arXiv:2301.09287v1 [math.CO] 23 Jan 2023

重新审视k-XORSAT 阈值

AMIN COJA-OGHLAN、MIHYUN KANG、LENA KRIEG、MAURICE ROLVIEN

摘要。我们给出了随机k-XORSAT 可满足性阈值定理的一个简化证明。作为一项扩展，我们还确定了有限域上每行恰有k 个非零元素的稀疏随机矩阵的满秩阈值。这一结果扩展了 [Ayre、Coja-Oghlan、Gao、Müller 在 Combinatorica 2020] 中的一项结果。该证明结合了受物理学启发的消息传递论证与精细矩计算。数学学科分类：60B20、15B52

1. 引言

随机 3-XORSAT 问题是最早能够精确确定可满足性阈值的随机约束满足问题之一。随机 3-XORSAT 实例由异或子句的合取构成，而常见的k-SAT 问题则由或子句构成。目标是找出随机异或子句数量的最大值，使得公式以高概率仍然可满足。Dubois 和 Mandler 的开创性论文 [14] 首次解决了这一问题，并引入了一项影响深远的技术，即将二阶矩方法应用于剪枝问题实例。在论文最后一句中，Dubois 和 Mandler 断言，他们的证明可以扩展到任意k-XORSAT ≥ 3。然而，由于估计$k > 3$的二阶矩存在分析上的困难，这一推广远非易事。十多年后，Pittel 和 Sorkin [26] 发表了首个完整证明，篇幅超过 30 页，并借助了一些（本可避免的）计算机辅助。此后，Ayre、Coja-Oghlan、Gao 和 Müller [4] 提出了另一种证明。该证明虽有所不同，但仍相当复杂；它依赖于耦合论证，而非矩计算。该结果不仅涵盖k-XORSAT，还扩展到有限域上的随机矩阵。

本文采用一种与 [4, 26] 显著不同的新方法，对k-XORSAT 阈值及其向随机矩阵的扩展作出了简洁且自成一体的推导。这一新证明部分受到统计物理思想以及近期一项与随机矩阵问题略有关联的研究 [5, 21] 的启发。具体而言，我们首先通过一种物理学家所谓的“淬火”论证，对随机k-XORSAT 公式的典型解作出定量刻画。这种淬火论证采用了警告传播（“WP”），这是一种受物理学启发的消息传递技术。随后，我们进行精细矩计算，但只考察符合 WP 所预测精确特征的情形。用物理学术语来说，第二部分相当于一次“退火”计算。通常，退火估计会因大偏差效应而不够紧致，而且往往复杂得令人头疼。但由于本文精心聚焦于具有正确“淬火”性质的解，计算不仅紧致，也十分简洁优雅。

令$\boldsymbol{F} = \boldsymbol{F}_k(n,m)$为一个随机$k$-XORSAT实例，其中包含$n$个布尔变量和$m$个长度为$k$的随机异或子句。具体而言，这些子句从变量集$x_1,\dots,x_n$上所有可能的$2^k\binom{n}{k}$异或子句中独立且均匀地抽取。下述定理最初分别在 [14] 针对$k = 3$以及在 [26] 针对$k > 3$的情形下得到证明，它给出了k-XORSAT的阈值。

定理 1.1. 对于 $k \geq 3$ 和 $d > 0$，令

$$\Phi_{d,k}(\alpha) = \exp\left(-d\alpha^{k-1}\right) + d\alpha^{k-1} - \frac{d(k-1)}{k}\alpha^k - \frac{d}{k} \quad \textit{and} \quad d_k = \sup\left\{d > 0 : \max_{\alpha\in[0,1]} \Phi_{d,k}(\alpha) = 1 - d/k\right\}. \tag{1.1}$$

对于任意 $\varepsilon > 0$，以高概率，随机 *k-XORSAT* 公式$\boldsymbol{F}$为

(i) 当 $m \leq (1-\varepsilon)d_k n/k$ 时可满足；

(ii) 当 $m \geq (1+\varepsilon)d_k n/k$ 时不可满足。

Amin Coja-Oghlan 得到了德国科学基金会 CO 646/3 和德国科学基金会 CO 646/5 的资助。Mihyun Kang 获得了洪堡基金会颁发的弗里德里希·威廉·贝塞尔研究奖（AUT 1204138 BES）。

简而言之，k-XORSAT 的可满足性阈值等于 d_k/k。该阈值有一个明确的组合解释，这一观察对最初的推导至关重要 [14, 26]。具体而言，我们将 k- XORSAT 公式 $\boldsymbol{F}$改写为如下的 $\mathbb{F}_2$ 上的线性方程组。构造一个随机的 $m \times n$-矩阵 $\boldsymbol{A}$，其第 i 行恰好在满足以下条件的 k 列 j上取值为 1：变量 xi 出现在 $\boldsymbol{F}$ 的第 i 个子句中。因此，$\boldsymbol{A}$ 的每一行都表示一个子句。此外，当 i 个子句中的否定数与 k 之和为奇数时，定义 $\boldsymbol{y}_i = 1$。那么，线性方程组 $\boldsymbol{A}\sigma = \boldsymbol{y}$ 的每个解 $\sigma \in \mathbb{F}_2^n$ 都对应于 $\boldsymbol{F}$的一个异或满足赋值，反之亦然。由于文字的符号与其底层变量的身份相互独立，向量 $\boldsymbol{y}$ 与 $\boldsymbol{A}$ 相互独立。因此，随机异或公式 $\boldsymbol{F}$ 以高概率可满足，当且仅当 $\boldsymbol{A}$ 以高概率具有满行秩 m。

现在考虑以下过程，它将$\boldsymbol{A}$修剪为一个子矩阵$\boldsymbol{A}^{(2)}$:

只要存在一列至多含有一个非零项，就删除该列以及该非零项所在的行（如果存在这样的行）。

这不过是用矩阵$\boldsymbol{A}$的术语表述的随机超图 2-核剥离过程。因此，可以追踪修剪过程（尽管并非易事），以确定$\boldsymbol{A}^{(2)}$ [23]可能的规模。分析表明，$d_k n/k$标志着一个阈值：超过该值后，$\boldsymbol{A}^{(2)}$ 以高概率具有比列更多的行。实际上，当 $m \geq (1+\varepsilon)d_k n/k$ 时，子矩阵$\boldsymbol{A}^{(2)}$ 不再可能具有满行秩，原矩阵$\boldsymbol{A}$也同样如此。因此，当$\boldsymbol{F}$ 的$m \geq (1+\varepsilon)d_k n/k$时，$\boldsymbol{F}$ 不可满足。

