arXiv:2302.02872v2 [math.NT] 5 Apr 2024

共轭代数整数的极限分布

BRYCE JOSEPH ORLOSKI 和 NASER TALEBIZADEH SARDARI

Abstract. Smith [Smi21]最近的一项进展，确立了 Fekete 关于 $\mathbb{R}$ 紧子集的著名定理的一个定量逆命题（由 Smyth 和 Serre 猜想）。针对 Smith 提出的一个基本问题，我们为 $\mathbb{C}$ 的一般对称紧子集提出并证明了 Fekete 定理的一个定量逆命题。我们着重阐释并利用该方法的算法性质，为有限域上的阿贝尔簇以及代数数论中的极值问题给出具体应用。

1. Introduction

1.1. 背景。 本文由以下问题引出：复平面 $\mathbb{C}$ 中哪些紧集 Σ包含无穷多个共轭代数整数集合，它们在 Σ 中是如何分布的? 本项目的思想源自许多人的研究工作，其中包括 Schur [Sch18], 、 Fekete [Fek23], 、Siegel [Sie45], 、Robinson [Rob64b], 、Smyth [Smy84], 、Rumely [Rum13], 、Serre [Ser19], 以及 Smith [Smi21] 关于代数整数的工作。关于这一主题，我们推荐读者参阅 Baker 和 Rumely [BR 10], 、McKee 和 Smyth [MS21] 以及 Serre [Ser20] 的优秀著作。我们介绍基本概念，并陈述我们的定理，这些定理回答了先前研究中提出的一些开放问题。

设 Σ 是复平面中的一个紧子集。设

$$d_\Sigma(n) := \max_{z_1,\dots,z_n\in\Sigma} \prod_{i<j} |z_i - z_j|^{\frac{2}{n(n-1)}}. \tag{1}$$

Fekete 证明了下列极限存在，并称其为 Σ 的超越有限直径 :

$$d_\Sigma := \lim_{n\to\infty} d_\Sigma(n). \tag{2}$$

例如，半径为 r 的圆的超越有限直径是 r。 Σ 的超越有限直径等于 Σ [的容量（Ahl10，第 2]章）。Fekete [Fek23], 推广了 Schur [Sch18],的一些结果，并证明：如果 $d_\Sigma < 1$，那么只有有限多个不可约首一整系数多项式，其所有根都位于 Σ中。最近，Kollar 和 Sarnak [KS21]将 Fekete 的这一结果与组合论论证相结合，给出了三种正则图的谱的大小和形状的一般下界。值得注意的是，这些界是锐的。

注意，Fekete 条件 $d_\Sigma < 1$是最优的。例如，令 Σ 为单位圆。此时，本原单位根给出无穷多个不可约整系数多项式，其所有根都位于 Σ中。严格的逆命题并不成立。例如，以原点为中心、半径为 $r > 1$ 的圆，其中 r 不是代数整数，便是一个反例。然而，Fekete 和 Szeg¨o[FS55] 证明，若 Σ 关于实轴对称且 $d_\Sigma \geq 1$，那么任意包含Σ 的开集 D 都包含无穷多个共轭代数整数集。Robinson [Rob64a] 利用 Σ的 Chebyshev 多项式的性质，证明了关于实点集的一个类似定理。

我们谨向 Pagano、Rumely、Sarnak、Serre 和 Smith 教授致谢，感谢他们对本文早期版本提出的意见。作者还感谢宾夕法尼亚州立大学计算与数据科学研究所允许我们使用其 ROAR 服务器进行数值实验。

Smyth 证明，若 μ 是与互不相同的共轭代数整数相联系的均匀概率测度的极限，且这些共轭元全都位于复平面的一个紧集 Σ中，那么

$$\int \log|Q(x)|d\mu(x) \geq 0$$

对于每个 $Q(x) \in \mathbb{Z}[x]$。最近的一项突破中，Smith [Smi21] 证明，当 Σ是满足某些条件的 $\mathbb{R}$ 子集时，这些必要条件足以保证 μ 是一个极限测度。本文将这一结果推广到复平面 Σ 中几乎任意的紧对称子集，而我们采用的新方法则以不同的方式处理 Smith 定理。特别地，我们对共轭代数整数的极限测度引入了一些新的约束。对于一个极限测度 μ，我们在定理 1.8 中证明

$$\int \log(|Q(x_1,\ldots,x_n)|)d\mu(x_1)\ldots d\mu(x_n) \geq 0$$

对于每个 $Q(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$。在一项即将发表的工作中，我们基于上述新约束建立一个凸优化问题，并将 Schur-Siegel-Smyth 迹问题的下界提升至新的最佳结果 1.7982。此外，定理 1.8 使我们能够改进 Smith [Smi21 命题 3.5] 中的一些结果，这些结果已在命题 2.13 中陈述。这一改进对于统计具有指定分布 [Tal23]的代数整数至关重要。

Smith 方法建立在 Hilbert [Hil94] 早期利用数论几何的研究，以及 Robinson [Rob64a] 的研究之上。如前所述，Robinson 利用了 $\Sigma \subset \mathbb{R}$ 的切比雪夫多项式的性质。Smith 使用了 [CSZ17a] 中证明的切比雪夫多项式的一些渐近性质，而这些性质对于复平面的紧子集尚不为人所知。本文主要的技术创新，是在不使用切比雪夫多项式性质的前提下，重新证明 Robinson 的结果和 Smith 的结果；见命题 2.16。我们的方法基于相对于平衡测度对根进行概率抽样，然后沿梯度向量用贪心算法对根进行形变；见小节 2.6 和命题 2.16。

除了将 Smith 的结果推广到复平面之外，我们还证明并实现了一种多项式时间算法：该算法以复平面上的矩形所构成的集合上的一个概率测度 μ （满足某些技术条件）的预言机，以及一个正整数 n 为输入，输出一个次数为 n 的多项式，其根分布模拟 μ。据我们所知，我们的算法及其实现此前都没有类似成果。数值结果揭示了代数整数的一些新特征，我们将在小节 1.2.2 中进一步讨论。

1.2. **主要结果**。

1.2.1. 算术概率测度。 设 $\Sigma \subset \mathbb{C}$ 是紧集，且关于实轴对称，并且满足 $d_\Sigma \geq 1$. 令 $\mathcal{P}_\Sigma$ 为支撑集包含于 Σ 的概率测度空间，并赋予弱*拓扑。令

$$\Sigma(\rho) := \{z \in \mathbb{C} : |z - \sigma| < \rho \text{ for some } \sigma \in \Sigma\}.$$

若 $\Sigma \subset \mathbb{R}$，令

$$\Sigma_{\mathbb{R}}(\rho) := \{x \in \mathbb{R} : |x - \sigma| < \rho \text{ for some } \sigma \in \Sigma\}.$$

注意， $\Sigma_{\mathbb{R}}(\rho) \subset \mathbb{R}$ ，且仅对 $\Sigma \subset \mathbb{R}$.有定义

定义 1.1. 若测度 $\mu \in \mathcal{P}_\Sigma$ 是由一列互不相同的、定义在共轭代数整数（全实代数整数）的完全集上的均匀概率测度的弱*极限，并且这些集合最终对每个 $\varepsilon > 0$都包含于 $(\Sigma_{\mathbb{R}}(\varepsilon)$，对每个 $\varepsilon > 0$都包含于 $\Sigma(\varepsilon)$，则称 $\mu \in \mathcal{P}_\Sigma$ 为（实）算术概率测度。所有算术概率测度的集合记为（用 $\mathcal{A}_{\Sigma_{\mathbb{R}}} \subset \mathcal{P}_\Sigma$） $\mathcal{A}_\Sigma \subset \mathcal{P}_\Sigma$.

接下来，我们定义 $\mathcal{P}_\Sigma$ 的一个凸子集，其中包含 $\mathcal{A}_\Sigma$. 。设 $P(x)$是一个次数为 n的复系数多项式。定义它在复平面上的相应根概率测度为

$$\mu_P := \frac{1}{n}\sum_{i=1}^{n}\delta_{\alpha_i},$$

其中 α_i 对于 $1 \le i \le n$ 是 P 的根，而 δ_α 是位于 α. 处的狄拉克概率测度。假设 $\mu \in \mathcal{A}_\Sigma$. 那么，当 $n \to \infty$ 时， $\mu_{P_n} \xrightarrow{*} \mu$ 趋于 $\{P_n\}$ ，其中 $\{P_n\}$ 是由互不相同的、具有整数系数的不可约首一多项式组成的序列。由于 P_n 具有实系数，其根关于实轴对称。因此， μ 也应关于实轴对称。设 Q是一个具有整数系数的多项式。注意，如果 $P_n \nmid Q$,

$$\int \log|Q(x)|d\mu_{P_n}(x) = \frac{\log|\mathrm{Res}(Q,P_n)|}{\deg(P_n)} \ge 0,$$

其中 $\mathrm{Res}(Q,P_n) \in \mathbb{Z}$ 是 P_n 与 Q. 的结式。通过取 $n \to \infty$，Serre [Ser19] 证明了

$$\int \log|Q(x)|d\mu(x) \ge 0 \tag{3}$$

对于每个非零的 $Q(x) \in \mathbb{Z}[x]$. 设 $\mathcal{B}_\Sigma \subset \mathcal{P}_\Sigma$ 为所有关于实轴对称且对每个非零的 $Q(x) \in \mathbb{Z}[x]$. 都满足 (3) 的 $\mu \in \mathcal{P}_\Sigma$ 所构成的集合。由于 $d_\Sigma \ge 1$，可知 Σ 的平衡测度属于 $\mathcal{B}_\Sigma$。注意， $\mathcal{B}_\Sigma$ 是 $\mathcal{P}_\Sigma$ 的凸子集，并且 $\mathcal{A}_\Sigma \subset \mathcal{B}_\Sigma$. Serre [宾夕法尼亚州08]证明了存在 $\Sigma \subset \mathbb{R}^+$ 和 $\mu \in \mathcal{B}_\Sigma$ ，使得 $\int_{\mathbb{R}} x d\mu < 1.8984$. Smith [Smi21] 证明，若 $\Sigma \subset \mathbb{R}$ 满足某些技术条件（包括 Serre 的构造），则 $\mathcal{A}_{\Sigma_{\mathbb{R}}} = \mathcal{B}_\Sigma$. 。这为 Schur–Siegel–Smyth 迹问题给出了明确的答案。寻找具有最小期望值 $\int_{\mathbb{R}} x d\mu$ 的 $\mu \in \mathcal{B}_\Sigma$ 是一个线性规划问题，而寻找其最优解仍是一个开放问题；参见 [Smi21]。这类似于 Cohn-Elkies 为球堆积问题所构造的线性规划问题中寻找魔法函数。

定理 1.2。 假设 $\Sigma \subset \mathbb{C}$ 是紧集，且关于实轴对称。若 $d_\Sigma < 1$，则 $\mathcal{A}_\Sigma = \mathcal{B}_\Sigma = \emptyset$. 否则，$d_\Sigma \ge 1$ 且 $\mathcal{A}_\Sigma = \mathcal{B}_\Sigma \ne \emptyset$. 此外，若 $\Sigma \subset \mathbb{R}$ 是紧集，则$\mathcal{A}_\Sigma = \mathcal{B}_\Sigma = \mathcal{A}_{\Sigma_{\mathbb{R}}}$.

接下来，我们引入一些记号，并陈述一个由我们的结果推出的推论，它将 Smith [Smi21] 的主定理推广到复平面。令

$$[a,b]\times[c,d] := \{z \in \mathbb{C} : \mathrm{Re}(z) \in [a,b] \text{ and } \mathrm{Im}(z) \in [c,d]\} \subset \mathbb{C}.$$

我们称 $[a,b]\times[c,d]$为矩形；若 $c = d = 0$，则称其为实区间。若存在 $\delta > 0$ 和 $A > 0$ ，使得测度 μ是 Hölder 概率测度，则称之为 Hölder 概率测度

$$\mu([a,b]\times[c,d]) \le A\max(|b-a|,|c-d|)^\delta$$

对每个 $a < b$， $c < d$. 假设 $\Sigma \subset \mathbb{R}$ 是闭区间的有限并，且 $d_\Sigma > 1$ ，并且$\mu \in \mathcal{B}_\Sigma$ 是 Hölder 连续的。Smith 的主定理 [Smi21，定理 1.6] 等价于 [Smi21，命题 2.4]，: 存在一个共轭代数整数序列，这些代数整数位于 Σ 内，并在分布上趋于 μ. 如前所述，令 $C_r \subset \mathbb{C}$ 为以原点为圆心、半径为 $r > 1$ 的圆，其中 r 不是代数整数；令 $\mu_r \in B_{C_r}$ 为 C_r上的均匀测度。那么 μ_r 给出了一个反例 [FS55] ，说明 Smith 定理在 $\mathbb{C}$上不成立。了解到这一点后，Smith 提出了将其结果推广到 $\Sigma \subset \mathbb{C}$. 的问题。我们陈述一个主定理的推论，它既能推出 Smith 定理，也将其推广到复平面。

推论 1.3. 假设 $\Sigma \subset \mathbb{C}$ 是紧集，关于实轴对称，并且是由有限个互不相交的矩形和实区间组成的有限并，且 $d_\Sigma > 1$。如果 $\mu \in \mathcal{B}_\Sigma$，那么存在一个共轭代数整数序列，它们位于 Σ 内并且在 μ. 上等分布

Smith 方法不能直接推出推论 1.3。例如，他的方法要求 $\Sigma \subset \mathbb{C}$ 的补集是连通的。对于紧 $\Sigma \subset \mathbb{R}$，这一条件显然成立，但对于某些 $\Sigma \subset \mathbb{C}$ 则不成立。我们引入新的思路来证明上述定理。相关内容将在第 1.4 节中讨论。

接下来，我们引入一些新记号，以便在若干假设下陈述定理 1.2 的一个定量版本。设

$$U_\mu(z) := \int \log|z-w| d\mu(w), \tag{4}$$

这称为 μ 的对数势。在其他文献中，这一势的定义被替换为 $\int -\log|z-w| d\mu(w)$。

我们引用 Smith [Smi21，定义 2.7] 中的以下定义。

定义 1.4. 取一个 H¨older 测度 μ，其支撑集包含于紧子集 $\Sigma \subset \mathbb{C}$ 中。给定一个次数小于或等于 n 的复多项式 P，定义 P 关于 (μ, Σ) 的 n-范数为

$$\|P\|_n := \max_{z\in\mathbb{C}} \left(e^{-nU_\mu(z)} |P(z)| \right).$$

由 [ST97，定理 III.4.2] 可知，若 $\Sigma \subset \mathbb{C}$ 是紧集，且具有空内部和连通补集，并且对于次数为 n 的一列首一多项式 P_n，有 $n \geq 1$

$$\limsup_n \|P_n\|_n^{1/n} \leq 1,$$

那么 P_n 的根在 μ 上等分布。

定理 1.5. 假设 $\Sigma \subset \mathbb{C}$ 是紧集，且内部为空、补集连通。假设 $\mu \in \mathcal{B}_\Sigma$ 是指数为 δ 的 ***H¨older*** 测度，而 D 是包含 Σ的任意开集。对于所有足够大的整数 $n \geq 1$，存在一个次数为 n 的首一不可约多项式 h_n，使得 h_n 的所有根都位于 D 内，并且

$$\|h_n\|_n \leq e^{n^{1-\delta'}}$$

其中 $\delta' > 0$ 仅取决于 μ的 ***H¨older*** 指数。因此， h_n 的根等分布于 μ. 。此外，若 $\Sigma \subset \mathbb{R}$ 是紧集，则可以在实点集拓扑中取任意包含 Σ 的开集 $D \subset \mathbb{R}$，并证明相同的结果。

1.2.2. 逼近算术概率测度的复杂度。 接下来的目标是研究如何找到一个由互不相同的不可约首一多项式 $\{P_n\}$ 构成的序列的复杂度，使得 $\{\mu_{P_n}\}$在弱* 拓扑下收敛到给定的 $\mu \in \mathcal{B}_\Sigma$.

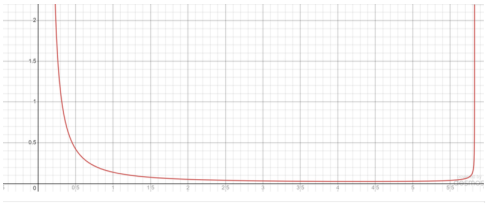
定理 1.6. 设 Σ 如定理 *1.5* 中所述。假设 $\mu \in \mathcal{B}_\Sigma$ 是一个 ***H¨older*** 概率测度，且 D 是包含 Σ的任意开集。存在一个在 n 中的多项式时间算法，它能返回一个次数为 n 的整系数不可约首一多项式 g_n，使得 P_n 的所有根都位于 D 内，并且

$$\|g_n\|_n \leq e^{\frac{Cn\log(\log(n))^3}{\log(n)}}$$

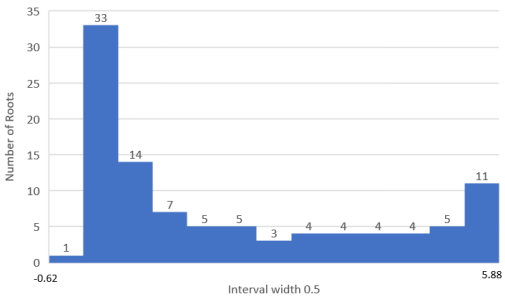
其中 $C > 0$ 仅取决于 μ，与 n无关。因此， g_n 的根等分布于 μ. 此外，如果 $\Sigma \subset \mathbb{R}$ 是紧集，那么可以取实点集拓扑中包含 Σ 的任意开集 $D \subset \mathbb{R}$，并证明同样的结果。

我们为 Serre [AP08] 构造的算术概率测度 $\mu \in \mathcal{B}_\Sigma$ 实现了该算法的一个版本。具体而言，设 $\Sigma = [a, b]$,

$$\mu = c\mu_{[a,b]} + (1-c)\nu_{[a,b]},$$



(A) μ的密度函数



(B) $P_{100}(x)$的根的数量

FIGURE 1. 这将 μ 的密度函数与我们的算法在输入 $n = 100$时输出结果的根的直方图进行比较。

$a = 0.1715$, $b = 5.8255$, $c = 0.5004$, $\mu_{[a,b]}$ 是 $[a, b]$上的平衡测度，而 $\nu_{[a,b]}$ 是 $[b^{-1}, a^{-1}]$ 上平衡测度在映射 $z \to 1/z$. 下的推前测度。图 1a 显示了 μ 的密度，图 1b 显示了我们的算法针对 $n = 100$ 的输出多项式的根的直方图。

1.3. 有限域上的阿贝尔簇的应用。最近，Shankar 和 Tsimer- man [ST18], [ST21] 猜想，对于每个 $g \geq 4$，每个定义在$\mathbb{F}_q$ 上的阿贝尔簇都同源于一个定义在 $\mathbb{F}_q$. 上的曲线的雅可比簇。根据 Honda-Tate 理论， $\mathbb{F}_q$ 上的简单阿贝尔簇的同源类与 $\mathbb{F}_q$ 上的同源，对应于这样一些代数整数：它们的所有共轭元的范数均为$\sqrt{q}$.。我们应用主要定理和 Honda-Tate 理论来证明以下结论。

定理1.7。给定任意有限域 $\mathbb{F}_q$ 和任意整数 n，我们的算法会返回无穷多个 $\mathbb{F}_q$ 上的简单阿贝尔簇同源类；对于每个 $1 \leq m \leq n$，这些同源类中的阿贝尔簇都不同源于任何 $\mathbb{F}_{q^m}$ 上的曲线的雅可比簇。

作者使用论文第 4 节中讨论的算法，找到了一个显式多项式，其最高次项为

$$x^{290} - 28x^{289} - 484x^{288} + 20784x^{287} + \cdots,$$

该多项式不可约，且所有根都位于 $[-2\sqrt{3}, 2\sqrt{3}] \subset \mathbb{R}$ 内；它表示一个定义在 $\mathbb{F}_3$ 上的阿贝尔簇的同源类，而该阿贝尔簇不同源于 $\mathbb{F}_9$ 上任何曲线的雅可比簇。

1.4. 证明方法。 本节中，我们概述主要定理的证明。研究多项式的根的分布时，我们主要使用詹森公式。设 $P(z)$ 是一个复系数多项式，并固定 $w \in \mathbb{C}$.。若 $z_1, \ldots, z_m$ 是 $P(z)$ 在圆盘 $|z-w| < R$ 内的根，且在 $|z - w| = R$, 上没有零点，则詹森公式表明

$$\frac{1}{2\pi}\int_0^{2\pi} \log|P(Re^{i\theta} + w)|d\theta - \log|P(w)| = \log\frac{R^m}{|z_1 - w|\ldots|z_m - w|}.$$

特别是，

$$\frac{1}{2\pi}\int_0^{2\pi} \log|P(Re^{i\theta} + w)|d\theta - \log|P(w)| \geq 0. \tag{5}$$

假设 P是一个首一多项式。我们有 $|P(w)| = |z_1 - w|\cdots|z_n - w|$ 其中 $n = \deg(P)$。因此，对于首一多项式 P，我们有

$$\frac{1}{2\pi}\int_0^{2\pi} \frac{\log|P(Re^{i\theta} + w)|}{n}d\theta = \frac{m}{n}\log R + \frac{1}{n}\sum_{i=m+1}^{n} \log|z_i - w|,$$

其中 $|z_i - w| < R$ 对于 $1 \le i \le m$ 以及 $|z_i - w| > R$ 对于 $m+1 \le i \le n$. 我们将上式改写为

$$\frac{1}{2\pi}\int_0^{2\pi} \frac{\log|P(Re^{i\theta}+w)|}{n} d\theta = \int \log(z;w,R) d\mu_P(z), \tag{6}$$

其中

$$\log(z;w,R) := \begin{cases} \log|z-w| & \text{if } |z-w| > R, \\ \log R & \text{otherwise.} \end{cases}$$

由 (6) 可得， (33) 和 (34) 可知， $\{\mu_{P_n}\}$ 弱收敛到给定的概率测度 μ i f

$$\frac{\log|P_n(z)|}{n} = U_\mu(z) + o(1) \tag{7}$$

对每个满足 $z \in \mathbb{C}\,|z - z_{i,n}| > e^{-\sqrt{n}}$ 的 $z_{i,n}$ ¯，其中 $z_{i,n}$ 是 P_n. 的复根。我们注意到对数 $|P_n($ $z|)$ n 是一个调和函数，其奇点位于 P_n 的根处，并且

$$\frac{\log|P_n(z)|}{n} = \log|z| + O\left(\frac{1}{|z|}\right).$$

我们注意到 $U_\mu(z)$ 与 $|z| \to \infty$. 具有类似的行为。由于 $U_\mu(z)$ 和 对数 $|P_n($ $z|)$ 在 P_n 的根以及 μ 的支撑集之外都是调和函数，且在无穷远处具有类似的渐近行为，因此由调和函数平均值定理可知， (7) 等价于

$$\frac{\log|P_n(z)|}{n} \le U_\mu(z) + o(1) \tag{8}$$

对于每个 $z \in \mathbb{C}$ ，假设 $\mathbb{C} \setminus \Sigma$ 是连通的且 Σ 的内部为空集 [ST97，第三章，定理 4.2]。令

$$K_n := \left\{ p(x) \in \mathbb{R}[x] : \deg(p) \le n, \frac{\log|p(z)|}{n} \le U_\mu(z) \text{ for every } z \in \mathbb{C} \right\}. \tag{9}$$

K_n 是次数小于或等于 n 的实系数多项式向量空间中的一个对称凸区域。为证明定理 1.5，我们使用闵可夫斯基第二定理来证明，在 K_n 中存在次数为 n 的整系数多项式，其误差至多达到 n 中的一个亚指数因子。关键观察是，必要条件 (3) 蕴含 K_n 形状良好，这意味着相对于 K_n 的整系数多项式格的连续最小值彼此接近，并且 K 的体积下界蕴含着在 K_n 中存在次数为 n 的整系数多项式，其误差至多达到 n 中的一个亚指数因子。下面的定理是一个重要的技术结果，使我们能够使用闵可夫斯基第二定理。

定理 1.8。 设 μ 是复平面上具有紧支撑的概率测度。以下各项等价：

(1) μ 关于复共轭保持不变，且 (3) 对每个非零的 $Q(x) \in \mathbb{Z}[x]$.*(2)* μ 关于复共轭保持不变，并且

$$\int \log|Q_m(x_1,\dots,x_m)| d\mu(x_1)\dots d\mu(x_m) \ge 0 \tag{10}$$

for every non-zero $Q_m(x_1,\dots,x_m) \in \mathbb{Z}[x_1,\dots,x_m]$.

