arXiv:2304.13605v1 [cs.CC] 26 Apr 2023

幂级数的阶与平方根和问题

Louis Gaillard * Gorav Jindal †

摘要

本文重点研究给定有限个幂级数的线性组合的阶。形式幂级数的阶，记作 ord(f)，定义为在$f(x)$中系数非零的x 的最小指数。我们的首个结果表明，这些幂级数的朗斯基行列式的阶与它们的线性组合所能达到的最大阶相差至多一个多项式因子。这意味着，(Kayal 和 Saha, TOCT'2012) 中用于给平方根和的阶求上界的朗斯基行列式方法，在至多多项式级别的增长范围内是最优的。我们还针对其他多种情形，给出了与 (Kayal 和 Saha, TOCT' 2012) 中类似的幂级数阶上界。此外，我们还解决了 (Etessami 等人, TOCT'2014) 中提出的不等式判定问题的一个特殊情形。

在论文的第二部分中，我们研究平方根和问题的等式变体。根据（Bl¨omer，FOCS' 1991），该问题可在多项式时间内判定。我们研究了这一问题的一个自然推广，即输入整数以直线程序的形式给出。在广义黎曼假设（GRH）成立的前提下，我们证明该问题可以归约为所谓的"一维"变体。我们确定了解决这一"一维"变体所面临的关键数学挑战。

关键词 形式幂级数、平方根和、朗斯基行列式、微分方程、直线程序。

2012 年 ACM 学科分类 计算理论 → 代数复杂性理论、计算数学 → 概率算法。

1 引言

对于许多需要确定实数表达式符号的判定问题，其复杂性类（例如，它们是否属于 P）通常是未知的。平方根和问题就是一个著名实例，可以描述如下：

问题 1 （平方根和问题（SSR））。 给定一个由正整数组成的列表（$a_1, a_2, \ldots\ldots, a_n$）以及（$\delta_1, \delta_2, \ldots\ldots, \delta_n$）$\in \{-1, 1\}^n$，判断 $\sum_{i=1}^{n} \delta_i \sqrt{a_i} > 0$ 是否成立。

根据 Garey、Graham 和 Johnson 的研究，这个问题的复杂度已得到广泛探讨，但仍未解决 [GGJ76]。此外，Malajovich 在 2001 [Mal01] 中提出，该问题可能属于 P。SSR 问题与欧几里得旅行商问题（ETSP）等经典几何问题有着深刻联系，而后者尚不确定是否属于 NP。显然，相对于 SSR 预言机，它属于 NP。另一个相关的重要问题是判定一个由直线程序编码的整数的符号，这就是所谓的 PosSLP 问题。若一个整数序列$P(b_0, b_1, b_2, \ldots, b_\ell)$ 满足$b_0 = 1$ 且对所有$1 \le i \le \ell$，都有$b_i = b^j \circ_i b_k$，其中 $\circ_i \in \{+, -, *\}$ 且j、$k < i$，则称该序列为直线程序（SLP）。我们称该 SLPP 计算出整数b_ℓ。我们称 ℓ 为该 SLPP的规模（或长度）。

* ´里昂高等师范学院。电子邮箱：louis.gaillard@ens-lyon.fr
†马克斯·普朗克软件系统研究所。电子邮箱：gjindal@mpi-sws.org

问题 2(PosSLP)。 给定一个 *SLP P*，判断 P 计算出的整数 n_P 是否为正 $e.$

将 $\sqrt{a_i}$ 在问题 1 中近似到适当精度，可将 SSR 归约为 PosSLP，正如 [ABKPM09] 所展示的。PosSLP 在该研究中被引入，旨在弥合经典计算模型与 Blum-Shub-Smale（BSS）模型 [BCSS97], 中的实数计算之间的差距。后者是数值分析中研究计算复杂性时广泛采用的一种模型。

文献 [ABKPM09] 证明，PosSLP 在多项式时间内通过多项式时间图灵归约刻画了 BSS 模型中可判定语言的“布尔部分”。此外，已证明 PosSLP 属于计数层次结构 CH，这意味着 SSR 也属于CH。迄今为止，这是已知的 SSR 复杂性最佳上界。

我们的贡献见第1.2节；此前，我们将在问题 1的第1.1节中介绍一些有用的既有研究。

1.1 相关工作

在不同的场景中，我们需要确定平方根和是否等于零，而不是确定该表达式的符号。因此，我们遇到了一个称为 SSR^{eq}的有趣问题。

问题 3 (SSR^{eq})。 给定一个整数列表（$a_1, a_2, \ldots\ldots$， a_n）以及（δ_1， δ_2，$\ldots\ldots$， δ_n）$\in \{-1, 1\}^n$，判断 $\sum_{i=1}^{n} \delta_i \sqrt{a_i} = 0$。

Bl ¨omer [Bl¨o91]提出了一种用于计算根式和的多项式时间算法，并证明 SSR^{eq} 属于 P。因此，检验带符号的平方根和是否为零似乎比判定其符号更容易。一个自然的 SSR 问题算法思路，是借助经典数值算法，用浮点数近似该平方根和。然而，需要关于近似所需精度位数的结果，以确保两个符号一致。已知（[Bre76]），对于位大小至多为B的整数，其平方根可以在时间 poly（B，m）内近似到m 精度位数。这意味着，若能解决下面的数论问题，就可以得到一个用于 SSR 问题的多项式时间算法。

问题 4 （非零平方根和的下界）。 给定一个和 $S = \sum_{i=1}^{n} \delta_i \sqrt{a_i}$，其中$\delta_i \in \{-1, 1\}$ 且 $1 \leq a_i < 2^B$，我们能否找到一个多项式 q（n，B），使得

$$S \neq 0 \implies |S| \geq \frac{1}{2^{q(n,B)}}?$$

与问题 4 相比，也可以尝试找到$_i$个 a 以及相应的 δ_i个，使得 $\sum_{i=1}^{n} \delta_i \sqrt{a_i}$ 的绝对值很小。在这一方向上， [QW06] 中证明了$\left|\sum_{i=0}^{m} ({}^{m}\mathrm{i})(-1)^i \sqrt{\mathrm{n} + \mathrm{i}}\right| = \mathrm{O}(\mathrm{n}^{-m+\frac{1}{2}})$。Kayal 和 Saha [KS12] 通过在多项式上提出一个相关问题来处理问题 4。这种方法证明更加简单。他们关注多项式平方根的非零和，并将其视为幂级数，证明了这类级数的赋值（或阶）不可能过高。

定理 *1*（多项式平方根之和的阶的界 [*KS*12]）。对于 $1 \leq i \leq n$，设 $c_i \in \mathbb{C}$ *and* f_i、$g_i \in \mathbb{C}[x]$ 的次数至多为 d，且 $f_i(0) \neq 0$。我们记并固定 $\sqrt{f_i(x)} \in \mathbb{C}[[x]]$ 为 $f_i(x)$ 的两个平方根之一。若平方根和 $S(x) = \sum_{i=1}^{n} c_i g_i(x) \sqrt{f_i(x)}$ 非零，则 $ord(S) \leq dn^2 + n$。

这项证明的主要技术论证是研究函数族$(g_i \sqrt{f_i})_{1 \leq i \leq n}$的朗斯基行列式，因为根据克拉默法则，可以很容易地用这个朗斯基行列式的阶来界定S 的阶。

接下来，他们将整数表示为多项式，并把这一结果应用于一组整数，从而确认问题 4 对于一类重要的整数子集——称为多项式整数——有肯定答案。

定理 2 (SSR，关于多项式整数 [KS12])。假设 $S = \sum_{i=1}^{n} \delta_i \sqrt{a_i}$ 非零，且满足 $\delta_i \in \{-1, 1\}$，使得每个正整数 a_i 都可表示为 $a_i = X^{d_i} + b_{1,i}X^{d_i-1} + \cdots + b_{d_i,i}$，其中 $d_i > 0$，X 为正整数，且 d_i、$b_{j,i}$ 均为整数。令 $B =$ 为 $\left(\{|b_{j,i}|\}_{j,i} \text{ 的最大值}, 1\right)$ 并令 $d =$ 为 $_i d_i$ 的最大值。存在两个固定的关于 n 和 d 的整系数多项式 $p(n, d)$、$q(n, d)$，使得若 $X \geq (B+1)^{p(n,d)}$，则 S 的下界为 $|S| \geq {}^{1}X^{q(n,d)}$。 ——

