arXiv:2603.17288v1 [math.AG] 18 Mar 2026

通过同伦图认证伽罗瓦/单值化作用

TIMOTHY DUFF 和 KISUN LEE

Abstract. 我们开发了一种经认证的数值算法，用于计算参数化多项式系统的伽罗瓦/单值化群。我们的方法采用经认证的同伦路径跟踪，以保证算法所产生的单值化作用的正确性，并建立在以往的“同伦图”框架之上。我们通过该算法的一个实现开展了广泛的实验，并利用它认证了若干重要伽罗瓦/单值化群的性质；这些群源自纯数学与应用数学中的多个实例。

1. Introduction

Many 问题自然地建模为参数化代数方程组 s,

$$F(x;z)=0, \tag{1}$$

其性质是：对于一般参数 z，该系统 F 具有固定且有限数量的复值孤立解 x。确定此类问题的结构以及求解它们的难度，是应用与计算代数几何中的核心主题。

与其他数学领域的情况一样，“难度”和“结构”这类词的含义往往事后才最为清晰。在我们的设定中，解的数量或许是衡量问题难度最简单的指标。不过，更精细的衡量指标则由问题的单值化群（也称为几何伽罗瓦群）刻画。在我们的设定中，“单值”沿用其传统含义：当参数 z 沿参数空间中的一条回路移动并避开分歧轨迹时，解会连续变化，最终发生置换。

已有大量工作将数值方法用于计算单值群——例如参见 [4, 8, 10, 11, 13, 16, 21, 29, 33]。这些工作中提出的许多方法有两个共同特点：（1）尽管可能会用到数值启发式方法，最终结果仍可得到严格的认证；（2）在求解问题（1）时，计算单值化群也同时进行，只需很少额外开销。本文提出一种经过认证的伽罗瓦/单值化群计算方法，将这两个特点融为一体。不同于以算法方式确定完整伽罗瓦/单值化群的先前工作，我们更倾向于采用实验性方法，同时仍能严格认证伽罗瓦群某个子群的作用（定义3.3）。即使只能恢复群的部分信息，我们也能据此对某些群不变量作出严格论断，例如伽罗瓦宽度： [8]。

我们的方法建立在先前利用同伦解路径跟踪计算伽罗瓦／单值化群的研究之上。尽管浮点跟踪速度快且灵活，但可能导致路径跳跃，即切换到另一条解路径，从而产生错误的对应关系，进而得到错误的群。在此背景下，对解 F 事后（例如 [5, 6, 22, 25–27]）的数值近似进行认证是不够的。我们必须确保跟踪过程始终沿着单条解路径进行。本文改进了基于区间算术 [12, 17, 18, 24, 30, 38, 39], 的认证路径跟踪方法；这些方法构造一个覆盖解路径的区域，从而保证跟踪过程沿着单条解路径进行而不会发生跳跃。

为了计算单值化置换并恢复单值化群，我们重新审视了 [9], 提出的基于图的框架：该框架将同伦路径组合起来，形成嵌入参数空间中的同伦（多重）图。每个顶点都是参数空间中的一个一般点，两个顶点之间的每条边都对应一条连接它们的路径。通过沿这些

边进行认证式跟踪，我们可以严格地获得单值化置换。相较于 [9] 首次提出的框架，改进之处包括：(1) 经认证的路径跟踪，使定义3.3和定义3.6等情形下的伽罗瓦群计算更加严格；(2) 使用生成树来组织单值子群的生成元；(3) 采用饱和策略，确保对环路进行全面探索。

本文组织如下。第 2 节介绍区间算术、Krawczyk 方法和单值化群的背景，并回顾经认证的路径跟踪的基本算法。第 3 节详细介绍基于图的框架：构造参数同伦、认证边对应关系，以及从（饱和）图生成单值化置换。最后，第 4 节展示实验结果，使用我们的 Julia 实现，将该方法应用于从计算机视觉到代数几何的各类测试用例，以及一些单变量基准测试。

2. Background

2.1. **区间算术与 Krawczyk 方法**。区间算术将标准算术扩展到区间上，从而执行保守且可靠的计算。对于算子 $\odot$ 和区间 I, J，我们定义 $I \odot J := \{x \odot y \mid x \in I,\ y \in J\}$。关于显式公式以及浮点数相关问题的讨论（我们大多忽略这些问题），请参阅标准教材 [31]。

我们在 $\mathbb{C}$上工作，对实部和虚部分别应用实区间算术，例如 $I := \Re(I) + i\Im(I)$。对于区间向量 $I = (I_1, \ldots, I_n) \subset \mathbb{C}^n$，我们定义范数

$$\|I\| := \max_{1 \leqslant i \leqslant n} \max\{|\Re(I_i)|,\ |\Im(I_i)|\}$$

其中 $|J| = \max_{a \in J} |a|$ 表示区间 J的幅度。这对应于 ∞-范数在 $\mathbb{C}^n$上的情形。

给定区间向量 $I \subset \mathbb{C}^n$ 以及函数 $f : \mathbb{C}^n \to \mathbb{C}$，函数 在 f 上的 I 区间包络是满足 $\square f(I) \supset \{f(x) \mid x \in I\}$的区间。实际应用中，这类包络并不唯一，因为它们取决于计算 f时采用的策略，而且可能过于保守。

设 $F : \mathbb{C}^n \to \mathbb{C}^n$ 是由多项式或有理函数构成的方形方程组，并设 $x \in \mathbb{C}^n$。对于$r > 0$ 和可逆矩阵 A，*Krawczyk* 算子为

$$K(F, x, r, A) := -AF(x) + (Id - A \square JF(x + rB))rB$$

其中 $B = ([-1,\ 1] + i[-1,\ 1])^n$。我们回顾 Krawczyk 检验的一种定量变体 [25]。

定理2.1。 [18, 定理 2.1] 若 $K(F,\ x,\ r,\ A) \subset r\rho B$ 对某个 $\rho < 1$ 成立，则系统 $F(x) = 0$ 在盒 $x + rB$ 中有唯一解 x^*，且 $\|x - x^*\| \leqslant r\rho$。此外，拟牛顿映射$x \mapsto x - AF(x)$ 在 $x + rB$ 上是 ρ-Lipschitz 的。

当定义 2.1 的假设成立时，我们称 x为一个 ρ-近似解，其认证半径为 r。在实践中，可以通过选择 $A \approx JF(x)^{-1}$ 来应用定义 2.1，而包含关系$K(F,\ x,\ r,\ A) \subset r\rho B$可通过计算适当的区间包络 $\square F$，$\square JF$ 来检验。

与定义 2.1 密切相关的是算法 *1* 中的 *Krawczyk* 检验。该检验在数学上等价于将半径 r归一化后检查定义 2.1 中的包含关系，并贯穿于我们的经认证的预测-校正框架。

至关重要的是，用于在 Krawczyk 检验中计算 F 的常数本身也可以是区间。在这种情况下，检验结果为“true”就证明：对于这些区间内任意取值，$x + rB$ 中都存在唯一根。

2.2. **多项式系统的伽罗瓦/单值化群**。 参数多项式系统通常具有这样的性质：对于参数 $z \in \mathbb{C}^m$ 的一般取值，存在有限个 $d > 0$ 复解 $x \in \mathbb{C}^n$。因此，这些解在局部可表示为代数函数$x_1(z), \ldots, x_d(z)$，它们通过一个由“问题-解对”构成的关联簇隐式定义，

$$X = \{(z, x) \in \mathbb{C}^m \times \mathbb{C}^n \mid \tilde{F}(x; z) = 0\}, \tag{2}$$

算法 1 Krawczyk 检验

输入： • 一个方形方程组 $F = \{f_1, \ldots, f_n\}$，可能包含区间常数
• 一个点 $x \in \mathbf{C}^n$，或更一般地，一个区间 $x \subset \mathbf{C}^n$，
• 一个半径 $r > 0$，
• 一个可逆矩阵 $A \in \mathbf{C}^{n\times n}$，以及
• 一个参数 $\rho \in (0,\ 1)$。
输出： 一个布尔值，表示 x 是否能证明 $x + rB$ 中存在唯一根。1: 计算 $K := -\frac{1}{r}AF(x) + (I_n - A \square JF(x + rB))\, B$。2: **返回** $\|K\| < \rho$。

˜其中 $F(x;\ z)$ 是一个定义 X 的多项式方程组（不一定是方阵）。簇 X 配备了一个投影 $\pi : X \to \mathbb{C}^m$，其一般为 d 对一。通常，我们还可以假设 X 是不可约的，此时称 X 其为解簇。整数 d 通常称为一般根数或次数，表示求解 F. 对于一般的问题实例 z，纤维 $\pi^{-1}(z)$恰好由 d 个孤立点组成。

当 z 沿着$\mathbb{C}^m$ 中避开 π的分支轨迹移动时， d 解会进行解析延拓并发生置换。假设 X 是不可约的，这些置换构成传递子群 $\mathrm{Mon}_\pi \hookrightarrow S_d$，称为该问题的单值化群。该群在 S_d中在共轭意义下是良定义的。按照惯例，我们省略其对一般点 z_0的依赖。

注记 2.2。 对于某些问题，簇 X 可能是可约的，甚至可能具有多个分支 X_1，.....， X_k，使得限制 π_k： $X_k \to \mathbf{C}^m$ 是占优的。我们在第 4.3 节讨论了这样一个例子，其中讨论了对称三次曲面上的 27 条直线。在这种情况下，单值化群作为 $\mathrm{Mon}_{\pi_1} \times \cdots \times \mathrm{Mon}_{\pi_k}$ 的子群是不传递的。

