arXiv:2603.04255v1 [cs.CC] 4 Mar 2026

学习只读一次行列式与主子式赋值问题

Abhiram Aravind[1], Abhranil Chatterjee[2],Sumanta Ghosh[3],Rohit Gurjar[4],Roshan Raj[5],和 Chandan Saha[1]

[1]印度科学研究所（班加罗尔） [2]印度理工学院坎普尔分校 [3]印度统计研究所（加尔各答）[4]印度理工学院孟买分校 [5]塔塔基础研究所，孟买

摘要

秩一限制下的符号行列式计算形如 $\det(A_0 + A_1y_1 + \ldots + A_ny_n)$ 的多项式，其中 $A_0, A_1, \ldots, A_n$ 是域 $\mathbb{F}$ 上的方阵，且对于每个 $i \in [n]$，$\mathrm{rank}(A_i) = 1$。自 Edmonds （1967 年）的工作以来，这类多项式在线性拟阵、匹配、矩阵补全和多项式恒等式检验的背景下得到了广泛研究。我们研究这类多项式的以下学习问题：给定一个 n 元多项式 f 的黑盒访问，且 $f = \det(A_0 + A_1y_1 + \ldots + A_ny_n)$，其中 $A_0, A_1, \ldots, A_n$ 是 $\mathbb{F}$ 上的未知方阵，且对于每个 $i \in [n]$，$\mathrm{rank}(A_i) = 1$，求一个方阵 B_0 和秩一方阵 $B_1, \ldots, B_n$，它们均在 $\mathbb{F}$ 上，并满足 $f = \det(B_0 + B_1y_1 + \ldots + B_ny_n)$。在本文中，我们给出一个随机多项式时间算法来解决这一问题；该算法可以在准多项式时间内去随机化。据我们所知，这是针对这类多项式的首个高效学习算法。由于上述多项式类已知等价于只读一次行列式（ROD）类，我们将这一问题称为学习 ROD。一个 ROD 计算的是某个矩阵的行列式，该矩阵的元素为域常数或变量，且每个变量在矩阵中至多出现一次。因此，ROD 类是一个罕见的例子：一个经过充分研究的多项式类能够实现高效适当学习。

学习 ROD 的算法是通过联系线性代数中一个著名的开放问题——主子式赋值问题 (PMAP) 得到的。该问题要求找出（如果可能的话）一个具有给定主子式的矩阵。机器学习领域也研究过 PMAP，以学习行列式点过程的核矩阵。在这里，我们研究 PMAP 的一个自然的黑盒版本：给定对一个 n 元多项式 $f = \det(A + Y)$ 的黑盒访问，其中 $A \in \mathbb{F}^{n\times n}$ 未知，且 $Y =$ 为 $\mathrm{diag}(y_1, \ldots, y_n)$，求一个 $B \in \mathbb{F}^{n\times n}$，使得 $f = \det(B + Y)$。我们证明，黑盒 PMAP 可在随机多项式(n) 时间内求解；此外，它与学习 ROD 随机多项式时间等价。这两个问题之间的算法和归约都可以在准多项式时间内去随机化。据我们所知，此前尚无高效算法能够求解这一黑盒版本的 PMAP。

我们通过考察稠密矩阵的一项关键性质来解决黑盒 PMAP，我们将其称为秩一扩张性质。理解具有此性质的矩阵的“割”，并设计黑盒割查找算法，以仅使用 4 阶或更低阶的主子式来求解此类矩阵的 PMAP，构成了本文的技术核心。沿途获得的见解也帮助我们给出了首个用于主子式等价问题的 NC 算法。该问题要求检验给定的两个矩阵是否具有相等的对应主子式。

目录

1 引言 1
1.1 我们的结果 .31.2 证明思路 .51.3 与先前研究的比较 .101.4 其他相关工作 .11

2 预备知识 11
2.1 可约矩阵与不可约矩阵 .112.2 对角相似 .122.3 主子式等价 .122.4 矩阵切割 .132.5 切割转置操作 .142.6 对取逆输入的黑箱求值 .15

3 学习 ROD 与黑盒 PMAP 之间的等价性 15
3.1 从学习 ROD 到黑盒 PMAP .173.2 从黑盒 PMAP 到学习 ROD .19

4 对具有性质 $\mathcal{R}$ 20 的矩阵进行黑盒 PMAP 到 PMAP 的归约
4.1 $(A+D)^{-}$ 的不可约块满足性质 $\mathcal{R}^1$ .20 4.2 从 det(A +Y) 的黑盒访问得到 $\det((A+D)^{-1}+Y)$ 的黑盒访问.22 4.3 学习 $\det((A+D)^{-1}+Y)$ 的不可约块的指标集 . . . . . 23 4.4 恢复一个与 A 主子式等价的矩阵.25 4.5 去随机化归约.25

5 PME 至 4 阶的充分性：定理 1.3 的证明26

6 黑箱割查找346.1 割寻找算法.34**7 具有性质 $\mathcal{R}$ 的矩阵的 PMAP：定理 1.4 的证明42**7.1 4×4 矩阵的重构.437.2 具有性质 $\mathcal{R}$ 且无割的矩阵的 PMAP.457.3 具有性质 $\mathcal{R}$的矩阵的 PMAP：归约到无割情形.50

8 PME 的 NC 算法：定理 1.2 的证明 52
8.1 确保非零非对角元 .528.2 确保性质 $\mathcal{R}$ .53**A 第5节缺失的证明 60**A.1 引理 5.4 的证明 .60A.2 引理 5.7 的证明 .62A.3 引理 5.8 的证明 .64

B 性质 $\mathcal{R}$ 能否去掉? 64

1 引言

学习算术电路是代数复杂性理论中的一个基本问题。算术电路是布尔电路在算术方面的对应物，由加法和乘法运算组成，并计算输入变量的多元多项式。电路类 $\mathcal{C}$ 的学习问题（又称重构问题）要求通过黑盒访问一个多项式f，找到一个电路C；该多项式可由类 $\mathcal{C}$ 中的电路计算，且C 计算f。黑盒访问f 使我们能够在一个时间步内获得f 在任意选定点处的值。如果输出电路C 属于类 $\mathcal{C}$，则称这种学习是适当的。

尽管相关研究已持续二十余年，但目前已知能够高效地进行适当学习的电路类仍屈指可数。这并不令人意外，因为对于大多数电路类而言，适当学习被认为是一个计算困难的问题。已知能够进行适当学习的一些重要电路类包括稀疏多项式（即深度二电路） [BT88, KS01], 只读一次公式（ROF） [HH91, BHH95, SV14, MV18], 以及变量顺序已知的只读一次无关代数分支程序（ROABP） [BBB+00, KS06]。代数分支程序（ABP）可视为偏斜电路，是一种强大的算术计算模型（电路类）。代数复杂性中最重要的多项式之一——行列式多项式——可由多项式规模的 ABP 计算 [Ber84, MV97]。根据一项已知的从 ABP 到符号行列式的归约 [Val79], ，可以假设 ABP 计算的多项式具有如下形式：$\det(A_0 + A_1y_1 + \ldots + A_ny_n)$，其中 $y_1, \ldots, y_n$ 是变量，$A_0, A_1, \ldots, A_n \in \mathbb{F}^{r\times r}$ 是底域 $\mathbb{F}$上的 $r \times r$ 矩阵。

过去备受关注的一类 ABP 子类是秩一限制下的符号行列式。若多项式 f 可表示为 $\det(A_0 + A_1y_1 + \ldots + A_ny_n)$，其中 $A_1, \ldots, A_n \in \mathbb{F}^{r\times r}$ 为秩一矩阵，而对 $A_0 \in \mathbb{F}^{r\times r}$没有任何限制，则称 f 可由该类计算。在过去几十年中，该类在拟阵问题、矩阵补全和多项式恒等式检验的背景下得到了广泛研究 [Edm67, Edm68, Edm79, Lov89, Mur93, Gee99, HKM05, IKS10, IKQS15, GT20]。该类的边界复杂度最近也得到了研究 [CGGR23]。在本工作中，我们研究该类的学习问题。

问题*1.1.* 给定对 n元多项式 $f = det(A_0 + A_1y_1 + \ldots + A_ny_n)$ 的黑盒访问，其中 $A_0, A_1, \ldots, A_n$ 是 $\mathbb{F}$上的未知方阵，且对每个 $i \in \{1, \ldots, n\}$，$rank(A_i) = 1$，求 $\mathbb{F}$ 上的一个方阵 B_0 以及秩一方阵 $B_1, \ldots, B_n$，使得 $f = det(B_0 + B_1y_1 + \ldots + B_ny_n)$。

已知，在秩一限制下可由符号行列式计算的多项式，也可由小规模的只读一次行列式（ROD）计算（参见 [GT20]中的引理 4.3）。

只读一次行列式。ROD 是一个矩阵的行列式，M 其元素为变量或域常数，并且每个变量在M中至多出现一次。矩阵M 的维数决定了该 ROD 的规模。反过来说，很容易看出，根据定义，ROD 是一种施加秩一限制的符号行列式。由于 ROD 与施加秩一限制的符号行列式这两类对象本质上相同，我们将把问题1.1称为学习 *ROD*。ROABP 和 ROD 都是比 ROF 表达能力更强的类 [Val79]。但是，与 ROABP 不同，ROD并非通用，也就是说，并非每个多项式都能表示为 ROD。例如，初等对称多项式和永久多项式都不能表示为 ROD [AJ15]。另一方面，行列式和迭代矩阵乘法多项式（它们都定义了重要的代数复杂性类代数分支程序的完备多项式族）可以由小规模 ROD 表示 [Val79]。值得注意的是，任何计算行列式的 ROABP 都具有指数规模 [Nis91], ，因此，即使允许不恰当地学习，学习 ROABP 也不是学习 ROD 的可行方法。因此，问题1.1 在代数复杂性理论中本身就很有意义

理论。此外，研究这个问题还有另一个重要动机，这源于它与主子式赋值问题(PMAP)之间的联系。

主子式赋值问题。PMAP 是线性代数中的一个著名未解问题[HS02, GT06b]。给定一个由 2^n-1 域元素组成的列表 $\mathcal{P}=(\mathrm{p}_S)^{\varnothing\neq S\in 2^{[n]}}$，PMAP 要求找出（如果可能）一个矩阵 $\mathrm{A}\in\mathbb{F}^{n\times n}$，使得对于所有非空的 $\mathrm{S}\in 2^{[n]}$，由 S 所索引的行和列定义的 A 的主子式均为 p_S。如果 $\mathcal{P}$ 已知是某个未知矩阵 A 的主子式列表，通常假设 $\mathcal{P}$ 以预言机的形式给出，查询 S 时返回 p_S；目标是尽可能减少对预言机的查询次数 $\mathcal{P}$。如果待重构的矩阵 A 具有特殊性质，例如是对称矩阵或幅值对称矩阵 [RKT15, Bru18, BU24]，或某种稠密矩阵 [GT06b]，则已有高效算法可在多项式时间内仅向预言机查询 poly(n) 次来解决 PMAP。但利用预言机访问主子式列表 $\mathcal{P}$，在多项式时间内学习任意矩阵 A 的问题仍未解决。尽管 PMAP 本身就是线性代数中一个有趣的问题，研究它的另一动机则来自对行列式点过程（DPP）的学习。

与一个 $n\times n$ 核矩阵 K 相关联的 DPP 是定义在一个包含 n 个项目的集合的子集上的概率分布，其中任意子集 $T\subseteq[n]$ 的概率由以 K 中 T 为索引的主子式给出（参见 [KT12]）。DPP 适用于需要抽取多样化对象集合的场景。DPP 的学习问题是：给定来自该概率分布的样本，学习与之相关的核矩阵。针对对称矩阵的高效 PMAP 算法 [Oed11，RKT15]在推动对称 DPP 学习取得重大进展方面发挥了关键作用 [UBMR17]，因为可以利用矩法，根据观测到的样本准确估计核矩阵的主子式。通过 PMAP，在学习底层核矩阵为幅值对称的带符号行列式点过程方面也取得了类似进展 [Bru18，BU24]。

现在注意，多项式 $f=\det(A+Y)$ 的系数，其中 $Y=\mathrm{diag}(y_1,\ldots,y_n)$，且 $A\in\mathbb{F}^{n\times n}$，就是 A 的主子式。这自然促使我们研究主子式赋值问题的以下黑盒版本。

问题 1.2。给定一个 n 元多项式 $f=\det(A+Y)$ 的黑盒访问，其中 $A\in\mathbb{F}^{n\times n}$ 未知，且 $Y=\mathrm{diag}(y_1,\ldots,y_n)$，求一个 $B\in\mathbb{F}^{n\times n}$，使得 $f=\det(B+Y)$。

由于通过插值，黑盒允许我们在 A 上以 $\mathrm{poly}(n)$ 时间恢复一个主子式（假设 $|\mathbb{F}|>n$），我们将问题 1.2 称为 黑盒 *PMAP*。注意，$\det(A+Y)$ 是一个只读一次行列式，因此，问题 1.2 显然与问题 1.1有关。此外，两者都是适当学习问题。

注意，问题 *1.2* 中的输出 B 与 A 具有相同的对应主子式。若两个矩阵所有阶的对应主子式均相等，则称它们为主子式等价 (PME)。判定两个给定矩阵是否 PME 的问题与 PMAP 自然相关。对于某些特殊情形，例如对称矩阵 [ES80], 无割矩阵 [HL84、Loe86], 以及其他一些与反对称性相关的类别 [BC15、BC16、BCCL21]，此前已知 PME 的一些刻画。最近，针对一般情形的 PME 刻画已得到证明 [CGGR25], ，并给出了一个多项式时间确定性算法，用于检验两个给定矩阵是否 PME。简而言之，他们的刻画证明，两个矩阵 PME 当且仅当它们可通过一系列称为割转置（见小节 2.5）的简单运算相互转换。该算法从其中一个矩阵出发，不断应用适当的割转置运算，并在至多 $2n$ 步内到达另一个矩阵，否则便判定它们不 PME。该算法似乎本质上是串行的，由此引出了一个有趣的问题：

问题 1.3。是否存在高效的并行（*NC*）算法来检验 *PME*?

NC 类包含这样一类问题：我们可以使用多项式数量的处理器，在多对数时间内运行并行算法。有趣的是，如果允许随机化，那么可以通过归约到多项式恒等式检验（PIT），得到一种简单的并行算法来检验 PME。如前所述，两个矩阵 A 和 B 是 PME，当且仅当多项式恒等式 行列式$(A + Y) =$ 行列式$(B + Y)$ 成立。检验多项式恒等式的一种简单随机化算法是为变量代入随机数并检查两边是否相等 [Sch80、DL78、Zip79]，，该方法以高概率成功。注意，行列式可以通过高效的并行（NC）算法计算（例如参见 [Csa76、Ber84]），因此上述算法属于 RNC。尽管对多项式恒等式检验进行去随机化是一个颇具挑战性的开放问题，我们仍可探究能否对 PME 中出现的特定实例进行去随机化，从而得到一个 NC 算法。

在本文中，我们给出了随机化多项式时间算法，用于解决问题 1.1 （学习 ROD）和问题 1.2 （黑盒 PMAP）（见定理 1.1）。事实上，我们证明了这两个问题之间存在随机化多项式时间等价关系（见第 3 节），随后在随机化多项式时间内解决后者（见第 4-7 节）。等价证明和算法中涉及随机化的步骤，都可以在准多项式时间内去随机化。因此，ROD 所定义的多项式类是少数能够实现高效适当学习的多项式类之一。此外，据我们所知，在本文工作之前，尚无针对任何自然的 PMAP 黑盒版本的高效算法。我们还给出了一个 NC 算法来检验 PME，从而解决问题 1.3 （见定理 1.2 和第 8 节）。这些算法是通过研究稠密矩阵中阶数至多为 4 的主子式而得出的，这些矩阵满足一项我们称为“秩一扩张”的关键性质（见定理 1.3 和1.4）。

1.1 我们的结果

现在我们正式陈述我们的结果。这些结果在底层域 $\mathbb{F}$ 的大小满足一个温和条件时成立。我们还假设一次域运算所需时间为单位时间，且可以在多项式时间内对 $\mathbb{F}$ 进行平方根计算[1]。

定理 1.1 (主定理)。设 $n \in \mathbb{N}$且 $|\mathbb{F}| > n^6$。

1. (学习 ROD) 存在一个多项式(n) 时间的随机化算法，其输入为一个 n 元多项式 $f = \det(A_0 + A_1y_1 + \ldots + A_ny_n)$的黑盒访问，其中 $A_0 \in \mathbb{F}^{r\times r}$ 未知，$A_1,\ldots,A_n \in \mathbb{F}^{r\times r}$ 是未知的秩一矩阵，$r \in \mathbb{N}$ 也未知；算法输出（以高概率）一个矩阵 $B_0 \in \mathbb{F}^{n\times n}$ 及秩一矩阵 $B_1,\ldots,B_n \in \mathbb{F}^{n\times n}$，使得 $f = \det(B_0 + B_1y_1 + \ldots + B_ny_n)$。该算法可以在准多项式时间内去随机化。

2. （黑盒 PMAP）存在一个多项式(n) 时间随机化算法，其输入为对 n元多项式 $f = \det(A + Y)$的黑盒访问，其中 $A \in \mathbb{F}^{n\times n}$ 未知，且 $Y = \mathrm{diag}(y_1,\ldots, y_n)$；算法输出一个矩阵 $B \in \mathbb{F}^{n\times n}$，使得（以高概率）$f = \det(B + Y)$。该算法可以在准多项式时间内去随机化。

PMAP 的一种算法。黑盒 PMAP 的算法立即推出了一个用于 PMAP 的 $2^n \cdot \mathrm{poly}(n)$ 时间随机化算法，因为输入列表 $\mathcal{P} = (p_S)_{\varnothing\neq S\in 2^{[n]}}$ 可用于在 $2^n \cdot \mathrm{poly}(n)$ 时间内实现对黑盒的一次查询。注意，复杂度几乎与输入的大小线性相关 $\mathcal{P}$；如果没有承诺 $\mathcal{P}$ 与

[1]在 $\mathbb{Q}$上，可以在确定性多项式时间内求得平方根。在有限域上，有多种随机化多项式时间平方根求解算法。此外，如果已知 $\mathbb{F}_q$ 上的一个二次非剩余（在广义黎曼猜想下，这是一个有充分依据的假设），那么可以在确定性多项式时间内求得 $\mathbb{F}_q$上的平方根

某个矩阵的主子式一致，那么在没有这种承诺的情况下，就需要检查 $\mathcal{P}$ 是否与重构矩阵的主子式一致。由于 $\mathcal{P}$ 的大小为 $2^n - 1$，且矩阵的主子式可以在$O(2^n)$ 时间内计算 [GT06a], ，任何用于 PMAP 的算法都需要 $\Omega(2^n)$ 时间。从这个意义上说，我们给出了一个近乎最优时间算法来解决 PMAP。据我们所知，在本工作之前，PMAP 尚无 $\tilde{O}(2^n)$ 时间算法。将问题朴素地归约到多项式可解性需要付出$n^{O(n^4)}$ 的代价，因为矩阵有 $\mathbb{C}$ [Ier89],个n^2 个未知元素。

若已知 $\mathcal{P}$ 是某个矩阵的主子式列表，那么或许只需向预言机 $\mathcal{P}$ 查询少得多的次数即可。例如，若 $\mathcal{P}$ 是某个对称矩阵的主子式列表，那么$O(n^2)$ 次查询是必要且充分的 [RKT15]。该算法基于[Oed11] 对对称矩阵主子式簇的刻画。遗憾的是，通用 $n \times n$ 矩阵的主子式所满足的多项式关系理想尚未得到充分理解（除 $n = 4$ [LS09]外）。尽管如此，我们证明，对于满足某种一般性条件的矩阵，PMA 可以通过 $\mathrm{poly}(n)$ 次查询求解（见定理 1.4）。

证明梗概 定理 1.1 的证明梗概见小节 1.2.1。下面给出几点说明 :

说明。 1. 定理 1.1 中对 $\mathbb{F}$ 大小的条件源于应用多项式恒等式引理的需要（见引理 4.2）。如果黑盒允许我们在域扩张中的点进行查询，则可以去掉对域大小的这一假设。2. 对平方根求解效率的假设源于求解二次方程的需要（见小节 6 中的算法 7）。如果 $\mathrm{char}(\mathbb{F}) = 2$，那么求解二次方程可以归结为在 $\mathbb{F}_2$上求解线性方程组。

关于 PME 的下述定理的证明概要见第 1.2.3 节。

定理 1.2 （PME 属于 NC 复杂度类）。 判定两个给定矩阵的主子式等价性属于 *NC* 复杂度类。

定理 1.1 与1.2 中的算法，是通过研究我们接下来将定义的矩阵的一个关键性质而得到的。下面定理 1.3 的证明概要见第 1.2.2 节。

定义 1.1 （秩一扩张与性质 $\mathcal{R}$）。 若一个矩阵的所有非对角元均非零，则称该矩阵是稠密 的。我们称矩阵 A 满足秩一扩张 性质，如果下述条件成立：若秩$(A[\{i,j\},\{k,\ell\}]) = 1$ 对任意四个互异指标 $i,j,k,\ell \in [n]$, 成立，则存在一个子集 $S \subseteq [n]$，满足 $i,j \in S$ 且 $k,\ell \in S$，并使得秩$(A[S,S]) = 1$。我们称一个矩阵满足性质 $\mathcal{R}$，如果它是稠密的且满足秩一扩张性质。

理解并利用秩一扩张性质是本工作的技术贡献的核心。下面的定理展示了这一性质的实用性。

定理 1.3 （PME 充分性至阶数 4）。 设 A 是满足性质 $\mathcal{R}$ 的矩阵。设 B 是另一个与 A 大小相同的矩阵，且 A 和 B 的阶数至多为 4 的对应主子式相等。则 A 和 B 的所有阶数的对应主子式都相等。

性质 $\mathcal{R}$ 之所以如此有效，是因为任意矩阵的黑盒 PMAP 可以随机归约为满足性质 $\mathcal{R}$ 的矩阵的情形（见小节 4）。这一事实，加上下一个定理（其证明概要见小节1.2.1），给出了定理 1.1的证明。

定理 1.4（具有性质 $\mathcal{R}$的矩阵的 PMAP。）存在一种多项式时间算法：给定满足性质$\mathcal{R}$的矩阵 A 的所有阶数不超过4 的主子式的预言机访问 $\in \mathbb{F}^{n\times n}$，可重构出一个矩阵 B，使得 A 和 B 的对应主子式相等。

备注：1. 上述定理解决了满足性质 $\mathcal{R}$ 的矩阵的 PMAP，且所需时间为 $\mathrm{poly}(n)$，因为我们只需要访问阶数不超过 4 的主子式的预言机。相比之下，为了解决任意矩阵 A 的黑盒 PMAP，我们使用对$\det(A+Y)$ 的黑盒访问（见定理1.1）。事实证明，定理1.1的证明只需要访问矩阵 A 的主子式以及随机对角矩阵 $\mathrm{D}+D$ 所对应矩阵 A的主子式。

2. 随机矩阵满足性质 $\mathcal{R}$，因为它以高概率不含 2×2 秩一子矩阵。因此，性质 $\mathcal{R}$ 定义了一般性条件。在 [GT06b], 中，针对满足另一种一般性条件（即多项式(n)时间的 PMAP 算法被提出，该条件为矩阵非对角满秩（*ODF*）。性质 $\mathcal{R}$ 与 ODF 似乎不可比较（见第 1.3 节）。然而，任意矩阵的黑盒 PMAP 可归约为满足性质 $\mathcal{R}$ 的矩阵的 PMAP（见第 4 节）。尚不清楚对满足 ODF 的矩阵是否也成立。

3. DPP 的随机核可定义如下：令 $\mathrm{n}>1$, $\lambda\in(0,1/2)$，且 $\mu\in[0,\lambda/(\mathrm{n}-1))$. 令 $\mathrm{D}\in\mathbb{R}^{n\times n}$ 为一个对角矩阵，其中 $\mathrm{D}[\mathrm{i},\mathrm{i}]\in[\lambda,1-\lambda]$ 对所有 $\mathrm{i}\in[\mathrm{n}]$,均成立；再令 $\mathrm{A}\in\mathbb{R}^{n\times n}$ 的各个元素从 $[-1,1]$中随机且独立地选取。由于存在一个以 $\mathrm{K}=\mathrm{D}+\mu\mathrm{A}$ 为核的 DPP（见 [Bru18] 中的第 2.2 节），我们可以称 K 为随机核。注意，K 满足性质 $\mathcal{R}$，因为 A 是随机矩阵。从这个意义上说，可以使用定理 1.4，在多项式时间内通过其主子式预言机学习随机核。

1.2 证明思路

1.2.1 定理 1.1 和定理 1.4 的证明概要

为证明定理 1.1，我们首先建立一个从学习 ROD 到黑盒 PMAP 的随机多项式时间归约（事实上，我们在第 3 节证明这两个问题等价）。随后，我们使用下方算法中概述的三个主要步骤来解决黑盒 PMAP。该算法使用矩阵切割的概念：大小介于 2 和 n 之间的集合 $\mathrm{X}\subset[\mathrm{n}]$ 是矩阵 $\mathrm{A}\in\mathbb{F}^{n\times n}$ 的一个切割，当且仅当子矩阵 $\mathrm{A}[\mathrm{X},\mathrm{X}]$ 和 $\mathrm{A}[\mathrm{X},\mathrm{X}]$ 的秩至多为 1。矩阵 $\mathrm{A}\in\mathbb{F}^{n\times n}$ 的主子式预言机接受一个非空集 $\mathrm{S}\subseteq[\mathrm{n}]$ 作为输入，并输出由行和列中以 S 为索引的元素构成的 A 的主子式。

算法 1黑盒 PMAP

输入：对 $\mathrm{f}=\det(\mathrm{A}+\mathrm{Y})$ 的黑盒访问，其中 $\mathrm{Y}=\mathrm{diag}(\mathrm{y}_1,\ldots,\mathrm{y}_n)$，且 $\mathrm{A}\in\mathbb{F}^{n\times n}$ 未知。输出：一个矩阵 $\mathrm{B}\in\mathbb{F}^{n\times n}$，使得 $\mathrm{f}=\det(\mathrm{B}+\mathrm{Y})$。1：将该问题归约为在可访问 M 的主子式预言机的条件下学习 $\mathrm{M}\in\mathbb{F}^{n\times n}$，其中 M 满足性质 $\mathcal{R}$（见第 4 节中的算法 3）。2：使用黑箱割查找算法（第 6 节中的~~算法 5），将该问题进一步归约为根据~~ N 的主子式预言机学习 $\mathrm{N}\in\mathbb{F}^{m\times m}$，其中 N 满足性质 ~~$\mathcal{R}$ 且无割。（见~~第 7 节中的算法 9。）3：求解具有性质 $\mathcal{R}$ 且无割的矩阵的 PMAP（使用第 7 节中的算法 7）。

第 2 步中的割寻找算法仅访问阶数至多为 4 的主子式，并有助于将具有性质 $\mathcal{R}$ 的矩阵的 PMAP 归约为无割情形。因此，上述算法的最后两步以确定性多项式时间运行，并构成本工作的主要技术部分，从而给出定理1.4的证明。我们在下文简要讨论这些步骤。

步骤 0：将学习 ROD 归约为黑盒 PMAP。我们可以黑盒访问 $f=\det(A_0+\sum_{i\in[n]}A_iy_i)$，其中 $A_0,\ldots,A_n\in\mathbb{F}^{r\times r}$ 和$A_1,\ldots,A_n$ 均为秩一矩阵。我们将该问题归约为

在随机多项式时间内学习 $h = \det(A + Z)$，其中 $Z = \mathrm{diag}(z_1, \ldots, z_n)$，方法如下：

1. 首先，将f齐次化，得到次数为n的多重线性多项式$f' = t_1 t_2 \ldots t_n f\left(\frac{y_1}{t_1}, \frac{y_2}{t_2}, \ldots, \frac{y_n}{t_n}\right)$。
2. 使用隔离引理 [MVV87，第 3] 节，找出f'中的一个单项式（其系数非零）。将该单项式中的变量标记为$z_1, z_2, \ldots, z_n$，其余变量记为 $\bar{z}_1, \bar{z}_2, \ldots, \bar{z}_n$。
3. 令 γ 为 $z_1 z_2 \cdots z_n$ 在 f'中的系数。接着我们证明（在定理 3.1的证明中），

$$f' = \gamma \det\left(\begin{bmatrix} I_n & I_n \end{bmatrix} \begin{bmatrix} Z & O_{n,n} \\ O_{n,n} & \bar{Z} \end{bmatrix} \begin{bmatrix} I_n \\ A \end{bmatrix}\right) = \gamma \det(Z + \bar{Z}A),$$

对于某个域 $\mathbb{F}$上的 $n \times n$ 矩阵 A。这里，$Z = \mathrm{diag}(z_1, z_2, \ldots, z_n)$，且 $\bar{Z} = \mathrm{diag}(\bar{z}_1, \bar{z}_2, \ldots, \bar{z}_n)$。令 $\bar{z}_1, \bar{z}_2, \ldots, \bar{z}_n$ 为 1，进行缩放，并学习多项式 $h = \det(A + Z)$。

4. 若 $h = \det(A' + Z)$，则 $f' = \gamma \det\left(\begin{bmatrix} I_n I_n \end{bmatrix} \begin{bmatrix} Z\, O_{n,n} \\ O_{n,n}\ \bar{Z} \end{bmatrix} + \begin{bmatrix} Z \\ I_n A' \end{bmatrix}\right)$。令 $t_1, \ldots, t_n$ 为 1 并化简，得到 $f = \det(B_0 + \sum_{i \in [n]} B_i y_i)$，其中 $B_0, \ldots, B_n \in \mathbb{F}^{n \times n}$ 和 $B_1, \ldots, B_n$ 均为秩 1。

涉及隔离引理的步骤可以在准多项式时间内去随机化 [GT20]。

步骤 1：归约到具有性质 $\mathcal{R}$ 的矩阵的 PMAP。我们可以黑盒访问 $f = \det(A + Y)$，其中 A 是任意的 $n \times n$ 矩阵，且 $Y = \mathrm{diag}(y_1, \ldots, y_n)$。我们分三步将问题归约到 A 满足性质 $\mathcal{R}$ 的情形：

1. 我们首先证明，对于由随机选取的元素构成的对角矩阵 D，$B = (A + D)^{-1}$ 的极大不可约子矩阵（见定义 2.1 和观察 2.1）以高概率满足性质 $\mathcal{R}$（推论 4.1）。这里要求域的大小至少为 n^6。利用引理 4.3，我们可以黑盒访问 $\det(B + Y)$。 2. 由于 B 的不可约块具有非零非对角元，我们发现，当且仅当 $B[\{i, j\}]$ 不可约时，$i, j \in [n]$ 是同一不可约子矩阵的指标（可利用命题 4.5 检验）。随后，我们在算法 4 中比较足够多的指标对 i, j，从而找出与 B 的不可约子矩阵 $B_1, B_2, \ldots, B_s$ 相对应的指标，并获得它们的主子式预言机（利用命题 4.3）。 3. B 的每个不可约子矩阵 B_i 都满足性质 $\mathcal{R}$，分别学习这些子矩阵，就转化为求解满足性质 $\mathcal{R}$ 的矩阵的主子式赋值问题。设 C_1 PME$= B_1, C_2$ PME$= B_2, \ldots, C_s$ PME$= B_s$ 是我们学习得到的矩阵。那么，根据引理 2.1，存在一个置换矩阵 P，使得 $C = P^T \mathrm{diag}(C_1, \ldots, C_s) P$ PME $= B = (A + D)^{-1}$。由于我们已知与不可约子矩阵相对应的指标，因此 P 是已知的。接着，我们在引理 4.4 中证明 $C^{-1} - D$ PME $= A$。

利用小节 4.5 中概述的策略，可以在准多项式时间内对这一步进行去随机化。

步骤 2：利用黑箱割查找归约到无割情形。给定一个未知矩阵 M，它具有性质 $\mathcal{R}$，我们通过其主子式预言机证明：如果 M 存在一个割，那么 M 的学习问题可以归约为学习它的若干个主子矩阵，这些主子矩阵的总规模约等于 M 的规模（引理 6.7）。我们递归地应用这一归约，直到矩阵不存在割，然后使用步骤 3 中所述的学习算法。为了得到这些较小的主子

矩阵，我们必须找到 M 的一个割，或找到与之主子式等价的其他矩阵。给定一个显式矩阵，[CGGR25] 将查找割的问题归约为次模函数最小化。尚不清楚如何利用主子式预言机（或 $\det(M + Y)$ 求值预言机）获取他们所最小化的次模函数。

给定一个非对角元均非零的矩阵 M，容易看出，集合 S 是一个割，当且仅当对于每个 $\{i, j\} \subset S$ 和 $\{k, l\} \subset S$，$M[\{i, j, k, l\}]$ 具有 $\{i, j\}$（等价地，$\{k, l\}$）作为割。仅能访问 M 的主子式时，我们无法直接判断 $M[\{i, j, k, l\}]$ 是否具有这样的割。不过，我们可以高效地检验是否存在另一个与之主子式等价的矩阵，并且该矩阵以 $\{i, j\}$ 为割（观察 6.1）。结合 [CGGR25] 关于割的一些结构性质，我们证明这对于具有性质 $\mathcal{R}$ 的矩阵已足够。具体而言，集合 S 是具有性质 $\mathcal{R}$ 的矩阵 M 的割，或是某个与其主子式等价的矩阵的割，当且仅当对于所有 $\{i, j\} \subset S$ 和 $\{k, l\} \subset S$，都存在一个与 $M[\{i, j, k, l\}]$ 主子式等价且具有相应割的矩阵（引理 6.2）。我们称这样的集合为可信集合（定义 6.2）。

利用这一想法，我们给出算法 5 来寻找一个合理集合。为说明该想法，我们描述一个相对简单的算法，用于寻找显式给定矩阵的一个割。同一想法稍作修改即可推广到寻找合理集合（见注 6.1）。给定矩阵 M、指标集中四个元素构成的集合 $\{i, j, k, l\}$，以及满足 $i, j \in S$ 且 $k, l \in S$ 的集合 S，假设我们需要判定 S 是否为 M 的一个割。首先，$M[\{i, j, k, l\}]$ 必须以 $\{i, j\}$ 为一个割。若 S 是这样的割，则当 $M[\{i, e, k, l\}]$ 不以 $\{i, e\}$ 为割时，元素 e 不能属于 S。类似地，若 $M[\{i, j, k, e\}]$ 不以 $\{i, j\}$ 为割，则 e 不能在 S 中。此外，对于两个元素 p、q，若 $M[\{i, p, q, l\}]$ 不以 $\{i, p\}$ 为割，则不能出现 $p \in S$、$q \in S$ 的情形。可以证明，这些局部条件足以检验 S 是否为割。引理 6.3 表明，对于具有性质 $\mathcal{R}$ 的矩阵，类似的局部条件足以使一个集合成为合理集合。这样的集合可通过将该问题归约为一个 2-SAT 实例来找到，其中每个变量对应一个指标，每个子句强制上述条件之一（详见算法 5）。

