它的展開式的 x^n 項係數便是 (7) 式的右邊。至此，便完成了 (7) 的證明。

細心的讀者不難發現，上述 (7) 式的證明中，我們僅從左邊推導出右邊。這既是證明，也可看作求和。因此，用萬金油方法，不

僅僅可以證明組合恆等式，也可以發現組合恆等式。

我們再從下例，領略一下萬金油的“療效”。

例 2: 求證

$$\begin{aligned} &\sum_k \binom{m}{k} \binom{n+k}{m} \\ &= \sum_k \binom{m}{k} \binom{n}{k} 2^k, \quad (m, n \geq 0) \quad (9) \end{aligned}$$

證：左邊乘以 x^n ，對 $n \geq 0$ 求和並交換求和次序得

$$\begin{aligned} &\sum_k \binom{m}{k} x^{-k} \sum_{n \geq 0} \binom{n+k}{m} x^{n+k} \\ &= \sum_k \binom{m}{k} x^{-k} \frac{x^m}{(1-x)^{m+1}} \\ &= \frac{x^m}{(1-x)^{m+1}} \left(1 + \frac{1}{x}\right)^m \\ &= \frac{(1+x)^m}{(1-x)^{m+1}} \end{aligned}$$

如果用 x^n 乘右邊，類似上述求和，得

$$\begin{aligned} &\sum_k \binom{m}{k} 2^k \sum_{n \geq 0} \binom{n}{k} x^n \\ &= \frac{1}{1-x} \sum_k \binom{m}{k} \left(\frac{2x}{1-x}\right)^k \\ &= \frac{1}{1-x} \left(1 + \frac{2x}{1-x}\right)^m \\ &= \frac{(1+x)^m}{(1-x)^{m+1}} \end{aligned}$$

於是，(9) 式成立。

用萬金油方法，可以成功地發現和證明一大類組合恆等式。例如，在組合數學中的一批反演公式以及超幾何函數中的恆等式。如果說，直接用簡單的組合恆等式去證明其它恆等式的方法是內部方法的話，那麼，萬金油

方法便是組合恆等式證明的外部方法。這種方法近乎是程序性的，然而它需要更多的人工技巧。那麼，能否尋求一種用計算機符號運算程序來證明組合恆等式的方法呢？近年來，機器證明在幾何學上的成功更激勵數學家在組合恆等式的計算機證明上躍躍欲試。

1990年，美國費城的兩位數學家合作，找到了這樣的一種方法。

三. 電腦，還是要用電腦！

Zeilberger, 1950年生於以色列海法。1976年在 Weizmann 科學研究院獲博士學位。後赴美，先在費城 Drexel 大學任教，後在費城 Temple 大學任教授。

Wilf, 1931年生於費城，在麻省理工學院上學，1958年，在哥倫比亞大學獲博士學位。先在伊利諾大學任教，1962年在賓州大學任教，現任 Thomas. A. Scott 教授。

他們刊登在「美國數學雜誌」上的獲獎論文。提供了一個證明組合恆等式的新方法，用這一方法，可統一處理一些從未解決的極難恆等式的證明。更重要的，它展示了用電腦證明組合恆等式的前景。

下面，讓我們追溯一下 Wilf 和 Zeilberger 考慮問題的思路。

若要證明一個恆等式

$$\sum_k U(n, k) = rhs(n), \quad n = 0, 1, 2, \dots \quad (10)$$

我們可以把它變形，用右邊的 $rhs(n)$ 除兩邊，便得到一個標準形式

$$\sum_k F(n, k) = 1, \quad n = 0, 1, 2, \dots \quad (11)$$

這樣，我們便把 (10) 式的證明，轉化為 (11)，即證明一個和式與 n 無關。

爲此，把 (11) 式用 $n+1$ 代替 n ，然後減去 (11) 得

$$\sum_k \{F(n+1, k) - F(n, k)\} = 0, \quad n = 0, 1, \dots \quad (12)$$

如果存在一個很好的函數 $G(n, k)$ ，使得

$$F(n+1, k) - F(n, k) = G(n, k+1) - G(n, k) \quad (13)$$

這樣，(12) 式便能“壓縮”，即

$$\begin{aligned} & \sum_{k=-L}^{k=K} \{F(n+1, k) - F(n, k)\} \\ &= \sum_{k=-L}^{k=K} \{G(n, k+1) - G(n, k)\} \\ &= G(n, K+1) - G(n, -L) \end{aligned} \quad (14)$$

如果函數 $G(n, k)$ 具有性質 $G(n, \pm\infty) = 0$ ，則在 (14) 中，令 $K, L \rightarrow \infty$ ，便知 (12) 成立。

