计算实代数曲线的连通分支

Elisabetta Rocchi Mohab SafeyEl
DinElisabetta.Rocchi@lip6.fr Mohab.Safey@lip6.fr 索邦大学,
LIP6，法国国家科学研究中心，UMR7606，巴黎，法国

arXiv:2603.16283v1 [cs.SC] 17 Mar 2026

摘要

实代数集的连通分支是半代数的，即它们可以由一个布尔公式描述，该公式的原子是具有实系数的多项式约束。计算这类描述在光学系统设计和机器人学中有着重要的应用。在本文中，我们设计了一种用于计算实代数曲线的此类半代数描述的新算法。值得注意的是，该算法的复杂度低于目前已知的、用于计算与所研究实空间曲线同痕的图的最佳算法。

1 引言

问题陈述。实代数集的连通分支是半代数集，因此可由一个关于具有实系数的多项式约束的布尔公式描述。“计算连通分支”意味着计算此类描述。

本文致力于计算由 $\mathbb{R}^n$ 给出的实代数曲线的连通分支。

先前工作与研究动机。这项研究的动机来自光学应用：其中，光学同轴设计分类问题 [34, 19] 可归结为计算空间曲线的连通分支。一种初步方法是结合柱面代数分解（CAD）算法 [15]，以及用于确定 CAD 所计算胞腔之间邻接关系的算法，例如 [36, 3, 4]，或 [44]。该方法的复杂度关于 n [8] 呈双指数级。

[6, 第 16] 章表明，对于由次数至多为 d 的 s 个多项式定义的半代数集，可以使用 $s^{n+1}d^{O}(n^4)$ 次算术运算来计算其连通分支（另见 [10, 29]）。

对于维数为一的集合，从实代数曲线出发，人们或许会期待更好的结果。许多研究致力于“计算拓扑”，涉及平面曲线（例如 [1, 5, 7, 9, 11, 14, 20, 21, 28,30, 33, 18, 43]）以及 $\mathbb{R}^3$ 中的空间曲线（例如 [2, 12, 17, 23, 26, 32]）。“计算拓扑”在这里指计算一个与所研究曲线同痕的嵌入图。对于 $f \in \mathbb{Z}[\boldsymbol{x}]$ （其中 $\boldsymbol{x} = x_1, \ldots\ldots, x_n$），设 (d, τ) 表示其大小，即 d 和 τ 分别是其次数及系数的最大比特大小。据我们所知，$\mathbb{R}^3$ 中空间曲线的最佳复杂度由 [13] 中的确定性算法实现，该算法使用 $O^{\sim}(d^{18} + d^{17}\tau)$ 次位运算，其中 (d, τ) 界定了输入多项式的大小（$O^{\sim}(.)$ 表示省略了多对数因子）。

计算给定曲线的连通分支数量，或回答连通性查询，可能成本更低。为进一步说明，我们现在回顾如何对这类查询点和曲线进行编码。
零维参数化 $\mathfrak{P}$ 是 $\lambda, (w, v_1, \ldots, v_n)$ 属于 $\mathbb{Q}[\boldsymbol{x}] \times \mathbb{Q}[t]^{n+1}$，其中 λ 是线性形式，w 是无平方因子且首一的。它定义集合 $\mathsf{Z}(\mathfrak{P}) = \left\{ \left(\frac{v_1}{\partial w/\partial t}, \ldots, \frac{v_n}{\partial w/\partial t} \right)(\theta) \mid w(\theta) = 0 \right\}$。所有由 $\mathbb{Q}$ 代数点构成的有限集都可以用零维参数化编码。这就是查询点的编码方式。

一维 维参数化 $\mathfrak{R} = (\lambda, \mu, (w, v_1, \ldots, v_n)) \in \mathbb{Q}[\boldsymbol{x}]^2 \times \mathbb{Q}[t, u]^{n+1}$ 其中 λ, μ

其中各项均为线性形式，且 w 在 t 和 u 中是无平方因子的首一多项式，它定义了曲线 $\mathsf{Z}(\mathfrak{R})$，该曲线是 $\left\{\left(\frac{v_1}{\partial w/\partial u},\ldots,\frac{v_n}{\partial w/\partial u}\right)(\theta,\eta) \mid w(\theta,\eta)=0, \frac{\partial w}{\partial t}(\theta,\eta)\neq 0\right\}$ 的扎里斯基闭包。所有 $\mathbb{Q}$-代数曲线都可以由这样的参数化定义。

[31] 表明，给定一个大小为（δ，τ）、编码了 $\mathbb{C}^n$ 中的一条$\mathcal{C}$ 的μ，以及一个大小为（μ，κ）、编码 $\mathcal{P}\subset\mathcal{C}$的 $\mathcal{C}\cap\mathbb{R}^n$，可以使用 $O^{\sim}(\delta^6+\mu^6+\delta^5\tau+\mu^5\kappa)$ 次位运算来计算 $\mathcal{C}\cap\mathbb{R}^n$的连通分支数量，并回答涉及 $\mathcal{P}\cap\mathbb{R}^n$的连通性查询。对于由两个最大大小为（$d$，$\tau$）的多项式的交集定义的 $\mathbb{R}^3$，这将得到 $O^{\sim}(d^{12}(1+\tau))$ 的位复杂度，因此低于 [13]所需的复杂度。

然而，对于计算实代数曲线的连通分支，仍然缺乏具有相当复杂度的算法。

主要贡献。我们设计了一种名为 CurveComponents的算法，用于计算 $\mathbb{R}^n$ 中一条实代数曲线的连通分支。该曲线给定为多项式方程组 $f_1=\cdots=f_{n-1}=0$ 的解集，其系数属于 $\mathbb{Q}$ 并生成一个根理想；与之对应的代数曲线记为 $\mathcal{C}$。

该算法基于 [31]，其展示了如何通过分析 $\mathcal{C}$ 在足够一般的位置平面上的投影的拓扑，来分析 $\mathcal{C}_{\mathbb{R}}=\mathcal{C}\cap\mathbb{R}^n$ 的连通性。因此，首先进行由 $\boldsymbol{A}_1\in \mathsf{GL}_n(\mathbb{Q})$ 诱导的坐标变换，以确保一般性性质（在 [31] 中称为 (H)），并获得 $\mathcal{C}^{\boldsymbol{A}_1}=\{\boldsymbol{A}_1^{-1}x \mid x\in\mathcal{C}\}$ 的一维参数化 $\mathfrak{R}_1$。在这种情况下，$\mathcal{C}^{\boldsymbol{A}_1}$ 在前两个坐标上的投影 $\mathcal{C}_{2,\,\boldsymbol{A}_1}$ 是一条代数曲线。如 [31], 所示，$\mathcal{C}_{2,\,\boldsymbol{A}_1}\cap\mathbb{R}^2$ 的连通性可以轻易地提升至 $\mathbb{R}^n$，但表观奇点集 $\mathsf{app}(\mathcal{C}_{2,\,\boldsymbol{A}_1})$ 除外；该集合是 $\mathcal{C}_{2,\,\boldsymbol{A}_1}$ 的奇点中位于 $\mathcal{C}^{\boldsymbol{A}_1}$ 的奇点投影之外的部分。[31] 中的一项重要成果，是展示了在经过 $\mathsf{app}(\mathcal{C}_{2,\,\boldsymbol{A}_1})\cap\mathbb{R}^2$ 时，如何将连通性提升至 $\mathbb{R}^n$。

我们的第一个辅助性贡献是一个名为 GenPlanarComponents的算法，它使用 $O^{\sim}(\delta^6(\tau+\delta))$ 次位运算，计算 $\mathcal{C}_{2,\boldsymbol{A}_1}\cap\mathbb{R}^2\setminus\mathsf{app}(\mathcal{C}_{2,\boldsymbol{A}_1})$（或 $\mathcal{C}_{2,\boldsymbol{A}_1}\cap\mathbb{R}^2$）的所有连通半代数分支曲线的半代数描述，其中（$\delta,\tau$）是 $\mathfrak{R}_1$ 的大小（因此 δ 是 $\mathcal{C}$的次数）；参见定理 2.2。注意，这一复杂度是 δ 中用于计算 $\mathcal{C}_{\mathbb{R}}$的连通分支的算法复杂度的 δ 倍。

这些半代数描述可以在 $\mathbb{R}^n$中提升。借助 [31], ，可以汇集位于 $\mathcal{C}_{\mathbb{R}}$同一连通分支中的那些半代数曲线。不过，我们仍缺少 $F_1=\mathcal{C}^{\boldsymbol{A}_1}\setminus\pi_2^{-1}(\mathsf{app}(\mathcal{C}_{2,\boldsymbol{A}_1}))$中的“失败”点（其中 π_2 表示到前两个坐标的投影）。为弥补这一点，可以尝试计算 F_1。然而，次数估计表明，$\mathsf{app}(\mathcal{C}_{2,\boldsymbol{A}_1})$的次数属于 $O(\delta^2)$，于是 F_1 的次数属于 $O(\delta^3)$。若不超过先前的计算代价，似乎很难计算 F_1。

我们所依赖的基本思路如下。若偶然使用第二个不同的矩阵 $\boldsymbol{A}_2$ 进行相同的计算，得到的失败点 F_2 满足 $F_1^{\boldsymbol{A}_1^{-1}}\cap F_2^{\boldsymbol{A}_2^{-1}}=\emptyset$，那么我们可以尝试重新组合这些半代数描述，而不增加此前的计算成本。我们正是这样做的，并证明只要对$\boldsymbol{A}_1$ 和 $\boldsymbol{A}_2$的选取作出一般性假设，这一方法就能奏效。

现在我们可以陈述主要结果，该结果用外在量（输入多项式的大小）来表述。

定理 1.1. 设 $\boldsymbol{f}=(f_1,\ldots,f_{n-1})\subset\mathbb{Q}[x_1,\ldots,x_n]$ 生成一个维数为 1 的根理想，$\mathcal{C}\subset\mathbb{C}^n$ 为其定义的代数曲线，且 (d,h) 为这些 f_i的最大大小。设 $0<\epsilon<1$ 为一个概率参数。

存在一个扎里斯基闭子集 $\mathscr{Z}\subsetneq\mathsf{GL}_n(\mathbb{C})$，使得对于任意 $\boldsymbol{A}_1\in GL_n(\mathbb{Q})\setminus\mathscr{Z}$，都存在一个扎里斯基闭子集 $\mathscr{Z}_{\boldsymbol{A}_1}$，使得对于任意 $\boldsymbol{A}_2\in\mathscr{Z}_{\boldsymbol{A}_1}$，令 $\overline{\tau}$ 为 $\boldsymbol{A}_1$ 和 $\boldsymbol{A}_2$ 的元素的最大比特大小，则 CurveComponents$(\boldsymbol{f},\varepsilon,\boldsymbol{A}_1,\boldsymbol{A}_2)$ 使用以下方法计算 $\mathcal{C}_{\mathbb{R}}=\mathcal{C}\cap\mathbb{R}^n$ 的每个连通分支的半代数描述：

使用 $\widetilde{O}(n^{12}d^{7n-7}(h+\overline{\tau}+1)+(h+\log\frac{1}{\varepsilon})(n^{14}d^{6n-5}+\binom{n+d}{n}n^{16}d^{3n}))$ 次位运算，成功概率至少为 $1-\varepsilon$。

这里有几点值得说明。首先请注意，当 $n=3$ 时，我们得到的复杂度为 $O^{\sim}(d^{14}(h+\overline{\tau}+1)+\log(\frac{1}{\epsilon})d^{13})$。这表明，目前在 $\mathbb{R}^3$ （在我们的假设及 $\overline{\tau}\in\log\left(d^{O(1)}\right)$ 下）计算曲线的连通分支，比计算与所研究曲线同位的图更快。

此外，该算法归结为计算曲线的一维参数化 $\mathcal{C}$（应用 $\boldsymbol{A}_1$ 和 $\boldsymbol{A}_2$ 之后），再加上 $\mathcal{C}$ 中的一些额外点（见第3节），然后执行两次 GenPlanarComponents；其复杂度实际上取决于曲线的实际次数（我们将其上界估计为 d^{n-1}）。因此，可以给出更精确的复杂度表述。特别是，假设这些参数化已给定（如 [31] 中所述），我们得到的复杂度“仅”为 [31] 的 δ 倍。

最后请注意，如果 $\mathfrak{D}$ 界定了 $\mathscr{Z}$ 和 $\mathscr{Z}_{\boldsymbol{A}_1}$ 的次数之和，那么只需选取 $\boldsymbol{A}_1$ 和 $\boldsymbol{A}_2$，使其元素的比特大小为 $O^{\sim}(\log(\frac{1}{\epsilon})+\log(\mathfrak{D}))$，即可确保成功概率为$>1-\epsilon$。如果 $\mathfrak{D}\in d^{n^{O(1)}}$，那么在我们的复杂度结论中，只有 n 的幂会受到影响。第 4 节的证明表明， $\mathscr{Z}_{\boldsymbol{A}_1}$ 的次数为 $d^{O(n)}$。集合 $\mathscr{Z}$ 与 [31]中考虑的集合相同。我们猜想它也属于 $d^{O(n)}$ 。

论文结构。第2节致力于设计 GenPlanarComponents。第3节介绍我们的主要算法 CurveComponents。第 4 节证明我们的一般性结论。

2 平面曲线

令 $f\in\mathbb{Q}[x_1,x_2]$ 为定义曲线 $\mathcal{C}\subset\mathbb{C}^2$ 的无平方因子多项式，并令 $\mathcal{C}_{\mathbb{R}}=\mathcal{C}\cap\mathbb{R}^2$。我们的方法对算法 TopoNT [37, Sec. 3.1], 稍作修改；该算法本身建立在 [7],之上，并在 $\mathbb{R}^2$中生成一个与 $\mathcal{C}_{\mathbb{R}}$同痕的平面直线图。

设 $\mathcal{G}$ 是嵌入在 $\mathbb{R}^2$ 中的图，其顶点集为 $\mathcal{V}(\mathcal{G})\subset\mathbb{R}^2$，边集为 $\mathcal{E}(\mathcal{G})$。我们将 $\mathcal{C}_{\mathcal{G}}$ 记为这样得到的平面曲线：取 $\mathcal{V}(\mathcal{G})$ 中所有顶点的并集，再加上连接 $\mathcal{G}$ 中各边端点的线段。