步骤 3：求解具有性质 $\mathcal{R}$ 且无割的矩阵的 PMAP。设 $A \in \mathbb{F}^{n \times n}$ 是满足性质 $\mathcal{R}$ 且无割的矩阵。我们可以获取 A 的主子式。若存在可逆对角矩阵 D，使得 $N = D^{-1}MD$，则称两个矩阵 M、$N \in \mathbb{F}^{n \times n}$ 对角相似。由于 A 的所有非对角元均非零，存在唯一一个矩阵 M，使得 M 与 A 对角相似，且对所有 $i \in [n] \setminus \{1\}$，$M[1,i] = 1$。此外，M 的 $PME = A$，即 M 与 A 的对应主子式相等。因此，不失一般性，我们可以假设对所有 $i \in [n] \setminus \{1\}$，$A[1,i] = 1$。我们的目标是计算一个矩阵 B，使得 B 的 $PME = A$。此外，对所有 $i \in [n] \setminus \{1\}$，矩阵 B 的元素 $B[1,i]$ 为 1。

我们通过迭代构造 B。不过，在迭代过程中，我们并不遵循任意的指标序列。相反，我们从 I 中计算出一个由互不相同的元素组成的序列 $\mathcal{X} = (i_n, i_{n-1}, \ldots, i_3, i_2) \setminus \{1\}$，使得对所有 $j \in \{4, 5, 6, \ldots, n\}$，$A[I_j]$ 均无割，其中 $I_j = \{1, i_2, i_3, \ldots, i_j\}$。由于 A 满足性质 $\mathcal{R}$，这样的序列存在，且可在多项式时间内计算得到（参见推论 5.1 和算法 8）。

该序列的用途 $\mathcal{X}$ 可解释如下：在第 j 次迭代中，我们构造子矩阵 $B[I_j]$，使得 $B[I_j] \overset{\text{PME}}{=} A[I_j]$。由于 $A[I_j]$ 无割，根据 [Loe86，定理 1]（或者参见引理 2.3），再结合 A 和 B 两者的其他结构性质，我们得到

$$B[I_j] = A[I_j], \text{ or } B[I_j] \text{ is diagonally similar to } A^T[I_j] \tag{1}$$

这将有助于正确执行迭代。相比之下，如果 $A[I_j]$ 有一个割，根据 [CGGR25，定理 11]，，我们得到 $A[I_j]$ 与 $B[I_j]$ 之间较弱的关系，但尚不清楚如何将其用于我们的目的。

在第 j 次迭代开始时，$A[I_j]$ 中唯一未知的元素位于由 i_j索引的行和列中。注意，$B[i_j, i_j] = A[i_j, i_j]$，因此这个对角元是已知的。由于 $B[1, i_j] = 1$，根据条件 $B[\{1, i_j\}]$ PME= $A[\{1, i_j\}]$，元素 $B[i_j, 1]$ 也已确定。接下来，我们通过迭代计算所有满足 $s \in I_j \setminus \{1, i_j\}$ 的 $B[i_j, s]$。

与之前一样，我们避免沿着任意序列进行。相反，我们从 $I_j \setminus \{1, i_j\}$ 中找出一个由互不相同的元素组成的序列 $(k_j, k_{j-1}, \ldots, k_3)$，使得对于所有 $\ell \in \{4, 5, 6, \ldots, j\}$，子矩阵 $A[L_\ell]$ 均无割，其中 $L_\ell = \{1, i_j, k_3, \ldots, k_\ell\}$。由于 A 满足性质 $\mathcal{R}$，子矩阵 $A[L_\ell]$ 也满足该性质（见引理 5.1 ）。此外，由于 $A[I_j]$ 无割，这样的序列必然存在，并且可以在多项式时间内计算得到（见推论 5.1 和算法 8）。

注意，$L_j = I_j$。我们通过迭代计算矩阵 $B[L_j]$，使得 $B[L_j]$ PME= $A[L_j]$。在第 ℓ 次迭代中，唯一未知的元素是 $B[i_j, k_\ell]$ 和 $B[k_\ell, i_j]$。此外，一旦确定 $B[i_j, k_\ell]$，$B[k_\ell, i_j]$ 就由条件 $A[\{i_j, k_\ell\}]$ PME= $B[\{i_j, k_\ell\}]$ 唯一确定。注意，$A[\{1, i_j, k_\ell\}]$ 必须与 $B[\{1, i_j, k_\ell\}]$ 主子式等价。这使得 $B[i_j, k_\ell]$ 的取值至多有两种可能，分别对应某个适当二次方程的根（见引理 7.2）。此外，我们注意到：

1. 由于 $L_\ell - i_j$ 是 I_{j-1} 的子集，对第 $(j-1)$ 次迭代应用公式 (1)，可得 $B[L_\ell - i_j] = A[L_\ell - i_j]$，或者它与 $A^T[L_\ell - i_j]$ 对角相似。2. 由于 $A[L_{\ell-1}]$ PME= $B[L_{\ell-1}]$ 且 $A[L_{\ell-1}]$ 无割，再由 Loe86 的定理 1]（或参见引理 2.3），可得 $B[L_{\ell-1}] = A[L_{\ell-1}]$，或者它与 $A^T[L_{\ell-1}]$ 对角相似。

结合上述事实，我们得到四种可能情形，并据此计算满足 $B[L_\ell]$ PME= $A[L_\ell]$ 的 $B[L_\ell]$。为确定 $B[L_\ell]$ 的正确候选，定理 1.3 起着关键作用。对于 $B[L_\ell]$ 的每种可能选择，我们都会验证 $A[L_\ell]$ 与 $B[L_\ell]$ 的 4 阶及以下对应主子式是否相等。由于 $A[L_\ell]$ 满足性质 $\mathcal{R}$，根据定理 1.3，这项验证足以确定 $A[L_\ell]$ PME= $B[L_\ell]$ 是否成立。因此，我们可以在多项式时间内找到正确的 $B[L_\ell]$。

更多细节请参见算法7 及其在第7.2.1节中的正确性。

1.2.2 定理1.3的证明概要

考虑两个矩阵 A、$B \in \mathbb{F}^{n \times n}$，它们阶数不超过 4 的对应主子式相等。进一步假设A 满足性质 $\mathcal{R}$。我们的目标是证明A 和B 的所有阶数不超过n的对应主子式都相等。我们先考虑A 无割的情形，这构成了证明中主要的技术部分。

1. 假设A 无割。我们通过对n进行归纳法，证明A 与B 主子式等价。基例$n = 4$显然成立。

   对于任意 $k \in [n]$,，令 A_k 和 B_k 分别表示从 A 和 B 中删去第 k 行和第 k 列后得到的主子矩阵。令 $I \subseteq [n]$ 为这样一个指标集合：其中 A_i与 B_i 或 B_i^T对角相似。根据引理 2.2 [HL84、引理 1],，只需证明$|I| \geq 5$，因为这将意味着 A 与 B 或 B^T对角相似。因此，A 和 B 主子式等价 [Loe86，定理 1]（另见引理 2.3）。

   对于 $n \geq 5$，我们证明至少存在三个指标 $i_1, i_2, i_3 \in [n]$，使得每个 A^{i_j} 都没有割。我们关键地利用性质 $\mathcal{R}$ 来证明这些指标的存在（见推论 5.1）。根据归纳假设，A^{i_j} 与 B^{i_j}主子式等价。由于 A^{i_j} 没有割，再由 [Loe86 定理 1]（另见引理 2.3）可知，A^{i_j} 与 B^{i_j} 或其转置对角相似。

我们有 $|I| \geq 3$，其中 $i_1, i_2, i_3 \in I$。接着，我们利用 A 和 B 在至多 4 阶时的主子式等价，以及 A 的性质 $\mathcal{R}$，证明如果 $|I|$ 是 3 或 4，那么 A 必然有割（见引理 5.5 和引理 5.6）。这与 A 没有割的假设相矛盾。[Loe86 的定理 2 和定理 4] 中也出现了类似结果，其假设是 A 和 B 是稠密矩阵，且所有阶的主子式都等价。另一方面，我们证明，即使假设矩阵仅在至多 4 阶时主子式等价，并且 A 还满足秩一扩张性质，该结果仍然成立。

2. 若 A 有割，我们就考虑 A 的一个极小割 S。我们首先证明，S 也可能是 $\widetilde{B}$ 的割，或者存在另一个矩阵 B，它与 B 主子式等价，且 S 是 B 的割（参见引理2.7、引理5.8）。引理2.7 和引理5.8 的一些较弱版本见[CGGR25，引理 3.5 和引理 3。6]。我们注意到，几乎相同的证明也适用于我们的情形。接下来的论证依赖于分解引理（参见引理5.7），该引理断言以下两个命题等价：

(a) A 与 B 主子式等价。(b) 对于 A 和 B 的某个公共割 S，$A[S + t]$ 与 $B[S + t]$ 主子式等价，并且对于任意 $s \in S$，$A[S + s]$ 与 $B[S + s]$ 主子式等价，且 $t \in S$。

我们使用 [CGGR25中证明引理 2 的思路12] 来证明分解引理。在上述设置下，归纳证明从以下情形开始：基例要么是 $n = 4$，要么是 A 具有无割。

1.2.3 定理1.2的证明概要

为了设计一个用于主子式等价的 NC 算法，我们首先考虑一个特殊情形：其中一个矩阵满足性质 $\mathcal{R}$。在这种情形下，定理1.3 立即给出一个 NC 算法，因为我们可以并行验证对于所有 $S \subseteq [n]$ 中大小至多为 4 的 S，是否有 $\det(A[S]) = \det(B[S])$，从而确定 A 与 B 的主子式等价性。为解决一般情形，我们通过以下步骤对上述特殊情形给出一个 NC 归约。

1. 矩阵 A 和 B 是主子式等价的，当且仅当它们的极大不可约子矩阵在指标集 $[n]$, 上诱导出相同的划分，并且相应的主子矩阵本身也是主子式等价的（见引理 2.1）。极大不可约子矩阵对应于与输入矩阵相关联的图的强连通分量（见观察 2.1），可以使用用于寻找强连通分量的标准并行算法在 NC 中计算得到 [GM88、CV89]。

2. 令 M^{adj} 表示矩阵 M 的伴随矩阵，Y 为一个 $n \times n$ 对角矩阵，其对角线上是不重复的不定元。当且仅当 $(A + Y)^{adj}$ 和 $(B + Y)^{adj}$ 主子式等价时，A 与 B 主子式等价（[HL84，引理 4]）。此外，我们证明 $(A + Y)^{adj}$ 满足性质 $\mathcal{R}$（见断言 4.1）。

我们现在的目标是在 NC 复杂度类中计算一个对角矩阵 D，使得 $(A + D)^{adj}$ 满足性质 $\mathcal{R}$。因此，这将两个不可约矩阵 A 和 B 的主子式等价判定归约为对 $(A + D)^{adj}$ 与 $(B + D)^{adj}$ 的主子式等价判定。然而，我们不知道有直接计算这样的 D 的 NC 算法。相反，我们首先在 NC 复杂度类中计算一个对角矩阵 D_1，使得 $A_1 = (A + D_1)^{adj}$ 的所有元素均非零（引理 8.1）。接下来，我们在 NC 复杂度类中计算另一个对角矩阵 D_2，使得 $A_2 = (A_1 + D_2)^{adj}$ 满足性质 $\mathcal{R}$（引理 8.2）。由于矩阵的行列式可以在 NC 复杂度类中计算 [Csa76, BCP83], ，所有这些矩阵都可以在 NC 复杂度类中计算。

1.3 与以往工作的比较

本节中 , we 提供与我们的工作直接相关的已知结果的比较 .

文献 [HH91、BHH95] 给出了针对 ROF 的随机多项式时间学习算法。这些算法在 [SV14、MV18] 中通过使用 ROF 的命中集实现了多项式时间去随机化。类似地，文献 [BBB+00、KS06] 中针对 ROABP（变量顺序已知）的随机多项式时间学习算法，在 [FS13] 中通过使用 ROABP 的命中集实现了准多项式时间去随机化。如果变量顺序未知，那么学习 ROABP 是困难的[BDGT24]。ROD 类比 ROF 更强（通过 [Val79] 中的一个归约）。容易证明，三次行列式多项式有一个规模为 3 的 ROD，却无法由 ROF 计算。不过，ROD 无法涵盖 ROABP—— 具有多项式规模 ROABP 的初等对称多项式无法表示为 ROD [AJ15]。另一方面，任何计算 n 次行列式多项式的 ROABP，其规模至少为 $2^{\Omega(n)}$ [Nis91]。因此，针对 ROF 和 ROABP 的学习算法并不能说明 ROD 可以被高效学习。此外，用于学习 ROF 和 ROABP 的偏导数及求值维数方法似乎不适用于学习 ROD。不过，与 ROF 和 ROABP 学习的情形一样， [GT17] 中针对 ROD 的命中集可用于将我们的 ROD 学习算法去随机化至准多项式时间（见第 4.5 节）。

已知，对于以下几类矩阵，PMA 问题存在多项式时间解法：对称矩阵 [Oed11、RKT15], 模对称矩阵（|A(i, j)| =|A(j, i)|） [UBMR17、BU24], 以及 ODF（非对角满秩）矩阵 [GT06b]。前两种算法的核心都依赖于对称性或模对称性，因此其方法似乎不能直接用于非对称情形。GT06b], 引入的 ODF 性质涉及一个技术条件：算法每一步的解都必须唯一。尽管一般而言这一条件成立，但它似乎并不对应于给定矩阵的任何结构性质，因而无法保证 PMA 问题存在高效解法。另一方面，我们用于求解 PMA 问题（定理 1.4）的性质 $\mathcal{R}$是矩阵上的一种一般性结构条件。还需注意，根据定义，ODF 矩阵不可能存在割，而性质 $\mathcal{R}$ 没有这样的限制。此外，我们证明，任意矩阵上的黑盒 PMA 问题可归约为具有性质 $\mathcal{R}$的矩阵上的 PMA 问题。目前尚不清楚 ODF 矩阵是否也存在这样的归约。

如第1.1节所述，识别性质 $\mathcal{R}$ 并利用它解决 PMAP，是我们的关键技术思路之一。尽管文献中并未明确出现性质 $\mathcal{R}$，但其定义的灵感来自 Hartfiel-Loewy [HL84的定理 2] 以及 Loewy [Loe86的引理 6]中的证明。对于如下结果也是如此：任意不可约矩阵A，$(A + D)^{-1}$ 在随机对角矩阵 $\mathcal{R}$ D 下满足性质（引理4.2）。

我们对 PMAP 的求解建立在这样一个事实之上：对于具有性质 $\mathcal{R}$的矩阵，4 阶以内的 PME 蕴含 PME（定理1.3）。对于其他几类矩阵，也已有类似结果，例如满足某些其他条件的反对称矩阵 [BC16、BC15], 广义竞赛矩阵 [BCCL21], 以及模对称矩阵 [BU。与我们的代数方法不同，这些结果大多从根本上依赖图论技术。

这些结果还意味着，可以高效地并行测试这些类别中的 PME：通过并行计算，可以测试所有阶数不超过 3 或 4 的对应主子式是否相等。对于一般情形，此前尚无此类并行算法。已知唯一的高效 PME 测试算法 [CGGR25] 需要找到一系列切换转置操作，而这似乎无法并行化。这里我们利用性质 $\mathcal{R}$ 和定理1.3，为两个任意矩阵的 PME 测试提供并行算法（定理 1.2）。

1.4 其他相关研究

已知少数其他多项式类别也可进行适当学习。这些类别由顶层扇入有界的受限三层和四层算术电路定义 [Shp09, KS09, GKL12, Sin16, BSV20, BSV21]。与 ROD 一样，这些模型并非通用模型。ROABP 的学习算法意味着，两个重要的三层电路子类可以进行非适当学习，即三层幂电路（对称张量）和集合多线性三层电路（张量）。然而，在最坏情形下，学习一般的三层或四层电路（即使是不适当学习）想必很困难（关于学习困难性的讨论，见[KS19, GKS20]）。因此，人们已研究了各种电路模型（包括三层和四层电路）在平均情形下的学习复杂度 [GKL11, GKQ14, KNS19, KS19, GKS20, BGKS22]。值得注意的是，定义 PMAP 问题平均情形版本的一种自然方式，是令输入矩阵随机选取。由于随机矩阵以高概率满足性质$\mathcal{R}$ （见定理 1.4 之后的第二条备注），根据定理 1.4，我们便有该 PMAP 平均情形版本的确定性多项式时间算法。

2 预备知识

我们用 $[n]$ 表示正整数集合 $\{1,2,3,\ldots, n\}$。对于集合 S 及其子集 T，S，T表示 T的补集，即 $T = S \setminus T$。对于集合 S 及元素 s，我们用 $S + s$ 和 $S - s$分别表示集合 $S \cup \{s\}$ 和 $S \setminus \{s\}$。

对于一个 $n \times n$ 矩阵 A 以及子集 S、T $\subseteq [n]$，我们用 A[S, T] 表示 A 的子矩阵，其行由 S 索引，列由 T 索引。对于 S = T，我们用 A[S] 表示 A[S, S]。对于方阵 A，A^{adj} 表示 A 的伴随矩阵。对于向量 $(a_1, a_2, \ldots, a_n)$，$diag(a_1, a_2, \ldots, a_n)$ 表示 $n \times n$ 对角矩阵 D，其中对于 $i \in [n]$，D[i, i] $= a_i$。I_n 表示 $n \times n$ 单位矩阵，$0_{m,n}$ 表示 $m \times n$ 零矩阵。

2.1 可约矩阵与不可约矩阵

定义 2.1（可约矩阵与不可约矩阵）。若一个矩阵经过行置换及相应的列置换后可写成分块上三角矩阵，则称该矩阵为可约矩阵。不可约的矩阵称为不可约矩阵。

等价地，若将非零非对角元替换为 *1*，将对角元替换为 *0*，则可约矩阵对应于一个具有多个强连通分量的有向图的邻接矩阵。

从上述定义容易看出，所有非对角元均非零的矩阵A 是不可约矩阵。上述定义直接得出以下观察。

观察 2.1。 设 A 是域 F 上的 $n \times n$ 矩阵，且 A 的行和列由 $[n]$ 编号。设 G_A 是如下定义的有向图：顶点集为 $[n]$，且当且仅当 $i \neq j$ 且 $A[i, j] \neq 0$时，元组(i, j) 是 G_A 的一条边。设 $I_1, I_2, \ldots, I_s$ 是 A 的强连通分量。经过行置换及相应的列置换后，矩阵 A 可变为分块上三角矩阵，其对角块 $A[I_1]$, $A[I_2], \ldots, A[I_s]$ 均为不可约矩阵。

对于两个可约矩阵A 和B，下面的引理有助于将检验$A \overset{\text{PME}}{=} B$ 是否成立，归约为多次检验两个不可约矩阵是否具有相同的对应主子式。下面的引理直接由 [Ahm23的推论 54]得到。

引理 2.1。设 A 和 B 是域 $\mathbb{F}$ 上的两个 $n \times n$ 矩阵。假设在对行及其对应的列进行置换后，A 可以写成具有 s 个对角块的分块上三角矩阵 $A_1, A_2, \ldots, A_s$，其中每个 A_i 都是不可约的，并且 A_i 的行和列由集合 $T_i \subseteq [n]$ 索引。那么，当且仅当满足以下条件时，$A \overset{PME}{=} B$：

1. 经过置换若干行及其对应的列后，B 可以写成一个分块上三角矩阵，其有 s 个对角块 $B_1, B_2, \ldots, B_s$，其中每个 B_i 都不可约，且 B_i 的行和列由相同的集合 T_i 索引。

2. 对每个 $i \in [s]$, $A_i \overset{PME}{=} B_i$。

2.2 对角相似

设 A 和 B 是复数域上的 n $\times$n 矩阵。若存在可逆对角矩阵 D，使得 B $=$ D^{-1}AD，则称 A 与 B 对角相似，记作 A DS $=$ B。若不存在这样的矩阵 D，我们用 A $\neq$ B 表示 A 与 B 不对角相似。若 A DS $=$ B 或 A DS $=$ B^T，则称 A 与 B 对角等价，记作 A DE $=$ B。对于非对角元均非零的矩阵，我们有如下观察。

观察 2.2. 设 $A \in \mathbb{F}^{n \times n}$ 的非对角元均非零。那么，对于每个 $i \in [n]$, ，存在唯一的 $n \times n$ 矩阵 M_i，使得

$$M_i \overset{DS}{=} A \text{ and } M_i[i,j] = 1 \ \forall j \in [n] \setminus \{i\}.$$

对于固定的 $i \in [n]$, ，上述观察中的矩阵 M_i 可视为所有与A对角相似的矩阵的一个典范代表元 。接下来，我们定义两个子集 $\mathcal{D}_1(A,B)$和 $\mathcal{D}_2(A,B)$，它们都属于 $[n]$。

$$\mathcal{D}_1(A,B) := \{i \in [n] \mid A[[n] \setminus \{i\}] \overset{DS}{=} B[[n] \setminus \{i\}]\} \tag{2}$$

$$\mathcal{D}_2(A,B) := \{i \in [n] \mid A[[n] \setminus \{i\}] \overset{DS}{=} B[[n] \setminus \{i\}]^T\} \tag{3}$$

由这两个子集可得以下结果。

引理 2.2 ([HL84], 引理 1). 设 $n \geq 4$ 为一个整数。设 A 和 B 是两个 $n \times n$ 域上的矩阵$\mathbb{F}$。假设 A 的所有非对角元均非零。那么，

1. 若 $|\mathcal{D}_1(A,B)| \geq 3$，则 $A \overset{DS}{=} B$。*2.* 若 $|\mathcal{D}_2(A,B)| \geq 3$，则 $A \overset{DS}{=} B^T$。*3.* 若 $|\mathcal{D}_1(A,B) \cup \mathcal{D}_2(A,B)| \geq 5$，则 $A \overset{DE}{=} B$

2.3 主子式等价

设 A 和 B 是定义在 $\mathbb{F}$ 上的两个 n $\times$n 矩阵。若 A 和 B 的所有对应主子式都相等，则称矩阵 A 和 B 主子式等价，即对于所有 S $\subseteq$ [n], det A[S] $=$ det B[S]。我们用 A PME $=$ B 表示 A 与 B 主子式等价，用 PME(A, B, k) 表示 A 和 B 的所有阶数至多为 k 的对应主子式都相等，也就是说，对于所有 S $\subseteq$ [n] 且满足 |S| $\leq$ k，det A[S] $=$ det B[S]。用 PME(A, B, $\geq$ k) 表示

A 和 B 的所有阶数至少为 k 的对应主子式都相等，也就是说，对于所有$S \subseteq [n]$ 且满足 $|S| \geq k$，det $A[S] = \det B[S]$。

现在我们讨论对角等价与主子式等价之间的关系。首先，陈述如下观察结果。

观察 2.3. 设 A 和 B 是 $n \times n$ 阶矩阵，且其元素属于 $\mathbb{F}$，满足 $A \overset{DE}{=} B$。那么，$A \overset{PME}{=} B$.

接下来我们考虑上述观察结果的逆命题。Hartfiel 和 Loewy [HL84，定理 3]证明了：如果 A 和B 是阶数为$n = 2$ 或 3 的不可约矩阵，那么$A \overset{PME}{=} B$ 意味着$A \overset{DE}{=} B$。随后，Loewy [Loe86，定理 1] 证明了：对于不可约矩阵A 和B，若A</style'>无割，则$A \overset{PME}{=} B$ 意味着$A \overset{DE}{=} B$。结合这些结果，我们得到以下引理。

引理 2.3 。设 A 和 B 是 $n \times n$ 阶矩阵，元素属于 $\mathbb{F}$，且 A 不可约，并且 $A \overset{PME}{=} B$。那么，

1. 若 $n = 2$或3，则 $A \overset{DE}{=} B$ *2.* 若 $n \geq 4$且 A 无割，则 $A \overset{DE}{=} B$。

2.4 矩阵切割

定义 2.2 (矩阵切割)。设 A 是域 $\mathbb{F}$ 上的 $n \times n$ 矩阵，其中 $n \geq 4$。若集合 $[n]$ 的子集 X 满足 $2 \leq |X| \leq n - 2$，且子矩阵 $A[X, X]$ 和 $A[\overline{X}, \overline{X}]$ 的秩至多为一，则称 X 为矩阵 A 的一个割 。

特别地，若 A 是不可约矩阵，则 秩 $A[X,\overline{X}] =$ 秩 $A[\overline{X}, X] = 1$。

下面的引理说明如何从已有的一组割导出新的割。

引理2.4。设 A 是域 $\mathbb{F}$ 上的 $n \times n$ 矩阵，其中 $n \geq 2$，且 A 的所有非对角元均非零。设 X_1 和 X_2 是 $[n]$ 的两个子集，且 $X_1 \cap X_2$ 和 $X_1 \cap \overline{X_2}$ 均非空。令秩 $A[X_1, \overline{X_1}] =$ 秩 $A[\overline{X_2}, X_2] = 1$。那么，

$$\operatorname{rank} A[X_1 \cap X_2, \overline{X_1} \cup \overline{X_2}] = \operatorname{rank} A[X_1 \cup X_2, \overline{X_1} \cap \overline{X_2}] = 1.$$

证明。 根据引理的假设，我们有

$$\operatorname{rank} A[X_1 \cap X_2, \overline{X_1}] = \operatorname{rank} A[X_1 \cap X_2, \overline{X_2}] = 1$$

设 $k \in \overline{X_1} \cap \overline{X_2}$。那么，上述条件意味着，对于所有 $j \in X_1 \cup X_2$，，列 $A[X_1 \cap X_2, j]$都是$A[X_1 \cap X_2, k]$的标量倍；也就是说，

$$A[X_1 \cap X_2, j] = cA[X_1 \cap X_2, k] \text{ for some } c \in \mathbb{F}.$$

因此可知，$A[X_1 \cap X_2, X_1 \cup X_2] = 1$的秩为 1。类似的论证表明，$A[X_1 \cup X_2, X_1 \cap X_2] = 1$的秩为 1。 □

设A 是域 $\mathbb{F}$ 上的一个$n \times n$ 矩阵。于是，定义由 $\mathcal{A}(A)$ 给出的 $[n]$ 的不相交子集有序对族如下

$$\mathcal{A}(A) := \left\{(S, \overline{S}) \mid S \subseteq [n],\ 2 \leq |S| \leq n - 2,\ \operatorname{rank} A[S, \overline{S}] = 1\right\} \tag{4}$$

接下来，我们考虑 $[n]$ 的以下两个子集。

$$\mathcal{B}_1(A) := \{i \in [n] \mid \exists X \subseteq [n] \setminus \{i\} \text{ s.t. } (X+i, \overline{X}) \in \mathcal{A}(A) \text{ and } (\overline{X}+i, X) \in \mathcal{A}(A)\} \tag{5}$$

$$\mathcal{B}_2(A) := \{i \in [n] \mid \exists X \subseteq [n] \setminus \{i\} \text{ s.t. } (X, \overline{X}+i) \in \mathcal{A}(A) \text{ and } (\overline{X}, X+i) \in \mathcal{A}(A)\} \tag{6}$$

注意，在上述方程中，$X = [n] \setminus (\overline{X} + i)$。根据上述定义，Loewy [Loe86]给出了以下引理：

引理 2.5 ([Loe86], 定理 A.1)。 设 A 是一个 $n \times n$ 阶矩阵，其元素属于 $\mathbb{F}$，并且A 不可约且无割。令 $\mathcal{B}_1(A)$ 和 $\mathcal{B}_2(A)$ 分别定义为方程(5) 和方程(6)。那么，

$$|\mathcal{B}_1(A) \cup \mathcal{B}_2(A)| \leq n - 3.$$

2.5 切割转置操作

受 [Ahm23 的启发，CGGR5], [CGGR25] 引入了切割转置操作的概念，并利用该操作给出了主子式等价的刻画。下面我们介绍其定义以及在本文研究中有用的一些结果。更多细节请参见 [CGGR25，第 2 节。5]。

定义 *2.3 ([CGGR25], 定义 2.10)*。设 A 是一个 $n \times n$ 阶不可约矩阵，且 $X \subseteq [n]$ 是 A 的一个割。设 q、$u \in \mathbb{F}^{|X|}$ 满足 q^T 是 $\overline{A[X, X]}$ 的第一行非零行，而 u 是 $A[X, \overline{X}]$ 的第一列非零列。设 p、$v \in \mathbb{F}^{|X|}$ 满足 $A[X, \overline{X}] = p \cdot q^T$ 且 $A[X, X] = u \cdot v^T$。也就是说，

$$A = \begin{pmatrix} A[X] & p \cdot q^T \\ u \cdot v^T & A[\overline{X}] \end{pmatrix}$$

那么，关于 X 的 A 的切割转置操作记作，$\mathrm{ct}(A, X)$，它将 A 变换为以下矩阵：

$$\mathrm{ct}(A, X) = \begin{pmatrix} A[X] & p \cdot u^T \\ q \cdot v^T & A[\overline{X}]^T \end{pmatrix}$$

与对角等价（参见第2.2节）类似，矩阵的主子式在切割转置操作下保持不变。

引理 2.6。 设 A 是域 $\mathbb{F}$ 上的一个 $n \times n$ 阶不可约矩阵。设 $X \subseteq [n]$ 是矩阵 A 的一个割。那么，$A_{\text{与}} = \mathrm{ct}(A, X)$满足 *PME*。

证明见 [CGGR24，附录 A]（[CGGR25]的完整版本）。下一个引理描述了两个矩阵的割之间的一种关系：它们的对应主子式在阶数不超过4 时相等。

引理 2.7。 设 A 和 B 是两个具有非零非对角元的 $n \times n$ 阶矩阵，且$\mathrm{PME}(A, B, 4)$成立，$S = \{s_1, s_2\}$ 是 A 的一个割。那么，S 要么是 B 的一个割，要么对于每个 $i \in \{1, 2\}$，定义集合 X_i如下：

$$X_i = \{t \in \overline{S} \mid A[S+t] \overset{DS}{=} B[S+t]\} \cup \{s_i\},$$

是 B 的一个割，且 S 是$\mathrm{ct}(B, X_i)$中的一个割。

类似的结果见 [CGGR25，引理 3。5], 关键区别在于，他们的假设更强：他们要求 $A_{\text{PME}} = B$，而上述引理仅假设 $\mathrm{PME}(A, B, 4)$。尽管如此，证明的思路基本相同。仔细阅读他们的论证可以发现，实际只用到了阶数至多为 4 的主子式相等这一条件。详情请参阅 [CGGR25，引理 3 的证明。5]。

2.6 输入取逆元时的黑盒求值

在定理 3.1 和引理 4.3中，我们可以黑盒访问某些多项式，其中黑盒的部分输入取了逆元。例如，给定次数为 d 的多项式$f(y)$的黑盒访问，考虑利用f的黑盒构造的多项式$g(y,\ z)\ =z^{d}f(^{y}{}_{z})$ 的黑盒。z 的逆元是该g黑盒的一个输入。由于g 是一个可以在所有点上求值的多项式，因此我们需要能够在z 为零的点上对g 进行黑盒求值。

为进行推广，假设我们有一个次数为 d 的多项式 $\mathrm{f}(\mathrm{y}_1,\ldots,\mathrm{y}_m,\mathrm{z}_1,\ldots,\mathrm{z}_n)$，其中 $\mathrm{z}_1,\ldots,\mathrm{z}_n$ 的逆元是黑盒的输入。此外，假设我们要计算 f 在一个点处的值，该点上有 $\mathrm{k}\ \leq \mathrm{n}$ 个 z_i 变量被设为零。不失一般性，假设该点为 $(\mathrm{a}_1,\mathrm{a}_2,\ldots,\mathrm{a}_m,\mathrm{b}_1,\mathrm{b}_2,\ldots,\mathrm{b}_{n-k},0,0,\ldots,0)$。我们可以将变量 $\mathrm{z}_{n-k+1},\mathrm{z}_{n-k+2},\ldots,\mathrm{z}_n$ 设为一个新变量 t，从而得到

$$f(a_1,a_2,\ldots,a_m,b_1,b_2,\ldots,b_{n-k},t,t,\ldots,t)=\sum_{i=0}^{d}c_it^i.$$

令 $\mathrm{g(t)}\ =\mathrm{f}\ (\mathrm{a}_1,\ldots,\mathrm{a}_m,\mathrm{b}_1,\ldots,\mathrm{b}_{n-k},\mathrm{t},\ldots,\mathrm{t})$。注意，$\mathrm{f}\ (\mathrm{a}_1,\ldots,\mathrm{a}_m,\mathrm{b}_1,\ldots,\mathrm{b}_{n-k},0,\ldots,0)\ =\ \mathrm{g}(0)\ =\mathrm{c}_0$ 就是我们需要计算的值。如果 $|\mathbb{F}|\ >\mathrm{d}\ +1$，我们可以找出 $\mathrm{d}\ +1$ 个互不相同的非零值 $\beta_0,\ldots,\beta_d$，并使用插值计算 c_0:

$$\begin{pmatrix}g(\beta_0)\\ g(\beta_1)\\ \vdots\\ g(\beta_d)\end{pmatrix}=\begin{pmatrix}1&\beta_0&\beta_0^2&\cdots&\beta_0^d\\ 1&\beta_1&\beta_1^2&\cdots&\beta_1^d\\ \vdots&\vdots&\vdots&\ddots&\vdots\\ 1&\beta_d&\beta_d^2&\cdots&\beta_d^d\end{pmatrix}\begin{pmatrix}c_0\\ c_1\\ \vdots\\ c_d\end{pmatrix}.$$

右侧是一个范德蒙德矩阵。于是，我们可以将c_0表示为线性组合 $\sum_{i=0}^{d}\alpha_ig(\beta_i)$，其中 α_i可由 β_i 计算得到。这需要向f的黑盒进行$d\ +1$次查询。

观察 2.4。假设我们可以黑盒访问一个次数为 d 的多项式 $f(y_1,\ldots,y_n)$，其中黑盒的部分输入是取倒数后的变量。那么，如果 $|\mathbb{F}|\ >d\ +1$，我们可以使用 $d\ +1$ 次黑盒查询，在任意点计算该多项式。

注释。1. 对　　于多重线性多项式，$d\ \leq n$，我们至多需要$n\ +1$ 次查询。

2. 数值 α_0、...、 α_d 仅取决于 β_0、...、 β_d，因此可以预先计算。

3 学习 ROD 与黑盒 PMAP 之间的等价性

本小节中，我们证明学习只读一次行列式与黑盒主子式赋值问题之间存在随机多项式时间等价。首先，我们证明可以通过随机多项式时间归约，将学习形如 $\mathrm{f}\ (\mathrm{y}_1,\ldots,\mathrm{y}_n)\ =\det(\mathrm{A}_0+\sum_{i\in[n]}\mathrm{A}_i\mathrm{y}_i)$ 的多项式（其中 $\mathrm{A}_1,\ldots,\mathrm{A}_n$ 是秩一矩阵）转化为学习形如 $\mathrm{h}(\mathrm{y}_1,\ldots,\mathrm{y}_n)\ =\det(\mathrm{A}\ +\mathrm{Y})$ 的多项式，其中 $\mathrm{Y}\ =\mathrm{diag}(\mathrm{y}_1,\ldots,\mathrm{y}_n)$。注意，对于多项式 f，若 $\mathrm{A}_i=\mathrm{u}_i\mathrm{v}_i^T$，其中 u_i 和 v_i 是向量，则 $\mathrm{f}\ (\mathrm{y}_1,\ldots,\mathrm{y}_n)\ =\det(\mathrm{UYV}^T+\mathrm{A}_0)$，其中 u_i 和 v_i 分别是 U 和 V 的列。除了交替使用这两种表示形式外，我们还将使用以下引理将 f 表示为只读一次行列式:

引理 3.1 ([GT　20，引理 4。3]). 对于矩阵 U，$V\ \in\mathbb{F}^{r\times n}$、$A_0\in\mathbb{F}^{r\times r}$和 $Y\ =\mathrm{diag}(y_1,\ldots,y_n)$　，

$$\det(UYV^T+A_0)=\det\begin{pmatrix}I_n&Y&0_{n,r}\\ 0_{n,n}&I_n&V^T\\ U&0_{r,n}&A_0\end{pmatrix}.$$

我们证明，对于 $f(y_1,\ldots,y_n) = \det(A_0 + \sum_{i\in[n]} A_i y_i)$，可以假设矩阵 A_i 的阶数不超过 $n \times n$。

引理 3.2。对于一个非零多项式 $f(y_1,\ldots,y_n) = \det(UYV^T + A_0)$，其中 $U, V \in \mathbb{F}^{r\times n}$ 和 $A_0 \in \mathbb{F}^{r\times r}$，不失一般性，我们可以假设 $r \le n$ 且 U 满秩。

证明。设 $k \le n$ 是矩阵的秩U。根据引理 3.1，

$$f(y_1,\ldots,y_n) = \det \begin{pmatrix} I_n & Y & 0_{n,r} \\ 0_{n,n} & I_n & V^T \\ U & 0_{r,n} & A_0 \end{pmatrix}.$$

对U 进行行变换，并将所得标量吸收到最后一行中，

$$f(y_1,\ldots,y_n) = \det \begin{pmatrix} I_n & Y & 0_{n,r} \\ 0_{n,n} & I_n & V^T \\ \hat{U} & 0_{k,n} & C_1 \\ 0_{r-k,n} & 0_{r-k,n} & C_2 \end{pmatrix},$$

其中 $\hat{}U \in \mathbb{F}^{k\times n}$，复数域$_1 \in \mathbb{F}^{k\times r}$，复数域$_2 \in \mathbb{F}^{(r-k)\times r}$ 且 $\hat{}U$ 满秩。要使f 非零，复数域$_2$ 必须满秩。对复数域$_2$ 进行行变换和列变换，并将标量吸收到 $\hat{}A_0$, 的一列中，我们得到

$$\begin{aligned} f(y_1,\ldots,y_n) &= \det \begin{pmatrix} I_n & Y & 0_{n,k} & 0_{n,r-k} \\ 0_{n,n} & I_n & \hat{V}^T & \hat{V}_1^T \\ \hat{U} & 0_{k,n} & \hat{A}_0 & C_3 \\ 0_{r-k,n} & 0_{r-k,n} & 0_{r-k,k} & I_{r-k} \end{pmatrix} \\ &= \det \begin{pmatrix} I_n & Y & 0_{n,k} \\ 0_{n,n} & I_n & \hat{V}^T \\ \hat{U} & 0_{k,n} & \hat{A}_0 \end{pmatrix} \\ &= \det(\hat{U}Y\hat{V}^T + \hat{A}_0), \end{aligned}$$

其中 $\hat{}V \in \mathbb{F}^{k\times n}$ 且 $\hat{}A_0 \in \mathbb{F}^{k\times k}$。 □

以下引理有助于在秩 1 限制下将只读一次行列式还原为符号行列式。

引理 3.3. 若 $A \in \mathbb{F}^{(n-r)\times r}$,$B \in \mathbb{F}^{(n-r)\times(n-r)}$ 和 $C \in \mathbb{F}^{r\times(n-r)}$，则

$$\det \begin{pmatrix} A & B \\ I_r & C \end{pmatrix} = (-1)^{r(n-r)} \det \left(\begin{pmatrix} A & B \end{pmatrix} \begin{pmatrix} -C \\ I_{n-r} \end{pmatrix} \right).$$

证明。将 $\begin{pmatrix} I_r & C \end{pmatrix}$ 移至顶部（每个r 行交换$n - r$ 次，共计r（$n - r$）次交换），并使用分块高斯消元，

$$\begin{aligned} \det \begin{pmatrix} A & B \\ I_r & C \end{pmatrix} &= (-1)^{r(n-r)} \det \begin{pmatrix} I_r & C \\ A & B \end{pmatrix} \\ &= (-1)^{r(n-r)} \det \begin{pmatrix} I_r & 0_{r,n-r} \\ A & B - AC \end{pmatrix} \\ &= (-1)^{r(n-r)} \det(B - AC) \\ &= (-1)^{r(n-r)} \det \left(\begin{pmatrix} A & B \end{pmatrix} \begin{pmatrix} -C \\ I_{n-r} \end{pmatrix} \right). \end{aligned}$$

□

3.1 学习 ROD 到黑盒 PMAP

我们首先参照 [GT20，定理 4，3] 对多项式进行齐次化 f。然后我们使用隔离引理 [MVV87] 将学习 f 归约为黑盒主子式赋值问题。

定理 3.1。设 $|\mathbb{F}| > n+1$。给定对 $f(y_1,\ldots,y_n) = det(A_0 + \sum_{i\in[n]} A_i y_i)$ 的黑盒访问，其中 $A_0,\ldots,A_n \in \mathbb{F}^{r\times r}$ 和 $A_1,\ldots,A_n$ 均为秩 1，我们可以在随机多项式时间内构造对多项式 $h(z_1,\ldots,z_n) = det(A+Z)$ 的黑盒访问，其中 $A \in \mathbb{F}^{n\times n}$ 且 $Z = diag(z_1,\ldots,z_n)$。此外，给定满足 $det(A+Z) = det(A'+Z)$ 的矩阵 $A' \in \mathbb{F}^{n\times n}$，我们可以恢复矩阵 $B_0,\ldots,B_n \in \mathbb{F}^{n\times n}$，使得 $f(y_1,\ldots,y_n) = det(B_0 + \sum_{i\in[n]} B_i y_i)$，且 $B_1,\ldots,B_n$ 均为秩 1。

证明。令 U 和 $V \in \mathbb{F}^{r\times n}$ 为满足 $f(y_1,\ldots,y_n) = \det(UYV^T + A_0)$ 的矩阵，其中 $Y = \mathrm{diag}(y_1,\ldots,y_n)$。我们首先将多线性多项式 f 齐次化为

$$f'(y_1,y_2,\ldots,y_n,t_1,t_2,\ldots,t_n) = t_1t_2\ldots t_n f(\frac{y_1}{t_1},\frac{y_2}{t_2},\ldots,\frac{y_n}{t_n}).$$

其中 $t_1,\ldots,t_n$ 是一个全新的变量集合。根据观察 2.4，我们可以黑盒访问 f'。根据引理 3.1，有

$$\begin{aligned} f'(y_1,\ldots,y_n,t_1,\ldots,t_n) &= \det(T)\det\begin{pmatrix} I_n & T^{-1}Y & 0_{n,r} \\ 0_{n,n} & I_n & V^T \\ U & 0_{r,n} & A_0 \end{pmatrix} \\ &= \det\begin{pmatrix} T & Y & 0_{n,r} \\ 0_{n,n} & I_n & V^T \\ U & 0_{r,n} & A_0 \end{pmatrix}, \end{aligned}$$

其中 $T = \mathrm{diag}(t_1,t_2,\ldots,t_n)$。注意，矩阵 $(U\,A_0)$ 必须满秩，f' 才能非零，进而 f 也非零。现在，我们对最后 $n+r$ 行进行初等行变换，并置换各列，得到

$$f'(y_1,\ldots,y_n,t_1,\ldots,t_n) = \alpha\det\begin{pmatrix} \leftarrow & L'W' & \rightarrow \\ & I_{n+r} & H \end{pmatrix},$$

其中，令 P 为与所执行的列置换相对应的 $(2n+r)\times(2n+r)$ 置换矩阵，

- L' 是 $n\times(2n+r)$ 矩阵 $(I_n\,I_n\,0_{n,r})\,P$。
- W' 是 $(2n+r)\times(2n+r)$ 对角矩阵 $P^T \begin{pmatrix} T & & \\ & Y & \\ & & 0_{r,r} \end{pmatrix} P$。
- H 是由这些变换得到的 $(n+r)\times n$ 矩阵。
- α 是由这些变换得到的标量。

令 $R' = \begin{pmatrix} -H^T \\ I_n \end{pmatrix}$。注意到 R' 的大小为 $n\times(2n+r)$。根据引理 3.3，

$$f'(y_1,\ldots,y_n,t_1,\ldots,t_n) = (-1)^{n(n+r)}\alpha\det(L'W'R'^T).$$

我们可以删去 L' 和 R' 中对应于W'对角线上的零元素的列，从而得到

$$f'(y_1,\dots,y_n,t_1,\dots,t_n)=\det(LWR^T)$$

其中 L 和 R 是得到的 $n\times 2n$ 矩阵，而 W 是由 y_i 和 t_i 变量构成的 $2n\times 2n$ 对角矩阵。常数 $(-1)^{n(n+r)}\alpha$ 被吸收到矩阵 R中。

观察 3.1。 L 是矩阵 $\begin{pmatrix} I_n & I_n\end{pmatrix}$ 的一个列置换。对于所有 i，L 中与 y_i 和 t_i 对应的列相同。

注意，f 是一个次数为 n 的齐次多重线性多项式。我们可以使用隔离引理 [MVV87，第 3] 节来隔离一个单项式 [NSV94，第 4 节.1]。设该单项式由变量 $z_1,z_2,\dots z_n$ 构成，其中 $z_i = y_i$ 或 t_i。类似地，若 $z_i = y_i$，则令 $\bar{z}_i = t_i$，反之亦然。根据观察 3.1，L 中与 z_is 对应的列必须构成一个单位矩阵。因此，我们可以将 f′ 写为

$$f'(y_1,\dots,y_n,t_1,\dots,t_n)=\det\left(\begin{pmatrix} I_n & I_n\end{pmatrix}\begin{pmatrix} Z & 0_{n,n}\\ 0_{n,n} & \bar{Z}\end{pmatrix}\begin{pmatrix} R_1\\ R_2\end{pmatrix}\right),$$

其中 $Z = \mathrm{diag}(z_1,\dots,z_n)$，$\bar{Z} = \mathrm{diag}(\bar{z}_1,\dots,\bar{z}_n)$，$R_1$ 是 R^T 中对应于 Z 的行，而 R_2 是 R^T中的其余行。由于 $z_1\dots z_n$ 的系数为 $\det(R_1)$ 且非零，我们可以将 f′ 右乘 $\det({R_1}^{-1})$，令 $A = {R_2}{R_1}^{-1}$，得到

$$\begin{aligned} g(y_1,\dots,y_n,t_1,\dots,t_n) &= f'(y_1,\dots,y_n,t_1,\dots,t_n)\det({R_1}^{-1})\\ &= \det\left(\begin{pmatrix} I_n & I_n\end{pmatrix}\begin{pmatrix} Z & 0_{n,n}\\ 0_{n,n} & \bar{Z}\end{pmatrix}\begin{pmatrix} I_n\\ A\end{pmatrix}\right)\\ &= \det\left(\begin{pmatrix} Z & \bar{Z}\end{pmatrix}\begin{pmatrix} I_n\\ A\end{pmatrix}\right)\\ &= \det\left(Z+\bar{Z}A\right).\end{aligned}$$

令 $h(z_1,\dots,z_n,\bar{z}_1,\dots,\bar{z}_n)=\bar{z}_1\bar{z}_2\dots\bar{z}_n g(z_1,z_2,\dots,z_n,\frac{1}{\bar{z}_1},\frac{1}{\bar{z}_2},\dots,\frac{1}{\bar{z}_n})$。我们看到

$$\begin{aligned} h(z_1,z_2,\dots,z_n,\bar{z}_1,\dots,\bar{z}_n) &= \det(\bar{Z})\det(Z+\bar{Z}^{-1}A)\\ &= \det(\bar{Z}Z+A).\end{aligned}$$

观察 3.2。 在 h 的单项式中，z_i 出现当且仅当 $\bar{z}_i$ 出现。这显然是因为 y 变量来自对 f 的齐次化；t_i 出现在 g 的单项式中，当且仅当 y_i 不出现。

设有一个矩阵 $A'\in \mathbb{F}^{n\times n}$，使得 $\det(Z+A') = h(z_1,\dots,z_n,1,1,\dots,1) = g(z_1,\dots,z_n,1,1,\dots,1) = \det(Z+A)$。根据观察 3.2，$h(z_1,\dots,z_n,\bar{z}_1,\dots,\bar{z}_n) = \det(\bar{Z}Z+A')$。这意味着

$$\begin{aligned} g(y_1,\dots,y_n,t_1,\dots,t_n) &= \det\left(Z+\bar{Z}A'\right)\\ &= \det\left(\begin{pmatrix} Z & \bar{Z}\end{pmatrix}\begin{pmatrix} I_n\\ A'\end{pmatrix}\right)\\ &= \det\left(\begin{pmatrix} I_n & I_n\end{pmatrix}\begin{pmatrix} Z & 0_{n,n}\\ 0_{n,n} & \bar{Z}\end{pmatrix}\begin{pmatrix} I_n\\ A'\end{pmatrix}\right).\end{aligned}$$

令 l_{y_i} 为$I_n\ I_n)$ 中与y_i对应的列，并令$r_{y_i}^T$ 为$I_n\ A')$ 中与y_i对应的行。同样，令l_{t_i} 和r_{t_i} 表示t_i对应的列和行。我们看到

$$g(y_1,\ldots,y_n,t_1,\ldots,t_n) = \det\left(\left(\sum_{i\in[n]} l_{y_i} r_{y_i}^T y_i\right) + \left(\sum_{i\in[n]} l_{t_i} r_{t_i}^T t_i\right)\right).$$

将所有t_i变量设为 1，并令$C = \sum_{i\in[n]} l_{t_i} r_{t_i}^T$，我们得到

$$f(y_1,\ldots,y_n) = \det(R_1)\det\left(\left(\sum_{i\in[n]} l_{y_i} r_{y_i}^T y_i\right) + C\right).$$

令$B_i = l_{y_i} r_{y_i}^T$的第一行乘以 $\det(R_1)$，并令$B_0 = C$的第一行乘以 $\det(R_1)$，则有$f(y_1,\ldots,y_n) = \det(B_0 + \sum_{i\in[n]} B_i y_i)$。

□

总　　结而言，给定对$f(y_1,\ldots,y_n)$的黑盒访问，归约算法如下　　：

算法 2将学习 ROD 归约为黑盒 PMAP

输入： 黑盒访问$f = \det(A_0 + \sum_{i\in[n]} A_i y_i)$，其中$A_i \in \mathbb{F}^{r\times r}$和$A_1,\ldots,A_n$均为秩一矩阵。

输出： 矩阵 $B_0,\ldots,B_n \in \mathbb{F}^{n\times n}$，其中 $B_1,\ldots,B_n$ 均为秩一矩阵，使得$f = \det(B_0 + \sum_{i\in[n]} B_i y_i)$。

假设：　　对 $\det(A + Z)$ 的学习算法进行预言机访问，其中 $Z = \mathrm{diag}(z_1,\ldots,z_n)$。*1*：将$f$齐次化，得到$f'(y_1,\ldots,y_n,t_1,\ldots,t_n) = t_1 t_2 \ldots t_n f(\frac{y_1}{t_1},\frac{y_2}{t_2},\ldots,\frac{y_n}{t_n})$。*2*：使用隔离引理隔离出$f'$的一个单项式。令该单项式为 $z_1\ldots z_n$，其系数为 γ。*3*：$h(z_1,\ldots,z_n) = \frac{1}{\gamma} f'(z_1,\ldots,z_n,1,\ldots,1)$ 将作为黑盒主子式赋值问题的输入。*4*：假设 A' 是黑盒主子式赋值问题的输出。那么 $f' = \gamma \det\left((I_n\ I_n)\begin{pmatrix} Z & 0_{n,n} \\ 0_{n,n} & Z \end{pmatrix}\begin{pmatrix} I_n \\ A' \end{pmatrix}\right)$。*5*：将 t_i 变量设为 *1* 并化简，以恢复f

$= det(B_0 + \sum_{i\in}$

$_{[n]} B_i y_i)$。输出 B_0,。 ....., B_n。

3.2 从黑盒 PMAP 到学习 ROD

定理 *3.2*。给定对 $h(y_1,\ldots,y_n) = det(A + Y)$ 的黑盒访问，其中 $Y = diag(y_1,\ldots,y_n)$，且 $A \in \mathbb{F}^{n\times n}$；假设我们有矩阵 $B_0,\ldots,B_n \in \mathbb{F}^{r\times r}$，$B_1,\ldots,B_n$，它们的秩均为 *1*，且 $det(A + Y) = det(B_0 + \sum_{i\in[n]} B_i y_i)$。那么我们可以在确定性多项式时间内恢复一个矩阵 $A' \in \mathbb{F}^{n\times n}$，使得 $h(y_1,\ldots,y_n) = det(A' + Y)$。

证明。 设 $U,V \in \mathbb{F}^{r\times n}$ 是满足以下条件的矩阵：$h(y_1,\ldots,y_n) = \det(A + Y) = \det(UYV^T + B_0)$。根据引理3.2，我们可以假设 $r \le n$。根据引理 3.1，

$$h(y_1,\ldots,y_n) = \det\begin{pmatrix} I_n & Y & 0_{n,r} \\ 0_{n,n} & I_n & V^T \\ U & 0_{r,n} & B_0 \end{pmatrix}.$$

注意，$y_1 \ldots y_n$ 的系数为 $(-1)^n \det \begin{pmatrix} 0_n, & {}_n V_0^T \end{pmatrix} = 1$ U B 。若 r $<$ n，则该式为零，因此 r $=$ n。于是，$(-1)^n \det \begin{pmatrix} 0_n, & {}_n V_0^T \end{pmatrix} =$ U B det(U) det(V^T) $= 1$。这意味着 U 和 V^T 均可逆，且 det(U^{-1}) det($(V^T)^{-1}$) $= 1$。因此，

$$h(y_1, \ldots, y_n) = \det(U^{-1}) \det(UYV^T + B_0) \det((V^T)^{-1}) = \det(Y + U^{-1}B_0(V^T)^{-1}).$$

□

4 具有性质 $\mathcal{R}$ 的矩阵的黑盒 PMAP 到 PMAP

在本小节中，我们展示如何将满足性质 $\mathcal{R}$ 的矩阵的黑盒 PMAP 归约为 PMAP。我们首先证明，对于任意矩阵 A，矩阵 $(A + D)^{-1}$ 的不可约块（其中 D 是由随机选取的域元素构成的对角矩阵）以高概率满足性质 $\mathcal{R}$，并说明如何利用 det(A $+$Y) 的黑盒访问来获得 det($(A + D)^{-1}$ $+$Y) 的黑盒访问。随后，我们找出与 $(A + D)^{-1}$ 的不可约块相对应的指标。由于 $(A + D)^{-1}$ 的不可约块满足性质 $\mathcal{R}$，对它们的学习可归约为满足性质 $\mathcal{R}$ 的矩阵的 PMAP。最后，对于与 $(A + D)^{-1}$ 的不可约块主子式等价的矩阵 $C_1, \ldots$、C_k，我们找出一个满足 C PME $=$ A 的矩阵 C。

算法 3将具有性质 $\mathcal{R}$ 的矩阵的黑盒 PMAP 化归为 PMAP

输入：对 det(A $+$Y) 的黑盒访问，其中 Y $=$ diag($y_1, \ldots, y_n$)。输出：一个矩阵 B $\in \mathbb{F}^{n\times n}$，使得 B PME $=$ A。假设：可以访问预言机 PMAP-Prop-R(PM_M)，该预言机能够在可访问满足性质 $\mathcal{R}$ 的矩阵 M 的主子式预言机 PM_M （见定义 7.1 ）的情况下求解 PMAP。1：利用引理 4.3，获得对 det($(A + D)^{-1}$ $+$Y) 的黑盒访问。2：利用算法 4，找出对应于 $(A + D)^{-1}$ 的不可约块的指标 $T_1, \ldots, T_s$。3：对 i $\in$ [s] 执行 4：令 $C_i \leftarrow$ PMAP-Prop-R($PM_{(A+D)^{-1}[T_i]}$)。5：结束循环。6：找出置换矩阵 P，使得 P^T diag(Y[T_1], . . . , Y[T_s])P $=$ Y。7：令 C $\leftarrow P^T$ diag($C_1, \ldots, C_s$)P。8：返回 $C^{-1} -$ D。

4.1 $(A + D)^{-1}$ 的不可约块满足性质 $\mathcal{R}$

要找到一个对角矩阵 D，使 $(A + D)^{-1}$ 的每个不可约块都满足性质$\mathcal{R}$，只需找到一个 D，使 det(A $+$ D) $\neq 0$，且 $(A + D)^{adj}$ 的每个不可约块都满足性质 $\mathcal{R}$。首先，我们将证明，对于任意不可约矩阵 A，矩阵 $(A + Y)^{adj} \in \mathbb{F}(y_1, y_2, \ldots, y_n)^{n\times n}$ 满足性质 $\mathcal{R}$，其中 Y $=$ = diag($y_1, \ldots, y_n$)。Hartfiel 和 Loewy [HL84, 定理 2] 的以下结果将会用到。

定理 4.1 ([HL84], 定理 2)。设 $n \geq 2$，M 是域 F 上的 $n \times n$ 矩阵。令 Z $=$对角矩阵$(0,0, z_3, z_4, \ldots, z_n)$，其中 $z_3, z_4, \ldots, z_n$ 是相互独立的不定元。设 $\det(M + Z) = 0$。那么，存在 $\{3, 4, \ldots, n\}$ 的一个划分 (X_1, X_2)，使得

$$\operatorname{rank}(M[\{1,2\} \cup X_1, \{1,2\} \cup X_2]) \leq 1.$$

除了上述定理外，我们还需要以下结果。以下引理的证明直接可由 [CGGR24，断言 A。1]。

引理 4.1. 设 $n \geq 4$ 为正整数。设 $M \in \mathbb{F}^{n\times n}$ 和 $X \subseteq [n]$ 满足 秩$(M[X,\overline{X}]) = 1$。那么，秩$M^{\mathrm{adj}}[X,\overline{X}] = 1$。

下面的断言表明，$(A+Y)^{\mathrm{adj}}$ 满足性质 $\mathcal{R}$。

断言 4.1. 定义 $Y = \mathrm{diag}(y_1,\ldots,y_n)$。对于任意不可约矩阵 $A \in \mathbb{F}^{n\times n}$，矩阵 $(A+Y)^{\mathrm{adj}}$满足性质 $\mathcal{R}$。

证明。 性质 $\mathcal{R}$ 的第一个条件由 [HL84，定理 1]得出。对于第二个条件，我们需要证明，对于任意四个互不相同的元素 i、j、k、$\ell \in [n]$，

$$\mathrm{rank}(A+Y)^{\mathrm{adj}}[\{i,j\},\{k,\ell\}] = 1 \Longrightarrow \mathrm{rank}(A+Y)^{\mathrm{adj}}[X,\overline{X}] = 1$$

对于某个 $X \subset [n]$，其中 $\{i、j\} \subseteq X$ 且 $\{k、\ell\} \subseteq \overline{X}$。不失一般性，我们可以假设$i = 1$、$j = 2$、$k = 3$、$\ell = 4$。注意

$$\mathrm{rank}((A+Y)^{\mathrm{adj}}[\{1,2\},\{3,4\}]) = 1 \Longrightarrow \det((A+Y)^{\mathrm{adj}}[\{1,2\},\{3,4\}]) = 0.$$

现在，应用雅可比恒等式 [Gan60，第 21], 页，我们得到 $\det((A+Y)[\{3,4\},\overline{\{1,2\}}]) = 0$。注意，对于矩阵 $A = (a_{i,j})_{i,j\in[n]}$,

$$(A+Y)[\overline{\{3,4\}},\overline{\{1,2\}}] = \begin{pmatrix} a_{1,3} & a_{1,4} & a_{1,5} & \cdots & a_{1,n} \\ a_{2,3} & a_{2,4} & a_{2,5} & \cdots & a_{2,n} \\ a_{5,3} & a_{5,4} & a_{5,5}+y_5 & \cdots & a_{5,n} \\ \vdots & & & \ddots & \\ a_{n,3} & a_{n,4} & a_{n,5} & \cdots & a_{n,n}+y_n \end{pmatrix}.$$

由上可得

$$(A+Y)[\overline{\{3,4\}},\overline{\{1,2\}}] = A'+Y' \text{ where } A' = A[\overline{\{3,4\}},\overline{\{1,2\}}] \text{ and } Y' = \mathrm{diag}(0,0,y_5,\ldots,y_n).$$

由于 $\det(A'+Y') = 0$，根据定理 4.1，存在一个划分 X_1, X_2，其属于 $\{5,6,\ldots,n\}$，使得

$$\mathrm{rank}\, A[X_1 \cup \{1,2\}, X_2 \cup \{3,4\}] = 1.$$

令 $X = X_1 \cup \{1,2\}$。则 $\overline{X} = \overline{X_2} \cup \{3,4\}$。因此，我们得到秩 $\mathrm{rank}(A+Y)[X,\overline{X}] = 1$。根据引理 4.1，秩 $\mathrm{rank}(A+Y)^{\mathrm{adj}}[X,\overline{X}] = 1$。引理得证。 □

接下来，我们证明对角矩阵 D 满足 $(A+D)^{\mathrm{adj}}$ 具有性质 $\mathcal{R}$ 所需的性质。

断言 4.2. 令 $D \in \mathbb{F}^{n\times n}$ 为一个对角矩阵，使得 $(A+D)^{\mathrm{adj}}$ 满足以下性质：

1. $A+D$ 可逆，即 $\det(A+D) \neq 0$。
2. $(A+D)^{\mathrm{adj}}$ 具有非零非对角元，即对每个 $1 \leq i, j \leq n$，$\det((A+D)[i,j]) \neq 0$。
3. 对于任意四个互不相同的元素 i、j、k、$\ell \in [n]$,

$$\det\left((A+D)^{\mathrm{adj}}[\{i,j\},\{k,\ell\}]\right) = 0 \Longrightarrow \det\left((A+Y)^{\mathrm{adj}}[\{i,j\},\{k,\ell\}]\right) = 0. \tag{7}$$

那么，$(A+D)^{\mathrm{adj}}$ 满足性质 $\mathcal{R}$。

证明。Let i、j、k、$\ell \in [n]$ 为四个互不相同的元素。于是，第三条性质蕴含

$$\det\Big((A+D)^{\mathrm{adj}}[\{i,j\},\{k,\ell\}]\Big)=0 \Longrightarrow \det\Big((A+Y)^{\mathrm{adj}}[\{i,j\},\{k,\ell\}]\Big)=0.$$

由断言 4.1，我们知道 $(A+Y)^{\mathrm{adj}}$ 满足性质 $\mathcal{R}$。因此，

$$\mathrm{rank}(A+D)^{\mathrm{adj}}[\{i,j\},\{k,\ell\}]=1 \Longrightarrow \mathrm{rank}(A+Y)^{\mathrm{adj}}[X,\overline{X}]=1 \Longrightarrow \mathrm{rank}(A+D)^{\mathrm{adj}}[X,\overline{X}]=1$$

对某个 $X \subset [n]$，使得 i、$j \in X$ 且 k、$\ell \in X$。因此，$(A+D)^{\mathrm{adj}}$ 将满足性质 $\mathcal{R}$。 □

下述结果表明，$(A+D)^{\mathrm{adj}}$ 满足性质 $\mathcal{R}$，其中 D 是一个“随机”对角矩阵。

引理 4.2. 设 $|\mathbb{F}| \geq n^6$。考虑一个矩阵 $D \in \mathbb{F}^{n\times n}$，使得 $D=\mathrm{diag}(d_1,d_2,\ldots,d_n)$，且每个 d_i 均从 $\mathbb{F}$ 中独立且均匀随机选取。则对任意不可约矩阵 $A \in \mathbb{F}^{n\times n}$，$(A+D)^{\mathrm{adj}}$ 以高概率满足性质 $\mathcal{R}$。

证明。只需证明随机选取的对角矩阵 D 满足断言 4.2 中所述的性质。考虑以下一小组多项式，其中 $Y=\mathrm{diag}(y_1,\ldots,y_n)$：

1. $\det(A+Y)$.

2. 对每个 $1 \leq i$、$j \leq n$，$\det((A+Y)[\bar{i},\bar{j}])$。3. 对每个互不相同的 i、j、k、$\ell \in [n]$, $\det\left((A+Y)^{\mathrm{adj}}[\{i,j\},\{k,\ell\}]\right)$。

由多项式恒等式引理 [Sch80、Zip79、DL78] 可知，将每个y_i替换为随机选取的 $d_i \in \mathbb{F}$后，该集合中的每个非零多项式以高概率仍为非零多项式。因此，对于对角矩阵 $D=\mathrm{diag}(d_1,d_2,\ldots,d_n)$，断言 4.2 中提到的所有性质均成立。因此，$(A+D)^{\mathrm{adj}}$ 满足性质 $\mathcal{R}$。 □

备注 *4.1.* 即使对于每一组互异的 i、j、k、ℓ，我们将集合中的 $\det\left((A+Y)^{\mathrm{adj}}[\{i,j\},\{k,\ell\}]\right)$ 替换为多项式 $\det((A+Y)[\{k,\ell\},\{i,j\}])$，引理 *4.2* 的证明仍然成立。这可由雅可比恒等式 *[Gan60，第 21]*,页得出，该恒等式表明 $\det\left((A+Y)^{\mathrm{adj}}[\{i,j\},\{k,\ell\}]\right) \neq 0$当且仅当 $\det((A+Y)[\{k,\ell\},\{i,j\}]) \neq 0$。此外，该集合中的每个多项式现在都可由只读一次行列式（只读一次行列式）计算。因此，我们可以利用 *ROD* 的准多项式规模命中集 *[GT20]*，计算出一个准多项式规模的、由 $n \times n$ 对角矩阵构成的集合，使得其中存在一个对角矩阵 D，使 $(A+D)^{\mathrm{adj}}$ 满足性质 $\mathcal{R}$。

推论 4.1。考虑一个矩阵 $D \in \mathbb{F}^{n\times n}$，使得 $D=\mathrm{diag}(d_1,d_2,\ldots,d_n)$，且每个 d_i 都从 $\mathbb{F}$ 中独立且均匀随机地选取。那么，对于任意矩阵 $A \in \mathbb{F}^{n\times n}$，$(A+D)^{\mathrm{adj}}$ 的每个不可约块（因此，$(A+D)^{-1}$）以高概率满足性质 $\mathcal{R}$。

4.2 从 $\det((A+D)^{-1}+Y)$ 的黑盒访问到 $\det(A+Y)$

我们可以黑盒访问某个矩阵 A 和 $Y=\mathrm{diag}(y_1,\ldots,y_n)$对应的 $\det(A+Y)$。下面说明如何由此获得 $\det((A+D)^{-1}+Y)$ 的黑盒访问：

引理 4.3. 若 $|\mathbb{F}|>n+1$，则由对 $\det(A+Y)$ 的黑盒访问（其中 $Y=\mathrm{diag}(y_1,\ldots,y_n)$），我们可以获得对 $\det((A+D)^{-1}+Y)$ 的黑盒访问，其中 D 是一个对角矩阵，使得 $(A+D)$ 可逆。

证明. 通过对 $y_1,\ldots,y_n$ 作平移，我们得到对 $\det((A+D)+Y)$ 的黑盒访问。由于我们知道 $\det(A+D)$ 的值且它非零，我们看到

$$\det(A+D)^{-1}\det((A+D)+Y)=\det(I_n+(A+D)^{-1}Y).$$

根据观察 2.4，我们可以对变量取倒数，并乘以 $y_1\cdots y_n$，从而获得对以下对象的黑盒访问：

$$\det((A+D)^{-1}Y^{-1}+I_n)\det(Y)=\det((A+D)^{-1}+Y).$$

□

令 D 为一个由随机选取的域元素构成的对角矩阵。由于 $\det(A+Y)$ 可逆，因此 $\det(A+D)$ 以高概率可逆。因此，我们可以黑盒访问 $\det((A+D)^{-1}+Y)$，并且根据推论 4.1，$(A+D)^{-1}$ 的不可约块以高概率满足性质 $\mathcal{R}$。

4.3 Le学习 detdet$((A+D)^{-1}+Y)$ 的不可约块的指标集

假设我们有一个指标集 $T\subseteq[n]$，并希望从对 $\det(A[T]+Y[T])$ 的黑盒访问中，获得对 $\det(A[T])$ 这一主子式的黑盒访问，以及对 $\det(A+Y)$ 的黑盒访问，其中$Y=\mathrm{diag}(y_1,\ldots,y_n)$。我们可以通过多项式插值做到这一点：

命题 4.3. 设 $|\mathbb{F}|>n$。假设我们拥有对 $\det(A+Y)$ 的黑盒访问，其中 $Y=\mathrm{diag}(y_1,\ldots,y_n)$，且 $A\in\mathbb{F}^{n\times n}$。那么，对于任意集合 $T\subseteq[n]$，，我们可以模拟对 $\det(A[T]+Y[T])$ 的一次查询（从而得到主子式 $\det(A[T])$），这需要使用对黑盒 $\det(A+Y)$ 的 $n-|T|+1$ 次查询。

证明。不失一般性，我们可以假设 $T=[k]$。令 $f(y_1,\ldots,y_n)=\det(A+Y)$，并假设我们想在点 $\alpha_1,\ldots,\alpha_k$ 处计算 $\det(A[T]+Y[T])$。令 $g(z)=f(\alpha_1,\ldots,\alpha_k,z,z,\ldots,z)$，其中 z 是一个新引入的变量。由于 f 是多重线性的，我们可以写出

$$g(z)=\sum_{i=0}^{n-k}\gamma_i z^i.$$

根据多项式 $\det(A+Y)$的性质，很容易看出，γ_{n-k}就是我们需要的值。我们找到$n-k+1$个不同的值 β_0、……、β_{n-k}，并使用插值计算 γ_{n-k}。

如果 $\alpha_1=\alpha_2=\cdots=\alpha_k=0$，我们看到 $\gamma_{n-k}=\det(A[T])$。 □

根据前一小节，我们可以黑盒访问 $\det((A+D)^{-1}+Y)$，其中 $Y=\mathrm{diag}(y_1,\ldots,y_n)$。令 $B=(A+D)^{-1}$。假设 $T_1\sqcup T_2\sqcup\cdots\sqcup T_s=[n]$ 是这些指标集，使得 B 的不可约块为 $B[T_1],B[T_2]\ldots,B[T_s]$。根据引理 2.1，存在一个置换矩阵 P，使得 $BPME=P^T\mathrm{diag}(B[T_1],\ldots,B[T_s])P$。

为了分别了解B 的不可约块，我们首先需要找到指标集$T_1\sqcup T_2\sqcup\cdots\sqcup T_s$。我们可以借助以下命题来做到这一点：

命题 4.4。 设 B 是一个 $n\times n$ 矩阵，其不可约块都含有非零非对角元。那么 $i,j\in[n]$ 属于 B 的同一个不可约块，当且仅当 $B[\{i,j\}]$ 是不可约的。

证明。 若i 和j 属于同一个不可约块，那么根据B的不可约块都含有非零非对角元这一事实，$B[i,j]$ 和$B[j,i]$ 必定非零。因此$B[\{i,j\}]$ 是不可约的。