假设 X 不可约，Mon_π 与分歧覆盖的伽罗瓦群重合π。如果 K 是有理函数域$\mathbb{C}(X)$ 在函数域 $L = \mathbb{C}(\mathbb{C}^m)$上的正规闭包，那么 Mon_π 作为一个抽象群，同构于域有限扩张的伽罗瓦群K/L [35, 第 1]节。不过，这里我们主要关注 Mon_π 作为一个置换群在 $\pi^{-1}(z)$.上作用。

了解单值化群可以提供解集的结构信息，例如传递性、可分解性或是否存在非平凡对称性。沿环路对解进行数值跟踪，可以直接得到纤维上的置换。第 3 节将构建一个框架，利用参数同伦和区间算术计算这些置换。

2.3. 经认证的路径跟踪。同伦路径跟踪，也称为数值延拓，是求解非线性方程组的一种标准数值方法。这类方法构造一个起始系统 $G : \mathbf{C}^n \to \mathbf{C}^n$，其解已知，并构造一个同伦函数 $H(x;\ t) : \mathbf{C}^n \times [0, 1] \to \mathbf{C}^n$，使得 $H(x; 0) = G(x)$。理想情况下， G的任意孤立非奇异解都可延拓为解析解路径 $x(t) : [0, 1] \to \mathbf{C}^n$，且对所有 $t \in [0, 1]$. 都有 $H(x(t); t) = 0$

实际上，从 $t = 0$ 到 $t = 1$ 跟踪一个解路径，采用的是数值预测—校正方法 [34, 第 2 章3]。从 $t_0 = 0$ 和一个近似值 $x_0 \approx x(0)$出发，此类方法接下来会确定某个点 $t_1 \in (t_0,\ 1]$ 以及相应的近似值 $x_1 \approx x(t_1)$。重复这一过程，可以获得一系列离散时间步 $0 = t_0 < t_1 < \cdots < t_k = 1$以及局部解路径的相应近似值 x_0，x_1，..... $x_k \in \mathbf{C}^n$。

经认证的同伦路径跟踪算法通过将路径包含在 $x(t)$ 一个紧区域内，严格保证正确性，其中 $H(x;\ t^*) = 0$ 对于所有 $t^* \in [0,\ 1]$均具有唯一解。该区域通过计算离散时间步 $0 = t_0 < t_1 < \cdots < t_k = 1$ 以及包含解路径的区间盒 I_i 来构造，并且在每个子区间 $x(t)$ 上唯一地包含该解路径 $[t_{i-1},\ t_i]$。

从实际角度来看，经认证的同伦路径跟踪面临的主要挑战是，其相关步长 $t_i - t_{i-1}$ 通常远小于非经认证方法所采用的步长

。这一挑战促使人们在经认证的跟踪方面开展了大量研究，主要集中于两类方法。一类方法 [1, 2, 20] 依赖于 Smale 的 α-理论 [3,第 8], 章，另一类方法 [12, 17, 18, 24, 30, 38, 39] 则使用区间算术来验证近似解，并构造路径的认证包围。

本文紧密沿用了 [18], 的基于区间的方法；该方法在实证中显示，相较于以往经认证的路径跟踪器，有了显著改进。该方法包含三个主要要素：

(1) 预测： 任何认证路径跟踪算法的核心思想，都是构造一系列区间盒 $I_1, \ldots, I_k$，这些区间盒从路径 $x(t)$ 上的某一点（或其附近）出发，并唯一覆盖路径的一部分。为构造这样的区间盒，我们使用数值近似 $x \approx x(t)$。如果 Krawczyk 检验（算法 1）对包含 x的适当区域通过，我们便继续进行下一步跟踪。

给定一条解路径 $x(t)$ 以及某个 $t^* \in (0,1)$处的近似值 $x \approx x(t^*)$，预测器只是一个映射 $X(\eta) : [t^*, \infty) \to \mathbb{C}^n$，其中 $X(t^*) = x$，其构造目的是在 t^*.附近对 t 的 $x(t)$进行近似。最简单的选择或许是 0 阶常数预测器；$X(\eta) = x$ 对所有 $\eta \geqslant t^*$. 均成立。另一类更有效的高阶预测器，用于 [18, 第 6 节3] 和 [38], 中的认证同伦跟踪，其基础是泰勒模型的概念 [31,第 9 节3], ，泰勒模型可用于构造一个弯曲的区间盒，其中包含 $x(t)$的高阶近似；例如，下文公式 (6) 中定义的 Hermite 预测器。

(2) 细化： 算法 2 对细化过程进行了形式化，该过程尝试通过将某个系统 F 的 τ 近似解替换为满足 $\rho \ll \tau$. 的 ρ 近似解，从而改进x。这使得后续预测步骤可以选择更大的步长。

算法 2 精化（参见 [18, 算法 2]）

输入：
- 一个由多项式或有理函数构成的方形方程组 $F = \{f_1, \ldots, f_n\}$,
- 一个 τ近似解 $x \in \mathbb{C}^n$，其认证半径为 r（因此 $\tau, r \in (0,1)$），
- 一个 $n \times n$ 可逆矩阵 A,
- 一个收缩因子 $g \in (0, 1-\tau)$, 以及
- 一个目标常数 $\rho \in (0,\ 1)$（算法 1 中使用的参数；通常为 $\rho < \tau$）。

输出： 一个 ρ-近似解 x、一个认证半径 $\tilde{r}$和一个可逆矩阵 $\tilde{A} \in \mathbb{C}^{n \times n}$。

1: 设置 $\tilde{r} = r$
2: 设置 $\tilde{A} = A$
3: **当** Krawczyk 检验$(F,\ x,\ \tilde{r},\ \tilde{A},\ \rho) = false$**执行**
4: **如果** $\|AF(x)\| \leqslant g\rho\tilde{r}$**，则**
5: 设置 $\tilde{r} = \frac{1}{2}\tilde{r}$
6: **else**
7: 设置 $x = x - AF(x)$
8: **结束如果**
9: Set $\tilde{A} = JF(x)^{-1}$
10: **结束循环**
11: **当** $2\tilde{r} \leqslant 1$并且执行 Krawczyk 检验$(F$时，$x,\ 2\tilde{r},\tilde{A},\ \rho) = true$ **执行**
12: 设定 $\tilde{r} = 2\tilde{r}$。
13: **结束循环**
14: 返回 $x\ \ , \tilde{r}, \tilde{A}$.

算法 2 中的第一个 while 循环（从第 3 行开始）在每次迭代时都会缩小半径，因此可能导致区域变窄。当区间过窄时，解路径更可能漂移到盒外，使得可靠跟踪变得困难。第二个 while 循环（第 11 行）试图缓解这一影响：它利用第一个循环得到的改进估计，为 Krawczyk 检验认证一个更大的半径。

算法 2 大致等同于 [18,算法 2], ，其中选择了参数 g, ρ 和 τ 的特定取值，以兼顾良好的实际性能与自适应精度模型下关于终止的理论分析 [18, 第 4 节2]。

(3) 跟踪： 对于同伦 $H(x;t)$ ， 0)完整认证的路径跟踪算法会从起始系统 $H(x;0)$的认证近似解 x 出发，在上述预测器步骤与精化步骤之间交替执行。算法 3 对此作了概述。

算法 3 CertifiedTrack

输入： • 一个同伦 $H(x;t) : \mathbb{C}^n \times [0,1] \to \mathbb{C}^n$ ， 以及一条正则解路径 $x(t)$,
• 常数 $\rho \in (0, \frac{1}{2}]$ 和 $\tau \in (\frac{1}{2}, 1)$, –
• 一个 ρ-近似解 $x \in \mathbb{C}^n$ ， 对应于 $H(x;0)$,
• 一个预测器 $X(\eta)$ （可能带有其他参数），
• 一个常数 $0 < h < 1$,
• 一个常数 $0 < r < 1$, and
• 常数 $\delta_{inc} > 1$ and $0 < \delta_{dec} < 1$。
输出： ρ-近似解 x of $H(x;1)$。

1: 设置 $t = 0$, 2: 设置 $A = \partial_x H(x;t)^{-1}$。 3: 当 $t < 1$ 时执行 4: 设置 $(x, r, A) =$ 精化$(H(x;t), x, r, A, \rho)$。 ▷算法 2 5: 设置 $h = \delta_{inc} h$。 6: 当 Krawczyk 检验$(H(x;\ [t, t+h]), X([t, t+h]), r, A, \tau) = false$时执行 7: $h = \delta_{dec} h$。 8: 结束循环 9: 设置 $t = \min(t+h, 1)$。 10: 结束循环 11: 设置 $(x, r, A) =$ 精化$(H(x;\ 1), x, r, A, \rho)$。 12: 返回 x。

在外层 while 循环 (3) 中，我们精化先前的近似解 x，以获得同伦 $H(x$ 在时刻 t 的 ρ-近似解； $t)$ 内层 while 循环（算法 3）通过应用 Krawczyk 检验（算法 1）来确定合适的时间步长 h ，使得 x 在时刻 $t + h.$ 仍是该同伦的近似解

