arXiv:2512.23121v1 [cs.CC] 29 Dec 2025

路径宽度有界图上的连通性问题之纯动态规划下界 *

Kacper Kluk† Jesper Nederlof‡

摘要

我们针对纯动态规划算法给出了无条件的参数化复杂性下界。这类算法以热带电路 为模型，可用于求解旅行商问题等连通性问题。我们的下界高于当前依赖代数方法的最快算法所达到的下界，这表明，若要获得有竞争力的最坏情况运行时间，这些代数方法不可或缺。

具体而言，我们研究树宽和路径宽度等宽度参数较小的输入图，并证明，对于任意 k，都存在一个路径宽度至多为 k 、且有 $k^{O(1)}$ 个顶点的图 G，使得任何用于计算旅行商环游最优值的热带电路都至少需要 $2^{\Omega(k \log\log k)}$ 个门。我们通过将热带电路复杂度与特定兼容性矩阵的非确定性通信复杂度联系起来，确立了这一结果。这些矩阵编码了两个部分解能否组合成一个完整解，而 Raz 和 Spieker [此前已在 Combinatorica 1995] 中证明了这一复杂度度量的一个下界。

1 引言

理论计算机科学中一种常见的研究范式，是通过在精确的算法模型中形式化某种算法技术，然后证明该模型存在严格的局限，从而明确哪些算法技术能够或不能实现某些核心目标。经典例子包括线性规划算法的无条件下界（即扩展复杂性 [FMP+15, Rot17]）、参数化复杂性中预处理算法的条件下界（以多项式层级不会坍缩为前提 [BDFH09, FS11]），以及用于反驳强指数时间假设的基于归结的算法的无条件下界 [BI13]。这一范式揭示了哪些算法细节从根本上不可避免，也让我们知道真正的突破必须从何而来。

这类算法细微之处的一个显著例子是代数消去：对于若干组合计算问题，目前已知的最快算法都以相当违反直觉的方式，关键性地利用了某些代数消去。一个长期受到深入研究的开放问题是，这些算法能否由（更自然且在某种意义上更稳健的）“组合”算法匹敌。这个问题出现在诸如布尔矩阵乘法 [VW18], ，以及通过归约到行列式计算来求解完美匹配问题的各种变体 [KUW86, MVV87], ，还有求解哈密顿性的快速指数时间算法 [Bjö14]等情形中。是否必须使用代数消去这一问题，不仅出现在算法设计中，也出现在其他多个领域。例如，在极值组合学中，人们在各种情形下仍未解决组合证明能否匹敌代数证明这一问题（例如，关于斜两族的组合证明

*K.K. 获得波兰国家科学中心 SONATA BIS-12 项目资助，项目编号为 2022/46/E/ST6/00143。J.N. 获得 COALESCE 项目资助，该项目由欧洲研究理事会（ERC）资助，资助协议编号为 853234。

†波兰华沙大学信息学研究所。k.kluk@uw.edu.pl。
‡荷兰乌得勒支大学信息与计算科学系。j.nederlof@uu.nl。

定理仍未明朗 [Cal23]）；而通信复杂度中的对数秩猜想则探讨矩阵的代数低秩分解是否通常意味着低秩组合分解（或者更具体地说，布尔矩阵的秩与划分数是否存在准多项式关系），例如参见 [Lov14]。

在参数化复杂性领域中，我们希望用组合论证取代代数论证的一个场景，是以树宽为参数的连通性问题：2011 年，有研究表明，许多以树宽为参数的连通性问题都能比当时认为可能的速度更快地求解 [CNP+22]。具体而言，对于给定一个宽度为 k、包含 N 个顶点的输入图的树分解，哈密顿回路和斯坦纳树等问题可以通过随机化算法在 $2^{O(k)}N^{O(1)}$ 时间内求解。在这项工作之前，以树宽为参数的问题中已知的最快算法基于直接的组合动态规划技术，这些技术自然会导致形如 $k^{O(k)}N^{O(1)}$ 的运行时间，而且似乎很难进一步改进。后续研究沿用了 [CNP+22] 的思路，为有界树宽图上的旅行商问题（TSP）等问题的加权扩展提供了确定性算法 [BCKN15]；另一种变体则将该方法与上述双族定理的一种基于拟阵的扩展联系起来 [FLPS16]。

所有这些工作 [CNP+22、BCKN15、FLPS16] 都依赖于代数消去，其利用了某些兼容性矩阵的秩较小这一事实。与此前简单而简洁的组合 $k^{O(k)}N^{O(1)}$ 时间算法相比，这是一种尤其反直觉的方法。如何消除确定性算法和加权扩展在运行时间中所提到的额外开销，是一个值得关注的开放问题。例如，如果这一开放问题得到肯定解决，我们将更接近于以时间 1.9999^N [Ned20], 解决旅行商问题，其中 N 是城市的数量。

但是，要做到这一点，似乎必须更好地从组合角度理解所涉及的兼容性矩阵，同时避开不理想的代数消去论证。在本文中，我们通过热带电路这一算法模型，给出了强有力的迹象，表明仅仅采用初等组合技术是不够的。

热带电路。热带电路是一种算术电路，其中输入标记为变量，这些变量取整数值；两个算术门分别对应最大值与求和运算，或者最小值与求和运算。精确定义见第 2 章节。研究热带电路表达能力的动机在于，它能够建模一大类动态规划算法。具体而言，对于一个最大化问题（其每个实例由一组输入权重定义），如果存在一种“纯粹”的动态规划算法，即其对应的递推关系只包含最大值和求和运算，那么就存在一个热带电路，能够输出最优目标值，且其电路规模与该动态规划算法的运行时间成正比。

例如，经典的 Bellman-Held-Karp [Bel62, HK62] $O(N^2 2^N)$ 时间旅行商问题算法，可以自然地转换为一个具有 $O(N^2 2^N)$ 个门的热带电路；而计算每对顶点之间最短路径长度的 $O(N^3)$ 时间 Floyd-Warshall [Flo62, War62] 算法，也可以自然地转换为一个具有 $O(N^3)$ 个门的热带电路。这两个热带电路都无法得到实质性的改进 [JS82, Ker70]（另见 [Juk23, 推论 2.2]）。

在参数化复杂性的领域，很容易看出，动态规划的典型应用可以高效地建模为热带电路。例如，终端点和元素数量较少时，斯坦纳树和集合覆盖的动态规划算法（例如参见 [CFK+15, 第 6.1] 节）；以及与本文尤为相关的，在给定宽度为 k、具有 N 个顶点的树分解的图上求解最大独立集问题的 $O(2^k N)$ 时间算法。

关于热带电路的更多详细内容，请参阅 Jukna [Juk23] 撰写的优秀教科书。

以树宽为参数的问题。一条非常热门的研究方向始于 [LMS18a, LMS18b]，旨在研究各种NP困难问题在以输入图的树宽等宽度度量为参数时的细粒度复杂性。特别是，对于许多 NP困难问题，我们现在能够设计出运行时间为$f(k)N^{O(1)}$的算法，其中 k和 n分别表示某种宽度度量以及输入图的顶点数；同时还能证明，将运行时间改进至 $f(k)^{1-\Omega(1)}N^{O(1)}$ 甚至 $f(k)^{o(1)}N^{O(1)}$ 的任何做法，都会违背指数时间假设（ETH）或强指数时间假设（SETH）。这类算法通常称为*(S)ETH*紧确算法。这类紧确算法有助于洞察相关问题对分治算法的适用程度，因为在标准假设成立的条件下，它们揭示了部分子解中究竟有多少信息是确切相关的。

上述这类连通性问题，例如旅行商问题和斯坦纳树，构成了一类重要问题。对于这类问题，我们通常还没有达到 SETH 紧致的算法，恰恰是因为所采用的代数算法构成了瓶颈，阻碍了确定性算法以及加权变体的扩展，而这些似乎本应由组合论证取代。

我们的结果。本文通过给出热带电路的无条件下界，提供证据表明，仅靠直接的组合技术不足以设计出更快的连通性问题算法。我们用输入图的路径宽度来表述下界。这与图的树宽类似，不同之处在于，我们要求以更具体的路径式而非树状方式分解图。因此，图的路径宽度总是不小于图的树宽，所以我们的下界也蕴含以树宽为参数的下界。定义见第 2 章。在研究连通性问题之前，我们先研究一个更基础问题的复杂度：

最大权独立集。在最大权独立集问题中，给定一个图 $G=(V,\ E)$，以及每个 $v\in V$对应的顶点权重 x_v，要求计算以下值 $IS_G := \max_{I\in\mathcal{I}(G)}\sum_{v\in I}x_v$，其中 $\mathcal{I}(G)$ 表示 G的所有独立集构成的集合。我们对该问题给出的下界如下（完整定义将在第 2 章节中给出）：

定理 1.1。对于任意 $k\geq 1$，存在一个含有 $k^{O(1)}$ 个顶点、路径宽度至多为 k 的图 G，使得任何计算 IS_G 的热带电路都至少需要 $\Omega(2^k)$ 个门。

请注意，路径宽度是一种宽度度量，且始终不小于图的树宽。由于对于路径宽度为 k的 N 顶点图，存在一个大小为 $O(2^kN)$的简单热带电路来计算 IS_G，因此从紧确的意义上说，这一结果是最优的。Korhonen [Kor21] 此前证明，对于树宽为 k、最大度为 d 的每一个图 G，任何计算IS_G 的热带电路大小都至少为 $2^{\Omega(k/d)}$。这一结果不如我们的新结果紧确，而且似乎关键依赖于最大权独立集问题的某些性质。尽管 [Kor21] 所给出的普适下界类型颇为有趣，但在我们的最坏情况复杂度分析背景下，它并未带来直接的额外价值，因此本文不再进一步探讨。

定理 1.1 是通过以下两个要素得到的。我们证明其下界的图，是基于从合取范式可满足性到最大权独立集的经典归约中的思想构造的。热带电路规模下界本身，则是通过分析所谓矩形的结构得出的。矩形是一种组合概念，通常出现在热带电路的研究中，它刻画了热带电路某个节点计算出的部分解如何与电路其余部分所进行的计算相结合，参见例如 [Juk23]。

连通性问题。我们证明了以下图连通性问题的热带电路复杂度下界。设 G 是一个具有 N 个顶点的图，对于每一对不同的顶点 u 和 v，都有一条边权为 $x_{u,\ v}\in\mathbb{N}$ 的边。令 $\mathcal{H}(G)$ 表示所有序列的集合

由 $N+1$ 个顶点 $(u_i)_{i=0}^{N}$ 组成，满足 $u_0 = u_N$ 和 $u_0 \to u_1 \to \cdots \to u_{N-1} \to u_N$ 在 G 中构成一个有向哈密顿圈。我们将 $DTSP_G$ 定义为对所有 $(u_0, \ldots, u_N) \in \mathcal{H}(G)$ 取 $\sum_{i\in[N]} x_{u_{i-1},\, u_i}$ 的最小值。对于无向图，我们类似地定义其无向变体 TSP_G，同时对所有 $uv \in E(G)$，令变量 $x_{u,\, v}$ 和 $x_{v,\, u}$ 相同。

有了这些定义，我们可以陈述主要结果如下：

定理 1.2。对于任意 $k \geq 1$，存在一个图 G，其路径宽度至多为 k，且有 $k^{O(1)}$ 个顶点，使得任何用于计算 $DTSP_G$ 的热带电路都至少需要 $2^{\Omega(k \log\log k)}$ 个门。

定理 1.3。对于任意 $k \geq 1$，存在一个图 G，其路径宽度至多为 k，且有 $k^{O(1)}$ 个顶点，使得任何用于计算 TSP_G 的热带电路都至少需要 $2^{\Omega(k \log\log k)}$ 个门。

