arXiv:2611.29358v1 [cs.LO] 22 Nov 2026

两个素数足以实现可定义图规范化

Vaani
Goenka阿育王大学

Aalok ThakkarVachani高级计算学院，阿育王大学

摘要。 我们研究顶点无序、具有有序数值类型的有限简单图上的膨胀不动点逻辑。对于素数 r，量词 M_r 用于检验满足某个公式的关系数量是否模 r非零。对于任意不同的素数 p， q，结合 M_p 和M_q 的逻辑能够定义数值类型上某个规范副本的邻接矩阵。对于带标号输入，该矩阵可通过确定性多项式时间算法与 Mod$_p$P 预言机计算得到。对于每个素数 p，仅使用 M_p 的逻辑无法在所有图上定义规范副本。这些素数在布尔查询方面也有所不同。存在一个定义在顶点集上的一阶公式 $\beta(S)$，使得只要 $p \neq q$， $M_q S\,\beta(S)$就无法仅用 M_p 定义。对于正整数值函数 g，考虑由所有自同构不超过 $g(|V(G)|)$个的图 G 组成的等价类。对于每个固定的素数 p，当且仅当 g 有界时，结合M_p 的逻辑才能规范化该等价类。

引言

一条单边的两个端点是不可区分的。公式无法首先选择其中任何一个，但两种排序都会得到相同的邻接矩阵。对于一个含有 n 个顶点的图，规范化 指定了一个含有 $I_n = \{0, \ldots, n-1\}$的同构图，其邻接矩阵只取决于输入的同构类型。

在有序结构上，不动点逻辑可以捕获多项式时间（PTIME）（Immerman，1986年；Vardi，1982）。可定义规范化使我们能够通过在其有序副本上求值一个句子，将该定理应用于无序图。这正是 Grohe（2017）如何在具有排除小图的图类上获得一种用于 PTIME 的逻辑。在任意图上，问题在于是否存在一种具有有效语法的逻辑，能够表达每个 PTIME图性质，并为每个句子有效地指定一个多项式时间求值算法（Gurevich，1988）。对于一种在规范副本上求值有序不动点句子的逻辑，只需在多项式时间内计算出该副本即可。

输入包含一个无序顶点类型，以及一个有序数值类型 I_n。对于素数 p，当满足 φ 的关系 R 的数量模 p 不为零时，公式 $M_p R\,\varphi$ 成立。每个关系变量都有固定的元数和指定的参数类型。例如，它可以计数那些编码从顶点到数值的映射的顶点集或二元关系。令 $\mathcal{L}_p$ 表示带膨胀不动点的一阶逻辑以及 M_p，并令 $\mathcal{L}_{p,\,q}$ 允许使用两种模量词。我们的第一个定理仅通过将一组顶点作为计数关系，便区分了这些语言。

定理（布尔分离）。存在一个一阶图公式 $\beta(S)$，带有一个一元关系参数，使得对于任意两个不同的素数 p、q，图性质 $M_q S\,\beta(S)$ 在 $\mathcal{L}_p$ 中不可定义。因此，单素数语言在图上两两不可比较，且加入任意第二个素数都会严格增强表达能力。

要构造 β，取域 $\mathbb{F}_p$ 上的一个连通网络，并为每个顶点规定净流出量。如果规定值之和为零，则对生成树之外的 d 条边进行任意赋值，都可以将其延拓为唯一的流。这样的流共有 p^d 个。如果总和不为零，则不存在流。模任意其他素数计数都能区分这两种情况。图编码了局部约束，而每个流都对应于一个满足 β 的集合。

要证明这种可分性，我们必须排除每个可能区分这两个负载的 $\mathcal{L}_p$ 句子。我们使用 Cai–Fürer–Immerman 构造的素域版本（Cai 等人，1992；Grädel 等人，2019）。其自同构构成一个 p-群，即其阶为 p 的幂的群。当该群作用于满足某个公式的关系时，只有被整个群固定的关系才会对模 p 计数作出贡献。我们在两个结构之间匹配这些不动关系，并证明这种匹配在进一步量化以及不动点的每个阶段都保持不变。

Kontinen 和 Szymanik（2014年，定义 2.7 和推论 3.6）在给定的集合族上区分了互素的二阶整除量词。在这里，单个一阶公式定义了简单图上的集合族，而竞争逻辑可以对任意固定元数的关系进行计数。仿射方程组还为无穷计数逻辑（Atserias 等，2009年）以及带线性代数算子的逻辑（Grädel 和 Pakusa，2019年；Dawar 等，2019年）提供了下界。在我们的例子中，对 $\mathbb{F}_p$ 进行高斯消元即可判定方程组是否有解，尽管在两个图上，解的数量都可被 p 整除。

定理（规范化）。对于任意不同的素数 p、q，一个 $\mathcal{L}_{p,\,q}$ 公式 $\gamma_{p,\,q}(i,j)$ 在其数值排序上定义了每个有限简单图的规范副本的邻接矩阵。不存在 $\mathcal{L}_p$ 公式能在所有有限简单图上定义这样的副本。

对于下界，一个假设存在的单素数公式会在两个不同构的 CFI 图的每个数值位置上给出相同的邻接位。对于上界，设 Q 是 I_n 的置换群中的一个 Sylow p 子群，其阶是整除 $n!$ 的最大 p 次幂。若两个标记相差一个 Q 中的置换，就将它们归为一组。每个等价类称为一个框架，含有 $|Q|$ 个标记，框架的数量与 p 互素。置换群下的规范放置（Babai 和 Luks，1983年）会为每个框架选出一个邻接字符串。内部量词 M_q 可以识别具有给定前缀的框架，因为 q 不整除兼容标记的数量。外部量词 M_p 对每个这样的框架计数一次。从空前缀开始，我们总能扩展一位，使其计数仍非零。最终字符串就是该图的一个副本。

我们的配套论文（Goenka 和 Thakkar，2026）使用相同的 Sylow 子群陪集计数。其算法在带标号输入上为每个陪集猜测一个代表元

。在这里，我们用无序顶点上的关系来表示每个陪集。借助模电路可满足性预言机，可以在多项式时间内计算该矩阵。这个预言机用于检验满足赋值数模 p 是否非零；这是 Mod$_p$P 的一个完全问题。在副本上使用这一电路测试来计算有序不动点句子，可以捕获 $\mathrm{P}^{\mathrm{Mod}_p\mathrm{P}}$ 中的同构不变查询。

一个素数足够时。置换群的基是一个点元组，其逐点稳定子仅包含恒等元。现在，我们考察自同构群 Aut(G) 的 Sylow p-子群在顶点上的作用的基。对于正整数值函数 g，令 $\mathcal{G}_g = \{G : |\mathrm{Aut}(G)| \le g(|V(G)|)\}$。

定理（单素数规范化与捕获）。固定一个素数 p 和一个整数 $k \ge 0$。对于 *Sylow* p- 子群的 $\mathrm{Aut}(G)$ 具有至多 k 个顶点的基的图， $\mathcal{L}_p$ 定义一个规范的有序副本，并捕获$\mathrm{Mod}p\mathrm{P}$ 布尔查询中的不变性。

对于 $\mathcal{G}_g$，当且仅当 g 有界时，这些结论中的每一项都成立。存在一个 *PTIME*图性质，对于每个素数 p 和每个无界的g，它都见证捕获失败。当 g 界定 *Sylow* p-子群的阶或其最小基大小时，这两个等价关系同样成立。

有界大小的基的各个元素允许使用一个固定元数的单一关系来编码整个标记轨道。反过来，我们从图中读取域以及流方程。于是，可解性对于所有素数都是一个 PTIME图性质。将每个图与具有相同长路径的 CFI 对中的另一个图作不交并，同时保持两个答案不变，并使每个自同构群的阶加倍。因此，在任意足够大的规模下，只要 g 超过这两个阶，我们就能满足该界。

我们首先对简单图上的流问题进行编码，并证明单素数逻辑保留由此得到的数对。随后，我们构造有序副本，并展示如何在其上计算查询。最后几节讨论具有有界对称性的图、奇部有界的循环图上的多项式时间前缀检验，以及可在奇圈上计算的计数。

语法与有序输出

记 V为顶点域， $I_n = \{0, \dots, n-1\}$ 为数域，其中 $n = |V|$。等号比较相同类型的元素。邻接是 V上的一个关系，序是 I_n上的一个关系。对于其他输入词汇表，所有输入关系的参数同样都是对象。若 D 是 R的参数类型的乘积，则

$$M_r R\,\varphi(R, \bar{a}) \quad \Longleftrightarrow \quad \big|\{S \subseteq D : \varphi(S, \bar{a})\}\big| \not\equiv 0 \pmod{r}.$$

