arXiv:2304.07284v1 [cs.CC] 14 Apr 2023

求解唯　一博弈：在全局超收缩图上　S

Mitali Bafna * Dor Minzer†

摘要

我们研究全局超收缩图上的仿射唯一博弈（UG）的复杂性。这类图本身不是小集扩张图，但可以对所有违反小集扩张性质的小集合进行有用且简洁的刻画。这类图包括 Johnson 图和 Grassmann 图，它们在近期针对 UG 的 PCP 构造中发挥了关键作用；此外还包括通过高维扩张图得到的推广。

我们的算法展示了如何对平方和（SoS）半正定规划中的“低熵”解进行舍入，从而广泛拓展 [BBK+21] 提出的算法框架。我们为 SoS 提出了一种新的舍入方案，它能消除给定伪分布中的全局相关性，使其在条件化后仍保留各种良好性质。条件化后对伪分布进行结构性控制，是许多基于 SoS 的算法面临的根本挑战。由于这些挑战，[BBK+21] 未能为全局超收缩图建立强有力的算法，只能针对可认证小集扩张图做到这一点。我们的结果在多个方面改进了 [BBK+21] 的结果：我们能够处理完备性任意小（但为常数）的实例；最重要的是，他们的算法所得的可靠性保证会随图的其他参数而变差（而在所有 PCP 构造中，这些参数都会随字母表大小增长），而我们的算法则不会。

我们的结果表明，在全局超收缩图上，唯一博弈问题很容易求解，因此凸显了在 UG 的 PCP 归约中，那些无法用此类特征刻画的图的重要性。

1 引言

1.1 唯一游戏

唯一游戏猜想（简称 UGC）是计算复杂性理论中的一个重要未决问题[Kho02]。人们之所以对 UGC 感兴趣，主要是因为如果它成立，就意味着大量近似困难性结果，而且这些结果往往是紧的 [KR08，KKMO07，Aus07，KNS10，Rag08]（参见 [Kho10，Tre12]）。例如，UGC 最引人注目的推论之一是：对于一类半定规划，在约束满足问题上，它们能够达到最佳的近似比（在所有高效算法中）[Rag08]。

另一方面，直到最近，关于证明 UGC 的研究大多陷入停滞。与 3-SAT 等问题不同，随机采样的唯一游戏（UG）实例很容易求解，这引出了一个问题：UG 的困难实例究竟是什么样的？为了讨论这一点，我们先给出唯一博弈问题的形式化定义，以及唯一游戏猜想的表述。

定义 1.1。唯一游戏的一个实例 Ψ 由一个图 $G=(V,E)$、一个有限字母表 Σ 以及一组约束组成：$\Phi=\{\Phi_e\}_{e\in E}$，每条边 G对应一个约束。对于所有 $e\in E$，约束 Φ_e 的形式为 $\Phi_e=\{(\sigma,\phi_e(\sigma)) \mid \sigma\in\Sigma\}$，其中 $\phi_e\colon \Sigma\to\Sigma$ 是一个一一映射。

*卡内基梅隆大学。部分经费由 CMU 计算机科学系和 CMU CYLAB 的捐赠提供。

†麻省理工学院数学系。经费由斯隆研究奖学金、美国国家科学基金会计算与通信基金项目 2227876 和美国国家科学基金会职业奖项目 2239160 提供。

唯一博弈问题的目标是找到一个赋值 $A\colon V \to \Sigma$，使其满足尽可能多的约束，也就是说，使 $(A(u)\ A(v)) \in \Phi_e$ 对尽可能多的边 $e=(u,v)\in E$ 成立。我们将实例 Ψ 的值定义为：

$$\mathsf{val}(\Psi) = \max_{A\colon V\to\Sigma} \frac{\#\{e \mid A \textit{ satisfies } e\}}{|E|}.$$

有鉴于此，唯一游戏猜想表述如下：

猜想 1.2. 对于所有 $\varepsilon,\delta>0$，存在 $k\in\mathbb{N}$，使得给定一个字母表大小至多为 k 的唯一博弈实例 Ψ，判断以下两种情形是 NP 困难的：
是情形：$\mathsf{val}(\Psi)\geq 1-\varepsilon$。
否情形：$\mathsf{val}(\Psi)\leq\delta$。

事实证明，底层图 G 的拓扑结构在其上定义的唯一游戏实例 [AKK+08、MM10、AIMS10]的复杂性中起着关键作用。具体而言，事实证明，扩张图上的唯一游戏很容易求解：

定义 1.3. 给定一个正则图 $G=(V,E)$ 和一个顶点集合 $S\subseteq V$，S 的边扩张定义为：

$$\Phi(S) = \Pr_{u\in S, v\in\Gamma(u)}[v\notin S].$$

如果对于每个大小至多为 $\xi|V|$ 的 $S\subseteq V$，都有$\Phi(S)\geq\gamma$，则称图 G 为 (γ,ξ)-小集扩张图。非正式地说，如果 G 是 (γ,ξ)-小集扩张图，其中 ξ 是一个小常数，我们就称 G 为小集合扩张图；如果 $\xi=1/2$，则称 G 为扩张图。 [AKK+08、MM10、AIMS10、BBK+21] 的结果表明，在小集合扩张图上，完备性接近 1 的 UG 实例很容易求解。因此，若要有任何机会证明唯一游戏猜想，就必须使用不属于扩张图和小集合扩张图范畴的图。

事实上，近期关于唯一游戏猜想的进展 [KMS17、DKK+18a、DKK+18b、KMS18] 采用了非小集合扩张图。在这些研究中，人们证明了二对一游戏是 NP困难的（这与唯一博弈是非常相似的问题，唯一的区别是，每个用于 ϕ_e 定义约束的映射都是二对一映射）。这还意味着，除其他结果外，对于所有 $\varepsilon>0$，给定一个字母表足够大的唯一游戏实例 Ψ，区分 $\mathsf{val}(\Psi)\geq 1/2$ 与 $\mathsf{val}(\Psi)\leq\varepsilon$的情形是 NP困难的。为了证明这些结果，这些研究以两种不同的方式使用了非小集合扩张图：

1. 光滑平行重复：KMS17、DKK+18a、DKK+18b、KMS18]的归约中的一个关键步骤，是应用平行重复定理 [Raz98]，从而为一个足够光滑的外层PCP构造得到困难性结果。粗略地说，这一过程中的这一步可以与交参数较大的 Johnson 图联系起来。也就是说，考虑图 $J(n,\ell,t)$，其顶点为 $\binom{[n]}{\ell}$；若两个顶点 A 和 B 满足 $|A\cap B|=\ell-t$，则它们相邻。我们认为 t 远小于 ℓ（例如，$t=\sqrt{\ell}$）。

2. 与 Grassmann 编码复合：Grassmann 编码是基于 $\mathbb{F}_2$ 上的格拉斯曼图 $\mathrm{Grass}(n,\ell)$ 对线性函数进行编码的一种方式。$\mathbb{F}_2$ 上的格拉斯曼图，其顶点是 $\mathbb{F}_2^n$ 的所有 ℓ 维子空间，记作 $\begin{bmatrix}n\\ \ell\end{bmatrix}$；若两个顶点 L 和 L' 满足 $\dim(L\cap L')=\ell-1$，则它们相邻。

上述两种图，即交集大小较大的 Johnson 图和格拉斯曼图，都不是小集合扩张图。不过，非常重要的是，格拉斯曼图中扩张性质不佳的小集合类具有简洁直观的刻画，而 2 对 1 游戏定理的证明很大程度上依赖于这一刻画。

虽然这个术语尚未正式定义，但我们将上述格拉斯曼图之类的图称为全局超收缩图。具体而言，我们指的是存在一族“显然非扩张的局部集合”，使得任何扩张效果不佳的小集合都必须与该族中的某个集合有较大的交集（半正式定义见第 5.1 节）。除格拉斯曼图之外，这类图还包括交集大小较小的 Johnson 图 [KMMS18], 、对称群上的某些 Cayley 图 [FKLM20]、 p-biased cubes f or $p = o(1)$、其他乘积域 [KLLM21] 以及高维扩展体 [GLL22、BHKL22b]。

因此，一个自然的问题是，研究定义在全局超收缩图上的唯一博弈的复杂性；这也是本文探讨的核心问题。其动机有两方面：

1. 首先，鉴于 [KMS17、DKK+18a、DKK+18b、KMS18]的归约以及上述讨论，一个有趣的问题是，是否存在一种归约，仅使用全局超收缩图，就能证明唯一博弈是 NP困难的。深入理解这些问题，将进一步揭示这一归约中困难性的来源，并阐明上述“光滑平行重复”步骤与“通过格拉斯曼编码进行复合”步骤各自的不同作用。

2. 其次，UGC 与另一个著名的计算问题有关，即小集合扩张问题 [RS10, RST12]。在 SSE 问题中，给定一个图 $G = (V, E)$，满足以下条件之一：(a) 对所有大小至多为 $\gamma|V|$ 的 $S \subseteq V$，都有 $\Phi(S) \geq 1 - \varepsilon$；或 (b) 存在一个大小至多为 $\gamma|V|$ 的 $S \subseteq V$，使得 $\Phi(S) \leq \delta$。小集合扩张假设（SSEH）断言，对于所有 $\varepsilon, \delta > 0$，当 γ 足够小时，该问题是 NP 困难的；论文 [RS10, RST12] 证明了这一假设蕴含 UGC。[1]

   尽管近期在 UGC 方面取得了进展，但 SSEH 尚无新的结果。从某种意义上说，要证明 SSE 的困难性结果，似乎只需使用小集合扩展图或全局超收缩图构件。否则，在最终的图中可能会产生非预期的小型非扩张集合（也就是说，这些集合并不对应于我们所归约的初始问题的任何解）。这促使人们研究全局超收缩图在与唯一游戏相关的归约中的作用。

近期，[BBK+21]（后续工作由 [BHKL22a]完成）研究了仿射唯一游戏这一类问题，我们将在下一节中对其进行定义和讨论。

1.2 全局超收缩图上的唯一游戏

定义 1.4。仿射唯一游戏的一个实例，是指字母表为模 q 的整数环 $\mathbb{Z}_q$，且所有约束映射 ϕ_e 均为仿射平移的唯一游戏实例；也就是说，它们具有如下形式： $\phi_e(\sigma) = \sigma + b_e$，其中 $b_e \in \mathbb{Z}_q$。

以一种等价但略有不同的方式来看，仿射唯一游戏问题可以表示为一个线性方程组 (X, E)，定义在 $\mathbb{Z}_q$ 上。E 中的每个方程都具有以下形式： $x_i - x_j = b$ 其中 x_i、 $x_j \in X$ 是变量，而 $b \in \mathbb{Z}_q$ 是某个常数。尽管看起来限制颇多，但已知 [KKMO07]，唯一游戏猜想成立，当且仅当它

[1] 更准确地说，这意味着唯一游戏猜想的一个更强版本，即唯一博弈在扩张轮廓与噪声超立方体相同的图上仍然是困难的。

对仿射唯一游戏这一类成立。此外，这一类涵盖了许多有趣的优化问题，例如最大割和图着色，因此下文将重点关注仿射唯一游戏。[2]

在 [BBK+21] 中，作者研究了 Johnson 图上仿射唯一博弈的复杂性，不过交集大小较小；在这种情形下，非扩张集合的刻画定理成立。具体而言，他们考虑的是 $t = \alpha\ell$ 时的“α-含噪” Johnson 图 $J(n,\ell,t)$，其中 $\alpha \in (0,1)$ 与 0 保持一定距离，并被视为独立于 ℓ 的固定常数。[BBK+21] 的结果表明，当 $\varepsilon > 0$ 足够小时，存在一个多项式时间算法：给定一个定义在 $J(n,\ell,t)$ 上、值至少为 $1-\varepsilon$ 的唯一博弈实例，该算法能找到一个满足至少 $C(\ell,\alpha,\varepsilon) > 0$ 个约束的赋值。这一结果最重要的特点是不依赖图 n 的大小和字母表大小，不过它有两个明显的缺点：

1. 算法得以运行所需的完备性保证接近 1(ε 接近 0)。因此，在他们结果所涉及的范围内，定义在含噪约翰逊图和格拉斯曼图上的唯一博弈，仍可能在完备性小于 $1/2$ 时是困难的（其中一般的唯一博弈现已知是困难的），但完备性超过 $1/2$时却突然变得容易。事实上，完备性为 $> 1/2$ 的格拉斯曼图上的唯一博弈，可通过扩展图唯一游戏算法本身轻易求解，因此，尽管格拉斯曼图具有全局超收缩性，他们的结果并未对格拉斯曼图上唯一博弈的复杂性给出任何非平凡的结论。因此，他们的算法对 [DKK+18b] 中那些完备性小于 $1/2$的困难实例究竟意味着什么，并不清楚：(1) 它们之所以困难，是由于光滑平行重复这一步骤，还是由于与格拉斯曼图的复合？(2) 外层PCP的光滑性是否必不可少——是否可以不用交集大小较大的 Johnson 图，而改用含噪约翰逊图？

2. 它们的可靠性保证取决于 ℓJohnson 图中集合的均匀度，而在大多数 PCP 构造中，该均匀度会随着实例的字母表大小而增长。事实上，这类图通常用于编码全局函数 $f\colon [n] \to \Gamma$（通常来自纠错码），其中 $|\Gamma| = O(1)$。在这种情况下，Johnson 图对应于编码 $F[A] = f|_A$的限制；此时，Johnson 图的每个顶点 A 都会被分配一个来自 Γ^ℓ 的标签，该标签对应于将 f 限制到A。因此，在通过 PCP 构造获得的唯一游戏实例的困难实例中（特别是上述实例），参数 ℓ 会随着唯一游戏实例的字母表大小而增长，所以我们希望算法的性能不依赖于该参数。

   不过我们要指出的是，算法的运行时间依赖于该参数是可以接受的（就像一个运行时间为 n^k 且能够解决唯一游戏的算法会推翻这一猜想一样，但能够满足至少 $1/k$ 比例约束的平凡随机算法并不会）。

1.3 我们的结果

我们的主要结果表明，存在一种多项式时间算法，可以在全局超收缩图上求解仿射唯一博弈，并绕过这两个障碍，从而回应第 1.1 节提出的动机。由于全局超收缩图这一术语尚无正式定义，下面列出一些适用的具体图实例。在第 5.1 节中，我们给出全局超收缩图的半形式化定义，并说明如何将我们的算法及其分析抽象化，以便在这类图上求解唯一博弈，前提是能够提供全局超收缩性的平方和证书。

[2] 我们指出，约简 [KKMO07] 并不保留图的拓扑. 因此，我们无法将我们的结果直接推广到一般唯一游戏类，并认为这是一个值得进一步研究的有趣方向。

我们首先考虑含噪约翰逊图，并给出以下两个结果。第一个结果讨论实例完备性接近 1 的情况；此时，我们的算法达到了 [BBK+21] 针对可认证小集合扩张图所给出的算法保证，尤其适用于 α-噪声超立方体图：

定理 1.5. 存在 $\varepsilon_0 > 0$，使得对于所有 $\alpha \in (0,1)$，以下结论对所有 $0 < \varepsilon \leq \varepsilon_0$ 均成立。存在一种算法，其运行时间为 $n^{\mathrm{poly}(\ell,|\Sigma|,1/\varepsilon)}$；该算法以 Ψ 为输入（它是定义在 $J(n,\ell,\alpha\ell)$ 上的仿射唯一博弈实例，并保证至少可满足 $(1-\varepsilon)$），并能找到一个赋值，使其满足 Ψ 中至少 $2^{-O\left(\frac{\sqrt{\varepsilon}}{\alpha}\right)}$ 比例的约束。

第二个结果讨论完备性任意小（但有正下界）的 UG 实例；在这种情况下，我们的算法可以满足常数比例的约束：

定理 1.6. 对于所有 $\alpha \in (0,1)$ 以及 $c > 0$，存在 $\delta > 0$，使得以下结论成立。存在一种算法，其运行时间为 n^D，其中 $D = \ell^{\mathrm{poly}(|\Sigma|\ell^{1/c})}$[3] 该算法以 Ψ 为输入（它是定义在$J(n,\ell,\alpha\ell)$ 上的仿射唯一博弈实例，并保证至少 c 可满足），并能找到一个赋值，使其满足 Ψ 中至少 δ 比例的约束。

请注意，当 ℓ为 $\alpha = \Omega(1)$时，上述定理中的可靠性保证与 α 无关；但随着 α 趋近于，保证会逐渐减弱。在下文第 1.3 节中，我们将讨论为什么无法得到一个多项式时间算法，在 $\alpha = o$满足 - 值解（例如 $1/\sqrt{\ell}$）的情形下获得 α，从而说明这种对 α 的依赖是必要的。

对于前面提到的任意全局超收缩图，我们都可以得到类似的结果。下面给出一个关于格拉斯曼图的推论。我们证明，存在一个多项式时间算法，能够求解格拉斯曼图上的仿射唯一博弈，即使实例的完备性很低：

定理 1.7。对于所有 $c > 0$，都存在 $\delta > 0$，使得以下结论成立。存在一个运行时间为 n^D、满足 $D = \ell^{\mathrm{poly}(|\Sigma|\ell^{1/c})}$ 的算法；该算法以 Ψ 作为输入，其中 Ψ 是 Grass(n,ℓ) 上的仿射唯一博弈实例，并承诺至少有 c 个约束可满足；该算法能够找到一个赋值，使其满足 Ψ 中至少 δ 比例的约束。

如前所述，由于格拉斯曼图的谱隙为 $1/2$，基于扩张图的唯一游戏算法已经能够推出定理 1.7，适用于 $c \gg 1/2$。因此，定理 1.7 的主要贡献，是给出了适用于完备性任意小情形的格拉斯曼图算法。

下面我们陈述关于高维扩展体（HDX）上随机游走的结果。高维扩展体是一大类图，它们推广了约翰逊图，但不一定具有约翰逊图的强对称性。这些图包括源自 [LSV05]构造拉马努金复形时所用截断的图，以及 [KO18]构造陪集复形扩展体时得到的图。这些图具有约翰逊图良好的高维扩张性质（例如全局超收缩性），但在其他方面有显著差异，例如它们具有有界度。

定理 1.8。对于所有 $\alpha \in (0,1)$ 和 $c > 0$，存在 $\delta > 0$ 使得以下结论成立。设 X 是任意一个 d 维的双侧 γ 局部谱扩张图，满足 $\gamma \ll o_\ell(1)$ 和 $d > \ell$。存在一种算法，其运行时间为 n^D，且具有 $D = \ell^{\mathrm{poly}(|\Sigma|\ell^{1/c})}$。该算法以 Ψ 为输入；Ψ 是一个定义在深度为 α 的 $X(\ell)$ 上的典范随机游走 M 上的仿射唯一游戏实例，并且保证其至少有 c 可满足；算法会找出一个赋值，使得 Ψ 中至少有 δ 比例的约束得到满足。

[3]需要指出的是，我们并未针对 D 进行优化，而 $\exp(\ell)$依赖于第 4节中平方和证明的次数。我们使用了一个黑箱命题，将其中的一些证明转化为平方和证明；我们猜想，若处理得当，实际上可以将平方和次数改进为 $O(\ell)$。

由于我们尚未定义任何高维扩展体术语，这里指出，这确实是定理 1.6 的推广。Johnson 图对应于完全复形 X（这是双侧局部谱扩张图最简单的一种实现），而 α-噪声 Johnson 图 $J(n,\ell,\alpha\ell)$ 对应于在 $X(\ell)$ 上的一种“典范”随机游走：它向下走 $\alpha\ell$ 层，再随机向上返回到 $X(\ell)$，同时确保顶点中的元素恰好改变 $\alpha\ell$ 个。事实上，在上述定理中，我们可以允许 M 是 $X(\ell)$ 上的任意完全随机游走，而我们的可靠性保证只取决于 c 以及 M 的某些参数；这些参数本质上独立于 ℓ[4]。

为使论述简洁，本文前半部分聚焦于约翰逊图。在第5节中，我们将对所用技术进行抽象，并讨论适用于一般全局超收缩图的算法，尤其是格拉斯曼图和高维扩展体上的随机游走。

我们结果的解读

我们的结果表明，通过[KMS17、DKK+18a、DKK+18b、KMS18] 的归约得到的唯一博弈实例，其困难性并非来自格拉斯曼图（它是全局超收缩的），而是来自光滑平行重复这一步骤。回顾一下，这一步骤使用了交集参数较大的约翰逊图（$J(n,\ \ell,\ \alpha\ell)$ 其中 $\alpha\approx 0$），该图并非全局超收缩。因此，结合归约中的知识和我们的算法可知，当 $\alpha = o(1)$ 时，α-含噪约翰逊图对于唯一博弈来说是困难的；而当 α 与0相距一定距离时，则变得容易。这也解释了为什么我们的可靠性保证必然会随着 α（在 $P\neq NP$条件下）而衰减。事实上，如果我们的结果适用于一般唯一博弈（而不仅仅是仿射唯一博弈），或者上述归约产生的是仿射唯一博弈实例，我们就能作出这样的断言。尽管我们相信，沿着我们算法的思路，应该存在适用于一般唯一博弈的算法，但我们不知道如何证明这一点，因此将其留作一个有趣的研究方向。

尽管忽略一般唯一博弈与仿射唯一博弈之间的细微区别，这意味着未来任何关于唯一游戏猜想的进展，都必须使用不具备全局超收缩性的图；这或许仍要借助光滑平行重复技术。

1.4 技术：适用于更高度平方和的新舍入方案

我们的算法通过一种新颖的舍入方案，以及对唯一游戏标准高阶平方和半定规划松弛的分析得出。Raghavendra 的 [Rag08] 开创性成果证明，在唯一游戏猜想成立的前提下，基本半定规划对所有约束满足问题都是最优的；这一成果促使研究者尝试利用高阶平方和松弛来推翻唯一游戏猜想 [Las01, Par00]。此后，对平方和算法的研究在诸多领域带来了大量算法进展：例如高维鲁棒统计 [BKS14, MSS16, BDH+20, BDJ+22]、量子计算 [BKS17]，以及半随机模型的算法 [BKS22], 。不过，这些工作大多将平方和方法用于平均情形问题；遗憾的是，针对最坏情形优化问题分析高阶平方和松弛的技术仍然十分匮乏。目前已知的少数最坏情形舍入技术包括 [BRS11, RT12] 中的全局相关性舍入技术，以及 [BKS17] 中通过重新加权对该技术的推广。

在这一背景下，最近 [BBK+21] 提出了一种新的舍入技术，用于处理具有“低熵”的唯一博弈（UG）松弛问题，其中熵是通过一个称为移位划分大小的函数来衡量的。给定该实例的两个固定赋值，其移位划分大小大致定义为这些赋值一致的变量所占的比例

[4]具体而言，它取决于 M 在[BHKL22a]中定义的某个阈值以上的剥离阈值秩。例如，当 M 是深度为 α、定义在 $X(\ell)$上的典范随机游走，且完备性为 $c = 1-\varepsilon$时，这个量为 $r(M) = O(\sqrt{\varepsilon}/\alpha)$，而我们的可靠性保证为$\exp(-r)$，与定理1.5相匹配。

（忽略对称性）。将半定规划解等价地视为非整数解上的一个分布 $\mathcal{D}$（称为伪分布），那么从 $\mathcal{D}$ 中抽取两个随机赋值，其移位划分大小的期望大致等于在 $\mathcal{D}$ 下局部碰撞概率的平均值，因而可作为 熵的 $\mathcal{D}$一种替代指标。他们的分析表明：（1）当移位划分大小（等价地，碰撞概率）的期望较大时，可以舍入得到高值解；此外，（2）当图是可认证小集扩张图时，伪分布的移位划分大小总是较大！不过，他们无法将这一思路推广到更广泛的全局超收缩图类，以得到高值解，因为在这种情况下，伪分布可能支撑在多个赋值上，因此其碰撞概率并不高。然而事实证明，即使在这个更难的情形下，伪分布在对事件 $\mathcal{D} \times \mathcal{D}$ 进行条件化之后， E仍具有较大的移位划分大小期望。但他们无法利用这一性质，因为条件化后，移位划分大小可能只是出于平凡的原因而较大[5]，因此不再是分布 $\mathcal{D}$的碰撞概率／熵的良好替代指标。

我们的主要技术贡献在于强化并广泛扩展这一舍入低熵伪分布的框架。我们证明，对伪分布进行适当的预处理后，实际上可以对任意事件 E （其概率不能太小）进行条件化，同时保留分布的大部分所需局部独立性。因此，即使在对 E 条件化后， $\mathcal{D} \times \mathcal{D} \mid E$ 的期望移位划分大小仍然很大，这也意味着伪分布 $\mathcal{D}$ 具有较高的碰撞概率。随后，可以使用一个简单的舍入过程，得到一个高值的唯一博弈解。对伪分布进行条件化，是我们所知少数几种能够利用高阶伪分布力量的方法之一，因此我们认为，在条件化后获得对分布的结构性控制这一思路，也可能适用于分析其他平方和算法。

从宏观上看， [BBK+21] 的算法可以理解为展示了如何对一个本质上支撑在单个赋值（在解空间的对称性意义下）上的伪分布进行舍入。不过，一般而言，我们的问题可能没有这么规整，因此由此得到的伪分布在这种受限意义下也可能不是低熵的[6]。我们扩展了“低熵”这一概念，从而纳入更广泛的一类伪分布；直观而言，这些伪分布“拥有少数几个优良解”，因而可归入这一类别，并适用于舍入。我们预计，这一强化后的框架应能广泛应用于其他优化问题的算法设计。下面将详细概述我们的技术，首先介绍 [BBK+21]的框架。

1.4.1 [BBK+21]的方法：通过移位划分进行舍入分析

固定一个仿射唯一博弈实例 $\Psi = (G = (V, E), \mathrm{F}_q, \Phi)$。在唯一游戏问题的平方和松弛中，我们有一组变量 $X_{v,\,\sigma}$，每个顶点对 $v \in V$及其对应的标签 $\sigma \in \Sigma$各有一个变量。~该程序的输出是一个伪期望算子 E，它为至多涉及 d个变量的每个单项式赋予一个实数，并满足：

1. 该值较高：

$$\widetilde{\mathbb{E}} \left[\sum_{(u,v) \in E} \sum_{\sigma \in \Sigma} X_{v,\sigma} X_{u,\phi_{u,v}(\sigma)} \right] \geq c \cdot |E|.$$

[5]在最坏情况下，事件 E 可能会使两个随机赋值上的乘积分布退化，从而第二个随机赋值总是等于第一个随机赋值。在这种情况下，从 $\mathcal{D} \times \mathcal{D} \mid E$ 中抽取的一对赋值相等，并不能说明 $\mathcal{D}$的碰撞概率。[6]例如，该分布可能以 $O(1)$ 个解为支撑；此时只有在对适当的事件进行条件化之后，碰撞概率才会很高。

2. $\widetilde{\mathrm{E}}$ 是一个线性半正定算子（视为 $\mathbb{R}^{M\times M}$ 上的矩阵时，M 是度至多为 $d/2$ 的单项式集合），满足关于 $X_{u,\,\sigma}$ 的各种布尔性约束。

3. 缩放：$\widetilde{\mathrm{E}}[1]=1$。

从直观上说，伪期望 $\widetilde{\mathrm{E}}$ 应当这样理解：存在一个未知的赋值分布 $\mathcal{D}$，……，A_m，其中每个赋值的值至少为 c。对于赋值 A_i，我们将其视为变量 $X_{u,\,\sigma}$ 上的布尔值赋值：当且仅当 $A_i(u)=\sigma$ 时，将变量赋为 1；并与之关联一个期望算子 E_i，它按照 A_i 以自然的方式将单项式映射为布尔值。于是，算子 $\widetilde{\mathrm{E}}$ 就是按照 $i\sim\mathcal{D}$ 对算子 E_i 求平均。[7]

移位划分：给定 $\widetilde{\mathrm{E}}$，可以构造另一个伪期望算子，从而能够访问两个赋值 $X=A_i$、$X'=A_j$ 的矩，其中 i、$j\sim\mathcal{D}$ 是独立选取的。取期望后，至少有 c^2 比例的边同时被 X 和 X' 满足；算法尝试满足这些边。为此，给定两个固定赋值 X 和 X'，我们定义 V 的顶点的移位划分：$V=\cup_{s\in\mathbb{F}_q}F_s$，其中对于每个 $s\in\mathbb{F}_q$，我们定义

$$F_s(X,X')=\left\{v\in V\mid X(v)-X'(v)=s\right\}.$$

移位划分大小定义如下：

$$\widetilde{\mathbb{E}}_{X,X'\sim\mathcal{D}}\left[\sum_{s\in\Sigma}\left(\frac{|F_s(X,X')|}{|V(G)|}\right)^2\right].$$

重新整理后可得，当 X 和 X' 相互独立时，该表达式是若干局部碰撞概率的平均值（准确地说，是 $\mathrm{E}_{u,v}[CP(X_u-X_v)]$），因此，移位划分大小的期望较大，对舍入很有帮助。

另一方面，注意到，如果边 (u,v) 同时被 X 和 X' 满足，那么 $X(u)-X(v)=X'(u)-X'(v)$，重新整理后可知，u 和 v 位于移位划分的同一部分 F_s 中。因此我们可以得出结论：对 X、$X'\sim\mathcal{D}$ 取期望时，图 G 中至少有 c^2 比例的边留在移位划分的同一部分内，这意味着移位划分的扩张率较小。

小集合扩展图。如果图 G 是小集扩张图，那么上述结论意味着，至少有一个集合 F_s/移位划分大小较大，并且在这种情况下，以下舍入过程有效：

1. 采样 $\widetilde{\mathrm{E}}$ 选择一个顶点 $v\in V$，并根据分布 $p(\sigma)=\mathrm{E}[X_{v,\sigma}]$ 选择 $A(v)=\sigma$。

2. 对任意 $u\in V$，根据分布 $p(a)=\frac{\mathbb{E}[X_{u,a}X_{v,\sigma}]}{\mathbb{E}[X_{v,\sigma}]}$ 对 $A(u)$ 进行采样。

为了理解这种舍入方案为何有效，可以把 X 视为固定值，把 X' 视为随机变量。因此，移位划分中部分 s 较大这一事实意味着，对于顶点中占固定比例的部分，$X'=X+s$。所以，在算法的第一步中对 v 进行赋值采样后，s的值便已确定。在第二步中，我们在给定 v取值的条件下，对其他节点进行赋值采样。然而，u 的某个取值比其他取值可能性大得多——也就是 $X(u)+s$，因此

[7]严格来说，给定 $\widetilde{\mathrm{E}}$ 时，我们无法保证存在如上所述、定义在良好赋值上的实际分布 $\mathcal{D}$，不过，为了进行非正式介绍，这种直觉已经足够。

我们可以预期，对于顶点 u中占固定比例的部分， $X'(u) = X(u) + s$ 。特别是，对于 F_s 内部任何一条由 X满足的边 (u,w)，以固定的概率，采样得到的 u 和 w 的赋值分别为 $X(u)+s$和 $X(w)+s$，此时我们就能满足 (u,w)。为了从形式上分析这种舍入策略， [BBK+21]关键地利用了 X 与 X'的独立性。

本质上，上述结论表明，较大的移位划分意味着 X 的解空间具有较高的碰撞概率，进而可用于舍入。具体来说，我们的分布实际上只包含一个赋值（模平移对称性）及其扰动。

非小集合扩张图。考虑一个不是小集合扩张图的图，例如 G 是 Johnson 图 $J(n,\ell,t=\ell/2)$。在这种情况下，上述推理不再成立，因为 F_s 可能确实全由小集合组成。不过，正如前文所述，利用全局超收缩性，我们可以推知，集合 F_s 中必有一个具有某种特定结构——它在某个典范非扩张集合内的密度较大。具体来说，对于 Johnson 图，这些典范集合具有如下形式：

$$H_R = \left\{ A \in \binom{n}{\ell} \;\middle|\; A \supseteq R \right\},$$

对于 $R \subset [n]$ 和 $|R| = r = O(1)$。事实上，全局超收缩性给出了以下更强的结构性质：集合 $H = \bigcup_{R\in\mathcal{R}} H_R$（其中 $\mathcal{R}$ 由所有满足某个部分 F_s 在其内部稠密的 R 组成）具有常数测度。经过简单的计数可知， $|\mathcal{R}| \geq$ 为 $\Omega($ $n^r/\ell^r)$；又由于不同的典范集合至多有 $\binom{n}{r}$ 个，因此 $|\mathcal{R}|$ 包含这些集合中 $\Omega(1/\ell^r)$ 比例的集合。

不过，对于每种 X 和 X' 的选择，我们可能会得到不同的一组稠密子立方体 $\mathcal{R}$。但由于 $\mathcal{R}$ 包含了所有子立方体中 $\Omega(1/\ell^r)$ 的比例，因此至少存在一个子立方体 H_R，它在 X、 $X' \sim \mathcal{D}$ 上以 $\Omega(1/\ell^r)$ 的概率是稠密的。令 H_R 为这样一个子立方体，并令 $E_R(X,X')$ 表示 H_R 是稠密的这一事件。理想情况下，此时我们希望对 E_R 进行条件化，使移位划分 F_s 中的一部分在 H_R 内变大，然后寄望于像小集扩张图的情形那样，能够满足 $F_s \cap H_R$ 内的许多边。

遗憾的是，这一设想并未实现——对 E_R 进行条件化后，尽管移位划分很大，上述舍入策略仍可能失效。事实上，在舍入过程中，我们希望对于每个顶点 u， X、 $X' \sim \mathcal{D}$ 上的 $X(u)$ 和 $X'(u)$ 的取值彼此独立。然而，条件化后，(X,X') 上的联合分布 $\mathcal{D}\times\mathcal{D} \mid E_R$ 可能存在 X 与 X' 之间的相关性。特别是，该分布甚至可能仅支持这样的数对 (X,X')：其中两者总是相等。在这种情况下，移位划分之所以很大只是出于显而易见的原因，因此其规模大并不能说明 $\mathcal{D}$ 的碰撞概率或熵有任何性质。

因此，在 [BBK+21] 中，作者无法实现这种条件化，因此只能满足$\Omega\left(\frac{1}{\ell^{2r}}\right)$比例的 H_R约束。之后，他们多次迭代这一算法，以满足整个图中$\Omega\left(\frac{1}{\ell^{2r}}\right)$比例的约束。

1.4.2 **O**我们的方法：通过（消除）全局相关性对事件 E 进行条件化 **s**

我们对上述框架的主要贡献是证明，通过增加一个额外的预处理步骤，我们可以确保即使在对上述事件 E_R 进行条件化之后，赋值 X 和 X' 仍然高度独立。具体而言，移位划分中的某一部分变大这一现象必然会发生——正如在小集扩张图的情形中一样——这是因为我们的分布具有较高的碰撞概率。

由于事件 $E = E_R(X,X')$ 的概率至少为 $\Omega\left(\frac{1}{\ell^r}\right)$，只要我们处于 SoS 层级足够高的位置（$\Theta(\ell^r)$层就足够，整体运行时间为 $n^{\Theta(\ell^r)}$），我们就能获得条件化

伪期望

$$\widetilde{\mathbb{E}}[Y \mid E] = \frac{\widetilde{\mathbb{E}}[Y 1_E]}{\widetilde{\mathbb{E}}[1_E]}.$$

这意味着，我们可以在事件 E 条件下对顶点的标签进行采样。不过，要让这种方法发挥作用，我们必须改变舍入过程。为了获得一些直观认识，不妨考虑极端情况：在对 $E(X, X')$ 进行条件化后，我们的分布中 X 和 X' 之间仍存在很强的相关性。

也就是说，假设在对 E 进行条件化之后，对于几乎所有顶点 u，都有 $X(u) = X'(u)$。在这种情况下，如果我们从 $\mathcal{D} \times \mathcal{D}$ 中抽取 X、X'（不对 E进行条件化），那么事件 E 成立的概率至少为 $\mathbf{Pr}[E] \geq \Omega\left(\frac{1}{\ell^r}\right)$；此时，$X$ 和 X' 在几乎所有顶点上的取值都一致。这意味着，如果 $\mathcal{D}$ 是一个实际分布，那么这些赋值具有很强的全局相关性：对于满足 $\mathbf{Pr}_{\mathcal{D}}[E(X, X_0) = 1] \geq \mathbf{Pr}_{\mathcal{D}\times\mathcal{D}}[E]$ 的 X_0，固定 $X' = X_0$。一旦 E 成立，对于几乎所有顶点对，都有 $X(u) - X(v) = X_0(u) - X_0(v)$；因此，赋值 X 在顶点 u和 v 上的取值跨$\mathcal{D}$相关。于是，一个自然的想法是将 $\mathcal{D}$ 变换为另一种不存在全局相关性的分布，以此避免这个问题；所谓不存在全局相关性，是指典型顶点对 u 和 v 上的赋值几乎相互独立。

为此，我们采用 [RT12]，中的一个思想。将其适配到我们的设定后，它表明，对于任意 $\tau > 0$，都存在 $d = d(\tau, |\Sigma|)$，使得在随机选取的 d 个顶点的取值条件下，事件 E 的全局相关性至多为 τ。也就是说，对于两个典型顶点 u 和 v，$X(u)$ 与 $X(v)$ 的取值之间的相关性至多为 τ，而 X' 也同样如此。接着，我们在引理 3.10 中证明，如果起始时有一个缺乏全局相关性的伪分布，那么可以对事件 E 进行条件化，并保留赋值 X 和 X' 之间的近似独立性，至少在大多数顶点上如此。更准确地说，我们证明，对于 $Y_{u,v} = (X(u), X(v))$ 和 $Y'_{u,v} = (X'(u), X'(v))$，几乎所有顶点对 u、v 上的 $Y_{u,v}$、$Y'_{u,v} \mid E$ 与 $Y_{u,v}$、$Y'_{u,v}$ 之间的统计距离都很小。[8]

利用这一思路，我们能够在某个基本集合 H_R 上得到一个取值为 Ω(1) 的解。总而言之，我们首先对伪分布进行预处理，以消除全局相关性。随后，我们可以找到一个事件 $E(X, X')$，对应于移位划分中的某个部分 F_s 已在某个基本集合 H_R 中变得稠密这一事实。此外，在对 E 条件化后，大多数配对 $(X(u), X(v))$、$(X'(u), X'(v))$ 仍然近乎独立。接着，在 H_R 上运行一个简单的舍入过程（如 [BBK+21] 中所述），我们便能满足 H_R 内相当一部分边。不过，H_R 可能只占图的 $o(1)$ 比例，因此，和 [BBK+21] 一样，我们会多次重复这一过程，从而为整个图得到一个取值为 Ω(1) 的解。这就给出了一个针对 Johnson 图上的仿射唯一博弈的高效算法，如定理 1.5 所述。

要证明定理 1.6 （即 c 不接近 1 的情形），还需要做更多工作。事实上，当 c 接近 1 时，我们可以得出结论：几乎所有边都落在移位划分的某个部分 F_s 内。因此，只要我们的集合 H_R 覆盖了某个 F_s内部常数比例的边，它们就必然也覆盖了同时被 X 和X'满足的边中的常数比例，而这些正是我们的舍入过程能够满足的边。如果 c 仅仅与 0保持一定距离，我们就无法再作出这样的论证，甚至无法确定集合 H_R 是否覆盖了我们有望满足的边。

1.4.3 实现小完备性：捕获所有非扩张边

为了针对完备性 c 仅能保证与 0 保持正距离的情况设计算法，我们必须首先论证，在移位划分中，我们能够捕获几乎所有留在.....之内的边

[8]为了使舍入成功，我们需要使用更复杂版本的 $Y_{u,v}$（见定义 3.5）。证明引理 3.10 在技术上颇具挑战，因为这些 $Y_{u,v}$ 并非指示变量，只是近似如此；此外，我们还需要确保证明适用于伪分布，而不仅仅适用于实际分布。

一部分 F_s 使用 th 基本集合 H_R（以确保我们包含满足 X 和 X' 的边).