尽管当$m \leq (1-\varepsilon)d_k n/k$时，子矩阵$\boldsymbol{A}^{(2)}$的行数少于列数，但$\boldsymbol{A}^{(2)}$也以高概率具有满行秩，这绝非板上钉钉的结论。事实上， [14, 26] 中的主要技术难点在于通过二阶矩方法证明这一事实。必要的计算相当微妙，因为它们基于修剪过程的结果$\boldsymbol{A}^{(2)}$；该矩阵的各行是随机相关的。因此，二阶矩涉及微妙的大偏差权衡。幸运的是，我们在此提出的证明策略既不需要显式分析修剪过程，也不需要复杂的大偏差论证。

定理 1.1 可自然推广到 $\mathbb{F}_2$ 之外的有限域上的矩阵。设 $q \geq 2$ 为一个素数幂，并设 $\mathfrak{A} = (\mathfrak{A}_{ij})_{i,j\geq 1}$ 是一个元素取自 $\mathfrak{A}_{ij} \in \mathbb{F}_q \setminus \{0\}$ 的无限矩阵。此外，给定整数 m、$n > 0$ 和 $k \geq 3$，设 $(\boldsymbol{e}_i)_{i\geq 1}$ 是由 $[n]$ 个大小为 $|e_i| = k$ 的独立均匀随机子集构成的族，并定义一个随机的 $m \times n$ 矩阵 $\boldsymbol{A} = \boldsymbol{A}(k,m,n,q,\mathfrak{A})$，其元素取自 $\mathbb{F}_q$，定义如下：

$$\boldsymbol{A}_{ij} = \mathfrak{A}_{ij}\mathbb{1}\{j \in \boldsymbol{e}_i\} \qquad (i \in [m],\, j \in [n]). \tag{1.2}$$

因此，$\boldsymbol{A}$ 的每一行恰有 k 个非零元素。非零元素的位置由 $\boldsymbol{e}_i$ 决定，而元素本身则从 $\mathfrak{A}$ 复制而来。显然，当 $q = 2$ 时，我们得到的正是由 k-XORSAT 公式 $\boldsymbol{F}$所诱导的矩阵。因此，以下定理将定理 1.1 包含为一个特例。

定理 1.2. 对于任意 $k \geq 3$、任意素数幂 $q \geq 2$，以及任意由 $\mathbb{F}_q$ 中非零元素构成的无限矩阵 $\mathfrak{A}$，以下结论成立。设 d_k 为 (1.1) 中的阈值。那么，对于任意 $\varepsilon > 0$,

(i) 如果 $m \leq (1-\varepsilon)d_k n/k$，则 $\boldsymbol{A}$以高概率具有满行秩；*(ii)* 如果 $m \geq (1+\varepsilon)d_k n/k$，则 $\boldsymbol{A}$以高概率不具有满行秩。

定理 1.2 是对 [4, 定理 1.1], 的补充，后者仅考察了具有同分布行的随机矩阵。相比之下，在定理 1.2 中，矩阵 $\mathfrak{A}$ 可以规定每一行具有不同的非零元素。话虽如此，事后看来，该定理表明，满秩阈值与 q 和 $\mathfrak{A}$均无关。下面我们概述定理 1.2 的证明所依据的策略。

2. 证明策略

证明正向结论定理 1.2(i)的主要困难在于：假设我们能够证明，当 $m < (1-\varepsilon)d_k n/k$时，以高概率，随机向量 $\boldsymbol{\sigma} \in \ker \boldsymbol{A}$近似“平衡”，即每个值 $s \in \mathbb{F}_q$出现的次数都约为 $\boldsymbol{\sigma}$ about n/q。由于直接的矩计算表明，平衡的 $\sigma \in \ker \boldsymbol{A}$的期望数量等于 $(1+o(1))q^{n-m}$，于是我们可以得出结论：$|\ker \boldsymbol{A}| = (1+o(1))q^{n-m}$以高概率成立，从而 $\boldsymbol{A}$ 以高概率具有满行秩。

然而，我们无法直接证明随机 $\boldsymbol{\sigma} \in$ 核$\boldsymbol{A}$ 以高概率是平衡的。我们将改为研究一个矩阵$\boldsymbol{A}^\dagger$，它由$\boldsymbol{A}$ 经过一种影响深远但幅度很小的扰动——“钉扎”——得到。矩阵$\boldsymbol{A}^\dagger$ 包含$\boldsymbol{A}$作为其前$m \times n$阶子矩阵，但$\boldsymbol{A}^\dagger$ 还多出$O(\log n)$行。钉扎保证$\boldsymbol{A}^\dagger$ 只有相对较少的“短线性关系”，这一性质将为我们运用警告传播（“WP”）消息传递方案铺平道路。最终，我们将论证随机 $\boldsymbol{\sigma}^\dagger \in$ 核$\boldsymbol{A}^\dagger$ 以高概率是平衡的。正如上一段所述，这意味着$\boldsymbol{A}^\dagger$ 以高概率具有满行秩，因此$\boldsymbol{A}$也同样如此。

WP 的目的是表明$\boldsymbol{A}^\dagger$ 的核中的向量具有一种特殊结构。具体而言，存在一些坐标$j \in [n]$，它们在$\boldsymbol{A}^\dagger$中是“冻结”的，这意味着 $\sigma_j = 0$ 对所有 $\sigma \in$ 核$\boldsymbol{A}^\dagger$均成立。相较之下，未冻结坐标所取的值基本上是平衡的。因此，如果有 $\boldsymbol{\alpha} n$ 个变量节点被冻结，那么在随机$\boldsymbol{\sigma}^\dagger \in$ 核$\boldsymbol{A}^\dagger$中，每个非零值$s \in \mathbb{F}_q \setminus \{0\}$约出现 $(1-\boldsymbol{\alpha})n/q$次。最终，我们将论证 $\boldsymbol{\alpha} = o(1)$ 以高概率成立，这意味着 $\boldsymbol{\sigma}^\dagger$ 以高概率是平衡的。

但是，要证明 $\boldsymbol{\alpha} = o(1)$ 以高概率成立，还需要几个步骤。首先，根据 WP，我们得知，$j \in [n]$ 被冻结的概率取决于j列$\boldsymbol{A}^\dagger$中的非零元素个数。事实上，WP 提供了关于冻结坐标分布的详细“局部”信息。在分析的淬火部分，我们将仔细提取这些信息，以尚未知晓的 $\boldsymbol{\alpha}$ 值为参数，定量刻画核向量的结构。此外，我们将看到，WP 交换的消息满足某种不动点性质。

随后，我们将发展一种“退火”（矩计算）论证，以界定与任意可能的 $\boldsymbol{\alpha}$ 值相关联的 WP 不动点数量。此外，我们将计算与给定 WP 不动点相容的向量 $\sigma \in \ker \boldsymbol{A}^\dagger$ 的期望数量。该计算将表明，当 $m < (1-\varepsilon)d_k n/k$ 时，以高概率，不存在具有 $\Omega(n)$ 个冻结坐标的 WP 不动点能够产生 $q^{n-m-o(n)}$ 个核向量；而由于$\boldsymbol{A}^\dagger$ 的秩与零度之和为n，我们知道其核必定包含这么多个向量。因此，我们得出 $\boldsymbol{\alpha} = o(1)$ 以高概率成立，正如所需。

