arXiv:2512.19028v1 [quant-ph] 22 Dec 2025

环面丛拓扑不变量的经典与量子算法

Nelson Abdiel Col´on Vargas剑
桥大学nac52@cam.ac.uk

CarlosOrtiz Marrero科罗拉多州立大学计算机科学系
carlos.ortiz.marrero@colostate.edu

2025年12月23日

摘要

计算三维流形的拓扑不变量通常难以处理，但专门的代数结构能够实现高效算法。对于环面丛的 Witten-Reshetikhin-Turaev（WRT）不变量，我们利用非交换环面结构，在单位根处将闭环面的编织代数嵌入其对称子代数。这给出了一个固定N^2维表示，支持使用 $O(N^2)$ 空间进行多项式时间经典计算；此外，还有一种仅使用 $O(\log\ N)$ 个量子比特的量子算法——具有指数级空间优势。我们进一步证明，提取单个展开系数是 #P 完全问题；然而，存在一种量子算法，能够高效近似非微小比例配置所对应的这些系数。

1 引言

Witten-Reshetikhin-Turaev（WRT）不变量 [Wit89, RT91] 是区分三维空间（三维流形）的基本工具，源自量子场论，并将琼斯多项式 [Jon85] 从纽结推广到完整的三维流形拓扑。然而，计算一般三维流形的这些不变量是 #P-困难的 [AL17]。

尽管一般情况下难以计算，环面丛——即由作用于环面上的元素 $g \in SL_2(\mathbb{Z})$ 构成的映射环面——却是一个显著的例外。其特殊的代数结构使我们能够将 Kauffman 括号 skein 代数 $K_N(\Sigma_{1,\ 0})$ 嵌入非交换环面 [KF20, FG00] 的对称子代数中。由此，在单位根处可得到一个固定的 N^2 维表示，其中 Frohman-Gelca 乘积规则中数量呈指数级增长的展开项会归并为一组可处理的系数。与用于计算纽结不变量的基于辫子的量子算法 [AJL09, LRS+25] 不同，后者计算固定三维流形中一维曲线的性质，且所需量子比特数与辫宽成线性关系；我们的方法只需 $O(\log\ N)$ 个量子比特，就能计算三维流形本身的不变量。

我们提出三项利用非交换环面嵌入的主要结果。首先，我们开发了一种显式的经典动态规划算法，运行时间为 $\Theta((m+\ell)N^2)$，空间复杂度为 $\Theta(N^2)$，其中 m 是 skein 插入的数量，ℓ 是单值化字长度；从拓扑量子计算的角度来看，该算法计算环面 [BP08] 上 $SU(2)_k$ 个任意子的振幅。其次，我们开发了一种节省空间的量子算法，使用 $O(\log N + m)$ 个量子比特

相比之下，经典存储器需要 $\Theta(N^2)$，该算法通过酉元的线性组合相干地实现 skein 代数运算，从而获得指数级空间优势。第三，我们证明，系数提取这一子问题通过从 #SUBSET-SUM 进行保计数归约，在精确计算意义下是 #P 完全的，但仍可通过多项式时间量子加性近似求解，这表明存在可证明的计算分离。

1.1 计算问题

在全文中，我们固定一个奇整数 $N \geq 3$，令

$$t \;=\; e^{2\pi i/N},$$

并对 $\mathbb{Z}_N^2$ 中的指标模 N 运算。相位由辛形式 $\omega((p,s),(r,u)) = pu - sr$ 产生。

定义 1 (环面丛的 WRT 不变量**)。** 对于带有 ***skein*** 插入 $x_1, \ldots, x_m \in K_N(\Sigma_{1,0})$ 的环面丛 M_g（$g \in SL_2(\mathbb{Z})$ 的映射环面），其在层级 $k = N-2$ 处的 ***WRT*** 不变量为：

$$Z_N(M_g; x_1, \ldots, x_m) = \mathrm{Tr}(\rho(g) L_{x_m} \cdots L_{x_1})$$

其中 $\rho(g)$ 是模作用，而 L_{x_i} 是 ***skein*** 代数中的左乘算子。

这个计算问题自然分解为两项任务：计算完整的迹（即 WRT 不变量本身），以及从算子表示中精确确定特定系数。正如我们将看到的，这两项任务的计算复杂性有着根本差异。迹计算可通过在固定的 N^2 维系数表上进行动态规划，在经典计算机上以多项式时间完成；而当 N 足够大、足以避免模混叠时，精确系数提取则成为 #P-困难问题。这揭示了量子优势真正出现之处（即使精确计算难以处理，量子算法仍能高效近似这些系数）。

1.2 主要结果

定理 （经典动态规划算法）。 环面丛的 ***WRT*** 不变量 $Z_N(M_g; x_1, \ldots, x_m)$ 可以通过在非交换环面的系数表上进行动态规划，以经典方式在 $\Theta((m+\ell)N^2)$ 时间和 $\Theta(N^2)$ 空间内计算，其中 $\ell = |g|_{S,T}$ 是单值化的字长。

该算法在非交换环面中维护一个 N^2 维系数表，并针对每次编织插入和单值化生成元逐步更新，从而避免显式枚举所有 2^m 个展开项。字长 ℓ 随矩阵元素呈对数增长：对于 $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$，通过欧几里得算法分解 [FM11]，有 $\ell = O(\log \max(|a|,|b|,|c|,|d|))$。

定理 （量子算法）。 存在一种量子算法，能够以至少为 $1-\delta$ 的概率，将环面丛 M_g 的归一化 ***WRT*** 振幅 $\widetilde{Z} = \frac{1}{N^2}\mathrm{Tr}(W(g;\ \overline{x_1}, \ldots, x_m))$ 近似到 ϵ 的加性精度，所需资源如下：

$$\begin{aligned}
\textit{Qubits:} \quad & 2 \times \lceil \log_2 N \rceil + m + 1 \ \textit{(}O(\log N)\ \textit{data qubits,}\ m+1\ \textit{ancillas)} \\
\textit{Base circuit depth:} \quad & D = O(\ell \log^2 N + m \log^2 N)\ \textit{where}\ \ell = |g|_{S,T} \\
\textit{Total operations:} \quad & O(D \cdot \log(1/\delta)/\epsilon^2)\ \textit{via sampling}
\end{aligned}$$

这为经典算法提供了一种节省空间的替代方案，使用 $O(\log N + m)$ 空间，而非 $O(N^2)$ 空间。

量子算法将 N^2 维系数表格编码到 $O(\log\ N)$ 个量子比特中，并以相干方式实现缠结操作。对于较大的 N 或内存受限的量子硬件，指数级空间优势（$O(\log\ N)$ 个量子比特，而非$\Theta(N^2)$ 经典存储器）尤为显著。

定理 (系数计数的量子优势)。 当模数 N 大于 $\sum_i |a_i|+|z|$时，*FG* 系数计数问题（定义 *11*）在从 # 子集和进行保数归约的意义下是 *#P* 完全的，从而避免模混叠。尽管该问题在经典计算中很困难 *[Val79],*量子算法（定理 *9*）仍能以至少 $1-\delta$ 的概率，将归一化系数 $\alpha = 2^{-m}c(z)$ 估计到加性精度 ϵ，所需总量子比特数为 $O(\log N + m)$，基础电路深度为 $D = O(m\log^2 N)$，并通过采样实现 $O(D\cdot\log(1/\delta)/\epsilon^2)$ 次总操作。对于大小为 $\Omega(2^m)$ 的系数，这种加性近似具有实际意义。

这确立了一种计算分离：提取系数 $c(z)$ 需要对某个求和问题的解进行计数，其难度不亚于 # P 中的任何问题；而量子叠加则借助哈达玛测试实现多项式时间的加性近似。这些结果建立在以下结构基础之上：

定理 (结构分解)。 嵌入 $K_N(\Sigma_{1,0}) \hookrightarrow \mathcal{W}_t^\nu$ *(*非交换环面的对称子代数*)*给出了一种一致分解，其中每个编织生成元都可表示为 $L_{B_{(p,s)}} = U_{p,s} + U_{-p,-s}$，其中 $U_{p,s}$ 是可在深度 $O(\log^2 N)$内实现的带相位置换酉算子。

这种一致的二项结构（定理 1 和 3）与局部化 skein 代数中宽度可变的分解形成对比，使得经典动态规划和量子线性组合酉算子实现都能够高效进行。

1.3 与现有方案的比较

以 AJL 算法 [AJL09],为代表的早期拓扑不变量量子算法，主要通过辫群表示研究琼斯多项式。AJL 算法能够高效近似 S^3 中链环的琼斯多项式，而我们的方法针对的是缠结装饰的环面丛的 WRT 不变量。近期的实现 [LRS+25]已在量子硬件上展示了基于辫子的方案，为拓扑量子场论中的量子算法建立了实验基准。

基于辫子的琼斯多项式算法所依赖的技术方法，与我们的非交换环面框架有着根本区别。标准的基于辫子的方法需要选择一个位点（中心特征），而该选择会影响所得的矩阵表示。这种局部化带来了两个技术挑战：首先，每个 skein 元素的泡利分解宽度取决于元素本身和所选位点，因此辅助量子比特需求各不相同；其次，局部化结构将计算限制在链环不变量，而非一般的三维流形拓扑。相比之下，我们将其嵌入非交换环面的对称子代数 $\mathcal{W}_t^\nu$，从而得到一个固定的 N^2 维表示，不受位点选择影响（详细比较见附录 A）。这种无位点结构为所有 skein 元素提供统一的二项分解 $L_{B_{(p,s)}} = U_{p,\ s} + U_{-p,\ -s}$，可通过酉算子线性组合实现量子计算（为确保块编码的复合正确，每次编织乘法使用一个辅助量子比特），并可直接计算一般映射环面的迹型 WRT 振幅。

除了这些技术差异之外，所刻画数学对象的维度还存在根本区别。基于辫子的量子算法 [AJL09、LRS+25] 计算纽结不变量——即嵌入于

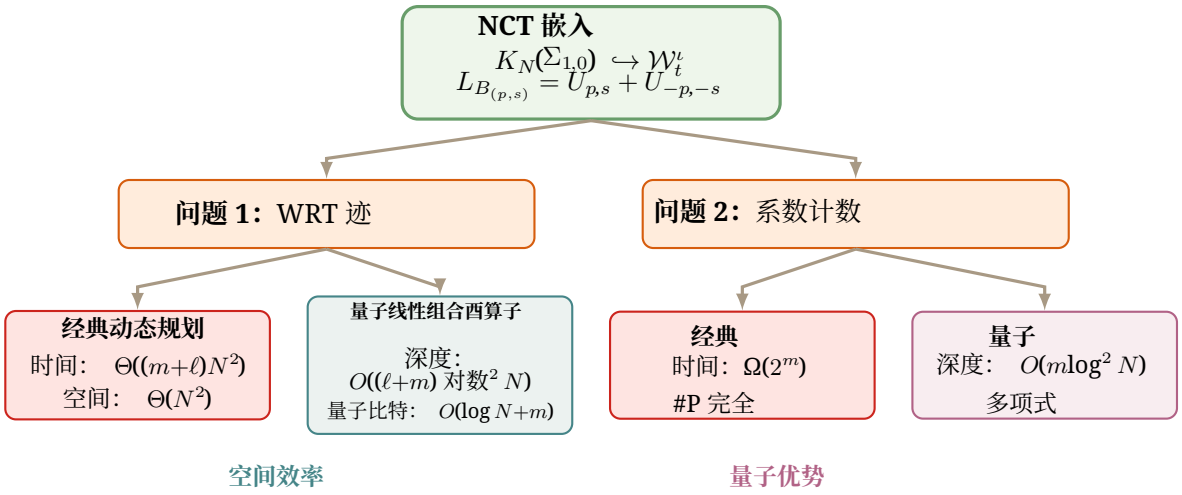


图 1：NCT 嵌入所构建的计算图景。结构基础（上方）支撑着两个不同的计算问题。**左侧（WRT 迹）：**经典动态规划算法的运行时间为 $\Theta((m+\ell)N^2)$，但需要 $\Theta(N^2)$ 的空间。量子 LCU 方法在使用 $O(\log\ N+m)$ 个总量子比特的情况下，仍可将运行时间保持在多项式时间 $O((\ell+m)\log^2 N)$，而经典存储器需要 $\Theta(N^2)$，因此具有指数级空间优势。**右侧（系数计数）：**经典枚举是 #P 完全问题，精确计数需要指数级 $\Omega(2^m)$ 时间，因此难以处理。量子哈达玛测试可实现多项式时间加性近似，电路深度为 $O(m\log^2 N)$，通过对所有 2^m 项进行相干叠加，展现出已获证实的计算优势。

固定三维流形中的一维曲线（纽结和链环）的拓扑性质（通常为 S^3）。我们的算法计算三维流形不变量，刻画三维空间 M_g 本身的拓扑性质。两种方法都源于相同的 TQFT 框架 [Wit89、RT 91], ，但它们作用于根本不同的结构层级：纽结不变量描述三维流形内的 对象，而我们的 WRT 不变量描述三维流形本身。当三维流形为 S^3且 WRT 不变量包含链结插入 [Tur94]时，可将琼斯多项式作为特殊情形恢复。

这种维度差异体现在资源扩展上。基于辫子的算法需要 n 个量子比特，才能计算由 $(n-1)$ 股辫子构成的辫子闭包的琼斯多项式，其量子比特数随辫宽线性增长。我们的算法需要 $2\lceil\log_2 N\rceil+m+1$ 个量子比特，才能计算层级为 N、采用 m 次 skein 插入的表示中的 WRT 不变量，呈现出随模参数对数增长的趋势（ $m+1$ 个辅助量子比特的数量随插入次数而非表示维度增长）。例如，使用 14 个数据量子比特时，基于辫子的方法可处理 13 股辫子，而我们的方法可处理 $N=127$ （维度为 16,129）。量子比特效率方面的这一指数级优势，反映了几何结构的差异：在 $\mathbb{Z}_N^2$ 上进行模运算，与辫群的斐波那契表示。

除了用于纽结不变量的基于辫子的方案以及我们针对环面丛的 skein 代数嵌入之外，三维流形不变量的其他计算框架还包括量子 Teichm¨uller 理论 [CF99、AK14], ，该理论利用 Faddeev 量子二对数通过态积分计算 WRT 型不变量；以及由 Regina [Bur13] 和 SnapPy [CDGW], 等计算拓扑软件实现的基于三角剖分的方法，这些方法能够计算一般三维流形的 Turaev-Viro 不变量，但代价是最坏情况下的指数复杂度。这些方案涉及不同的适用范围和数学框架：量子 Teichm¨uller 理论提供了

