通过对称异或电路证明无选择多项式时间的下界

Benedikt Pago ✉计算机科学数学基础，德国亚琛工业大学

摘要

有限模型论中的一个核心问题是，是否存在一种能够刻画多项式时间的逻辑。在秩逻辑和更一般的线性代数逻辑已被证明与多项式时间不等价之后，最重要的候选逻辑是无选择多项式时间（CPT），以及其扩展——带见证的对称选择算子。

本文旨在推进将 CPT 与多项式时间区分开来的研究：首先建立 CPT 的表达能力与某些对称电路族存在性之间的联系；其次，证明这些电路的下界。

我们聚焦于无序 Cai-Fürer-Immerman 图的同构问题（即 CFI 查询），将其视为区分 CPT 与 P 的潜在候选问题。Dawar、Richerby 和 Rossman，以及随后 Pakusa、Schalthöfer 和 Selman 的研究表明，在具有小规模颜色类的线性有序和预序基图上，CFI 查询是 CPT 可定义的。我们定义一类 CPT 算法，称为“CFI 对称算法”，它概括了所有已知算法，并证明：若这类算法能在给定基图类上定义 CFI 查询，则必定存在一族具有特定性质的对称异或电路。这些性质包括：电路与基图具有相同的对称性、大小为多项式级别，并满足某些扇入限制。接着，我们证明，对于以 n 维超立方体为基图的情形，即便稍微加强要求（即要求更强的对称性以及更严格的扇入和扇出限制），这样的电路仍不存在。这使我们几乎能够将 CFI 对称算法与多项式时间区分开来；目前尚存的差距在于，我们能够证明不存在的电路，与 CFI 对称算法定义 CFI 查询所必需的电路之间仍有距离。在一定程度上，异或电路与用于处理 CFI 查询的 CPT 算法之间的联系也可以推广到非 CFI 对称算法（尽管目前尚未发现此类算法

).

2012 年 ACM 学科分类 计算理论 → 有限模型论

关键词和短语 有限模型论、描述复杂度、对称计算、对称电路、图同构

数字对象标识符 10.4230/LIPIcs...

致谢 感谢 Daniel Wiebking 在附录中的群论证明方面提供帮助。

arXiv:2302.05426v1 [cs.CC] 8 Feb 2023

1 引言

无选择多项式时间 （CPT） [5] 是有限模型论中用于刻画多项式时间的最 prominent 候选逻辑之一。它可以看作是带计数的定点逻辑 [7] 的扩展，并将遗传有限集 作为数据结构。原则上，这使得我们能够在 CPT 中模拟任意计算——唯一的限制是，所计算的遗传有限集必须在输入结构的自同构下保持对称，并且大小受到多项式界的限制。

其他研究较少的候选包括带有见证选择构造的逻辑，例如带有见证对称选择和解释的 不动点逻辑 [27]以及扩展了见证对称选择的 CPT [28]。在 Lichter 的突破性成果 [26], 之前，他通过对著名的 Cai-Fürer-Immerman（CFI）

©Benedikt Pago；依据知识共享署名 4.0 国际许可协议授权 莱布尼茨国际信息学会议录 达格施图尔城堡 – 莱布尼茨信息学中心，达格施图尔出版社，德国

LIPICS

构造 [6], 的变体将秩逻辑与多项式时间区分开来，带线性代数算子的逻辑 [8]也曾被视为合理的候选。然而，正如 [9], 所概述的， [26] 和 [8] 的结果共同表明，没有任何一组同构不变的线性代数算子能够用于定义一种刻画多项式时间的逻辑。不过，无选择多项式时间的强下界仍难以确立。受 Gurevich 猜想启发——该猜想认为任何逻辑都无法刻画多项式时间——本文旨在推动将 CPT 与多项式时间区分开来。关于尚未解决的问题“是否存在刻画多项式时间的逻辑？”的概述，以及对 CPT 逻辑的介绍，可参阅例如 [18], [21], [30], 或 [36]。

关于 CPT 下界，目前所知甚少：对于 Ptime 中的一个函数型问题，已有不可定义性结果，即无法在 CPT [34] 中定义给定有限向量空间的对偶。我们希望得到的则是某个多项式时间判定问题的不可表达性。我们聚焦于有限模型论中的一个标准基准问题，即*CFI* 查询。给定一个 CFI 图，该问题要求输出它是奇数还是偶数。第 3 节将解释其含义（在这些实例上，它等价于图同构问题）。CFI 查询可在多项式时间内判定，但无法用带计数的定点逻辑或秩逻辑定义（对于广义 CFI 结构而言）。对于无序实例，它是否 CPT 可定义仍是一个开放问题，而我们的最终目标是对此给出否定答案。我们的方法从正面结果出发：确实存在针对线性有序和预序版本的 CFI 查询的 CPT 算法 [10, 32] ，也存在针对基图次数为线性的 CFI 图的 CPT 算法 [32]。这些算法都基于遗传有限集的构造，这些集合以某种方式在其结构中编码了给定 CFI 图的奇偶性。在 [10] 中，这些集合被称为超对称。

在 [29] 中，研究表明，存在一些（定义在 n 维超立方体上的）无序 CFI 图，其次数并非线性，而且无法在 CPT 中对其进行预序，使得可以应用 [32] 中基于拟序的算法（或 [10] 中基于全序的算法）。这表明，针对 CFI 查询的预序版本，这些已知的无选择算法无法推广到无序情形，因为必要的组合对象（即所谓的拟序）不够对称：CPT 的主要限制在于，它无法定义那些“过度”打破输入结构对称性的对象——这也正是无序（因而高度对称的）CFI 实例看起来有望用于证明下界的原因。

在本文中，我们将这一策略进一步推进：我们定义了一个用于 CFI 查询的 CPT 算法通用类别，涵盖了上述所有已知算法，并证明其表达能力取决于某些对称组合对象的存在，即带有布尔异或门的电路。我们证明，对于给定的一类基图$\mathcal{K}$ ，只有在存在一族具有某些性质的多项式规模异或电路时，该类中的算法才能定义其上的 CFI 查询；特别是，这些电路必须与$\mathcal{K}$ 中的图具有相同的对称性（定理 1）。这意味着，只需证明不存在具有所需性质的对称电路，就能证明$\mathcal{K}$ 上的 CFI 查询不可定义。事实上，我们几乎实现了这一目标：我们的第二个主要结果给出了针对这类电路的下界；它表明，若将$\mathcal{K}$ 取为 n 维超立方体族，并将电路性质设定得比定理 1 的要求略为严格，那么不存在任何电路族能够同时满足所有这些性质。因此，我们几乎证明了，无序超立方体上的 CFI 查询无法由我们所考虑的通用类别中的任何 CPT 算法定义。

结果

我们在第4节定义了一个用于 CFI 查询的 CPT 算法类别，其中包含目前已知的所有此类算法，并证明，要通过此类算法解决给定一类无序基图$\mathcal{K}$ 上的 CFI 查询，必须存在某些对称异或电路。沿用 [10]„ 我们将基图 G 上的 CFI 实例记作 $\mathfrak{G}^S$，其中 S是其 CFI 小工具为奇数的顶点集合（见第 3 节）。在下述定理中，我们考虑输入门以基图 G_n 的边为标签、且所有内部门均为异或门的电路。群$\mathbf{Aut}(G_n) \leq \mathbf{Sym}(V(G_n))$是基图 G_n 的自同构群。电路的$\mathbf{Aut}(G_n)$-轨道指的是在输入门上施加$\mathbf{Aut}(G_n)$中的置换进行重新标记后，该电路所有像构成的集合。如果翻转某个输入位会改变电路的输出，则称该电路对该输入位敏感。电路的扇入维数是本文定义的一个参数，是扇入度的推广。关于这些电路的所有概念均在第5节中详细介绍。

▶ **定理 1** (主要定理，非正式表述)。 设$(G_n = (V_n, E_n))_{n\in\mathbb{N}}$ 是一个基图序列。设 $\mathfrak{G}_n^S$ 是 G_n 上的一个 *CFI* 图，并设tw_n 表示 G_n的树宽。如果存在一个超对称 且CFI-对称 的 *CPT* 程序 Π， 它能对所有 $n \in \mathbb{N}$的实例 $\mathfrak{G}_n^S$判定 *CFI* 查询，那么还存在一个异或电路族$(C_n)_{n\in\mathbb{N}}$， 使得

1. 门的数量 C_n 是关于 $|\mathfrak{G}_n^S|$的多项式。2. 该电路的 $\mathbf{Aut}(G_n)$-轨道大小关于 $|\mathfrak{G}_n^S|$是多项式。3. C_n 对 $\Omega(\mathrm{tw}_n)$ 个输入位敏感。4. 该电路的 扇入维数 为 C_n， 其大小为 $\mathcal{O}(\log|\mathfrak{G}_n^S|)$。

该定理的详细版本是第5节中的定理 31。术语超对称 和*CFI*-对称 指程序 Π 为判定 CFI 查询而构造的遗传有限集所具有的性质。超对称性 这一遗传有限集的性质可追溯至[10]，其含义是遗传有限集在所有 针对 CFI 结构 $\mathfrak{G}^S$的边翻转下均保持不变，而不仅仅是在 $\mathfrak{G}^S$ 的自同构所对应的边翻转下保持不变（见第 3.1 节）。*CFI* 对称性 是本文提出的一个概念，用来描述遗传有限集的内部结构和“局部对称性”。 [10] 和 [32] 中的 CFI 算法都基于同时具有超对称性和 CFI 对称性的遗传有限集。可以说，这两种性质对所有这些算法的成功都至关重要：它们的工作方式是将 $\mathfrak{G}^S$ 的所有 CFI 小工具汇集到一个大的遗传有限集 μ 中，使其在对边组件进行的所有翻转下保持对称。然后，将 μ 边组件中的顶点 e_0 和 e_1 替换为常数 0 和 1。由于 CPT 是无选择性的，它不能任意选择哪个顶点 e_0，e_1 对应替换为哪个常数；它必须以两种方式都执行替换。 μ 的超对称性确保这两种替换都会产生同一个对象。为了避免尝试所有组合时产生指数数量的遗传有限集，这一点必不可少。当 μ中的所有原子都替换为 0 和 1 后，就可以提取出原始 CFI 图 $\mathfrak{G}^S$ 的奇偶性。我们称 μ 具有 CFI 对称性，这本质上意味着 μ 由若干子对象组成，而这些子对象的行为类似于 CFI 小工具。这似乎是超对称对象的一种自然设计模式，它们编码了 $\mathfrak{G}^S$ 的奇偶性；不过，也可以设想并非 CFI 对称的超对称对象（反之亦然）。简言之，超对称性是使所有已知 CFI 算法得以运行的遗传有限集的主要性质，而 CFI 对称性则是实现超对称性的既定设计原则。

定理 1 将关于 CFI 查询的 CPT 可定义性问题，归结为是否存在某些非平凡组合对象的问题，即多项式规模的

对称异或电路。其证明基于将 CFI 结构上的遗传有限集转换为异或电路（定理 21）。随后将这一结果与 [10] 给出的下界结合起来，该下界针对判定 CFI 查询所需的遗传有限集的支撑大小——支撑大小在某种程度上衡量了一个集合有多不对称（见第 3.2 节）。正如我们的第二个主要结果所示，对于所有基图，所需的电路族是否确实存在并不明朗，因此，通过对称电路的下界来获得 CPT 的下界，确实有可能实现。

在讨论第二个结果之前，我们还会在第 6 节证明上述定理的一个版本，该版本不再限制算法必须是*CFI*-对称算法。它要求算法构造的遗传有限集具有某种对称基，而我们证明这是一种比 CFI 对称性更一般的性质。不过，由于目前已知的所有针对 CFI 查询的 CPT 算法都是 CFI-对称的，因此尚不清楚，为了将 CPT 与多项式时间分离，是否终有必要用到这个更一般（且证明复杂得多）的定理版本。满足上述对称基条件的无选择算法类可能严格大于 CFI-对称算法类；但也可能每个针对 CFI 查询的 CPT 算法都等价于某个 CFI-对称算法（在这种情况下，原则上定理 1 就足以通过对称电路下界将 CPT 与 P 分离）。

我们在第 8 节证明的第二个主要结果表明，如果我们选择 n 维超立方体作为基图族，并对电路施加稍强的条件，那么就不可能同时满足所有这些条件。

▶**定理 2.** 设$(H_n)_{n\in\mathbb{N}}$ 为 n 维超立方体族，并令树宽n 表示 H_n 的树宽。令 $\mathfrak{H}_n^S$ 表示 H_n 上的一个 *CFI* 结构。不存在 满足以下条件的对称异或电路$(C_n)_{n\in\mathbb{N}}$ 族：

1. 中门的数量 C_n 是 $|\mathfrak{H}_n^S|$的多项式。
2. 该电路在 $\mathbf{Aut}(\mathcal{H}n)$ 下的轨道大小恰为一。
3. C_n 对Ω(树宽n) 个输入位敏感。
4. 对于任意两个门 g、h ，在 C_n 中，若 h 是 g的父节点，则有 $|\textbf{轨道}^{(h)}(g)| \in \mathcal{O}(\log|\mathfrak{H}_n^S|)$，且 $|\textbf{轨道}^{(g)}(h)| \in \mathcal{O}(\log|\mathfrak{H}_n^S|)$。

此处，$\textbf{轨道}^{(h)}(g)$ 表示相对于固定门 g 的$\mathbf{Aut}(H_n)$子群所对应的门轨道（$\textbf{轨道}^{(g)}(h)$的情况反之亦然）。

如果这四项电路性质与定理 1 中的相同，那么这就能将超对称和 CFI 对称无选择算法类与多项式时间区分开来。这两个定理的区别在于，此处电路的轨道大小为一，也就是说，它被整个群 $\mathbf{Aut}(\mathcal{H}n)$ 稳定；而在定理 1 中，只要求电路的轨道大小为多项式级。此外，此处每个门的父节点和子节点（按轨道计）均有对数界，而定理 1 中，对数界针对的是门的扇入维数 。我们在第5节定义这一概念；我们不知道对数扇入维数是否意味着子节点数（按轨道计）具有对数界（反之亦然），而且它可能并不意味着父节点数有界。因此，我们两项主要结果之间的“差距”涉及电路必须具备多强的对称性，以及相邻两个电路层之间的连接受到多大限制。定理 2 的证明运用了群论技术，其基础是 [1] 中的相关技术。

相关工作

对称电路下界的研究在许多领域都卓有成效：Anderson 和 Dawar 建立了由多数门构成的高度对称布尔电路族，并证明这种计算模型等价于带计数的定点逻辑 [1]。这类电路的一种推广也能够刻画秩逻辑 [12]。关于 CPT 的结果较弱，因为我们没有给出 CPT 的电路刻画，而只是对 CPT 可用于判定 CFI 查询的相关遗传有限集给出了结构性描述。相较于 [1] 和 [12] 中的电路，要证明针对我们这类电路的下界，通常似乎更难，因为我们的对称性要求较弱（至少对于有趣的基图类而言）。

除了与有限模型论中的逻辑之间的这些联系外，对称电路在 VP 与 VNP 问题的背景下也颇具研究价值。Dawar 和 Wilsenach 针对永久式 [11] 和行列式 [13], 在不同对称群下的对称算术电路证明了超多项式下界。将这些下界推广到对称性较弱的永久式电路，将是推动 VP 与 VNP 分离的一步。

对称电路下界的其他例子包括针对奇偶函数 [35], 的 AC^0 电路，以及用于置换矩阵乘法的布尔电路 [23]。Rossman 关于计算奇偶性的 AC^0 电路下界有一个有趣之处，即他所考虑的对称群：与其他提及的结果不同，此处的对称群并非作用于输入变量的大型置换群，而是一个布尔向量空间，它通过交换指定的输入文字$\{X_1, \neg X_1, \ldots\ldots, X_n, \neg X_n\}$及其各自的否定来作用于输入文字集合 X_i。这让人联想到本文中遇到的 CFI 小工具的翻转。不过，Rossman 的下界与我们的结果似乎没有直接联系，因为他的下界针对的是奇偶函数，而在我们的框架中，只需一个异或门就能轻松表示该函数。

与这一主题相关的另一个研究方向是 CPT 的扩展。Lichter 和 Schweitzer 发展了带有见证对称选择 [28]的无选择多项式时间。这是一种逻辑，允许从结构的可定义轨道中任意选择元素，前提是见证某个选择集合为轨道的自同构也必须是可定义的。该逻辑能够在所有可以定义同构问题的结构类上捕获多项式时间，因此，见证选择算子本质上将规范化归约为同构判定。一个问题是，我们提出的通过对称电路建立下界的方法，在多大程度上也适用于带有见证选择的 CPT。正如 [28], 所示，带有见证选择的 CPT 可以毫无困难地在具有单一轨道的结构上定义 CFI 查询，即无序 CFI 图。然而，这些恰恰是我们已得到电路下界的例子，因此看来，电路方法利用了 CPT 的某种弱点，而这种弱点在见证选择扩展中并不存在。

2 预备知识

有界变量计数逻辑

对于 $k \in \mathbb{N}$，$\mathcal{C}^k$ 表示一阶逻辑中含 k 个变量的片段，并带有计数量词。该逻辑中的计数量词形式为 $\exists^i x\varphi(x)$，对每个 $i \in \mathbb{N}$ 都表示结构中至少有 i 个元素满足 $\varphi(x)$。请注意，这类计数量词可以用普通的一阶逻辑模拟，但需要多于一个变量。若两个结构 $\mathfrak{A}$ 和$\mathfrak{B}$ 满足完全相同的$\mathcal{C}^k$-句子，则称它们是$\mathcal{C}^k$-等价的，记作 $\mathfrak{A} \equiv_{\mathcal{C}^k} \mathfrak{B}$。

证明两个给定结构之间 C^k-等价性的标准工具是双射 k-棋子游戏。游戏在一对结构 $(\mathfrak{A}, \mathfrak{B})$ 上进行，由两名玩家 Spoiler 和复制者参与。当且仅当 $\mathfrak{A} \equiv_{\mathcal{C}^k} \mathfrak{B}$ [24] 时，复制者拥有获胜策略。游戏过程如下：游戏中的一个局面是由棋子对 $\pi \subseteq A \times B$ 组成的集合，其大小至多为 k。每一回合中，Spoiler 可以拿起任意数量的棋子对，并将它们从棋盘上移除，使得在得到的局面 π' 中，剩下的棋子对少于 k 个。随后，复制者指定一个双射 $f\colon A \longrightarrow B$，使得对每个 $(a,b) \in \pi'$, $f(a) = b$。接着，Spoiler 在自己选择的某个元素 $a \in A$ 上放下一枚新棋子，并在 B 中的 $f(a)$ 上放置对应的棋子。如果得到的棋子对集合不构成局部同构，则 Spoiler 获胜。如果复制者能够确保游戏永远进行下去而不输，则她拥有获胜策略。若一个局面 $\pi = \{(a_1, b_1) ..., (a_k, b_k)\}$ 所对应的映射 g 将每个 a_i 映射到 b_i（其中 $i \in [k]$），并且该映射是从 $\mathfrak{A}$ 的诱导子结构（论域为 $\{a_1, ..., a_k\}$）到 $\mathfrak{B}$ 的诱导子结构（论域为 $\{b_1, ..., b_k\}$）的同构，则称该局面构成局部同构。

复制者具有获胜策略的位置，由在 $\mathfrak{A}$ 和 $\mathfrak{B}$ 中具有相同 $\mathcal{C}^k$-类型 的那些元组给出。元组 $a \in A^{\leq k}$ 的 $\mathcal{C}^k$-类型 是由 a 在 $\mathfrak{A}$ 中满足的所有 $\mathcal{C}^k$-公式构成的集合。已知在每个有限结构中，每个$\mathcal{C}^k$-类型都可以由单个 $\mathcal{C}^{\overline{k}}$-公式定义，因此，尽管一个类型是由无限多个公式构成的集合，但如果结构固定，它在语义上等价于一个有限的 $\mathcal{C}^k$-公式 [19]。

遗传有限集

设 A 是一个有限的原子集合。通常，原子将构成某个结构的论域 $\mathfrak{A}$ （并且按照惯例，每当一个结构记作 $\mathfrak{A}$ 时，A 就表示它的论域）。
在 A 上的遗传有限对象集合 $\mathrm{HF}(A)$ 定义为 $\bigcup_{i\in\mathbb{N}} \mathrm{HF}_i(A)$，其中 $\mathrm{HF}_0(A) := A \cup \{\emptyset\}$,$\mathrm{HF}_{i+1}(A) := \mathrm{HF}_i(A) \cup 2^{\mathrm{HF}_i(A)}$。遗传有限集 $x \in \mathrm{HF}(a)$ 的大小通过其传递闭包 $\mathrm{tc}(x)$来衡量：集合 $\mathrm{tc}(x)$ 是包含 $x \in \mathrm{tc}(x)$ 的最小传递集。传递性意味着，对于每个 $a \in \mathrm{tc}(x)$, $a \subseteq \mathrm{tc}(x)$。直观地说，可以将 $\mathrm{tc}(x)$ 看作在 x 内部某个嵌套深度上作为元素出现的所有集合构成的集合。

无选择多项式时间

CPT 始终指带计数的无选择多项式时间。有关详情以及 CPT 的各种形式化定义方式，请参阅相关文献： [18]中有一篇简明综述。Blass、Gurevich 和 Shelah 最初将 CPT 作为一种抽象状态机模型引入，其相关著作发表于 1999 年，见 [5] ；后来又提出了更具“逻辑风格”的 CPT 表述，例如多项式解释逻辑 [17, 36]和 BGS逻辑 [34, 18]。简言之，CPT 类似于研究得更为深入的带计数的不动点逻辑 [7] ，再加上一种构造多项式大小的同构不变遗传有限集的机制。在有限结构 A中求值 CPT 语句 Π 时， Π 可以用其论域上的遗传有限集扩充 A 。其中出现的不同集合总数（即遗传有限集的传递闭包大小之和）以及计算步数，均受$p(|A|)$限制，其中 $p(n)$是语句 Π中明确给出的多项式。下面我们简要介绍 BGS逻辑的定义：

BGS逻辑的句子称为程序。程序是一个元组 $\Pi = (\Pi_{\mathrm{step}}(x), \Pi_{\mathrm{halt}}(x)\ \Pi_{\mathrm{out}}(x)\ p(n))$。其中，$\Pi_{\mathrm{step}}(x)$ 是一个 BGS项， Π_{halt} 和 Π_{out} 是 BGS公式，而 $p(n)$ 是一个多项式，用于界定程序所用的时间和空间。BGS项

以遗传有限集作为输入，并输出一个遗传有限集。这类项的例子包括 Pair(x, y)，其求值结果为 $\{x, y\}$；以及 Union$(x) = \bigcup_{y \in x} y$。此外，如果 s 和 t 是项，x 是变量，φ 是公式，那么 $\{s(x) : x \in t : \varphi(t)\}$ 就是一个概括项。它将项 s 应用于由 t 定义且满足 φ 的集合中的所有元素，并输出由此得到的对象 $s(x)$ 所构成的集合。当在给定的有限结构 A 中求值一个程序时，项 $\Pi_{\text{step}}(x)$ 会从 $x_0 = \emptyset$ 开始，反复作用于自身的输出。如果计算出的集合 $x_i = (\Pi_{\text{step}})^i(\emptyset)$ 满足 $A \models \Pi_{\text{halt}}(x_i)$，迭代便在第 i 步停止。公式 Π_{out} 根据 x_i 定义运行是接受还是拒绝，也就是说，定义是否 $A \models \Pi$。如果运行长度或 x_i 的传递闭包大小在某个时刻超过 $p(|A|)$，则计算会中止，并且 $A \not\models \Pi$。

程序 Π 在结构 $\mathfrak{A}$ 上运行时出现的遗传有限集，称为程序 Π 在输入 $\mathfrak{A}$ 上激活的集合。形式上，活跃对象集合是所有迭代阶段 x_i 的传递闭包的并集。对于本文而言，精确定义并不重要；文献 [10, 34, 36] 中存在多个略有差异的定义，但它们本质上描述的是同一个概念。

对称群

我们利用 CPT 的两个关键性质来证明下界：多项式有界性和对称不变性。对于论域为 A 的结构 $\mathfrak{A}$，我们用Aut$(\mathfrak{A}) \leq$ Sym(A) 表示其自同构群。任意 $\pi \in$Sym(A) 也会通过按照 π 重命名遗传有限集中的原子，自然地作用于 HF(A) 上。据此，CPT 的对称不变性可概括如下：

▶命题 3。设 $\mathfrak{A}$ 为一个结构，$x \in$ HF(A)为 $\mathfrak{A}$ 上的一个遗传有限集，$\pi \in$ Aut($\mathfrak{A}$)为一个自同构。任何在 $\mathfrak{A}$ 上运行时激活了 x 的 CPT 程序，也会激活 π(x)。

我们省略证明，因为这一事实众所周知，并且可由遗传有限集的构造步骤在逻辑上可定义这一事实直接推出。作为该命题的推论，CPT 可定义对象在其 **Aut**$(\mathfrak{A})$-轨道下封闭。集合 $x \in$HF(A) 的轨道是 $\{\pi(x) \mid \pi \in \mathbf{Aut}(\mathfrak{A})\}$，即其在 **Aut**$(\mathfrak{A})$ 作用下所有像的集合。由于 CPT 可定义对象还必须满足多项式大小界，任何轨道大小相对于 $|A|$ 为超多项式的对象，都不可能由任何 CPT 程序在输入 $\mathfrak{A}$ 上激活。这一考量也反映在定理 1 中的电路性质中。

在这一语境下，我们有时需要用到群论中的一个重要事实，即轨道-稳定子定理。将其应用于结构上的遗传有限集，可表述如下。

▶ **命题4。** 设 $\mathfrak{A}$ 为一个结构，$x \in \mathrm{HF}(A)$ 为 $\mathfrak{A}$ 上的一个遗传有限集。则 $|\mathbf{Orbit}(x)| = |\mathbf{Aut}(\mathfrak{A} \mid x)/\mathbf{Stab}(x)|$。

这里，**稳定子**$(x) = \{\pi \in \mathbf{Aut}(\mathfrak{A}) \mid \pi(x) = x\}$ 表示固定 x 的自同构群的子群。更一般地，如果 H 是 G 的子群（记作 $H \leq G$），那么 H 在 G 中的指数为 $[G : H] = |G|/|H|$。这等于 H 在 G 中的陪集数；如果 H 是某个对象 x 的稳定子，那么 $[G : H]$ 恰好是 x 的轨道大小。

线性代数

我们用 $\mathbb{F}_2$ 表示含有两个元素{0，1}的有限域，用 $\mathbb{F}_2^n$ 表示 $\mathbb{F}_2$ 上所有 n 元组构成的集合，并将其视为一个 n 维向量空间。我们还将讨论一些空间

由某个有限（无序）集合 J 索引的情形；此时，我们用 $\mathbb{F}_2^J$ 表示坐标由 J 中元素构成的 $|J|$ 维向量空间。同样，矩阵的行和列也可以由这样的有限无序集合索引，因此矩阵 $M \in \mathbb{F}_2^{I\times J}$ 描述了一个线性变换 $M\colon \mathbb{F}_2^J \longrightarrow \mathbb{F}_2^I$。$M$ 的像是 $\mathrm{Im}(M) = \{M\cdot \mathbf{v} \mid \mathbf{v}\in \mathbb{F}_2^J\}$，核是 $\mathrm{Ker}(M) = \{\mathbf{v} \in \mathbb{F}_2^J \mid M\cdot \mathbf{v} = \mathbf{0}\}$。秩定理指出，$|J| = \mathrm{rk}(M) + \dim(\mathrm{Ker}(M))$。秩 $\mathrm{rk}(M)$ 表示 $\mathrm{Im}(M)$ 的维数。它既等于 M 的列向量所张成空间的维数，也等于行向量所张成空间的维数。

3 无序的 Cai-Fürer-Immerman 图

固定一个无向（且无序）的连通图 $G = (V, E)$，作为 CFI 构造的基图 。我们通过用特定的边小装置替换边、用顶点小装置替换顶点，将 G 转换为 CFI 图。顶点小装置分为两种，称为奇和偶。为了在 G 上构造一个具体的 CFI 图，我们必须固定一个顶点集合 $S \subseteq V$，其中的顶点将替换为奇 构件。$V \setminus S$ 中的顶点将转换为偶 构件。按照 [10]，中的记法，我们将所得的 CFI 图记为 $\mathfrak{G}^S$.$\widehat{\ }$精确定义如下：令 $E := \{e_0, e_1 \mid e \in E\}$。这些顶点将构成 $\mathfrak{G}^S$ 的边小装置，因此每个边小装置包含两个顶点。为了定义顶点小装置中的顶点，我们对每个 $v \in V$ 令，

$$v_S^* := \begin{cases} \{v^X \mid X \subseteq E(v), |X| \text{ even }\} & \text{if } v \notin S \\ \{v^X \mid X \subseteq E(v), |X| \text{ odd }\} & \text{if } v \in S \end{cases}$$

这里， $E(v) \subseteq E$ 是 G中与 v 相邻的边。 v_S^* 中的顶点构成了 v的顶点小装置。总之，我们令

$$\widehat{V}_S := \bigcup_{v\in V} v_S^*.$$

那么， $\mathfrak{G}^S$ 的顶点集合为 $V(\mathfrak{G}^S) := \widehat{V}_S \cup \widehat{E}$。CFI 图的边定义如下：

$$E(\mathfrak{G}^S) := \{\{v^X, e_i\} \mid v^X \in \widehat{V}_S, e_i \in \widehat{E}, |X \cap \{e\}| = i\} \cup \{\{e_0, e_1\} \mid e \in E\}.$$

换句话说，对于每个 $v \in V$，我们将每个 $v^X \in v_S^*$ 与所有边$e \in E(v)$的边小装置相连，使得当 $e \notin X$时， v^X 与 e_0 相连；否则， v^X 与 e_1相连。此外，我们将 e_0 和 e_1 相连，以确保 $\mathfrak{G}^S$ 的任何自同构都无法拆开边小装置。我们的 CFI 图是无序的，因此结构 $\mathfrak{G}^S$ 的唯一关系是边关系 E。

下面是两个顶点 $v, w \in V$对应的构件 v_S^*, w_S^*，以及连接它们的边 $e \in E$对应的构件。在此例中，我们有 $v \notin S, w \in S$，以及 $E(v) = \{e, f, g\}$ $E(w) = \{e, h, i\}$。图中只画出了边 e。请注意，如果只考虑它们与 e-构件的连接， v_S^*和 w_S^*看起来完全相同，尽管一个构件为偶，另一个为奇。

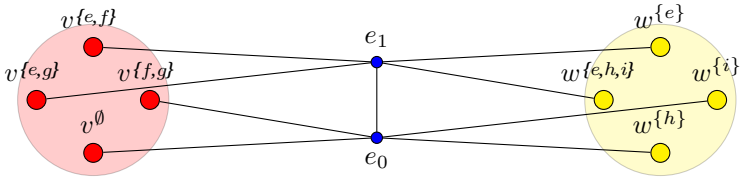

图 1 构件 v^*_S，w^*_S，通过用于边 e 的构件连接。

CFI 查询 要求给定一个 CFI 图 $\mathfrak{G}^S$，求出 $|S|$的奇偶性。这本质上与 CFI 图的图同构问题是同一个问题：

▶ **定理 5** ([6] [10])。 对于同一基图上的两个给定 *CFI* 图，成立

$$\mathfrak{G}^S \cong \mathfrak{G}^R \text{ if and only if } |S| \equiv |R| \mod 2.$$

另一种表述是，判定 $|S|$ 的奇偶性可以写成关于变量 E、在 $\widehat{\ }$ 上的 $\mathbb{F}_2$ 线性方程组（见 [2]）。由于可以根据给定的 CFI 图 $\mathfrak{G}^S$ 轻松构造出该线性方程组，并且可以使用例如高斯消元法高效求解线性方程组，因此 CFI 查询可以在多项式时间内判定。

对于缺乏创建高阶对象能力的逻辑，例如有界变量计数逻辑及其扩展固定点计数逻辑，只要基图的树宽是超常数，就可以证明它们不可能区分非同构的 CFI 图：

▶ **定理 6** ([6] [2])。 设 $G = (V, E)$ 是一个树宽为 t 的无向连通图。那么对于任意两个集合 S、$S' \subseteq V$，均有 $\mathfrak{G}^S \equiv_{C^t} \mathfrak{G}^{S'}$，即使 $\mathfrak{G}^S \ncong \mathfrak{G}^{S'}$ 也成立。

这是因为复制者在 $\mathfrak{G}^S$和 $\mathfrak{G}^{S'}$上的双射 t 棋子游戏中拥有获胜策略。直观地说，$\mathfrak{G}^S$ 和 $\mathfrak{G}^{S'}$ 之间的差异体现在一条边上，该边的构件发生了扭曲；复制者的目标是移动这一扭曲，使其不会被 t 个棋子暴露出来。为此，复制者可以像警察与强盗游戏中的强盗那样行动，而该游戏证明树宽至少为 t。

3.1 无序 CFI 图的自同构

对于底层图为 $G = (V, E)$ 的 无序 CFI 图 $\mathfrak{G}^S$，两种不同类型的自同构发挥着作用：首先，有我们称为“CFI 自同构”或“CFI 同构”的变换。它们是通过交换某些边小装置中的 e_0 和 e_1 诱导出来的（这称为 “ 翻转边 ” ）。其次，还有底层图 G 本身的自同构。

为讨论 CFI 同构，我们采用文献 [10]中的术语：给定一个基图 G，我们不仅考虑一个由奇、偶顶点构件组成的具体 CFI 实例，还可以构造“完整的”CFI 图 $\mathfrak{G}$，其中每个顶点构件既是偶的，也是奇的。形式上，对于 $v \in V$，令 $v^* := v^*_\emptyset \cup v^*_{\{v\}} = \{v^X \mid X \subseteq E(v)\}$，且 $\widehat{V} := \bigcup_{v \in V} v^*$.$\widehat{\ }$ $\widehat{\ }$ $\mathfrak{G}$ 的顶点集为 $V \cup E$，其边集为

$$E(\mathfrak{G}) := \{\{v^X, e_i\} \mid v^X \in \widehat{V}, e_i \in \widehat{E}, |X \cap \{e\}| = i\} \cup \{\{e_0, e_1\} \mid e \in E\}.$$

每个 CFI 实例 $\mathfrak{G}^S$ 都是 $\mathfrak{G}$ 的诱导子图。
对于每条边 $e = \{v, w\} \in E$，令 ρ_e 表示由翻转边 e所诱导的 $\mathfrak{G}$ 的自同构。形式化地，$\rho_e(e_0) = e_1$，$\rho_e(e_1) = e_0$，且 $\rho_e(v^X) = v^{X \triangle \{e\}}$, $\rho_e(w^X) = w^{X \triangle \{e\}}$

对所有 $v^X, w^X \in v^* \cup w^*$均成立。 $\widehat{V}$中的所有其他顶点在 ρ_e作用下保持不变。可以验证，这确实是 $\mathfrak{G}$的一个自同构；此外， ρ_e 是从任意 CFI 实例 $\mathfrak{G}^S$ 到 $\mathfrak{G}^{S\triangle\{v,w\}}$ 的一个同构（另见 [10]）。不难看出，这些边翻转自同构彼此可交换，因此对于 $F = \{e^1, ..., e^m\} \subseteq E$，我们可以将 ρ_F 记作 $\rho_{e^1} \circ \rho_{e^2} \circ ... \circ \rho_{e^m}$。因此，对于每个 $F \subseteq E$， ρ_F 都是 $\mathfrak{G}$的一个自同构。对于任意边集 $F \subseteq E$和 $v \in V$，令 $\deg_F(v) := |E(v) \cap F|$，即属于 F的关联边的数量。我们有$\rho_F(\mathfrak{G}^S) = \mathfrak{G}^{S\triangle T}$，其中 $T = \{v \in V \mid \deg_F(v)$ 为奇数 $\}$。特别地，如果每个 $v \in V$在 F 中都关联偶数条边（因此 F 是若干圈的对称差），那么 ρ_F 也是 $\mathfrak{G}^S$的一个自同构，而不仅仅是 $\mathfrak{G}$的自同构。总而言之，我们得到 $\mathfrak{G}$ 和 $\mathfrak{G}^S$的以下 CFI 自同构群：

$$\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G}) := \{\rho_F \mid F \subseteq E\}.$$

该群同构于布尔向量空间 $\mathbb{F}_2^E$：每个 $F \subseteq E$ 都由其特征向量 $\chi(F) \in \mathbb{F}_2^E$ 标识。成立 $\rho_F \circ \rho_{F'} = \rho_{F\triangle F'}$，这对应于向量 $\chi(F) + \chi(F') \in \mathbb{F}_2^E$。

如前所述，对于 CFI 实例 $\mathfrak{G}^S$，即 $\mathfrak{G}$ 的一个诱导子图，我们有

$$\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G}^S) := \{\rho_F \in \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G}) \mid \deg_F(v) \text{ is even for every } v \in V\}.$$

该群同构于 $\mathbb{F}_2^E$ 的一个子空间。除了 CFI 自同构之外，我们还必须考虑 **自同构**$(G) \leq$ **对称群**(V)，即无序底层图的自同构群；这不同于文献中研究的典型情形，在该情形中，G 是有序的，因此 $\mathfrak{G}^S$ 的自同构仅由边翻转给出。总之，完整 CFI 图 $\mathfrak{G}$ 的自同构群同构于以下半直积：

$$\mathbf{Aut}(\mathfrak{G}) \cong \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G}) \rtimes \mathbf{Aut}(G) = \{(\rho_F, \pi) \mid \rho_F \in \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G}), \pi \in \mathbf{Aut}(G)\}.$$

$\widehat{\ }$ $\widehat{\ }$一对 (ρ_F, π) 在 $V(\mathfrak{G})$ 上的作用由其在 E 上的作用决定：令 $e_i \in E$满足 $i \in \{0, 1\}$，且 $e = \{v, w\} \in E$。那么 $(\rho_F, \pi)(e_i) = f_j$，其中 $f = \{\pi(v)\ \pi(w)\}$，且 $j = i + |F \cap \{e\}|$ 模 2。此作用以唯一的方式扩展为 $\mathfrak{G}$ 的一个自同构。具体 CFI 实例的自同构群 $\mathrm{Aut}(\mathfrak{G}^S)$ 是它的一个子群。

3.2 CFI 结构上的遗传有限集的对称性和支撑

令 $\mathfrak{G}^S$ 为定义在 $G = (V, E)$ 上的一个 CFI 图，并令 $x \in \mathrm{HF}(\widehat{E})$。我们只考虑 $\mathrm{HF}(\widehat{E})$ 中的对象，而不考虑 $\mathrm{HF}(\widehat{E} \cup \widehat{V})$ 中的对象，因为这样更简单，而且原子 $v^X \in \widehat{V}$ 可以通过其在 $\mathfrak{G}^S$ 中的邻域唯一地描述；这个邻域本身又是由原子 $\widehat{E}$ 构成的集合。因此，我们可以$\widehat{\ }$假定，任何用于 CFI 查询的 CPT 算法只使用定义在 E 上的遗传有限集。
自同构群 $\mathbf{Aut}(\mathfrak{G}^S)$、边翻转群 $\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})$ 以及基图 $\mathbf{Aut}(G)$ 的$\widehat{\ }$ $\widehat{\ }$
自同构作用于 E，因此也作用于 $\mathrm{HF}(E)$：例如，令 $\pi \in \mathbf{Aut}(G)$，且 $x \in \mathrm{HF}(E)$。那么 $\pi x = \{\pi y \mid y \in x\}$。如果 x 是一个原子 e_i，其中$i \in \{0,1\}$ 且 $e \in E$，那么 $\pi x = \pi(e)_i$。

$\widehat{\ }$自同构 $\pi \in \mathbf{Aut}(G)$ 稳定对象 $x \in \mathrm{HF}(E)$，若 $\pi x = x$。更准确地说，这意味着 π作用于 x 的原子，并扩展为 DAG 结构 $(\mathrm{tc}(x) \ni)$ 的某个自同构 σ，使得对于每个原子 $e_i \in \mathrm{tc}(x)$， $\sigma(e_i) = \pi(e)_i$。如前所述，$\mathbf{Aut}(\mathfrak{G}^S)$ 由边翻转和基图的自同构组成。我们分别$\widehat{\ }$考察这两个子群对 $\mathrm{HF}(E)$ 中元素的作用，并考虑 $x \in \mathrm{HF}(E)$ 的以下轨道$\widehat{\ }$和稳定子。由于边翻转群 $\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})$ 同构于

布尔向量空间 $\mathbb{F}_2^E$，我们通常将自同构 $\rho_F \in \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})$ 与其特征向量 $\chi(F) \in \mathbb{F}_2^E$ 等同。

$$
\begin{aligned}
\mathbf{Orb}_E(x) &:= \{\rho_F(x) \mid \rho_F \in \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})\}.\\
\mathbf{Stab}_E(x) &:= \{\chi(F) \mid \rho_F \in \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G}), \rho_F(x) = x\} \le \mathbb{F}_2^E.\\
\mathbf{Orb}_{\mathrm{CFI}}(x) &:= \{\rho_F(x) \mid \rho_F \in \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G}^S)\}.\\
\mathbf{Stab}_{\mathrm{CFI}}(x) &:= \{\chi(F) \mid \rho_F \in \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G}^S), \rho_F(x) = x\} \le \mathbb{F}_2^E.\\
\mathbf{Orb}_{\mathfrak{G}^S}(x) &:= \{(\rho_F, \pi)(x) \mid (\rho_F, \pi) \in \mathbf{Aut}(\mathfrak{G}^S)\}.\\
\mathbf{Stab}_{\mathfrak{G}^S}(x) &:= \{(\rho_F, \pi) \in \mathbf{Aut}(\mathfrak{G}^S) \mid (\rho_F, \pi)(x) = x\}.\\
\mathbf{Orb}_G(x) &:= \{(\rho_\emptyset, \pi)(x) \mid \pi \in \mathbf{Aut}(G)\}.\\
\mathbf{Stab}_G(x) &:= \{\pi \in \mathbf{Aut}(G) \mid (\rho_\emptyset, \pi)(x) = x\}.\\
\mathbf{maxOrb}_E(x) &:= \max_{y \in \mathrm{tc}(x)} |\mathbf{Orb}_E(y)|.\\
\mathbf{maxOrb}_{\mathrm{CFI}}(x) &:= \max_{y \in \mathrm{tc}(x)} |\mathbf{Orb}_{\mathrm{CFI}}(y)|.
\end{aligned}
$$

应当强调的是，**稳定子**$_E(x)$ 是 $\mathbb{F}_2^E$ 的子空间，因此讨论其维数并对其应用线性变换是有意义的。此处我们注意到一个供后文参考的事实：同一$\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})$-轨道中的所有对象都有相同的 $\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})$-稳定子，因为该群是阿贝尔群：

引理 7. 设 $x, x' \in \mathrm{HF}(E)$ 满足 $x' = \rho_F(x)$，其中 $\rho_F \in \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})$。则**稳定子**$_E(x)$ = **稳定子** $_E(x')$。

证明。我们有 $\mathrm{Stab}_E(x') = \{\chi(F) + \alpha + \chi(F) \mid \alpha \in \mathrm{Stab}_E(x)\}$。由于 $\chi(F) = \chi(F)^{-1}$，且 $\mathbb{F}_2^E$ 是阿贝尔群，因此我们有 $\mathrm{Stab}_E(x') = \mathrm{Stab}_E(x)$。◀

我们还注意到，一个遗传有限集的两个不同的**maxOrb**参数，可以用 x的大小和轨道大小来界定。

引理 8。设 $x \in$ HF(E)。则 $\mathbf{maxOrb}_E(x) \le |\mathbf{Orb}_E(x)| \cdot |\mathbf{tc}(x)|$，且 $\mathbf{maxOrb}_{\mathrm{CFI}}(x) \le |\mathbf{Orb}_{\mathrm{CFI}}(x)| \cdot |\mathbf{tc}(x)|$。

证明。令 $y \in \mathrm{tc}(x)$为使 $\mathrm{maxOrb}_E(x)$ 取得最大值的集合，即 $|\mathrm{Orb}_E(y)| = \mathrm{maxOrb}_E(x)$。令 $Y := \mathrm{Orb}_E(y) \cap \mathrm{tc}(x)$。显然，对于任意 $\rho_F \in \mathrm{Aut}_{\mathrm{CFI}}(\mathfrak{G})$，$\rho_F(Y) \subseteq \mathrm{tc}(\rho_F(x))$，且$\rho_F(x) \in \mathrm{Orb}_E(x)$。因此：

$$
|\mathbf{Orb}_E(y)| \le \Big| \bigcup_{\rho_F \in \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})} \rho_F(Y) \Big| \le |\mathbf{Orb}_E(x)| \cdot |\mathrm{tc}(x)|.
$$

同理，$\mathbf{maxOrb}_{\mathrm{CFI}}(x)$ 的命题也得证。 ◀

在 [10], 中，我们为那些在$\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})$中所有自同构作用下都保持不变的遗传有限集引入了超对称性 这一术语。定理 1 所需的超对称性概念可以稍作放宽，即相对于$\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})$的轨道大小不必恰好为一。

▶ **定义 9** (超对称对象)。 固定一族 *CFI* 图$(\mathfrak{G}_n^S)_{n\in\mathbb{N}}$，并为每个 n 固定一个 $\mu_n \in \mathrm{HF}(\widehat{E}_n)$。若 $|\mathbf{Orb}_E(\mu_n)| \le \mathrm{poly}(|\mathfrak{G}_n^S|)$，则对象 μ_n 是超对称的。

如果一个集合是超对称的且 CPT 可定义的，那么我们可以确定其参数$\mathbf{maxOrb}_E$:

▶**引理 10**。 如果 μ_n 在 $\mathfrak{G}_n^S$ 中是超对称 且CPT 可定义 的，那么$\mathbf{maxOrb}_E(\mu_n)$ 在 $|\mathfrak{G}_n^S|$ 中有多项式上界。

证明。 根据超对称性， $|\mathbf{轨道}_E(\mu_n)|$有多项式上界。根据 CPT 可定义性，$|\mathrm{tc}(\mu_n)|$ 有多项式上界。因此，结论由引理 8 得出。 ◀

因此，这种意义下的超对称对象满足相同的轨道界：相对于更大的对称群 $\mathbb{F}_2^E \cong \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})$，所有 CPT 可定义对象自然地也满足这一界；对后者而言，所考虑的是输入结构的自同构群。

CFI 自同构的支撑

一般而言，置换群 $\Gamma \leq \mathbf{Sym}(A)$ 的一个支撑 是一个子集 $S \subseteq A$ ，满足 S 在$\mathbf{Sym}(A)$ 中的逐点稳定子是 Γ 的子群。遗传有限集的支撑是其稳定子群的支撑。对于$\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})$ 的子群，我们将采用另一种概念，称为*CFI* 支撑。之所以需要为这些群定义一种特定类型的支撑，是因为否则，群 $\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})$ 不存在唯一的最小支撑。