如果 i 和 j 分别属于两个不同的不可约块 $B[T_q]$ 和 $B[T_r]$，那么根据引理 2.1，存在一个置换矩阵 P，使得 P^TBP 是一个分块三角矩阵，其块包括 $B[T_q]$ 和 $B[T_r]$。因此，$B[T_q,T_r]$ 和 $B[T_r,T_q]$ 中至少有一个是零矩阵，这意味着 B[i, j] 和 B[j, i] 中至少有一个为零。因此，$B[\{i,j\}]$ 是可约的。 □

推论 4.2. 对于 $i,j,k \in [n],$，如果 $B[\{i,j\}]$ 和 $B[\{j,k\}]$ 均不可约，那么 $B[\{i,k\}]$ 也不可约。

根据推论 4.1，$B = (A+D)^{-1}$ 的不可约块 $\mathcal{R}$满足性质，因此具有非零非对角元。根据命题 $\det(B[\{i,\ j\}]+Y[\{i,\ j\}])$ 给出的黑盒访问4.3，我们可以轻松检查 $B[\{i,\ j\}]$ 是否不可约。

命题 4.5。 令 $\det(B[\{i,\ j\}]+Y[\{i,\ j\}]) = y_iy_j+\alpha y_i+\beta y_j+\gamma$，则 $B[\{i,\ j\}]$ 可约，当且仅当 $\gamma=\alpha\beta$。

证明。

$$\begin{aligned}\det(B[\{i,j\}]+Y[\{i,j\}]) &= (y_i+B[i,i])(y_j+B[j,j])-B[i,j]B[j,i]\\ &= y_iy_j+y_iB[j,j]+B[i,i]y_j+B[i,i]B[j,j]-B[i,j]B[j,i].\end{aligned}$$

B[i, i]B[j, j] − B[i, j]B[j, i] = B[i, i]B[j, j] 当且仅当 B[i, j]B[j, i] = 0，也就是说 B[{i, j}] 可约。 □

现在我们有以下算法来找出不可约块的指标集：

算法 4 寻找 $\det((A+D)^{-1}+Y)$的不可约块的指标

输入： 可通过黑箱访问 $\det(B+Y)$，其中 $Y=\mathrm{diag}(y_1,\ldots,y_n)$，且$B$的不可约块具有非零非对角元。

输出： 一个指标集的集合 $\mathcal{T}=\{T_1,\ldots,T_s\}$，使得$B[T_1],\ldots,B[T_s]$ 是B的不可约块。

1：令 E ← ∅. 2：令 $\mathcal{T}$ ← ∅. 3：对于 i ∈ [n] 执行 4：如果 i ∉ E，则 5：E ← E ∪ {i}. 6：T ← { i}. 7：对于 j ∈ [n]执行 8：如果 j ∉ E 且 B[{i, j}] 不可约，则 9：E ← E ∪ {j}. 10：T ← T ∪ {j}. 11：结束 if 12：结束 for 13：$\mathcal{T}$ ← $\mathcal{T}$ ∪ {T}. 14：结束 if 15：结束 for 16：对于 T ∈ $\mathcal{T}$执行 17：对于 i, j ∈ T,i ≠ j 执行 18：如果 B[{i, j}] 可约，则 19：返回错误。20：结束 if 21：结束 for 22：结束 for 23：返回 $\mathcal{T}$。

在算法 4 的第 8 步和第 18 步中，我们使用断言 2×2 检查矩阵的不可约性 4.5。注意，当 B 的不可约块具有非零的非对角元素时，推论 4.2保证算法在第 19 步绝不会报错。

一旦我们得到指标集 $T_1, \ldots, T_s$，利用命题 4.3，我们就可以黑盒访问 $\det(B[T_1]+Y[T_1])$、$\det(B[T_2]+Y[T_2])$、$\ldots$、$\det(B[T_s]+Y[T_s])$，以及它们的主子式。我们可以分别学习矩阵 $B[T_1], B[T_2], \ldots, B[T_s]$。由于 $B[T_1], B[T_2], \ldots, B[T_s]$ 满足性质 $\mathcal{R}$，且我们可以访问它们的主子式（这恰好就是矩阵 B 的主子式），学习这些矩阵可归约为对满足性质 $\mathcal{R}$ 的矩阵求解 PMAP。

备注 *4.2*。在对角矩阵 D 是"坏的"的情形下，即 $(A+D)^{-1}$ 的不可约块并非都具有非零非对角元时，注意，如果 i、j 不属于同一个不可约块的指标，那么算法 *4* 仍能正确地将 i 和 j 识别为属于不同块的指标（因为矩阵 $B[\{i,j\}]$ 仍然是可约的）。算法可能失败的情形是 i、j 属于同一个不可约块时：由于不再保证对角元非零，$B[\{i,j\}]$ 可能是可约的。因此，对于"坏的"对角矩阵 D，算法 *4* 要么发现推论 *4.2* 的一个违反之处并抛出错误，要么报告的不可约块数量多于实际正确的数量。

如果给定拟多项式数量的对角矩阵 $D_1, \ldots, D_k$，并且保证其中至少有一个是"好的"（如备注 *4.1*中的情形），那么对所有矩阵$(A+D_1)^{-1}, (A+D_2)^{-1}, \ldots, (A+D_k)^{-1}$运行该算法，我们可以看到，对于"好的"对角矩阵 D_i，算法将输出最少的指标集数量，因此我们仍然可以在确定性拟多项式时间内找到与$(A+D_i)^{-1}$ 的不可约块相对应的指标集（其与 A 的不可约块相同）。

4.4 恢复一个与 A 主子式等价的矩阵

设 $T_1 \sqcup T_2 \sqcup \cdots \sqcup T_s = [n]$ 为对应于 $(A+D)^{-1}$ 的不可约块的指标，其中 D 是对角矩阵，其元素随机选取。设 $C_1, C_2, \ldots, C_s$ 为满足 $C_i \text{ PME} = (A+D)^{-1}[T_i]$ 的矩阵。由于算法 4 给出了指标集 $T_1, T_2, \ldots, T_s$，我们可以找到一个置换矩阵 P，使得 $C = P^T \operatorname{diag}(C_1, \ldots, C_s) P$ 与 $(A+D)^{-1}$ 主子式等价（根据引理 2.1）。现在我们说明如何从 C 恢复一个满足 $B \text{ PME} = A$ 的矩阵 B。

引理 4.4. 设 $C_{\text{PME}} = (A+D)^{-1}$，其中 D 是对角矩阵，且 $A+D$ 可逆。那么，$C^{-1} - D_{\text{PME}} = A$。

证明。由于 C 是 $(A+D)^{-1}$ 的 PME $=$，$\det(C+Y) = \det((A+D)^{-1}+Y)$，其中 $Y = \operatorname{diag}(y_1, \ldots, y_n)$。由于 $\det(C) = \det((A+D)^{-1}) \neq 0$,

$$\begin{aligned} &\det(C^{-1})\det(C+Y) = \det(A+D)\det((A+D)^{-1}+Y) \\ \implies &\det(I_n + C^{-1}Y) = \det(I_n + (A+D)Y). \end{aligned}$$

对变量求逆并乘以 $y_1 \ldots y_n$，可得

$$\begin{aligned} &\det(C^{-1}Y^{-1} + I_n)\det(Y) = \det((A+D)Y^{-1} + I_n)\det(Y) \\ \implies &\det(C^{-1}+Y) = \det(A+D+Y). \end{aligned}$$

将Y 替换为 $-D$，可知 $\det(C^{-1} - D + Y) = \det(A+Y)$。因此，$C^{-1} - D_{\text{是 PME}} = A$。 □

4.5 去随机化归约

前几节展示的、针对具有性质 $\mathcal{R}$的矩阵，将黑盒 PMAP 归约到 PMAP 的随机化归约，可利用 [GT20]中的击中集构造，在准多项式时间内去随机化。下面简述这一确定性归约：

1. 使用 Re 引理 4.2，我们可以找到与 A 的不可约块相对应的指标集 .

2. 根据注记 4.1，利用 [GT20] 击中集，我们有一个包含准多项式数量的对角矩阵的列表 D_1,...，D_k，其中至少有一个矩阵 D 使得 $(A+D)^{-1}$ 的不可约块满足性质 $\mathcal{R}$。我们称这样的 D 是正确的。

3. 如何在上述列表中识别正确的 D？如果我们采用了错误的 D，那么重构矩阵 B 很可能与A并非主子式等价。如果我们能在最后成功检验重构的 B 确实与A主子式等价，就可以避免这个问题。接下来，我们说明如何做到这一点。

4. 要验证 B PME $=$ A 是否成立，已知 B 的显式表示以及 det(A $+$Y) 的黑盒访问，我们首先检查它们的不可约块是否具有相同的指标集（使用备注 4.2）。然后，分别验证各不可约块是否主子式等价。在余下的论证中，假设 A 和 B 不可约。由备注 4.1 可知，我们有准多项式数量的对角矩阵 $D_1,\ldots,D_r$，其中至少有一个矩阵 D 满足 $(B+D)^{-1}$ 具有性质 $\mathcal{R}$。由于我们知道 B 的显式表示，可以通过检查 D 是否满足断言 4.2 中列出的条件，找到正确的 D；第三个条件可以通过检查 $\det\left((B+D)^{\mathrm{adj}}[\{i,j\},\{k,l\}]\right)=0 \Longrightarrow \forall m \in [r], \det\left((B+D_m)^{\mathrm{adj}}[\{i,j\},\{k,l\}]\right)=0$ 来验证。由引理 4.3 可知，我们可以黑盒访问 $\det((A+D)^{-1}+Y)$ 及其主子式。现在可以验证 $(A+D)^{-1}$ 和 $(B+D)^{-1}$ 的阶数至多为 4 的对应主子式是否相等。如果相等，那么由定理 1.3，$(B+D)^{-1}$ PME$=(A+D)^{-1}$；再由引理 4.4，B PME $=$ A。

PME 到 4 阶的充分性4：定理1.3的证明

本文的一项关键技术贡献是识别出一种性质，记作 $\mathcal{R}$，使得对于任意两个所有非对角元均非零的方阵A 和B，若A 满足 $\mathcal{R}$，则A 与B 是 PME 等价的，当且仅当 PME(A、B、4)成立。本小节首先定义性质 $\mathcal{R}$，然后证明定理1.3。最后，我们构造一个反例，说明若A 不满足 $\mathcal{R}$，则 PME(A、B、4) 可能成立，而A 和B 并非主子式等价。

定义 5.1 (性质 $\mathcal{R}$)。设 A 是域 $\mathbb{F}$ 上的一个 n 阶 $\times n$ 方阵。若 A 满足以下条件，则称 A 具有性质 $\mathcal{R}$：

1. 所有非对角元均非零。

2. 若秩 $A[\{i,j\},\{k,\ell\}]=1$ 对任意四个互不相同的元素 i，j、k，$\ell \in [n]$,，则存在 $[n]$ 的一个子集 X，使得 i，$j \in X$，k、$\ell \in X$，且秩 $A[X,X]=1$。

下面的引理表明，若矩阵 A 满足性质 $\mathcal{R}$，则 A 的每个主子矩阵也满足性质 $\mathcal{R}$。

引理 5.1. 设 A 是域 $\mathbb{F}$ 上的一个 $n \times n$ 矩阵，其中 $n \geq 5$。假设 A 满足性质 $\mathcal{R}$。设 $S \subseteq [n]$ 且 $|S| \geq 5$。那么，$A[S]$ 也满足性质 $\mathcal{R}$。

证明。注意，A[S] 的非对角元也是 A 的非对角元。因此，它们均非零。取集合 S 中互不相同的四个元素 i、j、k、ℓ，使得秩 $A[\{i,j\},\{k,\ell\}]=1$。由于 A 满足性质 $\mathcal{R}$，存在 [n] 的一个子集 X，使得 i、j $\in$ X，k,$\ell \in$ X，且秩 A[X, X] $=1$。令 $X_S = X \cap S$ 且 $X_S = X \cap S$。那么，子矩阵 $A[X_S, X_S]$ 是 A[X, X] 的子矩阵。因此，秩 $A[X_S, X_S]=1$。 □

我们的下一个引理受到 [Loe86，引理 6] 的启发。设 A 是一个 $n \times n$ 矩阵。该引理提供了一种方法，可从 A 的某个 $(n-1) \times (n-1)$ 主子矩阵中的一个割，推导出 A 的某些子矩阵上的秩一约束。假设 A 无割。那么，结合引理 2.5，该结果意味着 A 至少有三个$(n-1) \times (n-1)$ 无割主子矩阵。这将有助于我们证明中的归纳步骤。

引理 5.2. 设 $n \geq 5$ 是一个正整数。设 A 是一个定义在 $\mathbb{F}$ 上、满足性质 $\mathcal{R}$的 $n \times n$ 矩阵。设 $X \subseteq [n] \setminus \{i\}$ 是矩阵 $A[[n] \setminus \{i\}]$ 的一个割，且 $X = \overline{[n] \setminus (X \cup \{i\})}$。那么，

$$\operatorname{rank} A[X + i, \overline{X}] = 1 \text{ or } \operatorname{rank} A[X, \overline{X} + i] = 1,$$

and

$$\operatorname{rank} A[\overline{X} + i, X] = 1 \text{ or } \operatorname{rank} A[\overline{X}, X + i] = 1.$$

证明。 根据矩阵的割的定义，我们知道 X 和 $\overline{X}$ 的基数都至少为 2。设 $s \in X$，且 $t \in \overline{X}$。设 $\overline{X}' = X - s$，且 $\overline{X}' = X - t$。由于对于所有$u \in X'$ 和$v \in \overline{X}'$，秩 $\operatorname{rank} A[X,\overline{X}] = 1$，

$$\operatorname{rank} A[\{s, u\}, \{t, v\}] = 1.$$

性质 $\mathcal{R}$的 A 意味着，对于所有 $u \in X'$ 和 $v \in X'$，存在一个子集 X_{uv}，它是 $[n]$ 的子集，使得 at

$$s, u \in X_{uv}, \quad t, v \in \overline{X}_{uv} = [n] \setminus X_{uv} \text{ and } \operatorname{rank} A[X_{uv}, \overline{X}_{uv}] = 1.$$

现在，对于每个 $u \in X'$，考虑 $[n]$的以下子集。

$$X_u = \bigcap_{v \in \overline{X}'} X_{uv} \text{ and } \overline{X}_u = [n] \setminus X_u = \bigcup_{v \in \overline{X}'} \overline{X}_{uv}.$$

于是，引理2.4 意味着对所有$u \in X'$，秩$A[X_u, X_u] = 1$。此外，注意对所有$u \in X'$，X 是X_u 的子集，且 $\{s, u\} \subseteq X_u$。现在考虑以下 $[n]$的子集。

$$T = \bigcup_{u \in X'} X_u \text{ and } \overline{T} = [n] \setminus T = \bigcap_{u \in X'} \overline{X}_u.$$

注意，$X \subseteq T$ 且$X \subseteq \overline{T}$。此外，由引理2.4，可得秩$A[T,T] = 1$。由于$X \subseteq T$、$X \subseteq \overline{T}$，且(X,X) 是 $[n] \setminus \{i\}$的一个划分，

$$\text{either } T = X + i \text{ and } \overline{T} = \overline{X}, \text{ or } T = X \text{ and } \overline{T} = \overline{X} + i,$$

and

$$\operatorname{rank} A[X + i, \overline{X}] = 1, \quad \text{or} \quad \operatorname{rank} A[X, \overline{X} + i] = 1 \tag{8}$$

类似地，利用秩$A[X,X] = 1$，我们可以证明

$$\operatorname{rank} A[\overline{X} + i, X] = 1, \quad \text{or} \quad \operatorname{rank} A[\overline{X}, X + i] = 1 \tag{9}$$

因此，式（8）和式（9）合在一起完成了该引理的证明。 □

引理2.5 与引理5.2 结合可得以下推论。

推论 5.1. 设 $n \geq 5$ 为正整数。设 A 是一个 $\mathbb{F}$ 上的 $n \times n$ 矩阵，满足性质 $\mathcal{R}$。假设 A 无割。那么，至少存在三个元素 $i_1, i_2, i_3 \in [n]$，使得对于 $j = 1$、2、3，子矩阵 $A[[n] \setminus \{i_j\}]$ 均无割。

证明. 注意，A 无割。因此，对于每个 $i \in [n]$，若 $A[[n] \setminus \{i\}]$ 有割，则引理 5.2应用于 A后，会得到一个类型为等式（5）或等式（6）的约束。因此，应用引理 2.5即可得出该推论。

□

假设 $n \geq 5$ 是一个正整数。设 A 与 B 为两个 $n \times n$ 矩阵，使得 A 无割且 A 满足性质 $\mathcal{R}$。此外，假设 PME$(A, B, n-1)$。则由推论 5.1和引理2.3，我们知道

$$|\mathcal{D}_1(A,B) \cup \mathcal{D}_2(A,B)| \geq 3.$$

另一方面，应用引理 2.2，如果

$$|\mathcal{D}_1(A,B) \cup \mathcal{D}_2(A,B)| \geq 5,$$

则 $A \overset{\text{对角等价}}{=} B$，从而利用观察 2.3，$A \overset{\text{PME}}{=} B$。我们还证明假设

$$|\mathcal{D}_1(A,B) \cup \mathcal{D}_2(A,B)| = 3 \text{ or } 4. \tag{10}$$

会导致矛盾。因此，

$$|\mathcal{D}_1(A,B) \cup \mathcal{D}_2(A,B)| \neq 3 \text{ or } 4.$$

这进而使我们能够证明 $A \overset{\text{PME}}{=} B$ 当且仅当 PME$(A, B, 4)$。首先，我们证明若式 (10) 成立，则 $\mathcal{D}_1(A, B)$ 与 $\mathcal{D}_2(A, B)$ 不能有非空交集。

引理 5.3. 设 $n \geq 5$ 为正整数。假设 A 与 B 是两个 $n \times n$ 矩阵，A 的所有非对角元均非零，且 PME$(A, B, 3)$。设

$$|\mathcal{D}_1(A,B) \cup \mathcal{D}_2(A,B)| = 3 \textit{ or } 4.$$

那么，$\mathcal{D}_1(A, B)$ 与 $\mathcal{D}_2(A, B)$ 的交集为空。

注记 5.1. 若 $|\mathcal{D}_1(A, B) \cup \mathcal{D}_2(A, B)| = 4$，我们的证明不需要假设 PME$(A, B, 3)$。此外，当 $|\mathcal{D}_1(A, B) \cup \mathcal{D}_2(A, B)| = 3$ 时，只需假设 $A[S] \overset{\text{PME}}{=} B[S]$，其中 S 是 $\mathcal{D}_1(A, B)$ 与 $\mathcal{D}_2(A, B)$的并集。

证明。 反设 $\mathcal{D}_1(A, B)$ 与 $\mathcal{D}_2(A, B)$ 的交集非空。现在我们将证明分为以下两种情形。

情形 I ($|\mathcal{D}_1(A, B) \cup \mathcal{D}_2(A, B)| = 4$)。 $\mathcal{D}_1(A, B)$ 与 $\mathcal{D}_2(A, B)$ 的交集非空，这意味着 $|\mathcal{D}_1(A, B)| = 3$ 或 $|\mathcal{D}_2(A, B)| = 3$。因此，根据引理 2.2，$\mathcal{D}_1(A, B) \cup \mathcal{D}_2(A, B) = [n]$，，这就产生了矛盾。因此，$\mathcal{D}_1(A, B)$ 与 $\mathcal{D}_2(A, B)$ 的交集为空。

情形 II（$|\mathcal{D}_1(A, B) \cup \mathcal{D}_2(A, B)| = 3$）。若 $\mathcal{D}_1(A, B)$ 与$\mathcal{D}_2(A, B)$ 的交集的基数至少为二，则要么 $|\mathcal{D}_1(A, B)| = 3$，要么 $|\mathcal{D}_2(A, B)| = 3$。因此，与情形 I 类似，引理 2.2 表明 $\mathcal{D}_1(A, B) \cup \mathcal{D}_2(A, B) = [n]$，，这是一个矛盾。故 $|\mathcal{D}_1(A, B) \cap \mathcal{D}_2(A, B)| = 1$。不失一般性，假设

$$\mathcal{D}_1(A,B) = \{1,2\} \text{ and } \mathcal{D}_2(A,B) = \{2,3\}.$$

对所有 $k \in [n],$ ，令 $N_k = [k]$。注意

$$\{1,2\} \subseteq \mathcal{D}_1(A[N_4], B[N_4]) \quad \text{and} \quad \{2,3\} \subseteq \mathcal{D}_2(A[N_4], B[N_4]).$$

由引理的假设可知，$A[N_3] \overset{\text{PME}}{=} B[N_3]$。因此，应用引理2.3，$4 \in \mathcal{D}_1(A[N_4],B[N_4])$ 或 $4 \in \mathcal{D}_2(A[N_4], B[N_4])$。据此，利用引理 2.2，我们得到

$$A[N_4] \overset{\text{DS}}{=} B[N_4] \quad \text{or} \quad A[N_4] \overset{\text{DS}}{=} B[N_4]^T.$$

因此，通过反复应用引理 2.2，我们得到 $A[N_k] \overset{\text{对角等价}}{=} B[N_k]$ 对所有 $k \in \{5,6,\ldots,n\}$成立。因此，$\mathcal{D}_1(A,B) \cup \mathcal{D}_2(A,B) = [n],$ ，这是一个矛盾。至此证明完成。 □

上述引理表明，在式（10）中，我们可以假设 $\mathcal{D}_1(A,B)$ 与$\mathcal{D}_2(A, B)$ 的交集为空。接下来我们证明 $|\mathcal{D}_1(A, B) \cup \mathcal{D}_2(A, B)| \neq 4$。为此，下面的引理确立了 4×4 具有非零非对角元素的矩阵的一个关键性质。

引理 5.4. 设 A 和 B 是两个 4×4 矩阵，A 的所有非对角元均非零，且 $A \overset{\text{PME}}{=} B$。设 $X \subseteq \{1,2,3,4\}$ 满足 $|X| = 2$, $\mathcal{D}_1(A,B) = X$，且 $\mathcal{D}_2(A,B) = X$。那么，X 是 A 的一个割。

证明与 [HL84，定理 4] 的证明非常相似。详情参见 A.1 节。下面的引理讨论 $\mathcal{D}_1$(A, B) 与 $\mathcal{D}_2$(A, B) 的并集包含四个元素的情形（见公式（10））。 [Loe86，定理 2] 中也出现了一个风格相似的引理，但有以下几点不同。他们在假设中要求 A PME = B，这比我们的假设 PME(A, B, 4) 更强。另一方面，我们假设 A 满足性质 $\mathcal{R}$，而他们只要求 A 的非对角元非零，也就是性质 $\mathcal{R}$的第一个条件。尽管如此，两种情形下的结论相同。此外，与 [Loe86，定理 2] 的证明相比，我们的引理证明简单得多。

引理 5.5。 设 n 为满足 $n \geq 4$ 的正整数。设 A 和 B 是域 $\mathbb{F}$ 上的两个 $n \times n$ 矩阵，其中 A 满足性质 $\mathcal{R}$，且 PME(A，B，4)。设 $i_1, i_2, i_3, i_4 \in [n]$ 为四个互不相同的正整数，使得 $\mathcal{D}_1(A, B) = \{i_1, i_2\}$ 且 $\mathcal{D}_2(A, B) \equiv \{i_3, i_4\}$。那么，存在一个 $X \subseteq [n]$，使得 $i_1, i_2 \in X$，$i_3, i_4 \in X$，且 X 是 A 的一个割。

注 5.2。 在上述引理中，只需使用 $A[\{i_1,i_2,i_3,i_4\}] \overset{\text{PME}}{=} B[\{i_1,i_2,i_3,i_4\}]$，而不必使用PME($A$，$B$，4)，即可得出相同的结论。

证明。证 不失一般性，我们可以假设 $\{i_1, i_2\} = \{1,2\}$ 且 $\{i_3, i_4\} = \{3,4\}$.

注意到存在一个矩阵 A'，使其与 A 对角相似，并且 $A'[[n] \setminus \{j\}] = B[[n] \setminus \{j\}]$，其中 $j = 1$, 2。此外，我们可以不使用 A，而改为使用任何与 A对角相似的矩阵。因此，不失一般性，我们可以假设 $A[[n] \setminus \{j\}] = B[[n] \setminus \{j\}]$，其中 $j = 1$，2。这意味着

$$A[i,j] = B[i,j] \text{ for all } (i,j) \notin \{(1,2),(2,1)\}. \tag{11}$$

设 C 为一个 $(n-1) \times (n-1)$ 对角矩阵，其行和列由 $[n] \setminus \{3\}$索引；对于 $i \in [n] \setminus \{3\}$，$C[i,i] = c_i$，其中 $c_1 = 1$。设 D 为另一个 $(n-1) \times (n-1)$ 对角矩阵，其行和列由 $[n] \setminus \{4\}$ 索引；对于 $i \in [n] \setminus \{4\}$，$D[i,i] = d_i$，其中 $d_1 = 1$。此外，假设

$$B[[n] \setminus \{3\}]^T = C^{-1} A[[n] \setminus \{3\}] C \quad \text{and} \quad B[[n] \setminus \{4\}]^T = D^{-1} A[[n] \setminus \{4\}] D. \tag{12}$$

上述方程意味着

$$c_2 = d_2 = \frac{B[2,1]}{A[1,2]}, \text{ and for all } 5 \leq i \leq n, c_i = d_i = \frac{A[i,1]}{A[1,i]} \tag{13}$$

此外，由式（11）、式（12）和式（13），我们有如下结论：

1. B[1, 2] = A[2, 1]$c_1 c_2^{-1}$且 B[2, 1] = A[1, 2]$c_1^{-1} c_2$2. A[j, 4] = A[4, j]$c_j c_4^{-1}$ 对所有 j $\in \{1, 2, 5, 6, \ldots, n\}$3. A[j, 3] = A[3, j]$c_j d_3^{-1}$对所有 j $\in \{1, 2, 5, 6, \ldots, n\}$4. A[j, i] = A[i, j]$c_j c^{-1}$ i 对所有 j $\in \{1, 2, 5, 6, \ldots, n\}$ 且 i $\in \{5, 6, \ldots, n\}$

令 $e_1 = 1, e_2 = c_2, e_3 = d_3, e_4 = c_4$，且对所有 $5 \le k \le n$，$e_k = c_k$。那么，根据上述讨论，我们得到

$$A[j,i] = A[i,j] \cdot \frac{e_j}{e_i} \quad \text{for all } (i,j) \notin \{(1,2),(2,1),(3,4),(4,3)\}. \tag{14}$$

令 E 是一个 $n \times n$ 对角矩阵，使得对所有 $i \in [n], E[i, i] = e_i$。因此，应用等式（14），对于任意 $S \subseteq [n]$ 满足 $\{1,2\} \subseteq S$ 且 $\{3,4\} \subseteq S$，

$$A[\overline{S}, S] = E[\overline{S}] \cdot A[S, \overline{S}]^T \cdot E[S]^{-1}. \tag{15}$$

根据引理的假设，我们知道

$$\{1,2\} \subseteq \mathcal{D}_1\left(A[\{1,2,3,4\}], B[\{1,2,3,4\}]\right) \text{ and } \{3,4\} \subseteq \mathcal{D}_2\left(A[\{1,2,3,4\}], B[\{1,2,3,4\}]\right).$$

接下来，我们证明

$$\mathcal{D}_1\left(A[\{1,2,3,4\}], B[\{1,2,3,4\}]\right) = \{1,2\} \text{ and } \mathcal{D}_2\left(A[\{1,2,3,4\}], B[\{1,2,3,4\}]\right) = \{3,4\}.$$

为导出矛盾，首先假设 3 或 4 中有一个属于 $\mathcal{D}_1$(A[{1, 2, 3, 4}], B[{1, 2, 3, 4}])。那么，根据引理 2.2，A[{1, 2, 3, 4}] DS= B[{1, 2, 3, 4}]。应用等式（11），我们得到 A = B。这意味着 $\mathcal{D}_1$(A, B) = [n], ，这与假设矛盾。现在，假设 1 或 2 中有一个属于$\mathcal{D}_2$(A[{1, 2, 3, 4}], B[{1, 2, 3, 4}])。那么，同样根据引理 2.2，A[{1, 2, 3, 4}] DS= B[{1, 2, 3, 4}]^T。结合等式（12），可知 $B^T = E^{-1}AE$。因此，$\mathcal{D}_2$(A, B) = [n], ，这与假设矛盾。于是，

$$\mathcal{D}_1\left(A[\{1,2,3,4\}], B[\{1,2,3,4\}]\right) = \{1,2\} \text{ and } \mathcal{D}_2\left(A[\{1,2,3,4\}], B[\{1,2,3,4\}]\right) = \{3,4\}. \tag{16}$$

式 (16) 与引理 5.4 结合起来表明，{1, 2} 是矩阵 A[{1, 2, 3, 4}]的一个割。由于 A 满足性质 $\mathcal{R}$，存在子集 X $\subseteq$ [n]，使得 1, 2 $\in$ X，3, 4 $\in$ X，且秩 A[X, X] = 1。现在应用式 (15)，秩 A[X, X] = 1。因此，X 就是我们为矩阵 A 所求的割。 □

我们的下一个引理所处理的情形是，$\mathcal{D}_1(A,B)$ 与 $\mathcal{D}_2(A,B)$ 之并包含三个元素（见式 (10)）。与前一个引理一样，风格相近的结果出现在 [Loe86，定理 4]。此外，我们的引理与 [Loe86，定理 4] 之间的假设差异与之前相同：他们假设 $A \text{ PME } = B$，而我们仅假设 PME($A, B, 4$)；并且我们假设 A 满足性质 $\mathcal{R}$，而他们仅要求 A 的非对角元非零。尽管如此，两种情形的结论仍然相同。

引理 5.6. 设 n 是一个满足 $n \ge 4$ 的正整数。设 A 和 B 是域 F 上的两个 $n \times n$ 矩阵，且 A 满足性质 $\mathcal{R}$，并且满足 PME(A，B，4)。设 $i_1, i_2, i_3 \in [n]$ 是三个互不相同的正整数，并且$\mathcal{D}_1(A, B) = \{i_1, i_2\}$ 以及 $\mathcal{D}_2(A, B) = \{i_3\}$。设

$$T_1 := \left\{ j \in [n] \setminus \{i_1, i_2, i_3\} \mid B[\{i_1, i_2, i_3, j\}]^T \overset{DS}{=} A[\{i_1, i_2, i_3, j\}] \right\}$$

and

$$T_2 := \left\{ j \in [n] \setminus \{i_1, i_2, i_3\} \mid B[\{i_1, i_2, i_3, j\}]^T \overset{DS}{\neq} A[\{i_1, i_2, i_3, j\}] \right\}.$$

那么，存在 X 是 $[n]$ 的一个子集，使得 $\{i_1, i_2\} \subseteq X$，$T_2 + i_3 \subseteq \overline{X}$，并且 X 是矩阵 A 的一个割。

证明。 不失一般性，我们可以假设 $\{i_1, i_2\} = \{1, 2\}$ 且 $i_3 = 3$。我们将证明分为两种情形。

情形 I ($n = 4$). 我们证明，对于 $n = 4$，引理的假设不成立。由于 $A[\{1,2,3\}] \overset{PME}{=} B[\{1,2,3\}]$，根据引理 2.3, $A[\{1,2,3\}] \overset{对角等价}{=} A[\{1,2,3\}]$。因此，$4 \in \mathcal{D}_1(A, B) \cup \mathcal{D}_2(A, B)$，这就产生了矛盾。因此，当 $n = 4$ 时，引理显然成立。

情形 II ($n \geq 5$). 我们首先证明 T_2 非空。为导出矛盾，假设$T_2 = \emptyset$。对于所有 i、$j \in \{4, 5, \ldots, n\}$，令 $S_{i,j} = \{1, 2, 3, i、j\}$。注意到

$$T_2 = \emptyset \Longrightarrow \{3, i, j\} \subseteq \mathcal{D}_2(A[S_{i,j}], B[S_{i,j}]).$$

因此，根据引理 2.2，$A[S_{i,j}]^T \overset{DS}{=} B[S_{i,j}]$。于是，反复应用引理 2.2，我们得到 $\mathcal{D}_2(A,B) = [n]$，这就产生了矛盾。因此，T_2 是一个非空集。

由于 PME$(A, B, 4)$，$A[\{1,2,3\}] \overset{PME}{=} B[\{1,2,3\}]$。因此，根据引理 2.3，$A[\{1,2,3\}] \overset{DS}{=} B[\{1,2,3\}]$，或者 $A[\{1,2,3\}] \overset{DS}{=} B[\{1,2,3\}]^T$。假设 $A[\{1,2,3\}] \overset{DS}{=} B[\{1,2,3\}]$。那么，对于所有$i \in \{4, 5, 6, \ldots\ldots, n\}$

$$\{1, 2, i\} \subseteq \mathcal{D}_1(A[\{1,2,3,i\}], B[\{1,2,3,i\}]).$$

因此，应用引理 2.2，$A[\{1,2,3,i\}] \overset{DS}{=} B[\{1,2,3,i\}]$ 对于所有$i \in \{4, 5, 6, \ldots\ldots, n\}$。于是，反复应用引理 2.2，我们得到 $A \overset{DS}{=} B$。因此，$\mathcal{D}_1(A,B) = [n],$，这就产生了矛盾。因此，

$$A[\{1,2,3\}] \overset{DS}{=} B[\{1,2,3\}]^T, \text{ but } A[\{1,2,3\}] \overset{DS}{\neq} B[\{1,2,3\}] \tag{17}$$

假设 $i \in T_2$。于是，由 $T_2, A[\{1,2,3,i\}] \neq B[\{1,2,3,i\}]^T$ 的定义。由该引理的假设以及公式（17），我们有

$$\{1,2\} \subseteq \mathcal{D}_1(A[\{1,2,3,i\}], B[\{1,2,3,i\}]) \quad \text{and} \quad \{3,i\} \subseteq \mathcal{D}_2(A[\{1,2,3,i\}], B[\{1,2,3,i\}]).$$

此外，应用公式（17），我们得到 $\mathrm{i} \not\in \mathcal{D}_1(\mathrm{A}[\{1,2,3,\mathrm{i}\}], \mathrm{B}[\{1,2,3,\mathrm{i}\}])$。由于 PME(A, B, 4)，由引理 2.3，$\mathrm{A}[\{1,2,\mathrm{i}\}] \mathrm{DS}= \mathrm{B}[\{1,2,\mathrm{i}\}]$ 或 $\mathrm{A}[\{1,2,\mathrm{i}\}] \mathrm{DS}= \mathrm{B}[\{1,2,\mathrm{i}\}]^T$。若 $\mathrm{A}[\{1,2,\mathrm{i}\}] \mathrm{DS}= \mathrm{B}[\{1,2,\mathrm{i}\}]$，则应用引理 2.2，$\mathrm{A}[\{1,2,3,\mathrm{i}\}] \mathrm{DS}= \mathrm{B}[\{1,2,3,\mathrm{i}\}]$。这意味着 $\mathrm{A}[\{1,2,3\}] \mathrm{DS}= \mathrm{B}[\{1,2,3\}]$，而这与公式（17）矛盾。因此，$\mathrm{A}[\{1,2,\mathrm{i}\}] \mathrm{DS}= \mathrm{B}[\{1,2,\mathrm{i}\}]^T$ 但 $\mathrm{A}[\{1,2,\mathrm{i}\}] \mathrm{DS}\neq \mathrm{B}[\{1,2,\mathrm{i}\}]$。于是，

$$\{1,2\} = \mathcal{D}_1(A[\{1,2,3,i\}], B[\{1,2,3,i\}]) \quad \text{and} \quad \{3,i\} \subseteq \mathcal{D}_2(A[\{1,2,3,i\}], B[\{1,2,3,i\}]).$$