$\mathbb{R}^n$ 的同痕是一个连续映射 $\mathcal{I}$，它从 $\mathbb{R}^n\times[0,1]$ 映到 $\mathbb{R}^n$，其中 $p\mapsto\mathcal{I}(p,0)$ 是恒等映射，且 $p\mapsto\mathcal{I}(p,t)$ 是同胚（$t\in[0,1]$）。如果存在 $\mathbb{R}^n$ 的同痕 $\mathcal{I}$，使得 $\mathcal{I}(Y,1)=Z$，则称 $\mathbb{R}^n$ 的两个子集 Y 和 Z 同位等价。

现在我们引入一种更精细的图结构，它与 $\mathcal{C}_{\mathbb{R}}$ 仍然同痕，但满足额外的性质，可作为辅助结构，用于获得 $\mathcal{C}_{\mathbb{R}}$ 的连通分支的半代数描述。设 $\mathcal{P}\subset\mathrm{reg}(\mathcal{C})$ 是 $\mathcal{C}$ 上的一个有限点集。我们将 $\mathscr{K}(\pi_1,\mathcal{C})\subset\mathbb{C}^2$ 记为 $f=\frac{\partial f}{\partial x_2}=0$ 的解集。

定义 2.1. 设 $\mathcal{H}=(\mathcal{V},\mathcal{E})$ 是一个图，且具有 $\mathcal{V}\subset\mathbb{R}^2$。若满足以下条件，我们称 $\mathcal{H}$ 是 $(\mathcal{C},\mathcal{P})$ 的半代数实同痕图：

- $\mathcal{C}_{\mathbb{R}}$ 与 $\mathcal{C}_{\mathcal{H}}$同位等价；
- $\mathscr{K}(\pi_1,\mathcal{C}_{\mathbb{R}})$ 的点 $\cup\,\mathcal{P}$ 嵌入在 $\mathcal{V}$ 中；
- $\mathscr{K}(\pi_1,\mathcal{C}_{\mathbb{R}})$ 中任意两个点在 $\mathcal{H}$ 中都没有相邻顶点；
- 对于每个对应于点 $\xi\in\mathcal{C}_{\mathbb{R}}$ 的顶点 $v\in\mathcal{V}$；我们给出了 ξ的半代数描述σ_v ；
- 每条边 $e\in\mathcal{E}$ 都带有一个半代数描述 σ_e，用于描述与 e同痕的 $\mathcal{C}_{\mathbb{R}}$ 实分支。

我们假设 f 处于 *[7]*所指的一般位置坐标中。我们设计了一种算法 GEN-PLANARCOMPONENTS，其输入为：

- $f \in \mathbb{Z}[x_1, x_2]$ 大小为 (δ, τ) 的无平方因子多项式，使得 $V(f) = \mathcal{C}$；
- 一个零维参数化 $\mathfrak{P}$，使得 $\mathcal{P} = \mathsf{Z}(\mathfrak{P}) \subset \mathcal{C}$；

关于 x_2，整除 f 与 $\frac{\partial f}{\partial x_2}$ 的结式。

令 $\mathcal{V}_{\mathscr{K}}, \mathcal{V}_{\mathcal{P}} \subset \mathcal{V}$ 为对应于 $\mathscr{K}(\pi_1, \mathcal{C}_{\mathbb{R}})$ 和 $\mathcal{P}$ 的顶点。它输出 $(\mathcal{C}, \mathcal{P})$ 的半代数实同痕图 $\mathcal{H} = (\mathcal{V}, \mathcal{E})$，以及分别对应于 x_1 坐标为 q 的根的顶点子集 $\mathcal{V}_{\mathcal{P}}$ 和 $\mathcal{V}_q \subset \mathcal{V}_{\mathscr{K}}$。令 (δ, τ)、$(\delta_{\mathcal{P}}, \tau_{\mathcal{P}})$、$(\delta_q, \tau_q)$ 分别为 f、$\mathfrak{P}$ 和 q 的大小。

定理 2.2. GENPLANARCOMPONENTS$(f, \mathfrak{P}, q)$ 使用以下方法计算 $(\mathcal{C}, \mathcal{P})$ 的半代数实同痕图 $\mathcal{H}$

$$\widetilde{O}((\delta^6 + \delta^4\delta_{\mathcal{P}} + \delta\delta_{\mathcal{P}}^2)(\tau + \delta) + (\delta^5 + \delta^3\delta_{\mathcal{P}} + \delta_{\mathcal{P}}^2)\tau_{\mathcal{P}} + \delta_{\mathcal{P}}^3 + \delta_q^2\tau_q)$$

位运算。此外，$|\mathcal{V}(\mathcal{H})| \in O(\delta^4 + \delta\delta_{\mathcal{P}})$ 和 $|\mathcal{E}(\mathcal{H})| \in O(\delta(\delta^3 + \delta_{\mathcal{P}} + 1))$。

2.1 构造概述

$\mathcal{C}$ 的正则（分别地，奇异）轨迹记为 $\mathsf{reg}(\mathcal{C})$（分别地，$\mathsf{sing}(\mathcal{C})$）。由于 f 无平方因子，$\mathsf{sing}(\mathcal{C}) = V(f, \partial f/\partial x_1, \partial f/\partial x_2)$。

设 $\mathcal{S}_k = V\left(f, \partial^k f/\partial x_2^k\right)$。我们假设 f 满足假设 (S)：对于所有$1 \le k \le d_2 = \mathsf{deg}(f, x_2)$，$\mathcal{S}_k$ 均为有限集。令 $\mathcal{S}(f) = \cup_{k=1}^{d_2} \mathcal{S}_k$。

我们将投影 $(\xi_1, \xi_2) \to \xi_1$记为 π_1。

在 [37, 第 3] 节算法的投影阶段，将 $\mathscr{K}(\pi_1, \mathcal{C})$ 投影到 x_1-轴上。如 [37], 中所述，我们将这些值记为 $\alpha_1, \ldots, \alpha_m$，并将其隔离区间记为 $I_1, \ldots, I_m$。在同一阶段，还会计算任意值 $\beta_0, \ldots, \beta_{m+1} \in \mathbb{Q}$，其中对于所有 $i = 0, \ldots, m$，$\alpha_m < \beta_{m+1}$和$\beta_{i-1} < \alpha_i < \beta_i$。

用 $\gamma_1, \ldots, \gamma_t$表示 $\pi_1(\mathcal{S}(f))$ 中的点，用 $J_1, \ldots, J_t$表示它们的隔离区间。计算这些区间的过程与在 [37] 中求得 α_i 所用的方法类似。在提升阶段，计算 $f(\alpha_i, x_2)$ 和 $f(\beta_i, x_2)$ 的实根的隔离区间，以及对应的重数。由于 f 处于一般位置坐标，这些多项式至多有一个重根（见 [7, 定理 5] 的证明）。在我们的设定中，还会计算 $1 \le i \le t$ 对应的 $f(\gamma_i, x_2)$ 的实根。

获得与曲线同位的图的最后一个阶段是连接步骤。图的顶点 $\mathcal{G}$ 定义如下

$$V(\mathcal{G}) = \{(x, y) \in \mathbb{R}^2 \mid \exists i \text{ with } x = \alpha_i \text{ or } x = \beta_i \text{ and } f(x, y) = 0\}.$$

此时，连接这些顶点很直接；详情见 [7, 第 3.2 节。3] 从该图出发，我们构造图 $\mathcal{H}$。这个新图的顶点定义如下

$$V(\mathcal{H}) = V(\mathcal{G}) \cup \{(x, y) \in \mathbb{R}^2 \mid \exists i \text{ with } x = \gamma_i \text{ and } f(x, y) = 0\},$$

而新图的边则按如下方式获得：从 $V(\mathcal{G})$ 中的每个顶点发出的边数，与 $\mathcal{G}$ 中相同。设该集合中的 r 点 (γ_{i_j}, y_j)（$j = 1, \ldots, r$），

$$\{(x, y) \in \mathbb{R}^2 \mid \exists\, i \text{ such that } x = \gamma_i \text{ and } f(x, y) = 0\} \setminus V(\mathcal{G})$$

位于 $\mathcal{G}$ 的同一条边 (v, w) 上（在同痕意义下），并假设相应的 γ_{i_j} 按递增顺序排列。于是，这条边被细分为 $r+1$ 条边，其端点按顺序为 $v, (\gamma_{i_1}, y_1) \ldots, (\gamma_{i_r}, y_r)$ w。我们将这一构造称为过程 UPDATEEDGES,

该过程将在算法1中用于构造 $\mathcal{H}$ 的边集。现在，我们说明如何确定新顶点属于 $\mathcal{G}$ 的哪条边。设 α_k 和 α_{k+1} 是按上述方法得到的两个相邻的 x_1 坐标。对于任意选取的 $\overline{x} \in (\alpha_k, \alpha_{k+1})$，$f(\overline{x}, y)$ 的实根数保持不变，且等于图 $\mathcal{G}$ 中位于以下任一区间上方的边数：该区间包含于 (α_k, α_{k+1})，且其端点是 $\mathcal{G}$ 中顶点的相邻 x_1 坐标。因此，如果 $\gamma_i \in (\alpha_k, \alpha_{k+1})$，那么 $f(\gamma_i, x_2)$ 的实根数等于 $\mathcal{G}$ 与竖直线 $\{x_1 = \gamma_i\}$ 的交点数。接着，通过对 $f(\gamma_i, x_2)$ 的实根排序，我们便可确定这些点分别属于 $\mathcal{G}$ 的哪条边。

对于 $(x, y) \in \mathbb{R}^2$，定义 $\sigma(x, y)$ 为 $\partial^k f/\partial x_2^k(x, y)$ 对于 $k \in \{1, \ldots, d_2\}$ 的符号序列。

定理 2.3. 设 $f \in \mathbb{R}[x_1, x_2]$ 满足 (S)。设 $\pi_1(\mathcal{S}(f)) = \{\xi_1, \ldots, \xi_\ell\}$, $K_i := (\xi_i, \xi_{i+1}) \subset \mathbb{R}$对于 $i = 1, \ldots, \ell - 1$，并将 $C_{i,1}, \ldots, C_{i,m_i}$ 记为 $\pi_1^{-1}(K_i)$ 的连通分支。于是，对于所有 $i = 1, \ldots, \ell - 1$ 和 $j = 1, \ldots, m_i$，序列 $\sigma(x, y)$ 沿着 $C_{i,j}$ 保持不变。此外，$\pi_1^{-1}(K_i)$ 的每个连通分支 $C_{i,j}$ 都由其符号序列唯一确定。

证明。固定 $i \in \{1, \ldots, \ell - 1\}$ 和 $j \in \{1, \ldots, m_i\}$ 以及 $\pi_1^{-1}(K_i)$ 的一个分支 $C_{i,j}$。根据 $\mathcal{S}(f)$ 的定义及其有限性，对于每个 $(x, y) \in C_{i,j}$，以及所有满足 $0 < k < d_2$ 的 k，导数 $\partial^k f/\partial x_2^k(x, y)$ 在该半代数子集上处处不为零。

由于 f 及其所有偏导数都是多项式，因此它们在 $\mathbb{R}^2$ 上连续。因此，在不为零的连通子集上，它们的符号不会改变。因此，对于所有 $(x, y) \in C_{i,j}$，符号序列 $\sigma(x, y)$ 保持不变。

对于第二个结论，我们借助 Thom编码的概念（见 [6, 命题 2.28]）。设 $\alpha \in K_i$，并考虑 $f(\alpha, x_2) \in \mathbb{R}[x_2]$。它的实根与 $\pi_1^{-1}(K_i)$ 的连通分支一一对应。事实上，对于 $f(\alpha, y)$ 的每个实根 β，点 (α, β) 恰好位于一条分支 $C_{i,j}$ 上；而每条分支 $C_{i,j}$ 对于所选的 α 恰好包含这样一个点。$f(\alpha, x_2)$ 的每个根都有唯一的 Thom编码，即导数 $\frac{\partial^k f}{\partial x_2^k}$ 在 $1 \le k \le d_2$ 时的唯一符号序列。该序列唯一确定包含该根的相应分支$C_{i,j}$。

□

我们用 $\sigma_{i,\ j}$ 表示与多项式序列$\big(\partial^k f/\partial x_2^k(x, y)\ 1 \le k \le \deg_y(f)\big)$ 沿着 $C_{i,\ j}$相关联的符号条件。

推论 2.4. 使用上述记号，沿着曲线 $\mathcal{C}$ 上对应于图 $\mathcal{H}$的一条边的每条弧，多项式 $\partial^k f/\partial x_2^k$ 关于 $1 \le k \le d_2$ 的偏导数序列的符号保持不变。此外，$\mathcal{H}$ 中端点具有相同 x_1 坐标的每条边都对应一个不同的符号模式。

证明. 注意，$\pi_1(\mathcal{S}(f))$是由上述定义的点 α_i 和 γ_i 构成的并集。对于图 $\mathcal{H}$ 的顶点，我们只需添加与那些 x_1坐标为β_i的顶点对应的点。于是，每条与 $\mathcal{H}$ 的一条边同痕的曲线弧都包含在某个连通分支$C_{i,\ j}$中。这就证明了第一部分。对于第二部分，我们像前一个证明中那样使用 Thom 编码。

□

回顾一下，对于每个 $i \in \{1, \ldots, \ell - 1\}$ 和 $j \in \{1, \ldots, m_i\}$，符号模式 $\sigma_{i,\ j}$ 是 $\{-1, 1\}^{d_2}$中的一个元素，其中 $d_2 = \deg_{x_2}(f)$。

我们定义半代数集 Reali($\sigma_{i,\ j}$) $\subset \mathbb{R}^2$

$$\mathrm{Reali}(\sigma_{i,j}) := \left\{ (x, y) \in \mathbb{R}^2 \;\middle|\; \Big(\mathrm{sign}\Big(\partial^k f/\partial x_2^k(x, y)\Big)\Big)_{1 \le k \le \delta} = \sigma_{i,j} \right\}.$$