回顾一下，

$$\Sigma(\rho) := \{z \in \mathbb{C} : |z-\sigma| < \rho \text{ for some } \sigma \in \Sigma\}.$$

注意，对于包含 Σ 的任意开集 D ，都存在 $\rho > 0$ ，使得 $\Sigma(\rho) \subset D$.

对于 $\Sigma \subset \mathbb{C}$，我们使用 Rouch´e 定理证明，我们的不可约多项式的所有根都位于 $\Sigma(\rho)$ 内，因此 D。这类似于 Fekete 和 Szeg¨o [FS55 的方法，定理 I]。对于 $\Sigma \subset \mathbb{R}$,

Robinson 使用了 Chebychev 多项式，并构造了一个次数为 n 、在 $\Sigma_{\mathbb{R}}(\rho)$ 上具有 n 个符号变化的整系数多项式 $\subset \mathbb{R}$ ，以证明这些根为实数且位于 $\Sigma_{\mathbb{R}}(\rho)$ 内。我们的结果并不依赖于 Σ 上 Chebychev 多项式的存在；参见小节 2.6 和命题 2.16。命题 2.16 使我们能够改进 Smith [Smi21 的一些结果，命题 4.1]。

为证明定理 1.6，我们应用 Schnorr 提出的格算法，并在多项式时间内找到一个不可约的$_{Cn\log(\log(n))}$[3]整系数多项式，它属于 $e^{\log(n)}K_n$，其中 n，某个常数 C 依赖于 μ。事实上，我们取该多项式为首一多项式，并且关于素数 2 满足艾森斯坦判别法。请注意，这不同于我们证明存在性时所得到的最强界，即对于某个显式的$\delta_0 > 0$，有 $e^{Cn^{1-\delta_0}}K_n$ 。Schnorr算法的其他版本可以达到更强的界，但运行时间为超多项式。

2. Minkowski's theorem applied to the lattice of integral polynomials

2.1. 对数势。回顾小节 1.2 和 1.4 中的记号。本节中，我们假设 μ 支撑在一个紧集 $\Sigma \subset \mathbb{C}$ 上，并且是复平面上的一个指数为 $\delta > 0$. 的 Hölder 概率测度。因此，对于每个 $a < b,\ c < d$，以及某个 $A > 0$,

$$\mu([a,b]\times[c,d]) \le A\max(|b-a|,|c-d|)^{\delta}.$$

对于两个紧子集 $B,\ B' \subset \mathbb{C}$，令

$$d(B,B') := \inf_{\substack{z\in B\\ z'\in B'}} |z-z'|.$$

回顾式 **(4)** 中 μ 的对数势定义：

$$U_\mu(z) = \int \log|z-w| d\mu(w).$$

最后，将 μ 的对数能量定义为

$$I(\mu) := \int \log|z_1-z_2| d\mu(z_1)d\mu(z_2) = \int U_\mu(z)d\mu(z).$$

我们证明一个关于对数势渐近行为的引理。

引理 2.1。设 μ 是一个概率测度，其紧支撑位于 $|z|<r$ 内，其中 $z\in\mathbb{C}$. 若 $|w|>2r$，则有

$$U_\mu(w) = \log|w| + O\left(\frac{r}{|w|}\right).$$

证明。我们有

$$\begin{aligned}|U_\mu(w)-\log|w|| &\le \int |\log|w-x| - \log|w||\, d\mu(x)\\ &= \int \left|\log\left|1-\frac{x}{w}\right|\right| d\mu(x) \ll \frac{r}{|w|}.\end{aligned}$$

□

引理 2.2. 设 μ 是复平面上的 *H¨older* 概率测度，其指数为$\delta > 0$。那么对于任意的 z_1、$z_2 \in \mathbb{C}$，若满足 $|z_1-z_2|<1/2$，我们有

$$|U_\mu(z_1)-U_\mu(z_2)| \ll |z_1-z_2|^{\delta'},$$

其中 $\delta' < \min(1/2, \delta/2)$ 是任意正指数。

证明。 假设 $z_1, z_2 \in \mathbb{C}$ 和 $|z_1 - z_2| < 1/2.$。我们有

$$|U_\mu(z_1) - U_\mu(z_2)| = \left| \int \log \frac{|z_1 - w|}{|z_2 - w|} d\mu(w) \right|.$$

我们定义如下对 $\mathbb{C} \setminus \{z_1, z_2\}$ 的覆盖:

$$\begin{aligned} U_0 &:= \left\{ w \in \mathbb{C} : |w - z_2| > 2\sqrt{|z_1 - z_2|} \right\}, \\ U_1 &:= \left\{ w \in \mathbb{C} : |z_1 - z_2| < \min(|w - z_2|, |w - z_1|) \le 2\sqrt{|z_1 - z_2|} \right\}, \\ U_k &:= \left\{ w \in \mathbb{C} : |z_1 - z_2|^k < \min(|w - z_2|, |w - z_1|) \le |z_1 - z_2|^{k-1} \right\}, \end{aligned}$$

其中 $k \ge 2$。因此,

$$|U_\mu(z_1) - U_\mu(z_2)| \le \sum_{i \ge 0} \left| \int_{U_i} \log \frac{|z_1 - w|}{|z_2 - w|} d\mu(w) \right|.$$

对于 $w \in U_0$, 有 $\left| \frac{z_1 - z_2}{z_2 - w} \right| < 1/2$。我们写出 log 的泰勒展开, 得到

$$\left| \int_{U_0} \log \frac{|z_1 - w|}{|z_2 - w|} d\mu(w) \right| = \left| \int_{U_0} \log \left| 1 + \frac{z_1 - z_2}{z_2 - w} \right| d\mu(w) \right| \le \sum_{m \ge 1} \int_{U_0} \frac{1}{m} \left| \frac{z_1 - z_2}{z_2 - w} \right|^m d\mu(w) \ll |z_1 - z_2|^{1/2}.$$

对于 $w \in U_k$, 其中 $k \ge 1$, 有

$$\left| \int_{U_k} \log \frac{|z_1 - w|}{|z_2 - w|} d\mu(w) \right| \le \mu(U_k) k \big| \log |z_1 - z_2| \big| \ll |z_1 - z_2|^{\frac{k\delta}{2}} k \big| \log |z_1 - z_2| \big|,$$

其中我们用到了 $\mu(U_k) \ll |z_1 - z_2|^{\frac{k\delta}{2}}$, 因为 μ 是一个指数为 $\delta > 0$ 的 H¨older 概率测度。因此,

$$|U_\mu(z_1) - U_\mu(z_2)| \ll |z_1 - z_2|^{1/2} + \sum_{k \ge 1} |z_1 - z_2|^{k\delta/2} k \big| \log |z_1 - z_2| \big| \ll |z_1 - z_2|^{1/2} + |z_1 - z_2|^{\delta/2} \big| \log |z_1 - z_2| \big|.$$

最后, 我们有

$$|U_\mu(z_1) - U_\mu(z_2)| \ll |z_1 - z_2|^{\delta'},$$

其中 $\delta' < \min(1/2,\ \delta/2)$ 是任意正指数。 □

2.2. **闵可夫斯基定理**。 回顾 (9) 中 K_n 的定义:

$$K_n = \left\{ p(x) \in \mathbb{R}[x] : \deg(p) \le n \text{ and } \frac{\log |p(z)|}{n} \le U_\mu(z) \text{ for every } z \in \mathbb{C} \right\}.$$

我们将次数小于或等于 n 的实系数多项式空间与 $\mathbb{R}^{n+1}$ 等同起来, 方法是将多项式映射到其系数。容易看出, K_n 是 $\mathbb{R}^{n+1}$ 的一个对称凸区域。

引理 2.3。 设 μ 是一个概率测度, 其紧支撑位于 $|z| < r$ 内, 且适用于 $z \in \mathbb{C}$.。令 $p(x) \in \lambda K_n$, 其中 $\lambda > 0$, 且 $\deg(p) < n$。那么

$$xp(x) \in r\lambda K_n.$$

证明。 令

$$h(z) := U_\mu(z) - \frac{\log |zp(z)|}{n}.$$

注意到 $h(z)$ 是定义在 $|z| > r$ 上且在 $p.$ 的根之外的调和函数。由引理 2.1, 我们有

$$h(z) = \frac{n - \deg(p) - 1}{n} \log |z| + \frac{\log |a_p|}{n} + O(1/|z|),$$

其中 a_p 是 $p.$ 的最高次系数。由上可知，并且由于 $\deg(p) < n$ 且 $h(z)$ 是调和函数， $h(z)$ 的最小值在 $|z| < r$ 内取得。令 $C := \inf_{z\in\mathbb{C}} h(z) = \inf_{|z|<r} h(z)$。由于 $p(x) \in \lambda K_n$，我们有

$$|zp(z)| \le r\lambda e^{nU_\mu(z)}$$

对任意 $|z| < r.$ 这意味着

$$C \ge -\frac{\log r\lambda}{n}.$$

因此，

$$e^{nU_\mu(z)-\log|zp(z)|} = e^{nh(z)} \ge e^{nC} \ge (r\lambda)^{-1}$$

对任意 $z \in \mathbb{C}.$ 这就完成了引理的证明。 □

引理 2.4. 假设 $p(x) \in \lambda K_n$ 对某个 $\lambda > 0.$ 成立。我们断言

$$p'(x) \in An^C\lambda K_n,$$

其中 p' 是 p 的导数，而 A 和 C 是仅依赖于 $\mu.$的常数

证明。设 $D(z_0, r)$ 是以某个 $z_0 \in \mathbb{C}$ 为中心、半径为 $0 < r < \frac{1}{2}.$ 的圆盘。根据伯恩斯坦不等式 [BE95，推论 5.1.6]，对任意 $r > 0,$

$$\sup_{z\in D(z_0,r)} \left|p'(z)\right| \le \frac{\deg p}{r} \sup_{z\in D(z_0,r)} |p(z)|.$$

因此，我们有

$$|p'(z_0)| \le \frac{n}{r} \sup_{z\in D(z_0,r)} |p(z)| \le \lambda\frac{n}{r} \sup_{z\in D(z_0,r)} e^{nU_\mu(z)}.$$

由引理 2.2，对于任意 $z \in D(z_0, r)$，我们有

$$e^{nU_\mu(z)} = e^{n(U_\mu(z)-U_\mu(z_0))}e^{nU_\mu(z_0)} \le e^{A'nr^{\delta'}}e^{nU_\mu(z_0)}.$$

对于某个仅取决于 $\mu.$ 的 $A' > 0$ 和 $\delta' > 0$ 。取任意 $C' > 1/\delta'$ 的 $r = n^{-C'}$ ，即可得到

$$|p'(z_0)| \le \lambda\frac{n}{r}e^{A'nr^{\delta'}}e^{nU_\mu(z_0)} \le A\lambda n^{C'+1}e^{nU_\mu(z_0)},$$

对于任意 $z_0 \in \mathbb{C}$，其中 $A = e^{A'}$。这意味着 $p'(x) \in An^C\lambda K_n$ ，其中 $C = C' + 1.$ □

设 Γ_n 为嵌入到 $\mathbb{R}^{n+1}$ 中的次数不超过 n 的整系数多项式格。 K_n 在 Γ_n 上的连续最小值定义如下：第 k 个连续最小值 λ_k 是满足 λK_n 含有 $k+1$ 个线性无关的 Γ_n 向量的数 λ 的下确界。我们有 $0 < \lambda_0 \le \lambda_1 \le \cdots \le \lambda_n < \infty$。闵可夫斯基第二定理指出

$$\frac{2^{n+1}\mathrm{vol}(K_n)^{-1}}{(n+1)!} \le \lambda_0\lambda_1 \ldots \lambda_n \le 2^{n+1}\mathrm{vol}(K_n)^{-1}. \tag{11}$$

命题 2.5。我们有

$$\lambda_{m+1} \le An^C\lambda_m$$

对于任意 $0 \le m < n,$ 以及某些仅取决于 $\mu.$ 的常数 A 和 C

证明。假设 $p_i \in \Gamma_n$ 对于 $0 \le i \le m$ 构成一组线性无关的整系数多项式，且满足 $p_i \in \lambda_i K_n.$ 。若存在某个 $0 \le i \le m,$ 使得 p_i' 与 $\{p_i : 0 \le i \le m\}$线性无关，则由引理 2.4 可得，

$$p_i'(x) \in An^C\lambda_m K_n.$$

因此，

$$\lambda_{m+1} \le An^C\lambda_m$$

这就证明了我们的命题。否则， $V_m :=$ 由$_{\mathbb{R}} \langle p_0, \ldots, p_m \rangle$ 张成的空间在求导运算下封闭。因此

$$V_m = \operatorname{span}_{\mathbb{R}} \langle 1, x, \ldots, x^m \rangle .$$

这意味着存在 $0 \le l \le m$ ，使得对于每个 $0 \le j \le m.$ ，都有 deg(p_j) $\le$ deg(p_l) $= m$ 。令$q(x) := xp_l(x)$。由于 deg $q > m$， q 与 $V_m.$ 线性无关。由引理 2.3,

$$q(x) \in A\lambda_m K_n$$

其中某个常数 $A > 0$ 仅取决于 $\mu.$ 。因此,

$$\lambda_{m+1} \le A\lambda_m$$

由此完成了命题的证明。 □

2.3. 的体积下界 K_n。 在本小节中，我们给出 K_n 作为 $\mathbb{R}^{n+1}.$ 的子集时其欧几里得体积的下界。我们的方法是在 K_n 内找出 $n+1$ 个次数至多为 n 的线性无关多项式，并计算由原点与这些 $n+1$ 个点的凸包所确定的单纯形的体积。由于 K_n 是对称的，通过为 $n+1$个顶点选择不同的符号，在 K_n 内可得到 2^{n+1} 个体积相同且内部互不相交的单纯形。这些单纯形的总体积给出了 $K_n.$ 体积的下界。

2.3.1. 在 K_n 中寻找一个单纯形。 为简化本节的讨论，我们假设 n 为奇数，并在 K_n 中寻找一个单纯形，估算其体积。对于偶数的情形，固定下文定义的某个 z 值，使其为固定实数。渐近性质相同。回顾一下， μ 在复共轭下保持不变。设 $[a,b] \times [-c,c] \subset \mathbb{C}$ 为包含 $\Sigma.$ 的一个矩形。固定 $0 < M \in \mathbb{Z}$ 和 $0 < L \in \mathbb{R}$ ，其中 $n^{\varepsilon} < M \le n^{1/2-\varepsilon}$ 和 $L < n^{1-\varepsilon}M^{-2}$ 对某个固定的 $\varepsilon > 0.$ 成立。我们将矩形的每条边划分为 $2M$ 个等长子区间，从而得到矩形的一个划分，如下所示:

$$[a,b] \times [-c,c] = \bigcup_{0 \le i,j < 2M} B_{ij},$$

其中 $B_{ij} := [a_i, a_{i+1}] \times [c_j, c_{j+1}]$ 和 $a_i := a + \frac{i}{(b-a)\ 2M}$ ，且 $c_j := -c + \frac{j}{(2c)\ 2M}$ 。由于 μ 是一个指数为 δ 的 H¨lder 测度，我们有

$$\mu(B_{ij}) \ll M^{-\delta} \tag{12}$$

对每个 $0 \le i,\ j < 2M.$ 类似地，对于 $\Sigma \subset \mathbb{R}$，取包含 Σ 的 $[a,b]$，并写作

$$[a,b] = \bigcup_{0 \le i < 2M} B_i,$$

其中 $B_i := [a_i, a_{i+1}]$ 且 $a_i := a + \frac{i}{(b-a)\ 2M}$ 其中 $n^{\varepsilon} < M < n^{1-\varepsilon}$ 且 $L < n^{1-\epsilon}M^{-1}$。令

$$n_{ij} := \lfloor (n+1)\mu(B_{ij}) \rfloor + \varepsilon_{ij} \ll nM^{-\delta}, \tag{13}$$

其中 $\varepsilon_{ij} \in \mathbb{Z}$ 和 $|\varepsilon_{ij}| \le L$ 的选取满足 $\sum_{i,\ j} n_{ij} = n+1$ 且 $n_{ij} = n_{i(2M-j-1)}.$ 。由于我们假设 n 为奇数，因此这是可能的。通过覆盖论证，可以找到满足 $z_{ijk} = z_{i(2M-j-1)k}$ 的 $z_{ijk} \in B_{ij}$ ，使得对于$0 \le i,\ j < 2M$ 和 $1 \le k \le n_{ij}$ ，以及每个 $w \in \partial B_{ij}$ 和每个$1 \le k,\ k' \le n_{ij}$,

$$\begin{aligned} |z_{ijk} - w| &\gg n^{-A} \\ |z_{ijk} - z_{ijk'}| &\gg n^{-A} \end{aligned} \tag{14}$$

对于某个固定的 $A > 0.$ ，类似地，对于 $\Sigma \subset \mathbb{R}$，我们定义 $n_i := \lfloor (n+1)\mu(B_i) \rfloor + \varepsilon_i \ll nM^{-\delta}$ 以及 $z_{ik} \in B_i$，其中 $1 \le k \le n_i$ 满足 $|\varepsilon_i| < L, \sum_i n_i = n+1$，并且对于每个 $w \in \partial B_i$ 以及每个 $1 \le k, k' \le n_i$,

$$\begin{aligned} |z_{ik} - w| &\gg n^{-A} \\ |z_{ik} - z_{ik'}| &\gg n^{-A} \end{aligned} \tag{15}$$

对于某个固定的 $A > 0$.

