arXiv:2303.00252v1 [cs.CC] 1 Mar 2023

植入着色比植入团更容易吗?

Pravesh K. Kothari*[1]、Santosh S. Vempala†[2]、Alexander S. Wein‡[3]和 Jeff Xu§[1]

[1]卡内基梅隆大学计算机科学系[2]佐治亚理工学院计算机科学学院[3]加州大学戴维斯分校数学系

摘要

我们研究两个相关问题的计算复杂性：在$G(n,1/2)$中恢复植入的 q-着色，以及在 $G(n,1/2)$中寻找可高效验证的非q-可着色性证据（又称反证）。我们的主要结果表明，对于这两个问题，一类受限但强大的算法也存在困难；这类算法基于对输入计算低次多项式。

恢复植入的 q-着色问题，等价于恢复覆盖所有顶点的 q 个不相交植入团——这是一个可能比广为研究的植入团问题更容易的变体。我们的第一个结果表明，在低次多项式计算模型中，这一变体与原始植入团问题一样困难：每个团都需要具有大小 $k \gg \sqrt{n}$ ，才能实现高效恢复。对于相关的变体，即这些团覆盖了 $(1-\epsilon)$ 比例的顶点，我们也通过从植入团问题归约证明了其困难性。

我们的第二个结果表明，在低次多项式模型中，当 $q \gg n^{2/3}$ 时，判定 $G(n,1/2)$ 是否不具备 q-可着色性是困难的；而当 $q \lesssim n^{1/2}$ 时则很容易。我们将这一差距留待未来工作弥合。我们的证明比植入团问题中的类似结果更为微妙，并涉及构造一种关于 q-可着色图的非标准分布。我们指出，尽管这项工作与若干先前研究相关，但它是首项明确在低次多项式模型中表述反证问题的工作。

我们的主要结果的证明涉及展示：在一对经过适当构造的分布之间进行假设检验具有低次困难性。对于反证，我们展示了这种方法的 *completeness*：在低次模型中，反证任务的难度恰好等同于最难的相关检验问题；也就是说，要证明反证具有困难性，就需要找到一个“困难”分布。

1 引言

植入团问题由 [Jer92] and [Kuˇc95], 提出，要求设计一种多项式时间算法，在埃尔德什–雷尼随机图 $G(n,1/2)$ 中找到一个大小为 k 的团。与之相关的任务是在 $G \sim G(n,1/2)$ 中否定 k-团的存在，即设计一种多项式时间算法，计算一个可高效验证的证书，以推断 G 中不存在 k-团。尽管已有大量研究，两项问题目前最先进的多项式时间算法 [AKS98] 仅在 $k = \Omega(\sqrt{n})$ 时才能成功。相比之下， $G(n,1/2)$ 的团数以高概率至多为 $\lceil 2\log_2 n \rceil + 1$，因此，任何大小为 $k > \lceil 2\log_2 n \rceil + 1$ 的植入团都可被唯一识别。在马尔可夫链 [Jer92], 、统计查询模型 [FGR+17]、凸松弛 [FK03], 尤其是平方和层次及相关的计算低次多项式模型 [BHK+16、Hop18], 等各种受限模型中，已有大量下界研究。这些结果表明，两种变体的算法阈值——即高效算法能够找到所添加的 k-团，或否定 $G(n,1/2)$ 中存在 k-团的最小 k ——为 $\Omega(\sqrt{n})$。

*电子邮箱： praveshk@cs.cmu.edu。本研究得到 NSF CAREER奖 #2047933、阿尔弗雷德·P·斯隆奖学金和谷歌研究学者奖的支持。

†电子邮箱： vempala@gatech.edu。本研究部分得到 NSF 项目 CCF-2007443 和 CCF-2106444 的资助。

‡电子邮箱： aswein@ucdavis.edu。本研究部分工作是在佐治亚理工学院算法与随机性中心任职期间完成的，并得到 NSF 项目 CCF-2007443 和 CCF-2106444 的资助。§电子邮箱： jeffxusichao@cmu.edu。本研究部分得到 NSF CAREER奖 #2047933 的资助。

在过去二十年里，“不存在能够超越已知算法上述保证的多项式时间过程”这一假设，已成为平均情形复杂度理论的一个焦点，也成为大量归约的根源；这些归约指向各个领域中出现的平均情形问题（例如，[BR13、HWX15、BBH18、KM18]）。

两个动机问题：恢复和反证 q-着色。本文研究以下看似无害（表面上也比植入团更容易）的问题：在恢复问题中，我们研究以高成功概率精确恢复 $G \sim G(n, 1/2)$ 中的 $\approx n/k$ 个互不相交的植入 k-团的复杂度。如果这些不相交的植入团覆盖了图中的所有顶点，那么该图的补图就有一个植入的 (n/k)-着色。因此，这个问题的这一版本等同于研究：在 $G(n, 1/2)$ 中恢复一个植入的 q-着色，是否比恢复一个植入团更容易。在相关的反证问题中，目标是找到一种算法，以图 G 为输入并输出 NO 或 MAYBE，同时保证：(1) 每当算法输出 NO 时，该图必定不允许对其顶点进行有效的 q-着色；(2) 当 $G \sim G(n, 1/2)$ 时，算法应以 $1 - o(1)$ 的概率输出 NO，其中概率是针对 G 的抽样而言。

恢复任务与反证任务之间的关系颇为微妙：尽管这两个问题看起来彼此相关，但据我们所知，目前尚无任何方向上的正式归约。在本文中，我们分别研究恢复问题和反证问题，并指出，要在这两种情形下证明下界，需要采用截然不同的方法。我们注意到，对于稀疏随机正则图的可着色性，恢复阈值与反证阈值之间似乎存在一个常数因子的差距 [BBK+21]。

证明策略：假设检验。理解恢复或反证复杂度的一种常见策略，是引入一个辅助假设检验任务：给定一个图 G，它可能是从某个“零假设”分布 $\mathbb{Q}$（例如，$G(n, 1/2)$）或某个“植入”分布 $\mathbb{P}$（例如，某个集中于 q-可着色图上的分布）中抽样得到的，设计一个可高效计算的统计检验，以较高的成功概率判断给定样本 G 是由这两个分布中的哪一个生成的，其中成功概率取自对 G的抽样。注意，如果对于某个分布 $\mathbb{Q}$存在高效的反证算法，那么我们立即可以得到一个区分 $\mathbb{Q}$ 与任意集中于 q-可着色图上的分布 $\mathbb{P}$ 的高效区分器。类似地，如果对于某个分布 $\mathbb{P}$存在高效的恢复算法，那么我们立即可以得到一个区分 $\mathbb{P}$ 与任意集中于非-q-可着色图上的分布 $\mathbb{Q}$ 的区分算法。基于这种联系，我们可以得出：

（I）要证明在特定的植入分布 $\mathbb{P}$ 中，精确恢复植入的 q-着色在计算上是困难的，只需构造一个零分布 $\mathbb{Q}$，使得 (i) 以高概率，$G \sim \mathbb{Q}$ 不可 q-着色；且 (ii) 在计算上难以区分 $\mathbb{P}$ 与 $\mathbb{Q}$。

（II）要证明对于特定的零分布 $\mathbb{Q}$，反证 q-可着色性在计算上是困难的，只需构造一个植入分布 $\mathbb{P}$，使得 (i) $\mathbb{P}$ 的支撑集包含于 q-可着色图；且 (ii) 在计算上难以区分 $\mathbb{P}$ 与 $\mathbb{Q}$。

请注意，我们可以灵活选择 $\mathbb{Q}$（若研究恢复）或 $\mathbb{P}$（若研究反证）。我们将在后文看到，构造合适的分布可能并非易事。研究恢复和研究反证时，出现的检验问题不一定相同。

策略（II）被称为构造计算上静默的植入分布[BKW20]，其中“静默”指的是高效算法无法检测到植入结构的存在。同样，策略（I）对应于构造计算上静默的零假设分布。

目前，基于标准困难性假设证明平均情形假设检验问题的下界仍是一项难以企及的目标（尽管近期已有一些成功成果 [BBH18，BB20]在某些有限的情形下，以植入团及其变体的困难性为出发点），因此，我们将聚焦于一类受限但功能强大且经过充分研究的检验，以此为检验问题的困难性提供证据。接下来，我们将介绍这类检验。

低次检验。假设检验的低次多项式模型将检验的类别限制为输入的一种自然表示上的多项式函数，并以多项式的次数来衡量检验的复杂度。具体而言，将图视为 $\{-1, 1\}^{\binom{n}{2}}$ 中的元素，并用 $\{\pm 1\}$ 指示变量表示每条可能边

是否存在，低次多项式检验可以粗略地理解为计算边指示变量的任意次数为 D 的多项式的阈值。由于次数为 D 的多项式可以在时间 $n^{O(d)}$ 内计算（若以单项式系数表示），常数次检验可得到多项式时间区分算法。尽管受到限制，这些低次检验已经涵盖了基于图的基本统计量的检验，例如边数、三角形数，以及更一般的小子图计数（子图中的边数对应于多项式的次数）。各种谱方法（例如邻接矩阵的最大特征值，或某个其他对称矩阵的最大特征值，其矩阵元素是输入变量的低次多项式）也可以用关于变量数量的对数次数多项式检验来近似；参见 [KWB22，第 4.2 节。3]。因此，对于各种高维统计检验任务，低次检验（次数为 $O(\log n)$）已经涵盖了目前已知的最佳多项式时间算法（尽管我们在此不打算精确刻画哪些任务属于此类；讨论可参见例如 [HKP+17、Hop18、KWB22、HW21、ZSWB22] ）。因此，如果我们能够证明，对于某个 $D = \omega(\log n)$，所有次数为 D 的检验都无法解决某个特定检验问题，就称该问题是“低次困难”的。这可以被视为假设检验问题在计算上困难的证据。这是一个适用范围广、如今已被普遍采用的框架，起源于一系列针对平方和层级证明下界的工作 [BHK+16、HS17、HKP+17] （进一步阐述另见 [Hop18、KWB22] ）。

结果概述。我们的主要结果运用上述策略 (I) 和 (II)，揭示了恢复和反证 q-着色的计算复杂度。形式化模型和论述将在下一节给出，这里先作简要概述。在全文中，我们将默认假设处于渐近范围 $n \to \infty$，此时其他参数（例如 q、k）可能随 n 缩放。若某事件发生的概率为 $1 - o(1)$（当 $n \to \infty$ 时），我们称其以“高概率 (w.h.p.)”发生。由于我们关注的是确定精确到 n 的正确幂次的计算阈值，因此在非正式讨论中，我们用符号 $\ll$ 隐去 $n^{o(1)}$ 因子。

我们关于恢复问题的主要结果表明，加入 $\approx n/k$ 个大小为 k 的互不相交团（而非单个团），并不会让恢复所添加的植入团变得更容易。也就是说，我们的下界表明，每个添加的团都需要达到大小 $\gtrsim \sqrt{n}$，高效恢复才有可能实现。

相比之下，或许令人惊讶的是，事实证明，增加更多团后，仅通过计算边总数，就能更容易地区分植入图与 $G(n, 1/2)$。这揭示了一个检测-恢复差距，这与单个植入团问题形成对比（见第2.1.2节）。

更确切地说，我们关于恢复的结果如下：

- 在植入部分着色模型中，部分顶点被着色（等价地，在 $G(n, 1/2)$ 中存在许多不相交植入团，它们至多覆盖图的 $(1-\epsilon)$-比例），我们证明：

  (i) 如果每个团的大小为 $k \gg \sqrt{n}$，则可以使用一种简单算法恢复这些团。
  (ii) 如果每个团的大小为 $k \ll \sqrt{n}$，那么在植入团假设下，恢复这些团在计算上是困难的。也就是说，恢复许多植入的 k-团，与恢复单个植入的 k-团同样困难。

- 在完整植入着色模型中（q 个大小为 $k = n/q$ 的植入团划分整个图），我们无法通过归约证明其难度，而是给出一个间接论证，支持与上述相同的结论：

  (i) 如果每个团的大小为 $k \gg \sqrt{n}$，则同样存在一个简单算法可以恢复它们 .
  (ii) 如果每个团的大小为 $k \ll \sqrt{n}$，我们通过策略 (I) 论证恢复在计算上是困难的，其中将零分布 $\mathbb{Q}$ 设为植入的 $(q+1)$-着色。换言之，我们证明，低次数测试甚至无法区分植入的 q-可着色图与植入的 $(q+1)$-可着色图。这表明，可以通过第 2.1.3 节所述的两阶段论证，推得恢复的难度。

对于反证 q-可着色性问题（在 $G(n, 1/2)$ 中），已知当$k := n/q \gg \sqrt{n}$ [CO05]时，存在多项式时间算法。为探究这一问题的复杂度，我们首次明确提出了低次多项式模型中的反证问题，并证明如下：

- 如果 $k \gtrsim \sqrt{n}$（即 $q \lesssim \sqrt{n}$），那么存在一个低次多项式，可以反证 q-可着色性问题（在 $G(n,1/2)$ 中）。
- 如果 $k \ll n^{1/3}$（即 $q \gg n^{2/3}$），那么没有低次多项式能反证 $G(n,1/2)$ 中的 q-可着色性。证明采用策略（II），并涉及构造一个非平凡的植入分布 $\mathbb{P}$。
- 我们猜想 $k \sim \sqrt{n}$ 是真正的低次反证阈值，并将此留待未来工作。改进下界的一种方法是构造一个“更安静”的植入分布，也就是说，构造一个支撑在 q-可着色图上的分布，使得当 $k \ll \sqrt{n}$ 时，难以用低次方法将其与 $G(n,1/2)$ 区分。我们的最终结果是一个对偶性论证，表明事实上，该猜想等价于此类植入分布的存在。