集合 Reali($\sigma_{i,\ j}$) 由一个半代数描述给出，该描述固定了 $\partial^k f/\partial x_2^kfor1 \le k \le d_2$的符号。我们将其记为 $\Sigma_{i,\ j}$。

现在让我们 考虑图 $\mathcal{H}$ 的一条边，并将其端点记为 v_1 和 v_2。如果两个 h

顶点属于 $\mathcal{S}(f)$，则该边与定理 2.3 中描述的分支 $C_{i,\ j}$ 之一同痕，其半代数描述为

$$\{\pi_1(v_1) < x_1 < \pi_1(v_2)\} \wedge \Sigma_{i,j} \wedge \{f = 0\}. \tag{2.1}$$

若一个端点反而位于 $\{(x,y) \in \mathbb{R}^2 \mid \exists i$，使得 $x = \beta_i$ 且 $f(x,y) = 0\}$，那么我们必须先确定边所属的连通分支 $C_{i,\ j}$，相应的半代数描述随后由 (2.1) 给出。为确定这个连通分支 $C_{i,\ j}$，注意到从 $\{(x,y) \in \mathbb{R}^2 \mid \exists i$ 中满足 $x = \beta_i$ 且 $f(x,y) = 0\}$ 的每个顶点恰好有两条边发出，并且该集合中的两个顶点永不相邻（即它们永远不会是同一条边的端点）。因此，举例来说，如果 v_1 属于这个集合，只需查看与它相连的另一个顶点（不同于 v_2），即可确定相应的连通分支 $C_{i,\ j}$。

因此，图 $\mathcal{H}$ 是定义 2.1 意义下的半代数同位图，其中与每条边 e 相关联的信息 σ_e 对应于某个 $\sigma_{i,\ j}$，并且边e 要么与连通分支 $C_{i,\ j}$重合，要么包含于其中。每个连通分支 C_i of$\mathcal{C}_{\mathbb{R}}$ 均可通过取属于 C_i的所有边的半代数描述的并集，以及位于其上的顶点，来进行半代数描述。

$\mathcal{H}$ 的顶点通过隔离区间以及多项式方程进行描述。令w_k为 $\mathrm{Res}_{x_2}(f, \partial^k f/\partial x_2^k)$，其中 Res_{x_2} 表示关于变量 x_2的结式。对于 $k \geq 2$，设 $g_k :=$ 为 $\gcd(w_1, \ldots, w_{k-1}, w_k)$，并设 $\overline{w}_k := \frac{w_k}{g_k}$。位于 $\pi(\mathcal{K}(\pi_1, \mathcal{C}))$上方的顶点由 $w_1(x_1) = 0$ 和 $f(x_1, x_2) = 0$描述，而其余所有顶点则对应于方程 $\overline{w}_k(x_1) = 0$ 和 $f(x_1, x_2) = 0$，其中 k取适当的值。

为了将 $\mathcal{P}$ 纳入 $\mathcal{H}$，令 (λ, θ_2) 为 $\mathcal{P}$ 的零维参数化，并设$\overline{\lambda} :=$ λ/为 $\gcd(w_1 \cdots w_\delta, \lambda)$。$\overline{\lambda} = f = 0$的解定义了新的正则顶点，将其添加到 $\mathcal{H}$ 中并使用 UpdateEdges连接；随后利用 $\mathcal{P}$的参数化确定子集 $\mathcal{V}_{\mathcal{P}}$。

最后，通过识别 $\mathcal{V}_{\mathscr{K}}$ 中那些 x_1 坐标为 q 的根的顶点，即可得到子集 $\mathcal{V}_q$。

2.2 指定符号模式的策略

在 $\mathcal{C}_{\mathbb{R}} \setminus \big(\mathscr{K}(\pi_1, \mathcal{C}) \cup \mathcal{S}_k\big)$的每个这样的光滑连通分支上，$\partial^k f/\partial x_2^k$ 的符号保持不变。因此，只需在每个这样的分支上选取一个点计算 $\partial^k f/\partial x_2^k$，即可确定整个分支上的符号模式。

我们用 $\mathcal{Q}_k$ 表示一个与 $\mathcal{C}_{\mathbb{R}} \setminus \big(\mathscr{K}(\pi_1, \mathcal{C}) \cup \mathcal{S}_k\big)$的所有连通分支都相交的有限子集。过程 PropagateSigns 的输入为满足 $\mathcal{K}(\pi_1, \mathcal{C}_{\mathbb{R}}) \cup \mathcal{S}(f) \subset V(\mathcal{H})$ 的图 $\mathcal{H}$，以及一族符号映射 $\{s_k : \mathcal{Q}_k \to \{-1, 0, +1\}\}_{k=1}^{d_2}$，其中 $s_k(q) =$ $\mathrm{sign}(\partial^k f/\partial x_2^k(q))$。对于每条边 $e \in \mathcal{E}(\mathcal{H})$，该过程返回一个符号向量$\sigma_e = \big(\sigma_{e,1}, \ldots, \sigma_{e,d_2}\big) \in \{-1, 0, +1\}^{d_2}$，使得 $\sigma_{e,k}$与由 e 编码的光滑连通分支上任意一点处 $\partial^k f/\partial x_2^k$ 的符号一致。

引理 2.5。设 $f \in \mathbb{Q}[x_1, x_2]$ 的大小为（δ，τ），处于一般位置坐标下并满足（S）。令 w_1、...、$w_\delta \in \mathbb{Q}[x_1]$ 由 w_k 定义：对于 $k = 1$、...、δ，$=\mathrm{Res}_{x_2}(f$、$\partial_{x_2}^k f)$。算法 SignSam-ples 以（f，w_1，...、w_δ）为输入，为每个 $k \in \{1, \ldots, \delta\}$ 计算如上的一个有限集 $\mathcal{Q}_k$，以及相应的符号映射 s_k，使用 $\widetilde{O}$（$\delta^7 + \delta^6\tau$）次位运算。

正确性证明。对于每个 $k \in \{1, \ldots, d_2\}$，算法按如下方式构造集合 $\mathcal{Q}_k$。我们定义 $P_k :$ $= w_1 w_k$，并约定 $P_1 := w_1$，将 $\zeta_{k,\ 1} < \cdots < \zeta_{k,\ \ell_k}$ 记为 P_k的实根。我们需要构造有理数 $\theta_0^{(k)} < \zeta_{k,\ 1} < \theta_1^{(k)} < \cdots < \zeta_{k,\ \ell_k} < \theta_{\ell_k}^{(k)}$，并将 $\pi_1|_{\mathcal{C}_{\mathbb{R}}}$ 在这些值上方的实纤维纳入 $\mathcal{Q}_k$。根据构造，每个开区间（$\zeta_{k,\ i}$、$\zeta_{k,\ i+1}$）都不包含 P_k的实根。由于导数 P_k'在每个这样的区间内至少有一个实根，因此，对 P_k' 的实根进行足够精确的近似，就能得到区间（$\zeta_{k,\ i}$、$\zeta_{k,\ i+1}$）内的值$\theta_i^{(k)}$。由于 w_k（x_1）$= Res_{x_2}$（f、$\partial_{x_2}^k f$），这意味着 $\partial^k f/\partial x_2^k$不会

在纤维 $\pi_1^{-1}(\theta_i^{(k)}) \cap \mathcal{C}_{\mathbb{R}}$ 的任何实点处为零，并且 $\partial^k f/\partial x_2^k$ 的符号在 $\mathcal{Q}_k$的每一点上都有定义。对于 $\theta_0^{(k)}$ 和 $\theta_m^{(k)}$，我们利用 $k = 1$、.....、d_2 时 w_k 的根的绝对值上界（见 [6, 引理 10.2]），并据此选取两个超出该界的有理数。

□

复杂度证明推迟到第 2.3 节，算法的明确描述则见附录。我们定义算法 AssignSigns，它以整数$k \geq 1$ 和多项式 $g \in \mathbb{Q}[x_1]$为输入。它输出一个有限集 $\mathcal{Q}_k \subset \mathcal{C}_{\mathbb{R}}$ 以及一个符号映射 $s_k : \mathcal{Q}_k \to \{-1, 0, 1\}$。集合 $\mathcal{Q}_k$ 通过计算方程组 $g(x_1) = f(x_1, x_2) = 0$的实解的隔离区间得到；对于每个 $q \in \mathcal{Q}_k$，值 $s_k(q)$ 定义为$s_k(q) :=$ 符号$\left(\partial_{x_2}^k f(q)\right)$。

2.3 算法与复杂度分析

IsolatingRealSol以单变量多项式 $R(x_1) \in \mathbb{Q}[x_1]$ 和定义零维方程组的二元多项式 $F(x_1, x_2) \in \mathbb{Q}[x_1, x_2]$ 为输入，并返回 $R(x_1) = F(x_1, x_2) = 0$的实解的隔离盒。

算法 1 PlanarComponents

要求： f属于 $\mathbb{Q}[x_1, x_2]$，满足 $\mathcal{S}$，并且给定一个零维参数化（$\lambda(x_1)$ θ_2）
定义 $\mathcal{P} \subset \mathsf{reg}(\mathcal{C})$，二者均采用一般位置坐标，并且 $q \in \mathbb{Z}[x_1]$ 使得 q 整除 w_1。
确保： 得到一个关于（$\mathcal{C}_{\mathbb{R}}$， $\mathcal{P}$）的半代数同位图 $\mathcal{H}$，以及为每条边指定的符号向量 σ_e
边 $e \in \mathcal{E}(\mathcal{H})$。

1: $\mathcal{G} \leftarrow$ TopoNT(f) ▷ $\mathcal{G}$ 与 $\mathcal{C}_{\mathbb{R}}$是同痕的，见 [37]
2: $V(\mathcal{H}) \leftarrow V(\mathcal{G})$
3: $V_q \leftarrow$ IsolatingRealSol($q(x_1)$, 0)
4: $w_1 \leftarrow$ 结式$_{x_2}(f, \partial_{x_2} f)$
5: </style}对于 $k = 2$, . . . , δ **do**
6: $w_k \leftarrow$ 结式$_{x_2}(f, \partial_{x_2}^k f)$
7: $g_k \leftarrow$ 最大公因式$(w_1 \cdots w_{k-1}, w_k)$
8: $\overline{w}_k \leftarrow w_k/g_k$
9: $V(\mathcal{H}) \leftarrow V(\mathcal{H}) \cup$ IsolatingRealSol($\overline{w}_k(x_1)$ $f(x_1, x_2)$)
10: 结束循环
11: $\overline{\lambda} \leftarrow \lambda/gcd(w_1 \cdots w_\delta, \lambda)$
12: $\mathcal{V}(\mathcal{H}) \leftarrow \mathcal{V}(\mathcal{H}) \cup$ IsolatingRealSol($\overline{\lambda}(x_1)$ $f(x_1, x_2)$)
13: $V_{\mathcal{P}} \leftarrow$ IsolatingRealSol($\lambda(x_1)$, $(\lambda' x_2 - \theta_2)(x_1, x_2)$)
14: $\mathcal{H} \leftarrow$ UpdateEdges($\mathcal{V}(\mathcal{H})$ $\mathcal{G}$)
15: $\{(\mathcal{Q}_k, s_k)\}_{k=1}^d \leftarrow$ SignSamples $(f, w_1, \ldots, w_d)$
16: $\{\sigma_e\}_{e \in \mathcal{E}(\mathcal{H})} \leftarrow$ PropagateSigns $\left(\mathcal{H}, \{s_k\}_{k=1}^d\right)$
17: 返回 $\left(\mathcal{H}, \{\sigma_e\}_{e \in \mathcal{E}(\mathcal{H})}\right)$
18: 返回 $\mathcal{H}$

命题 2.6. 算法 PlanarComponents是正确的。

证明。算法 TopoNT(f) 返回一个与 $\mathcal{C}_{\mathbb{R}}$ [37, （定理 6]）同痕的图。步骤 3 标识与 q对应的顶点，而对 k 的循环则计算与 $\mathcal{S}(f)$ 相关的附加顶点。步骤 11–13 引入与 $\mathcal{P}$对应的顶点。过程 Upda-teEdges 在不改变图的同痕类的前提下对图进行细化。最后，由引理 2.5 可知，SignSamples 计算并由 PropagateSigns传播的符号信息是正确的（因为 f 处于一般位置坐标中，该引理适用）。

□

令 (δ, τ) 表示 f 的大小，$(\delta_{\mathcal{P}}, \tau_{\mathcal{P}})$ 表示 $\mathcal{P}$ 的大小。我们可以假设多项式 $w_1, \ldots, w_\delta$ 两两互素。对于大小为 (p, η) 的 $P \in \mathbb{Z}[X]$，其对数

P 的根的分离距离的对数介于 $\log_2(1/\operatorname{sep}(P)) = O(p\eta + p\log\ p)$ 之间（见 [6,Cor. 10.22]）。此外，根据 [38, Lem. 66], ，隔离此类多项式 P 的实根所需的位精度为 $\overline{k}$ ，可以在 $\tilde{O}\left(p^3 + p^2\eta + p\overline{k}\right)$ 次位运算内完成。

引理 2.7. 分离 ω_i 和 ω_j 的实根所需的位精度为$\widetilde{O}(\delta^3(\tau + \delta\log\delta))$。

证明. $\partial^k f/\partial y^k$ 的系数比特大小上界为 $\tau_k := \tau + O(k\log\ \delta)$。应用 [38,引理 65] ，其次数上界为 δ ，系数位大小上界为 $\max\{\tau, \tau_k\} = \tau_k$，可得$w_k$的大小为 (D, η_k)，其中 $D = O(\delta(\delta - k))$，且 $\eta_k = O\big(\delta(\log\ \delta + \tau_k)\big) = O\big(\delta(k\log\ \delta + \tau)\big)$。多项式 $w_i w_j$ 的大小为 $(O(\delta(2\delta - i - j))\ O(\delta(2\tau + (i + j)\log\ \delta)))$；应用分离界可得，所需精度为 $\widetilde{O}(\delta^3(\tau + \delta\log\delta))$ 位。 □

引理 2.8。分离 ω_i 和 λ 的根所需的位精度为 $\widetilde{O}((\delta^2 + \delta_{\mathcal{P}})(\delta\log\ \delta + \tau + \tau_{\mathcal{P}}))$。