命题 2.6。我们有

$$\sum_{\substack{ij,i'j' \\ d(B_{ij},B_{i'j'})<M^{-1}}} \sum_{\substack{k,k' \\ i'j'k'\neq ijk}} \frac{\log|z_{ijk}-z_{i'j'k'}|}{(n+1)^2} = O(\log(n)M^{-\delta}), \tag{16}$$

and

$$\sum_{ijk} \sum_{ijk\neq i'j'k'} \frac{\log|z_{ijk}-z_{i'j'k'}|}{(n+1)^2} = I(\mu) + O\left(\frac{M^2\log(n)L}{n} + M^{-\delta/2}\log(n)^{1/2}\right), \tag{17}$$

其中， O 记号中的隐含常数仅取决于 Σ、 μ 和 A ，如 (14) 中所示。类似地，对于 $\Sigma \subset \mathbb{R}$，我们有

$$\sum_{\substack{i,i' \\ d(B_i,B_{i'})<M^{-1}}} \sum_{\substack{k,k' \\ i'k'\neq ik}} \frac{\log|z_{ik}-z_{i'k'}|}{(n+1)^2} = O(\log(n)M^{-\delta}), \tag{18}$$

and

$$\sum_{ik} \sum_{ik\neq i'k'} \frac{\log|z_{ik}-z_{i'k'}|}{(n+1)^2} = I(\mu) + O\left(\frac{M\log(n)L}{n} + M^{-\delta/2}\right), \tag{19}$$

其中的隐含常数 仅取决于 O 记号中的 Σ、 μ 和 A ，如 (15) 中所示。

证明。 注意，对于一对 $(i,\ j)$，至多存在 $O(1)$ 对 $(i',\ j')$，其中 $d(B_{ij},\ B_{i'j'}) < M^{-1}$。由 (13) 和 (14)，我们有

$$\sum_{\substack{ij,i'j' \\ d(B_{ij},B_{i'j'})<M^{-1}}} \sum_{\substack{k,k' \\ i'j'k'\neq ijk}} \frac{\log|z_{ijk}-z_{i'j'k'}|}{(n+1)^2} \ll \sum_{\substack{ij,i'j' \\ d(B_{ij},B_{i'j'})<M^{-1}}} \frac{n_{ij}n_{i'j'}\log(n)}{(n+1)^2} = O(\log(n)M^{-\delta}).$$

这就完成了命题第一部分的证明。我们有

$$I(\mu) = \sum_{ij}\sum_{i'j'} \int_{z\in B_{ij}} \int_{z'\in B_{i'j'}} \log|z-z'| d\mu(z) d\mu(z'). \tag{20}$$

同理，我们有

$$\sum_{\substack{ij,i'j' \\ d(B_{ij},B_{i'j'})<M^{-1}}} \int_{z\in B_{ij}} \int_{z'\in B_{i'j'}} \log|z-z'| d\mu(z) d\mu(z') = O(\log(n)M^{-\delta}).$$

事实上，固定 $z_0 \in B_{ij}$ 并令 $B^m_{i'j'} := B_{i'j'} \cap (B(z_0, M^{-1}2^{-m}) \setminus B(z_0, M^{-1}2^{-m-1}))$。那么

$$\begin{aligned}
\int_{B_{i'j'}} \log|z-z_0| &\ll \sum_{m=0}^{\infty} \int_{B^m_{i'j'}} \log|z-z_0| d\mu \\
&\ll \sum_{m=0}^{\infty} m\log(M)\left(2^{-m}M^{-1}\right)^{\delta} \\
&\ll_{\delta} \log(n)M^{-\delta}.
\end{aligned}$$

因此，

$$\sum_{\substack{ij,i'j' \\ d(B_{ij},B_{i'j'})<M^{-1}}} \int_{z\in B_{ij}} \int_{z'\in B_{i'j'}} \log|z-z'| d\mu(z) d\mu(z') = O_{\delta}(\log(n)M^{-\delta}).$$

假设 $d(B_{ij},\ B_{i'j'}) > M^{-1}$. 我们有

$$\frac{1}{(n+1)^2}\sum_k\sum_{k'}\log|z_{ijk}-z_{i'j'k'}| = \int_{z\in B_{ij}}\int_{z'\in B_{i'j'}}\log|z-z'|d\mu(z)d\mu(z') + O\left(\frac{M_1L}{n}\left(\mu(B_{ij})+\mu(B_{i'j'})\right)+\frac{M_1L^2}{n^2}+\mu(B_{ij})\mu(B_{i'j'})M_2\right) \tag{21}$$

其中 $M_1 := \left|\sup_{z'\in B_{i'j'}}^{z\in B_{ij}}\log\ |z-z'|\right|$ 且 $M_2 := \sup_{z_1'}\ {}_{z_1\ z_2\in B_{ij}\ ,,z_2'\in B_{i'j'}}\left|\log\ |z_1-z_1'|-\log\ |z_2-z_2'|\right|$. 我们有

$$M_1 \ll \log(n)$$

and

$$M_2 \ll \frac{M^{-1}}{d(B_{ij},B_{i'j'})}.$$

因此,

$$\left|\sum_{ijk}\sum_{ijk\neq i'j'k'}\frac{\log|z_{ijk}-z_{i'j'k'}|}{(n+1)^2}-I(\mu)\right| \ll \log(n)M^{-\delta} + \sum_{\substack{ij,i'j'\\ d(B_{ij},B_{i'j'})>M^{-1}}}\frac{\log(n)L}{n}\left(\mu(B_{ij})+\mu(B_{i'j'})\right)+\frac{\log(n)L^2}{n^2}+\mu(B_{ij})\mu(B_{i'j'})\frac{M^{-1}}{d(B_{ij},B_{i'j'})}.$$

注意到

$$\sum_{\substack{ij,i'j'\\ d(B_{ij},B_{i'j'})>M^{-1}}}\frac{\log(n)L}{n}\left(\mu(B_{ij})+\mu(B_{i'j'})\right) \ll \frac{\log(n)M^2L}{n}. \tag{22}$$

由柯西-施瓦茨不等式,

$$\sum_{ij,i'j'}\mu(B_{ij})\mu(B_{i'j'})\frac{M^{-1}}{d(B_{ij},B_{i'j'})} \le \left(\sum_{ij,i'j'}\mu(B_{ij})^2\mu(B_{i'j'})\right)^{1/2}\left(\sum_{ij,i'j'}\frac{M^{-2}\mu(B_{i'j'})}{d(B_{ij},B_{i'j'})^2}\right)^{1/2},$$

其中求和遍及满足 $ij, i'j'$ 且 $d(B_{ij},B_{i'j'}) \ge M^{-1}$. 的项。我们有

$$\sum_{ij,i'j'}\mu(B_{ij})^2\mu(B_{i'j'}) \ll M^{-\delta}\sum_{ij,i'j'}\mu(B_{ij})\mu(B_{i'j'}) = M^{-\delta}.$$

此外,

$$\sum_{ij,i'j'}\frac{M^{-2}\mu(B_{i'j'})}{d(B_{ij},B_{i'j'})^2} \le \max_{i'j'}\sum_{ij}\frac{M^{-2}}{d(B_{ij},B_{i'j'})^2} \ll \log(M). \tag{23}$$

因此,

$$\left|\sum_{ijk}\sum_{ijk\neq i'j'k'}\frac{\log|z_{ijk}-z_{i'j'k'}|}{(n+1)^2}-I(\mu)\right| \ll \log(n)M^{-\delta}+\frac{\log(n)M^2L}{n}+M^{-\delta/2}\log(M)^{1/2}.$$

实数情形几乎完全相同。为了得到实数界，我们看到方程（22）和（23）发生了变化。方程（22）变为

$$\sum_{\substack{i,i' \\ d(B_i,B_{i'})>M^{-1}}} \frac{\log(n)L}{n}\left(\mu(B_i)+\mu(B_{i'})\right) \ll \frac{\log(n)ML}{n}.$$

最后，(23) 变为

$$\sum_{i,i'} \frac{M^{-2}\mu(B_{i'})}{d(B_i,B_{i'})^2} \leq \max_{i'} \sum_{i} \frac{M^{-2}}{d(B_i,B_{i'})^2} \ll 1.$$

因此，对于 $\Sigma \subset \mathbb{R}$, $\sum_{ik}\sum_{ik\neq i'k'} \log|z_{ik}-z_{i'k'}|$ $(n+1)_2$ $= I(\mu) + O(M^{-\delta/2} + \frac{M}{\log(n\ L)})$。 □

令 $\mathcal{Z} := \{z_{ijk} : 0 \leq i,j < 2M, 1 \leq k \leq n_{ij}\}$ 以及

$$p_{\mathcal{Z}}(x) := \prod_{i,j,k}(x - z_{ijk}). \tag{24}$$

对于 $e,f < 2M$和 $g \leq n_{ef}$,

$$\begin{aligned} p_{\mathcal{Z}}^{efg+}(x) &:= \frac{\frac{p_{\mathcal{Z}}(x)}{(x-z_{efg})} + \frac{p_{\mathcal{Z}}(x)}{(x-\overline{z_{efg}})}}{2}, \\ p_{\mathcal{Z}}^{efg-}(x) &:= \frac{\frac{p_{\mathcal{Z}}(x)}{(x-z_{efg})} - \frac{p_{\mathcal{Z}}(x)}{(x-\overline{z_{efg}})}}{2i\mathrm{Im}(z_{efg})}. \end{aligned} \tag{25}$$

类似地，对于 $\Sigma \subset \mathbb{R}$，令 $\mathcal{Z} := \{z_{ik} : 0 \leq i < 2M, 1 \leq k \leq n_i\}$ 以及

$$p_{\mathcal{Z}}(x) := \prod_{i,k}(x - z_{ik}), \tag{26}$$

以及对于 $e < 2M$ 和 $g \leq n_e$,

$$p_{\mathcal{Z}}^{eg}(x) := \frac{p_{\mathcal{Z}}(x)}{(x - z_{eg})}. \tag{27}$$

对于每个 $z \in \mathbb{C}$，令 $\hat{z} \in \mathcal{Z}$ 使 $|z - \hat{z}|$ 最小。

引理 2.7. 我们有 $p_{\mathcal{Z}}(x) \in \mathbb{R}[x]$ 且

$$p_{\mathcal{Z}}^{efg+}(x) = \frac{p_{\mathcal{Z}}(x)}{(x-z_{efg})(x-\overline{z_{efg}})}(x - \mathrm{Re}(z_{efg})) = p_{\mathcal{Z}}^{e(2M-f-1)g+}(x)$$

and

$$p_{\mathcal{Z}}^{efg-}(x) = \frac{p_{\mathcal{Z}}(x)}{(x-z_{efg})(x-\overline{z_{efg}})} = p_{\mathcal{Z}}^{e(2M-f-1)g-}(x).$$

特别地， $p_{\mathcal{Z}}^{efg\pm}(x) \in \mathbb{R}[x]$, $\deg(p_{\mathcal{Z}}^{efg+}(x)) = n$，且 $\deg p_{\mathcal{Z}}^{efg-}(x) = n-1$。

证明。 这很容易由 $z_{ijk} = z_{i(2M-j-1)k}$. 得出 □

命题 2.8. 假设 $n \geq 2$ 最大$\{|a|,|b|,|c|\}$. 我们有

$$p_{\mathcal{Z}}^{efg\pm}(x) \in \lambda^{efg\pm} K_n$$

对于某个 $\lambda^{efg\pm} > 0$，其中

$$\frac{\log(\lambda^{efg\pm})}{n} \leq C\left(\frac{M^2 L\log(n)}{n} + M^{-\delta/2}\log(n)^{1/2}\right)$$

对于某个常数 C，它仅取决于 Σ、μ 和 A，由 (14) 可得。特别地，取 $M=\lfloor n^{1/3}\rfloor$ 和 $L=\lfloor n^{1/3-\delta/6}\rfloor$，可得

$$|\lambda^{efg\pm}|\le e^{Cn^{1-\frac{\delta}{6}}\log(n)}. \tag{28}$$

对于 $\Sigma\subset\mathbb{R}$，我们得到一个更强的结果。特别地，对于某个 $\lambda_{eg}>0$，有 $p_{\mathcal{Z}}^{eg}(x)\in\lambda^{eg}K_n$，其中

$$\frac{\log(\lambda^{eg})}{n}\le C\left(\frac{ML\log(n)}{n}+M^{-\delta/2}\right).$$

证明。我们给出 $p_{\mathcal{Z}}^{efg+}(x)$ 的证明；$p_{\mathcal{Z}}^{efg-}$ 和 $p_{\mathcal{Z}}^{eg}$ 的情形可用类似论证得出。注意，$\deg(p_{\mathcal{Z}}^{efg+})=n$ 且

$$\frac{\log|p_{\mathcal{Z}}^{efg+}(z)|}{n}=\int\log|z-x|d\mu_{p_{\mathcal{Z}}^{efg+}}=U_{\mu_{p_{\mathcal{Z}}^{efg+}}}(z).$$

因此，若 $|z|\ge n$ 且 $n\ge 2\max\{|a|,|b|,|c|\}$，则由引理 2.1，

$$\frac{\log|p_{\mathcal{Z}}^{efg+}(z)|}{n}-U_\mu(z)=O\left(\frac{1}{n}\right).$$

因此不失一般性，我们假设 $|z|<n$。对于 $z\in\mathbb{C}$，我们有

$$\frac{\log|p_{\mathcal{Z}}^{efg+}(z)|}{n}-U_\mu(z)=\sum_{i,j}\left(\sum_{k\le n_{ij}}\frac{\log|z-z_{ijk}|}{n}-\int_{B_{ij}}\log|z-x|d\mu(x)\right)+\frac{\log\frac{|z-\mathrm{Re}(z_{efg})|}{|z-z_{efg}||z-\overline{z_{efg}}|}}{n}. \tag{29}$$

令 $d(z,B_{ij}):=\inf_{w\in B_{ij}}|z-w|$。如前所述，至多有 $O(1)$ 对 (i,j) 满足$d(z,B_{ij})<M^{-1}$。首先，我们给出 (29) 中关于 i,j 的和的上界，其中 $d(z,B_{ij})\le M^{-1}$。回忆一下，$\hat{}z$ 是 $\mathcal{Z}$ 中使 $|z-\hat{}z|$最小的元素。由 (12)、(13) 和 (14)，我们有

$$\sum_{i,j}\left(\sum_{k\le n_{ij}}\frac{\log|z-z_{ijk}|}{n}-\int_{B_{ij}}\log|z-x|d\mu(x)\right)=\frac{\log|z-\hat{z}|}{n}+O(\log(n)M^{-\delta}), \tag{30}$$

其中求和遍历 i,j，其中 $d(z,B_{ij})\le M^{-1}$。这是因为根据 (14)，$|z_{ijk}-z_{ijk'}|\gg n^{-A}$，且 $d(\hat{}z,\partial B_{ij})\gg n^{-A}$。

接下来，我们给出上述关于 i,j的和的一个上界，其中 $d(z,B_{ij})\ge M^{-1}$。设 $d(z,B_{ij})\ge M^{-1}$,则有

$$\left|\sum_{k\le n_{ij}}\frac{\log|z-z_{ijk}|}{n}-\int_{B_{ij}}\log|z-x|d\mu(x)\right|\le\frac{M_1L}{n}+\mu(B_{ij})M_2.$$

其中 $M_1:=\left|\text{上确界}_{z_1\in B_{ij}}\log|z-z_1|\right|$，且 $M_2:=\text{上确界}_{z_1,z_2\in B_{ij}}\left|\log|z-z_2|-\log|z-z_1|\right|$。由于我们知道 $d(z,B_{ij})\ge M^{-1}$,因此有

$$M_1\ll\max(|\log(\mathrm{diam}(\Sigma)+|z|)|,\log(M))\ll\log(n).$$

假设 $z_1,z_2\in B_{ij}$. 令 $r_1:=|z-z_1|$ 且 $r_2:=|z-z_2|$，并假设 $r_1\le r_2$.。根据中值定理，我们有

$$M_2=\frac{|r_1-r_2|}{r_3}$$

对于某个 $r_3,$，其中 $r_1 \le r_3 \le r_2.$。我们有 $|r_1 - r_2| \le |z_1 - z_2| \le M^{-1}$，并且

$$r_3 \gg d(z, B_{ij}).$$

因此，

$$M_2 \ll \frac{M^{-1}}{d(z, B_{ij})}.$$

所以，

$$\sum_{i,j} \left| \sum_{k \le n_{ij}} \frac{\log|z - z_{ijk}|}{n} - \int_{B_{ij}} \log|z - x| d\mu(x) \right| \ll \frac{M^2 L \log(n)}{n} + \sum_{i,j} \mu(B_{ij}) \frac{M^{-1}}{d(z, B_{ij})}, \tag{31}$$

其中 求和遍历 $i, j,$ 其中 $d(z, B_{ij}) \ge M^{-1}$。根据柯西-施瓦茨不等式 y,

$$\sum_{i,j} \mu(B_{ij}) \frac{M^{-1}}{d(z, B_{ij})} \le \left(\sum_{i,j} \mu(B_{ij})^2 \right)^{1/2} \left(\sum_{i,j} \frac{M^{-2}}{d(z, B_{ij})^2} \right)^{1/2} \ll M^{-\delta/2} \log(M)^{1/2},$$

其中我们使用了 $\sum_{i,j} \mu(B_{ij})^2 \ll M^{-\delta} \sum_{i,j} \mu(B_{ij}) = M^{-\delta}$和 $\sum_{i,j} \overline{\substack{M^{-2} \\ d\ z \\ (,B_{ij})_2}} \ll \log(M)$，其中求和遍历 $i, j,$满足 $d(z, B_{ij}) \ge M^{-1}.$。因此，由（31）及上述不等式，我们得到

$$\sum_{i,j} \left| \sum_{k \le n_{ij}} \frac{\log|z - z_{ijk}|}{n} - \int_{B_{ij}} \log|z - x| d\mu(x) \right| \ll \frac{M^2 L \log(n)}{n} + M^{-\delta/2} \log(M)^{1/2}, \tag{32}$$

其中求和遍历 $i, j,$其中 $d(z, B_{ij}) \ge M^{-1}.$。最后，由（29）、（30）和（32），我们得到

$$\frac{\log|p_{\mathcal{Z}}^{efg+}(z)|}{n} - U_\mu(z) = \frac{\log \frac{|z-\hat{z}||z-\mathrm{Re}(z_{efg})|}{|z-z_{efg}||z-\overline{z}_{efg}|}}{n} + O\left(\log(n) M^{-\delta} + \frac{M^2 L \log(n)}{n} + M^{-\delta/2} \log(M)^{1/2} \right). \tag{33}$$

根据定义 ，$z, \frac{|z-\hat{z}||z-\mathrm{Re}(z_{efg})|}{|z-z_{efg}||z-\overline{z}_{efg}|} \le 1$ Re()并令 $M = \lfloor n^{1/3} \rfloor$ 和 $L = \lfloor n^{1/3-\delta/6} \rfloor$，我们得到

$$\frac{\log|p_{\mathcal{Z}}^{efg+}(z)|}{n} \le U_\mu(z) + O(n^{-\frac{\delta}{6}} \log(n)).$$

与命题 2.6 中的推理相同， $\Sigma \subset \mathbb{R}$ 的证明几乎完全相同，但

$$\frac{\log|p_{\mathcal{Z}}^{eg}(z)|}{n} - U_\mu(z) = \frac{\log \frac{|z-\hat{z}|}{|z-z_{eg}|}}{n} + O\left(\frac{ML \log(n)}{n} + M^{-\delta/2} \right). \tag{34}$$

□

2.3.2. 单纯形体积的下界。设

$$\mathcal{M} := \left[p_{\mathcal{Z}}^{ijk\pm} \right],$$

其中 $0 \le i < 2M, 0 \le j < M, k \le n_{ij}$ 是大小为 $(n+1) \times (n+1)$ 的方阵，其列向量为 $p_{\mathcal{Z}}^{efg\pm}$ 的系数。若 $\Sigma \subset \mathbb{R}$，则令 $\mathcal{M}_{\mathbb{R}} := [p_{\mathcal{Z}}^{eg}]$。

命题 2.9。有

$$|\det(\mathcal{M})| = 2^{-\frac{n+1}{2}} \prod_{ijk} \frac{1}{|\mathrm{Im}(z_{ijk})|^{1/2}} \prod_{ijk < i'j'k'} |z_{ijk} - z_{i'j'k'}|,$$

其中 $0 \le i$、$i' < 2M$、$0 \le j$、$j' < 2M$、$k' \le n_{i'j'}$ 和 $k \le n_{ij}$。如果 $\Sigma \subset \mathbb{R}$,

$$|\det(\mathcal{M}_{\mathbb{R}})| = \prod_{ik<i'k'} |z_{ik} - z_{i'k'}|$$

其中 $0 \le i$、$i' < 2M$、$k \le n_i$ 和 $k' \le n_{i'}$。

证明。设

$$\mathcal{N} := \left[\frac{p_{\mathcal{Z}}(x)}{(x - z_{ijk})}\right],$$

其中 $0 \le i < 2M$，$0 \le j < M$，以及 $k \le n_{ij}$ 是一个大小为 $(n+1) \times (n+1)$ 的方阵，其列向量为 $\frac{p_{\mathcal{Z}}(x)}{(x-z_{ijk})}$ 的系数。由 (25)，对于固定的指标 efg，可得

$$\left[p_{\mathcal{Z}}^{efg+}, p_{\mathcal{Z}}^{efg-}\right] = \left[\frac{p_{\mathcal{Z}}(x)}{(x - z_{efg})}, \frac{p_{\mathcal{Z}}(x)}{(x - \overline{z_{efg}})}\right] \begin{bmatrix} 1/2 & \frac{1}{2i\mathrm{Im}(z_{efg})} \\ 1/2 & -\frac{1}{2i\mathrm{Im}(z_{efg})} \end{bmatrix}.$$

因此,

$$|\det(\mathcal{M})| = |\det(\mathcal{N})| 2^{-\frac{n+1}{2}} \prod_{ijk} \frac{1}{|\mathrm{Im}(z_{ijk})|^{1/2}} \tag{35}$$

其中 $0 \le i < 2M$，$0 \le j < 2M$，$k \le n_{ij}$. 设

$$V := [z_{ijk}^e]$$

是一个大小为 $(n+1) \times (n+1)$，的范德蒙德矩阵，其中 $0 \le e < n+1$. 众所周知,

$$|\det V| = \prod_{ijk} \prod_{ijk<i'j'k'} |z_{ijk} - z_{i'j'k'}|.$$

我们有

$$V\mathcal{N} = \mathrm{diag}\left[\prod_{ijk \ne efg} (z_{efg} - z_{ijk})\right].$$

