

最大根方法

——一段往事

聂子佩

这是一个历史悠久的故事, 从头讲起至少应该追溯到六十年前, 但我们先从幂级数的定义开始说.

壹

幂级数是多项式的推广形式, 指的是形如 $\sum_{n=0}^{\infty} a_n t^n$ 的式子, 我们可以认为这里的 t 和求和号都只是符号, 那么幂级数的意义就只在于一个数列 $\{a_n\}$. 不过我们不会满足于此. 当幂级数作为一个级数在某些意义下收敛时, 它又可以代表一个函数. 我们可以对函数作各种运算, 而泰勒公式提示我们, 在一些时候运算得到的函数又可以写成幂级数的形式. 如此一来, 我们有时可以直接定义幂级数上的运算. 比如加法, 我们有

$$\sum_{n=0}^{\infty} a_n t^n + \sum_{n=0}^{\infty} b_n t^n = \sum_{n=0}^{\infty} (a_n + b_n) t^n,$$

看上去天经地义.

那么, 乘法呢?

美国人发明了一个词 “freshman’s dream”, 指代的是 $(x + y)^n = x^n + y^n$ 这个式子. 在实践中, 大一学生做得更多事情是将矩阵中对应项相乘得到的矩阵当作矩阵的乘法. 类似地, 我们也可以定义幂级数的 “乘法” 为

$$\sum_{n=0}^{\infty} a_n t^n \circ \sum_{n=0}^{\infty} b_n t^n = \sum_{n=0}^{\infty} a_n b_n t^n,$$

简洁明了. 然而这样的乘法却和幂级数对应的函数之间的乘法是不相容的. 如果要相容, 我们只能定义

$$\sum_{n=0}^{\infty} a_n t^n \cdot \sum_{n=0}^{\infty} b_n t^n = \sum_{n=0}^{\infty} \left(\sum_{k=0}^n a_k b_{n-k} \right) t^n.$$

本文 2018 年 5 月 21 日首发于爱哞客栈, 2018 年 5 月 22 日收到修改稿.

为了区分这两种乘法, 我们把第一种称为幂级数的哈达玛乘法, 第二种称为幂级数的乘法.

那么幂级数的哈达玛乘法与幂级数对应的函数之间就没有多大联系了吗? 也不完全是. 至少, 我们还可以有这样的命题:

命题 1. 如果两个幂级数对应的函数是有理函数, 那么它们的哈达玛乘积对应的函数也是有理函数.

有理函数指的是多项式的商, 这与这些多项式的系数是不是有理数无关, 请注意不要混淆.

设有理函数 $\frac{P(t)}{Q(t)}$ 对应的幂级数为 $\sum_{n=0}^{\infty} a_n t^n$, 由于满足

$$Q(t) \cdot \sum_{n=0}^{\infty} a_n t^n = P(t),$$

由幂级数的乘法可知, 数列 $\{a_n\}$ 自某项起形成一个常系数线性递推数列. 反之亦然. 由特征方程法或者考虑部分分式, 我们可以推得, 有理函数对应的幂级数系数自某项起有通项公式

$$a_n = \sum_{i=1}^s p_i(n) \alpha_i^n,$$

这里 α_i 是一些两两不同的复数, 而 p_i 是一些非零复系数多项式.

注意: 即使 a_n 全是实数, 甚至全是正整数, 我们也无法保证 p_i 的系数是实数或者 α_i 是实数, 事实上, α_i 是 $Q(t)$ 的某些根.

因为两个有理函数对应的哈达玛乘积的幂级数系数的通项公式也有这样的形式, 故我们可以反其道而行之, 推得其幂级数系数某项起也形成一个常系数线性递推数列, 因而哈达玛乘积对应的函数也是有理函数, 即命题 1 成立.

那么, 除法呢?

我们定义哈达玛除法为哈达玛乘法的逆运算, 即当 b_n 全不为零时, 定义 $\sum_{n=0}^{\infty} a_n t^n$ 和 $\sum_{n=0}^{\infty} b_n t^n$ 的哈达玛商为 $\sum_{n=0}^{\infty} \frac{a_n}{b_n} t^n$.