算法 3 深受 [18, 算法 4], 的启发，该算法对预测器 X 以及步长增减因子 δ_{inc}, δ_{dec}. 作出了特定选择。从理论上讲，假设起始解可延拓为一条光滑解路径，且所有算术运算均为精确运算，那么该算法将产生目标系统 $H(x$的一个近似解； $1) = 0$实际上，当然必须考虑定精度浮点运算中的误差。 [18,第 6 节3], 对该算法的一个版本在采用自适应精度进行非精确运算时的终止性进行了仔细的理论分析。

另一方面，即便使用非精确的固定精度算术，只要算法 3 确实终止，并且区间算术的实现满足某些性质（例如对端点进行保守的向外舍入），我们就能确信算法 3 认证了一条解路径。特别是，假设跟踪过程终止，输出的 x 将是目标系统 $H(x;1) = 0$ 的一个经认证的近似解。在我们的实验中，我们始终使用固定精度，并将精度设得足够高，以确保所有跟踪的路径都能终止。

3. Certified monodromy computation with homotopy graphs

本节将详细介绍如何利用参数同伦计算单值化作用，并以完全经过认证的方式获得最终的单值化置换。

3.1. **参数同伦与边对应关系。** 通常，单值化启发式必须首先调用某种构造过程，以生成一个（足够一般的）问题－解对 $(z_0,\ x_0) \in X \subset \mathbb{C}^m \times \mathbb{C}^n$（或者更一般地，为 X 中支配参数空间的每个连通分支 $\mathbb{C}^m$各生成一个这样的解对）。尽管具体采用的构造策略通常取决于问题本身，但我们假设除了 X 之外，输入中还给定了这样一种策略。这个假设或许看起来有所限制，但对于科学和工程领域的许多问题而言，它相当自然：对于给定的 x，求解方程（1）是关于更易处理的逆问题而言的正问题，即从 z 构造出 x.

我们进一步要求一个方程组 $F = \{f_1(x;\ z),\ \ldots\ldots,\ f_n(x;\ z)\}$，该方程组在 $(z_0,\ x_0)$附近局部定义 X。更准确地说，方程组 F 可以由多项式或有理函数组成，并且我们要求关于解变量的雅可比矩阵，

$$\partial_x F(x_0; z_0) = \left(\frac{\partial f_i}{\partial x_j}\right)_{i,j=1}^{n} \Bigg|_{(z_0,x_0)},$$

对于任意一般样本 $(z_0,\ x_0) \in X$都具有满秩 n。根据隐函数定理，这确保了解变量在 $(z_0,\ x_0)$附近可以局部表示为光滑函数 $x = g(z)$。

给定一个构造的问题－解对 $(z_0、\ x_0) \in X$，我们在参数空间上生成一个同伦图（定义如下）。为创建同伦图中的顶点，我们为 $i = 1、\ldots\ldots、\ \ell$生成 ℓ个新的一般问题实例 $z_i \in \mathbb{C}^m$。为构造同伦图的边，我们考虑问题实例对 $(z_i、\ z_j)$ 之间的路径 $i、\ j = 0、\ldots\ldots、\ \ell$。每条路径 $p(t)$ 定义为线段 $p(t) :\ = (1-t)z_i + tz_j$。我们假设对于所有 $t \in [0、\ 1]$，纤维 $\pi^{-1}(p(t))$由 d 个互异的孤立解组成。对于每条这样的路径 $p(t)$，我们定义相应的参数同伦 $H(x;\ t) :\ = \{f_1(x;\ p(t))、\ldots\ldots、\ f_n(x;\ p(t))\}$。每条边 $e = (z_i、\ z_j) \in E$都配备其相应的参数同伦。由所选路径 $p(t)$ 给出的顶点 $V = \{z_0、\ldots\ldots、\ z_\ell\}$和边 E的集合构成一个完全图，并记为 $\mathcal{G} = (V、\ E)$。

更一般地，同伦图 $\mathcal{G}$ 可以是如下所述的任意连通多重图 [9], ，允许两个顶点之间由任意数量的边连接。在同一对顶点之间存在平行边时，应为这些边分别配上不同的解析连接路径 $p_e(t)$（并非全部为直线！）。在所有情况下，都要求纤维 $\pi^{-1}(p_e(t))$ 由d 个彼此不同且孤立的解组成，对于所有的 $t \in [0,\ 1]$即每个 $p_e(t)$ 都避开判别式。

在构造的同伦图中，沿着一条边进行跟踪 e从一个参数实例 z_i 及其已知解 x_i 到相邻的z_j 会得到一个新的解x_j。在此情况下，我们得到新的问题－解对 $(z_j,\ x_j)$。此外，我们记录从 x_i 到x_j 的具体对应关系，该对应关系与边 e. 相关。我们将这一记录下来的关系称为边对应。

作为一个说明性示例，考虑一个由顶点 $z_0、\ z_1、\ z_2$组成的 3-循环。利用构造出的参数同伦，我们跟踪从 z_0 到 z_1 的路径，以获得一个解 x_1，从而建立沿第一条边的对应关系。继续进行，我们从 z_1 跟踪到 z_2 ，找到一个解 x_2，最后再跟踪回到 z_0。通过这种方式，该 3-循环定义了一个单值化回路，它在纤维上诱导出一个置换 $\pi^{-1}(z_0)$。这意味着，该过程可能在 $\pi^{-1}(z_0)$ 中得到一个不同于初始 x_0的解。在这种情况下，所记录的边对应关系序列使我们能够明确重构单值化作用是如何沿该循环形成的。因此，随着纤维中发现更多点，同伦图各循环所诱导的置换会生成单值化群中相应的部分。

原则上，要恢复完整的单值化群，并不需要确定所有边的对应关系；只需收集一组环路，使其诱导的置换能够生成该群即可（见第 4.3 节）。然而，由于目标群的阶和结构通常事先未知，因此最好找出完整的纤维。检查纤维是否完整的一种严格停止准则是多齐次迹检验 [28]。不过，这种停止准则可能效率不高，因为它需要求解一个解很多的辅助系统。实践中，一种常见的

启发式方法是：一旦连续若干次单值化环路均未能在纤维中产生任何新解，就终止计算。

我们称同伦图中的一条边 $e = (u, v)$ 为饱和的，如果$\pi^{-1}(u)$ 中的每个已发现解都已追踪到 $\pi^{-1}(v)$ 中的一个解，反之亦然。若同伦图 $\mathcal{G}$ 的所有边均已饱和，则称该图为饱和图。假设所有路径均已使用算法 3 进行可认证追踪，则这意味着每个顶点处找到的解的数量都是某个常数k. 理想情况下，而且实践中也常常如此，我们发现 $k = d$ 就是真实的参数系统根数。需要强调的是，尽管非饱和图可能更适合高效地寻找解，但使同伦图饱和往往会提高恢复完整单值化群的概率。

3.2. **从同伦图生成单值化置换**。给定一个每个顶点都有 k 个解的饱和同伦图，我们按如下方式提取单值化作用：

(1) 对于选定的基顶点 z_0，我们构造一棵以 z_0为根的生成树 $\mathcal{T}$。(2) 对于 $\mathcal{G}$中的每个顶点 z，沿着 $\mathcal{T}$中从 z_0 到 z 的唯一一条路径合成边对应关系，可得到一个双射

$$\phi_{\mathcal{T},z} : \pi^{-1}(z_0) \to \pi^{-1}(z).$$

(3) 每条不属于生成树 $\mathcal{T}$的边 $e = (u, v)$ 都会与 $\mathcal{T}$形成唯一的基本回路，并且每个这样的回路都会产生一个单值群置换。相应的 $\pi^{-1}(z_0)$ 上的单值群置换为

$$\sigma_{\mathcal{T},e} = \phi_{\mathcal{T},v}^{-1} \circ \gamma_e \circ \phi_{\mathcal{T},u}, \tag{3}$$

此处 γ_e： $\pi^{-1}(u) \to \pi^{-1}(v)$ 表示与之关联的边对应关系 e.

(4) 以此方式得到的置换集合$\{\sigma_{\mathcal{T},e}\}$ 在 e 遍历 $\mathcal{G}$的所有非生成树边时，生成一个由同伦图 $\mathcal{G}$编码的置换群

我们在算法 4 中对这一过程进行形式化描述。

算法 4 单值群群

输入： • 一个饱和同伦图 $\mathcal{G} = (V, E)$，包含 k 个解和一个基顶点 $z_0 \in V$，

• 对于每条边 $e = (u, v) \in E$，一个双射对应关系 γ_e： $\pi^{-1}(u) \to \pi^{-1}(v)$。输出：作用 $\mathrm{Mon}_{\mathcal{G},z_0} \subset \mathrm{Mon}_\pi$ 在 $\pi^{-1}(z_0)$ 上的生成元 1：初始化生成元集合 $S = \varnothing$。2：构造一棵生成树 $\mathcal{T} = (V, E_\mathcal{T})$，其根为 z_0。3：确定相对于 $= E \setminus E_\mathcal{T}$ 的非树边集合 E。4：对于每条边 $e = (u,v) \in E$，若其为非树边，则执行 5：沿 $\mathcal{T}$ 中唯一的 uv-路径找到 $\phi_{\mathcal{T},u}$ 和 $\phi_{\mathcal{T},v}$。6：按照 (3) 在 $\pi^{-1}(z_0)$ 上构造置换 $\sigma_{\mathcal{T},e} = \phi_\mathcal{T}^{-1},_v \circ \gamma_e \circ \phi_{\mathcal{T},u}$。7：$S = S \cup \{\sigma_{\mathcal{T},e}\}$。8：结束循环。9：返回 S。

同伦图 $\mathcal{G}$ 编码了一个传递置换群 $\mathrm{Mon}_{\mathcal{G},z_0} \hookrightarrow S_k$，该群由从以 z_0. 为起点的无限多个闭合游走所得到的环路诱导的所有置换生成， $\mathcal{G}$ 下面证明的直接图论引理指出了该群的一个有限生成集，其中包含由式 (3) 定义的所有置换 $\sigma_{\mathcal{T},e}$。

引理 3.1. 算法 4 生成的置换生成群 $\mathrm{Mon}_{\mathcal{G},z_0}$.