为此，我们需要一个更精细的全局超收缩性推论：如果 Johnson 图中有一个较小的顶点集合 F，其边扩张至多为 $1-\eta$，那么我们可以找到一组基本集合 $\mathcal{R}$，满足：

1. 有界且稠密：每个 $R \in \mathcal{R}$ 的大小为 $|R| = O(1)$，并且 F 在每个 H_R中都是稠密的。也就是说，对于每个 $R \in \mathcal{R}$，$\delta(F \cap H_R) \geq \Omega\eta(\delta(H_R))$。
2. 最大稠密：对于所有 $R \in \mathcal{R}$，所有 $R' \subsetneq R, F$ 在 $H_{R'}$中都不是很稠密。
3. 捕获几乎所有非扩张边：留在 F 内部的边，几乎也都留在某个 $R \in \mathcal{R}$对应的H_R 内部。

事实上，我们证明，诸如 [KMMS18] 中的全局超收缩不等式，可以用来证明这样的结果（以黑箱方式）。

利用这一结果，我们可以证明，对于 $R \in \mathcal{R}$，位于子立方体 H_R 内部的边覆盖了移位划分中位于同一部分内部的大多数边。这里有一些需要处理的细节，例如“正则性问题”：有多少个不同的 R 覆盖给定的一条边。上面的第二项旨在处理这类问题，大致来说，它表明没有顶点或边会被过度重复计数。之后，我们可以对事件 E 进行条件化；和之前一样， E 表示某个部分 F_s 在某个基本集合 H_R 内变得稠密，因此得到的分布在 H_R 内具有较大的移位划分。此时，我们（从本质上说）又回到了这样一个问题：如何在具有较大移位划分的集合上对平方和解进行舍入，只不过现在我们的解的值为 $c' > 0$（而不是接近 1）。值得注意的是，我们再次运用了前文提出的“消除全局相关性”这一思路，以便在条件化后仍保留近似独立性。通过更细致的处理，我们采用与完备性接近 1 时类似的分析，在 c 任意小时完成证明。

1.5 未解决的问题

我们通过陈述几个对未来研究具有意义的开放方向，结束本节的介绍。第一个问题探讨我们的结果是否仍适用于非仿射唯一游戏：

问题 1. 对于全局超收缩图 G，例如 Johnson 图（交集大小较小的情形）和格拉斯曼图，是否存在一种多项式时间算法：给定一个在 G 上的唯一游戏实例 Ψ，满足 $\text{val}(\Psi) \geq 1-\varepsilon$（其中 $\varepsilon > 0$ 被认为较小），找出一个至少满足 δ 比例约束的赋值 Ψ？当 $\text{val}(\Psi) \geq c$ 时又如何，其中 c 与 1 的距离有正的下界？

第二个问题探讨是否还有其他组合优化问题可以通过我们的技术获得改进的算法。非正式地说，我们展示了如何对低熵伪分布进行舍入，其中包括那些支撑在 O 个赋值上的伪分布（以及它们的扰动）。我们的做法是证明，在消除全局相关性之后，即使经过条件化，仍然可以保留局部独立性。我们相信，这项技术应当能够应用于唯一博弈之外的领域——对于任何能够在平方和中证明“良好解很少”的问题，都可以应用我们的舍入技术来获得这样一个解。

问题 2：能否利用低熵舍入框架，缩短其他组合优化问题的运行时间，例如用尽可能少的颜色对 3-可着色图进行着色？

第三，值得探究我们的技术能否帮助设计改进的次指数时间算法，用于求解组合优化问题，例如一般图上的最大割（理想情况下），或特殊类别图上的最大割。

问题 3。能否使用低熵舍入框架，在时间复杂度为 $2^{n^{\varepsilon}}$ 的情况下，获得更优的最大割近似算法?

2 预备知识

记号。对于一个（带权）图 $G=(V,E)$，我们用 (u,v) 表示边上的分布，其中各边的概率与其权重成正比；用 A_G 表示与图 G 上随机游走相关的转移矩阵。我们将图 G 的拉普拉斯算子定义为 $L_G = I - A_G$，并用 π_G 表示图 G 的平稳分布。本文主要研究正则图，因此使用 G 上的均匀分布。我们用 $\langle f,g\rangle_G$ 表示 $\mathrm{E}_{u\sim\pi_G}[f(u)g(u)]$。上下文明确时，我们通常省略 G 的下标。

如果 A 是某个概率事件或条件，我们用 $\mathrm{I}(A)$ 表示 A 的指示随机变量（即，如果 A 发生，则 $\mathrm{I}(A)=1$；否则 $\mathrm{I}(A)=0$）。

2.1 唯一游戏的平方和松弛

我们的算法基于平方和半正定规划（半定规划）松弛，特别是将其视为对伪期望算子进行优化的观点。本节将简要介绍必要的背景知识以及我们将用到的若干基本事实；更系统的介绍请参阅综述 [BS14、RSS18、FKP19]。

给定唯一博弈实例 $I=(G=(V,E),\Sigma,\Pi)$，I 的值可通过以下关于零一变量 $\{X_{u,a}\}_{u\in V、a\in\Sigma}$ 的整数规划计算：

$$\begin{aligned}\max_{X}\ & \mathop{\mathbb{E}}_{(u,v)\in E}\sum_{a\in\Sigma}X_{u,a}X_{v,\pi_{uv}(a)} && (1)\\ s.t.\quad & X_{u,a}^2 = X_{u,a} && \forall u\in V, a\in\Sigma,\\ & X_{u,a}X_{u,b}=0 && \forall u\in V, a\neq b\in\Sigma,\\ & \sum_{a}X_{u,a}=1 && \forall u\in V.\end{aligned}$$

事实上，对变量 $X_{i、a}$ 的一次赋值代表对 G 的顶点的一次赋值，其中顶点 $v\in V$ 在 $X_{v、a}=1$ 时取标签 $a\in\Sigma$，而目标函数统计满足的约束所占的比例。

上述规划的度为 D 的平方和松弛是一个用于松弛上述规划的凸优化规划。该规划可以写成一个优化问题，其目标是为变量 $X_{S,\sigma}$ 寻找一个向量值赋值；对于每个大小至多为 D 的顶点集合 S 及其标签 $\sigma\in\Sigma^S$，我们都有这样一个变量。该规划的约束涉及这些向量之间的内积，旨在确保对于任意两个满足 $|S\cup T|\le D$ 的顶点集合 S 和 T，内积 $\langle X_{S,\sigma}, X_{T,\sigma'}\rangle$ 表示在 $S\cup T$ 上的赋值分布，并且这些分布局部一致。对我们而言，以伪期望的语言来描述平方和松弛的解会更方便；下一节将介绍这种不同但等价的视角。

2.2 伪期望、伪分布与伪概率

伪期望。度为 D 的伪期望 $\widetilde{\mathrm{E}}$ 是一个算子 $\widetilde{\mathrm{E}}: X^{\leq D} \to \mathrm{R}$，其中 $X^{\leq D}$ 是 X 变量中次数至多为 D 的所有单项式的集合，并且 E 满足上述等式约束以及作为公理的布尔性约束 $\{X_{u,a}^2 = X_{u,a}\}$。为简便起见，我们将这组公理称为 $\mathcal{A}_I$；当 I 的含义可从上下文中明确时，省略下标。更一般地，给定一个多项式优化程序 $P = \{\max_x p(x) \ s.t.\ q_i(x) = 0, \forall i \in [m]\}$，其度为 D 的平方和半正定规划松弛是一个规模为 $n^{O(D)}$ 的半正定规划，它返回一个伪期望算子 $\widetilde{\mathrm{E}}: x^{\leq D} \to \mathrm{R}$。通过线性性（下文将给出精确定义），可以将该算子唯一地扩展为作用于所有次数至多为 D 的多项式的伪期望算子。该算子满足以下四个性质：

- 缩放：$\widetilde{\mathrm{E}}[1] = 1$。
- 线性性：$\widetilde{\mathrm{E}}[a \cdot f(x) + b \cdot g(x)] = a \cdot \widetilde{\mathrm{E}}[f(x)] + b \cdot \widetilde{\mathrm{E}}[g(x)]$，对所有 $a, b \in \mathrm{R}$ 以及所有度为 $\leq D$ 的多项式 f, g 均成立。
- 低次平方的非负性：$\widetilde{\mathrm{E}}[s(x)^2] \geq 0$ 对所有满足 $\deg(s) \leq \frac{D}{2}$ 的多项式 $s(x)$ 均成立。
- 程序约束：$\widetilde{\mathrm{E}}[f(x) \cdot q_i(x)] = 0$ 对所有 $i \in [m]$ 和满足 $\deg(f q_i) \leq$ 的多项式 $f(x)$ 均成立D。

根据我们要解决的问题，我们还会讨论伪期望 E 所达到的值，该值定义为目标函数的伪期望。对于我们感兴趣的情形，即仿射唯一游戏的情形，E 在实例 I 上的值记为 $\mathrm{val}_\mu(I)$，定义为

$$\widetilde{\mathbb{E}}[\mathrm{val}_I(X)] = \widetilde{\mathbb{E}}\left[\mathop{\mathbb{E}}_{(u,v)\in E} \sum_{a\in\Sigma} X_{u,a} X_{v,\pi_{uv}(a)}\right].$$

我们的伪期望将保证取得与完备性保证相匹配的值（例如，在定理 1.6、1.7 的情境中，它将满足 $\mathbb{E}[\mathrm{val}_I(X)] \geq c$）。

伪分布。我们常将伪期望算子 E 称为对应于变量 X 上的伪分布 μ 的算子。这类似于我们有一个实际分布 μ 及其对应的期望算子 $\mathrm{E}_\mu[\cdot]$ 的情况。这种记号使我们使用 E 算子进行的分析更为直观，因为实际分布的许多性质对伪分布也成立。因此，当我们说给定一个度为 D 的伪分布 μ 时，我们指的是度为 D 的伪期望算子 E_μ。

伪概率。

定义 2.1（事件的伪概率）。设 μ 是一个度为 D 的伪分布。对于事件 $\mathcal{E}(X, X')$，若 $\mathrm{I}[\mathcal{E}(X)]$ 可表示为关于 X 的度-D 函数，则我们将 $\mathcal{E}(X)$ 的伪概率定义为

$$\widetilde{\Pr_\mu}[\mathcal{E}(X)] = \widetilde{\mathbb{E}}_\mu[\mathbb{I}(\mathcal{E}(X)].$$

类似地，若 $\mathcal{F}(X)$ 是一个事件，且 $\deg(\mathrm{I}[\mathcal{F}(X)]) + \deg(\mathrm{I}[\mathcal{E}(X)]) \le D$，则我们将以 $\mathcal{F}(X)$ 为条件的$\mathcal{E}(X)$的伪概率定义为

$$\widetilde{\Pr}_{\mu}[\mathcal{E}(X) \mid \mathcal{F}(X)] = \widetilde{\mathbb{E}}_{\mu}[\mathbb{I}(\mathcal{E}(X)) \mid \mathbb{I}(\mathcal{F}(X))] = \frac{\widetilde{\mathbb{E}}[\mathbb{I}(\mathcal{E}(X)) \cdot \mathbb{I}(\mathcal{F}(X))]}{\widetilde{\mathbb{E}}[\mathbb{I}(\mathcal{F}(X))]}.$$

2.3 对数学证明进行平方和化

我们的论证将用到若干数学陈述（例如全局超收缩性），而且我们需要能够论证这些陈述在平方和程序及其变量的语境下也成立。因此，我们需要确保使用的工具能够通过低度平方和不等式（以及公理）来证明。下面我们汇集了一些将会用到的标准工具。我们使用以下记号来表示平方和证明。

平方和证明的记号。给定一组关于多项式$q_i, g_j \in \mathrm{R}[X]$的公理 $\mathcal{A} = \{q_i = 0\}_i \cup \{g_j \ge 0\}_j$，如果满足以下条件，我们就称“存在一个度为-$d$ 的平方和证明，表明 $f \ge h$ 模 $\mathcal{A}$成立”：$f = h + s + \sum_k c_k \cdot Q_k + \sum_t r_t \cdot G_t$其中，每个多项式 Q_k和 G_t分别是若干个来自$\{q_i\}$和 $\{g_j\}_j$的多项式的乘积，$s, \{c_k\}_k, \{r_t\}_t \in \mathrm{R}[X]$是实多项式，且 s和 $\{r_t\}_t$都是平方和；而 $s, \{c_k Q_k\}_k, \{r_t G_t\}_t$中的最大度不超过 d。我们用记号$\mathcal{A} \vdash_d f(x) \ge h(x)$表示存在这样一个等式。有时我们也用 $f(x) \ge h(x)$表示该不等式是一个平方和不等式。

2.3.1 基本不等式

其中首先介绍柯西-施瓦茨不等式和霍¨尔德不等式的以下基本形式。其证明如今已是标准内容，例如可见于 [BKS14、OZ13]。

引理 2.2（柯西-施瓦茨不等式）。对于所有 $\epsilon \in \mathrm{R}_+$,

$$\vdash_2 YZ \le \frac{\epsilon}{2} Y^2 + \frac{1}{2\epsilon} Z^2.$$

引理 2.3（柯西-施瓦茨不等式）。一个度为 D 的伪期望算子，其中 $D \ge 2\max(\deg(f), \deg(g))$，满足

$$\widetilde{\mathbb{E}}[fg]^2 \le \widetilde{\mathbb{E}}[f^2]\,\widetilde{\mathbb{E}}[g^2].$$

事实 2.4（霍¨尔德不等式）。对于所有实数 $\nu > 0$，我们有：

$$\vdash_4 Y^3 Z \le \frac{3\nu}{4} Y^4 + \frac{1}{4\nu^3} Z^4.$$

单变量平方和理论（尤其是卢卡奇定理）指出，若一个单变量多项式在某个区间上非负，那么这一事实也可由平方和证明。卢卡奇定理的以下推论广为人知。

推论 2.5（Luk´acs 定理的推论）。设 q 是一个在$[a, b]$上非负的d 次多项式。那么，给定公理 $\mathcal{A} = \{x \ge a\} \cup \{x \le b\}$，存在一个$2d$度平方和证明，证明 q非负，$\mathcal{A} \vdash_{2d} q(x) \ge 0$。

我们将多次使用上述结果，以黑箱方式将单变量不等式转换为平方和不等式。

对于多变量不等式，上述定理不再成立。不过，对于一个严格为正且 f 与0相距一定距离的多项式，可以利用$\deg(f)$ 次的平方和证明，其次数关于 [Sch04]呈指数级增长。这里我们陈述 [Sch04] 的一个推论，它足以满足我们的需要。

定理 2.6 ([Sch04]的推论)。 设 S为集合 $[0,1]^k$。设 $f(x)$ 为一个次数为 d的多项式，且$\nu = \min\{f(x) \mid x \in S\} > 0$，并令 $||f||$表示 f的系数的绝对值的最大值。则 f有一个有界次数的平方和证书：

$$\{x_i \in [0,1] | i \in [k]\} \vdash_D f(x) \geq 0,$$

其中 $D = \text{poly}(k^{\deg(f)}, ||f||/\nu)$。

我们将在第 4 节利用上述事实，将涉及常数次数多项式和常数个变量的不等式转化为平方和不等式。我们认为，在多项式 $\text{poly}(\deg(f))$ 合理的情况下，上述次数上界应当可以达到 f，不过据我们所知，这一点尚未在一般情形下得到证明。

2.3.2 用低次多项式逼近指示函数

我们的论证将涉及诸如 $f(X) \geq \beta$ 这样的事件指示函数，其中 f 是一个低次多项式；我们还需要对这类事件进行条件化。严格来说，函数 $\mathbb{I}[f(X) \geq \beta]$ 不是低次多项式，因此我们无法据此进行条件化。不过，不难证明，这类指示函数可以用低次多项式逼近，而我们也需要运用这类思路。事实上，本节将介绍一个逼近定理，并在后续证明中反复使用。

以下定理由 [DGJ+10]提出，它给出了阶跃函数的一个低次逼近。

定理 2.7。设 $\mathbb{I}[x \geq \beta]$ 是在 $\beta \in (0,1)$ 处的阶跃函数。那么，对每个 $0 < \nu < \beta$，都存在一个一元多项式 $p_{\beta,\nu}$，其度为 $O(\frac{1}{\nu}\log^2 \frac{1}{\nu})$，满足：

1. $|p_{\beta,\nu}(x) - \mathbb{I}[x \geq \beta]| \leq \nu$ *for all* $x \in [0,\beta] \cup [\beta+\nu, 1]$.
2. $p_{\beta,\nu}$ 在 $(\beta, \beta+\nu)$ 上单调递增。
3. 对所有 $x \in [0,1]$, $0 \leq p_{\beta,\nu}(x) \leq 1$。
4. $p_{\beta,\nu}$ 的所有系数的绝对值均不超过 $2^{O(\log(1/\nu)/\nu)}$。

此外，前三个事实都是度为 $2\deg(p_{\beta,\nu})$ 的 SoS 可证结论。

前三项由[DGJ+10的定理 4 得出。5], 第四项由马尔可夫兄弟不等式立即得到，而 SoS 可认证性则由推论 2.5 得出。

以下事实为指示函数的逼近多项式提供了方便的逐点上界。

~事实 2.8 （有界多项式的马尔可夫不等式）。 设 $p := p_{\beta,\nu}$ 为定理 $D = O(1/\nu)$ 保证存在的度为的多项式。则 p满足马尔可夫不等式：

$$\{0 \leq x \leq 1\} \vdash_{\deg(p)} \{p(x) \geq 1 - \frac{1-x}{1-\beta-\nu} - \nu\} \cup \{p(x) \leq \frac{x}{\beta-\nu} + \nu\}$$

证明。 我们对 x 进行分类讨论，然后利用推论 2.5 得出证明是平方和。对于第一个不等式，当 $x \in [0, \beta + \nu)$ 时，有

$$p(x) \succeq 0 \succeq 1 - \frac{1-x}{1-\beta-\nu},$$

其中我们用到了 $p(x) \succeq 0$ 和 $\frac{1-x}{1-\beta-\nu} \succeq 1$。对于 $x \in [\beta + \nu, 1]$,

$$p(x) \succeq 1 - \varepsilon \succeq 1 - \varepsilon - \frac{1-x}{1-\alpha-\delta},$$

其中我们用到了 $x \in [0, 1]$，因此我们减去的是一个正量。结合这些结论，即可证明第一个结论。

要看出第二个结论，注意对于 $x \in [0, \beta-\nu]$, $p(x) \leq \nu$；对于 $x \in (\beta-\nu, 1]$, $p(x) \leq 1 \leq \frac{x}{\beta-\nu}$。证明完毕。 □

2.4 伪期望的操作

2.4.1 重新加权与条件化：

有时我们会通过多项式 $s(x)$ 对度为 D 的伪分布进行重新加权或条件化，其中 $s(x)$ 在程序公理下非负，即对于 $d < D$, $\mathcal{A} \vdash_d s(x)$。从技术上说，这一操作相当于定义一个新的度为 $D - d$ 的伪期望算子 $\widetilde{\mathrm{E}}'$，定义如下：

$$\widetilde{E}'[x^\alpha] = \frac{\widetilde{\mathbb{E}}[x^\alpha \cdot s(x)]}{\widetilde{\mathbb{E}}[s(x)]},$$

对于每个次数至多为 $D - d$ 的单项式 x^α。例如，根据 1 中给出的唯一博弈公理，可以证明变量 X_i 属于 $[0, 1]$, ，因此可以用 X_i 对伪分布重新加权。可以证明，重新加权后，伪分布在次数至多为 $D - d$ 时仍满足四个性质。因此，我们也将这一操作称为“条件化”，并将 $\widetilde{\mathrm{E}}'$ 记作 $\widetilde{\mathrm{E}}[\cdot \mid s(x)]$。我们通常会用多项式 $s(x)$ 进行“条件化”，该多项式是某个事件 E 的平滑近似；在这种情况下，上述操作可理解为对来自伪分布的样本进行条件化，使其满足事件 E 所指定的某些性质。关于重新加权的进一步讨论，请参阅 [BRS11、BKS17] 。

2.4.2 独立样本

回忆一下，给定的伪期望算子 $\widetilde{\mathrm{E}} : X^{\leq D} \to \mathrm{R}$ 可以理解为对伪分布 $X \sim \mu$ 上的函数 $f(X)$ 取平均。我们需要能够模拟对两个独立选取的样本 $X, X' \sim \mu$,[9] 取平均，因此定义乘积伪期望 $\widetilde{\mathrm{E}}_{X,X'}$ 如下：令 $X^\alpha (X')^\beta$ 为变量 X, X' 中度至多为 D 的单项式；我们定义 $\widetilde{\mathrm{E}}_{X,X'}[X^\alpha (X')^\beta] := \widetilde{\mathrm{E}}_X[X^\alpha] \cdot \widetilde{\mathrm{E}}_X[X^\beta]$。容易验证， $\widetilde{\mathrm{E}}_{X,X'}$ 也是一个伪期望算子，它对应于从伪分布 μ 中抽取的两个独立样本；见事实 2.9。

[9] 文献中也使用过类似的构造，例如参见 [BKS14]。

给定两个独立样本 $X, X' \sim \mu$，我们经常会关注变量 $\{Z_{v,s}\}_{v\in V,\ s\in\Sigma}$，它们用于定义引言中讨论的移位划分。形式化地，我们将它们定义为

$$Z_{u,s} = \sum_{a\in\Sigma} X_{u,a} X'_{u,a+s}.$$

本节余下部分将介绍一些关于独立样本中的多项式以及它们上的伪分布 $\mathrm{E}_{X,\ X'}$ 的事实。其中一些事实具有普遍性，另一些则专门针对移位划分变量 $Z_{u,\ s}$。

~第一个事实表明，上文定义的 $\mathrm{E}_{X,\ X'}$ 是一个合法的伪分布，并且继承了 E 所满足的所有~约束。

~ ~事实 2.9. 若 E_X 是变量 X 上的一个有效伪分布，且其度为 D，那么 $\mathrm{E}_{X,\ X'}$ 是一个有效的伪分布，其度为 D。此外，若有其他对 E_X 成立的平方和不等式，它们对 $\mathrm{E}_{X,\ X'}$ 也成立。

现在，我们证明一些专门针对 Z 变量的性质。以下事实表明，移位划分变量 $Z_{v,\ s}$ 确实表现得像一个划分：如果 X 满足程序 1中的约束，那么变量 $Z_{v,\ s}$ 确实定义了一个划分。

事实 2.10。将移位变量 $Z_{u,\ s} = \sum_{a\in\Sigma} X_{u,\ a} X'_{u,\ a+s}$ 定义为 $X_u - X'_u = s$ 的指示函数，其中 X、X' 为唯一游戏整数规划的平方和松弛（1）的 8 度解；对于每条边 (u, v)，将变量 $Y_{(u,v)} = \sum_a X_{u,\ a} X_{v,\ \pi_{uv}(a)}$ 定义为边 (u, v) 上的约束得到满足的指示函数。则 Z 变量满足：

1. 布尔性：$Z^2_{v,\ s} = Z_{v,\ a}$。
2. 划分约束：对于 $s \neq s'$，$Z_{v,\ s} Z_{v,\ s'} = 0$；以及 $\sum_s Z_{u,\ s} = 1$。
3. 交叉边会违背赋值：对于每条边 (u, v)，$Z_{u,\ s} Z_{v,\ s'} Y_{(u,v)} Y'_{(u,\ v)} = 0 \in E$ 且 $s \neq s'$。

证明。前两项可通过直接计算并利用变量 $X_{u,\ a}$ 的性质轻松验证。我们证明最后一项性质成立。由于我们的唯一游戏实例是仿射的，对于每个 i、$j \in E$、π_{ij}，都有 $(a) = a + h_{ij}$，其中某个 $h_{ij} \in \Sigma$。因此，

$$\begin{aligned} Z_{i,s} Z_{j,t} Y_{(i,j)} Y'_{(i,j)} &= \sum_{a,b,c,d\in\Sigma} X_{i,a} X'_{i,a+s} \cdot X_{j,b} X'_{j,b+t} \cdot X_{i,c} X_{j,c+h_{ij}} \cdot X'_{i,d} X'_{j,d+h_{ij}} \\ &= 0, \end{aligned}$$

我们根据互不相交约束（即当 $a \neq b$ 时，$X_{i,\ a} X_{i,\ b} = 0$）得出最后一个等式：要使上面的项非零，必须满足 $a = c$、$d = a + s$、$b = d - t + h_{ij} = a + s - t + h_{ij}$，并且还要满足 $b = c + h_{ij}$，这意味着 $a + s - t = c$。但由于 $t \neq s$，这就产生了矛盾。由此证明了最后一个性质。 □

2.4.3 平移对称性

接下来，我们定义移位对称函数和伪分布的概念，并确立它们满足的一些性质。

定义 2.11（平移对称性）。如果对于任意单项式$D\prod X_{u_i,\ a_i}$和 $s \in \Sigma$，均有$_{i=1}$成立，则称伪分布 μ 是移位对称的。

$$\widetilde{\mathbb{E}}_{\mu}\left[\prod_{i=1}^{D} X_{u_i,a_i}\right] = \widetilde{\mathbb{E}}_{\mu}\left[\prod_{i=1}^{D} X_{u_i,a_i+s}\right].$$

如果对所有 $s \in \Sigma$，多项式 $p(X_{u_1,\sigma_1},\ldots)$（等价地，也可视为函数 $f\colon\ \Sigma^n \to \mathrm{R}$）满足 $f(X) = f(X+s)$，则称其具有移位对称性。

给定一个由仿射唯一博弈的平方和松弛得到的伪分布，我们可以通过如下方式定义一个新的伪分布 μ^{sym}，将其变换为具有相同取值的移位对称伪分布：

$$\widetilde{E}_{\mu^{\mathrm{sym}}}\left[\prod_{i=1}^{D} X_{u_i,a_i}\right] = \frac{1}{|\Sigma|}\sum_{s\in\Sigma}\widetilde{\mathbb{E}}_{\mu}\left[\prod_{i=1}^{D} X_{u_i,a_i+s}\right].$$

~容易验证，$\mathrm{E}_{\mu^{\mathrm{sym}}}$ 是一个有效的伪期望，且其取值相同；事实上，这是因为如果 $(a,b) \in \Sigma$ 满足仿射唯一博弈实例中的一个约束，那么对于任意 $s \in \Sigma$，$(a+s,b+s)$ ~ ~也满足该约束。更一般地，可以验证，对于所有移位对称多项式 p，$\mathrm{E}_{\mu^{\mathrm{sym}}}[p(X)] = \mathrm{E}_{\mu}[p(X)]$。因此，以下我们将假设，我们的伪期望和伪分布可以在不损失取值的情况下变为移位对称，并且一般而言，仍能保持移位对称多项式的伪期望。

2.5 信息论

我们用 $\mu|_R$ 表示随机变量 $R \sim \mu$ 的边缘分布。我们用 $TV(A,B)$ 表示两个分布 A,B 之间的全变差距离。

定义 2.12（互信息）。给定定义在 (X,Y) 上的分布 μ，X,Y 之间的互信息定义为：

$$I_{\mu}(X;Y) = D_{KL}(\mu \,||\, \mu|_X \times \mu|_Y),$$

其中 D_{KL} 是 Kullback-Leibler散度。关于随机变量 Z，(X,Y) 之间的条件互信息定义为：

$$I(X;Y|Z) = \mathop{\mathbb{E}}_{z\sim Z}[I_{\mu|Z=z}(X;Y)].$$

引理 2.13（Pinsker 不等式）。给定任意两个分布 D_1, D_2：

$$TV(D_1,D_2) \le \sqrt{\frac{1}{2}D_{KL}(D_1||D_2)}.$$

利用这一点，我们得到，对于定义在 (Y,Y') 上的分布 μ：

$$TV(\mu,\mu_Y\times\mu_{Y'}) \le O(\sqrt{I(Y;Y')}).$$

引理 2.14（数据处理不等式）。设 X、Y、A、B为随机变量，使得 $H(A|X) = 0$且$H(B|Y) = 0$，即 A 完全由 X 确定，且 B 完全由 Y 确定。则：

$$I(A;B) \le I(X;Y).$$

3 定理1.5 的证明

本节在 1.6 满足 $c = 1 - \varepsilon$ 且 $\varepsilon > 0$ 较小的情况下证明定理 1.6，以便如引言中所述，将“对事件进行条件化”这一难题单独提取出来。在下一节中，我们将说明为完整证明定理 1.6所需的修改。

我们先正式定义约翰逊图。

定义 3.1（约翰逊图）。对于任意 $\alpha \in (0, 1)$ 和 $n, \ell \in \mathbb{N}$，其中 $\alpha\ell \in \mathbb{N}$ 且 $n > \ell$，我们定义 (n, ℓ, α)-约翰逊图 $J(n, \ell, \alpha\ell)$ 为这样一个图：其顶点集为 $\binom{[n]}{\ell}$，并且当且仅当 $|U \cap V| = (1 - \alpha)\ell$ 时，顶点对 $U, V \in \binom{[n]}{\ell}$ 之间存在边。上下文明确时，我们省略 $(n, \ell, \alpha\ell)$，并用 $[N]$ 表示 J 的顶点集。

我们常将 α 称为该图的噪声参数。

记号：$(n, \ell, \alpha\ell)$-约翰逊图包含其他作为子图的约翰逊图，它们对应于引言中的基本集合。事实上，对于任意大小小于 ℓ 的 $S \subset [n]$，我们可以考虑由所有满足 $A \supseteq S$ 的顶点 A 所诱导的子图。我们常将这类子图称为 $|S|$-限制，并记作 $J|_S$。之所以这样命名，是因为对于给定的函数 $F\colon V(J) \to \mathbb{R}$ 和 S，我们可以定义限制函数 $F|_S\colon V(J|_S) \to \mathbb{R}$，其中 $F|_S[A] = F[A \cup S]$。我们用记号 $\delta(F|_S)$ 表示 $\mathbb{E}_{u \in J|_S}[F(u)]$。

3.1 Johnson 图上的仿射唯一游戏算法

本节将介绍我们针对 $J(n, \ell, \alpha)$ 上的仿射唯一游戏算法。全文中，当我们说 $q = \exp(r)$ 时，意指存在通用正常数 c_1, c_2，使得 $2^{c_1 r} \le q \le 2^{c_2 r}$。此外，如果我们将参数 q 设为 $\exp(r)$，则意指我们令 $q = 2^{cr}$，其中 c 是某个通用常数。我们还有一个误差参数 $\nu > 0$，将在最后确定，但应将其视为较小且远离 0 的值。

算法的高层次描述

1. 首先，我们的算法求解程序（ D ）的度 1 平方和松弛，以找到一个伪~期望 $\mathbb{E}\mu$，它对应于一个值至少为 $1 - \varepsilon$ 的伪分布。

2. 接下来，利用上文所述的变换，我们构造一个新的对象，它对应于两个独立样本，如第 2.4.2 节所示。

3. 在新的伪分布中，对于样本 X和 X'，期望目标函数均至少为 $1 - \varepsilon$，因此从直观上说， X 和 X' 同时满足的边的比例为 $1 - 2\varepsilon$。我们论证，在这种情况下，存在一个子立方体 C，它对应于一个大小为常数的限制，并且在该子立方体上，移位划分势 [10] 很大。我们很快会正式定义这一概念；但目前先指出，它保证了按照引言中所述的简单舍入过程，能够满足该子立方体内常数比例的约束。

4. 我们使用一个称为 SubRound 的子过程，先找出一个具有较大移位划分势的子立方体 C，然后为该子立方体中的顶点找到一个 $\Omega(1)$ 值的赋值 C。

[10]这类子立方体的存在性可通过全局超收缩性来论证。为了确保这一结论适用于我们的伪分布，我们必须确保所用的全局超收缩性结果是在平方和系统内证明的。

5. 我们随机化与 C 中顶点相连的边，以得到一个新的实例 I'（其值可能较低），并再次迭代该算法。此步骤的目标是，在下一次迭代中，我们能够找到一个子立方体 C'，它与迄今为止已赋值的顶点仅有非常小的重叠。以我们对 C 所采用的相同方式满足 C' 中很大一部分约束，就能确保满足新的边并取得进展。如此迭代下去，我们便能满足图中 $\Omega(1)$ 比例的部分。这种迭代方法也曾用于 [BBK+21]，但他们每一步只能满足一个 $\Omega(1/\ell^r)$ 比例的 r 子立方体中的约束。

3.1.1 移位划分势 [BBK+21]

我们的分析采用了 [BBK+21] 中对移位划分势的定义，但为了完整起见，我们在此加以说明。回顾一下，给定仿射唯一博弈实例 I 的两个赋值 X 和 X'，可以定义移位划分 F_s，它由满足 $X(v) - X'(v) = s$ 的顶点 v 构成。正如引言中所述，我们将大量使用移位划分，但出于技术原因，我们只希望处理那些与其相邻的许多约束都得到满足的顶点 u。对于赋值 X 和顶点$v \in V(G)$，令 $\mathrm{val}_v^G(X)$ 表示 v 的值，即与 v 相连且也由 X 满足的 G 的边所占比例。上下文明确时，我们省略上标 G。

自然地，这意味着我们只希望在满足以下条件时才将 v纳入 F_s：仅当 $X(v) - X'(v) = s$并且 $\mathrm{val}_v^G(X)$、$\mathrm{val}_v^G(X')$至少达到一定大小。不过，为了仍处于平方和的范畴内，我们按照定理 2.7，用逼近多项式替代这些指示函数约束。

定义 3.2 (移位划分 [BBK+21])。 给定两个仿射唯一游戏赋值 X 和 X'，对 G 定义以下函数 $\{F_s : V(G) \to \mathbb{R}\}_{s\in\Sigma}$

$$F_s^G(u) = \mathbb{I}(X_u - X'_u = s) \cdot p_{\beta,\nu}(\mathrm{val}_u^G(X)) p_{\beta,\nu}(\mathrm{val}_u^G(X')), \tag{2}$$

其中 $p_{\beta,\nu}(x)$ 是一个次数为$O(1/\nu)$ 的多项式，它是对 $\mathbb{I}[x \geq \beta]$ 的多项式近似，精度参数为 ν，如定理 2.7所述。当图的含义明确时，我们省略 G 在 F_s^G中的上标。

有了移位划分的定义后，我们现在可以定义移位划分势，它支配着我们在子立方体内最基本的舍入过程。

定义 3.3 (移位划分势 [BBK+21])。 给定图 G上的两个 UG 赋值 X和 X'，移位划分大小定义为：

$$\Phi_{\beta,\nu}^G(X, X') = \sum_{s\in\Sigma} \mathop{\mathbb{E}}_{u\in G} [F_s^G(u)]^2.$$

伪分布 $\mathcal{D}$ 在 (X, X') 上的移位划分势定义为：

$$\Phi_{\beta,\nu}^G(\mathcal{D}) = \mathop{\widetilde{\mathbb{E}}}_{(X,X')\sim\mathcal{D}} [\Phi_{\beta,\nu}^G(X, X')].$$

直观地说，$\mathrm{E}_{u\in G}[F_s^G(u)]$ 衡量了移位划分中 F_s 的分数大小，因此移位划分势衡量的是移位划分的碰撞概率。特别地，当且仅当存在 s，使得划分中的部分 F_s 具有常数密度时，它可以达到 $\Omega(1)$。

在整个 John- son 图以及其中的子立方体上，我们的论证始终会考察移位划分势。考察子立方体 $J|_a$ 上的移位划分势时，我们将其简写为 $\Phi_{\beta,\nu}^a(\mathcal{D})$。

3.1.2 主程序

现在我们给出一种形式 我们算法的完整描述（暂不包括稍后介绍的 SubRound 过程） .

算法 3.4（Johnson 图上的唯一游戏）。该算法的输入是在 Johnson 图 $J(n,\ell,\alpha)$ 上的仿射唯一游戏实例 I，满足 val(I) $\geq 1-\varepsilon$。该算法的输出是对 $V(J)$ 的赋值。

1. 令 $r=\left\lfloor\frac{64\sqrt{\eta}}{\alpha}\right\rfloor$，$\delta:=\varepsilon_{\exp(r)}$，$\gamma=\varepsilon$ 且 $D=\frac{|\Sigma|^3\ell^{O(r)}}{\varepsilon^3}$。固定 $\mathcal{A}_I$ 为实例 I 上的唯一博弈公理/整数规划集合 (程序 (1))。

2. 设定 $j=1, I_0=I, R_0=\phi$。

3. 当 $|R_{j-1}|<\frac{\gamma}{2}|V(J)|$ 时，执行以下操作：

   (a) 求解整数规划 $\mathcal{A}_{I_{j-1}}$ 的度数为 D 的平方和半定规划松弛，并应用第 2.4.2 节中的变换，得到对应于两个独立样本的伪期望。令 $\mu_j\times\mu_j$ 为对应的伪分布。(b) 找到 $r'\leq r$ 和一个 r' 受限子立方体 C_j，使其具有较高的 SubRound 值 [11]，，即满足 SubRound-val$_{\mu_j}(C_j)$ $\geq\delta$。(c) 在 C_j 上运行 SubRound （算法 3.8 ），使用伪分布 μ_j，得到对 V （ C_j ）的赋值 f_j。(d) 令 S_j 为 C_j 的一个子图，其由尚未被任何部分赋值 f_k、$k<j$ 赋值的顶点诱导而成，并使用 f_j 为这些顶点赋值。设置 $R_j=R_{j-1}\cup H_j$。(e) 在与 V（R_j）相邻的边上随机选取仿射约束，并令新实例为 I_j。(f) 递增 j。

4. 输出满足上述所有针对 S_j 的部分赋值 f_j 的、关于 $V(J)$ 的任意赋值。

3.1.3 SubRound 子程序与条件化与舍入

在描述 SubRound 子程序之前，我们先介绍若干分析所需的记号。对于顶点 $u\in V(G)$，我们将引入新的辅助布尔变量 p_u 和 p'_u。从直观上说，p_u 是指示函数，表示与 u 相邻的许多约束是否由赋值 X 满足；但严格来说，我们用多项式对其进行近似。

首先请注意，给定一个有效的度为 D 的伪分布 $\mathcal{D}$，我们可以从中提取任意 D 个变量上的有效且一致的局部分布。例如，考察 $\mathcal{D}$ 中 (X_u,X_v) 的边缘分布，我们便得到 $\Sigma\times\Sigma$ 上的一个分布。类似地，对于 $\mathcal{D}$ 中的任意指示变量 R（其中，在 $\mathcal{D}$ 的公理下，$R_u=R_u^2$），也可以用类似的方法，从 X,X',R,R' 中定义 D 个变量上的局部分布。遗憾的是，指示 u 的值较大的指示函数不是多项式。不过，利用 $\mathcal{D}$，我们可以提取以下关于 X,X',p,p' 的局部分布集合，其中 p 是我们引入的一组新变量，在 μ 中并不存在。我们将此集合记为 $\mathcal{L}(\mathcal{D},p_{\beta,\ \nu})$。

~形式化地，给定一个关于 $\mathcal{A}_I$ 上（X,X'）赋值的、度为 $D>O(1/\nu)$ 的伪分布 $\mathcal{D}$，使得相应的伪期望具有高值，我们按以下方式定义变量 p,p',X,X' 上的局部分布 $\mathcal{L}(\mathcal{D},p_{\beta,\ \nu})$：

[11]这是子程序 SubRound 返回的赋值的值（3.8）。

定义 **3.5** $\mathcal{L}$ $\mathcal{D}$ p_{β} ν $\mathcal{D}$ $D \geq$.（局部分布集合（，，））。设 是关于 $\mathcal{A}_I$ 上（X, X'）赋值的、度为 $\Omega(d/\nu)$ 的伪分布，且多项式 $p_{\beta,\nu}$ 是定理 2.7 中针对 $\varepsilon = \delta = \nu$ 和 $\alpha = \beta$ 的多项式。我们定义来自 p, p', X, X' 的 d 个变量集合上的联合分布如下：

$$\widetilde{\Pr_{\mathcal{L}}}[p_u = 1] := \widetilde{\mathbb{E}}_{\mathcal{D}}[p_{\beta,\nu}(\mathrm{val}_u(X))], \quad \widetilde{\Pr_{\mathcal{L}}}[p_u = 0] = 1 - \widetilde{\mathbb{E}}_{\mathcal{D}}[p_{\beta,\nu}(\mathrm{val}_u(X))], \quad \widetilde{\Pr_{\mathcal{L}}}[X_u = \sigma] = \widetilde{\mathbb{E}}[X_{u,\sigma}],$$

对于 X'_u、p'_u，也可类似地定义。更一般地，我们可以将上述定义扩展为定义变量 X、X'、p、p' 中事件合取的概率。对于所有满足 $|S| + |T| + |A| + |B| \leq d$、$b_1$、……、$b_{|S|}$、$b'_1$、……、$b'_{|T|} \in \{0,1\}$ 且 σ_1、……、$\sigma_{|A|}$、σ'_1、……、$\sigma'_{|B|} \in \Sigma$ 的子集 S、T、A、$B \subseteq [N]$，定义：

$$\widetilde{\Pr_{\mathcal{L}}}\left[\bigcap_{u\in S} p_u = b_u, \bigcap_{v\in T} p'_v = b'_v, \bigcap_{a\in A} X_a = \sigma_a, \bigcap_{b\in B} X'_b = \sigma'_b\right]$$

$$= \widetilde{\mathbb{E}}_{\mathcal{D}}\left[\prod_{u\in S}(1 - b_u + (-1)^{1-b_u} p_{\beta,\nu}(\mathrm{val}_u(X))) \prod_{v\in T}(1 - b_v + (-1)^{1-b_v} p_{\beta,\nu}(\mathrm{val}_v(X'))) \prod_{a\in A} X_{a,\sigma_a} \prod_{b\in B} X'_{b,\sigma_b}\right].$$

注 3.6。注意，由于 $\mathcal{D}$ 的度足够大，且 $\mathcal{A}_I \vdash_{\widetilde{O}(1/\nu)} p_{\beta,\ \nu}(\mathrm{val}_u(X)) \in [0,1]$，容易验证上述局部分布集合构成了有效的概率分布：每次涉及 d 个变量，并且彼此一致。

利用变量 p, p'，我们进一步定义辅助随机变量 $Y_{u,\ v}$ 和 $Y'_{u,\ v}$，用于 $u \neq v \in [N]$，它们在描述和分析我们的算法时尤为有用：

$$Y_{u,v} = (X_u, X_v, p_u, p_v), \quad Y'_{u,v} = (X'_u, X'_v, p'_u, p'_v). \tag{3}$$

此外，类似于记号 $Y_{u,\ v}$，对于所有 $S = \{i_1, \ldots, i_{|S|}\} \subseteq [N]$，定义随机变量$Y_S, Y'_S$ 如下：

$$Y_S = (X_{i_1}, \ldots, X_{i_{|S|}}, p_{i_1}, \ldots, p_{i_{|S|}}), \quad Y'_S = (X'_{i_1}, \ldots, X'_{i_{|S|}}, p'_{i_1}, \ldots, p'_{i_{|S|}}).$$

根据定义 3.5，我们知道事件 $Y_S = y_S$ 自然对应于一个平方和多项式 Q_S，使得 $\widetilde{\ }$满足 $\Pr_{\mathcal{L}(\mu\times\mu,p_{\beta,\nu})}[Y_S = y_S] = \mathrm{E}_{\mu}[Q_S]$；对于关于 Y'_S的事件，情况也类似。因此，我们将使用“在 $Y_S = y_S$上条件化 μ”这一记号，表示对相应的多项式 Q_S上的 μ 进行重新加权。我们将经常考察诸如 $\Pr_{\mathcal{L}}[\mathrm{I}[Y_S = y_S] \wedge \mathrm{I}[Y_T = y_T]]$ 和 $I(Y_S; Y_T)$ 这样的量，其中 $|S \cup T| \leq d$。在这些地方，我们强调，考虑的是 $Y_{S\cup T}$ 上的局部分布，并在该分布上计算概率或互信息。

子程序 Condition&Round。为了形式化地陈述 SubRound，我们首先需要介绍 [BBK+21] 中的子程序 Condition&Round，它与引言中的基本舍入过程类似。

算法 3.7(Condition&Round [BBK+21])。
输入：一个针对 UG 实例 $I' = (G = (V, E)\ \Pi)$、定义在字母表 Σ 上的度为-D （针对 $D \geq 2$）的移位对称伪分布 μ。
输出：返回一个赋值 $x \in \Sigma^V$。

采样一个随机解 Z：
1. 对顶点 $u \sim \pi$ 进行抽样，并以 $X_u = 0$ 为条件化依据，得到新的边缘分布 $\mathrm{E}_{\mu}[\cdot \mid X_u = 0]$。2. 通过根据每个折叠变量的标签独立抽样，得到一个解 Z；抽样依据是其边缘分布 $\widetilde{\ }$：$Z_v \sim \mathrm{E}_{\mu}[X_v \mid X_u = 0]$。

去随机化条件化与舍入。为便于后续分析，我们将分析条件化与舍入的去随机化版本，该版本使用条件期望法等标准方法，将上述过程确定化。我们省略显而易见的细节；对我们而言，只需知道这一去随机化过程所达到的值始终不低于条件化与舍入所产生结果的期望值。

现在我们可以描述用于求得 Johnson 图部分赋值的 SubRound。

SubRound 的高层描述。在这个例程中，给定一个伪期望和一个子立方体$J|_a$（我们希望其上的值较大），我们希望为给定子立方体中的节点找到一个良好的赋值，或者退出。当子立方体上的移位划分势函数较大时，这种方法能够成功为 $V(J|_a)$ 赋值。

为此，我们找出对随机变量 $Y_{u、v}$ 的适当条件化，使得在进行条件化后，它们几乎两两独立（我们用互信息来表示这一点；这一步就是我们在引言中所说的消除全局相关性）。将得到的新分布记为 $\mu_1 \times \mu_2$。

与此同时，我们还找出一个事件（为保持在平方和的范畴内，我们将其表述为一个多项式）$P_a(X,\ X')$，它大致表示部分 $\{v:\ \ X(v) - X'(v) = s\}$ 在 $J|_a$中是稠密的，并且该事件具有显著的概率；在以该事件为条件后，$J|_a$ 内部的移位划分较大。这两项事实都是相对于 $\mu_1 \times \mu_2$来衡量的。我们在引理 $P_a(X,\ X')$ 中给出 3.9 的正式定义。

最后，我们使用 μ_1 或 μ_2的对称化版本运行条件化与舍入过程；如果前面的步骤成功，该过程就会为给定的子立方体返回一个良好的赋值。

现在我们转向 SubRound 的形式化描述。

算法 3.8（SubRound：子图舍入）。
输入：一个仿射唯一博弈实例 $I = (G, \Pi, \Sigma)$，其定义在 $(n, \ell, \alpha\ell)$-Johnson 图 G和字母表 Σ上；一个伪分布 μ，满足 val$_\mu(I) \geq 1 - \eta$；一个 j-受限子立方体 $J|_a$，其中 $j \leq r = \left\lfloor \frac{32\sqrt{\eta}}{\alpha} \right\rfloor$.
输出：返回 $\Sigma^{|V(J|_a)|}$ 中 $J|_a$各顶点的一个赋值。

1. Fix $t = \frac{|\Sigma|^3 \ell^{\Theta(r)}}{\eta^3}, \tau = \Theta(\frac{\eta}{|\Sigma|^2 \ell^{2r} \exp(r)}), \beta = \sqrt{\eta}, \nu = \eta \exp(-r)$.