那么两个有理函数对应的幂级数的哈达玛商对应的函数也是有理函数吗? 答案是否定的.

类似地, 我们还可以定义 $\sum_{n=0}^{\infty} a_n t^n$ 的哈达玛 k 次方根为满足按哈达玛乘法自乘 k 次等于 $\sum_{n=0}^{\infty} a_n t^n$ 的所有幂级数. 然而, 有理函数对应的幂级数也未必有一个哈达玛 k 次方根, 使得其对应的函数是有理函数.

一切就到此为止了吗? 不, 让我们回到六十年前.

贰

1959 年, 法国数学家皮索在前人的特例 [1] 的启发下提出了如下的猜想 [2]:

命题 2. 如果两个整系数幂级数对应的函数是有理函数, 且它们的哈达玛商也是整系数幂级数, 则它们的哈达玛商对应的函数也是有理函数.

命题 3. 如果一个幂级数对应的函数是有理函数, 且它的系数都是整数的 k 次方, 则它有一个哈达玛 k 次方根, 使得其对应的函数也是有理函数.

命题 2 解决于八十年代 [3, 4, 5], 命题 3 解决于 2000 年 [6], 对于这些证明, 我们先放一放. 我们且来看看皮索是怎么处理这两个命题的.

皮索用了一种现在我们称为“最大根方法”的技巧. 他首先作了一些额外的假设: 在命题 2 中, 设除数 $\sum_{n=0}^{\infty} b_n t^n$ 的系数自某项起的通项公式

$$b_n = \sum_{i=1}^{s'} q_i(n) \beta_i^n$$

中, β_1 的模长大于任何 β_i ($2 \leq i \leq s'$) 的模长. 在命题 3 中, 设幂级数 $\sum_{n=0}^{\infty} a_n t^n$ 的系数自某项起的通项公式

$$a_n = \sum_{i=1}^s p_i(n) \alpha_i^n$$

中, α_1 的模长大于任何 α_i ($2 \leq i \leq s$) 的模长. 这种条件被称为最大根条件.

我们首先来看命题 2.

设被除数 $\sum_{n=0}^{\infty} a_n t^n$ 的系数自某项起的通项公式为

$$a_n = \sum_{i=1}^s p_i(n) \alpha_i^n,$$

除数 $\sum_{n=0}^{\infty} b_n t^n$ 的系数自某项起的通项公式为

$$b_n = \sum_{i=1}^{s'} q_i(n) \beta_i^n,$$

那么哈达玛商的系数自某项起的通项公式则为

$$\begin{aligned} \frac{a_n}{b_n} &= \frac{\sum_{i=1}^s p_i(n) \alpha_i^n}{\sum_{i=1}^{s'} q_i(n) \beta_i^n} = \frac{\sum_{i=1}^s \frac{p_i(n)}{q_1(n)} \left(\frac{\alpha_i}{\beta_1}\right)^n}{1 + \sum_{i=2}^{s'} \frac{q_i(n)}{q_1(n)} \left(\frac{\beta_i}{\beta_1}\right)^n} \\ &= \left(\sum_{i=1}^s \frac{p_i(n)}{q_1(n)} \left(\frac{\alpha_i}{\beta_1}\right)^n \right) \sum_{j=0}^{\infty} \left(- \sum_{i=2}^{s'} \frac{q_i(n)}{q_1(n)} \left(\frac{\beta_i}{\beta_1}\right)^n \right)^j, \end{aligned}$$

展开后可以写作

$$\frac{a_n}{b_n} = \sum_{i=1}^{\infty} r_i(n)\gamma_i^n,$$

这里 $\{r_i(n)\}$ 是一列非零有理函数, 而 $\{\gamma_i\}$ 是模长不增的复数列. 估计每一项的大小, 我们得到, 存在正整数 l 和实数 $0 < \gamma < 1$, 使得 $|r_i(n)\gamma_i^n| \ll n^{li}\gamma^{ni}$.