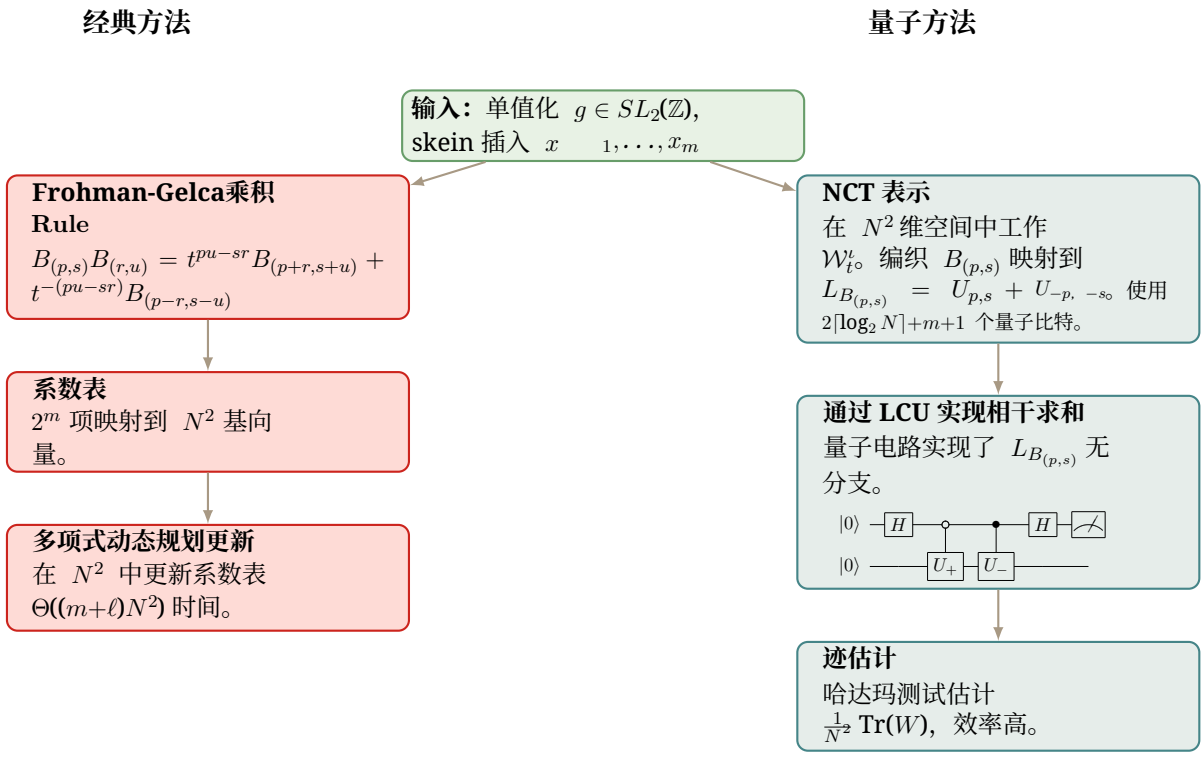


图2：WRT计算的经典方法与量子方法。**经典方法（左）：** Frohman–Gelca二项规则在概念上生成 2^m 个项，但这些项会映射到一张 N^2 系数表，从而支持多项式时间动态规划，并使用 $\Theta(N^2)$ 空间。**量子方法（右）：** 通过将 skein 代数嵌入非交换环面的对称子代数 $\mathcal{W}_t^{\iota}$ 中，我们利用线性组合酉算子实现相干求和，将每次乘法实现为相干求和，使用 $O(\log N)$ 个数据量子比特以及 $m+1$ 个辅助量子比特——相较于经典存储器所需的 $\Theta(N^2)$，空间需求呈指数级减少。

一种以双曲几何和体积猜想为基础的互补视角，而三角剖分方法则以计算效率为代价，实现了更高的普适性（适用于任意三维流形）。我们对环面丛的研究利用了其特殊结构：在该结构下，skein代数嵌入非交换环面；而在单位根处，后者变为有限维，从而能够进行一般三维流形无法实现的多项式时间计算。

1.4 论文组织结构

第 2 节奠定数学基础：Witten-Reshetikhin-Turaev不变量、映射环面以及考夫曼括号斯凯因代数。第3节介绍核心数学框架——将 skein代数嵌入非交换环面的对称子代数 $\mathcal{W}_t^{\iota}$ 中——并提出经典动态规划算法，利用该嵌入所提供的固定 N^2 维结构，实现 $\Theta((m+\ell)N^2)$ 时间复杂度和 $\Theta(N^2)$ 空间复杂度。第 4 节构建量子算法，推导二项算子分解，并通过酉算子的线性组合实现该分解，使总量子比特数的增长达到 $O(\log N + m)$。第 5 节证明 FG 系数计数问题是 #P 完全问题，并针对这一困难问题提出具有计算优势的量子算法。第 6 节总结其对量子算法设计和拓扑量子计算的启示。另有三个附录提供补充背景：附录 A 介绍无位置表示方法，

附录 B 介绍映射环面和模作用的背景，附录 C 则说明我们的算法与 $SU(2)_k$ 任意子模型之间的精确对应关系。

我们首先建立计算问题所依据的数学基础：我们希望计算的拓扑对象（WRT 不变量、映射环面）和代数结构（skein代数）。

2 数学基础

我们建立三项数学基础：Witten-Reshetikhin-Turaev不变量、我们所研究的环面丛（映射环面）类，以及考夫曼括号斯凯因代数。尽管计算一般三维流形的 WRT 不变量是#P-困难的 [AL17], 环面丛由于其特殊的代数结构，可以高效计算。

2.1 Witten-Reshetikhin-Turaev不变量

拓扑量子场论（TQFT）提供了一个数学框架，用于从量子力学结构中提取流形的拓扑不变量。1989年，Witten 证明，纽结的琼斯多项式可以通过规范群为 SU(2) 的三维陈-西蒙斯规范理论来理解 [Wit89]。这种路径积分方法不仅为琼斯多项式提供了新的视角，还产生了任意闭三维流形的不变量。

Reshetikhin 和 Turaev [RT91] 利用量子群表示论构造了这些不变量的严格数学定义，绕开了路径积分的分析难题。他们的构造产生了如今所称的 Witten-Reshetikhin-Turaev（WRT）不变量——以层级 k （或等价地，以$N = k + 2$ 为参数，其中 $t = e^{2\pi i/N}$ 是单位根）的三维流形拓扑不变量。

定义 2 （Witten-Reshetikhin-Turaev 拓扑量子场论）。层级为 k 的（$2 + 1$）维 ***WRT*** 理论赋予：

$$\textit{To each surface } \Sigma: \quad \textit{a finite-dimensional Hilbert space } V_N(\Sigma) \tag{1}$$

$$\textit{To each cobordism } M: \quad \textit{a linear map } Z(M): V_N(\partial_{in} M) \to V_N(\partial_{out} M) \tag{2}$$

$$\text{对每个闭三维流形 } M\text{：一个复数 } Z_N(M) \in \mathbb{C} \tag{3}$$

这些赋值满足拓扑量子场论公理 *[Ati88]*：在粘合映射复合下具有函子性，在不交并下具有乘法性，并满足归一化条件（空流形映射为 $\mathbb{C}$）。分解选择的无关性由这些公理保证 *[Tur94]*。

对于环面 $\Sigma_{1,\,0} = T^2$，标准的 SU(2) WRT 希尔伯特空间 $V_N(\Sigma_{1,\,0})$ 的维数为 $N - 1$（对应于层级为 $k = N - 2$ 的可积表示）。然而，在本文中，我们采用 N^2 维的 Weyl（非交换环面）表示，通过归一化迹来计算迹型振幅。这一 N^2 表示允许环面的映射类群 作用——该群由保向微分同胚的同伦类构成——并且同构于 $SL_2(\mathbb{Z})$ [FM11]。附录 A 解释了为什么这种无位置表示有利于量子计算。

该拓扑量子场论结构在映射环面上的特化如下。圆柱 $T^2 \times [0, 1]$ 是一个从 T^2 到自身的协边；为了构造映射环面 M_g，我们通过单值化 $g \in SL_2(\mathbb{Z})$ 将边界分量粘合起来。拓扑量子场论将一个经 g 扭曲的圆柱映射为线性映射 $\rho(g) : V_N(T^2) \to V_N(T^2)$，称为 模表示。当我们通过识别入射边界与出射边界来闭合这个协边时，赋值 (3) 给出 WRT 不变量 $Z_N(M_g)$，它

根据函子性等于迹 Tr(ρ(g))。沿纤维方向插入 skein 元素 $x_1, \ldots, x_m$ 后，这一结果可推广为

$$Z_N(M_g; x_1, \ldots, x_m) = \mathrm{Tr}(\rho(g) L_{x_m} \cdots L_{x_1}),$$

定义 1 的迹公式。

2.2 映射环面

映射环面是由单值化 $g \in SL_2(\mathbb{Z})$ 构造的、以 S^1 为底空间的环面丛。我们将计算其 WRT 不变量的三维流形正是这类流形。

定义 1（映射环面）。对于 $g \in SL_2(\mathbb{Z})$，映射环面是三维流形

$$M_g = \frac{T^2 \times [0,1]}{(x,1) \sim (g \cdot x, 0)},$$

其中 g 通过标准线性作用作用于 $T^2 = \mathbb{R}^2/\mathbb{Z}^2$。三维流形 M_g 是通过沿由 g 诱导的微分同胚粘合圆柱 $T^2 \times [0,1]$ 的边界环面得到的，该微分同胚称为单值化 *[Hatnd]*。

2.3 考夫曼括号斯凯因代数

斯凯因代数为迹公式（定义 1）中的乘法算子 L_{x_i} 提供了代数框架。对于曲面 Σ，考夫曼括号 skein 代数 $K_N(\Sigma)$ 由框架链环的同伦类生成（链环配有连续选取的法向量，或等价地，配有嵌入环带），乘法由堆叠定义，其关系则体现考夫曼括号。

定义 4 (考夫曼括号 skein 代数)。考夫曼括号 skein 代数 $K_N(\Sigma)$ 是由 $\Sigma \times [0,1]$ 中框架链环的同伦类生成的 $\mathbb{C}$-模，并对以下斯凯因关系取商：

$$\langle L_+ \rangle = A\langle L_0 \rangle + A^{-1}\langle L_\infty \rangle \tag{4}$$

$$\langle L \cup \bigcirc \rangle = (-A^2 - A^{-2})\langle L \rangle \tag{5}$$

其中 $A = e^{\pi i/N}$、L_+、L_0、L_∞ 表示仅在一个交叉处不同的三个链环（其中 L_0、L_∞ 是两种光滑化）。乘法由沿 $[0,1]$ 方向堆叠定义。

注 1 (参数约定)。本文中，考夫曼括号 *skein* 代数采用两种记号形式。对于一般的非零参数，我们遵循通用约定，记作 $K_t(\Sigma)$，其中 $t \in \mathbb{C}^*$ 为斯凯因参数（在量子环面模型中通常记作 $t = e^{2\pi i\theta}$）。当专门取单位根层级 层级 时，我们记作 $K_N(\Sigma)$，表示考夫曼括号参数 A 为本原 $2N$ 次单位根且 N 为奇数时的特化。在此情形下，记录平方参数也很方便

$$t := A^2,$$

使得 t 是一个本原的 N 次单位根；等价地，如果 $t = e^{2\pi i\theta}$，那么 $\theta = \frac{1}{N}$。 —

对于环面 $\Sigma_{1,0}$，$K_N(\Sigma_{1,0})$ 的元素对应于环面上曲线的线性组合。每条不可缩简单闭曲线在同伦意义下由其斜率 $(p, s) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ 唯一确定，表示绕子午线的 p 圈数和绕经线的 s 圈数；数对 (p, s) 和 $(-p, -s)$ 表示定向相反的同一条曲线。

定义 5 (本原对)。 数对 $(p, s) \in \mathbb{Z}^2$ 若满足 互素 条件 $\gcd(p, s) = 1$，则称为本原对。本原对对应于环面上的简单（无自交）闭曲线。

定义 6 （切比雪夫多项式）。 切比雪夫多项式（采用迹归一化）定义为 $T_0 = 2$、 $T_1 = x$ 和 $T_{n+1} = x \cdot T_n - T_{n-1}$。

定义 7 （缠绕记号 [FG00]）。 对于 $(p,\ s) \in \mathbb{Z}^2$，其中 $d = \gcd(p,\ s)$，缠绕元素为

$$(p, s)_T := T_d\big((p/d, s/d)\big),$$

其中， $\gamma =$ $(p/d, s/d)$ 是本原曲线，而 T_d（γ） 表示在 ***skein*** 元 γ 上使用 ***skein***代数乘法计算的切比雪夫多项式： T_0（γ） $= 2$、 T_1（γ） $= \gamma$，以及 T_{d+1}（γ） $=\gamma \cdot T_d$（γ） $- T_{d-1}$（γ）。

关键的代数结构是 Frohman–Gelca 乘积法则，该法则将任意两个缠绕元素的乘积表示为恰好两项之和：

命题 1 （二项乘法 [FG00]）。 在 $K_t(\Sigma_{1,\ 0})$ 中， $t \in \mathbb{C}^*$，对于任意 $(p,\ s)$、$(r,\ u)$ $\in \mathbb{Z}^2$：

$$(p, s)_T \cdot (r, u)_T = t^{pu-sr}(p + r, s + u)_T + t^{-(pu-sr)}(p - r, s - u)_T.$$

这种二项结构对于高效计算至关重要：它限制了 skein 元素相乘时项数的增长，从而使第3节和第4节中提出的多项式时间算法得以实现。

注 2。 有关 $K_N(F)$ 构造的详细说明，请参阅我们此前与 ***Frohman*** *[AF16]* 合作完成的工作。

2.4 复杂性概况

一般三维流形的 WRT 不变量 [AL17] 和任意链环的琼斯多项式 [JVW90] 都具有 #P 困难性，这自然引出一个问题：是什么结构性质使环面丛易于处理?