证明。 考虑任意一个以 z_0, 为底点、沿着边 $e_1 = (u_1, v_1), \ldots, e_k = (u_k, v_k)$ 行进的闭合游走，其中 $u_{i+1} = v_i$ 对于 $1 \leqslant i < k,$ ，且 $u_1 = v_k = z_0.$ 。该游走编码了置换

$$\gamma_{e_k} \circ \cdots \circ \gamma_{e_1} = \left(\phi^{-1}_{\mathcal{T},v_k} \circ \gamma_{e_k} \circ \phi_{\mathcal{T},u_k}\right) \circ \cdots \circ \left(\phi^{-1}_{\mathcal{T},v_1} \circ \gamma_{e_1} \circ \phi_{\mathcal{T},u_1}\right). \tag{4}$$

对于每个 e_i，有两种情况需要考虑:

(1) $e_i \notin E_{\mathcal{T}}$, in which case $\phi^{-1}_{\mathcal{T},v_i} \circ \gamma_{e_i} \circ \phi_{\mathcal{T},u_i} = \sigma_{\mathcal{T},e_i}$ as defined in Algorithm 4, or

(2) $e_i \in E_{\mathcal{T}}$, in which case $\phi^{-1}_{\mathcal{T},v_i} \circ \gamma_{e_i} \circ \phi_{\mathcal{T},u_i} = \mathrm{id}$.

我们得出置换 (4) 属于由所有 $\sigma_{\mathcal{T}、e}$ （满足 $e \notin E_{\mathcal{T}}$.）生成的群。 □

备注 3.2。 我们可以调整算法 4，使其适用于非饱和图：构造由对应关系在所有 k 解上都有定义的边组成的子图，然后将 $\mathcal{G}$ 替换为该子图中包含 z_0的连通分支。

3.3. **经认证的单值化计算**。 结合用于经认证的跟踪的算法 3 与算法 4 的组合式置换提取方法，我们得到一种完整的经认证的单值化计算算法。图1展示了该算法的示意图。完整的伪代码及正确性陈述见算法 5。

定理3.3。 在算法 5 的整个执行过程中均满足定理2.1的假设时，输出集合 S 由参数空间中环路所诱导的置换组成。$\langle S\rangle \hookrightarrow S_k$ 的传递作用与群 $\mathrm{Mon}_{\mathcal{G}、z_0}$ 在 $z_0.$ 处已知的 k 解上的作用一致。特别地，若 $k = d$ 为一般根数，则有以下关系

$$\langle S\rangle = \mathrm{Mon}_{\mathcal{G},z_0} \subset \mathrm{Mon}_{\pi}\,.$$

注 3.4。 如果 $\mathcal{G}$ 未饱和，则可修改定义 3.3，使其得出较弱的结论：$\langle S\rangle$ 在 k 解上的作用与 $\mathrm{Mon}_{\mathcal{G},\ z_0}$ 的某个子群的作用一致。

我们指出，一般而言，$\mathrm{Mon}_{\mathcal{G},\ z_0}$ 可能不等于完整的单值化群 Mon_{π}。要验证二者相等，例如需要确认 $k = d$，也就是说，完全恢复 z_0 的纤维。实践中，人们往往依赖启发式证据：如果随着图 $\mathcal{G}$不断扩展，群 $\mathrm{Mon}_{\mathcal{G},\ z_0}$ 趋于稳定，这或许能为恢复出的群 $\langle S\rangle$ 等于 Mon_{π}这一主张提供一些支持。

算法 5 经认证的单值群计算**输入：** • 一个系统 $F(x;\ z)$ 局部定义了解簇 $X \subset \mathbf{C}^m \times \mathbf{C}^n$,

• 一个构造出的一般点对 $(z_0,\ x_0) \in X$。

• 一个连通多重图 $\mathcal{G}$，其包含 $V(\mathcal{G}) = \{z_0、\ldots\ldots、\ z_\ell\} \subset \mathbf{C}^m$，以及路径 $p_e(t)$，适用于所有 $e \in E(\mathcal{G})$输出：生成元 $S \subset S_k$，它们对应 $\mathrm{Mon}_{\mathcal{G}、z_0} \subset \mathrm{Mon}_{\pi}$ 在 $\pi^{-1}(z_0)$上的作用。1：当 $\mathcal{G}$ 未饱和时，执行以下操作 2：对于 $\mathcal{G}$ 中的每条边 $e = (u、\ v)$，执行以下操作 3：如果 e 未饱和，则 4：使用 CertifiedTrack 沿 e将 u 处所有已知解传输到 v 。▷ 算法 3 5：在 e处记录每个由此得到的边对应。6：结束条件判断 7：结束循环 8：结束循环 9：设置 S =MonodromyGroup($\mathcal{G}$)。▷ 算法 4 10：返回 S。

备注 3.5. 如果为 X 中支配参数空间的每个不可约分支都提供一个伪造对，我们可以将算法 5 扩展到 X 具有多个此类不可约分支的情形。

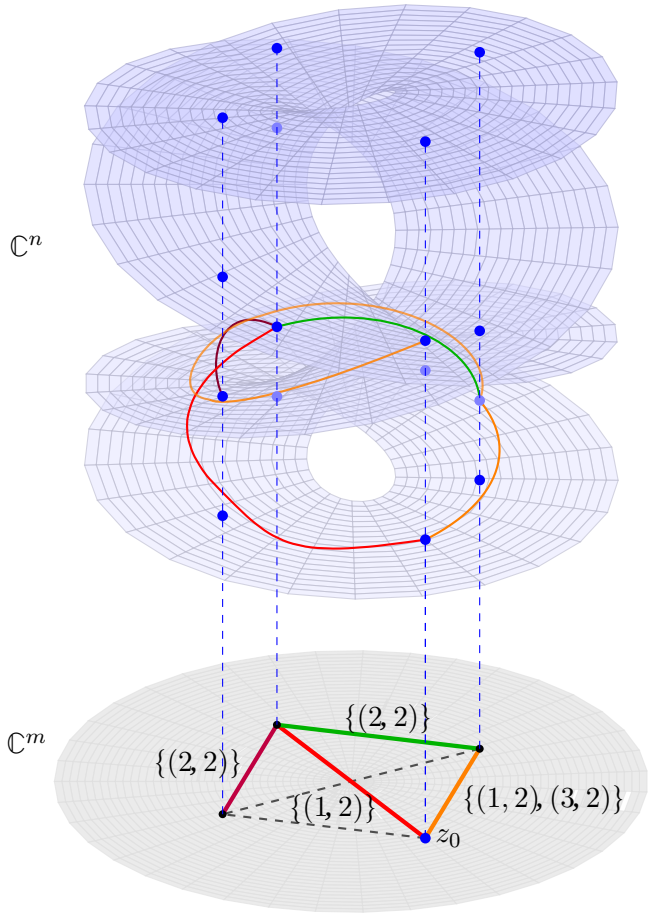

FIGURE 1. 四对一投影π：$X \to \mathbb{C}^m$的经认证单值化计算示意图。灰色圆圈表示带有同伦图的参数空间 $\mathbb{C}^m$（底顶点 z_0 以蓝色标出）。对于每条边（虚线），经认证的路径跟踪会将参数路径提升为关联簇 $X \subset \mathbb{C}^m \times \mathbb{C}^n$上的一条曲线。由此得到边对应，并将其记录下来以获得单值群置换。同伦图的边在其对应关系计算完成后会着色；彩色曲线表示相应的经认证提升。

即使在算法 5 无法恢复所有 d 解的情形下，我们仍可能获得关于完整伽罗瓦／单值化群 Mon_π的有用信息。为说明这一点，我们回顾伽罗瓦宽度这一概念，它由 [8]引入。对于任意有限群 G，不变量 $\mathrm{gw}(G)$ 可用于衡量 G的结构复杂度，其定义如下：

$$\mathrm{gw}(G) := \min_{\substack{\text{unrefinable subgroup chains} \\ id=H_m \leqslant \cdots \leqslant H_0 = G}} \left(\max_{0 \leqslant i < m} [H_i : H_{i+1}] \right). \tag{5}$$

我们现在 ob 证明伽罗瓦宽度关于算法 5 的输出是单调的。

Pr命题 3.6. 对于任意同伦图 $\mathcal{G}$，都有 $\mathrm{gw}(\mathrm{Mon}_{\mathcal{G},\ z_0}) \leqslant \mathrm{gw}(\mathrm{Mon}_\pi$).