对 R 的每一种解释，都会给出输入结构的一个扩张。Compton 和 Grädel（1996）将满足扩张的数量作为一种计数

函数进行研究。对于字符串，Kontinen 和 Vollmer（2010年）研究了关于一元关系的相关二阶量词。在这里， R 可以接受任一类型的参数。

该语言对于两种类型的布尔运算和一阶量化都是封闭的。我们采用 Gurevich 和 Shelah（1986年）的膨胀语义。一个体为 $\psi(T, \bar{x})$ 的不动点从 $T_0 = \varnothing$ 开始，并依次设置 $T_{h+1} = T_h \cup \{\bar{a} : \psi(T_h, \bar{a})\}$。它返回第一个稳定关系。在迭代过程中，参数保持其取值不变。该约定允许在体中使用否定和模测试，而无需单调性假设。同时表可以通过带有数值标签的一个关系来表示。这种编码中有限的例外定义域大小列表，都可以通过一阶情形处理。

规范化公式具有两个自由数变量。其输出是定义域为 I_n 、边由该公式定义并配备通常序的图。其图约化必须与输入同构，而同构的输入必须具有相同的输出。对于我们语言中的公式，后一条件是自动满足的，因为输入同构在 I_n 上作用为恒等元。该公式直接给出数值上的边，无需选择从 V 到 I_n的双射。只有在将输入定义为数值排序上的有序计算之后，我们才应用 Immerman–Vardi 定理。

图上的流问题

固定一个素数 p 和一个连通有序三正则图 $D = (W, F)$，其中 F 是其无向边集合。其上的 CFI 结构在一个独立于 p 的词汇表中编码了一个流问题（Grädel 等人，2019，Section 5）。对于每条边的每一种定向 e，其定义域都包含一个纤维 $\{(e, x) : x \in \mathbb{F}_p\}$。基序在有向边上诱导出一个序。定义域上的预序按边比较元素，并使每个纤维中的元素相互并列。后继关系在每个纤维中通过 $x \mapsto x + 1$ 作用，而逆关系则将 (e, x) 与 $(e^{-1}, -x)$ 连接起来。

一个负载 $\lambda : W \to \mathbb{F}_p$ 指定了净流出量。在每个顶点 w 处，按基序列出三条出边。它们的纤维上的三元关系恰好包含坐标之和为 $\lambda(w)$ 的三元组。将所得结构记作 $A(D, \lambda)$。只有关系属于词汇表。域坐标用于描述该构造。

用 $x \sim y$ 表示纤维预序中的等价关系，用 $J_0(x, y)$ 表示逆关系，并用 U 表示 CFI 三元关系。定义：当存在某些 $x' \sim x$、$y' \sim y$、$z' \sim z$ 满足 $U(x', y', z')$ 时，$U^*(x, y, z)$ 成立。它记录了与某个基顶点关联的有序纤维三元组。截面是一个集合 S，它从每个纤维中恰好选取一个元素。我们用 $\mathrm{Sec}(S)$ 表示这样的一阶条件：S 是一个同时满足两个约束的截面。当 $J_0(x, y)$ 成立时，选择 x 会强制选择其逆 y。对于三个已选元素 x、y、z，关联条件 $U^*(x, y, z)$ 会强制 $U(x, y, z)$。

引理（流计数）。在 $A(D, \lambda)$ 上，满足 Sec 的集合数量在 $\sum_{w} \lambda(w) \neq 0$ 时为零，否则为 $p^{|F| - |W| + 1}$。

证明。为进行计算，给无向边定向。每个正向纤维中选定的点指定一个域值。逆条件将反向纤维中的值固定为其相反数。三元条件恰好给出了规定散度为 λ 的带符号关联方程。将这些方程相加，得到必要的总和为零条件。反过来，选取一棵生成树，并为其外的 $|F|-|W|+1$ 条边任意赋值。每个叶节点方程都会确定与该叶节点相连的剩余树边。逐步剥去叶节点即可确定所有树边，而最后一个方程由总和为零条件保证成立。每个由此得到的流对应一个不同的集合 S。

例如，将四个顶点的完全图作为 $\mathbb{F}_2$ 上的基。它的六条边中有三条不属于某棵生成树。总负载为零时，有八个集合满足 Sec；总负载为一时则没有。对截面数量取模三即可区分这两种负载。若要排除模数为二的所有 公式，我们需要更大的基础图。

将见证编码为顶点集

图编码必须保留见证的数量。在证明下界时，它还必须使我们能够识别图元组上的关系。我们为每个元组使用一个单独的顶点，并为每个辅助顶点赋予一个在原结构上的唯一编码。

引理（关联编码）。对于一个固定的、元数均为正的有限关系词汇表，存在一种忠实编码 $J(A)$，可将其编码为简单图。其大小仅取决于 $|A|$。每个图顶点都可由一个有限标签和一个 A 元素构成的有界元组唯一表示。这些编码上的邻接关系是一阶可定义的。对象域及其关系都可以在图中一阶恢复。

证明。 首先为每个对象创建一个元素顶点。对于每个元数为s 的符号 U 以及每个 $\bar{a} \in A^s$，添加一个元组顶点、一个标记顶点和 s 个位置顶点。将每个位置顶点与元组顶点及其元素 a_j相连。当且仅当 $U(\bar{a})$成立时，将标记顶点与元组顶点相连。通过为每种类型附加不同的固定数量的私有叶节点（且始终至少为两个），区分元素、元组、标记和位置类型，并标明关系符号及位置索引。现在，元素、元组、标记和位置顶点的度至少为二。私有叶节点的度为一。每个非叶顶点的类型可根据其叶邻点的数量判定。因此，只需沿位置边并测试标记边，即可通过一个固定的一阶公式恢复元素顶点上的关系。每个结构同构都可扩展为图同构，而每个图同构都会导出一个结构同构。私有叶节点的编码由其父顶点的编码和固定的叶节点索引构成。所有编码域都仅取决于 $|A|$，即使元组的成员关系发生变化也是如此。

在简单图上，通过在解码后的元素顶点上解释 Sec(S)，并要求 S 的每个成员都是元素顶点，来定义 β(S)。于是，每个流在图上恰好给出一个见证。解码器和 β 都没有提及域大小。

在一个素数处的保持性

流计数说明了为什么对截面按 p 取模计数会丢失总负载。为证明不可定义性，我们针对任意 $\mathcal{L}_p$ 公式比较这两个 CFI 结构。我们首先描述元组轨道之间的对应如何扩展到关系。

固定 K，并考虑至多使用 K 个变量符号、允许任意合取和析取的公式。对于每个整数 $m \geq 0$，这些公式还允许使用一个量词，询问是否至少有 m 个元素满足某个公式。计数类型 $\mathrm{tp}_K(A, \bar{a})$ 是这些在 A 中关于 $\bar{a}$ 为真的公式的集合。若两个元组的类型相同，我们就称它们*相匹配*。若存在数值参数，则它们必须逐坐标相同。计数类型是在原始对象词汇表中定义的。证明中，我们用这些类型来比较结构。

两个结构之间的匹配关系

设 A, B 是具有相同词汇表和基数的有限结构，且 Γ_A, Γ_B 分别是它们的自同构群的 p-子群。假设空元组相匹配。另假设，对于长度至多为 $d \leq K$ 的元组，在任一结构中，两个元组具有相同的 K-类型，当且仅当它们属于其指定群的同一轨道。将赋予的对象参数组成的元组称为*上下文*。用 $\Gamma_{A,\bar{a}}$ 表示其逐点稳定子，即固定 $\bar{a}$ 每个分量的子群；并类似地定义 $\Gamma_{B,\bar{b}}$。假设上下文 $\bar{a}, \bar{b}$ 相匹配。对于 $|\bar{a}| + s \leq d$，对应关系

$$\Gamma_{A,\bar{a}}\bar{u} \iff \Gamma_{B,\bar{b}}\bar{v} \qquad \text{when} \qquad \mathrm{tp}_K(A, \bar{a}, \bar{u}) = \mathrm{tp}_K(B, \bar{b}, \bar{v})$$

是 s-元组上稳定子轨道之间的双射。事实上，在两个有限结构中实现的元组里，任意一个 K-类型都可以通过合取一些公式来单独刻画，这些公式能将它与其他已实现的类型区分开来。对 s 个新变量进行存在量化，即可在相同的 K 个槽中检验该类型是否能在上下文中实现。这些检验在匹配上下文中一致。在每一侧，扩展类型相等意味着存在一个群元素将一个扩展映射到另一个扩展，同时固定公共前缀。对于混合类型元组，我们在每个数值元组上分别使用相同的双射。

对于匹配上下文 $\bar{a}$，$\bar{b}$，记 $\tau_{\bar{a},\,\bar{b}}(S)$ 为与 S 中的轨道相对应的轨道之并，只要 S 是 $\Gamma_{A,\,\bar{a}}$-轨道之并。这种传递在每种允许的类型和元数的不变关系上构成双射。它保持并集和空关系。在纯数值的论域中，轨道都是单例，因此传递就是恒等映射。