2. 从引理 3.9给出的多项式集合中，选取一个多项式 $P_a(X, X')$、若干子集 $A, B \subseteq V(J|_a)$（大小至多为 t）以及字符串 y_A, y_B，使得对事件 $Y_A = y_A$ 和$Y_B = y_B$ 进行条件化后，得到伪分布 μ_1, μ_2，满足：

   (a) $J|_a$ 中的移位划分势显著：

$$\widetilde{\mathbb{E}}_{\mu_1 \times \mu_2}[\Phi^a_{\beta,\nu}(X, X') P_a(X, X')] \geq \exp(-r)\, \widetilde{\mathbb{E}}[P_a(X, X')].$$

   (b) P_a 的概率显著：

$$\widetilde{\mathbb{E}}_{\mu_1 \times \mu_2}[P_a(X, X')] \geq \Omega\left(\frac{\sqrt{\eta}}{|\Sigma| \ell^j \exp(r)}\right).$$

(c) 随机变量 $Y_{u,\ v}$ 在 $J|_a$ 内具有较小的全局相关性：

$$\mathop{\mathbb{E}}_{\substack{u_1,v_1\sim S:u_1\neq v_1\\ u_2,v_2\sim S:u_2\neq v_2}}[I(Y_{u_1,v_1};Y_{u_2,v_2})]\leq\tau.$$

(d) 随机变量 $Y'_{u,v}$ 在 $J|_a$ 内具有较小的全局相关性：

$$\mathop{\mathbb{E}}_{\substack{u_1,v_1\sim S:u_1\neq v_1\\ u_2,v_2\sim S:u_2\neq v_2}}[I(Y'_{u_1,v_1};Y'_{u_2,v_2})]\leq\tau.$$

这里 $S=V(J|_a)$，互信息是相对于局部分布集合 $\mathcal{L}(\mu_1\times\mu_2,p_{\beta,\nu})$ 取的。如果不存在这样的多项式或条件化，则在 $V(J|_a)$ 上输出全零赋值并退出。

3. 对 μ_1,μ_2 使用第 2.4.3 节中的过程进行对称化，得到 $\mu_1^{\text{sym}},\mu_2^{\text{sym}}$。对 μ_1^{sym} 或 μ_2^{sym} 执行去随机化条件化与舍入，并输出针对 $V(J|_a)$得到的较高值赋值。

3.2 算法分析3.4

3.2.1 分析的高层次描述

我们证明，算法 3.4 返回的解的值与字母表大小无关。我们先解释针对小集扩张图的分析思路 [BBK+21]，然后说明如何将此分析调整到我们的情形。

小集扩张图 **[BBK+21]**：考虑移位划分势，为了简化表述，假设将 p替换为实际的指示函数。那么函数 F_s 覆盖了图中几乎所有顶点，而移位划分中跨越不同部分的任意边，都必须被X 或 X'违反。因此，如果 X，X' 是$(1-\varepsilon)$-满足赋值，那么移位划分就是非扩张的，也就是说，至多有 2ε比例的边跨越不同部分（这些边被 X 或 X'违反）。

对于 $(2\varepsilon,\delta)$-小集合扩展图，[BBK+21] 于是得出，其中一部分的分数大小必须至少为 $\Omega(\delta)$，事实上，移位划分大小：$\sum_s \mathrm{E}_{u\sim G}[F_s(u)]^2$, 必须为 $\geq\Omega(\delta)$。另一方面，他们证明，如果移位划分势在 $\mu\times\mu$ 上很大，那么对 μ进行条件化与舍入，就能成功舍入为 $\Omega_{\varepsilon,\delta}(1)$-赋值。他们还正式证明了：

1. 给定图 G 的度为 D 的证书，证明其具有 $(O(\varepsilon)\ \delta)$-小集合扩张；并给定一个度为 $\Omega(D)$ 的伪分布 μ，其在任意仿射唯一博弈实例 $I=(G,\Pi)$ 上的值为 $1-\varepsilon$，可得 $\Phi^G_{\beta,\ \nu}(\mu\times\mu)\ \geq\delta$。

2. 证明如果 $\Phi^G_{\beta,\ \nu}(\mu\times\mu)$ 很大，那么条件化与舍入会输出一个值很大的赋值。

我们对约翰逊图的分析：下面来看看如何将这一分析适用于约翰逊图。步骤 (1) 远非成立，因为约翰逊图并非小集扩张图。但我们知道，在这些图中，限制到某个子立方体后，所有非扩张集合都必须具有较大的规模，尽管该集合在整个图中可能并不大。我们利用这一性质得出，移位划分势在某个子立方体上必须很大。事实证明，这部分分析比可认证的小集合扩张的情形复杂得多，也是我们技术工作的主要部分。

有了这一点后，我们对步骤 (2) 进行适当修改，便可得出：将条件化与舍入应用于该子立方体时，会输出一个该子立方体上的 $\Omega(1)$-赋值。随后，我们使用一个迭代引理多次运行该算法，从而输出整个图上的 $\Omega(1)$-满足赋值。

3.2.2 稍后证明的引理

本节陈述几个用于分析算法 3.4 的引理，其证明推迟到后续章节给出。在第 3.2.3 节中，我们使用这些引理来分析算法 3.4 的性能。

算法 3.4的分析通过证明以下结论来进行：给定一个高值的 I 伪分布，就存在一个子立方体，其 SubRound 值很高，也就是说，步骤 3(a) 成功。为此，我们首先证明，Johnson 图结构定理（定理 3.17）蕴含：给定一个值较大的伪分布μ，就存在一个移位划分势较大的子立方体 $J|_a$，记为 $\Phi^a_{\beta,\nu}$。不过，由于 Johnson 图并非小集扩张图，我们有以下更微妙的结论：存在一个 $r = O(\sqrt{\varepsilon}/\alpha)$-受限子立方体 a以及一个概率较大的事件 P_a，使得在以 P_a为条件对 $\mu \times \mu$ 进行条件化后，诱导出的移位划分势在子立方体 $J|_a$上很大。事件 P_a大致对应于以下指示函数：子立方体 $J|_a$内某个移位划分分量的大小很大，即 $\mathrm{I}(\delta(F_s|_a) > \exp(-r))$，且其概率为 $\geq \ell^{-O(r)}$。

引理 3.9。存在一个常数 $\varepsilon_0 \in (0,1)$，使得对于所有正常数 $\varepsilon \leq \varepsilon_0$, $\alpha, \tau \leq 1$,$\nu \leq \varepsilon \exp(-r)$，以及所有满足 $r = \lfloor \frac{32\sqrt{\varepsilon}}{\alpha} \rfloor$ 的整数 $\ell \geq \Omega(r)$ $n \geq \ell$，以下结论成立。

设 I是定义在 $J(n, \ell, \alpha\ell)$ 上的仿射唯一游戏实例，μ是 I上的赋值伪分布，其 $\mathrm{val}_\mu(I) \geq 1-\varepsilon$，且度至少为 $D = \widetilde{\Omega}\left(\frac{|\Sigma|^{\ell^r} \exp(r)}{\nu\tau\sqrt{\varepsilon}}\right)$。那么存在一个大小为 $\sim j \leq r$ 的限制 $a \subseteq [n]$、一个来自固定的 $|\Sigma|$ 个多项式集合的度为 $O(1/\nu)$ 的多项式 $P_a(X, X')$、大小至多为 $\widetilde{O}(|\Sigma|^{\ell^j} \exp(r)\, \tau\sqrt{\varepsilon})$ 的子集 $A, B \subseteq V(J|_a)$，以及字符串 y_A, y_B，使得将 μ条件化于事件 $Y_A = y_A$ 和$\sim Y_B = y_B$ 后，得到度为 $\Omega(1/\nu)$ 的伪分布 μ_1 和 μ_2，并满足：

1. $\mathcal{A}_I \vdash_{\widetilde{O}(1/\nu)} P_a(X, X') \in [0,1]$.
2. $\widetilde{\mathbb{E}}_{\mu_1 \times \mu_2}[\Phi^a_{\sqrt{\varepsilon},\nu}(X, X') P_a(X, X')] \geq \exp(-r)\, \widetilde{\mathbb{E}}[P_a(X, X')]$.
3. $\widetilde{\mathbb{E}}_{\mu_1 \times \mu_2}[P_a(X, X')] \geq \Omega\left(\frac{\sqrt{\varepsilon}}{|\Sigma|^{\ell^j} \exp(r)}\right)$.
4. $\mathbb{E}_{\substack{u_1, v_1 \sim S : u_1 \neq v_1 \\ u_2, v_2 \sim S : u_2 \neq v_2}}[I(Y_{u_1,v_1}; Y_{u_2,v_2})] \leq \tau$.
5. $\mathbb{E}_{\substack{u_1, v_1 \sim S : u_1 \neq v_1 \\ u_2, v_2 \sim S : u_2 \neq v_2}}[I(Y'_{u_1,v_1}; Y'_{u_2,v_2})] \leq \tau$,

其中 $S = V(J|_a)$，$Y_{u,\,v} = (X_u, X_v, p_u, p_v)$，$Y'_{u,\,v} = (X'_u, X'_v, p'_u, p'_v)$，且互信息是相对于局部分布集合 $\mathcal{L}(\mu_1 \times \mu_2, p_{\sqrt{\varepsilon},\,\nu})$ 计算的。

下一个引理阐明了这样一种直觉：给定一组随机变量 $Z_{u,\,v}$，它们大致两两独立（它们是赋值 X 和 X' 的函数），以及一个概率显著的事件 $E(X, X')$，那么通常 $Z_{u,\,v} \mid E$ 与 $Z_{u,\,v}$ 的统计距离很小。通俗地说，这表明对事件 E 进行条件化，不会局部改变 (X, X') 的分布。

引理 3.10。对于所有 $\tau, p, \beta, \nu, \delta \in (0,1)$ 以及整数 $D, N, m \leq N$，以下结论成立：设 $\mu_1 \times \mu_2$ 是关于 (X, X') 的一个 $\widetilde{}$ 度为 $D + \Omega(1/\nu)$ 的伪分布，满足 $\mathcal{A}_I(X, X')$，且 $E(X, X')$ 是一个多项式 $\widetilde{}$，使得 $\mathcal{A}_I \vdash_D E(X, X') \in [0,1]$，并且 $\mathrm{E}_{\mu_1 \times \mu_2}[E(X, X')] \geq p$。假设对于 $S \subseteq [N]$，我们有：

1. $\mathbb{E}_{\substack{u_1, v_1 \sim S : u_1 \neq v_1 \\ u_2, v_2 \sim S : u_2 \neq v_2}}[I(Y_{u_1,v_1}; Y_{u_2,v_2})] \leq \tau$.

2. $\mathbb{E}_{\substack{u_1,v_1\sim S:u_1\neq v_1\\ u_2,v_2\sim S:u_2\neq v_2}}[I(Y'_{u_1,v_1};Y'_{u_2,v_2})]\le\tau$,

其中 $Y_{u,\ v}=(X_u,\ X_v,\ p_u,\ p_v)$ $Y'_{u,\ v}=(X'_u,\ X'_v,\ p'_u,\ p'_v)$ 并且，互信息是相对于局部分布集合 $\mathcal{L}(\mu_1\times\mu_2,\ p_{\beta,\ \nu})$ (定义 3.5)。那么我们有：

$$\Pr_{u,v\sim S:u\neq v}[TV((Y_{u,v},Y'_{u,v})|E,(Y_{u,v},Y'_{u,v}))\ge\delta]\le O\left(\frac{\sqrt{\tau}+1/|S|}{p\delta^2}\right),$$

其中，分布 $(Y_{u,\ v},Y'_{u,\ v})|E$ 指由局部分布 $\mathcal{L}(\mu_1\times\mu_2|E,p_{\beta,\ \nu})$ 所定义的这些变量上的联合分布；类似地，$(Y_{u,\ v},Y'_{u,\ v})$ 指由 $\mathcal{L}(\mu_1\times\mu_2,p_{\beta,\ \nu})$ 定义的分布。

现在，我们将注意力限制在由引理 $J|_a$ 3.9 得到的良好子立方体 上；此后，我们只关注边缘化到 $\mu_1\times\mu_2|P_a$的相关伪分布（例如 $J|_a$）。为简化记号，我们仍使用原有记号指代边缘化后的伪分布。

我们证明，较大的移位势 $\Phi^a(\mu_1\times\mu_2|P_a)\ge\delta$，若还满足以下性质：从 $\mu_1\times\mu_2|P_a$ 中抽取的平均 $(Y_{u,\ v},Y'_{u,\ v})$-对，与从 $\mu_1\times\mu_2$ 中抽取时的分布接近，则条件化与舍入（应用于 $J|_a$）会在 μ_1 或 μ_2 上成功。

引理 3.11. 设 $I=(G,\Pi)$ 是字母表为 Σ 的唯一游戏仿射实例，且 $\mu_1\times\mu_2$ 是关于赋值 (X,X') 到 I 的 $\tilde{}$ 度 $D+O(1/\nu)$ 伪分布。设 $E(X,X')$ 是一个多项式，使得 $\mathcal{A}_I(X,X')\vdash_D E(X,X')\in[0,1]$。假设我们有：

$$\Pr_{u,v\sim V(G):u\neq v}[TV((Y_{u,v},Y'_{u,v})|E,(Y_{u,v},Y'_{u,v}))>\delta]\le\zeta,$$

其中，分布 $(Y_{u,v},Y'_{u,v})|E$ 指的是由局部分布 $\mathcal{L}(\mu_1\times\mu_2|E,p_{\beta,\nu})$ 的集合所定义的关于这些变量的联合分布；类似地，$(Y_{u,v},Y'_{u,v})$ 指的是由 $\mathcal{L}(\mu_1\times\mu_2,p_{\beta,\nu})$ 定义的分布（定义 3.5）。

如果 $\Phi^G_{\beta,\ \nu}(\mu_1\times\mu_2|E(X,X'))\ge\gamma$，那么在伪分布 μ_1^{sym} 或 μ_2^{sym} 算法 3.7 中的至少一个上运行时间为 $\mathrm{poly}(|V(G)|)$，并返回一个期望值至少为

$$(\beta-\nu)^2\left(\gamma-O(\delta+\zeta)-\frac{1}{|V(G)|}\right)-3\nu(\beta-\nu)$$

对于 I。

利用上述引理处理 $G=J|_a$，可以分析 SubRound 的单次迭代，并证明它能够为 I 中的一个子立方体赋值，且在其中满足一定比例的边。这个子立方体的大小可能只有整个图的 $o(1)$，因此，为了完成对算法的分析，我们需要下面这个引理。该引理断言，我们可以迭代此过程（如算法 3.4 所示），从而满足 I 中一定比例的约束。

引理 3.12. 设 $c,\gamma,\delta\in(0,1]$ 和 $r\in\mathbb{N}$。设 I 是一个字母表为 Σ、定义在 $J_{n,\ell,\alpha}$ 上的仿射唯一博弈实例，其中ℓ,n 足够大，且其值至少为 c。假设有一个子程序 $\mathcal{A}$，对于任意输入的、定义在 $J_{n,\ell,\alpha}$ 上且满足 $\mathrm{val}_\mu(I')\ge c-\gamma$ 的仿射唯一博弈实例 I'，都会返回一个定义在 J 上的 $\le r$-受限子立方体 H 以及一个部分赋值 f，使得 $\mathrm{val}_f(H)\ge\delta$。那么，若 $\mathcal{A}$ 的运行时间为 $T(\mathcal{A})$，则存在一个运行时间为 $O(|V(J)|T(\mathcal{A})+|V(J)|^3)$ 的算法，能够为 I 找到一个解，使其满足 J 中 $\Omega(\delta\gamma(1-\alpha)^r)$ 比例的边。

证明。 推迟至第 A节。 □

3.2.3 算法的分析 3.4

定理 3.13. 存在常数 $\varepsilon_0 \in (0,1)$，使得对于所有正常数 $\varepsilon \le \varepsilon_0, \alpha \in \mathbb{Q}$（满足$\alpha \le 1/2$），所有整数 $\ell \ge \Omega(r)$（满足 $\alpha\ell \in \mathbb{N}$ 和 $r = \Theta(\sqrt{\varepsilon}/\alpha)$），且 n 足够大时，算法 3.4 具有如下保证：若 I 是定义在 (n,ℓ,α)-Johnson 图 G 上的仿射唯一博弈实例，其字母表为 Σ，且 $\mathrm{val}(I) = 1-\varepsilon$，则算法 3.4 在时间 $|V(J)|^{\mathrm{poly}(\ell^r,|\Sigma|,1/\varepsilon)}$ 内返回一个对 I 的 $\mathrm{poly}(\varepsilon)\exp(r)$-满足赋值。

证明。设 $r = \lfloor 32\varepsilon/\alpha \rfloor$。给定 $\le r$-受限子立方体 $a \subseteq [n], P_a(X,X')$，由引理 3.9 可知 $\mu_1 \times \mu_2$，有 $\Phi^a_{\sqrt{\varepsilon},\nu}(\mu_1 \times \mu_2 | P_a) \ge \exp(-r)$，因此我们应用引理 3.10，其中 $S = J|_a$，多项式 $E(X,X') = P_a(X,X')$，参数为 $\beta = \sqrt{\varepsilon}, \nu = \exp(-r)\varepsilon, \delta = \exp(-r)$ $p = \Omega\left(|\Sigma|\ell^r{}^{\sqrt{\varepsilon}}\exp(r)\right)$ 以及 $\tau = \Theta(|\Sigma|^2\ell^{2r}{}^{\varepsilon}\exp(r))$。参数 τ 的选取满足 $O(\frac{\sqrt{\tau}+1/|S|}{p\delta^2}) = \exp(-r)$，因此我们可以应用舍入引理（引理 3.11），取 $\zeta = \exp(-r)$ 和 $\gamma = \exp(-r)$，并使用相同的 β,ν,δ 设置。这表明存在一个子立方体 $a \in \binom{[n]}{j}$，其 SubRound 值至少为 $\Omega(\varepsilon/\exp(r))$，若 $\deg(\mu) \ge \tilde{\Omega}\left(|\Sigma|\ell^r \exp(\nu\tau\sqrt{\varepsilon}^{\,r})\right)$。因此，只需使 μ 的度等于 $\frac{|\Sigma|^3\ell^{O(r)}}{\varepsilon^3}$ 。

通过将 SubRound 用作子程序，我们应用迭代引理 3.12，取 $c = 1-\varepsilon, \gamma = \varepsilon, \delta = \Omega(\varepsilon/\exp(r))$ 和 $r = \lfloor 64\sqrt{\varepsilon}/\alpha \rfloor$，使得 $(1-\alpha)^r = O(\sqrt{\varepsilon})$（命题 3.21），从而完成该定理的证明。我们可以验证 SubRound 满足该引理的假设：它能找到一个 $\le r$-受限子立方体及其上的一个赋值，使其值为 $\Omega(\delta)$，耗时 $|V(J)|^{\frac{|\Sigma|^3\ell^{O}}{\varepsilon^3}(r)}$（这可由 μ 的度上界推出）。因此，算法 3.4 能在时间 $|V(G)|^{\frac{|\Sigma|^3\ell^{O(r)}}{\varepsilon^3}}$ 内输出一个值至少为 $\Omega(\varepsilon^3/\exp(r))$ 的赋值。

□

3.3 引理 3.9 的证明：寻找具有较大移位划分的子立方体

本节中，我们使用 Johnson 图结构定理，证明存在一个大小为常数的限制 $a \subseteq [n]$（对应于导出子图 $J|_a$），使其在以非负多项式 P_a 为条件时具有较大的导出移位划分势，即 $\Phi^a_{\beta,\nu}(\mu \times \mu | P_a)$ 较大。不过，回顾一下，为了分析最终的条件化与舍入步骤，我们需要证明以 P_a 为条件对 $\mu \times \mu$ 进行条件化，不会在 X、X' 之间引入过多相关性。因此，我们首先对 $\mu \times \mu$ 执行全局相关性约简过程，得到乘积伪分布 $\mu_1 \times \mu_2$，同时保持 $\Phi^a_{\beta,\nu}(\mu_1 \times \mu_2 | P_a)$ 较大的性质。用于辅助舍入分析的精确量为：

$$I(Y_{u_1,v_1}; Y_{u_2,v_2}) = I(X_{u_1}, X_{v_1}, p_{u_1}, p_{v_1}; X_{u_2}, X_{v_2}, p_{u_2}, p_{v_2}),$$

根据定义 3.5中的局部分布集合所定义。我们使用 Raghavendra-Tan 的全局相关性约简过程 [RT12]。

3.3.1 将 ShiftPartition 限制到子图

为证明引理 3.9，我们需要引入限制在子立方体上的全局移位划分势 $J|_a$这一概念。它与 $J|_a$ 上的移位划分势几乎相同，只有一个关键区别：

定义 3.14 (限制在子图 [BBK+21]上的全局移位势)。 对于任意 ν， $\beta \in (0,1)$ 及 H 的子图 G，定义限制在子图 上的全局移位划分大小 H 为以下量：

$$\Phi_{\beta,\nu}(X,X')|_H = \sum_{s\in\Sigma} \mathop{\mathbb{E}}_{u\in H}[F_s^G(u)]^2,$$

其中 F_s 是定义移位划分（定义 3.3）的函数。相对于赋值对 $\mathcal{D}$ 上的伪分布 $\mathcal{D}$，全局移位划分势定义为：

$$\Phi_{\beta,\nu}(\mathcal{D})|_H = \mathop{\widetilde{\mathbb{E}}}_{(X,X')\sim\mathcal{D}}[\Phi_{\beta,\nu}(X,X')|_H].$$

注意全局势与 H 上移位划分势之间的区别：全局移位划分势 $\Phi_{\beta,\nu}(X,X')|_H$ 衡量的是 H 内全局划分的大小；也就是说，$\mathrm{val}_u^G(X)$ 是图中所有与 u 相 incident 的边的函数，而不仅仅是子图 H 中的边。另一方面，势 $\Phi_{\beta,\nu}^H(X,X')$ 只衡量顶点 u 在子图 H 内的值。

3.3.2 全局超收缩性

我们需要以下定义来描述 Johnson 图的结构定理：

定义 3.15（函数限制）。对于 (n,ℓ,α)-Johnson 图 J，给定函数 $F\colon V(J)\to\mathbb{R}$ 以及满足 $a=r$ 的集合 $a\subseteq[n]$，使得 $0\le r\le \ell-1$，我们将限制函数 $F|_a:\binom{[n]\setminus a}{\ell-r}\to\mathbb{R}$ 定义为：

$$F|_a(X) = F(a\cup X).$$

此外，令 $\delta(F|_a)$ 表示函数在子立方体 $J|_a$ 上的限制的分数大小，也就是 s,

$$\delta(F|_a) := \mathop{\mathbb{E}}_{X\sim\binom{[n]\setminus a}{\ell-r}}[F|_a(X)].$$

当 $a=\phi$ 且 $r=0$ 时，对于所有 $X\in\binom{[n]}{\ell}$，都有 $F|_a(X)=F(X)$，且 $\delta(F|_a)=\delta(F)=\mathbb{E}[F]$。

在 [KMMS18] 中证明了伪随机集合会扩张。形式化地，我们如下定义伪随机集合，以及更一般的伪随机函数：

定义 3.16（伪随机函数）。若集合 S 对所有 $\le r$-限制 a 都满足 $\delta(S|_a)\le\gamma$，则称其为 (r,γ)-伪随机的。类似地，若函数 F 在 $[0,1]$ 上有界，且对所有 $\le r$-限制 a 都满足 $\delta(F^2|_a)\le\gamma$，则称其为 (r,γ)-伪随机的。

我们需要将这一结果推广到一般的布尔函数和伪随机函数 F，此外还要证明它可由常数度的平方和证明系统证明。我们得到一个平方和证明，表明若对于所有大小为 $\le r$ 的 a，$\delta(F^2|_a)\le\gamma$，且 F 是布尔函数，则 $\langle F, LF\rangle$ 很大，其中 $q_a(F)$ 是公理 $\{\gamma-\delta(F^2|_a)\}_a$ 的平方和乘子，而 $(\Pi_{\ge\lambda_r}F)(X)$ 是公理$\{F(X)^3=F(X)\}$ 的乘子。我们有如下陈述：

定理 3.17（约翰逊图扩张定理）。对于所有 $\alpha\in(0,1)$、所有整数 $\ell\ge 1/\alpha$ 和 $n\ge\ell$，以下结论成立：设 $J(n,\ell,\alpha\ell)$ 为 α-噪声 Johnson 图。对于每个常数 $\gamma\in(0,1)$ 以及正整数 $r\le O(\ell)$，每个函数 $F\colon V(J)\to\mathbb{R}$ 若为 (r,γ)-伪随机函数，则具有高扩张：

$$\{F(X)\in[0,1]\}_{X\in V(J)}\vdash_{O(1)}$$

$$\langle F, LF\rangle \geq \delta(F)(1-(1-\alpha)^{r+1})(1-\gamma^{1/3}\exp(r)) - \sum_{j=0}^{r} \frac{c_j \ell^j}{\gamma} \mathop{\mathbb{E}}_{a\sim\binom{[n]}{j}} [q_a(F)(\delta(F^2|_a)-\gamma)] + B(F) \tag{4}$$

$$\{F(X)\in[0,1]\} \vdash_2 \quad 0 \leq q_a(F) \leq 1 \tag{5}$$

其中，对于所有 $j \leq r$， c_j's 都是大小至多为 $\exp(r)$ 的正常数；对于所有大小为 j 的子集， $a \subseteq [n]$ 和 $q_a(F)$ 是二次多项式，并且 $B(F) = \frac{4}{3}\mathrm{E}_X[(F^3-F)\Pi_{\geq\lambda_r}F]$ 对于 $\lambda_r = (1-\alpha)^r$，其中 $\Pi_{\geq\lambda}$ 表示将 J 投影到由特征值 $\geq\lambda$ 组成的最高特征子空间的投影算子。

证明。详见第 C 节。 □

也可以将 [KMMS18] 中的扩张结果理解为：若 F 是一个布尔函数，且它是集合 $\mathcal{F} \subseteq \binom{[n]}{\ell}$ 的指示函数，而该集合的边扩张与 1 相距一定距离，那么对于某个常数为 r 的 r 受限子立方体 a，有 $\delta(F|_a) \geq \Omega(1)$。事实上，如果 F 在 J_n 上的扩张至多为 $1-\varepsilon$，那么对于 $r = O(\varepsilon/\alpha)$，有 $\delta(F|_a) \geq \exp(-r)$。类似地，我们可以利用上述平方和陈述得出结论：即使 F 是"近似布尔"且非扩张的，对于某个 $O(1)$-限制 a，也有 $q_a(F)(\delta(F^2|_a) - \gamma) > 0$。在关于非扩张集合 F 上伪分布 μ 的语境中，可以得出结论：对 $q_a(F)$ 进行条件化后，得到新的伪分布 μ'，其中 $\delta(F^2|_a)$ 平均而言满足 $> \gamma$，因此 $q_a(F)$ 大致对应于"F 在 $J|_a$ 上稠密"这一"事件"。

我们利用这样一个观察：相对于 $(1-\varepsilon)$-满足赋值X 和 X' 定义的移位划分，其扩张至多为 2ε，因此是非扩张的。因此，与上文一样，利用结构定理，我们得出移位划分中至少有一个集合对于 $r = O(\varepsilon/\alpha)$ 和 $\gamma = \exp(-r)$ 而言不是 (r,γ)-伪随机的，也就是说，对于某个 $s \in \Sigma$ 以及 $\leq r$-限制 a， $\delta(F_s|_a) \geq \gamma$。令 $\mathrm{viol}(X)$ 表示赋值 X 在实例 I 中违反的边的比例。我们用以下引理在平方和中表述这一事实：

引理 3.18。 在引理3.9的条件下，对于所有 $\eta > 0$ 和 $r \leq \ell$，我们有：

$$\mathcal{A}_I \vdash_{\tilde{O}(1/\nu)} \tag{6}$$

$$\sum_{j=0}^{r} c_j \exp(r)\ell^j \mathop{\mathbb{E}}_{a\in\binom{[n]}{j}} [\sum_s q_a(F_s)(\delta(F_s|_a) - \exp(-r))]$$

$$\geq \frac{1-\lambda_{r+1}}{2} - (\mathrm{viol}(X)+\mathrm{viol}(X'))\left(1+\frac{3(1-\lambda_{r+1})+12+8\eta}{6(1-\beta-\nu)}\right) - \frac{2}{3\eta} - \nu\left(5-\lambda_{r+1}+\frac{8\eta}{3}\right), \tag{7}$$

其中 $\lambda_{r+1} = (1-\alpha)^{r+1}$、 q_a 是定理 3.17中的多项式， $\mathcal{A}_I$ 是程序（1）为 I 定义的公理集合。

证明。 对于可认证小集扩张图，这一证明与 [BBK+21] 中引理 4.4 的证明完全相同：我们将定理 3.17 应用于每个函数 F_s，并对 s 求和。这样便得到以下不等式：

$$\sum_s \langle F_s, LF_s\rangle \geq (1-\lambda_{r+1})(1-\gamma^{1/3}\exp(r))\sum_s \delta(F_s) - \sum_{j=0}^{r}\frac{c_j\ell^j}{\gamma}\mathop{\mathbb{E}}_{a\in[n]^j}[\sum_s q_a(F_s)(\delta(F_s^2|_a)-\gamma)]$$

$$+ \frac{4}{3}\sum_s \mathbb{E}[(F_s^3 - F_s)\Pi_{\geq\lambda_r}F_s] \tag{8}$$

现在，我们令 $\gamma = \exp(-r)$，使得 $(1-\gamma^{1/3}\exp(r)) = 1/2$。此外，我们对每一项 $\sum_s \langle F_s$、$LF_s\rangle$、$\sum_s \delta(F_s)$ 以及布尔性误差进行界定：$\frac{4}{3}\sum_s \mathrm{E}[(F_s^3 - F_s)\Pi_{\geq\lambda_r} F_s]$。

首先注意，取值较低的顶点所占比例很小，特别是至多为 $\mathrm{viol}(x)+\mathrm{viol}(x')^{1-\beta}$。~~由于这些函数覆盖了所有取值较高的顶点，我们得到 $\sum \delta(F_s) \gtrsim 1 - \mathrm{viol}(x)+\mathrm{viol}(x')^{1-\beta}$。接下来，$\sum_s \langle F_s, LF_s\rangle$ 统计穿过移位划分的边的比例。每条这样的边要么被 X 或 X' 违反，要么与一个取值较低的顶点相 incident，因此我们得到：$\sum_s \langle F_s, LF_s\rangle \lesssim \mathrm{viol}(X)+\mathrm{viol}(X')+\frac{2\mathrm{viol}(X)+2\mathrm{viol}(X')}{}^{1-\beta}$~~。这里我们写的是近似不等式，因为 F_s 并非精确的指示函数，因此会产生一些误差项。定理 3.17 中的布尔性项 $B(F)$ 也很小（求和后），因为 F_s 是近似指示函数（注意，对于 $0/1$ 函数，它为 0，因为 $F^3 = F$）[12]。这些论述已在 [BBK+21] 第 4.2 节的断言中形式化，具体来说是其中的断言 4.2、4.7 和 4.9。利用近似指示多项式 $p_{\beta,\nu}$ h 的性质，这些论述很容易证明，因此这里略去。

利用上述结论界定每个求和项，将这些界代入（8）并重新整理，即可得到所需不等式。

□

3.3.3 降低全局相关性

证明引理3.9 所需的最后一个要素是：给定一个度足够高的伪期望，可以构造出不同的伪期望（它们是对初始伪期望进行条件化所得），且这些伪期望没有全局相关性。更确切地说：

~引理 3.19。对于所有满足 $D' \geq \max(D, \Omega(1/\nu))$ 的 $\tau, p, \beta, \nu \in (0,1)$ 以及 $|\Sigma|, D, D' \in \mathbb{Z}$，以下结论成立。

假设存在一个度为 $D' + \widetilde{\Omega}(\log_{\frac{|\Sigma|}{p\nu\tau}})$ 的唯一游戏赋值上的伪分布 μ，满足 $\mathcal{A}_I$，~，并且存在一个多项式 $E(X, X')$，满足 $\mathrm{E}_{(X,X')\sim\mu\times\mu}[E(X, X')] \geq p$ 和 $\mathcal{A}_I \vdash_D E(X, X') \leq 1$。那么，对于所有子集 $S \subseteq [N]$，都存在大小至多为 $O(\frac{\log|\Sigma|}{p\tau})$ 的子集 $A, B \subseteq S$ 以及字符串 y_A, y_B，使得将 μ 条件化于事件 $Y_A = y_A$ 和 $Y_B = y_B$ 后，得到的伪分布 μ_1 和 μ_2 的度至少为 D'，并且：

1. $\widetilde{\mathbb{E}}_{X,X'\sim\mu_1\times\mu_2}[E(X, X')] \geq \frac{p}{2}$.
2. $\mathbb{E}_{\substack{u_1,v_1\sim S:u_1\neq v_1\\ u_2,v_2\sim S:u_2\neq v_2}}[I(Y_{u_1,v_1}; Y_{u_2,v_2})] \leq \tau$.
3. $\mathbb{E}_{\substack{u_1,v_1\sim S:u_1\neq v_1\\ u_2,v_2\sim S:u_2\neq v_2}}[I(Y'_{u_1,v_1}; Y'_{u_2,v_2})] \leq \tau$,

其中，对于 $A \subseteq [N]$，$Y_A = (X_{i_1}, \ldots, X_{i_{|A|}}, p_{i_1}, \ldots, p_{i_{|A|}})$（$Y'$ 亦同），互信息是相对于局部分布集合 $\mathcal{L}(\mu_1 \times \mu_2, p_{\beta,\nu})$ 而定义的。

证明。留待第3.4节。 □

[12]注意，如果函数 F_s 是使用 $\mathrm{I}[\mathrm{val}_u(X) \geq \beta]$ 定义的，那么我们就能得到不含涉及 η 的项、且带有 $\nu = 0$ 的引理陈述

3.3.4 引理3.9证明

我们结合引　　按照上一节所述，并设置参数以完成引理3。　　9.