2 结果

本研究的一个核心概念是对两个高维分布进行假设检验。我们考虑两个（序列）分布 $\mathbb{P} = \mathbb{P}_n$ 和 $\mathbb{Q} = \mathbb{Q}_n$。对我们而言，这些分布始终定义在 n 个顶点的图上。我们采用以下关于成功检验的渐近概念。

定义 2.1（强区分）。对于两个分布 $\mathbb{P}_n$ 和 $\mathbb{Q}_n$，如果一个算法 A_n 强区分 $\mathbb{P}$ 和 $\mathbb{Q}$，即以从这两个分布之一抽取的样本作为输入，并以概率 $1 - o(1)$ 正确判断样本来自哪个分布（当 $n \to \infty$ 时），我们就称该算法能够强区分这两个分布。换言之，第一类和第二类错误概率都必须是 $o(1)$。

我们还将关注以下这类“低次数”检验。次数为 D 的检验就是输入变量的一个（多元）多项式（或者更确切地说，是一系列这样的多项式，对每个问题规模 n 各有一个）。在我们的情形中，将有 $\binom{n}{2}$ 个输入变量——对于一个有 n 个顶点的图，每条可能的边对应一个变量——其取值为 $\{\pm 1\}$，其中 $+1$ 表示存在一条边，-1 表示不存在边。我们采用以下关于多项式检验“成功”的标准定义。

定义 2.2（分布的强分离/弱分离）。设 $\mathbb{P}_n$ 和 $\mathbb{Q}_n$ 是某个 $N = N_n$上的分布。一旦 $n \to \infty$，若多项式 $f_n : \mathbb{R}^N \to \mathbb{R}$ 满足以下条件，则称其强分离 $\mathbb{P}$ 和 $\mathbb{Q}$，

$$\sqrt{\max\left\{\operatorname*{Var}_{\mathbb{Q}}[f], \operatorname*{Var}_{\mathbb{P}}[f]\right\}} = o\left(\left|\operatorname*{\mathbb{E}}_{\mathbb{P}}[f] - \operatorname*{\mathbb{E}}_{\mathbb{Q}}[f]\right|\right),$$

若满足以下条件，则称其弱分离 $\mathbb{P}$ 和 $\mathbb{Q}$：

$$\sqrt{\max\left\{\operatorname*{Var}_{\mathbb{Q}}[f], \operatorname*{Var}_{\mathbb{P}}[f]\right\}} = O\left(\left|\operatorname*{\mathbb{E}}_{\mathbb{P}}[f] - \operatorname*{\mathbb{E}}_{\mathbb{Q}}[f]\right|\right).$$

请注意，强分离意味着 $\mathbb{P}$ 和 $\mathbb{Q}$ 可以通过对多项式 f的值设定阈值来强区分。弱分离意味着 f 的输出可用于实现优于随机猜测的区分；参见 [BEH+22，命题 6。1]。

在我们的情形中，输入变量的取值属于 $\{\pm 1\}$，因此不失一般性，多项式 f 可以是多线性的。

如果对于某个 $D = \omega(\log n)$，所有次数为 D 的多项式都无法强分离 $\mathbb{P}$ 和 $\mathbb{Q}$，则称该检验问题为“低次困难”。正如引言中所述，这可以视为强区分存在内在计算困难性的证据。

排除强分离或弱分离的证明通常通过界定下文定义的优势来进行：

$$\mathsf{Adv}_{\le D}(\mathbb{P}, \mathbb{Q}) \coloneqq \sup_{f \in \mathbb{R}[Y]_{\le D}} \frac{\operatorname*{\mathbb{E}}_{\mathbb{P}}[f]}{\sqrt{\operatorname*{\mathbb{E}}_{\mathbb{Q}}[f^2]}}, \tag{1}$$

其中 $\mathbb{R}[Y]_{\le D}$ 表示次数至多为 $\mathbb{R}^N \to \mathbb{R}$ 的多项式集合 D。众所周知，$\mathsf{Adv}_{\le D}$ 还可以表示为低次似然比的范数；参见 [Hop18、KWB22]。如果 $\mathsf{Adv}_{\le D} = O(1)$，则不可能实现强分离；如果 $\mathsf{Adv}_{\le D} = 1 + o(1)$，则不可能实现弱分离（见引理 4.1）。

2.1 恢复

2.1.1 模型

本节的主要目标是理解植入着色和植入部分着色这两个相关模型中的恢复问题。正如引言中所述，一个q-可着色图的补图可划分为 q 个团。为统一记号并与标准植入团模型进行比较，我们在此采用团的视角。因此，我们研究在$G(n,1/2)$中植入多个团的问题。

第一个模型 MC(n,q)（“多个团”）对应于真正的植入着色，即这些团划分了整个图。

定义 2.3。在模型 MC(n,q) 中，我们观测到一个具有 n 个顶点的图，其中每个顶点都独立地从 $[q]:=\{1,2,\dots,q\}$ 中均匀随机地分配一个标签。标签相同的顶点始终连通，而标签不同的顶点以 $1/2$ 的概率连通。给定该图，目标是以概率 $1-o(1)$ 精确恢复团划分，其中 $n\to\infty$，且 $q=q_n$ 可以随 n 增长。

下一个模型是部分着色的一种变体，即这些团并不划分整个图。为技术上的便利起见，该模型中的团大小完全相同，这不同于 MC(n,q)。

定义 2.4。在模型 MC(n,q,δ) 中，我们观测到一个具有 n 个顶点的图，其中 $(1-\delta)n$ 个顶点被划分为 q 个团，每个团的大小恰好为 $k:=(1-\delta)n/q$（我们假设其为整数）。同一团中的两个顶点始终连通，其余所有边均以 $1/2$ 的概率独立出现。给定该图，目标是以概率$1-o(1)$精确恢复团划分（并识别非团顶点），其中 $n\to\infty$，且参数 $q=q_n$ 和 $\delta=\delta_n$ 可以随 n 增长。

2.1.2 通过归约证明植入部分着色的困难性

现在考虑 MC(n,q,δ) 中的恢复问题。首先我们注意到，当 $k\gg\sqrt{n}$ 时，一种基于检查度数和公共邻居的简单算法可以精确恢复这些团。这与已知最优的、在 $G(n,1/2)$ 中恢复单个植入 k-团的算法在对数因子范围内相符。

定理 2.5（上界）。如果 q,δ 随 n 增长，且满足 $k:=(1-\delta)n/q=\omega(\sqrt{n\log n})$，那么存在一种多项式时间算法，能够在 MC$(n,q,\delta)$ 中以高概率实现精确恢复。

接下来我们证明一个匹配的下界：当 $k\ll\sqrt{n}$ 时，恢复这些团在计算上是困难的。此结果以植入团假设为条件；该猜想常被用作推导平均情形困难性结果的基础。在植入团模型 PC(N,K) 中，一个具有 N 个顶点的图含有一个由 K 个顶点构成的团，其余所有边均以概率 $1/2$独立出现。以下版本的猜想，例如见于 [BBH18]中的猜想 2.1。

猜想 2.6 (植入团假设)。若 $K=K_N$ 按 $K\le N^{1/2-\Omega(1)}$ 的尺度增长，则不存在任何一系列随机多项式时间算法 B_N 能够强区分（定义 2.1）PC(N,K) 与$G(N,1/2)$。

假设该猜想成立，我们可以得到关于 MC(n,q,δ) 的以下困难性结果。

定理 2.7 (下界)。假设植入团假设（猜想 2.6）成立。若 q,δ 按n 的尺度增长，使得 $k:=(1-\delta)n/q$ 满足 $(2+\Omega(1))\log_2 n\le k\le(\delta n)^{1/2-\Omega(1)}$ 则不存在任何一系列随机多项式时间算法 A_n 能够以高概率在 MC(n,q,δ)中实现精确恢复。

条件 $(2+\Omega(1))\log_2 n\le k$ 是自然的，因为 $2\log_2 n$ 是 $G(n,1/2)$ 中最大团的大小。要满足条件 $k\le(\delta n)^{1/2-\Omega(1)}$，只需有 $k=n^{\frac{1}{2}-\Omega(1)}$ 且 $\delta=n^{-o(1)}$。

证明定理 2.7 的归约非常简单，但（据我们所知）此前尚未见诸文献。直观而言，其思路如下：在多团模型中，即使预言机揭示了除一个团之外所有团的位置，剩下的问题仍然是植入团的一个困难实例。

注 2.8. 我们指出，当 $k\ll\sqrt{n}$ 时，植入团假设还意味着在 $n,1/2$ 的 G 中检测常数个植入 k 团是困难的。思路是先通过从植入团出发的归约证明，区分 q 个植入团和 $(q+1)$ 个植入团是困难的；该归约只需添加 q 个新团（位于新顶点上）。随后，经典的“混合论证”意味着，对于任意常数 q，区分 0 个团和 q 个团是困难的。（感谢 Guy Bresler 指出了这一论证。）

检测-恢复差距。在标准植入团模型中（只有一个团），$k \sim \sqrt{n}$ 是目前已知的、同时适用于高效恢复团和高效“检测”团的最佳阈值；所谓“检测”，即区分植入团模型与 $G(n,1/2)$。虽然我们已经证明，增加团的数量并不会让恢复变得更容易，但这确实会让检测变得更容易。例如，在极端情况下，若这些团覆盖整个图，那么只要 $q = o(n)$，边的总数就能显著地区分 MC(n,q) 与 $G(n,1/2)$。因此，多团问题呈现出单团情形中不存在的“检测-恢复差距”。

我们指出，我们的归约是一个罕见的（或许是独一无二的？）例子：它基于植入团假设建立了检测-恢复差距。例如，先前关于各种植入矩阵和图问题的研究[BBH18] 只能在这样一种情形下证明恢复的困难性：若归约自某个起始问题（并非植入团问题），且该问题已被猜想存在检测-恢复差距，那么检测是容易的。而 [CLR17] 声称通过将植入团归约到植入子矩阵恢复来克服这一问题，但其论证并不正确。[1]

最后我们指出，“检测-恢复差距”这一概念或许有些人为，因为它假定我们已为恢复问题选定一个“典型”的检验问题与之对应（本文避免采用这种视角）。

2.1.3 检验 q-可着色性与 $(q+\ell)$-可着色性

上一节的结果并未完全涵盖真着色的情形，即团划分整个图的情形。在这种情况下，当 $k := n/q \gg \sqrt{n}$ 时，精确恢复仍然容易；而当 $k \ll \sqrt{n}$ 时，我们预计它很困难；然而，我们不知道如何通过从植入团归约来证明这一点。我们将改为遵循引言中的策略 (I)：固定 $\mathbb{P} = \text{MC}(n,q)$，目标是设计一个零分布 $\mathbb{Q}$，使得以高概率 $G \sim \mathbb{Q}$ 不是 q-可着色的（或者更确切地说，它的补图不是），并且区分 $\mathbb{P}$ 与 $\mathbb{Q}$ 是低次困难的。实现这一目标后，我们便得到一个间接的两阶段论证来证明恢复的困难性：低次困难性使我们猜想不存在多项式时间算法能够区分 $\mathbb{P}$ 与 $\mathbb{Q}$；而这一猜想（若为真）正式意味着，不存在多项式时间算法能够恢复 $\mathbb{P}$ 中的团。

或许最自然的初步尝试是选择 $\mathbb{Q} = G(n,1/2)$。然而，这还不够，因为由于上一节讨论的检测-恢复差距，$G(n,1/2)$ 与 MC(n,q) 太容易区分了。我们将改为选择 $\mathbb{Q} = \text{MC}(n,q+1)$；当 $q \le \Omega(n/\log n)$ 时，它以高概率不是 q-可着色的；参见附录 A。我们将证明，当 $k := n/q \ll \sqrt{n}$ 时，检验 $\mathbb{P} = \text{MC}(n,q)$ 与 $\mathbb{Q} = \text{MC}(n, q+1)$ 的问题是低次困难的。如上所述，这意味着当 $k \ll \sqrt{n}$ 时，MC(n,q) 中的精确恢复很困难。

实际上，我们将考虑一个稍微更一般的检验问题：对某个 $\ell \ge 1$（其可能随 n 缩放），区分 $\mathbb{P} = \text{MC}(n,q)$ 与 $\mathbb{Q} = \text{MC}(n,q+\ell)$。这种一般化不会给我们带来太多额外负担，而且我们认为这是一个可能具有独立研究价值的问题。以下结果表明，在低阶框架下，当 $q^2 \ll \ell n$ 时该问题容易，而当 $q^2 \gg \ell n$ 时则困难。

定理 2.9（上界）。如果 q、ℓ 按照 n 缩放，使得 $1 \le q < q+\ell \le n$ 且 $q^2 = o(\ell n)$，那么存在一个 1 次多项式，在 $\mathbb{P} = \text{MC}(n,q)$ 与 $\mathbb{Q} = \text{MC}(n,q+\ell)$ 之间实现强分离。

定理 2.10（下界）。固定任意常数 $\epsilon > 0$，且该常数不依赖于 n。如果 q、ℓ 按照 n 缩放，使得 $1 \le q < q+\ell \le n$ 且 $q^2 \ge \ell n^{1+\epsilon}$，那么不存在一个次数为 $o(\log n/\operatorname{loglog} n)$ [2] 的多项式，能够在 $\mathbb{P} = \text{MC}(n,q)$ 与 $\mathbb{Q} = \text{MC}(n,q+\ell)$ 之间实现弱分离。

检验植入与植入。从技术层面来说，这个结果与几乎所有现有的低次下界都不同，因为这里检验的是两个不同的“植入”分布。相比之下，以往的大多数工作研究的是某个植入分布与独立同分布的零分布之间的检验，而这种情况更容易分析。最近，[RSWY22], 基于 [SW22]提出了首批“植入对植入”的低次下界。我们的证明基于类似的思想，但在技术层面上与 [RSWY22] 有所不同；RSWY22] 中关于稠密子图问题的下界并不