本节余下部分将更详细地讨论定理 1.2(i) 的证明。我们先在第 2.1 节介绍钉扎操作，然后讨论 WP 以及淬火和退火分析。第二个断言定理 1.2(ii) 的证明不过是顺带一提。事实上，正如第 1 节所述，这个第二个断言可以由关于子矩阵 $\boldsymbol{A}^{(2)}$ 大小的已知结果推导出来。尽管如此，第 5 节仍给出了一个基于插值法的自足证明，避免了对修剪过程的分析。

2.1. **钉扎**。 通过向矩阵添加几行，随机钉扎操作大多会消除“短线性关系”。这种形式的操作最初在 [7]，中提出，实际上适用于任意矩阵，而不仅仅是随机矩阵 $\boldsymbol{A}$。因此，设 A是一个大小为 $M \times N$ 的任意 $\mathbb{F}_q$-矩阵。对于整数 $t \geq 0$，通过向 A 添加 t 个新行，得到 $A[t]$；每一行都只含一个非零项，即在N 列中独立且均匀随机选取的位置上放置一个 1。

此操作的目的是减少短关系的数量。具体而言，按照 [7]，我们称列的集合 $J \subseteq [N]$ 为A 的关系，如果存在一个向量 $y \in \mathbb{F}_q^M$，使得

$$\operatorname{supp}(y^\top A) = \{j \in [N] : (y^\top A)_j \neq 0\}$$

是J的非空子集。换言之，$y^\top A \neq 0$ 所表示的A各行的线性组合，其非零元素仅位于J中。此外，如果单元素集合 $\{j\}$是A的关系，就称$j \in [N]$ 在 A 中冻结。因此，当且仅当对每个 $\sigma \in \ker A$都有 $\sigma_j = 0$ 时，j才是冻结的。令 $\mathscr{F}(A)$ 表示所有冻结的$j \in [N]$构成的集合。

此外，如果 $J \setminus \mathscr{F}(A)$ 是A的关系，就称$J \neq$ 为A的真关系。最后，如果对于任意 $2 \leq h \leq \ell$，A所含大小为 $|I| = h$的I中，真关系的数量少于 $\delta\binom{N}{h}$，我们就称A是 (δ, ℓ)-自由的。此定义旨在表达：A所含大小为 ℓ 的关系很少，这些关系并非只是由冻结的$j \in [N]$构成的。[1]

引理 2.1 （[7, 命题 2.4]）。 对于任意 $\delta > 0$，$\ell > 0$ 存在 $T_0 = O(\ell^3/\delta^4) > 0$ 使得对于任意 $T \geq T_0$ 以及随机 $\boldsymbol{t} \in [T]$ 对应的矩阵 A，都有 $\mathbb{P}[A[\boldsymbol{t}]$ 是 (δ, ℓ)-*free*$] > 1 - \delta$。

令$T = \lceil \log n \rceil$，对随机$\boldsymbol{t} \in [T]$，记$\boldsymbol{A}^\dagger = \boldsymbol{A}[\boldsymbol{t}]$。由于引理 2.1 中的$T_0$ 与A的大小无关，且随 ℓ, δ 呈多项式增长，因此得到以下结果。

推论 2.2。 令 $\omega = \lceil \log\log n \rceil$。以高概率，$\boldsymbol{A}^\dagger$ 是 (ω^{-1}, ω)-*free*。

得益于推论 2.2 所揭示的短真关系稀少这一性质，我们将能够通过 WP 消息传递方案刻画冻结集 $\mathscr{F}(\boldsymbol{A}^\dagger)$；这就是我们接下来要讨论的内容。

[1]引理 2.1 是我们在推导定理 1.2 时唯一不加证明便直接采用的、超出教科书知识范围的陈述。其证明依赖于势函数论证和少量线性代数，既不冗长，也不困难。

2.2. 警告传播。由于我们不仅要处理 $A^\dagger$，还要处理由它导出的其他几个矩阵，因此我们针对一个大小为 $M \times N$ 的一般矩阵 A 来介绍 WP。矩阵 A 自然会诱导出一个称为 Tanner 图的二分图 $G(A)$。其顶点集由一组变量节点 $V_N = \{v_1, \dots, v_N\}$ 和另一组校验节点 $F_M = \{a_1, \dots, a_M\}$ 组成。前者代表 A 的列，后者代表 A 的行。当且仅当 $A_{ij} \neq 0$ 时，$G(A)$ 中存在一条边 $a_i v_j$。对于一个顶点 $u \in V_N \cup F_M$，令 $\partial u = \partial_A u$ 表示其邻居集。此外，对于集合 $S \subseteq V_N \cup F_M$，令 $A \setminus S$ 表示从 A 中删除所有满足 $a_i \in S$ 的行 i 以及所有满足 $v_j \in S$ 的列 j 后得到的子矩阵。定义 WP 方案时，我们遵循 [5]。

警告传播的核心在于，仅通过变量与其相邻校验节点之间的直接局部交互，刻画冻结变量的集合 $\mathscr{F}(A)$。为此，我们在 Tanner 图的边上关联消息。具体而言，$v_j a_i$ 是 $G(A)$ 的一条边，它包含一条从 v_j 指向 a_i 的消息，以及一条方向相反的消息。这些消息取符号值 $\{u, f\}$，分别表示“未冻结”和“冻结”。令

$$\mathfrak{M}(A) = \left\{ \mathfrak{m} = (\mathfrak{m}_{v \to a}, \mathfrak{m}_{a \to v})_{v \in V_N, v \in \partial_A a} : \mathfrak{m}_{v \to a}, \mathfrak{m}_{a \to v} \in \{u, f\} \right\}$$

为所有可能的消息集合所构成的集合。此外，通过令下式成立，定义 A 的标准消息

$$\mathfrak{m}_{v_j \to a_i}(A) = \begin{cases} f & \text{if } j \in \mathscr{F}(A \setminus \{a_i\}) \\ u & \text{otherwise} \end{cases} \qquad \mathfrak{m}_{a_i \to v_j}(A) = \begin{cases} f & \text{if } v_j \in \mathscr{F}(A \setminus (\partial v_j \setminus \{a_i\})) \\ u & \text{otherwise} \end{cases} \qquad (i \in [M],\, j \in [N]). \tag{2.1}$$