证明。我们按上述方法进行。乘积 $w_i\lambda$的大小为 $(O(\delta(\delta - i) + \delta_{\mathcal{P}})\ O(\tau + i\log\ \delta + \tau_{\mathcal{P}}))$。隔离其所有根所需的位精度为 $\widetilde{O}((\delta^2 + \delta_{\mathcal{P}})(\delta\log\ \delta + \tau + \tau_{\mathcal{P}}))$。 □

复杂度引理 2.5 的证明。设 $P_i := w_1 w_i$，其大小以及 P_i'的大小均不超过 $(2\delta^2, \delta(\tau + \delta\log\ \delta))$。以足够的精度隔离 P_i'的根，使其与 w_k的根分离（其中 $2 \le k \le \delta$），需要 $\widetilde{O}(\delta^6 + \delta^5\tau)$ 次位运算。

根据 [18, 命题 20], ，可以计算方程组 $P_1'(x_1) = f(x_1, x_2) = 0$ 的所有解的隔离区间，以及这些点处 $\partial^k f/\partial x_2^k$的符号，所需位运算次数为 $\widetilde{O}(\delta^6 + \delta^5\tau)$。由于我们需要针对每个 $k \in \{1, \ldots, \delta\}$ 求解该方程组，此步骤的总成本为 $\widetilde{O}(\delta^7 + \delta^6\tau)$ 次位运算。

最后，我们处理这两个集合和考虑方程组的比特大小有如下上界0，其中 $j \in \{\widetilde{0}, m\}$。根据 [18, 命题 20], ，隔离它们的实解并确定 $\partial^k f/\partial x_2^k$ 在这些点处的符号，可通过 $\widetilde{O}(\delta^6 + \delta^5\tau)$ 次位运算完成。

□

命题 2.9. 算法 PlanarComponents使用

$$\widetilde{O}((\delta^6 + \delta^3\delta_{\mathcal{P}} + \delta\delta_{\mathcal{P}}^2)(\tau + \delta) + (\delta^5 + \delta^3\delta_{\mathcal{P}} + \delta_{\mathcal{P}}^2)\tau_{\mathcal{P}} + \delta^5\delta_{\mathcal{P}} + \delta_{\mathcal{P}}^3 + \delta_q^2\tau_q)$$

次位运算。此外，输出图 $\mathcal{H}$ 满足 $|\mathcal{V}(\mathcal{H})| \in O(\delta^4 + \delta\,\delta_{\mathcal{P}})$ 且$|\mathcal{E}(\mathcal{H})| \in O\big(\delta(\delta^3 + \delta_{\mathcal{P}} + 1)\big)$。

证明。计算所有偏导数 $\partial_y^k f$所需的位运算不超过 $\widetilde{O}\big(\delta^3(\tau + \delta\log\ \delta)\big)$ 次。

根据 [37], ，算法 TopoNT 的代价为 $\widetilde{O}(\delta^6 + \delta^5\tau)$。要确定子集 $\mathcal{V}_q \subset \mathcal{V}_{\mathcal{K}}$，只需按照由 w_1 的根导出的分离界隔离 q 的根，代价为 $\widetilde{O}(\delta_q^3 + \delta_q^2\tau + \delta_q\delta^3\tau)$ 次位运算。

根据 [18, 推论 2], 的证明，计算双变量结式 w_k 的位复杂度为 $\tilde{O}\big(\delta^4\tau_k + \delta^5\big) = \tilde{O}\big(\delta^4(\tau + k\log(\delta)) + \delta^5\big)$。因此，我们可以以可忽略的代价计算 $\overline{\lambda}$，它是 λ 的一个因子，且与所有 w_i 互素，其大小有界于 $(\delta_{\mathcal{P}}, O(\tau_{\mathcal{P}} + \delta_{\mathcal{P}}))$，见 [35]。由于引理 2.7 的精度界与 i 和 j 无关，因此可以按此精度隔离所有 w_k 的根，使它们彼此分离。再考虑与 $\overline{\lambda}$ 的根之间的分离（引理 2.8），所需精度由 $\widetilde{O}\Big((\delta^3 + \delta_{\mathcal{P}})(\tau + \delta) + (\delta^2 + \delta_{\mathcal{P}})(\tau_{\mathcal{P}} + \delta_{\mathcal{P}})\Big)$ 控制。

精度为 ω_k 的实根可以通过 $\widetilde{O}(\delta^6 + (\delta^5 + \delta^2\delta_{\mathcal{P}})\tau + \delta^4(\tau_{\mathcal{P}} + \delta_{\mathcal{P}}) + \delta^2\delta_{\mathcal{P}}\tau_{\mathcal{P}})$ 次位运算计算，而对于 λ 的根，采用引理 2.8 的位精度时，我们需要 $\widetilde{O}(\delta_{\mathcal{P}}^3 + \delta_{\mathcal{P}}^2\tau_{\mathcal{P}} + (\delta_{\mathcal{P}}(\delta^2 + \delta_{\mathcal{P}})(\delta + \tau + \delta_{\mathcal{P}} + \tau_{\mathcal{P}}))$

次位运算。由于计算 x_1 个坐标的所有顶点隔离区间的总体位复杂度有界于

$$\widetilde{O}((\delta^6+\delta^3\delta_{\mathcal{P}}+\delta_{\mathcal{P}}^2)(\tau+\delta)+(\delta^5+\delta^3\delta_{\mathcal{P}}+\delta_{\mathcal{P}}^2)\tau_{\mathcal{P}}+\delta^5\delta_{\mathcal{P}}+\delta^2\delta_{\mathcal{P}}^2+\delta_{\mathcal{P}}^3).$$

为了计算 $\mathcal{H}$ 中位于 w_i 的根上方的所有顶点的隔离盒，对于 $i=2,\ldots,\delta$，我们应用 [18, 命题 20]。隔离 $w_i(x_1)=f(x_1,x_2)\partial_{x_2}^k f(x_1,x_2)=0$ 的实解并确定 f 和 $\partial_{x_2}^k f$ 的公共根，需要 $\widetilde{O}(\delta^6+\delta^5\tau)$ 次位运算。对 $i=2,\ldots,\delta$ 重复此操作，总成本为 $\widetilde{O}(\delta^7+\delta^6\tau)$。

在隔离 $\mathcal{P}$ 中的点时，我们还使用 $\widetilde{O}({\delta_{\mathcal{P}}}^2\tau_{\mathcal{P}}+{\delta_{\mathcal{P}}}^3+\delta^5\tau+\delta^6+\delta(\delta^2+\delta_{\mathcal{P}})(\delta_{\mathcal{P}}\tau+\delta\tau_{\mathcal{P}}+\delta\delta_{\mathcal{P}}))$ 次位运算，隔离 $\overline{\lambda}(x_1)=f(x_1,x_2)=0$ 的实解。为了确定对应于 $\mathcal{P}$ 中各点的隔离区间，我们应用 [38, 定理 47]，。该定理以 $\widetilde{O}({\delta_{\mathcal{P}}}^3+{\delta_{\mathcal{P}}}^2\tau_{\mathcal{P}}+\delta_{\mathcal{P}}k)$ 次位运算，为由零维参数化 $(\lambda(x_1)\ \theta_2)$ 编码的实点计算隔离区间，其中 $k=\delta(\delta_{\mathcal{P}}\tau+\delta\tau_{\mathcal{P}}+\delta\delta_{\mathcal{P}})+\delta^4+\delta^3\tau$ 是将命题 15] 应用于 $\lambda=f=0$ 和 $w_i=f=0$ 所得的结果。
将所有步骤的复杂度界相加，从同痕图 $\mathcal{G}$ 计算图 $\mathcal{H}$ 的细化过程，其复杂度为 $\widetilde{O}((\delta^6+\delta^3\delta_{\mathcal{P}}+\delta\delta_{\mathcal{P}}{}^2)(\tau+\delta)+(\delta^5+\delta^3\delta_{\mathcal{P}}+\delta_{\mathcal{P}}^2)\tau_{\mathcal{P}}+\delta^5\delta_{\mathcal{P}}+\delta_{\mathcal{P}}^3)$。结合上述结果与 SignSamples 的复杂度，即可得到PlanarComponents 所声称的复杂度界。

□

2.4 最终算法

设 $f\in\mathbb{Q}[x_1,x_2]$ 的大小为 (δ,τ)，处于一般位置坐标下，并定义曲线 $\mathcal{C}\subset\mathbb{C}^n$。我们不再假设 f 满足 $\mathcal{S}$。令 $\mathcal{P}\subset\mathcal{C}$。若 f 不满足 $\mathcal{S}$，则存在 k，使得 $g=\gcd\left(f,\partial^k f/\partial x_2^k\right)$ 的次数为正。对 g 和 f/g 递归地重复此过程，可将 f 因式分解为满足 $\mathcal{S}$ 的多项式。我们将此算法命名为 PreCond （见附录）。

引理 2.10. 算法 PreCond 使用 $O^{\sim}(\delta^6\tau+\delta^7)$ 位运算。它输出大小为 $(\delta_i,\tau_i)_{1\le i\le r}$ 的多项式 $(f_i)_{1\le i\le r}$，使得 $\sum_{i=1}^r\delta_i=\delta$ 且 $\sum_{i=1}^r\tau_i\in O^{\sim}(\tau+\delta)$。
证明. PreCond 的计算可以组织成一棵二叉树，其节点标记为作为输入传给 PreCond 的多项式。对于每个节点 ν，我们用 (δ_ν,τ_ν) 表示其标记多项式的大小。在节点 ν 处调用 PreCond 至多执行 δ 次最大公因式计算，每次计算的比特复杂度为 $O^{\sim}(\delta_\nu^4\tau_\nu+\delta_\nu^5)$。设 ν 是一个子节点为 ν' 和 ν'' 的节点。所有后代节点到 ν 的累积成本 $\mathsf{C}(\delta_\nu,\tau_\nu)$ 满足 $\mathsf{C}(\delta_\nu,\tau_\nu)\in O^{\sim}(\delta_\nu^5\tau_\nu+\delta_\nu^6)+\mathsf{C}(\delta_{\nu'},\tau_{\nu'})+\mathsf{C}(\delta_{\nu''},\tau_{\nu''})$，其中 $\delta_{\nu'}+\delta_{\nu''}=\delta_\nu$，并且根据 [35], $\tau_{\nu'}+\tau_{\nu''}\in O^{\sim}(\tau_\nu+\delta_\nu)$。解这个递推关系即可得到结论。最终的次数和比特大小估计可直接由 $f=f_1\cdots f_r$ 和 [35] 得出。

□

我们可以使用PlanarComponents为 f_i 的每个无平方因子计算一个半代数实同痕图。为了得到由 f 定义的曲线的单个图，我们必须在 $\mathcal{I}_i$ 的点处连接这些部分图，$_j:=V_{\mathbb{R}}(f_i,f_j)$ 对于 $\{1,\ldots,r\}$ 中的 $i\neq j$，令 $\mathcal{I}_i:=\bigcup_{j\neq i}\mathcal{I}_{i,\ j}$。我们将接受 $f_1,\ldots,f_r\in\mathbb{Q}[x_1,x_2]$ 作为输入，并为 $i=1,\ldots,r$ 对应的集合返回零维参数化 $\mathscr{I}_i$ 的子程序记作 ConnectionPoints。

引理 2.11。 ConnectionPoints 使用 $O^{\sim}(\delta^6+\delta^4\tau)$ 次位运算。它输出大小以 $(d_i\delta,O^{\sim}(\delta(\delta+\tau)))$ 为上界的零维参数化 $\mathscr{I}_i$。
证明。方程组 $f_i=f_j=0$ 的此类参数化可通过 $O^{\sim}((\tau+\delta)(\delta_i\delta_j)^2+(\delta_i\delta_j)^3)$ 计算，其大小上界为 $(\delta_i\delta_j,O^{\sim}((\tau_j\delta_i+\tau_i\delta_j)+\delta_i\delta_j))$。由于必须对所有不同的点对 (i,j) 执行此计算，因此得到所述复杂度。固定 i 并取相应零维参数化的并集，即可得到集合 $\mathscr{I}_i$，其大小满足所述上界；该并集的代价可以忽略不计[40]。

□

对于每个$i \in \{1, \ldots, r\}$，将 $\mathcal{I}_i$ 中的点加入 $V_{\mathbb{R}}(f_i)$ 的半代数同痕图后，我们可以连接所有部分图，从而得到一个与 $\mathcal{C}_{\mathbb{R}}$ 同痕的单一图。

我们定义一个过程 ConnectGraphs ，以半代数同位图 $\mathcal{H}_1$、……、$\mathcal{H}_r$ 为输入，这些图分别对应实曲线 $V_{\mathbb{R}}(f_1)$、……、$V_{\mathbb{R}}(f_r)$，并返回 $\mathcal{C}_{\mathbb{R}}$的半代数同位图。该过程以迭代方式运行：令 $\mathcal{H} \leftarrow \mathcal{H}_1$，对于 $i = 2$、……、r，通过识别 $\mathcal{I}_i$中对应于相同实交点的顶点，将$\mathcal{H}$ 与 $\mathcal{H}_i$ 合并；随后相应地合并边集。

算法 2 GenPlanarComponents

要求：$f \in \mathbb{Q}[x_1, x_2]$，以及定义 $\mathcal{P} \subset \mathcal{C}$的零维参数化（$\lambda(x_1)\ \theta_2$），

二者均处于一般位置坐标，且 $q \in \mathbb{Z}[x_1]$满足 q整除 $Res_{x_2}(f, \partial_{x_2} f)$。

确保：$(\mathcal{C}_{\mathbb{R}}, \mathcal{P})$的半代数同位图 $\mathcal{H}$，以及每条边 $\mathcal{H}$ $(\mathcal{C}_{\mathbb{R}})$对应的一个符号向量 σ_e。