因此,

$$|\det(\mathcal{N})| = \prod_{ijk} \prod_{ijk<i'j'k'} |z_{ijk} - z_{i'j'k'}|.$$

因此，由（35）得,

$$|\det(\mathcal{M})| = 2^{-\frac{n+1}{2}} \prod_{ijk} \frac{1}{|\mathrm{Im}(z_{ijk})|^{1/2}} \prod_{ijk<i'j'k'} |z_{ijk} - z_{i'j'k'}|.$$

现在假设 $\Sigma \subset \mathbb{R}$，那么 $V_{\mathbb{R}} := [z_{ik}^e]$ 满足 $|\det V_{\mathbb{R}}| = \prod_{ik} \prod_{ik<i'k'} |z_{ik} - z_{i'k'}|$。因此,

$$V_{\mathbb{R}}\mathcal{M}_{\mathbb{R}} = \mathrm{diag}\left[\prod_{ik \ne i'k'} (z_{ik} - z_{i'k'})\right].$$

因此，我们有 $|\det(\mathcal{M}_{\mathbb{R}})| = \prod_{ik<i'k'} |z_{ik} - z_{i'k'}|$，如所求。 □

命题 2.10。我们有

$$\mathrm{vol}(K_n) \gg n^{-cn^{2-\frac{\delta}{6}}} e^{\frac{n^2}{2} I(\mu)}$$

其中，c 是仅取决于(14)中的 Σ、μ和 A 的常数。如果 $\Sigma \subset \mathbb{R}$，则有

$$\mathrm{vol}(K_n) \gg e^{-cn^{2-\frac{\delta}{6}}} e^{\frac{n^2}{2} I(\mu)}$$

对于某个仅依赖于 Σ、μ 和 A 的常数 c，由 (15) 得到。

证明。由命题 2.8，$e^{Cn^{1-\frac{\delta}{6}}\log(n)}K_n$ 包含一个顶点为 $\left\{0, p_{\mathcal{Z}}^{ijk\pm}\right\}$、体积为 $\frac{1}{|\det(A)|\,(n+1)!}$ 的单纯形，其中 $0 \le i < 2M, 0 \le j \le M-1, k \le n_{ij}.$。由于 K_n 是对称的，通过为 $n+1$ 个顶点 $\left\{0, \pm p_{\mathcal{Z}}^{ijk\pm}\right\}$ 选取不同的符号，可在 $e^{Cn^{1-\frac{\delta}{6}}\log(n)}K_n$ 内得到 2^{n+1} 个体积相同且内部互不相交的单纯形。因此，

$$\mathrm{vol}(K_n) \ge \frac{2^{n+1}}{(n+1)!} e^{-Cn^{2-\frac{\delta}{6}}\log(n)} |\det(\mathcal{M})|.$$

由命题 2.9，

$$\mathrm{vol}(K_n) \ge \frac{2^{\frac{n+1}{2}}}{(n+1)!} e^{-Cn^{2-\frac{\delta}{6}}\log(n)} \prod_{ijk} \frac{1}{|\mathrm{Im}(z_{ijk})|^{1/2}} \prod_{ijk<i'j'k'} |z_{ijk} - z_{i'j'k'}|.$$

We 有 $|\mathrm{Im}(z_{ijk})| \le c$，其中 $\mathrm{supp}(\mu) \in [a,b]\times[-c,c]$，且 $c \ge 1$。因此

$$\prod_{ijk} \frac{1}{|\mathrm{Im}(z_{ijk})|^{1/2}} \prod_{ijk<i'j'k'} |z_{ijk} - z_{i'j'k'}| \ge c^{-n/2} \prod_{ijk<i'j'k'} |z_{ijk} - z_{i'j'k'}|.$$

由 (17)，利用 $M = \lfloor n^{\frac{1}{3}} \rfloor$ 和 $L = \lfloor n^{\frac{1}{3}-\frac{\delta}{6}} \rfloor$，可得 $\prod_{ijk<i'j'k'} |z_{ijk} - z_{i'j'k'}| = e^{\frac{n^2}{2} I(\mu) + O(n^{2-\frac{\delta}{6}}\log(n))}$，因此存在某个（可能为负的）常数 C'，使其至少为 $e^{\frac{n^2}{2} I(\mu) + C' n^{2-\frac{\delta}{6}}\log(n)}$。这给出

$$\mathrm{vol}(K_n) \gg \frac{2^{\frac{n+1}{2}}}{(n+1)! c^{n/2}} e^{\frac{n^2}{2} I(\mu) + (C'-C) n^{2-\frac{\delta}{6}}\log(n)} \gg \frac{n^{(C'-C)n^{2-\frac{\delta}{6}}} e^{\frac{n^2}{2} I(\mu)}}{(n+1)^{n+1} c^n} \gg n^{\tilde{C} n^{2-\frac{\delta}{6}}} e^{\frac{n^2}{2} I(\mu)}$$

因为 $\frac{(n+1)_{n^n}}{n^{n+1}} \sim (n+1)e$，其中某个常数 $\tilde{C}$ 仅依赖于 A, Σ 和 μ。

若 $\Sigma \subset \mathbb{R},$，则得到

$$\mathrm{vol}(K_n) \ge \frac{2^{n+1}}{(n+1)!} e^{-Cn^{2-\frac{\delta}{6}}} |\det(\mathcal{M}_{\mathbb{R}})|.$$

由命题 2.9 和 (19)，

$$|\det(\mathcal{M}_{\mathbb{R}})| = \prod_{ik<i'k'} |z_{ik} - z_{i'k'}| = \frac{n^2}{2} I(\mu) + O(n^{2-\delta/6})$$

取 $M = \lfloor n^{1/3} \rfloor$ 和 $L = \lfloor n^{1/3-\epsilon} \rfloor$。因此，$|\det(\mathcal{M}_{\mathbb{R}})| = \frac{n^2}{2} I(\mu) + C' n^{2-\delta/6}$，其中常数 C' 仅依赖于 A，Σ 和 μ。因此，

$$\mathrm{vol}(K_n) \gg \frac{2^{n+1}}{(n+1)!} e^{\frac{n^2}{2} I(\mu) + (C'-C) n^{2-\frac{\delta}{6}}} \gg e^{\frac{n^2}{2} I(\mu) + \tilde{C} n^{2-\frac{\delta}{6}}}$$

˜，其中常数 C 仅依赖于 A，Σ 和 μ。 □

命题 2.11。假设 $\mu \in \mathcal{B}_{\Sigma}.$。存在一个整系数多项式 p_0，满足 $\deg(p_0) \le n$，使得

$$\frac{\log|p_0(x)|}{n} \le U_\mu(x) - \frac{I(\mu)}{2} + C\log(n) n^{-\delta/6},$$

其中 C 是一个与 $n.$ 无关的常数。此外，

$$I(\mu) \ge 0.$$

若 $\Sigma \subset \mathbb{R}$，则存在一个整系数多项式 p_0，满足 $\deg(p_0) \le n$，使得

$$\frac{\log|p_0(x)|}{n} \le U_\mu(x) - \frac{I(\mu)}{2} + C n^{-\delta/6}$$

对于某个与 n 无关的常数 C 。因此， $I(\mu) \geq 0$。

证明。 根据命题 2.10，存在常数 c，使得对所有 $n > 0$，vol(K_n) $\geq n^{cn^{2-\frac{\delta}{6}}} e^{\frac{n^2}{2} I(\mu)}$。根据闵可夫斯基第二定理 (11)，存在次数至多为 n 的 $p_0 \in \mathbb{Z}[x] \cap \lambda_0 K_n$ ，其中

$$\lambda_0 \leq 2\left(\mathrm{vol}(K_n)\right)^{-1/(n+1)} \ll n^{cn^{1-\frac{\delta}{6}}} e^{-\frac{n}{2} I(\mu)}. \tag{36}$$

根据 K_n的定义，

$$\frac{\log|p_0(x)|}{n} \leq U_\mu(x) + \frac{\log(\lambda_0)}{n}$$

利用 (36)，我们得到

$$\frac{\log|p_0(x)|}{n} \leq U_\mu(x) - \frac{I(\mu)}{2} + c\log(n) n^{-\frac{\delta}{6}}.$$

对上述不等式取期望值，得到

$$0 \leq \int \frac{\log|p_0(x)|}{n} d\mu(x) \leq \frac{I(\mu)}{2} + c\log(n) n^{-\frac{\delta}{6}},$$

其中，第一个不等式使用了假设 $\mu \in \mathcal{B}_\Sigma$ 。令 $n \to \infty$，得到

$$I(\mu) \geq 0.$$

对于 $\Sigma \subset \mathbb{R}$，同样的计算给出所需结果，只是 (36) 变为

$$\lambda_0 \ll e^{cn^{1-\frac{\delta}{6}}} e^{-\frac{n}{2} I(\mu)}.$$

将这一过程贯穿整个计算，

$$\frac{\log|p_0(x)|}{n} \leq U_\mu(x) - \frac{I(\mu)}{2} + cn^{-\frac{\delta}{6}}.$$

积分后得到 $0 \leq \frac{I(\mu)}{2} + cn^{-\frac{\delta}{6}}$ 。与之前一样，取 $n \to \infty$ 可得 $I(\mu) \geq 0$。 □

2.4. **定理 1.8 的证明**。 设 μ 是复平面上具有紧支撑的概率测度，并且对每个非零的 $Q(x) \in \mathbb{Z}[x]$,

$$\int \log|Q(z)| d\mu(z) \geq 0.$$

首先，根据以下命题，我们将定理 1.8 的证明归结为 H¨ölder 概率测度的情形。

命题 2.12。 设 $\Sigma \subset \mathbb{C}$ 是紧的，且 $\mu \in \mathcal{B}_\Sigma$. 。对于任意 $\rho > 0$，存在一个 *H¨ölder* 概率测度序列 $\mu_n \in \mathcal{B}_{\Sigma(\rho)}$ ，使得 $\lim_{n\to\infty} \mu_n = \mu$。此外，若$\Sigma \subset \mathbb{R}$ 是紧的且 $\mu \in \mathcal{B}_\Sigma$，则存在一个 *H¨ölder* 概率测度序列 $\mu_n \in \mathcal{B}_{\Sigma_{\mathbb{R}}(\rho)}$ ，使得 $\lim_{n\to\infty} \mu_n = \mu$。

证明。 令 λ_r 为以原点为中心、半径为 r 的圆上的均匀概率测度。令 $\mu * \lambda_r$ 为 μ 与 λ_r. 的卷积。我们证明，对于每个 $z \in \mathbb{C}$ 和每个 $r \geq 0.$ ，都有 $U_{\mu*\lambda_r}(z) \geq U_\mu(z)$。事实上，我们有

$$U_{\mu*\lambda_r}(z) - U_\mu(z) = \int \left(\int_0^1 \log|z - x + re^{2\pi i\theta}| - \log|z - x| d\theta \right) d\mu(x) \geq 0,$$

这里我们使用詹森公式 (5) 证明内积分为正。因此，对于任意 $r \leq \rho.$ ，都有 $\mu * \lambda_r \in \mathcal{B}_{\Sigma(\rho)}$。定义

$$\mu_n := \mu * \lambda_{\rho/n}.$$

根据定义显然，$\lim_{n\to\infty} \mu_n = \mu$ and μ_n 是一个指数至少为 1 的 H¨older 测度。这就完成了关于 $\Sigma \subset \mathbb{C}$ 的命题证明。由于 $\Sigma \subset \mathbb{R}$ 的紧性，它

可知 $\Sigma(\rho)$ 是有限个区间的并。根据 [Smi21，命题 2.5], ，存在一个概率测度序列 $\mu_n \in \mathcal{B}_{\Sigma_{\mathbb{R}}(\rho)}$ ，其 H¨older 指数至少为 $1/2$ ，使得 $\lim_{n\to\infty} \mu_n = \mu$。 □

定理 *1.8* 的证明。 第 (1) 部分是 $m = 1$. 下第 (2) 部分的特例。因此，只需证明第 (1) 部分蕴含第 (2) 部分。假设 μ 满足第 (1) 部分的条件，根据定义，这等价于 $\mu \in \mathcal{B}_\Sigma$ 。

接下来，我们将定理归结为 μ 是 H¨older 的情形。根据命题 2.12，存在一个 H¨older 概率测度序列 $\mu_n \in \mathcal{B}_{\Sigma(\rho)}$ ，使得 $\lim_{n\to\infty} \mu_n = \mu$。假设定理 1.8 对 H¨older 概率测度成立。那么

$$\int \log |Q(z_1, \dots, z_m)| d\mu_n(z_1) \dots d\mu_n(z_m) \geq 0,$$

对每个 $n.$，注意，$\log |Q(z_1, \dots, z_m)|$ 是一个上半连续函数。因此，根据单调收敛定理，我们有

$$\int \log |Q(z_1, \dots, z_m)| d\mu(z_1) \dots d\mu(z_m) \geq \limsup_{n\to\infty} \int \log |Q(z_1, \dots, z_m)| d\mu_n(z_1) \dots d\mu_n(z_m) \geq 0.$$

因此，不失一般性，我们假设 $\mu \in \mathcal{B}_\Sigma$ 是 H¨older 的。证明对 m,使用归纳法，第 (1) 部分是归纳的基础。假设第 (2) 部分对 m 成立，并证明它对 $m + 1.$ 成立。假设 $Q(x_1, \dots, x_{m+1}) \in \mathbb{Z}[x_1, \dots, x_{m+1}].$。不失一般性，我们假设 Q 在 $\mathbb{Z}[x_1, \dots, x_{m+1}]$ 中不可约，且不属于 $\mathbb{Z}[x_{m+1}].$。令

$$U_Q(z_{m+1}) := \int \log |Q(z_1, \dots, z_m, z_{m+1})| d\mu(z_1) \dots d\mu(z_m).$$

只需证明

$$\int U_Q(z) d\mu(z) \geq 0. \tag{37}$$

我们固定 $z_i \in \mathbb{C}$ ，令 $1 \leq i \leq m$ ，并将 Q 视为关于变量 x_{m+1} 的多项式，假设其在 $x_{m+1}.$ 中的次数为 d 。于是

$$Q(z_1, \dots, z_m, x_{m+1}) = \sum_{i=0}^{d} a_i(z_1 \dots, z_m) x_{m+1}^i = a_d(z_1, \dots, z_m) \prod_{i=1}^{d} (x_{m+1} - \xi_i(z_1, \dots, z_m))$$

其中 $\xi_i(z_1 \dots, z_m) \in \mathbb{C}$ 是 Q的复根。根据归纳假设，我们有 e

$$\int \log |a_d(z_1, \dots, z_m)| d\mu(z_1) \dots d\mu(z_m) \geq 0.$$

这意味着，对于几乎所有的 $z_1, \dots, z_m$，相对于乘积测度 $\mu \times \dots \times \mu$，有 $a_d(z_1, \dots, z_m) \neq 0$。我们在 $\mathbb{C}$ 上定义测度 μ_Q 如下

$$\mu_Q := \int \sum_i \delta_{\xi_i(z_1,\dots,z_m)} d\mu(z_1) \dots d\mu(z_m) \tag{38}$$

其中 δ_a 是以点 $a \in \mathbb{C}.$ 为支撑的狄拉克概率测度。我们有

$$U_Q(z) = a_Q + \int \log |z - x| d\mu_Q(x)$$

其中

$$a_Q := \int \log |a_d(z_1, \dots, z_m)| d\mu(z_1) \dots d\mu(z_m). \tag{39}$$

注意，根据归纳假设，我们有

$$a_Q \geq 0.$$

根据命题 命题 2.11，存在一个整系数多项式 $P_0(x)$，其次数为 $\deg(P_0) \leq n$ 使得 t

$$\frac{\log|P_0(x)|}{n} \leq \int \log|z-x| d\mu(z) + Cn^{-\delta}.$$

We 对上述不等式关于 $d\mu_Q$ 取期望值，得到 in

$$a_Q + \int \frac{\log|P_0(x)|}{n} d\mu_Q(x) \leq a_Q + \int \log|z-x| d\mu(z) d\mu_Q(x) + \frac{Cd}{n^\delta} = \int U_Q(z) d\mu(z) + \frac{Cd}{n^\delta}.$$

只需证明

$$na_Q + \int \log|P_0(x)| d\mu_Q(x) \geq 0, \tag{40}$$

因为令 $n \to \infty$. 即可得到（37）。事实上，我们证明：对于每个整系数多项式 $P(x)$,

$$\deg(P) a_Q + \int \log|P(x)| d\mu_Q(x) \geq 0. \tag{41}$$

这意味着（40），因为 $\deg(P_0) \leq n$ 且 $a_Q \geq 0$. 为证明（41），我们将 P 视为关于 x_{m+1}的整系数多项式。定义

$$R(Q,P)(x_1,\ldots,x_m) := Res(Q(x_1,\ldots,x_{m+1}), P(x_{m+1})) \in \mathbb{Z}[x_1,\ldots,x_m]$$

为 Q 和 P 作为关于变量 x_{m+1}的多项式时的结式。根据我们的假设， Q是不可约的，并且不整除 $P(x_{m+1})$。 因此， $Res(Q(x_1,\ldots,x_{m+1})\ P(x_{m+1})) \neq 0$. 根据我们的归纳假设,

$$\int \log R(Q,P)(z_1,\ldots,z_m) d\mu(z_1)\ldots d\mu(z_m) \geq 0.$$

我们注意到

$$\log R(Q,P)(z_1,\ldots,z_m) = \deg(P)\log|a_d(z_1,\ldots,z_m)| + \sum_{i=1}^{d} \log|P(\xi_i(z_1,\ldots,z_m))|.$$

因此,

$$\int \deg(P)\log|a_d(z_1,\ldots,z_m)| + \sum_{i=1}^{d} \log|P(\xi_i(z_1,\ldots,z_m))| d\mu(z_1)\ldots d\mu(z_m) \geq 0.$$

根据 (38) 和 (39) 中 μ_Q 和 a_Q 的定义，上述结果推出 (41)。这就完成了证明，并推出

$$\int \log|Q(z_1,\ldots,z_m,z_{m+1})| d\mu(z_1)\ldots d\mu(z_m) d\mu(z_{m+1}) \geq 0.$$

□

2.5. **闵可夫斯基极小值因子乘积的下界**。首先，我们利用定理 1.8 给出闵可夫斯基极小值因子乘积的一个下界。

命题 2.13. 我们有

$$\prod_{i=0}^{m-1} \lambda_i \geq \frac{1}{m!} e^{(-nm+\frac{(m-1)m}{2})I_\mu}.$$

证明。 根据 $\{\lambda_i$ 的定义： $0 \leq i \leq m-1\}$，存在一组线性无关的整系数多项式$\{P_0,\ldots,P_{m-1}\}$，其中

$$|P_i(z)| \leq \lambda_i e^{nU_\mu(z)}.$$

对每个 $z \in \mathbb{C}$. 令 $\{z_1, \ldots, z_m\} \subset \mathbb{C}$. 因此,

$$\det[P_i(z_j)] \leq m! \prod_{i=0}^{m-1} \lambda_i e^{nU_\mu(z_i)}. \tag{42}$$

另一方面，我们有

$$\det[P_i(x_j)] = Q_m(x_1, \ldots, x_m) \prod_{i<j} (x_i - x_j)$$

对于某个 $Q_m \in \mathbb{Z}[x_1, \ldots, x_m]$.，取上述结果的平均值，得到

$$\int \log|\det[P_i(z_j)]| d\mu(z_1) \ldots d\mu(z_m) = \frac{(m-1)m}{2} I_\mu + \int \log|Q_m(z_1, \ldots, z_m)| d\mu(z_1) \ldots d\mu(z_m),$$

其中

$$I(\mu) := \int \log|z_1 - z_2| d\mu(z_1) d\mu(z_2).$$

由定理（1.8）的第二部分，我们有

$$\int \log|Q_m(z_1, \ldots, z_m)| d\mu(z_1) \ldots d\mu(z_m) \geq 0.$$

因此,

$$\int \log|\det[P_i(z_j)]| d\mu(z_1) \ldots d\mu(z_m) \geq \frac{(m+1)m}{2} I_\mu.$$

由（42）可得

$$mnI_\mu + \sum_i \log|\lambda_i| + \log(m!) \geq \int \log|\det[P_i(z_j)]| d\mu(z_1) \ldots d\mu(z_m) \geq \frac{(m+1)m}{2} I_\mu.$$

因此,

$$\prod_i \lambda_i \geq \frac{1}{m!} e^{(-nm + \frac{(m-1)m}{2}) I_\mu}.$$

□

命题 2.14. 我们有

$$\lambda_n \leq n^{cn^{1-\frac{\delta}{12}}}.$$

若 $\Sigma \subset \mathbb{R}$，则 $\lambda_n \leq e^{cn^{1-\frac{\delta}{12}}}$。

证明。令 $m = n - n^{\delta_1}$，其中 $0 < \delta_1 < 1$ 稍后给出。由命题 2.13,

$$\prod_{i=0}^{m} \lambda_i \geq \frac{1}{m!} e^{-nm + \frac{(m-1)m}{2} I_\mu}.$$

由闵可夫斯基第二定理和命题 2.10,

$$\lambda_0 \lambda_1 \ldots \lambda_n \leq 2^{n+1} \mathrm{vol}(K_n)^{-1} \ll 2^{n+1} n^{cn^{2-\frac{\delta}{6}}} e^{-\frac{n^2}{2} I(\mu)}.$$

结合以上不等式，我们有

$$\prod_{i=m+1}^{n} \lambda_i \ll n^{cn^{2-\frac{\delta}{6}}} e^{-\frac{(n-m)^2}{2} I(\mu)}.$$

由命题 2.11，我们有 $I(\mu) \geq 0$ 且

$$\prod_{i=m+1}^{n} \lambda_i \ll n^{cn^{2-\frac{\delta}{6}}}.$$

因此，取 $\delta_1 = 1 - \delta/12$，我们得到

$$\lambda_{m+1} \le n^{cn^{2-\frac{\delta}{6}-\delta_1}} \le n^{cn^{1-\frac{\delta}{12}}}.$$

根据命题 2.5，我们有

$$\lambda_n \le \lambda_m(An)^{C(n-m)} \le n^{cn^{1-\frac{\delta}{12}}}.$$

这就完成了命题的证明。注意，在上述推导中，我们可以将常数 c 换成一个更大的常数。□

2.6. **平衡测度**。 在本小节中，我们将上一节的结果应用于平衡测度，并证明命题 2.15。我们的证明基于 Fekete 和 Szeg¨o [FS55, 定理 D] ， Robinson [Rob64a] 和 Smith [Smi21, 命题 4.1] 也使用了该结果来证明类似的结论。所有这些结果对于控制根使其保持在 $\Sigma(\rho)$。内至关重要

假设 Σ是紧集，在复共轭下保持不变，且其补集是开且连通的。令 D 为任意一个包含 Σ的开集。回顾一下，

$$\Sigma(\rho) := \{z \in \mathbb{C} : |z - \sigma| < \rho \text{ for some } \sigma \in \Sigma\}.$$

注意，对于任意包含 Σ的开集 D ，都存在 $\rho > 0$ 使得 $\Sigma(\rho) \subset D$.令 μ_{eq} 为 Σ. 的平衡测度。任取 $\rho > 0$ 和 $z_0 \in \Sigma$. 。众所周知 明白，

$$U_{\mu_{eq}}(z) \ge \log(d_\Sigma) + \delta_{\rho,\Sigma} \tag{43}$$

对于任意 $z \notin \Sigma(\rho)$，其中 $\delta_{\rho,\ \Sigma} > 0$ 是仅依赖于 Σ 和 ρ. 的常数。令 $p_{\mathcal{Z}}(x)$为与平衡测度相关联、按（24）构造的多项式。由（33）和（43），存在某个 $R > d_\Sigma$ 和 $\mathcal{Z}$，使得 $|\mathcal{Z}| = n_0$，从而

$$p_{\mathcal{Z}}(z) \ge R^{n_0}$$

对于任意 $z \notin \Sigma(\rho)$。固定 $z_0 \in \Sigma(\rho)$ 和 $p_{\mathcal{Z}}(x)$，并定义

$$T_m(x) := (x - z_0)^r p_{\mathcal{Z}}(x)^q, \tag{44}$$

其中 $m = n_0 q + r$ 是 m 除以 n_0所得的欧几里得商。令 $m \ge h$ 为两个正整数。由此可得

$$T_m(z) \ge CR^{m-h} T_h(z) \tag{45}$$

对于任意 $z \notin \Sigma(\rho)$，其中 C 仅依赖于固定参数 ρ 和 n_0.