公式决定了我们必须匹配多长的元组。令 t 为初始上下文中的对象变量数，包括所有自由对象变量。为所有约束变量指定不同的名称。令 b 为由单个量词约束或作为不动点体参数引入的对象变量总数。令 r 为公式中任一关系变量的对象参数数目的最大值；如果没有关系变量，则取 $r = 0$。于是，一个界 $d \geq t + b + r$ 涵盖每个子公式的上下文，以及关系的一个参数元组。重复的不动点阶段使用相同的变量。

引理（模关系量词下的保持性）。令$\varphi \in \mathcal{L}_p$，并令 A、B 满足上述轨道和计数型假设，且长度不超过¯。在匹配上下文 $\bar{a}$、b中计算 φ。对于每个自由关系，令其在 A 上的取值为 S，并使其在$\Gamma_{A,\ \bar{a}}$ 下不变；再令其在 B上的取值为$\bar{b}$（S），即$\tau_{\bar{a},}$。那么两次计算的结果相同。

证明。 我们对公式进行归纳，并在每一步保留外部上下文。

¯扩展上下文。 如果 $(\bar{a}, \bar{u})$ 和 $(b, \bar{v})$ 匹配，那么在$\bar{a}$ 处不变的每个关系 S 在 $(\bar{a}, \bar{u})$ 处也不变。此外，

$$\tau_{\bar{a}\bar{u},\bar{b}\bar{v}}(S) = \tau_{\bar{a},\bar{b}}(S).$$

扩展上下文中的对应轨道具有相同的扩展类型。忘掉新增坐标后，它们会映射为原始上下文中的对应轨道。 S 中的成员关系在每个原始轨道上都是恒定的，由此可证等号。特别是，当内部量词引入新参数时，受外部模量词约束的关系仍保持相同的解释。

原子公式因匹配的类型、数值参数相等以及关于自由关系的假设而一致。布尔步骤显然成立。对于一阶存在公式，用一个见证扩展上下文。轨道对应会在另一侧提供一个匹配的扩展。对于数值见证，使用相同的数。归纳假设适用，而且论证是对称的。

绑定一个关系。 对于 $M_p R\,\psi$ I_n A， $\bar{a}$ 的稳定子作用于满足 ψ、关于 R 的所有赋值构成的集合。由于其他自由关系均为不变关系，且对 R的每个赋值，公式求值都与自同构相交换，因此该集合在此作用下封闭。自同构将每个内部模测试的见证双射地映射到相应传输参数下的见证，并将每个不动点阶段映射到对应阶段。每个包含多个赋值的轨道，其大小都能被 p整除。因此，模 p 计数只取决于被稳定子固定的满足赋值。每个关于 R 的不动赋值都是其论元组上的若干轨道之并。轨道对应在两个结构之间将这些并一一对应。对 ψ 应用归纳假设，并对每一对对应的赋值进行考察，可知满足 ψ的赋值数量相同。因此，两个模计数相等。

迭代不动点。 令 $F_A(T)$ 表示原上下文 $\bar{a}$中的一次膨胀更新，并类似地定义 F_B。记作 $\tau = \tau_{\bar{a},\bar{b}}$。如果原稳定子固定 T，那么它也固定 $F_A(T)$，因为公式求值与自同构相交换。对于匹配的论元组 $\bar{u}, \bar{v}$，细化恒等式允许我们将 T, τ 及所有外层关系传递到主体。对主体应用归纳假设，可知在两侧对是否添加该元组会得出相同判断。旧的成员关系也一致。因此，更新满足

$$\tau(F_A(T)) = F_B(\tau(T)).$$

从空关系开始，在每个阶段 h 都得到 $T_h^B = \tau(T_h^A)$。 τ 的双射性意味着，两边恰好会在同一阶段发生变化，

另一边也会如此。在双方共同达到的稳定阶段，固定点公式的自变量处的成员关系一致。这个阶段论证只在更新体上使用归纳假设，而更新体本身可能包含不动点和模量词。

将引理应用于编码图

在同一个连通基底上，两个 CFI 结构同构，当且仅当它们的总负载相同。它们的自同构通过平移作用于边纤维，并构成一个 p-群（Grädel 等人，2019年，Sec 5.2 和定理 5.2）。

另外两个结果适用于有序三次扩展器基底。对于每个固定的K，在足够大的同一基底上，总负载不同的结构在所有 K变量计数句子上都一致（Grädel 等人，2019年，定理 5.6）。在任一结构中， ℓs 变量计数类型都能确定一个 s-元组的自同构轨道，其中常数 ℓ 与基底无关（Grädel 等人，2019年，定理 5.7）。给定元组界 d，先选择足够大的 $K \geq \ell d$ 以读取词汇表，然后再选择基底。这样便使 CFI 结构满足保持引理的两个假设。

证明（单素数下界）。固定一个拟议的规范化公式。将其元组长度界乘以图顶点编码（关联编码）中的对象坐标最大数量。使用这个扩大后的界，选取定义在同一基上、总负载分别为零和一的 CFI 结构 A、B 。令 Aut(A) 通过编码的坐标作用于 $J(A)$，并固定每个标签；同时在 $J(B)$上使用相应的作用。尽管具有相同父节点的私有叶节点也可以互换，这些指定群仍是 p-群。标签规定了这一作用在所构造图上的具体形式。拟议的规范化公式不会接收任何标签或叶节点索引。

当两个图元组的标签相同，且其串接后的对象坐标具有相同的计数类型时，就将它们匹配。对于固定的标签，扩展一个图元组相当于添加数量有界的对象坐标。因此，每个编码的唯一性给出了图元组上的轨道对应。遗忘一个图参数会恰好移除其标签和对象坐标，因此不变关系的细化恒等式也成立。原子邻接关系一致，因为它在编码上是一阶可定义的，且 K 取值足够大，可以容纳解码公式。这些图的大小相同，因此其数值参数通过等号匹配。

保持引理中的归纳只使用了原子公式上的一致性，以及一个与遗忘坐标相容的扩展轨道双射。图编码上的匹配同时提供了这两点，因此，对于每个数值对（$i,\ j$），所提出的公式在两个图上给出相同的答案。一个矩阵不可能同时是两个非同构图的副本。

证明（布尔分离）。固定 q 以及任意素数 $p \neq q$。对于编码 I_n 上 CFI 结构的图，流计数要么给出零个见证，要么给出 p 的幂。因此， $M_q S\,\beta(S)$ 在这些编码上恰好接受零总负载。若某个 $\mathcal{L}_p$ 句子定义了这个图查询，则前面对空

上下文的论证会使其在两个编码结构上具有相同的真值。这与计数结果矛盾。交换 p 和 q 的角色即可得到不可比较性。句法包含给出$\mathcal{L}_p \subseteq \mathcal{L}_{p,\,q}$，而所展示的句子使这一包含成为严格包含。

两个素数构成的典范矩阵

取两个不同的素数 p，q。框架将那些彼此只相差一个固定的 S_n 的西洛 p 子群中某个置换的标记归为一组。要用关系量词计数框架，我们需要为每个标记等价类指定一个关系。我们根据位置有序对的颜色来构造该关系。

框架及其标记

将 $n = \sum_h a_h p^h$ 写成以 p 为基的数。将 I_n 划分为一系列大小递减的连续槽，其中 a_h 个大小为 p^h 的槽分别编有索引。将每个此类槽中的元素对应到由 $\mathbb{F}_p$ 上长度为 h 的字组成的序列，顺序按数字顺序排列。对于一对位置，记录两个槽位索引。对于同一槽中不同的字，还要记录它们首次出现差异的位置，以及该处数字之差，并按参数顺序计算（第二个减第一个）。对角对和位于不同槽中的对使用不同标签，并将所有未使用的坐标固定为零。将此表视为关系 $\mathsf{Col}_n(i,\ j,\ \bar{c})$，其唯一取值 $\bar{c}$ 是一个定长数值元组。对于固定的 p，其各项均可在多项式时间内统一计算，因此有序不动点公式可以定义 Col_n。用 $v_p(n!)$ 表示 $n!$ 中 p 的指数。

引理（框架的群）。在颜色固定的情况下，表在其位置域上的自同构群 Q 的阶为 $p^{v_p(n!)}$。

证明。每个槽位都保持不变。在一个槽位内，第一个不同的位置决定了哪些数对在任意给定前缀上相同。因此，表的自同构会作用于前缀构成的有根树。如果它将一个节点映到另一个节点，则由此诱导的子节点数字之间的双射 σ 满足 $\sigma(b) - \sigma(a) = b - a$，对所有 $a,\ b$均成立。这是一个平移。反过来，在每个内部节点处选取一个平移，就定义了一个保持该表的树自同构。大小为 p^h 的槽位有 $(p^h - 1)/(p - 1)$ 个内部节点。因此，p在 $|Q|$ 中的指数为

$$\sum_h a_h \frac{p^h - 1}{p - 1} = \sum_{j \geq 1} \left\lfloor n/p^j \right\rfloor = v_p(n!).$$