我们还针对有向生成树问题给出了类似的下界。令$\mathcal{T}(G)$表示所有函数 $p\colon V(G) \to V(G)$ 的族，其中恰有一个顶点$v \in V(G)$满足 $p(v) = v$，并且其余所有顶点 u 上的边（$p(u)\ u$）构成一棵以v 为根的出树（即一棵从根向外定向的树）。此外，我们定义 DST_G 为最小值$\sum_{v\in V(G):\, p(v)\neq v} x_{p(v),v}$，取遍所有 $p \in \mathcal{T}(G)$（即，DST_G 是 G的最小权重生成树）。

定理 1.4。对于任意 $k \geq 1$，存在一个图 G，其路径宽度至多为 k，且具有 $k^{O(1)}$ 个顶点，使得任何计算 DST_G 的热带电路都至少使用 $2^{\Omega(k \log\log k)}$ 个门。

通过改编教科书中的动态规划算法，可以直接获得关于 $DTSP_G$、TSP_G和 DST_G 的大小为 $k^{O(k)}N$ 的热带电路，其中 G 具有 N 个顶点，且路径宽度/树宽为 k。因此，下界与上界之间仍存在差距；事实上，这似乎与通信复杂度领域中的一个类似差距密切相关（详见第 7 章节）。尽管如此，我们的结果表明，目前针对 TSP 和有向斯坦纳树（其推广了 DST）的最快 $2^{O(k)}N$ 时间算法无法仅通过纯动态规划来匹配。

这三个结果的证明结合了定理 1.1 证明的基本要素与匹配兼容性矩阵的性质，后者定义如下。这个二元矩阵的行和列都由二分图的完美匹配索引，矩阵中的一个条目表示这两个完美匹配的并集是否构成一个哈密顿回路。该矩阵此前已在通信复杂度中的对数秩猜想背景下于 [RS95] 进行研究，其中给出了非确定性通信复杂度的一个下界以及其秩的一个上界。事实证明，该矩阵的（一个轻微变体的）秩对于研究哈密顿回路和 TSP 问题的复杂度也十分重要；这两个问题都分别以输入图的路径宽度/树宽和顶点数作为参数 [CLN18, CKN18, Ned20]。

我们的主要技术贡献在于，可以利用来自 [RS95] 的该矩阵非确定性通信复杂度下界，得到上述关于热带电路规模的下界。

组织结构。本文组织如下：第 2 章节给出本文其余部分所需的定义和预备工具。第 3 章节给出定理 1.1 的证明。第 4 章节介绍上述匹配兼容性矩阵，并给出关于其结构的必要结果。第 5 章节证明定理 1.2 和定理 1.3。第 6 章节证明定理 1.4，并在第 7 章节给出一些总结性评论。

2 预备知识

我们使用以下基本记号。对于正整数 ℓ，我们用 $[\ell]$ 表示集合$\{1, 2, \ldots, \ell\}$。对于图 G，我们用 $V(G)$ 表示 G的顶点集合，并用 $E(G)$表示

G的边集合。对于图 G 和子集 $X \subseteq V(G)$，我们用 $G[X]$ 表示由 X诱导的 G 的子图，即顶点限制为 X 且保留 X 的顶点之间所有边的图。

¯用 $\mathcal{S}_k$ 表示集合 $[k]$上所有排列构成的群。用 $\mathcal{S}_k$ 表示 $\mathcal{S}_k$ 中恰好包含一个环的排列所构成的子集。用 $\mathcal{S}_{2k}^2$ 表示 $\mathcal{S}_{2k}$ 中恰好包含 k 个环且每个环的大小均为 2 的排列所构成的子集；用 $\mathcal{S}_{2k}^k$ 表示$\mathcal{S}_{2k}$ 中恰好包含 2 个环且每个环的大小均为 k的排列所构成的子集。

排列的循环类型 定义为其所有环的大小构成的多重集。排列 $\rho \in \mathcal{S}_k$ 被排列 $\pi \in \mathcal{S}_k$ 共轭 定义为 $\pi^{-1}\rho\pi$，即 π的逆置换、 ρ 和 π的复合。众所周知，排列共轭保持循环类型，因此 $\bar{\mathcal{S}}_k, \mathcal{S}_{2k}^2, \mathcal{S}_{2k}^k$ 在共轭运算下封闭。我们将用到排列及其共轭的以下群论性质。这些性质要么广为人知，要么通过对若干子群进行一些基本计算即可轻松得出。

命题 2.1。 对于任意 $k \geq 1$ 以及任意由相同循环类型的置换构成的极大集合 $\mathcal{Z}_k \subseteq \mathcal{S}_k$，下列等式成立。

1. $|\bar{\mathcal{S}}_k| = (k-1)!$，$|\mathcal{S}_{2k}^2| = (2k-1)!!$，$|\mathcal{S}_{2k}^k| = (2k-1)!/k$, *2.* $\{\pi^{-1}\rho\pi \mid \pi \in \mathcal{S}_k\} = \mathcal{Z}_k$ 对于每个 $\rho \in \mathcal{Z}_k$，*3.* $|\{\pi \in \mathcal{S}_k \mid \pi^{-1}\rho_1\pi = \rho_2\}| = |\mathcal{S}_k|/|\mathcal{Z}_k|$ 对于每个 $\rho_1, \rho_2 \in \mathcal{Z}_k$，*4.* $|\{\rho_2 \in \mathcal{S}_{2k}^2 \mid \rho_2\rho_1 \in \mathcal{S}_{2k}^k\}| = (2k-2)!!$ 对于每个 $\rho_1 \in \mathcal{S}_{2k}^2$。

路径宽度。 设 G 是一个图（无向或有向）。 G 的路径分解 是一个子集序列 $\beta_1, \beta_2, \ldots\ldots, \beta_\ell \subseteq V(G)$，称为包，满足:

- 对于每条边 $(u, v) \in E(G)$，存在某个 $i \in [\ell]$ 使得 $u, v \in \beta_i$，并且
- 对于每个顶点 $v \in V(G)$，都存在 $1 \leq i_1 \leq i_2 \leq \ell$ 使得 $\{i \mid v \in \beta_i\} = \{i_1, i_1+1, \ldots, i_2-1, i_2\}$，也就是说，包含 v的包在所有包构成的序列中形成一个连通子区间。

路径分解 $(\beta_i)_{i=1}^{\ell}$ 的宽度 定义为最大值$_{i\in[\ell]} |\beta_i| - 1$。 G 的路径宽度 定义为其路径分解可能达到的最小宽度。

2.1 热带多项式

我们将所有多项式视为定义在热带（最大值 $+$）半环上，即 $(f \cdot g)(x) = f(x)+g(x)$，且 $(f+g)(x) = \max(f(x)\ g(x))$，其中任意两个多项式为 f, g。

独立集多项式。 如果将权重 x_v 视为不定元，我们可以将 IS_G 看作（最大值，$+$）半环上的多项式，只需将最大值运算替换为加法，将 $+$ 运算替换为乘法:

$$IS_G := \sum_{I \in \mathcal{I}(G)} \left(\prod_{v \in I} x_v \right), \tag{1}$$

在此提醒读者， $\mathcal{I}(G)$表示 G的所有独立集构成的族。

旅行商问题多项式。 与独立集多项式IS_G类似，我们将 G 的有向旅行商问题多项式定义为

$$DTSP_G := \sum_{u_0,\ldots,u_N \in \mathcal{H}(G)} \left(\prod_{i\in[N]} x_{u_{i-1},u_i} \right),$$

在此提醒读者， $\mathcal{H}(G)$表示所有满足以下条件的 $N+1$ 顶点序列（u_i）$_{i=0}^{N}$的族： $u_0 = u_N$且 $u_0 \to u_1 \to \cdots \to u_{N-1} \to u_N$是 G中的有向哈密顿圈。自然地，我们也通过将变量$x_{u,\ v}$和$x_{v,\ u}$（对所有 $uv \in E$（G））视为相同，类似地将 TSP_G 视为一个多项式。

有向生成树多项式。我们还定义 G 的有向生成树多项式如下:

$$DST_G := \sum_{p\in\mathcal{T}(G)} \left(\prod_{v\in V(G):p(v)\neq v} x_{p(v),v} \right)$$

在此提醒读者， $\mathcal{T}(G)$表示所有满足以下条件的函数 p： V（G）$\to V$（G）：对于恰好一个顶点 $v \in V$（G），p（v）$= v$，且其余所有顶点 u 上的边（p（u） u）构成一棵以 v为根的出树。

单项式 $m = x_1^{a_1} \ldots x_\ell^{a_\ell}$的支撑集是变量 $\{x_1, \ldots, x_\ell\}$ 的集合，记作 $\mathrm{sup}(m)$。多项式的支撑集 $p = m_1 + \cdots + m_\ell$是所有$i \in [\ell]$的支撑集 $\mathrm{sup}(m_i)$ 的并集。我们用 $\mathrm{sup}(p)$ 表示多项式 p的支撑集。对于单项式 m 和多项式p，若将 p 视为形式表达式后，其形式为某个多项式q的 $m + q$，则记作 $m \in p$。当且仅当存在某个 $d \in \mathbb{N}$，使得所有单项式 $m \in p$ 的度均为 d时，我们称多项式 p 为齐次多项式。对于多项式 p，我们用 $|p|$ 表示满足 $m \in p$的单项式 m的数量。

赋值是一种将变量映射到 $\mathbb{R}$ 的函数。单项式 m 的特征赋值 χ_m 是一种赋值，使得若 $x \in \mathrm{sup}(m)$，则 $\chi_m(x) = 1$；否则 $\chi_m(x) = -1$。如前所述，我们在一个（最大值 $+$）半环中计算多项式，也就是说，给定赋值 v，单项式 x 的计算结果为 $v(x)$，$(f+g)(v)$ 的计算结果为 $\max(f(v)\ g(v))$，而 $(f\cdot g)(v)$ 的计算结果为 $f(v) + g(v)$。

对于两个多项式 p，q，若对于每个单项式 $m \in p$，都有 $m \in q$，则记作 $p \subseteq q$。当且仅当 $p \subseteq q$ 且 $q \subseteq p$ 时，记作 $p \simeq q$。特别地， $p \simeq q$ 并不意味着 $p = q$（例如取 $p = x$ 和 $q = x + x$）。$\simeq$ 的定义源于以下观察。

命题 2.2。 对于任意两个多线性多项式 f、g， $f \simeq g$ 当且仅当对于任意赋值 v，都有 $f(v) = g(v)$。

证明。从 $f \simeq g$ 到 $f(v) = g(v)$ 的蕴含是显然的。反过来，不妨设 $f \subseteq g$ 不成立，因此存在某个单项式 $m \in f$ 使得 $m \notin g$。容易看出， $f(\chi_m) = |\mathrm{sup}(m)|$ 且 $g(\chi_m) < |\mathrm{sup}(m)|$，这就产生了矛盾。

□

2.2 热带电路

热带电路是一种有向无环图，其中每个顶点（称为节点）的入度均为 0 或 2。入度为 0 的顶点标记为变量，此时称为输入节点；或者标记为常数 0，此时称为常数节点。入度为 2 的节点称为运算节点，并标记为一个二元运算符，可以是 $+$ 或最大值。图中有一个节点被指定为输出节点。

给定赋值 v 时，热带电路的求值定义如下。按照图的拓扑序处理各节点。常数节点的求值为 0。

标记为 x 的输入节点求值为 $v(x)$。分别标记为 $+$ 和 max 的运算节点，其求值分别为两个前驱节点的值之和与最大值。整个电路求值的输出为输出节点处得到的值。

如果对于变量 v的每种赋值， Γ 在 v 上的求值都等于 $p(v)$，我们就说热带电路 Γ 计算某个多项式 p。显然，从语义上看，对热带电路求值恰好计算出某个多项式：标记为 x 的输入节点计算出 x，极大节点计算两个多项式的和，而 $+$ 节点计算两个多项式的乘积。