设正整数 M 满足 $|\gamma_{M+1}| < 1$, 并将 $\frac{a_n}{b_n}$ 写作

$$\frac{a_n}{b_n} = \sum_{i=1}^M r_i(n)\gamma_i^n + \sum_{i=M+1}^{\infty} r_i(n)\gamma_i^n,$$

则后一半当 n 趋于无穷时趋于零. 由条件 a_n, b_n 均为整数, 故 p_i, q_j 的所有系数以及 α_i, β_j 均为代数数, 故 r_i 的所有系数以及 γ_i 也均为代数数. 因为 r_i 的所有系数都是代数数, 所以存在非零整系数多项式 R , 使得所有 $R(n)r_i(n)$ ($1 \leq i \leq M$) 均为多项式. 因为 γ_i 都是代数数, 所以

$$\sum_{i=1}^M R(n)r_i(n)\gamma_i^n$$

形成一个整系数线性递推数列, 即, 存在不全为零的整数 c_1, \dots, c_h , 使得

$$\sum_{k=1}^h c_k \left(\sum_{i=1}^M R(n+k)r_i(n+k)\gamma_i^{n+k} \right) = 0.$$

于是, 我们有

$$\sum_{k=1}^h \frac{a_{n+k}}{b_{n+k}} c_k R(n+k) = \sum_{k=1}^h c_k \left(\sum_{i=M+1}^{\infty} R(n+k)r_i(n+k)\gamma_i^{n+k} \right).$$

由于左边是整数, 右边当 n 趋于无穷时趋于零, 我们知道当 n 足够大时, 左右均等于零, 即幂级数 $\sum_{n=0}^{\infty} \frac{a_n}{b_n} R(n)t^n$ 的系数自某项起形成常系数线性递推数列, 换句话说, 幂级数 $\sum_{n=0}^{\infty} \frac{a_n}{b_n} R(n)t^n$ 对应的函数是有理函数.

如果我们额外假设了 $q_1(n)$ 是常数, 那么 $R(n)$ 也是常数, 此时我们已经不需要再做什么了. 而在一般情况下, 我们再回过头来看看命题 2 就会发现, 我们已经把最大根条件下的命题 2, 化归成了在除数 $\sum_{n=0}^{\infty} b_n t^n$ 的系数是整值多项式的条件下的命题 2. 换句话说, 我们只需证明如下命题, 这个命题的证明应该归功于皮索的后继者康托尔 [7]:

命题 4. 如果整系数幂级数 $\sum_{i=0}^{\infty} a_n t^n$ 对应的函数是有理函数, 且存在一个整值多项式 R , 使得 $\frac{a_n}{R(n)}$ 总是整数, 则幂级数 $\sum_{i=0}^{\infty} \frac{a_n}{R(n)} t^n$ 对应的函数也是有理函数.

与之前一样, 我们设 $\sum_{n=0}^{\infty} a_n t^n$ 的系数自某项起的通项公式为

$$a_n = \sum_{i=1}^s p_i(n) \alpha_i^n.$$

这时

$$\frac{a_n}{R(n)} = \sum_{i=1}^s \frac{p_i(n) \alpha_i^n}{R(n)},$$

其分母总是整数, 而其分子在一般情况下却只是个代数数, 看来我们在这里无论如何也得用一些代数数论的知识才能处理下去了. 世界就是如此, 有的问题高等而肤浅, 比如如何将一个初等数论的证明平行推广到代数数论中去, 而有的问题却初等而深刻, 比如生命的意义是什么. 为了让本文更可读, 我决定只证明其初等的特例, 而将完全版的证明留给了解一些代数数论或者对代数数论感兴趣的读者们. 我们假设, 这里 p_i 的系数和 α_i 都是有理数.