问题	# 变量	# 参数	伽罗瓦群	# 根	伽罗瓦宽度
Belyi函数，4.2	1	1	M_{23}	23	23
对称27条直线，4.3	8	2	$S_2 \times S_2$	27	2
曲面上的最近点，4.4	4	3	$S_4 \wr S_2$	8	3
三点绝对位姿（P3P），4.5	3	15	$(S_2 \wr S_4) \cap A_8$	8	3
五点相对位姿，4.6	3	20	$(S_2 \wr S_{10}) \cap A_{20}$	20	10

TABLE 1. 第4.2–4.6小节实验总结。

证明。 作为一个置换群，Mon$_{\mathcal{G},\ z_0}$ 的作用是某个子群 $H \subset$Mon$_\pi$ 在其轨道上的限制；该轨道由与 $x_0 \in \pi^{-1}(z_0)$ 通过 $\mathcal{G}$. 相连的解构成。因此，

$$\mathrm{gw}(\mathrm{Mon}_{\mathcal{G},z_0}) \leqslant \mathrm{gw}(H) \leqslant \mathrm{gw}(\mathrm{Mon}_\pi),$$

其中，第二个不等式由 [8, 定理 4] 得出；又因为 Mon$_{\mathcal{G},\ z_0}$ 是 H的一个同态像，所以第一个不等式由 [8, 命题 3]得出。□

4. EXPERIMENTS

我们使用 Julia 编程语言实现了经认证的跟踪与同伦图框架。除非另有说明，算法 5 中的同伦图始终是一个完全图，其顶点为 v_0、……、v_ℓ，坐标从复单位圆上均匀随机抽取，顶点之间的边则是简单的直线段。对于区间算术，我们使用 Nemo.jl 包 [15], ，它封装了 Arb 库 [23]。复区间的实部和虚部具有 $[x-r$、 $x+r]$的形式，其中半径 r 的尾数为 30 位，中点 x 的尾数精度由用户指定，而半径和中点的指数均为任意精度。为确保所有路径跟踪都不会失败，我们在所有实验中将精度固定为 256 位。不过，对于许多示例而言，所需精度要低得多。对于算法 2 和算法 3 的参数，我们选用 [18], 中使用的相同取值，即$\rho = \frac{1}{8}$、 $\tau = \frac{7}{8}$、 $g = \frac{1}{64}$、 $h = r = \frac{1}{10}$、 $\delta_{inc} = \frac{5}{4}$和 $\delta_{dec} = \frac{1}{2}$，以及下文定义的 Hermite 预测器 $X(\eta)$。该预测器的一个优点是能够利用前一步的信息。具体而言，设 x 为当前点（位于 $\eta = 0$），设 $x_{pr\bar{e}v}$ 为跟踪过程中得到的前一个点（位于 $\eta = -h_{prev}$）。令 v 和 v_{prev} 表示相应的切向量。Hermite 预测器 $X(\eta)$ 是满足 $X(0) = x$、 $X(-h_{prev}) = x_{prev}$、 $X'(0) = v$和 $X'(-h_{prev}) = v_{prev}$的唯一三次多项式，其显式表达式（参见 [18, §6.2]）为

$$X(\eta) = x + v\eta + \left(\frac{2v + v_{prev}}{h_{prev}} - \frac{3(x - x_{prev})}{h_{prev}^2}\right)\eta^2 + \left(\frac{v + v_{prev}}{h_{prev}^2} - \frac{2(x - x_{prev})}{h_{prev}^3}\right)\eta^3. \tag{6}$$

第一小节介绍了一系列针对单变量示例集开展的实验，结果汇总于表 2。表 1 总结了后续小节介绍的实验。所有代码和数据均可通过以下网址获取：

`https://github.com/klee669/certified_homotopy_tracking`

4.1. 简单单变量族。 我们首先考察几个次数较低的单变量基准测试。在每种情况下，参数都是多项式系数，并满足相应的对称性或稀疏性约束，且单值化作用是传递的。具体情况如下：

- **一般系数：** $\sum_{i=0}^{d} c_i x^i$，具有全对称单值化 Mon$_\pi \cong S_d$,
- **偶次项：** $\sum_{i=0}^{d} c_{2i} x^{2i}$，具有非本原单值化 Mon$_\pi \cong S_2 \wr S_d \cong S_2^d \rtimes S_d$,
- **偶次项 + 平方系数：** $\sum_{i=0}^{d} (c_{2i} x^i)^2$，具有 Mon$_\pi \cong S_2^{d-1} \rtimes S_d$,
- **回文式：** $\sum_{i=0}^{d} c_i x^i$ 其中 $c_i = c_{d-i}$，具有 Mon$_\pi \cong S_2 \wr S_d$。

一般系数次数：3
$\mathrm{Mon}_\pi = S_3$, 伽罗瓦宽度：3

# 节点	3	4	5	6
Mon_π =$\mathrm{Mon}_\mathcal{G}$	0%	49 %	78 %	87 %
$\mathrm{Mon}_\mathcal{G} \curvearrowright \pi^{-1}(p)$	23 %	68 %	87 %	91 %
$\mathrm{gw}(\mathrm{Mon}_\pi) = \mathrm{gw}(\mathrm{Mon}_\mathcal{G})$	23%	68 %	87 %	91 %

一般系数次数：4
$\mathrm{Mon}_\pi = S_4$, 伽罗瓦宽度：3

# 节点	3	4	5	6
Mon_π =$\mathrm{Mon}_\mathcal{G}$	0%	55 %	77%	94 %
$\mathrm{Mon}_\mathcal{G} \curvearrowright \pi^{-1}(p)$	4 %	63 %	78 %	94 %
$\mathrm{gw}(\mathrm{Mon}_\pi) = \mathrm{gw}(\mathrm{Mon}_\mathcal{G})$	10 %	74 %	86%	96 %

一般系数次数：5
$\mathrm{Mon}_\pi = S_5$, 伽罗瓦宽度：5

节点数	3	4	5	6
Mon_π =$\mathrm{Mon}_\mathcal{G}$	0%	42 %	83 %	91 %
$\mathrm{Mon}_\mathcal{G} \curvearrowright \pi^{-1}(p)$	3 %	46 %	85 %	91 %
$\mathrm{gw}(\mathrm{Mon}_\pi) = \mathrm{gw}(\mathrm{Mon}_\mathcal{G})$	4%	46 %	85 %	91 %

一般系数次数：6
$\mathrm{Mon}_\pi = S_6$, 伽罗瓦宽度：6

节点数	3	4	5	6
Mon_π =$\mathrm{Mon}_\mathcal{G}$	0%	29 %	75%	91 %
$\mathrm{Mon}_\mathcal{G} \curvearrowright \pi^{-1}(p)$	4 %	36 %	76 %	93 %
$\mathrm{gw}(\mathrm{Mon}_\pi) = \mathrm{gw}(\mathrm{Mon}_\mathcal{G})$	0 %	33 %	76%	93 %

一般系数次数：7
$\mathrm{Mon}_\pi = S_7$, 伽罗瓦宽度：7

# 节点	3	4	5	6
Mon_π =$\mathrm{Mon}_\mathcal{G}$	0%	23 %	74 %	95 %
$\mathrm{Mon}_\mathcal{G} \curvearrowright \pi^{-1}(p)$	2 %	28 %	76 %	96 %
伽罗瓦宽度(Mon_π) = 伽罗瓦宽度($\mathrm{Mon}_\mathcal{G}$)	2%	28 %	76 %	96 %

偶数次项之和：次数 4
$\mathrm{Mon}_\pi = S_2 \wr S_2$, 伽罗瓦宽度：2

# 节点	3	4	5	6
Mon_π =$\mathrm{Mon}_\mathcal{G}$	0%	18 %	43%	64 %
$\mathrm{Mon}_\mathcal{G} \curvearrowright \pi^{-1}(p)$	27 %	62 %	89 %	96 %
伽罗瓦宽度(Mon_π) = 伽罗瓦宽度($\mathrm{Mon}_\mathcal{G}$)	47 %	75 %	96%	98 %

偶数次项之和：6 次
$\mathrm{Mon}_\pi = S_2 \wr S_3$, 伽罗瓦宽度：3

# 节点	3	4	5	6
Mon_π =$\mathrm{Mon}_\mathcal{G}$	0%	37 %	73 %	95 %
$\mathrm{Mon}_\mathcal{G} \curvearrowright \pi^{-1}(p)$	24 %	56 %	83 %	97 %
$\mathrm{gw}(\mathrm{Mon}_\pi) = \mathrm{gw}(\mathrm{Mon}_\mathcal{G})$	27%	60 %	86 %	99 %

偶数次项之和：8 次
$\mathrm{Mon}_\pi = S_2 \wr S_4$, 伽罗瓦宽度：3

# 节点	3	4	5	6
Mon_π =$\mathrm{Mon}_\mathcal{G}$	0%	32 %	67%	95 %
$\mathrm{Mon}_\mathcal{G} \curvearrowright \pi^{-1}(p)$	2 %	49 %	70 %	95 %
$\mathrm{gw}(\mathrm{Mon}_\pi) = \mathrm{gw}(\mathrm{Mon}_\mathcal{G})$	11 %	83 %	82%	100 %

偶数次（平方系数）：次数 4
$\mathrm{Mon}_\pi = S_2 \rtimes S_2$, 伽罗瓦宽度：2

# 节点	3	4	5	6
Mon_π =$\mathrm{Mon}_\mathcal{G}$	0%	30 %	68 %	89 %
$\mathrm{Mon}_\mathcal{G} \curvearrowright \pi^{-1}(p)$	0 %	30 %	68 %	89 %
$\mathrm{gw}(\mathrm{Mon}_\pi) = \mathrm{gw}(\mathrm{Mon}_\mathcal{G})$	56%	85 %	98 %	100 %