引理 3.20（引理 3.9 的重述）。存在一个常数 $\varepsilon_0 \in (0,1)$，使得对所有正常数 $\varepsilon \le \varepsilon_0, \alpha, \tau \le 1, \nu \le \varepsilon \exp(-r)$、所有整数 $\ell \ge \Omega(r)$ $n \ge \ell$，其中 $r = \lfloor \frac{32\sqrt{\varepsilon}}{\alpha} \rfloor$，以下结论成立：设 I 是定义在 $J_{n,\ell,\alpha}$ 上的一个仿射唯一游戏实例，μ 是关于 I 的赋值上的伪分布，满足 $\mathrm{val}_\mu(I) \ge 1-\varepsilon$，且度至少为 $\widetilde{\Omega}\left(\frac{|\Sigma|^{\ell^r}}{\exp(\frac{r}{\nu\tau\sqrt{\varepsilon}})}\right)$。则存在一个大小为 $j \le r$ 的限制 $a \subseteq [n]$、一个关于固定集合 $|\Sigma|$ 中多项式的 O 度 $1/\nu$ 多项式 $P_a(X, X')$、大小至多为 $\widetilde{O}(|\Sigma|^{\ell^j} \exp(r)\, \tau\sqrt{\varepsilon})$ 的子集 $A, B \subseteq V(J|_a)$，以及字符串 y_A, y_B，使得将 μ 条件化于事件 $Y_A = y_A$ 和 $Y_B = y_B$ 后，得到度为 $\Omega(1/\nu)$ 的伪分布 μ_1 和 μ_2，并且：

1. $\mathcal{A}_I \vdash_{\widetilde{O}(1/\nu)} P_a(X, X') \in [0,1]$.
2. $\widetilde{\mathbb{E}}_{\mu_1\times\mu_2}[\Phi^a_{\sqrt{\varepsilon},\nu}(X,X')P_a(X,X')] \ge \exp(-r)\,\widetilde{\mathbb{E}}[P_a(X,X')]$.
3. $\widetilde{\mathbb{E}}_{\mu_1\times\mu_2}[P_a(X,X')] \ge \Omega\left(\frac{\sqrt{\varepsilon}}{|\Sigma|^{\ell^j}\exp(r)}\right)$.
4. $\mathbb{E}_{\substack{u_1,v_1\sim S:u_1\neq v_1\\ u_2,v_2\sim S:u_2\neq v_2}}[I(Y_{u_1,v_1};Y_{u_2,v_2})] \le \tau$.
5. $\mathbb{E}_{\substack{u_1,v_1\sim S:u_1\neq v_1\\ u_2,v_2\sim S:u_2\neq v_2}}[I(Y'_{u_1,v_1};Y'_{u_2,v_2})] \le \tau$,

其中 $S = V(J|_a)$、$Y_{u,v} = (X_u, X_v, p_u, p_v)$、$Y'_{u,v} = (X'_u, X'_v, p'_u, p'_v)$，且互信息是相对于局部分布集合 $\mathcal{L}(\mu_1 \times \mu_2, p_{\sqrt{\varepsilon},\nu})$ 定义的。

证明。我们将使用以下参数应用引理 3.18：$r = \lfloor 32\sqrt{\varepsilon}/\alpha \rfloor$，因此 $1-\lambda_{r+1} \ge 16\sqrt{\varepsilon}$、$\eta = 1/\sqrt{\varepsilon}$ 和 $\beta = 201\sqrt{\varepsilon}$。由于 ε 足够小，且 $\nu \le \varepsilon/2$，我们得到 $1/(1-\beta-\nu) < 2$。根据假设 $\mathrm{E}_\mu[\mathrm{viol}(X)] = \mathrm{E}_\mu[\mathrm{viol}(X')] \le \varepsilon$，$\mathrm{E}_\mu$ 的度为 $O(1/\nu)$，且 E_μ 满足 $\mathcal{A}_I$，因此对伪分布 $\mu\times\mu$ 取方程 7 的伪期望，可得：

$$\sum_{j=0}^{r} c_j \exp(r)\ell^j \mathop{\mathbb{E}}_{a\in\binom{[n]}{j}} \widetilde{\mathbb{E}}_{\mu\times\mu}[\sum_s q_a(F_s)(\delta(F_s|_a) - \exp(-r))] \ge \frac{\sqrt{\varepsilon}}{3}. \tag{9}$$

由于 c_j 小于 $\exp(r)$，由平均论证可得一个大小为 $j \le r$ 的限制 $a \subseteq [n]$ 和一个 $s \in \Sigma$，使得：

$$\widetilde{\mathbb{E}}_{\mu\times\mu}[q_a(F_s)(\delta(F_s|_a) - \exp(-r))] \ge \Omega\left(\frac{\sqrt{\varepsilon}}{|\Sigma|^{\ell^j}\exp(r)}\right). \tag{10}$$

令 $P_a(X, X')$ 表示上文中的多项式 $q_a(F_s(X, X'))$，以下简记为 P_a。首先注意到 $\widetilde{}$，由于 q_a 是一个度为 $O(1)$ 的平方和多项式，我们立即得到 P_a 是一个度为 $O(1/\nu)$ 的平方和多项式，使得：

$$\mathcal{A}_I \vdash_{\widetilde{O}(1/\nu)} F_s(u) \in [0,1] \vdash_{O(1)} q_a(F_s(X,X')) = P_a(X,X') \in [0,1],$$

从而证明了定理中的第一个结论。现在我们利用引理3.19来约化全局相关性。具体而言，我们取 μ，其中 S 是对应于子立方体的变量集合 a、多项式$E(X,X') = P_a(\delta(F_s|_a) - \exp(-r))$（我们已知 $\mathcal{A} \vdash_{\widetilde{O}(1/\nu)} E(X,X') \le 1$），$\beta = \sqrt{\varepsilon}$

以及引理陈述中的 τ, ν。因此，我们得到一个关于子立方体 a 上 UG 赋值的伪分布 $\mu_1 \times \mu_2$，满足：

$$\widetilde{\mathbb{E}}_{\mu_1\times\mu_2}[P_a(\delta(F_s|_a) - \exp(-r))] \geq \Omega\left(\frac{\sqrt{\varepsilon}}{|\Sigma|\ell^j \exp(r)}\right), \tag{11}$$

以及关于 μ_1、μ_2 的互信息条件。这就证明了引理陈述中的第 (4)、(5) 点。

证明引理的第 (2) 点。现在我们来推导如下事实：全局移位划分势$\Phi(\mu_1 \times \mu_2)|_a$ 在给定 P_a的条件下很大。重新整理（11），得到：

$$\widetilde{\mathbb{E}}_{\mu_1\times\mu_2}[P_a\delta(F_s|_a)] \geq \exp(-r)\,\widetilde{\mathbb{E}}_{\mu_1\times\mu_2}[P_a] + \Omega\left(\frac{\sqrt{\varepsilon}}{|\Sigma|\ell^j \exp(r)}\right) \geq \exp(-r)\,\widetilde{\mathbb{E}}_{\mu_1\times\mu_2}[P_a]. \tag{12}$$

~ ~由于 P_a 是一个平方和多项式，我们可以用 P_a 对 $\mathbb{E}_{\mu_1\times\mu_2}[\cdot]$ 重新加权，得到 $\mathbb{E}'$，再应用柯西-施瓦茨不等式，得到：

$$\exp(-r) \leq \widetilde{\mathbb{E}}'[\delta(F_s|_a)] \leq \sqrt{\widetilde{\mathbb{E}}'[\delta(F_s|_a)^2]} = \sqrt{\frac{\widetilde{\mathbb{E}}_{\mu_1\times\mu_2}[\delta(F_s|_a)^2 P_a]}{\widetilde{\mathbb{E}}_{\mu_1\times\mu_2}[P_a]}},$$

重新整理后，我们得到：$\widetilde{\mathbb{E}}_{\mu_1\times\mu_2}[\delta(F_s|_a)^2 P_a] \geq \exp(-r)\,\widetilde{\mathbb{E}}_{\mu_1\times\mu_2}[P_a]$。根据定义，限制在 a 上的全局势等于 $\sum_{s\in\Sigma}\delta(F_s|_a)^2$。因此，将 $\widetilde{\mathbb{E}}_{\mu_1\times\mu_2}[\delta(F_{s'}|_a)^2 P_a]$（对$s' \in \Sigma$而言 $s' \neq s$，这些项都非负）加到（12）的左侧，得到：

$$\widetilde{\mathbb{E}}_{\mu_1\times\mu_2}[\Phi_{\beta,\nu}(X, X')|_a P_a] \geq \exp(-r)\,\widetilde{\mathbb{E}}_{\mu_1\times\mu_2}[P_a]. \tag{13}$$

现在，我们将讨论全局势与 a上的移位划分势之间的关系。这两个量的唯一区别在于，前者中一个顶点的值是整个图中满足条件的边的比例，而后者中其值仅根据子立方体 a 内的边计算（按术语 p_β, ν(val(u))）。

首先注意，当 r-受限子立方体的 r 不太大时，其扩张有界：$\phi(J|_a) \leq O(\sqrt{\varepsilon})$ (断言 3.21)。利用这一点，我们得到：

$$\Phi^a_{\beta-200\sqrt{\varepsilon},\nu}(X, X') \geq \Phi_{\beta,\nu}(X, X')|_a - 4\nu,$$

我们将在断言 3.22中给出其形式化证明。

综上，我们得到：

$$\widetilde{\mathbb{E}}_{\mu_1\times\mu_2}[\Phi^a_{\sqrt{\varepsilon},\nu}(X, X')P_a] \geq \widetilde{\mathbb{E}}_{\mu_1\times\mu_2}[(\Phi_{201\sqrt{\varepsilon},\nu}(X, X')|_a - 4\nu)P_a] \geq \exp(-r)\,\widetilde{\mathbb{E}}_{\mu_1\times\mu_2}[P_a],$$

因为 $\nu \leq \exp(-r)/8$，这就证明了引理的第 (2) 点。

（3）由（11）得出。事实上，由于 $\delta(F_s|_a) \leq 1$ 且 $P_a(X, X') \geq 0$（这两个事实均可在度 $O(1/\nu)$ 下证明 ~），我们得到：$\mathcal{A}_I \vdash_{\widetilde{O}(1/\nu)} P_a(X, X')(\delta(F_s|_a) - \exp(-r))] \leq (1 - \exp(-r))P_a(X, X')$。~取 $\mathbb{E}_{\mu_1\times\mu_2}$ 并将其代入方程（11），我们得到：

$$\widetilde{\mathbb{E}}_{\mu_1\times\mu_2}[P_a] \geq \Omega\left(\frac{\sqrt{\varepsilon}}{|\Sigma|\ell^j \exp(r)}\right) \qquad \square$$

3.3.5 辅助引理

我们以给出断言 3.21 和 3.22 的证明来结束本节。这些证明也在 [BBK+21] 中用到，但为了完备性，我们在此给出证明。

命题 3.21 (命题 6.10 [BBK+21])。若 $r = \left\lfloor \frac{32\sqrt{\varepsilon}}{\alpha} \right\rfloor < \frac{\ell}{4}$ 且 $s < r$，则 s-受限子立方体 $J(n,\ \ell,\ \alpha\ell)$ 的扩张至多为 $200\sqrt{\varepsilon}$。

证明。设 $J|_Y$ 是一个 s-受限子立方体。我们有：

$$1 - \phi(J|_Y) = \frac{\binom{\ell-|Y|}{\alpha\ell}}{\binom{\ell}{\alpha\ell}} \geq \frac{\binom{\ell-r}{\alpha\ell}}{\binom{\ell}{\alpha\ell}} = \left(\frac{\ell-\alpha\ell}{\ell}\right)\left(\frac{\ell-\alpha\ell-1}{\ell-1}\right)\cdots\left(\frac{\ell-\alpha\ell-r+1}{\ell-r+1}\right).$$

现在，由假设可知 $r \leq \ell/4$，每个括号中的项都至少为 $\left(\frac{3\ell/4-\alpha\ell}{3\ell/4}\right) = (1-4\alpha/3)$，因此

$$1 - \phi(J|_Y) \geq \left(1 - \frac{4\alpha}{3}\right)^r \geq 1 - \frac{4r\alpha}{3}.$$

由于 $r = \left\lfloor \frac{32\sqrt{\varepsilon}}{\alpha} \right\rfloor < \frac{75\sqrt{\varepsilon}}{\alpha}$，我们得到 $\phi(J|_Y) < 200\sqrt{\varepsilon}$，如所需。 □

命题 3.22 (命题 6.11 [BBK+21])。设 C 是 $J_{n,\ \ell,\ \alpha}$ 的一个 r-受限子立方体，且满足 $r = \left\lfloor \frac{32\sqrt{\varepsilon}}{\alpha} \right\rfloor$。那么，若 Φ^C 是限制在 C 上的移位划分势，则对任意 $\beta \geq 201\sqrt{\varepsilon}$ 和 $\nu < \varepsilon$，

$$\Phi^C_{\beta-200\sqrt{\varepsilon},\nu}(X, X') \geq \Phi_{\beta,\nu}(X, X')|_C - 4\nu,$$

此外，这可以通过度为 $O(1/\nu)$ 的平方和证明。

证明。当 $r = \left\lfloor \frac{32\sqrt{\varepsilon}}{\alpha} \right\rfloor$ 时，C 的扩张至多为 $1 - (1-4\alpha/3)^r \leq 200\sqrt{\varepsilon}$，由断言 3.21可知。此外，根据 Johnson 图的定义，这对每个顶点都成立；每个 $v \in C$ 至多有其邻居的 $200\sqrt{\varepsilon}$比例指向外部。因此，

$$\mathbb{I}[\mathrm{val}^C_u(X) \geq \beta - 200\sqrt{\varepsilon}] \geq \mathbb{I}[\mathrm{val}_u(X) \geq \beta],$$

此外，由于 $\nu < \varepsilon$，

$$p_{\beta-200\sqrt{\varepsilon},\nu}(\mathrm{val}^C_u(X)) + \nu \geq p_{\beta,\nu}(\mathrm{val}_u(X)) - \nu.$$

$p(\mathrm{val}_u(X'))$ 也同样成立。令 $Z_{u,\ s} = \mathrm{I}[X_u - X'_u = s]$。因此，根据定义 ，

$$\begin{aligned}
\Phi_{\beta-200\sqrt{\varepsilon},\nu}(X|_C, X'|_C) &= \sum_{s\in\Sigma} \mathop{\mathbb{E}}_{u\in C}\left[Z_{u,s} \cdot p_{\beta-200\sqrt{\varepsilon},\nu}(\mathrm{val}^C_u(X)) \cdot p_{\beta-200\sqrt{\varepsilon},\nu}(\mathrm{val}^C_u(X'))\right]^2 \\
&\geq \sum_{s\in\Sigma} \mathop{\mathbb{E}}_{u\in C}\left[Z_{u,s} \cdot (p_{\beta,\nu}(\mathrm{val}_u(X)) - 2\nu) \cdot (p_{\beta,\nu}(\mathrm{val}_u(X')) - 2\nu)\right]^2 \\
&\geq \Phi_{\beta,\nu}(X, X')|_C - 4\nu,
\end{aligned}$$

其中每个不等式都是一个平方和不等式，其度至多为 2 deg(p)。 □

3.4 引理 3.19 的证明：简化全局相关性

我们将使用以下引理，出自 [RT12]。

引理 3.23。存在 $t \le r$，使得：

$$\mathop{\mathbb{E}}_{i_1,\dots,i_t\sim[M]} \mathop{\mathbb{E}}_{i,j\sim[M]} [I(Y_i; Y_j \mid Y_{i_1},\dots,Y_{i_t})] \le \frac{\log q}{r-1},$$

其中，q 是 Y_i 的定义域大小。

注意，只要存在一个关于变量 $(Y_1,\dots,Y_M)$ 的局部分布集合，其中的分布都是定义在所有 $t+2$ 变量集合上的有效概率分布，且彼此一致，上述引理就成立。我们将应用上述引理，简化 $(Y_{u_1,v_1}; Y_{u_2,v_2})$ 之间的全局相关性（Y' 的情况类似），其中局部分布集合为 $\mathcal{L}$（定义 3.5）。

~~引理 3.24（重述引理 3.19）。对于所有 $\tau, p, \beta, \nu \in (0,1)$ 和 $|\Sigma|, D, D' \in \mathbb{Z}$，$D' \ge \max(D, \Omega(1/\nu))$，以下结论成立：假设存在一个度为 $D' + \widetilde{\Omega}(\log \frac{|\Sigma|}{p\nu\tau})$ 的唯一游戏赋值伪分布 μ，满足 $\mathcal{A}_I$；并且存在一个多项式 $E(X,X')$，满足 $\mathrm{E}_{(X,X')\sim\mu\times\mu}[E(X,X')] \ge p$ 且 $\mathcal{A}_I \vdash_D E(X,X') \le 1$。那么对于所有子集 $S \subseteq [N]$，都存在大小至多为 $O(\frac{\log|\Sigma|}{p\tau})$ 的子集 $A, B \subseteq S$ 以及字符串 y_A, y_B，使得将 μ 条件化于事件 $Y_A = y_A$ 和 $Y_B = y_B$ 后，得到度至少为 D' 的伪分布 μ_1 和 μ_2，并且：~~

1. $\widetilde{\mathbb{E}}_{X,X'\sim\mu_1\times\mu_2}[E(X,X')] \ge \frac{p}{2}$.
2. $\mathbb{E}_{\substack{u_1,v_1\sim S: u_1\neq v_1 \\ u_2,v_2\sim S: u_2\neq v_2}} [I(Y_{u_1,v_1}; Y_{u_2,v_2})] \le \tau$.
3. $\mathbb{E}_{\substack{u_1,v_1\sim S: u_1\neq v_1 \\ u_2,v_2\sim S: u_2\neq v_2}} [I(Y'_{u_1,v_1}; Y'_{u_2,v_2})] \le \tau$,

其中，对于 $A \subseteq [N]$, $Y_A = (X_{i_1},\dots,X_{i_{|A|}}, p_{i_1},\dots,p_{i_{|A|}})$（$Y'$ 同理），互信息是相对于局部分布集合 $\mathcal{L}(\mu_1\times\mu_2, p_\beta, \nu)$ 而言的。

证明。不失一般性，假设 $S \subseteq [N]$ 是 $[m]$。令 $\binom{[m]}{r}$ 表示 $[m]$ 中所有大小为 r 的子集，并令 m_r 表示 $\binom{m}{r}$。令 $Y = (Y_{a_1},\dots,Y_{a_{m_2}})$ 表示 $a_t = (u,v)$ 的 $\in \binom{[m]}{2}$。为简洁起见，我们用 $[m_2]$ 表示 $\binom{[m]}{2}$。给定定义在赋值 (X,X') 上的伪分布 $\mu\times\mu$，我们将考虑变量 X, X', p, p' 上的局部分布集合 $\mathcal{L}(\mu\times\mu, p_\beta, \nu)$，并且也用它表示由此诱导的关于 (Y,Y') 的分布集合（定义 3.5）。回顾随机变量 Y_A 的记号，对于任意 $A \subseteq [m]$:$Y_A = (X_{i_1},\dots,X_{i_{|A|}}, p_{i_1},\dots,p_{i_{|A|}})$。我们用 y_S 表示 Y_S 的实例化。

令 $\mathcal{L}$ 表示 $\mathcal{L}(\mu\times\mu, p_\beta, \nu)$。将引理 3.23 应用于 $\mathcal{L}$ 上的分布集合 Y，可得，对于所有 $\tau' > 0$，对 $t = O(\frac{\log|\Sigma|}{\tau'})$ 变量进行条件化可得：

$$\mathop{\mathbb{E}}_{i_1,\dots,i_t\sim[m_2]} [\mathop{\mathbb{E}}_{a,b\sim[m_2]} I(Y_a; Y_b \mid Y_{i_1},\dots,Y_{i_t})] \le \tau'. \tag{14}$$

令 $\mathcal{L}|_R$ 表示 $\mathcal{L}$ 在随机变量 R 上诱导的分布。我们知道，分布 $\mathcal{L}|_{(Y_{i_1},\dots,Y_{i_t})}$ 可以通过舍弃 i_1、……、i_t 中的重复索引，化简为分布 $\mathcal{L}|_{Y_{i_1}\cup\dots\cup i_t}$。这是因为，当顶点 u 出现在 $Y_{u,v}$ 或 $Y_{u,v'}$ 中时，$\mathcal{L}$ 为其赋予的值始终一致。我们将

在随机变量可从上下文中明确判断时，省略 $\mathcal{L}|_R$ 中的下标 R。因此，展开条件互信息的定义可得：

$$\begin{aligned} I(Y_a; Y_b \mid Y_{i_1}, \ldots, Y_{i_t}) &= \mathop{\mathbb{E}}_{(y_{i_1},\ldots,y_{i_t})\sim\mathcal{L}|_{(Y_{i_1},\ldots,Y_{i_t})}} [I(Y_a; Y_b \mid Y_{i_1} = y_{i_1}, \ldots, Y_{i_t} = y_{i_t})] \\ &= \mathop{\mathbb{E}}_{y_{i_1\cup\ldots\cup i_t}\sim\mathcal{L}|_{Y_{i_1\cup\ldots\cup i_t}}} [I(Y_a; Y_b \mid Y_{i_1\cup\ldots\cup i_t} = y_{i_1\cup\ldots\cup i_t}]. \end{aligned}$$

将上述内容代入式子（14），并应用马尔可夫不等式，我们得到，对所有 $\alpha \in (0,1$ ）：

$$\Pr_{\substack{i_1,\ldots,i_t\sim[m_2]\\ y_{i_1\cup\ldots\cup i_t}\sim\mathcal{L}}} \left[\mathop{\mathbb{E}}_{a,b\sim[m_2]} [I(Y_a; Y_b \mid Y_{i_1\cup\ldots\cup i_t} = y_{i_1\cup\ldots\cup i_t})] \geq \frac{\tau'}{\alpha} \right] \leq \alpha. \tag{15}$$

对 Y' 重复上述分析，我们得到：

$$\Pr_{\substack{j_1,\ldots,j_t\sim[m_2]\\ y'_{j_1\cup\ldots\cup j_t}\sim\mathcal{L}}} \left[\mathop{\mathbb{E}}_{a,b\sim[m_2]} [I(Y_a; Y_b \mid Y'_{j_1\cup\ldots\cup j_t} = y_{j_1\cup\ldots\cup j_t})] \geq \frac{\tau'}{\alpha} \right] \leq \alpha. \tag{16}$$

现在回顾一下（定义 3.5），在 $\mathcal{L}$下，事件 $(X_u, p_u) = (\sigma, b)$ 的概率，对于某些 $\sigma \in \Sigma$和 $b \in \{0,1\}$，对应于 μ 下某个适当多项式的伪期望，我们将其记作 $Q_{u,(\sigma,b)}$：

$$\begin{aligned} \widetilde{\Pr_{\mathcal{L}}}[(X_u, p_u) = (\sigma, b)] &= \widetilde{\mathbb{E}}[X_{u,\sigma}(1 - b + (-1)^{1-b} p(\mathrm{val}_u(X)))] \\ &:= \widetilde{\mathop{\mathbb{E}}_{\mu}}[Q_{u,(\sigma,b)}]. \end{aligned} \tag{17}$$

我们可以扩展上述定义，令 $Q_{S,\cup_{u\in S}(\sigma_u,b_u)}$ 表示多项式 $\prod_{u\in S} Q_{u,(\sigma_u,b_u)}$。对于$y_S = (\cup_{u\in S}\sigma_u, \cup_{u\in S} b_u)$，我们得到：

$$\widetilde{\Pr_{\mathcal{L}}}[(\cup_{u\in S} X_u, \cup_{u\in S} p_u) = Y_S = y_S] = \widetilde{\mathop{\mathbb{E}}_{\mu}}[Q_{S,\cup_{u\in S}(\sigma_u,b_u)}]. \tag{18}$$

可以为 Y' 定义类似的记号（例如，多项式 $Q'_{u,(\sigma,b)}$ 等），并推导出上述结论。我们知道 $\mathcal{A}_I \vdash_t \tilde{O}(1/\nu)\, Q_{S,\cup_{u\in S}(\sigma_u,b_u)} \in [0,1]$。为简化记号，我们定义以下表达式：

$$\begin{aligned} \widetilde{\mathop{\mathbb{E}}_{\mu\times\mu}}[E(X, X') \mid Y_S = y_S, Y'_T = y'_T] &:= \widetilde{\mathop{\mathbb{E}}_{\mu\times\mu}}[E(X, X') \mid Q_{S,y_S} \cdot Q'_{T,y'_T}] \\ &= \frac{\widetilde{\mathbb{E}}_{\mu\times\mu}[E(X, X') Q_{S,y_S} Q'_{T,y'_T}]}{\widetilde{\mathbb{E}}_{\mu\times\mu}[Q_{S,y_S} Q'_{T,y'_T}]} \\ &= \frac{\widetilde{\mathbb{E}}_{\mu\times\mu}[E(X, X') Q_{S,y_S} Q'_{T,y'_T}]}{\widetilde{\Pr}_{\mathcal{L}}[Y_S = y_S, Y'_T = y'_T]}, \end{aligned}$$

其中最后一个等号由方程（18）得出。类似于条件期望的定义，我们可以验证：

$$\widetilde{\mathop{\mathbb{E}}_{\mu\times\mu}}[E(X, X')] = \mathop{\mathbb{E}}_{\substack{i_1,\ldots,i_t\sim[m]\\ j_1,\ldots,j_t\sim[m]\\ y_{i_1\cup\ldots\cup i_t}, y'_{j_1\cup\ldots\cup j_t}\sim\mathcal{L}}} [\widetilde{\mathop{\mathbb{E}}_{X,X'}}[E(X, X') \mid Y_{i_1\cup\ldots\cup i_t} = y_{i_1\cup\ldots\cup i_t}, Y'_{j_1\cup\ldots\cup j_t} = y'_{j_1\cup\ldots\cup j_t}]].$$

由于 $\mathcal{A}_I \vdash_D E(X,X') \leq 1$ 且 $\deg(\mu) \geq D + \widetilde{\Omega}(t/\nu)$，我们得到：即使在对度为 $O(t/\nu)$ 的非负事件 Q 进行条件化后，$E(X,X') \leq 1$ 仍然成立：$\mathrm{E}[E(X,X') \mid Q] \leq 1$。平均论证表明：

$$\Pr_{\substack{i_1,\ldots,j_1,\ldots\sim[m_2] \\ y_{i_1\cup\ldots\cup i_t}, y'_{j_1\cup\ldots\cup j_t}\sim\mathcal{L}}} \left[\widetilde{\mathbb{E}}_{\mu\times\mu}[E(X,X') \mid Y_{i_1\cup\ldots\cup i_t} = y_{i_1\cup\ldots\cup i_t}, Y'_{j_1\cup\ldots\cup j_t} = y'_{j_1\cup\ldots\cup j_t}] \geq \frac{p}{2} \right] \geq \frac{p}{2}. \tag{19}$$

选择 $\alpha = p/8$ 和 $\tau' < p\tau/8$，我们可以对方程（15）、（16）、（19）中的事件应用并合界，从而得到存在集合 $i_1, \ldots\ldots, i_t$、$j_1, \ldots\ldots, j_t \in [m_2]$ 以及 $y_{i_1\cup\ldots\cup i_t}$、$y'_{j_1\cup\ldots\cup j_t} \sim \mathcal{L}$，使得：

$$\mathbb{E}_{a,b\sim[m_2]}[I(Y_a; Y_b \mid Y_{i_1\cup\ldots\cup i_t} = y_{i_1\cup\ldots\cup i_t}] \leq \frac{\tau'}{\alpha} < \tau.$$

$$\mathbb{E}_{a,b\sim[m_2]}[I(Y'_a; Y'_b \mid Y'_{j_1\cup\ldots\cup j_t} = y'_{j_1\cup\ldots\cup j_t})] \leq \frac{\tau'}{\alpha} < \tau.$$

$$\widetilde{\mathbb{E}}_{\mu\times\mu}[E(X,X') \mid Y_{i_1\cup\ldots\cup i_t} = y_{i_1\cup\ldots\cup i_t}, Y'_{j_1\cup\ldots\cup j_t} = y'_{j_1\cup\ldots\cup j_t}] \geq \frac{p}{2}.$$

令 μ_1 为 X 上的伪分布，它是将 μ 对 $Q_{i_1\cup\ldots\cup i_t}$、$y_{i_1\cup\ldots\cup i_t}$ 条件化后得到的；令 μ_2 为 X' 上的伪分布，它是将 μ 对 $Q_{j_1\cup\ldots\cup j_t}$、$y'_{j_1\cup\ldots\cup j_t}$ 条件化后得到的。容易验证：

$$\mathcal{L}(\mu\times\mu, p_{\beta,\nu}) | (Y_{i_1\cup\ldots\cup i_t} = y_{i_1\cup\ldots\cup i_t}, Y'_{j_1\cup\ldots\cup j_t} = y'_{j_1\cup\ldots\cup j_t}) = \mathcal{L}(\mu_1\times\mu_2, p_{\beta,\nu}),$$

由此得到引理中所需的三个性质。还需要验证我们要求的 μ 的次数上界。我们对 $t = O$ 中的 (Y, Y') 条件化了 $(\log |\Sigma|/p\tau)$ 个变量，每个变量在 X, X' 中的度为 $\widetilde{O}(1/\nu)$，因此只需使 μ 的度为 $\widetilde{\Omega}\left(\frac{\log|\Sigma|}{p\tau\nu}\right)$。条件化后，若 $\deg(\mu) \geq D' + \widetilde{\Omega}\left(\frac{\log|\Sigma|}{p\tau\nu}\right)$，则 $\deg(\mu_1\times\mu_2) \geq D'$，从而完成证明。□

3.5 引理 3.10：条件化不会引入相关性

在本节中，我们证明：给定关于变量 (Y, Y') 满足低全局相关性的 (X, X') 上的乘积分布，其中 $Y_u, v = (X_u, X_v, p_u, p_v)$，以及以较大概率成立的事件 $E(X, X')$，在对 E 进行条件化后，不会使太多对 (Y_i, Y'_i) 产生相关性。这是一个一般性的引理：只要变量 (Y, Y') 是底层变量 (X, X') 的局部函数，并且满足低全局相关性，该引理就成立；但此处我们仅针对具体应用陈述它。

引理 3.25（引理 3.10 的重述）。对于所有 $\tau, p, \beta, \nu, \delta \in (0,1)$ 以及整数 $D, N, m \leq N$，以下内容成立：设 $\mu_1\times\mu_2$ 是 (X, X') 上的一个度为 $D + \Omega(1/\nu)$ 的伪分布，满足 $\mathcal{A}_I(X, X')$，并且 $E(X, X')$ 是一个多项式，使得 $\mathcal{A}_I \vdash_D E(X, X') \in [0,1]$ 且 $\mathrm{E}_{\mu_1\times\mu_2}[E(X, X')] \geq p$。假设对于 $S \subseteq [N]$，我们有：

1. $\mathrm{E}_{u_1,v_1\sim S:\ u_1\neq v_1}[I(Y_{u_1,v_1}; Y_{u_2,v_2})] \leq \tau.$
2. $\mathrm{E}_{u_1\ v_1\sim S\ u_1\neq v_1,:\ ,:\ u_2\neq v_2\ u_2\ v_2\sim S}[I(Y'_{u_1,v_1}; Y'_{u_2,v_2})] \leq \tau,$

其中 $Y_{u,\ v} = (X_u,\ \ X_v,\ \ p_u,\ \ p_v) Y'_{u,\ v} = (X'_u,\ \ X'_v,\ \ p'_u,\ \ p'_v)$ 互信息是相对于局部分布集合 $\mathcal{L}(\mu_1 \times \mu_2,\ p_{\beta,\ \nu})$ (定义 3.5）。那么我们有:

$$\Pr_{u,v\sim S:u\neq v}[TV((Y_{u,v}, Y'_{u,v})|E, (Y_{u,v}, Y'_{u,v})) \geq \delta] \leq O\left(\frac{\sqrt{\tau} + 1/|S|}{p\delta^2}\right),$$

其中，分布 $(Y_{u,\ v}, Y'_{u,\ v})|E$ 指由局部分布集合 $\mathcal{L}(\mu_1 \times \mu_2|E, p_{\beta,\ \nu})$定义的这些变量上的联合分布; 类似地，$(Y_{u,\ v}, Y'_{u,\ v})$ 指由 $\mathcal{L}(\mu_1 \times \mu_2, p_{\beta,\ \nu})$ 定义的分布。

证明。与引理 3.19 的证明一样，不失一般性，设 $S = [m]$，令 $[m_2]$ 表示 m 的大小为 2 的子集，并令 $Y = (Y_{a_1}, \ldots, Y_{a_M})$ 表示 $a_t = (u, v), (u, v) \in [m_2]$。给定关于赋值 (X, X') 的伪分布 $\mathcal{D}$，我们将考虑变量 X, X', p, p' 上的局部分布集合 $\mathcal{L}(\mathcal{D}, p_\beta, \nu)$，从而得到关于 (Y, Y') 的诱导分布集合 $= (Y_{a_1}, \ldots, Y_{a_M}, Y'_{a_1}, \ldots, Y'_{a_M})$ （定义 3.5 ）。

在整个证明中，我们将考虑从局部分布集合 $\mathcal{L}(\mu_1 \times \mu_2, p_\beta, \nu)$ 和经条件化的分布集合 $\mathcal{L}(\mu_1 \times \mu_2|E, p_\beta, \nu)$ 中抽取的随机变量 (Y, Y')。为简化记号，我们用 $(Y_a, Y'_a)|E$ 表示由 $\mathcal{L}(\mu_1 \times \mu_2|E, p_\beta, \nu)$ 在 (Y_a, Y'_a) 上诱导的联合分布，并用 (Y_a, Y'_a) 表示由 $\mathcal{L}(\mu_1 \times \mu_2, p_\beta, \nu)$ 诱导的分布。我们将 $\mathcal{L}(\mu_1 \times \mu_2, p_\beta, \nu)$ 简记为 $\mathcal{L}$。令 U 为满足 $TV((Y_a, Y'_a)|E, (Y_a, Y'_a)) \geq \delta$ 的变量 $a \in [m_2]$ 所构成的集合，并令 U 的分数大小为 γ。若 Ω 表示 Y_u 的定义域，Y'_u 则对每个 $a \in U$，都存在一个集合 $S_a \subseteq \Omega \times \Omega$，使得:

$$\widetilde{\Pr_{\mathcal{L}}}[(Y_a, Y'_a) \in S_a \mid E] - \widetilde{\Pr_{\mathcal{L}}}[(Y_a, Y'_a) \in S_a] \geq \delta. \tag{20}$$

令 e_a 表示 $\widetilde{\Pr}_{\mathcal{L}}[(Y_a, Y'_a) \in S_a]$。定义随机变量 $Z_a = \mathbb{1}((Y_a, Y'_a) \in S_a) - e_a$。定义 :

$$Z = \mathop{\mathbb{E}}_{a\sim U}[Z_a] = \mathop{\mathbb{E}}_{a\in U}[\mathbb{1}((Y_a, Y'_a) \in S_a) - e_a].$$

令 $\widetilde{\mathrm{E}}_{\mathcal{L}}$ 表示与局部分布 $\mathcal{L}$对应的自然期望算子。可以验证 that $\widetilde{\mathrm{E}}_{\mathcal{L}}[Z] = \widetilde{\mathrm{E}}_{\mathcal{L}}[Z_a] = 0$，现在我们来计算它的方差。对于变量 Y, Y' 上的两个事件 A, B，令 $\widetilde{\mathrm{Cov}}(A, B)$ 表示 $\mathrm{E}_{\mathcal{L}}[AB] - \mathrm{E}_{\mathcal{L}}[A]\mathrm{E}_{\mathcal{L}}[B]$。首先，对于所有 $a, b \in [m_2]$，利用 Pinsker 不等式和数据处理不等式，我们有:

$$\begin{aligned}
\widetilde{\mathrm{Cov}}(\mathbb{1}((Y_a, Y'_a) \in S_a), \mathbb{1}((Y_b, Y'_b) \in S_b)) &\leq TV((Y_a, Y'_a, Y_b, Y'_b), (Y_a, Y'_a) \times (Y_b, Y'_b)) \\
&\leq O(\sqrt{I(Y_a, Y'_a; Y_b, Y'_b)}) \\
&\leq O(\sqrt{I(Y_a; Y_b) + I(Y'_a; Y'_b)})
\end{aligned}$$

证明将通过给 $\widetilde{\mathbb{E}}_{\mathcal{L}}[Z^2]$建立上界和下界来进行，其中上界利用了 Y 和 Y' 的低全局相关性性质，下界则利用了由公式 20得到的大偏差。

$\widetilde{\mathrm{E}}_{\mathcal{L}}[Z^2]$ 的上界：我们有以下上界:

$$\widetilde{\mathop{\mathbb{E}}_{\mathcal{L}}}[Z^2] = \mathop{\mathbb{E}}_{a,b\sim U}[\widetilde{\mathop{\mathbb{E}}_{\mathcal{L}}}[(\mathbb{1}((Y_a, Y'_a) \in S_a) - e_a)(\mathbb{1}((Y_b, Y'_b) \in S_b) - e_b)]]$$

$$
\begin{aligned}
&= \mathop{\mathbb{E}}_{a,b\sim U}[\widetilde{\mathop{\mathbb{E}}_{\mathcal{L}}}[\mathbb{1}((Y_a,Y'_a)\in S_a)-e_a]\widetilde{\mathop{\mathbb{E}}_{\mathcal{L}}}[\mathbb{1}((Y_b,Y'_b)\in S_b)-e_b]+\widetilde{\mathbb{C}\mathrm{ov}}(\mathbb{1}((Y_a,Y'_a)\in S_a),\mathbb{1}((Y_b,Y'_b)\in S_b))]\\
&\le \mathop{\mathbb{E}}_{a,b\sim U}[O(\sqrt{I(Y_a;Y_b)+I(Y'_a;Y'_b)})]\\
&\le O(\sqrt{\mathop{\mathbb{E}}_{a,b\sim U}[I(Y_a;Y_b)+I(Y'_a;Y'_b)]})\\
&\le O\left(\frac{\sqrt{\tau}}{\gamma}\right),
\end{aligned}
$$

其中，最后一个不等式成立是因为 $\mathrm{E}_{a,\ b\sim[m_2]}[I(Y_a;\ Y_b)]\ge\gamma^2\mathrm{E}_{a,\ b\sim U}[I(Y_a;\ Y_b)]$,，并且根据假设 $\mathrm{E}_{a,\ b\sim[M]}[I(Y_a;\ Y_b)]\le\tau$（$Y'$ 的情况类似）。

$\widetilde{\mathrm{E}}_{\mathcal{L}}[Z^2]$ 的下界：令 Q_a 为与事件 $\mathrm{I}[(Y_a,Y'_a)\ \in\ S_a]$ 相对应的多项式，即 $\widetilde{\mathrm{Pr}}_{\mathcal{L}}[(Y_a,Y'_a)\in S_a]=\mathrm{E}_{\mu_1\times\mu_2}[Q_a]$。将 $P(X,X')$ 简记为 P，表示多项式 $\mathrm{E}_a[Q_a-e_a]$。令 $Q_{a\cup b}$ 为满足 $\widetilde{\mathrm{Pr}}_{\mathcal{L}}[(Y_a,Y'_a)\in S_a\wedge(Y_b,Y'_b)\in S_b]=\mathrm{E}_{\mu_1\times\mu_2}[Q_{a\cup b}]$ 的多项式。如果 $a\cap b=\phi$，则有 $Q_{a\cup b}=Q_a\cdot Q_b$；但若它们在一个或两个变量上相交，这一点可能不成立。不过，我们有 $\mathrm{Pr}_{a,b\sim U}[a\cap b\ne\phi]\le O(1/|U|)$。利用这些事实，我们先通过以下两个等式证明 $\widetilde{\mathrm{E}}_{\mathcal{L}}[Z^2]+O(1/|U|)\ge\widetilde{\mathrm{E}}_{\mu_1\times\mu_2}[P^2]$:

$$
\begin{aligned}
\widetilde{\mathop{\mathbb{E}}_{\mathcal{L}}}[Z^2] &= \mathop{\mathbb{E}}_{a,b\sim U}[\widetilde{\mathop{\mathbb{E}}_{\mathcal{L}}}[(\mathbb{1}((Y_a,Y'_a)\in S_a)-e_a)(\mathbb{1}((Y_b,Y'_b)\in S_b)-e_b)]]\\
&= \Pr_{a,b\sim U}[a\cap b=\phi]\mathop{\mathbb{E}}_{a,b\sim U:a\cap b=\phi}[\widetilde{\mathop{\mathbb{E}}_{\mu_1\times\mu_2}}[(Q_a-e_a)(Q_b-e_b)]]\\
&+ \Pr_{a,b\sim U}[a\cap b\ne\phi]\mathop{\mathbb{E}}_{a,b\sim U:a\cap b\ne\phi}[\widetilde{\mathop{\mathbb{E}}_{\mathcal{L}}}[(\mathbb{1}((Y_a,Y'_a)\in S_a)-e_a)(\mathbb{1}((Y_b,Y'_b)\in S_b)-e_b)]]\\
&\ge \Pr_{a,b\sim U}[a\cap b=\phi]\mathop{\mathbb{E}}_{a,b\sim U:a\cap b=\phi}[\widetilde{\mathop{\mathbb{E}}_{\mu_1\times\mu_2}}[(Q_a-e_a)(Q_b-e_b)]]-O\left(\frac{1}{|U|}\right). \qquad (21)
\end{aligned}
$$

另一方面，我们有:

$$
\begin{aligned}
\widetilde{\mathop{\mathbb{E}}_{\mu_1\times\mu_2}}[P^2] &= \mathop{\mathbb{E}}_{a,b\sim U}[\widetilde{\mathop{\mathbb{E}}_{\mu_1\times\mu_2}}[(Q_a-e_a)(Q_b-e_b)]]\\
&= \Pr_{a,b\sim U}[a\cap b=\phi]\mathop{\mathbb{E}}_{a,b\sim U:a\cap b=\phi}[\widetilde{\mathop{\mathbb{E}}_{\mu_1\times\mu_2}}[(Q_a-e_a)(Q_b-e_b)]]\\
&+ \Pr_{a,b\sim U}[a\cap b\ne\phi]\mathop{\mathbb{E}}_{a,b\sim U:a\cap b=\phi}[\widetilde{\mathop{\mathbb{E}}_{\mu_1\times\mu_2}}[(Q_a-e_a)(Q_b-e_b)]]\\
&\le \Pr_{a,b\sim U}[a\cap b=\phi]\mathop{\mathbb{E}}_{a,b\sim U:a\cap b\ne\phi}[\widetilde{\mathop{\mathbb{E}}_{\mu_1\times\mu_2}}[(Q_a-e_a)(Q_b-e_b)]]+O\left(\frac{1}{|U|}\right) \qquad (22)
\end{aligned}
$$