边 $e \in \mathcal{E}(\mathcal{H})$。

1: $(f_1, \ldots, f_r) \leftarrow$ PreCond(f)
2: $(\mathscr{I}_i)_i \leftarrow$ ConnectionPoints$(f_1, \ldots, f_r)$,
3: 对于 $i = 1, \ldots, r$ **do**
4: $(\mathcal{H}_i, \mathcal{V}_{\mathcal{P}_i} \cup \mathcal{V}_i) \leftarrow$ PlanarComponents$\big(f_i, \mathcal{P} \cup \mathcal{I}_i, 1\big)$
5: 结束循环
6: $\mathcal{H} \leftarrow$ ConnectGraphs$\big(\mathcal{H}_1, \ldots, \mathcal{H}_r\big)$
7: $\mathcal{V}_q \leftarrow$ IsolatingRealSol$(q(x_1), 0)$
8: $\mathcal{V}_{\mathcal{P}} \leftarrow \bigcup_i \mathcal{V}_{\mathcal{P}_i}$
9: 返回 $(\mathcal{H}, \mathcal{V}_{\mathcal{P}}, \mathcal{V}_q)$

引理 2.12. ConnectGraphs 使用 $\widetilde{O}(\delta^4 + \delta\delta_{\mathcal{P}})$ 位运算。

证明。该过程扫描 $\mathcal{H}_1, \ldots, \mathcal{H}_r$的顶点集，并合并对应于相同交点的顶点。根据命题 2.9 中顶点数量的界，我们得出位运算次数为 $\widetilde{O}(\sum_i(\delta_i^4 + \delta_i(\delta_{\mathcal{P}} + \delta_i\delta))$。

□

注意，与图 $\mathcal{H}$ 相关联的顶点集 $\mathcal{V}_{\mathscr{K}}$满足 $V_{\mathscr{K}} = \bigcup_{i=1}^{r}\big(V_{\mathscr{K}_i} \cup V_i\big)$，其中 $V_{\mathscr{K}_i}$ 表示与 $\mathscr{K}(\pi_1, \mathcal{C}_i)$相关联的顶点集。隔离出 q 的实根后，即可利用这一事实确定子集$V_q \subset \mathcal{V}_{\mathscr{K}}$。

定理 2.2 的证明。根据引理 2.10、引理 2.11 和引理 2.12，分别可得 PreCond、ConnectionPoints 和 Connect-Graphs的复杂度。随后，对每个 i，我们将 $(\delta, \tau) \mapsto (\delta_i, O^{\sim}(\tau + \delta))$ 和 $(\delta_{\mathcal{P}}, \tau_{\mathcal{P}}) \mapsto (\delta_{\mathcal{P}} + \delta_i\delta,\ \tau_{\mathcal{P}} + O^{\sim}(\delta(\tau + \delta)))$ 代入命题 2.9 的复杂度界 PlanarComponents，并对所有指标求和。集合 $\mathcal{V}_q$ 的处理沿用命题 2.9 证明中的相同策略，唯一额外的代价为 $\widetilde{O}(\delta_q^2\tau_q)$。

□

3 空间曲线

我们用 $\mathcal{C} \subset \mathbb{C}^n$ 表示一条代数曲线，其对应的理想由 $\boldsymbol{f} = (f_1, \ldots, f_{n-1}) \in \mathbb{Q}[\boldsymbol{x}]$ 生成，其中 f_i 的大小以 (d, h) 为界。对于 $1 \le i \le n$，我们用 π_i 表示投影 $(\xi_1, \ldots, \xi_n) \to (\xi_1, \ldots, \xi_i)$。令 $\mathsf{app}(\mathcal{C}_2) := \mathsf{sing}(\mathcal{C}_2) \setminus \pi_2\big(\mathsf{sing}(\mathcal{C})\big)$ 表示 $\mathcal{C}_2$ 的表观奇点集。令 $\mathcal{P} \subset \mathsf{reg}(\mathcal{C})$ 为一个有限集，且 $\mathcal{P}_2 = \pi_2(\mathcal{P})$。我们假设 $(\mathcal{C}, \mathcal{P})$ 处于一般位置，即它们满足 [31] 的性质 (H)，而这些性质可在一般线性坐标变换下恢复，见命题 2.5]。于是，投影曲线 $\mathcal{C}_2$ 的表观奇点可被显式确定，见命题 3.2]。令 $q_{\mathrm{app}} \in \mathbb{Q}[x_1]$为命题 5.1] 中给出的过程 ApparentSingularities 的输出；该过程以 $\mathcal{C}$ 的参数化 $\mathfrak{R}$ 为输入，并返回一个多项式，用以定义 x_1-投影的

$\mathcal{C}_2$ 的表观奇点。我们用 $\mathfrak{P}$ 表示一个编码 $\mathcal{P}$ 的零维参数化。

3.1 图构造

令 $\mathcal{H}_w$ 为 PlanarComponents$(\omega, \mathfrak{P}, q_{\text{app}})$ 返回的 $\mathcal{C}_2$ 的半代数同痕图。 $\mathcal{C}$ 的参数化无法提升到 $\mathbb{R}^n$ 的点，正是那些使 $\partial w/\partial x_2 = 0$ 相消的点。所有这些点都作为顶点出现在图 $\mathcal{H}_w$ 中。于是， $\mathcal{H}_w$ 每条边以及 $V(\mathcal{H}_w)$ 中每个顶点的半代数描述，都可以根据 $\setminus \mathcal{K}(\pi_1, \mathcal{C}_2)$ 提升到 $\mathbb{R}^n$。此外，由于 π_2 在 $\mathcal{C}$ 上的限制在 $x \in \mathcal{C}$ 处非单射，当且仅当 $\pi_2(x) \in \mathsf{app}(\mathcal{C}_2)$ [31,Cor. 2.4],，因此 $\mathcal{K}(\pi_1, \mathcal{C}_2)$ 中顶点的半代数描述也可以根据 $\setminus \mathsf{app}(\mathcal{C}_2)$ 提升到 $\mathbb{R}^n$：只需将方程 $\boldsymbol{f} = 0$ 添加到它们在 (x_1, x_2) 平面中的描述中。

我们需要确定与 $\mathcal{H}_w$ 的边相对应的哪些曲线段属于 $\mathcal{C}_{\mathbb{R}}$ 的同一个连通分支，以及如何描述缺失的点。第一个问题由 [31] 中的分析解决。该分析使我们能够将局部描述汇集起来，得到 $\mathcal{C}_{\mathbb{R}}$ 连通分支的整体结构。

$\mathcal{C}_2$ 与 $\mathcal{C}$ 的连通性性质仅在 $\mathsf{app}(\mathcal{C}_2)$ 中的点处有所不同。根据 [31, 引理 4.5]，可知曲线在这些点邻域内的行为。设 v_0 是图 $\mathcal{H}_w$ 中对应于 $\mathsf{app}(\mathcal{C}_2)$ 的一个实点的顶点。那么恰有四条 $\mathcal{H}_w$ 的边从 v_0 发出。设这些边为 $e_1, \ldots, e_4$，沿每条边从 v_0 向外走到达的顶点为 $v_1, \ldots, v_4$。边 $e_1, \ldots, e_4$ 围绕 v_0 有唯一的循环排序。按照这一排序，这些边分成两对对边：(e_1, e_3) 和 (e_2, e_4)。[31, 引理 4.5] 表明，提升到 $\mathbb{R}^n$ 后，对应于每一对对边的 $\mathcal{C}_{\mathbb{R}}$ 分支在 $\mathcal{C}_{\mathbb{R}}$ 中连通，而对应于不同边对的分支则不连通。设 $V_{\text{app}} \subset V(\mathcal{H}_w)$ 为对应于 $\mathsf{app}(\mathcal{C}_2)$ 中各点的顶点集合。过程 SANodeResolution 以 $(\mathcal{H}_w, V_{\text{app}})$ 为输入，生成一个新图 $\mathcal{H}'$，汇集 $\mathcal{H}_w$ 中属于 $\mathcal{C}_{\mathbb{R}}$ 同一连通分支的顶点和边；其定义与 NodeResolution [31, 定义 4.6], 相同，因此 $\mathcal{H}'$ 与 $\mathcal{C}_{\mathbb{R}}$ 具有相同的连通性（见 [31, 命题 4.7]）。每条边相关联的半代数数据 σ_e 均予以保留，因此调用 SANodeResolution 后，对于 $\mathcal{C}_{\mathbb{R}}$ 的每个连通分支 D_i，我们都能得到半代数描述 $\Theta_i, 1, \ldots, \Theta_{i,\ell_i}$，其解集与 $D_i \setminus \pi_2^{-1}(\mathsf{app}(\mathcal{C}_2))$ 一致。这就是我们所说的 $\mathcal{C}_{\mathbb{R}}$ 连通分支的部分描述。算法 Par-tialComponents 以 $\mathfrak{R}$ 和 $\mathfrak{P}$ 为输入，通过依次调用 ApparentSingularities、GenPlanarComponents 和 SANodeResolution 返回这样的部分描述（见附录）。

引理 3.1. 算法 PartialComponents 正确，且使用$O\tilde{}((\delta^6 + \delta^4\delta_{\mathcal{P}} + \delta\delta_{\mathcal{P}}^2)(\tau + \delta) + (\delta^5 + \delta^3\delta_{\mathcal{P}} + \delta_{\mathcal{P}}^2)\tau_{\mathcal{P}} + \delta_{\mathcal{P}}^3)$ 位运算。

证明. 根据 [31, 命题 5.1],，ApparentSingularities 使用 $O\tilde{}(\delta^6 + \delta^5\tau)$ 位运算，其输出的大小为 $(\delta^2, O\tilde{}(\delta^2 + \delta\tau))$。将此代入定理 2.2，可得步骤 2 的比特复杂度为 $O\tilde{}((\delta^6 + \delta^4\delta_{\mathcal{P}} + \delta\delta_{\mathcal{P}}^2)(\tau + \delta) + (\delta^5 + \delta^3\delta_{\mathcal{P}} + \delta_{\mathcal{P}}^2)\tau_{\mathcal{P}} + \delta_{\mathcal{P}}^3)$。

正确性由它们的正确性（见 ApparentSingularities）、 PlanarCom-ponents（定理 2.2 ）以及上述讨论与 NodeRes-olution 的正确性共同推出。 □

3.2 算法描述与正确性

我们的主要算法在应用两种不同的线性坐标变换后，会调用两次 PartialComponents，使得两个不同坐标系下的半代数描述能够覆盖那些此前遗漏的点。对于 $\boldsymbol{A} \in \mathrm{GL}_n(\mathbb{C})$，我们用 $\mathcal{C}_{2,\boldsymbol{A}}$ 表示 $\pi_2(\mathcal{C}^{\boldsymbol{A}})$ 的扎里斯基闭包。

定理 3.2. 假设点对 $(\mathcal{C}, \mathcal{P})$ 满足条件 (H)。存在一个非空的扎里斯基开集 $\mathcal{A} \subset GL_n(\mathbb{C})$，使得对于所有 $\boldsymbol{A} \in \mathcal{A}$，$(\mathcal{C}^{\boldsymbol{A}}, \mathcal{P}^{\boldsymbol{A}})$ 满足 (H)，且集合 $\pi_2^{-1}(\text{app}(\mathcal{C}_2))$ 与 $\pi_2^{-1}(\text{app}(\mathcal{C}_{2,\boldsymbol{A}})))^{\boldsymbol{A}^{-1}}$ 的交集为空。

定理 3.2 的证明推迟到第 4 节。由此可知，通过选取 $\mathcal{C}^{\boldsymbol{A}}$ 的第二个参数化，对于 $\boldsymbol{A} \in \text{GL}_n(\mathbb{Q})$，我们可以为 $\mathcal{C}_{\mathbb{R}}$ 的每个连通分支 D_i 得到半代数描述 $\Xi_{i,1}, \ldots, \Xi_{i,s_i}$，使其解集与 $D_i \setminus \pi_2^{-1}(\text{app}(\mathcal{C}_2))^{\boldsymbol{A}^{-1}}$一致。由于失效集互不相交，将这两个描述合并即可得到 $\mathcal{C}_{\mathbb{R}}$ 每个连通分支的半代数描述。下面说明如何进行合并。设 $\mathfrak{T}$ 表示一个有限集 $\mathcal{T} \subset \text{reg}(\mathcal{C})$，它与 $\mathcal{C}_{\mathbb{R}}$ 的每个连通分支都相交。分别令 $\mathcal{H}_1$ 和 $\mathcal{H}_2$ 为将 PartialComponents 应用于 $(\mathfrak{R}, \mathfrak{T})$ 和 $(\mathfrak{R}^{\boldsymbol{A}}, \mathfrak{T}^{\boldsymbol{A}})$ 后得到的输出，其中 $\boldsymbol{A} \in \text{GL}_n(\mathbb{Q})$ 满足定理 3.2 的假设。过程 ConnectParams 以 $\mathfrak{T}$、$\mathcal{H}_1$ 和 $\mathcal{H}_2$ 为输入，并输出 $\mathcal{C}_{\mathbb{R}}$ 每个连通分支的半代数描述。其步骤如下。设 $\Theta_{i,1}, \ldots, \Theta_{i,t_i}$ 为从 $\mathcal{H}_1$ 得到的半代数描述，用于描述 $D_i \setminus \pi_2^{-1}(\text{app}(\mathcal{C}_2))$。如果 $D_i \setminus \pi_2^{-1}(\text{app}(\mathcal{C}_2))$ 归结为一个奇点，那么$t_i = 1$ 和 D_i 可由 $\Theta_{i,1}$ 描述。否则，存在 $\zeta \in \mathcal{T}$ 和 $\alpha \in \{1, \ldots, t_i\}$，使得 $\zeta \in \Theta_{i,\alpha}$。接着，我们选取从 $\mathcal{H}_2$ 得到的半代数描述 $\Xi_{j,1}, \ldots, \Xi_{j,s_j}$；这些描述对应于 $\mathcal{C}_{\mathbb{R}}$ 同一连通分支中的若干部分，并且存在 $\beta \in \{1, \ldots, s_j\}$ 使得 $\zeta \in \Xi_{j,\beta}$。D_i 的半代数描述为$D_i = \Theta_{i,1} \cup \cdots \cup \Theta_{i,t_i} \cup \Xi_{j,1} \cup \cdots \cup \Xi_{j,s_j}$。

命题 3.3. 算法 ConnectParams 是正确的，且执行 $O\left(\delta^4 + \delta\delta_{\mathcal{T}}\right)$ 位运算。这里，δ 表示 $\mathfrak{R}$ 和 $\mathfrak{R}^{\boldsymbol{A}}$的次数上界，而 $\delta_{\mathcal{T}}$表示 $\mathfrak{T}$的次数上界。