定义 11 (CFI 支撑)。 对象 $x \in \mathrm{HF}(E)$ 的 CFI 支撑 是一个子集 $S \subseteq E$，使得每个满足 $F \cap S = \emptyset$ 的 $\rho_F \in \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})$ 都会固定 x。

总是存在唯一的最小 CFI 支撑：

▶ **引理 12**。 设 $\mathfrak{G}^S$ 是一个 *CFI* 实例，且 $x \in \mathrm{HF}(\widehat{E})$。设 A_1、$A_2 \subseteq E$ 是 x的 *CFI* 支撑。那么 $A_1 \cap A_2$ 也是 x的 *CFI* 支撑。

证明。假设 $A_1 \cap A_2$ 不是 x的 CFI 支撑。那么存在一个与 $A_1 \cap A_2$ 不相交的 $F \subseteq E$，使得 $\rho_F(x) \neq x$。设 $F_1 := F \cap A_1$，且 $F_2 := F \cap A_2$。这些集合都非空，因为：如果 F 与 A_1 没有交集，那么 $\rho_F(x) = x$，因为 A_1 是 x 的 CFI 支撑。对 A_2 也同理。此外，根据假设， F_1 和 F_2 都与 $A_1 \cap A_2$不相交，因此 $F_1 \cap F_2 = \emptyset$也与之不相交。进一步， $F' := F \setminus (F_1 \cup F_2)$ 与 $A_1 \cup A_2$ 不相交，因此 $\rho_{F'}$ 固定 x。由此可知，翻转 $F_1 \cup F_2$ 中的边会移动 x，因为根据假设， $\rho_F(x) \neq x$。但这产生了矛盾，因为 $\rho_{F_1}(x) = x$ （因为 F_1 与支撑 A_2不相交），同理， $\rho_{F_2}(x) = x$。 ◀

这证明了以下定义是合理的：

定义 13 (最小 CFI 支撑)。 对于 $x \in \mathrm{HF}(E)$，$\mathrm{sup}_{\mathrm{CFI}}(x) \subseteq E$ 表示 E 的唯一最小子集，且该子集是 x 的 *CFI* 支撑。

如上所述，对于一般的 CPT 可定义对象，只有考虑“真正的”自同构群 $\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G}^S)$，才能对轨道大小给出上界。只有当对象还具有超对称性时，其$\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})$-轨道大小才是多项式级的。不过，取决于基图的结构，即使对象不一定具有超对称性，有时我们也能对 $\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})$-轨道大小给出上界：

▶ **引理 14**。 设 $\mu \in \mathrm{HF}(\widehat{E})$ 是 $\mathfrak{G}^S$ 上的一个遗传有限集。设 k 为图 $G - \mathrm{sup}_{\mathrm{CFI}}(\mu)$ 中的连通分量数（即移除最小 *CFI* 支撑中的边后得到的基图）。那么 $|\mathbf{Orb}_E(\mu)| \leq 2^{k^2} \cdot |\mathbf{Orb}_{\mathfrak{G}^S}(\mu)|$。

证明。 令 $A = \text{支撑}_{\mathrm{CFI}}(\mu) \subseteq E$ 为 μ的最小 CFI 支撑。则对于每个 $\rho_F \in$**自同构**$_{\mathrm{CFI}}(\mathfrak{G})$ 满足 $F \cap A = \emptyset$，都有 $\rho_F(\mu) = \mu$。因此，边翻转 ρ_F对μ 的影响仅取决于 $F \cap A$。所以有：

$$|\mathbf{轨道}_E(\mu)| \leq 2^{|A|},$$

因为任何 $F \subseteq E$ 与支撑 S 相交的方式有 $2^{|A|}$ 种，而且如果 $F \cap A = F' \cap A$，那么也有 $\rho_F(\mu) = \rho_{F'}(\mu)$。
现在，我们通过分析对于自同构 $\rho_F \in \mathrm{Aut}_{\mathrm{CFI}}(\mathfrak{G}^S)$ 而言，有多少个 A 的子集可以作为交集 $F \cap A$ 出现，来计算 $|\mathrm{Orb}_{\mathfrak{G}^S}(\mu)|$ 的下界。与 $\mathrm{Aut}_{\mathrm{CFI}}(\mathfrak{G})$ 中的边翻转不同，这些是沿着 G 中的环进行的边翻转。令 $X_1, ..., X_k \subseteq V(G)$ 表示图 $G - A$ 中连通分量的顶点集。我们根据边所连接的连通分量，将边集 A 划分为至多 k^2 个子集。因此，对于每一对 $(i, j) \in [k]^2$，令 $A_{(i,j)} \subseteq A$ 表示 A 中连接连通分量 X_i 和 X_j 的那些边。现在可以看出，对于每一对 $i \neq j$，对于每个具有偶数基数的 $B \subseteq A_{(i,j)}$，都存在 G 中若干环的某个对称差，其与 A 的交恰好为 B。这是因为任意两条边 $e, e' \in A_{(i,j)}$ 都位于一条经过连通分量 X_i 和 X_j 的环上。对于 $A_{(i,i)} \subseteq A$，每个子集 $B \subseteq A_{(i,i)}$ 都可以由某些环的对称差生成，因为每个 $e \in A_{i,i}$ 的端点都在同一个连通分量中（但为简单起见，我们也假设在这种情况下，只有 $A_{(i,i)}$ 的偶数子集能够通过某些环的对称差得到）。综上所述，我们有：

$$|\{B \subseteq A \mid \text{ there exists a } \rho_F \in \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G}^S) \text{ such that } F \cap A = B\}| \geq \prod_{(i,j)\in[k]^2} 2^{|\mathcal{A}_{(i,j)}|-1} = 2^{|A|-k^2}.$$

令 s 表示上述集合中满足翻转 B 会稳定 μ 的 $B \subseteq A$ 数量。于是，根据轨道-稳定子定理，我们有 $|\mathbf{轨道}_{\mathfrak{G}^S}(\mu)| \geq 2^{|A|-k^2}/s$，且 $|\mathbf{轨道}_E(\mu)| \leq 2^{|A|}/s$。将这两个不等式结合起来，便得到所需的界 $|\mathbf{轨道}_E(\mu)| \leq 2^{k^2} \cdot |\mathbf{轨道}_{\mathfrak{G}^S}(\mu)|$。◀

这个引理实质上表明，只要一个对象的 CFI 支撑将基图分成的连通分量数量较少，那么相对于由所有边翻转构成的群 **自同构群**$_{\mathrm{CFI}}(\mathfrak{G})$，还是相对于由环边翻转构成的群 **自同构群**$_{\mathrm{CFI}}(\mathfrak{G}^S)$ 来考察轨道大小，并无区别：

▶ **推论 15**。 固定一个 *CFI* 结构族 $(\mathfrak{G}_n^S)_{n\in\mathbb{N}}$。设 $\mu_n \in \mathrm{HF}(\widehat{E}_n)$。若 $G_n - \mathrm{sup}_{\mathrm{CFI}}(\mu_n)$ 中的连通分量数量至多为 $O(\sqrt{\log |\mathfrak{G}_n^S|})$，则 $|\mathbf{轨道}_E(\mu_n)| \leq \mathrm{poly}(|\mathfrak{G}_n^S|) \cdot |\mathbf{轨道}_{\mathfrak{G}^S}(\mu)|$。

4 CFI-对称遗传有限集和算法

对于源自线性有序基图、附带颜色类大小为对数级的拟序的基图，以及次数为线性的基图 [10, 32] 的实例，CPT 可以定义 CFI 查询。所有这些 CPT 算法都依赖于构造一个特定的超对称遗传有限集 $\mu \in \mathrm{HF}(E)$，它在给定实例 $\mathfrak{G}^S$ 时编码 $|S|$ 的奇偶性。除了超对称性之外，我们还找出了这类遗传有限集的另一种性质，它使其轨道大小较小，并适合用于编码奇偶性。我们称之为 *CFI* 对称性。直观地说，集合 $\mu \in \mathrm{HF}(E)$ 是 CFI 对称的，是指它的“构件”表现得类似于 CFI 图中的 CFI 小工具，即每当偶数个“关联小工具”发生翻转时，这些构件也会“翻转”。这些构件就是集合的连通分量。为定义它们，固定一个 CFI 图 $\mathfrak{G}^S$ 和一个集合 $\mu \in \mathrm{HF}(\widehat{E})$，并令 $\sim_E$ 为元素 $x \in \mathrm{tc}(\mu)$ 上的如下等价关系：对于 x，$x' \in \mathrm{tc}(\mu)$，若存在一个边翻转 $\rho_F \in \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})$ 使得 $x' = \rho_F(x)$，则记作 $x \sim_E x'$。对象 $x \in \mathrm{tc}(\mu)$ 在 $\mathrm{tc}(\mu)$ 中的 $\sim_E$-等价类记作 $[x]_{\sim_E}$ 或 $[x]$。关系 $\sim_E$ 诱导出一个划分

$\mathcal{C}(x)$，将每个 $x \in \mathrm{tc}(\mu)$ 划分为$\mathcal{C}(x) := \{([z]_{\sim_E} \cap x) \mid z \in x\}$。在 [10]，中，$\mathcal{C}(x)$ 的元素称为 x 的连通分量 。现在，在一个 *CFI* 对称 对象中，对于每个 $x \in \mathrm{tc}(\mu)$，每个连通分量 $\gamma \in \mathcal{C}(x)$ 的表现都像一个 CFI 小工具。也就是说，该连通分量在 $\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})$ 下恰有两个像：它要么被翻转，要么被稳定，而这两种情况取决于 γ 中元素的翻转连通分支的奇偶性。在将其形式化之前，我们先考虑一个小型“奇偶性追踪”遗传有限集示例，其构造方式与 [10] 和 [32] 中的算法类似。

例 16. 下面是一个遗传有限集 $\mu_{\{e,f,g\}} \in \mathrm{HF}(E)$ 的示例，其中包含 $E = \{e, f, g\}$。它记录边 e, f, g 的边翻转奇偶性。为了便于阅读，这个集合以结构化形式呈现，因此集合 $\mu_{\{f,g\}}$ 和 $\widetilde{\mu}_{\{f,g\}}$ 显示在下一层。

$$\mu_{\{e,f,g\}} = \Big\{ \{\mu_{\{f,g\}}, e_0\}, \{\widetilde{\mu}_{\{f,g\}}, e_1\} \Big\}$$

$$\{\{f_0, g_0\}, \{f_1, g_1\}\} \qquad \{\{f_0, g_1\}, \{f_1, g_0\}\}$$

每个 μ-对象都只有一个连通分量，该分量由两个通过 $\sim_E$ 关联的集合组成。例如，每当翻转的边数为偶数时，$\mu_{\{e,f,g\}}$ 的两个元素就会相互映射。$\mu_{\{e,f,g\}}$ 这两个元素本身有两个连通分量：显然， e_0 和 $\mu_{\{f,g\}}$ 无法通过任何边翻转相互映射。 f_0 和 g_0 也是如此。它们构成集合 $\{f_0, g_0\}$ 的不同连通分量；而 $\{\{f_0, g_0\}, \{f_1, g_1\}\}$ 则仍然只有一个连通分量，当且仅当 $\{f, g\}$ 中偶数条边发生翻转时，该连通分量才会稳定。集合在拥有两个连通分量和拥有一个连通分量之间交替变化的模式，是已知 CFI 算法所构造的奇偶性跟踪对象的典型特征。

现在我们可以观察到，与 CFI 小工具行为类似的对象是集合内部的连通分量，而不是 $\mathrm{tc}(\mu_{\{e,f,g\}})$ 本身的集合。例如，集合 $\{f_0, g_0\}$ 和 $\{\mu_{\{f,g\}}, e_0\}$ 无法像 CFI 小工具那样在两种状态之间“翻转”。它们相对于边翻转的轨道大小为四。但每当这些集合作为另一个集合的元素出现时，它们都会与其轨道中的对应集合一同出现，从而确保它们在父节点集合内部的连通分量再次具有“CFI 性质”：其轨道大小为二，并且当且仅当偶数个元素发生翻转时，它才会“翻转”。请注意，连通分量中每个成员被翻转的元素数量总是相同的。例如，在连通分量 $\{\{f_0, g_0\}, \{f_1, g_1\}\}$ 中，显然 f_0 被翻转当且仅当 f_1 被翻转，且 g_0 被翻转当且仅当 g_1 被翻转；因此，$\{f_0, g_0\}$ 和 $\{f_1, g_1\}$ 总是受到相同数量的翻转影响，$\{\mu_{\{f,g\}}, e_0\}$ 和 $\{\widetilde{\mu}_{\{f,g\}}, e_1\}$ 也是如此。因此，将每个集合内部的连通分量视为 CFI 顶点小工具的类似物，并将某个分量的任意成员中的元素视为其“关联边”是合理的；这些边的翻转会影响该“顶点小装置”。

将这个例子推广开来，这类追踪奇偶性的对象所具有的结构模式可以形式化如下：

定义 *17*（*CFI*-对称连通分量与对象）。设 $\mu \in HF(E)$， $x \in tc(\mu)$，且$\gamma \subseteq x$ 是 x的一个连通分量。则称 γ 是 *CFI*-对称的，当且仅当 $|Orb_E(\gamma)| = 2$，并且对于每个 $\rho_F \in Aut_{\mathrm{CFI}}(\mathfrak{G})$，都有 $\rho_F(\gamma) = \gamma$ ；这等价于对于每个 / 任意 $y \in \gamma$， y 中翻转连通分支的数量为偶数，即 $|\{\gamma' \in C(y) \mid \rho_F(\gamma') \neq \gamma'\}|$。

集合 μ 若满足以下两个条件，则为 CFI-对称 ：

1. 对于每个 $\rho_F \in Aut_{\mathrm{CFI}}(\mathfrak{G})$，都有 $\rho_F(\mu) = \mu$；这等价于 μ中翻转连通分支的数量为偶数，即 $|\{\gamma \in C(\mu) \mid \rho_F(\gamma) \neq \gamma\}|$。*2.* 对于每个 $x \in tc(\mu)$，每个连通分量 $\gamma \in C(x)$ 都是 *CFI*-对称的。

我们绝不会处理这样的对象 $\mu \in \mathrm{HF}(E)$：其中 $\mathrm{tc}(\mu)$ 中集合的连通分量只有一部分而非全部是 CFI-对称的。因此，在上述定义中，当我们谈到“ y 的翻转连通分支”并将其记作 $\{\gamma' \in \mathcal{C}(y) \mid \rho_F(\gamma') \neq \gamma'\}$ 时，连通分量 $\rho_F(\gamma') \neq \gamma'$ 确实是 γ' 的“翻转”，因为 γ' 的轨道大小恰好为二。

我们仍需证明，正如示例中所指出的，定义 17 中“每个/任意”的表述确实是合理的。

引理18。 令 $\mu \in \mathrm{HF}(E)$、$x \in \mathrm{tc}(\mu)$，并令 $\gamma \subseteq x$ 为 x 的一个连通分量。对于任意两个 y、$y' \in \gamma$ 以及每个 $\rho_F \in \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})$，有

$$|\{\gamma' \in \mathcal{C}(y) \mid \rho_F(\gamma') \neq \gamma'\}| = |\{\gamma' \in \mathcal{C}(y') \mid \rho_F(\gamma') \neq \gamma'\}|.$$

证明。固定 $\rho_F \in \mathrm{Aut}_{\mathrm{CFI}}(\mathfrak{G})$。此外，令 $\rho \in \mathrm{Aut}_{\mathrm{CFI}}(\mathfrak{G})$ 为满足 $\rho(y) = y'$ 的自同构。之所以存在这样的自同构，是因为 $y \sim_E y'$。因此，ρ 诱导了从 $\mathrm{C}(y)$ 到 $\mathrm{C}(y')$ 的一个双射，因为它将 y 的每个连通分量映射到 y' 的一个连通分量。我们证明，对于每个分量 $\gamma' \in \mathrm{C}(y)$，都有：$\rho_F(\gamma') = \gamma'$ 当且仅当 $\rho_F(\rho(\gamma')) = \rho(\gamma')$。如果 $\rho_F(\gamma') = \gamma'$，那么（由于 $\mathrm{Aut}_{\mathrm{CFI}}(\mathfrak{G})$ 是阿贝尔的）：$\rho_F(\rho(\gamma')) = \rho(\rho_F(\gamma')) = \rho(\gamma')$。反之，如果 $\rho_F(\rho(\gamma')) = \rho(\gamma')$，那么 $\gamma' = \rho^{-1}(\rho(\gamma')) = \rho^{-1}(\rho_F(\rho(\gamma'))) = \rho_F(\gamma')$，其中最后一个等式同样由交换性得到。由于 $|\mathrm{C}(y)| = |\mathrm{C}(y')|$，引理得证。◀

▶ **定义19**（CFI-对称和超对称算法）。如果一个 *CPT* 程序 Π 在基图类 *K* 上判定 *CFI* 查询，并且对每个基图 $G \in K$ 上的输入 $\mathfrak{G}^S$ 都会激活一个 *CFI* 对称 *h.f.* 集合 $\mu \in \mathrm{HF}(\widehat{E})$（且判定 *CFI* 查询必须用到该集合 μ），则称其为CFI-对称。类似地，如果 Π 必然会激活一个超对称集合，则称其为超对称。当 Π 同时具有 *CFI* 对称性和超对称性时，它所激活的相关遗传有限集同时满足这两种性质。

“μ 对判定查询是必需的”这一条件，意指 Π 若不激活 μ 就无法成功。定理 29 指出，在 CPT 中定义 CFI 查询必须激活一个具有大支撑的遗传有限集；这一点也说明了上述说法的合理性。目前已知的所有用于 CFI 查询的 CPT 算法，在此意义下都是 CFI-对称的。我们没有在这里明确证明这一点，因为这还需要介绍 [10] 和 [32] 中的算法，而本文已经很长。不过，要验证这两篇论文中定义的遗传有限集恰好满足我们在此称为 CFI 对称性的设计模式，并不困难。

5 将遗传有限集合转换为异或电路

异或电路是一种连通有向无环图 $C = (V_C, E_C)$，具有唯一指定的根 r。其内部节点视为异或门，叶节点对应电路的输入门。如果 $(g, h) \in E_C$，那么门 h 的输出是门 g的输入。每个异或电路都计算其输入位某个子集上的布尔异或函数。

这类电路是我们用来刻画 $\mathrm{HF}(E)$ 中CFI 对称遗传有限集结构的组合对象。考察这些遗传有限集时，我们始终将它们视为定义在某个基图 $G = (V, E)$ 上的给定 CFI 结构 $\mathfrak{G}^S$ 之上的对象。在 CPT 中定义它们时，必须保留输入结构 $\mathfrak{G}^S$的对称性，尤其是

基图的自同构 $\mathbf{Aut}(G)$。这种对称性会反映在相应异或电路的对称性中。因此，我们必须形式化描述图 G 的自同构如何作用于异或电路：

我们称一个异或电路 C 是定义在图 $G = (V,\ E)$上的电路，如果C 的输入门带有 E中边的标记。更准确地说，设 $L \subseteq V_C$ 为 C的叶节点。存在一个单射标记函数 $\ell:\ L \longrightarrow E$，它将输入门与 G的边对应起来。为讨论该电路的语义，我们引入一组形式命题变量$\mathcal{V}(G)$: $= \{X_e \mid e \in E\}$。对于每个输入门 $g \in L$，该门的输入位是变量 $X_{\ell(g)}$的值。

由于每个内部门都是异或门，它所计算的函数是对 $\mathsf{V}(G)$ 的某个子集取异或。就我们的目的而言，这个子集是门的主要有趣性质，我们将其称为 $\mathsf{X}(g)$。形式地，若 $g \in L$，则 $\mathsf{X}(g)$: $= \{\ell(g)\} \subseteq E$。若 g 是一个内部门，则 $\mathsf{X}(g)$: $= \bigtriangleup_{h \in gE_C} \mathsf{X}(h)$，即对 g的所有子节点的 $\mathsf{X}(h)$ 取对称差。换言之，$\mathsf{X}(g) \subseteq E$ 恰好是 E 中的边集合，使得 g 计算布尔函数$\bigoplus_{e \in} \mathsf{X}(g)\ X_e$。电路 C所计算的函数是对 $\mathsf{X}(r) \subseteq E$取异或，其中 r 是 C的根。另一种理解方式是：对于任意门 g，$\mathsf{X}(g)$ 是 g 所计算的函数敏感的输入位集合，也就是说，当且仅当被翻转的边位于 $\mathsf{X}(g)$ 中时，翻转电路的单个输入位才会改变 g 的值。

5.1 电路的对称性

图 G 上的电路 C 受自同构群 $\mathsf{Aut}(G) \leq \mathsf{Sym}(V)$ 的作用。任意 $\pi \in \mathsf{Aut}(G)$ 都会改变 L 中输入门的标签。因此，设 $g \in L$ with$\ell(g) = e = \{u, v\} \in E$。那么，$\pi(g)$ 是一个输入门，其 $\ell(\pi(g)) = \pi(e) = \{\pi(u)\ \pi(v)\} \in E$。这也适用于 C 的子电路以及 C 本身，因此 $\pi(C)$ 只是相应修改输入标签后的 C。如果存在一个双射 $\sigma:\ V_C \longrightarrow V_C$，它是图 (V_C, E_C) 的自同构，并且对每个输入门 $g \in V_C$ 都满足 $\ell(\sigma(g)) = \pi(\ell(g))$，我们就称 π 可扩展为 C 的自同构。我们记作

$$\textbf{稳定子}_G(C) = \{\pi \in \textbf{自同构}(G) \mid \pi \text{ 可扩展为 } C \text{ 的自同构}\} \leq \textbf{自同构}(G),$$

以及：$\mathbf{Orb}_G(C) = \{\pi(C) \mid \pi \in \mathbf{Aut}(G)\}$。

5.2 参数扇入维数

我们将从 CFI 对称遗传有限集构造的异或电路，将满足某种关于门的扇入界。不过，这个界并不像通常那样针对门的输入连线数量，而是针对所谓的“输入信息的线性代数复杂度”。E 的子集在对称差运算下构成一个布尔向量空间。这个空间同构于 $\mathbb{F}_2^E$。

对于异或电路 $C = (V_C,\ E_C)$ 的每个内部门 g，我们可以关联一个布尔矩阵 $M(g) \in \mathbb{F}_2^{gE_C \times E}$，称之为门矩阵：索引为 $h \in gE_C$ 的行定义为 $\mathcal{X}(h) \subseteq E$ 的特征向量的转置，即 $M(g)_{h-} = \chi(\mathcal{X}(h))^T$。在此处及下文中，我们用 χ 表示从 $\mathcal{P}(E)$ 到 $\mathbb{F}_2^E$ 的双射，它将 E 的每个子集映射为其特征布尔向量。若 g 是输入门，则定义 $M(g) \in \mathbb{F}_2^{[1] \times E}$ 为仅含一行的矩阵，其唯一一行为 $\chi(\mathcal{X}(g)))^T = \chi(\{\ell(g)\})^T$。

▶ **定义 20**（扇入维数）。门 g 的扇入维数是 $M(g)$ 的行空间维数，或者等价地，$\boldsymbol{rk}(M(g))$。
g 的扇入维数，限制在空间 $\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G}^S)$（也称为受限扇入维数）上，为

$$\dim(M(g)\cdot \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G}^S)) = \dim\{M(g)\cdot \mathbf{v} \mid \mathbf{v}\in \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G}^S)\}.$$

电路 C 的（受限）扇入维数，是 C 中任一门的最大（受限）扇入维数。

因此，门 g 的扇入维数就是 $\mathbb{F}_2^E$ 的子空间的维数；该子空间由特征向量 $\chi(\mathcal{X}(h)) \in \mathbb{F}_2^E$ 张成，其中 h 遍历 g 的所有子节点。对$\mathbf{rk}(M(g))$ 的一种解释是，它告诉我们门 g 处可能出现多少种不同的输入比特模式：当我们考虑电路的所有 $2^{|E|}$ 种可能输入时，$\{0,1\}^{gE_C}$ 中作为 g 的子节点值而出现的不同二进制字符串数量为 $2^{\mathbf{rk}(M(g))}$。

有时我们还需要受限扇入维数。如果只允许电路输入向量 $\mathbf{x}\in\mathbb{F}_2^E$，且$\mathbf{x}$ 中值为 1 的项在基图 G 中构成一个圈的集合（即来自$\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G}^S)$ 的输入向量），它描述了门可能出现多少种不同的输入模式。

这些扇入维数的概念是不同寻常的电路参数，但正如我们将要证明的，它们很好地刻画了原始遗传有限集相对于边翻转群$\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})$ 和 $\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G}^S)$ 的轨道大小。总体而言，遗传有限对象的电路表示相较于 CFI 图的优势在于，它简化了复杂自同构群$\mathbf{Aut}(\mathfrak{G}^S) \le \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G}) \wr \mathbf{Aut}(G)$ 的作用：为了证明 CFI 查询不属于 CPT，我们最终希望证明，某些遗传有限集相对于$\mathbf{Aut}(\mathfrak{G}^S)$ 必然具有超多项式轨道。通过将这些对象转换为电路，我们可以用扇入维数来表示$\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})$ 所施加的限制，剩下的任务就是分析其相对于$\mathbf{Aut}(G)$ 的轨道大小。

5.3 电路构造

T以下定理是定理 1 的证明核心。我们将先证明它，然后
e我们将在下一节说明，还需要哪些步骤才能由此得出定理 1。

▶**定理 21**。固定一族$(G_n)_{n\in\mathbb{N}}$ 基图。对于每个 $n\in\mathbb{N}$，令 $\mathfrak{G}_n^S$ 为基于 $G_n=(V_n,E_n)$ 的 *CFI* 图，并令 $\mu_n\in \mathrm{HF}(E_n)$ 为一个CFI-对称 遗传有限集，在输入 $\mathfrak{G}_n^S$ 上 *CPT* 可定义（对整个图族使用同一个 *CPT* 程序）。那么对于每个$n\in\mathbb{N}$，都存在一个异或电路 $C(\mu_n)=(V_C,E_C)$，其定义在 G_n 上并满足：

1. 电路的大小，即 $|V_C|$，关于 $|\mathfrak{G}_n^S|$ 是多项式。*2.* 电路的轨道大小 $|Orb_G(C(\mu_n))|$ 关于 $|\mathfrak{G}_n^S|$ 是多项式。*3.* $C(\mu_n)$ 对边 $e\in E_n$ 敏感，当且仅当 $e\in sup_{\mathrm{CFI}}(\mu_n)$。*4.* $C(\mu)$ 的扇入维数为 $O(log(maxOrb_E(\mu)))$。限制在空间 $Aut_{\mathrm{CFI}}(\mathfrak{G}_n^S)$ 上的扇入维数为 $O(log(maxOrb_{\mathrm{CFI}}(\mu)))$。

现在我们给出该电路的构造，并证明若干引理，由此可得该电路具有所需的性质。固定 $\mu\in \mathrm{HF}(E)$，并将相应的异或电路记为 $C(\mu)=(V_C,E_C)$，我们将在下文定义该电路。电路的门是 $\mathsf{tc}(\mu)$ 中对象的$\sim_E$-等价类。回顾一下，$\sim_E$-等价是关于边翻转 $\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})$ 的同轨道关系。每当我们对一个 $x\in\mathsf{tc}(\mu)$ 写 $[x]$ 时，形式上指的是满足 $\rho_F(x)\in\mathsf{tc}(\mu)$ 的 $[x]=\{\rho_F(x) \mid \rho_F\in \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})\}$。电路$C(\mu)$定义如下：

$V_C := \text{tc}(\mu)/\sim_E = \{[x] \mid x \in \text{tc}(\mu)\}$. $E_C := \{([x], [y]) \mid$ 存在 $y' \in [y]$ 使得 $y' \in x\}$。根据定义，$C(\mu)$ 的叶节点对应于 $\text{tc}(\mu)$ 中原子的 $\sim_E$-等价类。原子的集合是 E，因此 C 的任意叶节点都具有 $[e_0]$ 的形式，其中 $e \in E$。令 $\ell([e_0]) := e$。$C(\mu)$ 的根 r 是 $[\mu]$。换言之，该电路就是有向无环图 $(\text{tc}(\mu), \in)$，其中已将 $\sim_E$-等价关系取商。

首先，我们必须检查边集 E_C 是否确实可以这样定义，也就是说，$[x]$ 与 $[y]$ 之间是否存在 E_C-边，与定义中为 $[x]$ 选取哪个代表元无关。在下述引理中，令 $\in^\mu$ 表示遗传有限集 μ中 $\text{tc}(\mu)$ 上的元素关系。

▶ **引理 22.** 设 $[x], [y] \subseteq \text{tc}(\mu)$ 是两个 $\sim_E$ 等价类。若存在 $y' \in [y]$ 使得 $y' \in^\mu x$，则对每个 $x' \in [x]$，都存在一个 $y' \in [y]$ 使得 $y' \in^\mu x'$。

证明。设 $y' \in [y]$ 使得 $y' \in^\mu x$。现在任取 $x' \in [x]$，并令 $\rho_F \in \text{Aut}_{\text{CFI}}(\mathfrak{G})$满足 $\rho_F(x) = x'$。于是 $\rho_F(y') \in^\mu \rho_F(x)$，因为该运算是逐元素进行的。集合 $\rho_F(x) \in [x]$ 是 $\text{tc}(\mu)$ 的一个元素，因为 $[x]$ 表示 $\text{tc}(\mu)$ 内的 $\sim$等价类。因此，我们也有 $\rho_F(y') \in \text{tc}(\mu)$，从而 $\rho_F(y') \in [y]$。这就证明了该引理。◀

定理 21 的性质 2 指出，$C(\mu)$ 的 $\mathbf{Aut}(G)$-轨道足够小。我们通过证明该轨道不会大于遗传有限集 μ 的 $\mathbf{Aut}(G)$-轨道来说明这一点；对于 μ，我们知道其轨道关于 $|\mathfrak{G}^S|$ 是多项式规模的，因为根据定理 21 的假设，它是 CPT 可定义的。

▶ **引理 23。** 每个 $\pi \in$ **稳定子**$_G(\mu) \leq$ **对称群**(V) 都可以扩展为电路 $C(\mu)$ 的一个自同构，即：**稳定子**$_G(\mu) \leq$**稳定子**$_G(C(\mu))$。

证明。令 $\pi \in \text{Stab}_G(\mu) \leq \text{Aut}(G)$。也就是说，$\pi$ 可扩展为有向无环图 $(\text{tc}(\mu), \in^\mu)$ 的一个自同构 $\sigma : \text{tc}(\mu) \longrightarrow \text{tc}(\mu)$。我们定义 $\sigma' : V_C \longrightarrow V_C$，令 $\sigma'([x]) = [\sigma(x)]$。这是良定义的，因为 $x \sim_E x'$ 当且仅当 $\sigma(x) \sim_E \sigma(x')$（$\sigma$ 是 μ 的一个自同构）。现在我们检查 σ' 是由 π 诱导的 $C(\mu)$ 的一个自同构。

显然，σ' 是 V_C上的双射，即是$\text{tc}(\mu)$的 $\sim_E$-类集合上的双射：因为σ 是满射，所以它也是满射；由于它将 V_C 映射到 V_C，因此已经是双射。令 $[e_0] \in V_C$ 为一个输入门。于是，$\ell([e_0]) = e$。我们有 $\sigma(e_0) = \pi(e)_0$。因此，$\sigma'([e_0]) = [\pi(e)_0]$。所以，$\ell(\sigma'([e_0])) = \pi(\ell([e_0]))$，如所要求。

现在令$([x], [y]) \in E_C$。那么存在一个 $y' \in [y]$，使得 $y' \in^\mu x$。由于 σ 是一个自同构，因此同样有 $\sigma(y') \in^\mu \sigma(x)$。因此，$([\sigma(x)], [\sigma(y')]) \in E_C$。有$([\sigma(x)], [\sigma(y')]) = (\sigma'[x], \sigma'[y']) = (\sigma'[x], \sigma'[y])$，所以$(\sigma'[x], \sigma'[y]) \in E_C$。总之，这意味着 $\pi \in \text{Aut}(G)$扩展为电路 $C(\mu)$的自同构σ'。◀

▶ **推论 24.** $|$**轨道**$_G(C(\mu))| \leq |$**轨道**$_G(\mu)|$.

证明。由引理 23 和轨道-稳定子定理可得，该定理指出$|$轨道$_G(C(\mu))| = |\text{Aut}(G)|/|$稳定子$_G(C(\mu))|$ 且 $|$轨道$_G(\mu)| = |\text{Aut}(G)|/|$稳定子$_G(\mu)|$。◀

接下来，我们希望分析 $C(\mu)$ 的扇入维数，以及 $C(\mu)$ 与 $\text{sup}_{\text{CFI}}(\mu)$ 之间的联系。为此，关键是要建立所有 $x \in \text{tc}(\mu)$ 对应的稳定子**稳定子**$_E(x)$ 与相应门矩阵的核之间的联系。关于这些矩阵的定义，请参阅第 5.2 节。我们从以下观察开始，它将 $\text{tc}(\mu)$ 中对象的稳定子与其元素的稳定子联系起来。

▶ **命题 25**。 对于每个 $x \in \mathrm{tc}(\mu)$，均有 **稳定子**$_E(x) = \bigcap_{y \in x}$**稳定子**$_E([y] \cap x) = \bigcap_{\gamma \in \mathcal{C}(x)}$ **稳定子**$_E(\gamma)$。

这显然成立，因为当且仅当 x 被 $\rho_F \in \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})$ 稳定时， x 内的每个 $\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})$-轨道都被 ρ_F 按集合固定。

▶ **引理 26**。 对于每个门 $[x] \in V_C$ 及其门矩阵 $M[x] \in \mathbb{F}_2^{[x]E_C \times E}$，有：

$$\boldsymbol{Ker}(M[x]) = \mathbf{Stab}_E(x) = \mathbf{Stab}_E(x') \text{ for every } x' \in [x].$$

对于每一行 $M[x]_{[y]-}$，当 $[y] \in [x]E_C$ 时，有：

$$\boldsymbol{Ker}(M[x]_{[y]-}) = \mathbf{Stab}_E([y] \cap x) \qquad (\star)$$

证明。对于每个 $x' \in [x]$，均有 $\mathrm{Stab}_E(x) = \mathrm{Stab}_E(x')$；此外，对于每个 $x' \in [x]$，也有 $\mathrm{Stab}_E([y] \cap x) = \mathrm{Stab}_E([y] \cap x')$（由引理 7）。因此，$(\star)$ 不依赖于代表元的选择。由 $(\star)$ 立即可得 $\mathrm{Ker}(M[x]) = \mathrm{Stab}_E(x)$，这是由于命题 25，以及 $\mathrm{Ker}(M[x])$ 是 $M[x]$ 各行的核的交集这一事实。现在，我们通过从输入门到根的归纳法证明 $(\star)$。如果 $[x] = [e_0]$ 是一个输入门，则 $M[x]$ 只有一行，即 $\chi(e)^T$。 $\chi(e)^T$ 的核是 $\mathbb{F}_2^E$ 中在指数 e 处取零的所有向量的集合。这恰好是 $\mathrm{Stab}_E(e_0) = \mathrm{Stab}_E(e_1)$，如所需。现在假设 $[x]$ 是一个内部门，即 x 是 $\mathrm{tc}(\mu)$ 中的一个非原子 h.f. 集合。 $M[x] \in \mathbb{F}_2^{[x]E_C \times E}$ 的每一行都是 X $[y] \subseteq E$ 的特征向量，其中 $[y] \in [x]E_C$。我们有

$$\mathcal{X}[y] = \bigtriangleup_{[w] \in [y]E_C} \mathcal{X}[w].$$

用矩阵向量记法，我们可以将其写为 s:

$$M[x]_{[y]-} = \chi(\mathcal{X}[y])^T = \sum_{[w] \in [y]E_C} (M[y]_{[w]-})^T = (1\ 1\ \ldots\ 1) \cdot M[y].$$

设 $\gamma \in \mathcal{C}(x)$ 是满足 $\gamma = [y] \cap x$ 的连通分量。上式意味着 $\mathbf{Ker}(M[x]_{[y]-}) = \mathcal{E}_y$，其中 $\mathcal{E}_y$ 表示 $\mathbb{F}_2^E$ 中所有在 $M[y]$ 下的像具有偶汉明重量的向量所构成的集合。因此，我们必须证明 $\mathcal{E}_y = \mathbf{Stab}_E(\gamma)$。每一行 $M[y]_{[w]-}$ 对应一个满足 $w \in \gamma'$ 的连通分量 $\gamma' \in \mathcal{C}(y)$。

根据归纳假设，对每一行 $M[y]_{[w]-}$ 和每个 $\mathrm{v} \in \mathbb{F}_2^E$，都有 $M[y]_{[w]-} \cdot \mathrm{v} = 1$ 当且仅当 $\mathrm{v} \notin \mathrm{Stab}_E([w] \cap y)$。因此， $M[y] \cdot \mathrm{v}$ 具有偶汉明重量，当且仅当 $\rho_{\chi^{-1}}(\mathrm{v}) \in \mathrm{Aut}_{\mathrm{CFI}}(\mathfrak{G})$ 翻转 y 的偶数个连通分量。这又当且仅当 $\rho_{\chi^{-1}}(\mathrm{v})$ 在每个 $y' \in \gamma$ 中都翻转偶数个连通分量（由引理18可知）。根据 CFI 对称性的定义（定义 17），这当且仅当 $\mathrm{v} \in \mathrm{Stab}_E(\gamma)$，因为 μ 是 CFI 对称的，因此 γ 是一个 CFI 对称分量。总之，我们证明了 $\mathrm{v} \in \mathrm{E}_y$ 当且仅当 $\mathrm{v} \in \mathrm{Stab}_E(\gamma)$。这就证明了 $M[x]$ 的每一行都满足 $(\star)$。◀

根据核与稳定子之间的这种对应关系，我们可以给出 $C(\mu)$ 的扇入维数上界。这证明了定理 21 中的**性质 4** 。

▶ **引理 27.** 扇入维数 $C(\mu)$为 $\log(\mathbf{maxOrb}_E(\mu))$。

证明。 令 $x \in \mathrm{tc}(\mu)$。由轨道-稳定子定理以及 $|\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})| = 2^{|E|}$这一事实，可得

$$\mathbf{Orb}_E(x) = \frac{2^{|E|}}{|\mathbf{Stab}_E(x)|} \leq \mathbf{maxOrb}_E(\mu).$$

这意味着 $\log(\mathbf{maxOrb}_E(\mu)) \geq |E|$ –维数 **稳定子**$_E(x)$。根据引理 26，**稳定子**$_E(x)$ =**核**($M[x]$)。
由秩定理可得：$\mathbf{rk}(M[x]) = |E| -$ 维数 **稳定子**$_E(x) \leq \log(\mathbf{maxOrb}_E(\mu))$。由于存在一个对象 $x \in \mathrm{tc}(\mu)$，使得 $\mathbf{maxOrb}_E(\mu)$ 取得最大值，因此 $\mathbf{rk}(M[x])$ =$\log(\mathbf{maxOrb}_E(\mu))$ 确实是 $C(\mu)$ 的任意门矩阵的最大秩。◀

▶ **引理 28.** $C(\mu)$ 相对于空间 $\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G}^S)$ 的扇入维数 为$\log(\mathbf{maxOrb}_{\mathrm{CFI}}(\mu))$。也就是说，对于 $C(\mu)$ 中的每个门 $[x]$，我们有

$$\dim(M[x] \cdot \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G}^S)) \leq \log(\mathbf{maxOrb}_{\mathrm{CFI}}(\mu)).$$

证明。 令 $x \in \mathrm{tc}(\mu)$。由轨道-稳定子定理可得

$$\mathbf{Orb}_{\mathrm{CFI}}(x) = \frac{|\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G}^S)|}{|\mathbf{Stab}_{\mathrm{CFI}}(x)|} = 2^{\dim \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G}^S) - \dim \mathbf{Stab}_{\mathrm{CFI}}(x)} \leq \mathbf{maxOrb}_{\mathrm{CFI}}(\mu).$$

因此，

$$\log \mathbf{maxOrb}_{\mathrm{CFI}}(\mu) \geq \dim \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G}^S) - \dim \mathbf{Stab}_{\mathrm{CFI}}(x).$$

利用引理 26，可得 **稳定子**$_{\mathrm{CFI}}(x) \subseteq$ **稳定子**$_E(x) \subseteq$ **核**($M[x]$)。因此，

$$\dim(M[x] \cdot \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G}^S)) \leq \dim \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G}^S) - \dim \mathbf{Stab}_{\mathrm{CFI}}(x) \leq \log \mathbf{maxOrb}_{\mathrm{CFI}}(\mu).$$

◀

定理 21 的证明。 首先，由假设可知，μ 在结构$\mathfrak{G}^S$中是 CPT 可定义的，因此，大小 $|\mathrm{tc}(\mu)|$ 和轨道 $|\mathbf{Orb}_{\mathbf{Aut}(\mathfrak{G}^S)}(\mu)|$ 关于 $|\mathfrak{G}^S|$是多项式级的。因此，定理 21 中的**性质 1** 显然对 $C(\mu)$成立，因为 $|V_C| \leq |\mathrm{tc}(\mu)|$。**性质 2**由 $|\mathbf{Orb}_{\mathbf{Aut}(\mathfrak{G}^S)}(\mu)|$ 的界、推论 24 以及$|\mathbf{Orb}_G(\mu)| \leq |\mathbf{Orb}_{\mathbf{Aut}(\mathfrak{G}^S)}(\mu)|$这一事实推出。

性质 4 由引理 27 和 28 得证。最后，**性质 3** 可如下看出：设 $C(\mu)$ 对一条边 $e \in E$敏感。这意味着，对于 $C(\mu)$的根 $r = [\mu]$，$e \in \mathcal{X}(r)$。当且仅当对奇数个子节点 $[y] \in [\mu]E_C$，$e \in \mathcal{X}([y])$时，情况才是如此。这等同于说，列 $M[\mu]_{-e}$ 具有奇数汉明重量。根据引理 26 中的等式 $(\star)$，当且仅当对奇数个子节点 $[y] \in [\mu]E_C$，$\chi(e) \notin$ **稳定子**$_E([y] \cap x)$时，这一结论成立。由于 μ 是 CFI-对称的，根据定义 17，当且仅当 $\rho_e(\mu) \neq \mu$时，情况才是如此。而这当且仅当 $e \in \mathrm{sup}_{\mathrm{CFI}}(\mu)$ 成立（因为 $\mathrm{sup}_{\mathrm{CFI}}(\mu)$ 是 μ最小的 CFI 支撑）。◀

5.4 证明主要定理

至此，我们已经将 HF(E) 中的 CFI 对称遗传有限集转换为具有定理 21 所述性质的异或电路。要据此得出定理 1，还缺少的一步是证明：任何同时具有超对称性和 CFI 对称性、并判定 CFI 查询的 CPT 算法，都必须构造一个遗传有限集，其性质可转换为定理 1 中的电路性质。幸运的是，已有一个与此相关的结果。Dawar、Richerby 和 Rossman [10] 给出了针对判定 CFI 查询的一般 CPT 程序的以下支撑下界。

▶ **定理 29** (定理 40 的证明中隐含的 [10])。设$(G_n)_{n\in\mathbb{N}}$ 是一个基图族，并设$\boldsymbol{tw}_n$ 表示 G_n 的树宽。设$\mathfrak{G}_n^S$、$\mathfrak{G}_n^{S'}$ 表示两个非同构的

定义在 G_n上的 *CFI* 结构。设 $f(n) \leq tw_n$ 是一个函数，使得对于所有长度为 $\leq 2f(n)$的元组， $\mathfrak{G}_n^S$ 和 $\mathfrak{G}_n^{S'}$ 都是 $\mathcal{C}^{tw_n}$-齐次的。
因此，任何对所有 $n \in \mathbb{N}$ 都能区分 $\mathfrak{G}_n^S$ 和 $\mathfrak{G}_n^{S'}$ 的 *CPT* 程序，都必须在输入 $\mathfrak{G}_n^S$ 上激活一个遗传有限集 x，其最小支撑的大小至少为 $\Omega(f(n))$。

如果对于任意两个元组 a 和 b，它们在 $\mathfrak{G}_n^S$ 中具有相同的$\mathcal{C}^{\mathbf{tw}_n}$-类型，那么存在一个 $\mathfrak{G}_n^S$ 的自同构，将 a 映射到 b，则结构 $\mathfrak{G}_n^S$ 是 $\mathcal{C}^{\mathbf{tw}_n}$- 齐次的。元组 a 在 $\mathfrak{G}_n^S$ 中的 $\mathcal{C}^{\mathbf{tw}_n}$- 类型，是所有在 $(\mathfrak{G}_n^S, a)$ 中为真的 $\mathcal{C}^{\mathbf{tw}_n}$-公式的集合。通过仔细检查 [10]，中的整个证明可以看出，实际上只需在较弱的意义下要求齐性：对于某个 有界长度的所有元组，$\mathcal{C}^{\mathbf{tw}_n}$-类型划分与轨道划分一致——因此才有上述定理中的明确限制。

正如 [10] 中所述并在 [31], 中证明的那样，某些有序 CFI 图满足齐次性条件；正如我们将要证明的那样，我们用于定理 2 下界的超立方体上的无序 CFI 图也满足该条件。因此，在我们所关注的情形中，齐次性条件实际上并不是一种限制，这也是我们在定理 1 中省略它的原因。我们还省略了一点，即必须联系两种不同的支撑概念。定理 21 涉及遗传有限集的最小 CFI 支撑，而上述支撑下界涉及最小的 $\mathbf{Aut}(\mathfrak{G}^S)$-支撑。因此，为了完整且正确地表述定理 1，我们必须讨论这两种支撑之间的比值。

▶ **定义 30**（CFI 支撑间隙）。设 $G = (V, E)$ 是一个基图， $\mathfrak{G}^S$ 是其上的一个 *CFI* 图。设 $\mu \in \mathrm{HF}(\widehat{E})$。记 $s(\mu)$ 为 μ 的最小 $\mathbf{Aut}(\mathfrak{G}^S)$ 支撑的大小（而$\mathrm{sup}_{\mathrm{CFI}}(\mu)$ 仍表示最小 *CFI* 支撑）。

那么我们称比值

$$\alpha(\mu) = \frac{s(\mu)}{|\sup_{\mathrm{CFI}}(\mu)|}$$

为 μ 的CFI 支撑间隙 （相对于 $\mathfrak{G}^S$）。

那么，定理 1 的详细版本如下：

▶ 定理 *31.* 设 $(G_n = (V_n, E_n))_{n\in\mathbb{N}}$ 是一个基图序列。设 $\mathfrak{G}_n^S$ 是 G_n 上的一个 *CFI* 图，令 tw_n 表示 G_n 的树宽。设 $f(n) \in O(tw_n)$ 是一个函数，使得对于所有长度为 $\leq 2f(n)$ 的元组，每个 $\mathfrak{G}_n^S$ 都是 $\mathcal{C}^{tw_n}$-齐次。设 $g(n)$ 是一个函数，使得对于每个 $\mu \in HF(E_n)$，若其最小支撑为 $s(\mu) \in \Omega(f(n))$，则其 *CFI* 支撑间隙有界于 $g(n)$。