结合（21）和（22），可得:

$$
\widetilde{\mathop{\mathbb{E}}_{\mathcal{L}}}[Z^2]+O\left(\frac{1}{|U|}\right)\ge\widetilde{\mathop{\mathbb{E}}_{\mu_1\times\mu_2}}[P^2].
$$

回顾一下 $|U|=\gamma|S|$。由于 $\mathcal{A}_I\vdash_D E(X,X')\in[0,1]$，我们得到:

$$
\widetilde{\mathop{\mathbb{E}}_{\mathcal{L}}}[Z^2]+O\left(\frac{1}{\gamma|S|}\right)\ge\widetilde{\mathop{\mathbb{E}}_{\mu_1\times\mu_2}}[P^2]\ge\widetilde{\mathop{\mathbb{E}}_{\mu_1\times\mu_2}}[E]\widetilde{\mathop{\mathbb{E}}_{\mu_1\times\mu_2}}[P^2|E]\ge p\widetilde{\mathop{\mathbb{E}}_{\mu_1\times\mu_2}}[P|E]^2=p\widetilde{\mathop{\mathbb{E}}_{\mathcal{L}}}[Z|E]^2,
$$

其中最后一个不等式是对伪分布应用柯西-施瓦茨不等式得到的 $\mu_1 \times \mu_2|E$，最后一个等式则由 P 和 Z 的定义得出。利用方程（20），我们知道，对于所有 $a \in U$：

$$\widetilde{\mathbb{E}}_{\mathcal{L}}[Z_a \mid E] = \widetilde{\Pr}_{\mathcal{L}}[(Y_a, Y'_a) \in S_a \mid E] - e_a \geq \delta,$$

这意味着 $\mathrm{E}_{\mathcal{L}}[Z \mid E] \geq \delta$。
结合 $\mathrm{E}_{\mathcal{L}}[Z^2]$ 的上界和下界，可得 $\gamma \leq O\left(\frac{\sqrt{\tau}+1/|S|}{p\delta^2}\right)$，从而完成引理的证明。

□

3.6 引理 3.11 的证明：具有较大移位势的子图舍入 al

本节将证明，当相对于伪分布 $\Phi^G_{\beta,\,\nu}$（定义 3.3）的移位划分势较大时（该伪分布具有某些良好性质），条件与舍入算法（算法 3.7）能够成功地为唯一游戏实例返回一个良好的赋值。本节的证明沿用 [BBK+21] 中对条件化与舍入的分析思路，不过我们只有近似局部独立性，而非 X，X' 之间的独立性。由于我们始终处理图 G，下文将省略移位划分势中的上标 G。本节将证明以下定理：

引理 3.26（引理 3.11 的重述）。设 $I = (G, \Pi)$ 是一个定义在 $\sim$ 上、字母表为 Σ 的唯一游戏仿射实例，且 $\mu_1 \times \mu_2$ 是一个关于 I 上赋值 (X, X') 的度为 $D + O(1/\nu)$ 的伪分布。设 $E(X, X')$ 是一个多项式，使得 $\mathcal{A}_I(X, X') \vdash_D E(X, X') \in [0, 1]$。假设：

$$\Pr_{u,v \sim V(G): u \neq v}[TV((Y_{u,v}, Y'_{u,v})|E, (Y_{u,v}, Y'_{u,v})) > \delta] \leq \zeta,$$

其中，分布 $(Y_{u,v}, Y'_{u,v})|E$ 指由局部分布 $\mathcal{L}(\mu_1 \times \mu_2|E, p_{\beta,\nu})$ 的集合定义在这些变量上的联合分布；类似地，$(Y_{u,v}, Y'_{u,v})$ 指由 $\mathcal{L}(\mu_1 \times \mu_2, p_{\beta,\nu})$ 定义的分布（定义 3.5）。

若 $\Phi^G_{\beta,\,\nu}(\mu_1 \times \mu_2|E(X,\ X')) \geq \gamma$，那么，对于至少一个伪分布 μ_1^{sym} 或 μ_2^{sym}，算法 3.7 的运行时间为 $\mathrm{poly}(|V(G)|)$，并返回一个期望值至少为以下数值的赋值：

$$(\beta - \nu)^2 \left(\gamma - O(\delta + \zeta) - \frac{1}{|V(G)|}\right) - 3\nu(\beta - \nu)$$

对于 I。

引理的证明3.26。 沿用 [BBK+21] 的证明策略，我们定义替代移位势$\Psi(\mu)$：

定义 3.27 (替代移位势 [BBK+21])。 度为 替代移位势 的 $D \geq 4$伪分布 μ定义为

$$\Psi(\mu) := \mathop{\mathbb{E}}_{u,v \sim \pi(G)}\left[\sum_{s \in \Sigma} \widetilde{\Pr}_{\mu}[X_v - X_u = s]^2 \cdot \widetilde{\mathbb{E}}[\mathrm{val}_v(X) \mid X_v - X_u = s]\right],$$

其中，$\pi(G)$ 是 G 上的平稳测度，而 $\mathrm{val}_v(X)$ 表示顶点 v 的值。

我们将证明，如果 $\Phi(\mu_1 \times \mu_2|E)$ 很大，且 E 不会引入过多相关性，那么 $\Psi(\mu_1)$ 或 $\Psi(\mu_2)$ 必有一个很大：

~引理 3.28。设 $\mu_1 \times \mu_2$ 是定义在 (X, X') 上、度为 $O(D + 1/\nu)$ 的伪分布，并设 $E(X, X')$ 是一个多项式，使得 $\mathcal{A}_I \vdash_D E(X, X') \in [0, 1]$。假设我们有：

$$\Pr_{u,v\sim V(G):u\neq v}[TV((Y_{u,v}, Y'_{u,v})|E, (Y_{u,v}, Y'_{u,v})) > \delta] \leq \zeta.$$

如果 $\mu_1 \times \mu_2|E(X, X')$ 的移位划分势很大，那么 μ_1 或μ_2 的交替移位势也必然很大：

$$\Phi_{\beta,\nu}(\mu_1 \times \mu_2|E(X, X')) \leq \frac{\Psi(\mu_1)}{2(\beta-\nu)^2} + \frac{\Psi(\mu_2)}{2(\beta-\nu)^2} + \frac{3\nu}{\beta-\nu} + 2\delta + 2\zeta + \frac{1}{|V(G)|}.$$

证明。 详见第 3.6.1。 □

给定一个伪分布 μ，回顾一下， μ^{sym} 是如第 2.4.3 节所定义的移位对称化伪分布。注意， $\Psi(\mu) = \Psi(\mu^{\text{sym}})$，因为 Ψ 如 $\Pr_{\mu^{\text{sym}}}[X_u - X_v = s] = \Pr_{\mu}[X_u - X_v = s]$ ~，且对所有 s，$\mathrm{E}_{\mu^{\text{sym}}}[\mathrm{val}_v(X)|X_v - X_u = s] = \mathrm{E}_{\mu}[\mathrm{val}_v(X)|X_v - X_u = s]$。因此，我们可以使用来自 [BBK+21] 的以下引理：该引理表明，当移位对称伪分布的交替移位势很大时，经过一步条件化和舍入即可得到目标值很高的解：

引理 3.29 (引理 3.6 [BBK+21])。 设 $I = (G, \Pi)$ 是字母表为 Σ 的唯一游戏仿射实例，设 $\kappa > 0$，并设 μ 是针对 4 度移位对称伪分布 I。若 $\Psi(\mu) \geq \kappa$，则算法 *3.7* 返回一个期望值至少为 κ 的解。

现在，只需对 μ_1^{sym} 或 μ_2^{sym} （取决于哪一个的 Ψ 更高）应用最后一个引理，即可得出该结论。 □

3.6.1 势的关联：引理的证明3.28

引理 3.28 的证明。我们首先回顾，在 $\Phi_{\beta,\eta}$ 的定义中，我们使用了一个 ν-可加的多项-~式近似 $p(x)$，其度为 $O(1/\nu)$，用于近似区间 $x \in [0, 1]$ 上的指示函数 $\mathrm{I}[x \geq \beta]$，该近似由定理 2.7 保证。我们将用 E 表示多项式 $E(X, X')$，用 $\mathcal{D}$ 表示伪分布 $\mu_1 \times \mu_2|E$，并用 π 表示在 $V(G)$ 上的均匀（一般而言是平稳）测度。令 p_u 表示多项式 $p_{\beta,\nu}(\mathrm{val}_u(X))$ 和 $p'_u = p_{\beta,\nu}(\mathrm{val}_u(X'))$。还请回顾局部分布集合 $\mathcal{L}(\cdot, p_{\beta,\nu})$（定义 3.5）。我们将滥用记号 p_u, p'_u，使其既表示定义 3.5 中的变量，也表示多项式 $p_{\beta,\nu}(\mathrm{val}_u(X))$，具体含义应由上下文明确。展开 $\Phi_{\beta,\nu}(\mathcal{D})$ 的定义，我们得到：

$$\begin{aligned}
\Phi_{\beta,\nu}(\mathcal{D}) &= \widetilde{\mathbb{E}}_{\mathcal{D}}\left[\sum_{s\in\Sigma}\left(\mathop{\mathbb{E}}_{u\sim\pi}\mathbb{I}[X_u - X'_u = s]p_u p'_u\right)^2\right] \\
&= \widetilde{\mathbb{E}}_{\mathcal{D}}\left[\sum_{s\in\Sigma}\mathop{\mathbb{E}}_{u,v\sim\pi}\mathbb{I}[X_u - X'_u = X_v - X'_v = s]p_u p_v p'_u p'_v\right] \\
&= \mathop{\mathbb{E}}_{u,v\sim\pi}\widetilde{\mathbb{E}}_{\mathcal{D}}\left[\mathbb{I}[X_u - X_v = X'_u - X'_v]\cdot p_u p_v p'_u p'_v\right],
\end{aligned}$$

$$= \mathop{\mathbb{E}}_{u,v\sim\pi}\Big[\mathop{\widetilde{\mathbb{E}}}_{\mu_1\times\mu_2}\left[\mathbb{I}[X_u - X_v = X'_u - X'_v]\cdot p_u p_v p'_u p'_v\right] + \mathsf{err}(u,v)\Big], \tag{23}$$

对于每一对 (u,v)，相应地定义 $\mathsf{err}(u,v)$（注意，我们在最后一步转换中从伪分布$\mathcal{D}$ 切换到了伪分布 $\mu_1\times\mu_2$）。

界定 (23) 中的误差项。对于 $u=v$，我们得到 $\mathsf{err}(u,v) = \widetilde{\mathrm{E}}_{\mathcal{D}}[p_u^2(p'_u)^2] - \widetilde{\mathrm{E}}_{\mu_1\times\mu_2}[p_u^2(p'_u)^2] \le 1$。接下来，我们对 $u\neq v$ 的 $\mathsf{err}(u,v)$ 进行界定。令 $R(X_u, X_v, X'_u, X'_v, p_u, p_v, p'_u, p'_v)$ 为多项式 $\mathrm{I}[X_u - X_v = X'_u - X'_v]p_u p_v p'_u p'_v$（$p_u$ 表示多项式 $p_{\beta,\nu}(\mathsf{val}_u(X))$）。在此处，我们将记号 p_u 过载使用，使其也表示定义 3.5 中的指示变量，并令 $R(a_1,\ldots,a_4,b_1,\ldots,b_4)$ 对于 $a_1,\ldots,a_4\in\Sigma$ 和 $b_1,\ldots,b_4\in\{0,1\}$ 也表示将 $R(X_u,\ldots,p'_v)$ 在取值 $a_1,\ldots,b_4$ 上进行求值所得的结果：$\mathrm{I}[a_1 - a_2 = a_3 - a_4]b_1b_2b_3b_4$。3 5 $u\neq v$ $\mathcal{D}[R] = \mathcal{L}(\mathcal{D},p_{\beta,\nu})[X_u - X_v = X'_u - X'_v, p_u = p_v = p'_u = p'_v = 1]$。利用定义 $\mu_1\times\mu_2$ $\mathcal{D}$，我们有当： E Pr)，类似地，对于分布，以 替代 。因此，对于 $u\neq v$，我们得到：

$$\begin{aligned}
&\mathsf{err}(u,v)\\
&= \mathop{\widetilde{\mathbb{E}}}_{\mathcal{D}}[R(X_u,\ldots,p'_v)] - \mathop{\widetilde{\mathbb{E}}}_{\mu_1\times\mu_2}[R(X_u,\ldots,p'_v)]\\
&= \mathop{\widetilde{\Pr}}_{\mathcal{L}(\mathcal{D},p_{\beta,\nu})}[X_u - X_v = X'_u - X'_v, p_u = \ldots = p'_v = 1] - \mathop{\widetilde{\Pr}}_{\mathcal{L}(\mu_1\times\mu_2,p_{\beta,\nu})}[X_u - X_v = X'_u - X'_v, p_u = \ldots = p'_v = 1]\\
&= \sum_{a_1,\ldots,a_4\in\Sigma} R(a_1,\ldots,a_4,1,\ldots,1)\Big(\mathop{\widetilde{\Pr}}_{\mathcal{L}(\mathcal{D},p_{\beta,\nu})}[X_u = a_1,\ldots,p_u = 1,\ldots] - \mathop{\widetilde{\Pr}}_{\mathcal{L}(\mu_1\times\mu_2,p_{\beta,\nu})}[X_u = a_1,\ldots,p_u = 1\ldots]\Big)\\
&\le \sum_{a_1,\ldots,a_4\in\Sigma}\left|\mathop{\widetilde{\Pr}}_{\mathcal{L}(\mathcal{D},p_{\beta,\nu})}[X_u = a_1,\ldots,p_u = 1,\ldots] - \mathop{\widetilde{\Pr}}_{\mathcal{L}(\mu_1\times\mu_2,p_{\beta,\nu})}[X_u = a_1,\ldots,p_u = 1,\ldots]\right|\\
&= 2TV((Y_{u,v},Y'_{u,v})|E,(Y_{u,v},Y'_{u,v})),
\end{aligned}$$

其中，$Y_{u,v} = (X_u, X_v, p_u, p_v)$、$Y'_{u,v} = (X'_u, X'_v, p'_u, p'_v)$ 如引理中所述；分布 $(Y_{u,v},Y'_{u,v})|E$指由局部分布集合 $\mathcal{L}(\mu_1\times\mu_2|E,p_{\beta,\nu})$ 定义在这些变量上的联合分布；类似地，$(Y_{u,v},Y'_{u,v})$ 指由 $\mathcal{L}(\mu_1\times\mu_2,p_{\beta,\nu})$ 定义的分布（定义 3.5）。

综合可得：

$$\begin{aligned}
\mathop{\mathbb{E}}_{u,v\sim\pi}[\mathsf{err}(u,v)] &\le \mathop{\mathbb{E}}_{u,v\sim\pi:u\neq v}[\mathsf{err}(u,v)] + \Pr_{u,v\sim\pi}[u=v]\,\mathop{\mathbb{E}}_{u}[\mathsf{err}(u,u)]\\
&\le \mathop{\mathbb{E}}_{u,v\sim\pi:u\neq v}[2TV((Y_{u,v},Y'_{u,v})|E,(Y_{u,v},Y'_{u,v}))] + \frac{1}{|V(G)|}\\
&\le 2\delta + 2\zeta + \frac{1}{|V(G)|},
\end{aligned} \tag{24}$$

根据引理陈述中的假设。

对（(23)）中的主项进行上界估计。 现在我们对（23）中的第一项进行上界估计。

$$\begin{aligned}
&\mathop{\mathbb{E}}_{u,v\sim\pi}\Big[\mathop{\widetilde{\mathbb{E}}}_{\mu_1\times\mu_2}\left[\mathbb{I}[X_u - X_v = X'_u - X'_v]\cdot p_u p_v p'_u p'_v\right]\\
&= \mathop{\mathbb{E}}_{u,v\sim\pi}\left[\sum_{s\in\Sigma}\mathop{\widetilde{\mathbb{E}}}_{\mu_1}[\mathbb{I}[X_u - X_v = s]\cdot p_u p_v]\mathop{\widetilde{\mathbb{E}}}_{\mu_2}[\mathbb{I}[X'_u - X'_v = s]\cdot p'_u p'_v]\right].
\end{aligned}$$

接下来，我们利用 $p(x)$、$\mathrm{val}_u(X)$、$\mathrm{val}_u(X')\in[0,1]$，以及事实 2.8 所断言的 $p(x)\le\frac{x}{\beta-\nu}+\nu$对所有$x\in[0,1]$均成立，而且这是 SoS 可证的。因此，提取因子 p_v，p'_v并应用事实 2.8 对 p_u，p'_u 进行上界估计，可得（23）右侧的第一项至多为

$$\begin{aligned}
&\mathop{\mathbb{E}}_{u,v\sim\pi}\left[\sum_{s\in\Sigma}\widetilde{\mathbb{E}}_{\mu_1}\left[\mathbb{I}[X_u-X_v=s]\cdot\frac{\mathrm{val}_u(X)}{\beta-\nu}\right]\widetilde{\mathbb{E}}_{\mu_2}\left[\mathbb{I}[X'_u-X'_v=s]\cdot\frac{\mathrm{val}_u(X')}{\beta-\nu}\right]\right]+\frac{3\nu}{\beta-\nu}\\
&\le\frac{1}{2}\mathop{\mathbb{E}}_{u,v\sim\pi}\left[\sum_{s\in\Sigma}\widetilde{\mathbb{E}}_{\mu_1}\left[\mathbb{I}[X_u-X_v=s]\cdot\frac{\mathrm{val}_u(X)}{\beta-\nu}\right]^2\right]+\frac{1}{2}\mathop{\mathbb{E}}_{u,v\sim\pi}\left[\sum_{s\in\Sigma}\widetilde{\mathbb{E}}_{\mu_2}\left[\mathbb{I}[X'_u-X'_v=s]\cdot\frac{\mathrm{val}_u(X')}{\beta-\nu}\right]^2\right]\\
&+\frac{3\nu}{\beta-\nu},
\end{aligned}$$

其中我们用到了算术-几何平均不等式。第一项可界为

$$\begin{aligned}
&\mathop{\mathbb{E}}_{u,v\sim\pi}\left[\sum_{s\in\Sigma}\widetilde{\mathbb{E}}_{\mu_1}\left[\mathbb{I}[X_u-X_v=s]\cdot\frac{\mathrm{val}_u(X)}{\beta-\nu}\right]^2\right]\\
\le&\mathop{\mathbb{E}}_{u,v\sim\pi}\left[\sum_{s\in\Sigma}\widetilde{\mathbb{E}}_{\mu_1}\left[\mathbb{I}[X_u-X_v=s]\cdot\frac{1}{\beta-\nu}\right]\widetilde{\mathbb{E}}_{\mu_1}\left[\mathbb{I}[X_u-X_v=s]\frac{\mathrm{val}_u(X)}{\beta-\nu}\right]\right]\\
=&\frac{1}{(\beta-\nu)^2}\mathop{\mathbb{E}}_{u,v\sim\pi}\left[\sum_{s\in\Sigma}\widetilde{\mathbb{E}}_{\mu_1}[\mathbb{I}[X_u-X_v=s]]^2\cdot\widetilde{\mathbb{E}}_{\mu_1}[\mathrm{val}_u(X)\mid X_u-X_v=s]\right]\\
=&\frac{\Psi(\mu_1)}{(\beta-\nu)^2},
\end{aligned}$$

其中我们用到了值$_u(X)\le1$并应用了条件伪期望的定义；类似地，第二项的上界为 $^{\Psi}{}_{(\mu_2)}{}_{(\beta-\nu)^2}$。将该结果和24代入23即可完成证明。 ——— □

4 低完备性的唯一游戏

本节将分析推广到完备性任意小（但与 0 保持一定距离）的 UG 实例。唯一发生变化的步骤，是在条件化之后得出存在一个具有较大移位划分势的子立方体。

回顾一下，在高完备性情形对应引理（引理3.9）的证明中，我们使用断言3.21和3.22 得出：如果一个子立方体具有较大的全局移位划分势，那么它也具有较大的移位划分势。这之所以成立，是因为当子立方体的扩张较小时，所有具有高全局值的顶点在子立方体内也具有高值（$O(\varepsilon)$ 如果完备性为 $1-\varepsilon$）。在低完备度情形下，这一事实不再成立，因为子立方体的扩张现在可能接近1。为规避这一问题，我们不再经过中间的全局移位划分这一途径，而是直接尝试得出子立方体上的移位划分势较大。为此，我们需要全局超收缩性的一个更强结论，并将其称为“边覆盖”陈述：移位划分的某一部分较大的子立方体几乎覆盖移位划分的全部内部边。

正如我们将看到的，如果我们的伪分布最初的值为 c，那么内部边的比例至少为 c^2（特别是，c^2比例的边同时满足 X 和 X'）。由于我们能够覆盖几乎所有内部边，因此可以得出存在一个完备性较高的子立方体，事实上，其移位划分势也很高。给定引理3.9的这一版本，其余分析保持不变。

记号：在本节中，我们先考虑由函数$\{G_s : V(G) \to \mathrm{R}[X, X']\}_{s\in\Sigma}$定义的较简单的移位划分：

$$G_s(u) = \mathbb{1}(X_u - X'_u = s).$$

注意，G_s覆盖了所有顶点，也就是说$\sum_s \delta(G_s) = 1$，并满足布尔性：对于所有$u \in V(G)$，$G_s(u)^2 = G_s(u)$。

给定两个赋值X、X'，令$\mathrm{val}_u(X \wedge X')$表示与$u$相incident的边中，同时被$X$和$X'$满足的边的比例。注意，$\mathrm{val}_u(X \wedge X')$是关于$(X, X')$的四次多项式：

$$\mathrm{val}_u(X \wedge X') = \mathop{\mathbb{E}}_{v:(u,v)\in E}[(\sum_{\sigma\in\Sigma} X_{u,\sigma}X_{v,\pi_{u,v}(\sigma)})(\sum_{\sigma\in\Sigma} X'_{u,\sigma}X'_{v,\pi_{u,v}(\sigma)})].$$

令$\mathrm{val}_I(X \wedge X') = \mathrm{E}_u[\mathrm{val}_u(X \wedge X')]$表示图中同时被$X$和$X'$满足的边的比例。此外，对于一个$i$-限制$a \in \binom{[n]}{i}$和一个顶点$u \in J|_a$，令$\mathrm{val}^a_u(X \wedge X')$表示在$J|_a$中与$u$相incident的边中，同时被$X$和$X'$满足的边的比例。这也是关于$(X, X')$的四次多项式。

定义 4.1（稠密子立方体的近似指示函数）。令$\varepsilon_0, \ldots, \varepsilon_r \in$为稍后确定的$(0, 1)$中的值。对于任意$i$-限制$a$，令$R_{s,a}$表示如下（近似）指示函数：$G_s$在$J|_a$中是$\varepsilon_i$-稠密的，但在任何满足$b \subsetneq a$的子立方体$J|_b$中都不是$\varepsilon_{|b|}$-稠密的。为了将其定义为多项式，我们先定义近似指示函数$p_{<\beta,\nu}(x) = 1 - p_{\beta,\nu}(x)$。可以验证，当$x \in [0, 1]$时，$p_{<\beta,\nu}$近似于$\mathrm{I}[x < \beta]$，且具有与近似$\mathrm{I}[x \geq \beta]$（当$x \in [0, 1]$时）的$p_{\beta,\nu}$（定理 2.7）类似的性质。形式化地，利用指示函数的多项式近似，定义

$$R_{s,a} = p_{\varepsilon_i,\nu}(\delta(G_s|_a)) \prod_{j<i} \prod_{b\subset a:|b|=j} p_{<\varepsilon_j,\nu}(\delta(G_s|_b)).$$

4.1 边覆盖定理

我们的论证需要给出可同时发生的事件$R_{s,\ a}$数量的上界。粗略地说，这相当于询问：给定集合F能在多少个i-受限子立方体上是稠密的？照此表述，这个数量没有好的上界：如果F在某个$i-1$-受限子立方体上是稠密的，那么它在许多包含该子立方体的i-受限子立方体上也会相当稠密。这就是为什么在事件$R_{s,\ a}$中，我们要求i-受限子立方体是稠密的，但不存在包含它的j-受限子立方体（$j < i$），使得我们的集合在其中仍有一定程度的稠密性。

断言 4.2. 如果ε_0、...、ε_r满足$\varepsilon_{i-1} \leq \varepsilon_i/(2^{i+1}i)$，那么我们得到：

$$\vdash_{\ell^{O(\ell^i/\nu)}} \mathop{\mathbb{E}}_{a\sim\binom{[n]}{i}}[R_{s,a}] \leq \frac{4\delta(G_s)}{\varepsilon_i^2\ell^i} + O(\nu).$$

证明。我们首先说明一种论证：将$R_{s,\ a}$中的多项式$p_{\beta,\ \nu}$替换为指示函数。然后，我们简要说明如何将该证明转化为平方和证明。

将$p_{\beta,\nu}$转换为指示函数后，我们得到$R_{s,a}$对应于$T_{s,a}$：

$$T_{s,a} = \mathbb{1}(\delta(G_s|_a) \geq \varepsilon_i) \prod_{j<i} \prod_{b\subset a:|b|=j} \mathbb{1}(\delta(G_s|_b) < \varepsilon_j)$$

也就是说，事件 G_s 在 a 中是 ε_i-稠密的，但对于所有 a 的子集 b，其稠密度至多为 ε_j。我们将证明，此类限制 a 所占的比例必定很小。

我们考虑傅里叶分析函数 $f_{i,\ F}$ 其定义见第 C 节，定义 C.6，并使用引理C.10中的另一种公式：

$$f_{i,F}(a) = \sum_{b\subseteq a}(-1)^{i-|b|}\delta(F|_b) \geq \delta(F|_a) - \sum_{b\subsetneq a}\delta(F|_b).$$

严格来说，我们只为约翰逊图 $C_{n,\ \ell,\ \alpha}$ 的 Cayley 版本定义了这些函数，但也可以将上述定义用于约翰逊图，并推导出我们在此使用的相同性质，误差为 $o(1)$。在本证明中，我们将忽略这些 $o(1)$ 误差项。

如果 $T_{s,\ a} = 1$ 我们得到，$\delta(F|_a) \geq \varepsilon_i$，但每个 $\delta(F|_b)$ 至多为 $\varepsilon_{|b|} < \varepsilon_i/(2^{i+1}i)$，因此得到：

$$f_{i,G_s}(a) \geq \varepsilon_i - \sum_{j<i}\binom{i}{j}\varepsilon_j \geq \varepsilon_i - \sum_{j<i}2^i\varepsilon_j \geq \frac{\varepsilon_i}{2}.$$

这立即给出：

$$T_{s,a} \leq 1 \leq 4f_{i,G_s}(a)^2/\varepsilon_i^2, \tag{25}$$

如果 $T_{s,\ a} = 1$。如果 $T_{s,\ a} = 0$，那么上述结论仍然成立。

另一方面，根据 f_i 引理C.11可得：

$$\mathbb{E}[f_{i,G_s}(a)^2] = \frac{W^i[G_s]}{\ell^i} \leq \frac{\mathbb{E}[G_s^2]}{\ell^i}.$$

结合方程25 可得：

$$\mathop{\mathbb{E}}_{a\sim\binom{[n]}{i}}[T_{s,a}] \leq \mathop{\mathbb{E}}_{a}\left[\frac{4f_{i,G_s}(a)^2}{\varepsilon_i^2}\right] \leq \frac{4\delta(G_s)}{\varepsilon_i^2\ell^i}.$$

平方和证明：我们简要说明如何为命题 $R_{s,\ a}$ 在满足 $a \in \binom{[n]}{1}$ 时给出平方和证明。完整的命题可用类似的方法证明。

令 δ_0 表示 $\delta(G_s)$，并令 δ_1 表示 $\delta(G_s|_a)$。类似于 (25)，我们先证明：

$$\frac{4(\delta_1-\delta_0)^2}{\varepsilon_1^2} + 2\nu - R_{s,a} > \nu \tag{26}$$

若 $\delta_1,\ \delta_0 \in [0,1]$。这并非平方和证明，但证明这一点后，我们可以利用黑盒定理，根据定义域 $[0,1]^2$的性质将其转化为平方和证明。（26）可通过分类讨论得出。

1. 若 $R_{s,\ a} > \nu$ 则意味着 $p_{\varepsilon_1,\ \nu}(\delta_1) > \nu$ 且 $p_{<\varepsilon_0,\ \nu}(\delta_0) > \nu$。根据多项式的定义$p_{\beta,\ \nu}$ 这意味着 $\delta_1 > \varepsilon_1$ 和 $\delta_0 < \varepsilon_0 < \varepsilon_1/2$，由此可得 $(\delta_1-\delta_0)^2 \geq \varepsilon_1^2/4$。由于 $R_{s,\ a}$ 总是 ≤ 1，因此可得：

$$R_{s,a} \leq 1 \leq \frac{4(\delta_1-\delta_0)^2}{\varepsilon_1^2} < \frac{4(\delta_1-\delta_0)^2}{\varepsilon_1^2} + \nu.$$

2. 如果 $R_{s,\ a} \leq \nu$ 我们得到：

$$R_{s,a} \leq \frac{4(\delta_1-\delta_0)^2}{\varepsilon_1^2} + \nu.$$

因此，重新整理上述内容并在两边加上 ν 得到式（26）。现在可以应用定理 2.6 ，该定理表明，在定义域 $[0,1]^k$ 上与 0 保持正距离的正多项式具有有界度平方和证明，从而得到：

$$\delta_0, \delta_1 \in [0,1] \vdash_{\exp(1/\nu)} R_{s,a} \leq \frac{4(\delta_1 - \delta_0)^2}{\varepsilon_1^2} + 2\nu.$$

可以验证，证明的其余部分已经是平方和，因此我们得到：

$$\mathcal{A}_I \vdash_{\tilde{O}(1/\nu)} \delta_0, \delta_1 \in [0,1] \vdash_{\exp(1/\nu)} \mathop{\mathbb{E}}_{a \sim \binom{[n]}{1}} [R_{s,a}] \leq \frac{4\delta(G_s)}{\varepsilon_1^2 \ell} + 2\nu.$$

我们可以完全重复相同的步骤，并使用定理 2.6 中的平方和次数上界，得到对完整命题的平方和证明，其次数为 $\ell^{O(\ell^i/\nu)}$。定理 2.6 给出的上界关于我们想要证明为平方和的多项式 f 的次数呈指数增长，因此我们的次数上界也是 $\exp(\ell^i/\nu)$。我们认为，或许可以通过更直接的分析，将次数上界改进为 $\mathrm{poly}(1/\nu, \ell^i)$ 。

□

现在我们转而陈述边覆盖定理。下面，我们考察移位划分中留在同一部分内的边，并证明这些边几乎都可以被包含在某些子立方体中，而在这些子立方体上，某个部分变得稠密。

定理 4.3（边覆盖定理）。对于所有常数 $r \in \mathbb{N}$、ε_0、……、$\varepsilon_r \in [0,1]$，其中 $\varepsilon_r \leq \exp(-r)$，且 ε_0、……、ε_r 满足 $\varepsilon_{i-1} \leq \varepsilon_i^5/(2^{6r})$，我们得到：

$$\mathcal{A}_I \vdash_{\ell^{\mathrm{poly}(\ell^r/\nu)}} \mathrm{val}_I(X \wedge X') \leq T_0(X, X') + \ldots + T_r(X, X') + \mathsf{err}, \tag{27}$$

其中：

$$T_0(X, X') = \sum_s p_{\varepsilon_0,\nu}(\delta(G_s)) \mathop{\mathbb{E}}_{u \sim G} [G_s(u) \mathrm{val}_u(X \wedge X')],$$

$$T_i(X, X') = \ell^i \mathop{\mathbb{E}}_{a \in \binom{[n]}{i}} [\sum_s R_{s,a} \mathop{\mathbb{E}}_{u \sim J|_a} [G_s(u) \mathrm{val}_u^a(X \wedge X')]]$$

$$\mathsf{err} = 4(1-\alpha)^{r+1} + 2^{6r} \max_i \frac{\varepsilon_{i-1}}{\varepsilon_i^4} + |\Sigma| \ell^{O(r)} \sqrt{\nu}.$$

证明。我们首先给出该命题的一个证明：在定义$R_{s,a}$ 中，用实际的指示函数替代多项式$p_{\beta,\nu}$。形式上，对于一个 $i \leq r$-限制 $a \in \binom{[n]}{i}$ ，令$R_{s,a}$ 为一个指示变量：若对所有 $b \subsetneq a$， $\delta(G_s|_a) \geq \varepsilon_i$ 且 $\delta(G_s|_b) \leq \varepsilon_{|b|}$ ，则其值为 1。然后，我们将概述如何将其转化为平方和证明，并使用$R_{s,a}$的真正定义。

对于任意集合 S ，令#$sat(S)$表示集合 S 内部同时满足 X 和 X'的边数。首先有：

$$\mathrm{val}_I(X \wedge X') \leq \sum_s \frac{\#sat(G_s)}{|E|}, \tag{28}$$

因为我们知道（根据事实 2.10），移位划分中跨越不同部分的任意边至少会被 X 或 X'中的一个违反。因此，我们来求$\#sat(G_s)$的上界。

考虑固定 $s \in \Sigma$ 时由 G_s 指示的集合。令 G_s 的稠密子立方体集合定义如下：

$$\mathcal{C}_s^0 = \begin{cases} \{J\} & \text{if } \delta(G_s) \geq \varepsilon_0 \\ \phi & \text{otherwise} \end{cases}$$

$$\mathcal{C}_s^{(1)} = \{a \in [n] : R_{s,a} = 1\}$$
$$\vdots$$
$$\mathcal{C}_s^{(r)} = \left\{a \in \binom{[n]}{r} : R_{s,a} = 1\right\}.$$

令 D_s 表示 G_s 的稠密部分：$\cup_{i\le r}\cup_{a\in\mathcal{C}_s^{(i)}} G_s \cap J|_a$，并令 $H_s = G_s \setminus D_s$ 表示 G_s 的伪随机部分。容易验证，H_s 是 (r,ε_r)-伪随机的。G_s 内的边可分为四种类型：位于稠密子立方体内部的边、连接两个不同稠密子立方体的边、位于 H_s 内部的边，以及连接 H_s 和 D_s 的边。在 $\#sat(G_s)$ 上应用这种边的细分，可得：

$$\frac{\#sat(G_s)}{|E(J)|} \le \sum_{i\le r}\sum_{a\in\mathcal{C}_s^{(i)}} \frac{\#sat(G_s\cap J|_a)}{|E(J)|} + \frac{|E(H_s,H_s)|}{|E(J)|} + \frac{|E(H_s,D_s)|}{|E(J)|}$$
$$+ \sum_{i,j\le r}\sum_{h=0}^{\min(i,j)}\sum_{a\in\mathcal{C}_s^{(i)}}\sum_{H\subseteq a,|H|=h}\sum_{\substack{b\in\mathcal{C}_s^{(j)}\\ a\ne b, a\cap b=H}} \frac{|E(J|_a,J|_b)|}{|E(J)|}. \tag{29}$$

我们将验证，第一项中的 i^{th} 求和项可以重新排列，从而得到 $T_i(X,X')$ 中的 s^{th} 求和项。我们有：

$$\sum_{a\in\mathcal{C}_s^{(i)}} \frac{\#sat(G_s\cap J|_a)}{|E(J)|} = \frac{\binom{[n]}{i}|E(J|_a)|}{|E(J)|} \mathop{\mathbb{E}}_{a\sim\binom{[n]}{i}}\left[R_{s,a}\frac{\#sat(G_s\cap J|_a)}{|E(J|_a)|}\right]. \tag{30}$$

通过直接计算，我们得到 $\frac{\binom{[n]}{i}|E(J|_a|\ )()|}{|E\ J}\le \ell^i$。至于上面的第二项，我们得到：

$$\frac{\#sat(G_s\cap J|_a)}{|E(J|_a)|} \le \frac{\sum_{u\in J|_a}\mathbb{I}[u\in G_s]\#sat_a(u)}{|V(J|_a)|d_a} = \mathop{\mathbb{E}}_{u\in J|_a}[\mathbb{I}[u\in G_s]\mathrm{val}_u^a(X\wedge X')],$$

其中，d_a 表示子图 $J|_a$ 中一个顶点的度，而 $\#sat_a(u)$ 表示 $J|_a$ 中与 u 相 incident，且同时被 X 和 X'满足的边数。因此，将其代入（30），并对 $i\le r$ 求和后，我们得到（29）中的第一项为：

$$\sum_{i\le r}\sum_{a\in\mathcal{C}_s^{(i)}} \frac{\#sat(G_s\cap J|_a)}{|E(J)|} \le \sum_{i\le r}\ell^i \mathop{\mathbb{E}}_{a\sim\binom{[n]}{i}}[R_{s,a}\mathop{\mathbb{E}}_{u\in J|_a}[\mathbb{I}[u\in G_s]\mathrm{val}_u^a(X\wedge X')]]. \tag{31}$$

我们将用某个较小的常数来界定（29）中的其他项。

界定式（29）中的最后一项。我们聚焦于 $i\le j$，最后将得到的界乘以 2。如果 $R_{s,\ \phi}=1$，也就是说，$\delta(G_s)\ge\varepsilon_0$，那么我们可以验证其值为 0，因为其他子立方体都不会有 $R_{s,\ a}=1$。因此，假设情况并非如此。固定大小为 h 的 i 和 $H\subseteq i$。对于任意相交于一个大小为 h 的集合的 $a\in\binom{[n]}{i}$、$b\in\binom{[n]}{j}$，我们有 $\frac{|E_{(J|_a\ J|_b\ |,\ )()}}{|E\ J}\le\left(\frac{2\ell}{n}\right)^{i+j-h}$。确实，为了理解这一点，可以设想在 J 中均匀随机地抽取一条边 (x,y)，并询问 $a\subseteq x$ 和 $b\subseteq y$ 的概率是多少。为此，我们希望 $a\cap b$ 同时包含于 x 和 y 中（这种情况发生的概率为

概率至多为 $(2\ell/n)^h$），并且 $a \setminus (a \cap b) \subseteq x$，$b \setminus (a \cap b) \subseteq y$，其发生的概率至多为 $(2\ell/n)^{i-h} \cdot (2\ell/n)^{j-h}$。因此，我们得到式（29）中的最后一项至多为

$$\sum_{i \le j \le r} \sum_{h=0}^{i-1} \sum_{a \in \mathcal{C}_s^{(i)}} \sum_{H \subseteq a, |H|=h} |\{b \,|b \in \mathcal{C}_s^{(j)}, a \cap b = H, a \neq b\}| \left(\frac{2\ell}{n}\right)^{i+j-h}.$$

这里我们注意到，h 不可能是 i，因为那样我们考察的将是子立方体 $J|_a \subseteq J|_b$，因此$R_{s,a} = 1$和$R_{s,b} = 1$不可能同时成立。

在限制 4.2 上应用命题 $G_s|_H$，我们得到

$$|\{b \,|b \in \mathcal{C}_s^{(j)}, a \cap b = H, a \neq b\}| \le \frac{n^{j-h}}{\ell^{j-h}} \frac{\delta(G_s|_H)}{\varepsilon_j^2} \le \frac{n^{j-h}}{\ell^{j-h}} \frac{\varepsilon_h}{\varepsilon_j^2}.$$

我们用到了这样一个事实：当 $R_{s,b} = 1$, G_s 至多是 ε_h 在 $J|_h$中稠密时。将其代入上式可知，右侧（29）中的最后一项至多为

$$\sum_{i \le j \le r} \sum_{h=0}^{i-1} \sum_{a \in \mathcal{C}_s^{(i)}} \sum_{H \subseteq a, |H|=h} \frac{n^{j-h}}{\ell^{j-h}} \frac{\varepsilon_h}{\varepsilon_j^2} \le \sum_{i,j \le r} 2^i \cdot i \cdot \frac{n^{j-h}}{\ell^{j-h}} \frac{\varepsilon_h}{\varepsilon_j^2} \cdot |\mathcal{C}_s^{(i)}| \left(\frac{2\ell}{n}\right)^{i+j-h},$$

并且由于 $|\mathcal{C}_s^{(i)}| \le \frac{\delta(G_s\, n^i)}{\varepsilon_i^2 \ell^i}$根据命题 4.2，我们可以进一步将其上界估计为

$$\sum_{i,j \le r} 2^i \cdot i \cdot \frac{n^{i+j-h}}{\ell^{i+j-h}} \frac{\varepsilon_h \delta(G_s)}{\varepsilon_j^2 \varepsilon_i^2} \left(\frac{2\ell}{n}\right)^{i+j-h} \le 2^{3r+1} r^2 \delta(G_s) \max_i \frac{\varepsilon_{i-1}}{\varepsilon_i^4} \le 2^{6r} \max_i \frac{\varepsilon_{i-1}}{\varepsilon_i^4} \delta(G_s).$$