基于这些观察，一个问题随之而来：关于幂级数和的阶的界这一概念，能否推广到平方根以外的其他函数族？这或许能为判定涉及无理实数的表达式的正性所需的复杂度带来重要见解。

1.2 我们的结果

从现在起，$\mathbb{K}$ 表示一个特征为0的域。除非另有说明，本文中的所有对数均为以e为底的自然对数。现在我们定义一些量，以便正式陈述结果。

定义 1. 设 $\mathcal{F} \subseteq \mathbb{K}[[x]]$ 是一个有限维线性子空间。对于 $\mathbb{K}[[x]]$，，我们定义

$$\mathcal{O}(\mathcal{F}) := \sup\{\operatorname{ord}(f) \mid f \in \mathcal{F} \setminus \{0\}\} \in \mathbb{N} \cup \infty.$$

对于一族线性无关幂级数$\mathbf{f} = (f_1, f_2, \ldots, f_n)$，我们定义

$$\mathcal{O}(f_1, f_2, \ldots, f_n) = \mathcal{O}(\mathbf{f}) := \mathcal{O}(\operatorname{span}(f_1, f_2, \ldots, f_n)).$$

如果存在标量 $c_1, c_2, \ldots, c_n \in \mathbb{K}$（不全为零），使得 $\sum_{i=1}^{n} c_i f_i$ 为零，则称由 n 个函数构成的集合 $\{f_1, f_2, \ldots, f_n\}$ 在 $\mathbb{K}$ 上线性相关。为了定义 $\{f_1, f_2, \ldots, f_n\}$的朗斯基行列式，我们假设每个 f_i 均 $n-1$ 次可微。$\{f_1, f_2, \ldots, f_n\}$的朗斯基行列式记作 $W(f_1, f_2, \ldots, f_n)$，定义为下列矩阵的行列式：

$$W(\mathbf{f}) = W(f_1, f_2, \ldots, f_n) := \det \begin{pmatrix} f_1 & \cdots & f_n \\ f_1^{(1)} & \cdots & f_n^{(1)} \\ \vdots & \vdots & \vdots \\ f_1^{(n-1)} & \cdots & f_n^{(n-1)} \end{pmatrix}$$

命题 1. 设 $\mathcal{F} \subseteq \mathbb{K}[[x]]$ 是一个 n 维线性子空间。对于 $\mathcal{F}$ 的任意一组基 $(f_1, f_2, \ldots, f_n)$，阶$(W(f_1, f_2, \ldots, f_n))$ 不依赖于基 $(f_1, f_2, \ldots, f_n)$的选取。我们将这个量记为 $W_{\text{ord}}(\mathcal{F})$。

证明。 设 $(g_1, g_2, \ldots, g_n)$ 是 $\mathcal{F}$ 的另一组基。存在一个可逆的 $n \times n$ 矩阵 A，其元素属于 $\mathbb{K}$，使得

$$\begin{bmatrix} g_1 & \cdots & g_n \end{bmatrix} = \begin{bmatrix} f_1 & \cdots & f_n \end{bmatrix} \cdot A.$$

由微分的线性性可知，对于所有 $0 \leq j < n$，我们也有：

$$\begin{bmatrix} g_1^{(j)} & \cdots & g_n^{(j)} \end{bmatrix} = \begin{bmatrix} f_1^{(j)} & \cdots & f_n^{(j)} \end{bmatrix} \cdot A.$$

因此，我们有 $W(g_1, g_2, \ldots, g_n) = W(f_1, f_2, \ldots, f_n) \cdot \det(A)$。利用 $\det(A) \in \mathbb{K}^*$这一事实，即可得到结果。 □

以下定理用 $\mathcal{O}(\mathcal{F})$ 界定了其与 $W_{\text{ord}}(\mathcal{F})$的关系。该定理实际上是 Voorhoeve 和 Van der Poorten [VV75]的结果。Kayal 和 Saha [KS12]也采用了相同的思路来证明 定理 1中的界。

定理 3 （ [VV75]中的定理 1）。 设 $\mathcal{F}$ 是 $\mathbb{K}[[x]]$的 n 维线性子空间。那么，$\mathcal{O}(\mathcal{F}) \leq W_{\text{ord}}(\mathcal{F}) + n - 1$。

在 第 2 节中，我们证明了 定理 3 几乎是紧的，其含义是：一族 $(h_1, h_2, \ldots, h_n)$ 幂级数的朗斯基行列式的阶，与这些 h_i的非零线性组合的最大阶相差一个多项式因子。该结果在下文的 定理4中予以形式化。

定理 4。 设 $\mathcal{F}$是 $\mathbb{K}[[x]]$的 n 维线性子空间。那么，$W_{\text{ord}}(\mathcal{F}) \leq n \cdot \mathcal{O}(\mathcal{F}) - \binom{n}{2}$。

关于定理 4的完整证明，请参阅 第 2 节。随后，我们证明 Kayal 和 Saha 在 定理 1 中采用的方法可以扩展到具有多项式系数的 1 阶线性微分方程的解的和，从而得到关于该和的阶的相当界。该结果在下文的定理 5 中正式陈述。

定理 5. 设 $S(x) = \sum_{i=1}^{n} c_i g_i(x) y_i(x)$，其中 $y_i' - p_i q_i y_i = 0$，且 $c_i \in \mathbb{K}$ 和 g_i，p_i，$q_i \in \mathbb{K}[x]$ 的次数至多为 d。我们假设 $q_i(0) \neq 0$，并且每个 $y_i \in \mathbb{K}[[x]]$。若 $S \neq 0$，则

$$\operatorname{ord}(S) \leq \sum_{i=1}^{n} \operatorname{ord}(y_i) + n^2 d + n - 1.$$

定理 5 的证明思路 一旦我们利用定理 3 得到 S 的阶的界，便可推出该界；而要得到这一界，我们需要将函数族 $(g_i y_i)_{1 \leq i \leq n}$ 的朗斯基行列式的阶界定为 $\sum_i \operatorname{ord}(y_i) + n^2 d$。为此，我们研究朗斯基矩阵的各项，并利用微分方程将 y_i 的导数替换掉。我们证明，朗斯基矩阵的每个元素 (i, j) 都可写成 $y_i\, m_{i,j}\, q^{n-1}$ i 的形式，其中 q_i 是 y_i 所满足的微分方程中的分母，而 $m_{i,j}$ 是次数为 $\leq nd$ 的多项式。将多项式 $m_{i,j}$ 的阶用其次数界定，即可直接得到结论。定理 5 的完整证明见第 3 节。

在第 4 节中，我们研究以下问题 5 (SSR_{SLP})，它可以视为在 SLP 的背景下对问题 3(SSR^{eq}) 的推广。

问题 5 (SSR_{SLP})。 给定 n 个大小为 $\leq s$ 的直线程序$(P_1, P_2, \ldots, P_n)$ 以及$(\delta_1, \delta_2, \ldots, \delta_n) \in \{-1, 1\}^n$作为输入，其中 P_i 计算正整数 a_i，判断 $\sum_{i=1}^{n} \delta_i \sqrt{a_i} = 0$ 是否成立。

这里我们证明，假设 GRH，在随机多项式时间图灵归约下，SSR_{SLP} 可以归约为以下 SSR_{SLP} 的“一维”变体，

问题 6 (一维 SSR_{SLP})。 给定 n 个计算 n 个正整数的直线程序$(a_1, a_2, \ldots, a_n)$ 以及$(\delta_1, \delta_2, \ldots, \delta_n) \in \{-1, 1\}^n$，并承诺$\dim(\text{张成空间}_{\mathbb{Q}}(\sqrt{a_1}, \sqrt{a_2}, \ldots, \sqrt{a_n})) = 1$。判断 $\sum_{i=1}^{n} \delta_i \sqrt{a_i} = 0$ 是否成立。