对于一个双射 $f\colon\ V \to I_n$令 $H_f(u,\ v,\ \bar{c})$ 表示 $\mathsf{Col}_n(f(u)\ f(v)\ \bar{c})$。当且仅当 $gf^{-1} \in Q$ 时，两个映射f，g给出相同的关系。每个框架恰好是 $|Q|$ 个映射的拉回。因此共有 $n!/|Q|$ 个框架，该数模 p非零。

读取框架并选择前缀

各个节点处子节点的循环移位生成 Q。每次移位都保持后缀数字不变，而节点数仅为多项式级。将这些生成元作用于位置的无序对上，再次得到一个 p-群，因此是一个可解群。Babai 和 Luks（1983年，定理 3.3 和 3.5）的规范放置算法于是能在多项式时间内计算轨道 X 中的字符串 $\mathrm{cf}_Q(X)$，且该轨道中的所有字符串都得到相同输出。我们按字典序排列有序对 $i<j$，使用 $0<1$ 表示位，并遵循他们的首个轨道规则和首个最小块系统规则（第 3.2 节）。对于任何与框架 H兼容的标记 f，令

$$D(G,H)=\mathrm{cf}_Q(f(G)).$$

所有兼容标记都会给出相同的字符串，因为它们相差Q中的元素。

通过前缀 s 的长度或端点，以及其在序对 $i<j$的字典序中的已知位来编码该前缀。定义 $\theta(G,H,f,s)$，要求 $f\subseteq V\times I_n$ 是一个双射的图，要求 $H(u,v,\bar{c})$ 在每个参数上都与 $\mathrm{Col}_n(f(u),f(v),\bar{c})$一致，并要求 $\mathrm{cf}_Q(f(G))$以 s开头。最后一个检验是一个作用于带有编码 s的数值参数的有序图上的多项式时间谓词。将其转换为有序不动点逻辑，并代入

$$\exists u\,\exists v\,(f(u,i)\wedge f(v,j)\wedge E(u,v))$$

以替换传递过来的边关系。由此得到的关于 θ 的公式只使用一阶量词和不动点。

引理（统计具有给定前缀的框架）。该公式

$$M_pH\,(M_qf\,\theta(G,H,f,s))$$

当且仅当满足条件的框架 H 的数量 $D(G,H)$ 以 s 开头的部分对 p取模后非零时，公式成立。

证明。 对于无效表，没有双射能够通过拉回检验。对于有效框架，通过全部三个检验的映射数量要么为零，要么为 $|Q|$。由于 $|Q|$ 是 p 的幂，内部量词恰好接受具有指定前缀的有效框架。每个这样的框架为外部量词贡献一个赋值。

取一个由两条不相交边组成的图，并令 $p=2$。三个框架是将顶点划分为两对的三种方式，每种方式都有八种兼容标记。一个框架将两条边各自的端点配成一对，并将一个 1 放在首位。另两个框架将非邻点配成一对，并将一个 0 放在首位。利用 $q=3$，内部测试能识别出每个符合条件的框架，因为八模三不为零。有两个框架将空前缀扩展为 0，另一个框架将其扩展为 1。因此，奇偶性检验会选出 1。若按奇偶性统计标记，则两个子节点的计数都会是零。

证明（双素数构造）。令 $c_G(s)$ 统计放置字符串以 s 开头的框架数。空前缀处的计数与 p 互素。如果当前计数模 p 不为零，那么 $c_G(s0) + c_G(s1) = c_G(s)$ 意味着至少有一个子节点的计数模 p 不为零。若前缀计数引理中的测试接受 $s0$，则选择 0；否则选择 1。膨胀不动点存储三元组 (i, j, b)，记录已确定的位。其主体使用当前表和前缀测试，为第一个尚未确定的配对添加取值。根据归纳，每个阶段得到的都是计数不为零的前缀。经过 $\binom{n}{2}$ 步后，某个框架实现了整个字符串。该字符串是输入图的一个带标号副本。对输入图重新标号会将框架双射地映射，并保持其字符串不变，因此所有决策也保持不变。对称地读取存储的位，并令对角线为零。对于 $n \le 1$，输出边关系为空。

用一个预言机计算同一个矩阵。对于带标号输入，按固定顺序为框架表的每个条目猜测一个隶属位。每张表恰好对应一条分支。以下过程从每张有效表中恢复一个相容映射。根据对角线条目读取槽位索引。在每个槽位组内，按各个前缀长度下的一致性对叶节点分组，并使用首次差异字段。检查这些是否为大小符合要求的嵌套划分。在每个内部节点，选取包含最小输入顶点的子节点作为数字零所对应的子节点，并利用记录的差异确定其他顶点的位置。若任何检查失败，则拒绝。所有数字都分配完毕后，将整张表与沿所得双射的拉回进行比较。这个等号证明该表是一个框架。对于有效框架，平移对称性允许选择任意零子节点。用此映射计算 cf_Q，并检查前缀。接受路径计数恰好为$c_G(s)$。Mod$_p$P 预言机会在多项式数量的位置上回答零子节点查询。

在有序副本上求值

对于任意多项式时间图性质 P，Immerman–Vardi 定理给出了一个 IFP 句子 $\psi(E, <)$，用于在有序图上定义 P。在数值排序上运行 ψ，将每个邻接测试 $E(i, j)$ 替换为 $\gamma_{p,\,q}(i, j)$。根据规范化定理，ψ 所运行的图与输入图同构，因此所得句子定义了 P。已知矩阵后，对 ψ 求值只需通常的多项式时间。

我们还可以刻画那些可借助构造该矩阵的同一预言机计算的查询。固定 $\gamma_{p,\,q}$ 并允许有序 IFP 句子测试一个可定义的布尔电路是否具有模 p非零个满足赋值。用定长数字元组为门编索引，并拒绝格式错误或存在环路的电路描述。为表达这一测试，通过 M_p绑定一个门值关系，检查每个门及输出，并强制未使用的元组项为零。每个输入门上的满足赋值都唯一地扩展到所有门。

推论（在有序副本上求值）。在由$\gamma_{p,\,q}$定义的副本上求值时，带有模电路测试的有序不动点逻辑捕获了$\mathrm{P}^{\mathrm{Mod}_p\mathrm{P}}$中的同构不变布尔图查询。

证明。 首先使用 Mod$_p$P 预言机计算规范副本。对于任意固定的有序句子，关系表和不动点迭代的规模均有多项式界。每次电路调用的规模都是多项式的，并且在其描述求值后只需进行一次预言机查询。子公式的固定嵌套仍保持这一多项式界。

反之，取模电路可满足性作为完备预言机问题。多项式时间非确定性验证器可以表示为一个作用于其多项选择比特的电路，并将未使用的比特固定下来，同时保持路径计数不变。固定一个针对该查询的确定性多项式时间预言机机器。在有序副本上，元组为时间、带单元和查询门建立索引，范围截至该机器的多项式界。一个膨胀表记录每个时刻的配置。其后继行由固定转移规则给出；当执行预言机指令时，则使用前一查询带上的电路测试。初始行以及查询带的解码都是多项式时间有序谓词，因此可由有序不动点定义。接受状态定义了所需的句子。同构不变性保证了规范副本上的正确答案。

对称性界下的单素数

双素数构造通过用第二个素数检验框架的标记来进行计数。在单素数规范化定理的基假设下，我们可以直接计算标记的轨道。Wielandt（1969，定理 5.12）证明，$(k+1)$ 元组上的轨道能够确定一个具有大小为 k 的基的置换群。Köbler 和 Verbitsky（2008）利用整个自同构群的基，将并行规范化归约为彩色图的完备不变量。这里的基大小界适用于 Sylow 子群。输入既未提供该子群，也未提供基。指定候选图后，我们在数值排序上进行群计算。

当 $k = 0$ 时，我们有 $p \nmid |\mathrm{Aut}(G)|$，并且恰有 $|\mathrm{Aut}(G)|$ 个双射映射到 I_n，从而得到任意指定的副本。在数值排序上，单素数公式可以利用对预言机机器的有序模拟，检验该副本是否等于规范输出。统计通过此检验且在 $(i,\ j)$ 处给出 1 的双射数量，即可恢复规范比特。对于更大的 k，相同的重数模 p 后可能为零。因此，我们在一个适当的子群作用下统计双射的轨道。Faben 和 Jerrum（2015，引理 3.10）的一个相关结果指出，若两个图都没有阶为 p 的自同构，那么当它们来自每个图的同态计数模 p 后均相等时，这两个图同构。