将这些相加 er s 可知，（29）中的最后一项对（28）的贡献至多为 2^{6r}最大值$_i \frac{\varepsilon_{i-1}}{\varepsilon_i^4}$。

对(29)中的第二项和第三项进行界定。这里我们使用定理 3.17。关键在于，集合 H_s 是伪随机的，因此我们可以很好地控制它与其他集合之间的边。

更准确地说，对于第二项，注意到 H_s 是 $(r,\ \varepsilon_r)$-伪随机的，符合定义 3.16，因此根据定理 3.17）取 $\gamma = \varepsilon_r$，我们得到:

$$\frac{|E(H_s)|}{|E(J)|} = \delta(H_s) - \langle H_s, LH_s \rangle \le 2\delta(H_s)(1-\alpha)^{r+1} \le 2\delta(G_s)(1-\alpha)^{r+1}, \tag{32}$$

其中，只要 $\varepsilon_r \le (1-\alpha)^{r+1}\exp(-r)$，第一个不等式就成立。注意，结构定理 $q_a(H_s)(\delta(H_s|_a) - \varepsilon_r)$ 中的第二项非正，因为 q_a 是平方和，且 H_s 是伪随机的。对应于布尔性的第三项 $B(H_s)$ 为 0，因为 $H_s^3(u) = H_s(u)$。对 s 求和可得，这部分对 (28) 右侧的贡献至多为 $2(1-\alpha)^{r+1}$。

(29) 中第三项的上界类似。我们有:

$$\frac{|E(H_s, D_s)|}{|E(J)|} = \langle D_s, JH_s \rangle \le \sqrt{\langle D_s, D_s \rangle \cdot \langle H_s, J^2 H_s \rangle} \le 2\delta(G_s)(1-\alpha)^{r+1}. \tag{33}$$

在最后一个不等式中，我们使用了 $\langle D_S、\ D_s \rangle \le \delta(G_s)$ 以及 $\langle H_s、\ J^2 H_s \rangle \le 2\delta(G_s)(1-\alpha)^{2(r+1)}$ 这恰好可由定理 3.17 按照上述方法推出。对 s 求和，可得总贡献至多为 $2(1-\alpha)^{r+1}$。

将证明转化为平方和证明：下面给出一个证明概要，说明如何将其转化为平方和证明。为避免布尔性误差，我们将多次应用 (34)，把 $R_{s,\ a}$ 替换为 $p_{\beta,\ \nu}$，并取平均。我们知道$R_{s,\ a} = p_1(\delta_1) \cdot \ldots \cdot p_t(\delta_t)$，其中 p_i 是近似指示函数 $p_{\beta_i,\ \nu}$（或 $p_{<\beta_i,\ \nu}$），而 δ_i 的形式为$\delta(G_s|_b)$，其中 $b \subseteq a$。然后定义 $R^c_{s,\ a}$为 $p^c_1(\delta_1) \cdot \ldots \cdot p^c_t(\delta_t)$，其中对所有 $c \in \{0, \ldots, \lfloor 1/\nu \rfloor\}$，$p^c_i(\delta_i) = p_{\beta_i + c\nu^2,\ \nu^2}$（分别为 $p_{<\beta_i+c\nu^2,\ \nu^2}$）。

注意，按所写形式，G_s's 和函数 $\#sat(G_s \cap J|_a)$ 都是实际指示函数，因为我们可以将 $G_s(u) = \mathrm{I}[X_s - X'_u = s]$ and $\mathrm{I}[e$ is 表示为关于 (X, X') 的多项式，且 $]$。定义 $H^c_s(u) = G_s(u)\prod_{a \subset u : |a| \le r}(1 - R^c_{s,\ a})$ 和 $D^c_s = G_s(u)(1 - H^c_{s,a})$。用 $R^c_{s,a}$ 定义稠密子立方体后，我们得到与 (29) 类似的结果：

$$\frac{\#sat(G_s)}{|E(J)|} \le \sum_{i \le r} \sum_{a \in \binom{[n]}{i}} R^c_{s,a} \frac{\#sat(G_s \cap J|_a)}{|E(J)|} + \langle H^c_s, AH^c_s \rangle + \langle D^c_s, JH^c_s \rangle$$
$$+ \sum_{i,j \le r} \sum_{h=0}^{\min(i,j)} \sum_{a \in \binom{[n]}{i}} R^c_{s,a} \sum_{H \subseteq a, |H| = h} \sum_{\substack{b \in \binom{[n]}{j} \\ a \ne b, a \cap b = H}} R^c_{s,b} \frac{|E(J|_a, J|_b)|}{|E(J)|}. \tag{34}$$

然后，我们对 $c \in \{0, \ldots, \lfloor 1/\nu \rfloor\}$ 取期望，再对 $s \in \Sigma$ 求和。

现在，我们可以使用相同的分析来给这些项分别求上界。第一项的分析照旧；我们得到一个 $\mathbb{E}_c[R^c_{s,a}]$ (而不是 $R_{s,\ a}$)，但我们会忽略这一细微差异，因为它不会影响对算法的最终分析。对于第二项，我们使用命题 4.2 的平方和版本（如原文所述），说明 $\mathbb{E}_{a \in \binom{[n]}{i}}[R^c_{s,a}]$ 很小，并采用与命题 4.2 平方和化时类似的技巧。对于第三项和第四项，我们对近似布尔函数 H_s 应用结构定理，并将布尔性项 $\mathbb{E}_c[\sum_s B(H^c_s)]$ 用 $|\Sigma|\ell^{O(r)}\sqrt{\nu}$ 来界定。此外，在第四项中，我们还应用柯西-施瓦茨不等式的平方和版本。我们省略这些细节，因为此前已经进行了类似的论证，但会在附录中的命题 $\mathbb{E}_c[\sum_s B(H^c_s)]$ B.1 中正式证明其上界。 □

4.2 主要引理

本节中，我们考虑完备性远低于 1、甚至可能非常接近 0 的 UG 实例。我们的算法分析只有一个步骤有所不同：证明移位势很大。

下面的命题断言，从我们的伪分布中取两个赋值 X, X'，同时被 X 和 X' 满足的边的期望数量仍然远大于 0：

命题 4.4. $\widetilde{\mathbb{E}}_{\mu \times \mu}[\mathrm{val}_I(X \wedge X')] \ge c^2$.

$$\begin{aligned}
\widetilde{\mathbb{E}}_{\mu \times \mu}[\mathrm{val}_I(X \wedge X')] &= \widetilde{\mathbb{E}}_{\mu \times \mu}\Big[\mathop{\mathbb{E}}_{e \sim E(G)}[\mathbb{1}(e \text{ satisfied by } X)\mathbb{1}(e \text{ satisfied by } X')]\Big] \\
&= \mathop{\mathbb{E}}_{e \sim E(G)}[\widetilde{\Pr_{\mu}}[e \text{ satisfied by } X]^2] \\
&\ge \mathop{\mathbb{E}}_{e \sim E(G)}[\widetilde{\Pr_{\mu}}[e \text{ satisfied by } X]]^2 \qquad \text{(by Cauchy-Schwarz)} \\
&= \mathrm{val}_\mu(I)^2.
\end{aligned}$$

引理 4.5。对于所有正常数 $c, \alpha, \tau \le 1$, $\nu = \frac{c^4}{|\Sigma|^2 \ell^{O(r)}}$，以及所有满足 $\ell \ge \Omega(r)$ $n \ge \ell$ 的整数，其中$r = \Theta(\log c \log(1-\alpha))$，以下结论成立：设 I 是定义在 $J_{n,\ell,\alpha}$ 上的一个仿射唯一博弈实例，且 μ 是一个伪分布

定义在 I 的赋值上的分布，其 $\mathrm{val}_\mu(I)$ 为 $\geq c$，且度至少为 $\ell^{O(r)}\mathrm{poly}(|\Sigma|$ $+\ell^{\mathrm{poly}(|\Sigma|\ell^r/c)}\,\mathrm{poly}(c))$。那么，存在一个大小为 $i \leq r$ 的限制 $a \subseteq [n]$，一个度为 $O(1/\nu)$ 的多项式 $P_a(X, X')$，它属于一个由 $|\Sigma|$ 个多项式组成的固定集合；还存在大小至多为 $\frac{\ell^{O(i)}|\Sigma|^2}{c^2\tau}$ 的子集 $A, B \subseteq V(J|_a)$ 以及字符串 y_A, y_B，使得将 μ 条件化于事件 $Y_A = y_A$ 和 $Y_B = y_B$ 后，得到度为 $\Omega(1/\nu)$ 的伪分布 μ_1 和 μ_2，满足：

1. $\mathcal{A}_I \vdash_{\widetilde{O}(1/\nu)} P_a(X, X') \in [0, 1]$.
2. $\widetilde{\mathbb{E}}_{\mu_1\times\mu_2}[\Phi^a_{\beta,\nu}(X, X')P_a(X, X')] \geq \frac{c^{\Omega(r)}}{\exp(r^2)}\widetilde{\mathbb{E}}[P_a(X, X')]$.
3. $\widetilde{\mathbb{E}}_{\mu_1\times\mu_2}[P_a(X, X')] \geq \Omega\left(\frac{c^2}{8r\ell^i|\Sigma|}\right)$.
4. $\mathbb{E}_{\substack{u_1,v_1\sim S:u_1\neq v_1\\ u_2,v_2\sim S:u_2\neq v_2}}[I(Y_{u_1,v_1}; Y_{u_2,v_2})] \leq \tau$.
5. $\mathbb{E}_{\substack{u_1,v_1\sim S:u_1\neq v_1\\ u_2,v_2\sim S:u_2\neq v_2}}[I(Y'_{u_1,v_1}; Y'_{u_2,v_2})] \leq \tau$,

其中 $\beta = \left(\mathrm{poly}(c)\exp(r)\right)^{r-i+1}$，$S = V(J|_a)$，$Y_{u,v} = (X_u, X_v, p_u, p_v)$，$Y'_{u,v} = (X'_u, X'_v, p'_u, p'_v)$，互信息是相对于局部分布集合 $\mathcal{L}(\mu_1 \times \mu_2, p_{\beta,\nu})$ 定义的。

证明。我们的策略是使用边覆盖定理。我们将在 $\mathbb{E}_{\mu\times\mu}$ 的不等式两边应用，并利用断言 4.4 说明 $\mathbb{E}[\mathrm{val}_I(X \wedge X')]$ 很大。

我们将在证明的最后设置参数，使得：r 足够大，从而 $4(1-\alpha)^{r+1} \leq c^2/6$，$\nu$ 足够小，从而 $|\Sigma|\ell^{O(r)}\sqrt{\nu} \leq c^2/6$ 并且 ε_i 满足 $2^{6r}\max_i \frac{\varepsilon_{i-1}}{\varepsilon_i^4} \leq c^2/6$，此外 ε_i 满足定理 4.3 的条件。因此，定理 4.3 中的误差项很小，

$$\mathsf{err} = 4(1-\alpha)^{r+1} + 2^{6r}\max_i \frac{\varepsilon_{i-1}}{\varepsilon_i^4} + |\Sigma|\ell^{O(r)}\sqrt{\nu} \leq \frac{c^2}{2}. \tag{35}$$

在定理 $\mathbb{E}_{\mu\times\mu}$ 两边应用 4.3 (假设 $\deg(\mu) \geq \ell^{\mathrm{poly}(\ell^r/\nu)}$)，并利用命题 4.4 对左边的伪期望取下界，可得：

$$c^2 \leq \widetilde{\mathbb{E}}_{\mu\times\mu}[\mathrm{val}_I(X \wedge X')] \leq \sum_{i\in[r]}\widetilde{\mathbb{E}}_{\mu\times\mu}[T_i(X, X')] + \mathsf{err} \leq \sum_{i\in[r]}\widetilde{\mathbb{E}}_{\mu\times\mu}[T_i(X, X')] + \frac{c^2}{2},$$

因此，我们得到存在一个 $i \in [r]$，使得 $\mathbb{E}_{\mu\times\mu}[T_i(X, X')] \geq c^2/2r$，于是

$$\widetilde{\mathbb{E}}_{\mu\times\mu}\mathbb{E}_{a\sim\binom{[n]}{i}}[\sum_s R_{s,a}\mathbb{E}_{u\sim J|_a}[G_s(u)\mathrm{val}^a_u(X \wedge X')]] \geq \frac{c^2}{2r\ell^i}. \tag{36}$$

我们的目标是对 $\mathbb{E}_{\mu\times\mu}$ 进行条件化，条件是选取一个适当的多项式（如引理 3.20 的证明中所做的那样），从而使所得的伪期望算子满足：$\mathbb{E}'[\mathbb{E}_{u\sim J|_a}[G_s(u)\mathrm{val}^a_u(X \wedge X')]] \geq \Omega(c^2/r)$ 对于某个特定的 i-限制 a。为此，我们将 $\mathbb{E}_{\mu\times\mu}$ 应用于命题 4.2，并对 s 求和，得到

$$\widetilde{\mathbb{E}}_{\mu\times\mu}\left[\mathbb{E}_{a\sim\binom{[n]}{i}}\sum_s R_{s,a}\right] \leq \frac{4}{\varepsilon_i^2\ell^i} + O(|\Sigma|\nu) \leq \frac{5}{\varepsilon_i^2\ell_i},$$

其中，对于最后一个不等式，我们假设了 $\nu \le O(1/\ell^i|\Sigma|)$。

我们将等式右侧拆分为 36，得到 $c^2/4r\ell^i + c^2/4r\ell^i$；其中在第一项中，我们进一步使用上面的等式：$1/\ell^i \ge \frac{\varepsilon_i^2}{5} \widetilde{\mathbb{E}}_{\mu\times\mu}[\mathbb{E}_{a\sim\binom{[n]}{i}}[\sum_s R_{s,a}]]$，从而得到：

$$\widetilde{\mathbb{E}}_{\mu\times\mu}\mathbb{E}_{a\sim\binom{[n]}{i}}\left[\sum_s R_{s,a}\mathbb{E}_{u\sim J|_a}[G_s(u)\mathrm{val}_u^a(X\wedge X')]\right] \ge \frac{c^2\varepsilon_i^2}{20r}\widetilde{\mathbb{E}}_{\mu\times\mu}\left[\mathbb{E}_{a\sim\binom{[n]}{i}}[\sum_s R_{s,a}]\right] + \frac{c^2}{4r\ell^i},$$

重新整理后

$$\widetilde{\mathbb{E}}_{\mu\times\mu}\mathbb{E}_{a\sim\binom{[n]}{i}}\left[\sum_s R_{s,a}\left(\mathbb{E}_{u\sim J|_a}[G_s(u)\mathrm{val}_u^a(X\wedge X')] - \frac{c^2\varepsilon_i^2}{20r}\right)\right] \ge \frac{c^2}{4r\ell^i}.$$

取平均后，我们得到一个 $a\in\binom{[n]}{i}, s\in\Sigma$，使得：

$$\widetilde{\mathbb{E}}_{\mu\times\mu}\left[R_{s,a}\left(\mathbb{E}_{u\sim J|_a}[G_s(u)\mathrm{val}_u^a(X\wedge X')] - \frac{c^2\varepsilon_i^2}{20r}\right)\right] \ge \frac{c^2}{4r\ell^i|\Sigma|}. \tag{37}$$

最后一个结果与引理 3.20 证明中的等式（10）相同，它是完备性接近 1时的对应结论。证明的其余部分与引理 3.20的证明其余部分基本相同，概要如下。

应用引理 3.19 后，我们得到伪分布 μ_1，μ_2 其全局相关性较低（符合引理第 4、5 点的要求）：

$$\widetilde{\mathbb{E}}_{\mu_1\times\mu_2}\left[R_{s,a}\left(\mathbb{E}_{u\sim J|_a}[G_s(u)\mathrm{val}_u^a(X\wedge X')] - \frac{c^2\varepsilon_i^2}{20r}\right)\right] \ge \frac{c^2}{8r\ell^i|\Sigma|}. \tag{38}$$

令 $P_a(X,X') = R_{s,a}(X,X')$，容易验证：

$$\mathcal{A}_I \vdash_{\widetilde{O}(\exp(i)/\nu)} P_a(X,X')\in[0,1], \text{ and } \widetilde{\mathbb{E}}_{\mu_1\times\mu_2}[P_a(X,X')] \ge \frac{c^2}{8r\ell^i|\Sigma|},$$

这证明了引理陈述中的第 1 点和第 3 点。剩下唯一需要验证的是，条件化$\mu_1\times\mu_2$ 于 $R_{s,a}$ 会使 $J|_a$ 上的移位划分势变大。回顾一下，$J|_a$ 上的移位划分势为：$\phi^a_{\beta,\nu}(X,X') = \sum_s \mathbf{E}_{u\sim J|_a}[G_s(u)p_{\beta,\nu}(\mathrm{val}_u^a(X))p_{\beta,\nu}(\mathrm{val}_u^a(X'))]^2$。由方程（38）可知，条件化 $\mu_1\times\mu_2$ 于 $R_{s,a}$ 得到：

$$\widetilde{\mathbb{E}}_{\mu_1\times\mu_2|R_{s,a}}[\mathbb{E}_{u\sim J|_a}[G_s(u)\mathrm{val}_u^a(X\wedge X')]] \ge \frac{c^2\varepsilon_i^2}{20r}.$$

我们可以证明，对于 $x\in[0,1] \vdash_{\widetilde{O}(1/\nu)} x \le p_{\beta,\nu}(x) + \beta + O(\nu)$（使用第 2.3.2 节中的标准方法）。将此结果应用于 $\mathrm{val}_u^a(X\wedge X')$ 和 $\beta = \frac{c^2\varepsilon_i^2}{40r}$，并进一步注意到 $p_{\beta,\nu}(\mathrm{val}_u^a(X\wedge X')) \le p_{\beta,\nu}(\mathrm{val}_u^a(X))p_{\beta,\nu}(\mathrm{val}_u^a(X')) + O(\nu)$，得到：

$$\widetilde{\mathbb{E}}_{\mu_1\times\mu_2|R_{s,a}}[\mathbb{E}_{u\sim J|_a}[G_s(u)p_{\beta,\nu}(\mathrm{val}_u^a(X))p_{\beta,\nu}(\mathrm{val}_u^a(X'))]] \ge \frac{c^2\varepsilon_i^2}{40r} - O(\nu).$$

应用柯西-施瓦茨不等式可得：

$$\widetilde{\mathbb{E}}_{\mu_1\times\mu_2|R_{s,a}}[\mathbb{E}_{u\sim J|_a}[G_s(u)p_{\beta,\nu}(\mathrm{val}_u^a(X))p_{\beta,\nu}(\mathrm{val}_u^a(X'))]^2] \ge \Omega\left(\frac{c^4\varepsilon_i^4}{r^2}\right).$$

将对应其他 $s \in \Sigma$ 的项相加，我们立即得到：

$$\widetilde{\mathbb{E}}_{\mu_1 \times \mu_2 | R_{s,a}} [\phi^a_{\beta,\nu}(X, X')] \geq \Omega\left(\frac{c^4 \varepsilon_i^4}{r^2}\right). \tag{39}$$

根据上述所有要求设置 r、ε_i、ν，即可完成证明。

参数设置：为了使（35）中的 err 足够小，我们设置 $r = \Theta(\log_c \log(1-\alpha))$、$\nu = \frac{c^4}{|\Sigma|^2 \ell^{O(r)}}$、$\varepsilon_{j-1} = \varepsilon_j^5 / 2^{6r}$，其中 $\varepsilon_r = \Theta(c^2 \exp(-r))$。我们需要 $\beta = c^2 \varepsilon_i^2 / 40r$，其等于 $(\mathrm{poly}(c)/\exp(r))^{r-i+1}$。我们可以设置 $\deg(\mu) = \ell^{\mathrm{poly}(\ell^r/\nu)} = \ell^{\mathrm{poly}(|\Sigma|\ell^r/c)}$，使得可以应用边覆盖定理。此外，应用引理 3.19 时，我们需要 $\deg(\mu) \geq \Omega(\log |\Sigma| / p\tau\nu)$，其中 $p = c^2/4r\ell^i|\Sigma|$，因此只需取 $\deg(\mu) = \ell^{O(r)} \mathrm{poly}(|\Sigma|) \mathrm{poly}(c)_\tau$。可以验证，这些参数足以使证明中其余陈述成立。由（39）可得，条件化移位划分势至少为 $\Omega(c^2 \varepsilon_i^4 / r^2) \geq c^{O(r)} \exp(r)$，证明至此完成。 □

4.3 定理 1.6 的证明

针对任意完备性的算法与针对接近 1 的完备性的算法相同，只是主算法的参数 r、δ、D、γ 和 SubRound 的参数 t、τ、β、ν 设置不同。根据引理 4.5，算法分析的其余部分完全保持不变。我们将在下文设置这些参数，但省略算法的描述。该算法的保证可能比针对接近 1 的完备性的算法更差（运行时间为 $\approx n^{\ell^{\mathrm{poly}(\ell)}}$，近似比为 $\approx c^{O(\log 1/c)}$），但需要注意的重要一点是，运行时间关于 n 是多项式的（只要 ℓ、$|\Sigma|$ 是 $O(1)$），而近似比仅取决于 c，不取决于 ℓ、n 或 $|\Sigma|$。

定理 4.6. 对所有正常数 $c \in (0, 1]$，$\alpha \in \mathbb{Q}$，以及所有满足 $\alpha\ell \in \mathbb{N}$ 且 $r = \Theta_{\log c \log(1-\alpha)}$ 的整数 $\ell \geq \Omega(r)$，当 n 足够大时，算法 *3.4*（采用下文给出的修改后参数设置）具有以下保证：若 I 是定义在具有字母表 Σ 的 (n, ℓ, α)-Johnson 图 J 上的仿射唯一博弈实例，且 $\mathrm{val}(I) = c$，则算法 *3.4* 在时间 $|V(J)|^D$ 内返回一个满足赋值，使得其满足率为 $\Omega\left(\frac{c^{\Omega(r)}}{r^2 \exp()}\right)$，其中 $D = \frac{\ell^{\mathrm{poly}(|\Sigma|\ell^r/c)}}{c^{O(r)}}$。

证明。令 $r = \Theta(\log_c \log(1-\alpha))$。根据引理 4.5 中的 $\mu_1 \times \mu_2$，对于 $i \leq r$-受限子立方体 $a \subseteq [n], P_a(X, X')$，我们有 $\Phi^a_{\beta,\nu}(\mu_1 \times \mu_2 | P_a) \geq c^{\Omega(r)} \exp(r^2)$，因此应用引理 3.10，其中 $S = J|_a$，多项式 $E(X, X') = P_a(X, X')$，参数为 $\beta = \left(\frac{\mathrm{poly}(c)}{r} \exp(\,)\right)^{r-i+1}$，$\nu = \frac{c^4}{|\Sigma|^2 \ell^{O(r)}}$，$\delta = c^{O(r)} \exp(r^2)$ $p = \Omega\left(\frac{c^2}{8r\ell^i|\Sigma|}\right)$，以及 $\tau = c^{O(r)} \exp(r^2) \ell^{O(i)} |\Sigma|_\circ$ 参数 τ 的选取满足 $O(\frac{\sqrt{\tau}+1/|S|}{p\delta^2}) = c^{O(r)} \exp(r^2)$，因此我们可以应用舍入引理（引理 3.11），取 $\zeta = c^{O(r)} \exp(r^2)$ 和 $\gamma = c^{\Omega(r)} \exp(r^2)$，并使用相同的 β, ν, δ 设置。这表明存在一个子立方体 $a \in \binom{[n]}{i}$，其 SubRound 子轮值至少为 $c^{\Omega(r)} \exp(r^2)$，前提是 $\deg(\mu) \geq \ell^{O(r)} \mathrm{poly}(\frac{|\Sigma|}{\tau} + \ell^{\mathrm{poly}(|\Sigma|\ell^r/c)}) \mathrm{poly}(c))$。因此，只需令 μ 的度等于 $D = \frac{\ell^{\mathrm{poly}(|\Sigma|\ell^r/c)}}{c^{O(r)}}$。

通过将 SubRound 用作子程序，我们应用迭代引理3.12完成该定理的证明，其完备性为 $c, \gamma = c^2$，$\delta = c^{\Omega(r)} \exp(r^2)$，且 $r = \Theta(\log_c \log(1-\alpha))$，从而使 $(1-\alpha)^r = \mathrm{poly}(c)$。我们可以验证，SubRound（采用上述参数设置）满足该引理的假设：它能找到

一个 $\leq r$-受限子立方体及其上的一个赋值，其值为 $\Omega(\delta)$，耗时 $|V(J)|^D$（其中 D 是上文的次数上界）。由此可知，算法 3.4 会在$|V(G)|^{O(D)}$时间内输出一个值至少为 $\Omega\left(\frac{c^{\Omega(r)}}{r^2\exp()}\right)$ 的赋值。

□

5 Af其他全局超收缩图上的精细唯一游戏 s

本节将说明如何将第 3、4 节中的技术推广到一般的全局超收缩图。我们首先给出全局超收缩性的半形式化定义，并概述算法的各个步骤。我们此前虽以 Johnson 图为例陈述了该算法，但只要有全局超收缩性的平方和证书，该算法也适用于一般图。随后，我们将具体说明定理 1.7 和1.8 的证明：针对格拉斯曼图以及在高维扩展体上进行随机游走的唯一游戏算法。

5.1 算法的组成部分

用于证明定理 4 的各个组成部分，以及它们之间的相互作用，可以抽象如下。1.6

1. 全局超收缩性。算法的第一个组成部分是一个全局超收缩不等式（或其推论）。该结果断言，对于底层图 G，对于所有$\gamma > 0$，存在 $r \in \mathbf{N}$、ε_0、.....、ε_r、ζ、$\eta > 0$，以及一族 $\mathcal{C} = \mathcal{C}_0 \cup \ldots \cup \mathcal{C}_r$ 顶点集合（这些集合是基本集合的组合），满足以下性质：

(a) $\mathcal{C}$ 由非扩张集组成：G 中每条 $C \in \mathcal{C}$ 的边扩张为 $1-\zeta$。

(b) $\mathcal{C}$ 解释了所有扩张效果不佳的小集合。该性质的一种基本形式是：集合$S \subseteq V(G)$若在 $\mathcal{C}$的任何集合中都不稠密，即对于所有 $C \in \mathcal{C}$，都有 $\delta(S \cap C) \leq \varepsilon_1 \delta(C)$，则其扩张接近 1，也就是说，$\Phi(S) \geq 1-\gamma$。

该性质的一个更强版本通常可由上述性质推出（本文所关注的所有图都属于这种情况），并且定理 1.5 的证明中用到了这一版本：可以利用其中 S 稠密的 $C \in \mathcal{C}$，捕获 S 的一个常数比例。等价地，该性质表明，对于顶点集合 $S \subseteq V(G)$，取 $\mathcal{C}' = \{C \in \mathcal{C} \mid C \in \mathcal{C}_i,\ \delta(S \cap C) \geq \varepsilon_i \delta(C)\}$ 并定义$C' = \bigcup_{C \in \mathcal{C}'} C$，若 $\delta(S \cap C') \leq \eta\delta(S)$，则 $\Phi(S) \geq 1-\gamma$。

全局超收缩性的一种更强形式，在我们关心的情形下同样可以由最基本的形式推出，这就是边覆盖定理。我们在定理 1.6 的证明中使用了这种形式的全局超收缩性。非正式地说，这一结果表明，不仅可以用来自 $\mathcal{C}$ 的非扩张集合覆盖 S 中相当大的一部分，且这些集合中 S 是稠密的；事实上，还可以利用 $C \in \mathcal{C}$ 捕获几乎所有留在 S 内的边。更精确地说，该结果断言，我们可以选取 $\mathcal{C}'' \subseteq \mathcal{C}'$，使其满足以下性质：

i. 边覆盖：在 S 内抽样一条边 (u,v)，除概率为 ξ 的情况外，(u,v) 是某个 $C'' \subseteq \mathcal{C}''$ 内的一条边。ii. 最大稠密：换言之，这意味着每个 $C'' \in \mathcal{C}''$ 在 $\mathcal{C}$ 中都不存在这样的 $C \supsetneq C''$，使得 S 有一定程度的稠密。形式上，我们要求对于所有满足 $C_j \supseteq C''$ 的 $i = 1, \ldots, r$, $C'' \in \mathcal{C}'' \cap \mathcal{C}_i$, $j < i$ 和 $C_j \in \mathcal{C}_j$，均有 $\delta(S \cap C_j) < \varepsilon_j \delta(C_j)$。

边覆盖定理使我们能够论证，在我们的移位划分 $F_s(X, X') = \{v \in V \mid X(v) - X'(v) = s\}$ 中，我们可以利用来自 $\mathcal{C}$ 的基本集合，捕获几乎所有留在某个 F_s 内的边。在

尤其是，由于同时满足 X 和 X' 的边占边的一个常数比例，且它们都位于某个 F_s 内，这意味着我们可以用来自 $\mathcal{C}$ 的集合捕获几乎所有这些边。

2. 通过初等论证可知，存在这样的 $C \in \mathcal{C}$ 和 s，使得 F_s 以显著的概率在 C中变得稠密，并且在 C 内部，有一个常数比例的边同时被 X 和X'满足。在我们的论证中，我们考虑这一事件（在我们的算法中，为了将讨论限制在平方和的范围内，我们用多项式 $P_a(X, X')$ 对它进行近似）。正如我们在引言中所解释的，这种条件化可能会在 X 和 X' 之间产生相关性，导致我们的舍入技术无法奏效。

为了解决这一问题，我们证明了：

(a) 消除全局相关性： 通过使用条件化（如 [RT12]中所示），我们能够确保我们关注的两组随机变量 $, \{Z'_{u,v}\}_{u,\ v\in C}$（它们涉及赋值 X 和 X' 在顶点 u, v上的局部信息）大致两两独立。（b）条件化基本上保留独立性：由于事件 C 在 F_s 中变得稠密的概率显著，而且 $\{Z_{u,v}\}_{u,\ v\in C}$,$\{Z'_{u,v}\}_{u,\ v\in C}$ 起初两两独立，我们论证这种条件化不会在（$Z_{u,\ v}$,$Z'_{u,\ v}$）之间产生过多依赖关系。

3. 舍入。接着，我们给出了一个针对子立方体 C 和伪分布 $\mathcal{D}$ 的舍入过程。平均而言（对 $\mathcal{D}$ 取平均），我们设想的赋值 X、X' 满足了常数比例的边（通过移位划分势这一概念形式化），移位划分中的某个部分 F_s 很大，并且在该部分上，某些随机变量 $\{(Z_{u,\ v}$、$Z'_{u,\ v})\}_{u,\ v}$ 之间近似独立。舍入过程的输出是对 C 的顶点的一种赋值，它满足其中常数比例的约束。

4. 迭代结果。所谓迭代结果，是指这样一种结果：如果我们有一个如上所述的过程，能够找到一个 $C \in \mathcal{C}$，并找到一种对 C 的顶点的赋值，使其满足其中常数比例的约束，那么我们就可以迭代该过程，从而满足整个图中常数比例的约束。

这是通过对与 C 相 incident 的边进行随机化来实现的，这确保了我们之后找到的任何 C' 与此前找到的 C 都只有可忽略的重叠。其思路是，我们找到的任何 C 都至少有 δ 的相连边留在其内部；我们能够满足其中常数比例的边，因此最终能够满足与 C 相连的常数比例的边。作为回报，我们会对与 C 相连的边进行随机化，从而实际上放弃这些边带来的目标值。关键在于，我们成功满足的边数与放弃的边数之比为 $\Omega(1)$，因此经过几轮迭代后，在实例的目标值下降过多之前，我们就能满足此前常数比例的边。

在这 4 个组成部分中，第二、第三和第四部分适用于我们关注的任何图。事实上，相关性消除和条件化完全是通用的，而舍入过程只取决于约束是否为仿射。至于第四部分，它只依赖于我们的结构定理所保证的族 $\mathcal{C}$ 的性质，在其他方面也是通用的。

接下来我们讨论第一个组成部分，即全局超收缩不等式。为使讨论具体，我们考虑其最基本的形式。这个结果表明，一个集合 S 若在任何 $C \in \mathcal{C}$ 中都不稠密，就具有较大的扩张；而对于我们感兴趣的所有图，这类结果都已得到证明[KMMS18、KMS18、FKLM20、KLLM21、BHKL22b、GLL22]。要使这类结果能够导出算法，

我们还要求这一部分的证明属于常数度的平方和证明系统（上述所有例子都满足这一点，但原则上也可能不满足）。

对于 Johnson 图，集合 $\mathcal{C}$ 就是基本集合的集合

$$\mathcal{C} = \{J|_a \mid |a| \le r\}, \qquad \text{where } J|_a = \left\{ u \in \binom{[n]}{\ell} \;\middle|\; u \supseteq a \right\},$$

全局超收缩不等式的基本形式来自 [KMMS18]（附录中我们给出了该证明的平方和版本），并且我们已在第4 节说明了如何以黑盒方式由此推出边覆盖定理。

5.2 格拉斯曼图上的算法

现在我们来解释上述关于格拉斯曼图的第一个组成部分，该部分已在 [KMS18]中建立。回顾一下，格拉斯曼图 Grass(n,ℓ) 是一个图，其顶点为所有 ℓ维子空间$L \subseteq \mathbb{F}_2^n$，并且当$(L, L')$ 满足条件$\dim(L \cap L') = \ell - 1$时，它们之间有一条边。

在格拉斯曼图 Grass(n,ℓ) 中，我们有以下两个基本集合

$$Z_x = \{L \mid x \in L\} \text{ for } x \in \mathbb{F}_2^n, \qquad Z'_W = \{L \mid L \subseteq W\} \text{ for a hyperplane } W \subseteq \mathbb{F}_2^n,$$

利用它们，我们可以像上文那样定义集合 $\mathcal{C}_0$、……、$\mathcal{C}_r$ 和 $\mathcal{C} = \mathcal{C}_0 \cup \ldots \cup \mathcal{C}_r$。具体而言，对于子空间 $X \subseteq \mathbb{F}_2^n$，我们定义 $Z_X = \cap_{x \in X} Z_x$；对于子空间 $W \subseteq \mathbb{F}_2^n$，我们定义 $Z'_W = \cap_{W' \supseteq W} Z_{W'}$，于是

$$\mathcal{C}_m = \bigcup_{m_1+m_2=m} \left\{ Z_X \cap Z'_W \;\middle|\; \dim(X) = m_1, \dim(W) = n - m_2, X \subseteq W \right\}.$$

[KMS18] 的结果表明，对于所有 $\gamma > 0$，都存在 $r \in \mathbb{N}$ 和 $\varepsilon > 0$，使得如果 S 是 Grass(n,ℓ) 中的一个顶点集合，且对所有 $C \in \mathcal{C}$ 都有 $\delta(S \cap C) \le \varepsilon \delta(C)$，那么 $\Phi(S) \ge 1 - \gamma$。事实上，同样的证明表明，对于有界函数也成立一个稍微更一般的结论：如果 $F\colon V(\text{Grass}(n,\ell)) \to [0,1]$ 满足 $\mathbb{E}_x[F(x)^2 1_{x \in C}] \le \varepsilon \mathbb{E}_x[1_{x \in C}]$，那么

$$\langle F, TF \rangle \ge (1 - \gamma) \mathop{\mathbb{E}}_x [F^2(x)].$$

其中 T是 Grass(n,ℓ) 的归一化邻接矩阵。此外，由于证明中的每一步都使用了诸如 Parceval、柯西-施瓦茨不等式和 H¨older 不等式等关于变量 F 的多项式不等式，因此可以看出该证明可用 SoS 证明。我们在第 C 节中恰好使用了这些不等式，为 Johnson 图的全局超收缩性构造了一个平方和证书（定理 3.17）。事实上， [KMS18] 对 Grassmann 图的证明与 [KMMS18] 对 Johnson 图的证明非常相似，因此也可以类似地为 Grassmann 图构造一个平方和证书。

根据这一结果，可以沿用定理4.3的思路，以黑箱方式推导出格拉斯曼图的边覆盖定理：

定理5.1. 对所有 $\eta > 0$，存在 $r \in \mathbb{N}$ 和 ε_0、……、$\varepsilon_r > 0$，使得给定集合 $S \subseteq \text{Grass}(n,\ell)$，可以找到 $\mathcal{C}'_i \subseteq \mathcal{C}_i$，使得

1. 对于每个 i 和 $C \in \mathcal{C}'_i$，都有 $\delta(S \cap C) \ge \varepsilon_i \delta(C)$。
2. 对于 $\tilde{S} = \bigcup_{i=0}^{r} \bigcup_{C \in \mathcal{C}_i} C$，有

$$\Pr_{(L,L') \in E(\text{Grass}(n,\ell))} \left[L, L' \in S \wedge (L \notin \tilde{S} \text{ or } L' \notin \tilde{S}) \right] \le \eta \delta(S).$$

3. 对于所有满足 $C_j \supseteq C_i$ 的 $j < i$、$C_i \in \mathcal{C}'_i$ 和 $C_j \in \mathcal{C}_j$，都有 $\delta(S \cap C_j) \le \varepsilon_j \delta(C_j)$。

证明概要。我们令 ε_0，……，ε_r 待定；对我们而言，唯一重要的是 ε_r 足够小。令 $\mathcal{C}'_i$ 为所有满足 $\delta(S \cap C_i) \ge \varepsilon_i \delta(C_i)$ 的 $C_i \in \mathcal{C}_i$ 的集合，并且不存在 j 和 $C_j \in \mathcal{C}_j$ 使得 $C_j \supseteq C_i$ 且 $\delta(S \cap C_j) \ge \varepsilon_j \delta(S)$。

令 $F = 1_S$，$\tilde{F} = 1_{\tilde{S}}$，并注意 $G = F(1-F) = 1_{S \cap \overline{\tilde{S}}}$ 是 (r, ε_r) 根据 [KMS18]，的定义是伪随机的，因此 $\Phi(S \cap \overline{\tilde{S}}) \ge 1 - \eta^2/100$，前提是 ε_r 足够小。注意

$$\Pr_{(L,L') \in E(\mathsf{Grass}(n,\ell))} \left[L, L' \in S \wedge (L \notin \tilde{S} \text{ or } L' \notin \tilde{S}) \right] \le 2 \mathop{\mathbb{E}}_{(L,L')} [F[L]F[L'](1 - \tilde{F}[L])],$$

这等于 $2\langle G, TF \rangle$，其中 T 是带自环的格拉斯曼图的邻接算子。我们可以给出如下界：

$$\begin{aligned} \langle G, TF \rangle = \langle TG, F \rangle \le \|TG\|_2 \|F\|_2 = \sqrt{\langle TG, TG \rangle} \|F\|_2 \le \sqrt{\langle G, TG \rangle} \|F\|_2 \\ = \|G\|_2 \sqrt{1 - \Phi(S \cap \overline{\tilde{S}})} \|F\|_2. \end{aligned}$$

我们用到了 T 是半正定的这一事实。显然 $\|G\|_2, \|F\|_2 \le \sqrt{\delta(S)}$，因此得到 $\langle G, TF \rangle \le \delta(S) \frac{\eta}{10}$，代入上式即可得到第二项。 □

将这一结果调整到移位划分的情形，并按照标准方式将其表述为平方和陈述，可得到格拉斯曼图的定理 4.3的一个类似结果。为此，必须处理跨越不同 C_i 的边，并证明它们的贡献很小。为此，需要选择ε_i，使其远小于 ε_{i+1}，并且在 $\mathcal{C}'_i$ 中只纳入 $C_i \in \mathcal{C}_i$ 最大稠密的部分，然后在界定其中最后一项时，重复定理 4.3 中类似的计算。

接下来，我们的算法完全按照相同的方式进行。

5.3 高维扩展体的算法

本节考虑定义在双侧局部谱扩张图上的高阶游走所对应的唯一游戏实例，并讨论为何我们关于 Johnson 图（可视为完全复形上的部分交换游走）的结果可以推广到高维扩展体。关于高维扩展体的精彩介绍，请参阅 [DDFH18] 。

具体而言，考虑一个双侧局部谱扩张复形 X，以及其上深度为 α 的 $X(\ell)$ 部分交换游走。这种随机游走自然对应于定义在顶点 $X(\ell)$ 上的图 G。给定 G，与 Johnson 图中的子立方体类似，复形中有一族称为链接的基本集合。 [BHKL22b], [GLL22]推广了 [KMMS18] 的结果，证明了高维扩展体上的全局超收缩性；特别是，他们表明， G 中的任何非扩张集合在某个链接中的密度都必须是一个较大的常数。他们得到的参数与 [KMMS18] 对 α-噪声 Johnson 图的陈述中的参数相同。事实上， [BHKL22b] 的证明完全沿用了 [KMMS18] 的思路，因此很容易看出，可以用平方和证明的方法得到高维扩展体上定理 3.17 的对应结论。类似地，也可以得到高维扩展体上更强的边覆盖定理（对应于定理 4.3），这里省略细节。