此外，如果 1 或 2 属于 $\mathcal{D}_2(A[\{1,2,3,i\}], B[\{1,2,3,i\}])$，则再次根据式（17）和引理 2.2，$A[\{1,2,3,i\}] \overset{DS}{=} B[\{1,2,3,i\{\mathrm{v36}>$。这与 $i \in T_2$ 矛盾。因此，对于所有 $i \in T_2$，

$$\{1,2\} = \mathcal{D}_1(A[\{1,2,3,i\}], B[\{1,2,3,i\}]) \quad \text{and} \quad \{3,i\} = \mathcal{D}_2(A[\{1,2,3,i\}], B[\{1,2,3,i\}]). \tag{18}$$

引理 5.4 和式（18）意味着，对于所有 $i \in T_2$，$\{1,2\}$ 是矩阵 $A[\{1,2,3,i\}]$ 的一个割。因此，矩阵的秩为 $\operatorname{rank} A[\{1,2\},\{3,i\}] = 1$。由于 A 满足性质 $\mathcal{R}$，对于所有 $i \in T_2$，，存在 $X_i \subset [n]$，使得 1、$2 \in X_i$、3、$i \in X_i$，且矩阵的秩为 $\operatorname{rank} A[X_i, X_i] = 1$。考虑以下集合

$$X = \bigcap_{i \in T_2} X_i \quad \text{and} \quad \overline{X} = \bigcup_{i \in T_2} \overline{X}_i.$$

由引理2.4，我们得到

$$\operatorname{rank} A[X, \overline{X}] = 1 \quad \text{with} \quad 1,2 \in X, \quad \text{and} \quad T_2 + 3 \subseteq \overline{X}. \tag{19}$$

注意，存在一个矩阵 A'，使其与 A 对角相似，且 $A'[[n] \setminus \{j\}] = B[[n] \setminus \{j\}]$ 对 $j = 1$，2 成立。此外，我们可以使用任何与 A对角相似的矩阵来代替 A。因此，不失一般性，我们可以假设 $A[[n] \setminus \{j\}] = B[[n] \setminus \{j\}]$ 对 $j = 1$，2 成立。这意味着

$$A[i,j] = B[i,j] \text{ for all } (i,j) \notin \{(1,2),(2,1)\}.$$

设 复数域 是一个 $n \times n$ 对角矩阵，使得对所有 $i \in [n]$, 复数域$[i, i] = c_i$ 且 $c_1 = 1$，并满足以下条件：

1. $B[[n] \setminus \{3\}]^T = C[[n] \setminus \{3\}]^{-1} \cdot A[[n] \setminus \{3\}] \cdot C[[n] \setminus \{3\}]$2. $B[\{1,2,3\}]^T = C[\{1,2,3\}]^{-1} \cdot A[\{1,2,3\}] \cdot C[\{1,2,3\}]$3. 对所有 $i \in T_1, B[\{1,2,3,i\}]^T = C[\{1,2,3,i\}]^{-1} \cdot A[\{1,2,3,i\}] \cdot C[\{1,2,3,i\}]$

注意，这样一个 复数域 的存在性可由 $\mathcal{D}_2(A,B) = \{3\}$、等式 (17) 以及 T_1的定义推出。因此，

1. $\mathrm{B}[1,2] = \mathrm{A}[2,1]\mathrm{c}_1\mathrm{c}_2^{-1}$和 $\mathrm{B}[2,1] = \mathrm{A}[1,2]\mathrm{c}_1^{-1}\mathrm{c}_2$。2. 对所有 $\mathrm{j} \in \{4,5,$。。。$,\mathrm{n}\}$ 和 $\mathrm{i} \in \{1,2,4,5,$。。。$,\mathrm{n}\}$，$\mathrm{A[j,i]} = \mathrm{A[i,j]c}_j\mathrm{c}^{-1}\mathrm{i}$。3. 对所有 $\mathrm{i} \in \mathrm{T}_1 \cup \{1,2\}$，$\mathrm{A}[3,\mathrm{i}] = \mathrm{A}[\mathrm{i},3]\mathrm{c}_3\mathrm{c}^{-1}\mathrm{i}$。

这意味着，对于任意 $S \subseteq [n]$，其中 $1,2 \in S$ 且 $T_2 + 3 \subseteq S$，

$$A[\overline{S}, S] = C[\overline{S}] \cdot A[S, \overline{S}]^T \cdot C[S]^{-1}.$$

上面的方程结合方程（19）可得，X 是 A 的一个割，且 $1,2 \in X$ 和 $T_2 + 3 \subseteq X$。证明至此完成。□

现在，我们证明无割情形下的定理 1.3 。具体而言，我们证明，对于任意两个方阵 A 和 B，若 A 无割且满足性质 $\mathcal{R}$，则 A 和 B 的对应主子式相等，当且仅当它们阶数不超过 4的对应主子式相等。

定理 5.1。 设 A 和 B 是域 $\mathbb{F}$ 上的两个 $n \times n$ 矩阵。假设 A 满足性质 $\mathcal{R}$ 且无割。那么，$A \overset{\text{PME}}{=} B$，当且仅当 PME($A$、$B$、4)。

证明。 我们对n进行归纳证明。对于$n = 4$，结论显然成立。

假设 $n \geq 5$ 且 PME$(A, B,4)$。根据引理 2.2，要证明 $A \overset{\text{PME}}{=} B$，只需证明

$$|\mathcal{D}_1(A, B) \cup \mathcal{D}_2(A, B)| \geq 5.$$

根据我们的假设，A 满足性质 $\mathcal{R}$，且 A 没有割。应用推论 5.1，至少存在三个不同的指标 $i_1, i_2, i_3 \in [n]$，使得对于每个 $j \in \{1,2,3\}$，子矩阵 $A[[n] \setminus \{i_j\}]$ 都没有割。此外，根据引理 5.1，每个 $A[[n] \setminus \{i_j\}]$ 仍满足性质 $\mathcal{R}$。另外，PME$(A[[n] \setminus \{j\}], B[[n] \setminus \{j\}], 4)$。因此，根据归纳假设，对于每个 $j \in \{1,2,3\}$，$A[[n] \setminus \{j\}]$ PME$=$ $B[[n] \setminus \{j\}]$。由于 $A[[n] \setminus \{j\}]$ 没有割且所有非对角元均非零，根据引理 2.3，$A[[n] \setminus \{j\}]$ DE$=$ $B[[n] \setminus \{j\}]$。等价地，

$$|\mathcal{D}_1(A, B) \cup \mathcal{D}_2(A, B)| \geq 3.$$

然而，引理5.6 和引理 5.5 结合引理 5.3 排除了$|\mathcal{D}_1(A,B) \cup \mathcal{D}_2(A, B)|$ 分别等于 3 和 4 的可能性，因为这将意味着矩阵A具有一个会导致矛盾的割。

□

现在，我们着重证明本文的主要技术性结果：对于任意两个A 和 B，若它们是具有非零非对角元的方阵，且 A 满足性质 $\mathcal{R}$，则 A 和 B 主子式等价，当且仅当它们阶数不超过 4 的对应主子式相等。我们的证明对矩阵的大小进行归纳。为此，下面的引理将较大的矩阵分解为较小的矩阵，从而使我们能够对较小的矩阵应用归纳假设。该引理的核心思想已经出现在 [CGGR25],中，尽管其形式并不完全是这里所陈述的形式。

引理 5.7 (分解引理)。 设 A 和 B 是域 $\mathbb{F}$ 上的两个具有非零非对角元的 $n \times n$ 矩阵。设 $S \subseteq [n]$ 是 A 和 B 的一个割。取任意两个指标 s，t，使得 $s \in S$ 且 $t \in \overline{S}$。则 $A \overset{\text{PME}}{=} B$，当且仅当 $A[S + t] \overset{\text{PME}}{=} B[S + t]$ 且 $A[S + s] \overset{\text{PME}}{=} B[S + s]$。此外，如果 S 是 A 的极小割，则 $A[S + t]$ 无割。

证明见小节 A.2。我们还需要以下结果，它建立了两个矩阵的割之间的关系：这两个矩阵的阶数至多为 4 的对应主子式相等。

引理 5.8. 设 A 和 B 是两个具有非零非对角元的 $n \times n$ 矩阵，且满足 PME$(A, B,4)$。设 S 是 A 的一个大小大于2的极小割。那么，S 也是 B 的一个割。

一个密切相关的结果见 [CGGR25，引理 3。6], 其关键区别在于假设的强弱：虽然 [CGGR25] 假设 $A \overset{\text{PME}}{=} B$，但上述引理只要求较弱的假设 PME$(A, B,4)$。尽管如此，上述引理的证明总体思路与 [CGGR25，引理 3。6], 相同，此外还依赖定理 5.1。完整证明请参见小节 A.3。现在，所有必要工具均已就绪，我们可以正式证明定理 1.3。

定理的证明 1.3。 性质 $\mathcal{R}$ 保证A 的所有非对角元均非零。接下来，我们证明B 的所有非对角元也均非零。反设$B[i, j] = 0$，其中$i \neq j \in [n]$。那么，$\det(A[\{i, j\}]) \neq \det(B[\{i, j\}])$，这与 PME$(A, B, 4)$矛盾。因此$B$ 的所有非对角元均非零。

我们通过对 n 进行归纳法来证明该定理。对于 $n = 4$，结论显然成立。若A 没有割，则结论由定理 5.1 得出。

在归纳步骤中，假设 PME$(A, B, 4)$，且 A 有一个割，并设 $S \subseteq [n]$ 是 A 的极小割。现在我们将证明分为以下两种情形。

情形 I（S 是 B 的一个割）。根据引理 5.7，只需证明对于某些 s ∈S 和 t ∈S，A[S +t] PME= B[S +t]，且 A[S +s] PME=B[S +s]。注意，A[S +t] 和 A[S +s] 都继续满足引理 5.1 后的性质$\mathcal{R}$。此外，PME(A[S +t], B[S +t], 4) 和 PME(A[S +s], B[S +s], 4)。由此，证明可根据归纳假设得出。

情形 II（S 不是 B 的割）。由引理 5.8可知，S 的基数必须为二。于是，应用引理 2.7，存在 B 的一个割 X，使得 S 是 $B \quad = \mathrm{ct}(B,X)$的一个割。由于主子式在切割转置操作下保持不变（见引理 2.6），$B \overset{\text{PME}}{=} \widetilde{B}$，且 $\mathrm{PME}(A, \widetilde{B}, 4)$。此外，$S$ 现在也是 $\widetilde{B}$ 的一个割。因此，应用**情形 I**，可得 $A \overset{\text{PME}}{=} \widetilde{B}$。于是，$A \overset{\text{PME}}{=} B$。

□

性质 $\mathcal{R}$ 可以去掉吗？这里，我们讨论以下问题。设 A 和 B 是域 $\mathbb{F}$ 上两个 n ×n 矩阵，且其非零非对角元均非零。由定理 1.3 可知，若 A 具有性质 $\mathcal{R}$，则 A PME = B 当且仅当 PME(A, B, 4)。一个自然的问题是：我们能否去掉性质 $\mathcal{R}$，同时仍保证得到与定理 1.3 相同的结论？我们的答案是否定的。更具体地说，我们构造一对矩阵 A 和 B，使得 PME(A, B, 4) 成立，但 A 与 B 并非主子式等价。详情请见附录 B。

6 黑箱割查找

记号。我们首先介绍本节及下一节将使用的记号。设 $B \in \mathbb{F}^{4\times 4}$ 是一个非对角元均非零的矩阵。那么，$\mathcal{S}_B$ 是满足以下条件的所有 $\mathbb{F}$ 上的 4×4矩阵的集合：

1. for any matrix $C \in \mathcal{S}_B$, $C[1, j] = 1$ for $j = 2, 3, 4$, and
2. 对于 任意 4×4 矩阵 D 满足 $D \overset{\text{PME}}{=} B$，存在一个矩阵 $C \in \mathcal{S}_B$ 使得 $D \overset{\text{DS}}{=} C$.

根据 [CGGR25，引理 3。1] 和观察 2.2，族 $\mathcal{S}_A$ 是有限的。稍后，在第 7.1 节中，我们将给出一种算法，在已知 $\mathcal{S}_A$ 以及 A 的主子式的情况下计算它。设 I是一个有限集合。令 A 为一个 $\mathbb{F}$ 上的矩阵，其行和列均以 I为索引，且 A 的非对角元均非零。那么，

$$\mathcal{F}_A = \left\{ (T, \mathcal{S}_{A[T]}) \mid T \subseteq I \text{ with } |T| = 4 \right\}.$$

6.1 割寻找算法

假设 A 是域 $\mathbb{F}$ 上满足性质 $\mathcal{R}$ 的一个 $n \times n$ 矩阵。我们的目标是以黑盒方式判定 A 是否具有割；也就是说，我们不能直接访问 A 的各个元素，而只能查询其主子式。此外，若 A 具有割，该算法还会输出一个子集 $S \subseteq [n]$，且满足 $2 \le |S| \le n-2$，使得 S 是某个矩阵 $C \in \mathbb{F}^{n\times n}$ 中的一个割，该矩阵满足 $C \overset{\text{PME}}{=} A$。

我们强调，稍后（在第7.1节）将给出一个算法：对于任意$I \subseteq [n]$ 且满足$|I| = 4$的集合，在能够访问$A[I]$, 的主子式的情况下，计算出该族 $\mathcal{S}_{A[I]}$。因此，我们可以获得族 $\mathcal{F}_A$。访问该族对于我们的目的而言已经足够。此外，该算法还将作为之后重构算法中的一个子程序使用，在该重构算法中，$\mathcal{F}_A$ 将根据A的主子式显式计算得到。因此，在对求割算法的描述中，我们假设 $\mathcal{F}_A$ 作为输入给定，而不是访问主子式。

现在，我们为一个$n \times \times n$矩阵A的4×4主子矩阵定义一个性质。这一性质对于设计我们的算法至关重要。

定义 6.1 (性质 $\mathcal{P}$)。给定一个矩阵 A，若一组两对 $t = \{\{i, j\}, \{k, l\}\}$ 中的 i, j, k, l 互不相同，且存在一个 4×4 矩阵 $C_t = A[\{i, j, k, l\}]$，使得 $\{i, j\}$ （等价地，$\{k, l\}$）是 C_t的一个割，则称这组两对满足性质 $\mathcal{P}$。

以下观察表明，可以高效地验证一对是否满足性质 $\mathcal{P}$。

观察 6.1。对于任意矩阵 $A \in \mathbb{F}^{n \times n}$，给定族 $\mathcal{F}_A$ 和一对 $t = \{\{i, j\}, \{k, l\}\}$，我们可以在常数时间内检查 t 是否满足性质 $\mathcal{P}$。

直观地说，上述定义刻画了一种局部性质，它仅适用于大型$n \times n$矩阵A的 4×4 主子矩阵。接下来，我们利用这一局部性质为A定义一个全局对象。刻画满足性质 $\mathcal{R}$ 的矩阵A 是否有割，将会有所帮助。

定义 6.2 (合理集合). 给定一个 $n \times n$ 矩阵 A，一个大小至少为二且至多为 $n - 2$ 的子集 $S \subseteq [n]$ 称为合理集合，如果对于每个 $\{i,j\} \subset S$, $\{k,l\} \subset S$, $\{\{i,j\},\{k,l\}\}$ 均满足性质 $\mathcal{P}$。

接下来，我们介绍两个在设计算法时起到关键作用的引理。我们将这些引理的证明推迟到本小节末尾。假设A 是一个满足性质$\mathcal{R}$的矩阵。那么，下面的引理在所有满足性质 $\mathcal{P}$的数对 $\{\{i, j\}, \{k,l\}\}$的集合上确立了一种传递关系。直观地说，给定两个共享指标的此类数对，可以推导出一个也满足 $\mathcal{P}$的新数对。

引理 6.1 (性质的传递性 $\mathcal{P}$). 设 A 是一个满足性质 $\mathcal{R}$的 $n \times n$ 矩阵。设 $i,j,k,l_1,l_2 \in [n]$ 是互不相同的元素，且 $\{\{i,j\},\{k,l_1\}\}$ 和 $\{\{i,j\},\{k,l_2\}\}$ 均满足性质$\mathcal{P}$，那么 $\{\{i,j\},\{l_1,l_2\}\}$也满足性质 $\mathcal{P}$。

上述引理的证明见第6.1.2节。下面的观察给出了一个类似结果：将可信集合换成割，该结果很容易验证。

观察 6.2。设 A 是一个具有非零非对角元的 $n \times n$ 矩阵。设 i、j、k、l_1,$l_2 \in [n]$ 是互不相同的元素，且 $A[\{i、j、k、l_1\}]$ 和 $A[\{i、j、k、l_2\}]$ 都有割 $\{i、j\}$。那么，$\{i、j\}$ 也是 $A[\{i、j、l_1,l_2\}]$的一个割。换言之，$\{i、j\}$ 是 $A[\{i、j、k、l_1,l_2\}]$的一个割。

假设 A 是满足性质 $\mathcal{R}$ 的矩阵。假设我们无法访问 A 的矩阵元，而只能访问 A 的主子式。那么，A 有割，当且仅当任何与 A 主子式等价的矩阵都有割。由 [CGGR25，定理 1.1] 可知这一结论。因此，A 存在割这一事实，是所有与 A 主子式等价的矩阵所共有的全局性质。然而，对于某个特定子集 S 是否为 A 的割，情况并非如此。可能出现这样的情形：S 不是 A 的割，却是另一个矩阵 C 的割，其中 $A = C$。由 [CGGR25，定理 1.1 和引理 3.2] 可知这一结论。因此，若只能访问 A 的主子式，预计我们无法输出一个割。幸运的是，对于我们的目的，只需找到一个子集S，使得 S 是某个矩阵 C 的割，且 $C = A$；而可信集合恰好刻画了这类集合。我们先给出以下直接的观察。

观察 6.3。对于一个具有割 $S \subset [n]$ 的 $n \times n$ 矩阵 A，S 也是 A 的合理集合。

引理 6.2。设 A 是一个满足性质 $\mathcal{R}$ 的 $n \times n$ 矩阵。那么，子集 $S \subset [n]$ 是合理集合，当且仅当它是某个矩阵 C 的割，且 $C = A$。

上述引理的证明请参见第6.1.3小节。

6.1.1 割寻找算法的描述及其正确性

黑箱割寻找算法的伪代码请参见算法5。

算法 5割寻找算法

输入： 一个集合 I，满足 $|I| \geq 4$；族 $\mathcal{F}_A$，其中矩阵 A 的行和列以由I索引，其中A 满足性质 $\mathcal{R}$。

输出： 如果A 没有割，则输出“否”。否则，输出一个$S \subseteq I$，使得S 是某个具有$A_{\text{PME}} = C$的矩阵C 中的一个割。

令 $|I| = n$，不失一般性，假设 $I = [n]$。
对于 $t \leftarrow \{\{i, j\}, \{k, l\}\}$，其中 $i, j, k, l \in [n]$ **执行**
    如果 t 满足性质 $\mathcal{P}$ **则**
        对于每个 $e \in [n] \setminus \{i, j, k, l\}$，令 x_e 表示一个布尔变量。
        令 ϕ_t 为一个初始时不含任何子句的 2-SAT 实例。
        对于 $e \leftarrow [n] \setminus t$ **执行**
            如果 $\{\{i, j\}, \{k, e\}\}$ 或 $\{\{i, j\}, \{l, e\}\}$ 中的任一个不满足性质 $\mathcal{P}$ **则**
                $\phi_t \leftarrow \phi_t \wedge (x_e = \text{真})$
            结束如果
        结束 for
        对于 $e \in [n] \setminus t$ **执行**
            如果 $\{\{i, e\}, \{k, l\}\}$ 或 $\{\{j, e\}, \{k, l\}\}$ 中的任一个不满足性质 $\mathcal{P}$ **则**
                $\phi_t \leftarrow \phi_t \wedge (x_e = \text{假})$
            结束条件判断
        结束循环
        对于 (p, q) 满足 $p \neq q$ 且 $p, q \in [n] \setminus \{i, j, k, l\}$，$a \in \{i, j\}$，$c \in \{k, l\}$ **执行**
            如果 $\{\{a, p\}, \{c, q\}\}$ 不满足性质 $\mathcal{P}$ **则**
                $\phi_t \leftarrow \phi_t \wedge (x_q \vee \neg x_p)$.
            结束 if
        结束 for
        如果 ϕ_t 可满足，**则**
            $x^* \leftarrow$ 是 2-SAT ϕ_t 的一个满足赋值。
            $S \leftarrow \{i, j\} \cup \{e \in [n] \setminus \{i, j, k, l\} \mid x^*_e = \text{真}\}$。
            返回 S。
        结束 if
    结束 if
结束 for
返回‘否’

注 6.1。 我们对算法 5作如下两点说明。

1. 给定一个显式的不可约矩阵 A，只需稍作修改即可调整算法 5，以找到 A 的一个割。具体而言，每当算法验证一对 $\{\{i, j\}, \{k, l\}\}$ 是否满足性质 $\mathcal{P}$ 时，我们改为检查 $A[\{i, j, k, l\}]$ 是否以 $\{i, j\}$ 为割。正确性证明与算法 5 的证明非常相似，详见引理 6.3。*2.* 如果一个合理集合 S 的任意真子集都不是合理集合，则称 S 是极小的。如果我们能够为一个 *2-SAT* 实例找到一个包含最少1的满足赋值，那么它将对应于一个极小合理集合 S，因此根据引理 6.2，$C_{\text{PME}} = A$ 中以任意 S 为割的割将是极小的。如果存在

一个矩阵 $C' \underset{\text{PME}}{=} A$ 具有割 $X \subset S$，那么 X 将是一个合理集合，这与 S 是极小的这一事实相矛盾。给定一个 *2-SAT* 实例的满足赋值，我们可以通过逐个将*1*翻转为*0*，并检查其是否仍可满足，从而轻松找到一个极小满足赋值。这意味着可以调整算法 5，使其输出一个极小合理集合，从而得到某个 $C \underset{\text{PME}}{=} A$ 中的一个极小割。

下面的引理讨论算法 5 的正确性证明和运行时间。

引理 6.3。 设 A 是一个满足性质 $\mathcal{R}$ 的 $n \times n$ 矩阵。如果 A 有一个割，则算法 5 会在某个矩阵 C 中输出一个割 S，使得 $C \underset{\text{PME}}{=} A$；否则，它会在 多项式$(n)$ 时间内输出*"NO"*。

证明。 首先，我们证明如果 A 有一个割，那么算法不会输出"NO"。设 A 的某个割为 S。不失一般性，假设 $\{1,2\} \subset S$，$\{3,4\} \subset S$。接着，考虑如下赋值x，使得对每个 $e \in [n] \setminus [4]$,

$$x_e = \begin{cases} \text{True} & \text{if } e \in S \\ \text{False} & \text{otherwise} \end{cases}.$$

我们将证明 x 满足针对 $t = \{\{1,2\},\{3,4\}\}$ 的 2-SAT ϕ_t。

反设 x 不满足 ϕ_t。这意味着 x 不满足 ϕ_t 的某个子句。

情形 *1*：假设它不满足第 8 行中的子句。这意味着存在 $e \notin S$，使得 $\{\{1,2\},\{3,e\}\}$ 或 $\{\{1,2\},\{4,e\}\}$ 不满足性质 $\mathcal{P}$。然而，这与 S 是 A 的一个割（因此根据观察结果 6.3，它是一个合理集合），并且$\{1,2\} \subseteq S$ 和$\{3,4,e\} \subseteq S$ 相矛盾。

情形 *2*：与情形 *1*类似，我们可以论证 x 满足第 13 行中的子句。

情形 3：我们证明 x 满足第 18 行中的子句。假设这不成立。这意味着存在某些 $\text{p}, \text{q} \in [\text{n}] \setminus [4]$，使得 $\text{q} \in \text{S}$、$\text{p} \in \text{S}$，且存在 $\text{a}, \text{b} \in \{1,2\}$，使得$\{\{\text{a}, \text{p}\},\{\text{q}, \text{l}\}\}$ 不满足性质 $\mathcal{P}$。然而，这与 S 是 A 的一个割，且 $\{1,2,\text{p}\} \subseteq \text{S}$ 和 $\{3,4,\text{q}\} \subseteq \text{S}$ 相矛盾。

因此，x 满足 ϕ_t的所有子句，所以当A 有一个割时，该算法不会输出"NO"。

现在，我们证明：如果对于任意两对 $\{\{\text{i}, \text{j}\}、\{\text{k}, \text{l}\}\}$，该算法输出某个集合 S，那么 S 是一个合理集合。根据引理 6.2，这意味着 S 是某个矩阵 C 的割，且 $\text{C PME} = \text{A}$。为了证明 S 是一个合理集合，我们必须证明：对于每个 $\{\text{a}, \text{b}\} \subset \text{S}$、$\{\text{c}, \text{d}\} \subset \text{S}$，$\{\{\text{a}, \text{b}\}$和 $\{\text{c}, \text{d}\}\}$ 满足性质 $\mathcal{P}$。我们根据交集 $\text{T} = \{\text{i}, \text{j}, \text{k}, \text{l}\} \cap \{\text{a}, \text{b}, \text{c}, \text{d}\}$的大小，分情形进行分析。根据构造，$\{\text{i}, \text{j}\} \subseteq \text{S}$ 且 $\{\text{k}, \text{l}\} \subseteq \text{S}$。$|\text{T}| = 4$的情形可直接由算法第 3 行得出。

1. $|\text{T}| = 3$：不失一般性，设 $\{\text{a}, \text{b}\} = \{\text{i}, \text{j}\}$ 且 $\text{c} = \text{k}, \text{d} \neq \text{l}$。由于 x^* 满足 ϕ_t且 x^*_d为假，$\{\{\text{i}, \text{j}\},\{\text{k}, \text{d}\}\}$ 满足性质 $\mathcal{P}$，否则第 8 行的子句将被违反。
2. $|T| = 2$：这可以进一步分为以下几种子情形（对元素重新编号后）。

   (a) $\{\text{a}, \text{b}\} = \{\text{i}, \text{j}\}$ 与 $\{\text{c}, \text{d}\} \cap \{\text{k}, \text{l}\} = \emptyset$：由情形 1，$\{\{\text{i}, \text{j}\}、\{\text{k}, \text{c}\}\}$ 与 $\{\{\text{i}, \text{j}\}、\{\text{k}, \text{d}\}\}$ 均满足性质 $\mathcal{P}$。因此，由引理 6.1，$\{\{\text{i}, \text{j}\}、\{\text{c}, \text{d}\}\}$ 满足性质 $\mathcal{P}$。(b) $\text{a} = \text{i}, \text{c} = \text{k}$：由于 $\text{x}^*_b =$ 为真且 $\text{x}^*_d =$ 为假，$\{\{\text{i}, \text{b}\}、\{\text{k}, \text{d}\}\}$ 满足性质 $\mathcal{P}$，否则第 18 行的子句将被违反。

3. $|T| = 1$：不失一般性，设 $a = i$ 且 $\{j, k, l\} \cap \{b, c, d\} = \emptyset$。由情形 2(b)，$\{\{i, b\}, \{k, c\}\}$ 与 $\{\{i, b\}, \{k, d\}\}$ 满足性质 $\mathcal{P}$。因此，由引理 6.1，$\{\{i, b\}, \{c, d\}\}$满足性质 $\mathcal{P}$。

4. $|T| = 0$：由情形 3 可知，$\{\{i, a\}, \{c, d\}\}$ 和 $\{\{i, b\}, \{c, d\}\}$ 满足性质 $\mathcal{P}$。因此，根据引理 6.1，$\{\{a, b\}, \{c, d\}\}$ 满足性质 $\mathcal{P}$。

现在我们分析该算法的运行时间。对于任意一组t 对，该算法都能在多项式时间内构造出相应的公式 ϕ_t。这是因为可以在常数时间内验证性质 $\mathcal{P}$ 是否成立（根据观察6.1），而构造 ϕ_t的过程中只需要进行多项式次此类检查。由于每个 ϕ_t 都是一个含有多项式数量子句的 2-SAT 实例，并且$O(n^4)$ 中有种可能的两对t选择，因此该算法的总体运行时间是关于n的多项式。

□

6.1.2 引理6.1的证明

我们先陈述两个引理，这些引理来自 [CGGR25]，并将在后续证明中用到。

引理 6.4。 *[CGGR25，引理 3。1]* 设 A 是一个非零非对角元的 4×4 矩阵，且 $B \text{ PME} = A$ 是另一个矩阵。那么，要么 $A \text{ DE} = B$，要么存在一个公共割 S，使得 $\text{ct}(A, S) \text{ DE} = B$。

引理 6.5。 *[CGGR25，引理 3。2]* 设 A 是一个 $n \times n$ 阶矩阵，其元素属于 $\mathbb{F}$，且具有非零非对角元。设 $S \subseteq [n]$ 是 A中的一个割。那么，对任意 $T \subseteq [n]$，以下结论成立。

1. 若 T 或 $\overline{T}$ 是 S 或 S 的子集，则 T 是 A 中的割，当且仅当 T 是 $\text{ct}(A, S)$ 中的割。

2. 否则，T 是 A 中的割，当且仅当 $T\Delta S$ 是 $\text{ct}(A, S)$ 中的割。

观察 6.4。 设 A 是一个 $n \times n$ 阶矩阵，且具有非零非对角元。若 $\{\{i, j\}, \{k, l\}\}$ 满足性质 $\mathcal{P}$，则以下结论之一必定适用于 $A[\{i, j, k, l\}]$:

1. $\{i、j\}$ 是一个割。*2.* $\{i、k\}$ 和 $\{i、l\}$ 都是割，

但 $\{i、j\}$ 不是割。

证明。设 $A' = A[\{i、j、k、l\}]$。根据定义，存在一个 4×4 矩阵 C' PME$= A'$，使得 $\{i、j\}$ 是一个割。由引理 6.4，要么 A' 与 C' 对角等价，要么存在一个公共割，记为 S，使得 A' 与 $\text{ct}(C'、S)$对角等价。若属于前一种情形，则 A' 具有割 $\{i、j\}$。设属于后一种情形，且 A' 不具有割 $\{i、j\}$。不失一般性，设公共割 $S = \{i、k\}$。由于 $\{i、j\}$ 是 C'的一个割，根据引理 6.5，$\{i、k\}\Delta\{i、j\} = \{j、k\}$，等价地说 $\{i、l\}$，也是 $\text{ct}(C'、S)$ 的一个割，因而也是 A'的一个割。 □

现在，我们回到引理 6.1 的证明。不失一般性，设 $i = 1$，$j = 2$，$k = 4$，$l_1 = 3$，$l_2 = 5$。我们根据观察 $A_1 = A[\{1,2,3,4\}]$ 和 $A_2 = A[\{1,2,4,5\}]$ 满足观察 6.4 中哪些条件，分以下三种情形进行证明。令 $A_3 = A[\{1,2,3,5\}]$。

1. A_1 和 A_2 均满足条目 1。根据观察 6.2，$\{1,2\}$ 是 $A[[5]]$的一个割。因此，A_3 有割 $\{1,2\}$，这意味着 $\{\{1,2\},\{3,5\}\}$ 满足 $\mathcal{P}$。2. A_1 和 A_2 均满足条目 2。这意味着 $\{1,4\}$ 是 A_1 和 A_2的共同割。因此，$\{1,4\}$ 是 $A[[5]]$的一个割。由于 A_1 和 A_2 满足条目 2，$\{1,3\}$ 和 $\{1,5\}$ 分别是 A_1 和 A_2, 的割。这又意味着它们都以 $\{2,4\}$ 为割。因此，根据观察 6.2，$\{2,4\}$ 也是 $A[[5]]$的一个割。令 $C = \text{ct}(A[[5]], \{1,4\})$。那么，根据引理 6.5，$C$ PME $= A[[5]]$，且以 $\{1,4\}\Delta\{2,4\} = \{1,2\}$ 为割。这意味着 $C[\{1,2,3,5\}]$ PME$= A_3$，且以$\{1,2\}$ 为割。因此，$\{\{1,2\},\{3,5\}\}$ 也满足性质 $\mathcal{P}$。

3. A_1 满足条目 1 和 A_2 满足条目 2。由于 A 满足性质 $\mathcal{R}$，所以 $A[[5]]$也满足$A[\{1,2\},\{3,4\}]$ 的秩为一，因此 $A[\{1,2,5\},\{3,4\}]$ 或 $A[\{1,2\},\{3,4,5\}]$ 必有一个秩为一。同理，$A[\{3,4,5\},\{1,2\}]$ 或 $A[\{3,4\},\{1,2,5\}]$ 必有一个秩为一，因为 $A[\{3,4\},\{1,2\}]$的秩为一。这引出了以下四种子情形:

(a) $A[\{1,2\},\{3,4,5\}]$ 和 $A[\{3,4,5\},\{1,2\}]$ 的秩均为一。这意味着 $A[[5]]$ 有一个割 $\{1,2\}$。因此，$\{\{1,2\},\{3,5\}\}$ 满足 $\mathcal{P}$。(b) $A[\{1,2,5\},\{3,4\}]$ 和 $A[\{3,4,5\},\{1,2\}]$ 的秩均为一。由于 A 有非零的非对角元，因此存在一个与A 对角相似的矩阵，其第一行除对角元外全为 1。因此，不失一般性，我们可以假设A 的第一行除对角元外全为 1。假设 $A[2,3]=a$，且 $A[(3,4,5),\ 1]=(b、c、d)^T$。现在，我们利用已知的秩一子矩阵，证明$A[[5]]$ 具有如下矩阵的形式，其中 α 是某个非零标量。这进而意味着 $\{1,2\}$ 是$A[[5]]$ 的一个割，因此 $\{\{1,2\},\{3,5\}\}$ 满足性质 $\mathcal{P}$。

$$A[[5]]=\begin{bmatrix} * & 1 & 1 & 1 & 1 \\ a/\alpha & * & a & a & a \\ b & \alpha b & * & * & * \\ c & \alpha c & * & * & \alpha c \\ d & \alpha d & \alpha d & \alpha d & * \end{bmatrix}$$

由于 $A[\{3,4,5\},\{1,2\}]$ 的秩为一，存在非零标量 α 使得 $A[(3,4,5),\ 2]=\alpha(b,c,d)^T$。由于 A_2 满足条目 2，$A[\{1,5\},\{2,4\}]$ 和 $A[\{1,4\},\{2,5\}]$ 的秩均为一。因此，$A[5,4]=\alpha d$ 和 $A[4,5]=\alpha c$。由于 $A[\{1,2,5\},\{3,4\}]$ 的秩为一，$A[2,4]=a$，$A[5,3]=\alpha d$。由于 A_2 满足条目 2，$A[\{2,5\},\{1,4\}]$ 的秩为一。这意味着 $A[2,1]=A_{[5,1]}A_{[2,4]}A_{[5,4]}=a/\alpha$。最后，由于 $A[\{2,4\},\{1,5\}]$ 的秩为一，$A[2,5]=A_{[2,1]}A_{[4,5]}A_{[4,1]}=a/\alpha\cdot\alpha c\ c=a$。这就完成了说明 $A[[5]]$ 为何如上所示出现的论证。

(c) $A[\{1,2\},\{3,4,5\}]$ 与$A[\{3,4\},\{1,2,5\}]$ 具有秩一。这可归结为情形3(b)，若我们将A 替换为其转置。