将 SSR_{SLP} 归约为一维 SSR_{SLP} 的证明思路：给定一个 问题 5 实例，我们将输入分成若干个一维子群。这是可行的，因为我们利用 Kneser [Kne75] 的思想以及 Bl¨omer 在 [Bl¨o91] 中的工作，展示了一种高效的随机化算法，用于检验由 SLP 给出的整数的平方根是否线性相关。根据 Kneser 的结果 [Kne75], ，一组平方根在 $\mathbb{Q}$ 上线性相关，当且仅当该集合中存在一对线性相关的平方根。将 问题 5 的实例分成一维子群后，只需

确定每个子和是否为零，这可以通过使用 问题 6 的预言机来完成。完整的证明请参见第 4 节。

在第 5 节中，我们证明了一个与定理 1类似的上界，该定理涉及实多项式对数和的阶。

命题 2. 令 $S(x) = \sum_{i=1}^{n} c_i \log(f_i(x)) \neq 0$，其中 $c_i \in \mathbb{R}$，$f_i \in \mathbb{R}[x]$ 的次数至多为 d，且 $f_i(0) > 0$。那么$\operatorname{ord}(S) \leq nd$。

我们还证明了一个与定理 2 类似的结果，不过研究的是整数对数线性形式的正性检验问题，其复杂度与数论中的深层猜想相关 [ESY14], , 例如 Baker 提出的 *abc* 猜想的一个强化版本 [Bak98]。这一结果基本上可由下文的定理 6推出，它是我们对定理 2的类比。关于定理 6的完整证明，请参见第 5 节。

定理 6（多项式整数的对数和）。设 $E = \sum_{i=1}^{n} c_i \log a_i$ 非零，其中 $c_i \in \mathbb{Z}$，且每个 a_i 都是形如 $a_i = X^{d_i} + b_{1,i}X^{d_i-1} + \cdots + b_{d_i,i}$ 的正整数，其中 $d_i > 0$，X 是正整数且 d_i，$b_{j,i}$ 为整数。令 $B = \max\left(\{|b_{j,i}|\}_{j,i}, 1\right)$，$d = \max_i d_i + 1$，且 $C = \max_i |c_i|$。存在两个固定的整系数多项式 $p_1(n, d)$、$p_2(n, d)$，它们关于 n 和 d，使得若 $X > \max\left(C^2, (B+1)^{p_1(n,d)}\right)$，则 E 有下界 $|E| \geq {}^{1}X^{p_2(n,d)}$。

2 朗斯基行列式的阶

在本节中，我们将证明，对于一个幂级数族，非零线性组合中可能出现的最大阶，等于该族朗斯基行列式的阶乘以一个多项式因子。我们对定理 4 的证明受到以下文献中相关思想的启发： [BD10]。对于d，$k \in \mathbb{N}$，我们记作

$$(d)_k := d(d-1)\dots(d-k+1),$$

约定为 $(d)_0 = 1$。

定义 2 （范德蒙行列式）。 设 $(d_1, d_2, \dots, d_n) \in \mathbb{K}^n$，我们定义相应的范德蒙行列式如下：

$$V(d_1, d_2, \dots, d_n) := \det\left((d_j^{i-1})_{1\leq i,j\leq n}\right) = \prod_{1\leq i<j\leq n} (d_j - d_i).$$

引理 7（单项式的朗斯基行列式， [BD10]中的引理 1）。 单项式 $a_1x^{d_1}$，…，$a_nx^{d_n}$ 的朗斯基行列式为

$$W(a_1x^{d_1}, \dots, a_nx^{d_n}) = V(d_1, d_2, \dots, d_n)\left(\prod_{i=1}^{n} a_i\right) x^{d_1+\cdots+d_n-\binom{n}{2}}.$$

引理 8 （ [BD10]中的引理 2）。 设 $f_1, f_2, \dots, f_n$ 是一个由 $\mathbb{K}[[x]]$ 组成的族，并且在 $\mathbb{K}$上是线性无关的。存在一个可逆的 $n \times n$ 矩阵 A，其元素属于 $\mathbb{K}$，使得由幂级数 $g_1, g_2, \dots, g_n$ 定义为

$$\begin{bmatrix} g_1 & \dots & g_n \end{bmatrix} = \begin{bmatrix} f_1 & \dots & f_n \end{bmatrix} \cdot A \tag{1}$$

均非零，且阶互不相同。

引理 9（不同阶幂级数的朗斯基行列式）。若非零幂级数 $g_1, g_2, \ldots, g_n \in \mathbb{K}[[x]]$ 的阶 $d_1, d_2, \ldots, d_n$ 互不相同，则它们的朗斯基行列式 $W(g_1, g_2, \ldots, g_n)$ 非零，且满足：

$$\operatorname{ord}(W(g_1, g_2, \ldots, g_n)) = \sum_{i=1}^{n} d_i - \binom{n}{2}.$$

证明。若 g_j 是单项式，即 $g_j = a_j x^{d_j}$，则结论可直接由引理 7 得出，此时朗斯基矩阵的第 (i, j) 个元素为 $w_{i,j} = a_j (d_j)_{i-1} x^{d_j - i + 1}$。一般情况下，令 $g_j = a_j x^{d_j} + u_j$，其中 $u_j \in \mathbb{K}[[x]]$ 的阶为 $> d_j$。那么朗斯基矩阵的第 (i, j) 个元素变为 $w_{i,j} \times (1 + x r_{i,j})$，其中 $r_{i,j} \in \mathbb{K}[[x]]$。

因此，我们有 $W(g_1, g_2, \ldots, g_n) = a_1 \ldots a_n x^{d_1 + \cdots + d_n - \binom{n}{2}} \det(D)$，其中 D 是一个 $n \times n$ 矩阵 $D = ((d_j)_{i-1}(1 + x r_{i,j}))_{1 \le i,j \le n}$。现在将 D 在 $x = 0$ 处取值，得到 $D(0) = ((d_j)_{i-1})_{1 \le i,j \le n}$。如引理 7 的证明 [BD10]，中所示，通过初等行变换（该变换保持行列式不变），我们可以将 D(0) 化为与 $d_1, \ldots, d_n$ 相关联的范德蒙德矩阵。因此，$\det(D(0)) = V(d_1, d_2, \ldots, d_n) \neq 0$，因为 d_i 彼此不同。于是 det(D) 模 x 非零，因此 det D 的阶为零，结论得证。 □

现在我们提出定理 4 的一个紧确变体（定理 10），它立即蕴含定理 4。设 $\mathcal{F} \subseteq \mathbb{K}[[x]]$ 是 $\mathbb{K}[[x]]$的有限维子空间。引理 8 表明，如果 $\dim(\mathcal{F}) = n$，那么存在 n 个幂级数 $g_1, g_2, \ldots, g_n$ 属于 $\mathcal{F}$，它们的阶 $d_1, d_2, \ldots, d_n$ 各不相同。此外，$g_1, g_2, \ldots, g_n$ 也构成 $\mathcal{F}$ 的一组基。现在我们断言，任何属于 $\mathcal{F}$ 的幂级数，其阶只能是这些阶。假设 $d_1 < d_2 < \cdots < d_n$。如果 $f = \sum_{i=1}^{n} \lambda_i g_i$（其中 $\lambda_i \in \mathbb{K}$）是 $\mathcal{F}$ 中的一个非零幂级数，那么显然 $\operatorname{ord}(f) = d_j$，其中 j 是满足 $\lambda_j \neq 0$ 的最小指标。基于这一断言，我们提出定理 4 的以下紧确变体。

定理 10。设 $\mathcal{F}$ 是 $\mathbb{K}[[x]]$ 的 n 维线性子空间。假设 $d_1, d_2, \ldots\ldots d_n$ 是 $\mathcal{F}$ 中出现的幂级数的不同阶数。那么，$W_{\text{ord}}(\mathcal{F}) = \sum_{i=1}^{n} d_i - \binom{n}{2}$。

证明。根据引理 8，存在一个基 $(g_1, g_2, \ldots\ldots, g_n)$，其属于 $\mathcal{F}$，且具有不同的阶 $d_1, d_2, \ldots\ldots, d_n$。利用引理 9，$W_{\text{ord}}(\mathcal{F}) = \sum_{i=1}^{n} d_i - \binom{n}{2}$。 □

定理 4。设 $\mathcal{F}$ 是 $\mathbb{K}[[x]]$ 的 n 维线性子空间。那么，$W_{\text{ord}}(\mathcal{F}) \le n \cdot \mathcal{O}(\mathcal{F}) - \binom{n}{2}$.