答案在于上述确立的代数结构。以下三种性质共同实现了高效计算：

1. **二项乘法**。 Frohman–Gelca 乘积法则（命题 1）在每次乘法中恰好生成两项，从而限制中间表达式的增长。2. **有限维嵌入**。 在 N 次单位根处，skein 代数嵌入到一个固定的 N^2 维空间中——第3节将通过 Frohman–Gelca 嵌入定理对此加以形式化。3. **模运算**。 指标按模 N 化简，避免无限增长，并确保所有计算始终处于有限基之内。

这些结构性质将一个表面上呈指数复杂的问题——2^m 项来自 m 次乘法——转化为适合采用多项式时间动态规划和高效量子电路处理的问题，相关方法将在第 3 节和第 4 节中介绍。

3 数学框架：对称子代数结构

在确立了拓扑和代数对象（第 2 节）之后，我们现在介绍能够实现高效计算的数学框架：将skein代数嵌入非交换环面的对称子代数。通过 skein 代数乘法计算 WRT 不变量的关键挑战在于，Frohman-Gelca 乘积规则会生成 2^m项，其数量随插入次数呈指数增长 m。然而，这些项并非彼此独立：它们都属于一个 N^2 维的编织代数基。计算上的问题是，能否在这个固定维数的结构中高效地组织这一指数级展开。

答案在于将 skein代数 $K_N(\Sigma_{1,\ 0})$ 嵌入非交换环面 $\mathcal{W}_t$ 的对称子代数中。Frohman 和 Gelca[FG00] 最初在 WRT 拓扑量子场论框架 [RT91], 下研究特征簇时建立了这一嵌入，它恰好提供了实现高效计算所需的代数结构。具体而言，它带来：

1. 固定的 N^2 维表示（支持经典表存储）
2. 统　一的二项算子分解（支持量子线性组合酉算子的实现　　n)
3。环境代数中的单项乘法（支持高效更新　　s)

本节建立嵌入定理（定理 1），并阐述其对经典与量子算法的计算意义。全文中，我们强调这种表示的“无赋值”特性——它无需选择中心特征，因此能产生不受局部化选择影响的通用计算结构。附录 A 详细比较了基于赋值的途径，附录 C 则从 $SU(2)_k$ 任意子的角度说明其物理诠释。

3.1 非交换环面

其核心结构是非交换环面代数，其乘法形式尤为简单，适用于经典与量子计算。

定义 8 (非交换环面 [Rie81])。 非交换环面代数 $\mathcal{W}_t$ 是由酉元 l、m 生成的通用 C^*-代数，满足：

$$m \cdot l = t^2 \cdot l \cdot m$$

其中 t是一个本原 N 次单位根。本文中，我们取 $t = e^{2\pi i/N}$，与注 *1* 一致。

代数 $\mathcal{W}_t$ 也称为参数为 t 的量子环面。它是交换 C^*-代数 $C(T^2)$ 的一种变形，后者由二维环面上的连续函数构成：当 $t = 1$ 时，关系式$ml = t^2lm$ 变为 $ml = lm$，从而恢复 $C(T^2)$，其稠密子代数为 $\mathbb{C}[l^{\pm1}, m^{\pm1}]$（劳伦多项式）。对于 $t = e^{2\pi i\theta}$ 且 θ 为无理数的情形， $\mathcal{W}_t$ 是无理旋转代数 A_θ，也是非交换几何 [Rie81]中的基本对象。我们的选择 $t = e^{2\pi i/N}$ （有理 $\theta = 1/N$）得到一个有限维商代数：施加条件 $l^N = m^N = 1$ 后，dim $\mathcal{W}_t = N^2$，这是计算上易于处理的层级-N WRT 不变量情形。

这个代数有一个自然基，它将直接关联到我们的 skein 代数嵌入：

命题　　2 (韦尔基)。 $\mathcal{W}_t$ 的基为 $\{e_{p,s} = t^{-ps}l^pm^s : \ p, s \in \mathbb{Z}_N\}$，其乘法　　：

$$e_{p,s} \cdot e_{r,u} = t^{pu-sr}e_{p+r,s+u}$$

单项乘法结构源自 Weyl算子 [Rie81] 的交换关系。

注释 3 （单项乘法结构）。 韦尔基的关键计算优势在于，乘法恰好产生一个带有相位因子的基元素：$e_{p,\ s}\cdot e_{r,\ u}=t^{pu-sr}e_{p+r,\ s+u}$。这与产生两个基元素的双项 *Frohman-Gelca*乘积（命题 *1*）形成对比。 $\mathcal{W}_t$ 中的单项结构正是实现高效经典动态规划更新（公式 (6)）的关键。

3.2 对称子代数与 skein 代数嵌入

定义 9 （反向定向对合）。 由 $\iota(e_{p,\ s})=e_{-p,\ -s}$ 定义的对合 $\iota\colon\ \mathcal{W}_t\to\mathcal{W}_t$ 生成对称子代数：

$$\mathcal{W}_t^{\iota}=\{w\in\mathcal{W}_t:\iota(w)=w\}$$

对合 ι 揭示了一种基本对称性，而令人惊讶的是，这种对称性恰好对应于 skein 代数的代数结构。由此得到主要的结构性结果：

定理 1 （Frohman–Gelca嵌入 [FG00]）。 设 $t\in\mathbb{C}^{\times}$，并设 $\mathcal{W}_t$ 为以 $\{e_{p,s}\}_{(p,s)\in\mathbb{Z}^2}$ 为基、乘法为 $e_{p,\ s}e_{r,\ u}\ =\ t^{\,pu-sr}\,e_{p+r,\ s+u}$的非交换环面。令 $\iota\colon\ \ \mathcal{W}_t\ \to\ \mathcal{W}_t$ 为对合 $\iota(e_{p,\ s})=e_{-p,\ -s}$，并以 $\mathcal{W}_t^{\iota}$ 表示其不变子代数。存在一个代数同构

$$\phi_t\colon\ K_t(\Sigma_{1,0})\xrightarrow{\ \cong\ }\mathcal{W}_t^{\iota}$$

在穿线元素上的刻画为

$$\phi_t\big((p,s)_T\big)\ =\ e_{p,s}+e_{-p,-s}\qquad \textit{for all } (p,s)\in\mathbb{Z}^2.$$

嵌入定理对一般的 $t\in\mathbb{C}^{\times}$ 成立。对于算法应用，我们将其特化到单位根，从而得到适用于计算的有限维表示。

推论 1 (奇数阶单位根特化**)**。 设 A 是一个本原 $2N$ 次单位根，其中 N 为奇数，并令 $t=A^2$（因此 t 的阶为 N）。令$U=e_{1,0}$, $V=e_{0,1}$，并构造标准的 $N\times N$“时钟–位移”商/表示 ρ_N: $\mathcal{W}_t\to$矩阵$_N(\mathbb{C})$，其定义通过施加关系 $U^N=V^N=\mathbf{1}$ 得到。于是：

1. $\{(p,s)_T\}$ 在 $\rho_N\circ\phi_t$ 下的像仅取决于 (p,s) 模 N（至多相差一个仅依赖于 N 的整体归一化因子），而对合 $(p,s)\mapsto(-p,-s)$ 将互为相反的类对应起来。

2. 因此， $K_t(\Sigma_{1,0})$ 的像是 $\mathrm{Mat}_N(\mathbb{C})$ 中由 $\{\,U^pV^s+U^{-p}V^{-s}\mid(p,s)\in(\mathbb{Z}/N\mathbb{Z})^2\,\}$ 张成的 ι-不变子代数，其维数为

$$\dim\mathrm{Im}(\rho_N\circ\phi_t)\ =\ \frac{N^2+1}{2}.$$

证明。 第一个断言由周期性 $U^N=V^N=\mathbf{1}$得出，这意味着 $U^{p+N}=U^p$和$V^{s+N}=V^s$。对于维数计数：当 N为奇数时， $\mathbb{Z}_N^2$上的对合 $(p,s)\mapsto(-p,-s)$ 恰好有一个不动点，即 $(0,0)$，因为 $2p\equiv0$（模 N）意味着当 N为奇数时有 $p=0$（对 s亦然）。其余 N^2-1个元素分成 $(N^2-1)/2$个大小为 2 的轨道。每个轨道为对称子代数贡献一个基元素 $U^pV^s+U^{-p}V^{-s}$，因此总维数为 $1+(N^2-1)/2=(N^2+1)/2$。 □

备注 4 (范围)。 对于一般的 t，定理 *1* 是无限维代数之间的一个同构。推论 *1* 中的有限维表述源于单位根特化 $t = e^{2\pi i/N}$，它给出了一个商表示；*skein*代数 $K_N(\Sigma_{1,0})$ 本身仍然是无限维的。

嵌入定理带来了直接的算法后果。将编织元素表示在 $\mathcal{W}_t^\nu$ 的韦尔基中，我们就能在固定的 N^2 维系数表格中追踪 Frohman-Gelca 展开的所有 2^m 项。现在，我们介绍利用这一结构的经典动态规划算法。

3.3 算法概述

关键在于，尽管 Frohman-Gelca 乘积规则在概念上会生成 2^m 项，但这些项都映射到一个固定的 N^2 维空间。这种维数约化是因为我们在单位根 $t = e^{2\pi i/N}$ 处进行运算，它会引入模运算：虽然 skein代数 $K_N(\Sigma_{1,\,0})$ 最初以本原对 $(p,\ s) \in \mathbb{Z}^2$（不受限制的整数）为索引，但嵌入到 $\mathcal{W}_t^\nu$ 后，所有索引都会对 N 取模。因此，我们可以维护一个系数表格C： $\mathbb{Z}_N^2 \to \mathbb{C}$，并针对每次编织乘法高效地更新它。

对于由本原对 $v_i = (p_i, s_i) \in \mathbb{Z}^2$ 索引的 skein 元素 $x_i = B_{v_i}$（在单位根处化简为 $\mathbb{Z}_N^2$ 中的代表元），我们计算：

$$P_m = \prod_{i=1}^{m} L_{B_{v_i}} = \sum_{w \in \mathbb{Z}_N^2} C_m(w) U_w$$

其中，$U_w := e_w$ 表示命题 2 中的 Weyl 基算子。

3.4 动态规划更新

从 $C_0(0,0) = 1$ 和 $C_0(w \neq (0,0)) = 0$ 开始，我们对每个 skein 元素 $v = v_{k+1}$执行如下更新：

$$\boxed{C_{k+1}(w) = t^{\langle v,w\rangle} C_k(w - v) + t^{-\langle v,w\rangle} C_k(w + v)} \quad \text{(all indices modulo } N\text{)} \tag{6}$$

其中，$\langle (p,s),(r,u)\rangle = pu - sr$ 是辛形式（回忆一下 $t = e^{2\pi i/N}$）。对于固定的 skein 元素 $v = (p,s)$，我们定义相位网格 Φ： $\mathbb{Z}_N^2 \to \mathbb{C}$，使得 $\Phi(w) = t^{\langle v,w\rangle}$，从而更新式 (6) 变为 $C_{k+1}(w) = \Phi(w) \cdot C_k(w - v) + \Phi(w) \cdot C_k(w + v)$。

定理 2 (经典算法的复杂度)。 算法 *1* 计算环面丛的 *WRT* 不变量，其时间复杂度为 $\Theta(mN^2)$（用于动态规划阶段），加上 $\Theta(\ell N^2)$（用于计算单值化作用），再加上 $\Theta(N^2)$（用于计算迹），总时间复杂度为 $\Theta((m+\ell)N^2)$，空间复杂度为 $\Theta(N^2)$。

证明。 m 次更新中的每一次都会应用 Frohman-Gelca 乘积规则（命题 1），为每个已有系数生成两项。更新（6）处理系数表 C 的全部 N^2 个条目： $\mathbb{Z}_N^2 \to \mathbb{C}$，对每个条目执行：一次相位计算 $t^{\langle v,\ w\rangle}$（通过预计算查找表实现常数时间，或进行 $O(\log N)$ 的模幂运算），两次系数查找 $C(w \pm v)$（使用模索引运算），两次复数乘法，以及一次复数加法。因此，每次更新需要 $\Theta(N^2)$ 次运算，动态规划阶段总共需要 $\Theta(mN^2)$ 次运算。

单值化作用 $\rho(g)$ 通过复合 ℓ 个生成元计算得出，其中每个生成元 $\rho(S)$ 或 $\rho(T)$ 都通过结构化运算作用于 N^2 维空间（对 S 进行二维傅里叶变换，

算法 1 环面丛 WRT 不变量的经典动态规划

输入： 本原对 $v_1, \ldots, v_m \in \mathbb{Z}^2$（模 N 化简），单值化 $g \in SL_2(\mathbb{Z})$

输出： WRT 不变量 $Z_N(M_g; B_{v_1}, \ldots, B_{v_m})$

初始化 $C : \mathbb{Z}^2{}_N \to \mathbb{C}$ 当 $C(0, 0)$ 时为 $\leftarrow 1$，否则为 $C(w) \leftarrow 0$

对于 $i = 1$ 至 m，**执行**

  令 $v = v_i = (p, s) \in \mathbb{Z}_N^2$

  计算相位网格 $\Phi(w) = t^{\langle v,\ w\rangle}$ 对所有 $w \in \mathbb{Z}^2{}_N$

  构造循环移位 $C^+(w) = C(w - v)$，$C^-(w) = C(w + v)$ （索引对 N 取模）

  对所有 w 更新 $C(w) \leftarrow \Phi(w) \cdot C^+(w) + \Phi(w) \cdot C^-(w)$

结束循环

构造算子 $P = \sum_{w \in \mathbb{Z}_N^2} C(w)\, e_w$ 在韦尔基中

计算 $Z_N = \mathrm{Tr}\big(\rho(g) \cdot P\big)$

返回 $Z_N(M_g; B_{v_1}, \ldots, B_{v_m})$

对 T 进行对角矩阵与置换矩阵乘积运算），每次运算的代价为 $\Theta(N^2)$。由此可得单值化相位的 $\Theta(\ell N^2)$。最后，迹计算评估 $Z_N = \sum_{w \in \mathbb{Z}_N^2} C_m(w) \cdot \tau_g(w)$，其中 $\tau_g(w) = \mathrm{Tr}(\rho(g)\, e_w)$ 是从预先计算的单值化中提取的，总耗时为 $\Theta(N^2)$。空间占用主要来自存储 C 的 N^2 个复系数。

□

经典算法通过显式构造完整的系数表格，实现 $\Theta((m + \ell)N^2)$ 时间复杂度。现在我们转向量子算法，它以相干性换取空间：它不再显式存储 N^2 个复系数，而是在 $O(\log N)$ 个数据量子比特中维持叠加态——数据量子比特数按对数级增长，同时保持多项式时间的迹估计。

在继续介绍量子算法之前，我们先说明经典计算的一种替代性物理诠释，它与拓扑量子计算相关。

注 5 (拓扑量子场论视角：任意子编织的诠释)。 从拓扑量子场论的角度来看，*[Ati88, Wit89, RT91],* 经典动态规划算法可以理解为在$(2 + 1)$维拓扑量子场论中模拟任意子编织。每个纽结 ***skein*** 元 $B_{(p,s)}$都对应于产生一对任意子，其量子数由(p, s)确定，而左乘 $L_{B_{(p,s)}}$ 则实现编织操作。系数表 C： $\mathbb{Z}_N^2 \to \mathbb{C}$ 记录了不同任意子融合结果的振幅。这一视角将我们的方法与更广泛的拓扑量子计算框架联系起来 *[BP08],*，在该框架中，***WRT*** 不变量的求值通过环面希尔伯特空间上的模函子操作实现。

4 量子算法

在建立对称子代数结构（第3节）后，我们现在来构建量子算法。其关键基础是 skein 元素的一致双项分解；我们先推导该分解，再通过酉算子的线性组合（LCU） [CW12]加以实现。经典算法可在 N^2 表格上高效管理 2^m 项，而我们的量子方法仅使用 $O(\log N)$ 个数据量子比特和 $m + 1$ 个辅助量子比特来维持相干叠加，以牺牲内存为代价，直接估计迹，而无需生成完整的系数表。

4.1 算子表示与双项分解

为了在量子情形下实现编织乘法，我们将代数嵌入转换为算子语言。关键在于将 skein 元素表示为作用于非交换环面上的线性算子，再将其分解为可由量子实现的门。

定义 10 (左乘　　算子)。对于 $x \in \mathcal{W}_t$，定义 L_x：$\mathcal{W}_t \to \mathcal{W}_t$ 为 $L_x(y) = x \cdot y$　　.