偶数次（平方系数）：6 次
$\mathrm{Mon}_\pi = S_2^2 \rtimes S_3$, 伽罗瓦宽度：3

# 节点	3	4	5	6
Mon_π =$\mathrm{Mon}_\mathcal{G}$	0%	48 %	82%	96 %
$\mathrm{Mon}_\mathcal{G} \curvearrowright \pi^{-1}(p)$	0 %	51 %	82 %	96 %
$\mathrm{gw}(\mathrm{Mon}_\pi) = \mathrm{gw}(\mathrm{Mon}_\mathcal{G})$	28 %	80 %	94%	97 %

偶数次（平方系数）：8 次
$\mathrm{Mon}_\pi = S_2^3 \rtimes S_4$, 伽罗瓦宽度：3

# 节点	3	4	5	6
Mon_π =$\mathrm{Mon}_\mathcal{G}$	0%	35 %	83 %	97 %
$\mathrm{Mon}_\mathcal{G} \curvearrowright \pi^{-1}(p)$	0 %	54 %	87 %	97 %
$\mathrm{gw}(\mathrm{Mon}_\pi) = \mathrm{gw}(\mathrm{Mon}_\mathcal{G})$	27%	81 %	98 %	99 %

回文式：4 次
$\mathrm{Mon}_\pi = S_2 \wr S_2$, 伽罗瓦宽度：2

# 节点	3	4	5	6
Mon_π =$\mathrm{Mon}_\mathcal{G}$	0%	47 %	74%	90 %
$\mathrm{Mon}_\mathcal{G} \curvearrowright \pi^{-1}(p)$	10 %	61 %	68 %	93 %
$\mathrm{gw}(\mathrm{Mon}_\pi) = \mathrm{gw}(\mathrm{Mon}_\mathcal{G})$	53 %	89 %	97%	99 %

回文式：6 次
$\mathrm{Mon}_\pi = S_2 \wr S_3$, 伽罗瓦宽度：3

# 节点	3	4	5	6
Mon_π =$\mathrm{Mon}_\mathcal{G}$	0%	34 %	56 %	85 %
$\mathrm{Mon}_\mathcal{G} \curvearrowright \pi^{-1}(p)$	7 %	52 %	82 %	91 %
$\mathrm{gw}(\mathrm{Mon}_\pi) = \mathrm{gw}(\mathrm{Mon}_\mathcal{G})$	22%	67 %	77 %	93 %

回文式：8 次
$\mathrm{Mon}_\pi = S_2 \wr S_4$, 伽罗瓦宽度：3

# 节点	3	4	5	6
Mon_π =$\mathrm{Mon}_\mathcal{G}$	0%	21 %	66%	84 %
$\mathrm{Mon}_\mathcal{G} \curvearrowright \pi^{-1}(p)$	4 %	44 %	78 %	87 %
$\mathrm{gw}(\mathrm{Mon}_\pi) = \mathrm{gw}(\mathrm{Mon}_\mathcal{G})$	14 %	65 %	89%	97 %

TABLE 2. 3–8次单变量族的实验结果。

对于上文列出的每种情况以及不同的 $2 \leqslant d \leqslant 8$，我们都构造了包含 $k = 3$、4、5、6 个顶点的完备同伦图，并对算法 5 进行了 100 次试验。我们的目标是了解图规模和群性质如何影响完整或部分恢复。

结果汇总于表 2。我们报告了三项指标：

• $\mathrm{Mon}_\pi = \mathrm{Mon}_\mathcal{G}$：恢复出精确伽罗瓦／单值化群的案例百分比。• $\mathrm{Mon}_\mathcal{G} \curvearrowright \pi^{-1}(p)$：恢复出精确根数的案例百分比。• $\mathrm{gw}(\mathrm{Mon}_\pi) = \mathrm{gw}(\mathrm{Mon}_\mathcal{G})$：恢复出精确伽罗瓦宽度的案例百分比。

从数据中可以观察到若干趋势。

首先，不出所料，所有指标的成功率通常都会随着顶点数增加而提高，这证实了更稠密的同伦图往往能更可靠地恢复群性质。

其次，高次多项式通常需要更多节点才能达到较高的成功率。对于一般系数的情况，这与 [9], 中给出的概率启发式相悖；该启发式认为，随着 $d \to \infty$., 可能只需要常数个环路。我们的实验结果部分反映了使用较小 d. 值所带来的影响。对于解很多且具有全对称单值化的多元系统，我们通常只需绕过少数几个分支点，就能实现完整（尽管未经认证）的单值群恢复。

最后但同样重要的是，我们观察到，在三个非本原情形中，伽罗瓦宽度恢复的成功率往往高于传递性判定和精确群恢复的成功率。特别是在稀疏图上，即使没有找到全部解，该方法也经常能识别出正确的宽度。这凸显了伽罗瓦宽度的实际价值：在解空间尚未被充分探索之前，我们就可以用它来衡量问题的内在复杂度。

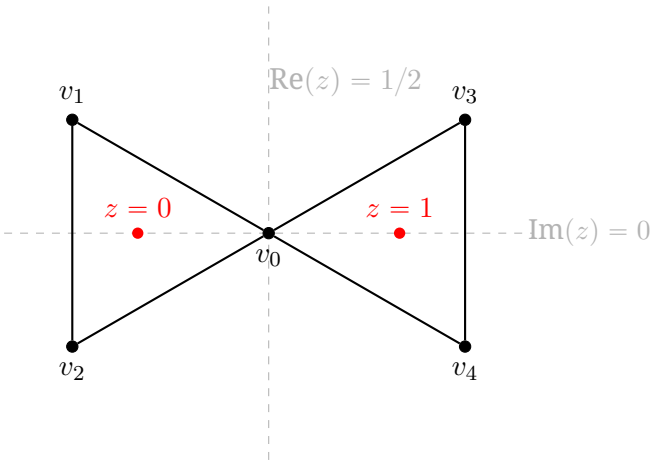

FIGURE 2. 围绕分支点的同伦图 $\mathcal{G}$ $z \in \{0,\ 1\}$ 对于 Belyi族 $f(x;\ g) = z$ 由 (7) 定义，其中 g 满足 (9)。

4.2. **Mathieu群的一个Belyi函数。** 作为另一个单变量示例，我们重新考察Elkies构造的一个23次Belyi多项式 [14] ，其伽罗瓦／单值化群是散在的Mathieu群 M_{23}. 。该示例被用于完成M¨uller [32]关于所有具有本原伽罗瓦群的多项式 $f(x) - z \in \mathbb{C}[x, z]$ 的分类，这些多项式定义在 $\mathbb{C}(z)$. 上。 有理数域 $\mathbb{Q}$ 上的逆伽罗瓦问题进一步促使我们研究这一示例。群 M_{23}是尚未得到肯定解决这一问题的最后一个散在有限单群。此外，根据近期的研究 [37], M_{23} ，它是唯一一个尚未构造出该问题明确解法的次数为 $\leqslant 23$ 的置换群。

为完整起见，我们在下方重现Elkies的方程：

$$\begin{aligned}
\tau &= (2^{38}3^{17}/23^3)(47323G^3 - 1084897G^2 + 7751G - 711002),\\
f_2(x;G) &= (8G^3 + 16G^2 - 20G + 20)x^2 - (7G^3 + 17G^2 - 7G + 76)x\\
&\quad + (-13G^3 + 25G^2 - 107G + 596),\\
f_3(x;G) &= 8(31G^3 + 405G^2 - 459G + 333)x^3 + (941G^3 + 1303G^2 - 1853G + 1772)x\\
&\quad + (85G^3 - 385G^2 + 395G - 220),\\
f_4(x;G) &= 32(4G^3 - 69G^2 + 74G - 49)x^4 + 32(21G^3 + 53G^2 - 68G + 58)x^3\\
&\quad - 8(97G^3 + 95G^2 - 145G + 148)x^2 + 8(41G^3 - 89G^2 - G + 140)x\\
&\quad + (-123G^3 + 391G^2 - 93G + 3228),\\
f(x;G) &= \tau^{-1} f_2^2(x) f_3(x) f_4^4(x),
\end{aligned}$$

(7)

其中我们对多项式 $f(x$采用了自己的归一化； $G)$，而 G是区间

(8) $G = [0.54947230454188887627333 1 \pm r] + i[0.67565033576789561392800491 \pm r], \quad r = 10^{-30},$

其中包含一个满足以下条件的四次代数数 g

$$g^4 + g^3 + 9g^2 - 10g + 8 = 0. \tag{9}$$

我们的归一化方式使得以下贝利映射的分支点 $\mathbb{C} \ni x \mapsto f(x;\ g) \in \mathbb{C}$位于$z = 0$ 和 $z = 1$. 这些分支点在图 2 中以可视化方式呈现，同时还展示了一个蝴蝶结形的同伦图 $\mathcal{G}$，我们用它来验证 Elkies 的结果。当我们沿着 z 图中的边变化时，会得到一系列包含解曲线的区间 $x_g(z)$，这些解曲线满足 $f(x_g(z)) = z$对所有 $g \in G$. 对于取值 $g \in G$ 若不满足（9），分支点 $z = 1$ 会分裂为若干簇，每簇由彼此邻近的不同分支点组成；对于这些取值，我们仅验证了 M_{23} 是完整伽罗瓦／单值化群的一个子群。然而，当 g 确实满足方程（9）时，我们验证了该贝利多项式的单值化群；按构造，该多项式只有两个分支点。