因此，$\mathfrak{m}_{v_j \to a_i}(A) = f$ 表示：删除矩阵 A 中的第 a_i 行后，变量 v_j 被冻结。类似地，$\mathfrak{m}_{a_i \to v_j}(A) = f$ 表示：若删除矩阵 A 中除 a_i 之外的所有 $a_h \in \partial_A v_j$ 行，则变量 v_j 被冻结。

如果冻结确实是一种沿 Tanner 图的边传播的完全局部现象，那么消息 (2.1) 在警告传播更新 WP_A 下应保持不变：$\mathfrak{M}(A) \to \mathfrak{M}(A)$，$\mathfrak{m} = (\mathfrak{m}_{\cdot \to \cdot}) \mapsto \mathrm{WP}(\mathfrak{m}) = (\hat{\mathfrak{m}}_{\cdot \to \cdot})$，其定义如下：

$$\hat{\mathfrak{m}}_{v_j \to a_i} = \begin{cases} f & \text{if } \exists a_h \in \partial v_j \setminus \{a_i\} : \mathfrak{m}_{a_h \to v_j} = f, \\ u & \text{otherwise,} \end{cases} \qquad \hat{\mathfrak{m}}_{a_i \to v_j} = \begin{cases} f & \text{if } \forall x_h \in \partial a_i \setminus \{v_j\} : \mathfrak{m}_{x_h \to a_i} = f, \\ u & \text{otherwise.} \end{cases} \tag{2.2}$$

事实上，第一个更新规则 $\hat{\mathfrak{m}}_{v_j \to a_i}$ 表示：我们预期，当且仅当某个其他校验节点 a_h“冻结”了 v_j 时，v_j 才会在 $A \setminus \{a_i\}$ 中被冻结。类似地，可以预期，当且仅当与 a_i 相邻的所有其他变量节点 x_h 都被冻结时，v_j 才会因 a_i 而冻结，从而除了始终将 x_j 也设为零之外，再无其他方式满足 a_i。

最后，为了从 WP 消息中提取冻结变量的集合，我们为变量节点和校验节点定义取值为 $\{u, s, f\}$ 的标签：对于 $\mathfrak{m} \in \mathfrak{M}(A)$，令

$$\mathfrak{m}_{v_j} = \begin{cases} f & \text{if } \mathfrak{m}_{a \to v_j} = f \text{ for at least two } a \in \partial v_j, \\ s & \text{if } \mathfrak{m}_{a \to v_j} = f \text{ for precisely one } a \in \partial v_j, \\ u & \text{otherwise,} \end{cases} \tag{2.3}$$

$$\mathfrak{m}_{a_i} = \begin{cases} f & \text{if } \mathfrak{m}_{v \to a_i} = f \text{ for all } v \in \partial a_i, \\ s & \text{if } \mathfrak{m}_{v \to a_i} = f \text{ for all but one } v \in \partial a_i, \\ u & \text{otherwise.} \end{cases} \tag{2.4}$$

这里，新标签 $\mathfrak{m}_{v_j}(A) = s$（“半冻结”）表示 v_j 处于“勉强”冻结状态，因为它只有一条传入的 f 消息。乍看之下，s 标签似乎是多余的，因为在 $\mathfrak{m}_{v_j}$ 的情况下可以直接将其归并为 f，在 $\mathfrak{m}_{a_i}$ 的情况下则可归并为 u。然而，在 (2.2) 下，标记为 s 的顶点所“返回”的消息不同于标记为 f 或 u 的顶点。例如，若 $\mathfrak{m}_{v_j} = s$，则当 $\mathfrak{m}_{a_i \to v_j} = f$ 时，$\hat{\mathfrak{m}}_{v_j \to a_i} = u$；而在 $\mathfrak{m}_{v_j} = f$ 的情况下，对于所有 $a_i \in \partial v_j$，都有 $\hat{\mathfrak{m}}_{v_j \to a_i} = f$。令 $\mathfrak{m}_{v_j}(A)$、$\mathfrak{m}_{a_i}(A)$ 表示通过 (2.3)–(2.4) 从 (2.1) 中的标准消息 $\mathfrak{m}_{\cdot \to \cdot}(A)$ 提取的标签。

容易验证，当 $G(A)$ 是无环的时，WP 消息 (2.1) 与更新后的消息一致，即：

$$\mathfrak{m}_{v_j \to a_i}(A) = \hat{\mathfrak{m}}_{v_j \to a_i}(A), \qquad \mathfrak{m}_{a_i \to v_j}(A) = \hat{\mathfrak{m}}_{a_i \to v_j}(A), \tag{2.5}$$

对所有 i、j，使得 $a_i \in \partial_A v_j$。但同样很容易构造出违反 (2.5) 的有环 Tanner 图。

尽管如此，以下命题表明，对于随机矩阵 $\boldsymbol{A}^\dagger$，以高概率，除 $o(n)$ 个相邻节点对 a_i, v_j 外，式 (2.5) 均成立。该命题还表明，通过式 (2.3) 提取的标签能够正确识别集合 $\mathscr{F}(\boldsymbol{A}^\dagger)$，至多有 $o(n)$ 个例外。此外，在大多数核向量中，未冻结变量的取值大致是“平衡”的。令 $\boldsymbol{\alpha} = |\mathscr{F}(\boldsymbol{A}^\dagger)|/n$ 表示 $\boldsymbol{A}^\dagger$ 中冻结变量所占的比例，并令 $\boldsymbol{\sigma}^\dagger$ 为 $\ker \boldsymbol{A}^\dagger$ 中均匀随机选取的元素。此外，令 $d_{\boldsymbol{A}^\dagger}(v_j)$ 表示 $G(\boldsymbol{A}^\dagger)$ 中变量节点 v_j 的度。

命题 2.3。令 $d>0, k\geq 3$。以高概率，我们有

$$\sum_{i=1}^{m}\sum_{v_j\in\partial_{\boldsymbol{A}^\dagger}a_i}\mathbb{1}\left\{\mathtt{m}_{v_j\to a_i}(\boldsymbol{A}^\dagger)\neq\hat{\mathtt{m}}_{v_j\to a_i}(\boldsymbol{A}^\dagger)\right\}+\mathbb{1}\left\{\mathtt{m}_{a_i\to v_j}(\boldsymbol{A}^\dagger)\neq\hat{\mathtt{m}}_{a_i\to v_j}(\boldsymbol{A}^\dagger)\right\}=o(n), \tag{2.6}$$

$$\left|\left\{j\in[n]:\mathtt{m}_{v_j}(\boldsymbol{A}^\dagger)\neq\mathtt{u}\right\}\triangle\mathscr{F}(\boldsymbol{A}^\dagger)\right|=o(n), \tag{2.7}$$

$$\sum_{s\in\mathbb{F}_q}\sum_{\ell\geq 0}\left|\sum_{j=1}^{n}\mathbb{1}\{d_{\boldsymbol{A}^\dagger}(v_j)=\ell,\mathtt{m}_{v_j}(\boldsymbol{A}^\dagger)=\mathtt{u}\}\left(\mathbb{1}\{\boldsymbol{\sigma}_j^\dagger=s\}-1/q\right)\right|=o(n). \tag{2.8}$$