证明。该结论立即由定理 10得出。 □

这就完成了定理 4的证明。结合定理 4 和定理 3，我们得出结论：朗斯基行列式的阶决定了幂级数线性组合的最大阶数，其精度相差一个关于n的多项式因子。

现在我们展示一个例子，其中定理 3 中给出的界是紧的。设 $\mathcal{G}$ 是由单项式 1、x、$x^2, \ldots$、x^{n-1}生成的 $\mathbb{K}[[x]]$ 的线性子空间。很容易看出，1、x、$x^2, \ldots$、x^{n-1} 的朗斯基行列式为 $\prod^{n-1} {}_{i=1}\, i!$。因此 $W_{\text{ord}}(\mathcal{G}) = 0$。我们还得到 $\mathcal{O}(\mathcal{G}) = n - 1$。

线性微分方程解的 3 个和

作为定理 1 的推广，并作为定理 3的一个应用，我们现在证明：对于由次数为 1 且多项式系数的线性微分方程的解所组成的幂级数之和，其阶存在一个多项式界。

定理 5。 设 $S(x)=\sum_{i=1}^{n} c_i g_i(x) y_i(x)$，其中 $y_i' - p_i q_i y_i = 0$，且 $c_i \in \mathbb{K}$ 和 g_i， p_i， $q_i \in \mathbb{K}[x]$ 的次数至多为 d。我们假设 $q_i(0) \neq 0$，并且每个 $y_i \in \mathbb{K}[[x]]$。若 $S \neq 0$，则

$$\operatorname{ord}(S) \leq \sum_{i=1}^{n} \operatorname{ord}(y_i) + n^2 d + n - 1.$$

证明。 令$h_i = g_i y_i$。 不失一般性，假设$\mathbf{h} = (h_1, h_2, \ldots, h_n)$ 线性无关。若它们不线性无关，则可将S 重写为h_i中某个线性无关子族的线性组合。

我们将朗斯基行列式的阶 $W(h_1, h_2, \ldots, h_n)$ 的上界，并应用定理 3。我们有 e:

$$y_i' = \frac{p_i}{q_i} y_i,$$
$$y_i'' = \frac{p_i' q_i - p_i q_i'}{q_i^2} y_i + \frac{p_i}{q_i} y_i' = \frac{p_i' q_i - p_i q_i' + p_i q_i}{q_i^2} y_i.$$

因此，由归纳法可得，对 $0 \leq j < n$，

$$y_i^{(j)} = \frac{P_{i,j}}{q_i^j} y_i = \frac{q_i^{n-1-j} P_{i,j}}{q_i^{n-1}} y_i,$$

其中$q^{n-1-j}{}_i P_{i,j}$ 是一个次数至多为$(n-1)d$的多项式。然后，根据莱布尼茨公式，$h^{(j)}{}_i = \sum^{j}{}_{k=0} \binom{j}{k} g^{(j-k)}{}_i y^{(j)}{}_i$，朗斯基行列式的形式为

$$W(h_1, h_2, \ldots, h_n) = \prod_{i=1}^{n} \frac{y_i}{q_i^{n-1}} \det M,$$

其中M 是一个矩阵，其元素都是次数至多为nd的多项式。特别地，$\operatorname{ord}(\det M) \leq \deg(\det M) \leq n^2 d$。由于$q_i(0) \neq 0$ 对所有i都成立，因此：

$$\operatorname{ord}(W(\mathbf{h})) = \sum_{i=1}^{n} \operatorname{ord}(y_i) + \operatorname{ord}(\det M) \leq \sum_{i=1}^{n} \operatorname{ord}(y_i) + n^2 d.$$

最后，定理 3 推出了所声称的上界。 □

作为定理 5的直接推论，我们在 $\mathbb{C}[[x]]$ 的若干不同情形下，得到了幂级数之和的阶的上界。

推论 1。 设 $S(x)=\sum_{i=1}^{n} c_i g_i(x) y_i(x)$ 为一个非零和，其中 $c_i \in \mathbb{C}$ 和 $g_i \in \mathbb{C}[x]$ 的次数至多为 d。设 $f_i \in \mathbb{C}[x]$ 的次数至多为 d。

(i) 若 $y_i = \exp(f_i)$，则 S 的阶 $\leq n^2(d-1) + n - 1$。

(ii) 若 $y_i = \varphi(f_i)$ 中含有 $\alpha_i \varphi \in$ {双曲余弦、双曲正弦、余弦、正弦}，则 S 的阶 $\leq 4n^2(d-1) + 2n - 1$。

(iii) 若 $y_i = \left(\underline{p_i^{\,i}}\right) q$，其中 p_i、$q_i \in \mathbb{C}[x]$ 的次数至多为 d， $\alpha_i \in \mathbb{R}$ 且 $p_i(0)$、$q_i(0) \neq 0$，则S 的阶 $\leq 2n^2 d + n - 1$。

证明。对于第 (i) 部分，$y_i = \exp(f_i)$，y_i具有幂级数展开，并且 $\operatorname{ord} y_i = 0$，因为 $y_i(0) = \exp f_i(0) \neq 0$。此外，$y_i' - f_i' y_i = 0$，其中 $\deg f_i' \leq d - 1$。根据定理 5，$\operatorname{ord} S \leq n^2(d-1) + n - 1$。

对于第 (ii) 部分，可以写成余弦双曲线 $f = \frac{e^f + e^{-f}}{2}$、双曲正弦 $f = \frac{e^f - e^{-f}}{2}$、余弦 $f = \frac{e^{if} + e^{-if}}{2}$，以及正弦 $f = \frac{e^{if} - e^{-if}}{2i}$。然后，我们可以对和式中的 $2n$ 项应用第 (i) 部分，从而得到所述界。

对于第 (iii) 部分，由于对于所有 i，$p_i(0)$ 和 $q_i(0)$ 都非零，y_i 在 0 处具有幂级数展开，且 $\operatorname{ord} y_i = 0$。此外，它满足 $y_i' - \alpha_i \frac{p_i' q_i - p_i q_i'}{p_i q_i} y_i = 0$。同样，该界可通过使用 定理5获得。

□

对于$y_i = \exp f_i$，类似的界已经在 [VV75] 中得到证明（见例 1）。证明同样依赖于朗斯基行列式。

4 S直线程序给出的整数平方根之和 s

正如我们在引言中提到的，判断一个涉及平方根的表达式是否为零是一个有趣的问题，而 Bl ¨ omer [Bl¨o91]开发了一种用于求解 SSR 的多项式时间算法eq。在 SSReq中，输入的整数以二进制给出，在这种情况下，该问题很容易。SSReq 的一个自然延伸是考察在代数计算模型下这个问题的复杂度会如何变化，也就是说，输入的整数由直线程序给出时的情况。更确切地说，我们希望研究问题 5。