[1]第 21—22 页的[CLR17]（arXiv v2）中的式（42）自举构造实际上并未生成子矩阵模型的实例，因为噪声矩阵的各个元素并非相互独立。第 22 页顶部附近存在一个问题：成对独立性并不意味着相互独立性。该归约确实证明了某种非标准子矩阵模型的困难性，其中噪声元素并非相互独立。

适用于子图极其稠密的情形（例如团），因此我们采用了略有不同的论证变体。

关键的技术挑战在于，由于 $\mathbb{Q}$ 不是独立同分布的，我们不知道有哪些便于使用的多项式正交基（相对于 $\mathbb{Q}$）。命题 4.2 克服了这一困难，表明只需控制某些递归定义的量 w_α即可。这推广了标准方法；参见注释 4.3。与 [RSWY22], 类似，量 w_α 具有一种便于分析的乘法性质（引理 4.4）。

我们指出，证明原始恢复问题具有困难性的另一种证据形式，是按照 [SW22], 的思路直接提出一个低次数恢复问题；但我们选择改为研究静默植入方法。

2.2 反证

研究反证问题平均情形复杂性的一种常见框架，是证明针对平方和（SoS）层级的下界。平方和（SoS）层级是一类基于半定规划的强大方法。对于反证 q-可着色性的问题，已知某种特定的 SoS 公式在$q \gg \sqrt{n}$ [KM21]中会失效；然而，对于更规范（且可能更强）的 SoS 半定规划，如何对其进行刻画仍是一个开放问题。该规划采用等式约束，而非不等式（参见 [KM21]的第 1.5 节）。

在本文中，我们提出了一种基于低次多项式的替代性反证下界表述，它直接建立在低次多项式之上，并对 SoS 方法形成补充。这种新表述的优点包括简洁，而且（与 SoS 不同）半定规划松弛的选择不存在歧义；我们只需说明如何将输入编码为实值变量。据我们所知，SoS 下界与我们的新框架之间，在任一方向上都不存在正式的蕴含关系。与 SoS 一样，我们的框架也涵盖谱方法（如下文定理2.16 的证明所示）。谱方法是一类强大的反证算法，能够为各种平均情形反证任务提供目前已知的最佳多项式时间算法。

我们注意到，先前有些工作通过低次下界来为反证问题的困难性提供证据，其方法是采用两阶段论证：首先将一个检验问题多项式时间归约到反证问题 [BKW20，BKW22]。我们的新框架在思路上相似，但更为直接，因为我们首次定义了多项式解决反证问题的含义（定义2.11）。

2.2.1 低次数反证框架

现在，我们将定义一种概念（定义 2.11），用以说明多项式反证某种性质意味着什么$\mathcal{R} \subseteq \mathbb{R}^N$（例如，$q$-可着色图的集合 $X \in \{\pm 1\}^{\binom{n}{2}}$）在分布 $\mathbb{Q}$（例如，$G(n, 1/2)$）上。稍后我们将论证，这一定义是合理的，因为它确实意味着反证问题的一个解（命题2.13）。我们还将说明，我们的定义涵盖了谱方法这一类强大的反证算法（见定理2.16的证明）。

定义 2.11（分布与性质的强／弱分离）。设 $\mathbb{Q}_n$ 是定义在 $\mathbb{R}^N$ 上的一个分布，其中某个 $N = N_n$，并设 $\mathcal{R} = \mathcal{R}_n \subseteq \mathbb{R}^N$。若多项式 $f_n \colon \mathbb{R}^N \to \mathbb{R}$ 满足以下条件，则称其强分离 $\mathbb{Q}$ 与 $\mathcal{R}$

$$f(X) \geq 1 \quad \forall X \in \mathcal{R} \qquad and \qquad \mathop{\mathbb{E}}_{\mathbb{Q}}[f^2] = o(1),$$

若满足以下条件，则称其弱分离 $\mathbb{Q}$ 与 $\mathcal{R}$

$$f(X) \geq 1 \quad \forall X \in \mathcal{R} \qquad and \qquad \mathop{\mathbb{E}}_{\mathbb{Q}}[f] = 0, \ \mathop{\mathbb{E}}_{\mathbb{Q}}[f^2] = O(1).$$

注 2.12。条件 $\mathbb{E}_{\mathbb{Q}}[f] = 0$ 可以选择性地添加到强分离的定义中：如果 $f = f_n$ 满足原始定义，则可以对其进行平移和缩放，使其满足修改后的定义。

更一般地，可以将分离定义为：存在 $B = B_n > \mathbb{E}_{\mathbb{Q}}[f]$，使得对所有 $X \in \mathcal{R}$，$f(X) \geq B$，且 $\sqrt{\mathrm{Var}_{\mathbb{Q}}[f]}$ 为 $o(B - \mathbb{E}_{\mathbb{Q}}[f])$（强分离）或 $O(B - \mathbb{E}_{\mathbb{Q}}[f])$（弱分离）。从以下意义上说，这与原定义等价：如果 $f = f_n$ 满足原定义，那么它也满足取 $B = 1$ 时的新定义；如果 f 满足新定义，则可以对其进行平移和缩放，使其满足原定义。

接下来我们将看到，强分离和弱分离是自然的充分条件：分别通过计算 f，以高概率或常数概率否定 $\mathcal{R}$。

命题 2.13. 假设 f 强（或弱，分别）分离 $\mathbb{Q}$ 和 $\mathcal{R}$。定义一个反证算法，其输入为 $X \in \mathbb{R}^N$，若 $f(X) < 1$，则输出 NO，否则输出 MAYBE。则该算法具有以下保证：(1) 每当它输出 NO 时，$X \notin \mathcal{R}$；(2) 当 $X \sim \mathbb{Q}$ 时，输出为 NO 的概率为 $1 - o(1)$（或 $\Omega(1)$，分别）。

证明. 保证 (1) 直接由性质 $f(X) \geq 1$ 对所有 $X \in \mathcal{R}$ 成立得出。对于强分离，(2) 可由马尔可夫不等式推出：$\mathbb{E}[f^2] = o(1)$ 意味着 $|f(X)| < 1$ 以概率 $1 - o(1)$ 成立。接下来验证弱分离下的 (2)：令 $\mathbb{E}_{\mathbb{Q}}[f^2] \leq C$ 和 $p \coloneqq \Pr_{\mathbb{Q}}\{f(X) < 1\}$，

$$0 = \mathbb{E}[f] \geq 1 \cdot \Pr\{f \geq 1\} + \mathbb{E}[f \cdot \mathbb{1}_{f<1}] \geq (1-p) - \sqrt{\mathbb{E}[f^2]} \cdot \sqrt{p} \geq 1 - p - C\sqrt{p} \geq 1 - (C+1)\sqrt{p},$$

这意味着 $p \geq 1/(C+1)^2$。 □

与引言中的策略（II）一致，排除强分离（或弱分离）的一种方法是构造一个植入分布，并对以下量 $\mathsf{Adv}_{\leq D}$（定义见（1））进行界定。

命题 2.14。假设对于 n 个值的一个无限子序列，我们有一个分布 $\mathbb{P} = \mathbb{P}_n$，其支撑集为 $\mathcal{R}$。若对于某个 $D = D_n$，$\mathsf{Adv}_{\leq D}(\mathbb{P}, \mathbb{Q}) = O(1)$（分别地，$1 + o(1)$），则不存在次数为 D 的多项式能够强分离（分别地，弱分离）$\mathbb{Q}$ 和 $\mathcal{R}$。

证明。由于 $\mathbb{P}$ 的支撑集为 $\mathcal{R}$，分离条件意味着 $\mathbb{E}_{\mathbb{P}}[f] \geq 1$。证明现在几乎与引理4.1的证明完全相同。 □

注 2.15。我们注意到，对于在 $G(n, 1/2)$ 中反驳单个 k-团这一研究充分的问题，现有工作在我们的新框架下给出了紧的上界和下界。对于下界，令 $\mathbb{P}$ 为标准的植入 k-团模型，并结合命题 2.14 与植入团的低次分析 [Hop18，第 2.4 节]，得出：若 $k \leq n^{1/2-\epsilon}$ 对某个常数 $\epsilon > 0$ 成立，则不存在次数为 $o(\log n/\log\log n)^2$ 的多项式，能够将 $G(n, 1/2)$ 与具有 k-团这一性质弱分离。上界则由下文定理 2.16 的证明得出：若 $k \geq 2.1\sqrt{n}$，则存在一个次数为 $O(\log n)$ 的多项式，能够将 $G(n, 1/2)$ 与具有 k-团这一性质强分离。

2.2.2 q-可着色性的低次反证

现在，我们将上一节的框架应用于在 $G(n, 1/2)$ 中反驳 q-可着色性的问题。与通常做法一样，全文将图表示为 $\{\pm 1\}^{\binom{n}{2}}$ 的元素，取 $\mathbb{Q} = G(n, 1/2)$，并用 $\mathcal{R}_q \subseteq \{\pm 1\}^{\binom{n}{2}}$ 表示 q- 可着色性这一性质（即所有 q- 可着色图组成的集合）。

首先，我们给出一个上界：低次多项式可以对 $q \lesssim \sqrt{n}$ 反驳 q-可着色性。证明方法是采用一种标准的谱反证算法（基于邻接矩阵的最大特征值），并用多项式对其进行近似。

定理 2.16（上界）。假设 $q \leq b\sqrt{n}$ 对某个常数 $b < 1/2$ 成立（该常数不依赖于 n）。那么存在一个常数 $C = C(b) > 0$，以及一个次数至多为 $C \log n$ 的多项式 $f = f_n$，使其强分离 $G(n, 1/2)$ 与 $\mathcal{R}_q$。

我们还给出了一个下界：不存在低次数多项式能够否证 $q \gg n^{2/3}$ 的 q-可着色性。请注意，我们的上界与下界之间存在差距，弥合这一差距是留待未来研究的一个有趣方向。

定理 2.17（下界）。如果 $q \geq n^{2/3+\epsilon}$ 对于某个常数 $\epsilon > 0$成立，那么不存在次数为-$o(\log n/\log\log n)^2$ 的多项式弱分离 $G(n, 1/2)$ 和 $\mathcal{R}_q$。

下界的证明将用到命题 2.14，它是引言中策略（II）的严格化表述。换言之，我们的目标是构造一种植入分布 $\mathbb{P}$，其支撑集为 q-可着色图，并且在 $\mathbb{Q} = G(n, 1/2)$ 的意义下难以与之区分 $\mathsf{Adv}_{\leq D}(\mathbb{P}, \mathbb{Q}) = 1 + o(1)$。

构造这种植入分布并非易事。最直观的选择是“典范”植入模型 $\mathrm{MC}(n,q)$（或者说，它的补图），但这并不是一个好选择，因为只要 $q \ll n$，就能通过计算边总数，轻松地将它与 $G(n,1/2)$ 区分开来。接下来可以尝试修改 $\mathrm{MC}(n,q)$，降低非团边出现的概率，从而校正边总数。这样得到的植入更隐蔽，在 $q \gg n^{3/4}$ 时难以与 $\mathbb{Q}$ 区分；但在 $q \ll n^{3/4}$ 时，只要计算带符号三角形就能轻松区分（完全图中的 $\binom{n}{3}$ 个三角形中，若其边中有偶数条存在，则每个三角形计为 $+1$；若有奇数条存在，则计为 -1）。我们下面定义的最终构造能够达到阈值 $q \sim n^{2/3}$，它更加复杂，同时植入了团和独立集。

定义 2.18（针对 $q \gg n^{2/3}$ 的静默植入）。设 n、q 为正整数。对 n 个顶点中的每一个，独立地从 $(a,\ b) \in [q]\times[q]$ 中均匀随机分配一个标签。给定这些标签后，对每一对不同的顶点 $\{u,v\}$ 独立地执行以下操作：将这两个顶点的标签分别记为 $(a_1,\ b_1)$ 和 $(a_2,\ b_2)$；若$a_1 = a_2$，则不包含边 $(u,\ v)$；若 $a_1 \neq a_2$ 且 $b_1 = b_2$，则包含边 $(u,\ v)$；否则，以概率 $1/2$ 包含边 $(u,\ v)$。

注意，具有给定 a 值的所有顶点构成一个独立集，因此该分布的支持集包含于 q-可着色图中。此外，具有给定 b 值的顶点几乎构成一个团，只排除了独立集所要求的非边。在定理2.17的证明中，我们证明，当 $G(n,\ 1/2)$ 满足 $q \gg n^{2/3}$ 时，该分布与 $G(n,\ 1/2)$ 在低次下不可区分。我们对该分布的分析是紧的，因为当 $q \ll n^{2/3}$ 时，带符号四环的数量可以将其与 $G(n,\ 1/2)$ 区分开来。

尽管我们尚未证明这一点，但我们预计可着色性的低次反证的真实阈值为 $q \sim \sqrt{n}$。

猜想 2.19。任取一个不依赖于 n 的 $\epsilon > 0$。如果 $q \geq n^{1/2+\epsilon}$，那么对于某个 $D = \omega(\log\ n)$，没有任何次数为 D 的多项式能够弱分离 $\mathbb{Q} = G(n,1/2)$ 与 $\mathcal{R}_q$。

2.2.3 静默植入方法的完备性

证明猜想2.19 的一种自然方法是构造一个更静默的植入分布 $\mathbb{P}$，其支撑集为 q-可着色图，但难以与 $G(n,\ 1/2)$ 区分，其中 $q \gg \sqrt{n}$。然而，人们可能会担心这甚至不可能实现：即使真实的低次反证阈值如我们所预期的那样处于$q \sim \sqrt{n}$，这样的植入分布也可能并不存在。如果确实如此，我们就需要找到一种不依赖静默植入的替代方法来证明该猜想。