注意，(2.8) 表明，未冻结变量不仅整体上是“平衡”的（也就是说，每个值$s\in\mathbb{F}_q$ 出现的频率约为 $1/q$），而且在将变量按特定度数 $\ell\geq 0$ 分组后，这种平衡仍然成立。我们在第 3 节给出的命题 2.3 的证明，依赖于推论 2.2 所保证的短线性关系的稀缺性。

2.3. **淬火分析**。回顾一下，我们的目标是证明 $\boldsymbol{\sigma}^\dagger$ 以高概率近似平衡。命题 2.3 将这一任务归结为证明 $\boldsymbol{\alpha}=o(1)$ 以高概率成立。为此，我们将提取更多关于变量节点与校验节点之间交换的 WP 消息的详细信息。具体而言，我们将估计具有特定标签的变量节点/校验节点数量，这些标签由 (2.3)–(2.4) 定义。事实上，我们还需要知道具有特定标签且具有特定数量入向/出向消息对的变量节点/校验节点数量。因此，我们接下来的目标是用（目前尚未知晓的）随机变量 $\boldsymbol{\alpha}$ 推导出这类公式。

为计入各类节点接收/发送的消息对数量，令 $\mathscr{L}$ 为所有向量$\ell=(\ell_{\mathtt{uu}},\ell_{\mathtt{uf}},\ell_{\mathtt{fu}},\ell_{\mathtt{ff}})\in\mathbb{Z}_{\geq 0}^4$组成的集合。对于 $\ell\in\mathscr{L}$、标签 $z\in\{\mathtt{f},\mathtt{s},\mathtt{u}\}$、矩阵 A 以及一组消息 $\mathtt{m}_{\cdot\to\cdot}\in\mathfrak{M}(A)$，令

$$\Delta_{z,\ell}(\mathtt{m}_{\cdot\to\cdot})=\{v\in V(A):(\mathtt{m}_v=z)\wedge(\forall s,t\in\{\mathtt{u},\mathtt{f}\}:|\{a\in\partial v:\mathtt{m}_{a\to v}=s,\mathtt{m}_{v\to a}=t\}|=\ell_{st})\}, \tag{2.9}$$

$$\Gamma_{z,\ell}(\mathtt{m}_{\cdot\to\cdot})=\{a\in F(A):(\mathtt{m}_a=z)\wedge(\forall s,t\in\{\mathtt{u},\mathtt{f}\}:|\{v\in\partial a:\mathtt{m}_{v\to a}=s,\mathtt{m}_{a\to v}=s\}|=\ell_{st})\}. \tag{2.10}$$

因此，$\Delta_{z,\ell}$ 由带有标签 z 的变量节点组成，其标签由 (2.3) 给出；这些节点接收/发送的 WP 消息数量如 ℓ 所详述。具体而言，ℓ_{st} 的第一个标签 s 表示传入消息，而第二个索引 t 指定传出消息。类似地，$\Gamma_{z,\ell}$ 统计具有给定标签和给定消息统计数据的校验节点数量。

我们将根据冻结变量的比例 $\boldsymbol{\alpha}$，计算$|\Delta_{z,\ell}(\mathtt{m}_{\cdot\to\cdot}(\boldsymbol{A}^\dagger))|,|\Gamma_{z,\ell}(\mathtt{m}_{\cdot\to\cdot}(\boldsymbol{A}^\dagger))|$。首先，以下集合包含与各类变量节点/校验节点相对应的所有可能向量 ℓ，与 (2.3)–(2.4) 一致：

$$\mathscr{D}(\mathtt{u})=\{\ell\in\mathscr{L}:\ell_{\mathtt{fu}}=\ell_{\mathtt{uf}}=\ell_{\mathtt{ff}}=0\},\qquad \mathscr{G}(\mathtt{u})=\{\ell\in\mathscr{L}:\ell_{\mathtt{uf}}=\ell_{\mathtt{ff}}=0,\ell_{\mathtt{uu}}\geq 2,\ell_{\mathtt{fu}}=k-\ell_{\mathtt{uu}}\}, \tag{2.11}$$

$$\mathscr{D}(\mathtt{s})=\{\ell\in\mathscr{L}:\ell_{\mathtt{fu}}=1,\ell_{\mathtt{ff}}=\ell_{\mathtt{uu}}=0\},\qquad \mathscr{G}(\mathtt{s})=\{\ell\in\mathscr{L}:\ell_{\mathtt{uu}}=\ell_{\mathtt{ff}}=0,\ell_{\mathtt{uf}}=1,\ell_{\mathtt{fu}}=k-1\}, \tag{2.12}$$

$$\mathscr{D}(\mathtt{f})=\{\ell\in\mathscr{L}:\ell_{\mathtt{uu}}=\ell_{\mathtt{fu}}=0,\ell_{\mathtt{ff}}\geq 2\},\qquad \mathscr{G}(\mathtt{f})=\{\ell\in\mathscr{L}:\ell_{\mathtt{uu}}=\ell_{\mathtt{uf}}=\ell_{\mathtt{fu}}=0,\ell_{\mathtt{ff}}=k\}. \tag{2.13}$$

此外，我们假设校验节点 $\mathtt{a}_i$ 处的传入消息基本上相互独立。这似乎是合理的，因为 Tanner 图 $\mathrm{G}(\mathrm{A}^\dagger)$ 是一个稀疏随机图，在变量一侧的平均度 $\mathtt{d}$ 有界，而在校验一侧的度 $\mathtt{k}$ 为常数。因此，通常相邻的变量节点 $\partial_{\boldsymbol{A}^\dagger}\mathtt{a}_i$ 在 $\mathrm{G}(\mathrm{A}^\dagger\setminus\{\mathtt{a}_i\})$ 中应当彼此相距很远，而相距甚远的顶点或许能够彼此去相关。类似地，我们预期典型变量节点 $\mathtt{v}j$ 收到的消息也应近乎独立。如果确实如此，并且假设变量到校验节点消息以某个概率 $0\leq\alpha\leq 1$取值 $\mathtt{f}$，那么校验到变量消息取值 $\mathtt{f}$ 的概率应为 α^{k-1}；因为根据 (2.2)，当且仅当校验节点其余 $\mathtt{k}$ 个 -1 传入消息全部为 $\mathtt{f}$ 时，校验到变量消息才会是 $\mathtt{f}$。结合 (2.11)–(2.13)，我们便能预测各种类型的变量/校验节点的出现频率。例如，若 $\boldsymbol{\alpha}=\alpha$，那么我们预期大约有$\bar{\delta}(\alpha,\mathtt{u})=\exp(-\mathtt{d}\alpha^{k-1})\mathtt{n}$ 个变量 $\mathtt{v}\,\mathtt{j}$ 满足 $\mathtt{m}_{v_j}(\mathrm{A}^\dagger)=\mathtt{f}$。这是因为根据 (2.11)，这样的变量 $\mathtt{v}\,\mathtt{j}$ 不得收到任何 $\mathtt{f}$ 消息，而这类传入消息的均值应为 $\mathtt{d}\alpha^{k-1}$。类似地，我们也能预测其他节点类型的出现频率：