命题 2.15。给定一个关于复共轭不变且具有连通补集的紧子集 $\Sigma \subset \mathbb{C}$ 、一个实系数首一多项式 $p(x)$ 以及 $\rho > 0$，存在固定整数 l_0 和 k_0，它们与 $p(x)$ 无关；并且存在一个首一多项式 $Q_m(x)$ ，满足 $\deg(Q_m) = m$ ，对每个 $m = kl_0$ 都成立，其中 $k > k_0$ 使得

$$|Q_m(z)| \ge \kappa^m$$

对于每个 $z \notin \Sigma(\rho)$ ，其中 $\kappa > d_\Sigma$. 此外，对于每个 $\deg(p) \le i \le \deg(p) + m - 1$， x^i 在 $p(x)$ $Q_m(x)$ 中的系数都是偶整数，并且 $Q_m(x)$ 的所有复根都在 $\Sigma(\rho)$内。

证明。 回顾 $T_m(x)$ 在 (44) 中对于 $m \in \mathbb{Z}$, 的定义，并定义

$$q_{k,l}(x) := (T_k(x) + a_1 T_{k-1}(x) + \cdots + a_k T_0(x))^l$$

其中， $|a_i| \le \frac{1}{l}$ 是递归选取的，使得对于 $1 \le i \le k$ ， $q_{k,l}(x)p(x)$具有偶系数$x^{\deg(p)+\deg(q_{k,l})-i}$, 其中 $1 \le i \le k$. 。注意，这是可行的，因为对于 $j \le l$ 中的q_k， $x^{\deg(p)+\deg(q_{k,l})-j}$的系数由下式给出

$$la_j + F_j(a_1, \ldots, a_{j-1})$$

其中， $F_j(a_1,\dots,a_{j-1})$是关于 a_i的多项式，其中 $i<j.$。由（45），我们有 e

$$\begin{aligned}|q_{k,l}(z)| &= \left|(T_k(z)+a_1T_{k-1}(z)+\cdots+a_kT_0(z))^l\right| \\ &\geq \left|T_k(z)\left(1-\frac{C}{l}\sum_{j\geq 1}\frac{1}{R^j}\right)\right|^l \geq |T_k(z)|^l\left(1-\frac{C}{l(R-1)}\right)^l.\end{aligned}$$

固定一个整数 $l_0 > \frac{C}{R-1}$，并令

$$C' := \left(1-\frac{C}{l_0(R-1)}\right)^{l_0} > 0.$$

因此，

$$|q_{k,l_0}(z)| \geq C'T_k(z)^{l_0} \geq C''|p_{\mathcal{Z}}(z)|^{\left\lfloor\frac{k}{n_0}\right\rfloor l_0} \tag{46}$$

其中 C'' 是依赖于我们所固定参数的固定常数。最后，令 $m:=l_0k$ 并令

$$Q_m(x) := q_{k,l_0}(x) - \sum_{i=0}^{m-k} b_iT_i(x),$$

其中 $|b_i|\leq 1$ 是递归选取的，使得对于 $0\leq i\leq m-k$， $Q_m(x)p(x)$ 具有偶系数，且 $\deg(p) \leq j \leq \deg(p)+m-k.$。由 (46)、(45) 和 (44)，我们得到

$$|Q_m(z)| \geq |q_{k,l_0}(z)| - \sum_{i=0}^{m-k}|T_i(z)| \geq |p_{\mathcal{Z}}(z)|^{\frac{kl_0}{n_0}}\left(C''-\frac{C_1}{R^{k-1}(R-1)}\right).$$

取 $k>k_0$ 即可得到我们的命题，其中 k_0 是一个固定常数。 □

假设 $\Sigma\subset\mathbb{C}$ 是紧的、关于实轴对称的，并且是矩形和实区间的有限不交并。记

$$\Sigma = \bigcup_{i=1}^{N_1}(R_i\cup\bar{R}_i)\bigcup_{j=1}^{N_2}I_j$$

其中 $R_i\subset\mathbb{C}$ 是矩形， $I_j\subset\mathbb{R}$ 是区间。我们定义

$$\Sigma_{\mathbb{R}}(\rho) := \bigcup_{i=1}^{N_1}(R_i(\rho)\cup\bar{R}_i(\rho))\bigcup_{j=1}^{N_2}I_{j\mathbb{R}}(\rho)$$

对于任意 $\rho>0$。注意，如果 $\bigcup_j I_{j\mathbb{R}}\neq\emptyset$，那么 $\Sigma_{\mathbb{R}}(\rho)\subsetneq\Sigma(\rho)$。

为证明将 Smith 的结果推广到 $\mathbb{C}$的推论 1.3，我们使用命题 2.16。该命题的表述受到 Smith [Smi21，命题 4.1]的启发。然而，Smith 方法并不能推出这一命题。Smith 方法建立在 Fekete 和 Szegö [FS55，定理 D] 以及 Robinson [Rob64a]的工作的基础上。Smith 和 Robinson 使用了 [CSZ17b] 中的切比雪夫多项式的性质，该性质仅对 $\mathbb{R}$ 的子集得到证明，并利用了这些多项式在实区间上的符号变化。这种方法不适用于复集，因此我们对命题 2.16 的证明在概念上有所不同。此外，它还使我们能够将根保留在 $\Sigma_{\mathbb{R}}(\rho)\subset\Sigma(\rho)$ 内。

命题 2.16。 假设 $\Sigma=\bigcup_i(R_i\cup R_i)\bigcup_j I_j$ 是紧集，关于实轴对称，且是矩形和实区间的有限不交并，并且 $\bigcup_j I_j\neq\emptyset$ 满足 $d_\Sigma\geq 1$。给定一个次数为 $n-m$、实系数的首一多项式 $p(x)$ $\rho>0$，以及一个偶整数$n^\varepsilon\leq m\leq n$，存在一个实系数首一多项式 $Q_m(x)$，使得 $\deg(Q_m)=m$，并且满足以下各项条件。

(1) 度 *gree* i 乘积的系数 pQ_m 对于 $n-m \le i \le n-1$是偶整数。（*2*）令 X 为 Q_m的根集。则 X 是 $\Sigma_{\mathbb{R}}$（ρ）的子集，并且关于实轴对称。（*3*）我们有

$$\frac{\log|Q_m(z)|}{m} = \frac{\min_{\alpha\in X}\log|z-\alpha|}{m} + U_{\mu_{eq}}(z) + O(m^{-\frac{\delta}{8}}\log(m))$$

对于所有 $z\in\mathbb{C}$ 以及某个 $\delta>0$成立，其中 μ_{eq} 是关于 $\Sigma_{\mathbb{R}}$（$\rho/10$）的平衡测度。（*4*）给定 Q_m 的任意根 α 以及任意 α'（它或者是 p 的根，或者是 $\Sigma_{\mathbb{R}}$（ρ）的边界点），有 $n^{-3}\le|\alpha-\alpha'|$.

证明。令 $m_1 = \lfloor m\mu_{eq}(\bigcup_i R_i(\rho/10))\rfloor$ 和 $m_2 = m-2m_1$，其中 μ_{eq} 是 $\Sigma_{\mathbb{R}}(\rho/10)$ 的平衡测度。令 x_1，……，x_m 如下

（1）对于 $i=1$、2、……、m_1，根据 μ_{eq}进行同分布独立抽取，条件是 $x_i\in\bigcup_i R_i(\rho/10)$，对于 $1\le i\le m_1$成立。（2） x_{i+m_1}：对于 $1\le i\le m_1$，$=\bar{x_i}$。（3）对于 $i=1$、2、……、m_2，根据 μ_{eq}进行同分布独立抽取，条件是 $x_i\in\bigcup_j I_j(\rho/10)$，对于 $2m_1<i\le m$成立。

我们注意到，μ_{eq}在有限个区间的并上是指数为 $\delta\ge1/2$ 的 H¨older 连续函数，因为如果 $[a,b]\subset\Sigma\subset\mathbb{R}$，那么$\mu_{eq,\ [a,b]}$ 的密度大于$\mu_{eq,\ \Sigma}$的密度。此外，$d\mu_{eq} = \frac{dx}{\pi\sqrt{(b-x)(x-a)}}$ 在 $[a,b]$上。令~~$\mathcal{Z}:=\{x_1,\dots$~~$,x_m\}$，并令 $P_{\mathcal{Z}}$为式（26）中构造的、根为 $x_1,\dots,x_m$的多项式。以概率 $1-o(1)$，我们注意到 $x_1,\dots,x_m$ 满足（13）、（14）和（15）中的条件，其中 $M=m^{1/4}$、$L=(mM^{-\delta})^{\frac{1}{2}+\varepsilon}<m^{1-\varepsilon}M^{-2}$，并且对任意 α'，若其为 p的根、任何其他$x_j\ne x_i$，或 $\Sigma_{\mathbb{R}}(\rho)$的边界点，则 $n^{-2-\varepsilon}\le|x_i-\alpha'|$。这可由博雷尔-坎特利型论证得出。事实上，回忆式（13）中 B_{ij}的定义，并令n_{ij}为 $\mathcal{Z}:=\{x_1,\dots,x_m\}$中落在 B_{ij}内的元素个数。固定 i 和 j，并定义以下随机变量

$$y_k^{ij} = \begin{cases} 1 & \text{if } x_k\in B_{ij} \\ 0 & \text{otherwise.}\end{cases}$$

令 $p=\mu(B_{ij})$。我们有 $\mathrm{Prob}(y_k^{ij}=1)=p$ 和 $\mathrm{Prob}(y_k^{ij}=0)=1-p$. 注意到

$$n_{ij} = \sum_k y_k^{ij}.$$

由马尔可夫不等式可得

$$\mathrm{Prob}\left(|n_{ij}-\mu(B_{ij})m|\ge L\right) \le \frac{\mathrm{E}\left((n_{ij}-\mu(B_{ij})m)^{2h}\right)}{L^{2h}}$$

对任意 $h\ge0$ 均成立。此外，

$$\begin{aligned}\mathrm{E}\left((n_{ij}-\mu(B_{ij})m)^{2h}\right) &= \mathrm{E}\left(\sum_k y_k^{ij}-\mathrm{E}(y_k^{ij})\right)^{2h} \\ &\ll \sum_{k_1,\dots,k_h}\prod_{l=1}^{h}\mathrm{E}\left(y_{k_l}^{ij}-\mathrm{E}(y_{k_l}^{ij})\right)^2 \ll m^h\left(p(1-p)\right)^h \\ &\ll m^h p^h = \left(\mu(B_{ij})m\right)^h.\end{aligned}$$

因此，

$$\mathrm{Prob}\left(|n_{ij}-\mu(B_{ij})m|\ge L\right) \le \frac{\left(\mu(B_{ij})m\right)^h}{L^{2h}} \le L^{-2h(\frac{\varepsilon}{1+\varepsilon})}.$$

其中我们使用了（12）中的不等式 $\mu(B_{ij})m \le mM^{-\delta}$。因此，

$$\sum_{i,j} \mathrm{Prob}\left(|n_{ij} - \mu(B_{ij})m| \ge L\right) \ll \sum_{i,j} L^{-2h(\frac{\varepsilon}{1+\varepsilon})} \ll M^2 L^{-2h(\frac{\varepsilon}{1+\varepsilon})}$$

对于任意 $h \ge 0$。由于 $L \gg m^{1/4}$，令 $h \gg \frac{1}{\varepsilon}$，我们得出结论：以概率$1-o(1)$，$x_1, \ldots, x_m$ 满足 (13)、(14) 和 (15) 中的条件，其中 $M = m^{1/4}$, $L = (mM^{-\delta})^{\frac{1}{2}+\varepsilon}$，并且 $n^{-2-\varepsilon} \le |x_i - \alpha'|$对于任意 α'，它要么是 p 的根、任意其他 $x_j \ne x_i$，要么是$\Sigma_{\mathbb{R}}(\rho)$的边界点。根据 (33) 和 (43)，该多项式满足上述所有条件，但第一条除外。我们的方法是使用贪心算法对 $P_{\mathcal{Z}}$ 的根进行形变，使其满足命题 2.16 的所有性质。我们从 $pP_{\mathcal{Z}}$. 的次数 $n-1$ 系数开始。我们至少选取其中的 $\lceil 10/\rho \rceil$ 个关于实轴对称的根，记为 $x_1, \ldots, x_{k_0}$，并将它们分别形变小于 $\rho/10$，使得 $pP_{\mathcal{Z}}$ 的次数 $n-1$ 系数变为偶数，同时根仍然位于 $\Sigma_{\mathbb{R}}(\rho)$ 内并关于实轴对称。我们证明这是可能的。

令 $Q_{m,0}(x) := P_{\mathcal{Z}}(x) = x^m + \sum_{i=1}^{m} a_i x^{m-i}$. $x^{\deg(p)+m-j}$ 关于 $j \le l$ 在 $Q_{m,0}(x)p(x)$ 中的系数由 $a_j + F_j(a_1, \ldots, a_{j-1})$ 给出，其中 $F_j(a_1, \ldots, a_{j-1})$ 是关于 a_i 的多项式。我们定义 $x_i(t) := x_i + t\frac{\rho}{10}$，其中 $i \le k_0$，并称变形后的多项式为 $Q_{m,0,t}$。根据介值定理，存在 $|t| \le 1$，使得 $pQ_{m,0,t}$ 的次数为 $n-1$ 的系数变为偶数，且根仍位于 $\Sigma_{\mathbb{R}}(\rho)$ 内。假设变形后，对于关于实轴对称的 $y_1, \ldots, y_k$，条件 (4) 不成立。由 (15)，可以选取 $Q_{m,0}(x)$ 的另外 k 个根，记为 $y_1', \ldots, y_k'$，它们关于实轴对称，并且在距离 $n^{-2-\varepsilon}$. 内，y_i' 附近没有其他根。我们用 $y_1 + t$ 和 $y_1' - t$. 更新 y_1 和 y_1'。根据覆盖论证，存在 $t \ll n^{-3}$，使得 $y_1 + t$ 与其他根的距离至少为 n^{-3}.。同样地，更新 y_i、y_i'，使条件 (4) 得以满足。将更新后的多项式记为 $Q_{m,1}$。注意，除第一项条件外，$Q_{m,1}$ 满足上述所有条件，且 $pQ_{m,1}$ 的次数为 $n-1$ 的系数是偶数。

我们按如下方式递归构造 $Q_{m,l}$，使其满足 $l \ge 1$。假设 $Q_{m,l}$ 满足除第一条以外的所有条件，并且乘积 $pQ_{m,l}$ 的 i 次系数对于 $n-l \le i \le n-1$ 是偶整数。我们希望在不改变更高次数的系数的前提下，通过像上一段那样形变 $Q_{m,l}$ 的根，使 $n-l-1$ 的系数也成为偶数。

假设 $l \le \log(n)^2$.。令 $l_1 = \lfloor l\mu_{eq}(\bigcup_i R_i(\rho/10)) \rfloor$ 和 $l_2 = l - 2l_1$。我们按如下方式选取至少 n^{ε} 个不同的对称子集族 $\mathcal{Z}_{\sigma_i} := \{x_{\sigma_i(1)} \cdots, x_{\sigma_i(l)}\} \subset \mathcal{Z} = \{x_1, \ldots, x_m\}$，每个族对于 $1 \le i \le n^{\varepsilon}$ 都含有 l 个元素，其中 $\varepsilon > 0$ 固定且任意小：

(1) $x_{\sigma_i(1)} \cdots, x_{\sigma_i(l_1)}$ 从 x_1, ..., x_{m_1} 中均匀地选取，概率为 $1 - o(1)$ 这些点在之前的步骤中未被变形或选取，我们对此作此假设。(2) $x_{\sigma_i(j+l_1)} = \bar{x}_{\sigma_i(j)}$ 对每个 $1 \le j \le l_1$ 都成立。(3) $x_{\sigma_i(2l_1+1)} \cdots, x_{\sigma_i(l)}$ 从 x_{2m_1+1}, ..., x_m 中均匀地选取，概率为 $1 - o(1)$ 这些点在之前的步骤中未被变形或选取，我们对此作此假设。

固定 $\mathcal{Z}_{\sigma_i}$ 并考虑 $\boldsymbol{x} = [x_{\sigma_i(1)} \cdots, x_{\sigma_i(l)}]$, 并令

$$s_k := \sum_{j=1}^{l} x_{\sigma_i(j)}^k,$$

and

$$e_k := \sum_{1 \le j_1 < \cdots < j_k \le l} x_{\sigma_i(j_1)} \ldots x_{\sigma_i(j_k)},$$

其中 $e_0 = 1$ 且 $s_0 = l.$ 令 $\nabla s_k = k[x_{\sigma_i\ j\ ()}^{k-1}]$ 为 $s_k.$ 的梯度。令

$$v_l := \left[\frac{1}{\prod_{j\neq 1}(x_{\sigma_i(1)} - x_{\sigma_i(j)})}, \frac{1}{\prod_{j\neq 2}(x_{\sigma_i(2)} - x_{\sigma_i(j)})}, \ldots, \frac{1}{\prod_{j\neq l}(x_{\sigma_i(l)} - x_{\sigma_i(j)})} \right].$$