如果存在一个CFI-对称 *CPT* 程序 Π，能够对所有 $\mathfrak{G}_n^S$ 判定 *CFI* 查询，那么对于每个 $G_n = (V_n, E_n)$，都存在一个基于 G_n 的异或电路 C_n，满足定理 *21* 中以下“实例化性质”：

1. C_n 中的门数是关于 $|\mathfrak{G}_n^S|$的多项式。*2.* 电路的轨道大小 $|Orb_{G_n}(C_n)|$ 是关于 $|\mathfrak{G}_n^S|$的多项式。*3.* C_n 对 E_n中的 $\Omega(f(n)/g(n))$ 条边敏感。*4.* 将 C_n限制在空间 $Aut_{\mathrm{CFI}}(\mathfrak{G}_n^S)$上时，其扇入维数为 $O(\log|\mathfrak{G}_n^S|)$。*5.* 如果程序 Π 除了是 *CFI*-对称之外还是超对称，或者如果删除任意 $f(n)/g(n)$ 条边后，基图 G_n 分解为至多 $O(\sqrt{\log}\ |\mathfrak{G}^S|)$ 个连通分量，那么 C_n 的（不受限）扇入维数也为 $O(\log|\mathfrak{G}_n^S|)$。

证明。假设存在这样的 CPT 程序 Π。令 $\mu_n \in \mathrm{HF}(E_n)$ 表示该程序在输入 $\mathfrak{G}_n^S$ 上激活的、具有大支撑的 CFI 对称遗传有限集。根据定理 29，对象 μ_n 的最小 $\mathrm{Aut}(\mathfrak{G}_n^S)$ 支撑大小为 $\Omega(f(n))$。由于 μ_n 在 $\mathfrak{G}_n^S$ 中的 CFI 支撑间隙至多为 $g(n)$，因此 μ_n 的最小 CFI 支撑大小至少为：$\mathrm{sup}_{\mathrm{CFI}}(\mu_n) \in \Omega(f(n)/g(n))$。将定理 21 应用于 μ_n，可得异或电路 C_n。定理 21 的性质 3 与界 $\mathrm{sup}_{\mathrm{CFI}}(\mu_n) \in \Omega(f(n)/g(n))$ 结合起来，意味着 C_n 对 E_n 中的 $\Omega(f(n)/g(n))$ 条边敏感。定理 21 的性质 4 分别将扇入维数和受限扇入维数界定为 $\log(\mathrm{maxOrb}_E(\mu_n))$ 和 $\log(\mathrm{maxOrb}_{\mathrm{CFI}}((\mu_n))$ 的函数。引理 8 指出，$\mathrm{maxOrb}_E(\mu_n) \le |\mathrm{Orb}_E(\mu_n)|\cdot|\mathrm{tc}(\mu_n)|$，且 $\mathrm{maxOrb}_{\mathrm{CFI}}(\mu_n) \le |\mathrm{Orb}_{\mathrm{CFI}}(\mu_n)| \cdot |\mathrm{tc}(\mu_n)|$。由于 μ_n 由 CPT 程序 Π 在输入 $\mathfrak{G}_n^S$ 上定义，$|\mathrm{tc}(\mu_n)|$ 和 $|\mathrm{Orb}_{\mathrm{CFI}}(\mu_n)|$ 均有关于 $|\mathfrak{G}_n^S|$ 的多项式界（轨道有界，是因为 $\mathrm{Aut}_{\mathrm{CFI}}(\mathfrak{G}^S)$ 是 $\mathrm{Aut}(\mathfrak{G}_n^S)$ 的子群）。由此可得 $\mathrm{maxOrb}_{\mathrm{CFI}}(\mu_n)$ 的多项式界。结合受限扇入维数的 $\log(\mathrm{maxOrb}_{\mathrm{CFI}}((\mu_n))$ 界，即可得到本定理的性质 4。

若 Π 是超对称的，则由引理 10 可推出性质 5；若从基图 G_n 中移除 $\mathrm{sup}_{\mathrm{CFI}}(\mu_n)$ 后，它分裂为有界数量的连通分量，则由推论 15 可推出性质 5。◀

6 更一般的遗传有限集的异或电路

到目前为止，我们已经证明，通过对边翻转群 $\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})$ 作用下的轨道取商，可以相当容易地将 CFI 结构 $\mathfrak{G}^S$ 上的 *CFI* 对称 遗传有限集转换为异或电路。重要的是，这种构造会自动将遗传有限集的相关性质（例如支撑大小和对称性）转换为较为自然的电路性质。因此，原则上，只要证明某些多项式大小的对称异或电路族具有适当的下界，我们就能限制 CFI 查询上的 *CFI* 对称 算法的能力。尽管目前已知的所有 CFI 查询无选择算法都是CFI 对称的，而且非 CFI 对称算法是否真的更强尚不明确，但如果电路转换足够通用，能够用于分离整个 CPT 与 P，而不只是 CFI 对称算法，那就更好了。本小节将探讨电路构造在多大程度上能够朝这个方向推广。我们将介绍对上述构造的一种修改：它使用附加构件，不再限制于 CFI 对称集，并且保留定理 21 的几乎所有性质。所谓“几乎所有”，是指我们必须在电路中引入的附加构件大小未知。因此，我们无法确定所构造的电路始终具有多项式大小。不过，我们可以针对遗传有限集提出一个条件，将 CFI 对称性推广，并保证电路大小为多项式。该条件涉及带有一个作用于指标集上的置换群的布尔向量空间。如果 $\mathbb{F}_2^E$ 的某些子空间（它们表现为 μ 中各集合连通分量的稳定子群）拥有一个在该置换群（它将是 $\mathbf{Aut}(G)$ 的子群）作用下（近似）不变的基，那么由 μ 构造的电路就具有多项式大小。本节的结果如下：

▶**定理 32.** 固定一个基图族 $(G_n)_{n\in\mathbb{N}}$。对于每个 $n \in \mathbb{N}$，令 $\mathfrak{G}_n^S$ 为基于 $G_n = (V_n, E_n)$ 的 *CFI* 图，并令 $\mu_n \in \mathrm{HF}(\widehat{E}_n)$ 为一个在输入 $\mathfrak{G}_n^S$ 上 *CPT* 可定义的遗传有限集（整个图族使用同一个 *CPT* 程序）。那么对于每个 $n \in \mathbb{N}$，存在一个异或电路 $C(\mu_n) = (V_C, E_C)$，其定义在 G_n 的边上，并满足：

1. 电路的轨道大小 $|\mathbf{Orb}_G(\widehat{C}(\mu_n))|$ 关于 $|\mathfrak{G}_n^S|$ 是多项式级的。2. $\widehat{C}(\mu_n)$ 对 E 中至少 $\lfloor \mathrm{sup}_{\mathrm{CFI}}(\mu) \log(\mathbf{maxOrb}_E(\mu)) \rfloor$ 条边敏感。

3. $C(\mu)$ 的扇入维数为 $O(\log(\max \mathrm{Orb}_E(\mu)))$。*4.* 如果对每个满足 $[y] \cap x \neq \emptyset$ 的 $x, y \in \mathrm{tc}(\mu)$，空间 $\mathrm{Stab}_E([y] \cap x)$ 都有一个对称基（见定义 *56*），那么 $|V_C|$ 的大小关于 $|\mathfrak{G}^S|$ 是多项式级的。

该定理与针对 CFI-对称对象的定理 21 有两方面不同。首先，电路 $C(\mu)$ 不一定对 $\sup_{\mathrm{CFI}}(\mu)$ 中的所有边都敏感，而只对其中对数比例的边敏感。其次，除非所有空间**稳定子** $_E([y] \cap x)$ 都具有对称基，否则我们无法保证电路的大小；我们将在第 6.3 节正式介绍这一概念。需要指出的是，定理中提到的第四个性质，据我们所知，并非“当且仅当”条件。即使 μ 不满足对称基条件，$C(\mu)$ 也可能具有多项式大小。

由此，我们得到定理 31 的以下版本，适用于判定 CFI 查询的非 CFI-对称 CPT 程序。用于判定 CFI 查询的具有大支撑的遗传有限集，其为 CFI-对称集这一条件，被弱化为对称基条件。正如我们稍后在引理 59 中所示，每个 CFI-对称集也都有对称基；此外，也有一些非 CFI-对称集具有对称基的简单例子（见例 60）。因此，对称基条件确实是 CFI 对称性的严格推广。

▶ **定理 33**。 设 $(G_n = (V_n, E_n))_{n \in \mathbb{N}}$ 是一个基图序列。设 $\mathfrak{G}_n^S$ 是定义在 G_n上的 *CFI* 图，令 tw_n 表示 G_n的树宽，并设 $f(n) \leq tw_n$ 是一个函数，使得对于所有长度为 $\leq 2f(n)$的元组，$\mathfrak{G}_n^S$都是 C^{tw_n}-齐次的。

设 $g(n)$ 是一个函数，使得对于每个 n 时，由 CFI 聚撑间隙 E_n 是最小支撑为 $\mathrm{tc}(\mu)$ 的 HF，$\widehat{\ }$

设 Π 是一个 *CPT* 程序，它使用具有充分支撑的遗传有限集 $\mu_n \in \mathfrak{G}_n^S$，在所有 $\mathfrak{G}_n^S$ 上判定 *CFI* 查询，并且对于所有满足 $[y] \cap x \neq \emptyset$的 $x, y \in \mathrm{tc}(\mu_n)$，$\mathbf{Stab}_E([y] \cap x)$ 都具有符合定义 *56* 的对称基 。

此外，假设 Π 是超对称，或者基图 G_n 在移除任意 $f(n)/g(n)$ 条边后，至多分解为 $O(\sqrt{\log |\mathfrak{G}^S|})$ 个连通分量。那么，对每个 $n \in \mathbb{N}$，都存在一个基于 G_n 的异或电路 C_n，满足定理 *32* 中以下“实例化性质”:

1. C_n 中的门数是关于 $|\mathfrak{G}_n^S|$的多项式。2. 该电路的轨道大小 $|\mathrm{Orb}_{G_n}(C_n)|$ 是关于 $|\mathfrak{G}_n^S|$ 的多项式。3. C_n 对 E_n中的 $\Omega(f(n)/(g(n) \cdot \log |\mathfrak{G}_n^S|))$ 条边敏感。4. C_n 的扇入维数为 $O(\log |\mathfrak{G}_n^S|)$。我们省略该定理的证明，因为它可由定理 32 以与定理 31 由定理 21 推出相同的方式得到。

现在我们开始证明定理 32，该证明贯穿本节余下部分。需要指出的是，定理 21 实际上是该定理的一个特例，因此我们本可以省略针对 CFI-对称对象的电路构造；然而，我们现在给出的更一般构造不如针对 CFI-对称对象的构造自然，而且描述起来要困难得多。

再次固定一个基图 $G = (V, E)$、其上的一个 CFI 图 $\mathfrak{G}^S$，以及一个对象 $\mu \in \mathrm{HF}(\widehat{E})$。这一次，$\mu$ 不必是 CFI-对称的。在上一小节中，我们用 $C(\mu)$表示将 $\mathrm{tc}(\mu)$ 中的 $\sim_E$ 类因子化后得到的电路。现在，我们将构造出的电路记为 $\widehat{C}(\mu)$。在说明构造之前，先来看看为什么 $C(\mu)$并不是“我们想要的电路”。

如果 μ 不是 CFI-对称的。上一小节中唯一用到 CFI 对称性的地方，是引理 26 的证明；该引理将门矩阵的核与向量空间 **稳定子**$_E(x)$ 联系起来。这种联系至关重要，因为它建立了 $\sup_{\mathrm{CFI}}(\mu)$ 与 $C(\mu)$ 对其输入位的敏感性之间的联系，而且对于得到 $C(\mu)$ 的扇入维数界也必不可少。没有这样的界，构造就没有意义，因为不施加扇入限制时，总是存在规模较小的对称异或电路。因此，我们希望确保即使 μ 不是 CFI-对称的，引理 26 的陈述对$\nsim C(\mu)$仍然成立。现在再看一遍引理 26 的归纳证明。归纳证明的关键在于，对于任意门矩阵 $M[x]$ 以及 $[x]$ 的任意一个子门 $[y]$，行 $M[x]_{[y]-}$ 都可以写成另一个矩阵与子门矩阵$M[y]$的乘积：$M[x]_{[y]-} = (1\ 1\ \ldots\ 1) \cdot M[y]$。这个等式成立是因为$\mu$具有 CFI 对称性。而在一般情形下，也会有一个类似的等式，即：$M[x]_{[y]-} = N \cdot M[y]$，其中矩阵 N 需要根据 **稳定子**$_E([y] \cap x)$ 来选取。因此，本章节的计划如下：首先，我们将定义这些 N矩阵，它们本质上是在非 CFI 对称情形下“修补”引理 26 的证明。基于这些矩阵以及$\nsim C(\mu)$，我们将通过引入一些构件来模拟所选N矩阵的作用，从而构造 $C(\mu)$。这样一来，即使 μ 不是 CFI-对称的，引理 26 的证明也能再次成立。从某种意义上说，我们可以将这些构件视为对 CFI 对称性局部违反情况的修正。

6.1 矩阵的定义

实际上，我们不仅要定义所述的 N-矩阵，还要为每个 $[x] \in \{[x] \mid x \in \mathrm{tc}(\mu)\}$ 定义一个布尔矩阵 $M[x]$。我们沿用上一小节中的记号 $M[x]$，尽管严格来说，$M[x]$ 并不是 $C(\mu)$ 中任何门的门矩阵；相反，它是一个满足 $\mathrm{Ker}(M[x]) = \mathrm{Stab}_E(x)$ 的矩阵，并将作为 $C(\mu)$ 中某个构件的一种构造规范。我们将要定义的 $M[x]$-矩阵取决于对象 μ 中 x 的连通分量的 M-矩阵和 N-矩阵。因此，这些矩阵的构造是从 μ 的原子开始，递归地推进到嵌套更深的集合。在此阶段，我们的主要目标是构造这些矩阵，使它们的核对应于其所属集合的稳定子空间。此外，这些矩阵还应满足关于 $\mathrm{Stab}_G(\mu) \leq \mathrm{Aut}(G)$ 作用的某些对称性要求。只有在构造出这些矩阵之后，我们才会用它们 $\widehat{\ }$ $\widehat{\ }$
来构造电路 $C(\mu)$，使得 $C(\mu)$ 的门矩阵符合预期。因此，本小节中的步骤与上一小节中的步骤正好相反：上一小节先构造电路，再分析其门矩阵；而现在，我们先指定 $\widehat{\ }$ 矩阵，然后构造电路，从而确保引理 26 的陈述通过构造对 $C(\mu)$ 成立。除矩阵外，我们还将给出某些确保对称性的群同态。为了讨论矩阵的对称性，我们引入记号来表示行置换和列置换的作用：

令 $M \in \mathbb{F}_2^{I \times J}$为任意布尔矩阵，$\sigma\colon I \longrightarrow I'$，$\pi\colon J \longrightarrow J'$为双射。那么 $(\sigma, \pi)(M) \in \mathbb{F}_2^{I' \times J'}$是一个矩阵，对每个 $(i, j) \in I \times J$，其 $(\sigma, \pi)(M)_{\sigma i, \pi j} = M_{i, j}$。特别地，若 $\sigma \in$ **对称群**(I) $\pi \in$ **对称群**(J)，那么 $(\sigma, \pi)(M)$ 就是对 M分别应用行置换和列置换后得到的矩阵。

▶ **命题 34.** 设$\mathbf{v}$、$\mathbf{w}$ $\in \mathbb{F}_2^I$ 是两个布尔向量，且 $\pi \in$ **对称群**(I) 是对其分量进行置换的一个置换。那么

$$\mathbf{v}^T \cdot \mathbf{w} = \pi(\mathbf{v}^T) \cdot \pi(\mathbf{w}).$$

因此，若 $M \in \mathbb{F}_2^{I\times J}$是一个矩阵，且$\mathbf{w} \in \mathbb{F}_2^J$ 是一个向量，那么

$$\sigma(M \cdot \mathbf{w}) = (\sigma, \pi)M \cdot \pi(\mathbf{w}),$$

对于每个 $\sigma \in$ **对称群**(I) $\pi \in$ **对称群**(J)。

根据向量标量积的定义，这个命题可直接得出，因为$\mathbf{v}^T \cdot \mathbf{w}$ 和 $\pi(\mathbf{v}^T) \cdot \pi(\mathbf{w})$ 是同一组乘积之和，只是求和顺序不同。于是，关于矩阵向量乘法的结论也随之得出，因为它不过是每个行向量与$\mathbf{w}$的标量积。本节有时会在未明确引用的情况下使用这个命题。

在本节其余部分中，我们经常会提到以下轨道和稳定子。它们与上一节中的轨道和稳定子的不同之处在于，它们涉及子群**稳定子**$_G(\mu)$ $\leq$**Aut**(G)，而不是**Aut**(G)本身。因此，我们覆盖了上一节中的记号。令 $x \in$tc(μ)。

$$\mathbf{Orb}_G([x]) := \{\pi([x]) \mid \pi \in \mathbf{Stab}_G(\mu) \leq \mathbf{Aut}(G)\}.$$
$$\mathbf{Stab}_G([x]) := \{\pi \in \mathbf{Stab}_G(\mu) \mid \pi([x]) = [x]\}.$$

同样，对于 x， $y \in$ tc(μ)，**稳定子**$_G([y] \cap x)$ 指的是集合 $[y] \cap x$ 在群**稳定子**$_G(\mu)$中的稳定子。

任意 $\sim$-类的轨道都是 $\sim$-等价类的集合：

▶**引理 35**。 对于任意 $\sim_E$-类 $[x] \subseteq \mathrm{tc}(\mu)$，以及任意 $\pi \in$ **稳定子**$_G(\mu)$， $\pi([x])$ 也是$\mathrm{tc}(\mu)$的一个$\sim_E$-类。

证明。不难验证，对于任意 $\pi \in$Aut(G) 以及任意 $\rho_F \in$Aut$_{\mathrm{CFI}}(\mathfrak{G})$，有 $\rho_{\pi F} = \pi \circ \rho_F \circ \pi^{-1}$。令 x'、$x'' \in [x]$，并令 $\rho_F \in$Aut$_{\mathrm{CFI}}(\mathfrak{G})$ 满足 $\rho_F(x') = x''$。根据上述等式， $\rho_{\pi F}(\pi x') = \pi x''$。因此， $\pi(x') \sim_E \pi(x'')$。类似地可以证明，如果 $x' \not\sim_E x''$，则 $\pi(x') \not\sim_E \pi(x'')$。所以， $\pi([x])$ 又是一个 $\sim_E$-类。$\pi([x]) \subseteq$ tc(μ) 这一事实是因为 π 可扩展为遗传有限集 μ 的一个自同构。◀

▶ **推论 36**。 设 $x, y \in \mathrm{tc}(\mu)$ 满足 $[y] \cap x \neq \emptyset$。则

$$\mathbf{Stab}_G([y] \cap x) \leq \mathbf{Stab}_G([y]).$$

证明。 群 **稳定子**$_G([y] \cap x)$ 将集合 $[y] \cap x \subseteq [y]$ 映射到其自身，因此它不会将该子集从 $\sim$-类 $[y]$ 映入另一个 $\sim$-类。根据引理 35，它必定将整个类 $[y]$ 映射到其自身，因为 $[y]$ 的像仍须是一个 $\sim$-类。◀

▶ **引理 37**。 对于任意 $x, x', y \in \mathrm{tc}(\mu)$ ，若满足 $x \sim_E x'$ 且 $[y] \cap x \neq \emptyset$，则有

$$\mathbf{Stab}_E([y] \cap x) = \mathbf{Stab}_E([y] \cap x').$$

证明。 集合 $[y]\cap x$ 和 $[y]\cap x'$ 通过 $\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G})$中的一个自同构相关联。因此，将引理 7 应用于集合 $[y] \cap x$ 即可得到所需结论。◀

现在我们来讨论前述 M-矩阵和 N-矩阵的归纳定义。以下是我们将要定义的对象的准确清单：

(a) 对于每个 $[x] \in \{[x] \mid x \in \mathrm{tc}(\mu)\}$:

(i) 一个指标集 $I_{[x]}$。 **(ii)** 一个矩阵 $M[x] \in \mathbb{F}_2^{I_{[x]} \times E}$ 满足以下性质： **核**$(M[x])$ = **稳定子**$_E(x)$ （注意，对于每个 **稳定子**$_E(x)$ =**稳定子**$_E(x')$，根据引理 7， $x' \in [x]$ ）。

令 $\mathcal{C}[x] := \{[y] \mid [y] \cap x \neq \emptyset\}$ 表示 x的连通分量的 $\sim$-类（注意，这与$[x]$ 的代表元无关——见引理 22）。

(b) 对于每个 $[x] \in \{[x] \mid x \in \mathrm{tc}(\mu)\}$，其中 x 是一个集合，并且每个 $[y] \in \mathcal{C}[x]$:

(i) 一个指标集 $J_{[x][y]}$。 **(ii)**一个矩阵 $N[x][y] \in \mathbb{F}_2^{J_{[x][y]} \times I_{[y]}}$满足以下性质： **核**$(N[x][y] \cdot M[y])$ =**稳定子**$_E([y] \cap x)$ （根据引理 37， **稳定子**$_E([y] \cap x)$ 与 $[x]$的代表元选择无关）。

(c) 对于每个轨道 $\Omega_{[x]} := \mathbf{Orb}_G([x])$，令 $I_{\Omega_{[x]}} := \biguplus_{[x'] \in \Omega_{[x]}} I_{[x']}$。对于每个 $\Omega_{[x]}$，我们给出一个群同态 $g_{[x]}$:**稳定子**$_G(\mu)$ $\longrightarrow$ **对称群**$(I_{\Omega_{[x]}})$，使得对于每个 $[x'] \in \Omega_{[x]}$以及每个 $\pi \in$**稳定子**$_G(\mu)$，都有 $g_{[x]}(\pi)(I_{[x']}) = I_{\pi[x']}$。 $M\pi[x'] = (g_{[x]}, \pi)M[x']$对于每个$[x'] \in \Omega_{[x]}$ 以及 $\pi \in$ **稳定子**$_G(\mu)$。

(d) 对于每个轨道 $\Omega_{[x]}$，令

$$J_{\Omega_{[x]}} := \biguplus_{\substack{[x'] \in \Omega_{[x]} \\ [y'] \in \mathcal{C}[x']}} J_{[x'][y']}.$$

对于每个 $\Omega_{[x]}$，我们给出一个群同态 $h_{[x]}$: **稳定子**$_G(\mu)$ $\longrightarrow$ **对称群**$(J_{\Omega_{[x]}})$，使得对于每个 $[x'] \in \Omega_{[x]}$ 以及每个 $[y'] \in \mathcal{C}[x']$，都有 $h_{[x]}(\pi)(J_{[x'][y']}) = J_{\pi[x']\pi[y']}$。此外，对于每个 $[x'] \in \Omega_{[x]}$、 $[y'] \in \mathcal{C}[x']$ 以及 $\pi \in$ **稳定子** $_G(\mu)$， $N\pi[x']\pi[y'] = (h_{[x]}(\pi)\, g_{[x]}(\pi))N[x'][y']$。

群同态的作用是确保——当我们利用这些矩阵构造电路时——每个作用于输入门的 $\pi \in$ **稳定子**$_G(\mu)$ 都确实能够扩展为 $C(\mu)$ 的自同构。在实际进行构造之前，我们必须验证，群同态所见证的对称条件与矩阵核上的条件确实能够同时满足。换言之，我们必须证明，预期与相应核相等的稳定子空间，会被 $_G(\mu)$ 中的置换映射到彼此： **稳定子**

▶ **引理 38**。 设 $x \in \mathrm{tc}(\mu)$ 且 $\pi \in$**稳定子**$_G(\mu)$。那么

$$\mathbf{Stab}_E(\pi x) = \pi(\mathbf{Stab}_E(x)) = \{\pi \mathbf{v} \mid \mathbf{v} \in \mathbf{Stab}_E(x)\},$$

其中， $\pi \in$**对称群**(E) 通过置换向量的各个分量来作用于 $\mathbb{F}_2^E$。此外，对于每个$[y] \in \mathcal{C}[x]$，我们有

$$\mathbf{Stab}_E(\pi[y] \cap \pi x) = \pi(\mathbf{Stab}_E([y] \cap x)).$$

证明。对于任意 $\pi \in \mathrm{Aut}(G)$，以及任意 $\rho_F \in \mathrm{Aut}_{\mathrm{CFI}}(\mathfrak{G})$，均有 $\rho_{\pi F} = \pi \circ \rho_F \circ \pi^{-1}$。因此，当且仅当 $(\pi \circ \rho_F \circ \pi^{-1})(\pi x) = \pi x$ 时， $\rho_{\pi F} \in \mathrm{Stab}_E(\pi x)$。这当且仅当 $(\pi \circ \rho_F)(x) = \pi x$，也就是当且仅当 $\rho_F(x) = x$。这就证明了引理的第一部分，因为 $\chi(\pi F) = \pi(\chi(F))$。第二部分可以用同样的方法证明，因为$\frown \pi[y] \cap \pi x = \pi([y] \cap x)$。最后这个等式成立，是因为 π 在 HF(E) 上的作用是一个从 HF(E) 到其自身的双射，所以 $\pi[y] \cap \pi x \subseteq \pi([y] \cap x)$（若 π 在 HF(E) 上不是单射，则该结论未必成立）。◀

归纳构造

基础情形：
设 $x = e_i$，其中 $e \in E$ 和 $i \in \{0, 1\}$，是 tc(μ) 中的一个原子。于是我们定义

$$M[x] := \chi(e)^T.$$

形式上，我们将行指标集定义为 $I_{[x]} := \{[x]\}$，但任何一个与所有其他指标集都不同的单元素集合都可以。
现在，对于每个轨道 $\Omega_{[x]}$，其中 x 是 tc(μ) 中的一个原子，我们定义同态 $g_{[x]} : \textbf{稳定子}_G(\mu) \longrightarrow \textbf{对称群}(I_{\Omega_{[x]}})$，令 $g_{[x]}(\pi)([x']) := [\pi x']$，对每个 $\pi \in \textbf{稳定子}_G(\mu)$ 都成立；$[x'] \in I_{\Omega_{[x]}}$（注意，根据指标集的定义，$I_{[x]}$, $I_{\Omega_{[x]}}$ 等于轨道 $\Omega_{[x]}$）。

归纳步骤：
我们按照顺序 (b)、(d)、(a)、(c) 处理上述列表中的各项。设 $x \in$tc(μ) 是一个非原子对象，也就是一个集合。假设对于每个 $[y] \in \mathcal{C}[x]$ 和每个 $[y] \in \mathcal{C}[x']$，以及每个 $[x'] \in \Omega_{[x]}$，相应的、指标集为 $I_{[y]}$ 的矩阵 $M[y]$ 均已构造。因此，我们还假设，对于任何这样的 $[y]$，对应于 $\Omega_{[y]}$ 的同态 $g_{[y]}$ 已经定义。我们固定一个 y，使得 $[y] \in \mathcal{C}[x]$。对于这个固定的 Pair $[x]$, $[y]$，我们现在将构造矩阵 $N[x][y]$。然后，我们将对其施加 $\textbf{稳定子}_G(\mu)$ 的作用，使其封闭。也就是说，给定这个矩阵 $N[x][y]$，我们将对所有 $[y'] \in \Omega_{[y]}$，以及所有满足 $[y'] \in \mathcal{C}[x']$ 的 $[x'] \in \Omega_{[x]}$，对称地定义 $N[x'][y']$。
此后，仍可能存在一些连通分量 $[y'] \in \mathcal{C}[x]$，其对应的 $N[x][y']$ 尚未定义。在这种情况下，我们固定这样一个 $[y'] \in \mathcal{C}[x]$，显式定义相应的矩阵 $N[x][y']$，并对 $[x]$ 的所有 $\textbf{稳定子}_G(\mu)$-像对称地定义矩阵 $[y']$，依此类推。因此，我们首先必须说明如何定义相应的初始矩阵，再通过对称性从中得到其他矩阵。

N 矩阵的定义

设 $y \in$ tc(μ) 满足 $[y] \in \mathcal{C}[x]$。假设 $M[y]$、$I_{[y]}$ 和 $g_{[y]}$ 已经构造完成。矩阵 $N[x][y]$ 定义为满足以下两个条件的最小布尔矩阵：

(i) $\mathrm{Ker}(N[x][y]) \cap \mathrm{Im}(M[y]) = M[y] \cdot \text{稳定子}_E([y] \cap x) = \{(M[y] \cdot \mathrm{v}) \mid \mathrm{v} \in \text{稳定子}_E([y] \cap x)\}$。（对于矩阵 $M \in \mathbb{F}_2^{I \times J}$，$\mathrm{Im}(M)$ 表示 $\mathbb{F}_2^J$ 在 M 作用下的像空间。）(ii) 存在一个同态 h，从 $g_{[y]}(\text{稳定子}_G([y] \cap x)) \leq \mathrm{Sym}(I_{[y]})$ 到 $N[x][y]$ 的行指标集上的对称群，使得对于每个 $\sigma \in g_{[y]}(\text{稳定子}_G([y] \cap x))$，都有 $(h(\sigma)\ \sigma)(N[x][y]) = N[x][y]$。

在第二个性质中，我们滥用了记号，将 $g_{[y]}(\textbf{稳定子}_G([y] \cap x))$ 写成 $\textbf{对称群}(I_{[y]})$ 的一个子群，尽管 $g_{[y]}(\textbf{稳定子}_G([y] \cap x))$ 正式来说是 $\textbf{对称群}(I_{\Omega_{[y]}})$ 的一个子群。不过，根据推论 36，我们知道 $\textbf{稳定子}_G([y] \cap x) \leq \textbf{稳定子}_G([y])$，因此 $g_{[y]}(\textbf{稳定子}_G([y] \cap x))$ 确实将 $M[y]$ 的行指标集，也就是 $I_{[y]}$，映射到自身（见 $g_{[y]}$ 的性质 (c)，该性质由归纳假设成立）。

“最小”矩阵指满足 (i) 和 (ii) 且行数最少的矩阵。如果有多个矩阵的最小行数相同，则为 $N[x][y]$ 任意选取其中一个。

令 m 为 $N[x][y]$ 的行数。我们将 $N[x][y]$ 的行指标集 $J_{[x][y]}$ 定义为一个含 m 个元素的集合，且该集合与此前构造的所有其他指标集均不相交。形式上，可以令 $J_{[x][y]} := \{(i,\ [x],\ [y])\ \mid i \in [m]\}$ 来实现。

我们必须证明，总是存在一个满足 (a) 和 (b) 的矩阵。可以使用线性代数中的方法找到一个满足 (a) 的矩阵：

▶ **引理 39**。设 $\Gamma \leq \Delta \leq \mathbb{F}_2^I$ 为布尔向量空间。设 d 为 Γ 的维数，$k =$ 维数 $\Delta - d$ 为 Γ 在 Δ 中的余维数。存在一个矩阵 $N \in \mathbb{F}_2^{[k]\times I}$，使得核 $(N) \cap \Delta = \Gamma$。

证明。N 的每一 k 行都可以作为一个线性方程组的解得到。对于 $i \in [k]$、$j \in I$，令 $n_{ij} := N_{ij}$ 表示第 i 行第 j列中所求的元素。固定 Γ的一个基 B_Γ，并将该基扩展为 $\mathrm{B} \supseteq \mathrm{B}_\Gamma$，使得 $\mathrm{B} = \mathrm{B}_\Gamma \uplus \{\mathrm{w}1, ..., \mathrm{w}_k\}$ 是Δ的一个基。对于每个 $i \in [k]$，我们定义一个方程组 $A_i \cdot \mathbf{x} = \mathrm{b}_i$，其唯一解向量就是所需的 N 的第 n_{i1} 行（ n_{i2}、 ...、 $n_{i|I|}$）。该方程组有 dim Δ 个方程，其中每个方程都与 B 中的一个基向量相关联。对于每个基向量 $\mathrm{v} \in \mathrm{B} \setminus \{\mathrm{w}_i\}$，我们有方程

$$\sum_{j\in I} \mathbf{v}(j) \cdot \mathbf{x}(j) = 0$$

在方程组 $A_i \cdot \mathbf{x} = \mathbf{b}_i$ 中。对于基向量 $\mathbf{w}_i \in \mathcal{B}$，我们有方程

$$\sum_{j\in I} \mathbf{w}_i(j) \cdot \mathbf{x}(j) = 1$$

在 $A_i \cdot \mathbf{x} = \mathbf{b}_i$ 中。通过这种方式，我们定义 k 方程组，每个 $i \in [k]$ 对应一个方程组。事实上，它们的系数矩阵 A_i 都相同。其行是 $\mathcal{B}$ 中的向量（转置后）。向量$\mathbf{b}_i$ 在包含 $\mathbf{w}_i$ 的那一行对应的位置上有一个 1 元素，其余位置均为零。每个 A_i 的秩和行数都是 dim Δ，因为 $\mathcal{B}$ 是 Δ 的一个基。因此，每个方程组都有唯一解。若将 N 的每个元素 n_{ij} 定义为 $A_i \cdot \mathbf{x} = \mathbf{b}_i$ 的解向量的第 j 个元素，那么根据方程组的定义，$\mathbf{Ker}(N) \cap \Delta = \Gamma$ 确实成立。◀

这表明满足条件 (a) 的矩阵总是存在的。可以将该矩阵扩展为在 $g_{[y]}(\mathbf{Stab}_G([y] \cap x))$ 的作用下封闭，从而使其也满足条件 (b)。这要求我们希望作为 $N[x][y]$ 的核的向量空间在该置换群下是不变的：

▶ 引理 *40*。空间 $M[y] \cdot$ 稳定子$_E([y] \cap x) \leq \mathbb{F}_2^{I_{[y]}}$ 在置换群 $g_{[y]}$(稳定子$_G([y] \cap x)) \leq$ 对其向量各分量的作用下是不变的。也就是说，对于每个 $v \in M[y] \cdot$ 稳定子$_E([y] \cap x)$ 和 $\pi \in g_{[y]}$(稳定子$_G([y] \cap x))$，都有 $\pi(v) \in M[y] \cdot$ 稳定子$_E([y] \cap x)$。

证明。设 $\mathrm{v} \in M[y]\cdot$稳定子$_E([y]\cap x)$ 且 $\pi \in g_{[y]}$(稳定子$_G([y]\cap x))$。我们可以将 v 写作 $= M[y]\cdot \mathrm{w}$，其中某个 $\mathrm{w} \in$稳定子$_E([y] \cap x)$。固定一个 a $\sigma \in g_{[y]}^{-1}(\pi)$，即 $\sigma \in$ 稳定子$_G([y] \cap x)$。由命题 34 可得：

$$(\pi, \sigma)(M[y]) \cdot \sigma(\mathbf{w}) = \pi(\mathbf{v}).$$

由归纳假设可知 $(\pi, \sigma)(M[y]) = M[y]$，因为 $\sigma \in$**稳定子**$_G([y] \cap x) \leq$**稳定子**$_G([y])$（见上述枚举中的 (c) 项）。**稳定子**$_G([y] \cap x) \leq$**稳定子**$_G([y])$ 这一事实由推论 36 证明。由此得出：$M[y] \cdot \sigma(\mathbf{w}) = \pi(\mathbf{v})$。如果 $\sigma(\mathbf{w}) \in$

稳定子$_E$([y] ∩ x)，那么我们就完成了，并且得到 π(v) ∈ M[y] · 稳定子$_E$([y] ∩ x)，正如所需。为了证明 σ(w) ∈ 稳定子$_E$([y] ∩ x)，我们应用引理 38：由于 w ∈ 稳定子$_E$([y] ∩ x)，因此有 σ w ∈ σ(稳定子$_E$([y] ∩ x)) = 稳定子$_E$(σ[y] ∩ σx)。最后，如引理 38 的证明中所述，我们有 σ[y] ∩ σx = σ([y] ∩ x)，并且 σ([y] ∩ x) = [y] ∩ x 成立，因为σ ∈ 稳定子$_G$([y] ∩ x)。◀

了解这一点后，我们可以看到，确实有可能同时满足条件（i）和（ii）同时。

▶ **引理 41.** 设 [y] ∈ C[x]。存在一个布尔矩阵 N，满足上述条件（*i*）和（*ii*），即：

(i) Ker(N) ∩*Im(M[y])* = M[y] · 稳定子$_E$([y] ∩ x)。*(ii)* 存在一个同态 h，从 $g_{[y]}$(稳定子$_G$([y] ∩ x)) ≤ 对称群$(I_{[y]})$ 映射到 N 的行指标集上的对称群，使得对于每个 σ ∈ $g_{[y]}$(稳定子$_G$([y] ∩ x))，都有 (h(σ) σ)(N) = N。

证明。将引理 39 应用于 Δ = Im(M[y]) 和 Γ = M[y] · Stab$_E$([y] ∩ x)，可得到一个满足条件 (i) 的矩阵$N' \in \mathbb{F}_2^{[k]\times I_{[y]}}$；这里，k = dim(Im M[y]) − dim(M[y] · Stab$_E$([y] ∩ x))。我们可以在 N′ 上取 $g_{[y]}$(Stab$_G$([y] ∩ x)) ≤ Sym$(I_{[y]})$ 的作用闭包，从而也满足条件 (ii)：对于 N′ 的每一行 N'_{i-}，令 Orb(N'_{i-}) :={π(N'_{i-}) | π ∈ $g_{[y]}$(Stab$_G$([y] ∩ x))}。这里，π ∈ Sym$(I_{[y]})$ 对列进行置换，即置换相应行 N'_{i-} 的各个元素。现在令 N 为其行集合是各个 Orb(N'_{i-}) 的不交并的布尔矩阵。显然，存在一个从 $g_{[y]}$(Stab$_G$([y] ∩ x)) 到 N 的行上的对称群（更准确地说，到 $\Pi_{i\in[k]}$Sym(Orb(N'_{i-}))）的同态。这个同态正是 $g_{[y]}$(Stab$_G$([y] ∩ x)) 在 N 的各行上的群作用（分别作用于各个轨道 Orb(N'_{i-})）。
还需证明这个对称闭矩阵 N 仍满足条件 (i)，即 Ker(N) ∩Im(M[y]) = M[y] · Stab$_E$([y] ∩ x)。我们有 Ker(N) ∩Im(M[y]) ⊆ M[y] · Stab$_E$([y] ∩ x)，因为对于任意向量 v ∉ M[y] · Stab$_E$([y] ∩ x)，要么 v ∉Im(M[y])，要么若 v ∈Im(M[y])，则 N′ · v ≠ **0**，因为 Ker(N′) ∩Im(M[y]) = M[y] · Stab$_E$([y] ∩ x)。由于 N′是 N的子矩阵，我们也有 N · v ≠ **0**，因此 v ∉Ker(N)。所以 Ker(N) ∩Im(M[y]) ⊆ M[y] · Stab$_E$([y] ∩ x)。还需证明：M[y] · Stab$_E$([y] ∩ x) ⊆Ker(N) ∩Im(M[y])。因此，设 v ∈ M[y] · Stab$_E$([y] ∩ x)。那么 N′ · v = **0**。我们必须证明，对于每一行 N'_{i-} 以及每个 π ∈ $g_{[y]}$(Stab$_G$([y] ∩ x))，都有 π(N'_{i-}) · v = 0。该结论成立（见命题 34）：

$$\pi(N'_{i-}) \cdot \mathbf{v} = \pi^{-1}(\pi(N'_{i-})) \cdot \pi^{-1}\mathbf{v} = N'_{i-} \cdot \pi^{-1}\mathbf{v} = 0.$$

最终等式成立是因为 **核**(N′) = M[y] · **稳定子**$_E$([y] ∩ x)，并且根据引理 40，$\pi^{-1}\mathbf{v} \in M[y]$ · **稳定子**$_E$([y] ∩ x)。由于 N的每一行都具有 π(N'_{i-}) 的形式，其中 N'_{i-}是N′的某一行，且 π ∈ $g_{[y]}$ (**稳定子**$_G$([y] ∩ x))，因此我们证明了 M[y] · **稳定子**$_E$([y] ∩ x) ⊆**核**(N) ∩**Im**(M[y])。◀

该引理表明，存在一个满足条件（i）和（ii）的布尔矩阵，因此确实可以为 N[x][y] 选取一个最小的矩阵。问题在于，我们事先不知道它究竟有多小。因此，我们所描述的 C(μ) 构造并没有保证的大小界。稍后在第 6.3 节中，我们将重新讨论对 N[x][y] 的选择，并证明当 **稳定子**$_E$([y]∩x) 具有对称基时，如何界定其大小。其思路是，此时可以界定 N′ 在 $g_{[y]}$(**稳定子**$_G$([y] ∩ x)) 的作用下的闭包大小，因为 **稳定子**$_E$([y] ∩ x) 的基的对称性会沿着用于定义 N′ 各行的方程组 $A_i \cdot \mathbf{x} = \mathbf{b}_i$ “ 传播 ”。

由于至少存在一个满足（i）和（ii）的矩阵，因此确实可以将 $N[x][y]$ 定义为其中最小的一个。请记住，这一定义针对的是固定的 $[y] \in \mathsf{C}[x]$。现在取 $[y'] \in \Omega[y]$，以及满足 $[y'] \in \mathsf{C}[x']$ 的 $[x'] \in \Omega[x]$，并且存在一个 $\pi \in$稳定子$_G(\mu)$，使得 $\pi([y] \cap x) = [y'] \cap x'$（也可能有 $[x'] = [x]$）。令 $\pi_{[x'][y']} := \pi$，以便日后可以指代这个特定的置换。我们令 $J_{[x'][y']} := \{(i, [x'], [y']) \mid i \in [m]\}$。这里，$m$ 仍表示先前定义的 $N[x][y]$ 的行数。令 $N[x'][y']$ 为 $\mathbb{F}_2^{J_{[x'][y']} \times I_{[y']}}$ 中的布尔矩阵，使得对于每个 $i \in I_{[y]}$ 和 $k \in [m]$，均有 $(N[x'][y'])_{(k,[x'],[y'])}$ $g_{[y]}(\pi_{[x'][y']})(i) = (N[x][y])_{(k,[x],[y]),i}$。通常，我们会写作 $N([x'][y'])_{k,-}$，而不是 $(N[x'][y'])_{(k,[x'],[y'])}-$，以表示该矩阵的第 k 行。这样，我们便为所有 $[y'] \in \Omega[y]$ 定义了矩阵 $N[x'][y']$。我们将 $\sim$-类 $[y] \in \mathsf{C}[x]$ 称为轨道 $\Omega[y]$ 的初始元：这是我们任意选作其轨道中第一个类、以便利用引理 41 定义 $N[x][y]$ 的类。接着，我们选取一个新的初始元 $[y] \in \mathsf{C}[x]$，使得此前尚未定义 $N[x][y]$，并对 $[y]$ 及其轨道 $\Omega[y]$ 重复这一构造。重复此过程，直到对于每个 $[y'] \in \mathsf{C}[x']$ 以及每个 $[x'] \in \Omega[x]$，均已为每个 $[y] \in \mathsf{C}[x]$ 定义 $N[x][y]$。

我们证明，所定义的矩阵具有所需的性质：

▶ **引理 42.** 设 $[x'] \in \Omega[x]$ 和 $[y'] \in C[x']$。那么

$$\boldsymbol{Ker}(N[x'][y'] \cdot M[y']) = \mathbf{Stab}_E([y'] \cap x').$$

证明。 设 $[y] \in \mathcal{C}[x]$ 为轨道 $\Omega[y']$ 在矩阵构造中所使用的初始元。那么 $[y'] = \pi_{[x'][y']}[y]$ 且 $[x'] = \pi_{[x'][y']}[x]$。若 $[y'] = [y]$，则 $\pi_{[x'][y']}$ 是 **对称群**(V)中的恒等置换。为便于记号表示，我们在下文记 $\pi := \pi_{[x'][y']}$ 根据引理 38，我们有

$$\mathbf{Stab}_E([y'] \cap x') = \mathbf{Stab}_E(\pi[y] \cap \pi x) = \pi(\mathbf{Stab}_E([y] \cap x)).$$

根据 $N[x][y]$ 的定义，并且由于 Ker$(M[y])$ $=$Stab$_E(y)$ $\leq$Stab$_E([y] \cap x)$，我们有 Ker$(N[x][y] \cdot$ $M[y])$ $=$Stab$_E([y] \cap x)$。有 $M[y'] = (g_{[y]}(\pi)\ \pi)M[y]$（归纳假设的 (c) 项）。因此，对于任意向量 $\mathbf{v} \in \mathbb{F}_2^E$，我们有 $M[y'] \cdot \pi(\mathbf{v}) = g_{[y]}(\pi)(M[y] \cdot \mathbf{v})$。这里，$g_{[y]}(\pi)$ 通过将向量 $\mathbf{w} \in \mathbb{F}_2^{I_{[y]}}$ 映射为向量 $\mathbf{w}' \in \mathbb{F}_2^{I_{[y']}}$ 来作用于向量 $\mathbf{w}$，其中 $\mathbf{w}'(g_{[y]}(\pi)(i)) = \mathbf{w}(i)$ 对每个 $i \in I_{[y]}$ 都成立。根据定义，对于 $N[x'][y']$:$N([x'][y'])_{k,-} = g_{[y]}(\pi)(N([x][y])_{k,-})$ 的第 k 行。总之，这意味着对于每个 $\mathbf{v} \in \mathbb{F}_2^E$，都有：

$$N([x'][y'])_{k,-} \cdot M[y'] \cdot \pi(\mathbf{v}) = N([x][y])_{k,-} \cdot M[y] \cdot \mathbf{v}.$$

因此，**核**$(N[x'][y'] \cdot M[y'])$ $=$ π**(核**$(N[x][y] \cdot M[y])$ $=$ π**(稳定子**$_E([y] \cap x))$ $=$**稳定子**$_E([y'] \cap x')$。
◀

接下来这些引理的证明见附录。它们涉及所构造的 N-矩阵的对称性，基本上可直接由第一个 N-矩阵的构造以及其他 N-矩阵与之对称这一事实推出。不过，形式化证明需要进行繁琐的计算。

▶**引理 43。** 设 $[x'] \in \Omega[x]$ 和 $[y'] \in C[x']$。存在一个同态 h' 从 $g_{[y']}$(**稳定子**$_G([y'] \cap x'))$ $\leq$ **对称群**$(I_{[y']})$ 映射到 $N[x'][y']$ 的行指标集上的对称群，使得对于每个 $\sigma \in g_{[y']}$(**稳定子**$_G($ $[y'] \cap x'))$，都有 $(h'(\sigma)\ \sigma)(N[x'][y'])$ $= N[x'][y']$。

证明概要。 令 $[y] \in \mathcal{C}[x]$ 为 $\Omega[y']$ 的初始元。那么对于 $N[x][y]$，该引理由构造直接成立，因为我们明确地将 $N[x][y]$ 的各行在这些对称性下封闭。对于