由命题 2.2 和定义，我们立即得到以下结论。

命题 2.3。设 f, g 是两个多线性多项式， Γ 是计算 f的热带电路。那么， Γ 计算 g 当且仅当 $f \simeq g$。

直观地说，这一断言表明，热带电路计算某个多项式，当且仅当其单项式集合恰好等于该电路求值过程中出现的所有单项式的集合。

关于热带电路，我们将使用的主要组合工具是以下分解引理。证明参见例如 [Juk23，引理 3.4]。

引理 2.4. 设 f 是由大小为 τ 的热带电路计算得到的齐次多项式，并令X 表示 $\sup(f)$的任意子集。那么， f 可以写成

$$f \simeq \sum_{i \in [\tau]} g_i \cdot h_i,$$

其中，对于每个 $i \in [\tau]$，有 $|\sup(g_i) \cap X| , |\sup(h_i) \cap X| \leq \frac{2}{3}|X|$。

3 独立集

在本章节中，我们证明定理 1.1 的界。我们所使用的图类受到从合取范式可满足性到最大权独立集的经典归约的启发。固定 $k > 0$ 并令$q = 4\binom{k}{2}$。考虑变量数为 k的所有可能的 2-CNF 子句：恰好有 q个。我们可以将每个子句视为一个元组 (a, b, n^a, n^b)，其中 $a, b \in [k]$ 表示一对无序变量，而 $n^a, n^b \in \{0, 1\}$ 表示第 a 个和第 b 个变量在子句中是否取反。我们按如下方式定义无向图 G_k 。我们放置

$$V(G_k) = \{v_{i,j} \mid i \in [k], j \in \{0, \ldots, 2q-1\}\} \cup \{w_j \mid j \in [q]\}.$$

顶点 $v_{i,j}$ 表示 CNF 公式中的文字： i 表示变量，而 j 的奇偶性决定该文字是否取反。每个文字都有 q 个副本，每个子句对应一个。顶点 w_j 表示所有可能的 2-CNF 子句。为方便起见，我们将使用w_{a,b,n^a,n^b}表示与上述由 a、 b、 n^a、 n^b表示的子句相对应的顶点。对于 $i \in [k]$, $r \in \{0, 1\}$，我们记 $V_{i,r} = \{v_{i,2j+r} \mid j \in \{0, \ldots q-1\}\}$ ，即表示第 i个变量的偶数顶点和奇数顶点。我们还记 $V_i = V_{i,0} \cup V_{i,1}$。

相应地添加边：

$$E(G_k) = \{(v_{i,j-1}, v_{i,j}) \mid i \in [k], j \in [2q-1]\} \cup \{(w_i, l_{i,j} \mid i \in [q], j \in \{1, 2\}\}$$

其中，$l_{i,1} = v_{a_i, 2(i-1)+n_i^a}$以及 $l_{i,2} = v_{b_i, 2(i-1)+n_i^b}$，其中 $w_i = w_{a_i, b_i, n_i^a, n_i^b}$。也就是说，$l_{i,j}$对应于由 w_i表示的子句中的文字。由于每个子句中的每个文字都有一个副本 $v_{i,j}$，因此每个 $v_{i,j}$ 至多与一个顶点 $w_{1+\lfloor j/2 \rfloor}$相连。每个 w_i 的度恰好为 2。

容易看出，图 G_k 的路径宽度至多为 $k+1$：我们可以从包 $\{v_{i,j}$ 开始：对于 $j \in \{0, \ldots, 2q-1\}$，取 $i \in [k]\}$，然后以自然的方式向其中添加集合 $N[w_j]$。证明下面的引理即可立即推出定理 1.1。

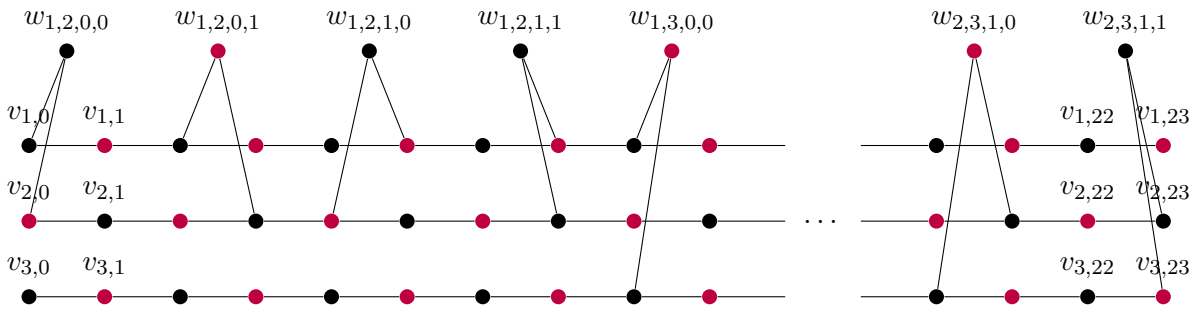


图1：图 G_3。红色顶点属于赋值 $\rho(1) = 1$，$\rho(2) = 0$，$\rho(3) = 1$ 对应的规范解。

Lemma 3.1. 对于任意 $k \geq 1$，任何计算 IS_{G_k} 的热带电路至少使用 $2^k/3$ 个门。

本章节余下部分将用于证明这个引理。固定 $k > 0$，并设 $G := G_k$。证明分两步进行。首先，我们将展示所描述的图中一种称为矩形的组合结构。然后，我们将把这一概念与热带电路所计算的多项式联系起来，并由此推出所需的下界。

由赋值 I_ρ 给出的规范解 ρ： $[k] \to \{0, 1\}$ 定义如下

$$I_\rho = \{v_{i,2j+\rho(i)} \mid i \in [k], j \in \{0, \ldots, q-1\}\} \cup \{w_i \mid \rho(a_i) \neq n_i^a \text{ and } \rho(b_i) \neq n_i^b\}.$$

也就是说，根据 $\rho(i)$，我们为所有 j 选取偶数或所有 j 选取奇数对应的顶点 $v_{i,\ j}$，并纳入所有与赋值 ρ 未满足的子句相对应的顶点 w_i。显然，每个赋值 ρ 对应一个规范解，共有 2^k 个规范解，并且每个规范解都是 G 的独立集。

我们称图 G 上的独立集族 $\mathcal{A}$，$\mathcal{B} \subseteq 2^{V(G)}$ 构成一个矩形 G（记作 $\mathcal{A} \cdot \mathcal{B}$），当且仅当任意一对集合 $A \in \mathcal{A}$，$B \in \mathcal{B}$ 互不相交且彼此不相邻（特别地，$A \cup B$ 构成图 G 的一个独立集）。我们称独立集族 $\mathcal{A}$，$\mathcal{B}$ 为该矩形的边。若矩形 $\mathcal{A} \cdot \mathcal{B}$ 包含 独立集 I，是指 $I = A \cup B$ 对某个 $A \in \mathcal{A}$，$B \in \mathcal{B}$ 成立。若存在 $B \in \mathcal{B}$ 使得 $A \cup B$ 是一个规范解，我们称集合 $A \in \mathcal{A}$ 是有用的。我们以类似方式定义集合 $B \in \mathcal{B}$ 是有用的。

为简单起见，这里引入的矩形概念是根据 G 的独立集族来定义的。然而，这一概念对于证明后续的所有界都至关重要，因此在后续章节中，我们将按照引理 2.4 的陈述，重新用热带多项式来定义矩形，以使定义更具一般性。

3.1 瘦矩形

计算 IS_G 的电路所具有的关键组合性质由以下引理表述。

引理 3.2。 设 $\mathcal{A} \cdot \mathcal{B}$ 是 G 中一个至少包含一个规范解 I_ρ 的矩形。那么，$\mathcal{A}$ 或 $\mathcal{B}$ 中包含的有用集合至多有一个。

在本小节余下部分，我们固定一个矩形 $\mathcal{A} \cdot \mathcal{B}$，并通过以下一系列断言来证明该引理。

断言 3.3。 设 I_1、I_2 是属于 $\mathcal{A} \cdot \mathcal{B}$ 同一侧的两个不同有用集合。那么，存在 $i \in [k]$、$j \in \{0, \ldots, 2q-1\}$，使得 $v_{i,\ j}$ 恰好属于 I_1、I_2 中的一个。

证明。 不失一般性，假设 $I_1, I_2 \in \mathcal{A}$。若两个集合与某个 V_i 的交集不同，则结论显然成立，因此不失一般性，假设对于某个 $l \in [q]$，有 $w_l \in I_1$and $w_l \notin I_2$。

由于 I_2 是有用的，因此存在 $J_2 \in \mathcal{B}$，使得 $I_2 \cup J_2$ 是一个规范解。由于 I_1 和 J_2 不相交，因此有 $w_l \notin I_2 \cup J_2$，故对于 w_l 的某个邻居 $v_{i,j}$，有 $v_{i,j} \in I_2 \cup J_2$。由于 I_1 和 J_2 不相邻，因此有 $v_{i,j} \notin J_2$，故有 $v_{i,j} \in I_2$。由于 I_1 是 G 的一个独立集，因此有$v_{i,j} \notin I_1$，从而完成了该命题的证明。

□

断言 3.4。设 I_1、I_2 是属于 $\mathcal{A} \cdot \mathcal{B}$ 同一侧的两个不同有用集合。那么，存在 $i \in [k]$、$r \in \{0,1\}$，使得 $V_{i,\ r} \subseteq I_1$ 且 $V_{i,\ 1-r} \subseteq I_2$。

证明。不失一般性，设 I_1，$I_2 \in \mathcal{A}$。根据前一个断言，存在某个 $i \in [k]$，$j \in \{0, \ldots, 2q-1\}$，使得不失一般性地有 $v_{i,\ j} \in I_1$ 且 $v_{i,\ j} \notin I_2$。令 $r = j$ 对 2 取模。由于 I_1，I_2 是有用集合，我们有相应的 J_1，$J_2 \in \mathcal{B}$。反设，令 $j' \in \{0, \ldots, 2q-1\}$ 为使 $|j - j'|$ 最小且 $v_{i,\ j'}$ 不属于预期集合的指标；也就是说，满足以下条件之一：j' 对 $2 = r$ 取模且 $v_{i,\ j'} \notin I_1$，或 j' 对 $2 \neq r$ 取模且 $v_{i,\ j'} \notin I_2$。

考虑 $j' \bmod 2 = r$ 的情况，另一种情况是对称的。由于 $v_{i,j} \in I_1 \cup J_1$，我们也有 $v_{i,j'} \in I_1 \cup J_1$。根据最小性，我们有 $v_{i,j'+1}$ 或 $v_{i,j'-1}$ 属于 I_2。如果 $v_{i,j'} \notin I_1$，那么$v_{i,j'} \in J_1$，但这意味着 $I_2 \cup J_1$ 不是一个独立集，矛盾。 □

命题 3.5. 设 I_1、$I_2 \in \mathcal{A}$ 是两个不同的有用集合，并设 $J_1 \in \mathcal{B}$ 满足 $I_1 \cup J_1$ 是一个规范解。那么 J_1 是 $\mathcal{B}$ 中唯一的有用集合。

证明。反设存在不同于 J_1 的有用 $J_2 \in \mathcal{B}$。将前一个命题分别应用于两边，我们得到 $i_A, i_B \in [k]$ 和 r_A，$r_B \in \{0,1\}$，使得：$V_{i_A,r_A} \subseteq I_1, V_{i_A,1-r_A} \subseteq I_2, V_{i_B,r_B} \subseteq J_1$ 和 $V_{i_B,1-r_B} \subseteq J_2$。显然，我们有 $i_A \neq i_B$。