注意到，对于 $j > 2l_1$ ， v_l 的坐标均为实数；对于 $j \leq l_1$， $v_{l,\ j} = v_{l,\ j+l_1}$。这意味着沿此方向对根的扰动仍保持对称。因此，对于每个 $1 \leq k \leq l-1$ 和 $\langle v_l,\ \nabla s_l\rangle = l.$ ， v_l 与 ∇s_k 正交。我们注意到

$$e_k = \frac{1}{k}\sum_{j=1}^{k}(-1)^{j-1}e_{k-j}s_j.$$

这意味着对于每个 $0 \leq k \leq l-1$ 和 $\langle v_l,\ \nabla e_l\rangle =$ ， $\langle v_l,\ \nabla e_k\rangle = 0\,(-1)^{l-1}.$。由（33）和（43）可知，以概率 1， v_l 的大小呈指数级小，因此我们有

$$|v_l| \leq d_{\Sigma_{\mathbb{R}}(\rho/10)}^{-l(1+O(l^{-\delta}))}$$

对于某个 $\delta > 0$。我们按照以下常微分方程对 $\boldsymbol{x}$ 变形，或等价地对$\mathcal{Z}_{\sigma_i}$ 变形： $\frac{d\boldsymbol{x}(t)}{dt} = v_l(t)$，初始条件为 $\boldsymbol{x}(0) = \boldsymbol{x}.$。我们注意到，相应的子集 $\mathcal{Z}_{\sigma_i}(t)$随 t连续变形，并且关于 x 轴保持对称。由介值定理可知，对于任意大的 $A > 0$，可以沿着 v_l的方向变形 n^{ε} 个互不相同的 l-元组$[x_1, \ldots, x_l]$，其中 $t < l^{-A}$ 为某个值，并使pQ_m中 x^{n-l-1} 的系数为偶数。显然，扰动仍在$\Sigma_{\mathbb{R}}(\rho)$内。假设变形后，条件（4）对 y_1, ..., y_k不成立，其中 $k \leq n^{\varepsilon}l$。由（15）可知，可以选取 $kl \leq n^{\varepsilon}\log(n)^4$ 个Q_m的其他根，即$l(x)$，记为 y_i，使得对于 $1 \leq i \leq k$ 和 $1 \leq j \leq l$， $_j$ 满足按 μ_{eq}独立同分布。我们按照以下常微分方程变形 $l+1$ 元组 $\boldsymbol{x}_i := [y_i, y_{i,1}, \ldots, y_{i,l}]$ $\frac{d\boldsymbol{x}_i(t)}{dt} = v_{l+1,\ i}(t)$，初始条件为 $\boldsymbol{x}_i(0) = \boldsymbol{x}_i$ ，其中

$$v_{i,l+1}(t) := \left[\frac{1}{\prod_j(y_i - y_{1,j})}, \frac{1}{(y_{i,1} - y_i)\prod_j(y_{i,1} - y_{i,j})}, \ldots, \frac{1}{(y_{i,l} - y_i)\prod_j(y_{i,l} - y_{i,j})} \right].$$

通过覆盖论证，存在 $t \ll n^{-3+\epsilon}$ 使得 $x_1(t)$与其他根相距至少 n^{-3}。将更新后的多项式记为 $Q_{m,\ l+1}$. 注意，$Q_{m,\ l+1}$ 满足上述所有条件，除了第一条；乘积 $pQ_{m,\ l+1}$ 的次数 i 系数对于 $n-l-1 \leq i \leq n-1$是一个偶整数。

最后，假设 $m \geq l \geq \log(n)^2.$ 我们选取一个对称子集 $\mathcal{Z}_\sigma := \{x_{\sigma(1)}, \ldots, x_{\sigma(l)}\} \subset \mathcal{Z} = \{x_1, \ldots, x_m\}$， 其中有 l 个元素，并满足上面列出的三个条件。和之前一样，令 $\boldsymbol{x} = [x_{\sigma(1)}, \ldots, x_{\sigma(l)}]$ 并且

$$v_l := \left[\frac{1}{\prod_{i\neq 1}(x_{\sigma(1)} - x_{\sigma(i)})}, \frac{1}{\prod_{i\neq 2}(x_{\sigma(2)} - x_{\sigma(i)})}, \ldots, \frac{1}{\prod_{i\neq l}(x_{\sigma(l)} - x_{\sigma(i)})} \right].$$

根据 (33) 和 (43)， v_l 的大小小于 n的任意负次幂

$$|v_l| \leq d_{\Sigma}^{-l} \leq e^{-\log(n)^2} \ll n^{-A}$$

对任意 $A > 0.$，我们按如下常微分方程 $\frac{d\boldsymbol{x}\ (t)\ dt}{} = v_l(t)$ 对 $\boldsymbol{x}$ 进行变形，初始条件为 $\boldsymbol{x}(0) = \boldsymbol{x}$。根据介值定理，存在 $|t| \leq 1$，使得 $n-l-1$ 的次数为偶数，即 $pQ_{m,\ l+1}$ 的系数为偶数。这次扰动不会改变条件 (2)、(3) 和 (4)，因为对于任意 A，扰动都小于 n^{-A}，并且当 $n-m \leq i \leq n-1$ 时，乘积 $pQ_{m,\ l+1}$ 的 i 次系数为偶整数。至此，我们完成了命题的证明。□

3. Proofs of main theorems

3.1. 定理 1.5 的证明。 在本小节中，我们假设 $\Sigma \subset \mathbb{C}$ 是紧集，且内部为空、补集连通。我们还假设 $\mu \in \mathcal{B}_\Sigma$ 是一个 H¨older 测度。

定理 *1.5* 的证明。假设 $\mu \in \mathcal{B}_\Sigma$ 是一个指数为 δ 的 Hölder 测度，且 D 是包含 Σ 的任意开集。固定 $\rho > 0$，使得 $\Sigma(\rho) \subset D.$。我们对 $p_{\mathcal{Z}}(x)$ 应用命题 2.15，其中 $|\mathcal{Z}| = n - m$ 如 (24) 中定义，且 $m := n^{1-\delta_0}$，对某个我们稍后指定的 $\delta_0 > 0$，从而得到 $Q_m(x)$，使得

$$p_{\mathcal{Z}}(x)Q_m(x) = x^n + \sum_{i=0}^{n-1} a_i x^i$$

其中 a_i 对 $n - m \le i \le n - 1.$ 均为偶数。令

$$r(x) := \frac{1}{2} + \sum_{i=0}^{n-1-m} \frac{a_i}{4} x^i.$$

我们将 $r(x)$ 表示为由 K_{n-1-m} 的闵可夫斯基逐次极小值导出的线性无关整系数多项式 $\{P_0, \dots, P_{n-1-m}\}$ 的线性组合，并得到

$$r(x) = \sum_{i=0}^{n-1-m} \alpha_i P_i(x).$$

Let

$$w(x) := \sum_{i=0}^{n-1-m} \lfloor \alpha_i \rfloor P_i(x)$$

and

$$h_n(x) := x^n + \sum_{i=n-m}^{n-1} a_i x^i + 4w(x) - 2.$$

根据素数 2 处的艾森斯坦判别法，$w(x)$ 不可约。此外，

$$h_n(x) = p_{\mathcal{Z}} Q_m(x) + \sum_{i=0}^{n-1-m} \beta_i P_i(x),$$

其中 $|\beta_i| = 4|\alpha_i - \lfloor \alpha_i \rfloor| < 4.$。注意

$$|P_i(z)| \le \lambda_i e^{(n-m)U_\mu(z)}$$

对于每个 $z \in \mathbb{C}$，根据命题 2.14,

$$\lambda_i \le n^{cn^{1-\frac{\delta}{12}}}.$$

此外，由 (33) 和命题 2.15,

$$|p_{\mathcal{Z}}(z)Q_m(z)| \ge e^{(n-m)U_\mu(z)} \kappa^m n^{-Cn^{1-\frac{\delta}{6}}}$$

对每个 $z \notin \Sigma(\rho)$，其中 $M = \lfloor n^{1/3} \rfloor$. 通过取 $\frac{\delta}{12} > \delta_0 > 0$ 和 $m = n^{1-\delta_0}$，可得

$$|p_{\mathcal{Z}} Q_m(z)| > \left| \sum_{i=0}^{n-m-1} \beta_i P_i(z) \right|$$

当 n 足够大且对每个 $z \notin \Sigma(\rho)$ 时。根据鲁歇定理，$h_n(z)$ 和 $p_{\mathcal{Z}}Q_m(z)$ 在 $\Sigma(\rho)$ 内的根的数量相同。由于 $p_{\mathcal{Z}}Q_m(z)$ 的所有根都在 $\Sigma(\rho)$ 内，$h_n(z)$ 的所有根也都在 $\Sigma(\rho)$内。根据引理 2.1，我们有

$$\frac{\log|Q_m(z)|}{m} \leq \max(\log|z|, 0) + C_\Sigma,$$

其中 C_Σ 是一个仅取决于 Σ. 的常数。由于 $m = n^{1-\delta_0}$，我们有

$$\frac{\log|h_n(z)|}{n} \leq U_\mu(z) + O(n^{-\delta_0}).$$

这就完成了 $\Sigma \subset \mathbb{C}$时的情形。对于 $\Sigma \subset \mathbb{R}$，论证类似。我们用命题 2.16 替代命题 2.15，并取 $p_{\mathcal{Z}}(x)Q_m(x)$，它有 n 个彼此相距 n^{-3}的不同根。我们利用介值定理以及在 $\Sigma_{\mathbb{R}}(\rho)$上有 n 次符号变化这一事实，证明所有根都是实数且位于 $\Sigma_{\mathbb{R}}(\rho)$内，而不使用 Rouch´e 定理。□

3.2. **定理 1.2 的证明**。本节中，我们证明定理 1.5 蕴含定理 1.2。为证明定理 1.5，我们假设 μ 是一个 H¨older 测度，μ 的支撑集空内部，且其补集是连通的。这里我们证明，在证明定理 1.2 时，这些条件并非必要。根据命题 2.12，对于任意 $\rho > 0$，存在一个 H¨older 概率测度序列 $\mu_n \in \mathcal{B}_{\Sigma(\rho)}$，使得 $\lim_{n\to\infty}\mu_n = \mu$。因此，通过对角线论证，证明可归结为 μ 为 H¨older 的情形。这足以处理 $\Sigma \subseteq \mathbb{R}$的情形，因此不妨设情况并非如此。

回顾第 2.3 节中的 $\Sigma \subset [a,b]\times[-c,c]$ 以及 $[a,b]\times[-c,c] = \bigcup_{0\leq i,j<2M} B_{ij}$，其中我们定义 $B_{ij} = [a_i, a_{i+1}]\times[c_j, c_{j+1}]$ 和 $a_i = a + \frac{i}{2M}(b-a)$ 以及 $c_j = -c + \frac{j}{2M}(2c)$。此外，对每个 $1 \leq k \leq n_{ij} = \lfloor (n+1)\mu(B_{ij})\rfloor + \epsilon_{ij}$，都有 $z_{ijk} \in B_{ij}$。通过覆盖论证，我们可以将 (15) 中的参数 A 取为 $-\frac{1}{2}\log_n(n^{-1}M^{-2+\delta}) \leq A < 1$。这里取 $M = \lfloor n^{1/3}\rfloor$ 和 $A = \frac{5}{6}$。现在我们定义一个测度，使其在围绕 z_{ijk} 的一组区间上均匀分布，从而模拟 μ。令 $\tilde{\mu}$ 为支撑在 $\bigcup_{ijk}\{z \text{ 上的测度：} |\mathrm{Re}(z - z_{ijk})| < \frac{1}{2(n+1)}, \mathrm{Im}(z) = \mathrm{Im}(z_{ijk})\}$，其中 $\tilde{\mu}$ 在每个区间上的限制都是该区间上的一维勒贝格测度。注意，由于 $|z_{ijk} - z_{i'j'k'}| \gg n^{-\frac{5}{6}}$，$\tilde{\mu}$ 是概率测度。现在令 $\tilde{\nu}$ 为 $\tilde{\mu}$ 的支撑集上的平衡测度，并令 $\tilde{\nu}_\epsilon$ 为 $\tilde{\nu}$ 在缩放映射 $x \mapsto (1+\epsilon)x$ 下的归一化推前测度。最后，定义 $\mu_{\epsilon,\epsilon'} = (1-\epsilon')\tilde{\mu} + \epsilon'\tilde{\nu}_\epsilon$，其中 $\epsilon, \epsilon' \in (0,1)$。

命题 3.1. 对于所有足够大的 n，$Q \in \mathbb{Z}[x]$、$0 < \epsilon$、$\epsilon' < \frac{1}{2}$、$\int$对数 $|Q(x)|d\mu_{\epsilon,\epsilon'}(x) \geq 0$。

证明。首先，我们将 $U_{\tilde{\mu}}$ 与 U_μ 联系起来。计算得

$$U_{\tilde{\mu}}(x) = \int \log|x-z|d\tilde{\mu} = \sum_{ijk}\int_{\frac{-1}{2(n+1)}}^{\frac{1}{2(n+1)}} \log|x-y-z_{ijk}|dy.$$

令 $\hat{z}$ 为 $P_{\mathcal{Z}}$ 的最近的根，使其最接近 x。那么根据 (14)，取 $M = \lfloor n^{1/3}\rfloor$ 可得 $\forall ijk \neq hrs$、$|x - z_{ijk}| \gg n^{-5/6}$。因此对于 $ijk \neq hrs$，我们有

$$\int_{\frac{-1}{2(n+1)}}^{\frac{1}{2(n+1)}} \log|x-y-z_{ijk}|dy - \frac{1}{n}\log|x-z_{ijk}| = \int_{\frac{-1}{2(n+1)}}^{\frac{1}{2(n+1)}} \log\left|1 - \frac{y}{x-z_{ijk}}\right| dy - \frac{\log|x-z_{ijk}|}{n(n+1)}.$$

由于 $\log\left|1 - \frac{y}{x-z_{ijk}}\right| \leq \frac{|y|}{|x-z_{ijk}|}$，这是 $O(n^{-7/6} + \frac{|\log|x-z_{ijk}||}{n^2})$。因此，若 $|x - \hat{z}| \geq n^{1/6}$，根据引理 2.1，我们有

$$U_{\tilde{\mu}}(x) = U_\mu(x) + O(n^{-1/6}).$$

否则，

$$U_{\tilde{\mu}}(x) = \int_{\frac{-1}{2(n+1)}}^{\frac{1}{2(n+1)}} \log|x-y-\hat{z}|dy + \frac{1}{n}\sum_{ijk\neq hrs} \log|x-z_{ijk}| + O(n^{-1/6})$$

在后一种情况下，$\int_{-1}^{2^{(n+1)}} \log|x-y-\hat{z}|dy \ll \max(n^{-1}\log(n)\int_{-1}^{2n}\log|y|dy) \ll n^{-1}\log(n)$。根据我们对命题 2.8 的证明，

$$\frac{\log|p_{\mathcal{Z}}^{efg+}(x)|}{n} - U_{\mu}(x) = \frac{\log\frac{|x-\hat{z}||x-\mathrm{Re}(z_{efg})|}{|x-z_{efg}||x-\overline{z_{efg}}|}}{n} + O\left(\frac{M^2\log(n)L}{n} + M^{-\delta/2}\log(n)^{1/2}\right).$$

取 $M \sim n^{1/3}$ 和 $L \sim n^{\frac{1}{3}-\frac{\delta}{6}}$，我们现在已经证明

$$U_{\tilde{\mu}}(x) = U_{\mu}(x) + O\left(n^{\frac{-1}{6}} + n^{\frac{-\delta}{6}}\log(n)\right).$$

因此，无论哪种情况，我们都有 $U_{\tilde{\mu}(x)} = U_{\mu}(x) + O(n^{-1/6} + n^{-\delta/6}\log(n))$。

现在，对于任意 $Q(x) = c\prod_{i=1}^{m}(x-\alpha_i) \in \mathbb{Z}[x]$，我们有

$$\int \log|Q(x)|d\mu_{\epsilon,\epsilon'} = (1-\epsilon')\int \log|Q(x)|d\tilde{\mu} + \epsilon'\int \log|Q(x)|d\tilde{\nu}_{\epsilon}$$

利用上面的计算，

$$\int \log|Q(x)|d\tilde{\mu} = \log|c| + \sum_{i=1}^{m} U_{\tilde{\mu}}(\alpha_i) = \int \log|Q(x)|d\mu + mO(n^{-1/6} + n^{\frac{-\delta}{6}}\log(n))$$

由于 $I_{\tilde{\nu}} \geq I_{\mu} \geq 0$，我们有

$$I(\tilde{\nu}_{\epsilon}) = \int\int \log|(1+\epsilon)(x-y)|d\tilde{\nu}d\tilde{\nu} = I(\tilde{\nu}) + \log|1+\epsilon| > I(\tilde{\nu}) + \epsilon - \epsilon^2. \tag{47}$$

现在我们估计 $I(\tilde{\nu})$。由于 $\tilde{\nu}$ 是 $\tilde{\mu}$支撑集上的平衡测度， $I(\tilde{\mu}) \leq I(\tilde{\nu})$。为了计算 $I(\tilde{\mu})$，我们首先注意到 $\int_{-1}^{2^{(n+1}} \int^{2)(n+1)-1} \log|\overline{x-y}|d\overline{x}d\overline{y} \ll n^{-2}\log(n)$。因此

$$I(\tilde{\mu}) = \sum_{ijk\neq i'j'k'} \int_{\frac{-1}{2(n+1)}}^{\frac{1}{2(n+1)}} \int_{\frac{-1}{2(n+1)}}^{\frac{1}{2(n+1)}} \log|z_{ijk} - z_{i'j'k'} + x - y|dxdy + O(n^{-1}\log(n)).$$

由前面的相同论证可知，这是 $\frac{1}{n^2}\sum_{ijk\neq i'j'k'}\log|z_{ijk}-z_{i'j'k'}| + O(n^{-1/6})$。将（17）应用于 $M \sim n^{1/3}$和 $L \sim n^{\frac{1}{3}-\frac{\delta}{6}}$， $I(\tilde{\mu}) = O(n^{-1/6} + n^{\frac{-\delta}{6}}\log(n))$。因此，当 n 足够大时， $|I(\tilde{\mu})| \leq \frac{\epsilon}{4}$。利用（47），我们有 $I(\tilde{\nu}_{\epsilon}) > \frac{\epsilon}{4}$，因为 $\epsilon < 1/2$。因此由于

$$\int \log|Q(x)|d\mu_{\epsilon,\epsilon'} = (1-\epsilon')\int \log|Q(x)|d\mu + m\left(\epsilon' I(\tilde{\nu}_{\epsilon}) + (1-\epsilon')O(n^{-1/6} + n^{\frac{-\delta}{6}}\log(n))\right)$$

根据 [ST97]，的公式 (I.1.9)，这表明当 n 充分大时， $\int \log|Q(x)|d\mu_{\epsilon,\epsilon'} > 0$。因此，对每个 $0 < \epsilon, \epsilon' < \frac{1}{2}$，都存在一个足够大的 n，使得 $\int \log|Q(x)|d\mu_{\epsilon,\epsilon'} > 0$，如所需。□

定理 *1.2* 的证明。假设 $d_{\Sigma} < 1$. 注意到

$$\log d_{\Sigma} = I(\mu_{eq}) = \sup_{\mu\in\mathcal{P}_{\Sigma}} I(\mu),$$

其中， μ_{eq} 是 Σ. 的平衡测度。因此，

$$I(\mu) < 0$$

对每个 $\mu \in \mathcal{P}_{\Sigma}.$，由多项式 $Q(x,\ y) = x - y$的定理 1.8,

$$\mathcal{B}_{\Sigma} = \emptyset.$$

由于 $\mathcal{A}_{\Sigma} \subset \mathcal{B}_{\Sigma}$，若 $d_{\Sigma} < 1.$，这就完成了定理 1.2 的证明

否则，$d_{\Sigma} \geq 1$ 且 $\mu_{eq} \in \mathcal{B}_{\Sigma}.$ 这意味着 $\mathcal{B}_{\Sigma} \neq \emptyset.$ 记 $\tilde{\mu}_{\epsilon,\ \epsilon'}$ 为命题 3.1 中所述、对应于给出该定理的 n 的最小值的测度。这说明 $\tilde{\mu}_{\frac{1}{m},\ \frac{1}{m}} \xrightarrow{*} \mu$当 $m \to \infty$ 时。此外，对于每个 m，存在一个多项式序列 $P_{m,\ n}$，满足 $\mu_{P_{m,\ n}} \xrightarrow{*} \tilde{\mu}_{\frac{1}{m},\ \frac{1}{m}}$ 当$n \to \infty$时。取一个子序列 $P_{m,\ n_m}$，我们有 $\mu_{P_{m,\ n_m}} \xrightarrow{*} \mu$ 当 $m \to \infty$ 时。因此，我们已经证明，μ 的支撑集必须具有非空内部且其补集必须连通这一假设是不必要的。定理 1.2 由定理 1.5 推出。□

最后，我们给出推论 1.3 的证明。

推论 *1.3* 的证明。设 $\Sigma = \bigcup_i (R_i \cup R_i) \bigcup_j I_j$ 且 $d_{\Sigma} > 1$。根据 [Smi21，命题 2.4]，，存在一个概率测度序列 $\mu_n \in \mathcal{B}_{\Sigma}$，其 H¨older 指数至少为 $1/2$，使得 $\lim_{n\to\infty} \mu_n = \mu$。因此，不妨设 μ 是 H¨older 的。根据命题 3.1，我们还可以进一步假设 μ 的支撑集包含于 Σ内，具有空内部，且其补集是连通的。

由超越有限直径 [FS55，定理 J], 的连续性可知，可以找到一个子集 $\Sigma_1 \subset \Sigma$，它是有限个矩形和区间的有限并，使得 $\Sigma_{1\mathbb{R}}(\rho) \subset \Sigma$ 且 $d_{\Sigma_1} > 1$。我们可以如下理解这一点。设 $\Sigma = \bigsqcup_i (R_i \sqcup R_i) \bigsqcup_j I_j$. 令 ℓ 为这些矩形和区间中最长边的长度，并令 d 为任意一对不同矩形或区间之间的最小距离；如果存在多个分量，则取该距离，否则取 1。现在令 $0 < \epsilon < \min(\frac{\ell\, d}{2\ell}\left(1 - \frac{1}{d_{\Sigma}}\right),)$。对于给定的$x \in \Sigma$，令 c_x 为它所在矩形或区间的中心。令 $\tilde{x} = x + \epsilon(c_x - x)$。这实质上是将每个矩形/区间以其中心为方向按因子 $1 - \epsilon$进行收缩。因此，对于 $x, y \in \Sigma$，如果 $c_x = c_y$，则 $|\tilde{x} - \tilde{y}| = (1 - \epsilon)|x - y| > \frac{1}{d_{\Sigma}}|x - y|$。否则，根据三角不等式，由于 $|c_x - x| < \ell$，我们有 $|\tilde{x} - \tilde{y}| \geq |x - y| - 2\epsilon\ell$。注意，如果 $c_x \neq c_y$，那么 $|x - y| > d$，在这种情况下

$$|\tilde{x} - \tilde{y}| \geq |x - y| - 2\epsilon\ell > \frac{1}{d_{\Sigma}}|x - y|.$$