$N[x'][y']$，该结果由构造的对称性得出。 ◀

引理 42 和 43 断言，所有构造出的矩阵 $N[x'][y']$ 都满足性质 (i) 和 (ii)，而 $N[x][y]$ 按构造本身就具有这两个性质。现在令

$$J_{\Omega_{[x]}} := \bigcup_{\substack{[x']\in\Omega_{[x]}\\ [y']\in\mathcal{C}[x']}} J_{[x'][y']}.$$

我们给出一个群同态 $h_{[x]}$: **稳定子**$_G(\mu)$ $\longrightarrow$ **对称群**$(J_{\Omega_{[x]}})$，使得对于每个$[x'] \in \Omega_{[x]}$ 和每个 $[y'] \in \mathcal{C}[x']$，都有 $h_{[x]}(\pi)(J_{[x'][y']}) = J_{\pi[x']\pi[y']}$。此外，我们希望对于每个 $[x'] \in\Omega_{[x]}$、$[y'] \in \mathcal{C}[x']$ 以及$\pi \in$ **稳定子**$_G(\mu)$，都有 $(N\pi[x']\pi[y']) = (h_{[x]}(\pi)\, g_{[x]}(\pi))N[x'][y']$。对于每个三元组 $(k, [x'], [y']) \in J_{\Omega_{[x]}}$，我们定义：

$$h_{[x]}(\pi)(k, [x'], [y']) := (\ell, \pi[x'], \pi[y']),$$

其中，ℓ 定义如下：令

$$t := |\{i \in \{1, 2, ..., k-1\} \mid (N[x'][y'])_{i,-} = (N[x'][y'])_{k,-}\}|.$$

也就是说，$N[x'][y']$的第 k 行中，有 t 行与它相同且指数较小。于是，ℓ 定义为使得

$$|\{i \in \{1, 2, ..., \ell-1\} \mid (N\pi[x']\pi[y'])_{i,-} = g_{[y']}(\pi)((N[x'][y'])_{k,-})\}| = t,$$

并且满足 $(N\pi[x']\pi[y'])_{\ell,\ -} = g_{[y']}(\pi)((N[x'][y'])_{k,\ -})$。换句话说，$\ell$是 $N\pi[x']\pi[y']$ 的第 $(t+1)$ 行，该行等于 $N[x][y]$的第 k 行，只是其列经过了由 $g_{[y']}(\pi)$ 给出的置换。

我们需要证明 $h_{[x]}(\pi)(k,\ [x'],\ [y'])$ 确实定义良好：

▶ **引理 44**。设 $[x'] \in \Omega_{[x]}$, $[y'] \in \mathcal{C}[x']$。设 $\pi \in$ **稳定子**$_G(\mu)$。那么，对于每个 $(k, [x'], [y']) \in J_{[x'][y']}$，$N[x'][y']$ 中与第 k 行相同的行数，等于 $N\pi[x']\pi[y']$ 中与 $N[x'][y']$的第 k 行在对列应用$g_{[y']}$ 之后相同的行数。形式化地说：

$$\begin{aligned}&|\{(i, [x'], [y']) \in J_{[x'][y']} \mid (N[x'][y'])_{(i,[x'],[y']),-} = (N[x'][y'])_{k,-}\}|\\ =&|\{(i, \pi[x'], \pi[y']) \in J_{\pi[x']\pi[y']} \mid (N\pi[x']\pi[y'])_{(i,\pi[x'],\pi[y']),-} = g_{[y']}((N[x'][y'])_{k,-})\}|\end{aligned}$$

证明概要。这再次由以下事实得出：根据构造，$N[x'][y']$和 $N\pi[x']\pi[y']$ 彼此对称。◀

这个引理表明，我们确实可以像之前那样定义 $h_{[x]}$。现在可以验证，$h_{[x]}$是一个具有所需性质的群同态。我们同样在附录中证明这一点；它由 $h_{[x]}$ 的定义和引理 44 得出。

▶ 引理 45。映射 $h_{[x]}$: $Stab_G(\mu) \longrightarrow Sym(J_{\Omega_{[x]}})$是一个群同态。对于每个 $[x'] \in \Omega_{[x]}$、$[y'] \in \mathcal{C}[x']$ 以及每个 $\pi \in Stab_G(\mu)$，都有 $h_{[x]}(\pi)(J_{[x'][y']}) = J_{\pi[x']\pi[y']}$。此外，对于每个 $[x'] \in\Omega_{[x]}$、$[y'] \in \mathcal{C}[x']$以及$\pi \in Stab_G(\mu)$，都有 $N\pi[x']\pi[y'] = (h_{[x]}(\pi)\, g_{[y']}(\pi))N[x'][y']$。

至此，已完成对所有 $[x'] \in \Omega_{[x]}$ 和 $[y'] \in \mathcal{C}[x']$ 的矩阵 $N[x'][y']$ 及相关同态 $h_{[x]}$: **稳定子**$_G$ $(\mu) \longrightarrow J_{\Omega_{[x]}}$ 的构造和正确性证明。因此，归纳步骤中的 (b) 和 (d) 两项已得到证明。要完成归纳步骤，我们还需要定义所有 $[x'] \in \Omega_{[x]}$ 对应的矩阵 $M[x']$。

M 矩阵的定义

设 $[x'] \in \Omega_{[x]}$。非正式地说，$M[x']$ 是通过收集所有 $[y'] \in \mathcal{C}[x']$ 对应的矩阵 $(N[x'][y'] \cdot M[y'])$ 的所有行，并将它们合并为 $M[x']$ 的行而得到的。形式化地，令

$$I_{[x']} := \biguplus_{[y'] \in \mathcal{C}[x']} J_{[x'][y']}.$$

注意，根据构造，集合 $J_{[x'][y']}, J_{[x'][y'']}$ 两两不相交，若 $[y'] \neq [y'']$。接下来，$M[x'] \in \mathbb{F}_2^{I_{[x']} \times E}$ 的行定义如下：对于 $[y'] \in \mathcal{C}[x']$ 和 $(i, [x'], [y']) \in J_{[x'][y']}$，令

$$M[x']_{(i,[x'],[y']),-} := (N[x'][y'] \cdot M[y'])_{(i,[x'],[y']),-}.$$

该矩阵具有所需的核：

▶ **引理 46.** 对于每个 $[x'] \in \Omega_{[x]}$，如上定义的矩阵 $M[x']$ 满足：

$$\boldsymbol{Ker}(M[x']) = \mathbf{Stab}_E(x').$$

证明。 根据 $M[x']$ 的定义，向量 $\mathbf{v} \in \mathbb{F}_2^E$ 属于 **核**$(M[x'])$ 当且仅当 $\mathbf{v} \in$ **核**$(N[x'][y'] \cdot M[y'])$ 对所有 $[y'] \in \mathcal{C}[x']$ 都成立。根据引理 42，当且仅当 $\mathbf{v} \in$ **稳定子**$_E([y'] \cap x')$ 对所有 $[y'] \in \mathcal{C}[x']$ 都成立。也就是说，

$$\mathbf{v} \in \bigcap_{[y'] \in \mathcal{C}[x']} \mathbf{Stab}_E([y'] \cap x').$$

这等价于 $\mathbf{v} \in$ **稳定子**$_E(x')$，因为 $x' = \bigcup_{[y'] \in \mathcal{C}[x']}([y'] \cap x')$（见命题 25）。◀

最后，我们必须给出同态 $g_{[x]}$:**稳定子**$_G(\mu) \longrightarrow$ **对称群**$(I_{\Omega_{[x]}})$，其中 $I_{\Omega_{[x]}} = \biguplus_{[x'] \in \Omega_{[x]}} I_{[x']}$。注意，根据指标集 $I_{[x']}$ 的定义，$I_{\Omega_{[x]}} = J_{\Omega_{[x]}}$。因此，我们只需令 $g_{[x]} := h_{[x]}$。这个同态确实满足所需的性质：

▶ **引理 47.** 对于每个 $[x'] \in \Omega_{[x]}$ 以及每个 $\pi \in$ **稳定子**$_G(\mu)$，都有 $g_{[x]}(\pi)(I_{[x']}) = I_{\pi[x']}$。此外，$M\pi[x'] = (g_{[x]}(\pi)\ \pi)M[x']$。

证明。 令 $\pi \in$ **稳定子**$_G(\mu)$ 以及 $[x'] \in \Omega_{[x]}$。根据引理 35，$\pi[x']$ 再次是 tc 中的一个 $\sim$-类(μ)。由于 π 可扩展为 μ的一个自同构，因此也有

$$\pi(\mathcal{C}[x']) = \{\pi[y'] \mid [y'] \in \mathcal{C}[x']\} = \mathcal{C}(\pi[x']).$$

因此，根据引理 45，$h_{[x]}(\pi)$ 将集合 $I_{[x']} = \biguplus_{[y'] \in \mathcal{C}[x']} J_{[x'][y']}$ 映射到集合 $I_{\pi[x']} = \biguplus_{\pi[y'] \in \mathcal{C}_{\pi[x']}} J_{\pi[x']\pi[y']}$。还需证明 $(M\pi[x'])_{g_{[x]}(\pi)(i)\ \pi(e)} = M[x']_{i,e}$ 对于每个 $i = (j, [x'], [y']) \in I_{[x']}$，以及 $e \in E$。根据 M-矩阵的定义，我们有：

$$\begin{aligned}(M\pi[x'])_{g_{[x]}(\pi)(i),\pi(e)} = (M\pi[x'])_{(j',\pi[x'],\pi[y']),\pi(e)} &= (N\pi[x']\pi[y'] \cdot M\pi[y'])_{(j',\pi[x'],\pi[y']),\pi(e)} \\ &= (N[x'][y'] \cdot M[y'])_{(j,[x'],[y']),e} \\ &= M[x']_{i,e}.\end{aligned}$$

这里，j' 满足 $(j', \pi[x'], \pi[y']) = g_{[x]}(\pi)(j, [x'], [y']) = h_{[x]}(\pi)(j, [x'], [y'])$。最终等式成立的原因如下：$(N\pi[x']\pi[y'] \cdot M\pi[y'])_{(j',\pi[x'],\pi[y'])\ \pi(e)}$ 是 $N\pi[x']\pi[y']$ 的行 j' 与 $M\pi[y']$ 的列 $\pi(e)$ 的乘积。我们目前正在证明的引理

由归纳假设，$M[y']$已经成立，因此$(M\pi[y'])_{-\pi(e)} = g_{[y']}(\pi)(M[y']_{-e})$。此外，根据引理45，我们有$(N\pi[x']\pi[y'])_{j',-} = g_{[y']}(\pi)((N[x'][y'])_{j,-})$。然后，命题34告诉我们$(N\pi[x']\pi[y'])_{j',-} \cdot (M\pi[y'])_{-,\pi(e)} = (N[x'][y'])_{j,-} \cdot (M[y'])_{-e}$，因为这些向量乘积实际上是相同的乘积之和，只是其中的各项被$g_{[y']}(\pi)$重新排序了。◀

6.2 电路的构造

我们根据上一节定义的矩阵构造电路$C(\mu) = (V_C, E_C)$。门的集合为

$$V_C := \biguplus_{\substack{x \in \mathrm{tc}(\mu) \\ (i,[x],[y]) \in I_{[x]}}} \mathbf{g}_{i,[x],[y]}.$$

因此，任意一个指数为$(i, [x], [y])$的$M[x]$-矩阵中的每一行都对应一个门$\mathbf{g}_{i,[x],[y]}$。该构造将确保

$$\chi(\mathcal{X}(\mathbf{g}_{i,[x],[y]})) = M[x]^T_{(i,[x],[y]),-}.$$

因此，该门将对标签为边、且在行$M[x]_{(i,[x],[y]),-}$中对应元素为1的输入门精确地计算异或。

对于每个原子$x \in \mathrm{tc}(\mu)$，都有$I_{[x]} = \{[x]\}$。我们将相应的门$\mathbf{g}_{[x]}$定义为$C(\mu)$的输入门，其中$\ell(\mathbf{g}_{[x]}) = e$，且$e \in E$是满足以下条件的边：$[x] \subseteq \{e_0, e_1\}$。

如果$x \in \mathrm{tc}(\mu)$不是原子，那么对于每个$(i, [x], [y]) \in I_{[x]}$，$\mathbf{g}_{i,[x],[y]}$是一个内部门，其输入线恰好来自满足以下条件的那些门$\mathbf{g}_{j,[y],[z]}$：矩阵$N[x][y]$在行$(i, [x], [y])$和列$(j, [y], [z])$处有一个1元素。注意，$(j, [y], [z]) \in I_{[y]}$，因此$[z] \in \mathsf{C}[y]$。形式化地说，$\mathbf{g}_{i,[x],[y]}$的子节点集合为：

$$\mathbf{g}_{i,[x],[y]} E_C := \{\mathbf{g}_{j,[y],[z]} \mid (j,[y],[z]) \in I_{[y]}, (N[x][y])_{(i,[x],[y]),(j,[y],[z])} = 1\}.$$

还需指定$C(\mu)$的根。考虑矩阵$M[\mu]$。设$(i, [\mu], [y])$是$M[\mu]$中1的个数最多的一行。我们将根r定义为门$\mathbf{g}_{i,[\mu],[y]}$。

下图展示了对象x的矩阵和异或门，该对象由两个连通分量$[y] \cap x$和$[y'] \cap x$组成。在这个例子中，矩阵$N[x][y]$和$N[x][y']$各只有一行，并且我们假设$\mathcal{C}[y] = \{[z]\}$和$\mathcal{C}[y'] = \{[z']\}$，且$M[y] = N[y][z] \cdot M[z]$有三行，$M[y'] = N[y'][z'] \cdot M[z']$有两行。

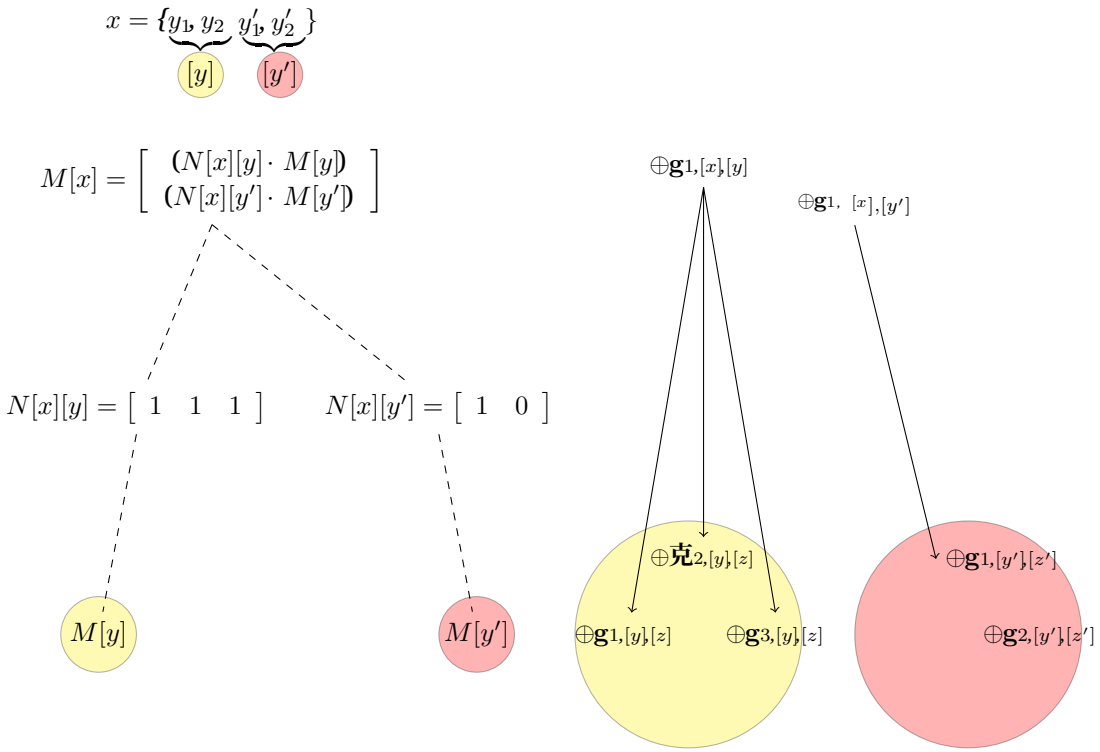

图 2 示例展示了异或门如何按照 N-矩阵连接。

现在我们证明 $C(\mu)$ 具有所需的性质。

引理 48. 每个 $\pi \in$**稳定子**$_G(\mu)$ 都可以扩展为电路 $C(\mu)$的一个自同构，也就是说：**稳定子**$_G(\mu) \leq$**稳定子**$_G(C(\mu))$。

证明。 令 $\pi \in$ **稳定子**$_G(\mu)$。我们断言，以下映射 $\sigma: V_C \longrightarrow V_C$ 是的一个自同构 $C(\mu)$，且 π 可以扩展到。令

$$\sigma(\mathbf{g}_{i,[x],[y]}) := \mathbf{g}_{g_{[x]}(\pi)(i,[x],[y])},$$

其中$g_{[x]}$：稳定子$_G(\mu) \longrightarrow$ 对称群$(I_{\Omega_{[x]}})$是 $\Omega_{[x]}$ 在上一小节构造矩阵时所对应的群同态。我们需要证明关于 σ的三点。首先，$\sigma \in$对称群(V_C)。其次，σ 将连线映射为连线，并将 $C(\mu)$中的非连线映射为非连线。最后，对于每个输入门 $\mathbf{g}_{[x]}$，都有：$\ell(\sigma(\mathbf{g}_{[x]})) = \pi(\ell(\mathbf{g}_{[x]}))$。最后这条结论实际上可直接由 $g_{[x]}$ 对原子 $x \in \mathsf{tc}(\mu)$ 的定义推出：若 $[x] \subseteq \{e_0, e_1\}$，则$\pi(\ell(\mathbf{g}_{[x]})) = \pi(e)$，且 $g_{[x]}(\pi)([x]) = \pi[x] \subseteq \{\pi(e_0)\ \pi(e_1)\}$，因此 $\ell(\sigma(\mathbf{g}_{[x]})) = \pi(e)$。

事实 $\sigma \in \mathbf{Sym}(V_C)$ 成立，是因为对于每个轨道 $\Omega_{[x]}$，都有 $g_{[x]}(\pi) \in \mathbf{Sym}(I_{\Omega_{[x]}})$，并且门的集合 V_C 可以划分为这些轨道，使得每个部分都具有形式 $\{\mathbf{g}_{i,[x'],[y]} \mid (i,[x'],[y]) \in I_{\Omega_{[x]}}\}$，其中 $\Omega_{[x]}$ 是某个轨道。

还需证明 σ 保持电路的连线结构。对于任意两个门$\mathbf{g}_{i,[x],[y]}$,$\mathbf{g}_{j,[x'],[y']}$，有

$$(\mathbf{g}_{i,[x],[y]}, \mathbf{g}_{j,[x'],[y']}) \in E_C \text{ if and only if } [y] = [x'] \text{ and } (N[x][y])_{(i,[x],[y]),(j,[y],[y'])} = 1.$$

后一个等式成立，当且仅当

$$(N\pi[x]\pi[y])_{h_{[x]}(\pi)(i,[x],[y]),g_{[y]}(\pi)(j,[y],[y'])} = 1.$$

根据引理 45，这一点成立。如果 $[x'] = [y]$，那么我们有 $\sigma(\mathbf{g}_{j,[x'],[y']}) = \mathbf{g}^{g_{[y]}(\pi)(j,[y],[y'])}$。此外，它满足 $\sigma(\mathbf{g}_{i,[x],[y]}) = \mathbf{g}^{g_{[x]}(\pi)(i,[x],[y])}$。根据上一节中的定义，$g_{[x]} = h_{[x]}$，并且 $g_{[x]}(\pi)(i,[x],[y])$ 的形式为 $(\ell, \pi[x], \pi[y])$，而 $g_{[y]}(\pi)(j,[y],[y'])$ 的形式为 $(\ell', \pi[y], \pi[y'])$，因此它们确实是矩阵$N\pi[x]\pi[y]$的行索引和列索引。综上，以上等式等价于：$(\sigma\mathbf{g}_{i,[x],[y]}, \sigma\mathbf{g}_{j,[x'],[y']}) \in E_C$. ◀

与电路 $C(\mu)$ 的情况相同，这个引理意味着，$C(\mu)$ 的轨道大小不能大于 μ 的轨道大小（这里，$\mathbf{Orb}_G(\mu)$ 仍然指 $\mathbf{Aut}(G)$-轨道，而不是 **稳定子**$_G(\mu)$-轨道；后者毫无意义）。

▶**推论 49**。

$$|\mathbf{Orb}_G(\widehat{C}(\mu))| \leq |\mathbf{Orb}_G(\mu)|.$$

证明。 与推论 24 的证明类似。 ◀

▶ **引理 50**。 对于每个内部门 $\mathbf{g} := \mathbf{g}_{i,[x],[y]} \in V_C$ 均成立：

$$\mathcal{X}(\mathbf{g}) = \chi^{-1}(M[x]^T_{(i,[x],[y]),-}).$$

证明。 由归纳法可得。对于每个输入门$\mathbf{g}_{[x]}$，其中 $[x] \subseteq \{e_0, e_1\}$，我们有$\mathcal{X}(\mathbf{g}_{[x]}) = \{e\}$.
现在令$\mathbf{g} = \mathbf{g}_{i,[x],[y]}$ 为一个内部门。根据 $C(\mu)$ 的定义，有

$$\mathbf{g}E_C = \{\mathbf{g}_{j,[y],[z]} \mid (j,[y],[z]) \in I_{[y]}, (N[x][y])_{(i,[x],[y]),(j,[y],[z])} = 1\}.$$

因此，

$$\begin{aligned}
\mathcal{X}(\mathbf{g}) &= \bigtriangleup_{\substack{(j,[y],[z]) \in I_{[y]}, \\ (N[x][y])_{(i,[x],[y]),(j,[y],[z])}=1}} \mathcal{X}(\mathbf{g}_{j,[y],[z]}) \\
&= \chi^{-1}\Big(\sum_{\substack{(j,[y],[z]) \in I_{[y]}, \\ (N[x][y])_{(i,[x],[y]),(j,[y],[z])}=1}} \chi(\mathcal{X}(\mathbf{g}_{j,[y],[z]})) \mod 2 \Big) \\
&= \chi^{-1}(((N[x][y])_{(i,[x],[y]),-} \cdot M[y])^T).
\end{aligned}$$

最后一步用到了归纳假设，以及 $I_{[y]}$ 是 $M[y]$的行索引集这一事实。根据上一小节中矩阵 $M[x]$ 的定义，我们有 $(N[x][y])_{(i,[x],[y]),-}.M[y] = M[x]_{(i,[x],[y]),-}$。由此证明完毕。 ◀

▶ **引理 51**。 $C(\mu)$ 的扇入维数 至多为$\log(\mathbf{maxOrb}_E(\mu))$。

证明。 考虑任意一个门$\mathbf{g} := \mathbf{g}_{i,[x],[y]} \in V_C$。根据 $C(\mu)$ 的定义，$\mathbf{g}$ 的子节点为

$$\mathbf{g}E_C = \{\mathbf{g}_{j,[y],[z]} \mid (j,[y],[z]) \in I_{[y]}, (N[x][y])_{(i,[x],[y]),(j,[y],[z])} = 1\}.$$

由引理 50 可知，对于这些子节点中的每一个：

$$\mathcal{X}(\mathbf{g}_{j,[y],[z]}) = \chi^{-1}(M[y]_{(j,[y],[z]),-}).$$

因此，门矩阵 $M\mathbf{g} \in \mathbb{F}_2^{\mathbf{g}E_C \times E}$是 $M[y]$的子矩阵：它恰好由 $M[y]$ 中满足 $(N[x][y])_{(i,[x],[y]),(j,[y],[z])} = 1$ 的那些行 $(j,[y],[z])$ 组成。因此，$\mathbf{rk}(M\mathbf{g}) \leq \mathbf{rk}(M[y])$。

现在，我们可以仿照引理 27 的证明来界定 $\mathbf{rk}(M[y])$。利用轨道-稳定子定理，我们再次得到：

$$\log(\mathbf{maxOrb}_E(\mu)) \geq |E| - \dim \mathbf{Stab}_E(y).$$

根据引理 46，我们有 $\mathbf{核}(M[y]) = \mathbf{稳定子}_E(y)$。因此，利用秩定理可得：

$$\mathbf{rk}(M[y]) = |E| - \dim\ \mathbf{Stab}_E(y) \leq \log(\mathbf{maxOrb}_E(\mu)).$$

总之，我们有 $\mathbf{rk}(M\mathbf{g}) \leq \log(\mathbf{maxOrb}_E(\mu))$。由于 $\mathbf{g} \in V_C$ 是任意的，因此这是对 $C(\mu)$的扇入维数的一个上界。◀

▶**引理 52**。对于 $C(\mu)$的根 r，有

$$|\mathcal{X}(r)| \geq \frac{|\sup_{\mathrm{CFI}}(\mu)|}{\log(\mathbf{maxOrb}_E(\mu))}.$$

证明。根据 $C(\mu)$的定义，对于某个满足$M[\mu]_{(i,[\mu],[y]),-}$ 为含有最多 1 的行的$(i,[\mu],[y]) \in I_{[\mu]}$，我们有 $r = \mathbf{g}_{i,[\mu],[y]}$。我们有

$$\mathcal{X}(r) = \chi^{-1}(M[\mu]^T_{(i,[\mu],[y]),-})$$

根据引理 50。因此，我们需要证明 $M[\mu]$ 有一行至少包含$|\sup_{\mathrm{CFI}}(\mu)|\ \log(\mathbf{maxOrb}_E(\mu))$ 个 1。

断言： 对于每个 $e \in \sup_{\mathrm{CFI}}(\mu)$，$M[\mu]$ 中都存在一行在列e上非零。

断言的证明：由于 $\sup_{\mathrm{CFI}}(\mu)$ 是 μ 的最小 CFI 支撑，因此有 $\chi(e) \notin \mathbf{稳定子}_E(\mu)$。否则就存在一个不包含 e的更小支撑。反设 $M[\mu]$ 的所有行在列 e 上都为零。那么 $\chi(e) \in \mathbf{核}(M[\mu])$。但这与 $\mathbf{核}(M[\mu]) = \mathbf{稳定子}_E(\mu)$（引理 46）矛盾。由此得证。

现在取 $M[\mu]$ 中行的一个子集$\mathcal{B}$，使其构成 $M[\mu]$ 的行空间的一个基。根据引理 51，有 $|\mathcal{B}| \leq \log(\mathbf{maxOrb}_E(\mu))$。对于每个 $e \in E$，只要 $M[\mu]$ 中有一行在列 e 上非零，$\mathcal{B}$ 中也必定有一行在列 e 上非零（否则$\mathcal{B}$就不能生成整个行空间）。因此，根据该断言以及$\mathcal{B}$的大小上界，$\mathcal{B}$ 中存在一行，其 1 项至少有$\lfloor \frac{|\sup_{\mathrm{CFI}}(\mu)|}{\log(\mathbf{maxOrb}_E(\mu))} \rfloor$ 个。◀

到目前为止，我们已经证明了定理 32 中的**性质 1**、**性质 2** 和**性质 3**。推论 49 证明了**性质 1**，引理 52 证明了**性质 2**，而引理 51 证明了**性质 3**。接下来需要在假设每个空间**稳定子**$_E([y] \cap x)$ 都有一个对称基的前提下，估算电路的大小。

6.3 电路大小的界

▶**引理 53.** 令 $\mathit{Atoms}(\mu) \subseteq \mathrm{tc}(\mu)$ 表示$\mathrm{tc}(\mu)$中的原子集合，而 $\mathit{Sets}(\mu) := \mathrm{tc}(\mu) \setminus \mathit{Atoms}(\mu)$。$C(\mu)$ 的大小为

$$|V_C| = |\{e \in E \mid e_0 \text{ or } e_1 \in \mathit{Atoms}(\mu)\}| + \sum_{\substack{([x],[y]),x \in \mathit{Sets}(\mu),\\ [y] \in \mathcal{C}[x]}} |J_{[x][y]}|.$$

换句话说：$C(\mu)$ 的大小由所有 $N[x][y]$ 矩阵的总行数决定。

证明。 根据 $C(\mu)$ 的定义，$|V_C| = \sum_{[x],\ x\in \mathrm{tc}(\mu)} |I_{[x]}|$。对于每个 $x \in \mathrm{tc}(\mu) \cap$集合$(\mu)$，我们都有$|I_{[x]}| = \sum_{[y]\in\mathcal{C}[x]} |J_{[x][y]}|$。每个集合 $J_{[x][y]}$ 都唯一地与对 $([x],\ [y])$ 相关联，因此

$$\sum_{[x],x\in \mathrm{tc}(\mu)} |I_{[x]}| = \sum_{\substack{([x],[y]),x\in \mathrm{Sets}(\mu),\\ [y]\in\mathcal{C}[x]}} |J_{[x][y]}|.$$

对于每个原子 $x \in \mathrm{tc}(\mu)$，$|I_{[x]}| = 1$。 ◀

因此，为了界定 $|V_C|$，我们必须界定每个 $N[x][y]$-矩阵的行数。为此，我们重新审视引理 39 和 41 的证明。我们将看到，如果存在一个 **稳定子**$_E([y] \cap x)$ 的对称基，那么这些引理中构造的矩阵可以选为多项式大小。引理 39 中构造 $N[x][y]$ 的第一步是求解一族线性方程组。现在我们证明，这类方程组的对称性对应于其解的对称性。

▶ **引理 54**。 设 I, J 为抽象指标集，且 $A, A' \in \mathbb{F}_2^{I\times J}$,$\mathbf{b},\mathbf{b}' \in \mathbb{F}_2^I$ 满足线性方程组 $A\cdot\mathbf{x} = \mathbf{b}$ 和 $A'\cdot\mathbf{x} = \mathbf{b}'$ 分别有唯一解 $\mathbf{s},\mathbf{s}'$，。设 $\mathbf{G} \le$ **对称群**(J) 是一个作用于 A 的列上的置换群。设 $\pi \in \mathbf{G}$ 是一个将扩展系数矩阵 $(A|\mathbf{b})$ 的行集映射到

$$R = \{(A_{i-}, \mathbf{b}_i) \mid i \in I\}$$

到 R' 的行集（$A'|\mathbf{b}'$）。这里，π 在 R 上的作用为 π（A_{i-},$\mathbf{b}_i$）：=（π（A_{i-}）,$\mathbf{b}_i$）。于是 π（$\mathbf{s}$）=$\mathbf{s}'$。

证明。我们只需证明 $\pi(\mathbf{s})$ 是 $A'\cdot\mathbf{x} = \mathbf{b}'$ 的一个解。于是，根据解的唯一性，我们有 $\pi(\mathbf{s}) = \mathbf{s}'$。若 $\pi \in \mathbf{G}$ 将 R 映射到 R'，则存在一个置换 $\sigma \in \mathrm{Sym}(I)$，它由 π 的作用诱导，即对所有 $i \in I$，都有 $\pi(A_{i-}, \mathbf{b}_i) = (A'_{\sigma i,-}, \mathbf{b}'_{\sigma i})$。对于每个 $i \in I$，都有 $A_{i-}\cdot\mathbf{s} = \mathbf{b}_i$，因为 $\mathbf{s}$ 是该方程组的一个解。由于（根据命题 34）$A_{i-}\cdot\mathbf{s} = \pi(A_{i-})\cdot\pi(\mathbf{s}) = A'_{\sigma i-}\cdot\pi(\mathbf{s})$，且 $\mathbf{b}_i = \mathbf{b}'_{\sigma i}$，$\pi(\mathbf{s})$ 是方程 $A'_{\sigma i-}\cdot\mathbf{x} = \mathbf{b}'_{\sigma i}$ 的一个解。由于 $(A'|\mathbf{b}')$ 的每一行在 π 下都有这样的原像，因此 $\pi(\mathbf{s})$ 是 $A'\cdot\mathbf{x} = \mathbf{b}'$ 中每个方程的一个解。根据假设，该方程组有唯一解。因此，$\pi(\mathbf{s}) = \mathbf{s}'$。◀

下面的引理在讨论向量空间的对称基时会变得很有用。它表明，向量集（例如对称基）的置换不变性在线性映射和适当的群同态作用下得以保持。

▶ 引理 *55.* 设 $M \in \mathbb{F}_2^{I\times J}$，且 $G \le \mathrm{Sym}(J)$ 是作用于 M 的列上的置换群。设 $B \subseteq \mathbb{F}_2^J$ 是一个向量集，且 $S := \mathrm{Stab}_{\mathbf{G}}(B)$。设 $g : G \longrightarrow \mathrm{Sym}(I)$ 是一个群同态，使得对所有 $\pi \in G$，都有 $(g(\pi)\ \pi)M = M$。那么 $g(S)$ 稳定集合 $M\cdot B = \{M\cdot\mathbf{v} \mid \mathbf{v} \in B\}$。

证明。 设 $\pi \in S$ 且 $\mathbf{v} \in B$。设 $\mathbf{w} = M\cdot\mathbf{v}$。我们证明 $(g(\pi))^{-1}(\mathbf{w}) = M\cdot\pi(\mathbf{v})$。对每个 $i \in I$，有

$$M_{i,-}\cdot\pi(\mathbf{v}) = \pi(M_{(g(\pi))(i),-})\cdot\pi(\mathbf{v}) = M_{(g(\pi))(i),-}\cdot\mathbf{v}.$$

第一个等式成立，是因为根据假设，$(g(\pi)\ \pi)M = M$；第二个等式则由命题 34 得出。因此，$g(\pi)(M\cdot\pi(\mathbf{v})) = M\cdot\mathbf{v} = \mathbf{w}$。所以，$(g(\pi))^{-1}(\mathbf{w}) = M\cdot\pi(\mathbf{v})$。我们有 $\pi(\mathbf{v}) \in B$，因为 $\pi \in S$。因此，$(g(\pi))^{-1}(\mathbf{w}) \in M\cdot B$。由于 $\mathbf{w} = M\cdot\mathbf{v}$ 是任意的，我们知道 $(g(\pi))^{-1} = g(\pi^{-1}) \in g(S)$ 稳定了集合 $M\cdot B$。由于 $\pi \in S$ 也是任意的，$g(S)$ 稳定了 $M\cdot B$。 ◀

最后，我们给出“对称基”的确切定义。此定义专为对象 tc(μ) 所对应的空间 **稳定子**$_E$($[y] \cap x$) 量身定制。我们所说的“对称基”实际上指两个基：我们要求，**稳定子**$_E([y] \cap x)$ 的基以及将其扩展为环境空间的一个基，都具有对称性。这里的对称性是指轨道的大小必须为多项式大小。

▶**定义 56.** 令 $x \in \mathrm{tc}(\mu)$ 和 $[y] \in C[x]$。我们称向量空间 $\Gamma := \textbf{稳定子}_E([y] \cap x) \leq \mathbb{F}_2^E$ 具有对称基，如果存在两个基

$$B_\Gamma \subseteq B$$

使得 B_Γ 是 $\Gamma = \textbf{稳定子}_E([y] \cap x)$ 的一个基，而 B 是 $\mathbb{F}_2^E$ 的一个基，并且满足：群

$$\mathbf{Stab}_{\mathbf{Stab}_G([y]\cap x)}(\mathcal{B}_\Gamma) \cap \mathbf{Stab}_{\mathbf{Stab}_G([y]\cap x)}(\mathcal{B}) = \{\pi \in \mathbf{Stab}_G([y] \cap x) \mid \pi(\mathcal{B}_\Gamma) = \mathcal{B}_\Gamma \text{ and } \pi(\mathcal{B}) = \mathcal{B}\} \leq \mathbf{Stab}_G([y] \cap x)$$

在 **稳定子**$_G([y] \cap x)$中的指数为 $\leq$ 多项式($|\mathfrak{G}^S|$) 。

在上述定义中，当然是指对于我们在定理 32 中考虑的整个 CFI 实例族，多项式 poly(·) 是固定的。现在继续讨论主要引理；该引理在假设存在对称基的情况下，给出 $N[x][y]$ 大小的上界。

▶ **引理 57**。 设 $x \in \mathrm{tc}(\mu)$ 且 $[y] \in C[x]$。如果 **稳定子**$_E([y] \cap x)$ 有一个对称基，那么 $N[x][y]$ 的行数是 $|\mathfrak{G}^S|$的多项式。

证明。 我们证明存在一个布尔矩阵 N，其行数为多项式，并且满足引理 41 中的条件（i）和（ii）。这就证明了该引理，因为 $N[x][y]$ 被定义为满足这些条件的最小矩阵。

考察引理 39 的证明。将其应用于 $\Gamma = M[y] \cdot \mathrm{Stab}_E([y] \cap x)$ 和 $\Delta = M[y] \cdot \mathbb{F}_2^E = \mathrm{Im}(M[y])$ 时，证明表明存在一个矩阵 $N \in \mathbb{F}_2^{[k] \times I_{[y]}}$，使得 $k = \dim(\mathrm{Im}\ M[y]) - \dim(M[y] \cdot \mathrm{Stab}_E([y] \cap x))$，且 $\mathrm{Ker}(N) \cap \mathrm{Im}(M[y]) = M[y] \cdot \mathrm{Stab}_E([y] \cap x)$。在证明中，定义了 k 个线性方程组 $A_i \cdot \mathbf{x} = \mathbf{b}_i$，每个方程组都有唯一解。然后，对于 $i \in [k]$，将 N 的第 i 行定义为方程组 $A_i \cdot \mathbf{x} = \mathbf{b}_i$ 的唯一解。对于每个 $i \in [k]$，矩阵 A_i 都相同。它取决于为 $M[y] \cdot \mathrm{Stab}_E([y] \cap x)$ 选择的基，以及将该基扩充为 $\mathrm{Im}(M[y])$ 的基。更准确地说，设 $\{\mathbf{w}_1, ..., \mathbf{w}_k\}$ 是将 $M[y] \cdot \mathrm{Stab}_E([y] \cap x)$ 的基扩充为 $\mathrm{Im}(M[y])$ 的基所需的向量。 A_i的各行是 $\mathrm{Im}(M[y])$ 的基向量，而向量 $\mathbf{b}_i$ 恰好在对应于 $\mathbf{w}_i$ 的行中有一个 1 元素。这样，对于每个 $i \in [k]$，都定义了 $\mathbf{b}_i$ 。

可以验证，如果用空间 $M[y]$ 生成集for the space $M[y] \cdot$ **稳定子**$_E([y] \cap x)$ 的生成集，来代替 A_i – 的各行所构成的基，那么引理 39 的这个证明仍然成立——只要将 $\{\mathbf{w}_1, ..., \mathbf{w}_k\}$ 扩充为整个空间 $\mathbf{Im}(M[y])$ 的基时，所添加的向量集是线性无关的。这样做不会改变任何结果；特别是，每个方程组 $A_i \cdot \mathbf{x} = \mathbf{b}_i$ 仍然有唯一解，因为我们只是添加了一些冗余方程。

现在我们选择适当的基。根据假设，$\mathrm{Stab}_E([y] \cap x)$ 有一个对称基，因此分别存在 $\mathrm{Stab}_E([y] \cap x)$ 和 $\mathbb{F}_2^E$ 的基 $\mathrm{B}_\Gamma \subseteq \mathrm{B}$，使得 $\mathrm{Stabs}_{\mathrm{Stab}_G([y]\cap x)}(\mathrm{B}_\Gamma) \cap \mathrm{Stabs}_{\mathrm{Stab}_G([y]\cap x)}(\mathrm{B})$ 在 $\mathrm{Stab}_G([y] \cap x)$ 中具有小指数。令 $\mathrm{B}'_\Gamma := M[y] \cdot \mathrm{B}_\Gamma \setminus \{0\}$，且 $\mathrm{B}' := M[y] \cdot \mathrm{B} \setminus \{0\}$。那么，$\mathrm{B}'_\Gamma$是 $M[y] \cdot \mathrm{Stab}_E([y] \cap x)$ 的生成集，而 $\mathrm{B}' \setminus \mathrm{B}'_\Gamma$ 将此生成集扩充为 $\mathrm{Im}(M[y])$ 的一个基。重要的是，$\mathrm{B}' \setminus \mathrm{B}'_\Gamma$ 是一个

线性无关向量集（而 B'_Γ 可能线性相关）。这是因为 $\mathrm{Ker}(M[y]) = \mathrm{Stab}_E(y)$（引理 46），且 $\mathrm{Stab}_E(y) \le \mathrm{Stab}_E([y] \cap x)$。因此，若存在子集 $K \subseteq B' \setminus B'_\Gamma$ 使得 $\sum K = 0$，那么这些向量的 $M[y]$-原像之和将属于 $\mathrm{Ker}(M[y]) = \mathrm{Stab}_E(y)$。这不可能成立，因为 B_Γ 是 $\mathrm{Stab}_E([y] \cap x) \ge \mathrm{Stab}_E(y)$ 的基，所以 $B \setminus B_\Gamma$ 中的向量的任何线性组合都不可能属于 $\mathrm{Stab}_E(y)$。

现在将引理 55 应用于矩阵 $M = M[y] \in \mathbb{F}_2^{I_{[y]} \times E}$、$G = \text{稳定子}_G([y] \cap x)$ $B = B_\Gamma$以及如下定义的同态 g： g：稳定子$_G([y] \cap x) \longrightarrow$ 对称群$(I_{[y]})$ 将任意$\pi \in$ 稳定子$_G([y] \cap x)$映射到置换 $g_{[y]}(\pi) \in$ 对称群$(I_{\Omega_{[y]}})$ 的 $I_{[y]}$-限制。该定义良好，且 $g(\pi) \in$ 对称群$(I_{[y]})$，因为根据推论 36，稳定子$_G([y] \cap x) \le$ 稳定子$_G([y])$，并且根据引理 47，$g_{[y]}$(稳定子$_G([y])$) 将 $I_{[y]}$ 映射到自身。

现在根据引理 55 可知，g(稳定子$_{\mathbf{Stab}_G([y]\cap x)}(B_\Gamma)) \le$ 对称群$(I_{[y]})$ 稳定集合$M[y] \cdot B_\Gamma \subseteq \mathbb{F}_2^{I_{[y]}}$。有 $B'_\Gamma = M[y] \cdot B_\Gamma \setminus \{0\}$，且零向量相对于对各项进行的置换构成单元素轨道，因此 B'_Γ 也由 g(稳定子$_{\mathbf{Stab}_G([y]\cap x)}(B_\Gamma)$)稳定。类似地，将引理 55 应用于 $B =$B，可得 g(稳定子$_{\mathbf{Stab}_G([y]\cap x)}$(B)) 稳定 B'。每个稳定集合 B'_Γ 和 B' 的置换 $\pi \in$对称群$(I_{[y]})$都会诱导一个置换$\sigma \in$对称群(B′)，其在 B'_Γ 上的限制是对称群(B'_Γ)中的一个置换。由于每个系数矩阵 A_i 的行都是 B', 中的向量，每个按集合方式固定 B' 的 $\pi \in$对称群$(I_{[y]})$都会对 A_i的行重新排序。右侧 b_i 只有一个 1 元素，位于对应于 $w_i \in B' \setminus B'_\Gamma$的行中。因此，如果 π 也稳定 B'_Γ，那么 π 在 $(A_i|b_i)$ 上的作用会将行向量$\pi^{-1}(w_i) \in B' \setminus B'_\Gamma$ 移至 b_i 含有其 1 元素的那一行。对行重新排序后，这会得到其他线性方程组 $\{(A_i|b_i) \mid i \in [k]\}$ 中的一个，因为在某个线性方程组中，系数向量 $\pi^{-1}(w_i)$ 对应的方程右侧为 1。因此，任何同时稳定 B'_Γ 和 B' 的 π，都会按照引理 54 的含义，在集合 $\{(A_i|b_i) \mid i \in [k]\}$ 上诱导一个置换（其中方程组行集上的列置换作用如该引理所定义）。令

$$\mathcal{S} := g(\mathbf{Stab}_{\mathbf{Stab}_G([y]\cap x)}(\mathcal{B}_\Gamma)) \cap g(\mathbf{Stab}_{\mathbf{Stab}_G([y]\cap x)}(\mathcal{B})).$$

如上所述，这个群同时固定$\mathcal{B}'$ 和$\mathcal{B}'_\Gamma$。因此，它在方程组上诱导出一个置换，所以引理 54 告诉我们，$\mathcal{S}$ 也在集合上诱导出相应的置换

$$\{\mathbf{s}_i \in \mathbb{F}_2^{I_{[y]}} \mid \mathbf{s}_i \text{ is the unique solution to } A_i \cdot \mathbf{x} = \mathbf{b}_i\}$$

（其中$\mathcal{S}$ 通过置换条目对这些向量作用）。这些解向量恰好构成正在引理 39 的证明中构造的矩阵 $N \in \mathbb{F}_2^{[k] \times I_{[y]}}$ 的各行。因此，作用在 N 的列上的群$\mathcal{S}$ 会在 N 的各行上诱导出相应的置换。换言之，对于每个 $\pi \in \mathcal{S}$，都存在一个 $\sigma \in \mathbf{Sym}_k$，使得 $(\sigma, \pi)N = N$。现在，我们按照引理 41 的证明中的做法，在 $g(\mathbf{Stab}_G([y] \cap x))$ 的作用下对 N 的各行取闭包。由此得到的矩阵满足所需的条件 (a) 和 (b)。现在我们证明，对于 N 的每一行，在 $g_{[y]}(\mathbf{Stab}_G([y] \cap x))$ 的作用下取闭包时，只会增加 $\mathrm{poly}(k + |\mathfrak{G}^S|)$ 行。

为证明这一点，我们必须界定$\mathbf{Orb}(N_{i-}) = \{\pi(N_{i-}) \mid \pi \in g(\mathbf{Stab}_G([y] \cap x))\}$的大小。令$\mathbf{Orb}(N)$表示集合 N 的行集在 $g(\mathbf{Stab}_G([y] \cap x))$-轨道下的轨道，并令$\mathbf{Stab}(N) \le g(\mathbf{Stab}_G([y] \cap x))$表示该行集的集合稳定子。由于行 N_{i-} 的任意像都是至少一个 k 元行集中的元素，因此有 $|\mathbf{Orb}(N_{i-})| \le k \cdot |\mathbf{Orb}(N)|$,

$\mathbf{Orb}(N)$。结合轨道-稳定子定理，我们得到

$$|\mathbf{Orb}(N_{i-})| \leq k \cdot |\mathbf{Orb}(N)| = k \cdot \frac{|g(\mathbf{Stab}_G([y] \cap x))|}{|\mathbf{Stab}(N)|}.$$

根据我们上面的论证，有 $\mathcal{S} \leq$ **稳定子**(N)，因此

$$\begin{aligned}\frac{|g(\mathbf{Stab}_G([y] \cap x))|}{|\mathbf{Stab}(N)|} &\leq \frac{|g(\mathbf{Stab}_G([y] \cap x))|}{|\mathcal{S}|} \\ &\leq \frac{|g(\mathbf{Stab}_G([y] \cap x))|}{|g(\mathbf{Stab}_{\mathbf{Stab}_G([y]\cap x)}(\mathcal{B}_\Gamma) \cap \mathbf{Stab}_{\mathbf{Stab}_G([y]\cap x)}(\mathcal{B}))|}.\end{aligned}$$

最后一个不等式成立，是因为 g(稳定子$_{\mathbf{Stab}_G([y]\cap x)}(\mathrm{B}_\Gamma) \cap$ 稳定子$_{\mathbf{Stab}_G([y]\cap x)}(\mathrm{B})) \leq \mathrm{S}$。不难证明，群同态的应用只会减小 H 在 G 中的指数，即 $[h(G) : h(H)] \leq [G : H]$。根据定义 56，稳定子$_{\mathbf{Stab}_G([y]\cap x)}(\mathrm{B}_\Gamma) \cap$ 稳定子$_{\mathbf{Stab}_G([y]\cap x)}(\mathrm{B})$ 在稳定子$_G([y] \cap x)$中的指数有多项式上界$|\mathfrak{G}^S|$。由于 g 是群同态，这也给出了 g 下像的指数上界，该指数等于上面的分数。综上，我们证明了：

$$|\mathbf{Orb}(N_{i-})| \leq k \cdot \mathrm{poly}(|\mathfrak{G}^S|) \leq \mathrm{poly}(k + |\mathfrak{G}^S|).$$

现在，这个轨道界适用于 N 的每一行 k，因此，在 g(**稳定子**$_G([y] \cap x)$) 的作用下对 N 的行取闭包时，我们至多向矩阵中添加 poly$(k+|\mathfrak{G}^S|)$ 个新行。因为 $k =$dim(**像** $M[y]$) $-$ dim($M[y] \cdot$**稳定子**$_E([y] \cap x)$) $\leq$dim(**像** $M[y]$) $\leq |E|$（这是因为 $M[y]$ 是定义在 $|E|$ 维空间 $\mathbb{F}_2^E$ 上的线性映射），poly$(k + |\mathfrak{G}^S|)$ =poly$(|\mathfrak{G}^S|)$。所得矩阵是 $N[x][y]$ 的一个候选，因此这表明 $N[x][y]$ 至多有 poly$(|\mathfrak{G}^S|)$ 行。◀

▶ **引理58**。 如果对于所有 $x \in \mathrm{tc}(\mu)$ 以及所有 $[y] \in C[x]$，**稳定子**$_E([y] \cap x)$ 都有对称基，那么 $|V_C|$的大小是关于 $|\mathfrak{G}^S|$的多项式。

证明。 这直接由引理 53 和引理 57 得出（注意，$|J_{[x][y]}|$ 是 $N[x][y]$的行数），并且由以下事实得出：$|\mathrm{tc}(\mu)|$ 是关于 $|\mathfrak{G}^S|$ 的多项式，因为 μ 在 $\mathfrak{G}^S$中是 CPT 可定义的。◀

这就证明了定理 32 中的**性质 4** 。

6.4 哪些向量空间有对称基?