(d) $A[\{1,2,5\},\{3,4\}]$ 与 $A[\{3,4\},\{1,2,5\}]$ 具有秩一。这意味着 $A[\{1,3,4,5\}]$ 以$\{1,5\}$ 为割。此外，已知 $A_2=A[\{1,2,4,5\}]$ 以 $\{1,5\}$ 为割。这意味着 $A[[5]]$ 以 $\{1,5\}$ 为割。类似地，由于 $A[\{2,3,4,5\}]$ 与 A_2 以 $\{2,5\}$ 为割，$A[[5]]$也以 $\{2,5\}$ 为割。令 $C=\mathrm{ct}(A,\{2,5\})$。由引理 6.5，$\{1,5\}\Delta\{2,5\}=\{1,2\}$是 C PME $=A$ 的一个割。这意味着 $C[\{1,2,3,5\}]$ PME$=A_3$ 并以 $\{1,2\}$ 为割。因此，$\{\{1,2\},\{3,5\}\}$ 也满足性质 $\mathcal{P}$。

6.1.3 引理6.2 的证明

一个方向显而易见。若 S 是矩阵 C 的某个矩阵切割 PME $=A$，那么 S 也是一个合理集合。现在我们证明另一个方向。假设 S 是某个合理集合。若不存在另一个合理集合 S，我们称其为极小的；如果存在另一个合理集合 S' 是 S的真子集。我们分三步证明引理 6.2。首先证明大小为二的合理集合成立，然后证明极小合理集合成立，最后证明任意合理集合成立。

S 大小为二。 假设 S 是 A 的一个大小为 2 的合理集合。如下在 $[n]\setminus S$ 上定义二元关系 $\sim$：

$$e\sim f \iff e=f \text{ or } A[S\cup\{e,f\}] \text{ has cut } S.$$

我们看到，$\sim$是 $[n]\setminus S$ 上的等价关系：

- $e \sim e$ 作为$e = e$.
- $e \sim f \iff f \sim e$。
- 如果 S 同时是 A[S $\cup$ {e, f }] 和 A[S $\cup$ { f , g}] 的割，那么根据观察 6.2，S 也必定是 A[S $\cup$ { e, g}] 的割，因此 e $\sim$ f $\wedge$ f $\sim$ g $\implies$ e $\sim$ g。

对于所有 $e \in [n]\setminus S$，令 T_e 为 e 的等价类，并令 $T_e = ([n]\setminus S)\setminus T_e$。

在证明以下断言之前，我们先讨论它如何蕴含存在一个矩阵 C PME = A，使 S $=$ {s_1,s_2} 作为割。该断言指出，要么 A 有割 S，要么对于所有 e $\in$ [n] $-$ S，{s_1} $\cup$ T_e 和 {s_2} $\cup$ T_e 都是割。在前一种情形下，C $=$ A。在后一种情形下，C $=$ ct(A, {s_1} $\cup$ T_e)。根据引理 6.5，({s_1} $\cup$ T_e)Δ({s_2} $\cup$ T_e) $=$ S 是 C 的一个割。

断言 6.1。 给定一个具有非零非对角元的 $n \times n$ 矩阵 A，假设 $S = \{s_1,s_2\}$ 是 A 的合理集合。那么，S 要么是 A 的一个割，要么对于所有 $e \in [n]\setminus S$，$\{s_1\} \cup T_e$ 和 $\{s_2\} \cup T_e$ 都是 A 的割。

证明。 我们对n使用归纳法。不失一般性，假设$S = \{1,2\}$。如果$n = 4$，则分两种情形：

1. 如果 $3 \sim 4$，那么 $\{1,2\}$ 是A的一个割。
2. 如果 $3 \not\sim 4$，那么根据观察 6.4，$\{1,3\}$、$\{2,3\}$、$\{1,4\}$ 和 $\{2,4\}$ 都是A的割。

现在我们处理$n \geq 5$的归纳情形。

断言 6.2。 若对于某个 $e \in [n]\setminus\{1,2\}$, $|T_e| \geq 2$，则 $\{1\} \cup T_e$ 和 $\{2\} \cup T_e$ 都是 A 的割。

证明。 对于每个$f \in T_e$，注意到 $\{1,2\}$ 仍是$A[[n]-f]$ 的合理集合；并且由于$f \in T_e$，T_e对于$A[[n]-f]$ 也保持不变。由归纳法，以下两种情况之一成立：

1. $\{1,2\}$ 是$A[[n]-f]$的割。
2. $\{1\} \cup T_e$ 和 $\{2\} \cup T_e$ 都是$A[[n]-f]$的割。

令 { f , g} $\subseteq$ T_e。现在证明对于任何 h $\in$ T_e，条目 1 都不可能成立；假设 {1,2} 是 A[[n] $-$ h]的割。不失一般性，令 h $\neq$ g。则 {1,2} 将是 A[{1, 2, e, g}]中的割，这与 g $\in$ T_e这一事实矛盾。因此，{1} $\cup$ T_e 和 {2} $\cup$ T_e 分别是 A[[n] $-$ f] 和 A[[n] $-$ g], 的割，从而 {1} $\cup$ T_e 和 {2} $\cup$ T_e 都是 A 的割。

□

若存在 $e \in [n]\setminus\{1,2\}$ 使得 $|T_e| = 0$，则对于所有$f \in [n]\setminus\{1,2,e\}$，$A[\{1,2,e,f\}]$ 都是割 $\{1,2\}$。因此，$\{1,2\}$ 是A中的一个割。现在假设对于所有$e \in [n]\setminus\{1,2\}$，$|T_e| \geq 1$。那么对于每个$e \in [n]\setminus\{1,2\}$,

1. 若 $|T_e| \geq 2$，则根据断言 6.2，$\{1\} \cup T_e$ 和 $\{2\} \cup T_e$ 都是A的割。
2. 如果 $|T_e| = 1$，令 T_e = { f }。那么 T f $=$ T_e = [n] $\setminus$ {1, 2, f } 且 $|T_f|$ = n $-$ 3 $\geq$ 2。由于 T_f = { f }，根据断言 6.2，{1, f } 和 {2, f } 都是 A 的割，这意味着 {1} $\cup$ T_e 和 {2} $\cup$ T_e都是 A 的割。

□

S 是极小的。现在，我们通过对 n 归纳，证明引理 6.2 对极小可信集合成立。由于 4×4 矩阵的任意可信集合大小为 2，因此 $n = 4$ 的基例已经证明。假设该引理对大小为 $< n$ 的矩阵的极小可信集合成立。设 A 是一个大小为 n 且具有非零非对角元的矩阵，并且有一个极小可信集合 S。由于我们已经证明了 $|S| = 2$ 的情形，不失一般性，我们可以假设 $|S| > 2$。在下面的断言中，我们证明，如果 $|S| > 2$，那么对于每个 $e \in S$，S 仍然是 $A[[n] - e]$ 的极小可信集合。根据归纳假设，对于每个 $e \in S$，S 都是某个矩阵 C_e PME= $A[[n] - e]$ 的割。根据断言 6.3，S 是 $A[[n] - e]$，的极小可信集合，因此它也是 C_e 的极小可信集合。根据归纳假设，S 是 C_e 的一个割。注意，极小可信集合必然对应极小割，这意味着 S 是 C_e 的一个极小割。由于 C_e PME= $A[[n] - e]$ 且 S 的大小为 > 2，根据引理 5.8，S 也是 $A[[n] - e]$ 的一个割。由于 $|S| > 2$，并且对于每个 $e \in S$，$A[[n] - e]$ 都有割 S，因此 S 也是 A 的一个割。事实上，S 是 A 的一个极小割。

断言 6.3。 设 A 是一个具有性质 $\mathcal{R}$ 的 $n \times n$ 矩阵，S 是 A 的一个满足 $|S| > 2$ 的极小可信集。设 $e \in S$。则，S 也是 $A[[n] - e]$ 的一个极小可信集。

证明。显然，S 是 $A[[n] - e]$ 的一个合理集合。假设 S 不是 $A[[n] - e]$ 的极小集合，并且存在某个 $X \subset S$，使其成为 $A[[n] - e]$ 的一个合理集合。由于 X 不是 A 的合理集合，且是 S 的子集，因此必定存在某些 $\{i, j\} \subseteq X$、$l \in S \setminus X$，使得 $\{\{i, j\}, \{l, e\}\}$ 不满足性质$\mathcal{P}$。令 $k \in S - e$。由于 S 是 A 的一个合理集合，$\{i, j\} \subseteq X \subset S$ 且 $k, e \in S$，因此 $\{\{i, j\}, \{k, e\}\}$ 满足性质 $\mathcal{P}$。同样地，由于 X 是 $A[[n] - e]$，的一个合理集合，且 $\{k, l\} \subset X - e$，因此 $\{\{i, j\}, \{k, l\}\}$ 满足性质 $\mathcal{P}$。由于 A 满足性质 $\mathcal{R}$，根据引理 6.1，$\{\{i, j\}, \{l, e\}\}$ 也必须满足性质 $\mathcal{P}$，这就产生了矛盾。因此，S 是 $A[[n] - e]$ 的一个极小可信集。

□

General S. 首先，我们陈述一个来自 [CGGR25 的结果，即引理 3。4] 然后证明引理 6.7，稍后会在证明中用到它。

引理 6.6. 设 A 是域 F 上的一个 $n \times n$ 矩阵，且其非零非对角元均非零。设 $X \subseteq [n]$ 是矩阵 A 的一个割，且 $s \in X$，并假设 $Y \subseteq X$ 是 $A[X + s]$ 中的一个割。那么，Y 也是矩阵 A 的一个割。

引理 6.7. 设 A 是一个非零非对角元均非零的 $n \times n$ 矩阵，且 S 是 A 的一个割。设 $s \in S$，$t \in S$，M 和 N 是两个矩阵，满足 $M \text{ PME} = A[S + t]$，且 $A[s + S] \text{ PME} = N$。那么，按如下方式定义的矩阵 A' 与 A 是 PME。

$$A' = \begin{array}{c} \\ S \\ \overline{S} \end{array} \begin{array}{c} \begin{array}{cc} S & \overline{S} \end{array} \\ \begin{pmatrix} M[S] & M[S,t] \cdot \frac{N[s,\overline{S}]}{N[s,t]} \\ \frac{N[\overline{S},s]}{N[t,s]} \cdot M[t,S] & N[\overline{S}] \end{pmatrix} \end{array}.$$

证明。 注意，$A'[S + t] = M$，因此$A[S + t] \text{ PME} = A'[S + t$<v34>。现在，我们证明$A'[s + S]$ 与 N对角相似。具体而言，我们断言$A'[s + S] = DND^{-1}$，其中

$$D[e, e] = \begin{cases} \frac{M[s,t]}{N[s,t]} & \text{if } e = s \\ 1 & \text{if } e \in \overline{S} \end{cases}.$$

根据构造，很容易验证$DND^{-1}[p, q] = A'[p, q]$ 对每个$p \in s + S$,$q \in S$都成立。剩下的只需验证对应于索引s的列。根据主子式

等价性，对于$A[s,t], M[s,t]$和$N[s,t],$，我们有$A[s] = N[s] = M[s]$以及$A[t] = N[t] = M[t],$，由此可推知

$$A[s,t]A[t,s] = M[s,t]M[t,s] = N[s,t]N[t,s].$$

注意，由于 $A[s,t]A[t,s]$ 非零，因此 $N[s,t], N[t,s], M[s,t],$ 和 $M[t,s]$ 也都必定非零。现在，对于 $e \in S$

$$A'[e,s] = \frac{N[e,s]M[t,s]}{N[t,s]} = \frac{N[e,s]N[s,t]}{M[s,t]} = N[e,s]\frac{D[e,e]}{D[s,s]}.$$

由于 S 是 A 和 A′ 的公共割，根据引理 5.7，A[S + t] PME= A′[S + t]，且 A[s + S] PME= A′[s +S],。因此，A $\overset{\text{PME}}{=}$ A′。

□

现在，我们回到一般合理集合 S 的证明。我们对 n 进行归纳证明。n = 4 的基例显然成立，因为 S 只能是大小为 2 的合理集合。假设对于任意大小为 < n、其中 n ≥ 5 的矩阵，结论都成立。设 A 是一个大小为 n 且具有性质 $\mathcal{R}$ 的矩阵，S 是 A 的一个合理集合。若 S 是极小可信集，那么根据前面的讨论，S 确实是某个矩阵 C PME = A 的割。假设 S 不是极小可信集，且存在一个极小可信集 X，它是 S 的子集。这意味着存在一个矩阵 C PME = A，使得 X 是一个割。设 s ∈ X。注意，S 是 A[s + X] 的合理集合，因此也是 C[s + X] 的合理集合。根据归纳假设，存在某个 N PME = C[s + X]，其割为 S。设 t ∈ S \ X，且 M = C[X + t]。设 C′ 为引理 6.7 中的矩阵，它与 C DE，因此也与 A DE。根据 C′ 的构造，X 是 C′ 的一个割，且 C′[s+ X] 与 N 对角相似。由于 N 的割是 S，C′[s + X] 也有割 S，而 S 是 X 的子集。因此，根据引理 6.6，S（因而 S）是 C′ 的一个割，且 C′ PME A。证明完毕。

具有性质 $\mathcal{R}$的矩阵的 PMAP：定理1.4的证明

本小节证明定理 1.4。具体而言，我们设计一种算法：给定一个具有性质 $\mathcal{R}$ 的$n \times n$ 矩阵 A 的主子式作为访问权限，该算法能在 poly(n) 时间内输出一个矩阵 $B \in \mathbb{F}^{n\times n}$，使得 A 与 PME 等价 $= B$。我们首先正式定义主子式预言机。

定义 7.1（主子式预言机）。设 A 是域 $\mathbb{F}$ 上的一个 $n \times n$ 矩阵。那么，PM_A 表示矩阵 A 的主子式预言机，也就是说，对于输入 PM_A 的任意非空子集 $S \subseteq [n]$，它会输出 $\det(A[S])$。

以下引理指出，给定对预言机 PM_A 的访问权限后，可以非常高效地完成一些任务。

引理 7.1。设 A 是 $\mathbb{F}$ 上的一个 $n \times n$ 矩阵。那么，以下结论成立。

1. 对于任意 $i \in [n], A[i, i]$ 可以通过向预言机 PM_A进行一次查询来计算。*2.* 对于任意 $\{i, j\} \subseteq [n], A[i, j]A[j, i]$，可以通过向预言机 PM_A进行三次查询来计算。*3.* 对于任意 $\{i, j, k\} \subseteq [n], A[i, j]A[j, k]A[k, i] + A[i, k]A[k, j]A[j, i]$，可以通过向 PM_A进行七次查询来计算。

证明。 对于所有 $i \in [n]$,，我们通过在输入为 $\{i\}$ 时向 PM_A 发起查询，得到 $A[i,i]$。对于每个 $\{i、j\} \subseteq [n]$,

$$A[i,j]A[j,i] = A[i,i]A[j,j] - \det(A[\{i,j\}]).$$

因此，可以通过在输入 $\{i\}, \{j\}$ 和 $\{i, j\}$ 上查询 PM_A，计算 $A[i, j]A[j, i]$。对于每个$\{i、j、k\}\subseteq[n]$

$$\begin{aligned} A[i,j]A[j,k]A[k,i] + A[i,k]A[k,j]A[j,i] = \det(A[\{i,j,k\}]) - \det(A[\{i,j\}])A[k,k] \\ - \det(A[\{j,k\}])A[i,i] - \det(A[\{i,k\}])A[j,j] \\ + 2A[i,i]A[j,j]A[k,k] \end{aligned}$$

因此，我们可以计算 $A[i, j]A[j, k]A[k, i] + A[i, k]A[k, j]A[j, i]$，只需向 PM_A进行七次查询。 □

我们沿用第6节开头定义的记号。本节安排如下：在第7.1节中，给定对具有非零非对角元的 4×4 矩阵 A 的主子式的访问权限，我们描述如何计算该 $\mathcal{S}_A$族。它将在本节的其他算法中使用。我们将具有性质 $\mathcal{R}$ 的矩阵的学习问题约化为具有性质 $\mathcal{R}$ 且无割的矩阵的学习问题。相应的算法将在第7.2节介绍。最后，在第7.3节中，我们描述具有性质 $\mathcal{R}$的矩阵的完整学习算法。

7.1 4×4 矩阵的重构

我们先介绍以下观察，它给出了计算主子式等价的 4×4 矩阵的过程。

观察 7.1。 设 A 是域 F 上一个非零非对角元均非零的 *4×4* 矩阵。那么，对于任意 *4×4* 矩阵 B, $A \equiv_{PME} B$，当且仅当 $A[i, i] = B[i, i]$ 对 $i = 1, 2$ 及

$$B[1,2]B[2,1] = A[1,1]A[2,2] - \det(A).$$

现在我们聚焦于主子式等价的 4×4 矩阵的学习。设 A 是一个非零非对角元均非零的 4×4 矩阵。根据观察 2.2 和观察 2.3，存在一个 4×4 矩阵 B，使得 $B \equiv_{PME} A$ 且 $B[1,2] = B[1,3] = 1$。下一个引理给出了一种计算这类主子式等价矩阵的方法。

引理 7.2。 设 A 是域 F 上一个非零非对角元均非零的 *4×4* 矩阵。那么，对于任意满足 $B[1,2] = B[1,3] = 1$ 的 *4×4* 矩阵 B，$A \equiv_{PME} B$，当且仅当满足以下条件：

1. $B[i, i] = A[i, i]$ 适用于$i = 1, 2, 3$,
2. $B[j, 1] = A[1, j]A[j, 1]$ 对于 $j = 2, 3$,
3. $B[2, 3]$ 是二次多项式 $az^2 - bz + c$ 的一个根，其中

$$a = A[1,3]A[3,1], \quad b = A[1,2]A[2,3]A[3,1] + A[1,3]A[3,2]A[2,1], \text{ and}$$

$$c = A[1,2]A[2,1]A[2,3]A[3,2],$$

4. $B[3,2] = A_{[2,3]}\underline{A_{[3,2]}\ B_{[2,3]}}$。

证明。 我们先假设$B \overset{\text{PME}}{=} A$。接着，

$$A[i,i] = B[i,i] \text{ for } i = 1,2,3 \tag{20}$$
$$\det(A[\{i,j\}]) = \det(B[\{i,j\}]) \text{ for } \{i,j\} \subseteq \{1,2,3\} \tag{21}$$
$$\det(A) = \det(B) \tag{22}$$

由方程 (20) 和方程 (21)，我们得到，对所有 $\{i, j\} \subset \{1,2,3\}$，

$$A[i,j]A[j,i] = B[i,j]B[j,i].$$

此外，由于$B[1,2] = B[1,3] = 1$，$B[2,1] = A[1,2]A[2,1]$且$B[3,1] = A[1,3]A[3,1]$。结合方程 (22)，可得

$$\begin{aligned} 0 &= A[1,2]A[2,3]A[3,1] + A[1,3]A[3,2]A[3,1] - B[1,2]B[2,3]B[3,1] - B[1,3]B[3,2]B[2,1] \\ &= A[1,2]A[2,3]A[3,1] + A[1,3]A[3,2]A[3,1] - B[2,3]A[1,3]A[3,1] - \frac{A[2,3]A[3,2]A[1,2]A[2,1]}{B[2,3]} \end{aligned}$$

这意味着$B[2,3]$是方程$az^2 - bz + c$的根，并且根据方程 (21)，$B[3,2] = \frac{A[2,3]A[3,2]}{B[2,3]}$。对于逆向，$B$是一个矩阵，且$B[1,2] = B[1,3] = 1$。此外，

$$B[i,i] = A[i,i] \; \forall i \in \{1,2,3\} \text{ and } B[i,j]B[j,i] = A[i,j]A[j,i] \text{ for } \{i,j\} \subseteq \{1,2,3\}.$$

因此，$\text{PME}(A, B, 2)$。由于A的非对角元均非零，$c \neq 0$。此外，$B[2,3]$是$az^2 - bz + c$的一个根。因此，$B[2,3]$非零。另外，

$$aB[2,3]^2 - bB[2,3] + c = 0.$$

因此，

$$\begin{aligned} b &= (A[1,3]A[3,1])\, B[2,3] + \frac{A[1,2]A[2,1]A[2,3]A[2,3]}{B[2,3]} \\ &= B[2,3]B[3,1] + B[3,2]B[2,1] \qquad (\because\ A[i,j]A[j,i] = B[i,j]B[j,i]) \\ &= B[1,2]B[2,3]B[3,1] + B[1,3]B[3,2]B[2,1] \qquad (\because\ B[1,2] = B[1,3] = 1) \end{aligned}$$

证明至此完成。 □

接下来，我们考虑这样一个问题：计算所有与给定 4×4 矩阵主子式等价的矩阵。假设$A \in \mathbb{F}^{4\times 4}$的非零非对角元均非零，并且我们可以获得它的所有主子式。我们的目标是构造一个矩阵族，使得对于每个满足C $C \overset{\text{PME}}{=} A$的矩阵，该矩阵族都包含一个与$C$对角相似的矩阵。算法6给出了完成这项任务的算法，引理7.3 证明了该算法的正确性。

算法 6 4×4 主子式等价矩阵的重构

输入： 访问预言机PM_A 对于某个矩阵$A \in \mathbb{F}^{4\times 4}$，其非对角元均非零**输出：** 族 $\mathcal{S}_A$（定义见第6节）**假设：** 可使用域 $\mathbb{F}$ 上二次一元多项式的求根算法。1：对于每个 $\{i、j\} \subseteq \{2,3,4\}$，其中 $i < j$，计算一元多项式

$$E_{i,j}(z) = a_{i,j}z^2 - b_{i,j}z + c_{i,j} \tag{23}$$

使得

- $aij = A[1,j]A[j,1]$
- $bi,\ j = A[1,i]A[i,\ ]A[j,\ 1] + A[1,j]A[j,\ i]A[i,\ 1]$
- $ci,\ j = A[1,i]A[i,\ 1]A[i,\ j]A[j,\ i]$

2：对于每个 $\{i,\ j\} \subseteq \{2,3,4\}$，计算多项式 $Ei,\ j(z)$ 的根集 $Ri,\ j$。3：$\mathcal{T} \leftarrow \emptyset$

4：对于每个$(r_1,r_2,r_3) \in R_{2,3} \times R_{2,4} \times R_{3,4}$，执行以下操作：

i）构造一个 4×4 矩阵B 使得

- $B[i,i] \leftarrow A[i,i]$ for all $i \in \{1,2,3,4\}$
- $B[1,j] \leftarrow 1$ for $j = 2,3,4$,
- $B[2,3] = r_1$, $B[2,4] = r_2$ and $B[3,4] = r_3$
- for $\{i,j\} \subseteq \{1,2,3,4\}$ with $i < j$, $B[j,i] \leftarrow \frac{A[i,j]A[j,i]}{B[i,j]}$

ii）如果$A_{\text{PME}} = B$，则$B\}$

5：输出 $\mathcal{T}$

引理 7.3。 设A 是一个 4×4 非零非对角元矩阵。那么，给定对PM_A的预言机访问，算法 6会在 $\mathcal{S}_A$ 上通过常数次运算输出集合 $\mathbb{F}$。

证明。 设$B \in \mathbb{F}^{4\times 4}$ 是一个矩阵，使得$A_{\text{PME}} = B$。那么B 的非对角元必须非零。否则，对于任意 $B[i,j] = 0$，可以证明以下情况必有一种成立：

$1.A[i,\ i] \neq B[i,\ i]2.A[j,\ j] \neq$
$B[j,\ j]3.\det(A[\{i,\ j\}]) \neq$
$\det(B[\{i,\ j\}])$

上述任何一种情况都会与假设 $A_{\text{PME}} = B$ 矛盾。

根据观察 2.2，不妨设 $B[1,j] = 1$ 对 $j = 2,\ 3,\ 4$成立。现在证明 $B \in \mathcal{S}_A$。

根据引理 7.2，对于每个 $\{\mathrm{i,j}\} \subseteq \{2,3,4\}$（其中 $\mathrm{i} < \mathrm{j}$），$\mathrm{B[i,j]}$ 是方程（23）的一个根，而 $\mathrm{B[j,i]} = \mathrm{A[i,j]A[j,i]}\ \mathrm{B[i,j]}$。因此，$\mathrm{B} \in \mathcal{S}_A$。此外，根据引理 7.1，我们只需向预言机 PM_A发起常数次查询即可计算方程（23）。

时间复杂度可直接从算法的描述中得出。 □

7.2 具有性质 $\mathcal{R}$ 且无割的矩阵的 PMAP

在本小节中，我们将介绍针对具有 $\mathcal{R}$ 性质且无割的矩阵的学习算法。算法的详细说明见算法 7。输入包括索引

集合 I、对预言机 PM_A的访问权限，以及族 $\mathcal{F}_A$（定义见第 6 节开头）。目标是输出一个矩阵 B，使得 $B^{\text{PME}} = A$。注意，如果我们只能访问 PM_A，那么根据引理 7.3，可以计算出族 $\mathcal{F}_A$。然而，由于该算法在算法 9中用作子程序，且届时族已经计算出来，因此我们将其作为输入的一部分，以避免重复计算。

7.2.1 算法7的正确性

算法 7 调用算法 8 作为关键子程序。因此，我们首先证明算法8的正确性。

算法 8的正确性。 算法 8 的输入包含以下部分：

1. 一个有限集合 I，其中 $|I| \geq 42$. 对某个矩阵 A 的族 $\mathcal{F}_A$，其行和列由I索引，其中A 满足性质 $\mathcal{R}$ 且无割；3. 两个元素r、$s \in I$。

令 $|I| = n$。算法8调用递归过程 Finding-no-cut-sequence，其输入为$(I、\mathcal{F}_A、r、s)$，并输出序列 $\mathcal{X} = (i_n、i_{n-1}、i_{n-2}、\ldots\ldots、i_3)$。对于所有$j \in \{3,4,5,\ldots\ldots、n\}$，令$I_j = \{r、s、i_3,\ldots\ldots、i_j\}$。那么，输出序列 $\mathcal{X}$满足以下性质。

断言 7.1。 将 $(I, \mathcal{F}_A, r, s)$ 作为 *Finding-no-cut-sequence* 的输入，它会返回一个序列

$$\mathcal{X} = (i_n, i_{n-1}, i_{n-2}, \ldots, i_3)$$

使得对于所有 $j \in \{4,5,6,\ldots,n-1\}$，$A[I_j]$ 均无割。

证明。我们对 $|\mathrm{I}|$ 进行归纳证明。由于矩阵 A 无割，基例 $|\mathrm{I}| = 4$ 显然成立。接下来，我们关注归纳步骤。设 I 为满足 $|\mathrm{I}| \geq 5$ 的输入集。由于输入 A 无割且满足性质 $\mathcal{R}$，根据推论 5.1，存在一个 $\mathrm{e} \in \mathrm{I} \setminus \{\mathrm{r}, \mathrm{s}\}$，使得 $\mathrm{A}[\mathrm{I} - \mathrm{e}]$ 无割。步骤 8 会找到这样的索引 e。由于 A 具有性质 $\mathcal{R}$，应用引理 5.1 可知，$\mathrm{A}[\mathrm{I} - \mathrm{e}]$ 也满足性质 $\mathcal{R}$。设 $(\mathrm{i}_{n-1}, \mathrm{i}_{n-2}, \ldots, \mathrm{i}_3)$ 为步骤 7 返回的序列。那么，根据归纳假设，对于所有 $\mathrm{j} \in \{4,5,6,\ldots,\mathrm{n}-1\}$，$\mathrm{A}[\mathrm{I}_j]$ 无割。令 $\mathrm{i}_n = \mathrm{e}$。于是，输出序列 $(\mathrm{i}_n, \mathrm{i}_{n-1}, \mathrm{i}_{n-2}, \ldots, \mathrm{i}_3)$ 满足性质 $\mathcal{R}$。 □

算法8的正确性7.1号断言直接可得。

算法7的正确性。算法7 可以使用以下输入：

1. 一个大小至少为 4 的集合I

2. 族 $\mathcal{F}_A$ 和预言机 PM_A，对应某个矩阵A，其行和列由A索引，其中A 没有割，并满足性质 $\mathcal{R}$。

根据观察2.2 和观察2.3，不失一般性，我们可以假设，对于所有$s \in I \setminus \{i_1\}$，都有$A[i_1,] = 1$，其中任取一个元素$i_1 \in I$，并在算法开始时固定。我们要证明算法7 会生成一个矩阵B，其行和列由I和A 索引，且$^{\text{PME}} = B$。此外，对于所有$s \in I \setminus \{i_1\}$，都有$B[i_1,s] = 1$。

算法 7具有性质 $\mathcal{R}$ 且无割的主子式等价矩阵的重构

输入： 集合 I 满足 $|I| \geq 4$；族 $\mathcal{F}_A$，以及对矩阵 $A \in \mathbb{F}^{n\times n}$的 PM_A 预言机的访问权限
其行和列由 I索引，其中 A 无割且满足性质 $\mathcal{R}$

输出： 矩阵 $B \in \mathbb{F}^{|I|\times|I|}$，使得 $A \,_{\mathrm{PME}} = B$

假设：</style}存在一个用于求解 $\mathbb{F}$ 上一元二次多项式的求根算法

1: 令$|I| = n$。任取两个元素 $i_1, i_2 \in I$。

2: 应用算法 8，输入为 $(I, \mathcal{F}_A, i_1, i_2)$，计算序列 $(i_n, i_{n-1}, \ldots, i_3)$。

3: 按如下方式构造输出矩阵 $B \in \mathbb{F}^{n\times n}$，其行和列由 I 索引：

4: $B[i_1, i_1] \leftarrow A[i_1, i_1]$, 和$B[i_2, i_2] \leftarrow \quad A[i_2, i_2]$

5: $B[i_1, i_2] \leftarrow 1$ 和 $B[i_2, i_1] \leftarrow A[i_1, i_2]A[i_2, i_1]$。

6: **对于** $j \leftarrow$ 3到 n **执行**

7: $B[i_j,\ i_j] \leftarrow A[i_j,\ i_j]$

8: $B[i_1, i_j] \leftarrow 1$ 以及$B[i_j,\ i_1] \leftarrow A[i_1, i_j]A[i_j,\ i_1]$

9: 令 $I_j = \{i_1, i_2, i_3, \ldots, i_j\}$.