选取 $w = w_{i_A,\ i_B,\ 1-r_A,\ 1-r_B}$。也就是说，对于某个 $j \in \{0, \ldots, q-1\}$，w的邻居恰好是 $v_A = v_{i_A,\ 2j+1-r_A}$ 和 $v_B = v_{i_B,\ 2j+1-r_B}$。我们有 $v_A \in I_2$ 和 $v_B \in J_2$。由于$V_{i_A,\ r_A} \subseteq I_1$ 且 I_1在 G 中是独立的，因此我们有 $v_A \notin I_1$。类似地，$v_B \notin J_1$。由于 I_2 和 J_1 不相交，因此我们有$v_A \notin J_1$，类似地还有 $v_B \notin I_1$。由于 I_2 和 J_1 不相邻，因此我们有 $w \notin J_1$，类似地还有$w \notin I_1$。然而，这意味着 $I_1 \cup J_1$ 不是规范解，因为 w 及其两个邻居都不属于 $I_1 \cup J_1$。这是矛盾，因此该断言得证。□

引理 3.2 可由最后一个论断立即得出。

3.2 细矩形电路的下界

在本小节中，我们证明定理 1.1。此时，我们可以不再考虑 G的具体结构。证明只依赖于上一小节中证明的细矩形性质。证明将紧密仿照 [Juk23，引理 2.18]的证明。

设 Γ 是任意一个计算 IS_G的热带电路。对于 Γ的任意节点 w，我们将其下方B_w 定义为：若指定 w 为输出节点，则由 Γ 计算得到的多项式。直观地说，B_w刻画了以 w 为根的子电路对整个计算输出的贡献。

同理，我们希望将节点 w 的上方 定义为电路其余部分的贡献。注意，B_w 不必包含在 IS_G 中；然而，假设输出节点可从 w到达，则至少对于一个单项式 m，有 $m \cdot B_w \subseteq IS_G$。我们将 A_w 定义为所有此类单项式的求和，即

$$A_w = \sum_{m : m \cdot B_w \subseteq IS_G} m.$$

显然，对于输出节点可从中到达的每个节点 w，$A_w \cdot B_w \subseteq IS_G$

A_w的 B_w 中的每个单项式都表示 G中的一个独立集。令 A_w^* 表示 A_w的有用单项式，即满足存在 $m' \in B_w$ 使得$m \cdot m'$ 表示一个规范解的单项式 $m \in A_w^*$。我们以类似方式定义 B_w^*。正如引理 3.2所证明的，对于每个节点 w，A_w^*和 B_w^* 中至少有一个的大小至多为 1。如果 $|A_w^*| \leq 1$，我们称 $A_w \cdot B_w$ 是A-薄的；否则，我们称其为 B-薄的。

如果 w 是一个输出节点，则有 $A_w = \{1\}$，$B_w = IS_G$，因此 $A_w \cdot B_w$ 是 A-薄的。如果 w 是标记为 x的输入节点，则有 $B_w = \{x\}$，因此 $A_w \cdot B_w$ 是 B-薄的。令 w_ℓ、……、w_1 为 Γ 中的任意一条路径，其中 w_1 是一个输出节点，w_ℓ 是某个输入节点。根据我们的观察，这条路径上存在某条边（w_{i+1}，w_i），使得 w_i 是 A-薄的，且 w_{i+1} 是 B-薄的，因此$|A^*_{w_i} \cdot B^*_{w_{i+1}}| \le 1$。

设 IS^*_G 是包含 IS_G 中所有表示规范解的单项式的多项式。下面的命题表明，属于上述矩形的所有规范解都可以沿着 Γ 中从输入到输出的路径传播。我们将用“前驱”指称电路中某个节点的入邻居。

命题 3.6. 设 w 是 Γ 中的一个节点，且 $c \in IS^*_G$ 满足：对于某个 $a \in A^*_w$，$c = a \cdot b$，$b \in B^*_w$。那么，至少存在 w 的一个前驱 u，使得 $c \in A^*_u \cdot B^*_u$。此外，若 w 是一个 $+$ 门，则上述结论对 w 的两个前驱都成立。

证明。设 u，v 是 w 的前驱。首先，考虑 w 是最大门的情况，也就是说，$B_w = B_u + B_v$。那么，$b \in B_u$ 或 $b \in B_v$。不失一般性，假设前者成立。我们有 $a \cdot B_u \subseteq a \cdot B_w \subseteq IS_G$，因此 $a \in A_u$。于是，$b \in B^*_u$，$a \in A^*_u$，从而得到所需的 $c \in A^*_u \cdot B^*_u$。

其次，考虑 w 是 $+$ 门的情况，也就是说，$B_w = B_u \cdot B_v$。那么，对于某个 $b_v \in B_v$ 和 $b_u \in B_u$，我们有 $b = b_v \cdot b_u$。我们有 $a \cdot b_v \cdot B_u \subseteq a \cdot B_v \cdot B_u \subseteq IS_G$，因此 $a \cdot b_v \in A_u$。所以，$b_u \in B^*_u$、$a \cdot b_v \in A^*_u$，从而 $c \in A^*_u \cdot B^*_u$。通过对称论证可得，$c \in A^*_v \cdot B^*_v$。 □

现在，考虑以下过程。我们固定一个规范解 $c \in IS^*_G$，并从输出节点 w_1开始。如果当前位于极大节点 w_i，就沿着断言所给出的前驱 w_{i+1} 移动。如果当前位于 $+$ 节点，就朝使 $|B^*_{w_{i+1}}|$ 较大的前驱 w_{i+1} 移动。该过程最终会在输入节点处终止，并生成一条路径 w_ℓ，……，w_1。如前所述，对于某个 $i \in [\ell - 1]$，我们有 $|A^*_{w_i} \cdot B^*_{w_{i+1}}| \le 1$。

我们有 $c \in A^*_{w_{i+1}} \cdot B^*_{w_{i+1}}$。如果 w_i 是一个最大值节点，则有 $B_{w_{i+1}} \subseteq B_{w_i}$，因此 $A^*_{w_{i+1}} \subseteq A^*_{w_i}$，进而 $c \in A^*_{w_i} \cdot B^*_{w_{i+1}}$，由此得到 $A^*_{w_i} \cdot B^*_{w_{i+1}} = \{c\}$。

如果 w_i 是一个 $+$ 节点，那么我们还可以得到 $c \in A^*_v \cdot B^*_v$，其中 v 是 w_i 除 w_{i+1}之外的前驱。根据我们选择 w_{i+1}的方式，可得 $|B^*_v| \le |B^*_{w_{i+1}}| \le 1$。由于 $B^*_{w_i} \subseteq B^*_{w_{i+1}} \cdot B^*_v$，我们有 $|B^*_{w_i}| \le 1$。因此，$A^*_{w_i} \cdot B^*_{w_i} = \{c\}$。

对每个规范 c 重复这一过程，就会得到一个从 IS^*_G 到集合 $V(G) \cup E(G)$的映射。如果将 c 映射到顶点 w，则可以保证 $A^*_w \cdot B^*_w = \{c\}$。如果将 c 映射到边 (u, w)，则可以保证 $A^*_w \cdot B^*_u = \{c\}$。这意味着该映射是单射，因此 $2^k = |IS^*_G| \le |V(G)| + |E(G)| \le 3|V(G)|$。至此，引理得证。

4 匹配相容矩阵

在以下章节中，矩阵是从 $I \times J$ 到任意值集的函数，其中 I 和J 分别是矩阵的行指标集和列指标集。我们不要求I, J 是某个 $n \in \mathbb{N}$所对应的形式为 $[n]$ 的集合。本章节中讨论的所有矩阵的取值都属于集合 $\{0, 1\}$。

定义 4.1. 对于一个行指标为 I、列指标为 J的 *0-1* 矩阵 M，若一对$I' \subseteq I, J' \subseteq J$构成 M的矩形，当且仅当它诱导出 M的一个全 *1* 子矩阵；也就是说，当且仅当对于每个 $i \in I', j \in J'$，都有 $M_{i,j} = 1$。矩形 R的大小 定义为 $|I'| \cdot |J'|$，记作 $|R|$。

定义 4.2. *0-1* 矩阵 M的矩形覆盖是由若干矩形 $(I_1, J_1) \ldots, (I_s, J_s)$组成的集合，这些矩形覆盖了 M 中的所有 *1*；也就是说，对于每个满足 $M_{i,j} = 1$ 的 i, j，都存在 $p \in [s]$，使得 $(i, j) \in I_p \times J_p$。覆盖的大小是其中矩形 s 的数量。

4.1 完全二部图

定义 4.3. 阶数为 k 的匹配相容矩阵 $\mathcal{M}_k$ 是一个大小为 $k! \times k!$ 的二元矩阵，其行和列由置换 $\mathcal{S}_k$ 索引，并满足

$$\mathcal{M}_k(\rho_1, \rho_2) = 1 \quad \textit{if and only if} \quad \rho_2\rho_1 \in \bar{\mathcal{S}_k}.$$

用 C_k 表示 $\mathcal{M}_k$的最小矩形覆盖的大小。

我们对热带电路规模的界将基于 Raz 和 Spieker 关于 C_k 的以下界。

引理 4.4 ([RS95])。 $C_k = 2^{\Omega(k \log\log k)}$。

值得注意的是，人们认为 C_k有上界 $2^{\Omega(k \log k)}$。证明这一点将使我们得到 C_k取值的渐近紧界，因为上界 $k! = 2^{\mathcal{O}(k \log k)}$是平凡的。然而，这仍然是一个开放问题。

矩阵的一个小矩形覆盖意味着其中存在大矩形，但一般而言，反过来并不成立。以下断言和引理表明，对于 $\mathcal{M}_k$，最小矩形覆盖的大小与最大矩形实际上存在关联，并且相差至多一个多对数因子。

断言 4.5。 令 R 为 $\mathcal{M}_k$ 中的任意一个矩形。那么，存在一个 $\mathcal{M}_k$ 的矩形覆盖，其大小为 $\ell = \frac{k!(k-1)!}{|R|} \cdot 2k \ln k$。

证明。 令 $Q \subseteq \mathcal{S}_k \times \mathcal{S}_k$ 表示满足 $\rho_2\rho_1 \in \mathcal{S}_k$ 的有序对 (ρ_1, ρ_2) 的集合，即 $\mathcal{M}_k$ 中 1 项的位置集合。令 P_1 和 P_2 分别表示作为 R 的行指标和列指标的置换集合。因此，对于每个 $\rho_1 \in P_1, \rho_2 \in P_2$，都有 $(\rho_1, \rho_2) \in Q$。考虑映射 $\mu_{\alpha,\beta}$： $\mathcal{S}_k \times \mathcal{S}_k \to \mathcal{S}_k \times \mathcal{S}_k$，它以置换 $\alpha, \beta \in \mathcal{S}_k$ 为参数，定义如下:

$$\mu_{\alpha,\beta}(\rho_1, \rho_2) = (\alpha\rho_1\beta, \beta^{-1}\rho_2\alpha^{-1}).$$

首先，注意到 $\rho_2\rho_1 \in \bar{\mathcal{S}_k}$ 当且仅当 $(\beta^{-1}\rho_2\alpha^{-1})(\alpha\rho_1\beta) = \beta^{-1}\rho_2\rho_1\beta \in \bar{\mathcal{S}_k}$，因为排列共轭保持循环类型，因此 $(\rho_1, \rho_2) \in Q$ 当且仅当 $\mu_{\alpha,\beta}(\rho_1, \rho_2) \in Q$。

令 α，β 为从 $\mathcal{S}_k$ 上的均匀分布中独立抽取的两个随机置换。首先，我们证明，对于任意两对 (ρ_1, ρ_2)，$(\sigma_1, \sigma_2) \in Q$，有

$$\Pr[\mu_{\alpha,\beta}(\rho_1, \rho_2) = (\sigma_1, \sigma_2)] \geq \frac{1}{k!(k-1)!}.$$