我们已经证明，如果对于所有 $x \in$tc(μ) 和所有$[y] \in C[x]$，稳定子空间 **稳定子**$_E([y] \cap x)$ 有对称基，那么 $C(\mu)$ 的大小可以用多项式界定。如果情况并非如此，那么我们对 $C(\mu)$ 的大小一无所知。或许还有其他方法可以对其进行界定，但原则上我们必须假设它是超多项式的。与 CFI 对称情形相比，这使得这些对称异或电路在推导针对 CPT 的下界时不那么有用；当然，除非我们知道对象 μ 满足对称基性质。

这引出了一个问题：具有对称基性质的遗传有限集类别是什么样的。我们没有确定的答案，但可以证明：所有 CFI 对称对象都存在对称基；有一些简单的例子表明，存在具有对称基但并非 CFI 对称的对象；此外，还存在一些不存在对称基、但原则上可能是 CPT 可定义的对象。后一结果表明，我们很遗憾，几乎不可能普遍证明所有基于 CFI 图的 CPT 可定义对象都存在对称基。

↝▶ **引理 59**。设 $\mu \in \mathrm{HF}(E)$ 是 *CFI* 对称的。那么 μ 满足定义 *56* 中的对称基条件。

证明概要。设 $x \in \mathrm{tc}(\mu)$ 且 $[y] \in \mathrm{C}[x]$。设 $\Gamma := \mathrm{Stab}_E([y] \cap x) \leq \mathbb{F}_2^E$。我们需要分别为 Γ 和 $\mathbb{F}_2^E$ 定义两个基 $\mathrm{B}_\Gamma \subseteq \mathrm{B}$，使群 $\mathrm{Stabs}_{\mathrm{Stab}_G([y]\cap x)}(\mathrm{B}_\Gamma) \cap \mathrm{Stabs}_{\mathrm{Stab}_G([y]\cap x)}(\mathrm{B})$ 在 $\mathrm{Stab}_G([y] \cap x)$ 中具有多项式指数。由于 μ 是 CFI-对称的，根据定义 17，$\mathrm{Aut}_{\mathrm{CFI}}(\mathfrak{G})$ 对 $[y] \cap x$ 的轨道大小恰好为二。可以证明，此时稳定子空间 $\mathrm{Stab}_E([y] \cap x)$ 是一个子空间与一个布尔空间的直和：前者定义在某个坐标集 $I \subseteq E$ 上，恰好包含所有偶汉明重量的向量；后者定义在坐标 $E \setminus I$ 上。构造这样一个空间的基相对容易，且其轨道大小仅为线性：对于 $\mathbb{F}_2^I$ 的偶权子空间，可以固定一个坐标 $i \in I$，并取基 $\{\chi(i) + \chi(e) \mid e \in I \setminus \{i\}\}$，该基除 i 的选取外是对称的。对于空间 $\mathbb{F}_2^{E\setminus I}$，只需取由单位向量组成的典范基。详情见附录。◀

因此，所有 CFI 对称遗传有限集都满足定义 56 中的对称基性质。但是否还有其他具有对称基的对象？答案是肯定的。为求简明，我们不提供完全具体的例子，只简要描述一类非 *CFI* 对称且具有对称基的遗传有限集可能是什么样子。下文中，我们始终用 $\widetilde{\mathbb{F}}_2^I$ 表示 $\mathbb{F}_2^I$ 的子空间，其中包含所有汉明重量为偶数的向量。

▶ 例 60。对于 $n \in \mathbb{N}$，令 E_n 表示含有 n条基边的集合。我们不指定基图族 $(G_n = (V_n, E_n))_{n\in\mathbb{N}}$ 的具体形式。令 $A_n \uplus B_n \uplus \{e\} = E_n$ 为边集的一个任意划分，其中一个部分是单元素集。再来看例 16。在那里，我们定义了 CFI 对称对象 $\mu_{\{e,f,g\}} = \{\{\mu_{\{f,g\}}, e_0\}, \{\widetilde{\mu}_{\{f,g\}}, e_1\}\}$。在这个构造中，$\mu_{\{f,g\}}$ 及其自同构像 $\widetilde{\mu}_{\{f,g\}}$ 都是集合；凡是翻转 $\{f, g\}$ 中偶数条边的 $\rho \in \mathrm{Aut}_{\mathrm{CFI}}(\mathfrak{G})$，都会稳定这两个集合。对于任意边集，都可以更一般地定义此类对象。CFI 算法[10, 32]中便采用了这种做法。因此，令 μ_{B_n}、$\widetilde{\mu}_{B_n}$ 表示两个集合，它们共同构成一个 $\mathrm{Aut}_{\mathrm{CFI}}(\mathfrak{G}_n)$-轨道，并且任何翻转 B_n 中偶数条边的 $\rho \in \mathrm{Aut}_{\mathrm{CFI}}(\mathfrak{G}_n)$ 都会稳定它们。换言之，$\mathrm{Stab}_E(\mu_{B_n}) = \mathbb{F}_2^{A_n \cup \{e\}} \oplus \widetilde{\mathbb{F}}_2^{B_n}$。现在，对于每个 $n \in \mathbb{N}$，令

$$\mu_n := \{\{\mu_{B_n}, e_0\}\} \in \mathrm{HF}(\widehat{E}_n).$$

这个对象与例 16 中的对象相似，不同之处在于，$\{\mu_{B_n}, e_0\}$ 的连通分量仅包含这个集合本身，因此，该分量的 $\mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{G}_n)$-轨道的大小为四，而不是二。因此，$\mu_n$ 并非 CFI-对称。不过，它确实满足对称基性质（假设 μ_{B_n} 满足该性质——这是可能的，因为例如 μ_{B_n} 可以是 CFI-对称的）。令 $y = \{\mu_{B_n}, e_0\}$ 和 $x = \mu_n$。那么 $[y] \cap x = y$，因此 **稳定子**$_E([y] \cap x)$ $=$ **稳定子**$_E(y)$ $=$ **稳定子**$_E(\{\mu_{B_n}, e_0\})$。为这个空间构造一个对称基并不难。根据 μ_{B_n}的性质，我们有

$$\mathbf{Stab}_E(y) \cong \mathbb{F}_2^{A_n} \oplus \widetilde{\mathbb{F}}_2^{B_n}.$$

换句话说，该空间包含所有在 B_n 上具有偶汉明重量且在坐标 e 处取值为零的向量。按照引理 59 的证明，可以定义该空间的一组基：固定某个 $f \in B_n$。然后，将每个 $g \in A_n$ 对应的单位向量 $\chi(g)$ 以及每个 $g \in B_n \setminus \{f\}$ 对应的向量$\chi(\{f, g\})$ 纳入基 B_Γ。令 $\mathrm{B} := \mathrm{B}_\Gamma \cup \{\chi(e)\ \chi(f)\}$。我们没有精确指定基图，因此没有对 $\mathrm{Aut}(G)$ 作出任何假设。现在假设 A_n 和 B_n 属于 $\mathrm{Stab}_G([y] \cap x)$ 的不同轨道。这样的假设是合理的，因为否则 μ_{B_n} 未必会被稳定。于是，$\mathrm{Stabs}_{\mathrm{Stab}_G([y]\cap x)}(\mathrm{B}_\Gamma) \cap \mathrm{Stabs}_{\mathrm{Stab}_G([y]\cap x)}(\mathrm{B})$ 是 $\mathrm{Stab}_G([y] \cap x)$ 中逐点稳定 $\{e, f\}$ 的子群。其指数为 $\leq n^2$，这是多项式级的。

因此，具有对称基的对象确实是 CFI-对称对象的严格推广。尽管如此，目前还不存在能够处理 CFI 查询的无选择算法，而这种算法需要构造超出 CFI-对称对象范围的对象。

最后，最重要的问题是，是否也存在既不是 CFI-对称的、又没有对称基的对象。理想情况下，我们希望答案是：每个CPT 可定义对象 μ 都满足对称基条件。这样，针对合适电路的超多项式规模下界就能真正将 CPT 与多项式时间分离，因为这将排除任何 CPT 算法能够求解 CFI 查询的可能，而不只是排除诸如 CFI-对称算法之类的特殊算法。我们不知道这种理想情况是否确实存在。不过，我们有一个例子表明事实可能并非如此。

思路如下：要证明每个 CPT 可定义对象 μ都具有对称基性质，一个显而易见的办法是利用这样一个事实：对于每个 $x \in \mathrm{tc}(\mu)$ 和每个 $[y] \in \mathsf{C}[x]$，$\mathrm{Stab}_E([y] \cap x)$ 在 $\mathrm{Aut}_{\mathrm{CFI}}(\mathfrak{G}^S) \leq \mathbb{F}_2^E$中的指数必定是多项式级的（否则，$[y] \cap x \subseteq \mathrm{tc}(\mu)$ 的轨道就会是超多项式规模，因此 μ 就不是 CPT 可定义的）。这或许是由 μ的 CPT 可定义性直接得出的最显而易见的结论。为简化讨论，我们假设 $\mathrm{Aut}_{\mathrm{CFI}}(\mathfrak{G}^S) = \mathbb{F}_2^E$。那么用向量空间的术语来说，$[\mathbb{F}_2^E : \mathrm{Stab}_E([y] \cap x)]$ 的指数为多项式级，意味着 $\mathrm{Stab}_E([y] \cap x)$ 在 $\mathbb{F}_2^E$中的余维数，也就是 $|E| - \dim \mathrm{Stab}_E([y] \cap x)$，是对数级的。引理 38 还告诉我们，空间 $\mathrm{Stab}_E([y] \cap x)$ 在置换群 $\mathrm{Stab}_G([y] \cap x)$ 的作用下是不变的。这就引出了一个问题：关于 $\mathrm{Stab}_E([y] \cap x)$ 的这两个限制，是否足以证明 $\mathrm{Stab}_E([y] \cap x)$ 必然具有定义 56 意义下的对称基？遗憾的是，答案是否定的。存在一族布尔向量空间及其指标集上的置换群，使得这些空间在这些置换下保持不变、在环境空间中的余维数至多为对数级，而且不具有对称基。我们将在下文的引理 61 中构造这样一个例子。由此并不能直接推出，实际上存在一些 CFI 图族及其上的 CPT 可定义遗传有限集不具有对称基性质。这只能说明，我们无法仅凭向量空间的显而易见的性质来证明一般 CPT 可定义集合具有对称基性质；这些性质适用于 CPT 可定义对象中可能作为 $\mathrm{Stab}_E([y] \cap x)$ 出现的向量空间。

▶**引理 61.** 存在一族布尔向量空间 $(\Gamma_n)_{n\in\mathbb{N}}$、一个函数 $t(n) \in \Theta(n)$，满足 $\Gamma_n \leq \mathbb{F}_2^{t(n)}$，以及一族置换群 $(\mathbf{G}_n)_{n\in\mathbb{N}}$，满足 $\mathbf{G}_n \leq$ **对称群**$^{t(n)}$，使得
1. Γ_n 是$\mathbf{G}_n$-不变的。**2.** Γ_n 在 $\mathbb{F}_2^{t(n)}$ 中的余维数为 $O(\log n)$。**3.** 对于任意一对基$B_\Gamma \subseteq B$，其中 B_Γ 是 Γ_n 的基，且 B 是 $\mathbb{F}_2^{t(n)}$ 的基，$[\mathbf{G}_n :$ **稳定子**$_{\mathbf{G}_n}(B)] \geq \binom{n}{(\log n)^2}^{\log n}$，它相对于 n是超多项式。

证明概要。 我们将 Γ_n定义为 $\log n$ 个偶空间 $\widetilde{\mathbb{F}}_2^{P_i}$的直和，其中 $i \in [\log n]$。指标集 P_i 两两不相交，并构成 $[n]$的一个划分。群 $\mathbf{G}_n$ 定义为该划分 $\{P_1, \ldots, P_{\log n}\}$的集合稳定子。因此，空间 Γ_n是 $\mathbf{G}_n$-不变的。显然，Γ_n 在 $\mathbb{F}_2^n$ 中的余维数为 $\mathcal{O}(\log n)$。任意一对基 $\mathcal{B}_\Gamma \subseteq \mathcal{B}$ 的轨道大小下界成立，这是因为要将任意 $\mathcal{B}_\Gamma$ 扩充为 $\mathbb{F}_2^E$的一组基，必须在每个部分 P_i中至少选取一个点，其中 $i \in [\log n]$。这相当于 $\log n$ 次选择，每次都从大小为 $^n\log n$的集合中选取。这个选择元组的轨道大小是关于 n的超多项式。详细证明见附录。◀

我们不知道是否确实存在 CFI 图（$\mathfrak{G}_n^S$）$_{n\in\mathbb{N}}$ 以及定义在其上的遗传有限集（μ_n）$_{n\in\mathbb{N}}$，使得对于某个 $x, y \in \mathrm{tc}(\mu_n)$，有 $\Gamma_n \cong$ **稳定子**$_E([y]\cap x)$，且 $\mathbf{G}_n \cong$ **稳定子**$_G([y]\cap x)$。原则上，这种情况是可能的。无论如何，我们可以得出结论：对于某个 CFI 实例 $\mathfrak{G}^S$ 上的 CPT 可定义对象 μ，是否对所有相关空间 **稳定子**$_E([y]\cap x)$都存在对称基，这个问题无法在不利用关于 $\mathfrak{G}^S$ 和μ的更多信息的情况下得到回答：看来，仅凭对象的 CPT 可定义性不足以推断出所需对称基的存在（或者说，这需要比仅使用余维数对数界更复杂的技术）。不过应当指出，只有当我们为这些电路建立足够强的下界，从而将 CFI 对称算法与多项式时间区分开来之后，沿这一方向取得进一步进展才有意义。届时，下一步可以尝试考察这一结果在多大程度上能推广到所有无选择算法。

7 超立方体 CFI 结构的应用

我们的第二个主要结果是针对 n 维超立方体上的对称异或电路给出的下界。该结果表明，如果将电路参数的限制设得比定理 31 稍严格一些，那么对应于超立方体 CFI 结构上 CFI 对称遗传有限集的电路就不存在（请注意，我们现在回到了*CFI* 对称的情形）。不过，首先我们必须确认这些超立方体 CFI 结构确实满足定理 31 的前提条件。该定理主要取决于基图的三个参数：图的树宽、遗传有限集的*CFI* 支撑间隙，以及基图上的 CFI 图是$\mathcal{C}^{\mathbf{tw}_n}$-齐次这一事实。

n 维超立方体 H_n 是一个论域为 $\{0,1\}^n$ 的无向图，其中汉明距离恰好为一的任意两个字之间都有一条边。我们用 E_n 表示该边关系，用 $V_n = \{0,1\}^n$ 表示 H_n 的顶点集。它的自同构群是半直积 $\mathbb{F}_2^n \rtimes \mathrm{Sym}_n$，其中 Sym_n 作用于二进制字的位置，而 $\mathbb{F}_2^n$ 通过按位异或运算 [22] 作用于 $\{0,1\}^n$。下文中我们将假定 $\mathrm{Aut}(\mathrm{H}_n) \cong \mathrm{Sym}_n$，也就是说，我们忽略 $\mathbb{F}_2^n$ 的作用。这样处理会更简单；此外，如果不存在具有所需性质的 Sym_n-对称异或电路，那么对于更大的对称群 $\mathbb{F}_2^n \rtimes \mathrm{Sym}_n$ 来说，这就“更加不可能”了。具体而言，对于每个字 $v \in \{0,1\}^n$ 以及 $\pi \in \mathrm{Sym}_n$，群作用定义为 $\pi(v_1 \ldots v_n) = v_{\pi^{-1}(1)} v_{\pi^{-1}(2)} \cdots v_{\pi^{-1}(n)}$。在超立方体中，这相当于对每个顶点的邻域施加相同的置换 π；这会保留超立方体的图结构。

接下来，谈到超立方体上的 CFI 结构时，我们不区分同构的结构，因此只考虑 H_n 上的偶 CFI 结构和H_n 上的奇 CFI 结构，分别记为 $\mathfrak{H}_n^0$ 和 $\mathfrak{H}_n^1$。这些 CFI 结构的大小 $|\mathfrak{H}_n^i|$ 关于 $2^n = |\mathcal{H}_n|$ 是多项式级的，因为 CFI 构造会使图的大小按最大度呈指数增长。$\mathcal{H}_n$ 的最大度为 n，因此大小增加 2^n 倍仍然关于 $|\mathcal{H}_n|$ 是多项式级的。现在来考察超立方体及其 CFI 结构的相关性质。

超立方体的树宽

▶ **引理 62** (定理 5，见 [37])。 n 维超立方体 H_n 的树宽 是关于 $\Theta(2^n/\sqrt{n})$的一个函数。
这接近于 $2^n = |\mathcal{H}_n|$的线性函数，因此足够大，可以转化为所得电路输入敏感度的有意义下界。特别是，它是

超常数，因此超立方体 CFI 查询无法用带计数的定点逻辑定义。

超立方体的齐次性

回忆一下，对于某个长度 $\ell \leq k$ 的所有元组，结构 $\mathfrak{A}$ 都是 $\mathcal{C}^k$-齐次的，意即对于所有长度为 $\leq \ell$ 的元组 a, b，若 a 和 b 在 $\mathfrak{A}$ 中具有相同的 $\mathcal{C}^k$-类型，那么就存在 $\mathfrak{A}$ 的一个自同构，将 a 映射到 b。下一个引理是证明超立方体 CFI 结构齐次性结果所需的一个技术性要素。它展示了特定元组满足齐次性条件。完整证明见附录。

我们称 α 中的一个元组 $V(\mathfrak{H}_n^i)$包含一个星，如果存在一个中心 $c \in V(\mathcal{H}_n)$，使得对于 r 每条关联边 $e \in E_n(c)$，边构件 e^* 中都有 α 的一个项。

▶引理 *63*。令 $tw_n \in \Theta(2^n/\sqrt{n})$ 表示 H_n 的树宽。设 α 是 $V(\mathfrak{H}_n^i)$ 中一个包含星且长度至多为 $(tw_n/n) - 2$ 的元组。设 $\gamma, \gamma' \in V(\mathfrak{H}_n^i)$，并令 $tp(\alpha\gamma)$ 表示这个扩展元组的 C^{tw_n}-类型。若 $tp(\alpha\gamma) = tp(\alpha\gamma')$，则存在一个自同构 $\rho \in Aut(\mathfrak{H}_n^i)$，使得 $\rho(\gamma) = \gamma'$ 且 $\rho(\alpha) = \alpha$。

证明概要。证明大体上是标准的，与[31] 和 [36]中的齐性证明类似。首先，可以证明，如果 $\mathrm{tp}(\alpha\gamma) = \mathrm{tp}(\alpha\gamma')$，那么 γ 和 γ' 必定位于 CFI 结构的同一个构件中。即使这些构件无法通过拟序识别，这一点仍然成立：利用参数 α，可以用常数个变量定义 γ 和 γ' 的构件。因此，我们知道 γ 和 γ' 位于同一个——比如说，边构件e^* 中（它们位于顶点构件中的情形类似）。如果 $\gamma = \gamma'$，那么无需证明其他内容。否则，我们需要在 $\mathrm{Aut}_{\mathrm{CFI}}(\mathfrak{H}_n^i)$ 中找到一个自同构，它翻转 e^*，且不移动 α中的任何元素。若 H_n 中存在一条经过 e 且不经过 α中任何边的环，这便是可能的。如果不存在这样的环，那么元组 $\alpha\gamma$ 就标记了 $\mathfrak{H}_n^i$的某个足够小的子图的边界；重要的是，该子图的树宽<为 tw_n。接着可以证明，利用参数 α，可以在 $\mathrm{C}^{\mathrm{tw}_n}$ 中定义 γ 和 γ'。具体做法是，将警察与强盗游戏中警察的获胜策略转换为双射 tw_n-棋子游戏中 Spoiler 的获胜策略，如 [2]所示。因此，所需的环以及相应的自同构必定存在，否则 $\mathrm{tp}(\alpha\gamma) \neq \mathrm{tp}(\alpha\gamma')$。◀

▶**引理 64.** 结构 $\mathfrak{H}_n^0$ 和 $\mathfrak{H}_n^1$ 在以下意义上是齐次的：令 tw_n 表示 H_n的树宽。对于 $V(\mathfrak{H}_n^i)$ 中长度为 $|\alpha| = |\alpha'| \leq tw_n/n - n - 1$ 的任意元组 α, α'，若 α 和 α' 在 $\mathfrak{H}_n^i$中具有相同的 C^{tw_n}-型，那么存在 $\mathfrak{H}_n^i$ 的一个自同构，将 α 映射到 α'。

证明。 首先，我们通过对 $|\alpha|$进行归纳法，证明以下断言。

断言 1： 设 s 是一个长度为 n 且包含一个星的元组。若 $\mathrm{tp}(s\alpha) = \mathrm{tp}(s\alpha')$，那么存在 e $\mathfrak{H}_n^i$ 的一个自同构，将元组 $s\alpha$ 映射到 $s\alpha'$。

断言的证明： 在基础情形 $|\alpha| = 0$中，无需证明任何内容，因为此时恒等置换就是所需的自同构。

对于归纳步骤，令 $\alpha = \beta\gamma$其中 $|\beta| = |\alpha| - 1$，并类似地记 $\alpha' = \beta'\gamma'$。由于 $\mathrm{tp}(s\alpha) = \mathrm{tp}(s\alpha')$，我们也有 $\mathrm{tp}(s\beta) = \mathrm{tp}(s\beta')$。因此，归纳假设给出一个自同构 $\pi \in \mathbf{Aut}(\mathfrak{H}_n^i)$，使得 $\pi(s\beta) = s\beta'$。由于自同构保持类型，我们有 $\mathrm{tp}(s\beta\gamma) = \mathrm{tp}(\pi(s\beta\gamma)) = \mathrm{tp}(s\beta'\pi(\gamma)) = \mathrm{tp}(s\beta'\gamma')$。元组 $s\beta'\pi(\gamma)$ 和 $s\beta'\gamma'$ 的长度至多为 $\mathbf{tw}_n/n - 1$，因此我们可以对它们应用引理 63。这给出了另一个自同构 σ，使得 $\sigma(s\beta'\pi(\gamma)) = s\beta'\gamma'$。总之， $\sigma \circ \pi \in \mathbf{Aut}(\mathfrak{H}_n^i)$ 是

所需的自同构，它将 $s\alpha$ 映射到 $s\alpha'$。

现在我们将使用断言 1 来证明引理。设 α 和 α' 如引理中所述。设 s 是一个长度为 n、包含一个星（且仅包含一个星）的元组。根据 [10], 中的引理34，存在一个元组 s'，使得 $\mathrm{tp}(s\alpha) = \mathrm{tp}(s'\alpha')$。这是因为 $(\mathfrak{H}_n^i, \alpha) \equiv_{C^{\mathbf{tw}_n}} (\mathfrak{H}_n^i, \alpha')$（定理 6），因此，对于仅通过 n 个元素扩展元组 α（其长度至多为 $\mathbf{tw}_n - n$）的任意扩展，都存在一个保持类型的 α' 的扩展。

断言2： 存在一个自同构 $\sigma \in \mathbf{Aut}(\mathfrak{H}_n^i)$，使得 $\sigma(s) = s'$。

断言的证明：设 $s_1, \ldots, s_n \in E_n$ 是由 s 覆盖的星的边，且 $s'_1, \ldots, s'_n \in E_n$ 是 s' 的星的边。存在一个自同构 $\sigma' \in \mathbf{Aut}(\mathcal{H}_n)$，使得对于每个 i，都有 $s'_i = \sigma'(s_i)$。这一点很容易看出，因为我们可以将一个星的中心 c 映射到另一个星的中心 c'，并对其关联边应用适当的置换。在 $\mathfrak{H}_n^i$ 中，构件 c^* 和 c'^* 关于元组 s 要么都具有偶奇性，要么都具有奇奇性。也就是说，如果我们假设顶点 s_i 是各自边小装置中的 1-顶点，那么顶点小装置 c^* 和 c'^* 具有相同的奇偶性：这是因为我们可以在比如说 $\mathcal{C}^5$ 中表达：c^* 中的每个顶点都与 s 中偶数个顶点相连（s' 中也是如此）。

我们称 $\sigma'(s)$ 与 s' 在位置 i 处失配，如果 $\sigma'(s)_i$ 是其边构件中的 0-顶点，而 s'_i 是 1-顶点，或者反之。根据刚才的论证，$\sigma'(s)$ 与 s' 之间的失配数量为偶数。我们可以用自同构 $\rho_F \in \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{H}_n^i)$ 来修正这一点：该自同构沿着从 c' 出发的 ℓ 个不相交环翻转边，其中 ℓ 是失配数量的一半。于是，$\sigma = \rho_F \circ \sigma'$ 是一个将 s 映射到 s' 的自同构。这就证明了该断言。

根据断言2，由于自同构保持类型，我们有 $\mathrm{tp}(s'\sigma(\alpha)) = \mathrm{tp}(s'\alpha')$。$s$ 包含一个星这一事实很容易用计数逻辑定义，因此 s' 也包含一个星。因此，该引理现在由断言 1 得证；断言 1 给出了一个将 $\sigma(\alpha)$ 映射到 α' 的自同构 π。于是，$\pi \circ \sigma$ 就是引理所断言存在的自同构。
◀

总之，对于长度不超过$\mathbf{tw}_n/n - n - 1$的所有元组，超立方体 CFI 结构都满足定理 31 所要求的齐次性条件，其大小为 $\Theta(\mathbf{tw}_n/n)$。

超立方体 CFI 结构的 CFI 支撑间隙

回顾定义 30，遗传有限集 μ 的 CFI 支撑间隙为 $\alpha(\mu) = s(\mu)^{|\mathrm{sup}_{\mathrm{CFI}}(\mu)|}$，其中$s(\mu)$表示最小支撑的大小；这取决于结构。仍令 $\mathfrak{H}_n^i$表示 n维超立方体上的奇/偶 CFI 结构，并令 E_n 为该超立方体的边集。令 $\mathfrak{H}_n$ 表示 H_n 上的完整 CFI 图（见第 3 节）。我们希望证明所有遗传有限集 $\mu \in \mathrm{HF}(E_n)$上的比值 $\alpha(\mu)$ 的一个上界。这里，$s(\mu)$表示 μ的最小 $\mathrm{Aut}(\mathfrak{H}_n^i)$-支撑的大小，而 $\mathrm{sup}_{\mathrm{CFI}}(\mu)$表示 μ的最小 CFI 支撑的大小。回顾定义 11，μ 的 CFI 支撑是边的集合 $S \subseteq E$，满足：任何固定了 S 中所有边的边翻转 $\rho_F \in \mathrm{Aut}_{\mathrm{CFI}}(\mathfrak{H}_n)$，也会固定 μ。这里考虑的边翻转不一定是 $\mathfrak{H}_n^i$的自同构，因此包括所有翻转边的组合，而不只是环。

引理 65. 设 $n \in \mathbb{N}$ 和 $\mu \in \mathrm{HF}(E_n)$。设 $S \subseteq E$ 是 μ的最小 *CFI* 支撑。那么存在一个 μ 的 $\mathbf{Aut}(\mathfrak{H}_n^i)$-支撑，其大小至多为 $|S| + n$。

证明。每个 $\rho_F \in \mathrm{Aut}_{\mathrm{CFI}}(\mathfrak{H}_n)$ 都满足 $F \cap S = \emptyset$ 固定 μ。特别地，这对每个这样的 $\rho_F \in \mathrm{Aut}_{\mathrm{CFI}}(\mathfrak{H}_n^i) \leq \mathrm{Aut}_{\mathrm{CFI}}(\mathfrak{H}_n)$ 都成立。因此，设 α 是 $\widehat{E}_n$ 中的任意一个元组，其中每条边 $e \in S$ 都恰好有一个顶点 e_i。于是 $|a| = |S|$。那么，任何形如 $(\rho_F, \mathrm{id}) \in \mathrm{Aut}(\mathfrak{H}_n^i)$ 且固定 α 的自同构，也会固定 μ。现在将 α 扩展为一个包含星的元组 β。总可以做到这一点，使得 $|\beta| \leq |\alpha| + n$。现在，$\mathrm{Aut}(\mathfrak{H}_n^i)$ 中任何固定 β 的自同构，其第二个分量都必须是 id，因为任何满足 $\pi \neq \mathrm{id}$ 的 $(\rho_F, \pi) \in \mathrm{Aut}(\mathfrak{H}_n^i)$ 都会移动超立方体中的每个星。因此，总之，每个固定 β 的自同构都会固定 μ，而 β 的长度至多为 $|S| + n$。◀

令 $\mathbf{tw}_n \in \Theta(2^n/\sqrt{n})$ 表示 n 维超立方体的树宽。令 $\alpha(n) := \max_{\mu \in \mathrm{HF}(\widehat{E}_n),\ s(\mu) \in \Omega(\mathbf{tw}_n/n)} \mathrm{HF}(E_n)$ 中，最小支撑大小至少为 $\Omega(\mathbf{tw}_n/n)$ 的任意对象可能具有的最大 CFI 支撑间隙。

▶ **推论 66.** 存在一个函数 $g(n) \in O(1)$，它是 $\alpha(n)$ 的一个上界。

证明。设 $\mu \in \mathrm{HF}(\widehat{E}_n)$ 是一个对象，其最小 $\mathrm{Aut}(\mathfrak{H}_n^i)$-支撑大小 $s(\mu)$ 至少为 $\Omega(\mathrm{tw}_n/n)$。根据引理 65，其最小 CFI 支撑 $\mathrm{sup}_{\mathrm{CFI}}(\mu)$ 的大小至少为 $s(\mu) - n$。因此，CFI 支撑间隙 $s(\mu) - |\mathrm{sup}_{\mathrm{CFI}}(\mu)|$ 至多为 $s(\mu) - s(\mu) - n = 1 + s^n(\mu) - n$。由于 $s(\mu) \in \Theta(2^n/n^{1.5})$，该表达式渐近等于 1。◀

因此，在定理 31 的设定下，我们可以用常数函数 $g(n)$ 作为 CFI 支撑间隙的上界。这很方便，因为这意味着定理 31 得出的异或电路对尽可能多的边敏感，即 $\Omega(\mathbf{tw}_n/n)$ 条边。我们的目标是证明定理给出的对称电路不可能存在，因此，支撑间隙不会放宽对这里电路的限制，这一点是有利的。

总而言之，我们可以这样概述关于超立方体 CFI 结构的结果：

▶**定理 67。** 如果存在一个超对称且CFI-对称的 *CPT* 程序 Π，能够判定所有超立方体 *CFI* 结构 $(\mathfrak{H}_n^i)_{n \in \mathbb{N}}$ 这一族上的 *CFI* 查询，那么对于每个 $H_n = (V_n, E_n)$，都存在一个在 H_n 上的异或电路 C_n，满足：

1. 门的数量 C_n 是 2^n 的多项式。**2.** 电路的轨道大小 $|\mathbf{Orb}_{\mathcal{H}_n}(C_n)|$ 是 2^n 的多项式。**3.** C_n 对 $\Omega(2^n/n^{1.5})$ 条边 E_n 敏感。**4.** （不受限制的）扇入维数为 C_n $\mathcal{O}(n)$。

这只不过是将定理 31 应用于超立方体 CFI 结构。下界源于 $|\mathfrak{H}_n^i| = \mathrm{poly}(2^n)$ 这一事实，以及 $\mathfrak{H}_n^i$ 的齐次性条件对长度至多为 $\mathcal{O}(\mathbf{tw}_n/n) = \mathcal{O}(2^n/n^{1.5})$ 的所有元组都成立。

8 超立方体上的对称异或电路族的下界

如果我们能够成功证明具有定理 67 中所述性质的电路不存在，就可以推出，没有超对称且 CFI-对称的无选择算法能够解决超立方体 CFI 问题。遗憾的是，我们只能在一定程度上做到这一点。我们对电路施加了略强的约束，然后证明，这样的电路族确实不可能存在于超立方体上。具体而言，我们加强了电路的对称性条件，并假设它们在基图（即 n 维超立方体）的所有 自同构作用下均保持不变，因此其轨道大小为一。定理 67 仅指出，电路的

轨道大小必须是多项式级的。此外，我们还施加了这样的条件：每个门的子节点和父节点数量（按轨道计）必须有对数界。这可能与我们从定理 67 得到的扇入维数对数界有关，但这很可能是一个更强的限制。对于 n 维超立方体上的、具有这些性质的电路，我们证明它们对足够多的输入门并不敏感，因此违反了定理 67 中的性质 3。

我们的下界受到一种“几乎正确”的电路构造的启发，这种电路满足定理 67 中的性质。构造这类电路最困难的部分似乎是这一条件：相对于**对称群**n 在$\{0,1\}^n$上的作用，它们应具有多项式轨道大小。一个初步想法是使用一棵次数为对数级的树，其叶节点标记为$\{0,1\}^n$中的元素。这样就能满足所有性质，唯独轨道大小或许例外。事实上，我们无法证明不存在具有所需轨道大小的树状电路，但我们怀疑树的对称性不够强。本节的结果也指向这一结论，稍后我们会对此加以说明。

除了树状电路，还有另一种或多或少显而易见的构造思路，可以说与树恰好相反：为了构造一个保证在超立方体自同构下对称的电路，我们可以直接使用超立方体本身：将超立方体从中间切开，并把其中一半用作电路。例如，输出门将是字符串 0^n，输入门则标记为汉明重量为 $(n/2)$ 的字符串，它们位于超立方体的“中间层”。下图展示了这一构造。

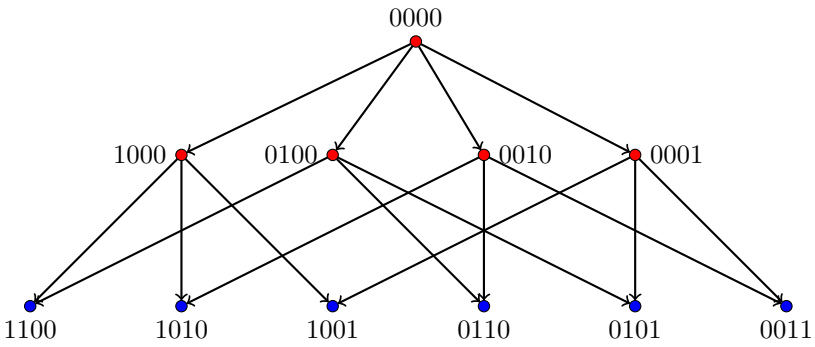

图 3 被切成两半的 4 维超立方体。红色节点是异或门，蓝色节点是输入门。

该电路满足正确的大小界和轨道大小界（具体来说，按构造，电路的轨道大小为 1），并且其次数为 n，相对于 $|\mathfrak{H}_n^i|$ 呈对数级。由于次数是扇入维数的上界，因此对数级扇入界也得到满足。然而，我们可以看到，该电路实际上对任何输入位都不敏感。从输入层开始数的第二层中，所有输入就已经相互抵消了（在上面的例子中，这发生在根节点）：每个输入位到达根节点的次数都是偶数。因此，我们从这一构造中得知，可以通过让电路具有非常明显的有向无环图式结构来构造高度对称电路；但任何给定输入位在电路中可能经过的大量不同路径，很容易导致该输入位在电路中的某处抵消自身。只要路径数量为偶数，就会发生这种情况。因此，粗略地说，树状电路和这些“半超立方体电路”处于两个极端：对于树来说，敏感性条件（定理 31 中的性质 3）显然成立，但

对称性条件则并不明显。相反，在半超立方体中，对称性按构造成立，但电路对任何输入位都不敏感。问题是：这两个极端之间是什么情形？我们现在将证明，半超立方体电路中的输入抵消效应实际上会出现在更大一类对称电路中。从某种意义上说，这排除了所有与半超立方体过于相似的电路。粗略地说，这类电路包括所有定义在 n 维超立方体上、由 **对称群**$_n$ 中的所有置换稳定，且具有“按轨道计算”的对数级入度和出度的电路。

固定一个异或电路族 $(C_n)_{n\in\mathbb{N}}$，其中 C_n 的输入门以 n维超立方体$\mathcal{H}_n$的边为标签。与上一节一样，这些电路是连通的有向无环图，并指定了唯一的输出门，即根。我们定义

$$\begin{aligned}\mathbf{Aut}(C_n) :=\{&\sigma \in \mathbf{Sym}(V_{C_n}) \mid \sigma \text{ is an automorphism of the rooted DAG } (V_C, E_C, r)\\ &\text{and there exists a } \pi \in \mathbf{Sym}_n \text{ s.t. } \ell(\sigma(g)) = \pi(\ell(g)) \text{ for every input gate } g\}.\end{aligned}$$

特别要注意的是，每个自同构都必须固定电路的根，并且必须以符合**对称群**$_n$ 作用于叶节点标签的置换的方式置换叶节点。若置换 $\pi \in$**对称群**$_n$ 延伸为自同构 $\sigma \in \mathbf{Aut}(C_n)$，则称其为扩展；此时$\sigma$ 会映射输入门 g，使得 $\ell(\sigma(g)) = \pi(\ell(g))$ 成立。对称群**对称群**$_n$ 中的恒等置换可能扩展为 C_n中的非平凡电路自同构。在这种情况下，电路不是刚性的，并且对称群**对称群**$_n$ 中的每个置换都有多个电路自同构与之对应。对于 C_n 中的门 g 及其父节点 h（属于 g），我们令

$$\mathbf{Orbit}_{(g)}(h) := \{\sigma(h) \mid \sigma \in \mathbf{Aut}(C_n), \sigma(g) = g\}.$$

同理,

$$\mathbf{Orbit}_{(h)}(g) := \{\sigma(g) \mid \sigma \in \mathbf{Aut}(C_n), \sigma(h) = h\}.$$

因此，g和 h分别是相对于固定子节点 g或父节点 h的那些电路自同构而言的轨道。注意，**轨道**$^{(g)}(h) \subseteq E_C g$，且**轨道**$^{(h)}(g) \subseteq hE_C$，因为电路自同构保持连线；如果一条连线的一个端点固定，那么另一个端点的像仍必须与这个固定门相连。在本节的其余部分，我们将证明：

▶**定理 68.** 设$(C_n)_{n\in\mathbb{N}}$ 是定义在 n维超立方体上的异或电路族，并且对所有 $n \in \mathbb{N}$，以下条件均成立：
1. 大小 $|V_{C_n}|$ 关于 2^n 是多项式级的（因此关于 $|\mathfrak{H}_n^i|$也是多项式级的）。*2.* 作用于$\{0,1\}^n$ 上的每个置换 $\pi \in Sym_n$ 都可扩展为 C_n的一个电路自同构。因此，Sym_n-轨道 C_n 的大小为一。*3.* 存在一个函数 $f(n) \in O(n)$，使得对于所有足够大的 n，对于每个门 g以及 C_n中 g 的每个父节点 h，|轨道$^{(g)}(h)$| 和 |轨道$^{(h)}(g)$| 均至多为 $f(n)$。

那么，对于任意常数 $\varepsilon > 0$，当 n 足够大时，以下结论成立：电路 C_n 只有在 $\ell(g) = \{u, v\}$ 是一条边，且二进制字符串 $u, v \in \{0,1\}^n$ 中的零一划分比 εn 与 $(1-\varepsilon)n$ 更不平衡时，才可能对输入门 g 敏感。换言之，只有当 u 和 v 中 1 的数量或 0 的数量为 $< \varepsilon n$ 时，该输入门才会对 C_n 的输出有所贡献。

特别是，这些电路不满足定理 31 中的性质 3，因此可以排除：

▶**推论 69.** 设$(C_n)_{n\in\mathbb{N}}$ 是定理 *68* 中的电路族。那么对于所有足够大的 n，电路 C_n 对严格少于 $o(2^n/n^{1.5})$ 个输入敏感。

证明。 根据第 492 页的习题 9.42，[20], 它对任意 $\alpha \leq \frac{1}{2}$ 均成立：

$$\sum_{k\leq \alpha n} \binom{n}{k} = 2^{nH(\alpha)-\frac{1}{2}\log n+\mathcal{O}(1)},$$

其中 $H(\alpha) = \alpha\log(\frac{1}{\alpha}) + (1-\alpha)\log(\frac{1}{1-\alpha})$。根据定理 68，$\mathcal{H}_n$ 中可能对 C_n 敏感的边，只存在于一或零的个数少于 εn 的二进制字符串之间，对任意 $\varepsilon > 0$ 均如此。这类边的潜在端点数是上述总和的两倍，对 $\alpha = \varepsilon$ 均如此。$\mathcal{H}_n$ 的次数为 n，因此总共，C_n 至多对 $\mathcal{H}_n$中的 $2n \cdot \sum_{k\leq \varepsilon n}\binom{n}{k}$ 条边敏感。我们可以计算得，对任意 $0 < \varepsilon < \frac{1}{2}$，其为 $o(2^n/n^{1.5})$：

$$\lim_{n\to\infty} \frac{2^n}{n^{1.5}\cdot 2n\cdot 2^{nH(\varepsilon)-\frac{1}{2}\log n+\mathcal{O}(1)}} = \lim_{n\to\infty} \frac{2^{(1-H(\varepsilon))n+\frac{1}{2}\log n-\mathcal{O}(1)}}{2n\cdot n^{1.5}} = \infty$$

最后一步中，我们用到了 $H(\varepsilon) < 1$，只要 ε 严格小于 $1\ 2$，该结论就成立。◀

这就证明了定理 2。不过，这一结果尚未完全排除存在定理 67 所要求的对称电路族：首先，我们假设这里的电路是完全对称的，也就是说，它们在$\mathbf{Sym}_n$ 中的每一个置换作用下都保持不变；而在定理 67 中，电路只需相对于基图的自同构具有多项式轨道，因此它们在许多（但不一定是所有）这些自同构作用下保持不变。其次，在定理 67 中，我们只有关于扇入维数的对数界，但尚不清楚这是否也意味着每个门的轨道上的子节点和父节点数量有界，如上文性质 3 所述。尽管如此，我们希望这一关于完全对称有界度异或电路不存在的否定性结果，能成为排除超立方体上的更多电路类的有用起点，并最终排除定理 67 中的所有电路。

8.1 置换群的支撑划分

该定理的证明依赖于群论技术，这些技术使我们能够将每个指数为 poly(2^n) 的置换群近似为大型交错群的乘积。这一思想源自 Anderson 和 Dawar 关于对称电路与不动点逻辑的论文[1]。其中证明了，任意群 $G \leq \mathbf{Sym}_n$ 都有唯一的最粗支撑划分$\mathbf{SP}(G)$。这是 $[n]$ 的最粗划分，使得每个逐集合稳定每个部分的 $\pi \in \mathbf{Sym}_n$ 都属于 G。在此基础上，我们扩展了这一概念，并定义了交替支撑划分。交错群 $\mathbf{Alt}_n \leq \mathbf{Sym}_n$ 是只包含偶符号置换的群。如果一个置换颠倒了 $[n]$ 中偶数对的顺序，则称该置换具有偶符号。

▶ **定义 70**（交替支撑划分）。设 A 是一个集合，$G \leq$**对称群**(A) 是作用于 A上的置换群。G 的一个交替支撑划分是指 A的一个划分 P，满足

$$\prod_{\substack{P\in\mathcal{P}\\ |P|<5}} \mathbf{Sym}(P) \times \prod_{\substack{P\in\mathcal{P}\\ |P|\geq 5}} \mathbf{Alt}(P) \leq G.$$

与“标准”支撑划分的区别在于，交替支撑划分中各部分内的奇置换不必属于受支撑群G。对于大小为 <5的部分，我们要求完整的对称群包含在 G中，否则下一条引理的证明会遇到问题；而且在我们的应用中，常数大小的部分本来也不会起太大作用。我们必须验证，交替支撑划分的性质与 [1]中的原始支撑划分相同。具体来说，我们希望群 G 总存在唯一的最粗支撑划分，并且 G 介于该划分的逐点稳定子与集合稳定子之间。