Theo引理 3 （双项线性组合酉分解）。对于每个编织生成元 $B_{(p,s)} \in \mathcal{W}_t^{\iota}$　　：

$$L_{B_{(p,s)}} = U_{p,s} + U_{-p,-s}$$

其中$U_{p,\ s}$ 为带相位置换酉算子：

$$U_{p,s} : e_{r,u} \mapsto t^{pu-sr} e_{p+r,s+u}$$

证明。根据 Frohman-Gelca 嵌入（定理 1），每个编织生成元映射为 $B_{(p,s)} = e_{p,\ s} + e_{-p,\ -s} \in \mathcal{W}_t^{\iota}$。对于任意基元素 $e_{r,\ u} \in \mathcal{W}_t$，我们计算其左乘作用：

$$\begin{aligned} L_{B_{(p,s)}}(e_{r,u}) &= B_{(p,s)} \cdot e_{r,u} = (e_{p,s} + e_{-p,-s}) \cdot e_{r,u} \\ &= e_{p,s} \cdot e_{r,u} + e_{-p,-s} \cdot e_{r,u} \\ &= t^{pu-sr} e_{p+r,s+u} + t^{(-p)u-(-s)r} e_{-p+r,-s+u} \quad \text{(Proposition 2)} \\ &= U_{p,s}(e_{r,u}) + U_{-p,-s}(e_{r,u}) \end{aligned}$$

其中 $U_{p,\ s}$:$e_{r,\ u} \mapsto t^{pu-sr} e_{p+r,\ s+u}$。

为验证 $U_{p,\ s}$ 是酉算子：指标映射 $(r,\ u) \mapsto (r+p,\ u+s)$ 是 $\mathbb{Z}_N^2$ 上的双射（其逆映射为 $(r,\ u) \mapsto (r-p,\ u-s)$），且相位因子满足 $|t^{pu-sr}| = 1$，因为 $t = e^{2\pi i/N}$ 位于单位圆上。因此，$U_{p,\ s}$ 以模长为 1 的相位置换标准正交基 $\{e_{r,u}\}$，这正是酉算子的特征。 □

对称子代数结构至关重要：虽然完整的非交换环面具有单项乘法，但只有对称子代数提供了与 skein代数的 Frohman-Gelca 规则相匹配的双项分解。这种精确对应关系使我们能够将编织乘法实现为相干量子和。

注释 6. 经典与量子算法利用相同的代数结构，但方式各不相同。在经典方法中，我们使用动态规划来更新一个 N^2 维系数表，高效地合并映射到相同基元素的 2^m 个概念项。在量子方法中，我们在 $O(\log N)$ 个量子比特中维持相干叠加，以空间换取直接估算迹的能力，而无需计算完整的系数表。当 N 较大且我们只需要迹、而不需要完整的算子表示时，量子方法尤其有优势。

4.2 通过哈达玛测试估算迹

双项分解使编织乘法能够通过线性组合酉算子实现。要提取 WRT 不变量——即迹——我们使用哈达玛测试 [CEMM98], ，这是一种用于估计内积和迹的基础量子子程序。

命题 3 (用于迹估计的哈达玛测试**)**。 给定一个作用于由 $\rho_{mix} = I/2^n$ 最大混合态制备的 n 量子比特~系统上的酉算子 U，归一化迹 $Z = \mathrm{Tr}(U)/2^n$ 可按如下方式估计。将一个辅助量子比特初始化为 $|0\rangle$，施加 H （哈达玛门），然后施加受控-U，再施加一次 H 。测量概率为:

$$P(measure\ |0\rangle) = \frac{1}{2}\left(1 + Re[\widetilde{Z}]\right), \tag{7}$$

$$P(measure\ |1\rangle) = \frac{1}{2}\left(1 - Re[\widetilde{Z}]\right). \tag{8}$$

~在最终的哈达玛门之前应用相位门 $S = diag(1, i)$，即可通过相同的测量提取 $Im[Z]$ 。

证明。 </style}初始量子态为 $\rho_0 = |0\rangle\langle 0| \otimes \rho_{\mathrm{mix}}$。经过量子电路（$H \otimes I$）$\circ$C-$U \circ (H \otimes I)$ 后，辅助量子比特基下最终密度矩阵的对角分量为:

$$\frac{1}{4}|0\rangle\langle 0| \otimes (I+U)\rho_{\mathrm{mix}}(I+U^\dagger) + \frac{1}{4}|1\rangle\langle 1| \otimes (I-U)\rho_{\mathrm{mix}}(I-U^\dagger).$$

在辅助量子比特上测得 $|0\rangle$ 的概率为:

$$P(0) = \frac{1}{4}\,\mathrm{Tr}[(I+U)\rho_{\mathrm{mix}}(I+U^\dagger)] = \frac{1}{4\cdot 2^n}\,\mathrm{Tr}[(I+U)(I+U^\dagger)].$$

展开（$I+U$）（$I+U^\dagger$） $= 2I + U + U^\dagger$，并利用 Tr($U^\dagger$) =Tr(U)，得到~$P(0) = \frac{1}{2}(1 +$Re[Tr(U)$/2^n$])。对于虚部，在最终的哈达玛门之前插入 $S =$diag$(1, i)$，会将干涉项中的（$I \pm U$）替换为（$I \pm iU$），从而得到 $P(0) = \frac{1}{2}(1 +$Im[Tr(U)$/2^n$])。 – □

注记 7 （与 DQC1 的关系）。 命题 *3* 正是 *DQC1*（单个干净量子比特确定性量子计算）协议 *[KL98, SJ08]*：一个干净辅助量子比特控制着作用于 n 个最大混合量子比特上的酉算子。最大混合输入至关重要，因为对于纯态，哈达玛测试 $|\psi\rangle$ 只能估计 $\langle\psi|U|\psi\rangle$——一个期望值——而迹$\mathrm{Tr}(U) = \sum_j \langle j|U|j\rangle$ 则需要对所有对角元素求和。最大混合态 $\rho_{mix} = I/2^n = \frac{1}{2^n}\sum_j |j\rangle\langle j|$ 隐式地实现了这一点，得到 $\mathrm{Tr}(U \cdot \rho_{mix}) = \mathrm{Tr}(U)/2^n$。一种等价的纯态表述使用最大纠缠态 $|\Phi\rangle = \frac{1}{\sqrt{2^n}}\sum_j |j\rangle_A|j\rangle_B$，其中 $\langle\Phi|(I_A \otimes U_B)|\Phi\rangle = \mathrm{Tr}(U)/2^n$，但这会使量子比特数量翻倍。

4.3 希尔伯特空间结构

注 8 （计算编码）。 由于 $\mathcal{W}_t$ 和希尔伯特空间 $\mathcal{H} = \mathcal{H}_p \otimes \mathcal{H}_s$ 同构为以 $\mathbb{Z}_N^2$ 为自然索引基的 N^2 维复向量空间，我们通过 $e_{p,\ s} \mapsto |p, s\rangle$ 将韦尔基元素编码为计算基态。在此编码下，左乘算子 $L_{e_{p,\ s}}$ 变为带相位置换（命题 *2*），可高效实现为量子门。

现在我们来刻画与对称子代数对应的子空间。

命题4 （对称子空间）。 对称 *skein* 元素对应于 $\mathcal{H}_p \otimes \mathcal{H}_s$ 中的量子态:

$$|\psi_{(p,s)}\rangle := \frac{1}{\sqrt{2}}(|p, s\rangle + |-p, -s\rangle) \quad for\ (p, s) \neq (0, 0),$$

其中 $|\psi_{(0,0)}\rangle := |0, 0\rangle$。这些张成一个维数为 $(N^2+1)/2$ 的子空间 $\mathcal{H}_{Skein} \subset \mathcal{H}_p \otimes \mathcal{H}_s$，其中$N$为奇数。

证明。对称子代数 $\mathcal{W}_t^\nu$ 由元素 $B_{(p,s)} = e_{p,s} + e_{-p,-s}$ 张成，其中 $B_{(p,s)} = B_{(-p,-s)}$（定理 1）。计算编码（注 8）将 $e_{p,s} \mapsto |p,s\rangle$ 映射为相应的归一化量子态 $|\psi_{(p,s)}\rangle = \frac{1}{\sqrt{2}}(|p,s\rangle + |-p,-s\rangle)$；当 $(p,s) \neq (0,0)$ 时，以及 $|\psi_{(0,0)}\rangle = |0,0\rangle$。注意，这些量子态彼此正交：$\langle\psi_{(p,s)}|\psi_{(p',s')}\rangle \neq 0$ 当且仅当 $(p',s') = \pm(p,s)$，因为 $|\psi_{(p,s)}\rangle$ 的计算基分量为 $\{|p,s\rangle, |-p,-s\rangle\}$。特别地，$|\psi_{(p,s)}\rangle = |\psi_{(-p,-s)}\rangle$，并且 $|\psi_{(0,0)}\rangle = |0,0\rangle$ 与所有满足 $(p,s) \neq (0,0)$ 的量子态正交。

对合 $(p,s) \mapsto (-p,-s)$ 将 $\mathbb{Z}_N^2$ 中的 N^2 个元素划分为若干轨道。对于奇数 N，只有 $(0,0)$ 是不动点（因为 $2p \equiv 0 \pmod N$ 推出 $p = 0$）。其余 $N^2 - 1$ 个元素组成 $(N^2-1)/2$ 对。每个轨道取一个代表元，得到 $\mathcal{H}_{\text{Skein}}$ 的 $(N^2+1)/2$ 个标准正交基向量，这与推论 1 一致。 □

4.4 模作用的量子电路实现

WRT 不变量 $Z_N(M_g;\, x_1, \ldots, x_m) = \mathrm{Tr}(\rho(g) L_{x_m} \cdots L_{x_1})$ 要求实现单值化 $g \in SL_2(\mathbb{Z})$ 对应的模作用 $\rho(g)$。我们将 g 表示为标准生成元 $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ 和 $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ 的词，因此只需实现 $\rho(S)$ 和 $\rho(T)$。

韦伊（亚稳表示）给出显式公式 [Sch09]。在 $\mathcal{H}$ 上，以计算基 $|p,\ s\rangle$ $(p,\ s \in \mathbb{Z}_N)$：[1]

$$\rho(S)\,|p,s\rangle \;=\; \frac{1}{N} \sum_{r,u \in \mathbb{Z}_N} t^{\,2(pu - sr)}\,|r,u\rangle, \tag{9}$$

$$\rho(T)\,|p,s\rangle \;=\; t^{\,s^2}\,|\,p{+}s,\ s\rangle, \tag{10}$$

其中 $t = e^{2\pi i/N}$。这是 $SL_2(\mathbb{Z})$ 的射影表示，实现了 WRT 理论的模函子结构 [RT91]。

注 9 (射影性)。 韦伊表示具有射影性：$\rho(S)$ 和 $\rho(T)$ 满足 $\rho(S)^4 = I$，但只能在相差标量相位的意义下生成 $SL_2(\mathbb{Z})$ *[Sch09]*。这种歧义不会影响我们的计算，因为迹 $\mathrm{Tr}(\rho(g)L_{x_m}\cdots L_{x_1})$ 在 $\rho(\cdot) \mapsto e^{i\phi}\rho(\cdot)$ 下保持不变。

现在我们将这些公式转化为量子电路。

引理 1 (模生成元电路)。 对于奇数 N 且满足 $t = e^{2\pi i/N}$，存在深度为-$O(\log^2 N)$[2]的量子电路来实现这些作用：

$$\rho(S) \;=\; (\mathrm{QFT}_N \otimes \mathrm{QFT}_N) \circ (\mathrm{NEG} \otimes I) \circ \mathrm{SWAP}, \qquad \rho(T) \;=\; \mathrm{QPHASE}_{s^2} \circ \mathrm{ADD}_{p \leftarrow p+s},$$

其中 QPHASE_{s^2}：$|p,s\rangle \mapsto t^{\,s^2}|p,s\rangle$ 是二次相位门，$\mathrm{ADD}_{p\leftarrow p+s}$：$|p,s\rangle \mapsto |p{+}s,s\rangle$，NEG：$|x\rangle \mapsto |-x\rangle$，而 QFT_N 是模 N 的 *QFT*。两个量子电路的深度均为 $O(\log^2 N)$。

证明。由于 N 是奇数，t^2 也是一个本原 N 次单位根，因此我们定义 $\mathrm{QFT}_N|j\rangle := \frac{1}{\sqrt{N}} \sum_{k \in \mathbb{Z}_N} t^{2jk}|k\rangle$。

对于 S-生成元，$(\mathrm{NEG} \otimes I) \circ \mathrm{SWAP}$ 将 $|p,s\rangle \mapsto |-s,p\rangle$ 映射为，并对每个寄存器应用 QFT_N，得到

$$(\mathrm{QFT}_N \otimes \mathrm{QFT}_N)|-s,p\rangle = \frac{1}{N} \sum_{r,u \in \mathbb{Z}_N} t^{-2sr} t^{2pu} |r,u\rangle = \frac{1}{N} \sum_{r,u \in \mathbb{Z}_N} t^{2(pu-sr)} |r,u\rangle,$$

[1]直观而言：忽略相位后，S 对应指标映射 $(p,s) \mapsto (-s,p)$，而 T 对应指标映射 $(p,s) \mapsto (p{+}s,s)$。在量子线路实现中，我们保留所有相位。[2]这个界是保守的；更准确地说，T 生成元在使用对数深度超前进位加法器 [DKRS06], 进行模乘时，需要深度 $O(\log N \cdot \log\log N)$；而 S 生成元进行双重量子傅里叶变换时，需要深度 $O(\log N)$。我们始终采用 $O(\log^2 N)$ 作为上界。

与 (9) 一致。对于 T-生成元，ADD$_{p\leftarrow p+s}$ 将 $|p,s\rangle \mapsto |p+s,s\rangle$ 映射为，随后二次相位给出 $t^{s^2}|p+s,s\rangle$，与 (10) 一致。深度上界由标准模算术基元 [DKRS06、RC18] 得出。

□

4.5 编织乘法的量子电路实现

WRT公式还要求实现编织乘法算子 $L_{B_{(p,s)}}$。根据定理 3，每个此类算子都可分解为 $L_{B_{(p,s)}} = U_{p,s} + U_{-p,-s}$，其中 $U_{p,s}$ 是带相位置换酉算子。我们首先给出 $U_{p,s}$的高效量子电路，然后通过酉算子线性组合（LCU）将它们组合起来。

引理2 (酉算子分解与电路深度**)。** 定理 *3* 中的每个带相位置换酉算子 $U_{p,s}$ 均可分解为 $U_{p,s} = \Phi_{(p,s)} \circ P_{(p,s)}$，其中：

- $P_{(p,s)}$ 是循环置换$(r,u) \mapsto (r+p \bmod N, u+s \bmod N)$，可通过基于量子傅里叶变换的模加法 *[Dra00]*以电路深度$O(\log N)$ 实现。
- $\Phi_{(p,s)}$ 是对角相位算子 $|r,u\rangle \mapsto t^{pu-sr}|r,u\rangle$，可通过模乘法 *[RC18]*以电路深度 $O(\log^2 N)$ 实现。