我们不妨设 $R(n)$ 模任何素数 p 都不恒同余于零, 不然我们用 $\frac{R(n)}{p}$ 代替 $R(n)$, 而这样的操作只能作有限次, 否则某个不为零的整值就会变成绝对值小于一的数. 取 N 为一大于所有 p_i 的系数的分母的绝对值, 所有 α_i 的分子和分母的绝对值, 所有 $\alpha_i - \alpha_j$ ($i \neq j$) 的分子和分母的绝对值, 以及所有 $R(n)$ 的系数的分母的绝对值的正整数. 由中国剩余定理, 存在无穷多个正整数 d , 使得 $R(d)$ 的所有素因子都不小于 N .

取任意这样的 d . 对 $R(d)$ 的每个素因子 p , 假设 p^h 恰好整除 $R(d)$, 那么 p^h 整除 $R(d + kp^h)$, 这里 $k = 0, \dots, s-1$. 由条件,

$$0 \equiv a_{d+kp^h} = \sum_{i=1}^s p_i(d+kp^h) \alpha_i^{d+kp^h} \equiv \sum_{i=1}^s p_i(d) \alpha_i^{d+kp^h} \pmod{p^h},$$

对每个 $k = 0, \dots, s-1$. 把这 s 个式子想成关于 $p_1(d), \dots, p_s(d)$ 的 s 元一次方程组. 由范德蒙行列式及费马小定理, 系数行列式等于

$$\prod_{i=1}^s \alpha_i^d \prod_{i>j} (\alpha_i^{p^h} - \alpha_j^{p^h}) \equiv \prod_{i=1}^s \alpha_i^d \prod_{i>j} (\alpha_i - \alpha_j) \pmod{p},$$

不是 p 的倍数, 由克莱姆法则, 系数矩阵可逆, 所以这个方程组在模 p^h 意义下没有非零解, 故 p^h 整除每个 $p_i(d)$. 由 p 的任意性, 我们知道每个 $p_i(d)$ 的分子都是 $R(d)$ 的倍数. 由于这样的 d 可以任意大, 我们知道 R 作为多项式整除每个 p_i . 我们便得到了命题 4 的结论.

皮索对于命题 3 的处理是类似的, 只是把幂级数展开式

$$\frac{1}{1-x} = \sum_{i=0}^{\infty} x^i$$

换作

$$(1+x)^{\frac{1}{k}} = \sum_{i=0}^{\infty} \binom{\frac{1}{k}}{i} x^i.$$

如此他得到的结论是: 若最大根条件成立, 且 $p_1(n)$ 是常数, 则命题 4 成立. 如果想要摆脱 $p_1(n)$ 是常数这个条件, 我们需要 [8, 9, 10] 通过分析素因子来区分多项式里的 n 和指数上的 n 带来的影响.

也许我们应该在陷入更多对细枝末节的探讨前停止, 再回头看看什么是最大根方法, 为什么我们需要最大根来处理这些问题.

一言以蔽之, 最大根方法就是以渐进的手段分析整数序列, 由于绝对值小于一的整数只有零, 或者, 等价地, 依据代数数论的刘维尔不等式, 在不等式中得到等式. 至于为什么需要最大根, 这是为了让得到的级数收敛.

如果最大根不唯一的时候, 这个方法就失效了吗? 也不是.

我们至少还有两种普遍的方法在最大根不唯一的时候依然用最大根方法处理问题.

第一, 是从最大根到最小根的转变. 如果 $\{a_n\} (n \in \mathbb{N})$ 是我们的常系数线性递推数列, 那么我们可以依样画葫芦将其定义拓展到 $\{a_n\} (n \in \mathbb{Z})$, 把数列倒过来看, 最大根就变成了最小根, 最小根则变成了最大根, 这时我们需要考虑两个问题: 第一, $\{a_n\} (n \in \mathbb{Z})$ 这时未必是整数数列了, 我们需要对我们的命题作一点推广; 第二, 我们需要证明对于 $n \in \mathbb{N}$ 时题目给的整除条件或者 k 次方数条件可以推到对于所有 $n \in \mathbb{Z}$ 成立, 这通常需要分别考虑每个素因子得到.