由此想法，Wilf 和 Zeiberger 便得到下列定理。

定理1: 設 (F, G) 滿足 (13)，並且

$$\lim_{k \rightarrow \pm\infty} G(n, k) = 0, \quad n = 0, 1, 2, \dots \quad (15)$$

則恆等式 $\sum_k F(n, k) = \text{常數}$ ， $n = 0, 1, 2, \dots$ 成立。

爲了明瞭用 WZ 定理證明組合恆等式的過程，我們先從一個最簡單的例子談起。

假設要證明恆等式

$$\sum_k \binom{n}{k} = 2^n, \quad n \geq 0 \quad (16)$$

仿照 (11), 便得

$$F(n, k) = \binom{n}{k} / 2^n, \quad n \geq 0 \quad (17)$$

現在要求函數 $G(n, k)$, 它就是

$$G(n, k) = -\binom{n}{k-1} / 2^{n+1} \quad (18)$$

驗證 $G(n, k)$ 合乎定理要求, 即 (13) 和 (15) 成立。經計算, 不難得到

$$\begin{aligned} & \binom{n+1}{k} / 2^{n+1} - \binom{n}{k} / 2^n \\ &= -\binom{n}{k} / 2^{n+1} + \binom{n}{k-1} / 2^{n+1}, \quad n \geq 0 \end{aligned}$$

及

$$\lim_{n \rightarrow \pm\infty} -\binom{n}{k-1} / 2^{n+1} = 0, \quad n \geq 0,$$

於是 (16) 成立。

從上述過程, 我們看到證明組合恆等式的關鍵在於從 F 尋找 G , 若滿足 (13), (15) 的 G 找出來, 我們就可以斷言, 恆等式已經由 WZ 對 (F, G) 所證明。

讀者急於知道的問題也許是: 如何從 F 尋找 G ?

WZ方法應用於證明這樣的一類組合恆等式, 它的標準形 (11) 的函數 F , 具有使

$$\frac{F(n+1, k)}{F(n, k)} \text{ 和 } \frac{F(n, k-1)}{F(n, k)} \quad (19)$$

都是 n 和 k 的有理函數的性質。於是由 (13) 的

$$\begin{aligned} & F(n+1, k) - F(n, k) \\ &= G(n, k+1) - G(n, k) \end{aligned}$$

得

$$\begin{aligned} & \frac{F(n+1, k)}{F(n, k)} - 1 \\ &= \frac{G(n, k+1)}{F(n, k)} - \frac{G(n, k)}{F(n, k)} \end{aligned}$$

進一步,

$$\begin{aligned} & \frac{F(n+1, k)}{F(n, k)} - 1 \\ &= \frac{G(n, k+1)}{F(n, k)} - \frac{G(n, k)}{F(n, k-1)} \cdot \frac{F(n, k-1)}{F(n, k)} \end{aligned} \quad (20)$$

注意到條件 (19), 我們令

$$\frac{G(n, k)}{F(n, k-1)} = R(n, k) \quad (21)$$

這裡 $R(n, k)$ 是 n 和 k 的有理函數。於是 (20) 寫成

$$\begin{aligned} & \frac{F(n+1, k)}{F(n, k)} - 1 \\ &= R(n, k+1) - R(n, k) \cdot \frac{F(n, k-1)}{F(n, k)} \end{aligned}$$

(21) 式可以寫成

$$G(n, k) = R(n, k)F(n, k-1) \quad (22)$$

因此, 我們可以簡化尋找 $G(n, k)$ 的方法。要得到 WZ 對 (F, G) , 只需得到有理函數 $R(n, k)$, 並加以驗證便可。

考察下列例子, 可以幫助我們進一步領會 WZ 方法的證明步驟。

例3: 證明

$$\sum_k (-1)^k \binom{n}{k} \binom{2k}{k} 4^{n-k} = \binom{2n}{n}, \quad n \geq 0 \quad (23)$$

證明: 易見

$$F(n, k) = (-1)^k \binom{n}{k} \binom{2k}{k} 4^{n-k} / \binom{2n}{n}$$

取 $R(n, k) = (2k - 1)/(2n + 1)$.

由 (22) 得

$$G(n, k) = (-1)^{k-1} \frac{2k-1}{2n+1} \binom{n}{k-1} \binom{2k-2}{k-1} \cdot \frac{4^{n-k+1}}{\binom{2n}{n}}$$

檢驗 (F, G) 是否是 WZ 對, 先檢驗條件 (13) 式是否成立。直接計算可得

$$F(n+1, k) - F(n, k) = G(n, k+1) - G(n, k) \quad (24)$$

再檢驗邊界條件 (15) 是否滿足。

易見, $G(n, k) \rightarrow 0$ (當 $k \rightarrow \pm\infty$), 事實上, 對每個 $k > n$ 的值和所有 $k < 0$ 的值 $G(n, k) = 0$ 。由 WZ 定理 $\sum_k F(n, k) =$ 常數 ($n = 0, 1, 2, \dots$)。