我们想知道，对这一类表达式进行零测试，是否与判断计算整数的直线程序是否输出零一样简单，也就是 [ABKPM09] 中定义的 EquSLP 问题。对于 EquSLP 问题，给定一个输入 SLP P，我们要测试 P 计算出的整数 n_P 是否为零。 [ABKPM09], 证明了 EquSLP 可归约为多项式恒等式检验（PIT），因此存在随机多项式时间算法。为了设计一个用于 $\mathrm{SSR}_{\mathrm{SLP}}$ 的随机多项式时间算法，本节将介绍如何在问题 5 的背景下，将 Bl¨omer 的一些思路用于 SSReq 。我们证明，在广义黎曼猜想（GRH）成立的条件下，问题 $\mathrm{SSR}_{\mathrm{SLP}}$ 可归约到一维情形，其中涉及的所有平方根都位于 $\mathbb{Q}$ 上的同一条直线上。事实上，这个特殊的一维情形涵盖了整个问题的所有难点。 [Bl¨o98、BNSW22] 中也有相关结果。这些工作给出了随机化算法，用于判断涉及深度为 1 的根式的表达式是否等于 0。 [BNSW22], 中的一些算法在 GRH 成立的条件下同样适用，并采用了与本节类似的论证，研究某些素数的密度。不过，这些结果中涉及的表达式有所不同：它们不只是平方根之和，而是一般的算术电路，其中包含以二进制给出的整数的平方根。

4.1 归约到一维情形

现在，我们正式解释为什么为了设计 *SSR* 的高效算法，只需关注 问题 5 的一维（问题 6）版本。实际上，我们将证明 定理 11。SLP

定理 11。 *在 GRH 下，存在一个从 问题 5 到 问题 6 的随机化多项式时间图灵归约。*

出发点是 Kneser 的以下结果 [Kne75]，由 Bl¨omer（[Bl¨o91],推论 2.6）重新表述。

引理 12。 *设 $a_1, a_2, \ldots, a_n$ 为 n 个正整数。实数 $\sqrt{a_1}, \sqrt{a_2}, \ldots, \sqrt{a_n}$ 当且仅当存在 $1 \le i < j \le n$，使得 $(\sqrt{a_i}, \sqrt{a_j})$ 在 $\mathbb{Q}$ 上线性相关，或者等价地*

$$\frac{\sqrt{a_i}}{\sqrt{a_j}} \in \mathbb{Q}. \tag{2}$$

推论 2。 *设 $a_1, \ldots, a_n$ 为正整数，且 $(\delta_1, \ldots, \delta_n) \in \{-1, 1\}^n$。设 $(\sqrt{a_{i_1}}, \ldots, \sqrt{a_{i_\ell}})$ 是张成空间$\mathbb{Q}$ $(\sqrt{a_1}, \ldots, \sqrt{a_i})$ 的一个基。那么对于所有 $1 \le i \le n$，存在唯一的 $1 \le j \le \ell$ 使得$\sqrt{a_i} \in \mathbb{Q} \cdot \sqrt{a_{i_j}}$。并且*

$$\sum_{i=1}^{n} \delta_i \sqrt{a_i} = 0 \iff \forall 1 \le j \le \ell, \sum_{i:\, \sqrt{a_i} \in \mathbb{Q} \sqrt{a_{i_j}}} \delta_i \sqrt{a_i} = 0. \tag{3}$$

证明。 不失一般性，我们可以假设$ij = j$。假设存在性成立，唯一性显然，因为如果 $\sqrt{a_i} \in \mathbb{Q} \cdot \sqrt{a_j}$ 和 $\sqrt{a_i} \in \mathbb{Q} \cdot \sqrt{a_{j'}}$，那么 $\sqrt{a_j}$ 和 $\sqrt{a_{j'}}$ 并非线性

无关。现在，对于基中的元素，存在性显然；对于 $\sqrt{a_i}$ 不在基中的，$(\sqrt{a_1},\ldots,\sqrt{a_\ell},\sqrt{a_i})$ 则线性相关。由引理 12可知，两个元素线性相关，且这两个元素不可能都属于基。因此a_i 必定属于这一对元素。

我们将 $\{1,\ldots,n\}=I_1\cup\cdots\cup I_\ell$ 划分，其中 $I_j=\{i|\ \sqrt{a_i}=q_{i,j}\sqrt{a_j},q_{i,j}\in\mathbb{Q}\}$。现在，$\sum_{i=1}^{n}\delta_i\sqrt{a_i}=\sum_{j=1}^{\ell}\left(\sum_{i\in I_j}\delta_i q_{i,j}\right)\sqrt{a_j}$。由于$(\sqrt{a_j})_{1\le j\le\ell}$ 构成一个基，前一个和为零，当且仅当对于所有 $1\le j\le\ell,\sum_{i\in I_j}\delta_i q_{i,j}=0$ 都成立。将等式两边乘以 $\sqrt{a_j}$，得到

$$\sum_{i=1}^{n}\delta_i\sqrt{a_i}=0\iff\forall 1\le j\le\ell,\sum_{i\in I_j}\delta_i\sqrt{a_i}=0.$$

□

关于定理 11 的归约分为两步，详见算法 1。给定一个问题 5的实例，我们首先构造集合中平方根的 ℓ一维子集划分，然后使用问题 6的预言机来检验每个相关子和是否为零。为构造该划分，算法 1 的步骤如下：对于每个整数a_i，要么我们已经见过某个整数a_j，使得 $\sqrt{a_i}/\sqrt{a_j}\in\mathbb{Q}$，于是将$a_i$ 与a_j 放入同一个一维和中；要么我们为a_i构造一个新的划分。为了完成定理 11的证明，只需说明在 GRH 条件下，可以高效地执行方程（2）的检验。

输入：$a_1,a_2,\ldots\ldots,a_n$ 由 SLP 表示的整数，符号为 δ_1、δ_2、……、$\delta_n\in\{-1,1\}$。
输出：判断$S=\sum_{i=1}^{n}\delta_i\sqrt{a_i}=0$。
子和集合 ← [ ] ;
对于 $1\le i\le n$ **执行**
  $k\leftarrow 0$；找到子和 ← 假；
  当 $k<|$子和集合$|$ 且不 FoundSubSum**时**
    在子和集合$[k]$ 中选择一个元素b ;
    如果 $\sqrt{a_i}/\sqrt{b}\in\mathbb{Q}$**那么**
      将a_i 加入子和集合$[k]$; 将 FoundSubSum ← 设为 true;
    else
      k++;
    end
  end
  如果 not FoundSubSum**则** 将 $\{a_i\}$ 加入子和集合;
end
对于子和集合中的每个元素，检验相应的一维和是否为零
使用预言机求解问题 6;

算法 1：问题 5 的算法

引理 13. 设 a,b 为两个正整数。$\sqrt{a}\sqrt{b}\in\mathbb{Q}$ 当且仅当 $\sqrt{ab}\in\mathbb{N}$。

证明。$\sqrt{a}/\sqrt{b}\in\mathbb{Q}$ 等价于以下陈述：对于任意素数 p，a/b 的 p 进赋值 $v_p(a/b)$ 为偶数，即 $v_p(a/b)=v_p(a)-v_p(b)$，或者等价地，$v_p(a)+v_p(b)=v_p(ab)$ 为偶数，也就是说 $\sqrt{ab}\in\mathbb{N}$。□

引理 13 表明，要检验 方程（2），我们只需检查 a_ia_j 是否为完全平方数。注意，如果 a_i 和 a_j 都可以由大小为 s 的 SLP 表示，那么 a_ia_j 具有一个大小为 $2s+1$的 SLP。下一节中，我们将在 GRH 条件下设计一种随机多项式时间算法来执行此任务。