为此，我们证明至少存在 k 个不同的对 α，β，使得 $\alpha\rho_1\beta = \sigma_1$ 和 $\beta^{-1}\rho_2\alpha^{-1} = \sigma_2$。根据命题 2.1，恰好有 k 个置换 β 满足$\sigma_2\sigma_1 = \beta^{-1}\rho_2\rho_1\beta$。对于其中每一个，我们可以令 $\alpha = \sigma_2^{-1}\beta^{-1}\rho_2$，从而得到一个满足条件的对。

对于任意一对 $(\rho_1, \rho_2) \in Q$，有 $(\rho_1, \rho_2) \in \mu_{\alpha,\beta}(R)$ 当且仅当 $\mu_{\alpha^{-1},\beta^{-1}}(\rho_1, \rho_2) \in R$，因此

$$\Pr[(\rho_1, \rho_2) \in \mu_{\alpha,\beta}(R)] \geq \frac{|R|}{k!(k-1)!}.$$

现在，从 $\mathcal{S}_k \times \mathcal{S}_k$ 中独立且均匀地抽取 ℓ 对 α_i，β_i，并令 $R_i = \mu_{\alpha_i,\beta_i}(R)$。显然，对于每个 $i \in [\ell]$，都有 $R_i \subseteq Q$。令 $\bar{R} = \bigcup_{i\in[\ell]} R_i$。对于任意 $(\rho_1, \rho_2) \in Q$，我们有

$$\Pr\left[(\rho_1, \rho_2) \notin \bar{R}\right] \leq \left(1 - \frac{|R|}{k!(k-1)!}\right)^{\ell} < e^{-2k\ln k} = k^{-2k} < (k!(k-1)!)^{-1}.$$

由并集界，我们有 $\Pr\left[\bar{R} \neq Q\right] < 1$，因此存在 α_i，β_i 的一种选择，使得 $\bar{R} = Q$。对于这一选择 α_i，β_i，我们有 R_1，……，R_ℓ 是一个矩形覆盖，证明完毕。 □

立即可得到以下引理作为推论。

引理 4.6。 $\mathcal{M}_k$ 中的每个矩形大小至多为 $k!(k-1)! \cdot C_k^{-1} \cdot 2k \ln k$。

$\mathcal{S}_k$ 中的置换与完全二分图 $K_{k,\ k}$的完美匹配之间存在自然的一一对应关系。我们分别将 $K_{k,\ k}$的二分划分两侧的顶点标记为 v_1、.....、 v_k和 $u_1 \ldots,\ u_k$。对于任意完美匹配 $M \subseteq \{v_1, \ldots, v_k\} \times \{u_1, \ldots, u_k\}$，其对应的置换 $\rho \in \mathcal{S}_k$定义如下：

$$\rho(s) = t \quad \text{if and only if} \quad (v_s, u_t) \in M.$$

容易看出，对于 $K_{k,\ k}$中的任意两个完美匹配 $M_1,\ M_2$，它们的并集 $M_1 \cup M_2$ 构成哈密顿回路，当且仅当 $\rho_2^{-1}\rho_1 \in \bar{\mathcal{S}}_k$ 当且仅当 $\rho_1^{-1}\rho_2 \in \bar{\mathcal{S}}_k$，其中 ρ_i 表示与 M_i对应的置换。

4.2 完全图

与二分团类似，完全图 K_{2k} 中的每个完美匹配都可以用集合 $\mathcal{S}_{2k}^2$中的一个排列表示。因此容易看出，两个完美匹配M_1、 M_2 在 K_{2k} 中的并集构成哈密顿回路，当且仅当 $\rho_2\rho_1$ 属于 $\mathcal{S}_{2k}^k$。

定义 4.7. 阶为 k 的团匹配相容矩阵 $\mathcal{M}_k^*$ 是一个大小为$(2k-1)!! \times (2k-1)!!$ 的二元矩阵，其行和列均以 $\mathcal{S}_{2k}^2$ 中的排列为指标，并满足

$$\mathcal{M}_k^*(\rho_1, \rho_2) = 1 \quad \textit{if and only if} \quad \rho_2\rho_1 \in \mathcal{S}_{2k}^k.$$

引理 4.8. $\mathcal{M}_k^*$ 中的每个矩形的大小至多为 $(2k-1)! \cdot C_k^{-1} \cdot 2k \ln k$。

证明. 任取这样的矩形 R，令 P_1, P_2 分别表示作为 R的行指标和列指标的排列集合。对于大小为 k的集合 $C \subseteq [2k]$，我们定义 $\mathcal{S}_C \subseteq \mathcal{S}_{2k}^2$ 为一类排列：其所有环的大小均为 2，并将 C 中的所有元素映射到 $[2k] - C$。注意到$\mathcal{S}_C = \mathcal{S}_{[2k]-C}$。此外，对于每一对 $\rho_1 \in P_1, \rho_2 \in P_2$，若令 C为由 ρ_1, ρ_2的边的并集所形成的环的两个极大独立集之一，则有 $\rho_1, \rho_2 \in \mathcal{S}_C$。因此

$$P_1 \times P_2 \subseteq \bigcup_{\substack{C \cup D = [2k] \\ |C| = |D| = k}} \mathcal{S}_C \times \mathcal{S}_C,$$

因此

$$|P_1| \cdot |P_2| \leq \sum_{\substack{C \cup D = [2k] \\ |C| = |D| = k}} |(P_1 \cap \mathcal{S}_C) \times (P_2 \cap \mathcal{S}_C)|.$$

因此，只需证明对于每个 C，$|(P_1 \cap \mathcal{S}_C) \times (P_2 \cap \mathcal{S}_C)| \leq k!(k-1)! \cdot C_k^{-1} \cdot 2k \ln k$。

固定 $C \cup D = [2k]$、$|C| = |D| = k$，并枚举 $C := \{c(1), \ldots, c(k)\}$ 以及 $D := \{d(1), \ldots, d(k)\}$（我们将 c和 d视为从 $[k]$到分别为 C和 D的双射函数）。令$P_1^* = \{d^{-1}\rho_1 c : \rho_1 \in P_1 \cap \mathcal{S}_C\}$，并令 $P_2^* = \{c^{-1}\rho_2 d : \rho_2 \in P_2 \cap \mathcal{S}_C\}$。注意，这两个集合都有良好定义，且 $P_1^*, P_2^* \subseteq \mathcal{S}_k$。由于 c, d是双射函数，我们有 $|P_1^*| = |P_1 \cap \mathcal{S}_C|$和 $|P_2^*| = |P_2 \cap \mathcal{S}_C|$。

最后，对于每个 $\rho_1^* \in P_1^*$，$\rho_2^* \in P_2^*$，我们有 $\rho_2^*\rho_1^* = c^{-1}(\rho_2\rho_1)c \in \bar{\mathcal{S}}_k$。因此，$P_1^*$，$P_2^*$在 $\mathcal{M}_k$ 中构成一个矩形，由引理 4.6 可知，

$$|(P_1 \cap \mathcal{S}_C) \times (P_2 \cap \mathcal{S}_C)| = |P_1^* \times P_2^*| \leq k!(k-1)! \cdot C_k^{-1} \cdot 2k \ln k.$$

对所有 C 求和，得到 $|P_1| \cdot |P_2| \leq \binom{2k-1}{k-1} \cdot k!(k-1)! \cdot C_k^{-1} \cdot k \ln k = (2k-1)! \cdot C_k^{-1} \cdot k \ln k$，由此完成引理的证明。 □

5 旅行商问题

5.1 有向图

设 $G_{n,k}$ 表示一个有向图，其 $V(G_{n,k}) = \{v_{c,r} : \ c \in [n], r \in [k]\}$ 且

$$E(G_{n,k}) = \{(v_{c,r_1}, v_{(c \bmod n)+1,r_2}) \mid c \in [n], r_1, r_2 \in [k]\}.$$

容易看出，$G_{n,k}$ 的路径宽度至多为 $3k$。将下面的引理与引理 4.4 结合起来即可立即得到定理 1.2。本章节的其余部分将专门用于证明该结论。

引理 5.1。对于任意 $k \geq 1$ 和 $n \geq 3k+3$，计算 $DTSP_{G_{n,k}}$ 的任何热带电路的规模至少为 $C_k/(2k \ln k)$。

证明。固定 n, k，并令 $G := G_{n,k}$。令 $V_i = \{v_{i,r} : \ r \in [k]\}$。令 $G^i = G[V_i \cup V_{(i \bmod n)+1}]$，并令 $E_i = E(G^i)$，即，E_i 包含所有尾部属于 V_i 的边。对于 G^i 的每个完美匹配 M，我们将其与如下定义的排列 $\rho \in \mathcal{S}_k$ 对应：

$$\rho(s) = t \quad \text{iff} \quad (v_{i,s}, v_{(i \bmod n)+1,t}) \in M.$$

对于 G 的每个哈密顿回路 H，集合 $E(H) \cap E_i$ 是 G^i 中的一个完美匹配。若置换序列 $\rho_1, \ldots, \rho_n \in \mathcal{S}_k$ 表示 H，我们将其表述为 $E(H) \cap E_i = \rho_i$ 对所有 $i \in [n]$ 均成立。注意，这样的表示集合是唯一的，而且还满足

$$\rho_i \rho_{i-1} \cdots \rho_2 \rho_1 \rho_n \rho_{n-1} \cdots \rho_{i+2} \rho_{i+1} \in \bar{\mathcal{S}}_k$$

对于任意 $i \in [k]$。反之，每个满足上述条件的置换序列都唯一表示 G 的一个哈密顿回路。特别地，这样的序列共有 $(k-1)! \cdot (k!)^{n-1}$ 个，因此 G 中有相应数量的哈密顿回路。此外，对于任意大小至多为 $n-1$ 的指标集 $i_1, \ldots, i_\ell \in [n]$，如果固定 $\rho_{i_1}, \ldots, \rho_{i_\ell}$，那么恰好有 $(k-1)! \cdot (k!)^{n-1-\ell}$ 种方式固定其余置换，使上述包含关系成立。

现在，考察多项式 $DTSP_G$。令 $E = \{(v_{i,1}, v_{(i \bmod n)+1,1}) \mid i \in [n]\}$，并令 $X = \{x_{s,t} \mid (s,t) \in E\}$。也就是说，集合 X 对于 $i \in [n]$ 中的每个 E_i，恰好包含一个与一条边对应的变量。类似地，令 X_i 表示集合 $\{x_{s,t} \mid (s,t) \in E_i\}$。

我们称一对多项式 g, h 在 $DTSP_G$ 中构成一个矩形 $g \cdot h$，如果 $g \cdot h \subseteq DTSP_G$，也就是说，对于每一对单项式 $g' \in g, h' \in h$，$\sup(g') \cup \sup(h')$ 中的变量对应的边构成了 G的一个哈密顿回路。此外，如果 $|\sup(g) \cap \bar{X}|, |\sup(h) \cap \bar{X}| \leq \frac{2}{3}|\bar{X}|$，我们就称这样的矩形是平衡的。我们希望证明以下断言。

断言 5.2. 设 $g \cdot h$ 是 $DTSP_G$中的任意一个平衡矩形。那么

$$|g \cdot h| \leq (k-1)! \cdot (k!)^{n-1} \cdot C_k^{-1} \cdot (2k \ln k).$$

首先，利用该断言完成引理的证明。令 τ 表示计算 $DTSP_G$的最小热带电路的规模。引理 2.4 表明，$DTSP_G$ 可以被若干个平衡矩形的并集覆盖。因此，

$$(k-1)! \cdot (k!)^{n-1} = |DTSP_G| \leq \tau \cdot (k-1)! \cdot (k!)^{n-1} \cdot C_k^{-1} \cdot (2k \ln k),$$

因此 $\tau \geq C_k/(2k \ln k)$. 本章节的其余部分将用于证明该结论。

固定任意一个平衡矩形 $g \cdot h$。显然，g 和 h 的支撑集互不相交。如果 $X_i \cap \sup(g)$ 或 $X_i \cap \sup(h)$ 为空集，我们就称 E_i 关于 $g \cdot h$ 是单色的。令 i_1，……，i_ℓ