10: 若$j = 3$，$k_3 \leftarrow i_2$, 否则，应用算法8，输入为（I_j，$\mathcal{F}_{A_I}$ $_j$, i_1, i_j),

11: 计算序列 $(k_j, k_{j-1}, \ldots, k_3)$。

12: **对于** $\ell \leftarrow$ 3到 j，**执行**

13: 设 $L_\ell = \{i_1, i_j,\ k_3, k_4, \ldots\ldots,\ k_\ell\}$

14: 令 $R_{j,\ell}$ 为多项式的根

$$az^2 - bz\ + c, \text{其中} \tag{24}$$

- $a = A[i_1, k_\ell]A[k_\ell, i_1]$,
- $b = A[i_1, i_j]A[i_j,\ k_\ell]A[k_\ell,\ i_1] + A[i_1, k_\ell]A[k_\ell,\ i_j]A[i_j,\ i_1]$, 和
- $c = A[i_1, i_j]A[i_j,\ i_1]A[i_j,\ k_\ell]A[k_\ell,\ i_j]$。

15: 令$B_1 \in \mathbb{F}^{|L_\ell|\times|L^\ell|}$ 为一个矩阵，使得

- $B_1[k_\ell$、$i_j]$ 和$B_1[i_j$、$k_\ell]$ 均为未知数，并且
- 其他元素与$B[L_\ell]$相同

16: 设$D_\ell \in \mathbb{F}^{|L_{\ell-1}|\times|L^{\ell-1}|}$ 为对角矩阵，使得

$$D_\ell[i_1, i_1] = 1 \text{ and } D[s, s] = B[s, i_1]\ \ \forall s \in L_{\ell-1} - i_1$$

17: 设$B_2 \in \mathbb{F}^{|L_\ell|\times|L^\ell|}$ 为另一个矩阵，满足

- $B_2[L_{\ell-1}] = D_\ell \cdot B[L_{\ell-1}]T \cdot D_\ell^{-1}$
- $B_2[k_\ell, i_j]$ 以及$B_2[i_j, k_\ell]$ 均为未知量，并且
- 其余元素与$B[L_\ell]$相同

18: **对于** $s \in \{1, 2\}$ 和 $\gamma \in R_{j,\ \ell}$ **执行**

19: $B_s[i_j,\ k_\ell] \leftarrow \gamma$ 和 $B_s[k_\ell,\ i_j] \leftarrow \frac{A[i_j,\ k_\ell]A[k_\ell,\ i_j]}{\gamma}$

20: **若** $\mathrm{PME}(A[L_\ell],\ B_s[L_\ell],\ 4)$ 成立，**则**

21: $B[L_\ell] \leftarrow B_s$

22: **退出**第18步的“for”循环

23: **结束 if**

24: **结束 for**

25: **结束 for**

26: **结束 for**

27: 输出B

算法 8 寻找满足无割性质的指标序列 输入：集合 I，满足 $|\mathbf{I}| \geq 4$；族 $\mathcal{F}_A$，其中某个行和列均由 I 标记的矩阵 A 满足性质 $\mathcal{R}$ 且无割；两个元素 r、s $\in$ I。输出：序列 $(\mathbf{i}_{|I|}, \mathbf{i}_{|I|-1}, \ldots, \mathbf{i}_3)$，使得所有 $\mathbf{i}_j$ 都是 I $\setminus$ {r、s} 且 j $\in$ {4, 5, . . . , |I|}中的互不相同的元素，子矩阵 $\mathbf{A}[\mathbf{I}_j]$ 无割，其中 $\mathbf{I}_j = \{$r、s、$\mathbf{i}_3, \ldots, \mathbf{i}_j\}$。1：返回 Finding-no-cut-sequence(I, $\mathcal{F}_A$, r, s) 2：函数 Finding-no-cut-sequence(I, $\mathcal{F}_A$, r, s) 3：如果 $|\mathbf{I}| = 4$，则 4：令 {i, j} = I $\setminus$ {r、s}。然后，返回 (i, j) 5：否则 6：对于所有 i $\in$ I $\setminus$ {r、s}，使用算法 5，以 $(\mathbf{I} - \mathbf{i}, \mathcal{F}_{A[I-i]})$ 为输入，找到一个 e $\in$ I $\setminus$ {r、s}，使得 $\mathbf{A}[\mathbf{I} - \mathbf{e}]$ 无割。7：$\mathcal{X} \leftarrow$ Finding-no-cut-sequence(I $-$e, $\mathcal{F}_{A[I-e]}$, r, s) 8：返回 (e, $\mathcal{X}$)。9：结束 if 10：结束函数

设 $(\mathbf{i}_n, \mathbf{i}_{n-1}, \mathbf{i}_{n-2}, \ldots, \mathbf{i}_3)$ 为步骤 2 生成的序列。对于所有 j $\in$ [n],，令 $\mathbf{I}_i$ 表示集合$\{\mathbf{i}_1, \mathbf{i}_2, \ldots, \mathbf{i}_j\}$。根据断言 7.1，对于所有 j $\in \{4, 5, 6, \ldots, \mathbf{n}\}$，子矩阵 $\mathbf{A}[\mathbf{I}_j]$ 无割。注意，对于每个 j $\in \{3, 4, 5, \ldots, \mathbf{n}\}$，在步骤 6 的“for”循环第 j 次迭代开始时，子矩阵 $\mathbf{B}[\mathbf{I}_{j-1}]$ 的所有元素都已知。我们的目标是证明步骤 6 满足以下循环不变式。

$$\forall j \in \{2, 3, 4, \ldots, n\},\ B[I_j] \overset{\text{PME}}{=} A[I_j] \text{ and } B[i_1, i_j] = 1. \tag{25}$$

这将立即推出，在第 n 次迭代后，我们得到所需的输出矩阵 B，也就是说，$B =_{\text{PME}} A$ 且$B[i_1,s] = 1$ 对于所有$s \in I \setminus \{i_1\}$。

我们证明式（25）中的不变式，通过对 j 使用归纳法。基例 $j = 2$ 由观察 7.1 得出。此外，通过应用引理 7.1，我们可以计算 $B[i_2,i_1]$，所用预言机为 PM_A。

我们现在证明归纳步骤。由归纳假设，对每个 j > 2，我们得到 $\mathbf{B}[\mathbf{I}_{j-1}]$ PME= $\mathbf{A}[\mathbf{I}_{j-1}]$，并且对所有 s $\in \mathbf{I}_{j-1} \setminus \{\mathbf{i}_1\}$ 有 $\mathbf{B}[\mathbf{i}_1,\mathbf{s}] = 1$。注意，最初，$\mathbf{B}[\mathbf{I}_j]$ 中除由 $\mathbf{i}_j$ 索引的行和列中的那些元素外，所有元素都是已知的。由引理 7.1，$\mathbf{A}[\mathbf{i}_j, \mathbf{i}_j]$ 可利用预言机 PM_A 计算得到。我们令 $\mathbf{B}[\mathbf{i}_j, \mathbf{i}_j] = \mathbf{A}[\mathbf{i}_j, \mathbf{i}_j]$。随后，我们以迭代方式计算 $\mathbf{B}[\mathbf{I}_j]$ 中其余未知元素。

由于 A 满足性质 $\mathcal{R}$，由引理 5.1，$\mathbf{A}[\mathbf{I}_j]$ 也满足性质 $\mathcal{R}$。此外，$\mathbf{A}[\mathbf{I}_j]$ 无割。因此，由断言 7.1，序列 $(\mathbf{k}_j, \mathbf{k}_{j-1}, \ldots, \mathbf{k}_3)$ 满足如下性质：对所有 $\ell \in \{3, 4, 5, \ldots, \mathbf{j}\}$，$\mathbf{A}[\mathbf{L}_\ell]$ 无割，其中 $\mathbf{L}_\ell = \{\mathbf{i}_1, \mathbf{i}_j, \mathbf{k}_3, \mathbf{k}_4, \ldots, \mathbf{k}_\ell\}$。令 $\mathbf{L}_2 = \{\mathbf{i}_1,\mathbf{i}_j\}$。接下来，我们证明步骤 12 处的 ‘for’ 循环所满足的如下循环不变式。

命题 7.2。 对于所有 $\ell \in \{2, 3, 4, \ldots, j\}$，$A[L_\ell] \text{ PME}= B[L_\ell]$

我们将推迟证明上述断言，并在假设该断言成立的前提下完成归纳步骤。具体而言，我们旨在证明 $\mathbf{A}[\mathbf{I}_j]$ 无割，且 $\mathbf{B}[\mathbf{i}_1,\mathbf{i}_j] = 1$。注意到 $\mathbf{L}_j = \mathbf{I}_j$。因此，根据命题 7.2，我们立即得到 $\mathbf{A}[\mathbf{I}_j]$ PME= $\mathbf{B}[\mathbf{I}_j]$。此外，我们稍后将证明，对于某个 s $\in \{1, 2\}$ and $\gamma \in \mathbf{R}_{j,\ell}$，步骤21必须执行。因此，根据 $\mathbf{B}_1$ 和 $\mathbf{B}_2$, 的定义，我们有 $\mathbf{B}[\mathbf{i}_1,\mathbf{i}_j] = 1$。

命题的证明7.2。 我们对 ℓ 使用归纳法进行证明。基例 $\ell = 2$ 由观察7.1得出。假设对于某个 $\ell > 2$, $A[L_{\ell-1}] \overset{\text{PME}}{=} B[L_{\ell-1}]$。接下来，我们要证明$A[L_\ell] \overset{\text{PME}}{=} B[L_\ell]$。

注意，$B[L_\ell]$的所有项（$B[ii$、$k_\ell]$ 和$B[k_\ell,i_j]$除外）均已知。引理7.1 保证我们可以通过对预言机24进行常数次查询来计算式（PM_A）。此外，利用现有的求根算法，可以计算出步骤R_j, ℓ 中的14 集合。

由于$A[I_{j-1}]$ 无割，且$B[I_{j-1}] \overset{\text{PME}}{=} A[I_{j-1}]$，根据引理2.3，

$$B[I_{j-1}] \overset{\text{DS}}{=} A[I_{j-1}], \text{ or } B[I_{j-1}] \overset{\text{DS}}{=} A^T[I_{j-1}].$$

由于 $\text{A PME} = \text{A}^T$，预言机 PM_A 与 PM_{A^T}相同。因此，不失一般性，我们可以假设 $\text{B}[\text{I}_{j-1}]$ DS= $\text{A}[\text{I}_{j-1}]$。然后，由观察 2.2 可得 $\text{B}[\text{I}_{j-1}] = \text{A}[\text{I}_{j-1}]$。注意，$\text{L}_\ell$ –ij是 I^{j-1}的子集。因此，我们得到

$$B[L_\ell - i_j] = A[L_\ell - i_j]. \tag{26}$$

同样，由于$A[L_{\ell-1}]$ 无割，且$A[L_{\ell-1}] \overset{\text{PME}}{=} B[L_{\ell-1}]$，根据引理2.3，

$$B[L_{\ell-1}] \overset{\text{DS}}{=} A[L_{\ell-1}], \text{ or } B[L_{\ell-1}] \overset{\text{DS}}{=} A^T[L_{\ell-1}].$$

因此，根据观察2.2，我们得到

$$B[L_{\ell-1}] = A[L_{\ell-1}], \text{ or } B[L_{\ell-1}] = D_\ell \cdot A^T[L_{\ell-1}] \cdot D_\ell^{-1}, \tag{27}$$

其中 D_ℓ 在步骤 16中定义。接下来，我们将证明分为以下两种情形。

情形 I ($\text{B}[\text{L}_{\ell-1}] = \text{A}[\text{L}_{\ell-1}]$)。由式 (26) 和式 (27) 可知，$\text{B}[\text{L}_\ell]$ 的所有元素均已知，除了 $\text{B}[\text{i}i, \text{k}_\ell]$和 $\text{B}[\text{k}_\ell,\text{i}_j]$；更具体地说，这些已知元素等于 $\text{A}[\text{L}_\ell]$中的对应元素。因此，根据步骤 15 中的定义，

$$B_1[L_{\ell-1}] = A[L_{\ell-1}] \text{ and } B_1[L_\ell - i_j] = A[L_\ell - i_j].$$

根据引理 7.2，$\text{A}[\text{i}i, \text{k}_j]$ 是式 (24) 的一个根。因此，对于 $\text{s} = 1$ 和步骤 18 中的 $\gamma = \text{A}[\text{i}i, \text{k}_j]$，我们得到一个 $\text{B}[\text{L}_\ell]$，使得 $\text{PME}(\text{A}[\text{L}_\ell], \text{B}[\text{L}_\ell],4)$。由于 $\text{A}[\text{L}_\ell]$ 根据引理 5.1 满足性质 $\mathcal{R}$，应用定理 5.1 可得 $\text{A}[\text{L}_\ell]$ PME= $\text{B}[\text{L}_\ell]$。

情形 II（$B[L_{\ell-1}] = D_\ell \cdot A^T[L_{\ell-1}] \cdot D_\ell^{-1}$）。这意味着

$$A[L_{\ell-1}] = D_\ell \cdot B^T[L_{\ell-1}] D_\ell^{-1}.$$

因此，根据第17步中的定义，$B_2[L_{\ell-1}] = A[L_{\ell-1}]$。结合式（26），我们可以看到，除$B_2[ii$，$k_\ell]$ 和 $B_2[k_\ell$，$i_j]$之外，其余各项均与$A[L_\ell]$中的对应项相等。剩余证明与**情形 I**类似。

□

7.2.2 算法7的时间复杂度

在第2 步和10步中，算法 7调用算法 8。因此，我们先分析算法8的时间复杂度。

算法 8 调用递归函数 FINDING-NO-CUT-SEQUENCE。该函数至多对自身进行一次递归调用，且输入集的大小 I 每次递归调用都会减少一。并且，在

步骤 6 中，每次递归调用至多调用算法 5 |次，其中 |I| 是输入集。根据引理 6.3，每次调用的运行时间都是多项式。因此，算法 8 的总运行时间为 poly(|I|)。

现在分析算法 7 的时间复杂度。该算法本质上是迭代式的。步骤 2 调用算法8，其运行时间为多项式时间。在步骤 6 中，它执行一个“for”循环，最多循环 n 次，其中 n 是输入集 I 的基数。对于该循环的第 j 次迭代，算法7:

1. 在步骤 10 中，调用算法 8，输入集的大小至多为 j，其中 $j \geq 4$。

2. 在步骤 12 中，执行另一个“for”循环，最多循环 j 次。在该循环的每次迭代中，它从集合 $\{1,2\} \times R_{j,\ell}$ 中找出一个正确对 (s, γ)，并在步骤 18 中处理。借助预言机 PM_A，我们可以在步骤 20 中用多项式时间验证 $\mathrm{PME}(A[L_\ell], B[L_\ell], 4)$。因此，可以在多项式时间内找到正确对 (s, γ)。

算法的所有其余步骤也都可以在多项式时间内完成。因此，算法7 的总体运行时间为（n）ispoly。

7.3 具有性质 $\mathcal{R}$ 的矩阵的 PMAP：归约到无割情形

现在，我们给出一种算法，用于计算给定矩阵的主子式等价矩阵$A \in \mathbb{F}^{n\times}$，该矩阵满足性质 $\mathcal{R}$。作为输入，我们可以访问预言机PM_A（见定义7.1）。这是一种递归算法，它将具有性质 $\mathcal{R}$ 的矩阵的学习问题归约为具有性质 $\mathcal{R}$ 且具有无割的矩阵的学习问题。详细描述请参见算法9。

Algorithm 9 R经济 truction of matri情况下w ith 性质 ty $\mathcal{R}$

输入：可访问某个矩阵 A 的预言机 PM_A，其中 A 具有 $\mathcal{R}$ 性质。输出：矩阵 B，使得 B PME = A。假设：可用一个在 $\mathbb{F}$ 上求一元二次多项式根的算法。1：对于 $\mathbf{n} = 2, 3$，分别使用观察 7.1 和引理 7.2 重构 B。否则，执行以下操作。2：对于每个满足 $|\mathbf{I}| = 4$ 的 $\mathbf{I} \subseteq [\mathbf{n}]$，应用算法 6，计算 $\mathcal{S}_{A_I}$。因此，我们计算 $\mathcal{F}_A$。3：输出 Reconstruction([n])。4：函数 Reconstruction(I)。5：对于 $|\mathbf{I}| \geq 4$，以 $(\mathbf{I}, \mathcal{F}_{A[I]})$ 为输入应用算法 5，判断 A[I] 是否有割。若存在割，则令 $\mathbf{S} \subseteq \mathbf{I}$ 为算法 5 的输出。6：如果 A 无割，或者 $|\mathbf{I}| = 3$，那么：7：若 $|\mathbf{I}| = 3$，使用引理 7.2 重构 B $\in \mathbb{F}^{|I|\times|I|}$，使得 A[I] PME= B。8：否则，以 $(\mathbf{I}, \mathcal{F}_{A[I]}, \mathrm{PM}_A)$ 为输入使用算法 7，重构 B $\in \mathbb{F}^{|I|\times|I|}$，使得 $\mathbf{A} \overset{\text{PME}}{=} \mathbf{B}$。9：返回 B。10：否则：11：令 $\mathbf{s} \in \mathbf{S}$，$\mathbf{t} \in \mathbf{S} = \mathbf{I} \setminus \mathbf{S}$。12：$\mathbf{B}_1 \leftarrow$重构 $(\mathbf{S} + \mathbf{t})$。13：$\mathbf{B}_2 \leftarrow$重构$(\mathbf{S} + \mathbf{t})$。14：使用引理 6.7 合并 $\mathbf{B}_1, \mathbf{B}_2$，，并得到矩阵 B，使得 B PME = A。15：返回 B。16：结束 if。17：结束函数。

注 7.1。 关于算法 7 和算法 9，我们作如下两点说明 .

1. 在算法 *7* 和算法 *9* 中，对 PME_A 的每次查询都涉及一个大小至多为 *4* 的输入子集 S。换言之，只需查询阶数至多为 *4* 的主子式。 *2.* 根据注 *6.1* 的条目 *2*，我们可以假设，算法 *9* 的步骤 *5* 中得到的割 S 是某个满足 $C\,PME = A$ 的矩阵 C 的极小割。于是，根据 *[CGGR25* 的引理 *3.3]* 和引理 *5.8*，只要 $|S| > 2$，$A[S + t]$ 就无割。因此，我们可以跳过步骤 *12* 中的递归调用，直接调用算法 *7* 来得到矩阵 B_1。这样，算法 *9* 不再需要两次递归调用，只需一次调用即可。

7.3.1 算法9的正确性

该算法可以访问矩阵 A 的预言机 PME_A （见定义 7.1），其中 $\mathrm{A} \in \mathbb{F}^{n\times n}$满足性质 $\mathcal{R}$。算法输出一个 $\mathrm{n} \times \mathrm{n}$ 矩阵 B。我们希望证明 $\mathrm{B\ PME} = \mathrm{A}$。对于 $\mathrm{n} = 2$和 $\mathrm{n} = 3$，算法的正确性分别由观察 7.1 和引理 7.2 得出。通过反复应用算法 6，我们计算出族 $\mathcal{F}_A$。在步骤 3 中，算法对输入 [n]调用递归过程 Reconstruction。更一般地，对于任意 $\mathrm{I} \subseteq [\mathrm{n}]$ 且满足 $|\mathrm{I}| \geq 3$，Reconstruction(I) 满足以下条件。

断言 7.3。 设 $n \geq 3$ 为正整数，且 $I \subseteq [n]$ 的大小至少为3。给定输入 I，函数重构返回一个矩阵 $B \in \mathbb{F}^{|I|\times|I|}$，使得 $B_{\text{PME}} = A[I]$。

证明。 我们用归纳法证明。

基例（$|I| = 3$ 或 $A[I]$ 无割）。 对于 $|I| = 3$，由引理7.2，矩阵$B_{\text{PME}} = A[I]$。如果A 无割，则根据算法7，该算法确保$B_{\text{PME}} = A$。

归纳步骤（$|\mathrm{I}| \geq 4$和 $\mathrm{A[I]}$ 有割）。算法 9 的步骤 5 找到 $\mathrm{A[I]}$的一个割 $\mathrm{S} \subseteq \mathrm{I}$。设 $\mathrm{s} \in \mathrm{S}$，$\mathrm{t} \in \mathrm{S} = \mathrm{I} \setminus \mathrm{S}$。由于 $2 \leq |\mathrm{S}| \leq |\mathrm{I}| - 2$，$|\mathrm{S} + \mathrm{t}|$ 和 $|\mathrm{S} + \mathrm{s}|$ 的大小都至少为 3。于是，根据归纳假设，分别在步骤 12 和步骤 13 中构造的矩阵 $\mathrm{B}_1 \in \mathbb{F}^{|S+t|\times|S+t|}$ 和 $\mathrm{B}_2 \in \mathbb{F}^{|S+s|\times|S+s|}$ 满足 $\mathrm{B}_1\,\mathrm{PME}= \mathrm{A[S + t]}$ 和 $\mathrm{B}_2\,\mathrm{PME}= \mathrm{A[S + t]}$。接着，根据引理 6.7，该算法将 B_1 和 B_2, 合并，并返回满足 $\mathrm{B\ PME} = \mathrm{A[I]}$的矩阵。 □

上述声 称立即推出，算法*9*的输出矩阵B 满足$B_{\text{PME}} = A$.

7.3.2 算法9的时间复杂度

根据引理7.3，在步骤2中，族 $\mathcal{F}_A$ 可以在多项式(n) 时间内计算得出。之后，算法9调用递归函数重构。

在某次对重构的调用中，给定输入 $|I| \geq 4$，根据引理6.3，算法5 可在 $\mathrm{poly}(|I|)$时间内判断$A[I]$ 是否有割。此外，如果$A[I]$ 有割，它还会在相同的时间复杂度内返回一个割$S \subseteq I$。如果$A[I]$ 无割，则在步骤8中，算法7 可在 $\mathrm{poly}(|I|)$ 时间内计算出矩阵B。

在步骤12 和13中，重构会以$S + t$ 和$S + s$ 为输入递归调用自身，其中$S = I \setminus S$、$s \in S$ 以及$t \in S$。最后，根据引理6.7，步骤14 在 $\mathrm{poly}(|I|)$时间内合并B_1 和B_2 。因此，对于满足 $|I| = n$的输入I，重构的时间复杂度满足

$$T(n) = T(n_1) + T(n_2) + \mathrm{poly}(n), \text{ where } n_1 + n_2 = n + 2.$$

解出这一递归后，我们得到算法 9 的运行时间关于 nn呈多项式级。 .

8 PME 的 NC 算法：定理1.2的证明

在本小节中，我们给出一种 NC 算法，用于检验两个矩阵是否主子式等价，并证明定理 1.2。总体思路如下：给定两个输入矩阵 A 和B ，其大小为$n \times n$，我们设计一种 NC 归约，将检验$A \overset{\text{PME}}{=} B$是否成立的问题，转化为检验多项式多个矩阵对 (A',B') 是否主子式等价，其中A'满足性质 $\mathcal{R}$。

根据 [Csa76、BCP83], ，我们知道矩阵的行列式可以在 NC 复杂度类中计算。结合定理 1.3，这意味着可以在 NC 复杂度类中判定矩阵 A' 和 B'的主子式等价，其中 A' 满足 $\mathcal{R}$。因此，我们的归约给出了一个 NC 算法，用于判定一般矩阵 A 和 B的主子式等价性。

NC 归约通过以下步骤进行。

步骤 ***I***：我们执行一个 NC 归约，将判定两个任意矩阵是否主子式等价的问题，归约为至多 n 个输入矩阵对均为不可约矩阵的主子式等价判定实例。根据引理2.1，矩阵 A 和 B 主子式等价，当且仅当它们的极大不可约子矩阵定义了相同的指标集划分，且对应的主子矩阵彼此主子式等价。

在有向图中，我们可以在 NC 复杂度类中找到强连通分量 [GM88，CV89]。因此，利用观察 2.1，我们可以在 NC 复杂度类中找到输入矩阵的极大不可约子矩阵。如果两个矩阵的不可约分量的指标集不匹配，我们输出$_{\text{PME}}$，即 $A \neq B$。否则，我们并行检验每一对对应的极大不可约子矩阵的主子式等价。

步骤 ***II***：在此步骤中，我们在 NC 复杂度类中将输入的一对不可约矩阵 $(A，B)$ 变换为另一对 $(A'，B')$，使得 A' 的所有非对角元均为非零，并且

$$A \overset{\text{PME}}{=} B \iff A' \overset{\text{PME}}{=} B'.$$

详情请见小节 8.1。

步骤 ***III***：给定一对 $(A，B)$，其中 A 的所有非对角元均为非零，我们进一步在 NC 复杂度类中将其变换为另一对 $(A'，B')$，其中 A' 满足性质 $\mathcal{R}$，使得

$$A \overset{\text{PME}}{=} B \iff A' \overset{\text{PME}}{=} B'.$$

详情请参见小节 8.2

目前，我们还不知道如何通过 NC 算法直接从不可约矩阵 (A,B)构造出这样一对矩阵 (A',B')。如果有这样的过程，我们就可以完全跳过**步骤 II**。

接下来，我们将详细介绍**步骤 II** 和**步骤 III**。

8.1 确保非对角元非零

下面的引理确保上述过程中的**步骤 II**可以完成。

引理 8.1。设 M 和 N 是域 F 上的两个 $n \times n$ 不可约矩阵，且 Y =对角矩阵$(y_1,y_2,\ldots,y_n)$。那么，

1. $M \overset{\text{PME}}{=} N$ 当且仅当 $(M+Y)^{\text{adj}} \overset{\text{PME}}{=} (N+Y)^{\text{adj}}$。

2. 此外，如果 $|\mathbb{F}| \geq 10n^5$，我们可以在 *NC* 中找到一个对角矩阵 $D \in \mathbb{F}^{n\times n}$（等价地，对 Y 进行代入），使得 $M+D$ 和 $N+D$ 可逆，并且 $(M+D)^{\text{adj}}$ 和 $(N+D)^{\text{adj}}$ 具有非零非对角元。

注 8.1。当 $|\mathbb{F}| \leq 10n^5$，时，我们可以在 *NC* 中构造一个 $\mathbb{K}$ 的扩域 $\mathbb{F}$，使得 $|\mathbb{K}| > 10n^5$，并在该域上进行运算。

证明概要。引理的第一部分由 [HL84，引理 4]得出。第二部分源于以下观察： [CGGR25，断言 4。1] 中所述构造过程的所有步骤都可以在 NC 中实现。在有向图中寻找两个顶点之间的最短路径，以及进行 [HPR97]，行列式计算 [Csa76、 BCP83]，多项式插值与求值，都已有相应的 NC 算法。因此， [CGGR25，断言 4。1] 中的构造可以在 NC 中完成。

□

结合上述引理与 [CGGR25，引理 2.9]，可知对于一对 (A,B) 阶为$n \times n$ 的不可约矩阵，我们可以在 NC 复杂度类中计算出一个对角矩阵 $D \in \mathbb{F}^{n\times n}$，使得

$$A \overset{\text{PME}}{=} B \iff (A+D)^{\text{adj}} \overset{\text{PME}}{=} (B+D)^{\text{adj}}.$$

经过**步骤 II**后，$(A+D)^{\text{adj}}$ 和$(B+D)^{\text{adj}}$ 将作为输出矩阵。由于矩阵的行列式可在 NC 复杂度类中计算 [Csa76， BCP83]，给定D后，我们可以在 NC 复杂度类中计算$(A+D)^{\text{adj}}$和$(B+D)^{\text{adj}}$。

8.2 确保性质 $\mathcal{R}$

在**步骤 III**中，我们假设A 和B 是两个输入矩阵，且A 的所有非对角元均非零。现在我们讨论一种 NC 算法，用于计算一个对角矩阵D，使得$(A+D)^{\text{adj}}$和$(B+D)^{\text{adj}}$ 都满足性质 $\mathcal{R}$。

引理 8.2. 设 $n \geq 5$ 和 $\mathbb{F}$ 为一个规模足够大的域。设 $A,B \in \mathbb{F}^{n\times n}$ 为具有非零非对角元的可逆矩阵，且 $Y = \text{diag}(y_1,y_2,\ldots,y_n)$。则我们可以在 *NC* 复杂度类中找到一个对角矩阵 $D \in \mathbb{F}^{n\times n}$，使其具有以下性质。

1. $A+D$ 与 $B+D$ 均可逆。

2. $(A+D)^{\text{adj}}$ 与 $(B+D)^{\text{adj}}$ 具有非零非对角元。

3. 对于任意四个互不相同的元素 i，j，k，$\ell \in [n]$，$(A+D)^{\text{adj}}$ 与 $(B+D)^{\text{adj}}$ 均满足式 (7)（见断言 4.2）。

注 8.2. 更具体地说，我们要求底层域的大小大于 $10n^5$。如果 $|\mathbb{F}| \leq 10n^5$，我们在 *NC* 复杂度类中构造一个大小大于 $10n^5$，的域扩张 $\mathbb{K}$（$\mathbb{F}$ 的），并在$\mathbb{K}$上进行计算。

证明。由引理 8.1，我们可以在 NC 复杂度类中计算出一个对角矩阵 $D \in \mathbb{F}^{n\times n}$，使得该引理的前两个性质成立。也就是说，$A+\tilde{D}$ 与 $B+\tilde{D}$ 均可逆，且 $(A+\tilde{D})^{\text{adj}}$具有非零非对角元。接下来，我们着重满足第三个性质。设

$$\mathcal{T}_A = \left\{(S,T) \mid S,T \subset [n], |S| = |T| = 2,\ S \cap T = \emptyset,\ \text{rank}(A+Y)^{\text{adj}}[S,T] = 2\right\}.$$

我们考虑以下断言。

断言 8.1. 对于任意 $(S,T) \in \mathcal{T}_A$，我们可以在 *NC* 复杂度类中计算出一个对角矩阵 $A_{S,T} \in \mathbb{F}^{n\times n}$ 使得

$$\operatorname{rank}(A + A_{S,T})^{\mathrm{adj}}[S,T] = 2 \iff \operatorname{rank}(A+Y)^{\mathrm{adj}}[S,T] = 2.$$

我们将断言的证明推迟到本小节末尾。构造出对角矩阵$\tilde{D}$和$A_{S,T}$对于$(S,T) \in \mathcal{T}_A$之后，我们采用基于拉格朗日插值的标准技术，在 NC 复杂度类中计算出一个满足引理全部三个性质的单个矩阵D。有关这一步的细节，请参见 [CGGR25中的断言 4 的证明。1][2]。 □

现在我们描述断言8.1的证明。

断言*8.1*的证明。注意，$A + Y$ 是非奇异的。因此，应用 [Gan60第 21],中的雅可比恒等式

$$\det\left((A+Y)^{\mathrm{adj}}[S,T]\right) = 0 \iff \det\left((A+Y)[\overline{T},\overline{S}]\right) = 0.$$

不失一般性，令$S = \{1,2\}$和$T = \{3,4\}$。令$A = (a_{i,j})_{i,j\in[n]}$。于是，

$$A' = (A+Y)[\overline{T},\overline{S}] = \begin{pmatrix} a_{1,3} & a_{1,4} & a_{1,5} & \cdots & a_{1,n} \\ a_{2,3} & a_{2,4} & a_{2,5} & \cdots & a_{2,n} \\ a_{5,3} & a_{5,4} & a_{5,5}+y_5 & \cdots & a_{5,n} \\ \vdots & & & \ddots & \\ a_{n,3} & a_{n,4} & a_{n,5} & \cdots & a_{n,n}+y_n \end{pmatrix}$$

现在我们对A'进行一些列变换。注意，A'的行和列由 $[n-2]$索引。注意$a_{1,3} = A'[1,1] \neq 0$。对于每个$i \in \{2,3,\ldots n-2\}$，我们从A'的第i列中减去$A'[1,i]/A'[1,1]$ 倍的第一列。这样便会将A'第一行中除第一个元素以外的所有元素都化为零，而且该操作可在 NC 复杂度类中完成。

Let $\tilde{Y}$ 由索引为 $\{2,3,\ldots,n\}$ 的行和列构成的结果主子矩阵。那么，我们有

$$\det(A') = a_{1,3}\cdot\det(\tilde{A}+\tilde{Y}),$$

因此，A' 的行列式非零，当且仅当 $\det(\tilde{A}+\tilde{Y})$ 非零

因此，只需找到一个代入$(a_1,a_2,\ldots,a_{n-4}) \in \mathbb{F}^{n-4}$，用于$(y_5,y_6,\ldots,y_n)$，使得

$$\det\left(\tilde{A}+\tilde{Y}\right) \neq 0 \Longrightarrow \det\left(\tilde{A}+\tilde{D}\right) \neq 0$$

其中 $\tilde{D} = \operatorname{diag}(0,a_1,a_2,\ldots,a_{n-4})$。这个问题可归约为以下问题：给定一个$M \in \mathbb{F}^{(n-1)\times(n-1)}$，求一个对角矩阵$C \in \mathbb{F}^{(n-1)\times(n-1)}$，使得

$$(M+Z)^{\mathrm{adj}}[1,2] \neq 0 \Longrightarrow (M+C)^{\mathrm{adj}}[1,2] \neq 0,$$

其中 $Z =$ 对角矩阵$(z_1,z_2,\ldots,z_{n-1})$。引理 8.1 已在 NC 复杂度类中解决了这个问题。

因此，对于所有$(S、T) \in \mathcal{T}_A$，我们都可以在 NC 复杂度类中计算所需的对角矩阵$A_{S,T}$。 □

[2]尽管 [CGGR25中的断言 41] 是以多项式时间算法的背景来阐述的，但它也可以在 NC 复杂度类中实现。

由于 $(A+D)$ 和 $(B+D)$ 均可逆， [CGGR25，引理 2。9] 推出

$$A \overset{\text{PME}}{=} B \iff (A+D)^{\text{adj}} \overset{\text{PME}}{=} (B+D)^{\text{adj}}.$$

因此，根据定理 1.3，

$$A \overset{\text{PME}}{=} B \iff \text{PME}((A+D)^{\text{adj}}, (B+D)^{\text{adj}}, 4).$$

我们可以计算 $(A+D)^{\text{adj}}$、$(B+D)^{\text{adj}} \in \mathbb{F}^{n\times n}$ [Csa76、BCP83]，并检查 $\text{PME}((A+D)^{\text{adj}}, (B+D)^{\text{adj}}, 4)$ 是否成立。因此，我们可以在 NC 复杂度类中测试 $A \text{ PME} = B$ 是否成立。至此，定理 1.2 的证明完成。

致谢 我们谨向匿名审稿人致谢，感谢他们提出的宝贵意见。

参考文献

[Ahm23] Abeer Al Ahmadieh. 主子式映射的纤维, 2023. 11, 14, 62, 63[AJ15] N. R. Aravind与Pushkar S. Joglekar. 论只读一次行列式的表达能力. 载于Adrian Kosowski与Igor Walukiewicz编, 《计算理论基础——第20届国际研讨会, FCT 2015, 波兰格但斯克, 2015年8月17日至19日, 会议论文集》, 计算机科学讲义第9210卷, 第95–105页. 施普林格, 2015. 1, 10[BBB+00] Amos Beimel, Francesco Bergadano, Nader H. Bshouty, Eyal Kushilevitz与Stefano Varricchio. 学习表示为重数自动机的函数. 《ACM 杂志》, 47(3):506–530, 2000. 会议版本发表于FOCS 1996会议论文集. 1, 10[BC15] Abderrahim Boussaïri与Brahim Chergui. 反对称矩阵及其主子式. 线性代数及其应用, 485:47–57, 2015. 2, 10[BC16] Abderrahim Boussaïri与Brahim Chergui. 一种保持反对称矩阵主子式的变换. 《线性代数电子期刊》, 32, 2016年6月. 2, 10[BCCL21] A. Boussaïri, A. Chaïchaâ, B. Chergui与S. Lakhlifi. 具有相同主子式的广义竞赛矩阵. 《线性与多重线性代数》, 70(20):5433–5444, 2021年4月. 2, 10[BCP83] A. Borodin, S. Cook与N. Pippenger. 富裕环与空间有界概率机器的并行计算. 《信息与控制》, 58(1):113–136, 1983. 9, 52, 53, 55[BDGT24] Vishwas Bhargava, Pranjal Dutta, Sumanta Ghosh与Anamay Tengse. ROABP的阶寻找复杂度. CoRR, abs/2411.18981, 2024. 10[Ber84] Stuart J. Berkowitz. 论使用少量处理器在较短并行时间内计算行列式. 《信息处理快报》, 18(3):147–150, 1984. 1, 3

[BGKS22] Vishwas Bhargava, Ankit Garg, Neeraj Kayal与Chandan Saha. 非退化情形下广义三层算术电路的学习. 载于Amit Chakrabarti与Chaitanya Swamy编, 《近似、随机化与组合优化：算法与技术（APPROX/RANDOM 2022）》, 莱布尼茨国际信息学会议论文集（LIPIcs）第245卷, 第21:1–21:22页. Schloss Dagstuhl – 莱布尼茨信息学中心, 2022. 11[BHH95] Nader H. Bshouty, Thomas R. Hancock与Lisa Hellerstein. 学习算术只读一次公式. SIAM J. Comput., 24(4):706–735, 1995. 会议版本发表于STOC 1992会议论文集. 1, 10[Bru18] Victor-Emmanuel Brunel. 通过主子式赋值问题学习带符号行列式点过程. 载于《第32届神经信息处理系统国际会议论文集》, NIPS'18, 第7376–7385页, 美国纽约州雷德胡克, 2018. Curran Associates Inc. 2, 5[BSV20] Vishwas Bhargava, Shubhangi Saraf与Ilya Volkovich. 四层多线性电路的重构. 载于《第十四届ACM-SIAM离散算法年会论文集》, 第2144–2160页. SIAM, 2020. 11[BSV21] Vishwas Bhargava, Shubhangi Saraf与Ilya Volkovich. 低秩张量与三层多线性电路的重构算法. 载于《第 53 届 ACM SIGACT 计算理论年会论文集》 , 第 809–822 页 , 2021. 11[BT88] Michael Ben-Or与Prasoon Tiwari. 稀疏多元多项式插值的确定性算法（扩展摘要）. 载于Janos Simon编, 《第 20 届 ACM 计算理论年会论文集 , 1988 年 5 月 2 日至 4 日 , 美国伊利诺伊州芝加哥》 , 第301–309页. ACM, 1988. 1[BU24] Victor-Emmanuel Brunel与John Urschel. 由其主子式恢复幅值对称矩阵. 线性代数及其应用, 703:232–267, 2024. 2, 10[CGGR23] Abhranil Chatterjee, Sumanta Ghosh, Rohit Gurjar与Roshan Raj. 秩一限制下符号行列式的边界复杂度. 载于Amnon Ta-Shma编, 《第38届计算复杂性会议, CCC 2023, 2023年7月17日至20日, 英国华威》, LIPIcs第264卷, 第2:1–2:15页. Schloss Dagstuhl - 莱布尼茨信息学中心, 2023. 1[CGGR24] Abhranil Chatterjee, Sumanta Ghosh, Rohit Gurjar与Roshan Raj. 矩阵主子式等价性的刻画与检验. CoRR, abs/2410.01961, 2024. 14, 21[CGGR25] Abhranil Chatterjee, Sumanta Ghosh, Rohit Gurjar与Roshan Raj. 矩阵主子式等价性的刻画与检验. 载于Michal Koucký与Nikhil Bansal编, 《第57届ACM计算理论年会论文集, STOC 2025, 捷克布拉格, 2025年6月23日至27日》, 第 1067–1078 页 . ACM, 2025. 2, 7, 9, 10, 14, 33, 34, 35, 38, 41, 51, 53, 54, 55, 62, 64[Csa76] L. Csanky. 快速并行矩阵求逆算法. SIAM J. Comput., 5(4):618–623, 1976. 3, 9, 52, 53, 55