用一个关系编码标记轨道

保留双素数构造中的 Sylow 子群 $Q \le S_n$ 和规范放置函数 cf$_Q$。对于顶点集为 I_n 的有序候选图 Y，令

$H_Y = Q \cap \mathrm{Aut}(Y)$，其中这里的自同构保持 Y的图约化。我们可以通过适用于在点对位置上作用的可解群 Q的 Babai–Luks稳定子算法（Babai 和 Luks, 1983年，引理 3.2 和定理 3.5），在数值排序上以多项式时间计算 H_Y 的生成元。对于 $n \geq 3$，此作用是忠实的，而且可以根据顶点置换在其关联点对上的作用还原该置换。较小的图可以直接处理。

假设 G 满足单素数规范化定理的基界 k。若 Y 是 G的一个副本，则 H_Y 属于 $\mathrm{Aut}(Y)$ 的某个 Sylow p-子群。根据 Sylow共轭性，该子群有一个大小至多为 k 的基，而这也是 H_Y 的一个基。我们只需要为这个最后的群找一个基。例如，在三角形上，单个顶点可以作为某个 Sylow 2-子群的基，尽管它在整个群 S_3 中的稳定子包含一个换位。

若某个候选 Y 可容许，则称其为可容许候选，当且仅当 $\mathrm{cf}_Q(Y) = Y$，且 H_Y 在 I_n^k中有一个基（允许重复元素）。对于一个可容许候选，取字典序最小的$^-$个这样的元组 b。根据其生成元计算 $|H_Y|$ （ Furst 等人，1980 ）。对于固定的 k，每个元组轨道的大小至多为 n^k，因此我们可以在多项式时间内枚举该轨道，并检验其大小是否等于 $|H_Y|$。在 $k = 0$ 处，唯一的候选基是空元组，且当且仅当 H_Y 是平凡群时，该候选基才通过检验。通过同样的枚举，可以在多项式时间内判定 $(k+1)$-元组的轨道成员关系。有序不动点逻辑可以定义这两种检验。

对于同构 $f\colon G \to Y$，定义混合类型关系

$$R_f(\bar{x}, u, i) \iff (\bar{b}, i) \in H_Y \cdot (f(\bar{x}), f(u)), \qquad \bar{x} \in V^k, \quad u \in V, \quad i \in I_n.$$

$^-$除非存在某个 $h \in H_Y$将 $f(\bar{x})$ 映射到 b，否则它在 $\bar{x}$ 处的切片为空。这样的 h 是唯一的$^-$，因为 b 是一个基。此时，该切片就是 hf的映射的图。反过来，每个 hf 都会出现在 $(hf)^{-1}(\bar{b})$ 处的切片中。因此，所有互不相同的非空切片恰好是轨道 $H_Y f$中的映射。

引理（每个标记轨道对应一个关系）。对于每个可容许的 Y，存在一个在顶点上使用一阶量词、在数值排序上使用不动点的公式，恰好识别关系 R_f。每个从 G 到 Y的同构的 H_Y-轨道对应一个这样的关系。

证明。对于一个候选关系 R，对顶点元组 $\bar{x}_0$ 作存在量化，并将切片 $R(\bar{x}_0, u, i)$ 视为映射 g的映射的图。验证它是一个双射，并且将 G 的边和非边映射到 Y的边和非边。对每个参数检验定义 R_g 的等价关系，并在 g 出现之处使用该切片。如果检验通过，则 $R = R_g$。对于 $R = R_f$， $\bar{x}_0 = f^{-1}(\bar{b})$ 处的切片给出 $g = f$，因此检验通过。与 H_Y 后复合会保留 R_f。反过来， $R_f = R_{f'}$ 意味着等于 f'的切片也出现在 R_f中，因此对于某个 $h \in H_Y$， $f' = hf$。元组 $\bar{x}_0$ 是检验中的普通存在性见证，因此选择它不会使关系计数出现重数。

对于前缀 s，统计满足以下条件的数对 (Y, R)： Y 是可接受的、扩展 s 的 Q-规范图，且 R 满足轨道编码条件。一个绑定子 M_p 即可统计这些数对。在一个混合类型关系中预留两个数值标签，

一个用于 Y，另一个用于 R。对于每个标签，要求成员关系不依赖于未使用的坐标。禁止使用任何其他标签。这样，在大小至少为二的定义域上，每个数对都恰好编码一次。候选邻接关系必须是对称的，且对角线为空。

令 $a = |\mathrm{Aut}(G)|$。从 G 到指定副本 Y 有 a 个同构。H_Y 对这些映射的自由作用产生 $a/|H_Y|$ 个不同的、针对 Y 的关系。反过来，Y 的 Q-轨道包含 $|Q|/|H_Y|$ 个带标号图。对每个副本轨道的唯一 Q-规范代表求和。所有这些代表都是可容许的，因此空前缀处的计数为

$$\sum_{Y} \frac{a}{|H_Y|} = \frac{a}{|Q|} \sum_{Y} |Q \cdot Y| = \frac{a}{|Q|} \frac{n!}{a} = [S_n : Q].$$

这个整数与 p 互素。在每个前缀处，相同的配对 $(Y,\ R)$ 会按 Y 的下一位进行划分。因此，我们可以利用前缀不动点来选出一个完整字符串。重新标号 G 会传递 R 并固定 Y，所以每种输入标记都会得到相同的字符串。

对于带标号输入，每个固定的 $\mathcal{L}_p$ 公式的数据复杂度都属于 Mod$_p$P。为此，对语法作归纳，并将当前自由关系作为显式表提供。模绑定量词猜测一张表，并通过一次预言机调用检验其体。对于固定公式，个体量化和不动点迭代只需要多项式次这样的调用。根据素模低阶定理 Mod$_p$P$^{\mathrm{Mod}_p\mathrm{P}}$ =Mod$_p$P（Beigel 和 Gill，1992，定理 6.7 和推论 6.8），归纳得以完成。反过来，在给定的等价类上，矩阵公式提供了一个有序副本。有序电路检验随后用相同的素数来表达每个不变的 Mod$_p$P 查询。因此，$\mathcal{L}_p$ 的句子恰好定义了这些查询在该等价类上的限制。即使多项式时钟图灵机仅在该承诺条件下正确，也能得出相同结论。在可定义矩阵上的模拟对所有输入都保持不变，并且在承诺的等价类上与该查询一致，即便该等价类的成员关系不可判定也是如此。

一个适用于所有素数的多项式时间见证

我们在所有简单图上定义一个布尔查询 U。首先，对 CFI 签名应用关联编码的一阶解码器。要求解码域非空、其上存在一个全预序，并且后继关系在该预序的每个等价类上各由一个有向环组成。要求所有环具有相同的素数长度 r。若任一项检查未通过，则拒绝。

在每个环中选择一个原点，并沿其后继关系，为其中的元素赋予 $\mathbb{F}_r$ 中的坐标。对每个等价类 C，在该域中引入一个未知量 z_C。对于解码得到的逆关系和三元关系，按其元组所对应等价类的有序列表对元组进行分块。每个列表为（C_1，……，C_j）的非空块给出一个表 $B \subseteq \mathbb{F}_r^j$，其中 $j = 2$ 或 3。要求 B 为一个仿射子空间，并施加约束（z_{C_1}，……，z_{C_j}）$\in B$。空块不产生约束。仅当所有测试均通过且所得方程组可解时接受。

这定义了一个不变的多项式时间查询，即使面对格式错误的编码也成立。高斯消元计算每个非空块的仿射包及其方程。仿射包维数为 e 的块，当且仅当它含有 r^e 个条目时，才恰好等于其仿射包。通过消元求解合并后的方程组。域大小至多为输入大小。改变原点会使每个未知量及其在所有表中的出现统一平移相同的偏移量。因此，可解性以及对仿射子空间的测试均与这些选择无关。对于编码的 $A(D,\ \lambda)$，逆块施加取负约束，而三元块规定每个顶点处的和。流计数给出

$$U(J(A(D,\lambda))) \quad \Longleftrightarrow \quad \sum_{w} \lambda(w) = 0.$$

域可从图中读出，因此该查询对所有素数都是公共的。

Blass 等人（2002）使用填充的 CFI 结构，将带计数的定点逻辑与无选择多项式时间区分开来。他们通过填充孤立顶点，允许对这些顶点进行任意置换。这里，完整自同构群的阶是条件的一部分，因此我们使用单条路径。

固定 p、一个无界的 g，以及一个候选的 $\mathcal{L}_p$ 公式。按照单素数下界，选取其编码的 CFI 对 X_0, X_1。令 m 为它们的公共阶，并令 $a_* = \max_i |\mathrm{Aut}(X_i)|$。$g$ 的每个尾部都是无界的，因此存在 N，使得 $N - m > \max(m, 3)$ 且 $g(N) \geq 2a_*$。向每个图中添加一条包含 $N - m$ 个顶点的不相交路径。它比每个旧连通分量都大，并且具有两个自同构。因此，新的自同构群的阶为 $2|\mathrm{Aut}(X_i)|$，且两个填充后的图都属于 $\mathcal{G}_g$。路径上的顶点都没有解码器所要求的两个叶邻点，因此 U 仍能区分这两个图。