4.2 检验 SLP 是否计算出完全平方数

现在我们针对以下问题 7给出一种算法。

问题 7. 给定一个大小为 t、计算正整数 a 的 *SLP*，判断 a 是否为完全平方数。

设 a 是由大小为 t 的 SLP 计算出的正整数。对 $t \geq 0$ 使用归纳法，可得界 $a \leq 2^{2^t}$。

我们的算法如下：随机选取一个素数 $\mathrm{p} \leq 2^{q(t)}$，其中 q 是稍后确定的多项式；计算 a mod p，并检验 a mod p 是否为 $\mathbb{F}_p$ 中的平方数。所有这些计算都可以在关于 t [BS96] 的多项式时间内完成。如果 a 实际上是完全平方数，那么对于所有这样的素数 p，a mod p 都是 $\mathbb{F}_p$ 中的平方数，算法的答案正确。相反，如果 a 不是完全平方数，切博塔廖夫密度定理保证，使多项式 $\mathrm{X}^2 - \mathrm{a}$ 在 $\mathbb{F}_p$ 中分裂的素数 p 集合，也就是 a 在 $\mathbb{F}_p$ 中为平方数的素数 p 集合，其密度为 $\frac{1}{2}$ [SL96]。为了确保我们能使用较小的素数，同时保持得到正确答案的概率不至于过低，我们需要一个有效版本。切博塔廖夫密度定理的这个有效版本需要 GRH，见 [Ser81]（定理 4）。

我们对有效切博塔廖夫密度定理的应用导出了以下关键引理。对于 $X^2 - a$ 的分裂域，该结论可直接由 [Ser81]（定理 4）得出。只有当 $\mathrm{disc}(X^2 - a) = 4a$ 在 $\mathbb{F}_p$ 中不为零时，这才有意义。这就是我们只考虑不整除 $4a$ 的素数 p 的原因。

引理 14. 设 a 为一个非完全平方数的正整数。对于 $x \geq 2$，我们定义：

$$d_a(x) := \frac{|\{p \text{ prime } \leq x, a \text{ is not a square mod } p \text{ and } p \nmid 4a\}|}{|\{p \text{ prime } \leq x\}|}.$$

存在一个常数 C，使得在 *GRH* 成立的条件下，对于所有 $x \geq 2$，

$$\left| d_a(x) - \frac{1}{2} \right| \leq C \frac{\log_2 x}{\sqrt{x}} \left(\log_2(4a) + 2\log_2 x \right).$$

现在我们可以陈述主要引理。

引理 15. 设 $a \leq 2^{2^t}$ 为一个非完全平方数的正整数。那么存在一个整系数多项式 q，使得对于 $x = 2^{q(t)}$，有 $d_a(x) \geq \frac{1}{4}$。

证明. 根据 引理 14，有以下不等式成立：

$$d_a(x) \geq \frac{1}{2} - C \frac{\log_2 x}{\sqrt{x}} (\log_2(4a) + 2\log_2 x).$$

总之，我们需要确保

$$C \frac{\log_2 x}{\sqrt{x}} (\log_2(4a) + 2\log_2 x) \leq \frac{1}{4}, i.e.,$$

$$\log_2(4a) \leq \frac{1}{4} \frac{\sqrt{x}}{C \log_2 x} - 2\log_2 x.$$

当 $a \leq 2^{2^t}$ 且 $x = 2^{q(t)}$ 时，只需满足

$$2^t + 2 \leq \frac{1}{4} \frac{2^{\frac{q(t)}{2}}}{Cq(t)} - 2q(t). \tag{4}$$

并且可以看出，$q(t) = O(t^2)$ 满足方程（4）。 □

如果选择$q(t)$ 如引理 15所示，我们的随机化算法可在多项式时间内运行，并且在求解问题 7 时具有单边错误。这就完成了定理 11 的证明。

4.3 关于一维变体

在上一节中，我们证明了只需关注问题 6。假设 span$_{\mathbb{Q}}(\sqrt{a1},$ $\sqrt{2},$ $\sqrt{n}) = \mathbb{Q}\cdot\sqrt{1}$ $\sqrt{i\ 1} \in \mathbb{N}$ $= \sum_{i=1}^{n}\delta_i\sqrt{i} = 0 \iff \sqrt{1} = a\ldots, a) a$。那么，对所有 i，a a。并且 S a S a$\sum_{i=1}^{n}\delta_i\sqrt{a_i}a_1 = 0$，其中 S$\sqrt{a_1} \in \mathbb{N}$。设计一种算法来检验 S$\sqrt{a_1} = 0$ 的一种方法，是对随机选取的素数 p 取模。这种方法的问题在于，一旦将 $a_i a_1$ 对 p 取模，就可以在 $\mathbb{F}_p$ 中求出它的两个平方根，但无法判断这两个根中哪一个才是 $\sqrt{a_1 a_i}$ 在 $\mathbb{F}_p$中的正确表示。要确定 S$\sqrt{a_1}$ 对 p 取模后的正确结果，似乎并非易事。为解决问题 6，我们很可能需要采用另一种方法。

5 对数和的一个应用

为了说明证明某些幂级数的阶的下界为何值得关注，我们展示 Kayal 和 Saha 的方法 [KS12]不仅能够为平方根和问题导出一个非平凡结论，也可用于为其他基本数论问题建立非平凡结论。本节特别关注对数和，这是一个研究较为充分的问题 [Bak98，ESY14] 并且与深刻的数论猜想有关。

P问题 8。给定两个整数列表（$a_1, a_2, \ldots\ldots, a_n$）、（$c_1, c_2, \ldots\ldots, c_n$），其中 $a_i > 0$，判断 *if*

$$\sum_{i=1}^{n} c_i \log a_i > 0.$$

与平方根和问题（问题 1）类似，问题 8在位模型下的复杂度仍是一个开放问题。Baker 提出的*abc*-猜想的一个强化形式 [BW93] 将意味着问题 8属于P。关于问题 8的复杂度与数论中的开放问题之间联系的有趣细节，可参见 [ESY14]。所有这些猜想本质上都断言存在一个间隔，即非零对数和不可能过于接近零。这些间隔或下界与问题 4非常相似，只不过这里讨论的是对数。我们的目标是利用多项式与整数之间的类比，通过实多项式的非零对数和的阶的下界，为问题 8的一类非平凡实例推导下界。

命题 2. 设 $S(x) = \sum_{i=1}^{n} c_i \log(f_i(x)) \neq 0$，其中 $c_i \in \mathbb{R}$，$f_i \in \mathbb{R}[x]$ 的次数至多为 d，且 $f_i(0) > 0$。则ord$(S) \leq nd$。

证明. 首先，如果 $f_i(0) > 0$，幂级数 $\log f_i(x)$ 在 0 的某个邻域内有定义。因此，S存在有效幂级数展开。现在，我们有

$$S'(x) = \sum_{i=1}^{n} c_i \frac{f_i'(x)}{f_i(x)} = \frac{\sum_{i=1}^{n} c_i F_i(x)}{\prod_{i=1}^{n} f_i(x)},$$

其中 $F_i(x) = f_i'(x)\prod_{j\neq i} f_j(x)$ 是一个次数为 $\leq (n-1)d + d - 1 = nd - 1$ 的多项式。由于 $f_i(0) \neq 0$，我们有：

$$\text{ord}(S') = \text{ord}\left(\sum_{i=1}^{n} c_i F_i(x)\right) \leq \deg\left(\sum_{i=1}^{n} c_i F_i(x)\right) \leq nd - 1.$$

最后，

$$\text{ord}(S) \leq \text{ord}(S') + 1 \leq nd.$$

□

现在，我们可以将命题 2应用于整数，并为一类受限但非平凡的问题 8实例得到以下间隔定理。

定理 6（多项式整数的对数和）。设 $E = \sum_{i=1}^{n} c_i \log a_i$ 不为零，其中 $c_i \in \mathbb{Z}$，且每个 a_i 都是形如 $a_i = X^{d_i} + b_{1,i}X^{d_i-1} + \cdots + b_{d_i,i}$ 的正整数，其中 $d_i > 0$，X 为正整数，且 d_i、b_j、$_i$ 为整数。令 $B = \max\left(\{|b_j、_i|\}_{j,i、} 1\right)$，$d = \max_i d_i + 1$，并令 $C = \max_i |c_i|$。存在两个关于 n 和 d 的固定整系数多项式 $p_1(n,d)$、$p_2(n,d)$，使得当 $X > \max\left(C^2, (B+1)^{p_1(n,d)}\right)$ 时，E 的下界为 $|E| \geq \frac{1}{X^{p_2(n,d)}}$。