现在，对每个 $n \in \mathbb{N}$，令 $x_{n,\ 1}$、$x_{n,\ 2}$、.....、$x_{n,\ i}$ 为 Σ 的费克特点。于是

$$d_{\Sigma_1} \geq \lim_{n\to\infty} \prod_{1 \leq i < j \leq n} |\tilde{x}_{n,i} - \tilde{x}_{n,j}|^{\frac{1}{\binom{n}{2}}} > \frac{1}{d_{\Sigma}} \lim_{n\to\infty} \prod_{1 \leq i < j \leq n} |x_{n,i} - x_{n,j}|^{\frac{1}{\binom{n}{2}}} = 1.$$

因此，存在某个由矩形和区间组成的有限不交并 Σ_1 和 $\rho > 0$，使得 $\Sigma_1(\rho) \subset \Sigma$，其中 $d_{\Sigma_1} > 1$，如所述。[1]

注意，第 (3.1) 节中定理 1.5 的证明所用的论证稍作修改后仍然适用。更确切地说，我们按照定理 1.5 的证明构造 $p_{\mathcal{Z}}$，并对 Σ_1 和 $P_{\mathcal{Z}}$ 应用命题 2.16，从而得到 $Q_m(x)$，使得 $p_{\mathcal{Z}}(x)Q_m(x)$ 在 Σ 内有 n 个不同根，这些根与 Σ 的边界相距 n^{-3}。此外，我们有

$$|p_{\mathcal{Z}}(z)Q_m(z)| \geq |z - \hat{z}|e^{(n-m)U_{\mu}(z)}\kappa^m n^{-Cn^{1-\frac{\delta}{6}}}.$$

其中 $|z - \hat{}z| = \min_{p_{\mathcal{Z}}(\alpha)Q_m(\alpha)=0} |z - \alpha|$。我们利用上述不等式和介值定理，在 $\bigcup I_j$ 上证明两个多项式 $p_{\mathcal{Z}}(x)Q_m(x)$ 和

[1]在一次私下交流中，Rumely 教授友好地概述了另一种论证，可用于证明更一般的 Σ 的容量的连续性。

$h_n(x) = p_{\mathcal{Z}}Q_m(x) - \sum_{i=0}^{n-1-m}\beta_i P_i(x)$ 相同。我们在 $\bigcup_i(R_i \cup R_i)$ 的边界上应用上述不等式和 Rouch´e's 定理，证明 $p_{\mathcal{Z}}(x)Q_m(x)$ 和 $h_n(x)$ 在 $\bigcup_i(R_i \cup R_i)$ 内的复根数相同。由此完成了推论的证明。□

4. The Algorithm

4.1. 格算法。 我们开发的算法需要在格中访问短向量。正如 Micciancio [Mic01], 的研究所示，计算出一个长度不超过格中最短向量长度某个常数倍的向量是 NP 难问题。这被称为最短向量问题，或 SVP。通常来说，在格中获得短向量仍然是有益的。由 Lenstra、Lenstra 和 Lov´asz 开发的一种称为 LLL算法的算法，可以在多项式时间内找到格的一组向量基 [LLL82] ，其中输出的最短向量长度不超过格中最短向量长度的一个指数倍。在该算法的实现中，我们使用 PARI/GP 内置的 qflll 方法。向 qflll 方法提供一个矩阵 A ，其列生成一个格后，它会返回一个变换矩阵 T，使得 AT构成该格的一组"LLL 约化"基。虽然 LLL算法在实践中相当实用，但其渐近界还不足以证明存在一个次指数因子。

1986年，Schnorr [Sch87] 提出了一族参数化算法，用于解决SVP问题。这些算法根据输入参数，输出的约化基所满足的条件介于严格的Korkine-Zolotarev约化要求与较宽松的LLL约化要求之间。精心选择参数，可以在多项式时间内达到略微亚指数的常数因子。Schnorr证明，若该算法生成基 $b_1, \ldots, b_n$，则 $||b_1||$ 与格中的最短向量相差一个亚指数因子。我们进一步证明，若 $\lambda_1, \ldots, \lambda_n$ 满足以下条件： λ_i 是存在 i 个范数不超过 λ_i的线性无关向量时所能取到的最小值，那么对每个 $i = 1, \ldots, n$， $||b_i||$ 与 λ_i相差一个亚指数因子。现在，我们介绍Schnorr研究中的一些记号，并回顾他的部分结果。

设 $b_1, \ldots, b_n$ 为一组基。令 b_i^* 为 b_i 在 $i = 1, \ldots, n$的张成空间的正交补上的投影。通过不进行归一化的Gram-Schmidt正交化过程，可以得到 $b_1 = b_1^*, b_2^*, \ldots,$ 和 b_n^*。现在定义 $\mu_{i,j} := \frac{\langle b_i \quad b_j^* \rangle}{||b_j^*||^2}$。

定义 4.1. 如果 $b_1, \ldots, b_n$ 满足 $\mu_{i,j} \leq 1/2$ 对所有 $i > j$成立，则称其为尺寸约化的。

定义 4.2. 设 Λ_i 是由 $b_i, b_{i+1}, \ldots, b_n$ 在 span$\{b_1, \ldots, b_{i-1}\}$ 的正交补上的投影所张成的格。若 $||b_i^*||$ 是 Λ_i 中非零向量里的最小向量，则称 $b_1, \ldots, b_n$ 为 Korkine-Zolotarev 约化的。

定义 4.3. 设 $k \mid n$。若 $b_1, \ldots, b_n$ 是半 k-约化的，则称其为半 k-约化的，当且仅当它是尺寸约化的，并且满足以下两个条件

$$||b_{ik}^*||^2 \leq 2||b_{ik+1}^*||^2, \tag{48}$$

并且，对于 $j = 1, \ldots, k$， b_{ik+j} 中与 $b_1, \ldots, b_{ik-1}$ 正交的分量都是 Korkine-Zolotarev 约化的。将此性质称为 KZ 性质。

最后，常数 α_k 定义为 max $\frac{||b_1||^2}{||b_k^*||^2}$，其中最大值取遍所有秩为 k的格上的 Korkine-Zolotarev 约化基。Schnorr 论文中的推论 2.5 表明， $\alpha_k \leq k^{1+\log k}$。

定理 4.4. 设 $b_1, \ldots, b_n$ 是一个半 k-约化基， λ_j 是使得由 $b_1, \ldots, b_n$ 张成的格中存在 j 个范数不超过 λ_j 的线性无关向量的最小实数。则 $||b_j|| \leq k^{\frac{n}{k}\text{对数 } k + O(\frac{n}{k}\text{+对数 } k)}\lambda_j$。

其核心是结合了 [Sch87] 中定理 2.3 和 3.4 的证明。

证明。固定 $1 \le j \le n$。假设 $v_1, \ldots, v_j$ 是格中的线性无关向量，且 $||v_i|| = \lambda_i$ 对于 $i = 1, \ldots, j$ 成立。对于每个 i，写作 $v_i = \sum_{s=1}^{n} c_{s,i} b_s$。令 s_i 为满足 $c_{s_i,i} \neq 0$ 的最大指标。由线性无关性，存在某些 $i = 1, \ldots, j$，使得 $s_i \ge j$。若 $c^*_{s,i}$ 满足 $v_i = \sum_{s=1}^{n} c^*_{s,i} b^*_s$，则 $c_{s_i,i} = c^*_{s_i,i} \in \mathbb{Z}$。这意味着 $\lambda_j = ||v_j|| \ge ||v_i|| \ge ||c^*_{s_i,i} b^*_{s_i}|| \ge ||b^*_{s_i}||$。现在注意，对于每个 $0 < s < t \le k$，以及满足 $(m+1)k \le n$ 的 m，则 $||b^*_{mk+s}|| \le \alpha_k ||b^*_{mk+t}||$，如 [Sch87] 中定理 2.3 的证明所述，并将此不等式记为 $(*)$。

利用 $b_1, \ldots, b_n$ 是尺寸约化的这一事实，

$$||b_j|| = \left|\left| b^*_j + \sum_{s=1}^{j} \mu_{j,s} b^*_s \right|\right| \le \sum_{s=1}^{j} ||b^*_s||.$$

为了界定 $||b^*_s||$ f 或者 $1 \le s \le j$，假设 $s = m_1 k + t_1$ 且 $s_i = m_2 k + t_2$，对于 $0 \le t_2, t_2 < k$。该 n

$$\begin{aligned}
||b^*_s|| &\le \alpha_k ||b^*_{(m_1+1)k}|| && \text{由 KZ 性质和 } (*) \text{ 得出} \\
&\le 2\alpha_k ||b^*_{(m_1+1)k+1}|| && \text{by (6)} \\
&\le (2\alpha_k)^{m_2 - m_1} ||b_{m_2 k+1}|| && \text{通过归纳法} \\
&\le (2\alpha_k)^{m_2 - m_1} \alpha_k ||b^*_{s_i}|| && \text{由 KZ 性质和 } (*) \text{ 得出，因为 } j \le s_i \\
&\le (2\alpha_k)^{\frac{n}{k} - \lfloor \frac{s}{k} \rfloor} \alpha_k \lambda_j && \because ||b^*_{s_i}|| \le \lambda_j.
\end{aligned}$$

由于 $\alpha_k \le k^{1+\log k}$，我们有 $||b^*_s|| \le k^{(\frac{n}{k}+1)(\log k+2) - \lfloor \frac{s}{k} \rfloor \log k}$。因此，

$$\begin{aligned}
||b_j|| &\le k^{\frac{n}{k}\log k + O(\frac{n}{k} + \log k)} \sum_{s=0}^{\infty} k^{-\lfloor \frac{s}{k} \rfloor \log k} \lambda_j \\
&\le k^{\frac{n}{k}\log k + O(\frac{n}{k} + \log k)} k \sum_{s=0}^{\infty} k^{-s \log k} \lambda_j && \text{since every group of } k \text{ is equal} \\
&\le k^{\frac{n}{k}\log k + O(\frac{n}{k} + \log k)} \left(1 - k^{-\log k}\right)^{-1} \lambda_j \\
&\le k^{\frac{n}{k}\log k + O(\frac{n}{k} + \log k)} \lambda_j && \text{since } (1 - k^{-\log k})^{-1} \le 3 \text{ for } k \ge 2.
\end{aligned}$$

证明至此完成。 □

根据 Schnorr 的论文，该算法对 $O(n\log B)$ 个整数执行 $O(n^4 \log B + k^{\frac{k}{2}+o(k)} n^2 \log B)$ 个算术步骤，其中 B 是最长输入向量的欧几里得长度。在我们的情形中，B 是依赖于 μ 的常数。取 $k = \log(n) \log(\log(n))$，则其为 $O(n^4 + n^2 \log(n)\, 3 \log_2 \frac{n}{\log \log n})$，这属于 $O(n^4)$，因此这种对 k 的选择使算法在 n 上具有多项式时间复杂度。在 $2n \log(\log(n))^3$ 这种情形下，当 n 足够大时，定理 4.4 中的因子至多为 $e \log(n)$；特别地，它是亚指数的。

4.2. 数论几何。 关于几何，我们的算法包含两种不同的子方法。第一种用于求给定格的短基。第二种用于求一个接近实系数多项式的整系数多项式，其中距离是相对于给定基来度量的。在这两种算法中，P 是一个根为 $\alpha_1, \ldots, \alpha_n$ 的整系数、无平方因子首一多项式。

4.2.1. 求短格基。 为了求短格基，我们实现了命题 2.11 的一个版本。该定理表明，在给定的凸空间中存在一个由多项式构成的短基。具体而言，令 K 为次数至多为 n、满足 $\log |P(x)| \leq nU_\mu(x)$ 的实多项式集合。存在 $P_0, \ldots, P_n$ 个线性无关的整系数多项式，使得对每个 $0 \leq k \leq n$，若 $P_k \in \lambda K$，其中 $\lambda \in \mathbb{R}$ 取最小值，则对于任何与 $P_0, \ldots, P_{k-1}$ 线性无关的 $\rho < \lambda$，ρK 中都不存在整系数多项式。我们在命题 2.14 中证明，这些 λ 中的最大值相对于 n 是亚指数的。因此，$\{P_0, \ldots, P_n\}$ 构成了一个基，其格点位于 K 的一个亚指数倍范围内。根据定理 4.4，我们可以在关于 n 的多项式时间内，计算出与 K 相差至多一个亚指数因子的显式整系数多项式。推论 4.5 对此作了形式化表述。本节余下部分中，假设 $\Sigma \subset \mathbb{C}$ 是紧的、内部为空且补集连通。

推论 4.5. 若 $\mu \in \mathcal{B}_\Sigma$ 是 *H¨older* 概率测度，则我们可以在多项式时间内计算出一组基 $Q_0, \ldots, Q_n$，它们是次数至多为 n 的整系数多项式，其中每个 $Q_i \in e^{Cn^{\log(\log(n))^3}} K_n$，这里某个固定常数 C 仅取决于 Σ 和 μ。更具体地说，该算法运行时间为 $O(n^4)$，并且假设 n 足够大，我们可以取 $C = 3$。

证明。 首先，按照 (25) 中的定义，取 $M = \lfloor n^{1/3} \rfloor$，计算次数小于 n 的多项式的一组基 $p_{\mathcal{Z}}^{efg\pm}$。将这组基记为 $\mathcal{S}$。根据命题 2.8，我们要找一组在基 $\mathcal{S}$ 下较短的整系数基。现在将 $\mathcal{E} := \{1, x, \ldots, x^{n-1}\}$ 用基 $\mathcal{S}$ 表示，并应用 Schnorr 算法，取 $k = \log n \log\log n$，得到一组半 k-约化基。我们在第 4.1 节末尾证明了，该算法的运行时间 在 $O(n^4)$ 时间内，并且输出多项式 Q_0、……、Q_n 满足：对于每个 i，当固定 ~~c 且 n~~ 足够大时，由命题 2.14 可得 $Q_i \in e^{2n \cdot \log(\log(n))^3} \log n \; n^{cn^{1-\frac{\delta}{12}}} K_n$。因此，当 n 足够大时，$Q_i \in e^{3n \cdot \log(\log(n))^3} \log n \; K_n$。 □

计算整系数多项式的一种方法如下。设 T 是一个矩阵，使得 AT 是 A 的约化形式（如Schnorr算法中所述），其中 A 是用基 $\mathcal{S}$ 表示的 $\mathcal{E}$ 的矩阵。那么，AT 的列线性无关，并且用基 $\mathcal{S}$ 表示这类多项式。因此，T 的列就如所需的那样，用基 $\mathcal{E}$ 表示这些多项式。由此可得到所需的 $n+1$ 个线性无关的整数系数多项式。此外，请注意，通过矩阵求逆进行基变换，对于大型矩阵而言，数值稳定性可能较差。幸运的是，我们可以显式地计算基变换矩阵。与通常做法一样，本文给出的时间界以算术运算次数计。本文不研究数值稳定性。

4.2.2. 寻找近似整数多项式。 以下讨论使我们能够通过算法构造出类似于 [Smi21] 的定理 3.2 中证明存在的多项式。此方法旨在用多项式时间找到一个接近给定实系数多项式的整系数多项式，其中距离是相对于给定基来度量的。在我们的情形中，我们使用推论 4.5 得到的基。

定理 4.6。 给定一个 *H¨older* 概率测度 $\mu \in \mathcal{B}_\Sigma$，存在一种多项式时间算法，输入一个次数小于 n 的实系数多项式 $Q(z)$，并输出一个次数小于 n 的整数系数多项式 H，使得 $\log(Q - H(x)) \leq U_\mu(x) + Cn \cdot \log(\log(n))^3 \log(n)$。运行时间为 $O(n^4)$，~~其中 C 仅依赖于 μ 和 Σ。假设 n 足够大~~，我们可以选取 $C = 4$。

证明。 令 $Q_0, \ldots, Q_{n-1}$ 为我们在推论 4.5 中描述的算法的输出。将此基 $\mathcal{Q}$ 记为 $\tilde{c}_0$ 假设 $[Q]_{\mathcal{Q}}$ 的第 c_j 个坐标为 $\tilde{c}_j$。取 $c_j \in \frac{1}{2}\mathbb{Z}$ 为最接近的整数（若 H 则向上取整），并令 $[H]_{\mathcal{Q}} = \begin{pmatrix} \\ \text{为满足} \\ \\ \tilde{c}_{n-1} \end{pmatrix}$ ... H 的

多项式。那么 $[H]_{\mathcal{Q}}$ 是整数系数多项式，因为 $\mathcal{Q}$ 是基 $[H]_{\mathcal{Q}}$ 中的整系数多项式的整数线性组合。我们知道

$Q-H=\sum_{j=1}^{n}(c_j-\tilde{c}_j)Q_j$。因此 $Q-H\leq \frac{n}{2}e^{3n\cdot \frac{}{\log(\log(n))^3\log(n)}}e^{nU_\mu}$所以 $Q-H\leq e^{\frac{4n}{\log(\log(n))^3\log(n)}}$ e^{nU_μ}对足够大的 n 成立，正如所需。关于运行时间的分析，我们注意到 Schnorr算法是瓶颈。根据推论 4.5，其运行时间为 $O(n^4)$。□

4.3. **主算法**。这里我们证明定理 1.6。我们已经介绍了主要概念。根据推论 4.5，我们可以用 K_n 的亚指数倍时间得到一组整系数多项式的基。现在，如果我们对 $_{14}(p_{\mathcal{Z}}-x^n)+\frac{1}{2}$ 应用定理 4.6，得到 $H(x)$，便可以输出 $P_n(x):=x^n+4H(x)-2$。这样就能在 K_n 的亚指数倍时间内得到一个艾森斯坦多项式。如果我们只需要一个 P，其 n 范数较小，这样就足够了；然而，对于给定的开集 $D\supset\Sigma$，我们还必须引入一些额外步骤，以确保 $\mathrm{supp}(\mu_{P_n})\subset D$。证明将仿照定理 1.5 的证明。

定理 *1.6* 的证明。设 $\mu\in\mathcal{B}_\Sigma$ 是指数为 δ 的 H¨older 测度，令 D 为包含 Σ 的任意开集，并选择 $\rho>0$ 使得 $\Sigma(\rho)\subset D$。按照第 2.3 节所述，在满足 $L=1$ 的条件下选择 $\mathcal{Z}=\{x_1,\ldots,x_{n-m}\}$。对 $p_{\mathcal{Z}}$ 应用命题 2.15，其中 m 将在稍后选定，从而得到多项式$Q_m(x)$。注意，命题 2.15 的证明明确地在多项式时间内计算 $Q_m(x)$。与定理 1.5 的证明一样，令 $p_{\mathcal{Z}}(x)Q_m(x)$ 由 $x^n+\sum_{i=0}^{n-1}a_ix^i$ 给出。对其应用定理 4.6

$$h(x):=\frac{1}{4}\left(p_{\mathcal{Z}}(x)Q_m(x)-x^n-\sum_{i=n-m}^{n-1}a_ix^i\right)+\frac{1}{2}$$

得到一个整数系数多项式 $H(x)$。最后，

$$p(x):=x^n+\sum_{i=n-m}^{n-1}a_ix^i+4H(x)-2$$

是一个在 2 处的艾森斯坦多项式。我们看到

$$|p_{\mathcal{Z}}(x)Q_m(x)-p(x)|=|4\left(h(x)-H(x)\right)-2|\leq e^{Cn\cdot\frac{\log(\log(n))^3}{\log(n)}}e^{(n-m)U_\mu(x)} \tag{49}$$

根据定理 4.6，存在一个仅依赖于 μ 和 Σ 的常数 C。如同定理 1.5 的证明中一样，我们有

$$|p_{\mathcal{Z}}(x)Q_m(x)|\geq\kappa^m n^{-cn^{1-\frac{\delta}{6}}}e^{(n-m)U_\mu(x)}$$

对于每个满足 $M=\lfloor n^{1/3}\rfloor$的 $x\notin\Sigma(\rho)$。当 n 足够大时，我们可以选择 $m<n$，使得 $m=\lceil\frac{2Cn}{\log(\kappa)\cdot\log(\log(n))^3\log(n)}\rceil$，其中我们按定理 4.6 中的方式选择 $C=4$。那么，当 n 足够大时，

$$|p_{\mathcal{Z}}(x)Q_m(x)|\geq|p_{\mathcal{Z}}(x)Q_m(x)-p(x)|$$

对于所有 $x\notin\Sigma(\rho)$。根据 Rouche 定理，由于 $p_{\mathcal{Z}}(x)Q_m(x)$ 的所有根都在 $\Sigma(\rho)$ 中，因此 $p(x)$ 的所有根也都在其中。此外，由 (49),

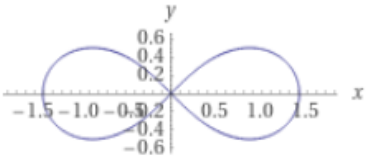
$$||p||_n\leq e^{Cn\cdot\frac{\log(\log(n))^3}{\log(n)}}+||p_{\mathcal{Z}}(x)Q_m(x)||_n\leq e^{\tilde{C}n\cdot\frac{\log(\log(n))^3}{\log(n)}}$$