最后，我们引用 [14] 对这个例子的评论：“单值化计算需要一些谨慎的估计，以确保精度足以得到正确的置换。”与此恰恰相反，算法 5 中使用区间算术，使我们能够轻松地认证这一单值化作用，无需任何先验估计。

4.3. 对称三次曲面上的 27 条直线。经典代数几何告诉我们，光滑三次曲面上有 27 条直线 $f(x_1,\ x_2,\ x_3,\ x_4) = 0$位于 $\mathbf{P}^3$. 这一计数几何问题可以编码为一个 27 次分歧覆盖，其底空间为参数化所有三次曲面的 $\mathbf{P}^{19}$。近期的一项研究 [4], 表明，将这一覆盖限制在坐标置换作用下保持不变的曲面上S_4，所得的伽罗瓦／单值化群为克莱因四元群 $S_2 \times S_2$，且该群在 27 条直线上非传递地作用。本文将详述该研究中报告的一项计算。

[4] 的作者证明了，S_4对称三次曲面的模空间同构于 $\mathbf{P}^2$，并且该问题的分支轨迹分解为四个不可约分支：即三条直线和一条三次曲线。通过追踪环绕这些分支的环路，作者生成了完整的单值化群，并通过计算验证其为 $S_2 \times S_2$。

为构造多项式方程组 F，我们用两个张成点 $u, v \in$来表示直线 $\ell \subset \mathbf{P}^3$，并引入八个变量 $u = (a_1, b_1, c_1, d_1)$和 $v = (a_2, b_2, c_2, d_2)$，使得 $\ell = \mathrm{span}\{u, v\} = \{su + tv \mid s, t \in \mathbf{C}\}$。 S_4-对称三次型空间的基为 [4, 第 2 节.3]

$$m_3 = \sum_i x_i^3, \quad m_{21} = \sum_{i \neq j} x_i^2 x_j, \quad m_{111} = \sum_{i<j<k} x_i x_j x_k,$$

因此，任意对称三次曲面都可以唯一地写成

$$f = m_3 + a_{21}m_{21} + a_{111}m_{111},$$

其中我们固定 m_3 的系数为 1。条件 $\ell \subset V(f)$ 表示三次多项式 $f(su+tv)$ 在 (s,t) 中恒等于零。展开该表达式可得一个二元三次型，其四个系数必须为零，从而得到关于 u 和 v 中变量的四个三次方程。为消除与格拉斯曼流形 $Gr(2,4)$ 相关的冗余自由度，我们加入四个一般线性形式。这样便得到一个由八个变量构成的八方程方形方程组。

沿参数空间中的环路改变参数 (a_{21}, a_{111})（避开分支轨迹），会传递对应于 $V(f)$ 上 27 条直线的 27 个解，由此得到单值化作用。总而言之，这定义了关联簇

$$X = \{(a_{21}, a_{111}, u, v) \mid \ell \subset V(f)\} \subset \mathbb{C}^2 \times Gr(2,4), \tag{10}$$

并且投影 $\pi\colon X \to \mathbb{C}^2$ 是占优的，且一般为 27 对 1。此处的关联簇 X 是可约的，这可由非传递的伽罗瓦／单值化群作用见证。具体而言，伽罗瓦／单值化群 $S_2 \times S_2$ 忠实地作用于 3 个轨道，每个轨道包含 4 条直线；此外还有 6 个轨道，每个包含 2 条直线，并固定剩余的 3 条直线。

4.4. **代数簇上的最近点**。 最近点问题 针对实代数簇 $X \subset \mathbb{R}^n$，要求找出一点 $x \in X$ 使其到给定数据点 $u \in \mathbb{R}^n$ 的欧几里得距离最小。该问题的代数复杂度通常用欧几里得距离次数 [7], 来衡量，它统计了对一般数据点而言，距离平方函数在 X 的光滑轨迹上的复值临界点数目 $u.$ 。这里，我们考虑由$\mathbb{R}^3$中的 $f(x_1,\ x_2,\ x_3) = x_3^4 - (x_1^2 + x_2^2)^3 = 0$ 所定义的曲面，该曲面此前曾作为 [8, 例 5]出现。

对于该方程组，未知数为坐标 $x = (x_1,\ x_2,\ x_3)$ 以及拉格朗日乘子 λ。给定数据点 $u \in \mathbb{R}^3$, , 临界点是增广方程组的解

$$F(x,\lambda;u) = \{\nabla_x(\|x-u\|^2 + \lambda f(x_1,x_2,x_3)), f(x)\} = \begin{Bmatrix} 2(x_1-u_1) - 6x_1\lambda(x_1^2+x_2^2)^2 \\ 2(x_2-u_2) - 6x_2\lambda(x_1^2+x_2^2)^2 \\ 2(x_3-u_3) + 4\lambda x_3^3 \\ f(x_1,x_2,x_3) \end{Bmatrix} = 0.$$

这些约束 定义了欧几里得距离对应 X，它是关联簇

$$X = \{(u,x,\lambda) \mid F(x,\lambda;u) = 0\} \subset \mathbb{C}^3 \times \mathbb{C}^4.$$

投影 $\pi : X \to \mathbb{C}^3$ 是占优的，且 $\deg(\pi)$ 等于欧几里得距离度，已知其值为 8。 使用算法 5，我们能够验证此例的伽罗瓦／单值化群包含非本原群 $S_4 \wr S_2.$ 。事实上，反向包含关系也成立，因为 $S_4 \wr S_2$ 是与 π 的分解相容的最大群，该分解见 [8]。

对于此例，与小得多的伽罗瓦宽度 3相比，欧几里得距离度 8 是对代数复杂度的一种悲观衡量。另一方面，预计最近点问题的“多数”实例都具有全对称单值化。我们提出的框架为验证这类问题的代数难度提供了一种新工具。

4.5. **P3P：透视三点问题**。 透视透视三点n点（PnP）问题是计算机视觉中的一个问题：求出能够将 n已知三维点映射到 n 对应二维点的透视相机的位置和方向。其中，情形 $n = 3$，称为*P3P*，是极小情形。感兴趣的读者可参阅综述论文 [19], ，其中介绍了基于求解三次方程的经典解法。我们还指出此前的工作 [11] ，该工作介绍了如何将计算机视觉中的极小问题建模为分歧覆盖，以及计算其伽罗瓦／单值化群的启发式方法。在本文中，我们的实验表明，至少对于 P3P 这样的小型示例，此类计算可以得到严格认证。

我们将算法 5 应用于 P3P 的一种经典表述：关于从第 i 个三维点 d_i 到未知相机中心的三个未知距离的三个方程，其中 $1 \leqslant i \leqslant 3$，。令 D_{ij} 表示第 i 个与第 j 个三维点之间的距离平方，并令 $\tilde{y}_i \in S^2$ 表示第 i 个二维点的单位长度齐次坐标，我们有

$$d_i^2 - 2u_{ij}d_j + d_j^2 = D_{ij}, \qquad 1 \leqslant i < j \leqslant 3, \tag{11}$$

其中

$$u_{ij} := \frac{\langle \tilde{y}_i, \tilde{y}_j \rangle}{\|\tilde{y}_i\|\|\tilde{y}_j\|}.$$

利用 S^2，的立体投影参数化，方程 (11) 定义了参数多项式系统 $F(d_1,\ d_2,\ d_3;\ z) = 0$ 其参数为 $z = (q_i,\ y_i)$，对应于 $i = 1$，2，3，而簇为

$$X = \{(z, d_1, d_2, d_3) \mid F(d; z) = 0\} \subset \mathbb{C}^{15} \times \mathbb{C}^3.$$

投影 $\pi:\ X \to$C^{15} 是占优的，并且一般而言是 8 对 1 的，且 gw(Mon$_\pi$) $= 3$.。利用算法 5，我们证明 Mon$_\pi$ 包含非本原群 $(S_2 \wr S_4) \cap A_8 \cong S_2^3 \rtimes S_4$。在这个例子中，由于解具有 $(d_1,\ d_2,\ d_3) \mapsto (-d_1,\ -d_2,\ -d_3)$. 所给出的对称性，非本原性很容易理解。与前一个例子一样，由于在 [11, §3] 中对该问题的平方判别式进行了显式计算，也已知反向包含关系 Mon$_\pi \subset (S_2 \wr S_4) \cap A_8$ 成立。因此，利用算法 5，我们证明了 Mon$_\pi \cong (S_2 \wr S_4) \cap A_8$.