第二, 是改变所在的度量空间. 级数 $\sum_{i=0}^{\infty} 2^i$ 在通常意义下发散, 却在 2 进度量中收敛于 -1 . 级数收敛条件的改变意味着最大根条件的改变.

叁

从方法到结论, 我们都可以利用本文中讲述的东西更深入地了解一些竞赛题的背景. 比如下面这道题是 2000 年全国高中数学联赛加试题. 证明一个常系数线性递推式总是完全平方数, 这种题目甚至已经成为了初中数学竞赛的套路.

问题 1. 设数列 $\{a_n\}$ 和 $\{b_n\}$ 满足 $a_0 = 1, b_0 = 0$, 且
$$\begin{cases} a_{n+1} = 7a_n + 6b_n - 3 \\ b_{n+1} = 8a_n + 7b_n - 4 \end{cases},$$

求证: a_n 是完全平方数.

如果你遇到类似的考题, 记住本文的命题 3, 求通项——开方/幂级数展开——算结果的线性递推式, 必然能得到证明.

以下三道题直接按最大根方法作幂级数展开就可以得到:

问题 2. 设 a, b 为整数, 使得对所有 $n \in \mathbb{N}$ 都有 $2^n a + b$ 是完全平方数. 证明 $a = 0$. (2001 年波兰数学奥林匹克第三轮)

问题 3. 设 a, b 为大于 1 的整数, 使得对所有 $n \in \mathbb{N}$ 都有 $a^n - 1$ 整除 $b^n - 1$. 证明存在正整数 k 使得 $b = a^k$. (美国数学月刊问题 10674)

问题 4. 设 a, b 为正整数, 使得对所有 $n \in \mathbb{N}$ 都有 $b^n + n$ 是 $a^n + n$ 的倍数. 证明 $a = b$. (2005 年 IMO 预选题 N6)

最后这个问题可以通过按最大根方法和系数比较得到, 其中的多项式部分不是常数, 这使得比较系数的过程大为简化:

问题 5. 设 $a_1, a_2, a_3, b_1, b_2, b_3$ 是两两不同的正整数, 使得对所有 $n \in \mathbb{N}$ 都有

$$(n+1)a_1^n + na_2^n + (n-1)a_3^n \mid (n+1)b_1^n + nb_2^n + (n-1)b_3^n.$$

证明存在正整数 k , 使得 $b_i = ka_i (i = 1, 2, 3)$. (2010 年中国数学奥林匹克)

感谢阅读, 希望大家能有所收获.

参考文献

- [1] Pólya, G. Arithmetische Eigenschaften der Reihenentwicklungen rationaler Funktionen. Journal für die reine und angewandte Mathematik 151 (1921): 1-31.
- [2] Pisot, C. Conférences données à l'Institut Fourier de Grenoble. 1959.
- [3] Pourchet, Yves. Solution du problème arithmétique du quotient de Hadamard de deux fractions rationnelles. CR Acad. Sci. Paris 288 (1979): 1055-1057.
- [4] van der Poorten, Alfred J. Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationnelles. CR Acad. Sci. Paris 306.97 (1988): 102.
- [5] Rumely, Robert. Notes on Van der Poorten's proof of the Hadamard quotient theorem. Séminaire de Th. de Nombres de Paris (1986).

- [6] Zannier, Umberto. A proof of Pisot's d -th root conjecture. *Annals of Mathematics* 151.1 (2000): 375-383.
- [7] Cantor, David. On arithmetic properties of coefficients of rational functions. *Pacific Journal of Mathematics* 15.1 (1965): 55-58.
- [8] Perelli, A., and Zannier, U. Arithmetic properties of certain recurrence sequences. *Journal of the Australian Mathematical Society* 37.1 (1984): 4-16.
- [9] Bézivin, Jean-Paul. Factorisation de suites récurrentes linéaires. *Groupe de travail d'analyse ultramétrique* 7.8 (1979): 1979-1981.
- [10] Rumely, Roberts, and Van der Poorten, Alfred J. A note on the Hadamard k th root of a rational function. *Journal of the Australian Mathematical Society* 43.3 (1987): 314-327.