$U_{p,s}$ 的整体量子电路深度为 $O(\log^2 N)$。

证明。 该分解直接由 $U_{p,s}$ 的定义得出：

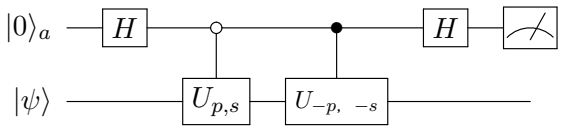
$$U_{p,s}|r,u\rangle = t^{pu-sr}|r+p,u+s\rangle = \Phi_{(p,s)} \circ P_{(p,s)}|r,u\rangle,$$

其中，相位使用原始坐标（r，u），因此必须在 $P_{(p,s)}$ 之后应用 $\Phi_{(p,s)}$。每次置换需要两次并行模加法，每次均可在深度为 $O(\log N)$ [Dra00] 的量子电路中实现。相位算子计算 $pu - sr \bmod N$ 并施加相应的旋转，所需深度为 $O(\log^2 N)$ [DKRS06, RC18]。组合这些操作后，总深度为 $O(\log^2 N)$。

□

在确立了 $U_{p,s}$ 的量子电路后，我们将它们组合起来，得到完整编织乘法算子的一种线性组合酉算子（LCU）实现。

定理 4 (LCU 实现**)。** 算子 $L_{B_{(p,s)}} = U_{p,s} + U_{-p,-s}$ 可由单辅助比特双分支酉算子线性组合实现为一个1_2 块编码：



证明。我们通过追踪量子电路对任意量子态的作用来验证块编码：

$$|0\rangle_a|\psi\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}(|0\rangle_a + |1\rangle_a)|\psi\rangle \tag{11}$$

$$\xrightarrow{\text{Controlled}} \frac{1}{\sqrt{2}}(|0\rangle_a U_{p,s}|\psi\rangle + |1\rangle_a U_{-p,-s}|\psi\rangle) \tag{12}$$

$$\xrightarrow{H\otimes I} \frac{1}{2}|0\rangle_a(U_{p,s}+U_{-p,-s})|\psi\rangle + \frac{1}{2}|1\rangle_a(U_{p,s}-U_{-p,-s})|\psi\rangle. \tag{13}$$

最后的哈达玛门使两个分支发生干涉，将所需的和 $L_{B_{(p,s)}} = U_{p,s} + U_{-p,-s}$置于 $|0\rangle_a$ 分量中，其系数为 $1/2$。因此，后选择得到 $L_{B_{(p,s)}}|\psi\rangle/2$，成功概率为 $\|L_{B_{(p,s)}}|\psi\rangle\|^2/4$。

□

4.6 总复杂度

量子算法通过重复进行哈达玛测试测量来估计 WRT 不变量。总成本取决于两个因素：每次电路执行的深度，以及达到目标精度所需的独立执行次数。我们将依次确定这两个因素，然后将它们结合起来。

定理 5 （每次执行的电路深度）。实现 $W = \rho(g)\, L_{x_m} \cdots L_{x_1}$的量子电路深度为 $D = O(\ell \log^2 N + m \log^2 N)$，其中 $\ell = |g|_{S,\,T}$是 g在生成元 S、T中的词长。

证明。模作用 $\rho(g)$ 需要 ℓ次应用 S 或 T 个生成元；根据引理 1，每个生成元都可用深度为 $O(\log^2 N)$ 的电路实现，因此总深度为 $O(\ell \log^2 N)$。 m 次编织乘法各需要一个 LCU块，其中带相位置换酉算子的深度为 $O(\log^2 N)$（根据引理 2），因此总深度为 $O(m \log^2 N)$。总计为 $D = O(\ell \log^2 N + m \log^2 N)$。 □

每次电路执行都会产生一个测量结果。现在我们来确定，要以高概率将迹估计到精度 ϵ，需要多少个独立样本。

命题5 （样本数）。设 $\widetilde{Z} = \mathrm{Tr}(W)/N^2$表示归一化迹。要以至少 $1-\delta$ 的成功概率将 $\widetilde{Z}$估计到加性精度 ϵ，需要进行 $n = O(\log(1/\delta)/\epsilon^2)$次独立的量子电路执行。

证明。每次 Hadamard测试测量（命题 3）都会得到 $X_i \in \{0,1\}$，其 $\mathbb{E}[X_i] = \frac{1}{2}(1 + \mathrm{Re}[Z])$。根据 Hoeffding不等式，经验均值 $\bar{X}_n$ 满足

$$\Pr\big(|\bar{X}_n - \mathbb{E}[X_i]| \geq \epsilon/2\big) \leq 2\exp\big(-n\epsilon^2/2\big).$$

令右侧等于 δ 并求解：$n = 2\log(2/\delta)/\epsilon^2 = O(\log(1/\delta)/\epsilon^2)$。于是，估计量 $2\bar{X}_n - 1$ 对 $\mathrm{Re}[Z]$ 的近似误差不超过 ϵ。通过相位门估计 $\mathrm{Im}[Z]$ 需要相同数量的样本，因此总样本数翻倍，但渐近复杂度不变。 □

将电路深度乘以样本数，即可得到量子计算的总成本。下述定理总结了基于采样的方法（适用于近期量子硬件）和量子振幅估计方法（对于容错硬件而言是最优的）。

定理 6 (WRT计算的总复杂度)。 设 M_g 是一个单值化为$g \in SL_2(\mathbb{Z})$ 且词长为 ℓ的环面丛，并设 $x_1, \ldots, x_m \in K_N(\Sigma_{1,0})$ 为 *skein* 元素。*WRT* 不变量 $Z_N(M_g; x_1, \ldots, x_m)$ 可被近似到加性精度 ϵ，且成功概率至少为 $1-\delta$，所用量子比特数为$2\lceil \log_2 N \rceil + m + 1$。令 $D = O(\ell \log^2 N + m \log^2 N)$ 表示基础电路深度（定理 *5*）。有两种方法可以实现这一点：

1. 采样（近期）： $O(\log(1/\delta)/\epsilon^2)$ 次独立运行，每次深度为 D，总操作数为

$$O\big(D \cdot \log(1/\delta)/\epsilon^2\big) = O\big((\ell \log^2 N + m \log^2 N) \cdot \log(1/\delta)/\epsilon^2\big).$$

2. 量子振幅估计 *[BHMT02]*（容错）： $O(\log(1/\delta))$ 次运行，每次深度为 $O(D/\epsilon)$，总操作数为

$$O\big(D \cdot \log(1/\delta)/\epsilon\big) = O\big((\ell \log^2 N + m \log^2 N) \cdot \log(1/\delta)/\epsilon\big).$$

抽样方法使用独立浅电路；量子振幅估计在每次运行中通过格罗弗式反射，相干地应用基础电路 $O(1/\epsilon)$ 次，因此需要更长的相干时间。

证明。 实现 $W = \rho(g)L_{x_m} \cdots L_{x_1}$ 的基础电路深度为 $D = O(\ell \log^2 N + m \log^2 N)$（定理 5）。量子比特数包括用于编码$\mathbb{Z}_N^2$和 m 的 p 与 s 寄存器各自所需的 $\lceil \log_2 N \rceil$ 个量子比特、用于 LCU 模块的 m 个辅助量子比特（每次编织乘法需要一个，因为将共享辅助量子比特的线性组合酉电路组合起来，无法得到乘积的正确块编码——见定理 4），以及用于哈达玛测试的一个干净量子比特（命题 3）。

对于抽样方法，每次 Hadamard测试测量都会产生一个独立样本。根据 Hoeffding不等式（命题5），只需 $O(\log(1/\delta)/\epsilon^2)$ 个样本，即可在置信度为 $1-\delta$ 的条件下，将迹估计到精度 ϵ。每个样本需要执行一次深度为 D 的量子电路，因此总操作数为 $O(D \cdot \log(1/\delta)/\epsilon^2)$。

对于量子振幅估计 [BHMT02], ，通过在每次运行中相干地应用基础电路（以及格罗弗反射）$O(1/\epsilon)$ 次，可达到精度 ϵ ，每次运行的电路深度为$O(D/\epsilon)$。要达到置信度 $1-\delta$，只需进行 $O(\log(1/\delta))$ 次独立运行。因此，总操作数为 $O(D \cdot \log(1/\delta)/\epsilon)$——在 ϵ 上实现了二次改进，但代价是需要 $O(1/\epsilon)$ 次相干受控重复，而非独立执行。 □

注 10 (硬件权衡)。 抽样方法适用于近期的 *NISQ* 硬件：每次量子电路执行彼此独立，便于直接进行误差缓解，且只需要较短的相干时间。量子振幅估计虽然能实现二次更优的精度缩放，但需要容错硬件能够在对基础电路进行 $O(1/\epsilon)$ 次连续应用并结合格罗弗式反射的过程中维持相干性。

4.7 完整量子算法

现在，我们将各个量子电路组件组合起来，构成完整的算法。下面的伪代码综合了模作用（引理 1）、线性组合酉算子分解（定理 4）和哈达玛测试（命题 3）；复杂度分析见定理 6。

算法 2 环面丛 WRT 不变量的量子算法 要求：单值化 $g \in \mathrm{SL}_2(\mathbb{Z})$、纽结 skein 元 $x_1, \ldots, x_m \in K_N(\Sigma_1, 0)$、精度 ϵ、置信度$1-\delta$确保：对 $Z_N(M_g; x_1, \ldots, x_m)/N^2$的估计，误差不超过 ϵ 1：将 $g = S^{a_1}T^{b_1} \cdots S^{a_k}T^{b_k}$分解为字长为 ℓ的形式（经典预处理） 2：设置样本数 $n \leftarrow O(\log(1/\delta)/\epsilon^2)$（命题5） 3：对于 $j = 1, \ldots, n$ 执行 4：初始化 $2\lceil \log_2 N \rceil + m + 1$ 个量子比特（数据寄存器、 m 个 LCU 辅助量子比特、哈达玛辅助量子比特） 5：对于 $i = 1, \ldots, m$ 执行 6：在辅助量子比特 a_i 上对 $L_{x_i} = U_{p_i, s_i} + U_{-p_i, -s_i}$ 应用 LCU 电路（定理 4） 7：结束循环 8：通过生成元电路应用模作用 $\rho(g)$（引理 1） 9：通过哈达玛测试进行测量（命题 3），记录 $X_j \in \{0, 1\}$10：结束循环_ ~ ~11：返回 $2X_n - 1$ 对 $\mathrm{Re}[Z]$ 的估计；使用相位门对 $\mathrm{Im}[Z]$ 重复执行 每次迭代的深度为 $O(\ell \log^2 N + m \log^2 N)$；总计： $O\big((\ell \log^2 N + m \log^2 N) \cdot \log(1/\delta)/\epsilon^2\big)$ 次运算。

定理 7 （算法正确性）。 算法 *2* 在 $2\lceil \log_2 N \rceil + m + 1$ 个量子比特上，输出归一化 *WRT* 不变量 $Z_N(M_g; x_1, \ldots, x_m)/N^2$ 的估计值，其加性误差至多为 ϵ，成功概率至少为 $1-\delta$。伪代码展示了基于采样的方法；定理 *6* 给出了

采样复杂度 $O(D \cdot \log(1/\delta)/\epsilon^2)$ 和量子振幅估计复杂度 $O(D \cdot \log(1/\delta)/\epsilon)$，其中 $D = O(\ell \log^2 N + m \log^2 N)$ 为基础电路深度。

证明。该算法构造 $W = \rho(g) L_{x_m} \cdots L_{x_1}$，其中 $L_{x_i} = L_{B_{(p_i,s_i)}}$ 表示由纽结 skein 元 x_i左乘。每个乘法算子都分解为 $L_{B_{(p_i,s_i)}} = U_{p_i,\ s_i} + U_{-p_i,\ -s_i}$（定理 3），并由双分支 LCU 电路（定理 4）精确实现。模作用 $\rho(g)$可通过生成元 S 和 T分解，这些生成元分别由引理 1 实现。哈达玛测试（命题 3）估计 $\mathrm{Tr}(W)/N^2$，根据定义，该值等于归一化 WRT 不变量。由于各个组成部分都得到了精确实现，正确性随之成立；定理 6 中的复杂度分析推导出了采样界和 QAE 界。

□

其关键成果是空间需求呈指数级降低：使用 $O(\log\ N + m)$ 个量子比特，而经典存储器需要 $\Theta(N^2)$，同时仍保持多项式时间。现在，我们转向一个相关但不同的计算问题：在这个问题中，量子叠加带来的不仅是空间效率，更是真正相较于经典方法的计算优势。从“计算迹”转向“精确提取特定系数”，会显著改变复杂性概况。

5 共线情形下的 FG 系数计数：困难性与节省空间的量子例程

虽然计算 WRT 不变量（迹）属于多项式时间，但从辫群乘积中精确提取特定系数则涉及不同的复杂度问题。现在，我们将这种区别形式化，并证明精确系数计数是 #P 完全的。

5.1 系数计数问题的动机与新颖性

系数提取问题自然源自 Frohman–Gelca 乘积法则，其计算挑战与迹计算有着根本区别。虽然 WRT 不变量可在多项式时间内计算，我们证明精确计数特定系数是 #P 完全的（定理 8），这意味着除非多项式层级坍缩，否则不存在多项式时间经典算法 [Tod91]。

我们以一种专门的量子例程（定理 9）补充这一经典计算困难性：该例程将第 4 节的线性组合酉算子框架加以改造，通过哈达玛测试提取矩阵元。由此实现了计算分离：尽管精确计数是 #P 完全的，仍可使用 $O(\log\ N)$ 个量子比特，在多项式时间内以加性精度估计系数。这与琼斯多项式的情形类似：其精确计算和乘法近似均为 #P-困难 [JVW90, Kup15], ，但量子算法仍能实现高效的加性近似 [AJL09]。与某些表示论中的系数问题不同，后者曾被猜想具有量子优势，后来却被经典算法匹配 [Pan25], ；我们问题的 #P 完全性则为精确计算提供了可证明的困难性保证。该问题与 #SIGNED-SUM 有关，而 #SIGNED-SUM 是 #P 完全的 #子集和问题的一种变体 [Val79],，因此本问题属于经典计数复杂性范畴。

环面上的 Frohman–Gelca（FG）乘积到求和规则指出

$$B_{(p,s)}\, B_{(r,u)} \;=\; t^{\,pu-sr}\, B_{(p+r,s+u)} \;+\; t^{-(pu-sr)}\, B_{(p-r,s-u)}, \qquad t = e^{2\pi i/N}.$$

当所有输入都共线，即具有 $v_i = (a_i, 0)$ 的形式时，辛形式 $\langle v_i, v_j \rangle = a_i \cdot 0 - 0 \cdot a_j$为零，因此所有 FG 相位都为 1。反复应用该规则即可得到对符号赋值进行展开的纯二进制展开，且不带权重。

注 11 (编码约定**)。** 在本节中，所有整数均采用标准二进制表示；输入规模为总位长 $\sum_i \lceil \log_2(|a_i|+1) \rceil + \lceil \log_2(|z|+1) \rceil$。