▶ **引理 71.** 每个置换群 $G \leq$**对称群**(A) 都有唯一的最粗交错支撑划分，记作$\mathbf{SP}_A(G)$。

证明。证明与 [1] 中引理 1 的证明类似。我们需要证明，对于任意两个交错支撑划分 P 和 P′, ，由它们共同细化得到的最细划分仍是交错支撑划分。于是该引理直接成立。P 和 P′, 的这个“最细公共粗化”记作 E(P, P′)，定义如下：令$\sim \subseteq A^2$ 为关系“a 和 b 在 P 或 P′的某个部分 P 中同时出现”的传递闭包。 $\sim$ 的等价类就是 E(P, P′) 的部分 $=:$ E。我们要证明，对于 E 的任意部分 Q 中的任意偶置换（该置换逐点固定 Q之外的所有元素）也属于 G。为此，我们证明：若 $P \in$P $P' \in$P′有非空交集，则 Alt($P \cup P'$) $\leq G$。由于 Alt($P \cup P'$) 由两两对换的乘积 $(xy)(x'y')$ 生成，只需证明所有此类乘积都属于 G。因此，考虑 $(xy)(x'y')$, 其中 x、y、x'、$y' \in P \cup P'$两两不同。分以下情形讨论：若 x、x'、y、y'都属于 P（或类似地，都属于 P'），则 $(xy)(x'y') \in$ Alt(P) $\leq G$ （利用 P 是G的交错支撑划分这一点）。

下一个情形是 $x \in P \setminus P', y \in P' \setminus P$ 和 x', y' 属于同一个部分，不妨设它们都属于 P'。在这种情形下，取 $z \in P \cap P'$，并令 $a, b \in P \setminus \{x, z\}$ 为两个不同的元素（如果不存在这样的 a, b，那么 $|P| \leq 3$，因此 Sym(P) $\leq G$，这意味着即使没有这些 a, b，以下论证仍然成立）。有 $(xy)(x'y') = (xz)(ab)(zy)(x'y')(xz)(ab)$。 P 内部和 P' 内部的对换数均为偶数（每当我们交换 x 和 z 时，总会同时交换 a 和 b，并且还会将 x' 和 y' 与 (zy) 一起交换），因此这个乘积属于 Alt(P) $\times$ Alt(P')，进而属于 G，因为 P 和 P′ 都是 G 的支撑划分。
另一种情况是 $x, x' \in P \setminus P'$and $y, y' \in P' \setminus P$。仍令 $z \in P \cap P'$，并固定某些 $a, b \in P \setminus \{x, x', z\}$ 和 $a', b' \in P' \setminus \{y, y', z\}$。同样，如果无法做到这一点，那么 P和 P'都小于 5，因此它们上的所有置换都属于 G，这样下一步就更容易了。考虑 $(xz)(ab)(zy)(a'b')(xz)(ab)(x'z)(ab)(zy')(a'b')(x'z)(ab)$。这等于 $(xy)(x'y')$，并且同样属于 Alt(P) $\times$ Alt(P')，因此属于 G。

剩下的情况是 $x, y \in P$and $x', y' \in P'$。我们可以假设 $x, y \in P \setminus P'$and $x', y' \in P'$，因为 Alt(P) $\times$ Alt(P') $\leq G$，所以我们可以分别将要交换的元素移动到 P, P' 中的任意位置。然后，我们可以通过将前一种情况应用两次来模拟置换 $(xy)(x'y')$：首先，执行 $(xx')(yy')$，然后执行 $(xy')(yx')$。如上所示，这两者都属于 Alt(P) $\times$ Alt(P')，因此总的来说，我们有 $(xy)(x'y') \in$Alt(P) $\times$Alt(P') $\leq G$。

因此，我们已经证明，可以取 $\mathcal{P}$ 和 $\mathcal{P}'$, 中两个相交部分的并，而这个并上的交错群也属于 G。通过迭代这一过程，我们可以证明，对于每个 $Q \in \mathcal{E}$，都有**交错群**(Q) $\leq G$，因为 $\mathcal{E}$ 的所有部分都可以通过迭代取 $\mathcal{P}$ 和 $\mathcal{P}'$ 中相交部分的并得到。剩下要证明的是，对于所有满足$|Q| < 5$ 的 $Q \in \mathcal{E}$，都有 **对称群** (Q) $\leq G$。但这显然成立，因为这样的部分 $Q \in \mathcal{E}$ 只能是小部分 $P \in \mathcal{P}$ 和 $P' \in \mathcal{P}'$ 的并。于是我们有 **对称群**(P) $\leq G$，以及 **对称群**(P') $\leq G$。我们可以

很容易看出，**对称群**($P \cup P'$) 中的每个对换也都属于 G；论证与上文相同，只是为了保持符号为偶，我们不再需要虚拟对换。◀

▶ **引理 72** （ [1] 中关于交错支撑划分的引理 3 的变体）。 对于任意$G \leq$ **对称群**(A)，以及任意 $\sigma \in$ **对称群**(A) $\sigma\mathbf{SP}_A(G) = \mathbf{SP}_A(\sigma G\sigma^{-1})$。

证明。正如 [1], 所述， σE(P, P′) =E(σP σP′) 对任意 $\sigma \in$ 对称群(A) 均成立。因此，剩下要证明的是：对于 G 的任意交错支撑划分 P，以及任意 $\sigma \in$ 对称群(A)，σP 是 $\sigma G\sigma^{-1}$的交错支撑划分。于是，令

$$\pi \in \prod_{\substack{P\in\sigma\mathcal{P}\\|P|<5}} \mathbf{Sym}(P) \times \prod_{\substack{P\in\sigma\mathcal{P}\\|P|\geq 5}} \mathbf{Alt}(P).$$

Then

$$(\sigma^{-1}\pi\sigma) \in \prod_{\substack{P\in\mathcal{P}\\|P|<5}} \mathbf{Sym}(P) \times \prod_{\substack{P\in\mathcal{P}\\|P|\geq 5}} \mathbf{Alt}(P).$$

因此，$(\sigma^{-1}\pi\sigma) \in G$，因为$\mathcal{P}$ 是 G的交错支撑划分。因此，$\pi \in \sigma G\sigma^{-1}$，所以， $\sigma\mathcal{P}$ 是 $\sigma G\sigma^{-1}$的交错支撑划分。◀

▶ **引理 73** （ [1] 中关于交错支撑划分的引理 4）。 设 $G \leq$**对称群**(A)。那么：

$$\prod_{\substack{P\in\mathbf{SP}_A\\|P|<5}} \mathbf{Sym}(P) \times \prod_{\substack{P\in\mathbf{SP}_A\\|P|\geq 5}} \mathbf{Alt}(P) \leq G \leq \mathbf{Stab}(\mathbf{SP}_A(G)).$$

证明。 第一部分由交替支撑划分的定义直接得出。对于第二部分，设 $\sigma \in G$。那么 $\sigma G\sigma^{-1} = G$。因此 $\sigma\mathbf{SP}_A(G)$ =$\mathbf{SP}_A(G)$ 由前面的引理可知。◀

因此，每个群都有唯一的最粗交错支撑划分，并且介于其逐点稳定子和集合稳定子之间。我们引入这些交替 支撑划分的原因是，它们具有一个有用的性质：对于指数为≤poly(2^n)的群，最粗交错支撑划分中的单元素部分至多有次线性数量。该结论的证明依赖于以下引理。由于证明相当冗长且需要一些额外的预备知识，我们只在附录中给出证明。简而言之，该引理的证明与 [14]中的定理 5.2 B类似。区别在于，此处指数的上界为 2^{nk}，而在 [14], 中，上界要小得多，只有 n^k。下文使用 [14], 中的记号，因此对于任意群 $H \leq$**对称群**$_n$以及任意子集$\Delta \subseteq [n]$, $H^{(\Delta)}$ 表示 H 中逐点固定 Δ 的子群。

▶ **引理 74.** 设 $(G_n)_{n\in\mathbb{N}}$ 是一个群族，使得对于所有的 n, $G_n \leq$**对称群**$_n$。假设存在某个常数 $k \in \mathbb{N}$，使得渐近地， [**对称群** $_n$： G_n] $\leq 2^{nk}$。

那么存在一个常数 $0 < c \leq 1$，使得对于所有足够大的 n， G_n 都有一个子群 H_n，满足 **交错群**(A) $\leq H_n^{([n]\setminus A)}$，其中 H_n 的某个轨道 A 的大小为 $|A| \geq cn$。

利用这个引理，可以证明：

▶**定理 75**。 设 $k \in \mathbb{N}$ 为一个常数，且 $(G_n)_{n\in\mathbb{N}}$ 为一族群，使得$G_n \leq$**对称群**$_n$，并且对所有足够大的 n，都有 [**对称群**$_n$： G_n] $\leq 2^{nk}$。那么，$\mathbf{SP}_A(G_n)$ 中的单元素部分数至多以次线性速度增长。换言之：不存在常数 $0 < c \leq n$，使得对所有足够大的 n，都存在一个大小为 $|\Delta_n| \geq cn$ 的 $\Delta_n \subseteq [n]$，且 $\mathbf{SP}_A(G_n)$仅包含单元素部分。

证明概要。 令 $\Delta_n \subseteq [n]$ 为 $\mathbf{SP}_A(G_n)$ 中属于单元素部分的点集。为导出矛盾，我们假设 $|\Delta_n|$ 线性增长。接着考虑 G_n 在 Δ_n 上的作用，同时固定 Δ_n 之外的每个点。将 G_n 的这个子群记为 H_n。将引理 74 应用于 H_n，便会得到矛盾。可以证明 $[$**对称群**$(\Delta_n) : H_n] \leq 2^{nk}$，这与假设的 G_n 在**对称群**$_n$ 中的指数相同。因此，引理 74 蕴含 H_n 包含一个作用于线性大小轨道 A 上的交错群。然而，此时 A 会是 $\mathbf{SP}_A(G_n)$ 中的一个部分，这与 H_n 的置换域是单元素部分中的位置集合这一事实相矛盾。完整证明见附录。◀

8.2 高度对称电路中的输入位抵消

现在我们回到定理 68 的证明。交替支撑划分用于近似各门的稳定子群。对于一个门 $g \in V_{C_n}$，我们用 $\mathbf{SP}_A(g)$ 表示群的最粗交错支撑划分

$$\mathbf{Stab}_n(g) := \{\pi \in \mathbf{Sym}_n \mid \pi \text{ extends to an automorphism of } C_n \text{ that fixes } g\}.$$

这里，我们的意思是，π 延拓到的自同构中至少有一个会固定 g。可以看出，$\mathbf{Stab}_n(g)$ 确实是 $\mathbf{Sym}_n$ 的一个子群，因为它包含恒等置换，并且：如果 π、$\pi' \in \mathbf{Stab}_n(g)$，那么存在电路自同构 σ、σ'，它们 π、π' 延拓后满足 $\sigma(g) = \sigma' g = g$。因此，$\sigma \circ \sigma'$ 固定 g，并且是一个可以 $\pi \circ \pi'$延拓到的电路自同构。因此，$\mathbf{Stab}_n(g) \leq \mathbf{Sym}_n$。

重要的是，$\mathbf{Stab}_n(g) \leq \mathbf{Stab}(\mathbf{SP}_A(g))$（引理 73），因此 $\mathbf{Stab}_n(g)$ 中的每个置换都作用为 $\mathbf{SP}_A(g)$ 的各部分上的置换。门的自同构像的支撑划分可以通过将 $\mathbf{Sym}_n$ 中相应的置换应用于支撑划分来获得：

▶ **引理 76**。 设 g、σg 是 C_n中的两个门，且 $\sigma \in$ **交错群**(C_n)。设 $\pi \in$ **对称群**$_n$ 是一个可扩展为电路自同构 σ的置换。那么

$$\mathbf{SP}_A(\sigma g) = \pi(\mathbf{SP}_A(g)).$$

证明。 由引理 72，划分 $\pi\mathbf{SP}_A(g)$ 是群 π**稳定子**$_n(g)\pi^{-1}$的最粗交错支撑划分。成立 π**稳定子**$_n(g)\pi^{-1} =$**稳定子**$_n(\sigma g)$。◀

接下来，我们将形式化描述给定输入门 g 在电路中自行抵消的含义：

▶**引理 77**。 设 g 是异或电路 C的一个输入门。当且仅当从根到 g 的不同路径数量为奇数时，电路 C 才对输入门 g 敏感。

证明。 对 C中的门数进行归纳。若 g 是根，则只有一条路径，且输入决定输出。从根到 g 的路径数量为偶数的最小可能情形是 C 由一个根、两个子节点 h_1、h_2以及一个输入门 g 构成，其中该输入门同时是 h_1 和 h_2的子节点。显然，输入位在根处抵消。

对于归纳步骤，令 h_1、.....、h_m为根 r的子节点。令 p_i为从 h_i 到输入 g的不同路径数。根据归纳假设，h_i 的输出依赖于 g，当且仅当 p_i 为奇数（使用以 h_i为根的较小子电路对应的结论）。从 r 到 g 的不同路径数为 $\sum p_i$。当且仅当 p_i 中为奇数的个数为偶数时，该数量为偶数。

那么，输入 g 不会影响在 r 处计算出的值，因为只有 p_i为奇数的 h_i 才对 g敏感，而这些影响在 r 处相互抵消，因为这样的数量为偶数。如果 p_i 中为奇数的个数为奇数，那么 r 对 g敏感。◀

因此，我们的目标是证明，从根到每个标记有“过于平衡的边”的输入门之间的路径数量都是偶数，其中$\mathcal{H}_n$ 。接下来我们要证明的技术性定理如下。由此，结合引理 77，即可推出定理 68。

▶**定理 78.** 设$(C_n)_{n\in\mathbb{N}}$ 是一个具有定理 *68* 中所述性质的异或电路族。固定每个中的一个门 g_n ，并固定一个常数 $\varepsilon > 0$ ，使得$\mathbf{SP}_A(g_n)$至少包含两个大小为 $\geq \varepsilon \cdot n$ 的部分。

那么，对所有足够大的 n，从 C_n 的根到 g_n 的不同路径数量都是偶数。

证明思路与一种称为“瓶颈计数”的技巧略有相似。这种技巧曾用于证明复杂性中，以建立归结的下界。粗略地说，我们为电路中的每个门关联一个特定量，并且已知该量在根处必须很大，而在输入门处要小得多。此外，我们将证明，沿着从一个门到其父节点的方向移动时，这个量每次只能发生微小变化。换言之，这个量无法从叶节点处的低值“跳跃”到根处的高值，而必须经过电路中间的许多中间值。接着，我们将证明，某些中间值必然会出现在某些门上，而这些值意味着从根到该门的路径数量为偶数。

首先，介绍一个关于支撑划分（或一般划分）的观察。在大多数情况下，它们的轨道大小至少是二次的，除非该划分具有非常特殊的形状。

▶ 引理*79*。设 *P* 是 $[n]$ 的某个划分，其中 $n \geq 4$，并令 $Stab_n(P) \leq Alt_n$ 表示交错群中该划分的集合稳定子。那么，*P* 的轨道大小，即 $(1/2)n!/|Stab_n(P)|$，至少为 $\Omega(n^2)$，除非 *P* 具有以下形式之一：$P = \{[n]\}$。$P = \{\{s\}\ [n] \setminus \{s\}\}$，其中 $s \in [n]$。$P = \{\{s\} \mid s \in [n]\}$。

证明概要。在上述三种情形中，容易看出 P 的 Alt_n-轨道大小为 1 或 n （因为我们假设 n 足够大，使得 Alt_n 在 $[n]$ 上传递）。剩下要证明的是，如果 P 具有其他任何形式，则其轨道大小至少是二次的。在这种情况下，P 必须包含某个大小为 $|P| \geq 2$ 的部分 P，其在 $[n]$ 中的补集大小也是 ≥ 2。由于 Alt_n 在 $[n]$ 的子集上是传递的（对于每个固定的子集大小），部分 P 有 $\binom{n}{|P|}$ 个不同的 Alt_n-像，而这属于 $\Omega(n^2)$。如果 $|P| > n/2$，那么结论即得，因为任何不将 P 映射到自身的置换都不属于 $\mathrm{Stab}_n(P)$，因此 P 的 Alt_n-轨道$_n$ 至少与所声称的一样大。否则，如果 $|P| \leq n/2$，那么$|\mathrm{Stab}_n(P)| \leq (1/2) \cdot k! \cdot (|P|!)^k \cdot (n - k|P|)!$，其中 k 是 P 中大小为 $|P|$ 的部分数。可以证明，该式在 $k = n/|P|$ 或 $k = 1$ 时达到最大值。现在只需利用轨道 - 稳定子定理计算轨道大小的一个合适下界即可。◀

结合我们关于父节点和子节点的轨道大小为$\mathcal{O}(n)$的假设，这条引理将帮助我们理清父门和子门的支撑划分之间的相互作用。现在，我们按照上文所述，定义与每个门相关联的量。实际上，这个量更确切地说是一个向量，我们称之为大小剖面 （即支撑划分的大小剖面）。它在对称性下保持不变，因此我们定义这一度量时并不针对

单个门，而是针对它们各自的整个轨道。对于门 $g \in V_{C_n}$，我们用 $[g]$ 表示它在 V_{C_n}中的 $\mathbf{Aut}(C_n)$轨道。大小剖面 是一个映射 $\zeta : \mathbb{N} \longrightarrow \mathbb{N}$。对于轨道 $[g]$，我们定义$\zeta[g] : \mathbb{N} \longrightarrow \mathbb{N}$ 如下：

$$\zeta[g](i) := |\{P \in \mathbf{SP}_A(g) \mid |P| = i\}|.$$

根据引理 76，此定义确实与轨道代表元 g的选取无关。请注意，正如我们先前所说，电路根节点和输入门处的度量 ζ 差异很大。对于根节点 r， $\zeta[r](n) = 1$，且对所有 $i < n$， $\zeta[r](i) = 0$。这是因为根据假设，我们的电路在 **对称群**$_n$ 中的所有置换作用下均不变，因此根节点被所有置换稳定，所以其最粗交错支撑划分只有一个大的部分。相比之下，对于输入门，我们知道其支撑划分总是有两部分：如果某个输入门标记为一条超立方体边，例如 $\{0^a 1^{n-a}, 0^{a-1}1^{n-a+1}\}$，那么它的支撑划分就是 $\{\{1, ..., a-1\}, \{a\}, \{a+1, ..., n\}\}$。除非 a 或 b 非常小，否则这个划分有两个大的部分。我们将证明，沿着电路的每一层，门的大小剖面不会发生太大变化；例如，沿电路向上移动一层时，最大的部分会增大一，而另一个部分会减小一。因此，在电路中间，我们必定会遇到支撑划分中大小各异的多个部分，之后才能到达根节点处的支撑划分 $\{[n]\}$。尤其是，我们会在某些门中遇到大小为偶数的部分，而一旦如此，路径数或多或少就会是偶数。下一个引理是我们证明的关键。它精确说明了子节点和父节点之间门的大小剖面可能有何差异。本质上，大部分的大小最多只能变化一。

▶ 引理 *80.* 设 $0 < \varepsilon < 1$ 为任意常数。设 g 为 C_n中的一个门， h 为 g的一个父节点。假设 $|$轨道$_{(g)}(h)| \in O(n)$ 且 $|$轨道$_{(h)}(g)| \in O(n)$。令 $\Delta : \{m \in \mathbb{N} \mid m \geq \varepsilon \cdot n\} \longrightarrow \mathbb{N}$为如下定义的函数： $\Delta(s) := \zeta[h](s) - \zeta[g](s)$。对于所有充分大的 $n \in \mathbb{N}$ 以及每个$s \geq \varepsilon \cdot n$，都有：

- $|\Delta(s)| \leq 2$。若 $\Delta(s) = 2$，则 $\Delta(s+1) = -1, \Delta(s-1) = -1$。若另外 s 为奇数，则 $|$轨道$_{(g)}(h)|$为偶数。若 $\Delta(s) = -2$，则 $\Delta(s+1) = 1, \Delta(s-1) = 1$。若另外 s 为偶数，则 $|$轨道$_{(g)}(h)|$为偶数。若 Δ 的值均不为 *2* 或 -2，则以下情形之一成立：若 $\Delta(s) = 1$，则 $\Delta(s-1) = -1$ 或 $\Delta(s+1) = -1$。若 s 为奇数且$\Delta(s+1) = -1$，则 $|$轨道$_{(g)}(h)|$为偶数。若 $\Delta(s) = -1$，则 $\Delta(s-1) = 1$ 或 $\Delta(s+1) = 1$。若 s 为偶数且$\Delta(s-1) = 1$，则 $|$轨道$_{(g)}(h)|$ 为偶数。若 $\Delta(s) \neq 0$，则对于上述情形中提及的值以外的所有其他 s'，都有$\Delta(s') = 0$。

证明。 令 $\mathbf{SP}^*_A(g) \subseteq \mathbf{SP}_A(g)$ 为大小为 $\geq \varepsilon \cdot n$ 的部分所构成的集合，并且 $\mathbf{SP}^*_A(h) \subseteq \mathbf{SP}(h)_A$ 为大小为 $\geq \varepsilon \cdot n - 1$ 在 $\mathbf{SP}_A(h)$ 中的部分。
断言： 存在一个双射 $\gamma : \mathbf{SP}^*_A(g) \longrightarrow \mathbf{SP}^*_A(h)$，使得：
(a) 对于每个 $Q \in \mathrm{SP}^*_A(g)$，都有 $|\gamma(Q) \cap Q| \geq |Q| - 1$。(b) 对于每个 $Q \in \mathrm{SP}^*_A(g)$，都有 $|\gamma(Q) \setminus Q| \leq 1$。(c) $Q \in \mathrm{SP}^*_A(g)$ 中至多有一个部分满足 $|\gamma(Q) \cap Q| = |Q| - 1$。(d) $Q \in \mathrm{SP}^*_A(g)$ 中至多有一个部分满足 $|\gamma(Q) \setminus Q| = 1$。



图4 这是 Q 和 $\gamma(Q)$ 可能存在的最极端差异：两者各自至多有一个元素未与另一部分共享。

断言的证明：通过定义 $\gamma(Q) \in \mathrm{SP}_A^*(h)$ 为与Q 交集尽可能大的部分，来构造 γ。这一定义良好，因为 $\mathrm{SP}_A(h)|_Q$只有两种可能的形式：它要么只包含一个部分，要么 $\mathrm{SP}_A(h)|_Q = \{\{s\}\ Q \setminus \{s\}\}$，其中$s \in Q$。其他所有情况都可由引理79和定理 75排除。这是因为根据假设，g 的父节点中只有 $O(n)$ 个属于 $\mathrm{Orbit}_{(g)}(h)$。因此，将 $\mathrm{SP}_A(h)$ 限制到 Q 上，记为 $\mathrm{SP}_A(h)|_Q$，在 $\mathrm{Alt}(Q)$ 作用下至多有 $O(n)$ 个像：具体而言，$\mathrm{Alt}(Q)$ 中的每个置换都可扩展为一个固定 g 的电路自同构，因为 Q 是 $\mathrm{SP}_A(g)$ 中的一个部分。此外，根据引理 76，$\mathrm{SP}_A(h)|_Q$ 的任意两个不同的 $\mathrm{Alt}(Q)$-像，都必须分别是 Q的两个不同父节点的支撑划分在 Q上的限制。因此，$\mathrm{Orbit}_{(g)}(h)$ 中的门数确实至少与 $\mathrm{SP}_A(h)|_Q$的 $\mathrm{Alt}(Q)$-轨道大小相同。只有当 $\mathrm{SP}_A(h)|_Q$ 仅由单元素集合构成、只有一个大部分，或是一个一对其余划分时，这个大小才可能为 $O(n)$（由引理79得出，此处还用到了$|Q| \in \Theta(n)$）。$\mathrm{SP}_A(h)|_Q$ 仅由单元素集合构成的情况不可能发生，因为 Q大小为线性，且根据定理 75，$\mathrm{SP}_A(h)$ 至多有 $o(n)$ 个单元素集合。因此，$\mathrm{SP}_A(h)|_Q$ 确实要么只包含一个部分，要么 $\mathrm{SP}_A(h)|_Q = \{\{s\}\ Q \setminus \{s\}\}$，其中$s \in Q$。由此，$\gamma(Q)$定义良好（并且 $\gamma(Q)\ \mathrm{SP} \in (_A)$ 中的每个部分大小都为 $\geq \varepsilon \cdot n - 1$）。

上述推理也直接证明了陈述（a）。陈述（b）可用类似方式得出，因为如果它不成立，那么 $\mathbf{SP}_A(g)|_{\gamma(Q)}$ 在 **交错群**$(\gamma(Q))$ 作用下将有 $\Omega(n^2)$ 个像（同样是由定理 75 和引理79 合并得出），从而导致 **轨道**$_{(h)}(g)$ 过大。

我们证明 γ 是单射：如果它不是单射，那么就存在某个 $P \in \mathbf{SP}_A^*(h)$ 和$Q_1, Q_2 \in \mathbf{SP}_A^*(g)$，使得 $|Q_1 \cap P| \geq |Q_1| - 1$ 和 $|Q_2 \cap P| \geq |Q_2| - 1$。这是不可能的，因为根据引理79，$\mathbf{SP}_A(g)|_P$ 在 **交错群**(P) 作用下有 $\Omega(n^2)$ 个自同构像，但 **交错群**(P) 固定了 h，因此 h 在 **轨道**$_{(h)}(g)$ 中有多于 $\mathcal{O}(n)$ 个子节点，这就产生了矛盾。

此外，γ是满射：假设存在一个大小为 $\geq g(n) - 1$ 的部分 $P \in \mathbf{SP}_A(h)$ 没有原像。那么 $\mathbf{SP}_A(g)|_P$必定由小于 $\varepsilon \cdot n$ 的部分组成。再者，根据引理79（同时利用 $\mathbf{SP}_A(g)$ 中单元素部分的数量是次线性的，因而根据定理 75 小于 $|P|$），$\mathbf{SP}_A(g)|_P$ 在 **交错群**(P) 作用下有 $\Omega(n^2)$ 个像。

如果陈述（c）不成立，那么将存在两个部分 $Q_1, Q_2 \in \mathbf{SP}_A^*(g)$，使得 $|\gamma(Q_i) \cap Q_i| = |Q_i| - 1$。那么 **交错群**$(Q_1) \times$ **交错群**(Q_2) 固定 g，但生成 $\mathbf{SP}_A(h)$ 的 $\Omega(n^2)$ 个彼此不同的自同构像。再者，$|\mathbf{Orbit}_{(g)}(h)|$ 大于 $\mathcal{O}(n)$，这与引理的假设相矛盾。

同样，陈述（d）也可以得到证明：如果它不成立，那么 h 在 $\mathbf{Orbit}_{(h)}(g)$ 中会有过多的子节点。这就证明了该断言。

现在结合该断言，我们可以看到有五种可能的情况：

1. $\gamma(Q) = Q$ 对于所有 $Q \in \mathbf{SP}_A^*(g)$。

2. 存在一个部分 $Q \in \mathrm{SP}_A^*(g)$，使得 $|\gamma(Q) \cap Q| = |Q| - 1$ 且 $\gamma(Q) \subseteq Q$；对于所有其他部分 Q'，$\gamma(Q') = Q'$。3. 存在一个部分 Q，满足 $|\gamma(Q) \setminus Q| = 1$ 且 $\gamma(Q) \supseteq Q$；对于所有其他部分 Q'，$\gamma(Q') = Q'$。4. 存在一个部分 Q，满足 $|\gamma(Q) \cap Q| = |Q| - 1$ 且 $|\gamma(Q) \setminus Q| = 1$。对于所有其他部分 Q'，$\gamma(Q') = Q'$。5. 存在一个部分 Q_1，满足 $|\gamma(Q_1) \cap Q_1| = |Q_1| - 1$（且 $\gamma(Q_1) \subseteq Q_1$），以及另一个部分 Q_2，满足 $|\gamma(Q_2) \setminus Q_2| = 1$（且 $Q_2 \subseteq \gamma(Q_2)$）；对于所有其他部分 Q'，$\gamma(Q') = Q'$。在情况 1 中，Δ-向量为零。在情况 2 中，我们有 $\Delta(|Q|) = -1$ 且 $\Delta(|Q| - 1) = 1$，并且 Δ 的所有其他条目均为零。在情况 3 中，我们有 $\Delta(|Q|) = -1$ 且 $\Delta(|Q| + 1) = 1$，并且 Δ 的所有其他条目均为零。在情况 4 中，Δ-向量为零。

在情形 5 中，我们需要区分几种情形。若 $|Q_1| = |Q_2|$，则 $\Delta(|Q_1|) = -2$和 $\Delta(|Q_1| - 1) = 1$，$\Delta(|Q_1| + 1) = 1$。若 $|Q_1| \neq |Q_2|$ 和 $|Q_1| - 1 \neq |Q_2| + 1$，则$\Delta(|Q_1|) = -1$，$\Delta(|Q_2|) = -1$，$\Delta(|Q_1| - 1) = 1$，$\Delta(|Q_2| + 1) = 1$。若 $|Q_1| = |Q_2| + 2$，则$\Delta(|Q_1|) = -1$，$\Delta(|Q_2|) = -1$，$\Delta(|Q_1| - 1) = 2$。

在情形 2 中，假设 $|Q|$ 为偶数。那么，$\mathrm{SP}_A(h)|_Q$ 在交错群 $\mathrm{Alt}(Q)$作用下有偶数个像（因为 $\mathrm{SP}_A(h)|_Q$ 由一个单元素部分和其余部分组成，而这个单元素可以在交错群 $\mathrm{Alt}(Q)$作用下映射到所有 $|Q|$ 个位置）。现在我们要论证，因此 $|\mathrm{Orbit}_{(g)}(h)|$必为偶数。令 $H(Q) \subseteq \mathrm{Orbit}_{(g)}(h)$为满足 $\mathrm{SP}_A(h')|_Q$ 由一个单元素部分和其余部分组成的父节点 h' 的集合。$|H(Q)|$ 是偶数：每个 $\pi \in \mathrm{Alt}(Q)$都可扩展为一个固定 g的 $\sigma \in \mathrm{Aut}(C_n)$。根据引理 76，这个 σ 将 g 的父节点 h 映射到 g 的另一个父节点，其 $\mathrm{SP}_A(\sigma h)|_Q = \pi(\mathrm{SP}_A(h))|_Q$。因此，$H(Q)$中每个元素在 $\mathrm{Alt}(Q)$下的轨道都是偶数；于是，H 可划分为交错群 $\mathrm{Alt}(Q)$下的轨道，且每个轨道都是偶数，所以 $|H(Q)|$是偶数。

现在，如果 $H(Q)$ 等于整个集合 $\mathrm{Orbit}_{(g)}(h)$，那么我们就完成了。否则，$\mathrm{Orbit}_{(g)}(h)$ 中包含一些门，它们在 Q 上的支撑划分不会分成一个单元素集和其余部分。设 $h' \in \mathrm{Orbit}_{(g)}(h)$ 是这样一个门。必定存在一个置换 $\pi \in \mathrm{Sym}_n$，它可扩展为电路自同构 σ，将 h 映射到 h'，并固定 g。因此，相应的 π 必须将划分 $\mathrm{SP}_A(g)$ 作为整体稳定下来，并将 $\mathrm{SP}_A(h)$ 映射到 $\mathrm{SP}_A(h')$。于是，$\pi(Q) \in \mathrm{SP}_A(g)$ 是一个部分；当我们将上述推理应用于 g 和 $h' = \sigma(h)$ 时，这里同样会出现情形 2。接着，我们可以将 $H(\pi Q) \subseteq \mathrm{Orbit}_{(g)}(h)$ 定义为所有父节点构成的集合，这些父节点在 πQ 上的支撑划分分成一个单元素集和其余部分；由此可得，$|H(\pi Q)|$ 是偶数。总之，通过这一推理，我们看到 $\mathrm{Orbit}_{(g)}(h)$ 被划分为若干偶数大小的集合 $H(\pi Q)$；对于所有可扩展为电路自同构、且固定 g 并置换其父节点的 $\pi \in \mathrm{Sym}_n$，这些集合都成立。因此总的来说，$|\mathrm{Orbit}_{(g)}(h)|$ 是偶数。

同样，假设在情形 5 中，$|Q_1|$ 是偶数。那么，同样的论证表明，$|\textbf{轨道}_{(g)}(h)|$ 是偶数。由此可直接推出该引理。◀

▶ **推论 81**。令 $0 < \varepsilon < 1$ 为任意常数。设 g 是 C_n 中的一个门（当n足够大时），h 是 g 的一个父节点。假设 $|\textbf{轨道}_{(g)}(h)| \in O(n)$ 且 $|\textbf{轨道}_{(h)}(g)| \in O(n)$，并且$|\textbf{轨道}_{(g)}(h)|$是奇数。

令 s 与 $\varepsilon \cdot n \leq s < n$ 为一个偶自然数。则

$$\sum_{i \geq s} \zeta[h](i) \geq \sum_{i \geq s} \zeta[g](i)$$

证明。 根据引理 80，对于任意 $i > s$，每当 $\zeta[h](i) < \zeta[g](i)$时，在求和 $\sum_{i\geq s}\zeta[h](i)$中，$\zeta[h](j)$ 的其他取值会抵消这一项。
现在只需考虑 $\zeta[h](s) < \zeta[g](s)$ 的情况。由于我们假设 $|\mathbf{Orbit}_{(g)}(h)|$ 为奇数，而 s 为偶数，引理 80 蕴含 $\zeta[h](s) = \zeta[g](s) - 1$，且 $\zeta[h](s+1) = \zeta[g](s+1) + 1$。因此，和 $\sum_{i\geq s}\zeta[h](i)$ 不可能严格小于 $\sum_{i\geq s}\zeta[g](i)$。◀

直观地说，这意味着：如果从根到某个门 g 的某条路径上，下一个父节点门在其子节点的稳定子群中的轨道大小始终为奇数，那么支撑划分中大部分的数量沿着朝向根的路径只能增加。这将使我们能够证明每条路径上都必然出现偶数轨道。这意味着，该路径及其轨道会在异或计算中自行抵消。

当我们考察从电路的根 r 到某个门 g 的路径 $P = (r = h_1, h_2, \ldots\ldots, g)$ 时，可以为它关联一个轨道剖面 $\Omega(P)$。这个轨道剖面指出，对于路径上的每个门 h_i，其前驱 h_{i-1} 属于哪个轨道。这里的轨道仍指**轨道**$_{(h_i)}(h_{i-1})$，因此我们指的是相对于固定 h_i 的对称群 **对称群**$_n$，将 h_i 的父节点划分为各个轨道所得的划分。路径的轨道剖面并不旨在唯一描述该路径；相反，我们希望多条路径共享同一个轨道剖面——从某种意义上说，我们希望轨道剖面描述的是将相应轨道**轨道**$_{(h_i)}(h_{i-1})$约去后得到的“路径”。我们必须证明这确实有意义：

▶**引理 82**。 设 g 是一个门，h 是 g 的一个父节点。设 g' 是另一个门，并且存在一个 $\sigma \in$ **自同构**(C) 满足 $g' = \sigma(g)$。在针对 $h' \in E_C g'$、将 $E_C g'$ 划分为轨道**轨道**$_{(g')}(h')$的划分中，存在唯一一个轨道**轨道**$_{(g')}(h')$，使得轨道$_{(g)}(h)$ 可以通过**自同构**(C)映射到该轨道。

证明。首先，显然，每个将 g 映射到 g' 的 $\sigma \in$Aut(C)，都必须将轨道 Orbit$_{(g)}(h)$ 映射到某个轨道 Orbit$_{(g')}(h')$，其中 $h' \in E_C g'$。现在我们证明，不可能存在两个不同的 Orbit$_{(g')}(h')$ 和 Orbit$_{(g')}(h'')$，使得 Orbit$_{(g)}(h)$ 可以映射到它们。反设存在 $\sigma, \sigma' \in$ Aut(C)，满足 $\sigma(g) = \sigma'(g) = g'$，且 $\sigma($Orbit$_{(g)}(h)) =$ Orbit$_{(g')}(h')$，以及 $\sigma'($Orbit$_{(g)}(h)) =$ Orbit$_{(g')}(h'')$。那么，$\sigma' \circ \sigma^{-1}$ 会将 Orbit$_{(g')}(h')$ 映射到 Orbit$_{(g')}(h'')$，同时固定 g'。因此，Orbit$_{(g')}(h')$ =Orbit$_{(g')}(h'')$，这与这些轨道彼此不同相矛盾。◀

因此，对于 C 中的任意门 g，以及 g 的任意父节点 h，我们可以定义

$$\mathbf{Orbit}(\mathbf{Orbit}_{(g)}(h)) := \{\sigma(\mathbf{Orbit}_{(g)}(h)) \mid \sigma \in \mathbf{Aut}(C)\},$$

并且，对于每个满足 $=\{\sigma(g) \mid \sigma \in \mathbf{Aut}(C)\}$ 的 $g' \in$ **轨道**(g)，该轨道的轨道恰好包含一个**轨道**$_{(g')}(h')$。路径 $P = (r = h_1, h_2, \ldots\ldots, h_\ell = g)$ 的轨道轮廓 $\Omega(P)$ 定义为

$$\Omega(P) : = (\textbf{轨道}(\textbf{轨道}_{(h_\ell)}(h_{\ell-1})), \textbf{轨道}(\textbf{轨道}_{(h_{\ell-1})}(h_{\ell-2})) \ldots\ldots, \textbf{轨道}(\textbf{轨道}_{(h_2)}(h_1)))。$$

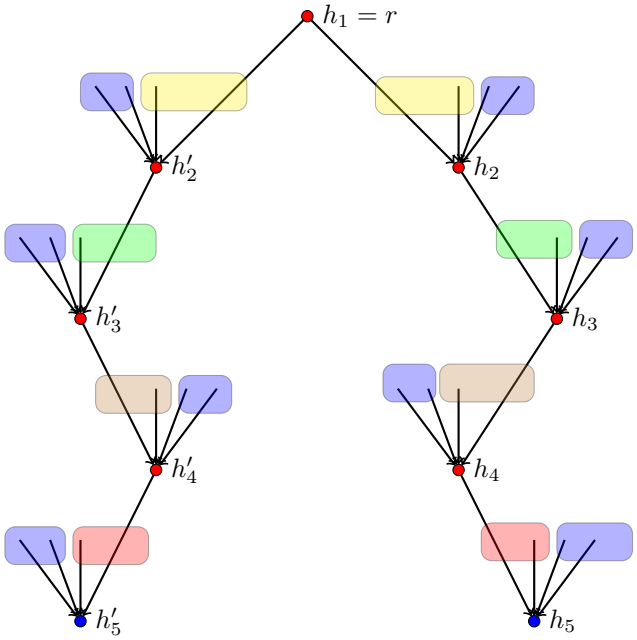

图 5 颜色表示每个父节点集合划分为轨道后的情况。颜色相同的轨道属于同一个轨道的轨道。因此，图中两条路径的轨道剖面为“红、棕、绿、黄”，且这两条路径可由该电路的一个自同构相互映射。

▶ **引理 83**。 设 $P = (r = h_1, ..., h_\ell = g)$ 是从 r 到 g 的 C_n中的一条路径。从 r 到 g 且轨道剖面为 $\Omega(P)$ 的 C_n 中的路径数恰好为

$$\prod_{2 \le i \le \ell} |\mathbf{Orbit}_{(h_i)}(h_{i-1})|$$

证明。我们从 $g = h_\ell$ 反向走向 r，并计数构造一条轨道剖面为 $\Omega(P)$ 的路径有多少种方式。起初，有 $|\mathrm{Orbit}_{(h_\ell)}(h_{\ell-1})|$ 种选择，可以选取一个前驱 g，使其属于 $\Omega(P)$ 所要求的轨道。设我们选择的 g 的前驱为 h。从这里出发，我们有 $|\mathrm{Orbit}_{(h_{\ell-1})}(h_{\ell-2})|$ 个前驱，可以继续前进，同时满足 $\Omega(P)$。为此，我们使用引理 82：无论为 h 选择哪个门，它都属于 $\mathrm{Orbit}(h_{\ell-1})$。因此，根据引理 82，在 $\{\mathrm{Orbit}_{(h)}(h') \mid h' \in E_C h\}$ 中，存在唯一一个 $\mathrm{Orbit}_{(h)}(h')$，它同时也是 $\mathrm{Orbit}(\mathrm{Orbit}_{(h_{\ell-1})}(h_{\ell-2}))$ 的成员。我们可以从这个 $\mathrm{Orbit}_{(h)}(h')$ 中选择路径上的下一个门，并且该轨道的大小与 $\mathrm{Orbit}_{(h_{\ell-1})}(h_{\ell-2})$ 相同。因此，到目前为止，我们有 $|\mathrm{Orbit}_{(h_\ell)}(h_{\ell-1})| \cdot |\mathrm{Orbit}_{(h_{\ell-1})}(h_{\ell-2})|$ 种可能，能够以符合轨道剖面 $\Omega(P)$ 的方式，从 g 朝 r 前进两步。我们以相同方式继续计数，直到到达根节点，从而得到引理中所述的路径数。◀

▶ **引理 84**。 设 $0 < \varepsilon \le 1$。对每个 n，固定 C_n 中的一个门 g_n，使得 $\mathbf{SP}_A(g_n)$ 至少有两个大小为 $\ge \varepsilon n$ 的部分。对于从 C_n 的根到 g_n 的任意路径 P 可能具有的每个轨道剖面 $\Omega(P)$，从根到 g_n 且具有恰好该轨道剖面的不同路径数量为偶数。

证明。 固定一条路径 P 从根到 g_n 在 C_n 以及相应的轨道剖面 $\Omega(P)$。我们将证明，从根到 g_n且具有轨道剖面 $\Omega(P)$的不同路径有偶数条。

根据关于 g_n 的假设，对于 $s_1, s_2 \geq \varepsilon \cdot n$，有 $\zeta[g_n](s_1) \geq 1$ 且 $\zeta[g_n](s_2) \geq 1$。对于根 r_n，对于每个 $s \neq n$，有 $\zeta[r_n](n) = 1$ 且 $\zeta[r_n](s) = 0$（因为所有置换都固定根，置换群为 Sym_n）。因此，大小剖面 ζ 必须沿着从 g 到 r 的路径 P 发生变化。令 s 为一个偶自然数，使得 $\varepsilon \cdot n \leq s \leq \min\{s_1, s_2\}$。这样的数总是存在的，因为否则我们只需将 ε 稍微调小一些，使得 $\min\{s_1, s_2\} - 1 \geq \varepsilon \cdot n$。

假设存在矛盾，即对于每个门 $h \in P$，其在路径 P上的前驱 h' 都满足：$|\mathbf{轨道}^{(h)}(h')|$ 是奇数。然后沿路径 P归纳应用推论 81，可得对于每个 $h \in P$，$\sum_{i \geq s} \zeta[h](i) \geq \sum_{i \geq s} \zeta[g_n](i) \geq 2$。这与 $\sum_{i \geq s} \zeta[r_n](i) = 1$这一事实矛盾。

这表明路径 P 上必定存在某个 h，使得 h的前驱 h' 满足：$|\mathbf{轨道}^{(h)}(h')|$ 是偶数。于是，从 r_n 到 g_n 且具有配置 $\Omega(P)$ 的路径总数为偶数，因为根据引理 83，这个数是一个乘积，其中包含偶数 $|\mathbf{轨道}^{(h)}(h')|$。◀

由此可得我们的主要技术定理：不仅具有给定轨道配置的路径数是偶数，从 r 到 g 的路径总数也是偶数：

定理 *78* 的证明：从 r_n 到 g_n 的每条路径恰好有一个轨道剖面。因此，从 r_n 到 g_n 的路径数就是

$$\sum_{\Omega \text{ an orbit profile of a path from } r_n \text{ to } g_n} \#(\Omega),$$

其中，#(Ω) 表示具有轨道剖面 Ω 且终止于 g_n 的路径数。根据引理 84，该和式中的所有被加数都是偶数。◀

最后，我们总结一下定理 68（“完全对称异或电路对所有输入都不敏感，唯一例外是那些标记为极不平衡二进制字符串的输入”）为何可以由定理 78 推出。

定理 *68* 的证明：
固定任意 $\varepsilon > 0$。设 g_n 是 C_n 的一个输入门，其标记为超立方体边 $\ell(g_n) = \{0^a 1^{n-a}, 0^{a-1}1^{n-a+1}\}$，满足 $a \geq \varepsilon n$ 和 $n - a \geq \varepsilon n$。容易看出，$\mathbf{SP}_A(g_n) = \{\{1, \ldots, a-1\}, \{a\}, \{a+1, \ldots, n\}\}$。其中包含两个大小为 $\geq \varepsilon n$ 的部分，因此定理 78 适用，从根到 g_n 的路径数为偶数。根据引理 77，电路 C_n 对输入门 g_n 不敏感。◀

9 结论与未来研究

我们根据无选择算法在 CFI 查询中必然激活的遗传有限集的性质，定义了不同类别的无选择算法。目前已知的三种算法均具有超对称性，同时也是 CFI-对称的。CFI 对称性的一种推广是对称基性质（定义 56）。我们证明，具有超对称性且同时满足 CFI-对称性或对称基性质的对象，可以以一种有意义的方式转化为多项式规模的对称异或电路。

我们利用这一电路构造，在证明不存在定义无序超立方体上的 CFI 查询的 CFI 对称 CPT 算法方面取得了进展：若此类算法存在，就意味着存在一个对称异或电路族，其大小和轨道大小都是关于 n 维超立方体大小（即 2^n）的多项式，并且

该电路族能够计算 $\Omega(2^n/n^{1.5})$ 个输入位的异或，且其扇入度有界于$\mathcal{O}(n)$（即关于超立方体大小的对数级）。我们的目标是证明此类电路族不存在。虽然尚未完全实现这一目标，但我们至少发现了电路还需满足一些有趣的附加限制，而这些限制合在一起无法满足：如果假设每个电路的轨道大小恰好为 1（而不只是多项式），并且不再采用扇入维数$\mathcal{O}(n)$ 上界，而是要求每个门的子节点数和父节点数（按该门稳定子中的每个轨道分别计算）均有$\mathcal{O}(n)$ 上界，那么这些电路就无法计算 $\Omega(2^n/n^{1.5})$ 个输入位的异或。因此，如果超立方体 CFI 查询确实存在 CFI 对称算法，那么相应的电路族要么具有 >1 轨道大小，要么必须违反按轨道计算的子门数或父门数上界。由此，下一步应当尝试将我们的下界技术推广到更一般的情形。这个目标似乎有望实现，但其中存在一些技术难题：

第一个问题是，如何论证轨道大小并非恰好为 1、而是被 2^n 中的某个多项式所界定的电路。此时，根的支撑划分不一定只由一个部分组成，而可能包含更多部分（不过，如果部分太多，轨道大小就会大于 2^{nk}，这是不允许的）。我们的论证利用了这样一个事实：沿着从输入门到根的路径，支撑划分中的线性大小部分的数量不可能减少，除非在某个位置父节点的数量为偶数。但如果根的支撑划分现在可以包含多个线性大小部分，那么这就不再能导出矛盾。不过，也许通过对电路进行更加细致的分析，我们仍然可以在这种情况下恢复原有论证。我们的关键技术引理（引理 80）实际上比证明中所需的更强，因为它给出了若干种情形，在这些情形下，门的父节点数量必须为偶数。因此，如果禁止出现偶数个父节点，那么沿着一条路径，支撑划分的大小剖面能够发生变化的方式就非常有限。但我们当然可以预期，并非所有门都具有相同的大小剖面，因此某些地方必然会发生变化，而这又会导致出现偶数个父节点。只是目前尚不清楚如何将这一点转化为形式化论证。