又因 $n = 0$ 時,

$$\sum_k F(n, k) = \sum_k F(0, k) = 1$$

便得 (23) 的證明。

現在, 我們總結一下用有理函數 $R(n, k)$ 證明恆等式的完整證明步驟。

- (1) 給定恆等式 $\sum U(n, k) = rhs(n)$ ($n = 0, 1, 2, \dots$)
- (2) 定義 $F(n, k)$ 對 $n \geq 0$ 的整數 k , $F(n, k) = U(n, k)/rhs(n)$ 。
- (3) 找出有理函數 $R(n, k)$, 從而
- (4) 定義 $G(n, k) = R(n, k)F(n, k - 1)$
- (5) 檢驗條件 (14) 是否滿足
- (6) 檢驗條件 (15) 是否滿足

(7) 檢驗當 $n = 0$ 時, $\sum_k F(n, k) = 1$ 是否成立。

作為練習, 讀者可按步驟操練下列兩個例子。

例 4: 證明 $\sum (-1)^k \binom{n}{k} / \binom{k+a}{k} = a/(n+a)$ ($n \geq 0$)

提示: 取 $R(n, k) = k/(n+a)$

例 5: 證明 $\sum (-1)^{n-k} \binom{2n}{k}^2 = \binom{2n}{n}$ ($n \geq 0$)

提示: 取 $R(n, k) = -(10n^2 - 6kn + 17n + k^2 - 5k + 7)/(2(2n - k + 2)^2)$

我們知道, 上述的第(5)步 (即 (24)) 將是一種並非簡易的計算 (雖然在 (24) 中, 我們給人以一種“易見”的錯覺), 不過, 事實上, 這一步完全可以用計算機去完成。已經設計了適用的符號運算程序, 只要我們鍵入函數 F 和 G , 就能用計算機驗證 (14) 式是否成立。

接踵而來的問題是: 上面的 $R(n, k)$ 的確不易求出, 能否有一些更機械化的方法。

事實上, 在已得到 $F(n, k)$ 的情形下, 我們的終極目標是要求 $G(n, k)$, 使得

$$F(n+1, k) - F(n, k) = G(n, k+1) - G(n, k), \quad n = 0, 1, \dots$$

認真觀察就可以看到, 上式的 n 僅是一個啞參數, k 才是活指標。因此, 可令

$$f_k = F(n+1, k) - F(n, k) \\ g_k = G(n, k)$$

上述問題歸結為: 如果 f_k 是給定的 k (以及其它參數) 的函數。怎樣求 g_k , 使得對所有整

數 k , 有

$$f_k = g_{k+1} - g_k \quad (25)$$

從形式上, 這是一個幾乎能立即給予解答的問題。我們只需令 $g_k = \sum_{j < k} f_j$ 就能滿足 (25)。

Zeilberger 和 Wilf 考察了一類稱為封閉形式的函數— 如果 f_{k+1}/f_k 是 k 的有理函數, 整數 k 的函數 f_k 稱為封閉形式的函數。例如 $k!$, $\frac{(3k+2)!}{(5k-6)!}$, $(-1)^k 4^{n-k} \binom{2k}{k} / \binom{n+k}{k}$ 都是封閉形式函數。對於這類函數, 有下列定理。

定理 2: 設 f_k 對整數 k 有定義, 並且是封閉形式的。則存在一個封閉形式的函數 g_k , 使得對所有整數 k , $f_k = g_{k+1} - g_k$ 。

令人欣慰的是, R. W. Gosper 在 1978 年發表的一個算法 ([4]) 給出了上述從 f_k 找 g_k 的算法上的回答。也就是說, 如果對 f_k 使用 Gosper 算法, 不僅能判斷 g_k 是否存在, 還能把存在的 g_k 找出來。目前, Gosper 算

法已寫進了某些商業用途的符號運算軟件包, 例如, 它已經能在 Macsyma, Mathematica 中實現, 這顯示了用計算機證明組合恆等式的新時代已經到來!

參考文獻

1. D. Zeilberger and H. Wilf, Rational functions certify combinatorial identities, J. Amer. Math. Soc., Vol.3(1990), 147-158.
2. 洪加威, 能用例證來證明幾何定理嗎?, 中國科學 (A), 1986, 第 3 期, 225 頁。
3. 柳柏濂, 別瞧不起它, 那個中學教材中的公式, 數學傳播, 22 卷第二期, 民 87 年 6 月。
4. Gosper, R. William, Jr. Decision procedures for indefinite hypergeometric summation, Proc. Nat. Acad. Sci, U.S.A., 75(1978), 40-42.

—本文作者任教於中國華南師範大學數學系和中國廣東職業技術師範學院計算機系—