定义 11 (FG–系数计数（共线）**)。** 给定整数 $a_1, \ldots, a_m$ 和一个目标值 z，根据 *FG* 规则展开乘积 $\prod_{i=1}^{m} B_{(a_i,0)}$，其中指标视为整数（不对 N 取模）。定义 $c(z)$ 为该展开式中 $B_{(z,0)}$ 的系数。FG–系数计数 问题要求精确计算 $c(z)$。

在共线情形下，有如下显式恒等式

$$\prod_{i=1}^{m} B_{(a_i,0)} \;=\; \sum_{\varepsilon \in \{\pm 1\}^m} B_{\left(\sum_{i=1}^{m} \varepsilon_i a_i,\, 0\right)} \quad \Longrightarrow \quad c(z) \;=\; \#\Big\{\varepsilon \in \{\pm 1\}^m : \sum_{i=1}^{m} \varepsilon_i a_i = z\Big\}. \tag{14}$$

该恒等式表明，系数 $c(z)$ 统计了使用输入 $a_1, \ldots, a_m$ 的带符号组合得到目标和 z 的方法数。这正是 #SIGNED-SUM 计数问题（#子集和的一种带符号变体，其中每个元素都必须选取并赋予一个符号），这表明系数提取可能是计算困难的。现在我们将严格证明这一联系。

5.2 复杂度：通过保计数归约证明 #P 完全 n

为了确立系数计数的计算难度，我们从经典 #子集和问题的一个带符号变体进行归约。标准的 #子集和问题对各个子多重集计数（即选择包含哪些元素）；而与我们的辫群乘积相关的变体则对符号赋值计数（每个元素都必须取 $+$ 或 $-$符号）。定义：

$$\#\text{SIGNED-SUM}(a_1, \ldots, a_m; z) \;=\; \#\Big\{\sigma \in \{\pm 1\}^m : \sum_{i} \sigma_i a_i = z\Big\}.$$

这种带符号表述是 #P 完全的。为说明这一点，注意符号赋值 $\sigma \in \{\pm 1\}^m$与子集 $S \subseteq [m]$之间存在双射，对应关系为 $S = \{i : \sigma_i = +1\}$。在这一对应关系下，$\sum_i \sigma_i a_i = 2\sum_{i \in S} a_i - \sum_i a_i$，因此 #SIGNED-SUM($a_1$, ..., a_m; z) =#子集和(a_1, ..., a_m; t)，其中当该数量为整数时，$t = (z + \sum_i a_i)/2$，否则为零。由于 #子集和是 #P 完全的，[Val79], ，#SIGNED-SUM 也是如此。

定理 8 (FG–系数计数是 #P 完全**)。** 定义 *11* 中的问题在保数归约下是 *#P* 完全的。

证明。 为证明其属于 #P，我们给出一台非确定性多项式时间图灵机 M，其接受路径数等于 $c(z)$。对于输入 (a_1, ..., a_m, z)，该机器 M使用 m 个非确定性比特，非确定性地猜测一个符号赋值 $\varepsilon \in \{\pm 1\}^m$，确定性地在多项式时间内计算 $\sum_{i=1}^{m} \varepsilon_i a_i$，并且当且仅当该和等于 z 时接受。根据方程 (14)，接受路径数为 $\#\{\varepsilon \in \{\pm 1\}^m : \sum_i \varepsilon_i a_i = z\} = c(z)$，由此证明其属于 #P [Val79]。

为证明 #P 困难性，我们给出一个从 #SIGNED-SUM 出发的保计数归约；如上所示，#SIGNED-SUM 是 #P 完全的。该归约就是恒等映射 f: (a_1, ..., a_m, z) $\mapsto$ (a_1, ..., a_m, z)，显然可在多项式时间内计算。根据方程 (14)，计数保持性直接成立：

$$\#\text{SIGNED-SUM}(a_1, \ldots, a_m; z) = \#\{\sigma \in \{\pm 1\}^m : \textstyle\sum_i \sigma_i a_i = z\} = c(z).$$

因此，FG–系数计数在保数归约下是 #P-困难的，证明完毕。

□

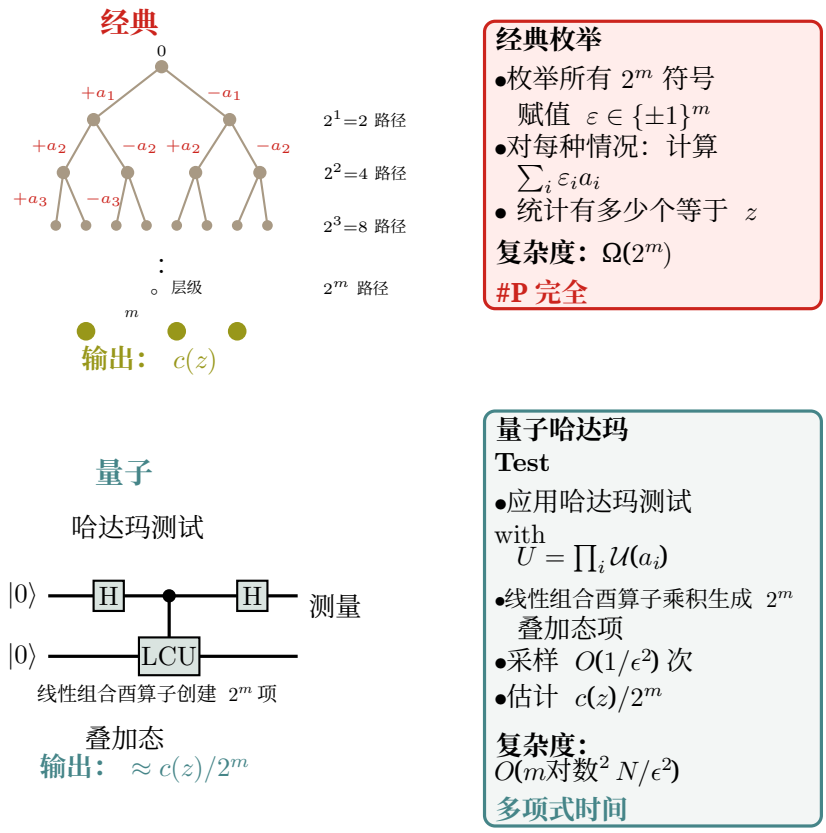


图 3：FG 系数计数的经典方法与量子方法。**上方（经典）：**二叉树展示了指数级增长。每个节点表示一个部分和，每条边表示加上 $+a_i$ 或 $-a_i$（边上的标签）。从和 0 开始，每次选择都会使路径数翻倍：第 1 层有 2^1=2 条路径，第 2 层有 2^2=4 条路径，到第 m层时总路径数达到 2^m 条。从根节点到叶节点的每条路径都对应一种符号赋值 $\varepsilon \in \{\pm 1\}^m$。经典算法必须枚举全部 2^m 条路径，统计其中哪些路径得到和 z（绿色节点）——这就是 #SIGNED-SUM 计数（#子集和的带符号变体），需要指数级 $\Omega(2^m)$ 时间。**下方（量子）：**哈达玛测试通过叠加态同时评估全部 2^m 种赋值。采样可在多项式时间 $O(m\log^2 N/\epsilon^2)$ 内，以加性精度 ϵ 估计归一化系数 $\alpha = c(z)/2^m$（定理 9），适用于常见目标值。

推论 2 (判定版本)。 对于共线输入，判定问题“ $c(z) > 0$? ”是 *NP* 完全的。

证明。 对于属于 NP，符号赋值 $\varepsilon \in \{\pm 1\}^m$ 可作为多项式大小的证书：给定 ε，可在多项式时间内验证 $\sum_i \varepsilon_i a_i = z$。

对于 NP-hard 性，我们从 SUBSET-SUM [GJ79]归约而来。给定整数 $b_1, \ldots, b_m$ 和目标值 T，令 $a_i = b_i$ 和 $z = 2T - \sum_i b_i$。若子集 S 满足 $\sum_{i\in S} b_i = T$，则对应于符号赋值 $\varepsilon_i = +1$：当 $i \in S$ 时取此值，否则取 $\varepsilon_i = -1$，从而得到 $\sum_i \varepsilon_i a_i = 2\sum_{i\in S} b_i - \sum_i b_i = 2T - \sum_i b_i = z$。反过来，任何满足 $\sum_i \varepsilon_i a_i = z$ 的 ε 都确定了 $S = \{i : \varepsilon_i = +1\}$ 满足 $\sum_{i\in S} b_i = T$。因此，$c(z) > 0$ 当且仅当该 SUBSET-SUM 实例有解。 □

引理 3 (整数到模等价)。 令 $c(z)$ 表示定义 *11* 中的整数系数，并令 $c_N(z)$ 表示满足 $\sum_i \varepsilon_i a_i \equiv z$ (模 N) 的符号赋值 $\varepsilon \in \{\pm 1\}^m$ 的数量。

Set

$$A := \sum_{i=1}^{m} |a_i|, \qquad B := A + |z|. \tag{15}$$

若 $N > B$，则 $c_N(z) = c(z)$。反之，对于任意 $N \geq 1$，都存在一些输入，使得 $N = B$ 和$c_N(z) \neq c(z)$。

证明。对于正向，所有可实现的和 $s = \sum_i \varepsilon_i a_i$ 都满足 $|s| \leq A$。设 $s \equiv z$(模 N)。若 $s \neq z$，则 $|s - z| \geq N$（因为它是 N 的非零倍数），然而根据三角不等式，$|s - z| \leq |s| + |z| \leq B$。假设 $N > B$ 导出矛盾 $N \leq B < N$，因此 $s = z$。于是$c_N(z) = c(z)$。

反过来，取 $m = 1$、$a_1 = N$ 和 $z = 0$。那么 $A = B = N$，而可实现的和$\{\pm N\}$都满足 $\pm N \equiv 0$ (模 N)，从而得到 $c_N(0) = 2 \neq 0 = c(0)$。 □

注 12 (固定-N 动态规划与精确整数问题的困难性)。我们的环面丛动态规划（第 *1* 节）之所以是多项式时间的，是因为它将所有 2^m 分支模 N 合并到一个 N^2 表格中。定理 *8* 讨论的是定义 *11* 中的整数系数 $c(z)$。根据引理 *3*，选择 $N > B$（其中 B 如式 (15) 所示），即可使两个问题等价——但此时动态规划表格的大小相对于输入数值是伪多项式的（相对于输入位长则为指数级），与 *#P*-困难性相符。

在证明精确系数提取在经典计算中是 #P 完全之后，我们现在证明量子计算能够高效近似 这一困难的计数问题。经典精确方法必须枚举指数多个项，而量子方法将所有 2^m 符号赋值编码为叠加态，使电路深度和量子比特数量均呈多项式增长。

5.3 针对 FG–系数计数的量子过程

现在我们展示如何利用迹估计算法中的二项结构，构造紧凑的量子过程来估计 $c(z)$。该量子电路在有限寄存器 $\mathbb{Z}_N$上运行；根据引理 3，选择 $N > B$（其中 B 如式 (15) 所示）可确保模计算得到正确的整数系数 $c(z)$。这只需要 O个（log N）数据量子比特和 $= O$个（log B）数据量子比特。

引理 4 (共线 LCU 特化)。对于共线输入$(p, s) = (a,0)$，定理 *3* 中的带相位置换酉算子在 $s = 0$ 子空间上简化为纯模平移：

$$U_{a,0}|r, 0\rangle = |r + a, 0\rangle, \qquad U_{-a,0}|r, 0\rangle = |r - a, 0\rangle.$$

令 $\mathcal{U}_{a_i}$ 表示定理 *4* 中专用于$(a_i,0)$的 *LCU* 电路，每个电路都作用于数据寄存器以及各自的辅助量子比特 $|0\rangle_{a_i}$。使用 m 个独立辅助量子比特进行复合，满足

$$\langle 0|_{\mathbf{a}}^{\otimes m} \left(\prod_{i=1}^{m} \mathcal{U}_{a_i} \right) |0\rangle_{\mathbf{a}}^{\otimes m} = 2^{-m} \prod_{i=1}^{m} L_{B_{(a_i,0)}}, \tag{16}$$

其中 $\langle 0|^{\otimes m}{}_{\mathbf{a}}$ 表示将所有 m 个辅助量子比特投影到 $|0\rangle$ 上。

证明。由定理 3，$U_{p,\,s}|r,\ u\rangle = t^{pu-sr}|r + p,\ u + s\rangle$。对于作用于满足 $u = 0$ 的量子态上的 $(p,\ s) = (a,$ 0)，相位变为 $t^{a\cdot 0-0\cdot r} = 1$，从而将 $U_{a,\,0}$ 和 $U_{-a,\,0}$ 化为所述平移。

根据定理 4，每个电路 $\mathcal{U}_{a_i}$ 都实现一个$1\ 2$ 块编码：$\langle 0|_{a_i} \mathcal{U}_{a_i} |0\rangle_{a_i} = \frac{1}{2} L_{B_{(a_i,0)^\circ}}$ 由于每个电路都作用于各自的辅助量子比特，投影在张量积结构上可以分解为：

$$\langle 0|_{\mathbf{a}}^{\otimes m} \left(\prod_{i=1}^{m} \mathcal{U}_{a_i} \right) |0\rangle_{\mathbf{a}}^{\otimes m} = \prod_{i=1}^{m} \langle 0|_{a_i} \mathcal{U}_{a_i} |0\rangle_{a_i} = 2^{-m} \prod_{i=1}^{m} L_{B_{(a_i,0)}}.$$

□

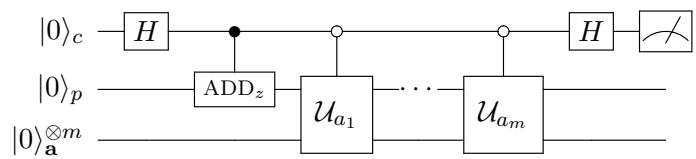
命题 6 (通过哈达玛测试进行系数提取)。 设 $\mathcal{U} := \prod_{i=1}^{m} \mathcal{U}_{a_i}$ 表示由 m 个线性组合酉电路组成的复合电路，每个电路都有各自的辅助量子比特（引理 *4*）。系数 $c(z)$ 可通过针对矩阵元 *[CEMM98]* 的哈达玛测试提取：制备

$$|\Omega\rangle \;:=\; \tfrac{1}{\sqrt{2}}\big(|0\rangle_c|0\rangle_{\mathbf{a}}^{\otimes m}|0,0\rangle + |1\rangle_c|0\rangle_{\mathbf{a}}^{\otimes m}|z,0\rangle\big),$$

施加受控-$\mathcal{U}$（条件为 $c=0$），然后测量控制量子比特上的泡利 X。其期望值满足

$$\mathbb{E}[X_c] \;=\; 2^{-m}\, c(z). \tag{17}$$

实现命题 6 的量子电路将矩阵元的哈达玛测试形式与线性组合酉算子（LCU）组合相结合：



(18)