第二个问题涉及我们从定理 31 得到的扇入维数对数界，与上一章节中施加的按轨道计算的扇入界和扇出界之间的关系。目前，我们还不知道其中一个界是否蕴含另一个界。父节点数量的界可能与扇入维数没有直接关系，但子节点数量的界或许有关。如果扇入维数的对数界能够蕴含每个轨道的子节点数量为对数级，那么我们的下界就能涵盖这一点。如果 $\mathbf{Orbit}^{(h)}(g) \subseteq hE_C$中的门都具有彼此不同的敏感集$\mathcal{X}(g')$，并且这些敏感集作为 $\mathbb{F}_2^E$ 中的向量也都线性无关，那么 $|\mathbf{Orbit}^{(h)}(g)|$ 确实至多等于扇入维数。但对于所有 $g' \in \mathbf{Orbit}^{(h)}(g)$，我们尚不清楚应如何推理这些集合$\mathcal{X}(g')$的性质。

为了去除门的轨道逐点父节点数的$\mathcal{O}(n)$界，我们有一个粗略的想法。具体来说，由于我们的电路是单根的，越靠近根，其层应该越窄。因此，似乎可以认为，在足够靠近根的位置，每个门确实只有有界数量的父节点；否则，电路就会变宽。我们的偶数路径定理（定理 78）的一个优点是，它可以应用于电路中的任意门，而不仅仅是输入门。因此，我们可以把注意力集中在电路最顶端的部分；在那里，各层只会越来越窄，并且可以证明这一顶端部分中的所有路径都会相互抵消。这样就足以证明该电路对足够多的输入位不敏感。

总而言之，我们感觉偶路径技术潜力更大，也可能适用于限制更少的电路类，甚至可能适用于所有 满足超立方体 CFI 问题存在 CFI 对称算法所需性质的电路。尤其是，我们或许也能改进群论定理 75；该定理指出，交替支撑划分不可能有线性数量的单元素部分。对指数为 $\leq 2^{nk}$ 的群的交替支撑划分进行更细致的研究，可能会有所帮助。因此，我们似乎还没有达到该技术的极限，但进一步取得进展在技术上可能会非常困难。

一个值得指导后续研究的具体问题是，尝试证明不存在满足定理 67 条件的树状电路。我们的结果间接表明，不存在相对于超立方体自同构轨道大小为 1、且扇入度为对数级的树状电路：这类电路会满足定理 68 的所有性质，并且由于树状电路中不会发生抵消，它们对所有输入门都敏感。这将与定理 68 矛盾。仍待解决的问题是，轨道大小大于 1 或次数限制较少的树状电路是否满足定理 67 的条件。我们希望答案是否定的。

最后，探究我们在此提出的新下界技术在多大程度上也能应用于其他情形，或许会很有意思。正如引言中所述，研究对称电路的下界似乎也是分离代数复杂性类 VNP 和 VP 的一种有前景的方法。Dawar 和 Wilsenach [13, 11] 已经证明了计算行列式和永久式多项式的对称算术电路的下界。他们提出了一个问题：这些下界在较弱的对称群下能在多大程度上得到改进；或许我们的技术可以为此加以调整。当然，偶数路径定理可能只适用于完全由异或门构成的电路；但关于各层电路的交替支撑划分不会有太大变化这一结论，或许能带来新的见解。与 [1, 12, 13, 11] 相比，我们这项技术的一项新颖之处在于，它不依赖任何“支撑定理”。支撑定理是以往所有这些研究的关键组成部分，通常指出，高度对称电路中的任意门都由置换域中的常数个元素支撑。对于我们在此研究的具有超立方体对称性、大小为多项式的电路，我们认为这种强形式的支撑定理并不成立。因此，通过交替支撑划分展开的方法，或许也能为研究较弱的对称群开辟新的视角。

参考文献

1 Matthew Anderson和Anuj Dawar。关于对称电路与不动点逻辑。 *Theory ofComputing Systems*，60(3):521–551，2017。2 Albert Atserias、Andrei Bulatov和Anuj Dawar。仿射方程组与计数无穷逻辑。 *Theoretical Computer Science*，410(18):1666–1683，2009。3 László Babai、Peter J Cameron和Péter P Pálfy。关于非阿贝尔合成因子受限的本原群的阶。 *Journal of Algebra*，79(1):161–168，1982。4 László Babai。准多项式时间内的图同构。2015。网址：`https://arxiv.org/abs/1512.03547`， `doi:10.48550/ARXIV.1512.03547`。5 Andreas Blass、Yuri Gurevich和Saharon Shelah。无选择多项式时间。 *Annals ofPure and Applied Logic*，100(1-3):141–187，1999。

6 J. Cai、M. Fürer和N. Immerman。图识别所需变量数的最优下界。Combinatorica，12:389–410，1992。7 Anuj Dawar。带计数的定点逻辑的本质与威力。ACM SIGLOG News，2(1):8–21，2015。8 Anuj Dawar、Erich Grädel和Wied Pakusa。同构的近似与带线性代数算子的逻辑。载于Christel Baier、Ioannis Chatzigiannakis、Paola Flocchini和Stefano Leonardi编，第46届自动机、语言与编程国际研讨会（ICALP 2019），第132卷《莱布尼茨国际信息学会议录》（LIPIcs），第112:1–112:14页，德国达格施图尔，2019。Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik。网址：http://drops.dagstuhl.de/opus/volltexte/2019/10688，doi:10.4230/LIPIcs.ICALP.2019.112。9 Anuj Dawar、Erich Grädel和Moritz Lichter。可逆映射等价关系的局限。逻辑与计算杂志，2022年9月。网址：https://academic.oup.com/logcom/advance-article/doi/10.1093/logcom/exac058/6687793?guestAccessKey=7349c158-be02-4116-815a-840ac7880a03，doi:10.1093/logcom/exac058。10 Anuj Dawar、David Richerby和Benjamin Rossman。无选择多项式时间、计数与Cai–Fürer–Immerman图。Annals of Pure and Applied Logic，152(1-3):31–50，2008。11 Anuj Dawar和Gregory Wilsenach。对称算术电路。载于Artur Czumaj、Anuj Dawar和Emanuela Merelli编，第47届自动机、语言与编程国际研讨会（ICALP 2020），第168卷《莱布尼茨国际信息学会议录》（LIPIcs），第36:1–36:18页，德国达格施图尔，2020。Schloss Dagstuhl–Leibniz-Zentrum für Informatik。网址：https://drops.dagstuhl.de/opus/volltexte/2020/12443，doi:10.4230/LIPIcs.ICALP.2020.36。12 Anuj Dawar和Gregory Wilsenach。秩逻辑的对称电路。ACM计算逻辑汇刊（TOCL），23(1):1–35，2021。13 Anuj Dawar和Gregory Wilsenach。行列式的对称电路下界。载于Mark Braverman编，第13届理论计算机科学创新大会（ITCS 2022），第215卷《莱布尼茨国际信息学会议录》（LIPIcs），第52:1–52:22页，德国达格施图尔，2022。Schloss Dagstuhl–Leibniz-Zentrum für Informatik。网址：https://drops.dagstuhl.de/opus/volltexte/2022/15648,doi:10.4230/LIPIcs.ITCS.2022.52。14 John Dixon和Brian Mortimer。置换群。Springer，纽约，1996。15 Luca Donetti、Franco Neri和Miguel A Muñ oz。最优网络拓扑：扩展图、笼图、拉马努金图、纠缠网络及其他。统计力学杂志：理论与实验，2006(08):P08007–P08007，2006年8月。网址：https://doi.org/10.1088%2F1742-5468%2F2006%2F08%2Fp08007，doi:10.1088/1742-5468/2006/08/p08007。16 Stanley F Florkowski III。超立方体的谱图论。技术报告，美国海军研究生院（加州蒙特雷），2008。17 E. Grädel、W. Pakusa、S. Schalthöfer和L. Kaiser。用一阶解释刻画无选择多项式时间。载于第30届年度ACM/IEEE计算机科学逻辑研讨会论文集，第677–688页，2015。18 Erich Grädel和Martin Grohe。多项式时间是否无选择？载于《逻辑与计算领域 II》，第193–209页。Springer，2015。19 Erich Grädel和Martin Otto。有限结构上带计数的归纳可定义性。载于《计算机科学逻辑：第六届研讨会，CSL'92，意大利圣米尼亚托，1992年9月28日至10月2日，精选论文 6》，第231–247页。Springer，1993。20 Ronald L. Graham、Donald E. Knuth和Oren Patashnik。具体数学。Addison-Wesley，第2版，1994。21 Martin Grohe。寻找刻画 PTIME 的逻辑。载于2008年第23届年度IEEE计算机科学逻辑研讨会，第267–271页。IEEE，2008。 doi:10.1109/LICS.2008.11。

22 Frank Harary。超立方体的自同构群。J. Univers. Comput. Sci., 6(1):136–138, 2000。23 William He 和 Benjamin Rossman。置换乘积的对称公式，2022。URL：https://arxiv.org/abs/2211.15520。24 Lauri Hella。多项式时间中的逻辑层级。I nformation and Computation, 129(1):1–19, 1996。25 Neil Immerman 和 Eric Lander。描述图：图规范化的一阶方法。载于《复杂性理论回顾》，第 59–81 页。Springer，1990。26 Moritz Lichter。《将秩逻辑与多项式时间分离》。J. ACM，2022 年 11 月。URL：https://doi.org/10.1145/3572918。27 Moritz Lichter。带计数的定点逻辑中的见证对称选择与解释，2022。URL：https://arxiv.org/abs/2210.07869。28 Moritz Lichter 和 Pascal Schweitzer。带见证对称选择的无选择多项式时间。LICS '22。计算机协会，2022。URL：https://doi.org/10.1145/3531130.3533348。29 Benedikt Pago。无选择计算与对称性：可定义性的局限。载于 Christel Baier 和 Jean Goubault-Larrecq 编，《第 29 届 EACSL计算机科学逻辑年会（CSL 2021）》，第 183 卷《莱布尼茨国际信息学会议录（LIPIcs）》，第 33:1–33:21 页，德国达格施图尔，2021。达格施图尔城堡–莱布尼茨信息学中心。URL：https://drops.dagstuhl.de/opus/volltexte/2021/13467,doi:10.4230/LIPIcs.CSL.2021.33。30 Wied Pakusa。线性方程组与多项式时间逻辑刻画的探索。博士论文，亚琛工业大学，2015。31 Wied Pakusa、Benedikt Pago、Martin Grohe 和 Erich Grädel。命题证明复杂性的有限模型论视角。Logical Methods in Computer Science, 15, 2019。32 Wied Pakusa、Svenja Schalthöfer 和 Erkal Selman。Cai-Fürer-Immerman问题在无选择多项式时间中的可定义性。ACM计算逻辑汇刊（TOCL），19(2):1–27, 2018。 doi:10.1145/3154456。33 Harvey Rose。级数、Jordan–Hölder定理与扩张问题。载于《有限群教程》，第 187–207 页。Springer London，伦敦，2009。 doi:10.1007/978-1-84882-889-6 9._34 Benjamin Rossman。无选择计算与对称性。载于《逻辑与计算领域》，第 565–580 页。Springer，2010。35 Benjamin Rossman。子空间不变 AC^0 公式。Logical Methods in Computer Science, 15, 2019。36 Svenja Schalthöfer。无选择计算与逻辑。博士论文，亚琛工业大学，2020。37 L. Sunil Chandran 和 T. Kavitha。超立方体的树宽和路径宽。离散数学，306(3):359–365, 2006。URL：https://www.sciencedirect.com/science/article/pii/S0012365X05006102, doi:https://doi.org/10.1016/j.disc.2005.12.011。

10 附录

10.1 第 6 节中归纳矩阵构造的正确性

▶**引理 43**。设 $[x'] \in \Omega[x]$ 和 $[y'] \in C[x']$。存在一个同态 h'，其将 $g_{[y']}$(**稳定子**$_G([y'] \cap x')$) $\leq$ **对称群** $(I_{[y']})$ 映入 $N[x'][y']$ 的行指标集上的对称群，并且对每个 $\sigma \in g_{[y']}$(**稳定子** $_G([y'] \cap x')$)，均有 $(h'(\sigma)\ \sigma)(N[x'][y']) = N[x'][y']$。

证明。令 $[y] \in C[x]$ 为 $\Omega[y']$ 的初始元。令 $\pi_{[x'][y']} \in \mathrm{Stab}_G(\mu)$ 为用于从 $N[x][y]$ 定义 $N[x'][y']$ 的置换。对于矩阵 $N[x][y]$，根据矩阵的定义，存在这样的同态 $h : g_{[y]}(\mathrm{Stab}_G([y] \cap x)) \longrightarrow \mathrm{Sym}(J_{[x][y]})$。我们按如下方式定义所需的同态 $h' : g_{[y']}(\mathrm{Stab}_G([y'] \cap x')) \longrightarrow \mathrm{Sym}(J_{[x'][y']})$。对于每个 $\pi \in \mathrm{Stab}_G([y'] \cap x')$ 以及每个 $(i, [x'], [y']) \in J_{[x'][y']}$，令

$$h'(g_{[y']}(\pi))(i, [x'], [y']) := (j, [x'], [y']),$$

其中，j 是满足以下条件的数

$$h(g_{[y]}(\pi^{-1}_{[x'][y']} \circ \pi \circ \pi_{[x'][y']}))(i, [x], [y]) = (j, [x], [y]).$$

对于每个 $\pi \in$ **稳定子**$_G([y'] \cap x')$，$h'(g_{[y']}(\pi))$ 确实是 **对称群**$(J_{[x'][y']})$ 中的一个置换，因为 $N[x][y]$ 和 $N[x'][y']$ 的行数相同（并且指标集 $J_{[x][y]}$ 和 $J_{[x'][y']}$ 仅在指标三元组的第二项和第三项上有所不同），且 $(\pi^{-1}_{[x'][y']} \circ \pi \circ \pi_{[x'][y']}) \in$ **稳定子**$_G([y] \cap x)$，所以 $h(g_{[y]}(\pi^{-1}_{[x'][y']} \circ \pi \circ \pi_{[x'][y']}))$ 是 $N[x][y]$ 各行上的一个置换。

h' 是群同态这一事实直接由 h 是群同态这一事实推出；此外，因为 $(\pi^{-1}_{[x'][y']} \circ \pi_1 \circ \pi_{[x'][y']}) \circ (\pi^{-1}_{[x'][y']} \circ \pi_2 \circ \pi_{[x'][y']}) = \pi_1 \circ \pi_2$。

最后，我们必须证明，对于每个 $\sigma \in g_{[y']}$(稳定子$_G([y'] \cap x')$)，均有 $(h'(\sigma)\ \sigma)(N[x'][y']) = N[x'][y']$。为证明这一点，我们证明：对于每个 $(j, [x'], [y']) \in J_{[x'][y']}$ 和 $i \in I_{[y']}$，$N[x'][y']_{h'(\sigma)(j,[x'],[y']),\sigma(i)} = N[x'][y']_{(j,[x'],[y']),i}$。接下来，我们将使用根据 $N[x'][y']$ 的定义所得的结论：$N[x'][y'] = (\mathrm{id}\, g_{[y]}(\pi_{[x'][y']}))(N[x][y])$。设对于一个 $\pi \in$ 稳定子$_G([y'] \cap x')$，$\sigma = g_{[y']}(\pi) = g_{[y]}(\pi)$。那么对于任意 $(j, [x'], [y']) \in J_{[x'][y']}$，$i \in I_{[y']}$，我们得到：

$$\begin{aligned} N[x'][y']_{h'(\sigma)(j,[x'],[y']),\sigma(i)} &= (N[x][y])_{h(g_{[y]}(\pi^{-1}_{[x'][y']} \circ \pi \circ \pi_{[x'][y']}))(j,[x],[y]),(g_{[y]}(\pi_{[x'][y']})^{-1} \circ \sigma)(i)} \\ &= (N[x][y])_{h(g_{[y]}(\pi^{-1}_{[x'][y']} \circ \pi \circ \pi_{[x'][y']}))(j,[x],[y]),g_{[y]}(\pi^{-1}_{[x'][y']} \circ \pi \circ \pi_{[x'][y']})(i')} \\ &= (N[x][y])_{(j,[x],[y]),i'}. \end{aligned}$$

在第二步中，我们利用了 $\sigma(i) = g_{[y']}(\pi)(i)$，并将 $i \in I_{[y']}$ 替换为某个 $i' \in I_{[y]}$ 的 $g_{[y]}(\pi_{[x'][y']})(i')$（这可以通过 $I_{[y]}$ 和 $I_{[y']} = I_{\pi_{[x'][y']}[y]}$ 的归纳假设中的 (c) 项得到）。我们还利用了 $g_{[y]}$ 是群同态。最后一步成立，是因为我们已经知道 h 满足我们要为 h' 证明的性质，即对于任意 $\sigma' \in g_{[y]}$（**稳定子**$_G([y] \cap x)$），都有 $(h(\sigma')\ \sigma')N[x][y] = N[x][y]$（这是由 $N[x][y]$ 和 h 的构造得出的）。我们可以再次利用 $N[x'][y']$ 的定义继续推导：

$$\begin{aligned} (N[x][y])_{(j,[x],[y]),i'} &= (N[x'][y'])_{(j,[x'],[y']),g_{[y]}(\pi_{[x'][y']})(i')} \\ &= (N[x'][y'])_{(j,[x'],[y']),i}. \end{aligned}$$

由此可得 $(h'(\sigma)\ \sigma)(N[x'][y']) = N[x'][y']$，证毕。 ◀

▶**引理 44.** 设 $[x'] \in \Omega[x]$，$[y'] \in C[x']$。设 $\pi \in$ **稳定子**$_G(\mu)$。那么，对于每个 $(k, [x'], [y']) \in J_{[x'][y']}$，$N[x'][y']$ 中与第 k 行相同的行数等于

$N\pi[x']\pi[y']$ 中与 $N[x'][y']$ 的第 k 行相同的行数（允许对列应用 $g_{[y']}$）。形式化地说：

$$\begin{aligned}&|\{(i,[x'],[y']) \in J_{[x'][y']} \mid (N[x'][y'])_{(i,[x'],[y']),-} = (N[x'][y'])_{k,-}\}|\\ =&|\{(i,\pi[x'],\pi[y']) \in J_{\pi[x']\pi[y']} \mid (N\pi[x']\pi[y'])_{(i,\pi[x'],\pi[y']),-} = g_{[y']}((N[x'][y'])_{k,-})\}|\end{aligned}$$

证明。 令 $[y] \in \mathcal{C}[x]$ 为 $\Omega_{[y']}$ 的初始元，并记 $\sigma := \pi_{[x'][y']}, \sigma' := \pi_{\pi[x']\pi[y']}$。因此，这两个置换属于 **稳定子**$_G(\mu)$，它们被用于从 $N[x][y]$ 构造出 $N[x'][y']$ 和 $N\pi[x']\pi[y']$。根据这些矩阵的构造，有 $N[x'][y'] = (\mathrm{id}_{g[y]}(\sigma))(N[x][y])$，且$N[x'][y'] = (\mathrm{id}_{g[y]}(\sigma'))(N[x][y])$。因此，$(N\pi[x']\pi[y'])_{k,-} = (g_{[y]}(\sigma') \circ g_{[y]}(\sigma)^{-1})((N[x'][y'])_{k,-})$。由于 $g_{[y]}$ 是群同态，我们也可以将其写成：

$$(N\pi[x']\pi[y'])_{k,-} = g_{[y]}(\sigma' \circ \sigma^{-1})((N[x'][y'])_{k,-}) \qquad (\star)$$

如果 $\sigma' \circ \sigma^{-1}$ 等于 π，那么这就足以证明该引理。然而，我们只知道 $(\sigma' \circ \sigma^{-1})([y'] \cap x') = \pi([y'] \cap x')$。我们利用这一点证明以下内容

断言： 设 m 为 $N[x'][y']$ 和 $N\pi[x']\pi[y']$ 的行数。存在一个置换 $\vartheta \in$ **对称群**$_m$，使得 $(N\pi[x']\pi[y'])_{\vartheta(k),-} = g_{[y]}(\pi)((N[x'][y'])_{k,-})$，对每个 $k \in [m]$ 都成立。

证明。成立的是 $(\pi \circ \sigma \circ (\sigma')^{-1}) \in$ 稳定子$_G([y'] \cap \pi x')$。由引理 43，存在一个$\vartheta \in$对称群$_m$，使得 $(\vartheta, g_{[y]}(\pi \circ \sigma \circ (\sigma')^{-1}))(N\pi[x']\pi[y']) = N\pi[x']\pi[y']$。成立的是 $\sigma \circ (\sigma')^{-1} = (\sigma' \circ \sigma^{-1})^{-1}$。因此，由 $(\star)$ 可得：$(N[x'][y'])_{k,-} = g_{[y]}(\sigma \circ (\sigma')^{-1})((N\pi[x']\pi[y'])_{k,-})$。由此可得 $(N\pi[x']\pi[y'])_{\vartheta(k),-} = g_{[y]}(\pi)(N[x'][y'])_{k,-}$ 对每个 $k \in [m]$ 都成立。这就证明了该断言。

该断言蕴含此引理，因为 $g_{[y']} = g_{[y]}$（作为 $\Omega_{[y]} = \Omega_{[y']}$），因此我们知道，$N\pi[x']\pi[y']$的行就是 $N[x'][y']$的行，对列应用$g_{[y']}(\pi)$，并且可能对行重新排序。◀

10.2 有对称基和无对称基的对象

引理 59. 设 $\mu \in \mathrm{HF}(E)$ 是 *CFI*-对称的。那么 μ 满足定义 *56* 中的对称基条件。

证明。设 $x \in \mathrm{tc}(\mu)$ 且 $[y] \in \mathrm{C}[x]$。设 $\Gamma :=$ 稳定子$_E([y] \cap x) \leq \mathbb{F}_2^E$。我们需要分别为 Γ 和 $\mathbb{F}_2^E$定义两个基 $\mathrm{B}_\Gamma \subseteq \mathrm{B}$，使得群 稳定子$_{\mathbf{Stab}_G([y]\cap x)}(\mathrm{B}_\Gamma)$ ∩稳定子$_{\mathbf{Stab}_G([y]\cap x)}(\mathrm{B})$ 在 稳定子$_G([y] \cap x)$ 中的指数为多项式。由于 μ 是 CFI-对称的，根据定义 17，$\mathrm{Aut}_{\mathrm{CFI}}(\mathfrak{G})$ 对 $[y] \cap x$ 的轨道大小恰为二。我们有 $\mathrm{Aut}_{\mathrm{CFI}}(\mathfrak{G}) \cong \mathbb{F}_2^E$，因此根据轨道-稳定子定理，稳定子$_E([y] \cap x)$ 是 $\mathbb{F}_2^E$的一个余维为一的子空间。我们利用这一点来分析空间 稳定子$_E([y] \cap x)$ 的结构。群 稳定子$_G([y] \cap x)$ 是 $\mathrm{Aut}(G) \leq$ 对称群(V) 的一个子群，因此也作用于边集 E。于是，我们可以将 E划分为其 稳定子$_G([y] \cap x)$-轨道。令 $\mathrm{P} = \{P_1, \ldots, P_m\}$ 表示 E的这一轨道划分。

断言： 存在一个划分 $E = A \uplus B$，使得 **稳定子**$_E([y] \cap x) = \mathbb{F}_2^A \oplus \widetilde{\mathbb{F}}_2^B$且 $B \neq \emptyset$。此外，A和 B是 **稳定子**$_G([y] \cap x)$-轨道的并集。

断言的证明。令 $\mathrm{P}' \subseteq \mathrm{P}$ 表示轨道的集合 P_i，使得对于任意 $e \in P_i$，单位向量 $\chi(e)$ 都属于 $\mathrm{Stab}_E([y] \cap x)$。注意，每当 $\chi(e) \in \mathrm{Stab}_E([y] \cap x)$ 时，对于轨道中每个 e'，都有$\chi(e') \in \mathrm{Stab}_E([y] \cap x)$，因为 $\mathrm{Stab}_G([y] \cap x)$ 在每个轨道上传递，且子空间 $\mathrm{Stab}_E([y] \cap x)$ 在 $\mathrm{Stab}_G([y] \cap x)$ 对坐标的作用下是不变的（引理 38）。令 $A := \bigcup \mathrm{P}'$，并令 $B := E \setminus A$。还需证明 $\widetilde{\mathbb{F}}_2^B$是 $\mathrm{Stab}_E([y] \cap x)$ 的子空间。反设存在某个

向量 $\mathbf{v} \in \mathbb{F}_2^E$，其在 B 上的汉明重量为偶数，且在 A 上为零，但不属于 $\mathrm{Stab}_E([y] \cap x)$。由于 $\mathrm{Stab}_E([y] \cap x)$ 在 $\mathbb{F}_2^E$中的余维恰为一，并且根据 P', 的定义，不存在满足 $e \in B$ 的单位向量 $\chi(e)$ 属于 $\mathrm{Stab}_E([y] \cap x)$，因此我们知道，对于任何这样的满足 $e \in B$的单位向量 $\chi(e)$，都存在某个 $\mathrm{w}_e \in \mathrm{Stab}_E([y] \cap x)$，使得 $\mathbf{v} = \mathrm{w}_e + \chi(e)$。但这样一来，在 B 上汉明重量恰为二的每个向量都属于 $\mathrm{Stab}_E([y] \cap x)$。具体而言，对于任意两个 e、$e' \in B$，都有 $\mathrm{w}_e + \mathrm{w}_{e'} = \chi(e) + \chi(e')$，并且 w_e、$\mathrm{w}_{e'} \in \mathrm{Stab}_E([y] \cap x)$。因此，$\mathrm{Stab}_E([y] \cap x)$ 确实包含 $\widetilde{\mathbb{F}}_2^B$。总之，这就证明了该断言（$B \neq \emptyset$ 成立，否则余维将为零）。

现在，不难为**稳定子**$_E([y] \cap x)$定义一个对称基。任取一条边$f \in B$。我们定义

$$\mathcal{B}_\Gamma := \{\chi(e) \mid e \in A\} \cup \{\chi(\{e, f\}) \mid e \in B \setminus \{f\}\}.$$

可以验证，这确实是 $\mathbb{F}_2^A \oplus \widetilde{\mathbb{F}}_2^B$的一个基。于是，$\mathbb{F}_2^E$的基$\mathcal{B}$ 定义为$\mathcal{B} := \mathcal{B}_\Gamma \cup \{\chi(f)\}$。

现在，群 $\mathrm{Stab}_{\mathrm{Stab}_G([y]\cap x)(\mathrm{B}_\Gamma)} \cap \mathrm{Stab}_{\mathrm{Stab}_G([y]\cap x)(\mathrm{B})}$ 包含 $\mathrm{Stab}_G([y] \cap x)$ 中所有固定边 f，并固定集合 A 和 B（作为集合）的置换。根据断言，A 和B 是 $\mathrm{Stab}_G([y] \cap x)$-轨道的并，因此所有 $\mathrm{Stab}_G([y] \cap x)$ 中的置换都满足后一条件。因此，$\mathrm{Stab}_{\mathrm{Stab}_G([y]\cap x)(\mathrm{B}_\Gamma)} \cap \mathrm{Stab}_{\mathrm{Stab}_G([y]\cap x)(\mathrm{B})}$ 就是 $\mathrm{Stab}_G([y] \cap x) \leq \mathrm{Sym}(E)$ 中 f 的逐点稳定子，其指数至多为 $|E|$。这是关于 $|\mathfrak{G}^S|$的多项式。◀

▶**引理 61.** 存在一个布尔向量空间族 $(\Gamma_n)_{n\in\mathbb{N}}$、一个函数 $t(n) \in \Theta(n)$，满足 $\Gamma_n \leq \mathbb{F}_2^{t(n)}$；以及一个置换群族 $(\mathbf{G}_n)_{n\in\mathbb{N}}$，满足 $\mathbf{G}_n \leq \mathbf{Sym}^{t(n)}$，使得
1. Γ_n 是$\mathbf{G}_n$-不变的。2. Γ_n 在 $\mathbb{F}_2^{t(n)}$ 中的余维数为 $O(\log n)$。3. 对于任意一对基 $B_\Gamma \subseteq B$，其中 B_Γ 是 Γ_n 的基，B 是 $\mathbb{F}_2^{t(n)}$ 的基，$[\mathbf{G}_n : \mathbf{稳定子}_{\mathbf{G}_n}(B)] \geq \binom{n}{(\log n)^2}^{\log n}$，其相对于 n 是超多项式的。

证明。 将 $t(n)$ 定义为不小于 $\geq n$ 的下一个偶自然数。现在我们来构造 Γ_n 和 $\mathbf{G}_n$。令 $\mathcal{P}_n$ 为 $[t(n)]$ 的一个划分，将其分成 $\approx \log n$ 个部分，使每个部分的大小大致相同，即 $\approx \frac{n}{\log n}$。重要的是，每个部分的大小都必须为偶数；这样的划分存在，因为 $t(n)$ 是偶数。对于一个部分 $P \in \mathcal{P}_n$，令 $\widetilde{\mathbb{F}}_2^P \leq \mathbb{F}_2^{t(n)}$ 表示包含所有满足以下条件的向量的布尔向量空间：它们在 P 上的投影具有偶汉明重量，并且在 P 之外为零。然后我们定义

$$\Gamma_n := \bigoplus_{P\in\mathcal{P}_n} \widetilde{\mathbb{F}}_2^P.$$

换句话说，Γ_n 恰好包含那些在$\mathcal{P}_n$ 的每个部分上都具有偶汉明重量的向量（但并非 $\mathbb{F}_2^{t(n)}$ 中所有具有偶汉明重量的向量，即不包含那些在偶数个部分上为奇的向量）。置换群$\mathbf{G}_n \leq \mathbf{Sym}^{t(n)}$定义为集合稳定划分$\mathcal{P}_n$的最大群。因此，$\mathbf{G}_n$ 包含直积$\mathbf{H_n} := \prod_{P\in\mathcal{P}_n} \mathbf{Sym}(P)$，以及所有将$\mathcal{P}_n$ 的每个部分映射到另一部分的置换。

显然，Γ_n 在$\mathbf{G}_n$下是不变的。此外，Γ_n 的余维数关于 $t(n) \approx n$呈对数级增长：设$\mathcal{B}_\Gamma$ 是 Γ_n 的任意一个基。那么，只需为每个部分 $P \in \mathcal{P}_n$添加一个单位向量 e_P，就可以将其扩展为 $\mathbb{F}_2^{t(n)}$ 的一个基，使得 e_P 在 P 中有一个 1 元素，其余

均为零。部分的数量呈对数级增长，因此余维数也如此。最后，我们必须证明第三个条件。

令 $B_\Gamma \subseteq B$ 分别为 Γ 和 $\mathbb{F}_2^{t(n)}$ 的任意基。注意，$\mathrm{Stab}_{G_n}(B) \leq \mathrm{Stab}_{G_n}(B \setminus B_\Gamma)$，因为 Γ_n 是 G_n-不变的，因此 $B \setminus B_\Gamma$ 中的向量无法移入 Γ。所以：$[G_n : \mathrm{Stab}(B \setminus B_\Gamma)] \leq [G_n : \mathrm{Stab}(B)]$。因此，只需证明 $[G_n : \mathrm{Stab}(B \setminus B_\Gamma)]$的所需下界。令 $w_1, \ldots, w_{\log n}$ 为 $B \setminus B_\Gamma$的一个枚举。对每个 $i \leq \log n$，令 $Q_i \subseteq P_n$ 表示满足 w_i 在其上具有奇数汉明重量的部分 $P \in P_n$ 的集合。我们知道，对每个 i，$Q_i \neq \emptyset$，否则 w_i 就会属于 Γ。此外，每个 $P \in P_n$ 至少属于一个 Q_i，否则 B 将无法生成整个空间 $\mathbb{F}_2^{t(n)}$。

现在，为了估计 $|\textbf{稳定子}(\mathcal{B} \setminus \mathcal{B}_\Gamma)|$，我们先估计 $\mathcal{B} \setminus \mathcal{B}_\Gamma$ 在 $\mathbf{H}_n$中的逐点稳定子的大小，即 $\textbf{稳定子}^\bullet_{\mathbf{H}_n}(\mathcal{B} \setminus \mathcal{B}_\Gamma)$。这是 $\mathbf{H}_n$ 中逐一稳定每个 $\mathbf{w}_i \in \mathcal{B} \setminus \mathcal{B}_\Gamma$的子群，因此它由固定每个部分 $P \in \mathcal{P}_n$ 和每个 $\mathbf{w}_i$的所有置换组成。我们可以如下界定这个稳定子：

$$|\mathbf{Stab}^\bullet_{\mathbf{H}_n}(\mathcal{B} \setminus \mathcal{B}_\Gamma)| \leq \prod_{P \in \mathcal{P}_n} (|P| - 1)!$$

这是因为对于每个部分 $P \in \mathcal{P}_n$，都存在一个向量 $\mathbf{w}_i \in \mathcal{B} \setminus \mathcal{B}_\Gamma$，它在 P 上的权重为奇数。由于每个部分 P 的大小都是偶数，$\mathbf{w}_i$ 不是 P 上的全1向量（当然也不是全零向量）；因此，向量 $\mathbf{w}_i$ 不会被**对称群** (P) 中的所有置换固定，至多只有 $(|P| - 1)!$ 个置换会固定它（更准确地说，是 $k! \cdot (|P| - k)!$ 个，如果 k 是 P中 1 的个数——但这至多为 $(|P| - 1)!$）。现在，由于 $[\mathbf{G}_n : \mathbf{H}_n] = (\log n)!$，我们有

$$|\mathbf{Stab}^\bullet_{\mathbf{G}_n}(\mathcal{B} \setminus \mathcal{B}_\Gamma)| \leq (\log n)! \cdot |\mathbf{Stab}^\bullet_{\mathbf{H}_n}(\mathcal{B} \setminus \mathcal{B}_\Gamma)|.$$

此外，$[\textbf{稳定子}_{G_n}(\mathcal{B} \setminus \mathcal{B}_\Gamma) : \textbf{稳定子}^\bullet_{\mathbf{G}_n}(\mathcal{B} \setminus \mathcal{B}_\Gamma)] \leq (\log n)!$。因此，总的来说，我们得到：

$$\mathbf{Stab}_{\mathbf{G}_n}(\mathcal{B} \setminus \mathcal{B}_\Gamma) \leq (\log n)!^2 \cdot \prod_{P \in \mathcal{P}_n} (|P| - 1)!$$

由于 $|\mathbf{G}_n| = (\log n)! \cdot \prod_{P \in \mathcal{P}_n} |P|!$，因此指数为：

$$[\mathbf{G}_n : \mathbf{Stab}_{\mathbf{G}_n}(\mathcal{B})] \geq [\mathbf{G}_n : \mathbf{Stab}_{\mathbf{G}_n}(\mathcal{B} \setminus \mathcal{B}_\Gamma)] \geq 1/(\log n)! \cdot \prod_{P \in \mathcal{P}_n} |P| \geq \left(\frac{n}{(\log n)^2}\right)^{\log n}.$$

最后一个不等式成立，是因为 $\mathcal{P}_n$ 由 $\log n$ 个大小为 ${}^{n}\log n$ 的部分组成，并且 $(\log n)! \leq (\log n)^{\log n}$。◀

10.3 超立方体的齐性

▶引理 *63*。令 $tw_n \in \Theta(2^n/\sqrt{n})$ 表示 H_n 的树宽。设 α 是 $V(\mathfrak{H}_n^i)$ 中一个包含星且长度至多为 $(tw_n/n) - 2$ 的元组。设 $\gamma, \gamma' \in V(\mathfrak{H}_n^i)$，并令 $tp(\alpha\gamma)$ 表示这个扩展元组的 C^{tw_n}-类型。如果 $tp(\alpha\gamma) = tp(\alpha\gamma')$，那么存在一个自同构 $\rho \in Aut(\mathfrak{H}_n^i)$，使得 $\rho(\gamma) = \gamma'$ 且 $\rho(\alpha) = \alpha$。

证明。我们假设 $tp(\alpha\gamma) = tp(\alpha\gamma')$。证明的前半部分在于证明此时，$\gamma$、$\gamma'$位于同一个边构件或顶点构件中。首先假设 γ，$\gamma' \in E$。现在反设 γ 和 γ' 的边构件并不相同。令 $\{u, v\} \in E_n$ 为包含 γ 的构件中的边，并令 $\{u', v'\} \in E_n$ 为 γ'对应的边。不妨设 $u \neq u'$ 和 $u \neq v'$。现在令 s_1，...，$s_n \in E_n$ 为根据假设由 α 覆盖、构成该星的边。我们可以假设该星的中心为字符串

0^n，因为超立方体的自同构群是传递的，因此我们总能将星的中心移动到 0^n。令 s_i 表示边 $\{0^n,\ 0^{i-1}10^{n-i}\}$，即沿着该边翻转位置 i 。

令 $U \subseteq [n]$ 为字符串 u 中取值为 1 的位置。我们构造一个 $\mathcal{C}^5$-公式 $\varphi_u(x)$，它使用星 $s_1, ..., s_n$ 作为参数，定义 $\mathfrak{H}_n^i$ 中的构件 u^*。更准确地说，令 $s'_1, ..., s'_n$ 为 α 中出现的边组件里的相应顶点。

我们的公式使用一些辅助公式：$\psi_{\mathrm{dist}=\ell}(x,y) \in \mathcal{C}^3$，它断言存在一条从 x 到 y、长度为 ℓ 的路径。这可以通过交替地重新量化变量，仅用三个变量来表达（例如参见 [25] 中的命题 3.2）。此外，我们还使用公式 $\psi_{\approx}(x,y)$，它断言 x 和 y 位于同一个顶点小装置中。这可以通过说明它们二者都恰有 n 个邻居来表达，并且：对于 x 的每个邻居 z，z 要么也是 y 的邻居，要么与某个邻居相邻（该邻居位于同一个边小装置中）。对于 y 的每个邻居 z，也必须满足同样的条件。表达这一点总共不需要超过五个变量。现在我们定义：

$$\varphi_u(x) := \bigwedge_{i \in U} \exists z(\psi_{\mathrm{dist}=1+2(|U|-1)}(s'_i, z) \wedge \psi_{\approx}(z,x)) \wedge \bigwedge_{i \in [n] \setminus U} \neg \exists z(\psi_{\mathrm{dist}=1+2(|U|-1)}(s'_i, z) \wedge \psi_{\approx}(z,x)).$$

断言： $\mathfrak{H}_n^i \models \varphi_u(a)$ 当且仅当 $a \in u^*$。

断言的证明： 我们假设 s_i 是连接 0^n 与位置 i 上为 1 的字符串的边。现在证明，若 $a \in u^*$，则 $\mathfrak{H}_n^i \models \varphi_u(a)$：我们需要检查对于每个 $i \in [n]$，公式中相应的合取项都成立。若 $i \in U$，那么对于任意 $s'_i \in s_i^*$，存在 $z \in u^*$，使得在 $\mathfrak{H}_n^i$ 中有一条从 s'_i 到 a 、长度恰为 $1 + 2(|U| - 1)$ 的路径：这条路径从 s'_i 出发，走一步进入 $0^{i-1}10^{n-i}$ 的顶点构件；随后，路径沿着 $0^{i-1}10^{n-i}$ 到顶点 u 的最短路径，在途中翻转其余的 $|U| - 1$ 个零，该最短路径在 $\mathcal{H}_n$ 中长度为 $|U| - 1$。在 CFI 结构 $\mathfrak{H}_n^i$ 中，这条路径的长度是其两倍，因为每条边都由一个构件细分。路径最终会到达顶点构件 u^* 中的某个节点。若 $i \notin U$，则不存在一条从 s'_i 出发、长度为 $1 + 2(|U| - 1)$ 且终点位于 u^* 中某个节点的路径：从 s'_i 到构件 u^* 的最短路径需要 $1 + 2|U|$ 步。因此，$\mathfrak{H}_n^i \models \varphi_u(a)$。

如果 $a \notin u^*$，那么 $\mathfrak{H}_n^i \not\models \varphi_u(a)$，因为只有当$\mathcal{H}_n$中存在（分别不存在）所需路径时，$\varphi_u(a)$ 才能成立；而上述论证也表明，只有当 a 位于 u的构件中时，这些条件才可满足。这就证明了该断言。

因此，我们有

$$\mathfrak{H}_n^i \models \exists x(Ex\gamma \wedge \varphi_u(x)),$$

but

$$\mathfrak{H}_n^i \not\models \exists x(Ex\gamma' \wedge \varphi_u(x)).$$

这与 $\alpha\gamma$ 和 $\alpha\gamma'$ 具有相同$\mathcal{C}^{\mathbf{tw}_n}$-类型的假设矛盾，因为$\varphi_u$ 仅使用了 $\mathcal{O}(n)$ 个变量。因此，我们证明了存在一条边 $g \in E_n$，使得 $\gamma, \gamma' \in g^*$。

如果 γ 和 γ' 都在顶点构件中，那么同样的论证表明它们必须在同一个构件 u^* 中，因为我们可以用上述公式定义这个构件。类似地，如果 γ 在顶点构件中，而 γ' 在边构件中，我们也可以这样论证：然后我们定义

γ 的顶点构件采用上述公式，而 γ' 不满足该公式。因此，元组类型相同意味着 γ 和 γ' 必须位于同一个构件中，无论它是边构件还是顶点构件。

在证明的后半部分，我们证明存在一个自同构 $\rho \in \mathbf{Aut}(\mathfrak{H}_n^i)$，它将 $\alpha\gamma$ 映射到 $\alpha\gamma'$；同样假设 $\mathsf{tp}(\alpha\bar{\gamma}) = \mathsf{tp}(\alpha\gamma')$。我们先处理 $\gamma, \gamma' \in g^*$ 对某个边构件 g^* 成立的情况。无需置换超立方体，因此只需找到一个边翻转自同构，即 $\rho \in \mathbf{Aut}_{\mathrm{CFI}}(\mathfrak{H}_n^i)$。

如果 $\gamma = \gamma'$，则无需证明任何内容。因此不失一般性地假设 $\gamma = g_0$ 和 $\gamma' = g_1$。我们需要找到 $\rho \in \mathrm{Aut}(\mathfrak{H}_n^i)$，使得 $\rho(g_0) = g_1$，并且 ρ 固定 α。现在，如果一条边 $e = \{u, v\} \in E_n$ 满足 e_0 或 e_1 出现在 α 中，我们就称该边为固定的。如果 v^* 中的某个节点出现在 α 中，我们就称顶点 $v \in V_n$ 为固定的。我们知道 g 不是固定的，因为若它是固定的，那么 αg_0 和 αg_1 的类型就不同。H_n 中的环若至少有一条边或一个顶点是固定的，就称为固定环；否则，该环是自由环。如果 H_n 中存在一个自由环，且 g 位于该环上，那么所需的自同构就是 $\rho_F \in \mathrm{Aut}_{\mathrm{CFI}}(\mathfrak{H}_n^i)$，其中 F 是该自由环的边集。

否则， g 所在的每个环都是固定的。我们要证明在这种情况下， $\alpha\gamma$ 和 $\alpha\gamma'$ 不具有相同的 $\mathcal{C}^{\mathbf{tw}_n}$-类型，因此这种情况不可能发生。

令 $u, v \in \{0,1\}^n$ 为 g 的端点。令 $X_u \subseteq \{0,1\}^n$ 为 $\mathcal{H}_n$ 中可从 u 沿仅使用自由顶点和自由边的路径到达的顶点集合，这些路径位于 $E_n \setminus \{g\}$ 中。集合 X_u 还包括以这种方式可达的固定顶点。类似地，我们将 X_v 定义为从 v 沿此类自由路径可达的顶点集合（也包括固定顶点）。由于不存在自由环，集合 X_u 和 X_v 必定不相交（可能共享的固定顶点除外）。我们将图限制在这两个集合中较小的一个上，不妨设它是 X_u。因此令 $X := X_u$。现在考虑图 G 和 G'，它们是 $\mathfrak{H}_n^i$ 在论域

$$\mathcal{X} := \{v^Y \mid v^Y \in v^*, v \in X\} \cup \{e_j \mid j \in \{0,1\}, e \in E(\mathcal{H}_n[X])\} \\ \cup \{a \in V(\mathfrak{H}_n^i) \mid a \text{ an entry in } \bar{\alpha}\gamma\} \cup \{\gamma'\}.$$

现在， $G := (\mathfrak{H}_n^i[\mathcal{X}], \alpha\gamma)$ 和 $G' := (\mathfrak{H}_n^i[\mathcal{X}], \alpha\gamma')$，也就是说，它们都是 CFI 图中相同的诱导子图，并分别扩展了相应的常数元组（严格来说， γ 和 γ' 的常数符号应该相同，但其解释分别为 γ 和 γ'）。

至于 $X \subseteq V(\mathrm{H}_n)$ 的大小，我们有： $|X| < |\alpha\gamma| \cdot n = \mathsf{tw}_n - n$。为此，令 $\delta X \subseteq E_n$ 为 H_n 中 X 的割，即 X 与其补集之间的边集。H_n 的切格常数（即对所有满足 $|A| \leq |V(\mathrm{H}_n)|/2$ 的 $A \subseteq V(\mathrm{H}_n)$， $\frac{|\delta A|}{|A|}$ 的最小值）介于 1 和 $2\sqrt{n}$ 之间。根据切格不等式（例如参见 [15]）以及如下事实即可得出这一点：任意超立方体的拉普拉斯算子的最小非零特征值为 2 [16]（实际上，最快的查找方法是访问维基百科）。这意味着 $|\delta X| \geq |X|$。由此可知 $|\alpha\gamma| \cdot n \geq |X|$，因为割 δX 中的边恰好是固定边，而 $\alpha\gamma$ 的每个元素至多固定 n 条边。此外，我们还可以断定该不等式实际上必须是严格的，因此 $|\alpha\gamma| \cdot n > |X|$。这是因为 α 中的元素并非都用于固定 δX 中的边； α 中的某些元素也必须属于 $\delta X_v \setminus \delta X_u$。因此，我们有 $|X| < |\alpha\gamma| \cdot n = \mathsf{tw}_n - n$。

断言： Spoiler 在 G 和 G' 上的双射 $\mathbf{tw}_n$-棋子游戏中获胜。

断言的证明： 显然，$\mathcal{H}_n[X]$ 的树宽严格小于 $\mathbf{tw}_n - n$，因为 $|X| < \mathbf{tw}_n - n$。因此，警察用 $\mathbf{tw}_n - n$ 名警察即可在 $\mathcal{H}_n[X]$ 上赢得警察与强盗游戏。Spoiler 的目标是在两个结构 G 和 G' 中，都将棋子放在顶点 e_1 上，覆盖每一条