我们将以很高的一般性证明，上述假设情形实际上不可能发生：对于每个低次数困难反证问题，都存在一种可用于证明其困难性的植入分布。换言之，猜想 2.19 等价于存在针对 $q \gg \sqrt{n}$ 的静默植入分布。

定理 2.20。固定序列 $N = N_n$、$D = D_n$，$\mathbb{Q} = \mathbb{Q}_n$是 $\mathbb{R}^N$上的一个分布，且 $\mathcal{R} = \mathcal{R}_n \subseteq \mathbb{R}^N$。假设对于每个 n，$\mathbb{Q}$ 的支撑集是有限集，且 $\mathcal{R}$ 是有限集（但这些集合的基数可能依赖于 n）。以下条件等价：

(1) 没有次数为 D 的多项式能将 $\mathbb{Q}$ 和 $\mathcal{R}$ 强分离。

(2) 对于 n 值的一个无限子序列，存在一个支撑于 $\mathcal{R}$ 的分布 $\mathbb{P} = \mathbb{P}_n$，使得 $\mathrm{Adv}^{\leq D}(\mathbb{P},\mathbb{Q}) = O(1)$。

同样，以下条件等价：

(1) 没有次数为 D 的多项式能将 $\mathbb{Q}$ 和 $\mathcal{R}$ 弱分离。

(2) 对于 n 的一个无限子序列，存在一个分布 $\mathbb{P} = \mathbb{P}_n$，其支撑于 $\mathcal{R}$，使得 $\mathrm{Adv}^{\leq D}(\mathbb{P},\mathbb{Q}) = 1 + o(1)$。

注意，我们已经证明了 (2) 蕴含 (1)；参见命题2.14。(1) 蕴含 (2) 的证明使用了冯·诺依曼极小极大原理。

注 2.21。我们假设 $\mathrm{supp}(\mathbb{Q})$ 和 $\mathcal{R}$ 都是有限的（这是 q-着色的相关情形），以简化极大极小原理所需的分析条件，但这些假设可以放宽；参见注 *6.2*。

结合 q-着色的背景，虽然形式上我们不知道当 $q \gg \sqrt{n}$时，是否存在一个低次多项式可以否定 q-着色，但考虑到平方和下界~[KM21] 用来否定 $O(\sqrt{n})$-可着色性 $G(n,1/2)$ q，若 $G(n,1/2)$ 在 $q \approx \sqrt{n}$ 时存在一种计算上难以察觉的植入式 q-着色，尽管我们不知道这种分布的显式构造，但这并不令人意外。若能找到这种构造，或许就能通过伪校准 [BHK+16] 方法，在更强的半正定规划形式中证明平方和下界。

3 多团恢复

3.1 上界

为方便读者，我们重述该定理。

定理 2.5（上界）。若 q, δ 随 n 变化，使得 $k := (1-\delta)n/q = \omega(\sqrt{n \log n})$，则存在一个多项式时间算法，能够在 $\mathsf{MC}(n, q, \delta)$ 中以高概率实现精确恢复。

证明。我们将使用以下标准形式的伯恩斯坦不等式：对于独立随机变量X_1、……、 X_n，若它们满足 $\mathbb{E}[X_i] = 0$ 且几乎必然满足 $|X_i| \le M$，则对任意 $t \ge 0$，有

$$\Pr\left(\sum_{i=1}^{n} X_i \ge t\right) \le \exp\left(-\frac{\frac{1}{2}t^2}{\sum_{i=1}^{n} \mathrm{Var}(X_i) + \frac{1}{3}Mt}\right).$$

固定任意序列 $\alpha_n = \omega(1)$。非团顶点 i 的次数 d_i 服从二项分布$d_i \sim \mathsf{Bin}(n-1, 1/2)$，根据伯恩斯坦不等式，以概率 $1 - n^{-\omega(1)}$ 满足 $d_i \le \frac{n}{2} + \alpha\sqrt{n \log n}$。另一方面，团顶点 i 的次数 $d_i \sim (k-1) + \mathsf{Bin}(n-k, 1/2)$，根据伯恩斯坦不等式，以概率 $1 - n^{-\omega(1)}$ 满足 $d_i \ge \frac{n+k}{2} - \alpha\sqrt{n \log n}$。通过对度进行阈值化，我们可以以概率 $1 - o(1)$ 完美地分类非团顶点，前提是 $k = \omega(\sqrt{n \log n})$。

剩下的任务是划分团顶点。若顶点 i、 j 属于不同的团，则它们的公共邻居数量为 $d_{ij} \sim \mathsf{Bin}(2(k-1), 1/2) + \mathsf{Bin}(n-2k, 1/4)$，以概率 $1 - n^{-\omega(1)}$ 满足 $d_{ij} \le \frac{n}{4} + \frac{k}{2} + \alpha\sqrt{n \log n}$。若顶点 i、 j 属于同一个团，则它们的公共邻居数量为 $d_{ij} \sim (k-2) + \mathsf{Bin}(n-k, 1/4)$，以概率 $1 - n^{-\omega(1)}$ 满足 $d_{ij} \ge \frac{n}{4} + \frac{3k}{4} - \alpha\sqrt{n \log n}$。通过对公共邻居数量设定阈值，我们可以以概率$1 - o(1)$ 精确恢复团划分，前提仍是 $k = \omega(\sqrt{n \log n})$。 □

3.2 通过归约得到下界

为方便读者，我们重新陈述该定理。

定理 2.7 (下界)。 假设植入团假设（猜想 2.6）。若 q， δ 按n 缩放，使得 $k := (1-\delta)n/q$ 满足 $(2 + \Omega(1))\log_2 n \le k \le (\delta n)^{1/2 - \Omega(1)}$ 那么，不存在任何一列随机多项式时间算法 A_n 能够在 $\mathsf{MC}(n, q, \delta)$中以高概率实现精确恢复。

证明。令 q, δ 按照规定的方式缩放。反设存在一个算法 A_n 能够在 $\mathsf{MC}(n, q, \delta)$ 中实现精确恢复。令 $K = k = (1-\delta)n/q$ 和 $N = K + \delta n$。注意，当 $n \to \infty$ 时，我们有 $N \to \infty$，因为

$$N \ge K = k \ge (2 + \Omega(1)) \log_2 n \to \infty,$$

并且 $K \le N^{1/2 - \Omega(1)}$，因为

$$K = k \le (\delta n)^{\frac{1}{2} - \Omega(1)} \le N^{\frac{1}{2} - \Omega(1)}.$$

我们将给出一个算法 B_N，能够在 $G(N, 1/2)$ 与 $\mathsf{PC}(N, K)$ 之间实现强检测，从而与植入团猜想矛盾。

算法 B_N的工作方式如下。给定一个有 N 个顶点的图，添加 $(q-1)k$ 个额外顶点（使总数达到 n），并将它们划分为 $q-1$ 个团，每个团的大小为 k。以概率 $1/2$ 独立地添加所有其他边（包括新顶点之间以及旧顶点与新顶点之间的边）。然后在所得图上运行 A_n。如果它找到 q 个互不相交、大小为 k 的团，且其中一个团完全位于原始的 N 个顶点之中，则输出“$\mathsf{PC}(N, K)$”；否则，输出“$G(N, 1/2)$”。

要论证 B_N 的正确性，首先假设输入来自 $\mathsf{PC}(N,K)$。那么，所生成的有 n 个顶点的图恰好是从 $\mathsf{MC}(n,q,\delta)$ 中抽取的一个样本，因此 A_n 必须以概率 $1-o(1)$ 正确识别出所有团，从而使 B_N 能正确回答 “$\mathsf{PC}(N,k)$”。现在反过来假设， B_N 的输入来自 $G(N,1/2)$。根据假设 $k \geq (2+\Omega(1))\log_2 n \geq (2+\Omega(1))\log_2 N$，以概率 $1-o(1)$，原始的 N 个顶点中不存在大小为 k 的团，此时 B_N 必须正确回答“$G(N,1/2)$”。□

4 团的数量检验

4.1 上界

为方便读者，我们重述该定理。

定理 2.9（上界）。若 q、ℓ 随 n 变化，且满足 $1 \leq q < q+\ell \leq n$ 和 $q^2 = o(\ell n)$，则存在一个一次多项式，能够在 $\mathbb{P} = \mathsf{MC}(n,q)$ 与 $\mathbb{Q} = \mathsf{MC}(n,q+\ell)$ 之间实现强分离。

证明。令 f 为计算图中符号边总数的一次多项式： $f(Y) = \sum_{1\leq i<j\leq n} Y_{ij}$，其中回顾一下 $Y_{ij} \in \{\pm 1\}$。利用期望的线性性，

$$\mathop{\mathbb{E}}_{Y\sim\mathsf{MC}(n,q)} f(Y) = \binom{n}{2}\frac{1}{q}$$

因此

$$\left|\mathop{\mathbb{E}}_{Y\sim\mathbb{P}} f(Y) - \mathop{\mathbb{E}}_{Y\sim\mathbb{Q}} f(Y)\right| = \binom{n}{2}\left(\frac{1}{q}-\frac{1}{q+\ell}\right) = \binom{n}{2}\frac{\ell}{q(q+\ell)}. \tag{2}$$

对于二阶矩，

$$\mathop{\mathbb{E}}_{Y\sim\mathsf{MC}(n,q)} f(Y)^2 = \sum_{i<j}\sum_{i'<j'} \mathbb{E}[Y_{ij}Y_{i'j'}].$$

存　　在几种不同的项需要考虑，具体取决于边 (i,j) 和 (i',j') 如何相互作用　　ct.

- 如果 $(i,j) = (i',j')$，那么 $\mathbb{E}[Y_{ij}Y_{i'j'}] = \mathbb{E}[Y_{ij}^2] = 1$。
- 如果 (i,j) 和 (i',j') 没有公共顶点，那么 Y_{ij}和 $Y_{i'j'}$相互独立，因此 $\mathbb{E}[Y_{ij}Y_{i'j'}] = \mathbb{E}[Y_{ij}]\,\mathbb{E}[Y_{i'j'}] = \frac{1}{q^2}$。
- 如果 (i,j) 和 (i',j') 有一个公共顶点，那么我们同样可以得出 Y_{ij}和 $Y_{i'j'}$相互独立：例如，若 $i=i'$，则 i, j 具有相同标签这一事件，与 i, j' 具有相同标签这一事件相互独立，这是由于 i可能的标签之间具有对称性。因此 $\mathbb{E}[Y_{ij}Y_{i'j'}] = \frac{1}{q^2}$。

综合起来，

$$\mathop{\mathbb{E}}_{Y\sim\mathsf{MC}(n,q)} f(Y)^2 = \binom{n}{2}\cdot 1 + \binom{n}{2}\left[\binom{n}{2}-1\right]\cdot\frac{1}{q^2}$$

因此

$$\begin{aligned}\mathop{\mathrm{Var}}_{Y\sim\mathsf{MC}(n,q)} f(Y) &= \binom{n}{2}\cdot 1 + \binom{n}{2}\left[\binom{n}{2}-1\right]\cdot\frac{1}{q^2} - \left[\binom{n}{2}\frac{1}{q}\right]^2 \\ &= \binom{n}{2}\left(1-\frac{1}{q^2}\right) \\ &\leq \binom{n}{2}.\end{aligned} \tag{3}$$

结合（2）和（3）， f 可实现强分离，条件是

$$\sqrt{\binom{n}{2}} = o\left(\binom{n}{2}\frac{\ell}{q(q+\ell)}\right), \qquad \text{i.e.,} \qquad q\left(\frac{q}{\ell}+1\right) = o(n).$$

因此，只需有 $q = o(n)$ 和 $q^2 = o(\ell n)$。注意， $q = o(n)$ 可由 $q^2 = o(\ell n)$ 与 $\ell \leq n$ 推出。

□

4.2 下界

为方便读者，我们重新陈述该定理。

定理 2.10（下界）。固定任意常数 $\epsilon > 0$，且不依赖于 n。若 q, ℓ 随 n 变化，使得 $1 \le q < q + \ell \le n$ 且 $q^2 \ge \ell n^{1+\epsilon}$，则不存在次数为 $o(\log n / \operatorname{loglog} n)^2$ 的多项式，能够在 $\mathbb{P} = \mathsf{MC}(n, q)$ 与 $\mathbb{Q} = \mathsf{MC}(n, q+\ell)$ 之间实现弱分离。

4.2.1 证明概述

我们首先进行一个标准的变换，说明只需对量 $\mathsf{Adv}^{\le D}$ 给出界。

引理 4.1。设 $\mathbb{P} = \mathbb{P}_n$ 和 $\mathbb{Q} = \mathbb{Q}_n$ 是定义在 $\mathbb{R}^N$ 上的分布，其中 $N = N_n$ 为某个值。对于某个 $D = D_n$，令 $\mathbb{R}[Y]_{\le D}$ 表示次数至多为 D 的多项式 $\mathbb{R}^N \to \mathbb{R}$ 的集合。如果

$$\mathsf{Adv}_{\le D}(\mathbb{P}, \mathbb{Q}) \coloneqq \sup_{f \in \mathbb{R}[Y]_{\le D}} \frac{\mathbb{E}_{\mathbb{P}}[f]}{\sqrt{\mathbb{E}_{\mathbb{Q}}[f^2]}} = 1 + o(1),$$

那么不存在次数为 D 的多项式 $f\colon \mathbb{R}^N \to \mathbb{R}$，能够弱分离 $\mathbb{P}$ 和 $\mathbb{Q}$。类似地，如果 $\mathsf{Adv}^{\le D}(\mathbb{P}, \mathbb{Q}) = O(1)$，那么不存在次数为 D 的多项式能够强分离 $\mathbb{P}$ 和 $\mathbb{Q}$。