矩阵元的哈达玛测试通过制备 $(|0\rangle|\phi\rangle + |1\rangle|\psi\rangle)/\sqrt{2}$ 来提取 $\mathrm{Re}\langle\psi|U|\phi\rangle$，施加以 c 为反控制的 U^{-}，然后测量 c 上的 X。这里 $|\phi\rangle = |0\rangle_{\mathbf{a}}^{\otimes m}|0\rangle_p$ 和 $|\psi\rangle = |0\rangle_{\mathbf{a}}^{\otimes m}|z\rangle_p$，因此 ADD_z 门（受控模加法器：当 $c=1$ 时为 $|p\rangle \mapsto |p+z\rangle$，可通过基于 QFT 的算术 [Dra00] 实现）会在初始哈达玛门之后制备所需的叠加态。反控制的 $\mathcal{U}_{a_i}$ 模块（每个都是来自定理 4 且拥有各自辅助量子比特的 LCU 电路）仅在 $c=0$ 时应用。将所有 m 辅助量子比特后选择为 $|0\rangle$，依据引理 4 可得到块编码 $2^{-m}\prod_i L_{B_{(a_i,0)}}$，而哈达玛测试则提取 $\langle z|2^{-m}\prod_i L_{B_{(a_i,0)}}|0\rangle = 2^{-m}c(z)$。

证明。 针对矩阵元 [CEMM98] 的哈达玛测试给出 $\mathbb{E}[X_c] = \mathrm{Re}(\langle 0|^{\otimes m}{}_{\mathbf{a}}\langle z,0|\,\mathcal{U}\,|0\rangle^{\otimes m}{}_{\mathbf{a}}|0,0\rangle)$。根据引理 4, $\langle 0|^{\otimes m}{}_{\mathbf{a}}\mathcal{U}\,|0\rangle^{\otimes m}{}_{\mathbf{a}} = 2^{-m}\prod_{i=1}^{m} L_{B_{(a_i,0)}}$。两项结构 $L_{B_{(a,0)}} = U_{a,0} + U_{-a,0}$（定理 3）意味着乘积算符会展开符号赋值二叉树：

$$\Big(\prod_{i=1}^{m} L_{B_{(a_i,0)}}\Big)|0,0\rangle \;=\; \sum_{\varepsilon\in\{\pm1\}^m} \Big|\sum_{i=1}^{m}\varepsilon_i a_i,\, 0\Big\rangle,$$

其中每个 $L_{B_{(a_i,0)}}$ 都会将叠加态分成 $|\cdot + a_i, 0\rangle$ 和 $|\cdot - a_i, 0\rangle$ 两个分量。与 $\langle z,0|$ 取内积后，即可统计满足 $\sum_i \varepsilon_i a_i = z$的符号赋值；根据方程（14），这等于 $c(z)$。因此 $\langle 0|^{\otimes m}{}_{\mathbf{a}}\langle z,0|\,\mathcal{U}\,|0\rangle^{\otimes m}{}_{\mathbf{a}}|0,0\rangle = 2^{-m}c(z)$。由于 $c(z) \in \mathbb{Z}_{\geq 0}$，虚部为零。

□

矩阵元的哈达玛测试可得期望值中的归一化系数 $\alpha = 2^{-m}c(z)$（命题 6）。下述定理总结了实现精度ϵ 且置信度为 $1-\delta$的两种方法，与定理 6 相呼应。

定理 9 （量子系数估计）。 对于 $N > B$（其中 B 如（15）所示），归一化系数 $\alpha := 2^{-m}c(z) \in [0,1]$ 可被估计到加性精度 ϵ，且成功概率至少为$1-\delta$，所需量子比特数为 $2\lceil\log_2 N\rceil + m + 1$（$O$（log N） 个数据量子比特和 $m+1$个辅助量子比特）。令 $D = O(m\log^2 N)$ 表示基础电路深度。实现这一目标有两种方法：

1. 采样 *(*近期*)*： $O(\log(1/\delta)/\epsilon^2)$次独立运行，每次深度为 D，总操作数为

$$O\big(D\cdot\log(1/\delta)/\epsilon^2\big) = O\big(m\log^2 N\cdot\log(1/\delta)/\epsilon^2\big).$$

2. 量子振幅估计 *[BHMT02] (*容错*)*： $O(\log(1/\delta))$次运行，每次深度为 $O(D/\epsilon)$，总操作数为

$$O\big(D\cdot\log(1/\delta)/\epsilon\big)=O\big(m\log^2 N\cdot\log(1/\delta)/\epsilon\big).$$

抽样方法使用独立的浅电路；量子振幅估计则通过格罗弗式反射，在每次运行中相干地应用基础电路 $O(1/\epsilon)$ 次，因此需要更长的相干时间（参见备注 *10*）。两种方法都提供了经典动态规划的一种节省空间的替代方案，使用 $O(\log\ N+m)$ 个量子比特，而经典存储器则需要 $O(N)$。

证明。量子电路需要 $2\lceil\log_2 N\rceil$ 个数据量子比特（$\lceil\log_2 N\rceil$ 个分别用于 p-寄存器和 s-寄存器）、m 个 LCU 辅助量子比特（每个共线块对应一个，这是引理 4 的要求，以确保块编码复合正确），以及一个 Hadamard测试控制量子比特，总计 $2\lceil\log_2 N\rceil+m+1$ 个量子比特。在共线情形下，若 $s=0$ 始终成立，则可以省略 s-寄存器，使数据量子比特减少至 $\lceil\log_2 N\rceil$。

对于基础电路深度，每个实现 $B_{(a_i,0)}$ 的 LCU 块由作用于辅助量子比特的哈达玛门（每个深度为 1）和受控-$U_{\pm a_i,0}$ 操作组成。在共线情形下，辛相位 t^{pu-sr} 消失，因为 $s=0$，因此 $U_{(\pm a,0)}$：$|p,0\rangle\mapsto|p\pm a,0\rangle$ 简化为纯模加法，无需计算相位。通过基于QFT的加法器 [Dra00]，每次模加法所需深度为 $O(\log\ N)$。为与一般（非共线）情形保持一致——该情形下相位计算需要 $O(\log^2 N)$ 深度 [RC 18],——我们给出保守上界：每个 LCU 块的深度为 $O(\log^2 N)$，因此 m 个顺序块的基础深度为 $D=O(m\log^2 N)$。

对于抽样方法，每次 Hadamard测试测量都会产生一个独立样本。根据 Hoeffding不等式（命题5），只需 $O(\log(1/\delta)/\epsilon^2)$个样本，即可在置信度为 $1-\delta$的条件下，将 α 估计到精度ϵ。每个样本需要执行一次深度为 D的量子电路，因此总操作数为 $O(D\cdot\log(1/\delta)/\epsilon^2)$。

对于量子振幅估计 [BHMT02]，，通过在每次运行中相干地应用基础电路（以及格罗弗反射） $O(1/\epsilon)$次，可达到精度 ϵ，每次运行的电路深度为$O(D/\epsilon)$。若要求置信度为 $1-\delta$，则只需进行 $O(\log(1/\delta))$次独立运行。因此，总操作数为 $O(D\cdot\log(1/\delta)/\epsilon)\ =O(m\log^2 N\cdot\log(1/\delta)/\epsilon)$——在 ϵ方面实现了二次改进。

□

注*13*（量子优势与复杂度障碍）。量子算法在空间和并行时间方面具有指数级优势，而在串行时间方面的情况则更为微妙。就空间而言，针对*#SIGNED-SUM*的经典动态规划需要一个大小为 $O(N)$的数组，以跟踪所有可达和的计数；由于有 m个值以 b位整数编码，因此 $B\le(m+1)\cdot 2^b$，所以只需$N=O(m\cdot 2^b)$即可避免回绕——这需要 $O(m\cdot 2^b)$的经典存储器，其规模相对于b呈指数增长。量子算法使用 $O(\log\ N+m)\ =O(b+m)$个量子比特，关于输入位长为多项式级。就并行时间而言，经典枚举需要 $O(2^m)$个连续步骤，而量子电路的深度为 $O(m\log^2 N)$，关于 m和 b均为多项式级。这两种优势都是无条件成立的。

对于串行时间，情况取决于目标和 z 是常见还是罕见。回顾一下，(14) 中，$c(z)$ 统计了满足 $\sum_i\varepsilon_i a_i=z$ 的 2^m 个符号配置 $\varepsilon\in\{\pm1\}^m$。如果有固定比例的配置能得到该目标（$c(z)=\Omega(2^m)$），则称该目标为常见；如果只有少数配置能得到该目标（$c(z)=O(1)$），则称其为罕见。

要实现精确恢复，需要精度达到 $\epsilon<2^{-(m+1)}$，这样对 $\alpha=c(z)/2^m$ 的估计值进行舍入后，就能恢复整数 $c(z)$。这需要 $O(2^m)$ 次量子操作，与经典枚举相当。指数级开销不可避免：精确计算 $c(z)$ 可解决一个 *#P* 完全问题（定理 *8*），而多项式时间算法将导致多项式层级坍缩 *[Tod91]*。

对于加性近似，量子算法估计 α，精度为 ϵ，在 $c(z)$上产生绝对误差 $\epsilon\cdot 2^m$。对于常见目标，相对误差为 $O(\epsilon)$，因此可获得有意义的近似

并且计算时间为多项式时间，而经典精确计数仍为$\Omega(2^m)$。对于罕见目标，误差会淹没信号，使近似结果毫无意义。

6 结论

本文提出了两种互补的算法，用于计算环面丛的 Witten-Reshetikhin-Turaev 不变量，其核心是利用将编织代数 $K_N(\Sigma_{1,0})$ 嵌入非交换环面的对称子代数这一结构。首先，我们对具有完整复杂度分析的多项式时间经典动态规划方法给出了明确的算法表述，并从拓扑量子计算 [BP08] 的视角解释了这一计算过程。该算法通过在 N^2 系数表上高效组合 Frohman-Gelca 乘积规则中的 2^m 概念项，在 $\Theta((m+\ell)N^2)$ 时间和 $\Theta(N^2)$ 空间内计算 WRT 不变量，其中 ℓ 是单值化的词长。其次，我们提出了一种以空间换取相干性的量子算法，仅使用 $2\lceil \log_2 N \rceil + m + 1$ 个量子比特（$O(\log\ N)$ 个数据量子比特加上 $m+1$ 个辅助量子比特）——相对于经典的 $\Theta(N^2)$ 需求，其关于 $\log\ N$ 和 m 呈多项式复杂度。

我们的工作从多个角度阐明了拓扑不变量的复杂性概况。对于任意链环的琼斯多项式以及一般三维流形的 WRT 不变量，计算仍然是 #P-困难的 [JVW90，AL17], 但环面丛这一特殊情形可以在多项式时间内计算，因为单位根处的非交换环面给出了一个固定的有限维表示。关键见解在于，纽结图乘积展开中的 2^m 项虽然在概念上呈指数级增长，却都映射到相同的 N^2 基元素，其系数可以一致地更新——这类似于 $(1+x)^m$ 虽然有 2^m 项，但仍可在多项式环中高效计算。

值得注意的是，我们证明共线 FG 系数计数问题（定义 11）是 #P 完全的（第 5 节），这表明，当指标被视为整数而非 $\mathbb{Z}_N$的元素时，计算难度便会显现。这种二分——采用模运算时，对固定的 N 可在多项式时间内计算，而整数问题则是 #P-困难的——揭示了拓扑不变量计算中易解与难解情形之间微妙的界限。这个系数计数问题是对计算拓扑的一项新贡献：此前尚未从复杂度理论的角度对其进行研究，但它自然源自纽结图理论的代数结构，并提供了一个具体实例：精确的经典计数是 #P 完全的，而量子算法则能对归一化系数实现多项式时间加性近似——当系数大小为 $\Omega(2^m)$ 时，这一近似具有实际意义。不同于一些关于系数问题量子优势的猜想后来被更优的经典算法所推翻[Pan25], ，我们的分离结果稳健可靠——由 #P 完全性证明保证，除非多项式层级坍缩，否则该结果始终成立 [Tod91]。

量子算法在特定场景下具有显著优势：当存储空间受限时（对于较大的 N，存储 N^2 个复数可能难以承受），当只需要迹时（无需计算完整的系数表），或者当近似结果已足够时。这种规模差异——总量子比特数为 $O(\log\ N+m)$，而经典存储器为 $\Theta(N^2)$——体现了指数级空间优势。

对我们算法的实验性实现，将在拓扑不变量量子优势演示的版图中占据独特且互补的位置。近期的琼斯多项式实验 [LRS+25]验证了纽结不变量的量子优势（三维流形中的一维对象），而我们的算法则针对三维流形不变量（刻画三维空间本身）。这种维度上的区别反映了 WRT 理论中的层级关系：当三维流形为 S^3

带有链接插入时，琼斯多项式是 WRT 不变量的特殊情形 [Tur94]。此外，我们的对数量子比特缩放 N 使我们能够探索相比基于辫子的方法大得多的指数级状态空间；后者采用线性的量子比特缩放。例如，使用 14 个数据量子比特时，我们的方法可以访问一个 16,129 维的空间（$N = 127$），而基于辫子的方法只能处理 13 股辫子。这两个实验方案都建立在严格的经典计算困难性结果之上：即使对于区分取值的近似，琼斯多项式求值仍是 #P-困难的 [JVW90, Kup15], ，而我们的 FG 系数计数对于精确计数而言是 #P 完全的（定理 8）。这些互补的方向——通过辫子研究纽结不变量与通过非交换环面研究三维流形不变量，线性缩放与对数缩放的量子比特——共同将为拓扑量子场论的完整范围内的量子计算优势提供全面验证。

未来工作的几个方向自然浮现。我们的系数计数分析聚焦于共线输入 $v_i = (a_i,\ 0)$；对于一般输入 $v_i = (p_i,\ q_i)$，Frohman-Gelca 权重会产生二次相位 $t^{\sum_{i<j} \varepsilon_i \varepsilon_j \det(v_i,\ v_j)}$，使得系数成为类伊辛配分和。通过将问题限制到共线情形，该问题仍然是 #P-困难的，但量子电路会自然累积这些相位，而经典算法必须对 2^m 振荡贡献求和——在这种情况下，量子干涉可能带来额外优势。将研究扩展到高亏格曲面 $\Sigma_{g,\ n}$ 且满足 $g > 1$，会面临更根本的挑战——与环面不同，高亏格 skein 代数没有定义好的乘积转求和公式，因此乘法难以处理。此外，我们的算法与拓扑量子计算之间的联系也值得进一步探索，因为对任意子编织的经典模拟与我们的动态规划方法本质上是等价的。随着量子硬件不断进步，对于 N 足够大、以至于经典存储难以承受，但又足够小、仍可进行相干量子计算的问题，节省空间的量子方法可能会变得越来越有价值。

参考文献

[AF16] N. Abdiel 和 C. Frohman. 由考夫曼括号 skein 代数导出的 Frobenius 代数. 《纽结理论及其分支》, 25(04):1650016, 2016.[AF17] N. Abdiel 和 C. Frohman. 局部化 skein 代数是 Frobenius 代数. 《代数与几何拓扑》, 17:3341–3373, 2017.[AJL09] D. Aharonov、V. Jones 和 Z. Landau. 一种用于近似计算琼斯多项式的多项式时间量子算法. *Algorithmica*, 55(3):395–421, 2009.[AK14] Jørgen Ellegaard Andersen 和 Rinat M. Kashaev. 一种来自量子 Teichm¨uller 理论的拓扑量子场论. 《数学物理通讯》, 330:887–934, 2014. arXiv:1109.6295.[AL17] Gorjan Alagic 和 Catharine Lo. 三维流形的量子不变量与 NP 与 #P。《量子信息与计算》, 17(1& 2):125–146, 2017.[Ati88] M. Atiyah. 拓扑量子场论. *Publications Math´ematiques de l'IH´ES*, 68:175–186, 1988.[BHMT02] Gilles Brassard、Peter Høyer、Michele Mosca 和 Alain Tapp. 量子振幅放大与估计. *Contemporary Mathematics*, 305:53–74, 2002.[BP08] Gavin K. Brennen 和 Jiannis K. Pachos. 为什么要关心用任意子进行计算？ 《伦敦皇家学会学报 *A* 辑：数学、物理与工程科学》, 464(2089):1–24, 2008.