[CV89] Richard Cole 和 Uzi Vishkin. 更快的最优并行前缀和与链表排序. Information and Computation, 81(3):334–352, 1989年6月. 9, 52[DL78] Richard A. Demillo 和 Richard J. Lipton. 关于代数程序测试的一则概率性评论. Information Processing Letters, 7(4):193 – 195, 1978年. 3, 22[Edm67] Jack Edmonds. 互异代表元系统与线性代数. Journal of research of the National Bureau of Standards, 71:241–245, 1967年. 1[Edm68] Jack Edmonds. 拟阵划分. Mathematics of the Decision Sciences, 11:335–345, 1968年. 1[Edm79] Jack Edmonds. 拟阵交. 收录于 P.L. Hammer 、 E.L. Johnson 和 B.H. Korte 编，Discrete Optimization I，Annals of Discrete Mathematics 第4卷，第39–49页. 爱思唯尔，1979年. 1[ES80] Gernot M. Engel 和 Hans Schneider. 对角相似于对称矩阵的矩阵. 线性代数及其应用, 29:131–138, 1980年. 献给 Alson S. Householder 的特别专辑. 2[FS13] Michael A. Forbes 和 Amir Shpilka. 非交换只读一次无关代数分支程序的准多项式时间恒等性测试. 收录于 54th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2013, Berkeley, CA, USA, October, 26-29, 2013, 第243–252页. IEEE计算机学会，2013年. 10[Gan60] F. R. Gantmacher. 矩阵理论（第一卷）. Chelsea Publishing Company, 纽约，1960年. 原著以俄语出版；由 K. A. Hirsch 翻译. 21, 22, 54[Gee99] James F. Geelen. 最大秩矩阵补全. 线性代数及其应用, 288:211–217, 1999年. 1[GKL11] Ankit Gupta、Neeraj Kayal 和 Satyanarayana V. Lokam. 随机多重线性公式的高效重构. 收录于 IEEE第52届计算机科学基础年会, FOCS 2011, Palm Springs, CA, USA, October 22-25, 2011, 第778–787页，2011年. 11[GKL12] Ankit Gupta、Neeraj Kayal 和 Satyanarayana V. Lokam. 顶层扇入为2的四层多重线性电路重构. 收录于 Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012, 第625–642页，2012年. 11[GKQ14] Ankit Gupta、Neeraj Kayal 和 Youming Qiao. 随机算术公式可以高效重构. Computational Complexity, 23(2):207–303, 2014年. 会议版本发表于 CCC 2013 论文集. 11[GKS20] Ankit Garg、Neeraj Kayal 和 Chandan Saha. 非退化情形下低次多项式幂和的学习. 收录于 2020年IEEE第61届计算机科学基础年会 (FOCS), 第889–899页. IEEE，2020年. 11[GM88] Hillel Gazit 和 Gary L. Miller. 一种改进的并行算法，用于计算有向图的广度优先搜索编号. Information Processing Letters, 28(2):61–65, 1988年6月. 9, 52

[GT06a] Kent Griffin 和 Michael J. Tsatsomeros. 主子式，第一部分：一种计算矩阵所有主子式的方法. 线性代数及其应用, 419:107–124, 2006. 4[GT06b] Kent Griffin 和 Michael J. Tsatsomeros. 主子式，第二部分：主子式赋值问题. 线性代数及其应用, 419(1):125–171, 2006. 2, 5, 10[GT17] Rohit Gurjar 和 Thomas Thierauf. 线性拟阵交属于准NC. 收录于 Hamed Hatami、Pierre McKenzie 和 Valerie King 编，Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017, 第821–830页. ACM，2017年. 10[GT20] Rohit Gurjar 和 Thomas Thierauf. 线性拟阵交属于准NC. Comput. Complex., 29(2):9, 2020年. 会议版本发表于 STOC 2017 论文集. 1, 6, 15, 17, 22, 25, 26[HH91] Thomas R. Hancock 和 Lisa Hellerstein. 域上只读一次公式与扩展基的学习. 收录于 Manfred K. Warmuth 和 Leslie G. Valiant 编，Proceedings of the Fourth Annual Workshop on Computational Learning Theory, COLT 1991, Santa Cruz, California, USA, August 5-7, 1991, 第326–336页. Morgan Kaufmann，1991年. 1, 10[HKM05] Nicholas J. A. Harvey、David R. Karger 和 Kazuo Murota. 通过矩阵补全实现确定性网络编码. 收录于 Proceedings of the Sixteenth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2005, Vancouver, British Columbia, Canada, January 23-25, 2005, 第489–498页. SIAM，2005年. 1[HL84] D.J. Hartfiel 和 R. Leowy. 关于具有相等对应主子式的矩阵. 线性代数及其应用, 58:147–167, 1984. 2, 8, 9, 10, 12, 13, 20, 21, 29, 53[HPR97] Yijie Han、Victor Y. Pan 和 John H. Reif. 计算有向图中所有点对最短路径的高效并行算法. Algorithmica, 17(4):399–415, 1997. 53[HS02] Olga Holtz 和 Hans Schneider. 关于 GKK tau-矩阵的公开问题. 线性代数及其应用, 345:263–267, 2002. 2[Ier89] D. Ierardi. 代数闭域理论中的量词消去. 收录于 Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing, STOC '89, 第138–147页, 纽约, NY, 美国, 1989年. 美国计算机协会. 4[IKQS15] Gábor Ivanyos、Marek Karpinski、Youming Qiao 和 Miklos Santha. 广义Wong序列及其在 Edmonds问题中的应用. J. Comput. Syst. Sci., 81(7):1373–1386, 2015年. 1[IKS10] Gábor Ivanyos、Marek Karpinski 和 Nitin Saxena. 矩阵补全问题的确定性多项式时间算法. SIAM J. Comput., 39(8):3736–3751, 2010年. 1[KNS19] Neeraj Kayal、Vineet Nair 和 Chandan Saha. 低宽度代数分支程序的平均情形线性矩阵分解与重构. Computational Complexity, 28(4):749–828, 2019年. 11

[KS01] Adam R. Klivans 和 Daniel A. Spielman。多元多项式的高效随机化恒等测试。载于第33届ACM计算理论研讨会年会论文集，2001年7月6日至8日，希腊克里特伊拉克利翁，第216–223页，2001年。 1[KS06] Adam R. Klivans 和 Amir Shpilka。算术电路受限模型的学习。计算理论，2(10)：185–206，2006年。会议版本发表于COLT 2003论文集。 1, 10[KS09] Zohar S hay Karnin 和 Amir Shpilka。具有有界顶层扇入的广义深度3算术电路的重构。载于第24届IEEE计算复杂性会议年会论文集，CCC 2009，法国巴黎，2009年7月15日至18日，第274–285页，2009年。 11[KS19] Neeraj Kayal 和 Chandan Saha。非退化齐次深度三电路的重构。载于第51届ACM SIGACT计算理论研讨会年会论文集，STOC 2019，美国亚利桑那州凤凰城，2019年6月23日至26日，第413–424页，2019年。 11[KT12] Alex Kulesza 和 Ben Taskar。用于机器学习的行列式点过程。机器学习基础与趋势，5：123–286，2012年。 2[Loe86] Raphael Loewy。矩阵的主子式与对角相似。线性代数及其应用，78：23–64，1986年。 2, 7, 8, 9, 10, 13, 14, 27, 29, 30, 65[Lov89] László Lovaśz。矩阵奇异空间及其在组合学中的应用。巴西数学学会通报，20：87–99，1989年。 1[LS09] Shaowei Lin 和 Bernd Sturmfels。4x4矩阵的主子式之间的多项式关系。代数，322(11)：4121–4131，2009年。 4[Mur93] Kazuo Murota。混合矩阵：不可约性与分解。载于 Richard A. Brualdi、Shmuel Friedland 和 Victor Klee（编），《线性代数中的组合学与图论问题》，第39–71页，纽约，纽约州，1993年。施普林格纽约。 1[MV97] Meena Mahajan 和 V. Vinay。行列式：组合学、算法与复杂度。《芝加哥理论计算机科学杂志》，1997年，1997年。会议版本发表于SODA 1997论文集。 1[MV18] Daniel Minahan 和 Ilya Volkovich。只读一次公式的恒等测试与重构的完全去随机化。ACM计算理论汇刊，10(3)：10:1–10:11，2018。会议版本发表于CCC 2017论文集。 1, 10[MVV87] Ketan Mulmuley、Umesh V. Vazirani 和 Vijay V. Vazirani。匹配与矩阵求逆一样容易。载于第十九届ACM计算理论研讨会年会论文集，STOC ’87，第345–354页，纽约，纽约州，美国，1987年。美国计算机协会。 6, 17, 18[Nis91] Noam Nisan。非交换计算的下界（扩展摘要）。载于 Cris Koutsougeras 和 Jeffrey Scott Vitter（编），第23届ACM计算理论研讨会年会论文集，1991年5月5日至8日，美国路易斯安那州新奥尔良，第410–418页。ACM，1991年。 1, 10

[NSV94] H. Narayanan、Huzur Saran 和 Vijay V. Vazirani。拟阵并与交集的随机并行算法及其在树形结构和边不相交生成树中的应用。SIAM计算杂志，23(2)：387–397，1994年。 18[Oed11] Luke Oeding。对称矩阵主子式簇的集合论定义方程。代数与数论，5(1)：75–109，2011年8月。 2, 4, 10[RKT15] Justin Rising、Alex Kulesza 和 Ben Taskar。对称主子式赋值问题的一种高效算法。线性代数及其应用，473：126–144，2015年。统计学专刊。 2, 4, 10[Sch80] Jacob T. Schwartz。用于验证多项式恒等式的快速概率算法。ACM学报，27(4)：701–717，1980年10月。 3, 22[Shp09] Amir Shpilka。具有两个乘法门的深度3算术电路的插值。SIAM计算杂志，38(6)：2130–2161，2009年。会议版本发表于STOC 2007论文集。 11[Sin16] Gaurav Sinha。顶层扇入为2的实深度3电路的重构。载于第31届计算复杂性会议，CCC 2016，2016年5月29日至6月1日，日本东京，第31:1–31:53页，2016年。 11[SV14] Amir Shpilka 和 Ilya Volkovich。只读一次公式的重构与测试。计算理论，10(18)：465–514，2014年。会议版本发表于STOC 2008论文集。 1, 10[UBMR17] John Urschel、Victor-Emmanuel Brunel、Ankur Moitra 和 Philippe Rigollet。利用矩与环学习行列式点过程。载于第34届国际机器学习会议论文集——第70卷，ICML'17，第3511–3520页。JMLR.org，2017年。 2, 10[Val79] Leslie G. Valiant。代数中的完备性类。载于第11届ACM计算理论研讨会年会论文集，1979年4月30日至5月2日，美国佐治亚州亚特兰大，第249–261页，1979年。 1, 10[Zip79] Richard Zippel。稀疏多项式的概率算法。载于国际符号与代数计算研讨会（EUROSAM）论文集，第216–226页。施普林格出版社，1979年。3, 22

A 节缺失的证明5

A.1 引理5.4 的证明

引理 5.4 （重述）。设 A 和 B 是两个 4×4 矩阵，A 的所有非对角元均非零，且 $A \overline{\ _{PME}\ } B$。设 $X \subseteq \{1,2,3,4\}$ 满足 $|X| = 2$, $\mathcal{D}_1(A, B) = X$ 且 $\mathcal{D}_2(A, B) = X$。那么，X 是 A 的一个割。

证明。 不失一般性，我们可以假设 $\mathcal{D}_1(A, B) = \{1,2\}$ 且 $\mathcal{D}_2(A, B) = \{3,4\}$。由于 $\mathcal{D}_1(A, B) = \{1,2\}$，存在一个矩阵 A'，它与 A 对角相似，且 $A'[\{j, 3, 4\}] =$

$B[\{j,3,4\}]$ 对于$j=1,2$。此外，不失一般性，我们可以考察任何与 A 对角相似的矩阵。因此，我们假设

$$A[\{j,3,4\}] = B[\{j,3,4\}] \text{ for } j=1,2.$$

这意味着A 和B 具有以下形式：

$$A=\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} \quad \text{and} \quad B=\begin{pmatrix} a_{11} & b_{12} & a_{13} & a_{14} \\ b_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} \tag{28}$$

设C为一个3×3对角矩阵，使得对所有$i=1$、2、3，$C[i,\ i]=c_i$且$c_1=1$。类似地，设D为一个3×3对角矩阵，使得对所有$i=1$、2、3，$D[i,\ i]=d_i$且$d_1=1$。此外，假设

$$B[\{1,2,3\}]^T = C^{-1}\cdot A[\{1,2,3\}]\cdot C \quad \text{and} \quad B[\{1,2,4\}]^T = D^{-1}\cdot A[\{1,2,4\}]\cdot D \tag{29}$$

因此，$c_2=d_2$。令$e_1=1$、$e_2=c_2=d_2$,$e_3=c_3$,$e_4=d_4$。因此，由式（28）和式（29），A 和B具有以下形式：

$$A=\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{13}e_3 & \frac{a_{23}e_3}{e_2} & a_{33} & a_{34} \\ a_{14}e_4 & \frac{a_{24}e_4}{e_2} & a_{43} & a_{44} \end{pmatrix} \quad \text{and} \quad B=\begin{pmatrix} a_{11} & \frac{a_{21}}{e_2} & a_{13} & a_{14} \\ a_{12}e_2 & a_{22} & a_{23} & a_{24} \\ a_{13}e_3 & \frac{a_{23}e_3}{e_2} & a_{33} & a_{34} \\ a_{14}e_4 & \frac{a_{24}e_4}{e_2} & a_{43} & a_{44} \end{pmatrix}$$

由于$A \overset{\text{PME}}{=} B$,

$$\begin{aligned} 0 &= \det(A)-\det(B) \\ &= (a_{12}a_{23}a_{34}a_{41}-a_{14}a_{43}a_{32}b_{21})+(a_{14}a_{43}a_{32}a_{21}-b_{12}a_{23}a_{34}a_{41}) \\ &\quad +(a_{12}a_{24}a_{43}a_{31}-a_{13}a_{34}a_{42}b_{21})+(a_{13}a_{34}a_{42}a_{21}-b_{12}a_{24}a_{43}a_{31}) \\ &= a_{12}a_{23}a_{14}(a_{34}e_4-a_{43}e_3)-\frac{a_{14}a_{23}a_{21}}{e_2}(a_{34}e_4-e_3a_{43}) \\ &\quad -a_{13}a_{24}a_{12}(a_{34}e_4-a_{43}e_3)+\frac{a_{13}a_{24}a_{21}}{e_2}(a_{34}e_4-a_{43}e_3) \\ &= (a_{34}e_4-a_{43}e_3)\left(a_{12}a_{23}a_{14}-\frac{a_{14}a_{23}a_{21}}{e_2}-a_{13}a_{24}a_{12}+\frac{a_{13}a_{24}a_{21}}{e_2}\right) \\ &= (a_{34}e_4-a_{43}e_3)(a_{13}a_{24}-a_{23}a_{14})\left(\frac{a_{21}}{e_2}-a_{12}\right) \end{aligned}$$

现在我们将证明分为以下三种情形。

1. **情形 I**（$a_{34}e_4-a_{43}e_3=0$）：在此情形下，可得$B^T=E^{-1}AE$，其中E是一个对角矩阵，满足$E[i,i]=e_i$，对所有$i=1$、2、3、4均成立。因此，$\mathcal{D}_2(A,\ B)=\{1,2,3,4\}$，这与引理的假设矛盾。

2. **情形 II (**$\frac{a_{21}}{e_2}-a_{12}=0$**):** 这意味着$A=B$，这与假设$\mathcal{D}_1(A,\ B)=\{1,2\}$矛盾。

3. **情形 III (**$a_{13}a_{24}-a_{23}a_{14}=0$**):** 在这种情形下，可以推出 $\{1,2\}$ 是A的一个割。

至此，该引理的证明结束。 □

A.2 引理5.7 的证明

引理 5.7（重述）。设 A 与 B 为域 $\mathbb{F}$ 上的两个 n ×n 矩阵，且具有非零非对角元。设 S ⊆ [n] 为 A 与 B 的一个割。考虑任意两个指标 s、t，使得 s ∈ S 且 t ∈ S。则 A PME = B 当且仅当 A[S + t] PME= B[S +t] 且 A[S +s] PME= B[S +s]。此外，若 S 是 A 的极小割，则 A[S +t] 无割。

证明。“仅当”方向是显然的。现在我们证明其逆命题。我们的论证思路沿袭了 [CGGR25，引理 2。12]。不失一般性，假设 $S = [|S|]$，$s = |S| - 1$ 且 $t = |S| + 1$。考虑以下定义。

$$p = A[t, S],\ \tilde{p} = B[t, S],\ q^T = \frac{A[s, \overline{S}]}{A[s, t]},\ \tilde{q}^T = \frac{B[s, \overline{S}]}{B[s, t]},\ \text{and}$$
$$u = A[s, \overline{S}],\ \tilde{u} = B[s, \overline{S}],\ v^T = \frac{A[t, S]}{A[t, s]},\ \text{and}\ \tilde{v}^T = \frac{B[t, S]}{B[t, s]}.$$

因此，A 和B 可以写成如下形式：

$$A = \begin{array}{c} \\ S \\ \overline{S} \end{array} \begin{array}{c} \begin{array}{cc} S & \overline{S} \end{array} \\ \begin{pmatrix} M & p \cdot q^T \\ u \cdot v^T & N \end{pmatrix} \end{array} \text{and}\ \ B = \begin{array}{c} \\ S \\ \overline{S} \end{array} \begin{array}{c} \begin{array}{cc} S & \overline{S} \end{array} \\ \begin{pmatrix} \tilde{M} & \tilde{p} \cdot \tilde{q}^T \\ \tilde{u} \cdot \tilde{v}^T & \tilde{N} \end{pmatrix} \end{array}$$

令 X ⊆ [n]。注意，若 X 是 S +t 或 S +s 的子集，则 det(A[X]) = det(B[X])。现在考虑 X = $X_1 \sqcup X_2$，使得 X_1 和 X_2 分别是 S 和 S 的非空子集。接下来，我们证明 det(A[X]) = det(B[X])。

假设坐标 p, ˜p, v, ˜v 的指标属于 S，而坐标 q, ˜q, u, ˜u 的指标属于 S。我们用 p^{X_1}、q^{X_2}、u^{X_2} 和 v^{X_1} 表示相应向量在相应坐标上的投影。同样，我们可以定义向量 $\tilde{p}^{X_1}$、$\tilde{q}^{X_2}$、$\tilde{u}^{X_2}$ 和 $\tilde{v}^{X_1}$。令 A′ 和 B′ 分别表示子矩阵 A[X] 和 B[X],。于是，

$$A' = \begin{pmatrix} M[X_1] & p_{X_1} \cdot q_{X_2}^T \\ u_{X_2} \cdot v_{X_1}^T & N[X_2] \end{pmatrix} \text{and}\ \ B' = \begin{pmatrix} \tilde{M}[X_1] & \tilde{p}_{X_1} \cdot \tilde{u}_{X_2}^T \\ \tilde{q}_{X_2} \cdot \tilde{v}_{X_1}^T & \tilde{N}[X_2]^T \end{pmatrix}$$

设 $\ell = |X|$，k = $|X_1|$，K = [k] 且 $\overline{K} = \{k+1, k+2, \ldots\ldots, \ell\}$。假设 A′和 B′的行和列由 [ℓ]索引，M[$X_1$] 和 $\tilde{M}[X_1]$ 的行和列由 K 索引。对于每个 i ∈ K，令 M_i 表示通过移除 M[X_1] 的第 i 列，并将 p^{X_1} 作为第 k 列添加进去后得到的 k ×k 矩阵。对于 j ∈ K，令 N^j 表示通过移除 N[X_2] 的第 j 列，并将 u^{X_2} 添加为第一列后得到的 (l − k) × (l − k) 矩阵。类似地，对于所有 i ∈ K 和 $\tilde{j} \in K$，我们可以分别从 $\tilde{M}[X_1]$ 和 $\tilde{N}[X_2]$,定义矩阵 $\tilde{M}_i$ 和 $\tilde{N}^j$。

利用广义拉普拉斯定理（参见 [Ahm23，定理 3.1]），det(A') 可写为如下形式。

$$\det(A') = \sum_{T \subseteq [\ell], |T| = k} (-1)^{\Sigma K + \Sigma T} \det(A'[K, T]) \det(A'[\overline{K}, \overline{T}]).$$

注意，对于所有满足 $|T \subset [\ell]\ |T \cap K| \geq 2$ 的$T \subset [\ell]$，子矩阵 $A'[K, T]$ 的秩不满，因为 rank(A'[K, K])≤ 1。因此，对于所有满足 $|T| = k$ 的此类$T \subseteq [\ell]$，det(A'[K,T]) = 0。这意味着

$$\det(A') = \det(M[X_1]) \det(N[X_2]) + \sum_{i \in K, j \in \overline{K}} (-1)^{j-i} \det(A'[K, K - i + j]) \det(A'[\overline{K}, \overline{K} + i - j]).$$

注意，对于所有$i \in K$和$j \in K$，

$$\det(A'[K, K - i + j]) = q_{X_2}[j - k] \det(M_i), \text{ 且 } \det(A'[K, K - i + j]) = v_{X_1}[i] \det(N_j)。$$

因此，根据上述两个方程，

$$\begin{aligned}\det(A') &= \det(M[X_1]) \det(N[X_2]) + \sum_{i \in K, j \in \overline{K}} (-1)^{j-i} v_{X_1}[i] q_{X_2}[j-k] \det(M_i) \det(N_j) \\ &= \det(M[X_1]) \det(N[X_2]) + \left(\sum_{i \in K} (-1)^i v_{X_1}[i] \det(M_i) \right) \left(\sum_{j \in \overline{K}} (-1)^j q_{X_2}[j-k] \det(N_j) \right)\end{aligned}$$

同样，利用广义拉普拉斯定理（参见 [Ahm23，定理 3。1]），我们得到

$$\det(B') = \det(\widetilde{M}[X_1]) \det(\widetilde{N}[X_2]) + \left(\sum_{i \in K} (-1)^i \tilde{v}_{X_1}[i] \det(\widetilde{M}_i) \right) \left(\sum_{j \in \overline{K}} (-1)^j \tilde{q}_{X_2}[j-k] \det(\widetilde{N}_j) \right)$$

由于 $A[S + t] \overset{\text{PME}}{=} B[S + t]$ 且 $A[S \dot{+} s] \overset{\text{PME}}{=} B[\overline{S} + s]$, $\det(M[X_1]) \cdot \det(N[X_2])$ 等于 $\det(\widetilde{M}[X_1]) \det(N[X_2])$。因此，$\det(A') = \det(B')$ 当且仅当上述 $\det(A')$ 和 $\det(B')$ 的表达式中的第二项相等。

设 P 和 P 是两个$(|X_2| + 1) \times (|X_2| + 1)$ 矩阵，定义如下：

$$P = \begin{pmatrix} 0 & q_{X_2}^T \\ u_{X_2} & N[X_2] \end{pmatrix} \text{ and } \widetilde{P} = \begin{pmatrix} 0 & \tilde{q}_{X_2}^T \\ \tilde{u}_{X_2} & \widetilde{N}[X_2] \end{pmatrix}$$

于是，

$$(-1)^k \det(P) = \sum_{j \in \overline{K}} (-1)^j q_{X_2}[j-k] \det(N_j) \text{ and } (-1)^k \det(\widetilde{P}) = \sum_{j \in \overline{K}} (-1)^j \tilde{q}_{X_2}[j-k] \det(\widetilde{N}_j).$$

类似地，令R 和R 为两个$(|X_1| + 1) \times (|X_1| + 1)$ 矩阵，定义如下

$$R = \begin{pmatrix} M[X_1] & p_{X_1} \\ v_{X_1}^T & 0 \end{pmatrix} \text{ and } \widetilde{R} = \begin{pmatrix} \widetilde{M}[X_1] & \tilde{p}_{X_1} \\ \tilde{v}_{X_1}^T & 0 \end{pmatrix}$$

于是，

$$(-1)^k \det(R) = \sum_{i \in K} (-1)^i v_{X_1}[i] \det(M_i) \text{ and } (-1)^k \det(\widetilde{R}) = \sum_{i \in K} (-1)^i \tilde{v}_{X_1}[i] \det(\widetilde{M}_i)$$

因此，考虑 $\det(A')$ 和 $\det(B')$的上述表达式，可得

$$\det(A') = \det(B') \iff \det(P) \det(R) = \det(\widetilde{P}) \det(\widetilde{R}).$$

根据q_{X_2}、u_{X_2}、 $\tilde{q}_{X_2}$和 $\tilde{u}_{X_2}$的定义，可写为

$$A[X_2 + s] = \begin{pmatrix} A[s,s] & A[s,t] \cdot q_{X_2}^T \\ u_{X_2} & N[X_2] \end{pmatrix} \text{ and } B[X_2 + s] = \begin{pmatrix} B[s,s] & B[s,t] \cdot \tilde{q}_{X_2}^T \\ \tilde{u}_{X_2} & \widetilde{N}[X_2] \end{pmatrix}$$

由于$A[S \dot{+} s] \overset{\text{PME}}{=} B[\overline{S} + s]$, $\det(A[X_2 + s]) = \det(B[X_2 + s])$。因此，

$$A[s,t] \det(P) = B[s,t] \det(\widetilde{P}) \tag{30}$$

根据p^{X_1}、v^{X_1}、 $\tilde{p}^{X_1}$、 $\tilde{v}^{X_1}$的定义，我们得到如下结果：

$$A[X_1+t]=\begin{pmatrix} M[X_1] & p_{X_1} \\ A[t,s]\cdot v_{X_1}^T & A[t,t]\end{pmatrix} \text{ and } B[X_1+t]=\begin{pmatrix} \widetilde{M}[X_1] & \tilde{p}_{X_1} \\ A[t,s]\cdot \tilde{v}_{X_1}^T & B[t,t]\end{pmatrix}$$

由于$A[S+t]\overset{\text{PME}}{=}B[S+t]$, $\det(A[X_1+t])=\det(B[X_1+t])$。因此，

$$A[t,s]\det(R)=B[t,s]\det(\widetilde{R}). \tag{31}$$

由于 A[S +t] PME= B[S +t], A[{s, t}] PME= B[{s, t}]。结合公式（30）和公式（31）可知，
$\widetilde{\det(P)}\det(R)=\det(P)\det(R)$。因此，$\det(A')=\det(B')$。引理的证明至此完成。

引理的第二部分直接由 [CGGR25，引理 33]得出。 □

A.3 引理5.8 的证明

引理 5.8 （重述）。设 A 和 B 是两个具有非零非对角元的 $n\times n$ 矩阵，并且PME(A，B，4)。设 S 是 A 的一个大小大于2的极小割。那么，S 也是 B 的一个割。

证明。 固定一个元素 $s\in S$。我们将证明，对于所有$t\in S+s$，集合$T_t:=\{s,t\}$ 是$B[S\cup T_t]$中的一个割。这将推出S 是B中的一个割。

由于 S 是 A 中大小大于二的极小割，根据 [CGGR25，引理 3.3]，，A[S +s]和 A[S +t] 都没有割。根据假设，PME(A, B, 4) 成立。然后，应用定理 5.1，得到 A PME = B。因此，根据引理 2.3，我们得出 A[S +s] 对角等价= B[S +s]，且 A[S +t] 对角等价= B[S +t]。因此，B[S +s] 和 B[S +t] 都没有割。

现在，假设存在矛盾，即 T_t 不是 $B[S\cup T_t]$中的一个割。注意，T_t 是 $A[S\cup T_t]$中大小为二的一个割。于是，根据引理 2.7，在矩阵 $B[S\cup T_t]$ 中存在一个割 $X\subseteq S\cup T_t$，使得 $s\in X$ 且 $t\notin X$。

由于 $|S\cup T_t|\geq 5$，要么 $|X|>2$，要么补集 X 的大小：$=(S\cup T_t)\setminus X$ 大于 2。

- 如果 $|X|>2$，则 $X-s$ 是 $B[S+t]$, 中的一个割，因为 X 是 $B[S\cup T_t]$ 中的一个割，并且 $s\in X$。
- 否则，如果 $|X|>2$，则 $\widetilde{X\setminus t}$ 是 $B[S+s]$中的一个割。

在这两种情形中，我们得到一个矛盾，因为我们已经证明 $B[S\cup s]$ 和 $B[S+t]$ 无割。

因此，对所有 $t\in S+s$，T_t 是 $B[S\cup T_t]$中的一个割。证明至此完成。 □

B 性质 $\mathcal{R}$ 能否去掉?

我们在此构造一对矩阵A、$B\in\mathbb{F}^{n\times n}$，使得

- A 不 满足性质 $\mathcal{R}$,
- PME(A、B、4) 成立，但A 与B不 主子式等价。

我们首先放宽性质 $\mathcal{R}$ 的第一个条件，即允许 A 的某些非对角元为零。设矩阵 A 和 B 定义如下：

$$A[i,i+1]=B[i,i+1]=1 \text{ for all } i\in[n-1],\ A[n,1]=1,\ B[n,1]=2,$$

而 A 和 B 的其他元素均为零。那么，不难验证，$\mathrm{PME}(A, B, n-1)_{\text{PME}}$，但 $A \neq B$。因此，如果允许 A 和 B 中的非对角元为零，那么 $\mathrm{PME}(A, B, 4)$ 并不意味着 $A \overset{\text{PME}}{=} B$。

现在假设A 和B 的非对角元均非零，但A 不满足性质 $\mathcal{R}$，也就是说，A 违反了性质 $\mathcal{R}$ 的第二个条件。设A 是如下形式的$n \times n$矩阵：

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & a_{15} & a_{16} & \cdots & a_{1n} \\ 2 & 1 & 1 & 1 & a_{25} & a_{26} & \cdots & a_{2n} \\ 1 & 1 & 1 & 2 & a_{35} & a_{36} & \cdots & a_{3n} \\ 1 & 1 & 1 & 1 & a_{45} & a_{46} & \cdots & a_{4n} \\ a_{15} & a_{25} & a_{35} & a_{45} & 1 & a_{56} & \cdots & a_{5n} \\ a_{16} & a_{26} & a_{36} & a_{46} & a_{56} & 1 & \cdots & a_{6n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & a_{3n} & a_{4n} & a_{5n} & a_{6n} & \cdots & 1 \end{pmatrix} \tag{32}$$

接下来，我们可以证明以下断言。

命题 B.1. 设 A 是一个 $n \times n$ 域 $\mathbb{F}$ 上的矩阵，其非零非对角元均非零，并假设A 具有式 (32)所给出的形式。假设 A 没有割 X 使得 $\{1,2\} \subseteq X$ 且 $\{3,4\} \subseteq X$。设 B 是另一个 $n \times n$ 矩阵，且满足

$$B[i,j] = A[i,j] \; \forall \, (i,j) \notin \{(1,2),(2,1)\}, \quad B[1,2] = A[2,1] = 2, \; \textit{and} \; B[2,1] = A[1,2] = 1 \tag{33}$$

$_{\text{PME}}$因此，PME(A、B、4)，但 $A \neq B$。

证明。注意，对于 j = 1, 2，有 A[[n] \ {j}] = B[[n] \ {j}]；对于 j = 3, 4，有 A[[n] \ {j}] = B[[n] \ {j}]^T。此外，B[{1,2,3,4}] = ct (A, {3,4})，因此 A[{1,2,3,4}] PME= B[{1,2,3,4}]（见引理 2.6）。于是，PME(A, B, 4)，并且

$$\{1,2\} \subseteq \mathcal{D}_1(A,B) \quad \text{and} \quad \{3,4\} \subseteq \mathcal{D}_2(A,B).$$

$_{\text{DS}}$ $_{\text{DS}}$由于 $A[\{1,2,3,4\}] \neq B[\{1,2,3,4\}]$ 且 $A[\{1,2,3,4\}] \neq B[\{1,2,3,4\}]^T$,

$$\mathcal{D}_1(A,B) = \{1,2\} \quad \text{and} \quad \mathcal{D}_2(A,B) = \{3,4\}.$$

若 A $_{\text{PME}}$ $= B$，则上述方程结合 [Loe86，定理 2] 可推出A 存在一个割X_{PME}，使得 $\{1,2\} \subseteq X$ 且 $\{3,4\} \subseteq X$。这与断言矛盾。因此,¯$A \neq B$。 □

显式构造。 利用上述断言，我们显式构造矩阵$_{\text{PME}}A$ 和B，使得 $\mathrm{PME}(A, B, 4)$，但$A \neq B$。我们构造一个$n \times n$ 矩阵A，使其满足以下性质：

1. 矩阵A 的形式如方程（32），而矩阵B 按方程（33）定义

2. 矩阵 A 不满足性质 $\mathcal{R}$ 的第二个条件。注意，子矩阵$A[\{1,2\},\{3,4\}]$ 的秩为 1。然而，该构造将表明，不存在子集$X \subseteq [n]$，使得 $\underline{1}, 2 \in X$、$3, 4 \in X$，且秩 $A[X$、$X] = 1$。

在该构造中，我们将矩阵 A 定义如下：

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 & 2 \\ 2 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 1 & 2 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 1 & 1 & 2 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 1 & 2 & 1 & 2 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 1 & 1 & 2 & 1 & 2 & \cdots & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 2 & 1 & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 & 2 \\ 2 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 2 & 1 \end{pmatrix},$$

也就是说，

1. $A[\{1,2,3,4\}]$ 的定义与式（32）中所述相同。2. 对所有 $i \in \{5$3. 其余所有项均为 1。$,6,7,\ldots,n\}$, $A[i-1,i] = A[i,i-1] = 2$, and additionally $A[1,n] = A[n,1] = 2$

现在，假设 X $\subseteq$ [n]，使得 $\{1,2\} \subseteq$ X 且 $\{3,4\} \subseteq$ X。由于 rank A$[\{1,2\},\{3,$n$\}] = 2$，为了使 X 成为 A 的一个割，它必须包含 n。继续归纳这一推理，我们可以证明 $\{4,5,6,$.....，n$\} \subseteq$ X，这与假设 4 $\in$ X 矛盾。因此，不存在这样的子集 X 能成为 A 的割 PME。因此，根据命题 B.1，A $\neq$ B。

上述讨论表明，要得出 PME（A，B，4）蕴含$A_{\text{PME}} = B$，性质 $\mathcal{R}$ 是必要的。此外，同一构造还能推出更强的结论。考虑以下问题：如果将假设从 PME（A，B，4）加强为 PME（A，B，ℓ），其中某个 $4 < \ell < n$，我们能否放宽性质 $\mathcal{R}$ 的第二个条件？上述构造同样对此问题给出了否定的回答。

令 $k \in \{5,6,7,\ldots,n\}$，并定义

$$X_k = \{1,2,k+1,k+2,\ldots,n\} \quad \text{and} \quad \overline{X}_k = [n] \setminus \{k\} \setminus X_k,$$

也就是说，$\overline{X}_k = \{3,4,5,6,\ldots k-1\}$。注意，$X_k$ 是矩阵 $A[[n] \setminus \{k\}]$的一个割，　　d

$$B[[n] \setminus \{k\}] = \text{ct}\left(A[[n] \setminus \{k\}], \overline{X}_k\right).$$

因此，由引理 2.6 可知，对于所有 k $\in \{5,6,\ldots,$ n$\}$，A$[[$n$] \setminus \{$k$\}]$ PME= B$[[$n$] \setminus \{$k$\}]$。另一方面，矩阵的结构保证，对于 k $= 1, 2, 3, 4$，有 A$[[$n$] \setminus \{$k$\}]$ PME= B$[[$n$] \setminus \{$k$\}]$。由此可得，对于所有 k $\in [$ n$]$,，A$[[$n$] \setminus \{$k$\}]$ PME= B$[[$n$] \setminus \{$k$\}]$，也就是说，PME(A, B, n $-$ 1)。然而，正如前面所示，A $\neq$ B。这证实，即使假设对于某个 $4 < \ell <$ n 有 PME(A, B, ℓ)，若 A 不满足性质 $\mathcal{R}$，也不足以保证 A PME = B。