总有 $\mathsf{Adv}_{\le D} \ge 1$，取 $f = 1$ 即可。

证明。反设存在某个次数为 D 的多项式 $g\colon \mathbb{R}^N \to \mathbb{R}$ 弱分离 $\mathbb{P}$ 和 $\mathbb{Q}$。通过平移和缩放，不失一般性地假设 $\mathbb{E}_{\mathbb{Q}}[g] = 0$ 和 $\mathbb{E}_{\mathbb{P}}[g] = 1$。当 n 足够大时，弱分离保证对某个常数 $C > 0$，$\mathsf{Var}_{\mathbb{Q}}[g] = \mathbb{E}_{\mathbb{Q}}[g^2] \le C$。定义 $f = g + C$ 并计算

$$\frac{\mathbb{E}_{\mathbb{P}}[f]}{\sqrt{\mathbb{E}_{\mathbb{Q}}[f^2]}} = \frac{1 + C}{\sqrt{\mathbb{E}_{\mathbb{Q}}[g^2] + C^2}} \ge \frac{1 + C}{\sqrt{C + C^2}} = \sqrt{\frac{1 + C}{C}},$$

这是一个严格大于 1 的常数，与 $\mathsf{Adv}_{\le D} = 1 + o(1)$ 矛盾。强分离的证明类似，此时取 $C = o(1)$。

□

证明的一个关键要素，是在以下一般情形下对 $\mathsf{Adv}^{\le D}$ 给出上界（我们的问题是其特例）。设 $\mathbb{Q}$ 具有如下形式：$Y = X \vee Z$，其中 X、$Z \in \{\pm 1\}^N$ 中的“噪声”Z 是独立同分布的拉ademacher变量，而“信号” X 服从任意分布（且独立于 Z），$\vee$ 表示逐项最大值。（在我们的情形中，$N = \binom{n}{2}$，且 X 是取值于 ± 1 的团边指示变量。）

命题 4.2。假设 $\mathbb{Q}$ 采用上述形式，且 $\mathbb{P}$ 是 $\{\pm 1\}^N$ 上的任意分布。对于 α、$\beta \subseteq [N]$，定义

$$c_\alpha = \mathop{\mathbb{E}}_{Y \sim \mathbb{P}}[Y^\alpha] \coloneqq \mathop{\mathbb{E}}_{Y \sim \mathbb{P}} \prod_{i \in \alpha} Y_i$$

and

$$M_{\beta\alpha} = \Pr_X(\alpha \setminus X = \beta).$$

此处以及下文中，我们滥用记号，使用 X 指代集合 $\{i \in [N] : \ X_i = 1\}$。

假设对于所有 $|\alpha| \le D$ 都有 $M_{\alpha\alpha} > 0$。则

$$\mathsf{Adv}^2_{\le D} \le \sum_{\alpha \subseteq [N],\, |\alpha| \le D} w_\alpha^2 \tag{4}$$

其中，w_α 通过以下递归方式定义

$$w_\alpha = \frac{1}{M_{\alpha\alpha}} \left(c_\alpha - \sum_{\beta \subsetneq \alpha} w_\beta M_{\beta\alpha} \right).$$

无明确基　　递归需要用到情形 e，但可以将 $w_\emptyset = 1$ 视为基本情形。

我们暂停一下，谈谈上述公式的由来。证明（见第 4.2.4 节）采用了基于 [SW22] 的策略：对 X （而不是 Z）应用詹森不等式，然后通过求解一个上三角线性系统，便可显式计算出结果。原始研究 [SW22] 在 估计 的背景下给出了类似公式。最近， [RSWY22] 首次证明，相关技术也可用于检验两个“植入”分布之间的差异（这也是当前研究所处的背景）。相比之下，以往针对检验问题的低次下界总是要求“零”分布 $\mathbb{Q}$ 具有独立坐标；参见下文的评论以作比较。

注释 4.3。 我们注意到，命题 *4.2* 推广了一个广为人知的公式，该公式用于低次检验“信号”与“纯噪声”。具体而言，考虑 $X = -\mathbb{I}$ 使得 $\mathbb{Q}$ 是独立同分布的 Rademacher 随机变量，而 $\mathbb{P}$ 是 $\{\pm 1\}^N$上的任意分布。在此情形下， $M_{\beta\alpha} = \mathbb{I}^{\beta=\alpha}$ 因此命题 *4.2* 可化为以下界

$$\mathsf{Adv}^2_{\le D} \le \sum_{|\alpha|\le D} \left(\mathop{\mathbb{E}}_{Y\sim\mathbb{P}}[Y^\alpha]\right)^2, \quad Y^\alpha := \prod_{i\in\alpha} Y_i,$$

这是标准结果（实际上等号成立）；参见 *[Hop18]* 的第 2.3 节。

回到证明，对于 w_α ，更方便的参数化形式是 $\hat{w}_\alpha = M_{\alpha\alpha} w_\alpha$。在这种情况下，由于 $M_{\emptyset\alpha} = \mathbb{E}_{\mathbb{Q}}[Y^\alpha]$，递推关系可以写成

$$\hat{w}_\emptyset = 1,$$

$$\hat{w}_\alpha \;=\; c_\alpha - \sum_{\beta\subsetneq\alpha} \hat{w}_\beta \frac{M_{\beta\alpha}}{M_{\beta\beta}} \;=\; \mathop{\mathbb{E}}_{\mathbb{P}}[Y^\alpha] - \mathop{\mathbb{E}}_{\mathbb{Q}}[Y^\alpha] - \sum_{\emptyset\subsetneq\beta\subsetneq\alpha} \hat{w}_\beta \frac{M_{\beta\alpha}}{M_{\beta\beta}} \qquad \text{for } |\alpha|\ge 1. \tag{5}$$

M之比可以看作一个条件概率：

$$R_{\beta\alpha} := \frac{M_{\beta\alpha}}{M_{\beta\beta}} = \frac{\Pr_X(\alpha \setminus X = \beta)}{\Pr_X(\beta \cap X = \emptyset)} = \Pr_X(\alpha \setminus X = \beta \mid \beta \cap X = \emptyset). \tag{6}$$

从这里开始，我们专门研究感兴趣的检验问题： $\mathbb{P} = \mathsf{MC}(n,\ q)$ 与 $\mathbb{Q} = \mathsf{MC}(n,\ q+\ell)$。如上所述，我们的目标是通过界定式（4）中的公式，证明 $\mathsf{Adv}_{\le D} = 1 + o(1)$。这个“1”来自 $\alpha = \emptyset$ 项，我们需要证明其余总和为 $o(1)$。

以下关于$\hat{w}$ 的性质将是分析的关键；它在引理 4.7 的证明中起着至关重要的作用。注意，我们可以将 α 视为顶点数为 n 的完全图的边子集，因此可以说 α 是连通的，或具有连通分量。

引理 4.4. 若 α 具有连通分量 $\alpha_1, \ldots, \alpha_t$， 则 $\hat{w}_\alpha = \prod_{i=1}^t \hat{w}_{\alpha_i}$。

证明。只需证明以下情形中的结论： α 由两个非空且不相交的边集α_1, α_2 组成，且二者没有共同顶点（也就是说，每个 α_i 都是若干连通分量的并）。在这种情形下证明 $\hat{w}_\alpha = \hat{w}_{\alpha_1}\hat{w}_{\alpha_2}$ 后，利用归纳法即可得到一般结论。

注意，由于各连通分量之间相互独立， $c_\alpha = c_{\alpha_1}c_{\alpha_2}$。任意 $\beta \subseteq \alpha$ 都可唯一分解为 $\beta = \beta_1 \cup \beta_2$，其中 $\beta_1 \subseteq \alpha_1$和 $\beta_2 \subseteq \alpha_2$。同样根据独立性， $R_{\beta\alpha} = R_{\beta_1\alpha_1}R_{\beta_2\alpha_2}$。我们还需要用到这一事实： $R_{\alpha\alpha} = 1$。我们对 $|\alpha|$进行归纳。如果 α_1 或 α_2 为空，结论立即成立，因为 $\hat{w}_\emptyset = 1$。否则，假设根据归纳法，对于任意 $\beta \subsetneq \alpha$，均有 $\hat{w}_\beta = \hat{w}_{\beta_1}\hat{w}_{\beta_2}$。于是

$$\begin{aligned}
\hat{w}_\alpha &= c_\alpha - \sum_{\beta\subsetneq\alpha} \hat{w}_\beta R_{\beta\alpha} \\
&= c_{\alpha_1}c_{\alpha_2} - \sum_{\substack{\beta_1\subsetneq\alpha_1\\ \beta_2\subsetneq\alpha_2}} \hat{w}_{\beta_1}\hat{w}_{\beta_2}R_{\beta_1\alpha_1}R_{\beta_2\alpha_2} - \sum_{\substack{\beta_1\subsetneq\alpha_1\\ (\beta_2=\alpha_2)}} \hat{w}_{\beta_1}\hat{w}_{\alpha_2}R_{\beta_1\alpha_1}R_{\alpha_2\alpha_2} - \sum_{\substack{\beta_2\subsetneq\alpha_2\\ (\beta_1=\alpha_1)}} \hat{w}_{\alpha_1}\hat{w}_{\beta_2}R_{\alpha_1\alpha_1}R_{\beta_2\alpha_2} \\
&= c_{\alpha_1}c_{\alpha_2} - \left(\sum_{\beta_1\subsetneq\alpha_1} \hat{w}_{\beta_1}R_{\beta_1\alpha_1}\right)\left(\sum_{\beta_2\subsetneq\alpha_2} \hat{w}_{\beta_2}R_{\beta_2\alpha_2}\right) - \hat{w}_{\alpha_2}\sum_{\beta_1\subsetneq\alpha_1} \hat{w}_{\beta_1}R_{\beta_1\alpha_1} - \hat{w}_{\alpha_1}\sum_{\beta_2\subsetneq\alpha_2} \hat{w}_{\beta_2}R_{\beta_2\alpha_2}.
\end{aligned}$$

利用递推关系（5），可得

$$\hat{w}_\alpha = c_{\alpha_1}c_{\alpha_2} - (c_{\alpha_1} - \hat{w}_{\alpha_1})(c_{\alpha_2} - \hat{w}_{\alpha_2}) - \hat{w}_{\alpha_2}(c_{\alpha_1} - \hat{w}_{\alpha_1}) - \hat{w}_{\alpha_1}(c_{\alpha_2} - \hat{w}_{\alpha_2}),$$

这就化简为 $\hat{w}_{\alpha_1}\hat{w}_{\alpha_2}$ ， 正如所需。 □

4.2.2 界定 $\hat{w}_\alpha$

在证明的其余部分，我们需要对这些值进行界定 w_α，并将其代入（4）。回想一下，当 α被视为一个图时，$|\alpha|$ 表示边的数量。我们还定义 V（α）为 α的顶点集合，即 $i \in [n]$ 中至少与一条边相接的顶点 α_i。

引理 4.5。对于任意 α，我们有 $M_{\alpha\alpha} \geq 1 - \frac{|\alpha|}{q+\ell}$。

证明。回想一下，$M_{\alpha\alpha}$ 是在 $\mathbb{Q}$ 下 α 不包含团边的概率。任意特定边是团边的概率为 $1/(q+\ell)$，因此由并集界可得结论。 □

引理 4.6。如果 $|\alpha| \geq 1$ 和 α 连通，则

$$0 \leq \mathop{\mathbb{E}}_{\mathbb{P}}[Y^\alpha] - \mathop{\mathbb{E}}_{\mathbb{Q}}[Y^\alpha] \leq \frac{\ell}{q^{|V(\alpha)|}}(|V(\alpha)| - 1).$$

证明。由于 α 连通，$\mathbb{E}_{\mathbb{P}}[Y^\alpha]$ 是 α 的所有顶点在 $[q]$ 中被赋予相同标签的概率（$\mathbb{E}_{\mathbb{Q}}[Y^\alpha]$ 中的情况也类似），即

$$\begin{aligned}
\mathop{\mathbb{E}}_{\mathbb{P}}[Y^\alpha] - \mathop{\mathbb{E}}_{\mathbb{Q}}[Y^\alpha] &= \left(\frac{1}{q}\right)^{|V(\alpha)|-1} - \left(\frac{1}{q+\ell}\right)^{|V(\alpha)|-1} \\
&= \left(\frac{1}{q}\right)^{|V(\alpha)|-1}\left[1 - \left(\frac{q}{q+\ell}\right)^{|V(\alpha)|-1}\right] \\
&= \left(\frac{1}{q}\right)^{|V(\alpha)|-1}\left[1 - \left(1 - \frac{\ell}{q+\ell}\right)^{|V(\alpha)|-1}\right] \\
&\leq \left(\frac{1}{q}\right)^{|V(\alpha)|-1}\left[1 - \left(1 - \frac{\ell}{q+\ell}(|V(\alpha)| - 1)\right)\right] \\
&= \left(\frac{1}{q}\right)^{|V(\alpha)|-1}\frac{\ell}{q+\ell}(|V(\alpha)| - 1) \\
&\leq \frac{\ell}{q^{|V(\alpha)|}}(|V(\alpha)| - 1).
\end{aligned}$$

□

引理 4.7。如果 $|\alpha| \geq 1$，则

$$|\hat{w}_\alpha| \leq \left(\frac{\sqrt{\ell}}{q}\right)^{|V(\alpha)|}(|\alpha| + 1)^{|\alpha|}.$$