表示那些不是单色的集合 E_i 的指标。我们根据 $\ell > k$ 是否成立分两种情况讨论。

假设 $\ell > k$，并固定一个非单色的指标 i_j。定义

$$V^g_{tail} = \{u \in V_{i_j} \mid \exists_{w \in V_{(i_j \bmod n)+1}} x_{u,w} \in \sup(g)\},$$

$$V^g_{head} = \{w \in V_{(i_j \bmod n)+1} \mid \exists_{u \in V_{i_j}} x_{u,w} \in \sup(g)\},$$

也就是说，V^g_{tail}（分别为 V^g_{head}）表示 E_{i_j} 中所有相关变量属于 g 支撑集的边的尾端（分别为头端）。我们类似地定义 V^h_{tail}，V^h_{head}。容易看出，$V^g_{tail} \cap V^h_{tail} = V^g_{head} \cap V^h_{head} = \emptyset$。

$g \cdot h$ 的任意单项式所诱导的 G^{i_j} 中的完美匹配必须将 V^g_{head} 与 V^g_{tail} 匹配，并将 V^h_{head} 与 V^h_{tail} 匹配；这样做的可能方式数为 $|V^g_{head}|! \cdot |V^h_{head}|!$，由于两个集合均非空且不相交，该数量至多为 $(k-1)!$。因此，与 $g \cdot h$ 的单项式对应的所有环的数量至多为

$$((k-1)!)^\ell \cdot (k!)^{n-\ell} = \frac{1}{k^\ell} \cdot (k!)^n \le \frac{1}{k^{k+1}} \cdot (k!)^n = (k-1)! \cdot (k!)^{n-1} \cdot \frac{1}{k^k}$$

且 $\frac{1}{k^k} \le C_k^{-1} \le C_k^{-1} \cdot (2k \ln k)$。

现在，假设 $\ell \le k$。因此，至少有 E_i 中的 $n - k \ge \frac{2}{3}n + 1$ 是单色的。由于 $g \cdot h$ 是平衡的，我们有两个指标 i_g，i_h，使得 E_{i_g}，E_{i_h} 均为单色的，并且两个交集 $X_{i_g} \cap \sup(h)$ 和 $X_{i_h} \cap \sup(g)$ 都为空。特别地，g 中的每个单项式的支撑集都对应于这样一组边：它们与 E_{i_g} 的交集在 G^{i_g} 中诱导出一个完美匹配。h 和 G^{i_h} 也同样如此。不失一般性，我们可以假设 $i_g < i_h$。令 $\bar{E} = E(G) - (E_{i_g} \cup E_{i_h})$。

对于单项式 $g' \in g$（$h' \in h$ 的情形类似），我们将其类型定义为以下集合

$$\lambda_{g'} := \left\{e \in \bar{E} \colon x_e \in \sup(g')\right\}.$$

固定一对任意类型 λ_{g^*}，λ_{h^*}，并令 g^*（分别是 h^*）表示具有该类型的 g（分别是 h）中的所有单项式构成的集合。这样的可能类型对的数量不超过哈密顿回路在 $\bar{E}$ 上的不同投影数量，因此至多为 $(k!)^{n-2}$。根据定义，与 $g^* \cdot h^*$ 中的某个单项式相对应的每个环 H，与 E 的交集都相同。

令 ρ_i for $i \in [n] - \{i_g, i_h\}$ 表示集合 $(\lambda_{g^*} \cup \lambda_{h^*}) \cap E_i$，它是 G^i 中的一个完美匹配。令 $\bar{\rho}_l = \rho_{i_h-1}\rho_{i_h-2}\dots\rho_{i_g+1}$ and $\bar{\rho}_r = \rho_{i_g-1}\rho_{i_g-2}\dots\rho_1\rho_n\dots\rho_{i_h+1}$。令 P_g（分别为 P_h）表示由 g^*（分别为 h^*）中的单项式诱导的 G^{i_g}（分别为 G^{i_h}）的完美匹配集合。乘积 $(\bar{\rho}_l P_g \bar{\rho}_r) \cdot P_h$ 中的每个排列都属于 $\mathcal{S}_k$，因此根据引理 4.6，

$$k(k-1)! \cdot C_k^{-1} \cdot (2k \ln k) \ge |\bar{\rho}_l P_g \bar{\rho}_r| \cdot |P_h| = |P_g| \cdot |P_h| = |g^*| \cdot |h^*| \ge |g^* \cdot h^*|.$$

因此 $|g \cdot h| \le (k!)^{n-1} \cdot (k-1)! \cdot C_k^{-1} \cdot (2k \ln k)$。

□

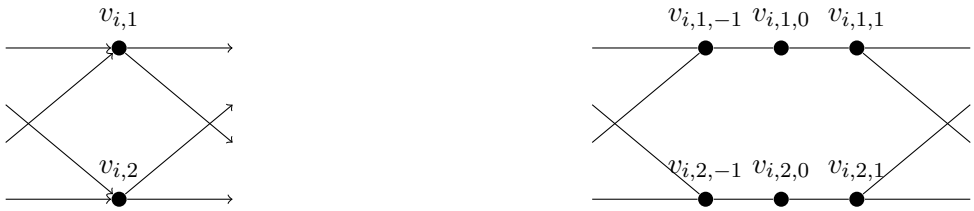
5.2 无向图

设 $G_{n,k}$ 为一个无向图，其 $V(G_{n,k}) = \{v_{c,r,i} \colon c \in [n],\ r \in [k],\ i \in \{-1, 0, 1\}\}$ 和

$$\begin{aligned} E(\bar{G}_{n,k}) = \{&(v_{c,r_1,1}, v_{(c \bmod n)+1,r_2,-1}) \mid c \in [n], r_1, r_2 \in [k]\} \cup \\ &\{(v_{c,r,-1}, v_{c,r,0}) \mid c \in [n], r \in [k]\} \cup \\ &\{(v_{c,r,0}, v_{c,r,1}) \mid c \in [n], r \in [k]\}. \end{aligned}$$

图 $G_{n,k}$ 是通过对 $G_{n,k}$ 进行教科书式归约，从有向版旅行商问题转换为无向版旅行商问题而得到的。

再次，$G_{n,k}$ 的路径宽度至多为 $3k$。将下面的引理与引理 4.4 结合即可立即得到定理 1.3。



(a) i第G_{n}列的2　　(b) 在 $\bar{G}_{n,2}$

¯图2：从 $G_{n,\ k}$ 到 $G_{n,\ k}$的归约

引理5.3。对于任意 $k \geq 1$ 和 $n > 3k$，任何计算 $TSP_{\bar{G}_{n,\ k}}$ 的热带电路至少需要$C_k/(2k \ln k)$个门。

¯证明。令 Γ为一个计算 $TSP_{\bar{G}_{n,\ k}}$的任意大小为 $\bar{\tau}$的热带电路。我们将证明，存在一个大小为 $\tau \leq \bar{\tau}$、计算 $DTSP_{G_{n,\ k}}$的热带电路 Γ。特别地，结合引理 5.1，这表明 $\bar{\tau} \geq C_k/(2k \ln k)$。

设 Γ　　¯为通过对 Γ 进行以下替换得到的热带电路　　s:

- 对于每个标记为变量 $x_{u_1,\ u_2}$ 的输入节点，其中 $u_1,\ u_2 \in V(G_{n,\ k}),\ u_1 = \bar{v}_{c,\ r,\ -1}$, $u_2 = v_{c,\ r,\ 0}$，我们将其替换为常数 0，_
- 对于每个标记为变量 $x_{u_1,\ u_2}$ 的输入节点，其中 $u_1,\ u_2 \in V(G_{n,\ k}),\ u_1 = v_{c,\ r,\ 0},\ u_2 = v_{c,\ r,\ 1}$，我们将其替换为常数 0，_
- 对于每个标记为变量 x_{u_1,u_2} 的输入节点，其中 $u_1, u_2 \in V(G_{n,k}), u_1 = v_{c,r_1}, 1, u_2 = v_{(c \text{ 模 } n)+1,r_2}$, -1，我们将其替换为变量 $x_{u_1',u_2'}$，其中 $u_1', u_2' \in V(G_{n,k}),\ u_1' = v_{c,r_1}, u_2' = v_{(c \text{ 模 } n)+1,r_2}$。

显然，Γ 的大小至多为 $\bar{\tau}$。令 f 表示由 Γ计算得到的某个多项式。该归约的构造方式保证了 $G_{n,\ k}$ 中的有向哈密顿回路与$G_{n,\ k}$中的¯无向哈密顿回路之间存在双射，且该双射直接源于 Γ定义中所描述的边替换。特别地，很容易看出$f \simeq DTSP_{G_{n,\ k}}$。

□

6 生成树

令$H_{n,\ k}$ 表示一个有向图，其 $V(H_{n,\ k}) = \{v_{c,r}$ 为：$c \in [n]$、$r \in [2k]\}$ 以及

$$E(H_{n,k}) = \{(v_{c_1,r_1}, v_{c_2,r_2}) \mid c_1, c_2 \in [n], r_1, r_2 \in [2k], |c_1 - c_2| = 1\} \cup \{(v_{c,r_1}, v_{c,r_2}) \mid c \in \{1, n\}, r_1, r_2 \in [2k], r_1 \neq r_2\}.$$

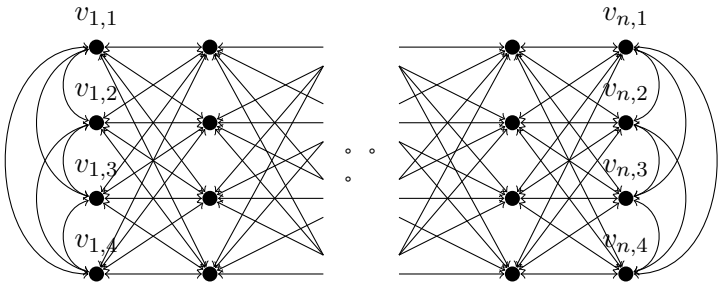


图3：$H_{n,\ 2}$

容易看出，$H_{n,k}$ 的路径宽度至多为 $4k$。将下面的引理与引理 4.4 结合，立即可得定理 1.4。

引理 6.1。 对于任意 $k \geq 1$ 和 $n > 12k^2 \ln k + 3$，任何计算 $DST_{H_{n,k}}$ 的热带电路都至少使用 $C_k/(2k^2 \ln k)$ 个门。

本章节的其余部分专门用于证明这一引理。证明的大部分内容沿用了证明引理 5.1 时所采用的论证思路。在本章节的其余部分，我们固定适当的 n, k 并令 $G := H_{n,k}$。令 $V_i = \{v_{i,r} : r \in [2k]\}$。对于 $i \in [n-1]$，令 $G^i = G[V_i \cup V_{i+1}] - (E(G[V_i]) \cup E(G[V_{i+1}]))$，并令 $G^0 = G[V_1], G^n = G[V_n]$。注意，对于 $1 \leq i \leq n-1$， G^i 是完全二部的；对于 $i \in \{0, n\}$，G^i 是完全的。我们对所有$i \in \{0, \ldots, n\}$ 记 $E_i = E(G^i)$，并令 $X_i = \{x_e\colon\ e \in E_i\}$。

对于 $i \in \{1, \ldots, n-1\}$ 的 G^i 的每个完美匹配 M，我们将其与一个排列$\rho \in \mathcal{S}_{2k}$ 对应，该排列定义为

$$\rho(s) = t \quad \text{iff} \quad (v_{i,s}, v_{i+1,t}) \in M \text{ or } (v_{i+1,t}, v_{i,s}) \in M.$$