$$\bar{\delta}(\alpha,\mathtt{u})=\exp(-d\alpha^{k-1}),\qquad \bar{\delta}(\alpha,\mathtt{s})=d\alpha^{k-1}\exp(-d\alpha^{k-1}),\qquad \bar{\delta}(\alpha,\mathtt{f})=1-\exp(-d\alpha^{k-1})(1+d\alpha^{k-1}), \tag{2.14}$$

$$\bar{\gamma}(\alpha,\mathtt{u})=1-k(1-\alpha)\alpha^{k-1}-\alpha^k,\quad \bar{\gamma}(\alpha,\mathtt{s})=k(1-\alpha)\alpha^{k-1},\qquad \bar{\gamma}(\alpha,\mathtt{f})=\alpha^k. \tag{2.15}$$

最后，扩展上一段中阐述的推理，我们可以预测具有各种标签的节点频率，以及给定的传入/传出消息统计量 $\ell\in\mathscr{L}$。其中 $\mathrm{Po}_{\geq 2}(\lambda)$

表示给定结果至少为二时的条件泊松/二项分布，我们得到以下表达式：其中 $\mathrm{Bin}_{\geq 2}(N,p)$

$$\bar{\Delta}_{\mathtt{u},\ell}(\alpha) = \bar{\delta}(\alpha,\mathtt{u})\mathbb{1}\{\ell \in \mathscr{D}(\mathtt{u})\}\mathbb{P}[\mathrm{Po}(d(1-\alpha^{k-1})) = \ell_{\mathtt{uu}}], \tag{2.16}$$

$$\bar{\Delta}_{\mathtt{s},\ell}(\alpha) = \bar{\delta}(\alpha,\mathtt{s})\mathbb{1}\{\ell \in \mathscr{D}(\mathtt{s})\}\mathbb{P}[\mathrm{Po}(d(1-\alpha^{k-1})) = \ell_{\mathtt{uf}}], \tag{2.17}$$

$$\bar{\Delta}_{\mathtt{f},\ell}(\alpha) = \bar{\delta}(\alpha,\mathtt{f})\mathbb{1}\{\ell \in \mathscr{D}(\mathtt{f})\}\mathbb{P}[\mathrm{Po}_{\geq 2}(d\alpha^{k-1}) = \ell_{\mathtt{ff}}]\mathbb{P}[\mathrm{Po}(d(1-\alpha^{k-1})) = \ell_{\mathtt{uf}})], \tag{2.18}$$

$$\bar{\Gamma}_{\mathtt{u},\ell}(\alpha) = \bar{\gamma}(\alpha,\mathtt{u})1\{\ell \in \mathscr{G}(\mathtt{u})\}\mathbb{P}[\text{二项式}_{\geq 2}(k,1-\alpha) = \ell_{\mathtt{uu}}], \tag{2.19}$$

$$\bar{\Gamma}_{\mathtt{s},\ell}(\alpha) = \bar{\gamma}(\alpha,\mathtt{s})1\{\ell \in \mathscr{G}(\mathtt{s})\}, \tag{2.20}$$

$$\bar{\Gamma}_{\mathtt{f},\ell}(\alpha) = \bar{\gamma}(\alpha,\mathtt{f})1\{\ell \in \mathscr{G}(\mathtt{f})\}。 \tag{2.21}$$

下述命题表明，前面提到的预测以高概率是准确的。

命题 2.4。设 $d > 0, k \geq 3$。则

$$\sum_{z\in\{\mathtt{f},\mathtt{s},\mathtt{u}\}}\sum_{\ell\in\mathscr{L}} \mathbb{E}\left||\Delta_{z,\ell}(\mathfrak{m}_{\cdot\to\cdot}(\boldsymbol{A}^\dagger))| - n\bar{\Delta}_{z,\ell}(\boldsymbol{\alpha})\right| + \mathbb{E}\left||\Gamma_{z,\ell}(\mathfrak{m}_{\cdot\to\cdot}(\boldsymbol{A}^\dagger))| - m\bar{\Gamma}_{z,\ell}(\boldsymbol{\alpha})\right| = o(n).$$

因此，$|\Delta_{z,\ell}(\mathfrak{m}_{\cdot\to\cdot}(\boldsymbol{A}^\dagger))|$, $|\Gamma_{z,\ell}(\mathfrak{m}_{\cdot\to\cdot}(\boldsymbol{A}^\dagger))|$ 近似等于 $\bar{\Delta}_{z,\ell}(\boldsymbol{\alpha})n$, $\bar{\Gamma}_{z,\ell}(\boldsymbol{\alpha})m$，其取值为 $\boldsymbol{A}^\dagger$ 中冻结变量的实际比例 $\boldsymbol{\alpha}$，这是一个随机变量。命题 2.4 的证明见第 3.3 节，其基于耦合论证。特别是，该证明并未揭示 $\boldsymbol{\alpha}$ 的可能取值。

2.4. **退火论证**。鉴于命题 2.3 中的 (2.8)，我们的主要任务是证明：当$d < (1-\varepsilon)d_k/k$时，$\boldsymbol{\alpha} = o(1)$ 以高概率成立。为此，我们将结合命题 2.4 与一阶矩论证，证明当$d < (1-\varepsilon)d_k/k$时，只有 $\boldsymbol{\alpha} = o(1)$ 以高概率成立这一情形，才能解释核中必然包含的$q^{n-m+o(n)}$ 个向量；这里的核属于 $(m + o(n)) \times n$-矩阵 $\boldsymbol{A}^\dagger$。换言之，我们将证明，具有$\Omega(n)$ 个冻结变量的 WP 不动点所对应的核向量数量过少。

在这方面，本文的论证与先前对定理 1.1 [14, 26] 的证明有显著不同。这些分析并未先研究核向量可能具有的形态（具体而言，它们“源自”具有某些统计特征的 WP 不动点），而是直接估计核中具有给定汉明重量的向量的期望数量；当然，这类论证只有在$q = 2$的情形下才适用。粗略进行矩计算的缺点在于，即便极其罕见的事件也会产生贡献。这种大偏差效应往往会带来复杂且在技术上要求很高的解析优化问题。