证明。对 $|\alpha|$进行归纳。首先考虑 α 不连通的情况。将 α 写成两个非空且不相交的边集 α_1, α_2，它们没有共同顶点。由引理 4.4 和归纳假设可得，

$$\begin{aligned}
|\hat{w}_\alpha| = |\hat{w}_{\alpha_1}| \cdot |\hat{w}_{\alpha_2}| &\leq \left(\frac{\sqrt{\ell}}{q}\right)^{|V(\alpha_1)|}(|\alpha_1| + 1)^{|\alpha_1|} \cdot \left(\frac{\sqrt{\ell}}{q}\right)^{|V(\alpha_2)|}(|\alpha_2| + 1)^{|\alpha_2|} \\
&\leq \left(\frac{\sqrt{\ell}}{q}\right)^{|V(\alpha_1)|+|V(\alpha_2)|}(|\alpha_1| + |\alpha_2| + 1)^{|\alpha_1|+|\alpha_2|} \\
&= \left(\frac{\sqrt{\ell}}{q}\right)^{|V(\alpha)|}(|\alpha| + 1)^{|\alpha|}
\end{aligned}$$

按需。

现在考虑 α 连通的情况。利用（5）和引理 4.6,

$$|\hat{w}_\alpha| \le \left| \mathop{\mathbb{E}}_{\mathbb{P}}[Y^\alpha] - \mathop{\mathbb{E}}_{\mathbb{Q}}[Y^\alpha] \right| + \sum_{\emptyset \subsetneq \beta \subsetneq \alpha} |\hat{w}_\beta| \cdot |R_{\beta\alpha}| \le \frac{\ell}{q^{|V(\alpha)|}} (|V(\alpha)| - 1) + \sum_{\emptyset \subsetneq \beta \subsetneq \alpha} |\hat{w}_\beta| \cdot |R_{\beta\alpha}|.$$

根据定义（6）以及 α 的连通性，我们可以推导出（对任意 $\emptyset \subsetneq \beta \subsetneq \alpha$）

$$0 \le R_{\beta\alpha} \le \left(\frac{1}{q+\ell}\right)^{|V(\alpha)|-|V(\beta)|} \le \left(\frac{1}{q}\right)^{|V(\alpha)|-|V(\beta)|},$$

因为一旦我们对 $V(\beta)$ 中的标签进行条件化，$V(\alpha) \setminus V(\beta)$ 中的每个顶点至多只有一个可能的标签能使事件 $\alpha \setminus X = \beta$ 发生。（更正式地说，任意顶点 $i \in V(\alpha) \setminus V(\beta)$ 都通过一条由 $\alpha \setminus \beta$ 中的边组成的路径与某个顶点 $j \in V(\beta)$ 连通。由于要使 $\alpha \setminus X = \beta$ 发生，这条路径上的每条边都必须是团边，因此 i 必须与 j 具有相同的标签。）现在利用上述界和归纳假设,

$$\begin{aligned}
|\hat{w}_\alpha| &\le \frac{\ell}{q^{|V(\alpha)|}} (|V(\alpha)| - 1) + \sum_{\emptyset \subsetneq \beta \subsetneq \alpha} \left(\frac{\sqrt{\ell}}{q}\right)^{|V(\beta)|} (|\beta|+1)^{|\beta|} \cdot \left(\frac{1}{q}\right)^{|V(\alpha)|-|V(\beta)|} \\
&\le \left(\frac{\sqrt{\ell}}{q}\right)^{|V(\alpha)|} \left[|V(\alpha)| - 1 + \sum_{\emptyset \subsetneq \beta \subsetneq \alpha} (|\beta|+1)^{|\beta|} \right] \qquad \text{since } |V(\alpha)| \ge 2 \text{ and } |V(\beta)| \le |V(\alpha)| \\
&= \left(\frac{\sqrt{\ell}}{q}\right)^{|V(\alpha)|} \left[|V(\alpha)| - 1 + \sum_{m=1}^{|\alpha|-1} \binom{|\alpha|}{m} (m+1)^m \right] \\
&\le \left(\frac{\sqrt{\ell}}{q}\right)^{|V(\alpha)|} \left[|V(\alpha)| - 1 + \sum_{m=1}^{|\alpha|-1} \binom{|\alpha|}{m} |\alpha|^m \right] \\
&= \left(\frac{\sqrt{\ell}}{q}\right)^{|V(\alpha)|} \left[|V(\alpha)| - 1 + (|\alpha|+1)^{|\alpha|} - 1 - |\alpha|^{|\alpha|} \right] \qquad \text{by the Binomial theorem} \\
&\le \left(\frac{\sqrt{\ell}}{q}\right)^{|V(\alpha)|} (|\alpha|+1)^{|\alpha|},
\end{aligned}$$

其中最后一步用到了 $|V(\alpha)| \le 2|\alpha| \le |\alpha|^{|\alpha|} + 1$。 □

4.2.3 综合起来

证明的其余部分与植入团的低次分析类似；参见 [Hop18] 的第 2.4 节。定理 *2.10* 的证明。 对于任意 $|\alpha| \le D$，由引理 4.5 可知

$$M_{\alpha\alpha} \ge 1 - \frac{|\alpha|}{q+\ell} \ge 1 - \frac{D}{q} = 1 - o(1),$$

由于我们对 q 和 D的假设。应用命题4.2,

$$\mathsf{Adv}^2_{\le D} \le \sum_{|\alpha| \le D} w_\alpha^2 = 1 + \sum_{1 \le |\alpha| \le D} \left(\frac{\hat{w}_\alpha}{M_{\alpha\alpha}}\right)^2 \le 1 + (1 + o(1)) \sum_{1 \le |\alpha| \le D} \hat{w}_\alpha^2.$$

由于我们的目标（根据引理 4.1）是证明 $\mathsf{Adv}_{\le D} = 1 + o(1)$，因此只需证明

$$\sum_{1 \le |\alpha| \le D} \hat{w}_\alpha^2 = o(1).$$

这由下述命题 4.9 推出：利用引理 4.7 中关于 $|\hat{w}_\alpha|$ 的界，以及假设 $q^2 \ge \ell n^{1+\epsilon}$。

□

引理 4.8。对于整数 $t \geq 2$ 和 $D \geq 1$，满足 $|\alpha| \leq D$ 且 $|V(\alpha)| = t$ 的图 $\alpha \subseteq \binom{n}{2}$ 的数量至多为 $n^t \min\{2^{t^2}, t^{2D}\}$。

证明。选择 t 个顶点的方法数为 $\binom{n}{t} \leq n^t$。选定顶点后，我们可以用两种不同的方式对含有 $\leq D$ 条边的图的总数给出上界：$2^{\binom{t}{2}} \leq 2^{t^2}$ 或 $\left(\binom{t}{2}+1\right)^D \leq (t^2)^D$。 □

命题 4.9 $\delta > 0$ $C > 0$ $\alpha \subseteq \binom{n}{2}$ $1 \leq$。假设 $|\alpha| \leq D$ ϕ_α $|\phi_\alpha| \leq n^{-\frac{1}{2}(1+\delta)\cdot|V(\alpha)|}(|\alpha|+1)^{C\cdot|\alpha|}$ $D = D_n$ 存在固定常数 和，使得对于 满足 的，我们有一个数量，其上界为 ()()()。如果 满足 $D = o(\log n/\log\log n)^2$，那么

$$\sum_{1\leq|\alpha|\leq D} \phi_\alpha^2 = o(1)$$

当 $n \to \infty$ 时。

证明。利用引理 4.8 以及事实 $|\alpha| \leq \binom{|V(\alpha)|}{2} \leq |V(\alpha)|^2$，

$$\sum_{1\leq|\alpha|\leq D} \phi_\alpha^2 \leq \sum_{2\leq t\leq\sqrt{D}} n^t 2^{t^2}\cdot n^{-(1+\delta)t}(t^2+1)^{2Ct^2} + \sum_{\sqrt{D}\leq t\leq 2D} n^t t^{2D}\cdot n^{-(1+\delta)t}(D+1)^{2CD}.$$

考虑上式右侧的第一个求和。首项 $t = 2$ 为 $O(n^2\cdot n^{-2(1+\delta)}) = o(1)$，而项 $t+1$ 与 t 之比为

$$n^{-\delta}\cdot 2^{2t+1}\cdot((t+1)^2+1)^{2C(2t+1)}\left(\frac{(t+1)^2+1}{t^2+1}\right)^{2Ct^2} \leq t^{O(t)}n^{-\delta} \leq \sqrt{D}^{O(\sqrt{D})}n^{-\delta} \leq \frac{1}{2}$$

当 n充分大时，在假设 $D = o\left(\log n\log\log n\right)^2$ 下。现在考虑第二个求和。首项 $t = \lceil\sqrt{D}\rceil$ 至多为

$$n^{-\delta\sqrt{D}}(\sqrt{D}+1)^{2D}(D+1)^{2CD} \leq n^{-\delta\sqrt{D}}(D+1)^{2(C+1)D} = o(1),$$

项 $t+1$ 与 t 之比为

$$n^{-\delta}\cdot\left(\frac{t+1}{t}\right)^{2D} \leq n^{-\delta}\left(1+\frac{1}{\sqrt{D}}\right)^{2D} \leq n^{-\delta}\cdot e^{O(\sqrt{D})} \leq \frac{1}{2}$$

当 n充分大时。 □

4.2.4 命题4.2的证明

该证明与 [SW22 第 3 节中植入团的下界证明类似。5]为方便起见，我们在此给出详细证明。

任意次数为-D的多项式 $f\colon \{\pm1\}^N \to \mathbb{R}$ 都有唯一展开式 $f(Y) = \sum_{\alpha\subseteq[N],\ |\alpha|\leq D}\hat{f}_\alpha Y^\alpha$。记

$$\mathop{\mathbb{E}}_{\mathbb{P}}[f(Y)] = \sum_{|\alpha|\leq D}\hat{f}_\alpha \mathop{\mathbb{E}}_{\mathbb{P}}[Y^\alpha] = \langle c, \hat{f}\rangle$$

其中，回顾一下，向量 $c = (c_\alpha)$ 定义为

$$c_\alpha = \mathop{\mathbb{E}}_{\mathbb{P}}[Y^\alpha].$$

根据詹森不等式，

$$\mathop{\mathbb{E}}_{\mathbb{Q}}[f(Y)^2] \geq \mathop{\mathbb{E}}_{Z}\left(\mathop{\mathbb{E}}_{X} f(X\vee Z)\right)^2 =: \mathop{\mathbb{E}}_{Z} g(Z)^2 = \|\hat{g}\|^2$$

其中

$$\begin{aligned} g(Z) &= \mathop{\mathbb{E}}_{X} f(X \vee Z) \\ &= \sum_{|\alpha| \le D} \hat{f}_\alpha \mathop{\mathbb{E}}_{X} (X \vee Z)^\alpha \\ &= \sum_{|\alpha| \le D} \hat{f}_\alpha \sum_{0 \subseteq \beta \subseteq \alpha} Z^\beta \Pr_X\{\alpha \setminus X = \beta\} \\ &= \sum_{\beta} Z^\beta \sum_{\alpha \supseteq \beta} \hat{f}_\alpha \Pr_X\{\alpha \setminus X = \beta\}. \end{aligned}$$

$\hat{}$ 换句话说，$\hat{}g = Mf$ 其中，回忆一下，矩阵 $M = (M_{\beta\alpha})$ 定义为

$$M_{\beta\alpha} = \mathbb{I}^{\beta \subseteq \alpha} \Pr_X\{\alpha \setminus X = \beta\}.$$

注意， M 是上三角矩阵，且（根据假设）对角线上的元素均为正，因此 M 可逆。现在我们已经证明 $\mathbb{E}_{\mathbb{Q}}[f]^2 \ge \|\hat{}g\|^2 = \|M\hat{}f\|^2$，因此

$$\mathsf{Adv}_{\le D} = \sup_{f \in \mathbb{R}[Y]_{\le D}} \frac{\mathbb{E}_{\mathbb{P}}[f]}{\sqrt{\mathbb{E}_{\mathbb{Q}}[f^2]}} \le \sup_{\hat{f}} \frac{\langle c, \hat{f} \rangle}{\|M\hat{f}\|} = \sup_{\hat{g}} \frac{c^\top M^{-1} \hat{g}}{\|\hat{g}\|},$$

其最优解为 $\hat{}g = (c^\top M^{-1})^\top$，从而得到

$$\mathsf{Adv}_{\le D} \le \|c^\top M^{-1}\| =: \|w\|$$

其中 w 是 $w^\top M = c^\top$的解。利用 M 的上三角结构求解 w ，得到递推关系

$$w_\alpha = \frac{1}{M_{\alpha\alpha}} \left(c_\alpha - \sum_{\beta \subsetneq \alpha} w_\beta M_{\beta\alpha} \right), \tag{7}$$

证明完毕。

5 反驳可着色性

5.1 上界

为方便读者，我们重述该定理。

定理 2.16（上界）。假设 $q \le b\sqrt{n}$ 对于一个常数 $b < 1/2$ 成立（该常数不依赖于 n）。那么存在一个常数 $C = C(b) > 0$ 以及一个次数至多为 $C \log n$ 的多项式 $f = f_n$，它强分离$G(n, 1/2)$ 和 $\mathcal{R}_q$。

证明。令 A 表示补图的 $\{\pm 1\}$ 值邻接矩阵，对角线上的元素为 0；若该图可用 q 种颜色着色，则 A 在每个颜色类内的值均为 1。对于稍后将选定的整数 $m \ge 1$ ，考虑多项式 $f(X) = (n/q - 1)^{-2m}$ 迹(A^{2m})，其关于输入变量$X \in \{\pm 1\}^{\binom{n}{2}}$的次数为 $2m$。