证明。正确性由 PartialComponents的正确性以及定理 3.2 得出；定理 3.2 保证了 $\zeta \in \cap D_i \setminus \pi_2^{-1}(\text{app}(\mathcal{C}_2))$ 的存在性以及失效集彼此不相交，因此所选描述的并集给出 D_i。由于 ConnectParams的大部分工作是遍历 $\mathcal{H}_1$ 和 $\mathcal{H}_2$ 的顶点与边（其基数属于 $O\left(\delta^4 + \delta\delta_{\mathcal{T}}\right)$，见定理 2.2），位运算的次数为 $O\left(\delta^4 + \delta\delta_{\mathcal{T}}\right)$。 □

根据 [31, 命题 2.5], , 存在一个非空的 Zariski开集 $\mathcal{U} \subset \text{GL}_n(\mathbb{C})$，使得对所有 $\boldsymbol{A} \in \mathcal{U}$，$(\mathcal{C}^{\boldsymbol{A}}, \mathcal{P}^{\boldsymbol{A}})$ 都满足 (H)。

算法 3 CurveComponents

要求：$\boldsymbol{f} \in \mathbb{Q}[\boldsymbol{x}]$、$0 < \epsilon < 1$、$\boldsymbol{A}_1 \in \mathcal{U}$和 $\boldsymbol{A}_2 \in \mathcal{A}$
确保：$\mathcal{C}_{\mathbb{R}}$的各分支的半代数描述,
1: $\mathfrak{P} \leftarrow \text{RegularPoints}(\boldsymbol{f}, \epsilon)$
2: $\mathfrak{R} \leftarrow \text{OneDimParam}(\boldsymbol{f}, \epsilon)$
3: 计算 $(\mathcal{C}^{\boldsymbol{A}_1}, \mathcal{P}^{\boldsymbol{A}_1})$
4: $\mathcal{H}'_w \leftarrow \text{PartialComponents}(\mathcal{R}^{\boldsymbol{A}_1}, \mathcal{P}^{\boldsymbol{A}_1})$
5: 计算 $(\mathcal{C}^{\boldsymbol{A}_2}, \mathcal{P}^{\boldsymbol{A}_2})$
6: $\mathcal{H}'_{w'} \leftarrow \text{PartialComponents}(\mathcal{R}^{\boldsymbol{A}_2}, \mathcal{P}^{\boldsymbol{A}_2})$
7: 返回 $(D_i)_{i=1}^r \leftarrow \text{ConnectParams}(\mathcal{H}'_w, \mathcal{H}'_{w'})$

正确性证明 定理 1.1。根据 [31, 命题 2.5], , 选择 $\boldsymbol{A}_1 \in \mathcal{U} = GL_n(\mathbb{Q}) \setminus \mathscr{Z}$可确保数对 $(\mathcal{C}^{\boldsymbol{A}_1}, \mathcal{P}^{\boldsymbol{A}_1})$ 满足假设（H）。然后，使用定理 3.2 中的记号，选择 $\boldsymbol{A}_2 \in \mathcal{A} = GL_n(\mathbb{Q}) \setminus \mathscr{Z}_{\boldsymbol{A}_1}$ 可保证两个参数化的失效集不相交，并且 $(\mathcal{C}^{\boldsymbol{A}_2}, \mathcal{P}^{\boldsymbol{A}_2})$ 满足（H）。根据引理 3.1 和引理3.3，可得出 PartialComponents和 ConnectParams的正确性。 □

3.3 子程序

引理 3.4。存在一种算法 RegularPoints ，它以 $\boldsymbol{f}$ 和$0 < \epsilon < 1$为输入，计算出 $\mathcal{P}$ 的零维参数化，其大小为$(O\left(n^3d^n\right), O\tilde{}(n^6d^{n+1}+n^8d^n(h+\log\left(\frac{1}{\epsilon}\right))$，需要 $O\tilde{}($ $n^{15}d^{2n+2}\binom{n+d}{n}\left(h+\log(\frac{1}{\epsilon})\right))$ 次位运算，且成功概率至少为 $1-\epsilon$。

证明。由于 $\langle \boldsymbol{f}\rangle$ 是根理想，在 reg($\mathcal{C}$) 的所有点处，与 $\boldsymbol{f}$ 相关联的雅可比矩阵 $J(\boldsymbol{f})$ 的某个 ($n-1$) 阶子式 $\Delta_1,\ldots,\Delta_{n-1}$ 非零。令 $\Delta\in\mathscr{D}=\{\Delta_1,\ldots,\Delta_{n-1}\}$ 和 T 为新变量。我们计算由 $\boldsymbol{f}=T\Delta-1=0$ 定义的实代数集的每个连通分支上的一个点，并在 Δ 遍历 $\mathscr{D}$ 时重复此过程。令 $\boldsymbol{g}=(\boldsymbol{f},\Delta)$。注意，雅可比矩阵 $J(\boldsymbol{g})$ 在 $V(\boldsymbol{g})$ 的任意点处均为满秩。因此， $\boldsymbol{g}$ 生成一个根理想并定义一个光滑代数集。我们采用 [24] 中介绍的 [39] 概率算法的变体。该算法选取一个足够一般的矩阵 $\boldsymbol{M}\in\mathrm{GL}_{n+1}(\mathbb{Q})$，并求解零维方程组 (1)$\boldsymbol{g}^{\boldsymbol{M}}=0, \boldsymbol{\lambda}J(\boldsymbol{g}^{\boldsymbol{M}})=(1,0,\ldots,0)$（其中 $\boldsymbol{\lambda}=(\lambda_1,\ldots,\lambda_n)$ 是一列拉格朗日乘子），以及 (2) $\boldsymbol{g}^{\boldsymbol{M}}=x_1-\eta=0$，其中 η 也选取得足够一般。两者都生成根理想。按照 [24]) 中的方法使用 [25]，为确保成功概率大于 $\frac{1}{\epsilon}$， η 的比特大小以及 $\boldsymbol{M}$ 的元素取为 $O\tilde{}(n+\log\left(\frac{1}{\epsilon}\right))$。

根据链式法则公式，求解 (1) 等价于求解 $\boldsymbol{g}=0$ 和 $\boldsymbol{\lambda}J(\boldsymbol{g})=\boldsymbol{m}$ 其中 $\boldsymbol{m}$ 是 $\boldsymbol{M}^{-1}$的第一列。如 [24], 中一样，我们使用 [41]的符号同伦算法。将变量划分为 $\boldsymbol{x}$、z、$\boldsymbol{\lambda}$，并为 (1) 中的每个方程指定其关于 $\boldsymbol{x}$、z、$\boldsymbol{\lambda}$的偏次数。由此可得，有 $(n-1)$ 个（分别有 n 个）三重次数为 (d, 0, 0)（分别为 $(n(d-1), 1, 1)$）的多项式，另有 1 个三重次数为 $(n(d-1), 1, 0)$ 的多项式和 1 个三重次数为 $(n(d-1), 0, 1)$ 的多项式。其系数的比特大小至多为 $\tau\in h+n(n+\log(\frac{1}{\epsilon}))$。关于多齐次 B´ézout 次数和高度界 [41, Prop. 3 & 4] 的技术性但简单的计算表明，该集合的次数和高度分别为$O\left(n^2d^n\right)$ 和 $O\tilde{}(n^6d^{n+1}+n^8d^n(h+\log\left(\frac{1}{\epsilon}\right))$（参见附录）。此外，根据 [24, Lemma 5],，(1) 可由长度为 $O\left(n^2+n\binom{n+d}{d}\right)$、整数系数上界为 $b\in O\tilde{}(h+n(n+\log(\frac{1}{\epsilon})))$ 的直线程序求值。令 $\tau\in O\tilde{}(h+n(n+\log(\frac{1}{\epsilon}))+d)$。按照 [24, Thm. 1], 的证明中的做法应用 [41, Thm.1]，即可用 $O\tilde{}(n^{14}d^{2n+2}\binom{n+d}{n}\left(h+\log(\frac{1}{\epsilon})\right))$ 次位运算求解 (1)。

式 (2) 的次数界和高度界来自 B´ezout 型界（仍适用 [41]），且小于式 (1) 的相应界。对 $\mathscr{D}$ 中的 Δ 迭代此过程，会使上述估计乘以 n。取并集不会增加复杂度（见 [40, 引理 J.3]）。 □

引理 3.5. 存在一个算法 OneDimParam ，它以 $\boldsymbol{f}$ 和 $0<\varepsilon<1$ 为输入，计算一个大小不超过 $\left(d^{n-1}\right.$、$O\tilde{}$（d^{n-1}（$nh+n$））$\left.\right)$的一维参数化；对于 $\mathcal{C}$，该算法使用 $O\tilde{}$（（$h+\log$（$\frac{1}{\epsilon}$））$\binom{n+d}{n}n^4d^{3n}$）次位运算，成功概率为 $>1-\epsilon$。

证明。这是民间知识，许多地方都陈述过相近的结果（据我们所知， [42, 第 15 章定理 18] 给出了最早的此类结果）。我们沿用 [42] 引入的策略。由 B´ezout 界可立即得到次数上界。根据 [41, 命题 5],，在某个素域（其特征足够大）中为 V（$\boldsymbol{f}$）$\cap\mathcal{H}$ 计算零维参数化，其中 $\mathcal{H}$ 是一个一般超曲面，需要 $O\tilde{}$（log $(\frac{1}{\epsilon})$ $nd^{2(n-1)}\left(\binom{n+d}{n}+d+n^2\right)$）次算术运算。根据 $O\tilde{}$（$n\left(\binom{n+d}{n}+n^3\right)d^{2n-1}$） [27, 引理 3], 将此参数化提升为所考虑素域中的一维参数化需要相应的计算。接下来，只需利用 [16, 定理 1] 给出的输出比特大小上界 $\tau=O\tilde{}$（d^{n-1}（$nh+n$））， 将这一维参数化提升到有理数域上。再次使用 [27, 引理 3], 即可得出结论。 □

3.4 定理 1.1 的证明（复杂度）

步骤 1 和 2 的开销由引理 3.4 和 3.5 给出。令 $\overline{\tau}$ 为矩阵 $\boldsymbol{A}_1$ 和 $\boldsymbol{A}_2$ 各元素的最大比特大小。根据 [40, 引理 J.1] 和 [40, 引理 J.7],，由 $\overline{\tau}$ 和 $\boldsymbol{A}_1$ 在参数化 $\boldsymbol{A}_2$ 和 [40, 上诱导的线性变换

使用 $\widetilde{O}\big((n^2d_{\mathcal{P}}+n^2\delta^2+n^3)(\tau_{\mathcal{P}}+n\overline{\tau})\big)$ 位运算，不会增加其次数，且系数的比特大小分别不超过 $\tau_{\mathcal{P}}+n\overline{\tau}$ 和 $\tau+n\overline{\tau}$。步骤 4 和 6 的开销由引理 3.1 给出。

综合前面的所有步骤，该算法执行的位运算次数为CurveComponents

$$\begin{aligned}&\widetilde{O}\Big(nd^{7n-7}h+n^6d^{6n-4}+n^9d^{5n-2}+n^{12}d^{3n+1}+\\&\quad\big(d^{6n-6}+n^4d^{5n-4}+n^7d^{3n-1}\big)\overline{\tau}+(h+\log\frac{1}{\varepsilon})\times\\&\quad\Big(n^8\big(d^{6n-5}+n^3d^{5n-3}+n^6d^{3n}\big)+\binom{n+d}{n}\big(n^4d^{3n}+n^{16}d^{2n+4}\big)\Big)\Big).\end{aligned}$$

对于 $n\geq 3$，可简化为

$$\widetilde{O}(n^{12}d^{7n-7}(h+\overline{\tau}+1)+(h+\log\frac{1}{\varepsilon})(n^{14}d^{6n-5}+\binom{n+d}{n}n^{16}d^{3n})).$$

4 定理 3.2 的证明

根据 [31, 命题 2.5], ，存在一个非空的扎里斯基开集 $\mathcal{U}\subset \mathrm{GL}_n(\mathbb{C})$，使得对于所有 $A\in\mathcal{U}$，$(\mathcal{C}^A,\mathcal{P}^A)$ 都满足 (H)。令 $\boldsymbol{Ax}=(\boldsymbol{a}_1,\ldots,\boldsymbol{a}_n)$，并令 $\pi_{\boldsymbol{a}_1,\boldsymbol{a}_2}$ 为投影$\xi\to\boldsymbol{a}_1(\xi)\ \boldsymbol{a}_2(\xi)$。

令 $\mathcal{C}\subset\mathbb{C}^n$ 为一条代数曲线，其对应的理想由$\boldsymbol{f}=(f_1,\ldots,f_{n-1})\subset\mathbb{Q}[\boldsymbol{x}]$生成。令 $\mathcal{C}_{2,\boldsymbol{A}}$ 为 $\pi_{\boldsymbol{a}_1,\boldsymbol{a}_2}(\mathcal{C})$ 的扎里斯基闭包，$w_{\boldsymbol{A}}$ 为其定义多项式。令 $\mathfrak{A}=(\mathfrak{a}_{i,j})$ 为一个元素未知的 $n\times n$ 矩阵，$\mathfrak{a}_i$ 为$\mathfrak{A}\boldsymbol{x}$ 的第 i 个元素，且 $\zeta=(\zeta_1,\ldots,\zeta_n)\in\mathrm{reg}(\mathcal{C})$。

引理 4.1. 存在一个非空的扎里斯基开集 $\mathcal{A}_\zeta\subset GL_n(\mathbb{C})$，使得对于所有 $A\in\mathcal{A}_\zeta$,$\pi_{\boldsymbol{a}_1,\ \boldsymbol{a}_2}(\zeta)$ 都不是 $\mathcal{C}_{2,\ \boldsymbol{A}}$ 的节点。