4.6. **五点相对位姿问题**。 最后，我们讨论五点相对位姿问题，这是计算机视觉中另一个研究充分的最小问题。在该问题的一种典型表述中，未知量包括旋转 $R \in SO(3)$ 和平移 $t \in \mathbb{C}^3$ （定义到尺度因子），二者共同描述相对相机几何。给定五对图像点 $(y_{1,\ i},\ y_{2,\ i}) \in \mathbb{C}^2 \times \mathbb{C}$ 对于 $i = 1, \ldots,$ 5，我们将它们提升到齐次坐标 $\tilde{y}_{1,\ i},\ \tilde{y}_{2,\ i} \in \mathbb{C}^3$。几何约束由极线约束编码，

$$\tilde{y}_{2,i}^\top ([t]_\times R)\, \tilde{y}_{1,i} = 0, \qquad i = 1, \ldots, 5. \tag{12}$$

这里，$[t]_\times$ 表示诱导出与 t 的叉积的反对称矩阵。注意，未知量可以合并为一个矩阵 $E = [t]_\times R$，称为本质矩阵。这些方程定义了一个带参数 $z = (y_{1,\ i},\ y_{2,\ i})$（其中 $i = 1,\ \ldots,\ 5$）的多项式方程组 $F(R,\ t$。输入数据的参数空间为 C^{20}„ 由此得到关联簇

$$X = \{(z; R, t) \mid F(R, t; z) = 0\} \subset \mathbb{C}^{20} \times (SO(3) \times \mathbb{P}^2).$$

投影 $\pi : X \to$C^{20} 是占优的，并且一般为 20 对 1。其单值群是非本原的，因为对于一般数据，只有 $10 =$ gw(Mon$_\pi$）个不同的本质矩阵与之相容，但每个本质矩阵都对应两个可能的相对位姿 $(R,\ t)$. 有关更多细节，参见例如 [36] 。

为了使经认证的跟踪更易于处理，我们通过注意到极线约束 (12) 关于 t 是线性的，消去平移变量 t 。由此可以单独针对旋转矩阵 R 推导出三个相互独立的三次约束；具体而言，其行列式

$$\det\left(\tilde{y}_{2,1} \times R\tilde{y}_{1,1} \;\middle|\; \tilde{y}_{2,2} \times R\tilde{y}_{1,2} \;\middle|\; \tilde{y}_{2,i} \times R\tilde{y}_{1,i} \right) = 0, \quad i = 3, 4, 5. \tag{13}$$

使用 SO(3) 的 *Cayley* 有理参数化，

$$R(x,y,z) = \frac{1}{1+x^2+y^2+z^2} \begin{pmatrix} x^2-y^2-z^2+1 & 2xy-2z & 2xz+2y \\ 2xy+2z & -x^2+y^2-z^2+1 & 2yz-2x \\ 2xz-2y & 2yz+2x & -x^2-y^2+z^2+1 \end{pmatrix}, \tag{14}$$

因此，我们得到一个含三个变量的参数系统，其伽罗瓦／单值化群同构于 Mon$_\pi$ · 。算法 5 证实 Mon$_\pi$ 包含非本原群 $(S_2 \wr S_{10}) \cap A_{20}$，从而强化了 [11, §4] 中的启发式证据，支持猜想 Mon$_\pi \cong (S_2 \wr S_{10}) \cap A_{20}$。

References

[1] C. Beltr´an 和 A. Leykin。经认证的数值同伦跟踪。《计算》，21(1):69–83，2012。[2] C. Beltr´an 和 A. Leykin。稳健的经认证数值同伦跟踪。，：–。[3] L. Blum、F. Cucker、M. Shub 和 S. Smale。《验证数值计算》。施普林格科学与商业媒体，2012。[4] T. Brazelton 和 S. Raman。对称三次曲面空间中的单值群与直线。，2024。[5] P. Breiding、K. Rose 和 S. Timme。使用区间算术认证多项式系统的零点。，。[6] M. Burr、K. Lee 和 A. Leykin。涉及解析函数的方程组近似解的有效认证。载于 *Foundations of Computational Mathematics* 13 253 295, 2013，第 267 274, 2019 页。[7] J. Draisma 、 E. Horobet、、 G. Ottaviani 、 B. Sturmfels 和 R. R. Thomas。代数簇的欧几里得距离度。，16:99–149，2016。[8] T. Duff。求解代数方程组的伽罗瓦论复杂度度量。，。[9] T. Duff、C. Hill、A. Jensen、K. Lee、A. Leykin 和 J. Sommars。通过同伦延拓和单值群求解多项式系统。，39(3):1421–1446，2019。[10] T. Duff、V. Korotynskiy、T. Pajdla 和 M. Regan。利用单值群恢复多项式系统的对称性。载于 *Proceedings of the 2023 International Symposium on Symbolic and Algebraic Computation*，第 251–259 页，2023。[11] T. Duff、V. Korotynskiy、T. Pajdla 和 M. H. Regan。用于分解三维重建中极小问题的伽罗瓦／单值化群。，6(4):740–772，2022。[12] T. Duff 和 K. Lee。使用 Krawczyk 方法进行认证同伦跟踪。载于 *Proceedings of the 2024 International Symposium on Symbolic and Algebraic Computation* 274 282, 2024，第 – 页。[13] P. B. Edwards 和 J. D. Hauenstein。关于局部单值群的计算和数值局部不可约分解。，13(1):e70025，2026。[14] N. Elkies。具有 Gal$(P(x)-t)\cong M_{23}$的复多项式 $P(x)$。，1(1):359–367，2013。[15] C. Fieker、W. Hart、T. Hofmann 和 F. Johansson。Nemo/Hecke：适用于 Julia 编程语言的计算机代数和数论软件包。载于 *Proceedings of the 2017 ACM International Symposium on Symbolic and Algebraic Computation* 157 164, 2017，第 – 页。[16] L. Granboulan。构造一个伽罗瓦群为 的 Q 的正则扩张。，( ): –。[17] A. Guillemot。使用 Algpath 进行经认证的代数路径跟踪。，59 3 53 56，2025 ( ): –。[18] A. Guillemot 和 P. Lairez。代数路径跟踪的验证数值计算。载于 *Proceedings of the 2024 International Symposium on Symbolic and Algebraic Computation* 36 45, 2024，第 – 页。[19] B. M. Haralick 、 C.-N. Lee 、 K. Ottenberg 和 M. N¨olle。三点透视位姿估计问题解的综述与分析。，13(3):331–356，1994。[20] J. D. Hauenstein、I. Haywood 和 A. C. Liddell Jr.。牛顿同伦的后验认证算法。载于 *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*，第 248–255 页，2014。[21] J. D. Hauenstein、J. I. Rodriguez 和 F. Sottile。伽罗瓦群的数值计算。，( ): –。[22] J. D. Hauenstein 和 F. Sottile。算法 921 *ACM*: *Transactions on Mathematical Software (TOMS)* 38 4 1 20, 2012 alphaCertified：多项式系统解的认证。，( ): –。[23] F. Johansson。Arb：高效的任意精度中点-半径区间算术。，( ): –。[24] R. B. Kearfott 和 Z. Xing。延拓方法中的区间步长控制。，( ): –。[25] R. Krawczyk。带误差界的牛顿零点求解算法。，：–。[26] K. Lee。在 Macaulay 2 *ACM Communications in Computer Algebra* 53 2 45 48, 2019 上认证多项式系统的近似解。，( ): –。[27] K. Lee。使用区间算术进行有效的 α 理论认证：区域上的 α 理论。载于 *International Congress on Mathematical Software* 275 284 2024，第 – 页。施普林格，。[28] A. Leykin 、 J. I. Rodriguez 和 F. Sottile。迹检验。，4(1):113–125，2018。

[29] A. Leykin 和 F. Sottile。通过同伦计算研究舒伯特问题的伽罗瓦群。 *Mathematics of Computation* 78 267 1749 1765, 2009 , （）：–。[30] B. Martin、A. Goldsztejn、L. Granvilliers 和 C. Jermann。针对一维流形的经认证的平行多面体延拓。 *SIAM Journal on Numerical Analysis*，51(6):3373–3401，2013。[31] R. E. Moore、R. B. Kearfott 和 M. J. Cloud。 *Introduction to interval analysis*。SIAM，2009。[32] P. M¨uller。多项式的本原单值群。 *Contemporary Mathematics*，186:385–385，1995。[33] E. Pichon-Pharabod 和 S. Telen。对称三次曲面的伽罗瓦群。 *arXiv preprint arXiv:2509.06785*，2025。[34] A. Sommese 和 C. Wampler。 *The Numerical Solution of Systems of Polynomials Arising in Engineering and Science* 2005 。世界科学出版社，。[35] F. Sottile 和 T. Yahl。计数几何中的伽罗瓦群及其应用。 *Expositiones Mathematicae*，43 6 125731，2025（）：。[36] H. Stew ´ ´ *ISPRS Journal of* enius、 *Photogrammetry and Remote Sensing* 60 4 284 294, 2006 C. Engels 和 D. Nister。直接相对定向的最新进展。，（）：–。[37] R. van Bommel、E. Costa、N. D. Elkies、T. Keller、S. Schiavone 和 J. Voight。17T7 是有理数域上的一个伽罗瓦群。 *arXiv preprint arXiv:2411.07857*，2024。[38] J. van der Hoeven。可靠同伦延拓。 *Technical Report*，2011。[39] J. Xu、M. Burr 和 C. Yap。认证同伦延拓路径的一种方法：单变量情形。载于*Proceedings of the 2018 ACM International Symposium on Symbolic and Algebraic Computation* 399 406, ，第–页。 2018

Department of Mathematics, University of Missouri - Columbia
Email address: tduff@missouri.edu*URL*: https://timduff35.github.io/timduff35/

School of Mathematical and Statistical Science, Clemson University, 220 Parkway Drive, Clemson, SC 29634*Email address*: kisunl@clemson.edu*URL*: https://klee669.github.io