首先令 $X \in \mathcal{R}_q$，并旨在证明 $f(X) \ge 1$。令 $S \subseteq [n]$ 为最大的颜色类，因此 $|S| \ge n/q$。令 $\mathbb{I}^S \in \{0,1\}^n$ 表示 S的指示向量。令 $\lambda_{\max} = \lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_n$ 表示 A的特征值，

$$\lambda_{\max} \ge \frac{\mathbb{I}^{S\top} A \mathbb{I}^S}{\|\mathbb{I}^S\|^2} = \frac{|S|(|S|-1)}{|S|} = |S| - 1 \ge \frac{n}{q} - 1$$

and

$$\lambda_{\max}^{2m} \le \sum_{i=1}^{n} \lambda_i^{2m} = \mathrm{Tr}(A^{2m}).$$

结合这些结果可得 $\mathrm{Tr}(A^{2m}) \geq (n/q-1)^{2m}$，因此 $f(X) \geq 1$。

剩下需要证明的是 $\mathbb{E}[f^2] = o$当 $X \sim G(n, 1/2)$。设 Y为一个 $n \times n$对称矩阵，其中$\{Y_{ij} : \ i \leq j\}$是独立同分布的 $\mathcal{N}(0, 1)$。通过直接展开，并将拉德马赫矩与高斯矩进行比较，可得 $\mathbb{E}[\mathrm{Tr}(A^{2m})^2] \leq \mathbb{E}[\mathrm{Tr}(Y^{2m})^2]$。用 $\|Y\|$ 表示 Y的谱范数，BvH16 中的界BvH16，引理 2。2给出

$$\mathbb{E}[\mathrm{Tr}(Y^{2m})^2] \leq \mathbb{E}[n^2\|Y\|^{4m}] \leq n^2(2\sqrt{n}+2\sqrt{4m})^{4m}.$$

综合以上结果，

$$\mathbb{E}[f^2] \leq \left(\frac{n}{q}-1\right)^{-4m} n^2(2\sqrt{n}+2\sqrt{4m})^{4m} = n^2\left(\frac{2q(\sqrt{n}+\sqrt{4m})}{n-q}\right)^{4m},$$

在定理的条件下，这就是 $o(1)$。 □

5.2 下界

为方便读者，我们重述该定理。

定理 2.17（下界）。如果 $q \geq n^{2/3+\epsilon}$ 对某个常数 $\epsilon > 0$成立，那么不存在次数为-$o(\log n/\log\log n)^2$的多项式弱分离 $G(n, 1/2)$ 和 $\mathcal{R}_q$。

根据命题 2.14，我们的目标是证明 $\mathsf{Adv}_{\leq D}(\mathbb{P}, \mathbb{Q}) = 1 + o(1)$，其中 $\mathbb{Q} = G(n, 1/2)$（且 $Y \sim \mathbb{Q}$ 由 $\{\pm 1\}\binom{n}{2}$ 中的一个元素编码）以及 $\mathbb{P}$ 是在定义 2.18中定义的植入分布。我们的出发点是备注 4.3中的著名公式：

$$\mathsf{Adv}^2_{\leq D} = \sum_{|\alpha| \leq D} \left(\mathop{\mathbb{E}}_{Y\sim\mathbb{P}}[Y^\alpha]\right)^2,$$

其中 $\alpha \subseteq \binom{n}{2}$。我们将 α 视为边集为 α的图，并将 $V(\alpha) \subseteq [n]$ 记为顶点集，即与 α中的至少一条边关联的顶点。我们的第一步是界定系数 $\lambda_\alpha := \mathbb{E}_{Y\sim\mathbb{P}}[Y^\alpha]$。

5.2.1 界定系数

引理 5.1（界定 λ_α）。对于任意图 $\alpha \subseteq \binom{n}{2}$，有

$$|\lambda_\alpha| := \left|\mathop{\mathbb{E}}_{Y\sim\mathbb{P}}[Y^\alpha]\right| \leq O(q^{-3/4})^{|V(\alpha)|}$$

其中 $O(\cdot)$ 隐含一个绝对常数因子。

证明。若 $\alpha = \cup_i \alpha_i$ 是 α 分解为连通分量后的结果，则由于各分量之间相互独立，我们有 $\lambda_\alpha = \prod_i \lambda_{\alpha_i}$。因此，只需证明 α 连通时的情形。

令 $c : V(\alpha) \to [q] \times [q]$ 表示根据 a、b 的定义，将标签赋给顶点的潜在赋值 $\mathbb{P}$（定义 2.18）。我们有

$$\lambda_\alpha = \mathop{\mathbb{E}}_{c} \mathop{\mathbb{E}}_{Y\sim\mathbb{P}|c}[Y^\alpha] = \sum_c \Pr[c] \cdot \mathbb{E}[Y^\alpha|c].$$

注意，除非 α 中的每条边都是 c中的独立集边或团边，否则 $\mathbb{E}[Y^\alpha|c] = 0$；在这种情况下，

$$\mathbb{E}[Y^\alpha|c] = (-1)^{\#\text{ ind-set edges}}.$$

因此，对 $|\lambda_\alpha|$ 的一个可能上界，是在 c 上每条 α 中的边要么是独立集边，要么是团边的概率。我们可以如下界定这个概率。回想一下，我们假设 α 是连通的，并按照广度优先搜索探索 α 的顶点。第一个顶点的标签不受约束。每条通向新顶点的边都必须是独立集边或团边，因此新顶点的标签至多有 $2q$ 种可能。由于总共有 q^2 种可能的标签，我们得出

$$|\lambda_\alpha| \leq \left(\frac{2q}{q^2}\right)^{|V(\alpha)|-1} = \left(\frac{2}{q}\right)^{|V(\alpha)|-1} \tag{8}$$

对于任意连通的 α。

界（8）蕴含所需结果 $|\lambda_\alpha| \le O(q^{-3/4})^{|V(\alpha)|}$，条件是 $|V(\alpha)| \ge 4$，因为在这种情况下，我们有 $|V(\alpha)|-1 \ge |V(\alpha)| - \frac{1}{4}|V(\alpha)| = \frac{3}{4}|V(\alpha)|$。对于 $|V(\alpha)| \le 3$，我们将通过检查所有可能的图来手动验证该结果：

- 如果 α 没有边，那么 $\lambda_\alpha = 1$。
- 如果 α 是一条边，那么需要考虑的 c 情形为 $\{(a,b),(a,b)\}$、$\{(a,b),(a,b')\}$，以及 $\{(a,b),(a',b)\}$（其中 $a \ne a', b \ne b'$）。由此得到

$$\lambda_\alpha = -\frac{1}{q^2} - \frac{1}{q}\left(1-\frac{1}{q}\right) + \frac{1}{q}\left(1-\frac{1}{q}\right) = -q^{-2}.$$

- 如果 α 是一条长度为 2 的路径，那么在给定中间顶点的任意标签后，两条边相互独立。重复单条边的计算，我们有 $\lambda_\alpha = (-q^{-2})^2 = q^{-4}$。
- 如果 α 是一个三角形，我们首先指出，只有那些重复出现某个标签 (a,b) 的标记方式 c 才会对 λ_α 有贡献。这是由 c 与反向标记方式 $\overline{c}$之间的对称性得出的；在反向标记方式中，每一对都颠倒为：$(a,b) \mapsto (b,a)$。如果 c 没有重复标签，那么 c 和 $\overline{c}$ 贡献的项相同，但符号相反，因为每条独立集边都会变成团边，反之亦然。因此，c需要考虑的其余情况为 $\{(a,b),(a,b),(a,b)\}$，$\{(a,b),(a,b),(a,b')\}$，以及$\{(a,b),(a,b),(a',b)\}$。由此得到

$$\lambda_\alpha = -\frac{1}{q^4} - 3\cdot\frac{1}{q^3}\left(1-\frac{1}{q}\right) - 3\cdot\frac{1}{q^3}\left(1-\frac{1}{q}\right) = O(q^{-3}).$$

现在，我们已经验证了对于每个连通 α，$|\lambda_\alpha| \le O(q^{-3/4})^{|V(\alpha)|}$ 都成立。如前所述，这意味着该结果对所有 α都成立。 □

5.2.2 综合起来

现在我们结合上述结果，以界定 $\mathsf{Adv}_{\le D}$。

定理 *2.17* 的证明。根据我们的假设 $q \ge n^{2/3+\epsilon}$，引理 5.1 给出

$$|\lambda_\alpha| \le O(n^{-\frac{3}{4}(\frac{2}{3}+\epsilon)})^{|V(\alpha)|} = O(n^{-\frac{1}{2}-\frac{3}{4}\epsilon})^{|V(\alpha)|} \le n^{-\frac{1}{2}(1+\epsilon)\cdot|V(\alpha)|}$$

f或当 n 足够大时。利用命题 4.9，对于任意 $D = o(\log n/\operatorname{loglog} n)^2$ ，

$$\mathsf{Adv}_{\le D}^2 - 1 = \sum_{1\le|\alpha|\le D} \lambda_\alpha^2 = o(1).$$

正如第 5.2 节开头所述，这就完成了证明。 □

6 QuietPlanting 的完备性

本节将给出一个简单论证，以说明在高度一般的情形下，不存在计算上静默的植入分布意味着存在低次反证算法。我们的证明是初等的，只需简单应用冯·诺依曼极小极大原理。为方便读者，我们重新陈述该定理。

定理 2.20. 固定序列 $N = N_n$、$D = D_n$、$\mathbb{Q} = \mathbb{Q}_n$（$\mathbb{R}^N$ 上的一个分布）以及 $\mathcal{R} = \mathcal{R}_n \subseteq \mathbb{R}^N$。假设对于每个 n，$\mathbb{Q}$ 的支撑集都是有限集合，并且 $\mathcal{R}$ 是有限集合（但这些集合的基数可能依赖于 n）。以下条件等价：

(1) 没有次数为D 的多项式能强分离 $\mathbb{Q}$ 和 $\mathcal{R}$。

(2) 对于 n 值的一个无限子序列，存在一个支撑在 $\mathcal{R}$ 上的分布 $\mathbb{P} = \mathbb{P}_n$，使得 $\mathsf{Adv}^{\leq D}(\mathbb{P}, \mathbb{Q}) = O(1)$。

同样，以下命题等价：

(1) 不存在次数为D 的多项式能弱分离 $\mathbb{Q}$ 和 $\mathcal{R}$。

(2) 对于 n 值的一个无限子序列，存在一个支撑在 $\mathcal{R}$ 上的分布 $\mathbb{P} = \mathbb{P}_n$，使得 $\mathsf{Adv}^{\leq D}(\mathbb{P}, \mathbb{Q}) = 1 + o(1)$。

证明。令 $\mathcal{P}$ 表示 $\mathcal{R}$上的概率分布空间。令 $\mathcal{F}$ 表示次数为D的多项式 f空间：$\mathbb{R}^N \to \mathbb{R}$满足 $\mathbb{E}_{\mathbb{Q}}[f] = 0$和 $\mathbb{E}_{\mathbb{Q}}[f^2] \leq 1$。考虑

$$\mathrm{val}_n = \inf_{\mathbb{P}\in\mathcal{P}} \sup_{f\in\mathcal{F}} \mathbb{E}_{\mathbb{P}}[f]. \tag{9}$$

根据冯·诺依曼极小极大原理（所需技术条件的讨论见下文），上确界和下确界可以交换：

$$\mathrm{val}_n = \sup_{f\in\mathcal{F}} \inf_{\mathbb{P}\in\mathcal{P}} \mathbb{E}_{\mathbb{P}}[f] = \sup_{f\in\mathcal{F}} \inf_{X\in\mathcal{R}} f(X). \tag{10}$$

次数为D 的多项式强分离（分别为弱分离）$\mathbb{Q}$ 和 $\mathcal{R}$，当且仅当（10）式的值为$\omega(1)$（分别为 $\Omega(1)$）。该陈述的否定是 $\mathrm{val}_n = O(1)$（分别为 $o(1)$），对于 n的一个无限子序列成立；根据（9），这等价于存在定义在一个无限子序列上的 $\mathbb{P}_n$，使得 $\sup_{f\in\mathcal{F}} \mathbb{E}_{\mathbb{P}}[f] = O(1)$（分别为 $o(1)$）。现在由恒等式 $(\sup_{f\in\mathcal{F}} \mathbb{E}_{\mathbb{P}}[f])^2 + 1 = \mathsf{Adv}^2_{\leq D}(\mathbb{P}, \mathbb{Q})$可得结果；见下文引理6.3 。

接下来需要验证极大极小原理的技术条件。形式上，我们使用以下变体，它是 Sion 极小极大定理的一个特例 [Sio58，Kom88]。

定理 6.1. 设 $\mathcal{P}$ 是线性拓扑空间中的紧凸子集，$\mathcal{F}$ 是线性拓扑空间中的凸子集。若 $\phi(x, y)$ 是定义在 $\mathcal{P} \times \mathcal{F}$上的连续实值函数，且对所有$x \in \mathcal{P}$，$\phi(x, \cdot)$ 都是凹函数；对所有 $y \in \mathcal{F}$，$\phi(\cdot, y)$ 都是凸函数，则 $\min_{x\in\mathcal{P}} \sup_{y\in\mathcal{F}} \phi(x, y) = \sup_{y\in\mathcal{F}} \min_{x\in\mathcal{P}} \phi(x, y)$。

在我们的设定中，线性拓扑空间就是某个 d的 $\mathbb{R}^d$。回想一下，我们选择的 $\mathcal{P}$ 是有限集合 $\mathcal{R} = \{r_1, r_2, \ldots, r_{|\mathcal{R}|}\}$上的概率分布空间。我们可以通过将分布 $\mathbb{P}$编码为概率向量 $(\mathbb{P}(r_1) \ldots, \mathbb{P}(r_{|\mathcal{R}|}))$，将 $\mathcal{P}$视为 $\mathbb{R}^{|\mathcal{R}|}$ 的紧凸子集。回想一下，我们选择的 $\mathcal{F}$是次数为 D的多项式 $f\colon \mathbb{R}^N \to \mathbb{R}$，满足 $\mathbb{E}_{\mathbb{Q}}[f] = 0$和 $\mathbb{E}_{\mathbb{Q}}[f^2] \leq 1$。令 $\mathcal{X} = \mathrm{supp}(\mathbb{Q}) \cup \mathcal{R} = \{x_1, \ldots, x_{|\mathcal{X}|}\}$，我们可以通过将函数 $f\colon \mathbb{R}^N \to \mathbb{R}$编码为向量 $(f(x_1) \ldots, f(x_{|\mathcal{X}|}))$，将 $\mathcal{F}$视为 $\mathbb{R}^{|\mathcal{X}|}$的凸子集（注意，$\mathcal{F}$不要求是紧的）。最后，注意 $\phi(\mathbb{P}, f) := \mathbb{E}_{\mathbb{P}}[f]$是连续的，关于 $\mathbb{P}$是凸的，关于 f是凹的；事实上，它关于两个变量都是线性的。这证明了我们先前交换 inf 和 sup 的合理性，从而完成证明。

□

注 6.2. 上文为简化极大极小原理所需的解析条件，假设 $\mathrm{supp}(\mathbb{Q})$ 和 $\mathcal{R}$ 都是有限集，但这些假设可以放宽。例如，也可以假设 $\mathbb{Q}_n$ 是定义在 $\mathbb{R}^N$ 上且所有矩均有限的任意分布，并且 $\mathcal{R}_n \subseteq \mathbb{R}^N$ 是紧集。由于 $\mathcal{R}$ 是紧集，$\mathcal{R}$ 上的概率分布空间 $\mathcal{P}$ 在弱-* 拓扑下也是紧的。

引理 6.3. $\sup_{f\in\mathcal{F}} \mathbb{E}_{\mathbb{P}}[f]^2 + 1 = \mathsf{Adv}^2_{\leq D}(\mathbb{P}, \mathbb{Q})$.