˜存在一个仅依赖于 Σ 和 μ 的常数 C。 □

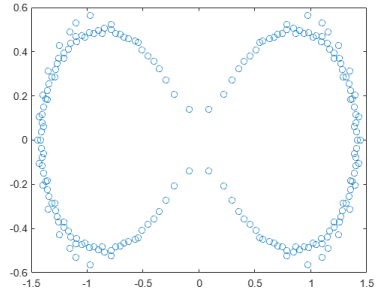
5. Applications

5.1. **数值数据**。我们对上述算法进行了简化实现。[2]首先，我们使用了 PARI/GP 中实现的 LLL算法 qflll。其次，我们没有按照论文中的指示选择 z_{ijk}，而是采用了各个数值示例中所述的合理抽样方法。此外，我们也没有执行额外步骤，将根强制置于测度支撑集的 ρ-邻域内

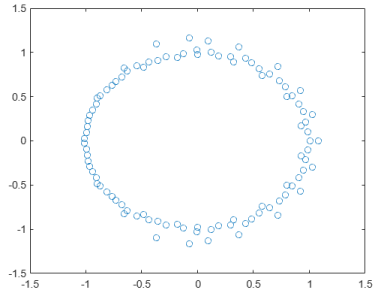
[2]第5节中的所有示例均可在 https://github.com/Bryce-Orloski/Limiting-Distributions-of-Conjugate-Algebraic-Integers-Applications 查阅。



(A) $|z^2 - 1| = 1$的图像



(B) 绘出的根或次数为 200 多项式



(C) 输出根的映射，通过 $z \mapsto z^2 - 1$

FIGURE 2. 这些结果展示了算法在双纽线上的有效性。

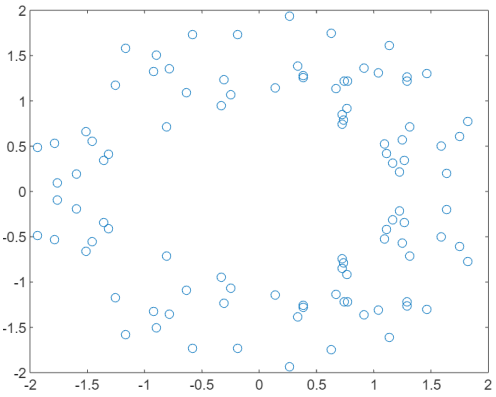
。因此，这些算法输出并未充分发挥算法的全部效能，但正如我们所见，它仍能快速给出有力的结果。本小节中的所有示例均使用宾夕法尼亚州立大学的 ROAR 服务器计算，且在最多两分钟内得出了结果。

我们讨论的第一个例子见图 1。图中所示的测度属于 Serre [宾夕法尼亚州08]构造的一个测度族。具体而言，它是 μ 上的概率分布，其中 $\Sigma = [a, b]$满足 $\mu = c\mu_{[a,b]} + (1 - c)\nu_{[a,b]}$，这里 $a = 0.1715$， $b = 5.8255$， $c = 0.5004$， $\mu_{[a,b]}$ 是 $[a, b]$上的平衡测度，而 $\nu_{[a,b]}$ 是 $[b^{-1}, a^{-1}]$ 上的平衡测度在映射 $z \to 1/z$下的推前测度。我们通过将 k^{th} 个样本点取为 μ 在 k/n处的分布函数的反函数，来计算 μ 的样本点。要求计算一个次数为 100 的多项式（样本点已预先计算）时，算法在 ROAR 服务器上运行了约 3 秒。输出多项式的根全为实根，其直方图见图 1b。图 1b 中的端点和区间宽度均为近似值。

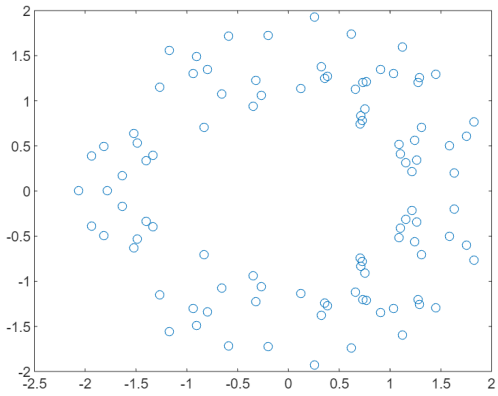
第二个例子如图 2 所示。图 2a 展示了通过 $|z^2 - 1| = 1$ 对单位圆上的均匀分布进行拉回后所得分布的支撑集。我们根据该分布对这个支撑集进行了抽样，并在 200 个样本上运行了算法。算法在两分钟内运行完毕，其根的图示见图 2b。我们希望对圆上的均匀分布进行拉回抽样。为了检验抽样是否充分，图 2c 绘出了这些根在映射 $z \mapsto z^2 - 1$ 下的像，可以看到它们大致近似于单位圆上的均匀分布。

最后一个例子如图 3 所示。这里，我们通过蒙特卡罗方法抽取 50 个复数，并取其复共轭，从而对环域 $1 \leq |z| \leq 2$ 中的 100 个复数进行了抽样。结果如图 3a 所示。将这些样本用于我们的算法后，算法在两分钟内返回了一个 100 次的首一整系数不可约多项式，其根绘于图 3b。请注意，定理 1.6 仅保证当 Σ 具有空内部且补集连通时，算法能在多项式时间内收敛。环域不具备这两个性质，不过算法仍然表现良好。

请注意，我们无法通过 LLL算法严格证明所需的收敛性；即使使用 Schnorr算法，我们所证明的收敛速度也非常慢。然而，这里我们应用 LLL算法，并且在图1、2c和3中可以看到，该算法生成的多项式的根的分布图与相应样本的分布图非常接近。



(A) 从环域 $1 \leq |z| \leq 2$ 中均匀采样的 50 个点及其共轭元的图



(B) 100 次多项式的根图
算法以这些样本为输入所得的结果

FIGURE 3. 左图显示从 $1 \leq |z| \leq 2$ 中均匀采样的 50 个点，右图显示算法输出的根；该算法试图近似左图中的分布。

5.2. **阿贝尔簇的应用**。 最近，Shankar 和 Tsimerman [ST18], [ST21] 猜想，对于每个 $g \geq 4$，每个定义在 $\mathbb{F}_q$ 上的阿贝尔簇都同源于一个定义在 $\mathbb{F}_q$. 上的曲线的雅可比簇。给定一个有限域 $\mathbb{F}_q$ 和任意大的扩域 $\mathbb{F}_{q^n}$，我们证明，在 $\mathbb{F}_q$ 上存在无穷多个阿贝尔簇，它们不同源于任何 $\mathbb{F}_{q^n}$ 上的曲线的雅可比簇。我们使用 Honda-Tate 理论，并构造一个满足若干矩条件的算术测度。首先，我们介绍受 Tsfasman 和 Vladut [TV97] 的工作启发而提出的矩条件。

设 X 是定义在 $\mathbb{F}_q$上的一条有限曲线。令 $N_r(X) := \#X(\mathbb{F}_{q^r})$ 表示 X. 的 $\mathbb{F}_{q^r}$ 个数。根据 Weil 公式，我们有

$$0 \leq N_r(X) = q^r + 1 - 2q^{r/2} \sum_{j=1}^{g} \cos(r2\pi\theta_j), \tag{50}$$

其中 $\sqrt{q}e^{2\pi i\theta_i}$ 是弗罗贝尼乌斯特征值。我们有

$$N_r(X) = \sum_{d|r} dM_d(X),$$

其中 $M_d(X)$ 是次数为 d. 的点的数量。由莫比乌斯反演公式，

$$M_r(X) = \frac{1}{r} \sum_{d|r} \mu(d) N_{\frac{r}{d}}(X).$$

特别地，我们有

$$\sum_{d|r} \mu(d) N_{\frac{r}{d}}(X) \geq 0$$

对于每个 $r \geq 0$.

设 $S_{\sqrt{\alpha}} := \{\sqrt{\alpha}e^{2\pi i\theta} : \theta \in [0,1)\}$ 为以原点为中心、半径为 $\sqrt{\alpha}$ 的圆，并在 $S_{\sqrt{\alpha}}$ 上定义如下概率测度

$$d\mu_q := \left(1 + \sum_{k=1}^{\infty} \frac{c}{k^2}\cos(k2\pi\theta)\right) d\theta.$$

其中 $c = \frac{6}{\pi^2 10}$. 注意

$$0 \le 0.9d\theta \le d\mu_q \le 1.1d\theta. \tag{51}$$

命题 5.1。 假设 $\alpha > 1.65$ 则 $U_{\mu_\alpha}(z) \ge 0$ 对任意 $z \in \mathbb{C}$. 因此， $d\mu_\alpha$ 是一个算术测度。

证明。这 只需证明 $U_{\mu_\alpha}(z) \ge 0$ 对任意 $z \in \mathbb{C}$. 假设 $|z| \ge 2\sqrt{\alpha}$，则

$$U_{\mu_\alpha}(z) = \int_{S_{\sqrt{\alpha}}} \log|z - \sqrt{\alpha}e^{2\pi i\theta}| d\mu_\alpha \ge \log\sqrt{\alpha} \ge 0.$$

否则，假设 $|z| < 2\sqrt{\alpha}$. 由 (51)，可得

$$\begin{aligned}
U_{\mu_\alpha}(z) &= \int_{S_{\sqrt{\alpha}}} \log|z - \sqrt{\alpha}e^{2\pi i\theta}| d\mu_\alpha \\
&= \int_{|z-\sqrt{\alpha}e^{2\pi i\theta}|<1} \log|z - \sqrt{\alpha}e^{2\pi i\theta}| d\mu_\alpha + \int_{|z-\sqrt{\alpha}e^{2\pi i\theta}|>1} \log|z - \sqrt{\alpha}e^{2\pi i\theta}| d\mu_\alpha \\
&\ge 1.1\int_{|z-\sqrt{\alpha}e^{2\pi i\theta}|<1} \log|z - \sqrt{\alpha}e^{2\pi i\theta}| d\theta + 0.9\int_{|z-\sqrt{\alpha}e^{2\pi i\theta}|>1} \log|z - \sqrt{\alpha}e^{2\pi i\theta}| d\theta \\
&= 1.1\int_{S_{\sqrt{\alpha}}} \log|z - \sqrt{\alpha}e^{2\pi i\theta}| d\theta - 0.2\int_{|z-\sqrt{\alpha}e^{2\pi i\theta}|>1} \log|z - \sqrt{\alpha}e^{2\pi i\theta}| d\theta \\
&\ge 1.1\log(\sqrt{\alpha}) - 0.2\log(3\sqrt{\alpha}) > 0.
\end{aligned}$$

这就完成了命题的证明。 □

推论 5.2. 存在一个由 $\{A_g\}$ 个普通阿贝尔簇组成的序列，它们定义在 $\mathbb{F}_q$ 上，且 $\dim(A_g) = g$，其弗罗贝尼乌斯特征值在 $g \to \infty$ 时按 μ_q 等分布。

证明。 令 $\alpha_n := \sqrt{q} - \frac{1}{10n}$, $\Sigma_n := [-2\alpha_n, 2\alpha_n]$ 且 $h_n(z) := z + \frac{\alpha_n}{z}$. 注意， h_n 是一个共形映射，它在无穷远处有无穷远不动点，且在无穷远处的导数为 1，并将 $\mathbb{C}\backslash S_{\alpha_n}$ 映到 $\mathbb{C}\backslash\Sigma_n$。 令 $h_n d\mu_{\alpha_n}$ 为 μ_{α_n} 经 h_n. 的推前测度。由势函数的共形不变性及命题 5.1 可知， $h_n d\mu_{\alpha_n}$ 具有正势函数，因此 $h_n d\mu_{\alpha_n}$ 是算术的。由定理 1.2 可知，存在一个不可约多项式序列 $\{p_m\}$，其位于 $\Sigma_n(\frac{1}{100n}) \subset [-2\sqrt{q}, 2\sqrt{q}]$ 内的根均为实根，且 $\gcd(p_m(0), q) = 1$，其根分布收敛于 $h_n d\mu_{\alpha_n}$. 。令

$$f_m(x) := x^{\deg p_m} p_m(x + \frac{q}{x}).$$

注意， $f_m(x)$ 的所有根都在 $S_{\sqrt{q}}$ 上，且 $\gcd(f_m(0), q) = 1$。由塞尔定理 [Ser20, 定理 3.1.2] 在普通情形下可知， f_m 是某个维数为 m 的阿贝尔簇普通同源类的特征多项式。现在，通过对角线论证，并令 $n \to \infty$ 且取 m 足够大，可知存在一个由定义在 $\mathbb{F}_q$ 上的普通阿贝尔簇构成的序列 $\{A_g\}$，使得 $\dim(A_g) = g$，且其弗罗贝尼乌斯特征值在 $g \to \infty$ 趋于无穷时按 μ_q 等分布。 □

定理 5.3。 设 $\{A_g\}$ 是定义在 $\mathbb{F}_q$ 上的任意阿贝尔簇族，使得 维数$(A_g) = g$，且其弗罗贝尼乌斯特征值的分布收敛于 μ_q. 。给定任意整数 $r \ge 0$，存在 N，使得若 $g \ge N$，则 A_g 不与定义在 $\mathbb{F}_{q^r}$ 上任何曲线的雅可比簇同源。

证明。 反设存在一个子序列 $\{A_{g_i}\}$，由定义在 $\mathbb{F}_q$ 上的阿贝尔簇组成，使得其弗罗贝尼乌斯特征值等分布于 μ_q，并且它们也与定义在 $\mathbb{F}_{q^r}$ 上的曲线 $\{X_{g_i}\}$ 的雅可比簇同源，其中 $r \geq 0.$。由 (50) 可得

$$0 \leq \frac{N_r(X_{g_i})}{g_i} = \frac{q^r + 1 - 2q^{r/2}\sum_{j=1}^{g_i}\cos(r2\pi\theta_j)}{g_i}.$$

令 $g_i \to \infty$ 趋于极限，我们得到

$$0 \leq -2q^{r/2}\lim_{g_i\to\infty}\frac{\sum_{j=1}^{g_i}\cos(r2\pi\theta_j)}{g_i} = -2q^{r/2}\int\cos(r2\pi\theta)d\mu_q = -q^{r/2}\frac{c}{r^2} < 0,$$

这就产生了矛盾。至此，我们的定理得证。 □

如引言中所述，我们使用论文第4节中描述的算法构造了一个次数为290的多项式 $p(x)$。与第5节中的其他结果一样，这一结果是通过LLL算法实现的，且没有使用迫使根落在所需支撑集内的构造方法。最高次项为

$$p(x) = x^{290} - 28x^{289} - 484x^{288} + 20784x^{287} + \cdots.$$

该多项式的最大系数有105位。所有根都位于 $[-2\sqrt{3}, 2\sqrt{3}] \subset \mathbb{R}$内，因此根据本田-泰特理论，[3] 它对应于 $\mathbb{F}_3$ 上的一个阿贝尔簇，其特征多项式为 $x^{290r}p(x+3/x)^r$，其中某个指数为 $r.$。我们通过计算 $p(x)$的常数项，验证了相应的阿贝尔簇是普通的；该常数项与3互素。事实上，它是

$$19875183005444505756032705281200952405059895953380115355156299268417070$$

它不能被3整除。根据Serre的一个定理 [Ser20，定理3.1。2]，在普通情形下 $r = 1$；参见 [Ser20] 第24页的例a）。[3] 计算该簇的 N_2，得到−2。因此，它不是 $\mathbb{F}_9$上任何曲线的雅可比簇。

References

[Ahl10] Lars V. Ahlfors. *Conformal invariants*。AMS Chelsea Publishing，普罗维登斯，罗得岛州，2010年。几何函数论专题，1973年原版重印，由 Peter Duren、F. W. Gehring 和 Brad Osgood 撰写前言。[AP08] Juli
´ *Number* an Aguirre 和 *theory and polynomials* 352 *London Math. Soc. Lecture Note Ser.* 1 19 Juan Carlos Peral。全正代数整数的迹问题。载于，第 卷，页码 – 。剑桥大学出版社，剑桥，2008年。附录由 Jean-Pierre Serre 撰写。[BE95] Peter Borwein 和 Tam
´ ´ *Polynomials and polynomial inequalities* 161 *Graduate Texts* as Erdelyi。， *in Mathematics* 1995 第 卷。Springer-Verlag，纽约，。[BR10] Matthew Baker 和 Robert Rumely。 *Potential theory and dynamics on the Berkovich projective line*，第159卷， *Mathematical Surveys and Monographs*。美国数学会，普罗维登斯，罗得岛州，2010年。[CSZ17a] Jacob S. Christiansen、Barry Simon 和 Maxim Zinchenko。切比雪夫多项式的渐近性质，I： ℝ的子集。 *Invent. Math.*，208(1):217–245，2017年。[CSZ17b] Jacob S. Christiansen、Barry Simon 和 Maxim Zinchenko。切比雪夫多项式的渐近性质，I： ℝ的子集。 *Invent. Math.*，208(1):217–245，2017年。[Fek23] M. Fekete。 ¨关于某些具有整数系数的代数方程的根的分布。 *Mathematische Zeitschrift*，17(1):228–249，1923年12月。[FS55] M. Fekete 和 G. Szeg¨o。关于根属于给定点集的整数系数代数方程。 *Math. Z.*，63:158–172，1955年。[Hil94] David Hilbert。关于勒让德多项式理论的一项贡献。 *Acta Math.*，18(1):155–159，1894年。[KS21] Alicia J. Koll
´ *Comm. Amer. Math. Soc.* 1 1 38, ar 和 Peter 2021 Sarnak。三次图谱的间隙集。，： –。[LLL82] A. K. Lenstra、H. W. Lenstra, Jr. 和 L. Lov
´ *Math.* asz。对有理 *Ann.* 261 4 515 534, 1982 数系数多项式进行因式分解。，( ): –。

[3] 作者谨向Serre教授致谢，感谢他进行了一次富有成果的讨论，使作者注意到了这一点，并帮助作者拟定了推论 5.2 和定理 5.3 的正确表述。

[Mic01] Daniele Micciancio。格中的最短向量难以在某个常数范围内近似。 *SIAM J. Comput.* 30 6 2008 2035, 2001 , ( ): – 。

[MS21] James McKee 和 Chris Smyth。 *Around the unit circle—Mahler measure, integer matrices and roots of unity*。Universitext。Springer，Cham， [2021] ©2021。[Rob64a] Raphael M. Robinson。实点集中的共轭代数整数。 *Math. Z.*，84:415–427，1964年。[Rob64b] Raphael M. Robinson。包含无穷多个共轭代数单位集的区间。 *Ann. of Math.* , ： –。[*(2)* 80 411 428, 1964

Rum13] Robert Rumely。 *Capacity theory with local rationality*，第193卷， *Mathematical Surveys and Monographs*。美国数学会，普罗维登斯，罗得岛州，2013年。曲线上的强 Fekete-Szeg¨o 定理。[Sch18] I. Schur。 ¨关于某些具有整数系数的代数方程的根的分布。 *Math. Z.*，1(4):377–402，1918年。[Sch87] C.-P. Schnorr。多项式时间格基约化算法的层级。 *Theoret. Comput. Sci.*，53 2 3 201(-): –224，1987年。[Ser19] Jean-Pierre Serre。弗罗贝尼乌斯自同态特征值的渐近分布——根据 [Abel、Chebyshev、Robinson、`。...], (414， *Astérisque*布尔巴基研讨会。2017/2018年卷。报告1136–1150：报告第1146号，379–426页，2019年。´Ser20] Jean-Pierre Serre。 *Rational points on curves over finite fields* 18 *Documents Mathématiques (Paris)* ，第 卷。*[Mathematical Documents (Paris)]* ´ ´ ´ [2020] 2020 法国数学会，巴黎，© 。由 Everett Howe、Joseph Oesterl´e 和 Christophe Ritzenthaler 撰写相关内容，Alp Bassa、Elisa Lorenzo Garc´ıa、Christophe Ritzenthaler 和 Ren´e Schoof 编。[Sie45] Carl Ludwig Siegel。全正实代数整数的迹。 *Ann. of Math. (2)*，46 312，1945 302: –。[Smi21] Alexander Smith。共轭元服从指定分布的代数整数。 *arXiv e-prints*，第 arXiv:2111.12660 页，2021年11月。[Smy84] C. J. Smyth。全实代数整数的平均值。 *Math. Comp.*，42(166):663–681，1984年。[ST97] Edward B. Saff 和 Vilmos Totik。 *Logarithmic potentials with external fields* 316 *Grundlehren der* ，第 卷。*mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]* Springer-Verlag，柏林，1997年。附录B由 Thomas Bloom 撰写。[ST18] ANANTH N. SHANKAR 和 JACOB TSIMERMAN。有限特征下的非典型交。 *Forum of Mathematics Sigma* 6 13, 2018 , , ： e 。[ST21] Ananth N. Shankar 和 Jacob Tsimerman。整体域上不同源于雅可比簇的阿贝尔簇。*arXiv e-prints*，第 arXiv:2105.02998 页，2021年5月。[Tal23] Naser Talebizadeh Sardari。共轭代数整数与二维库仑定律。 *arXiv e-prints*，第 arXiv:2304.10021 页，2023年4月。[TV97] M. A. Tsfasman 和 S. G. Vl˘adut。ζ 函数的渐近性质。第84卷，1445–1467页。1997年。代数几何，第7卷。

Penn State department of Mathematics, McAllister Building, Pollock Rd, State College, PA 16802 USA*Email address*: nzt5208@psu.edu,bjo5149@psu.edu