幸运的是， [BHKL22a] 将 [BBK+21] 的算法推广，得到了适用于高维扩展体的唯一博弈算法，尽管它也存在与 [BBK+21] 相同的两个缺点—— ℓ可靠性保证依赖于ε，且要求完备性接近于 1。[BHKL22a] 由此展示了 [BBK+21] 框架的普适性，并说明它并不依赖约翰逊图的对称性或正则性，因为高阶

游走可以发生在不规则稀疏且高度非对称的图上。我们也可以按照第5.1节概述的步骤，将 Johnson 结果推广为适用于高维扩展体上唯一博弈的算法。总而言之，其中的组成部分 1——高维扩展体的全局超收缩性平方和证书——可以使用[BHKL22b],获得；组成部分 2 和 3 适用于所有图，而组成部分 4 是一个迭代结果，我们可以像 [BHKL22a]中的迭代结果那样得到。

致谢

我们感谢 Boaz B arak 在本项目初期进行的富有见地的讨论并给予鼓励。

参考文献

[AIMS10] Sanjeev Arora、Russell Impagliazzo、William Matthews 和 David Steurer，《通过分治改进唯一游戏算法》，电子计算复杂性讨论会 17（2010年），41。[AKK+08] Sanjeev Arora、Subhash Khot、Alexandra Kolla、David Steurer、Madhur Tulsiani 和 Nisheeth K. Vishnoi，《扩展约束图上的唯一游戏很容易：扩展摘要》，第40届ACM计算理论研讨会论文集，加拿大不列颠哥伦比亚省维多利亚，2008年5月17日至20日，2008年，第21–28页。[Aus07] Per Austrin，《平衡最大 2-SAT 可能并非最难问题》，第39届ACM计算理论研讨会论文集，圣迭戈，加利福尼亚州，美国，2007年6月11日至13日（David S. Johnson 和 Uriel Feige 编），ACM，2007年，第189–197页。[BBK+21] Mitali Bafna、Boaz Barak、Pravesh K. Kothari、Tselil Schramm 和 David Steurer，《在经认证的小集合扩展图上玩唯一游戏》，STOC ’21：第53届ACM SIGACT计算理论研讨会，线上活动，意大利，2021年6月21日至25日，ACM，2021年，第1629–1642页。[BDH+20] Ainesh Bakshi、Ilias Diakonikolas、Samuel B. Hopkins、Daniel Kane、Sushrut Karmalkar 和 Pravesh K. Kothari，《高斯分布及其他非球形混合分布的离群值鲁棒聚类》，第61届IEEE计算机科学基础年会，FOCS 2020，美国北卡罗来纳州达勒姆，2020年11月16日至19日，IEEE，2020年，第149–159页。[BDJ+22] Ainesh Bakshi、Ilias Diakonikolas、He Jia、Daniel M. Kane、Pravesh K. Kothari 和 Santosh S. Vempala，《鲁棒地学习由 k 个任意高斯分布组成的混合分布》，STOC ’22：第54届ACM SIGACT计算理论年度研讨会，意大利罗马，2022年6月20日至24日，ACM，2022年，第1234–1247页。[BHKL22a] Mitali Bafna、Max Hopkins、Tali Kaufman 和 Shachar Lovett，《高维扩张图：特征值剥离、伪随机性与唯一游戏》，2022年 ACM-SIAM 离散算法研讨会论文集，SODA 2022，线上会议／美国弗吉尼亚州亚历山大市，2022年1月9日至12日，2022年，第1069–1128页。[BHKL22b] Mitali Bafna、Max Hopkins、Tali Kaufman 和 Shachar Lovett，《高维扩张图上的超收缩性》，第54届ACM SIGACT计算理论年度研讨会论文集，2022年，第185–194页。

[BKS14] Boaz Barak、Jonathan A. Kelner 和 David Steurer，《平方和松弛的舍入》，计算理论研讨会，STOC 2014，美国纽约州纽约市，2014年5月31日至6月3日，2014年，第31–40页。[BKS17] Boaz Barak、Pravesh K. Kothari 和 David Steurer，《量子纠缠、平方和与对数秩猜想》，第49届ACM SIGACT计算理论年度研讨会论文集，STOC 2017，加拿大魁北克省蒙特利尔，2017年6月19日至23日，2017年，第975–988页。[BKS22] Rares-Darius Buhai、Pravesh K. Kothari 和 David Steurer，《逼近半随机植入团阈值的算法》，CoRR abs/2212.05619（2022年）。[BRS11] Boaz Barak、Prasad Raghavendra 和 David Steurer，《通过全局相关性舍入半正定规划层级》，IEEE第52届计算机科学基础年度研讨会，FOCS 2011，美国加利福尼亚州棕榈泉，2011年10月22日至25日，2011年，第472–481页。[BS14] Boaz Barak 和 David Steurer，《平方和证明与迈向最优算法的探索》，arXiv 预印本 arXiv:1404.5236（2014年）。[DDFH18] Yotam Dikstein、Irit Dinur、Yuval Filmus 和 Prahladh Harsha，《高维扩张图上的布尔函数分析》，《近似、随机化与组合优化：算法与技术》（APPROX/RANDOM 2018），Schloss Dagstuhl-Leibniz 信息学中心，2018年。[DGJ+10] Ilias Diakonikolas、Parikshit Gopalan、Ragesh Jaiswal、Rocco A Servedio 和 Emanuele Viola，《有界独立性无法愚弄半空间》，SIAM计算杂志 39（2010年），第8期，3441–3462。[DKK+18a] Irit Dinur、Subhash Khot、Guy Kindler、Dor Minzer 和 Muli Safra，《关于格拉斯曼图中非最优扩张的集合》，第50届ACM SIGACT计算理论年度研讨会论文集，STOC 2018，美国加利福尼亚州洛杉矶，2018年6月25日至29日（Ilias Diakonikolas、David Kempe 和 Monika Henzinger 编），ACM，2018年，第940–951页。[DKK+18b] Irit Dinur、Subhash Khot、Guy Kindler、Dor Minzer 和 Muli Safra，《迈向证明 2对1游戏猜想？》，第50届ACM SIGACT计算理论年度研讨会论文集，2018年，第376–389页。[FKLM20] Yuval Filmus、Guy Kindler、Noam Lifshitz 和 Dor Minzer，《对称群上的超收缩性》，arXiv 预印本 arXiv:2009.05503 （ 2020 年）。[FKP19] Noah Fleming、Pravesh Kothari 和 Toniann Pitassi，《半代数证明与高效算法设计》，《理论计算机科学前沿与趋势》14（2019年），第1–2期，1–221。[GLL22] Tom Gur、Noam Lifshitz 和 Siqi Liu，《高维扩张图上的超收缩性》，第54届ACM SIGACT计算理论年度研讨会论文集，2022年，第176–184页。[Kho02] Subhash Khot，《唯一性双证明者单轮游戏的威力》，第34届ACM计算理论年度研讨会论文集，2002年5月19日至21日，加拿大蒙特利尔，2002年，第767–775页。

[Kho10] ———, 关于唯一博弈猜想（特邀综述），载于《第25届IEEE计算复杂性年度会议论文集》，CCC 2010，美国马萨诸塞州剑桥，2010年6月9日至12日，IEEE计算机学会，2010年，第99–121页。[KKMO07] Subhash Khot、Guy Kindler、Elchanan Mossel 和 Ryan O’Donnell，《MAX-CUT 与其他二变量约束满足问题的最优不可近似性结果？》，SIAM计算杂志 37 (2007)，第1期，319–357页。[KLLM21] Peter Keevash、Noam Lifshitz、Eoin Long 和 Dor Minzer，《全局超收缩性及其应用》，arXiv 预印本 arXiv:2103.04604 (2021)。[KMMS18] Subhash Khot、Dor Minzer、Dana Moshkovitz 和 Muli Safra，《Johnson 图中的小集合扩张》，电子计算复杂性讨论会 TR18-078 (2018)。[KMS17] Subhash Khot、Dor Minzer 和 Muli Safra，《关于独立集、2对2游戏和格拉斯曼图》，第49届ACM SIGACT计算理论研讨会论文集，STOC 2017，加拿大魁北克省蒙特利尔，2017年6月19日至23日，2017年，第576–589页。[KMS18] ———，《格拉斯曼图中的伪随机集合具有近乎完美的扩张》，第59届IEEE计算机科学基础年度研讨会，FOCS 2018，法国巴黎，2018年10月7日至9日，2018年，第592–601页。[KNS10] Guy Kindler、Assaf Naor 和 Gideon Schechtman，《Lp格罗滕迪克问题的唯一游戏猜想困难性阈值》，Math. Oper. Res. 35 (2010)，第2期，267–283页。[KO18] Tali Kaufman 和 Izhar Oppenheim，《新型局部谱高维扩张图的构造》，第50届ACM SIGACT计算理论研讨会论文集，2018年，第773–786页。[KR08] Subhash Khot 和 Oded Regev，《顶点覆盖可能难以在 2-epsilon 以内近似》，J. Comput. Syst. Sci. 74 (2008)，第3期，335–349页。[Las01] Jean B. Lasserre，《利用多项式进行全局优化与矩问题》，SIAM J. Optim. 11 (2000/01)，第3期，796–817页。MR 1814045[LSV05] Alexander Lubotzky、BethSamuels 和 Uzi Vishne，《ad型 Ramanujan 复形的显式构造》，欧洲组合学杂志 26 (2005)，第6期，965–993页。[MM10] Konstantin Makarychev 和 Yury Makarychev，《如何在扩张图上玩唯一游戏》，《近似与在线算法——第8届国际研讨会，WAOA 2010》，英国利物浦，2010年9月9日至10日。修订论文（Klaus Jansen 和 Roberto Solis-Oba 编），《计算机科学讲义》，第6534卷，Springer，2010年，第190–200页。[MSS16] Tengyu Ma、Jonathan Shi 和 David Steurer，《利用平方和进行多项式时间张量分解》，2016年IEEE第57届计算机科学基础年度研讨会（FOCS），IEEE，2016年，第438–446页。[OZ13] Ryan O’Donnell 和 Yuan Zhou，《可近似性与证明复杂性》，第24届ACM-SIAM离散算法年度研讨会论文集，SODA 2013，美国路易斯安那州新奥尔良，2013年1月6日至8日，2013年，第1537–1556页。

[Par00] Pablo A Parrilo，《结构化半正定规划与鲁棒性和优化中的半代数几何方法》，博士论文，加州理工学院，2000年。[Rag08] Prasad Raghavendra，《针对每个约束满足问题的最优算法与不可近似性结果？》，第40届ACM计算理论研讨会论文集，加拿大不列颠哥伦比亚省维多利亚，2008年5月17日至20日，2008年，第245–254页。[Raz98] Ran Raz，《平行重复定理》，SIAM计算杂志 27 (1998)，第3期，763–803页。[RS10] Prasad Raghavendra 和 David Steurer，《图扩张与唯一博弈猜想》，第42届ACM计算理论研讨会论文集，2010年，第755–764页。[RSS18] Prasad Raghavendra、Tselil Schramm 和 David Steurer，《利用平方和证明进行高维估计》，第3389–3423页，世界科学出版社，2018年。[RST12] Prasad Raghavendra、David Steurer 和 Madhur Tulsiani，《扩张问题之间的归约》，第27届计算复杂性会议论文集，CCC 2012，葡萄牙波尔图，2012年6月26日至29日，2012年，第64–73页。[RT12] Prasad Raghavendra 和 Ning Tan，《利用半定规划层级近似带全局基数约束的约束满足问题》，第23届ACM-SIAM离散算法年度研讨会论文集，工业与应用数学学会，2012年，第373–387页。[Sch04] Markus Schweighofer，《关于 Schm¨udgen 正定性定理的复杂性》，Journal of Complexity 20 (2004)，第4期，529–543页。[Tre12] Luca Trevisan，《关于 Khot 的唯一博弈猜想》，《美国数学学会通报（新系列）》49 (2012)，第1期。

迭代引理的证明

我们给出迭代引理的证明。令 $\mathrm{val}_f(H)$ 表示在 H 内由赋值 f 满足的边所占的比例。

引理 A.1. 设 $c,\gamma,\delta \in (0,1]$ 且 $r \in \mathbb{N}$）。设 I 是字母表为 Σ、定义在 $J_{n,\ell,\alpha}$ 上的仿射唯一游戏实例，其中 ℓ, n 足够大，且其值至少为 $c_\circ$ 假设我们有一个子程序 $\mathcal{A}$，对于输入的任意一个定义在 $J_{n,\ell,\alpha}$ 上、且满足 $\mathrm{val}_\mu(I') \geq c-\gamma$ 的仿射唯一游戏实例 I'，它会返回 J 上的一个 $\leq r$-受限子立方体 H 和一个部分赋值 f，使得 $\mathrm{val}_f(H) \geq \delta$。那么，如果 $\mathcal{A}$ 的运行时间为 $T(\mathcal{A})$，就存在一个运行时间为 $O(|V(J)|T(\mathcal{A}) + |V(J)|^3)$ 的算法，能够为 I 找到一个解，使其满足 J 中 $\Omega(\delta\gamma(1-\alpha)^r)$ 比例的边。

证明。 我们将使用算法 $\mathcal{A}$ 作为子程序。为了获得完整赋值，下面的算法是算法 3.4 的广义版本，其中我们将算法 3.4 中的一些步骤替换为任意子程序 $\mathcal{A}$，该子程序能够找到一个子立方体及其高值赋值。为保证完备性，我们在此给出该算法。

算法 A.2（从部分赋值到完整赋值）。

1. Set $j = 1, I_0 = I, R_0 = \phi$.

2. 当 $|R_{j-1}| < \frac{\gamma}{2}|V(J)|$ 时：

(a) 运行子程序 $\mathcal{A}$，在 I_{j-1} 上寻找一个 $\leq r$-受限子立方体 H_j 和部分赋值 f_j。(b) 令 S_j 为由集合 $H_j \setminus R_{j-1}$ 在 H_j 中导出的子图，并使用 f_j 对它们赋值。令 $R_j = R_{j-1} \cup H_j$。(c) 随机化与 R_j 相 incident 的边上的约束，并令新实例为 I_j。(d) 将 j 加一。

3. 输出任意一个赋给 V（G）且与上述所有部分赋值 f_j（赋给 S_j 的）一致的赋值。

我们来分析该过程的第 j^{th} 次迭代。给定一个实例 I_{j-1}。

命题 A.3. $\text{val}(I_{j-1}) \geq \text{val}(I) - \frac{2|V|}{|V\ G|}(|R_{j-1}|)()$。

证明。假设 X 是一个使 I 的值达到最优的赋值。可以验证，X 至少满足 I 的 $\text{val} - \frac{2|V|}{|V\ G|}(|R_{j-1}|)()$ ~~比例的边~~上的约束，因此命题得证。注意，与 R_{j-1} 相 incident 的边的比例，也就是被随机化的边的比例，至多为 $\frac{2|V|}{|V\ G|}(|R_{j-1}|)()$；而每条不与 R_{j-1} 相 incident ~~的边仍由~~ X 满足。 □

我们将证明，部分赋值 f_j to $H_j \setminus R_{j-1}$ 满足了很大比例的边（以整个图中的边数为准）。在此之前，我们先证明，对边进行随机化可以确保被随机化的边的值很小（即使将其限制在某个子立方体内）。令 $E(S)$ 表示与 S 相接的边（包括仅有一个端点在 S 中的边），并令 $E(S,S)$ 表示两个端点都在 S 中的边。对于边集 E，令 $\text{val}_f(E)$ 表示 E 中被 f 满足的边所占的比例。

命题 A.4. 以概率 $1 - o(1)$，实例 I_{j-1} 满足以下性质：对所有 r-受限子立方体 C：

$$\text{val}(E(C \cap R_{j-1})) \leq \frac{2}{|\Sigma|},$$

其中，$\text{val}(E(S))$ 表示任意 UG 赋值在 $E(S)$ 的端点上所能满足的 $E(S)$ 的最大比例。

证明. 令 k 表示 $|\Sigma|$。固定一个针对 $i \leq r$ 的 i-受限子立方体 C。我们知道，R_{j-1} 是若干个 $\leq r$-受限子立方体的并，因此 $C \cap R_{j-1}$ 在 C 内也构成若干个 $\leq r$-受限子立方体的并。将这些子立方体组成的集合记为 $\mathcal{C}$。考虑 C 内的边集 E，这些边上的约束在（前一次迭代中）经过了随机化；令 A 为 C 中作为这些边端点的顶点集合。我们声称，以概率 $1 - o(1)$，对所有赋值 F 到 A，F 至多满足 $2/k$ 个约束。首先，赋值的数量为 $k^{|A|}$，因此我们固定一个赋值 F 进行分析，然后对所有赋值应用并合界。

固定 F；对于每个 $e \in E$，F 满足 e 的概率为 $1/k$。因此，期望上 F 满足 $\mu = 1/k$ 比例的约束，根据切尔诺夫界

$$\Pr[\text{val}_F(E) \geq 2\mu] \leq e^{-\frac{|E|}{3k}}.$$

现在我们给出 $|E|$ 的下界。注意，如果 $v \in A$，那么要么 v 在 $\mathcal{C}$ 中的某个子立方体内，要么 v 与 $\mathcal{C}$ 中的某个子立方体内的一个顶点相邻。用 d 表示 v 在 C 内部的度，我们知道它是 $\binom{\ell-i}{\alpha\ \ell-i()}\binom{n-\ell}{\alpha\ \ell-i()}$。

1. 如果 $v \in C'$ 对某个 $C' \in \mathcal{C}$ 成立，那么与 v 相 incident 的边中，至少有 $(1-\alpha)^r$ 条留在 C' 中，因此也属于 E。

2. 如果 v 与 $u \in R_{j-1} \cap C$ 相邻，那么对于某个 $C' \in \mathcal{C}$， $u \in C'$ 。特别地，存在一个大小至多为 r 的子集$I \subseteq u$ ，使得 C' 是一个 I受限子立方体。因此，实际上 v 在 C'中至少有$\binom{\ell-i}{\alpha\ \ell-i()}\binom{n-\ell-r}{\ell-i\ \ ()-r}$ 个邻居。通过简单计算可知，这至少是 $n^{-r}d$，因此与 v 相邻的边中至少有 $n^{-r}d$ 条属于 E。

总之，无论如何，我们都能得到至少 $n^{-r}d$ 条与 $v \in A$ 相邻的边位于 E内部，因此 $|E| \geq n^{-r}d|A|/2 \gg 3n|\Sigma||A|$，所以 Chernoff 给出的概率为 $e^{-n|\Sigma||A|}$ ，这足以对所有 $(k^{|A|}$ 个) 到 A的赋值应用并合界。此外，我们还对所有 $\leq r$-受限子立方体 C 应用并合界；这类子立方体只有 $n^{O(r)}$ 个，从而得到引理的结论。 □

在 while 循环的第 j 次迭代中，由于满足 while 条件，我们知道 I_{j-1} 的值为 $\geq c - \gamma$（命题 A.3），因此在 while 循环中， $\mathcal{A}$ 总能找到一个 $\leq r$-子立方体 H_j 和赋值 f_j ，使得 val$_{f_j}(H_j) \geq \delta$。接下来，我们为顶点集合 V（S_j）找到一个赋值 f_j；根据定义，该集合与先前已赋值的顶点不相交。由于 f_j 不会重新为任何顶点赋值，因此在算法的最后一步，可以输出一个与所有先前考虑过的部分赋值一致的赋值。现在我们将证明，最终的部分赋值满足相当大比例的边；若一条边 (u, v) 的两个顶点 u, v都已在 f_j下赋予标签，且这些标签满足该边，则称这条边被部分赋值 f_j满足。

断言 A.5. 在第 j 次迭代中找到的部分赋值的值满足：

$$\mathrm{val}(f_j) \geq \delta(1-\alpha)^r \frac{|V(H_j)|}{2|V(G)|},$$

其中 val(f_j) 表示部分赋值 f_j 满足的 $E(G)$ 中边的比例。

证明. 令 $H_j = S_j \cup (H_j \cap R_{j-1})$，并令 $E_1 = E(S_j, S_j)$ 和 $E_2 = E(H_j \cap R_{j-1})$，使得 $E_1 \cup E_2 = E(H_j, H_j)$ 记为 E。由命题 A.4 可知，val$_{f_j}(E_2) \leq 2/k$，其中 k表示 $|\Sigma|$。通过平均论证：

$$\delta \leq \frac{\#\mathrm{sat}_{f_j}(E_1)}{|E|} + \frac{|E_2|}{|E|}\mathrm{val}_{f_j}(E_2) \leq \frac{\#\mathrm{sat}_{f_j}(E_1)}{|E|} + \frac{2}{k},$$

其中 #sat$_{f_j}(E_1)$ d 表示由 f_j 满足的 E_1 的边数。这意味着 $\#\mathrm{sat}^{f_j(E_1)}{}_{|E|} \geq \delta/2$。

由于 H_j 是一个 $\leq r$-受限子立方体，至少有 $(1-\alpha)^r$比例的边留在 H_j内部，因此 $|E|/|E(H_j)|$至少为 $(1-\alpha)^r$。利用 $|E(H_j)|/|E(J)| \geq |V(H_j)|/|V(J)|$，我们得到：

$$\mathrm{val}(f_j) = \frac{\#\mathrm{sat}_{f_j}(E_1)}{|E|} \cdot \frac{|E|}{|E(H_j)|} \cdot \frac{|E(H_j)|}{|E(J)|} \geq \frac{\delta}{2}(1-\alpha)^r \frac{|V(H_j)|}{|V(G)|},$$

其中，val(f_j)表示 f_j （被赋值为 S_j）满足的边占整个图中边的比例。 □

有了这些事实，结论便显而易见。首先，while 循环的迭代次数不可能超过 $V(G)$，因为每次迭代都会至少为一个新顶点赋值。每次迭代耗时$T(\mathcal{A}) + |V(G)|^2$，因此该算法的运行时间为 $|V(G)|(T(\mathcal{A}) + |V(G)|^2)$。

假设算法在第 $t+1$ 次迭代时退出 while 循环。那么我们知道 $R_t \geq \frac{\gamma}{2}|V(J)|$。利用上述 A.5中的结论，我们得到最终赋值的值与已赋值顶点的数量成正比：

$$\sum_{j=1}^{t} \mathrm{val}(f_j) \geq \delta(1-\alpha)^r \sum_{j=1}^{t} \frac{|V(H_j)|}{2|V(J)|} \geq \delta(1-\alpha)^r \frac{|R_t|}{2|V(J)|} \geq \delta(1-\alpha)^r \frac{\gamma}{4},$$

从而证明了该引理。 □

B 缺失的证明

下面的结论界定了布尔性误差项，并表明存在一个平方和证明，证明该误差项可以忽略不计（只要我们将参数 ν 设得足够小）。

命题 B.1。

$$\mathcal{A}_I \vdash_{\mathrm{poly}(\ell^r/\nu)} \quad \mathop{\mathbb{E}}_c[\sum_s B(H_s^c)] \le |\Sigma|\ell^{O(r)}\sqrt{\nu}.$$

证明。回忆一下，$B(F) = \frac{4}{3}\mathrm{E}_u[(F(u)^3 - F(u))(\Pi_{\ge\lambda_r}F)(u)] = \frac{4}{3}\langle F^3 - F, PF\rangle$，其中 Π 是投影算子 $\Pi_{\ge\lambda_r}$。利用柯西-施瓦茨不等式，我们得到对所有 $\eta > 0$：

$$B(F) \le \frac{4}{3}\left(\frac{\eta}{2}||F^3 - F||_2^2 + \frac{1}{2\eta}||\Pi F||_2^2\right) \le \frac{2\eta}{3}\mathop{\mathbb{E}}_u[F(u) - F(u)^3] + \frac{2}{3\eta}\delta(F^2), \tag{40}$$

最后一个不等式成立，是因为 $F \in [0,1]$ 和 Π 是投影算子。我们将用它来如下界定$B(H_s^c)$。固定 s, u，取 $F = H_s^c(u)$，上面的第一项为 $\mathrm{E}_c[(H_s^c(u) - H_s^c(u)^3]$，我们用 $O(\ell^r\nu)$ 给出其上界。事实上，首先由于 $0 \le H_s^c(u) \le 1$，我们有

$$\mathop{\mathbb{E}}_c[H_s^c(u) - H_s^c(u)^3] = (1 + H_s^c(u))\mathop{\mathbb{E}}_c[H_s^c(u) - H_s^c(u)^2] \le 2\mathop{\mathbb{E}}_c[H_s^c(u) - H_s^c(u)^2]. \tag{41}$$

接下来，回忆一下，$H_s^c(u)$ 是项 $(1 - R_{s,a}^c)$（其中 $a \subset u, |a| \le r$）的乘积。此外，每个变量$R_{s,a}^c$都是近似指示函数的乘积：也就是说，存在 $\beta_i \in (0,1)$，使得 $R_{s,a}^c(u) = p^{c,s\,a}_1, (\delta^{c,s\,a}_1,) \cdot \cdots \cdot p^{c,s\,a}_k, (\delta^{c,s\,a}_k,)$，其中 $p^{c,s\,a}_i = p_{\beta_i + c\nu^2, \nu^2}$ 或 $p_{<\beta_i+c\nu^2,\nu^2}$ 随 c 在 $\{0,1,\ldots,\lfloor 1/\nu\rfloor\}$中变化，而 δ_i是变量 $G_s(u)$ 的线性函数，并且在公理 $\mathcal{A}_I$下属于 $[0,1]$。由命题 B.2（应用两次）可得：

$$\mathop{\mathbb{E}}_c[H_s^c(u) - H_s^c(u)^2] \le \sum_{a\subset u:|a|\le r}\mathop{\mathbb{E}}_c[R_{s,a}^c - (R_{s,a}^c)^2] \le \sum_{a\subset u:|a|\le r}\sum_{i\in[k]}\mathop{\mathbb{E}}_c[p_i^{c,s,a}(\delta_i^{c,s,a}) - p_i^{c,s,a}(\delta_i^{c,s,a})^2],$$

因此，我们可以对上面的每一项分别进行界定。

我们将证明每一项都小于 $O(\nu)$。令 p 为一个近似指示多项式$p = p_{\beta,\nu}$并令 p^c 表示 $p_{\beta+c\nu^2,\nu^2}$其中 $c \in \{0,\ldots,\lfloor 1/\nu\rfloor\}$。对于所有 $\delta \in [0,1]$，我们证明

$$\delta \in [0,1] \vdash_{\widetilde{O}(1/\nu^2)} \quad \mathop{\mathbb{E}}_c[p^c(\delta) - p^c(\delta)^2] \le O(\nu). \tag{42}$$

事实上，这可以通过对 $\delta \in [0,1]$ 进行分类讨论得出（我们接下来会证明这一点），然后利用 Ł ukacs 定理（推论 2.5），我们得到一个度为 $\deg(p^c)$ 的平方和证明。

如果 $\delta \in [0,\beta] \cup [\beta+\nu, 1]$，那么可以验证，对于所有 c，$p^c(\delta) \in [0,\nu^2]$。因此，令 $\delta \in [\beta, \beta+\nu]$，具体而言，在其中一个区间内——对于 $t \in \{0,\ldots,\lfloor 1/\nu\rfloor\}$，$[\beta + t\nu^2, \beta + (t+1)\nu^2]$。于是我们得到，$p^t(\delta)$ 可以是 $[0,1]$ 之间的任意数，因此 $p^t(\delta) - p^t(\delta)^2 \le 1/4$。但对每个 $t' \ne t$，我们都有 $p^{t'}(\delta)$ 要么位于区间 $[0,\nu^2]$，要么位于 $[1-\nu^2, 1]$，这意味着 $p^{t'}(\delta) - p^{t'}(\delta)^2 \le O(\nu^2)$。因此，对 a 取平均可得：

$$\mathbb{E}[p^c(\delta) - p^c(\delta)^2] \le \nu \cdot \frac{1}{4} + (1-\nu)O(\nu^2) \le O(\nu).$$

总之，我们得到 $\mathbb{E}_c[H_s^c(u) - H_s^c(u)^2] \le O(k\ell^r\nu) = \ell^{O(r)}\nu$。将其代入（40），并取$\eta = 1/\sqrt{\nu}$，可得

$$\mathop{\mathbb{E}}_{c}[B(H_s^c)] \le \sqrt{\nu}\ell^{O(r)} + O(\sqrt{\nu}\mathop{\mathbb{E}}_{c}[\delta(H_s^c)]) \le \sqrt{\nu}\ell^{O(r)},$$

对 $s \in \Sigma$ 求和，即完成证明。 □

命题 B.2。

$$\{0 \le x_i \le 1\} \vdash_{2k} \prod_{i\in[k]} x_i - (\prod_{i\in[k]} x_i)^2 \le x_1 - x_1^2 + \ldots + x_k - x_k^2.$$

证明。我们用归纳法证明此结论。对于 $k = 1$，这显然成立；对于 $k = 2$，我们有

$$\begin{aligned} xy - (xy)^2 &= xy - xy^2 + xy^2 - x^2y^2 \\ &= x(y - y^2) + (x - x^2)y^2 \\ &\le y - y^2 + x - x^2. \end{aligned}$$

对于归纳步骤，令 $k \ge 3$，并记 $y = x_1 \cdots x_{k-1}$。先应用基例，再应用归纳假设，得到

$$\prod_{i\in[k]} x_i - \left(\prod_{i\in[k]} x_i\right)^2 = yx_k - (yx_k)^2 \le y - y^2 + x_k - x_k^2 \le x_1 - x_1^2 + \ldots + x_{k-1}^2 - x_{k-1}^2.$$

可以验证，所用的平方和次数至多为 $2k$。 □

C Johnson 图中扩张的平方和证书

本节中，我们给出一个定理 3.17 的平方和证明。我们的证明沿用 [KMMS18], 的思路，只是我们通过低度平方和证明，仔细地实现了每个步骤。为方便起见，我们在下文重述定理 3.17。

定理 C.1（重述 Johnson 图扩张定理 3.17 ）。对于所有 $\alpha \in (0, 1)$、所有整数$\ell \ge 1/\alpha$ 和 $n \ge \ell$，以下结论成立：设 $J_{n,\ell,\alpha}$ 为 α-噪声 Johnson 图。对于每个常数$\gamma \in (0, 1)$ 和正整数 $r \le O(\ell)$，每个满足 (r, γ)-伪随机性的函数 $F\colon V(J) \to \mathbb{R}$ 都具有较大的扩张：

1. $\{F(X) \in [0,1]\}_{X\in V(J)} \vdash_{O(1)}$
   $\langle F, LF\rangle \ge \delta(1 - (1-\alpha)^{r+1})(1 - \gamma^{1/3}\exp(r)) - \sum_{j=0}^{r} \frac{c_j\ell^j}{\gamma} \mathbb{E}_{a\sim\binom{[n]}{j}}[q_a(F)(\delta(F^2|_a) - \gamma)] + B(F)$
2. $\{F(X) \in [0,1]\} \vdash_2 0 \le q_a(F) \le 1,$

其中，对于所有 $j \le r$，c_j 均为大小至多为 $\exp(r)$ 的正常数；对于所有大小为 j 的 $a \subseteq [n]$，$q_a(F)$ 是一个二次多项式，并且对于 $\lambda_r = (1-\alpha)^r$，$B(F) = \frac{4}{3}\mathrm{E}_X[(F^3 - F)\Pi_{\ge\lambda_r}F]$。这里，$\Pi_{\ge\lambda}$ 是由 J 中特征值至少为 λ 的特征向量所张成空间上的投影算子。

对我们来说，转而研究一个密切相关的 Cayley 图会更方便，我们将其记作 $C_{n,\ell,\alpha}$。这个图本质上与 Johnson 图相同，只不过将其视为一个乘积域。在定理 C.18 中，我们陈述了一个类似的结构定理，适用于 $C_{n,\ell,\alpha}$ 上的“置换不变”集合；我们在定理 C.18 中证明了该定理，并且很容易由此推出上面的定理 C.1。

记号。我们用 $[n]$ 表示集合 $\{0,\dots,n-1\}$，也表示群 $(\mathbb{Z}/n\mathbb{Z})$，即模 n 的自然数。通常，当我们将一个集合 S 取正整数次幂 ℓ 时，指的是由 S 中大小为 ℓ 的元素有序多重集构成的集合。我们用 χ_t 表示 $t\in[n]$，以表示群 $\mathbb{Z}/n\mathbb{Z}$ 的特征函数（或 n-循环的特征向量），其中 $\chi_t:[n]\to\mathbb{C}$ 是函数 $\chi_t(x)=e^{\frac{2\pi itx}{n}}$。我们用 $\lambda_G(v)$ 表示 v 的特征值，其中 v 是图 G 的邻接矩阵的一个特征向量。对于一个字符串 $S\in\Sigma^m$、某个字母表 Σ 和一个集合 $I\subseteq[m]$，我们用 $S|_I$ 表示它在 I 中坐标所对应集合上的限制。

C.1 图 $C_{n,\ell,\alpha}$ 及其谱

定义 C.2（约翰逊近似凯莱图 $C_{n,\ell,\alpha}$）。设 α 是 (0,1) 中的一个数，ℓ 是一个正整数。设 n 是一个满足 $n>\ell$ 的正整数。

1. $C_{n,\ell,\alpha}$ 的顶点集为 $[n]^\ell$。当这些参数根据上下文可以明确确定时，我们将省略 $C_{n,\ell,\alpha}$ 中的下标 (n,ℓ,α)。2. 边由以下随机过程描述。对于顶点 $X=(x_1,\dots,x_\ell)$ $x_i\in[n]$，X 的邻居分布如下：从 $[n]^\ell$ 中均匀随机地选择 $(y_1,\dots,y_\ell)$，并选择 $b=(b_1,\dots,b_\ell)\sim\{0,1\}^\ell$，使得 b 的汉明重量等于 $\alpha\ell$，然后输出 $Z=(x_1+b_1\cdot y_1,\dots,x_l+b_\ell\cdot y_\ell)$ 作为 X 的邻居。

不难验证，上述定义的图是一个加权凯莱图，其顶点集为群 $[n]^\ell=(\mathbb{Z}/n\mathbb{Z})^\ell$ 的元素。与该集合相关联的自然群运算是模 n 的分量逐一相加。

接下来讨论 $C_{n,\ell\alpha}$ 的谱性质。沿用记号，我们令 $C=C_{n,\ell,\alpha}$ 也表示图 C 的归一化邻接矩阵。首先注意，C 的特征向量是群 $[n]^\ell$ 的特征函数，即 χ_T，其中 $T=(T_1,\dots,T_\ell)\in[n]^\ell$ 定义为 $\chi_T(x)=\chi_{T_1}(x_1)\cdot\ldots\cdot\chi_{T_\ell}(x_\ell)$，对于 $x\in[n]^\ell$。接下来定义特征向量的度。

定义 C.3 （χ_T 的度）。对于所有 $T\in[n]^\ell$，其中 $T=(T_1,\dots,T_\ell)$，定义 χ_T 的度 *s:*

$$\deg(\chi_T)=|T|:=|\{i\mid T_i\neq 0\}|.$$

下面的引理断言，χ_T 的特征值大约为 $(1-\alpha)^{|T|}$:

引理 C.4. 令 $\lambda_C(\chi_T)$ 表示 C 中对应于 $T\in[n]^\ell$ 的特征向量 χ_T 的特征值。我们有:

$$\lambda_C(\chi_T)=\begin{cases}\frac{\binom{\ell-|T|}{(1-\alpha)\ell-|T|}}{\binom{\ell}{(1-\alpha)\ell}}, & |T|\le(1-\alpha)\ell\\ 0, & \textit{otherwise.}\end{cases}$$

证明. 令 $T=(T_1,\dots,T_\ell)$。对于所有 $X\in[n]^\ell$，我们有:

$$\begin{aligned}C\cdot\chi_T(X)=\mathop{\mathbb{E}}_{y,b}[\chi_T(x_1+b_1y,\dots,x_l+b_ly_l)]&=\chi_T(X)\mathop{\mathbb{E}}_{y,b}[\chi_{T_1,\dots,T_l}(b_1y_1,\dots,b_ly_l)]\\&=\chi_T(X)\mathop{\mathbb{E}}_{y,b}[\chi_{(b_1T_1,\dots,b_lT_l)}(y)].\end{aligned}$$

对于 y、$S\in[n]$ 和 $S\neq 0$，我们知道特征向量 χ_S 与特征向量 χ_0 正交，等价地，$\mathbb{E}_y[\chi_S(y)]=0$；而如果 $S=0$，则 $\mathbb{E}_y[\chi_S(y)]=1$。因此我们得到:

$$\lambda_C(\chi_T) = \mathop{\mathbb{E}}_{y,b}[\chi_{(b_1T_1,\ldots,b_\ell T_\ell)}(y)] = \Pr_b[(b_1T_1,\ldots,b_\ell T_\ell) = 0^\ell]$$
$$= \begin{cases} \frac{\binom{l-|T|}{(1-\alpha)l-|T|}}{\binom{l}{(1-\alpha)l}}, & |T| \le (1-\alpha)\ell \\ 0, & \text{otherwise.} \end{cases}.$$

□

C.2 分析 Johnson 图的非扩张集合

由于我们要处理 Johnson 图 $J_{n,\ \ell,\ \alpha}$ 中的集合，因此只考虑 $C_{n,\ \ell,\ \alpha}$上的“置换不变”集合。注意，Johnson 图的顶点是 $[n]$ 中大小为 ℓ的子集，而 Johnson 近似图的顶点则是由 $[n]$组成的有序 ℓ 元组。因此，给定 Johnson 图中的一个集合 S，它有一个自然映射，对应到集合 S'；后者是 Johnson 近似图顶点的一个子集 C, $S' := \{(x_{\pi(1)},\ldots,x_{\pi(\ell)}) \mid \pi\colon [\ell] \to [\ell], \{x_1,\ldots,x_\ell\} \in S\}$。由此得到以下定义：

定义 C.5（置换不变性）。如果一个集合 $S \subseteq C_{n,\ \ell,\ \alpha}$ 满足：对于所有置换 $\pi \in \mathcal{S}_\ell$ 以及所有 $X = (x_1,\ldots,x_\ell) \in S$，都有 $X_\pi = (x_{\pi(1)},\ldots,x_{\pi(\ell)})$ 属于 S，那么我们称该集合是置换不变的。类似地，如果一个函数 $F\colon V(C) \to \mathrm{R}$ 满足：对于所有输入 $X = (x_1,\ldots,x_\ell)$，都有 $F(x_1,\ldots,x_\ell) = F(x_{\pi(1)},\ldots,x_{\pi(\ell)})$，且对所有 $\pi \in S_\ell$ 均成立，那么我们称该函数是置换不变的。此外，令 $\mathcal{A}_{inv}$ 表示满足 F 置换不变的公理集合，即

$$\mathcal{A}_{inv} := \{F(x_1,\ldots,x_\ell) = F(x_{\pi(1)},\ldots,x_{\pi(\ell)})\}_{\pi\in\mathcal{S}_\ell, X\in[n]^\ell}.$$

由于 C 中对应于 J 中某个顶点集合的顶点集合具有置换不变性，因此只需关注这些特殊集合。从现在起，每当我们提到 $V(C)$ 中的一个集合时，读者都可以认为该集合是置换不变的。

为了分析 C 的非扩张集，我们将考虑置换不变函数 $F\colon V(C) \to [0,1]$。通常会考虑取值于 $0/1$ 的函数 F，其中 F 是集合 S 的指示函数，即当 $X \in S$ 时，$F(X) = 1$。但由于我们需要分析“近似集”（指示函数由一个取值接近 $0/1$ 的多项式近似），$F(X)$ 可以取 $[0,1]$ 之间的任意值。

回想一下，F 的傅里叶分解告诉我们，$F(X) = \sum_T \widehat{F}(T)\chi_T(X)$。现在我们将为函数 F 定义如下内容：

定义 C.6。给定函数 $F\colon V(C) \to [0,1]$，我们有如下层分解：

1. 我们记作 $F = F_0 + \ldots + F_\ell$，其中 $F_i(X) = \sum_{T:\ |T|=i} \widehat{F}(T)\chi_T(X)$。如果一个函数 F 的层 i 傅里叶分解仅包含度为 i 的特征函数，我们就称它为$\widehat{}$，即对所有满足 $|T| \neq i$ 的 T，都有 $F(T) = 0$。

2. 设 $f_{i,\ F}\colon [n]^i \to \mathrm{R}$ 是一个定义为如下形式的函数，

$$f_{i,F}(x_1,\ldots,x_i) := \sum_{T_1,\ldots,T_i\in([n]\setminus 0)^i} \widehat{F}(T_1,\ldots,T_i,0,\ldots)\chi_{T_1,\ldots,T_i}(x_1,\ldots,x_i),$$

设 $X = (x_1,\ldots,x_j) \in [n]^j$和 I是 $\{1,\ldots,j\}$的一个子集。设 $I = \{k_1,\ldots,k_{|I|}\}$，其中 $k_1 < k_2 < \ldots < k_{|I|}$。我们用 $X|_I$表示元素 $(x_{k_1},\ldots,x_{k_{|I|}})$ 组成的有序元组。现在陈述一些由置换不变性所蕴含的 F 的简单性质。

引理 C.7. 对于所有置换不变的函数 $F\colon [n]^\ell \to \mathbb{R}$，我们有：

1. $\widehat{F}(T_1, \ldots, T_\ell)$ 对于所有 $(T_1, \ldots, T_\ell) \in [n]^\ell$ 以及所有置换 π，均有：$= \widehat{F}(T_{\pi(1)}, \ldots, T_{\pi(\ell)})\colon [\ell] \to [\ell]$。
2. 函数 F_i 和 $f_{i,F}$ 也是置换不变的。
3. $F_i(X) = \sum_{\substack{I \subseteq [\ell] \\ |I|=i}} f_{i,F}(X|_I)$.