将每个核心 X_i 上指定的 p-群扩展为在路径上作用恒等元。按照单素数下界匹配核心坐标，并通过等号匹配路径顶点和数字。一旦指定了元组中的路径顶点和数字，其稳定子轨道便由其核心坐标确定。因此，轨道对应关系也扩展到混合元组，并且仍与遗忘参数操作相交换。邻接关系得以保持，因为路径与核心互不相交。

这些正是保持引理归纳过程中所用的假设。模绑定子匹配扩展轨道的并集，而定点更新在每个阶段都保持这种匹配。公式的元组长度界不依赖于 N。因此，这两个填充后的图在所提出的句子上等价，尽管 U 能将它们区分开来。类似地，所提出的规范化器会为这两个非同构图赋予相同的矩阵。

对于有界情形，设 $|\mathrm{Aut}(G)| \leq C$。只要西洛 p-子群中的当前逐点稳定子非平凡，就选取一个被它移动的顶点。固定该顶点会使其阶至少缩小 p 倍。至多经过 $\lfloor \log_p C \rfloor$ 次选择后，稳定子就变为平凡，因此有界基结果适用。当 C 仅限制西洛子群的阶时，同样的论证也成立；而对基大小的限制本身就是所需假设。反过来，填充后的例子满足所有三种无界限制，因为整个群的阶同时限制了另外两个参数。单素数规范化定理中的等价关系涉及

仅由数值上界指定的等价类。具有无界自同构群的特定图类，例如完全图，仍可能具有可定义的规范副本。

多项式时间求值还剩下什么

该构造在有序副本上表达了每一种 PTIME图性质。其求值开销来自模前缀测试。Lichter 和 Schweitzer（2024）在带有见证化对称选择的无选择多项式时间中，得到了另一种联系。在他们的逻辑中，对于在个体化下封闭的等价类，可定义同构蕴含可定义规范化。

对于完整语言，模电路可满足性已经会出现在简单图上。用关联编码表示布尔电路的门类型和连线。一阶公式要求一个顶点集恰好由一致求值中被赋值为真的门组成，且输出为真。每个可满足的输入都恰有一个这样的扩展，因此，M_r 应用于该公式即可测试模电路可满足性。该编码可在多项式时间内完成。若能对每个固定的 $\mathcal{L}_{p,q}$ 句子进行多项式时间求值，那么 Mod$_p$P 和 Mod$_q$P 都将属于 P。

前缀测试。 固定素数 p, q 以及规范放置算法。若s 已到达 某个位置，即称其在 G 上构造矩阵的过程中出现。考虑如下承诺问题：输入为 G 和一个已到达但尚未完成的前缀 s。 $c_G(s0)$ 模 p是否非零?

该测试与矩阵在多项式时间内等价。从空前缀开始，$\binom{n}{2}$ 调用即可恢复矩阵，并且每次调用都使用迄今为止到达的前缀。反过来，给定矩阵，读取 s之后的位。当且仅当$c_G(s0)$模 p非零时，该位为零。因此，若存在一个用于该测试的多项式时间算法，就可以通过在副本上求值，得到一个捕获多项式时间的逻辑。比较两个图的矩阵也可以在多项式时间内判定同构。

有界奇部的循环图

如果一个图具有一个由单个环组成、且遍历其所有顶点的自同构，则称其为循环图。如果环长度的奇部有界，则旋转的二幂阶子群固定的框架数量仅为多项式数量。

命题（有界奇部的循环图）。固定 M。对于阶为 $n = m2^h$、 m 为奇数且 $m \le M$的循环图，仅根据图本身即可在确定性多项式时间内计算每个框架前缀奇偶性。因此，对于任意奇素数 q，在副本$\gamma_{2,q}$上求值的普通有序*IFP*在此等价类上捕获多项式时间。

证明。 Evdokimov 和 Ponomarenko（2004，定理1.1）可在多项式时间内计算出一个圈基。在循环图上，这给出了一个全循环自同构σ。令 $L = 2^h$。置换 $\tau = \sigma^m$ 有 m 个长度为 L的循环。由 τ 生成的循环群具有二幂阶，并保持其移动的每个框架的放置字符串

因此，每个前缀奇偶性都是其匹配的τ-固定框架的奇偶性。

当 $m = 1$ 时，这样的框架只有一个。沿着 σ I_n$\mathbb{Z}/2^h\mathbb{Z}$ 为顶点编号。固定二叉树的每一层都是一个在平移下保持不变的划分。包含零的块是一个子群，其余块则是它的陪集。在深度 j 处，循环群有唯一一个指数为 2^j 的子群。因此，各层恰好是模 2^j 的剩余类划分。只需对这个显式框架进行一次布局，就能回答所有前缀查询。

对于有界的 m，顶层槽的大小 kL 各不相同，其中 k 取遍 m 中出现的二次幂。将 τ 的整环分配到这些槽中，至多有 $m!$ 种方式。令 $F(k,\ L)$ 表示一个槽上由其 k 个环保持不变的平衡树数量。我们有 $F(1,\ L) = 1$，而 $F(k,\ 1)$ 计算 k 个叶节点上的所有平衡树。对于 $k,\ L \geq 2$,

$$F(k, L) = \tfrac{1}{2}\binom{k}{k/2} F(k/2, L)^2 + 2^{k-1} F(k, L/2).$$

在第一项中，每个根节点子节点分到一半的环。在第二项中，τ 交换这两个子节点，因此它们的叶节点沿每个环交替出现。共有 2^{k-1} 种无序的半数选择。其中一半带有 τ^2 的 k 个长度为 $L/2$ 的环。选定它的树后，另一棵树就由平移确定。

固定 k，对 k 进行归纳可得 $F(k,\ L) = O_k(L^{k-1})$。事实上，第一项为 $O_k(L^{k-2})$。除以 L^{k-1} 得到 $f(L) \leq f(L/2) + O_k(1/L)$，其中$f(L) = F(k,\ L)/L^{k-1}$。误差项在所有二的幂上的总和有界。相同的划分也能枚举这些树。始终先处理包含最小输入顶点的子节点，以避免重复。每种部分选择都能扩展为一个输出，且通往某个输出的路径至多包含 $n - 1$ 次划分。因此，平均而言，枚举过程为每个输出至多访问 n 种部分选择。每种选择都能在多项式时间内完成。m 的界保证了槽位数量的乘积关于 n 为多项式。对每个由此得到的框架运行 placement，并将所请求的前缀按模二计数。答案只取决于原始框架计数，因此算法返回的任何完整环都会给出相同的答案。通过在这个副本上计算有序 IFP，即可得到捕获断言。

奇圈上的奇偶性检验

按顺序为奇数环编号，就能得到它的规范形式。要计算由双素数构造定义的矩阵，我们必须恢复奇偶性检验选出的位。每个框架都是一片由满二叉树组成的森林，二进制展开中每个 2 的幂对应一棵树。单例槽位提供了一个特定叶节点。旋转该环，直到此叶节点位于顶点 0。于是，每个锚定框架对应 n 次旋转，这是一个奇数。关于 0 反射会将其余框架两两配对，除非反射保持它们的树不变。令 $\mathcal{F}^{\rho}$ 表示在此反射下保持不变的锚定框架。对于每个前缀 t,

$$c_{C_n}(t) \equiv \left|\{F \in \mathcal{F}^{\rho} : D(C_n, F) \text{ begins with } t\}\right| \pmod 2.$$

例如，在 C_7 上，有九个在反射下保持不变的锚定框架。其中七个将 00 排在首位。在这七个中，三个接着是 0，四个接着是 1，因此算法选出 000。统计这个环所有带标号副本，会给相同的字符串赋予不同的重数。

对于下面的计数，固定 $p = 2$ 并写出 $n = 2k + 1 \geq 5$。令 $B = 2b$ 为不超过 n的最大 2 的幂。按 0、1、……、k、$-k$、……、-1 的顺序写出该环，并在 0 处设置单例槽位。反射将 i 映射到 $-i$。我们采用双素数构造的放置算法和数值对顺序。在 C_3 每次放置中，所得字符串都是 111。

矩阵开头和末尾的计数

第 Q 个轨道中的第一个输出位置（0、1）由最大槽位中的 b 个兄弟对组成。Babai–Luks 算法将当前定义域中最小位置的位最小化。在非传递调用中，它首先放置该位置的轨道。在传递调用中，它保留递归放置字符串中最小的一个。对这两种情况进行归纳即可得到该结论。因此，当且仅当所有 b 个兄弟对都是环边时，所放置的第一位才为 1。

对于 2 的幂 h，令 $T(h)$ 统计在具有 h 个对换的对合下保持不变的、具有 $2h$ 个指定叶子的平衡二叉树数量。这是循环图计数中的 $F(h,\ 2)$ 项。我们有 $T(1) = 1$，并且对于 $h \geq 2$,

$$T(h) = h! + \tfrac{1}{2}\binom{h}{h/2} T(h/2)^2.$$

阶乘统计的是两半相互交换的树。包含最小叶子的那一半包含来自每个对换的一片叶子，因此该半边有 2^{h-1} 种选择。其叶子可以构成 $h!/2^{h-1}$ 棵树，其中每棵树都唯一确定另一半中的反射树。第二项统计的是两半保持不变的树。