边，其中 $E_n(u)\setminus\{g\}$，也就是说，所有与 u 相 incident 的边，除了 g。如果他做到这一点，就能在下一回合获胜：不失一般性地，假设构件 u^* 是偶数的。那么在 G' 中， u^* 中每个顶点的邻居里，作为棋子所在顶点或等于常数 $\gamma' = g_1$ 的顶点数都是偶数。而在 G 中，对于 u^*中的每个顶点，这个数都是奇数，因为 $\gamma = g_0$。因此，Spoiler 随后可以在 u^* 中的任意顶点上放置一枚额外的棋子，并获胜，因为复制者的双射必须将 G 中的构件 u^* 映射到 G'中的 u^* 。

现在，Spoiler 可以通过标准论证实现这一目标，例如 [2] 中给出的论证：最初，Spoiler 的“目标顶点”是 u_0。这意味着他必须在两张图中所有与其关联的边上放置棋子，标记 e_1 个顶点。复制者的双射可以翻转边，从而改变 Spoiler 的目标顶点集合。假设 $F \subseteq E$（$\mathcal{H}_n[X]$）是复制者在某一回合翻转的边集。其结果是，$\mathcal{H}_n[X]$ 中每个 F 次数为奇数的顶点都会在目标顶点与非目标顶点之间互换角色。然而，复制者不能翻转被 Spoiler 放置棋子的边。如果 Spoiler 根据警察的获胜策略，将棋子放在边上（或其端点上），而复制者则通过翻转路径来“移动强盗”，那么 Spoiler 最终就能锁定一个复制者无法将其移到别处的目标顶点。从这样的局面出发，他可以迫使棋局进入上述情形并获胜。这一论证广为人知；在我们的设定中，唯一额外的困难是基图没有顺序，因此我们必须论证复制者无法通过采取边翻转以外的双射来获胜。Spoiler 最多可以使用 n 个额外棋子来做到这一点：关键观察是，复制者的双射必须保持棋盘上所有棋子及参数 $\alpha\gamma$ 的距离。因此，复制者只有在顶点 w 与 $\pi(w)$ 到每个已放置棋子的顶点和参数的距离都相同的情况下，才能将一个构件 w^* 映射到另一个构件 $\pi(w^*)$。这是因为，如果复制者不保持这些已标记元素之间的距离，Spoiler 就可以沿着最短路径移动棋子，只用三枚棋子便轻易获胜。

现在，Spoiler 可以直接通过用 n 枚棋子在$\mathcal{H}_n[X]$ 中某个星上放置棋子来开始（这是可行的，因为我们使用 $\mathbf{tw}_n$ 枚棋子进行游戏，但模拟警察的获胜策略只需要 $\mathbf{tw}_n - n$ 枚）。一旦在 G 和 G' 中的某个星上放置了棋子，根据本引理证明中较早使用过的论证可知，任何 $w \in V(\mathcal{H}_n[X])$ 到该星各边的距离集合都是唯一的，因此，复制者随后被迫将每个 w^* 映射到唯一的顶点构件 $\pi(w^*)$。这意味着，她还必须将每个 e^* 映射到唯一的边构件 $\pi(e^*)$。因此，从那一刻起，复制者确实只能进行边翻转，随后 Spoiler 使用警察的策略，按照上述方式获胜。这就证明了该断言。

断言直接推出，如果 g 不位于任何自由环上，那么 $\alpha\gamma$ 和 $\alpha\gamma'$ 具有不同的 $\mathsf{C}^{\mathbf{tw}_n}$-类型。这就完成了 γ 和 γ' 位于边构件中的情形。另一种情形是， $\gamma = u^*_Y$ 和 $\gamma' = u^*_{Y'}$ 都位于某个顶点构件 u^* 中。此时，$\mathbf{H}_n$ 中有一个与 u 相邻的偶数大小的边集 $F = Y \triangle Y'$，为了将 γ 映射到 γ'，我们必须翻转 F 中的边（而不翻转 $E(u)$ 中的其他边）。如果我们能将 F 中的边两两配对，使得每一对 $\{f_1, f_2\} \subseteq F$ 都位于某个自由环上（该环避开 $E(u)$ 中的所有其他边），那么这就是可行的。反设存在一对 $\{f_1, f_2\} \subseteq F$，它不位于任何自由环上。于是令 $g := f_1$，并在我们想要翻转边 g 的情形下，采用与上文相同的论证（不同之处在于，现在我们同时移除 f_1 和 f_2，以得到两个不被任何自由路径连接的集合 X_u 和 X_v）。那么，上述证明表明，构件 f_1^* 中的两个节点在使用参数 α 时可由 $\mathsf{C}^{\mathbf{tw}_n}$ 区分。但这样一来， u^* 中的 γ 和 γ' 也可区分，因为其中一个与 f_1^* 中的 0-节点相邻，另一个与 f_1^* 中的 1-节点相邻。因此，同样地，

所需的自由环必定存在，因为否则， $\alpha\gamma$ 和 $\alpha\gamma'$ 就具有不同的 $\mathcal{C}^{\mathbf{tw}_n}$-类型。◀

10.4 交替支撑划分至多只有次线性的单元素部分

在这里，我们证明定理 75，它依赖于以下关键引理：

▶ **引理 74**。 设 $(G_n)_{n\in\mathbb{N}}$ 是一个群族，使得对于所有 n, $G_n \leq$**对称群**$_n$。假设存在某个常数 $k \in \mathbb{N}$，使得渐近地， [**对称群**$_n$： $G_n] \leq 2^{nk}$。

那么，存在一个常数 $0 < c \leq 1$，使得对于所有足够大的 n， G_n 都有一个子群 H_n，满足 **交错群**$(A) \leq H_n^{([n]\setminus A)}$，其中某个 H_n-轨道 A 的大小为 $|A| \geq cn$。

为了证明这个引理，我们首先要引入群论中的几个概念。例如，可以在教科书 [14] 中找到这些概念。对于群 $G \leq$**对称群**(Ω) 和子集 $\Delta \subseteq \Omega$， $G^{(\Delta)}$ 表示 Δ 在 G 中的逐点稳定子。如果 Δ 是 G 的若干轨道的并集，那么我们用 G^{Δ} 表示将 G 限制到其在 Δ 上的作用。这是**对称群**(Δ) 的一个子群。

如果群 $G \leq$**对称群**(Ω) 中的每个元素都能通过 G 将 Ω 中的任意元素映射到另一个元素，也就是说，Ω 本身是一个轨道，那么该群在 Ω 上是传递的 。如果 G 在 Ω 上传递地作用，那么非空集合 $\Delta \subseteq \Omega$ 称为一个块，若对于每个 $\pi \in G$， $\pi(\Delta) = \Delta$ 或 $\pi(\Delta) \cap \Delta = \emptyset$ 均成立。块系或非本原系是将 Ω 划分为块（且大小相同）的划分。群 G 在块的集合上作为置换群作用，因为它总是将块映射为块。每个传递群都有平凡的块系，其中每个点分别构成一个单点块，或者整个点集构成一个块。如果传递群 G 除这两种之外还有其他块系，那么 G 称为非本原；否则称为本原。特别地，本原群总是传递的。

子群 $N \leq G$ 称为 正规 子群（记作 $N \lhd G$），当且仅当其右陪集与左陪集相同，即对每个 $\gamma \in G$都有 $\gamma N = N\gamma$。一个等价的表述是，对于所有 $g \in G$， $h \in N$，都有$ghg^{-1} \in N$。我们之所以关注正规子群，是因为可以将它们因子化：如果 $N \lhd G$，那么 G/N就是元素为 N的陪集的群，也就是说：对于任意两个 γN， $\gamma' N$，商群 G/N中的群运算定义为 $(\gamma N) \circ (\gamma' N) = (\gamma \circ \gamma')N$。因此，商群的顺序 $|G/N|$等于指数 $[G: N]$，所以， $|G| = |N| \cdot |G/N|$。

如果 $G \leq$ **对称群**(Ω) 是非传递的，且 $\Delta \subseteq \Omega$ 是 G 的一个轨道，那么 $G^{(\Delta)}$，即该轨道的逐点稳定子，是 G 的正规子群，这一点很容易验证。商群$G/G^{(\Delta)}$ 与 G^{Δ} 同构，也就是 G 在 Δ 上的作用。此外，如果 G 有一个非平凡的块系，那么 G 中逐块集合稳定每个块的子群是 G的正规子群。将这个稳定子取商后，得到的群同构于 G 在这些块上的作用。因此，如果 G 是非传递或非本原的，它就有这些提到的“典范”正规子群。随后可以将这些子群取商，这在归纳证明中很有用。唯一不清楚如何取商掉正规子群的情形是 G 为本原群。注意，本原情形 $G =$ **对称群**(Ω) 或 $G =$ **交错群**(Ω) 并不难处理：对称群以交错群为正规子群，取商后剩下 $\mathbb{Z}_2$。交错群是单群，这意味着它只有自身和平凡群$\{1\}$ 这两个正规子群。其他本原情形则不那么明了，但所幸有限本原群已经被完全分类。对于我们的证明，以下 Babai 的定理足以概括相关的本原情形：

▶ **定理 85** (定理 3.2.1，见 [4])。 设 $G \leq$ **对称群**$_n$ 是一个阶为$|G| \geq n^{1+\log n}$ 的本原群，其中 n 大于某个绝对常数。那么 G 有一个指数为 $\leq n$ 的正规子群 N，使得 N 具有一个非本原系，且 N 在该系上的作用是一个 *Johnson* 群**交错群**$_k^{(t)}$，其中 $k \geq$ 对数 n。

请注意， [4]中的定理对 G的顺序有一处笔误，我们已在此更正。*Johnson* 群 **交错群**$_k^{(t)}$ 同构于**交错群**$_k$，即作用在 k 个元素上的交错群；但**交错群**$_k^{(t)}$ （以自然方式）作用于 $[k]$ 上的所有 t-元组集合。因此，上述定理保证了任何足够大的本原群中都存在正规子群 N；此外，它还告诉我们， N 在某种程度上近似于一个交错群。这基本上将是引理 74 证明中的一个基础情形。

在开始证明之前，我们还需要引入一个概念，即群 G的合成列 。它是一个序列 $1 = H_0 \lhd H_1 \lhd ... \lhd H_n = G$，其中每个 H_i 都是 H_{i+1}的极大真正规子群。这些因子 H_{i+1}/H_i 称为 G的合成因子 。每个有限群都有这样的合成列，但它不一定唯一。不过，根据 Jordan-Hölder 定理，每个合成列都会得到相同的合成因子（例如参见 [33]）。因此，无论我们以何种顺序将给定群 G的正规子群取商，最终都会遇到相同的合成因子（就像自然数的素因数分解一样）。即使每一步取商时，我们没有取极大 正规子群，这一点仍然成立。因此：

▶ **引理 86.** 设 G 是一个群， H 是 G的一个合成因子。设 $N \lhd G$ 是一个正规子群。那么 $H \cong G/N$，或者 H是 N或 G/N的一个合成因子。

证明。若 N 是 G的极大正规子群，则存在 G 的一个如下形式的合成列： $1 \lhd ... \lhd N \lhd G$。那么 $H = G/N$或 H 会在该合成列后续部分中作为合成因子出现，这意味着它是 N的一个合成因子。若 N 不是 G的极大正规子群，则对于包含 N的 G的正规子群 $k \geq 1$，有 $N \lhd N_1 \lhd ... \lhd N_k = G$。那么 H 要么是 N 的一个合成因子；要么，若不是，则它必定等于某个 $i \in [k]$，即 N_{i+1}/N_i。根据第三同构定理，$1 \lhd N_1/N \lhd ... \lhd N_k/N \lhd G/N$是 G/N的一个合成列，并且 $(N_{i+1}/N)/(N_i/N) \cong H$，所以在这种情况下， H 是 G/N 的一个合成因子。◀

我们还需要这样一个结论：如果一个群在其某个轨道 A 上是交错群，那么当其余部分逐点固定时，它要么仍在 A 上是交错群，要么其在 A 上的作用总是完全由其在 A 外的作用决定。关于这个引理的证明思路，感谢 Daniel Wiebking。

▶ **引理 87.** 设 $H \leq G \leq$ **对称群**$_n$，且 A 是 H 的一个轨道，使得 **交错群**$(A) \leq H^A$。那么，要么 **交错群**$(A) \leq (H^{([n]\setminus A)})^A$；要么对于每个 $h \in H$， h 在 $[n]\setminus A$ 上的作用也决定了 h 在 A上的作用。后者意味着，不存在两个不同的 g、 $h \in H$，它们在 $[n]\setminus A$ 上诱导相同的置换，却在 A上诱导不同的置换。

证明。 $N := (H^{([n]\setminus A)})^A$ 是 H^A的一个子群。此外，这个子群是正规子群。为此，设 $h \in N$, $g \in H^A$。我们要证明 $ghg^{-1} \in N$。存在$h' \in H^{([n]\setminus A)}, g' \in H$，使得 h', g'分别是 h和 g的扩张，即它们在 A上的限制分别对应于 h, g。显然， $g'h'g'^{-1} \in H^{([n]\setminus A)}$，因为这个置换固定了 A之外的每一个点。因此， $ghg^{-1} \in N$，因为这正是$g'h'g'^{-1}$ 在 A上的作用。所以 $N \lhd H^A$。由于 Alt(A) $\leq H^A$, H^A 要么是 Alt(A)，要么是 Sym(A)。如果它是 Alt(A)，那么 N 要么也是 Alt(A)，要么是平凡群{1}，因为 Alt(A)没有其他

正规子群。如果 H^A =**对称群**(A)，那么 N 是平凡的， N = **交错群**(A)，或者 N =**对称群**(A)。因此，如果 N 不是平凡的，那么 **交错群**(A) $\leq N = (H^{([n]\setminus A)})^A$。反之，如果 N 是平凡的，那么 $H^{([n]\setminus A)}$ 中的每个置换也逐点固定 A 。由此可知，不存在两个不同的 $g, h \in H$，使得 g, h 在 $[n] \setminus A$ 上相同、但在 A上不同。如果它们存在，那么$gh^{-1} \in H^{([n]\setminus A)}$，但 gh^{-1} 在 A上不是恒等置换。◀

现在我们将证明引理 74 所需的主要技术结果。它大致说明：如果群 G 有一个大型交错群作为合成因子，那么从某种意义上说，它也有这个大型交错群作为子群；否则， G 在 **对称群**$_n$中的指数必定很大。证明采用对 G的合成结构进行归纳的方法。也就是说，在归纳步骤中，我们选取一个正规子群并将其取商，然后按照引理 86 的思路，继续对该正规子群或商群进行归纳。借助下一个引理，我们可以利用文献中的一个事实证明引理 74：每个大型群都必定有一个大型交错群作为合成因子。因此，关键步骤是从合成因子过渡到子群。再次感谢 Daniel Wiebking 在证明中提供的帮助，尤其是解决了本原情形。

▶ **引理 88.** 设 $0 < c \leq 1$ 为一个常数。设 $(G_n)_{n\in\mathbb{N}}$ 是一个群族，使得对于所有 n, $G_n \leq$ **对称群**$_d$，其中 $c\cdot n \leq d \leq n$ （准确地说：每个 n都可以对应不同的 d），并且对于所有充分大的 n， G_n 都有一个同构于**交错群**$_m$的合成因子，其中某个 $m \geq c\cdot n$。那么，对于每个充分大的 n，以下两种情况之一会出现：

(i) 存在一个子群 $H_n \leq G_n$ 以及 H_n 的一个轨道 A，满足 $|A| \geq c\cdot n$，使得 **交错群**$(A) \leq H_n^{([d]\setminus A)}$。**(ii)** [**对称群**$_d : G_n] \geq \frac{1}{n}\cdot\left(\frac{2d\cdot\alpha}{e}\right)^{cn/2}\cdot\alpha^{\ell}$，其中 d 是 G_n的次数， ℓ 是从 G 开始、以合成因子 **交错群**$_m$ 结束的递归过程中，或在另一种非递归情形中，传递非本原情形出现的次数。因子 α 是 $1/(bc^{-1}c!)$。

证明。 固定 $n \in \mathbb{N}$ 并令 d 满足 $G_n \leq$ **对称群**$_d$ (在下文中省略下标 n 。我们根据 的合成结构进行归纳证明，并在每一步选取一个正规子群将其商去，直到得到合成因子**交错群**$_m$。根据引理的假设，它出现在 G 中。若 $G =$ **交错群**$_m$，则属于情况 (i)，结论得证。否则， G 必有正规子群，否则，G 将是单群，且不含合成因子 **交错群**$_m$。我们根据以下哪种情形成立来选取这个子群：

情况 *1*： G是非传递的。
令 $\Omega \subseteq [d]$ 为任意一个满足 $|\Omega| \geq cn$的轨道。这样的轨道必定存在，否则，G 就不能以**交错群**$_m$ 作为 $m \geq cn$ 的合成因子。为此，考虑一条正规子群链，其中的子群依次逐点固定一个轨道。相应的商群总是下一个正规子群在一个轨道上的限制，因此，如果所有轨道都太小，它们就不可能包含**交错群**$_m$ 。最终，所有轨道都被逐点固定，这就得到平凡群，而平凡群也不能包含**交错群**$_m$。因此，必定存在至少一个足够大的轨道 Ω。

令 $N := G^{(\Omega)}$ 为该轨道的逐点稳定子。成立 $N \lhd G$，且因子 G/N 同构于 G^{Ω}，即 G 在 Ω 上的作用。令 $\Delta := [d]\setminus\Omega$ 为该轨道的补集。现在应用引理 86。它说明，必须作为合成因子出现在 G 中的大型交错群，要么同构于 G/N，要么是 N 或 G/N的合成因子。

若 **交错群**$_m$ 是 N的合成因子，则对 $N^\Delta \cong N$应用归纳假设。由此在情况 (i) 中得到一个子群 $H \le N \le G$ 和一个集合 $A \subseteq [d]\setminus \Delta$，满足 $|A| \ge c\cdot n$ 是一个 H-轨道，并且满足 **交错群**$(A) \le H^{(\Delta\setminus A)}$。注意，归纳过程中只有次数 d减小，而对每个群 G_n，$c\cdot n$ 保持不变。因此，通过归纳得到的集合 A 的大小确实为 $\ge cn$。由于 N 逐点固定 Ω，H也如此，因此有**交错群**$(A) \le H^{([d]\setminus A)}$。所以对 G也有情况 (i)。

若 N 适用情况 (ii)，则令 $d' := |\Delta|$ 为 $N^\Delta \cong N$ 的次数。由归纳假设可得 [**对称群**$_d^{(\Omega)}$: $N] =$ [**对称群**(Δ): $N] \ge \frac{1}{n}\cdot \left(\frac{2d'\cdot\alpha}{e}\right)^{cn/2}\cdot \alpha^\ell$。我们有

$$[\mathbf{Sym}_d : N] = [\mathbf{Sym}_d : \mathbf{Sym}_d^{(\Omega)}]\cdot[\mathbf{Sym}_d^{(\Omega)} : N] = (d!/d'!)\cdot[\mathbf{Sym}_d^{(\Omega)} : N].$$

由于 $N \le G \le$**对称群**$_d$，我们也有 [**对称群**$_d$: $N] =$ [**对称群**$_d$: $G]\cdot$ [G: $N]$。我们知道 [G: $N] \le (d-d')!$，因为 [G: $N]$ 是 G/N 的阶，其置换域为 Ω。总之，对于 [**对称群**$_d$，使用斯特林近似 $n! \approx \sqrt{2\pi n}\cdot\left(\frac{n}{e}\right)^n$:，可得 G]

$$\begin{aligned}
[\mathbf{Sym}_d : G] = \frac{[\mathbf{Sym}_d : N]}{[G : N]} &\ge \frac{d!}{d'!\cdot(d-d')!}\cdot\frac{1}{n}\cdot\left(\frac{2d'\cdot\alpha}{e}\right)^{cn/2}\cdot\alpha^\ell \\
&\approx \frac{1}{n}\cdot\left(\frac{2d'\cdot\alpha}{e}\right)^{cn/2}\cdot\alpha^\ell\cdot\frac{\sqrt{2\pi d}\cdot(d/e)^d}{d'!\cdot(d-d')!} \\
&= \frac{1}{n}\cdot\left(\frac{2d\cdot\alpha}{e}\right)^{cn/2}\cdot\alpha^\ell\cdot\frac{d^{d-(cn/2)}\cdot d'^{cn/2}\cdot\sqrt{2\pi d}}{d'!\cdot(d-d')!\cdot e^d} \\
&\approx \frac{1}{n}\cdot\left(\frac{2d\cdot\alpha}{e}\right)^{cn/2}\cdot\alpha^\ell\cdot\frac{d^{d-(cn/2)}\cdot d'^{cn/2}\cdot\sqrt{2\pi d}}{d'^{d'}\cdot(d-d')^{d-d'}\cdot 2\pi\sqrt{d'(d-d')}}
\end{aligned}$$

现在，由于 $d' \ge cn$ （否则 N 不可能以 **交错群**$_m$ 作为合成因子），我们可以用分子中的 d–$(cn/2)$ 个 d-因子支配分母中的所有因子 $(d-d')$。由此得到：

$$\begin{aligned}
&\ge \frac{1}{n}\cdot\left(\frac{2d\cdot\alpha}{e}\right)^{cn/2}\cdot\alpha^\ell\cdot\frac{d^{d'-(cn/2)}\cdot\sqrt{2\pi d}}{d'^{d'-(cn/2)}\cdot 2\pi\sqrt{d'(d-d')}} \\
&\ge \frac{1}{n}\cdot\left(\frac{2d\cdot\alpha}{e}\right)^{cn/2}\cdot\alpha^\ell\cdot\frac{(1+(c/(1-c)))^{d'-(cn/2)}}{\sqrt{2\pi d'}}
\end{aligned}$$

在最后一步中，我们用到了 $d/d' \ge (d'+cn)/d' \ge 1+\frac{c}{1-c}$。这是因为 $d-d' \ge cn$根据 Ω 的选取（因此，$d' \le (1-c)n$）。此外，我们约去了 $\sqrt{d}$和 $\sqrt{d-d'}$。现在，指数 d'–$(cn/2)$ 至少为 $d'/2$（因为 $d' \ge cn$），底数是某个常数>1，因此可以验证，右侧因子中的整个分式是 ≥ 1，除非 d'，因而 cn 小于某个依赖于 c的常数。因此，对于足够大的 n，我们可以去掉右侧的因子，剩下：

$$\ge \frac{1}{n}\cdot\left(\frac{2d\cdot\alpha}{e}\right)^{cn/2}\alpha^\ell.$$

因此，对于 G，情况 (ii) 成立。接下来需要处理大型交错群是 $G/N \cong G^\Omega$ 的合成因子，或与 G/N 同构的情况。在后一种情况下，G 在 Ω 上的作用为 **交错群**$_m$，其中 $m = |\Omega| \ge cn$。如果 **交错群**$(\Omega) \le G^{(\Delta)}$，那么结论成立，且对于$G$，情况 (i) 成立。如果 G 在逐点固定 Δ 时的作用并非 **交错群**(Ω)，那么根据引理 87，对于每个$g \in G$，g 对 Ω 的作用完全由 g 对 Δ 的作用决定。因此，$|G| \le |\Delta|! = d'!$。于是 [**对称群**$_d$: $G] \ge \frac{d!}{d'!}$。由于 $|\Omega| \ge cn$，我们有 $d' \le d - cn$。因此

$$[\mathbf{Sym}_d : G] \ge \frac{d!}{d'!} \ge \frac{d!}{(d-cn)!} \ge \left(\frac{d}{e}\right)^{cn}\cdot\sqrt{d/(d-cn)} \ge \left(\frac{2d}{e\cdot\lfloor c^{-1}\rfloor!}\right)^{cn/2} = \left(\frac{2d\cdot\alpha}{e}\right)^{cn/2}.$$

第三个不等式再次用到了阶乘的斯特林近似，最后一个不等式成立是因为 $\frac{d}{e} \geq \frac{2}{c-1}$。因此，若这种情况发生，则对于 G，情况 (ii) 成立（情况 (ii) 中额外的因子 $\frac{1}{n} \cdot \alpha^{\ell}$ 只会使表达式更小）。

如果 G/N 不同构于交错群，那么 m 必须是 $G/N = G^{\Omega}$ 的一个合成因子。我们应用归纳假设。同样，这会使 G/N 有两种可能的情况。在情况 (i) 中，存在 $H \leq G^{\Omega}$ 以及 H 的一个轨道 $A \subseteq \Omega$，使得 $|A| \geq c \cdot n$，且 **交错群**$(A) \leq H^{(\Omega \setminus A)}$。接着，令 H' 为 G 的一个子群，其在 Ω 上的限制为 H。如果 **交错群**$(A) \leq H'^{([d] \setminus A)}$，那么对于 G，我们就得到了情况 (i)，其见证为 H'。否则，我们再次使用引理 87，该引理指出，H' 在 A 之外的作用决定了其在 A 上的作用。我们断言，对于 G 本身，这一点也成立；也就是说，不存在两个 $g, g' \in G$，它们在 A 上不同，却在 $[d] \setminus A$ 上相同。

断言的证明：如果断言不成立，那么 $G^{([d] \setminus A)}$ 是非平凡的。因此，$G^{([d] \setminus A)}$ 不是 H' 的子群，否则，H' 对 A 的作用将无法由其在 A之外的作用决定。如果 $G^{([d] \setminus A)}$ 不是 H'的子群，那么 $(G^{([d] \setminus A)})^{\Omega}$ 也不是 H的子群。但我们总可以假设 H 包含 $(G^{([d] \setminus A)})^{\Omega}$：即使将 $G^{([d] \setminus A)}$中的所有置换都加入 H，**交错群**$(A) \leq H^{(\Omega \setminus A)}$ 这一事实仍然成立。这至多会使 $H^{(\Omega \setminus A)}$ 从**交错群**(A)变为**对称群**(A)。因此，我们可以假设 H 使得断言成立，并且 G 对 A 的作用确实由其在 $[d] \setminus A$上的作用决定。

由此可得 $|G| \leq (d - |A|)!$，又由于 $|A| \geq cn$，我们得到[**对称群**$_d$ 的相同下界：与上面 $G/N \cong$ **交错群** $_m$ 的情况相同。因此，在这种情况下，情况 (ii) 适用于 G。

接下来需要检查归纳法对 G/N 得出情况 (ii) 时会发生什么。此时有 [**对称群**(Ω) : $G/N] \geq \frac{1}{n} \cdot \left(\frac{2}{e}^{(d-d') \cdot \alpha}\right)^{cn/2} \cdot \alpha^{\ell}$。它成立

$$|G/N| = |\mathbf{Sym}(\Omega)|/[\mathbf{Sym}(\Omega) : G/N] = \frac{(d-d')!}{[\mathbf{Sym}(\Omega) : G/N]}.$$

我们有 $|G| = |N| \cdot |G/N|$，并且有 $|N| \leq d'!$ 我们可以得到与之前类似的不等式链：

$$\begin{aligned}
[\mathbf{Sym}_d : G] &= \frac{d!}{|G|} = \frac{d!}{|N| \cdot |G/N|} \\
&\geq \frac{d! \cdot (2(d-d')\alpha)^{cn/2} \cdot \alpha^{\ell}}{d'! \cdot (d-d')! \cdot n \cdot e^{cn/2}} \\
&\approx \frac{1}{n} \cdot \left(\frac{2d\alpha}{e}\right)^{cn/2} \cdot \alpha^{\ell} \cdot \frac{d^{d-(cn/2)} \cdot (d-d')^{cn/2} \cdot \sqrt{2\pi d}}{d'^{d'} \cdot (d-d')^{d-d'} \cdot 2\pi\sqrt{d'(d-d')}} \\
&\geq \frac{1}{n} \cdot \left(\frac{2d\alpha}{e}\right)^{cn/2} \cdot \alpha^{\ell} \cdot \frac{d^{d'}}{d'^{d'} \cdot \sqrt{2\pi \cdot d'}} \qquad (\star)
\end{aligned}$$

在最后一步中，我们将分母中的所有因子 $(d - d')$ 与分子中的因子 d 和 $(d - d')$ 约去，并且还去掉了 $\sqrt{d}^{d}$。现在我们几乎可以像之前的情形那样继续，不过需要进行分类讨论。重要的区别在于，现在我们没有 d' 的下界，因为这次因子 **交错群**$_m$ 属于 G^{Ω}，所以 $[d] \setminus \Omega$ 可能任意小（至少为 1，因为它至少包含一个轨道）。我们区分 $d' \geq cn$ 和 $d' < cn$这两种情形。先来看后一种情形。和上面一样，我们有$d/d' \geq (d' + cn)/d'$，因为这只取决于 $|\Omega| \geq cn$这一事实，而根据 Ω 的选取，这一点仍然成立。若 $d' < cn$，则有：$d/d' \geq (d' + cn)/d' \geq 2$。因此，$(\star)$中的右侧因子至少为 $\sqrt{2^{d'}}^{d'}$。对于 $d' \geq 2$的所有取值，它都大于 1。若 $d' = 1$，那么

我们可以用不同的方法论证。此时，(⋆)中的右侧分数等于 $d/\sqrt{2\pi}$；对于足够大的 n，它也大于 1（因为 $d \geq cn$）。若 $d' \geq cn$，我们沿用之前的论证，并使用界 $d/d' \geq (d'+cn)/d' \geq 1 + \frac{c}{1-c}$。那么，(⋆)中的右侧因子至少为 $(1+\frac{c}{1-c})^{d'}$。同样，对于足够大的 d'，这就是 ≥ 1。由于 $d' \geq cn$，当 n 足够大时，这一情况便会发生。因此，在所有情形下，我们都可以去掉右侧因子，这样乘积只会变小。总之，我们有

$$[\mathbf{Sym}_d : G] \geq \frac{1}{n} \cdot \left(\frac{2d \cdot \alpha}{e}\right)^{cn/2} \alpha^{\ell},$$

如所需。这就完成了 G 为非传递的情形。

情形 2： G 是传递的，但不是本原的。
在这种情况下， G 具有一个非平凡的块系。设 $N \lhd G$ 为逐块保持每个块不变的正规子群。于是， G/N 是 G 在块集合上的作用。同样，根据引理 86，大型交错群或者是 N 的合成因子，或者是 G/N 的合成因子，或者同构于 G/N。在后一种情况下，(ii) 适用于 G：如果对于某个 $m \geq c \cdot n$， $G/N \cong \mathbf{Alt}_m$，那么该块系有 $m \leq d/2$ 个块。每个块的大小为 t，且 $2 \leq t \leq \lfloor c^{-1} \rfloor$（注意，只有当 $c \leq \frac{1}{2}$ 时这种情形才可能发生）。于是我们有 $|G| \leq (t!)^m \cdot m!$ 因此，

$$\begin{aligned}[\mathbf{Sym}_d : G] &\geq \frac{d!}{(t!)^m \cdot m!} \geq \frac{d!}{(t!)^m \cdot (d/2)!} \\ &\geq \frac{\sqrt{2} \cdot (2d/e)^{(d/2)}}{(t!)^{(d/2)}} \geq \left(\frac{2d \cdot \alpha}{e}\right)^{d/2} \\ &\geq \left(\frac{2d \cdot \alpha}{e}\right)^{c \cdot n/2} \geq \frac{1}{n} \cdot \left(\frac{2d \cdot \alpha}{e}\right)^{c \cdot n/2} \cdot \alpha^1.\end{aligned}$$

最后一步成立是因为 $\alpha \leq 1$。下一种情形是 $\mathbf{Alt}_m$ 是 G/N 的合成因子。此时我们也不需要归纳步骤，可以立即对 $[\mathbf{Sym}_d : G]$ 得出与上面相同的下界。这是因为，如果 $\mathbf{Alt}_m$ 是 G/N 的合成因子，则 G/N 的次数至少为 $m \geq cn$，因此块数也必须大于 cn，而块大小至多为 $\lfloor c^{-1} \rfloor$。

仍然有 N 含有**交错群**$_m$ 作为合成因子。我们对 N应用归纳假设。若 N满足情况 (i)，那么我们立即知道 G也满足情况 (i)，因为此时存在某个 $H \leq N \leq G$ （特别是 $H \leq G$）以及一个H-轨道 $A \subseteq [d]$，使得**交错群**$(A) \leq H^{([d] \setminus A)}$ （这比之前更容易，因为现在 N 和 G具有相同的置换域）。
反之，若 N满足情况 (ii)，则 [**对称群**$_d$: $N] \geq \frac{1}{n} \cdot \left(\frac{2d \cdot \alpha}{e}\right)^{c \cdot n/2} \cdot \alpha^{\ell-1}$。
每个块的大小至少为 $c \cdot n$，因为 N 以该次数的交错群为合成因子，并且这些块是 N 的轨道。若这些轨道小于 $c \cdot n$，那么正如我们在非传递情形中已经论证的那样， N 不可能以该次数的群为合成因子。因此，块数至多为 $\lfloor c^{-1} \rfloor$，所以，$|G/N| = [G : N] \leq \lfloor c^{-1} \rfloor !$
总计，我们有

$$\begin{aligned}[\mathbf{Sym}_d : G] &= [\mathbf{Sym}_d : N]/[G : N] \geq \frac{1}{n} \cdot \left(\frac{2d \cdot \alpha}{e}\right)^{c \cdot n/2} \cdot \frac{\alpha^{\ell-1}}{\lfloor c^{-1} \rfloor !} \\ &= \frac{1}{n} \cdot \left(\frac{2d \cdot \alpha}{e}\right)^{c \cdot n/2} \cdot \alpha^{\ell}.\end{aligned}$$

这就完成了传递非本原情形的证明。

情形 *3*： G是本原的。
剩下的情况是 G 为本原。由于 G 以交错群$_m$ 为合成因子，且$m \geq cn$，我们得到 G的阶为：$|G| \geq (cn)!/2 \approx \frac{1}{2}\left(\frac{cn}{e}\right)^{cn} \cdot \sqrt{2\pi cn} \geq n^{1+\log n} \geq d^{1+\log d}$。因此，根据定理 85， G 有一个指数为 $\leq d$ 的正规子群 N，使得 N 拥有一个块系，并在其上作为 Johnson 群交错群$_k^{(t)}$ 作用，其中 $k \geq \log d$。这里， k 是置换域的大小， t 是 Johnson 作用中定义在 $[k]$ 上的元组长度。由于 N 在 G 中的指数为 $\leq d$， G/N 的阶至多为 d，因此它太小，不可能以交错群$_m$为合成因子。因此， N 必定以交错群$_m$ 为合成因子。现在， N在其块系的各块上作为交错群$_k^{(t)}$ 作用。我们有 $k \geq \log d$，且每个块都对应于定义在一个 k元素域上的 t元组。因此，块数为 $k^t \geq (\log d)^t$。由此，块大小至多为 $d/(\log d)^t$。即使对于 $t = 1$，这也渐近地小于cn（回想一下 $d \leq n$）。所以，如果 n 足够大，那么我们要找的交错群就不可能是块稳定子 $N' \lhd N$（其轨道就是这些块）的因子，而必须是 N/N'的因子；后者是 N 在这些块上的作用。这要求块数为 $\geq cn$。那么，块大小至多为 $\mathsf{b}c^{-1}\mathsf{c}$，与上文情形 2 中一样。如果块大小为$\geq 2$，那么通过与情形 2 完全相同的计算，我们得到 [对称群$_d$： $N] \geq \left(\frac{2d\alpha}{e}\right)^{cn/2}$。接下来

$$[\mathbf{Sym}_d : G] = [\mathbf{Sym}_d : N]/[G : N] \geq \frac{1}{n} \cdot \left(\frac{2d \cdot \alpha}{e}\right)^{cn/2}.$$

这里，我们利用了 $[G :\ N] \leq d \leq n$。因此，我们得到了 G 的所需指数界，无需进一步递归。若 N 的块系是平凡的，且块都是单元素集合，则必有 $t = 1$：若 $t \geq 2$，则 N 同构于作用在 $\leq \sqrt{d} < cn$ 个点上的交错群。交错群除了平凡群和自身之外没有其他正规子群，因此在这种情况下， N 不可能以 **交错群**$_m$ 作为合成因子。因此剩下的情况是 $t = 1$，且 $N =$ **交错群**$_d$。由于 $N \leq G$，于是对 G，情况 (i) 成立。◀

现在，我们将这个引理与文献中的以下结果结合起来。该结果保证，任何足够大的群都存在一个大型交错群作为合成因子。

▶ **引理 89** (引理 2.2，见 [3])。 设 G 是一个次数为 n 的置换群。若 G 没有与次数为 $> C$ 的交错群同构的合成因子，则 $|G| \leq C^{n-1}(C \geq 6)$。

由此可得有界指数群的以下推论：

▶ **推论 90.** 设$(G_n)_{n\in\mathbb{N}}$ 是一个群族，使得对所有 n, $G_n \leq$**对称群**$_n$均成立。假设存在某个常数 $k \in \mathbb{N}$，使得渐近地有 [**对称群**$_n$： $G_n] \leq 2^{nk}$。那么存在一个函数 $f(n) \in \Theta(n)$，使得对所有足够大的 n， G_n 都含有一个与**交错群**$_m$同构的合成因子，其中某个 $m \geq f(n)$。

证明。令 $f(n)$： $\mathbb{N} \longrightarrow \mathbb{N}$ 为出现在 G_n 的合成因子中的交错群的最大度的最小上界。我们需要证明 $f(n)$ 关于 n 是线性的。假设 $f(n) \in o(n)$，以导出矛盾。令 $g(n) := f(n) + 1$，例如。于是 $g(n) \in o(n)$，并且对所有足够大的 n， G_n 都没有同构于 Alt$_{g(n)}$ 的合成因子。根据引理 89，我们有 $|G_n| \leq g(n)^{n-1}$。于是得到指数：

$$[\mathbf{Sym}_n : G_n] \geq \frac{n!}{g(n)^{n-1}}.$$

使用斯特林近似，我们得到：

$$\frac{n!}{g(n)^{n-1}} \approx \Big(\frac{n}{e\cdot g(n)}\Big)^{n-1}\cdot\Big(\frac{n\cdot\sqrt{2\pi n}}{e}\Big).$$

由于 $g(n)$ 是次线性的，因此比值 $e \overset{n}{\longrightarrow} g(n)$ 不受任何常数的上界约束，所以对于每个常数 $k\in\mathbb{N}$，都有 $[\textbf{对称群}_n : G_n] > 2^{nk}$。这就产生了矛盾，因此 $f(n)$ 必须是线性的。◀

最后，我们可以将所有结果结合起来，证明引理 74。

引理 74 的证明。推论 90 指出，所有足够大的 G_n 都有一个与 **交错群**$_m$同构的合成因子，其中 $m\geq f(n)$，对于某个函数 $f(n)\in\Theta(n)$。存在一个常数$0<c\leq 1$ 使得 $f(n)=c\cdot n$。因此，引理 88 适用（其中 $d:=n$）。

现在我们要证明，对于任意一个 G_n，引理 88 中的情况 (ii) 都不可能发生。反设 $[\textbf{对称群}_n : G_n] \geq \frac{1}{n}\cdot\binom{2n\cdot\alpha}{e}^{cn/2}\cdot\alpha^{\ell}$ 对某个足够大的 n 成立。首先，我们对 ℓ 作上界估计。在引理 88 中，它被定义为递归过程中传递非本原情形出现的次数。检查证明可知，只有当 G 是传递非本原群，并且 目标合成因子 **交错群**$_m$ 位于块稳定子 $N\lhd G$ 中时，这种情形才会出现。在这种情形下，块大小必须是 $\geq cn$。每当这种情形出现时，我们都会继续处理非传递情形，其中各轨道就是这些块；这意味着最终得到的群的次数至多等于 G 的块系的块大小。因此，每当我们遇到传递非本原情形并继续递归时，次数至少减半。我们只能这样做，直到次数降到 cn 以下，所以有 $\ell\leq\log\ n$（实际上，这个上界还能更小，但 $\log n$ 已经远比我们实际所需的紧得多）。因此，

$$\begin{aligned}[\mathbf{Sym}_n : G_n] &\geq \frac{1}{n}\cdot\Big(\frac{2n}{e\cdot\lfloor c^{-1}\rfloor!}\Big)^{cn/2}\cdot\Big(\frac{1}{\lfloor c^{-1}\rfloor!}\Big)^{\log n}\\ &\geq \Big(\frac{2n}{e\cdot\lfloor c^{-1}\rfloor!^2}\Big)^{cn/2}\end{aligned}$$

现在，对于我们可以选取的每个常数 $k\in\mathbb{N}$，2^{kn} 都可以写成 a^n，其中 a 是某个常数（可以任意大，但仍为常数）。将上述表达式与 a^n 进行比较，我们得到：

$$\begin{aligned}\frac{[\mathbf{Sym}_n : G_n]}{a^n} &\geq \Big(\frac{2n}{e\cdot(c^{-1})!^2}\Big)^{cn/2}\cdot\frac{1}{a^n}\\ &= \Big(\frac{2n}{a^{2/c}\cdot e\cdot(c^{-1})!^2}\Big)^{cn/2}.\end{aligned}$$

显然，对于任意常数 a，当取极限时，这个分数趋于无穷大。因此，如果 $[\textbf{对称群}_n : G_n]$ 有上界 2^{kn}，那么对于所有足够大的 n，引理 88 的情况 (ii) 不可能适用于 G_n。◀

现在我们可以利用引理 74 证明定理 75：

▶**定理 75**。设 $k\in\mathbb{N}$ 是一个常数，且 $(G_n)_{n\in\mathbb{N}}$ 是一个群族，使得$G_n \leq$**对称群**$_n$，并且对于所有足够大的 n，$[\textbf{对称群}_n : G_n] \leq 2^{nk}$。那么，$\mathbf{SP}_A(G_n)$ 中单元素部分的数量至多以次线性速度增长。换言之：不存在常数 $0<c\leq n$，使得对于所有足够大的 n，都存在一个大小为 $|\Delta_n|\geq cn$ 的 $\Delta_n\subseteq[n]$，使得$\mathbf{SP}_A(G_n)$仅包含单元素部分。

证明。 反设存在一个常数 $0 < c \leq 1$，使得对于每个足够大的 n，都存在一个子集 $\Delta_n \subseteq [n]$，其大小为 $|\Delta_n| \geq cn$，且恰好由 $\mathbf{SP}_A(G_n)$中单元素部分里的元素构成。接下来，我们假设 Δ_n 的大小不仅有线性下界，而且还存在另一个常数 $1 > d > c$，使得 $|\Delta_n| \leq dn$，对所有足够大的 n均成立。最后我们再处理另一种情况。

令 $H_n := (G_n^{([n]\setminus\Delta)})^{\Delta}$ 为 G_n 的子群，该子群固定 Δ 之外的每个点，并将其作用限制在 Δ 上。现在我们证明，对每个 $k \in \mathbb{N}$，都有 $[\mathrm{Sym}(\Delta) : H_n] > 2^{nk}$。事实上，如果存在一个 $k \in \mathbb{N}$，使得对于所有足够大的 n，都有 $[\mathrm{Sym}(\Delta) : H_n] \leq 2^{nk}$，那么根据引理 74，所有 H_n 都会有一个子群 H_n'，其中包含一个大小为$|A| \geq c' \cdot |\Delta|$的轨道 A 上的交错群；这里 c' 是引理中的常数。更确切地说，$\mathrm{Alt}(A) \leq H_n'^{(\Delta\setminus A)}$。因此， A 上每个偶置换（在 Δ 中固定 A 之外的一切）都包含在 H_n 中；又由于 H_n 是 G_n 的一个子群，且固定 Δ 之外的一切，这意味着 $\mathrm{Alt}(A) \leq G^{([n]\setminus A)}$。但这样一来， $A \subseteq \Delta$ 就会是最粗交错支撑划分 $\mathrm{SP}_A(G_n)$ 的一个部分。这与 $\mathrm{SP}_A(G_n)$ 在 Δ 上只有单元素部分这一事实矛盾。因此，对每个 $k \in \mathbb{N}$，必有 $[\mathrm{Sym}(\Delta_n) : H_n] > 2^{nk}$。

下一步，我们计算出这意味着违反了如下假设：对于某个 k， $[\mathbf{对称群}_n : G_n]$可以由 2^{nk} 上界。也就是说，如果对所有 $k \in \mathbb{N}$ 都有 $[\mathbf{对称群}(\Delta_n) : H_n] > 2^{nk}$，那么对于每种 k 的选择，都有 $|H_n| < \frac{|\Delta_n|!\,2^{nk}}{}$。于是我们还有 $|G_n| < |\Delta_n|!\,2^{nk} \cdot (n - |\Delta_n|)!$。这是因为根据引理 73， G_n 中的每个元素都逐集合稳定 $\mathbf{SP}_A(G_n)$，因此尤其会将单元素部分映射到单元素部分；所以， $[n] \setminus \Delta$ 是 G-轨道的并，因此 H_n 在 G_n 中正规。由此可得，对于每个 $k \in \mathbb{N}$，其指数为：

$$[\mathbf{Sym}_n : G_n] = \frac{n!}{|G_n|} > \frac{n! \cdot 2^{nk}}{|\Delta_n|! \cdot (n - |\Delta_n|)!}.$$

由于 $cn \leq |\Delta_n| \leq dn$，我们有 $|\Delta_n| \leq dn$ 和 $n - |\Delta_n| \leq (1 - c)n$。因此可以继续：

$$\begin{aligned}\frac{n! \cdot 2^{nk}}{|\Delta_n|! \cdot (n - |\Delta_n|)!} &\geq \frac{n! \cdot 2^{nk}}{(dn)! \cdot ((1 - c)n)!} \\ &\approx 2^{nk} \cdot \left(\frac{1}{d}\right)^{dn} \cdot \left(\frac{1}{1 - c}\right)^{(1-c)n} \cdot \frac{1}{\sqrt{2\pi \cdot d(1 - c) \cdot n}}\end{aligned}$$

由于 $d < 1$ 且 $(1 - c) < 1$，上述乘积大于 2^{nk} （当 n足够大时）。因为这个关于 $[\mathbf{对称群}_n : G_n]$ 的下界对每个 $k \in \mathbb{N}$都成立，我们可以得出，对于每个 k，都有$[\mathbf{对称群}_n : G_n] > 2^{nk}$。然而，定理 75 的假设表明，存在一个 $k \in \mathbb{N}$，使得对于所有足够大的 n，$[\mathbf{对称群}_n : G_n] \leq 2^{nk}$。这就产生了矛盾。这证明了当 $|\Delta_n|$ 可由某个线性函数$d \cdot n$（对 $d < 1$）上界时的定理。对于所有 $d < 1$， $|\Delta_n| > dn$的情形不可能发生：将引理 74 应用于 G_n 可知， G_n 包含一个线性度的交错群（它逐点固定其余部分）。因此，对于所有足够大的 n，$\mathbf{SP}_A(G_n)$ 必须至少有一个部分具有线性大小。所以，不可能在$\mathbf{SP}_A(G_n)$中， $[n]$ 中除次线性多个元素外的所有元素都处于单元素部分中。◀