目前的“退火”论证（即矩计算）分为两个层次。首先，我们估计具有（2.16）–（2.21）所给“正确”统计特征的 WP 不动点的期望数量。具体而言，回顾更新规则（2.2），若满足以下条件，我们称 $\mathfrak{m}_{\cdot\to\cdot} \in \mathfrak{M}(\boldsymbol{A}^\dagger)$ 为一个 α-*WP* 不动点：

$$\sum_{i=1}^{m}\sum_{v_j\in\partial_{\boldsymbol{A}^\dagger}a_i} \mathbb{1}\left\{\mathfrak{m}_{v_j\to a_i} \neq \hat{\mathfrak{m}}_{v_j\to a_i}\right\} + \mathbb{1}\left\{\mathfrak{m}_{a_i\to v_j} \neq \hat{\mathfrak{m}}_{a_i\to v_j}\right\} = o(n) \qquad \text{and} \tag{2.22}$$

$$\sum_{z\in\{\mathtt{f},\mathtt{s},\mathtt{u}\}}\sum_{\ell\in\mathscr{L}} \left||\Delta_{z,\ell}(\mathfrak{m})| - n\bar{\Delta}_{z,\ell}(\alpha)\right| + \left||\Gamma_{z,\ell}(\mathfrak{m})| - m\bar{\Gamma}_{z,\ell}(\alpha)\right| = o(n). \tag{2.23}$$

因此，我们要求大多数消息在更新（2.2）下保持不变，并且计数$|\Delta_{z,\ell}(\mathfrak{m})|$,$|\Gamma_{z,\ell}(\mathfrak{m})|$ 符合命题 2.4。通过对公式（2.16）–（2.21）进行相对简单的运算，我们最终将看到，对于任意 $0 \leq \alpha \leq 1$，α-WP 不动点的期望数量都是次指数级的。

接下来，我们将估计与特定 WP 不动点相对应的核向量 σ 的数量。具体而言，若满足以下条件，我们称 $\sigma \in \ker \boldsymbol{A}^\dagger$ 为 $\mathfrak{m}_{\cdot\to\cdot} \in \mathfrak{M}(\boldsymbol{A}^\dagger)$ 的扩展：

$$\sum_{i=1}^{n}\mathbb{1}\{\mathfrak{m}_{v_i} \neq \mathtt{u}, \sigma_i \neq 0\} + \sum_{s\in\mathbb{F}_q}\sum_{\ell\geq 0}\left|\sum_{i=1}^{n}\mathbb{1}\{d_{\boldsymbol{A}^\dagger}(v_i) = \ell, \mathfrak{m}_{v_i} = \mathtt{u}\}(\mathbb{1}\{\sigma_i = s\} - 1/q)\right| = o(n). \tag{2.24}$$

因此，σ 必须（在很大程度上）遵循 $\mathfrak{m}_{\cdot\to\cdot}$. 根据 (2.3) 判定为冻结的变量，具体做法是将它们设为零。此外，根据 $\mathfrak{m}_{\cdot\to\cdot}$. 判定为未冻结的变量需要以平衡的方式赋值，即使进一步细分到变量度的具体取值 ℓ 时也是如此，正如 (2.8) 中那样。事实上，命题 2.3 和 2.4 表明，随机核向量 $\boldsymbol{\sigma}^\dagger$ 是标准消息 $\mathfrak{m}_{\cdot\to\cdot}$.（$\boldsymbol{A}^\dagger$）的一个 $\boldsymbol{\alpha}$扩展。因此，令 $\boldsymbol{X}_\alpha$表示满足以下条件的有序对 $(\mathfrak{m}_{\cdot\to\cdot},\sigma)$ 的数量：$\mathfrak{m}_{\cdot\to\cdot}$ 是 $\boldsymbol{A}^\dagger$ 的一个 α-WP 不动点，且 σ 是 α的一个扩展。由此可见，$|\ker \boldsymbol{A}^\dagger| \sim \boldsymbol{X}_{\boldsymbol{\alpha}}$ 以高概率成立。相比之下，下面的命题（我们将在第 4 节中证明）利用函数 $\Phi_{d,k}$ 给出了任意 $0 \leq \alpha \leq 1$ 下 $\boldsymbol{X}_\alpha$ 的一阶矩上界，该函数见 (1.1)。

命题 2.5。令 $d > 0$，$k \geq 3$。以高概率，对所有 $\alpha \in [0,1]$，均有 $\mathbb{E}[\boldsymbol{X}_{\alpha} \mid \mathfrak{D}] \leq q^{n\Phi_{d,\,k(\alpha)+o(n)}}$。

由于当 $d < d_k$ 时，函数 $\Phi_{d,k}$ 在 $\alpha = 0$ 处达到唯一最大值，且 $q^{n\Phi_{d,k}}(0) = q^{n-m}$，因此利用命题 2.5 不难推导出估计 $\boldsymbol{\alpha} = o(1)$ 以高概率成立。由此，我们又可以推断，以高概率，核中的大多数向量都是“平衡”的，也就是说，每个值 $s \in \mathbb{F}_q$ 出现的频率大致相同。具体来说，对于一个向量 $\sigma \in \mathbb{F}_q^n$，令 $\rho(\sigma) = (\rho_s(\sigma))^{s\in\mathbb{F}_q}$ 为其各分量为 $\rho_s(\sigma) = \frac{1}{n}\sum_{i=1}^{n} \mathbb{1}\{\sigma_i = s\}$ 的向量。

推论 2.6. 设 $\varepsilon > 0$。若 $m < (1-\varepsilon)d_k n/k$，则以高概率有

$$\mathbb{E}\left[\|\rho(\boldsymbol{\sigma}^{\dagger}) - q^{-1}\mathbb{1}\|_2 \mid \boldsymbol{A}^{\dagger}\right] = o(1). \tag{2.25}$$

计算满足 $\|\rho(\sigma) - q^{-1}\mathbb{1}\|_2 = o(1)$ 的向量 $\sigma \in \ker \boldsymbol{A}^{\dagger}$ 的期望数量相当容易。回想一下，我们通过向 $\boldsymbol{A}$ 添加 $\boldsymbol{t}$ 行额外的行（每行各有一个非零项），得到了 $\boldsymbol{A}^{\dagger}$。我们将在第 4.4 节证明以下结论。

引理 2.7。对于 $ny\ d > 0$，$k \geq 3$ 存在 $\eta > 0$ 使得 $\mathbb{E}\left|\{\sigma \in \ker \boldsymbol{A}^{\dagger} : \|\rho(\sigma) - q^{-1}\mathbb{1}\|_2 < \eta\} \mid \boldsymbol{t}\right| \leq (1+o(1))q^{n-m-}$ $^{\boldsymbol{t}}$.