Simi类似地，对于 $i \in \{0, n\}$，我们将 G^i 的任意完美匹配 M 与满足条件 $\rho \in \mathcal{S}^2_{2k}$ 的对象对应起来 t

$$\rho(s) = t \quad \text{iff} \quad (v_{i,s}, v_{i,t}) \in M \text{ or } (v_{i,t}, v_{i,s}) \in M.$$

我们称 G 的哈密顿回路是优美的，如果它与每个 E_i 的交集在 G^i 中都是完美匹配（忽略边的方向）。我们称 G 的哈密顿路径是优美的，如果它是一个优美哈密顿回路的子图，并且其首尾顶点属于 V_1。每条优美路径恰好是一个优美环的子图；反过来，每个优美环都恰好包含 k 条优美路径作为子图。

我们将优美哈密顿回路 H 的内容定义为排列ρ_0，……， $\rho_n \in \mathcal{S}_{2k}$的唯一序列，使得对于所有 $0 \leq i \leq n$， $E(H) \cap E_i = \rho_i$。为清楚起见，对于这样的序列，我们定义以下记号。

$$\overleftarrow{\rho_i} := \rho_i \rho_{i-1} \cdots \rho_2 \rho_1$$

$$\overrightarrow{\rho_i} := \rho_{n-1} \rho_{n-2} \cdots \rho_{i+1} \rho_i$$

我们假设 $\overleftarrow{\rho_0} = \overrightarrow{\rho_n} =$ **恒等**$\mathcal{S}_{2k}$。请注意，如第 4.2 节所述，

$$\left(\overleftarrow{\rho_{i-1}} \cdot \rho_0 \cdot \overleftarrow{\rho_{i-1}}^{-1}\right) \cdot \left(\overrightarrow{\rho_i}^{-1} \cdot \rho_n \cdot \overrightarrow{\rho_i}\right) \in \mathcal{S}^k_{2k} \tag{2}$$

对于任意 $i \in [n]$。反过来，对于满足上述条件的每个排列序列（ i 可任意选择），恰有两个优美环 H，其内容为 ρ_0、……、 ρ_n。这两个环仅方向不同。特别地，如果公式 (2) 对某个这样的 i 成立，那么它对每个 $i \in [n]$ 都成立。

断言 6.2. 满足（*1*）的序列 $((2k)!)^{n-1} \cdot (2k-1)!$ 有 $(\rho_j)_{j=0}^n$ 个。

证明。 对于所有 $j \neq i$，我们任意固定 ρ_j；这样做有 $((2k-1)!!)^2 \cdot ((2k)!)^{n-2}$ 种方式。令 $\bar{\rho} = \left(\overrightarrow{\rho_i}^{-1} \cdot \rho_n \cdot \overrightarrow{\rho_i}\right)$，因此我们有 $\bar{\rho} = \rho_i^{-1} \tilde{\rho} \rho_i$，其中 $\tilde{\rho} \in \mathcal{S}^2_{2k}$ 已经固定。根据命题 2.1，为使公式 (2) 成立， $\bar{\rho}$ 可以取 $(2k-2)!!$ 个值。根据同一命题，给定 $\bar{\rho}$ 时， $\rho_i \in \mathcal{S}^2_{2k}$ 的数量为 $(2k)!!$。因此，固定所有 ρ_j 的总方式数为 $((2k-1)!!)^2 \cdot ((2k)!)^{n-2} \cdot (2k)!! \cdot (2k-2)!! = ((2k)!)^{n-1} \cdot (2k-1)!$。 □

特别地， G中的优美环数量为 $2 \cdot ((2k)!)^{n-1} \cdot (2k-1)!$。通过类似的论证，对于任意大小至多为 $n-2$ 的指标集 $1 \leq i_1$、……、 $i_\ell \leq n-1$，如果固定 ρ_{i_1}、……、 ρ_{i_ℓ} 以及 ρ_0 和 ρ_n，那么恰好有 $((2k)!)^{n-2-\ell} \cdot (2k)!! \cdot (2k-2)!!$ 种固定其余排列的方式，使得（1）成立。

证明（引理 *6.1*）。我们称一个矩形 $g \cdot h \subseteq DST_G$ 覆盖一个优美哈密顿回路 H，如果它包含一个编码优美哈密顿路径的单项式，且该路径是 H 的子图。由于所有优美哈密顿路径也都是生成出树，我们的电路所计算的多项式的任何矩形分解都必须覆盖所有优美环。按照引理 2.4 的陈述，我们相对于集合 $X = \{x_{(v_{c,1},v_{c+1,1})} \mid c \in [n-1]\}$定义平衡矩形。

断言 6.3。令 $g \cdot h$ 为 DST_G 中任意一个平衡矩形。那么，$g \cdot h$ 所覆盖的优美哈密顿回路数量至多为

$$((2k)!)^n \cdot C_k^{-1} \cdot 2k \ln k.$$

对于任何使用 τ 个门计算 DST_G 的热带电路，引理 2.4 意味着 DST_G 可以由 τ 个平衡矩形的并集覆盖。因此，为了覆盖每一个优美环，至少有一个平衡矩形必须覆盖其中至少 $^{2}{((2k)!)^{n-1}(2k-1)!\,\tau}$ 个；于是，假设断言 6.3 成立，

$$\tau \geq C_k/(2k^2 \ln k).$$

本章节余下部分将用于证明断言 6.3。任取一个平衡矩形 $g \cdot h$。g 和 h 的支撑集互不相交。若 $X_i \cap \mathrm{sup}(g)$ 或 $X_i \cap \mathrm{sup}(h)$ 为空集，则称 E_i 关于 $g \cdot h$ 是单色的。

断言 6.4。取 $1 \leq i \leq n-1$。如果 E_i 关于 $g \cdot h$ 不是单色的，那么存在一条边 $(u,v) \in E_i$，使得 $x_{u,\ v} \notin \mathrm{sup}(g) \cup \mathrm{sup}(h)$。

证明。反设对于每个 $(u,v) \in E_i$，都有 $x_{u,v} \in \mathrm{sup}(g)$ 或 $x_{u,v} \in \mathrm{sup}(h)$。由于 $g \cdot h$ 中的所有单项式都表示出树，对于形如 (u,v)、$(w,v) \in E_i$ 的任意一对边，要么 $x_{u,v}$,$x_{w,v}$ 都属于 $\mathrm{sup}(g)$，要么都属于 $\mathrm{sup}(h)$。类似地，对于任意 $(u,v) \in E_i$，$x_{u,v}$,$x_{v,u}$ 也必须属于同一个支撑集。

根据我们的假设，存在两条边 (p,q)、$(s,t) \in E_i$，使得 $x_{p,q} \in \mathrm{sup}(g)$ 且 $x_{s,t} \in \mathrm{sup}(h)$（因此 $x_{t,s} \in \mathrm{sup}(h)$ 也成立）。(q,s) 或 (q,t) 属于 E_i。在前一种情况下，有 $x_{q,s} \in \mathrm{sup}(h)$ 且 $x_{s,q} \in \mathrm{sup}(g)$。在后一种情况下，则有 $x_{q,t} \in \mathrm{sup}(h)$ 且 $x_{t,q} \in \mathrm{sup}(g)$。两种情况都会导致矛盾，由此得证。 □

令 $i_1 < \cdots < i_\ell$ 表示范围 $[n-1]$ 内的集合 E_i 中不是单色的指标。我们根据 $\ell > 4k^2 \ln k$ 是否成立分两种情况讨论。

假设 $\ell > 4k^2 \ln k$。舍弃至多一半的指标 i_j 后，我们可以假设这些指标互不相邻。也就是说，假设 $\ell > 2k^2 \ln k$，并且对所有 $j \in [\ell - 1]$，都有 $i_{j+1} - i_j > 1$。对于每个 $i \in \{i_j\}_{j=1}^{\ell}$，令 $(p_i,\ q_i)$ 表示由断言 6.4 给出的 E_i 的边。考虑以下随机过程，以生成 G 的一个良好的有向哈密顿回路 H。

- 均匀随机地选择 $\rho_0 \in \mathcal{S}_{2k}^2$。
- 按照 ρ_0 匹配 V_1 的顶点，并均匀且独立地选择边的方向，从而选出边子集 $F_0 \subseteq E_0$。令 V_1^{tail} 和 V_1^{head} 分别表示由 F_0 中各边的尾部和头部组成的 V_1 的顶点。

- 对于 $i \in \{1,\ldots,n-1\}$，执行以下操作。均匀随机地选取 $\rho_i \in \mathcal{S}_{2k}$，并通过将 $V(G^i)$ 的顶点按照 ρ_i 进行匹配来选择 $F_i \subseteq E_i$，同时选择边的方向，使其与 F_{i-1} 中边的方向一致（也就是说，如果将 v_{i,r_1} 与 v_{i+1,r_2} 匹配，并将 $v_{i,r_1} \in V_i^{tail}$ 与.....匹配，那么就将 (v_{i+1,r_2}, v_{i,r_1}) 加入 F_i；否则加入 $(v_{i,r_1}$,$v_{i+1,r_2})$。以类似方式定义 $V_{i+1}^{tail}, V_{i+1}^{head}$。
- 此时的并集 $F_0 \cup \cdots \cup F_{n-1}$ 构成了 k 条互不相交的有向路径，其端点恰好是 V_n。恰有 $(k-1)!$ 种方法可以选取 F_n，将这些路径连接成一个哈密顿回路。我们从中均匀随机地选取一种。

很容易看出，该过程以均匀概率分布生成所有符合条件的哈密顿回路。现在，我们可以根据断言 6.4，界定以这种方式生成的环不包含任何禁用边（p_i，q_i）的概率。注意，只有这样的环才能被 $g \cdot h$ 覆盖。

可行选择数量可能受到限制的步骤，是为某个 $j \in [\ell]$ 选择 F_{i_j} 时。不失一般性，假设 $p_{i_j} \in V_{i_j}$，$q_{i_j} \in V_{i_j+1}$，另一种情况是对称的。如果 $p_{i_j} \in V_{i_j}^{tail}$，那么 F_{i_j} 的每一种选择都是可行的，因为潜在添加的 p_{i_j}，q_{i_j} 之间的边总是会从 q_{i_j} 指向 p_{i_j}。若 $p_{i_j} \in V_{i_j}^{head}$，则将禁用边添加到 F_{i_j} 的概率恰好为 $\frac{1}{k}$，因为 ρ_{i_j} 是从整个 $\mathcal{S}_{2k}$ 中均匀选出的。

关键观察是，假设到目前为止我们没有选中任何禁用边，那么此时 p_{i_j} 属于 $V_{i_j}^{head}$ 的概率恰好为 $1/2$，且与先前的选择独立。这是因为 ρ_{i_j-1} 是从 $\mathcal{S}_{2k}$ 中均匀选出的，并且根据我们的假设，$i_j > i_{j-1}+1$。将 V_{i_j-1} 划分为 $V_{i_j-1}^{head}$ 和 $V_{i_j-1}^{tail}$ 的方式可以有任意分布；然而，这两个集合的大小始终都是 k，因此 p_{i_j} 与来自 $V_{i_j-1}^{tail}$ 的一个顶点匹配的概率恰好为 $\frac{1}{2}$。

这意味着，不包含任何禁用边的优美哈密顿环的概率至多为

$$\left(1-\frac{1}{2k}\right)^{\ell} < e^{-k\ln k} \le C_k^{-1} \le C_k^{-1} \cdot 2k^2 \ln k,$$

因此，这类环的数量至多为

$$\left(2((2k)!)^{n-1}(2k-1)!\right) \cdot \left(C_k^{-1} \cdot 2k^2 \ln k\right) = ((2k)!)^n \cdot C_k^{-1} \cdot 2k \ln k,$$