证明。直接根据定义进行操作即可。 □

注意到，傅里叶系数 $\widehat{F}(T)$ $\forall T \in (\{0,1\}^k)^\ell$、第 i 层函数 $F_i(X)$ 和 $f_i(X)$ 都是不定元 $\{F(X)\}$ 的线性函数，因此在讨论平方和证明时，我们也将把它们视为不定元。

C.3 限制

在本节中，我们定义函数 F 的限制，并陈述若干相关引理。

定义 C.8（C 的 r 受限子立方体）。给定一个有序元组 $A = (a_1, \ldots, a_r)$，对于 $a_i \in [n]$ 和 $r \le \ell - 1$，我们令 $C|_A$ 表示 C 的顶点子集，其中前 r 个坐标限制为 $(a_1, \ldots, a_r)$。我们称这样的子集为 C 的一个 r 受限子立方体。

定义 C.9（限制）。给定函数 $F\colon [n]^\ell \to \mathbb{R}$ 和一个有序元组 $A = (a_1, \ldots, a_r)$，其中 $a_i \in [n]$ 和 $1 \le r \le \ell - 1$，我们将限制函数 $F|_A\colon [n]^{\ell - r} \to \mathbb{R}$ 定义为，

$$F|_A(x_1, \ldots, x_{\ell-r}) = F(a_1, \ldots, a_r, x_1, \ldots, x_{\ell-r}).$$

此外，令 $\delta_A(F)$ 表示限制在 A 上的函数的质量，也就是说，

$$\delta_A(F) := \delta(F|_A) = \mathop{\mathbb{E}}_{X \in [n]^{\ell-r}}[F|_A(X)].$$

为方便起见，当 $A = \phi$ $(r = 0)$ 时，定义 $F|_A(X)\colon = F(X)$，以及 $\delta_A(F)\colon = \delta(F) = \mathrm{E}_{X \in [n]^\ell}[F(X)]$。

下面的引理给出了函数 F 的层函数与其限制的层函数之间的关系。

引理 C.10. 设 F 是 $V(C)$ 上的置换不变函数。则有以下结论 g：

1. 对所有 $a \in [n]$ 以及满足 $0 \le i \le \ell - 1$ 的所有 i，并且对所有 $X \in [n]^i$，有，

$$f_{i+1,F}(a, X) = f_{i,F|_{\{a\}}}(X) - f_{i,F}(X).$$

2. 对满足 $0 \le i \le \ell$ 的所有整数 i，以及所有 $X \in [n]^i$，我们得到关于 $f_i(X)$ 的容斥公式，该公式用 F 的限制表示：

$$f_{i,F}(X) = \sum_{B \subseteq \{1,\ldots,i\}} (-1)^{i-|B|} \delta_{X|_B}(F),$$

其中，$X|_B$ 是 X 中限制在 B所对应索引上的元素组成的有序元组。

证明。我们分别证明每一项。

第一项的证明。根据定义，我们可以展开 $f_{i+1,\ F}$，得到 tha t,

$$f_{i,F}(a,X)=\sum_{(T_1,\ldots,T_{i+1})\in([n]\setminus 0)^{i+1}}\widehat{F}(T_1,\ldots,T_{i+1},0,\ldots,0)\chi_{T_1,\ldots,T_{i+1}}(a,X).$$

我们可以将这个和拆分为两部分：一部分中 T_1 可以取任意值（包括 0），另一部分中 $T_1=0$。我们得到：

$$f_{i,F}(a,X)=\sum_{\substack{T_1\in[n]\\T\in([n]\setminus 0)^i}}\widehat{F}(T_1,T,0,\ldots,0,\ldots,0)\chi_{T_1,T}(a,X)-\sum_{\substack{T_1=0\\T\in([n]\setminus 0)^i}}\widehat{F}(0,T,0,\ldots,0)\chi_T(X).$$

我们将证明第一项等于 $f_{i,\ F|_{\{a\}}}(X)$，第二项等于 $f_{i,\ F}(X)$。这便推出了所需的结论。

对于第一项，我们有：

$$\begin{aligned}&\sum_{\substack{T_1\in[n]\\T\in([n]\setminus 0)^i}}\widehat{F}(T_1,T,0,\ldots,0)\chi_{T_1,T}(a,X)\\&=\sum_{\substack{T_1\in[n]\\T\in([n]\setminus 0)^i}}\mathop{\mathbb{E}}_{\substack{Y_1\in[n],\\Y\in[n]^{\ell-1}}}\left[F(Y_1,Y)\overline{\chi_{T_1}}(Y_1)\overline{\chi_{(T,0,\ldots,0)}(Y)}\right]\chi_{T_1}(a)\chi_T(X)\\&=\sum_{T\in([n]\setminus 0)^i}\mathop{\mathbb{E}}_{\substack{Y_1\in[n],\\Y\in[n]^{\ell-1}}}\left[F(Y_1,Y)\overline{\chi_{(T,0,\ldots,0)}(Y)}\sum_{T_1\in[n]}\chi_{T_1}(a-Y_1)\right]\chi_T(X).\end{aligned}\tag{43}$$

现在我们有 $\sum_{T_1\in[n]}\chi_{T_1}(a-Y_1)=0$，若 $Y_1\neq a$，则等于 n；否则。利用这一事实可得（43）等于

$$\sum_{T\in([n]\setminus 0)^i}\frac{1}{n}\cdot\mathop{\mathbb{E}}_{Y\in[n]^{\ell-1}}\left[F(a,Y)\overline{\chi_{(T,0,\ldots,0)}(Y)}\cdot n\right]\chi_T(X)=\sum_{T\in([n]\setminus 0)^i}\widehat{F|_{\{a\}}}(T,0,\ldots,0)\chi_T(X),$$

根据定义，这等于 $f_{i,\ F|_{\{a\}}}(X)$。

至于第二项，它等于

$$\begin{aligned}&\sum_{\substack{T_1=0\\(T_2,\ldots,T_{i+1})\in([n]\setminus 0)^i}}\widehat{F}(0,T_2,\ldots,T_{i+1},0,\ldots,0)\chi_{T_2,\ldots,T_{i+1}}(X)\\&=\sum_{(T_2,\ldots,T_{i+1})\in([n]\setminus 0)^i}\widehat{F}(T_2,\ldots,T_{i+1},0,\ldots,0)\chi_{T_2,\ldots,T_{i+1}}(X),\end{aligned}$$

由于根据引理C.7 (1)，我们有 $F(0,T_2,\ldots,T_{i+1},0,\ldots)=F(0,T_2,\ldots,T_{i+1},0,\ldots)$。由于最后一个等式就是 $f_{i,F}(X)$ 的定义，结论得证。

第二项的证明。我们将对 i 使用归纳法来证明这一结论。对于 $i=0$ 的基例，根据定义，我们有：

$$f_{0,F}(\phi) = \widehat{F}(0,\dots,0) = \mathop{\mathbb{E}}_{X\in[n]^\ell}[F(X)] = \delta(F) = \delta_\phi(F) = \sum_{B\subseteq\phi} \delta_{\phi|_B}(F).$$

现在假设对于所有置换不变函数 G，该结论对 $i-1$ 都成立，也就是说，对于所有$X \in [n^{i-1}]$，我们有 $f_{i-1,\ G}(X) = \sum_{B\in\{1,\dots,i-1\}}(-1)^{i-1-|B|}\delta_{X|_B}(G)$。现在我们将证明该结论对 $f_{i,\ F}$ 成立，从而完成归纳法。令 $X = (x_1, X')$，其中 $X \in [n]^i, x_1 \in [n]$ 和 $X' \in [n]^{i-1}$。那么，根据同一引理的性质 (1)，我们有：

$$f_{i,F}(X) = f_{i,F|_{\{x_1\}}}(X') - f_{i,F}(X').$$

展开 根据对函数 $F|_{\{x_1\}}$ 和 F 使用归纳假设展开右侧，我们得到 ，

$$\begin{aligned}
f_{i,F}(X) &= \sum_{B'\in\{1,\dots,i-1\}} (-1)^{i-1-|B'|}\delta_{X'|_{B'}}(F|_{\{x_1\}}) - \sum_{B'\in\{1,\dots,i-1\}} (-1)^{i-1-|B'|}\delta_{X'|_{B'}}(F) \\
&= \sum_{B'\in\{1,\dots,i-1\}} (-1)^{i-(1+|B'|)}\delta_{(x_1,X'|_{B'})}(F) + \sum_{B'\in\{1,\dots,i-1\}} (-1)^{i-|B'|}\delta_{X'|_{B'}}(F) \\
&= \sum_{B\in\{1,\dots,i\}:1\in B} (-1)^{i-|B|}\delta_{X|_B}(F) + \sum_{B\in\{1,\dots,i\}:1\notin B} (-1)^{i-|B|}\delta_{X|_B}(F) \\
&= \sum_{B\in\{1,\dots,i\}} (-1)^{i-|B|}\delta_{X|_B}(F).
\end{aligned}$$

至此，归纳步骤和引理的证明均已完成。 □

C.4 计算二阶矩

令 $W_i(F)$ 表示 F在 i^{th}层上的权重，也就是说，令 $\eta_i = W_i[F] = \mathrm{E}_X[F_i(X)^2]$。令 $\delta(F)$ 表示 $\mathrm{E}_X[F(X)]$。现在我们将推导一些关于二阶矩的引理。我们得到层级 i 上的傅里叶权重 η_i 与 ℓ_2-范数之间的如下关系，其中涉及 f_i。

引理 C.11. 对所有 $i \in [\ell]$，给定变量 $\{F(X)\}_{X\in V\ (C)}$：

$$\mathcal{A}_{inv} \vdash_2 \mathop{\mathbb{E}}_{X\in[n]^i}[f_{i,F}(X)^2] = \frac{\eta_i}{\binom{\ell}{i}}.$$

证明。由于 $F_i(A) = \sum_{I\subseteq[\ell]} f_i(A|_I)$，我们得到：

$$\begin{aligned}
\eta_i = \mathop{\mathbb{E}}_{A\sim[n]^\ell}[F_i(A)^2] = \mathop{\mathbb{E}}_{A}[(\sum_I f_i(A_I))^2] &= \sum_I \mathop{\mathbb{E}}_{A}[f_i(A_I)^2] + \sum_{I\neq I'} \mathop{\mathbb{E}}_{A}[f_i(A_I)f_i(A_{I'})] \\
&= \sum_I \mathop{\mathbb{E}}_{A}[f_i(A_I)^2] + 0 \\
&= \mathop{\mathbb{E}}_{(x_1,\dots,x_i)}[f_i(X)^2]\cdot\binom{\ell}{i},
\end{aligned}$$

重新排列后即可得到该引理。 □

引理 C.12. 对所有 $i \in [\ell]$，对所有 $a, b \in [i]$，对所有 $A \in (\{0,1\}^k)^a$，给定不定元 $\{F(X)\}_{X\in V\ (C)}$：

$$\mathcal{A}_{inv}(F) \vdash_2 \mathop{\mathbb{E}}_{X\in(\{0,1\}^k)^{i-a}}[f_i(A,X)^2] \le \frac{\delta(F^2|_A)}{\binom{l-a}{i-a}}.$$

证明。 根据引理C.11，我们有，

$$\mathop{\mathbb{E}}_{X\in(\{0,1\}^k)^{i-a}}[f_i(A,X)^2] = \mathop{\mathbb{E}}_{X\sim(\{0,1\}^k)^{i-a}}[f_{i-a,F|_A}(B)^2] = \frac{W^{i-a}(F|_A)}{\binom{l-a}{i-a}}. \tag{44}$$

我们还有，

$$W^{i-a}(F|_A) \le \mathop{\mathbb{E}}_{X\in(\{0,1\}^k)^{i-a}}[F|_A(X)^2] = \delta(F^2|_A), \tag{45}$$

其中第一个不等式是一个二次和平方不等式。将（44）、（45）合并即可完成证明。 □

C.5 四阶矩界

证明的下一部分是证明 F_i 的四阶矩下界（利用它与一个布尔值函数相关这一事实，因此其四阶矩应当较大），以及 F_i 的四阶矩上界（利用 F 是伪随机这一事实）。我们先给出以下引理，它给出了下界：

引理 C.13（下界）。对于所有实数 $\epsilon > 0$，给定不定元 $\{F(X)\}_{X\in V(C)}$，我们有，

$$\mathop{\mathbb{E}}_{X}[F_i^4(X)] \ge 4\epsilon^3\eta_i - 3\epsilon^4\delta(F) + B(F),$$

其中 $B(F) = 4\varepsilon^3 \mathrm{E}_X[(F^3 - F)F_i] + 3\varepsilon^4 \mathrm{E}_X[F - F^4]$。

证明。我们有：

$$\eta_i = \langle F, F_i\rangle = \mathop{\mathbb{E}}_{X}[F(X)^3 \cdot F_i(X)] + \mathop{\mathbb{E}}_{X}[(F(X) - F(X)^3)\cdot F_i(X)], \tag{46}$$

因为 $F = \sum F_i$ 是 F的正交分解。对第一项使用事实 2.4，我们得到 t:

$$\begin{aligned}
\mathop{\mathbb{E}}_{X}[F(X)^3 \cdot F_i(X)] &= \mathop{\mathbb{E}}_{X}[F(X)^3 \cdot F_i(X)] \\
&\le \frac{3\epsilon}{4}\mathop{\mathbb{E}}_{X}[F(X)^4] + \frac{1}{4\epsilon^3}\mathop{\mathbb{E}}_{X}[F_i(X)^4], \\
&= \frac{3\epsilon}{4}\mathop{\mathbb{E}}_{X}[F(X)] + \frac{3\epsilon}{4}\mathop{\mathbb{E}}_{X}[F(X)^4 - F(X)] + \frac{1}{4\epsilon^3}\mathop{\mathbb{E}}_{X}[F_i(X)^4],
\end{aligned}$$

对所有实数 $\epsilon > 0$。将其代入（46）并整理，即得引理。 □

现在我们将证明 $\mathrm{E}_X[F_i^4(X)]$ 的一个上界。下面的引理给出了 F_i 的四阶矩关于 F_i 的二阶矩的上界：

引理 C.14（上界）。对于所有整数 $i \in [\ell]$，存在正常数 c_1、…、$c_i \le \exp(i)$，使得对于所有 F：

$$\mathcal{A}_{inv} \vdash_{O(1)} \mathop{\mathbb{E}}_{X}[F_i(X)^4] \le \exp(i)\gamma\eta_i + \sum_{j=0}^{i} c_j \ell^i \mathop{\mathbb{E}}_{a\sim[n]^j}[\mathop{\mathbb{E}}_{b\sim[n]^{\ell-j}}[f_i(a,b)^2]\cdot(\delta(F^2|_a) - \gamma)].$$

证明。当集合 X 和函数 F 的含义可由上下文明确时，我们用 $f_i(I)$ 代替 $f_i(X|_I)$。因此，

$$\mathop{\mathbb{E}}_{X}[F_i^4(X)] = \sum_{\substack{I_1,\ldots,I_4\subseteq[l]\\ |I_j|=i,\forall j\in[4]}} \mathop{\mathbb{E}}_{X}[f_i(I_1)f_i(I_2)f_i(I_3)f_i(I_4)].$$

记作，

$$D(i,d) = \{(I_1,\ldots,I_4) \mid \forall j\in[4], I_j\subseteq[l], |I_j| = i, |I_1\cup I_2\cup I_3\cup I_4| = d\}.$$

注意，对所有 $d\in[i,4i]$，

$$|D(i,d)| \le \binom{\ell}{d}\cdot\binom{d}{i}^4 \le \left(\frac{\ell e}{d}\right)^d\left(\frac{de}{i}\right)^{4i} \le \ell^d\exp(i).$$

我们将证明以下关于四重乘积的引理，其中 $(I_1,\ldots,I_4)\in D(i,d)$。证明推迟到第C.6节。

引理 C.15. 设 i,d 为整数，满足 $i\le d\le 4i$，并设 $I_1,\ldots,I_4\subseteq[l]$，满足 $(I_1,I_2,I_3,I_4)\in D(i,d)$。那么存在整数 $t_1,t_2\in[i]$，使得对所有 γ:

$$\begin{aligned}
&\mathop{\mathbb{E}}_{X}[f_i(I_1)f_i(I_2)f_i(I_3)f_i(I_4)]\\
&\le \left(\frac{O(i)}{\ell}\right)^d\gamma\eta_i + \left(\frac{O(i)}{\ell}\right)^{d-i}\mathop{\mathbb{E}}_{a_1\sim[n]^{t_1}}\Big[\mathop{\mathbb{E}}_{b_1\sim[n]^{i-t_1}}[f_i(a_1,b_1)^2]\cdot(\delta(F^2|_{a_1})-\gamma)\Big]\\
&+ \left(\frac{O(i)}{\ell}\right)^{d-i}\mathop{\mathbb{E}}_{a_2\sim[n]^{t_2}}\Big[\mathop{\mathbb{E}}_{b_2\sim[n]^{i-t_2}}[f_i(a_2,b_2)^2](\delta(F^2|_{a_2})-\gamma)\Big].
\end{aligned}$$

现在我们使用引理C.15 来完成引理C.14的证明。事实上，我们得到

$$\begin{aligned}
&\mathop{\mathbb{E}}_{X}[F_i^4(X)]\\
&= \sum_{\substack{I_1,\ldots,I_4\subseteq[l]\\ |I_j|=i,\forall j\in[4]}}\mathop{\mathbb{E}}_{X}[f_i(I_1)f_i(I_2)f_i(I_3)f_i(I_4)]\\
&\le \sum_{d=i}^{4i}\sum_{\substack{I_1,\ldots,I_4\subseteq[l]\\ (I_1,\ldots,I_4)\in D(i,d)}}\mathop{\mathbb{E}}_{X}[f_i(I_1)f_i(I_2)f_i(I_3)f_i(I_4)]\\
&\le \sum_{d=i}^{4i}\sum_{\substack{I_1,\ldots,I_4\subseteq[l]\\ (I_1,\ldots,I_4)\in D(i,d)}}\left(\frac{O(i)}{\ell}\right)^d\gamma\eta_i + \left(\frac{O(i)}{\ell}\right)^{d-i}\mathop{\mathbb{E}}_{a_1\sim[n]^{t_1}}\Big[\mathop{\mathbb{E}}_{b_1\sim[n]^{i-t_1}}[f_i(a_1,b_1)^2]\cdot(\delta(F^2|_{a_1})-\gamma)\Big]\\
&\qquad + \left(\frac{O(i)}{\ell}\right)^{d-i}\mathop{\mathbb{E}}_{a_2\sim[n]^{t_2}}\Big[\mathop{\mathbb{E}}_{b_2\sim[n]^{i-t_2}}[f_i(a_2,b_2)^2](\delta(F^2|_{a_2})-\gamma)\Big]\\
&\le \exp(i)\gamma\eta_i + \sum_{j=0}^{i}c_j\ell^i\mathop{\mathbb{E}}_{a\sim[n]^j}\Big[\mathop{\mathbb{E}}_{b\sim[n]^{i-j}}[f_i(a,b)^2]\cdot(\delta(F^2|_a)-\gamma)\Big],
\end{aligned}$$

对于某些正常数 $c_j\le\exp(i)$，这里我们用到了 $|D(i,d)|\le\ell^d\exp(i)$。 □

C.6 引理 C.15的证明

我们先分析一个简单情形：存在一个指标只出现在某一个 I_j 中，并证明在这种情况下，期望恰好等于 0：

命题 C.16. 如果存在一个索引 j，只出现在一个 I_k 中，那么，

$$\mathop{\mathbb{E}}_{X}[f_i(I_1)f_i(I_2)f_i(I_3)f_i(I_4)] = 0.$$

证明. 不失一般性，我们可以假设 1 只出现在 I_4 中。于是有，

$$\begin{aligned}
\mathop{\mathbb{E}}_{X}[f_i(I_1)f_i(I_2)f_i(I_3)f_i(I_4)] &= \mathop{\mathbb{E}}_{x_1,\ldots,x_l}[f_i(I_1)f_i(I_2)f_i(I_3)f_i(I_4)] \\
&= \mathop{\mathbb{E}}_{x_2,\ldots,x_l}[f_i(I_1)f_i(I_2)f_i(I_3)\mathop{\mathbb{E}}_{x_1}[f_i(I_4) \mid x_2 = x_2', \ldots, x_l = x_l']] \\
&= \mathop{\mathbb{E}}_{x_2,\ldots,x_l}[f_i(I_1)f_i(I_2)f_i(I_3)\delta_{(x_2',\ldots,x_l')\cap I_4}(f_i)] \\
&= 0,
\end{aligned}$$

其中，最后一个等式由引理C.7得出。 □

在证明的其余部分，我们假设 $I_1 \cup I_2 \cup I_3 \cup I_4$ 中的每个索引至少出现在两个集合中。不失一般性，我们可以假设 $\cup_{j=1}^4 I_j = [d]$。令 H_2、H_3、$H_4 \subseteq [d]$ 分别表示在集合 $(I_1, \ldots, I_4)$ 中出现 2 次、3 次、4 次的元素集合。此外，令 $H_2 = X_{12} \cup X_{13} \ldots X_{34}$，其中 X_{jk} 是同时属于 I_j 和 I_k 的元素集合。我们滥用记号，用 H_j 也表示随机变量集合 $(x_{j_1}, \ldots, x_{j_m})$ $m \in H_j$ 和 $x_m \sim \{0,1\}^k$。首先，我们得到，

$$\begin{aligned}
&\mathop{\mathbb{E}}_{H_2}[f_i(I_1)f_i(I_2)f_i(I_3)f_i(I_4)] \\
=&\mathop{\mathbb{E}}_{X_{12},\ldots,X_{34}}[f_i(I_1)f_i(I_2)f_i(I_3)f_i(I_4)] \\
=&\mathop{\mathbb{E}}_{\substack{X_{13},X_{14},\\ X_{23},X_{24}}}[\mathop{\mathbb{E}}_{X_{12}}[f_i(I_1)f_i(I_2)]\mathop{\mathbb{E}}_{X_{34}}[f_i(I_3)f_i(I_4)]] \\
\le&\frac{\varepsilon}{2}\mathop{\mathbb{E}}_{\substack{X_{13},X_{14},\\ X_{23},X_{24}}}[\mathop{\mathbb{E}}_{X_{12}}[f_i(I_1)f_i(I_2)]^2] + \frac{1}{2\varepsilon}\mathop{\mathbb{E}}_{\substack{X_{13},X_{14},\\ X_{23},X_{24}}}[\mathop{\mathbb{E}}_{X_{34}}[f_i(I_3)f_i(I_4)]^2] &(47)\\
\le&\frac{\varepsilon}{2}\mathop{\mathbb{E}}_{\substack{X_{13},X_{14},\\ X_{23},X_{24}}}[\mathop{\mathbb{E}}_{X_{12}}[f_i(I_1)^2]\mathop{\mathbb{E}}_{X_{12}}[f_i(I_2)^2]] + \frac{1}{2\varepsilon}\mathop{\mathbb{E}}_{\substack{X_{13},X_{14},\\ X_{23},X_{24}}}[\mathop{\mathbb{E}}_{X_{34}}[f_i(I_3)^2]\mathop{\mathbb{E}}_{X_{34}}[f_i(I_4)^2]] &(48)\\
\le&\frac{\varepsilon}{2}\mathop{\mathbb{E}}_{X_{12},X_{13},X_{14}}[f_i(I_1)^2]\mathop{\mathbb{E}}_{X_{12},X_{23},X_{24}}[f_i(I_2)^2] + \frac{1}{2\varepsilon}\mathop{\mathbb{E}}_{X_{34},X_{13},X_{23}}[f_i(I_3)^2]\mathop{\mathbb{E}}_{X_{34},X_{14},X_{24}}[f_i(I_4)^2] \\
=&\frac{\varepsilon}{2}\mathop{\mathbb{E}}_{H_2}[f_i(I_1)^2]\mathop{\mathbb{E}}_{H_2}[f_i(I_2)^2] + \frac{1}{2\varepsilon}\mathop{\mathbb{E}}_{H_2}[f_i(I_3)^2]\mathop{\mathbb{E}}_{H_2}[f_i(I_4)^2], &(49)
\end{aligned}$$

其中不等式（47）、（48）由柯西-施瓦茨不等式（引理 2.2和引理 2.3）可得。

现在我们来界定表达式 $\mathrm{E}_X[f_i(I_1)f_i(I_2)f_i(I_3)f_i(I_4)]$。我们有，

$$\begin{aligned}
&\mathop{\mathbb{E}}_{X}[f_i(I_1)f_i(I_2)f_i(I_3)f_i(I_4)] \\
=&\mathop{\mathbb{E}}_{H_4,H_3}[\mathop{\mathbb{E}}_{H_2}[f_i(I_1)f_i(I_2)f_i(I_3)f_i(I_4)]]
\end{aligned}$$

$$
\begin{aligned}
&\le \frac{\varepsilon}{2} \mathop{\mathbb{E}}_{H_4,H_3}[\mathop{\mathbb{E}}_{H_2}[f_i(I_1)^2]\mathop{\mathbb{E}}_{H_2}[f_i(I_2)^2]] + \frac{1}{2\varepsilon}\mathop{\mathbb{E}}_{H_4,H_3}[\mathop{\mathbb{E}}_{H_2}[f_i(I_3)^2]\mathop{\mathbb{E}}_{H_2}[f_i(I_4)^2]] \\
&= \frac{\varepsilon}{2} \mathop{\mathbb{E}}_{A}[\mathop{\mathbb{E}}_{B_1}[f_i(I_1)^2]\mathop{\mathbb{E}}_{B_2}[f_i(I_2)^2]] + \frac{1}{2\varepsilon}\mathop{\mathbb{E}}_{C}[\mathop{\mathbb{E}}_{D_1}[f_i(I_3)^2]\mathop{\mathbb{E}}_{D_2}[f_i(I_4)^2]], \\
&= \frac{\varepsilon}{2} \mathop{\mathbb{E}}_{A}[\mathop{\mathbb{E}}_{B_1}[f_i(a,b_1)^2]\mathop{\mathbb{E}}_{B_2}[f_i(a,b_2)^2]] + \frac{1}{2\varepsilon}\mathop{\mathbb{E}}_{C}[\mathop{\mathbb{E}}_{D_1}[f_i(c,d_1)^2]\mathop{\mathbb{E}}_{D_2}[f_i(c,d_2)^2]], \qquad (50)
\end{aligned}
$$

其中 $A = H_4 \cup (H_3 \cap I_1 \cap I_2)$、$B_1 = (H_2 \cap I_1) \cup ((H_3 \cap I_1) \setminus I_2)$、$B_2 = (H_2 \cap I_2) \cup ((H_3 \cap I_2) \setminus I_1)$、$C = H_4 \cup (H_3 \cap I_3 \cap I_4)$、$D_1 = (H_2 \cap I_3) \cup ((H_3 \cap I_3) \setminus I_4)$、$D_2 = (H_2 \cap I_4) \cup ((H_3 \cap I_4) \setminus I_3)$。集合 a、b_1、b_2、c、d_1、d_2 是相应随机变量 A、…、D_2 的实例化。我们有，

$$
\begin{aligned}
\mathop{\mathbb{E}}_{A}[\mathop{\mathbb{E}}_{B_1}[f_i(a,b_1)^2]\mathop{\mathbb{E}}_{B_2}[f_i(a,b_2)^2]] &\le \mathop{\mathbb{E}}_{A}[\frac{\delta(F^2|_a)}{\binom{\ell-|A|}{i-|A|}}\mathop{\mathbb{E}}_{B_2}[f_i(a,b_2)^2]] \\
&= \frac{1}{\binom{\ell-|A|}{i-|A|}}\mathop{\mathbb{E}}_{A}[\gamma \mathop{\mathbb{E}}_{B_2}[f_i(a,b_2)^2]] + \mathop{\mathbb{E}}_{A}[(\delta(F^2|_A)-\gamma)\left(\frac{\mathbb{E}_{B_2}[f_i(a,b_2)^2]}{\binom{\ell-|A|}{i-|A|}}\right)], \\
&\le \frac{\gamma}{\binom{\ell-|A|}{i-|A|}}\cdot\frac{\eta_i}{\binom{\ell}{i}} + \mathop{\mathbb{E}}_{A}[(\delta(F^2|_A)-\gamma)\left(\frac{\mathbb{E}_{B_2}[f_i(a,b_2)^2]}{\binom{\ell-|A|}{i-|A|}}\right)],
\end{aligned}
$$

其中在第一个不等式中，我们使用引理 C.12 对每个 $\mathbb{E}_{B_1}[f_i(a,b_1)^2]$ 进行界定；最后一个不等式则使用了引理C.11。类似地，我们可以对方程（50）中的第二项进行界定：

$$
\mathop{\mathbb{E}}_{C}[\mathop{\mathbb{E}}_{D_1}[f_i(c,d_1)^2]\mathop{\mathbb{E}}_{D_2}[f_i(c,d_2)^2]] \le \frac{\gamma}{\binom{\ell-|C|}{i-|C|}}\cdot\frac{\eta_i}{\binom{\ell}{i}^{\frac{|A|-|C|}{2}}} + \mathop{\mathbb{E}}_{C}[(\delta(F^2|_C)-\gamma)\left(\frac{\mathbb{E}_{D_2}[f_i(c,d_2)^2]}{\binom{\ell-|C|}{i-|C|}}\right)].
$$

将这些界代入方程（50），并令 $\varepsilon = \left(\frac{O(i)}{\ell}\right)^{\frac{|A|-|C|}{2}}$，得到：

$$
\begin{aligned}
&\mathop{\mathbb{E}}_{X}[f_i(I_1)f_i(I_2)f_i(I_3)f_i(I_4)] \\
&\le \left(\frac{O(i)}{\ell}\right)^{\frac{4i-|A|-|C|}{2}}\gamma\eta_i + \mathop{\mathbb{E}}_{A}[\left(\frac{O(i)}{\ell}\right)^{\frac{2i-|A|-|C|}{2}}\mathop{\mathbb{E}}_{B_2}[f_i(a,b_2)^2]\cdot(\delta(F^2|_a)-\gamma)] \\
&+ \mathop{\mathbb{E}}_{C}[\left(\frac{O(i)}{\ell}\right)^{\frac{2i-|A|-|C|}{2}}\mathop{\mathbb{E}}_{D_2}[f_i(c,d_2)^2](\delta(F^2|_c)-\gamma)].
\end{aligned}
$$

我们知道 $4i-|A|-|C| = 2d$，代入后即可得到引理陈述。

C.7 合并关于 $\|F_i\|_4$ 的上界与下界：第 i 级不等式

合并关于 $\mathrm{E}[F_i(X)^4]$ 的上界与下界后，我们现在可以证明 η_i的一个上界。

引理 C.17（第 i 级不等式）。存在正常数 c_0、……、$c_i \le \exp(i)$，使得给定不定元 $\{F(X)\}_{X\in V(C)}$，

$$
\mathcal{A}_{inv} \vdash_{O(1)} \eta_i \le \exp(i)\gamma^{1/3}\delta + B(F) + \sum_{j=0}^{i}\frac{c_j\ell^i}{\gamma}\mathop{\mathbb{E}}_{a\sim[n]^j}[\mathop{\mathbb{E}}_{b\sim[n]^{i-j}}[f_i(a,b)^2]\cdot(\delta(F^2|_a)-\gamma)],
$$

其中 $B(F) = \frac{4}{3}\mathrm{E}_X[(F-F^3)F_i] + \exp(i)\gamma^{1/3}\mathrm{E}_X[F^4-F]$。

证明。设 $\delta = \mathrm{E}_X[F(X)]$ 和 $\eta_i = \mathrm{E}_X[F_i^2(X)]$。根据 F 上的布尔性公理，我们已经证明了 $\mathrm{E}_X[F_i^4(X)]$, 的上界和下界

- 引理中的上界C.14:

$$\mathop{\mathbb{E}}_{X}[F_i(X)^4] \le \exp(i)\gamma\eta_i + \sum_{j=0}^{i} c'_j \ell^i \mathop{\mathbb{E}}_{a\sim[n]^j}[\mathop{\mathbb{E}}_{b\sim[n]^{i-j}}[f_i(a,b)^2]\cdot(\delta(F^2|_a)-\gamma)], \tag{51}$$

  对于某些正常数 $c'_j \le \exp(i)$。

- 引理中的下界C.13：对于所有 $\varepsilon \in \mathbb{R}$，我们得到:

$$\mathop{\mathbb{E}}_{X}[F_i^4(X)] \ge 4\varepsilon^3\eta_i - 3\varepsilon^4\delta + B_1(F), \tag{52}$$

  where $B_1(F) = 4\varepsilon^3\,\mathbb{E}_X[(F^3-F)F_i] + 3\varepsilon^4\,\mathbb{E}_X[F-F^4]$.

结合（51）和（52），令 $\varepsilon = (\exp(i)\gamma)^{1/3}$ 并除以 $3\varepsilon^3$ 得到

$$\eta_i \le \exp(i)\gamma^{1/3}\delta + \sum_{j=0}^{i} \frac{c'_j}{3\gamma\exp(i)}\ell^i \mathop{\mathbb{E}}_{a\sim[n]^j}[\mathop{\mathbb{E}}_{b\sim[n]^{i-j}}[f_i(a,b)^2]\cdot(\delta(F^2|_a)-\gamma)] - \frac{B_1(F)}{3\gamma\exp(i)}.$$

因此，令 $c_j = {}_3{}^{c'_j}{}_{\exp(i)}$ 以及 $B(F) = \frac{4}{3}\mathrm{E}_X[(F-F^3)F_i] + \exp(i)\gamma^{1/3}\mathrm{E}_X[F^4-F]$，即可完成证明。

□

C.8 伪随机集合的扩张

引理C.17 直接推出关于 $C_{n,\ \ell,\ \alpha}$ 的扩张定理，如下所示:

定理 C.18（$C_{n,\ \ell,\ \alpha}$ 的扩张定理）。对于所有 $\alpha \in (0,1)$、所有整数 $\ell \ge 1/\alpha$ 和 $n \ge \ell$，以下结论成立：设 $C_{n,\ \ell,\ \alpha}$ 为约翰逊近似凯莱图。对于每个常数 $\gamma \in (0,1)$ 和正整数 $r \le O(\ell)$，每个置换不变函数 $F\colon V(C) \to \mathrm{R}$，若其为 (r,γ)-伪随机:

1. $\mathcal{A}_{inv}(F) \cup \{F(X) \in [0,1]\}_{X\in V(C)} \vdash_{O(1)}$
   $\langle F, LF\rangle \ge \mathbb{E}[F](1-(1-\alpha)^{r+1})(1-\gamma^{1/3}\exp(r)) - \sum_{j=0}^{r}\frac{c_j\ell^j}{\gamma}\,\mathbb{E}_{a\sim[n]^j}[q_a(F)(\delta(F^2|_a)-\gamma)] + B(F)$.
2. $\{F(X) \in [0,1]\} \vdash_2 0 \le q_a(F) \le 1$,

其中，对于所有 $j \le r$，c_j's 均为满足 $\le \exp(r)$ 的正常数；对于所有 $a \in [n]^j$，$j \le r$，$q_a(F)$ 均为二次多项式，且 $B(F) = \frac{4}{3}\mathrm{E}_X[(F^3-F)\sum_{i=0}^{r}F_i] + c\mathrm{E}_X[F-F^4]$，其中 $c \le$ 为满足 $\exp(r)\gamma^{1/3}$ 的正常数。

证明。首先有：$\langle F, LF\rangle = \mathrm{E}[F^2] - \langle F, CF\rangle$，其中 L 和 C 分别表示图 $C_{k,\ell,\alpha}$ 的归一化拉普拉斯矩阵和邻接矩阵。令 $1 = \lambda_1 \ge \ldots \lambda_\ell \ge -1$ 表示C的特征值。接下来我们将对 $\langle F, CF\rangle$进行界定:

$$\langle F, CF\rangle = \sum_{i\in[l]}\lambda_i\eta_i \le \sum_{i=0}^{r}\lambda_i\eta_i + (\mathbb{E}[F^2] - \sum_{i=1}^{r}\eta_i)\lambda_{r+1}$$

$$\leq (1-\lambda_{r+1})\sum_{i=0}^{r}\eta_i + \mathbb{E}[F]\lambda_{r+1},$$

其中最后一步用到了 $F(X)\in[0,1]$。令 δ 表示$\mathbb{E}[F]$。利用引理 C.17 可得：

$$\begin{aligned}
&\langle F, CF\rangle \\
&\leq (1-\lambda_{r+1})\sum_{i=0}^{r}\left(\exp(i)\gamma^{1/3}\delta + B_i(F) + \sum_{j=0}^{i}\frac{c'_{ij}\ell^i}{\gamma}\mathop{\mathbb{E}}_{a\sim[n]^j}[\mathop{\mathbb{E}}_{b\sim[n]^{i-j}}[f_i(a,b)^2]\cdot(\delta(F^2|_a)-\gamma)]\right) + \delta\lambda_{r+1} \\
&\leq (1-\lambda_{r+1})(\exp(r)\gamma^{1/3}\delta) + (1-\lambda_{r+1})\sum_i B_i(F) \\
&+\sum_{j=0}^{r}\mathop{\mathbb{E}}_{a\sim[n]^j}[(\delta(F^2|_a)-\gamma)(\sum_{i=j}^{r}(1-\lambda_{r+1})\frac{c'_{ij}\ell^i}{\gamma}\mathop{\mathbb{E}}_{b\sim[n]^{i-j}}[f_i(a,b)^2])] + \delta\lambda_{r+1},
\end{aligned}$$

对于某些正　值常数 $c'_{ij}\leq\exp(i)$ 和 $B_i(F) = \frac{4}{3}\mathrm{E}_X[(F-F^3)F_i] + \exp(i)\gamma^{1/3}\mathrm{E}_X[F^4 - F$　　$]$.

现在来看 $\delta(F^2|_a) - \gamma$ 的乘子。对于每个 $a\in[n]^j$，考虑多项式：$q_a(F) = \frac{1}{c_j\ell^j}\sum_{i=j}^{r}(1-\lambda_{r+1})c'_{ij}\ell^i\mathrm{E}_{b\sim[n]^{i-j}}[f_i(a,b)^2]$,，其中固定常数 $c_j\leq\exp(r)$ 将在稍后确定。利用引理 C.12 对 $\mathrm{E}_{b\sim[n]^{i-j}}[f_i(a,b)^2]$ 进行界定，我们得到：

$$\{F(X)\in[0,1]\}\vdash_2 \quad 0\leq q_a(F)\leq\frac{1}{c_j}\sum_{i=j}^{r}(1-\lambda_{r+1})c'_{ij}\ell^{i-j}\frac{\delta(F^2|_a)}{\binom{\ell-j}{i-j}}\leq 1,$$

对于 $c_j = \sum_{i=j}^{r}(1-\lambda_{r+1})c'_{ij}\frac{\ell^{i-j}}{\binom{\ell-j}{i-j}}\leq\exp(r)$。代入多项式 $q_a(F)$ 并重新整理可得

$$\langle F, LF\rangle \geq \delta(1-\lambda_{r+1})(1-\gamma^{1/3}\exp(r)) - \sum_{j=0}^{r}\frac{c_j\ell^j}{\gamma}\mathop{\mathbb{E}}_{a\sim[n]^j}[q_a(F)(\delta(F^2|_a)-\gamma)] + B(F),$$

对于某些正常数 $c_j\leq\exp(r)$ 和 $B(F) = \frac{4}{3}\mathrm{E}_X[(F^3-F)\sum_{i=0}^{r}F_i] + c\mathrm{E}_X[F-F^4]$，对于正常数 $c\leq\exp(r)\gamma^{1/3}$。

现在我们将 λ_i 的上界代入。根据引理 C.4，我们有 $\lambda_i = \binom{\ell-|T|}{(1-\alpha)\ell-|T|}\Big/\binom{\ell}{(1-\alpha)\ell}$，当 $i\leq(1-\alpha)\ell$ 时成立，否则为 0。可以验证，对于所有介于 1 和 ℓ 之间的 i，都有 $\lambda_i\leq(1-\alpha)\lambda_{i-1}$。由于 $\lambda_0 = 1$，我们得到 $\lambda_i\leq(1-\alpha)^i$，从而完成引理的证明。

□