证明。若似然比 $LR = d\mathbb{P}/d\mathbb{Q}$ 存在，则根据这些量的标准刻画，它们分别等于 $L^2(\mathbb{Q}$范数，即似然函数投影的范数（参见[Hop18]的第 2.3 节）；具体而言，左侧为 $\|LR^{\leq D} - 1\|^2_{\mathbb{Q}} + 1$，右侧为 $\|LR^{\leq D}\|^2_{\mathbb{Q}}$。下面我们也给出一个自包含的证明。

回顾 $\mathsf{Adv}^{\leq D}$ 的定义，我们的目标是证明

$$\sup_{f\in\mathcal{F}} \mathbb{E}_{\mathbb{P}}[f]^2 + 1 = \sup_{g\in\mathbb{R}[Y]_{\leq D}} \frac{\mathbb{E}_{\mathbb{P}}[g]^2}{\mathbb{E}_{\mathbb{Q}}[g^2]}.$$

注意，取 $f=0$ 或 $g=1$ 时，两边都可以达到值 1。为了证明“$\le$”，假设我们有 $f\in\mathcal{F}$，满足 $\mathbb{E}_{\mathbb{P}}[f]=a>0$，从而在左侧达到值 a^2+1。那么，$g=f+1/a$ 在右侧也能达到相同的值 a^2+1。

为证明“$\ge$”，假设 g 在右侧取得值 $b^2>1$，并对 g 进行缩放，使得 $\mathbb{E}_{\mathbb{Q}}[g^2]=1$ 且 $\mathbb{E}_{\mathbb{P}}[g]=b>1$。定义 $\Delta=\mathbb{E}_{\mathbb{Q}}[g]$，并注意到 $\mathbb{E}_{\mathbb{Q}}(g-\Delta)^2=1-\Delta^2\ge 0$ 且 $\mathbb{E}_{\mathbb{P}}(g-\Delta)=b-\Delta>0$。如果 $\Delta=1$，那么取 f 为 $g-\Delta$ 的任意倍数，即可使左侧无界。否则，令 $f=(g-\Delta)/\sqrt{1-\Delta^2}\in\mathcal{F}$，并计算左侧的值

$$\mathop{\mathbb{E}}_{\mathbb{P}}[f]^2+1=\frac{(b-\Delta)^2}{1-\Delta^2}+1=b^2+\frac{(b\Delta-1)^2}{1-\Delta^2}\ge b^2,$$

从而完成证明。 □

一个植入的 $(q+1)$-着色不是 q-可着色的

这里我们研究补图，并考虑将其划分为若干团，而非进行着色。回顾一下多团模型（定义 2.3）。

命题 A.1. 若 $1\le q\le\Omega(n/\log n)$，则以概率 $1-o(1)$，$\mathrm{MC}(n,q+1)$ 不存在将顶点划分为 q 个团的划分。

证明。固定一个绝对常数 $\epsilon>0$，稍后再选定。假设 $q\le cn/\log n$，其中 $c=c(\epsilon)>0$ 是一个稍后再选定的常数。证明依赖于以下 3 个基本事实，它们以高概率成立：

(i) $G(n,1/2)$ 不含完全二部图 $K_{m,\,m}$ 作为子图，其中 $m\ge(2+\epsilon)\log_2 n$。

(ii) 令 $S_1,\ldots,S_{q+1}$ 表示 $\mathrm{MC}(n,q+1)$ 的颜色类，则对所有 $i\in[q+1]$，都有 $|S_i|\in(1\pm\epsilon)\frac{n}{q+1}$。(iii) 在 $\mathrm{MC}(n,q+1)$ 中，任意顶点 $v\in S_i$ 在 S_j 中至多有 $(1/2+2\epsilon)\frac{n}{q+1}$ 个邻居，其中 $i\ne j$.

标准论证表明，(i)–(iii) 以概率 $1-o(1)$ 成立，具体细节从略。(i) 的证明是一个一阶矩计算（计算 $K_{m,m}$ 的副本数的期望，并应用马尔可夫不等式），而 (ii) 和 (iii) 的证明则使用伯恩斯坦不等式以及并集界。

设 $G\sim\mathrm{MC}(n,q+1)$。要完成证明，只需证明性质 (i)–(iii) 确定性地推出 G 不存在划分为 q 个团的划分（其中，性质 (i) 适用于用于生成 G 的底层随机图 $G'\sim G(n,1/2)$，即在添加 $q+1$ 个团之前的图）。假设 (i)–(iii) 成立，并反设 G 存在一个划分 $V(G)=T_1\sqcup T_2\sqcup\cdots\sqcup T_q$ 为若干个团。

我们首先断言，对于每个 $i\in[q]$，要么有（情形 I）$|T_i|\le\frac{3}{4}\cdot\frac{n}{q+1}$，要么（情形 II）存在某些 $j\in[q+1]$、$T_i\subseteq S_j$ 和 $|T_i|>\frac{1}{2}|S_j|$。为此，注意若情形 I 不成立，则 $|T_i|>\frac{3}{4}\cdot\frac{n}{q+1}$，因此为避免违反性质 (i)，必定存在 j 使得 $|T_i\cap S_j|\ge\frac{3}{4}\cdot\frac{n}{q+1}-(2+\epsilon)\log_2 n>(1/2+2\epsilon)\frac{n}{q+1}$。现在，性质 (iii) 表明 $T_i\subseteq S_j$。此外，性质 (ii) 表明 $|T_i|>\frac{1}{2}|S_j|$。这就证明了该断言。

利用上述断言，我们现在可以构造一个单射 $\phi\colon[q]\to[q+1]$，使得 $|T_i|\le|S_{\phi(i)}|$。首先，对于情形 II 中的 i，令 $\phi(i)$ 为相应的 j；然后，对于情形 I 中的 i，令 $\phi(i)$ 为任意一个尚未使用的 j 值。由于某个 $j\in[q+1]$ 不在 ϕ 的像中，因此有 $\sum_{i\in[q]}|T_i|<\sum_{j\in[q+1]}|S_j|=n$，矛盾。 □

参考文献

[AKS98] Noga Alon、Michael Krivelevich 和 Benny Sudakov。如何在随机图中找到一个大型隐藏团。Random Structures & Algorithms，13(3-4):457–466，1998。[BB20] Matthew Brennan 和 Guy Bresler。秘密泄露导致的可约性与统计—计算差距。载于《学习理论会议》，第648–847页。PMLR，2020。[BBH18] Matthew Brennan、Guy Bresler 和 Wasim Huleihel。植入式稀疏结构问题的可约性与计算下界。载于《学习理论会议》，第48–166页。PMLR，2018。

[BBK+21] Afonso S Bandeira、Jess Banks、Dmitriy Kunisky、Cristopher Moore 和 Alexander S Wein。谱植入，以及在随机图中否证割、可着色性和社区的困难性。载于《学习理论会议》，第410–473页。PMLR，2021。[BEH+22] Afonso S Bandeira、Ahmed El Alaoui、Samuel B Hopkins、Alexander S Wein、Tselil Schramm 和 Ilias Zadik。Franz–Parisi判据与高维统计中的计算权衡。载于第36届神经信息处理系统会议（NeurIPS 2022），2022。[BHK+16] Boaz Barak、Samuel B. Hopkins、Jonathan Kelner、Pravesh Kothari、Ankur Moitra 和 Aaron Potechin。植入团问题近乎紧的平方和下界。载于2016年IEEE第57届计算机科学基础年会（FOCS），第428–437页，2016。[BKW20] Afonso S Bandeira、Dmitriy Kunisky 和 Alexander S Wein。约束主成分分析问题中界的认证在计算上的困难性。载于第11届理论计算机科学创新会议（ITCS），第151卷，2020。[BKW22] Afonso Bandeira、Dmitriy Kunisky 和 Alexander Wein。非负主成分分析的平均情形整数性间隙。载于《数学与科学机器学习》，第153–171页。PMLR，2022。[BR13] Quentin Berthet 和 Philippe Rigollet。稀疏主成分检测的复杂性理论下界。载于《学习理论会议》，第1046–1066页。PMLR，2013。[BvH16] Afonso S Bandeira 和 Ramon van Handel。独立元素随机矩阵范数的尖锐非渐近界。《概率年刊》，44(4):2479–2506，2016。[CLR17] Tony Cai、Tengyuan Liang 和 Alexander Rakhlin。大型噪声矩阵中子矩阵定位的计算与统计边界。《统计年刊》，45(4):1403，2017。[CO05] Amin Coja-Oghlan。随机图的 Lov´asz 数。《组合、概率与计算》，14(4):439–465，2005。[FGR+17] Vitaly Feldman、Elena Grigorescu、Lev Reyzin、Santosh S Vempala 和 Ying Xiao。统计算法及检测植入团的一个下界。《美国计算机协会学报》（JACM），64(2):1–37，2017。[FK03] Uriel Feige 和 Robert Krauthgamer。最大独立集的 Lov´asz–Schrijver松弛的可能取值。《SIAM计算杂志》，32(2):345–370，2003。[HKP+17] Samuel B Hopkins、Pravesh K Kothari、Aaron Potechin、Prasad Raghavendra、Tselil Schramm 和 David Steurer。平方和方法在检测隐藏结构方面的威力。载于第58届计算机科学基础年会（FOCS），第720–731页。IEEE，2017。[Hop18] Samuel Hopkins。《统计推断与平方和方法》。博士论文，康奈尔大学，2018。[HS17] Samuel B Hopkins 和 David Steurer。基于少量样本的高效贝叶斯估计：社区检测及相关问题。载于第58届计算机科学基础年会（FOCS），第379–390页。IEEE，2017。[HW21] Justin Holmgren 和 Alexander S Wein。低次猜想的反例。载于第12届理论计算机科学创新会议（ITCS）。达格施图尔—莱布尼茨信息学中心，2021。¨HWX[Bruce Hajek、Yihong Wu 和 Jiaming Xu。随机图上社区检测的计算下界。载于《学习理论会议》，第899–928页。PMLR，2015。15] Jer[Mark Jerrum。大型团难以被Metropolis过程找到。Random Struct. Algorithms，3:347–360，1992。

[KM18] Pravesh K. Kothari 和 Ruta Mehta。平方和遇上纳什：寻找任意均衡的下界。载于第 50 届 ACM SIGACT 计算理论年会论文集，STOC 2018，第 1241–1248 页，美国纽约州纽约，2018 年。计算机协会。[KM21] Pravesh K. Kothari 和 Peter Manohar。无压力的着色平方和下界。载于第 36 届计算复杂性会议论文集，CCC '21，德国达格施图尔，2021 年。Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik。[Kom88] Hidetoshi Komiya。西翁极小极大定理的初等证明。Kodai 数学杂志，11(1):5–7，1988 年。[Kuˇc95] Ludˇek Kuˇcera。图划分问题的期望复杂度。离散应用数学，57(2-3):193–212，1995 年。[KWB22] Dmitriy Kunisky、Alexander S Wein 和 Afonso S Bandeira。关于假设检验计算困难性的注记：使用低次似然比进行预测。载于 ISAAC 大会（国际分析、应用与计算学会），第 1–50 页。施普林格，2022 年。[RSWY22] Cynthia Rush、Fiona Skerman、Alexander S Wein 和 Dana Yang。计算社区数量是否比找到它们更容易？arXiv 预印本 arXiv:2212.10872，2022 年。[Sio58] Maurice Sion。关于一般极小极大定理。Pacific J. Math.，8(4):171–176，1958 年。[SW22] Tselil Schramm 和 Alexander S Wein。基于低次多项式的估计的计算障碍。统计年刊，50(3):1833–1858，2022 年。[ZSWB22] Ilias Zadik、Min Jae Song、Alexander S Wein 和 Joan Bruna。基于格的方法在聚类中超越平方和。载于学习理论会议，第 1247–1248 页。PMLR，2022 年。