证明. 根据雅可比判据 [22, 定理 16.19], ， $\boldsymbol{f}$ 的雅可比矩阵 J_f 在 $\mathrm{reg}(\mathcal{C})$ 的任意点处秩为 $n-1$。令 Δ 为 J_f 的一个 $(n-1)\times(n-1)$ 子式 Δ。我们考虑方程组:

$$S_i(\zeta,\Delta)\begin{cases}u\cdot\Delta(\boldsymbol{x})-1=0,t\cdot(x_i-\zeta_i)-1=0,\\ f_1(\boldsymbol{x})=\cdots=f_{n-1}(\boldsymbol{x})=0,\\ \mathfrak{a}_1(\boldsymbol{x}-\zeta)=0,\mathfrak{a}_2(\boldsymbol{x}-\zeta)=0.\end{cases}$$

其中变量 t 和 u 是新的。令 $\mathfrak{c}_1$ 和 $\mathfrak{c}_2$ 分别为线性形式 $\mathfrak{a}_1$和 $\mathfrak{a}_2$的（未知）系数序列。现在我们考虑这 $n+3$ 个方程关于变量 $u,t,\boldsymbol{x},\mathfrak{c}_1,\mathfrak{c}_2$ 的雅可比矩阵 $J_{\boldsymbol{f}}$。它具有分块形式

$$\left(\begin{array}{c|c|c|c|c}\Delta(x)&0&u\nabla\Delta(x)&0&0\\\hline 0&x_i-\zeta_i&t&0&0\\\hline 0&0&J_f(x)&0&0\\\hline 0&0&\mathfrak{c}_1{}^{\mathsf{T}}&(x-\zeta)^{\mathsf{T}}&0\\\hline 0&0&\mathfrak{c}_2{}^{\mathsf{T}}&0&(x-\zeta)^{\mathsf{T}}\end{array}\right)$$

其中，$\nabla(\Delta(x))$表示多项式 Δ 关于变量 $\boldsymbol{x}$的梯度。简单验证可知，该雅可比矩阵的秩为 $n+3$。根据雅可比判据 [22,定理 16.19], ，我们可推知 $V(S_i(\zeta,\Delta))$要么为空，要么余维为 $n+3$（此时维数为 $2n-1$）。于是，其在 $\mathfrak{c}_1,\mathfrak{c}_2$ 空间上的投影 $\pi_{\mathfrak{c}}$ 的余维至少为 1。换言之，存在一个非零多项式$\Psi_{i,\zeta,\Delta}\in\mathbb{Q}[\mathfrak{c}_1,\mathfrak{c}_2]$，使得若$\Psi_{i,\zeta,\Delta}(\boldsymbol{c}_1,\boldsymbol{c}_2)\neq 0$，则 $\pi_{\mathfrak{c}}^{-1}(\boldsymbol{c}_1,\boldsymbol{c}_2)\cap V(S_i(\zeta,\Delta))=\emptyset$。我们用$\mathcal{B}_{i,\zeta,\Delta}\subset\mathrm{GL}_n(\mathbb{C})$表示由$\Psi_{i,\zeta,\Delta}\neq 0$定义的非空扎里斯基开集，并将 $\mathcal{B}_\zeta$ 记为所有$\mathcal{B}_{i,\zeta,\Delta}$的交集，其中 i 遍历 $\{1,\ldots,n\}$，而 Δ 遍历 $J_{\boldsymbol{f}}$的 $(n-1)\times(n-1)$子式。注意，当 $\boldsymbol{A}\in\mathcal{B}_\zeta$时，在 $\mathrm{reg}(\mathcal{C})\setminus\{\zeta\}$ 中不存在点z 使得 $\boldsymbol{a}_1(z)=\boldsymbol{a}_1(\zeta)$且 $\boldsymbol{a}_2(z)=\boldsymbol{a}_2(\zeta)$（$\boldsymbol{a}_1$ 和 $\boldsymbol{a}_2$ 分别表示 $\boldsymbol{Ax}$的第一和第二个分量）。

现在，取 $z\in\mathrm{sing}(\mathcal{C})$。由于根据假设 $\zeta\in\mathrm{reg}(\mathcal{C})$，我们有 $z\neq\zeta$。因此，

$\Phi_{z,\zeta} = (\mathfrak{a}_1(z) - \mathfrak{a}_1(\zeta))\,(\mathfrak{a}_2(z) - \mathfrak{a}_2(\zeta)) \in \mathbb{Q}[\mathfrak{c}_1, \mathfrak{c}_2]$ 不恒等于零。令 $\mathcal{B}_{z,\zeta}$ 为 $\mathrm{GL}_n(\mathbb{C})$ 中由 $\Phi_{z,\zeta} \neq 0$定义的非空扎里斯基开集。令 $\mathcal{B}_{\zeta,\mathrm{sing}} = \cap_{z \in \mathrm{sing}(\mathcal{C})} \mathcal{B}_{z,\zeta}$。取 $\boldsymbol{A} \in \mathcal{A}_\zeta = \mathcal{U} \cap \mathcal{B}_\zeta \cap \mathcal{B}_{\zeta,\mathrm{sing}}$。注意，$\mathcal{C}_{2,\boldsymbol{A}} = \pi_{\boldsymbol{a}_1,\boldsymbol{a}_2}(\mathcal{C}^{\boldsymbol{A}})$（由 (H)），并且对所有 $z \in \mathcal{C}$，不存在满足 $\boldsymbol{a}_1(z) = \boldsymbol{a}_1(\zeta)$ 且 $\boldsymbol{a}_2(z) = \boldsymbol{a}_2(\zeta)$ 的点；也就是说，$\pi_{\boldsymbol{a}_1,\boldsymbol{a}_2}(\zeta)$ 不是 $\mathcal{C}_{2,\boldsymbol{A}}$ 的节点。 □

定理 3.2 的证明。考虑有限集 $\pi_2^{-1}(\mathrm{app}(\mathcal{C}_2)) \cup \mathrm{reg}(\mathcal{C})$。由于成为表观奇点的条件比成为节点的条件更强，只需定义 $\mathcal{A} := \bigcap_\zeta \mathcal{A}_\zeta$，其中每个 $\mathcal{A}_\zeta$ 均由引理 4.1 给出。由此得到的集合 $\mathcal{A}$ 是一个非空的扎里斯基开集。 □

参考文献

[1] L. Alberti、B. Mourrain 和 J. Wintz。半代数平面曲线的拓扑与排列计算。《计算机辅助几何设计》，25(8):631–651，2008年。[2] J. G. Alc´azar 和 J. R. Sendra。实代数空间曲线的拓扑计算。《符号计算杂志》，39(6):719–744，2005年。[3] D. Arnon、G. Collins 和 S. McCallum。三维空间柱面代数分解的邻接算法。《符号计算杂志》，5(1):163–187，1988年。[4] D. Arnon、G. Collins 和 S. McCallum。柱面代数分解 II：平面邻接算法。载于 Bob F. Caviness 和 Jeremy R. Johnson 编，《量词消去与柱面代数分解》，第152–165页，维也纳，1998年。施普林格。[5] D. Arnon 和 S. McCallum。求实代数曲线拓扑类型的多项式时间算法。《符号计算杂志》，5(1-2):213–236，1988年。[6] S. Basu、R. Pollack 和 M.-F. Roy。《实代数几何算法》，《数学中的算法与计算》第10卷。施普林格，第2版，2006年。[7] E. Berberich、P. Emeliyanenko、A. Kobel 和 M. Sagraloff。平面代数曲线的精确符号-数值计算。《理论计算机科学》，491:1–32，2013年。[8] C. W. Brown 和 J. H. Davenport。量词消去与柱面代数分解的复杂度。载于《2007年国际符号与代数计算研讨会论文集》，ISSAC ’07，第54–60页，美国，2007年。ACM。[9] M. Burr、S. W. Choi、B. Galehouse 和 C. Yap。完整细分算法 II：奇异代数曲线的同位网格划分。《符号计算杂志》，47(2):131–152，2012年。[10] J. Canny、D. Yu. Grigor’ev 和 N. N. Vorobjov。在亚指数时间内求半代数集的连通分支。《应用代数、工程、通信与计算》，2(4):217–238，1992年5月。[11] C. Chen 和 W. Wu。一种用于可视化带奇点平面实代数曲线的延拓法。载于 V. Gerdt、W. Koepf、W. Seiler 和 E. Vorozhtsov 编，《科学计算中的计算机代数》，第99–115页，尚贝里，2018年。施普林格。[12] J. Cheng、K. Jin 和 D. Lazard。采用局部一般位置法对实代数空间曲线进行经认证的有理参数逼近。《符号计算杂志》，58:18–40，2013年。

[13] J. Cheng、K. Jin、M. Pouget、J. Wen 和 B. Zhang。实代数空间曲线拓扑计算的改进复杂度界。《符号计算杂志》，125:102309，2024年。[14] J. Cheng、S. Lazard、L. Pe˜naranda、M. Pouget、F. Rouillier 和 E. Tsigaridas。关于实代数平面曲线的拓扑。《数学与计算机科学》，4(1):113–137，2010年。[15] G. E. Collins。通过柱面代数分解对实闭域进行量词消去。《计算机科学讲义》，33:515–532，1975年。[16] X. Dahan、A. Kadri 和 E. Schost。正维三角集的位大小估计。《复杂性杂志》，28:109–135，2012年。[17] D. N. Daouda、B. Mourrain 和 O. Ruatta。关于非约化隐式空间曲线的拓扑计算。载于《2008年国际符号与代数计算研讨会论文集》，ISSAC 2008，奥地利林茨/哈根贝格，2008年7月20–23日，第47–54页。ACM，2008年。[18] D. N. Diatta、S. Diatta、F. Rouillier、M. F. Roy 和 M. Sagraloff。代数数上的多项式界及其在曲线拓扑中的应用。《离散与计算几何》，67:631–697，2022年。[19] A. Drogoul。一阶控制同轴望远镜的经认证分类，2025年。[20] A. Eigenwillig 和 M. Kerber。任意代数曲线的精确高效二维排列。载于《第十九届ACM-SIAM 离散算法年度研讨会论文集》，SODA 2008，美国加利福尼亚州旧金山，2008年1月20–22日，第122–131页。ACM、SIAM，2008年。[21] A. Eigenwillig、M. Kerber 和 N. Wolpert。实代数平面曲线的快速精确几何分析。载于《2007年国际符号与代数计算研讨会论文集》，ISSAC 2007，加拿大安大略省滑铁卢，2007年7月29日–8月1日，第151–158页。ACM，2007年。[22] D. Eisenbud。《从代数几何视角看交换代数》，《数学研究生教材》第150卷。施普林格，1995年。[23] M. El Kahoui。实代数空间曲线的拓扑。《符号计算杂志》，43(4):235–258，2008年。[24] J. Elliot、M. Giesbrecht、E. Gillot、M. Safey El Din 和 E. Schost。计算光滑完全交实代数集每个连通分支至少一个点的精细位复杂度。2025年。[25] J. Elliott、M. Giesbrecht 和 ´E. Schost。计算光滑实代数集每个连通分支中一个点的位复杂度。《符号计算杂志》，116:72–97，2023年。[26] G. Gatellier、A. Labrouzy、B. Mourrain 和 J. P. T´ecourt。三维代数曲线的拓扑计算。载于《代数样条曲面的计算方法》（COMPASS）。ESF探索研讨会，奥地利凯弗马克特，2003年9月29日–10月3日，第27–43页。施普林格，2005年。[27] M. Giusti、G. Lecerf 和 B. Salvy。一种不使用 Gröbner 基的多项式系统求解替代方法。《复杂性杂志》，17(1):154–211，2001年。[28] L. Gonzalez-Vega 和 I. Necula。隐式定义的代数平面曲线的高效拓扑判定。《计算机辅助几何设计》，19(9):719–743，2002年。

[29] J. Heintz、M.-F. Roy 和 P. Solern´o。关于在单指数时间内描述半代数集的连通分支。《离散与计算几何》，11(2):121–140，1994年。[30] H. Hong。分析平面实代数曲线拓扑的一种高效方法。《数学与计算机模拟》，42(4-6):571–582，1996年。[31] Md. N. Islam、A. Poteaux 和 R. Pr´ebet。实代数曲线连通性查询算法。2023年国际符号与代数计算研讨会论文集，2023年。[32] K. Jin 和 J. Cheng。实代数空间曲线的同位网格划分。《系统科学与复杂性杂志》，33(4):1275–1296，2020年。[33] A. Kobel 和 M. Sagraloff。关于平面代数曲线计算的复杂度。《复杂性杂志》，31(2):206–236，2015年。[34] Y. Liu、A. Bauer 和 J.-P. Viard T., Rolland。立方体卫星格式的自由曲面高光谱成像仪设计。《光学快报》，29(22)，2021年。[35] K. Mahler。关于多变量多项式的一些不等式。《伦敦数学学会杂志》，37:341–344，1962年。[36] S. Mc Callum 和 G. Collins。柱面代数分解的局部盒邻接算法。符号计算杂志，33(3):321–342，2002年。[37] K. Mehlhorn、M. Sagraloff 和 P. Wang。从近似因式分解到根隔离，并应用于柱面代数分解。符号计算杂志，66:34–69，2013年。[38] S. Melczer 和 B. Salvy。通过用于多项式系统的半数值算法，有效求取多元有理函数的系数渐近。符号计算杂志，103:234–279，2021年。[39] M. Safey El Din 和 ´E. Schost。极曲簇与在光滑实代数集的每个连通分支中计算一个点。载于：2003年国际符号与代数计算研讨会论文集，ISSAC ’03，第224–231页，美国，2003年。ACM。[40] M. Safey El Din 和 ´E. Schost。一种近乎最优的算法，用于判定光滑有界实代数集中的连通性查询。《ACM会刊》，63(6)，2017年1月。[41] M. Safey El Din 和 ´E. Schost。多齐次多项式系统求解的位复杂度——及其在多项式最小化中的应用。符号计算杂志，87:176–206，2018年。[42] ´E. Schost。关于含参数多项式系统的求解。博士论文，2000年。2000EPXX0056。[43] R. Seidel 和 N. Wolpert。关于实代数曲线拓扑的精确计算。载于：第21届年度计算几何研讨会论文集，SCG 2005，意大利比萨，2005年6月6–8日，第107–115页。ACM，2005年。[44] A. Strzebo´nski。使用验证数值计算进行柱面代数分解邻接计算。载于：2017年ACM国际符号与代数计算研讨会论文集，ISSAC ’17，第413–420页，美国，2017年。ACM。