证明。 我们任取满足以下条件的整系数多项式p_1,p_2，并证明它们满足所声称的上界：

$$p_1(n,d) \geq 20dn\log(dn), \tag{5}$$
$$p_2(n,d) \geq 1 + dn(\log(dn)+1). \tag{6}$$

可以将E 写成如下形式：

$$E = \underbrace{\sum_{i=1}^{n} c_i d_i \log X}_{=A} + \underbrace{\sum_{i=1}^{n} c_i \log\left(1 + \frac{b_{1,i}}{X} + \cdots + \frac{b_{d_i,i}}{X^{d_i}}\right)}_{=S}.$$

若 $A \neq 0$，由于 $\sum_{i=1}^{n} c_i d_i$ 是非零整数，则有

$$|A| \geq \log X.$$

因此，只需证明S 具有 $|S| \leq \frac{1}{2}\log X$ 形式的上界，即可证明 $|E| \geq \frac{1}{2}\log X$。而我们有以下上界

$$|S| \leq nC \max_{1\leq i\leq n} \log\left(1 + \frac{b_{1,i}}{X} + \cdots + \frac{b_{d_i,i}}{X^{d_i}}\right).$$

现在，由于当 $\forall x \geq 0$时，$\log(1+x) \leq x$，且$\frac{b_{1,i}}{X} + \cdots + \frac{b_{d_i,i}}{X^{d_i}} \leq \frac{B}{X-1}$，我们有

$$|S| \leq nC\frac{B}{X-1}.$$

但是，由于$C \leq X^{\frac{1}{2}}$ -

$$|S| \leq nC\frac{B}{X-1} \leq \frac{nBX^{\frac{1}{2}}}{X-1} \leq \frac{2nB}{X^{\frac{1}{2}}} \leq \frac{2nB}{(B+1)^{\frac{1}{2}p_1(n,d)}},$$

因为 $X - 1 \geq X$ 2,- 因为 $X \geq 2$。因此，要使 $|S| \leq \frac{1}{2}\log X$，只需满足：

$$p_1(n,d)\log(B+1)(B+1)^{\frac{1}{2}p_1(n,d)} - 4nB \geq 0. \tag{7}$$

利用方程（7）和方程（5）可以很容易地验证，因此，$|E| \geq \frac{1}{2}\log X \geq \frac{1}{X^{p_2(n,d)}}$。**如果 $A = 0$**，我们证明 $|E| = |S| \geq \frac{1}{X^{p_2(n,d)}}$。令$y = \frac{1}{X}$，则有

$$S = \sum_{i=1}^{n} c_i \underbrace{\log\left(1 + b_{1,i}y + \cdots + b_{d_i,i}y^{d_i}\right)}_{=h_i(y)} = \sum_{j\geq 1} y^j \underbrace{\sum_{i=1}^{n} c_i h_{i,j}}_{S_j}$$

$$\text{with } h_i(y) = \sum_{j=1}^{\infty} h_{i,j}y^j = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k}\left(b_{1,i}y + \cdots + b_{d_i,i}y^{d_i}\right)^k.$$

应用命题 2，最小指数 ℓ 使得 $S_\ell \neq 0$ 满足 $\ell \leq dn$。证明的思路是证明对于每个 $t \geq 1$,

$$\frac{|S_{\ell+t}|}{|S_\ell|} \leq \frac{1}{2^{t+1}}, \tag{8}$$

因为在这种情况下，我们会有

$$|S| \geq ||S_\ell| - |S_{\ell+1}| - \dots| \geq \left||S_\ell| - \frac{1}{2}|S_\ell|\right| = \frac{1}{2}|S_\ell|, \tag{9}$$

并且可以通过 $|S|$ 的下界得到 $|S_\ell|$ 的下界。但为了满足方程（8），还需要对$S_{\ell+t}$ 的每个t给出上界。

这两个下界和上界都可以按照定理 2 在 [KS12]中的证明方式得到。技术细节见第 5.1 节。最后，我们证明对p_1 和p_2 的条件（方程（5）和（6））足以满足方程（8）和（9），进而推出 $|E| = |S| \geq \quad {}^{1}\underline{X^{p_2(n,d)}}$。

□

用于证明定理 6的 5.1 下界

我们回顾一下已有的

$$S = \sum_{i=1}^{n} c_i \underbrace{\log\left(1 + b_{1,i}y + \dots + b_{d_i,i}y^{d_i}\right)}_{=h_i(y)} = \sum_{j\geq 1} \underbrace{y^j \sum_{i=1}^{n} c_i h_{i,j}}_{S_j}$$

$$\text{with } h_i(y) = \sum_{j=1}^{\infty} h_{i,j}y^j = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k}\left(b_{1,i}y + \dots + b_{d_i,i}y^{d_i}\right)^k.$$

目标是证明，满足$p_1(n,d)$ 和$p_2(n,d)$ 的方程（5）和（6）的条件，可以为S_j 给出一个上界和一个下界，从而使我们能够满足方程（8）。

S_j的上界：

对于任意j，$h_{i,j}$ 由和式中阶为j 的项 $\sum (-1)^{k+1} k\left(b_{1,i}y + \dots + b_{d_i,i}y^{d_i}\right)^k$ 对k 取值范围为 $[1, j]$时贡献。于是

$$h_{i,j} = \sum_{k=1}^{j} \frac{(-1)^{k+1}}{k} v_{k,i,j}, \text{ with}$$

$$v_{k,i,j} = \sum_{\substack{k_1+2k_2+\dots+d_ik_{d_i}=j \\ k_1+k_2+\dots+k_{d_i}=k}} \binom{k}{k_1, k_2, \dots, k_{d_i}} b_{1,i}^{k_1} \dots b_{d_i,i}^{k_{d_i}}.$$

其中 $k_1, k_2, \dots, k_{d_i}$ 为非负整数。注意，对于$k < j\, d_i$，$v_{k,i,j} = 0$，因为求和为空。于是

$$\begin{aligned} |v_{k,i,j}| &\leq \sum_{k_1+k_2+\dots+k_{d_i}=k} \binom{k}{k_1, k_2, \dots, k_{d_i}} |b_{1,i}|^{k_1} \dots |b_{d_i,i}|^{k_{d_i}} \\ &\leq (Bd_i)^k \leq (Bd)^k. \end{aligned} \qquad \text{（多项式定理）}$$

由于 $\left|\frac{(-1)^{k+1}}{k}\right| \le 1$,

$$|h_{i,j}| \le \sum_{k=0}^{j} (Bd)^k \le (Bd)^{j+1}.$$

因此，令 $S = \sum_{j\ge 1} S_j$，其中 $S_j = y^j \sum_{i=1}^n c_i h_{i,j}$ 对所有 $j \ge 1$均成立

$$|S_j| \le y^j nC(Bd)^{j+1}.$$

S_ℓ的下界：
现在我们证明 $|S_\ell| = y^\ell \left|\sum_{i=1}^n c_i h_{i,\ell}\right| \neq 0$ 的下界。我们有

$$\sum_{i=1}^n c_i h_{i,\ell} = \sum_{i=1}^n c_i \sum_{k=1}^{\ell} \frac{(-1)^{k+1}}{k} v_{k,i,\ell} = \sum_{k=1}^{\ell} \frac{(-1)^{k+1}}{k} \underbrace{\left(\sum_{i=1}^n c_i v_{k,i,\ell}\right)}_{\in \mathbb{Z}}.$$