由此便完成了在 $\ell > 4k^2 \ln k$ 时的证明。

现在，假设 $\ell < 4k^2 \ln k$。因此，E_i 中至少有 $n - 4k^2 \ln k \ge \frac{2n}{3} + 1$ 是单色的。由于 $g \cdot h$ 是平衡的，我们有两个指标 $i_g, i_h \in [n-1]$，使得 E_{i_g}, E_{i_h} 都是单色的，并且 $X_{i_g} \cap \sup(h)$ 和 $X_{i_h} \cap \sup(g)$ 都为空。不失一般性，假设 $i_g < i_h$。令 $E = E(G) - (E_{i_g} \cup E_{i_h})$。

对于单项式 $g' \in g$（$h' \in h$ 的情形类似），我们将其类型定义为集合

$$\lambda_{g'} := \{e \in \bar{E} : x_e \in \sup(g')\}.$$

固定一对任意类型 $\lambda_{g^*}, \lambda_{h^*}$，并令 g^*（分别为 h^*）表示具有该类型的 g（分别为 h）中所有单项式的集合。根据定义，对应于 $g^* \cdot h^*$ 中某个单项式的每棵生成出树，与 E 的交集都相同。如果 $g^* \cdot h^*$ 覆盖至少一个优美环，那么对于每个 $i \in [n] - \{i_g, i_h\}$，这个交集必须在 G^i 中导出一个完美匹配，并且在 G^0 中导出一个大小为 $k-1$ 的匹配。令 $(\rho_i)^{i \in [n]-\{i_g,i_h\}}$ 表示集合 $(\lambda_{g^*} \cup \lambda_{h^*}) \cap E_i$。令 ρ_0 表示包含 $(\lambda_{g^*} \cup \lambda_{h^*}) \cap E_0$ 作为子图的 $\mathcal{S}_{2k}^2$ 的唯一排列。

令 $\bar{\rho}_l = \overleftarrow{\rho_{i_g-1}}$、$\bar{\rho}_r = \overrightarrow{\rho_{i_h+1}}$ 和 $\bar{\rho}_m = \rho_{i_h-1}\rho_{i_h-2}\cdots\rho_{i_g+2}\rho_{i_g+1}$。令 P_g（分别为 P_h）表示由 g^*（分别为 h^*）中的单项式所诱导的 G^{i_g}（分别为 G^{i_h}）的完美匹配集合。最后，令

$$P_g^* = \left\{\rho \cdot \bar{\rho}_l \cdot \rho_0 \cdot \bar{\rho}_l^{-1} \cdot \rho^{-1} \mid \rho \in P_g\right\} \text{ and}$$

$$P_h^* = \left\{\bar{\rho}_m^{-1} \cdot \rho^{-1} \cdot \bar{\rho}_r^{-1} \cdot \rho_n \cdot \bar{\rho}_r \cdot \rho \cdot \bar{\rho}_m \mid \rho \in P_h\right\}.$$

由命题 2.1，得 $|P_g| \le (2k)!! \cdot |P_g^*|$ 且 $|P_h| \le (2k)!! \cdot |P_h^*|$。由公式 (2)，每一对 $\rho_g \in P_g^*$，$\rho_h \in P_h^*$ 都满足 $\rho_h^* \rho_g^* \in \mathcal{S}_{2k}^k$，因此应用引理 4.8 可得

$$2 \cdot |P_g| \cdot |P_h| \le 2((2k)!!)^2 \cdot |P_g^*| \cdot |P_h^*| \le 2((2k)!!)^2 (2k-1)! \cdot C_k^{-1} \cdot 2k \ln k.$$

最后请注意，$2 \cdot |P_g| \cdot |P_h|$ 从上界限制了 $g^* \cdot h^*$ 所覆盖的优美环的数量。

至少覆盖一个优美环的类型对数量为 λ_{g^*}，λ_{h^*} 其上界是优美路径在 E 上的不同投影数量，因此不超过

$$k((2k-1)!!)^2((2k)!)^{n-3}.$$

因此，$g \cdot h$ 所覆盖的优良环总数至多为

$$\left(k((2k-1)!!)^2((2k)!)^{n-3}\right) \cdot \left(2((2k)!!)^2(2k-1)! \cdot C_k^{-1} \cdot 2k\ln k\right) =$$

$$= ((2k)!)^n \cdot C_k^{-1} \cdot 2k\ln k,$$

由此完成了该论断的证明。

□

7 结论

如前所述，匹配相容性矩阵的精确非确定性通信复杂度仍未解决：尽管 $C_k = k^{O(k)}$ 显然成立，目前已知的最佳下界为 $C_k = 2^{\Omega(k\,\text{双对数}\,k)}$ [RS95]。证明这一下界将自动推出定理 1.2、定理 1.3 和定理 1.4 的相同下界。特别是，这一复杂度在渐近意义下是紧确的（相差至多 N 的多项式因子），因为遵循基于路径分解的朴素动态规划算法，可以轻易为所有这些问题构造大小为 $2^{\mathcal{O}(k\,\text{对数}\,k)} \cdot N^{\mathcal{O}(1)}$ 的热带电路。反过来，改进 C_k 的上界似乎也有助于为 $DTSP_G$、TSP_G 和 DST_G 获得更好的热带电路，甚至可能有助于获得路径宽度参数化 TSP 的更快算法。然而，正如 [RS95], 的作者也指出的那样，C_k 似乎更接近 $2^{\Omega(k\,\text{对数}\,k)}$，而不是 $2^{\Theta(k\,\text{双对数}\,k)}$。

另一个值得进一步研究的方向，是为其他计算问题寻找下界。例如，利用定理 1.1 中的工具以及 [LMS18a] 中的归约思路，似乎可以为计算路径宽度为 k 的图的最小权重支配集的热带电路，得到 $\Omega(3^k)$ 下界。

更进一步，一个自然的开放问题是，本文所定义的热带电路下界能否推广到表达能力更强的热带电路变体（参见 Jukna 的著作 [Juk23]）。

参考文献

[BCKN15] Hans L. Bodlaender、Marek Cygan、Stefan Kratsch 和 Jesper Nederlof。参数化树宽的连通性问题的确定性单指数时间算法。*Inf. Comput.*，243:86–111，2015。[BDFH 09] Hans L. Bodlaender、Rodney G. Downey、Michael R. Fellows 和 Danny Hermelin。关于没有多项式核的问题。*J. Comput. Syst. Sci.*，75(8):423–434，2009。[Bel62] Richard Bellman。旅行商问题的动态规划处理。*J. ACM*，9(1):61–63，1962。[BI13] Christopher Beck 和 Russell Impagliazzo。正规归结满足强 ETH。载于 Dan Boneh、Tim Roughgarden 和 Joan Feigenbaum（编辑），计算理论研讨会会议，*STOC'13*，美国加利福尼亚州帕洛阿尔托，*2013* 年 *6* 月 *1–4* 日，第 487–494 页。ACM，2013。[Bjö14] Andreas Björklund。无向哈密顿性的行列式和。*SIAM*计算杂志，43(1):280–299，2014。

[Cal23] Asier Calbet。 K_r-饱和图与双族定理。arXiv 预印本 arXiv:2302.13389，2023。[CFK+15] Marek Cygan、Fedor V. Fomin、Lukasz Kowalik、Daniel Lokshtanov、Dániel Marx、Marcin Pilipczuk、Michal Pilipczuk 和 Saket Saurabh。参数化算法。Springer，2015。[CKN18] Marek Cygan、Stefan Kratsch 和 Jesper Nederlof。通过完美匹配基快速检查哈密顿性。J. ACM，65(3):12:1–12:46，2018。[CLN18] Radu Curticapean、Nathan Lindzey 和 Jesper Nederlof。通过矩阵秩计数哈密顿回路的紧下界。载于 Artur Czumaj（编辑），第二十九届 ACM-SIAM 离散算法年度研讨会论文集，SODA 2018，美国路易斯安那州新奥尔良，2018 年 1 月 7–10 日，第 1080–1099 页。SIAM，2018。[CNP+22] Marek Cygan、Jesper Nederlof、Marcin Pilipczuk、Michal Pilipczuk、Johan M. M. van Rooij 和 Jakub Onufry Wojtaszczyk。单指数时间内求解参数化树宽的连通性问题。ACM Trans. Algorithms，18(2):17:1–17:31，2022。[Flo62] Robert W. Floyd。算法 97：最短路径。Commun. ACM，5(6):345，1962。[FLPS16] Fedor V. Fomin、Daniel Lokshtanov、Fahad Panolan 和 Saket Saurabh。代表族的高效计算及其在参数化算法和精确算法中的应用。J. ACM，63(4):29:1–29:60，2016。[FMP+15] Samuel Fiorini、Serge Massar、Sebastian Pokutta、Hans Raj Tiwary 和 Ronald de Wolf。组合优化中多面体的指数下界。J. ACM，62(2):17:1–17:23，2015。[FS11] Lance Fortnow 和 Rahul Santhanam。NP 的实例压缩和简洁 PCP 的不可行性。J. Comput. Syst. Sci.，77(1):91–106，2011。[HK62] Michael. Held 和 Richard M. Karp。序列问题的动态规划方法。Journal of the Society for Industrial and Applied Mathematics，10(1):196–210，1962。[JS82] Mark Jerrum 和 Marc Snir。半环上直线型计算的一些精确复杂度结果。J. ACM，29(3):874–897，1982。[Juk23] Stasys Jukna。热带电路复杂度：纯动态规划的界限。Springer International Publishing，Cham，2023。[Ker70] Leslie Robert Kerr。代数结构对矩阵乘法计算复杂度的影响。技术报告，康奈尔大学，1970。[Kor21] Tuukka Korhonen。最大权独立集动态规划的下界。载于 Nikhil Bansal、Emanuela Merelli 和 James Worrell（编辑），第 48 届国际自动机、语言与编程学术会议，ICALP 2021，英国苏格兰格拉斯哥（线上会议），2021 年 7 月 12–16 日，LIPIcs 第 198 卷，第 87:1–87:14 页。Schloss Dagstuhl - Leibniz-Zentrum für Informatik，2021。[KUW86] Richard M. Karp、Eli Upfal 和 Avi Wigderson。构造完美匹配属于随机 NC。组合学，6(1):35–48，1986。[LMS18a] Daniel Lokshtanov、Dániel Marx 和 Saket Saurabh。有界树宽图上的已知算法可能已经最优。ACM Trans. Algorithms，14(2):13:1–13:30，2018。

[LMS18b] Daniel Lokshtanov、Dániel Marx 和 Saket Saurabh。略超指数参数化问题。*SIAM*计算杂志，47(3):675–702，2018年。[Lov14] Shachar Lovett。通信复杂度中对数秩猜想的最新进展。*EATCS*公报，112，2014年。[MVV87] Ketan Mulmuley、Umesh V. Vazirani 和 Vijay V. Vazirani。匹配与矩阵求逆一样容易。组合学，7(1):105–113，1987年。[Ned20] Jesper Nederlof。在假设采用二次时间矩阵乘法的情况下，二分图旅行商问题可在 $o(1.9999^n)$ 时间内求解。载于 Konstantin Makarychev、Yury Makarychev、Madhur Tulsiani、Gautam Kamath 和 Julia Chuzhoy 编，第*52*届 *ACM SIGACT*计算理论研讨会年会论文集，*STOC 2020*，美国伊利诺伊州芝加哥，*2020*年*6*月*22–26*日，第40–53页。ACM，2020年。[Rot17] Thomas Rothvoss。匹配多面体的扩展复杂度为指数级。*ACM*学报，64(6):41:1–41:19，2017年。[RS95] Ran Raz 和 Boris Spieker。关于通信复杂度中的“对数秩”猜想。*Combinatorica*，15(4):567–588，1995年。[VW18] Virginia Vassilevska Williams 和 R. Ryan Williams。路径、矩阵和三角形问题之间的亚立方等价。*ACM*学报，65(5):27:1–27:38，2018年。[War62] Stephen Warshall。关于布尔矩阵的一个定理。*ACM*学报，9(1):11–12，1962年。