将 $r = \sum_j h_j$ 写成互不相同的 2 的幂之和。共有

$$A(r) = r! \prod_j \frac{T(h_j)}{h_j!}$$

种方法可将 r 个指定的反射对分配到大小为 $2h_j$ 的槽中，并在每个槽中选择一棵反射不变树。空积给出 $A(0) = 1$。总共有 $A(k)$ 个锚定的反射固定框架。将一个放在首位的数量为

$$N_1 = \binom{k - b/2}{b/2} T(b/2)\, A(k - b).$$

要看出这一点， b 兄弟边必须构成一个与单例不相交的反射不变匹配。由于 b 是偶数，该匹配不会包含由反射固定的唯一一条边 $\{k, -k\}$。在路径 1、……、k 上选取 $b/2$ 条互不相交的边，并取它们的镜像。将 b 条边收缩后，所得叶节点在上层树中构成 $b/2$ 对反射对。未使用的反射对填满剩余的槽。两个首位

计数因此分别为 $A(k) - N_1$ 和 N_1。这项计算中的所有整数都占用$O(n\log\ n)$位。

在第二个位置（0，2）处，每个框架都置零。在$\{0,1\}$和 $\{2,3\}$内进行交换会保留所有兄弟位，因此下一个轨道包含全部四个跨对。由于 C_n 不包含四圈，其中至少有一个是非边。在 C_7上，固定双叶槽中的距离对 $\{i,-i\}$ 。四叶槽有三种可能的兄弟划分。检查其跨对可得，$i=2$ 的前缀为000，000，000，而 $i=1$，3各自的前缀为100， 001，001。

补全最后几行。令 R 由 n位置上某个前缀的所有必需边组成。如果某个顶点的度超过二，或某个环使用的顶点少于 n 个，则无法完成。可以直接测试生成圈。否则， R由 $u=n-|E（R）|$ 条路径组成，其中包括孤立顶点。每种补全都会按循环顺序排列这些路径，并为非平凡路径确定方向。枚举以此方式得到的不同循环，丢弃违反指定零值的循环，仅保留满足 $\mathrm{cf}_Q（Y）=Y$ 的循环 Y。

根据 Sylow 基数界下的轨道计数，一个保留的环的重数为 $2n/|Q\cap \mathrm{Aut}(Y)|$。$Q$ 中的每个元素都固定单例槽位。在固定该顶点的环自同构中，只有恒等元和它的反射两种可能。因此，当且仅当反射保持二元框架时，重数为奇数。通过遍历，可以确定反射交换的顶点。接着，我们检查反射是否保持二元森林的每一层。通过记录每个被接受的环的下一位，可以在 $2^{O(u\log(u+1))}n^{O(1)}$ 时间内得到两种子节点奇偶性。在已完成的行之后还剩下 r 个顶点，而所有$2u$ 缺失的关联都属于这些顶点，因此 $u\le r$。特别是，最后$O(\log\ n/\log\log\ n)$ 行可以通过多项式时间检验。

初始前缀与二叉子树

令 d 为 2 的幂，且满足 $2\le d\le B$。在每个槽位中，取大小为 d 的子树的叶集；若整个槽位更小，则取整个槽位。将这些集合称为单元。最大的槽位中，前$d-1$ 个位置为 (0，1).....，(0，$d-1$)，它们都属于同一个单元。最大的槽位中这些单元内部的点对集合是 Q-不变的。在初始位置放置完毕之前，最小剩余位置的轨道包含于此集合中。对这样的轨道进行的每次调用只读取其内部位。因此，最大槽位的框架单元中的导出子图决定了最先放置的 $d-1$ 位。

对每个固定的初始长度进行多项式时间检验。单元类型记录了叶节点为 d 的二叉树及其导出子图，并视保树同构为同一类型。对于固定的 d，类型的数量与 n 无关。枚举其可能的重数m_T，使其总和为 B/d。为计算这些类型的互不相交的框架单元的选取数，取每种类型的 m_T 个编号副本，并计算将它们的叶节点单射到环上的单射数。在每个单元内部，要求边存在并禁止非边存在。不同单元之间的所有点对均不受限制。

对于类型 T，将禁用边的一个子集加入必需边中，并为该项赋予该子集对应的容斥符号。度数

大于二的顶点会使嵌入无法成立。环也会导致这种情况，因为 $B < n$。在其他每一项中，图都是路径并。将 $x^c y^a$ 连同相应的符号记录下来，其中 c 计数所有路径分支，包括孤立顶点，而 a 计数非平凡的路径分支。令 P_T 为所得的多项式。在 $\prod_T P_T^{m_T}$中，将 $x^c y^a$ 的系数乘以

$$n(c-1)!\,2^a \binom{n-B+c-1}{c-1}.$$

选择一个顺时针方向。指定路径从 n 个环位置之一出发。按环上顺序排列其余位置，为非平凡路径确定方向，并将 $n-B$ 个未使用的顶点分配到各个间隙中。求和即可得到单射计数。将这个整数除以 $\prod_T m_T!\,|\mathrm{Aut}(T)|^{m_T}$。阶乘消去了相同类型单元的排列。自同构因子消去了与其编号代表之间的同构。该乘积在每个变量中的次数至多为 B，且其系数的二进制位长度为多项式级。

剩下的工作是对连接各单元的树求和。按局部性，置换相同类型的单元不会改变测试结果。对于每种类型，将其 m_T 个单元划分成若干批次，每批的大小对应 m_T的二进制展开中的一项。在每个批次上放置一棵固定的二叉树。这些树的自同构群的乘积是一个 2-群，因此只有被其固定的上层树会对奇偶性作出贡献。每个批次都必须完整保留，并具有规定的层级结构。若一个换位固定所有其他叶节点，那么被它交换的两个叶节点必定是兄弟节点。归纳可知，若交换两个已识别的子树并固定它们以外的所有部分，则这两个子树也必定是兄弟节点。反过来，每棵连接这些完整批次的平衡树都会被固定。

如果有 s 种类型，则每种大小至多有 s 个新批次进入，且至多有 s棵树从前一种大小到达。在每一层，按所有可能的方式将这些树两两配对。对于固定的 d，每层至多有 $(2s)!$ 种选择，共有 $O(\log n)$ 层，因此树的数量为多项式级。对于每棵上层树，将单元之外的边设为零，然后运行放置过程。将通过前缀测试的方案数的奇偶性乘以单元选择数。最大槽位之外的森林有奇数种选择，即其在对称群中所属的二叉树群的编号。对重数求和即可得到所需的奇偶性。运行时间多项式的度取决于 d。

对增长单元的抵消。 假设 $B > 2d$。考虑在反射下保持不变、且反射交换最大树的两个子节点的锚定框架。对于长度至多为 $d-1$ 的每个前缀，给出该前缀的这类框架数量为偶数。即使 d 随 n 增长，这一结论仍然成立。

为证明这一点，按照包含 i 的单元的反射轨道，对距离标签 1，……，k 进行分组。包含 $-i$ 的单元也位于同一轨道中。固定由此得到的距离标签划分。对于每个部分中的每个极大连续区间，在该区间上交换 i 和 $-i$。这些置换保持该划分不变，且与反射可交换。它们保持所研究的锚定族，包括关于最大树的两个子节点的条件。

翻转只会改变区间边界两侧的邻接关系。在那里，两个连续标签属于不同的单元轨道，因此没有任何改变后的边对是

单元内部的。每次翻转都保持与 0 相 incident 的边集合不变，并将边 $\{k, -k\}$ 作为集合固定。根据局部性，每个前缀测试在由这些翻转生成的 2-群的轨道上都是常数。只需考虑在每次翻转下都固定不变的框架。如果反射在这样的框架中交换两个单元，那么它们的距离标签构成一个单一区间。否则，翻转某个极大区间将只把一个单元的一部分移到其镜像处。翻转整个区间会交换这两个单元，并固定所有其他叶节点。这些单元必须是兄弟节点，因为在它们的最近公共祖先处进行交换会移动其下方的每个叶节点。因此，反射将大小至少为 $2d$ 的每棵子树作为集合固定。当 $B > 2d$ 时，它无法交换两个根节点子节点，从而证明了抵消。对于 $B \geq 8$，我们可以取 $d = B/4$。

在 C_{17} 较后到达的前缀处，抵消失败。移除单例后，剩下的路径具有唯一的完美匹配。将其边收缩为八个叶节点后，只需检查这些叶节点上的 $315 = 8!/2^7$ 棵平衡树。保留经路径反转后仍保持不变的 51，并对每棵扩展树应用规范放置算法。在到达的前缀 $1\,0^{10},$ 处，交换的两半和保留的两半对应的零和一计数分别为 (21，1) 和 (27，0)。合起来得到 (48，1)，因此交换的两半决定了下一位。