[Bur13] Benjamin A. Burton. 使用 Regina 进行计算拓扑：算法、启发式方法与实现. 载于 Geometry and Topology Down Under，第 597 卷 Contemporary Mathematics，页 195–224. 美国数学学会，2013. arXiv:1208.2504.[CDGW] Marc Culler、Nathan M. Dunfield、Matthias Goerner 和 Jeffrey R. Weeks. SnapPy：用于研究三维流形几何与拓扑的计算机程序. 可访问 http://snappy.computop.org.[CEMM98] Richard Cleve、Artur Ekert、Chiara Macchiavello 和 Michele Mosca. 重新审视量子算法. 伦敦皇家学会学报 A 辑：数学、物理与工程科学，454(1969):339–354, 1998.[CF99] L. Chekhov 和 V. Fock. 量子 Teichm¨uller 空间. 理论与数学物理，120(3):1245–1259, 1999.[CW12] A. M. Childs 和 N. Wiebe. 使用酉运算的线性组合进行哈密顿量模拟.《量子信息与计算》，12(11-12):901–924, 2012.[DKRS06]Thomas G. Draper、Samuel A. Kutin、Eric M. Rains 和 Krysta M. Svore. 对数深度量子超前进位加法器.《量子信息与计算》，6(4):351–369, 2006. arXiv:quant-ph/0406142.[Dra00] T. G. Draper. 量子计算机上的加法. arXiv 预印本 quant-ph/0008033, 2000.[FG00] C. Frohman 和 R. Gelca. 骨架模与非交换环面. 美国数学会汇刊，352(10):4877–4888, 2000.[FM11] Benson Farb 和 Dan Margalit.《映射类群入门》，Princeton Mathematical Series 第 49 卷. 普林斯顿大学出版社，普林斯顿，新泽西州，2011.[GJ79] Michael R. Garey 和 David S. Johnson.《计算机与难解性：NP 完全性理论指南》. W. H. Freeman，旧金山，加利福尼亚州，1979.[Hatnd] Allen Hatcher. 三维流形拓扑基础笔记，未注明日期. 可访问 https://pi. math.cornell.edu/~hatcher/3M/3Mdownloads.html.[Jon85] V. F. R. Jones. 通过冯·诺伊曼代数构造纽结的多项式不变量. 美国数学会通报，12(1):103–111, 1985.[JVW90] F. Jaeger、D. L. Vertigan 和 D. J. A. Welsh. 琼斯多项式与 Tutte 多项式的计算复杂性. 剑桥哲学学会数学学报，108:35–53, 1990.[KF20] N. Kohen 和 C. Frohman. 模群的射影表示. arXiv 预印本，2020. arXiv:2010.08894v1 [math.GT].[KL98] E. Knill 和 R. Laflamme. 一比特量子信息的力量. Physical Review Letters, 81(25):5672–5675, 1998.[Kup15] Greg Kuperberg. 近似计算琼斯多项式有多难？计算理论，11:183–219, 2015. arXiv:0908.0512.

[LRS+25] Tuomas Laakkonen、Enrico Rinaldi、Chris N. Self、Eli Chertkov、Matthew DeCross、David Hayes、Brian Neyenhuis、Marcello Benedetti 和 Konstantinos Meichanetzidis。《量子越少，优势越大：一个端到端的琼斯多项式量子算法》。*arXiv* 预印本 *arXiv:2503.05625*，2025 年。[Pan25] Greta Panova。表示论重数的经典多项式时间算法与量子算法。*arXiv* 预印本，2025 年。arXiv:2502.20253。[RC18] Rich Rines 和 Isaac Chuang。高性能量子模乘法器。*arXiv* 预印本，2018 年。arXiv:1801.01081。[Rie81] M. A. Rieffel。与无理旋转相关的c^*-代数。《太平洋数学杂志》，93(2):415–429，1981 年。[RT91] N. Reshetikhin 和 V. Turaev。通过链环多项式和量子群构造三维流形的不变量。《数学新进展》，103(1):547–597，1991 年。[Sch09] Nils R. Scheithauer。$SL_2(\mathbb{Z})$ 的韦伊表示及其若干应用。《国际数学研究通知》，2009(8):1488–1545，2009 年。[SJ08] P. W. Shor 和 S. P. Jordan。估计琼斯多项式是单干净量子比特的完全问题。《量子信息与计算》，8(8-9):681–714，2008 年。[Tod91] Seinosuke Toda。PP 与多项式时间层次一样难。《*SIAM*计算杂志》，20(5):865–877，1991 年。[Tur94] Vladimir G. Turaev。《结与*3*维流形的量子不变量》，《德格鲁伊特数学研究丛书》第 18 卷。Walter de Gruyter，柏林，1994 年。[Val79] Leslie G. Valiant。枚举与可靠性问题的复杂度。《*SIAM*计算杂志》，8(3):410–421，1979 年。[Wit89] E. Witten。量子场论与琼斯多项式。《数学物理通讯》，121(3):351–399，1989 年。

无点方法与非交换环面嵌入

本附录阐明了为何我们的量子算法能够自然地实现无点方法，在保持完全一般性的同时简化电路构造。对于熟悉基于点的缠结代数表示的拓扑量子场论（TQFT）领域的研究者而言，这一区别尤为重要。

A.1 基于点的表示与无点表示

在单位根的 $2N$ 阶处采用标准的缠结–弗罗贝尼乌斯方法时，首先沿乘法集 $S \subset Z\big(K_N(T^2)\big)$（从特征簇中去除不良轨迹）进行局部化，以构造$S^{-1}K_N(T^2)$和 $S^{-1}Z$；随后将点 定义为一个中心特征 $\phi\colon S^{-1}Z \to \mathbb{C}$，并将 $S^{-1}K_N(T^2)$上的归一化迹与 ϕ复合，得到数值配对 [AF16]——这一步局部化至关重要，因为 $K_N(T^2)$不是自由的 Z–模，其纤维秩会发生跳变（在可约轨迹上甚至超过 N^2）；而转至 $S^{-1}K_N(T^2)$后，秩在 $S^{-1}Z$上保持稳定，且特化迹非退化。对于具有 $\chi(\Sigma) < 0$ （puncture 或边界）的任意非紧有限型曲面，也有类似的构造 [AF17]。

我们的无点方法将 $K_N(\Sigma_{1,\,0})$ 规范地嵌入非交换环面的对称子代数 $\mathcal{W}_t^{\nu}$ 中。我们始终在固定且忠实的 N^2 维左正则模型中工作，因此所有代数运算和中心值约化迹都与任何点无关。当需要标量时，我们要么与中心特征复合（从而恢复通常的基于点的值），要么采用后文规定的单一归一化和相位约定，使归一化矩阵迹与标准 WRT归一化保持一致。作为参考：固定中心特征后，非交换环面具有唯一的 N 维不可约表示；而我们有意保留在 N^2 维忠实模型中，以便在线性代数层面保持无点性。

A.2 量子计算的优势

无点方法具有决定性的优势：**(1) 固定的电路架构**——每个 skein 元恰好需要 $2\lceil \log_2 N \rceil$ 个数据量子比特，并采用统一的双项线性组合酉分解（每次乘法另需一个辅助量子比特，以实现正确的块编码复合），且与拓扑复杂度无关。**(2) 直接进行迹计算**——Tr(W) 直接给出 WRT 不变量，无需对不同点、基点选择进行平均，也无需后处理校准。**(3) 与基于辫子的方案比较**——传统的琼斯多项式算法使用基于点的表示，其中泡利分解宽度会随辫子和所选点而变化，从而使资源估算更加复杂。我们的无点方法提供了统一且高效的计算，能够直接从代数得到拓扑不变量。

B 映射环面与模作用背景

本附录为环面丛（映射环面）提供必要的背景知识，尤其面向量子算法领域的读者。我们概述其几何构造，并说明模群 $\mathrm{SL}_2(\mathbb{Z})$ 如何通过量子电路作用。

B.1 映射环面构造

由同胚 $f\colon \Sigma \to \Sigma$得到的映射环面是商空间 $M_f := (\Sigma \times [0,1])/(x,1) \sim (f(x),0)$，它自然地纤维化于 S^1 之上，纤维为 Σ，单值化为 f。对于环面 $\Sigma = T^2$，

映射类群 MCG(T^2) $\cong$ SL$_2(\mathbb{Z})$ 在同调 $H_1(T^2;\mathbb{Z}) \cong \mathbb{Z}^2$ 上作用，因此每个矩阵$g \in$SL$_2(\mathbb{Z})$ 都确定一个环面丛 M_g，其基底为 S^1。

B.2 WRT 不变量与编织插入

在 $2{+}1$ 维拓扑量子场论中，环面 T^2 的希尔伯特空间为 $V_N(T^2)$（层级为 N 的理论），WRT 不变量为 $Z_N(M_g) = \mathrm{Tr}(\rho(g))$，其中 $\rho\colon \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{GL}(V_N(T^2))$ 是模表示。沿纤维插入 m 个编织 skein 元 $x_1,\dots,x_m$ 后，带饰不变量变为

$$Z_N(M_g; x_1,\dots,x_m) = \mathrm{Tr}\big(\rho(g) L_{x_m}\cdots L_{x_1}\big),$$

其中 L_{x_i} 是 skein 元 x_i 对应的线性算子。此公式是我们算法的出发点。

B.3 SL$_2(\mathbb{Z})$ 的量子电路实现

模群的标准生成元 S, T 通过模运算作用于计算基态 $|p,s\rangle \in \mathbb{Z}_N^2$。$T$ 生成元将 $|p,s\rangle \mapsto$ 映射为 $|p+s \bmod N, s\rangle$，并带有二次相位 t^{s^2}；该操作通过模加法后接二次相位门实现，所需门数为 $O(\log^2 N)$。S 生成元将 $|p,s\rangle \mapsto$ 映射为 $|-s \bmod N, p\rangle$，可通过双重量子傅里叶变换、SWAP 和模取负实现，所需门数为 $O(\log^2 N)$。

任意 $g \in \mathrm{SL}_2(\mathbb{Z})$ 都可以表示为生成元 S, T [FM11],中长度为 $\ell = O(\log \|g\|)$ 的词，从而对 $\rho(g)$ 产生电路深度为 $O(\ell \log^2 N)$ 的量子电路。这种对数级缩放源于 SL$_2(\mathbb{Z})$ 分解与欧几里得算法之间的联系：对于 $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$，该分解本质上是在矩阵元素上运行欧几里得算法，并在经过 $O(\log \max(|a|,|b|,|c|,|d|))$ 步后终止。这种高效的模作用对于多项式时间的量子 WRT计算至关重要。

C 与 SU(2)$_k$ 任意子和拓扑量子场论的联系

本附录给出了我们算法中的代数结构（skein代数、非交换环面）与 $SU(2)_k$ 任意子和拓扑量子场论物理框架之间的对照表。

C.1 SU(2)$_k$ 层级 $k = N-2$处的任意子

本工作中计算的 WRT 不变量对应于层级为$k = N-2$的 $SU(2)$ 陈-西蒙斯理论。在模张量范畴的语言中，相关范畴 $\mathcal{C} = SU(2)_k$ 是预模的；将其限制到可积表示后便成为模范畴 [Tur94, RT91]。

简单对象（任意子类型）以半整数 $j \in \{0, 1/2, 1, \dots, k/2\}$ 标记，对应于 $\mathfrak{sl}(2)_k$的可积最高权表示 $\widehat{}$。使用整数标记 $a = 2j \in \{0, 1, \dots, N-2\}$时，标签 $a = 0$ 对应真空。任意子 a与 b的融合遵循截断的克莱布施-戈丹级数 [Tur94]:

$$a \times b = \sum_{c=|a-b|,\ \text{step } 2}^{\min(a+b,\,2k-(a+b))} c,$$

具有量子维数 $d_a = [a+1]_q = \sin(\pi(a+1)/N)/\sin(\pi/N)$。支配编织统计的模 S-矩阵的元素为 $S_{ab} = \sqrt{2/N}\sin(\pi(a+1)(b+1)/N)$，该矩阵通过维林德公式 [RT91] 将融合规则对角化。

C.2 迹分量的物理解释

迹公式 $Z_N(M_g;\, x_1, \ldots, x_m) = \mathrm{Tr}(\rho(g) L_{x_m} \cdots L_{x_1})$ 可以用拓扑量子场论的时空历史 [Wit89、Ati 88] 来作直接的物理解释。算子 $L_{B_{(p,s)}}$ 表示沿曲线类 $(p, s) \in H_1(T^2;\, \mathbb{Z})$ 插入一个携带基本表示的威尔逊环；在三维流形 M_g 中，这对应于一个绕纤维缠绕的着色链环分量。代数关系 $L_{B_{(p,s)}} = U_{p,s} + U_{-p,-s}$ 反映了非交换环面中通量算子的分解。

模作用 $\rho(S)$ 和 $\rho(T)$ 表示空间环面上的大微分同胚：$\rho(S)$ 实现模 S 矩阵生成的 S 变换（子午线和经线旋转 90 度），而 $\rho(T)$ 实现德恩扭转，为拓扑自旋为 $h_a = a(a+2)/4N$ 的任意子态 $|a\rangle$ 赋予相位 $e^{2\pi i h_a}$。迹运算对应于将 $T^2 \times [0,1]$ 的两个边界粘合起来形成 M_g，并对中间任意子态求和，从而得到配分函数 [Ati88]。

C.3 经典模拟与量子优势

经典算法（定理 5）通过计算拓扑不变量——配分函数和威尔逊环期望值——的精确值，来“模拟”这些任意子；这些值是在理想的拓扑量子计算机中测量得到的。通过在非交换环面基底中维护系数表，该算法明确追踪拓扑路径的相消干涉和相长干涉（即 2^m 考夫曼括号项）。

虽然环面丛的经典算法可在多项式时间内运行，但量子算法（定理 6）具有内在优势。经典模拟完整的拓扑量子场论态矢量需要 $\Theta(N^2)$ 存储空间，而量子算法则用 $O(\log N)$ 个量子比特以相干方式存储该态；对于较大的 N，这就将难以处理的经典存储需求转化为一个小型量子比特寄存器。此外，从任意子干涉图样中提取特定系数在经典计算中是 #P 完全问题（定理 8），而量子算法可通过哈达玛测试高效估计这些系数。