A 子程序

算法 4 SignSamples

要求： $f \in \mathbb{Q}[x_1, x_2]$ 和多项式 $w_1, \ldots, w_{d_2} \in \mathbb{Q}[x_1]$。

确保： 对于每个 $k \in \{1, \ldots, d\}$，一个有限集 $\mathcal{Q}_k \subset \mathcal{C}_{\mathbb{R}}$ 以及一个符号映射 $s_k : \mathcal{Q}_k \to \{-1, 0, +1\}$。

1: $w_1' \leftarrow \mathrm{d}w_1/\mathrm{d}x_1$
2: 计算 $B > 0$，以界定 w_1、……、w_{d_2} 的实根。
3: 选择 $\theta_1, \theta_2 \in \mathbb{Q}$，使得 $\theta_1 < -B$ 且 $\theta_2 > B$
4: $(\mathcal{Q}_1, s_1) \leftarrow \text{AssignSigns}(1, w_1')$
5: 对于每个 $k \in \{2, \ldots, d_2\}$，执行
6: $\quad P_k' \leftarrow \mathrm{d}(w_1 w_k)/\mathrm{d}x_1$
7: $\quad (\mathcal{Q}_k, s_k) \leftarrow \text{AssignSigns}(k, P_k'(x-\theta_1)(x-\theta_2))$
8: 结束循环
9: 返回 $\left(\{\mathcal{Q}_k\}_{k=1}^{d_2}, \{s_k\}_{k=1}^{d_2}\right)$

算法 5 PreCond

要求： $f \in \mathbb{Q}[x_1, x_2]$

确保： $(f_1, \ldots, f_r) \subset \mathbb{Q}[x_1, x_2]$ 使得 $f = f_1 \cdots f_r$，且对所有 $1 \le i \le r$，f_i 均满足 $\mathcal{S}$。

1: 对于 $k = 1, \ldots, d_2 - 1$ 执行
2: $\quad g \leftarrow$ 最大公因式 $(f, \partial^k f/\partial x_2^k)$
3: $\quad$ 若 $\deg(g) > 0$ 则
4: $\quad\quad$ 返回 $\text{PreCond}(g) \cup \text{Precond}(f/g)$
5: $\quad$ 结束条件判断
6: 结束循环
7: 返回 f

算法 6 PartialComponents

要求： $\mathfrak{R} = (w, \rho_2, \ldots, \rho_n)$以及 $\mathfrak{P}$ 一个一维和零维参数化。

确保： 在 $\mathcal{C}_{\mathbb{R}}$ 中、除 $\mathrm{app}(\mathcal{C}_2)$ 外，对其连通分支的部分描述。

1: $q_{\mathrm{app}} \leftarrow \text{ApparentSingularities}(\mathfrak{R})$
2: $[\mathcal{H}_w, V_{\mathrm{app}}, V_{\mathcal{P}}] \leftarrow \text{GenPlanarComponents}(w, \mathcal{P}_2, q_{\mathrm{app}})$
3: 返回 $\mathcal{H}_w' \leftarrow \text{SANodeResolution}(\mathcal{H}_w, V_{\mathrm{app}})$

B 引理 3.4 的次数、高度和复杂度

这里给出证明引理 3.4 中次数界和高度界的技术细节。我们研究的多项式方程组为 $\boldsymbol{g} = 0$, $z\Delta - 1 = 0, \boldsymbol{\lambda} J(\boldsymbol{g}) = \boldsymbol{m}$，其中包含 $\mathbb{Q}[\boldsymbol{x}, z, \boldsymbol{\lambda}]$ 以及 $\boldsymbol{x} = (x_1, \ldots, x_n)$ 和 $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_n)$。关于 $\boldsymbol{x}, z, \boldsymbol{\lambda}$, $\boldsymbol{g}$ 中的 n 多项式的三重次数上界为 $(d, 0, 0)$，下一个多项式的三重次数上界为 $(n(d-1), 1, 0)$。来自 $\boldsymbol{\lambda} J(\boldsymbol{g}) = \boldsymbol{m}$ 的前 n 个方程的三重次数上界为 $(n(d-1), 1, 1)$，而最后一个方程的三重次数上界为 $(n(d-1), 0, 1)$。请注意，这些多项式系数的比特大小上界为 $b \in \tilde{O}(h + n(n + \log(\frac{1}{\epsilon})))$。令 $\tau \in \tilde{O}(h + n(n + \log(\frac{1}{\epsilon})) + d)$。

为了估算由该方程组定义的代数集的次数和高度，我们按照[41,第 2] 节的做法，并考虑：

$$P_1 = (\tau\zeta + d\vartheta_1)^{n-1}, \quad P_2 = (\tau\zeta + n(d-1)\vartheta_1 + \vartheta_2 + \vartheta_3)^n$$
$$P_3 = (\tau\zeta + n(d-1)\vartheta_1 + \vartheta_2), \quad P_4 = (\tau\zeta + n(d-1)\vartheta_1 + \vartheta_3)$$

以及 $\mathbf{P} = P_1P_2P_3P_4$ 模 $\langle \zeta^2, \vartheta_1^{n+1}, \vartheta_2^2, \theta_3^{n+1}\rangle \in \mathbb{Z}[\zeta, \vartheta_1, \vartheta_2, \vartheta_3]$。

根据 [41, 命题 3], , V的次数有界于 $\mathbf{P}(0, \vartheta_1, \vartheta_2, \vartheta_3)$ 的系数之和。注意， $P_1P_2P_3P_4$是 $2n+1$次齐次的。唯一一个不属于 $\mathfrak{m} = \langle \vartheta_1^{n+1}$、 ϑ_2^2、 $\theta_3^{n+1}\rangle$ 的 $2n+1$ 次单项式是 $\vartheta_1^n\vartheta_2\vartheta_3^n$。我们由此推出，$\mathbf{P}(0, \vartheta_1, \vartheta_2, \vartheta_3) = C\vartheta_1^n\vartheta_2\vartheta_3^n$，其中 C 待确定。

有 $P_1(0, \vartheta_1, \vartheta_2, \vartheta_3) = d^{n-1}\vartheta_1^{n-1}$。 $P_2(0, \vartheta_1, \vartheta_2, \vartheta_3)$ 的贡献项具有如下形式：$\binom{n}{a_2\ b_2,,c_2}(n(d-1))^{a_2}\vartheta_1^{a_2}\vartheta_2^{b_2}\vartheta_3^{c_2}$，其中 $0 \le a_2 \le 1$、 $0 \le b_2 \le 1$ 和 $0 \le c_2 \le n$，且$a_2 + b_2 + c_2 = n$。

考虑到 P_3 和 P_4，我们推得 $\mathbf{P}(0, \vartheta_1, \vartheta_2, \vartheta_3)$ 等于

$$
\begin{aligned}
&d^{n-1}\sum \binom{n}{a_2, b_2, c_2}(n(d-1))^{a_2+2}\vartheta_1^{a_2+n+1}\vartheta_2^{b_2}\vartheta_3^{c_2} + \\
&d^{n-1}\sum \binom{n}{a_2, b_2, c_2}(n(d-1))^{a_2+1}\vartheta_1^{a_2+n}\vartheta_2^{b_2}\vartheta_3^{c_2+1} + \\
&d^{n-1}\sum \binom{n}{a_2, b_2, c_2}(n(d-1))^{a_2+1}\vartheta_1^{a_2+n}\vartheta_2^{b_2+1}\vartheta_3^{c_2} + \\
&d^{n-1}\sum \binom{n}{a_2, b_2, c_2}(n(d-1))^{a_2}\vartheta_1^{a_2+n-1}\vartheta_2^{b_2+1}\vartheta_3^{c_2+1}
\end{aligned}
$$

模 $\mathfrak{m}$，同样有 $0 \le a_2 \le 1, 0 \le b_2 \le 1$ 和 $0 \le c_2 \le n$ 以及 $a_2 + b_2 + c_2 = n$。第一个和为 0。在第二个和中，必有 $a_2 = 0, b_2 = 1$ 和 $c_2 = n-1$。在第三个和中，有 $a_2 = 0, b_2 = 0$ 和 $c_2 = n$。在第四个和中，必有 $a_2 = 1, b_2 = 0$和 $c_2 = n-1$。因此，总而言之，我们有

$$
\begin{aligned}
C =& d^{n-1}n(d-1)\left(\binom{n}{0,1,n-1} + \binom{n}{0,0,n} + \binom{n}{1,0,n-1}\right) \\
=& d^{n-1}n(d-1)(2n+1) \in O(n^2d^n).
\end{aligned}
$$

为了求得高度，我们计算 $\mathbf{P}$ [41, Prop. 4] 的系数之和。由于 $P_1P_2P_3P_4$是次数为 $2n+1$的齐次多项式，对此和有贡献的项，其对应的单项式为以下之一： $\vartheta_1^n\vartheta_2\vartheta_3^n, \zeta\vartheta_1^{n-1}\vartheta_2\vartheta_3^n, \zeta\vartheta_1^n\vartheta_3^n, \zeta\vartheta_1^n\vartheta_2\vartheta_3^{n-1}$。

注意，P_1模 $\mathfrak{m} = d^{n-1}\vartheta_1^{n-1} + \tau(n-1)d^{n-2}\zeta\vartheta_1^{n-2}$。我们还有 P_2模 $\mathfrak{m} = \sum \tau^{e_2}(n(d-1))^{a_2}\binom{n}{e_2\ a_2,\ ,\ b_2,\ c_2}\zeta^{e_2}\vartheta_1^{a_2}\vartheta_2^{b_2}\vartheta_3^{c_2}$，其中 $0 \le e_2 \le 1, 0 \le a_2 \le 2, 0 \le b_2 \le 1, 0 \le c_2 \le n$和 $e_2 + a_2 + b_2 + c_2 = n$。此外，由于 P_3P_4关于 ϑ_3的次数至多为一，且 $\mathbf{P}$ 中所有单项式的次数均为 $2n+1$，我们可得 $n-1 \le c_2 \le n$。其中满足 $e_2 = 0$的项的系数有界于 $n^4d^{a_2}$。其中满足 $e_2 = 1$的项的系数有界于 $\tau n^4d^{a_2}$。由此可得，$\mathbf{P}$ 的系数和有界于以下各项的系数和

$$
\begin{aligned}
&n^4d^{n-1}\left(d\vartheta_1^{n-1} + \tau n\zeta\vartheta_1^{n-2}\right) \\
&\left(\sum\left(\tau d^{a_2}\zeta\vartheta_1^{a_2}\vartheta_2^{b_2}\vartheta_3^{c_2} + d^{a_2'}\vartheta_1^{a_2'}\vartheta_2^{b_2'}\vartheta_3^{c_2'}\right)\right)P_3P_4 \mod \mathfrak{m}
\end{aligned}
$$

其中 $a_2 + b_2 + c_2 = n-1, 0 \le a_2 \le 2, 0 \le b_2 \le 1, n-1 \le c_2 \le n$ 和 $a_2' + b_2' + c_2' = n-1, 0 \le a_2' \le 2, 0 \le b_2' \le 1, n-1 \le c_2' \le n$。为了给上述多项式的系数之和设定上界，我们可以分别用 $(\zeta + nd\vartheta_1 + \vartheta_2)$和 $(\zeta + nd\vartheta_1 + \vartheta_3)$替换 P_3和 P_4。接着，我们通过拆分来自求和式 $d\vartheta_1^{n-1} + \tau n\zeta\vartheta_1^{n-2}$的贡献，分析所得多项式的系数。首先考虑项 $d\vartheta_1^{n-1}$。在这种情况下，必有 $a_2 \le 1$ 和 $a_2' \le 1$。此外，来自 P_3 或 P_4 的项 $nd\vartheta_1$ 与之相乘后，模 $\mathfrak{m}$ 不为零，当且仅当 $a_2 = 0$ 或 $a_2' = 0$成立。因此，这部分贡献产生的所有系数均有上界 τn^5d^{n+1}。对由项 $\tau n\zeta\vartheta_1^{n-2}$得到的多项式进行类似推理，可知第二个多项式的所有系数均有上界 τn^6d^n。最后，由于关于 $a_2, b_2, c_2, a_2', b_2', c_2'$的约束意味着 $\sum(\zeta\vartheta_1^{a_2}\vartheta_2^{b_2}\vartheta_3^{c_2} + \vartheta_1^{a_2'}\vartheta_2^{b_2'}\vartheta_3^{c_2'})$ 中的项数至多为 24，我们得出 P 的系数之和属于 $O\left(n^5d^{n+1} + \tau n^6d^n\right) \subset O\tilde{}(n^6d^{n+1} + n^8d^n(h + \log\left(\frac{1}{\epsilon}\right))$。最后，我们应用 [41, 定理 1]（沿用其中的记号），其中

$$
L \in O\left(n^2 + n\binom{n+d}{n}\right), \quad b \in \tilde{O}\left(h + n\left(n + \log(\frac{1}{\epsilon})\right)\right)
$$

$$\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d}) \in O\left(n^2 d^n\right), \quad \mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d}) \in \tilde{O}\left(n^6 d^{n+1} + n^8 d^n (h + \log\left(\frac{1}{\epsilon}\right)\right)$$
$$N = n+1, \quad \mathfrak{d} \leq nd, \quad \boldsymbol{\eta} = (\tau, \ldots, \tau) \text{ and } s \leq \tau.$$

由于对于 $d \geq 2$，有 $\binom{n+d}{n} \geq n^2$，因此我们有 $L \in O\left(n\binom{n+d}{n}\right)$。由此可得 $Lb \in n^2 h + n^3(n + \log(\frac{1}{\epsilon}))$，且 $\mathscr{C}_{\boldsymbol{n}}(\boldsymbol{d})\mathscr{H}_{\boldsymbol{n}}(\boldsymbol{\eta}, \boldsymbol{d})$属于 $O\left(n^7 d^{2n+1} + \tau n^8 d^{2n}\right) \subset O\tilde{}($ $n^{10} d^{2n+1}\left(h + \log(\frac{1}{\epsilon})\right)$)。综上，所需的位运算次数为

$$\tilde{O}\left(n^{14} d^{2n+2} (h + \log(\frac{1}{\epsilon}))\binom{n+d}{n}\right).$$