邻接位表示的宽度

令 S_s 为所有延伸自 s 且具有奇数框架重数的不同放置环所构成的集合。一个逐点因式分解 将其指示函数表示为 $\sum_z \prod_i f_i(Y,\ z)$，对于邻接位 Y_e的每一种赋值，该式都在 $\mathbb{F}_2$ 上成立，并带有辅助布尔变量 z。随后对除下一邻接位以外的所有变量求和，即可得到两个子节点的奇偶性。

在树分解中，每个节点都带有一组变量，即袋。每个因子的变量都共同出现在某个袋中，而包含每个变量的袋构成一个连通子树。宽度为 w 的消去序会产生大小至多为 $w + 1$ 的袋。

命题（前缀 00处的宽度）。对于 $n = 2^a - 1 \geq 7$，前缀 00 在 C_n 上达到。S_{00} 关于其邻接位的任意逐点因式分解，其袋大小为 $\Omega(\sqrt{n})$。

证明。存活族的大小。这里 $k = 2b - 1$。在第一位的计数中，$b/2$ 是 2 的幂。令 $h = b/2$，二项式系数为 $\binom{3h-1}{h}$。它是偶数，因为在 $\mathbb{F}_2$ 上，x^h 在 $(1 + x)^{3h-1} = (1 + x^{2h})(1 + x)^{h-1}$ 中的系数为零。根节点计数为奇数，因此算法选择 0。根据上文的兄弟节点交换论证，第二位始终为零。

至少有 $k!/2^k$ 个不同的 S_{00}成员。将每个反射对$\{i, -i\}$ 设为兄弟对，并在这些 k 对上任意选择一个二元框架。选择数为 $k!/2^{v_2(k!)}$。只有一个反射对是环边，因此最大的槽位包含一个兄弟非边，且已放置前缀为 00。两个锚定框架具有相同的放置字符串，当且仅当存在一个固定 0 的环自同构将其中一个映射到另一个。所有这类自同构都会固定每个构造出的框架。因此，这些字符串彼此不同，并且每个字符串在锚定不动框架中恰好出现一次。

固定度数的计数界。设 $\mathcal{F}$ 是定义在 m 条可能的边上的任意一族，其度数向量均为 D，且每个图有 $q \geq 1$ 条边。如果其指示函数的袋大小为 W，令 $b' = W + \lceil \log_2(2m+1) \rceil$。我们断言 $|\mathcal{F}| \leq (8b')^q$。

对每个可见位，在包含它的袋上附加一个叶节点，并用等号读取该位。将高阶袋拆分为由相同袋组成的二叉树，剪去不含可见叶节点的分支，并压缩一元节点。在所得二叉树中，m 个叶节点对应可能的边位置。对于任意一个割，行和列分别由割两侧的赋值索引的指示函数矩阵，其秩至多为 2^W。固定共享袋变量后，各因子便彼此独立。对这些变量的赋值求和，至多得到 2^W 个外积；对于 $\mathbb{F}_2$ 也同样如此。叶割的秩至多为二。

在后代侧实现的每个度数向量 u，都要求另一侧具有向量 $D - u$，其中度数均按整数计算。按这些向量对行和列分组。不同的已实现向量对应互不相交的非零对角块，因此每个割至多有 2^W 个这样的向量。

要从该族中编码一张图，就标记与其边对应的 q 个叶节点。自底向上处理，一旦某个非根子树包含至少 b' 个仍附着的标记，就将其分离。每个向上传递的子树所带的标记少于 b' 个，因此每个所得部分至多含有 $2b'$ 个标记。至多进行 $\lfloor q/b' \rfloor$ 次割。记录每个割以及整个原始后代子树的度数向量。用空白符号将列表补齐至 $\lfloor q/b' \rfloor$ 项后，可能的取值至多有 $((2m+1)2^W)^{\lfloor q/b' \rfloor} \leq 2^q$ 种。

从部分子树向量中减去其正下方割处的向量（在根节点使用 D），即可得到该部分内部的度数。若其中有 $j > 0$ 条带标记的边，这些度数便确定了 $2j$ 个带标签的边端点。至多需要考虑 $(2j)^j \leq (4b')^j$ 种配对。没有边的部分只有一种可能的图。将各部分的数量相乘，每条记录至多对应 $(4b')^q$ 张图，从而证明了该结论。现在取 $m = \binom{n}{2}$ 和 $q = n$。两个界给出 $8b' \geq (k!/2^k)^{1/n} = \Omega(\sqrt{n})$。减去对数项后，便得到所述的 W 下界。

定长算法可以在多项式时间内计算 00 处两个子节点的奇偶性。它无需在所有邻接位上表示 S_{00} 的成员关系。

即使对于奇圈，能否在每个到达的前缀处都于多项式时间内计算两个子节点的奇偶性，仍未解决。若能在任意图的每个到达前缀处，对零子节点进行多项式时间测试，那么通过在规范副本上求值，就能得到一种刻画多项式时间的逻辑。

参考文献

Albert Atserias、Andrei Bulatov 和 Anuj Dawar（2009）。仿射方程组与计数无穷逻辑。理论计算机科学410(18), 1666–1683。László Babai 和 Eugene M. Luks（1983）。图的规范标记。载于第*15*届*ACM*计算理论年会（*STOC*），171–183。

Richard Beigel 和 John Gill（1992）。计数复杂性类：阈值、奇偶性、模计数与少数性。理论计算机科学103(1), 3–23。Andreas Blass、Yuri Gurevich 和 Saharon Shelah（2002）。无序结构上的多项式时间计算。符号逻辑杂志67(3), 1093–1125。Jin-Yi Cai、Martin Fürer 和 Neil Immerman（1992）。图识别所需变量数量的最优下界。*Combinatorica* 12(4), 389–410。Kevin J. Compton 和 Erich Grädel（1996）。计数函数的逻辑可定义性。计算机与系统科学杂志53(2), 283–297。Anuj Dawar、Erich Grädel 和 Wied Pakusa（2019）。同构的近似与带线性代数算子的逻辑。载于第*46*届国际自动机、语言与编程研讨会（*ICALP*），LIPIcs 132，112:1–112:14。Sergei Evdokimov 和 Ilia Ponomarenko（2004）。循环图：多项式时间内的识别与同构测试。圣彼得堡数学杂志15(6), 813–835。John Faben 和 Mark Jerrum（2015）。奇偶图同态的复杂性：初步研究。计算理论11(2), 35–57。Merrick L. Furst、John E. Hopcroft 和 Eugene M. Luks（1980）。置换群的多项式时间算法。载于第*21*届计算机科学基础研讨会（*FOCS*），36–41。Vaani Goenka 和 Aalok Thakkar（2026）。通过模计数进行图与张量规范化。配套手稿。Erich Grädel、Martin Grohe、Benedikt Pago 和 Wied Pakusa（2019）。命题证明复杂性的有限模型论视角。计算机科学中的逻辑方法15(1), 4:1–4:55。修正版，2022年。Erich Grädel 和 Wied Pakusa（2019）。秩逻辑已死，秩逻辑万岁！符号逻辑杂志84(1), 54–87。Martin Grohe（2017）。描述复杂性、规范化与可定义图结构理论。逻辑讲义47。剑桥大学出版社。Yuri Gurevich（1988）。逻辑与计算机科学的挑战。载于 E. Börger 编，理论计算机科学当前趋势，1–57。计算机科学出版社。Yuri Gurevich 和 Saharon Shelah（1986）。一阶逻辑的不动点扩展。纯粹与应用逻辑年刊32, 265–280。Neil Immerman（1986）。可在多项式时间内计算的关系查询。信息与控制68(1–3), 86–104。Johannes Köbler 和 Oleg Verbitsky（2008）。从不变量到并行规范化。载于计算机科学：理论与应用（*CSR*），216–227。Juha Kontinen 和 Jakub Szymanik（2014）。二阶广义量词可定义性的一种刻画及其在不可定义性中的应用。计算机与系统科学杂志80(6), 1152–1162。Juha Kontinen 和 Heribert Vollmer（2010）。关于二阶单子、单值及群胚量词。计算机科学中的逻辑方法6(3)，第25篇文章。

Moritz Lichter 和 Pascal Schweitzer（2024）。带有见证对称选择的无选择多项式时间。*ACM*期刊 71(2)，第7篇文章，1–70。Moshe Y. Vardi（1982）。关系查询语言的复杂性（扩展摘要）。载于第*14*届*ACM*年度计算理论研讨会（*STOC*），137–146。Helmut Wielandt（1969）。通过不变关系和不变函数研究置换群。Frank Demana、William McWorter 和 Surinder Sehgal 编写的讲义。俄亥俄州立大学，哥伦布。