因此 $\ell!(\sum_{i=1}^n c_i h_{i,\ell})$ 是一个整数。于是，如果 $\sum_{i=1}^n c_i h_{i,\ell} \neq 0$,

$$\ell! \left|\sum_{i=1}^n c_i h_{i,\ell}\right| \ge 1.$$

最后，我们得到

$$|S_\ell| \ge \frac{y^\ell}{\ell!}.$$

利用所得到的上界和下界，我们现在可以推导出一个确保方程（8） 成立的条件。实际上，只需对每个 $t \ge 1$,

$$ny^t C(Bd)^{\ell+t+1}\ell! \le \frac{1}{2^{t+1}}, i.e. \tag{10}$$

$$X^t \ge 2^{t+1} nC(Bd)^{\ell+t+1}\ell!. \tag{11}$$

回忆一下，复数域 $\le X^{1/2}$ 且 $\ell \le dn$，因此只需满足

$$X^{t-\frac{1}{2}} \ge 2^{t+1} n(Bd)^{nd+t+1}(nd)!.$$

取对数后，只需对所有 $t \ge 1$，满足

$$\begin{aligned}(t-\frac{1}{2}) p_1(n,d)\log(B+1) \ge &(t+1)\log(2) + \log(n) \\ &+ (nd+t+1)\log(Bd) + nd\log(nd).\end{aligned}$$

因此，可以证明 $p_1(n,d) \ge 20dn\log(dn)$ 是充分的（这个界完全没有优化）。在这种情况下，由方程（9），我们有

$$|S| \ge \frac{1}{2}|S_\ell| \ge \frac{1}{2\ell! X^\ell} \ge \frac{1}{2^{\ell\log\ell+1} X^\ell} \ge \frac{1}{X^{p_2(n,d)}},$$

其中 $p_2(n,d) \ge dn(\log(dn)+1)+1$。

6 结论与开放问题

在定理 5中，我们极大地推广了 [KS12] 所提出的思想。这表明， [KS12] 中的结果可以推广到其他各种幂级数族，如推论 1所示。我们还证明， [KS12] 中的朗斯基行列式方法是紧的，至多相差一个多项式因子。我们的工作还在经典 SSR 等式问题的直线变体方面取得了重大进展。我们还将 [KS12] 中关于多项式整数平方根和的符号判定结果，推广到了多项式整数对数的线性组合，从而解决了 [ESY14]提出的问题 2 的一个特殊情形。未来研究有几个方向：

1. 推论 1 中的第 (ii) 部分适用于二阶微分方程解的一些特殊情形，例如 $\cos f$，其中f 是一个多项式。若能了解这一结论是否适用于高阶方程的一般解，将会很有意义。2. 我们能否通过界定任意代数幂级数之和的阶来推广定理 1？ 多项式的平方根是代数函数的例子。然而，要以令人满意的方式界定一族代数幂级数的朗斯基行列式的阶，颇具挑战性。我们能找到的最佳上界约为$r^{\mathrm{poly}(n)}d$ ，其中$(r、d)$ 是代数幂级数所满足的多项式方程双次数的一个上界。

3. 我们看到，平方根和与对数的符号判定都是 PosSLP 的具体例子。为了进一步理解 PosSLP 的复杂度，研究其他特殊情形十分重要。例如，以下是一些值得探索的 PosSLP 其他特殊情形。

(a) 给定二进制表示的正整数 a、b、c、n，确定 $a^n + b^n - c^n$ 的符号。据我们所知，即使是 PosSLP 的这一非常特殊情形仍未解决。(b) 给定整数三项式 $f(x) := c_1 + c_2 x_2^a + c_3 x^{a_3} \in \mathbb{Z}[x]$ 和有理数 p q，确定 $f\left(\frac{p}{q}\right)$ 的符号。该问题在 [Koi19] 中被提出。–[BDR 22] 对此取得了重大进展，但该问题的一般形式仍未解决。

7 致谢

Louis Gaillard 感谢 Peter B¨urgisser 在 2022 年夏季于柏林工业大学实习期间接待他，本研究工作即在那里开展。Gorav Jindal 曾是 Graduiertenkolleg ”Facets of Complexity/Facetten der Komplexit¨at” (GRK 2434) 和柏林工业大学数学研究所的成员，大部分工作在那里完成。

参考文献

[ABKPM09] Eric Allender、Peter Buergisser、Johan Kjeldgaard-Pedersen 和 Peter Bro Mil- tersen。《数值分析的复杂性》。《SIAM 计算杂志》，38(5):1987–2006，2009。[Bak98] A. Baker。《对数形式与 abc 猜想》，第 37–44 页。De Gruyter，柏林、纽约，1998。[BCSS97] Lenore Blum、Felipe Cucker、Michael Shub 和 Steve Smale。《复杂性与实数计算》。施普林格出版社，柏林、海德堡，1997。

[BD10] Alin Bostan 和 Philippe Dumas。朗斯基行列式与线性无关性。《美国数学月刊》，117(8):722–727，2010。[BDR22] Eric Boniface、Wei Deng 和 J. Maurice Rojas。三项式与实数求解的确定性复杂度界限，2022。[Bl ¨o91] Johannes Bl¨omer。多项式时间计算根式和。载于第 32 届年度计算机科学基础研讨会，1991 年 10 月 1–4 日，第 670–677 页，波多黎各圣胡安，1991。IEEE 计算机学会。[Bl ¨o98] Johannes Bl¨omer。涉及有理数根的表达式的概率零测试。载于 Gianfranco Bilardi、Giuseppe F. Italiano、Andrea Pietracap- rina 和 Geppino Pucci 编，《算法——ESA'98》，第 151–162 页，柏林、海德堡，1998。Springer Berlin Heidelberg。[BNSW22] Nikhil Balaji、Klara Nosan、Mahsa Shirmohammadi 和 James Worrell。根式表达式的恒等性测试。载于第 37 届年度 ACM/IEEE 计算机科学逻辑研讨会论文集，LICS '22，美国纽约州纽约市，2022。美国计算机协会。[Bre76] Richard P Brent。初等函数的快速多精度计算。《美国计算机协会会刊》（JACM），23(2):242–251，1976。[BS96] Eric Bach 和 Jeffrey Shallit。《算法数论》。麻省理工学院出版社，美国马萨诸塞州剑桥市，1996。[BW93] A. Baker 和 G. W ¨ustholz。对数形式与群簇。《纯粹与应用数学杂志》，442:19–62，1993。[ESY14] Kousha Etessami、Alistair Stewart 和 Mihalis Yannakakis。关于比较简洁表示的整数的复杂性及其在最大概率解析中的应用的注记。《美国计算机协会计算理论汇刊》，6(2):9:1–9:23，2014。[GGJ76] M. R. Garey、R. L. Graham 和 D. S. Johnson。一些 NP 完全几何问题。载于第八届年度 ACM 计算理论研讨会论文集，STOC '76，第 10–22 页，美国纽约州纽约市，1976。美国计算机协会。[Kne75] Martin Kneser。根的线性无关性。《算术学报》，26(3):307–308，1975。[Koi19] Pascal Koiran。三项式的根分离。《符号计算杂志》，95:151–161，2019。[KS12] Neeraj Kayal 和 Chandan Saha。关于多项式平方根之和及相关问题。《美国计算机协会计算理论汇刊》，4(4)，2012 年 11 月。[Mal01] Gregorio Malajovich。关于同时丢番图逼近的克罗内克定理的一个有效版本。技术报告，香港城市大学技术报告，2001。[QW06] Jianbo Qian 和 Cao An Wang。比较两个整数平方根和需要多高的精度？《信息处理快报》，100(5):194–198，2006。[Ser81] Jean-Pierre Serre。Chebotarev 密度定理的若干应用。《IHÉS 数学出版物》，54:123–201，1981。

[SL96] Peter Stevenhagen 和 Hendrik Willem Lenstra。Chebotar¨ev 及其密度定理。*The MathematicalIntelligencer*，18(2)：26–37，1996。[VV75] M Voorhoeve 和 A.J Van Der Poorten。朗斯基行列式与某些函数的零点。*IndagationesMathematicae (Proceedings)*，78(5)：417–424，1975。