定理 *1.2*（*i*）的证明。由于 m 是 $\boldsymbol{A}^{\dagger}$ 的前几行，且这些行与 $\boldsymbol{A}$ 相同，只需证明 $\boldsymbol{A}^{\dagger}$ 以高概率具有满行秩。因此，设 $\boldsymbol{y}^{\dagger} \in \mathbb{F}_q^{m+\boldsymbol{t}}$ 为一个均匀随机向量，在给定 $\boldsymbol{t}$ 的条件下，它与 $\boldsymbol{A}^{\dagger}$ 条件独立。为了得出 $\boldsymbol{A}^{\dagger}$ 以高概率具有满行秩，我们只需证明

$$\mathbb{P}\left[\exists \sigma \in \mathbb{F}_q^n : \boldsymbol{A}^{\dagger}\sigma = \boldsymbol{y}^{\dagger}\right] \sim 1. \tag{2.26}$$

令 $\boldsymbol{Z}$ 为满足 $\boldsymbol{A}^{\dagger}\sigma = \boldsymbol{y}^{\dagger}$ 的解的数量。由于在给定 $\boldsymbol{t}$ 的条件下，$\boldsymbol{y}^{\dagger}$ 与 $\boldsymbol{A}^{\dagger}$ 独立，因此有

$$\mathbb{E}[\boldsymbol{Z} \mid \boldsymbol{t}] = q^{n-m-\boldsymbol{t}}. \tag{2.27}$$

此外，令 $\mathscr{B}$ b e 表示 $\boldsymbol{A}^{\dagger}$ 满足性质（2.25）的事件。根据推论 2.6，$\boldsymbol{Z}$ 在 $\mathscr{B}$ 上的均值为 t o

$$\mathbb{E}[\boldsymbol{Z}\cdot\mathbb{1}_{\mathscr{B}} \mid \boldsymbol{t}] = \sum_{\substack{A^{\dagger}\in\mathbb{F}_q^{(m+\boldsymbol{t})\times n}\\ y^{\dagger}\in\mathbb{F}_q^{m+\boldsymbol{t}},\sigma\in\mathbb{F}_q^n}} \mathbb{1}\left\{A^{\dagger}\sigma = y^{\dagger},\, A^{\dagger}\in\mathscr{B}\right\}\mathbb{P}\left[\boldsymbol{A}^{\dagger} = A^{\dagger}, \boldsymbol{y}^{\dagger} = y^{\dagger} \mid \boldsymbol{t}\right] = q^{n-m-\boldsymbol{t}}\mathbb{P}\left[\boldsymbol{A}^{\dagger}\in\mathscr{B}\right] \sim \mathbb{E}[\boldsymbol{Z} \mid \boldsymbol{t}]. \tag{2.28}$$

同样，引理 2.7 得出

$$\begin{aligned}\mathbb{E}\left[\boldsymbol{Z}^2\cdot\mathbb{1}_{\mathscr{B}} \mid \boldsymbol{t}\right] &= \mathbb{E}\left[\boldsymbol{Z}|\ker \boldsymbol{A}^{\dagger}|\cdot\mathbb{1}_{\mathscr{B}} \mid \boldsymbol{t}\right] = \sum_{A^{\dagger},y^{\dagger},\sigma} \mathbb{1}\left\{A^{\dagger}\sigma = y^{\dagger},\, A^{\dagger}\in\mathscr{B}\right\}|\ker A^{\dagger}|\mathbb{P}\left[\boldsymbol{A}^{\dagger} = A^{\dagger}, \boldsymbol{y}^{\dagger} = y^{\dagger} \mid \boldsymbol{t}\right]\\ &= q^{n-m-\boldsymbol{t}}\mathbb{E}\left[|\ker \boldsymbol{A}^{\dagger}|\cdot\mathbb{1}_{\mathscr{B}} \mid \boldsymbol{t}\right] \leq (1+o(1))\,q^{2(n-m-\boldsymbol{t})}.\end{aligned} \tag{2.29}$$

结合 (2.27)–(2.29) 与切比雪夫不等式，我们可知 $\boldsymbol{Z} \sim q^{n-m-\boldsymbol{t}} > 0$ 以高概率成立，这意味着 (2.26)。 □

2.5. **讨论**。在 Dubois 和 Mandler [14] 确定精确的 3-XORSAT 阈值这一开创性贡献之前，Creignou、Daudé 和 Dubois [11] 通过一阶矩方法和二阶矩方法得到了上界和下界。这些方法后来成为随机约束满足问题理论的基石，并催生了许多重要进展 [2, 13]。独立于 [26], 一项针对一般 k 的 k-XORSAT 阈值的严格推导在 [12], 中被概述，当时该阈值是布谷鸟哈希的一项应用所需的。此后，人们又从物理学家的复制方法和腔方法视角进一步研究了 k-XORSAT 阈值 [22]。此外，文献 [1, 17] 详细研究了随机 k-XORSAT 公式的解空间几何结构。

关于修剪过程，人们提出了各种不同的分析方法 [8, 9, 15, 18, 20, 27, 29]。这些研究采用的方法从微分方程、分枝过程到枚举论证不一而足。鉴于这些证明都不算特别简单，与 [14, 26], 这些研究不同，本文推导 k-XORSAT 阈值时无需明确考察修剪过程，这一点显然是一大优势。

满秩阈值 [4] 的推导同样避开了对修剪过程的分析，转而依赖数学物理中的 Aizenman-Sims-Starr 耦合论证 [3]。[4] 的主要结果是定理 1.2 的一个变体，其中各行同分布。具体而言，各行中的非零元素独立地从 $(\mathbb{F}_q\setminus\{0\})^k$ 上的给定分布中抽取。本证明方法很容易扩展到这种情形，同时也允许非零元素取自给定的无限矩阵 $\mathfrak{A}$；在这种情况下，各行不再需要同分布。在 [4], 之前（该文仍有 50 多页），一项

将 k-XORSAT 阈值结果推广到 $\mathbb{F}_3$ 上的随机矩阵的工作，已通过对 [14, 26] 中矩方法的推广而得到 [16] 。这篇 80 多页的文章需要计算机辅助。

[4] 中发展的技术被扩展到了具有同分布行的更一般随机矩阵模型 [6]；该论文的主要结果也蕴含了k-XORSAT 阈值，但证明相当复杂。此外，对于一个更一般的模型——定义在一般域（不一定是有限域）上的随机矩阵——研究者借助 Aizenman-Sims-Starr 方案 [7]得到了归一化秩的渐近公式。另有一项独立研究得出了随机矩阵$\boldsymbol{A}$在$\mathbb{F}_2$上的渐近秩，但未能确定精确的满秩阈值 [10]。本文采用了 [7] 中的钉扎技术（引理 2.1）；这项技术是对 [24, 28]中为离散概率分布发展出的一般性钉扎方法的改编。

最后，近期一篇论文 [5] 研究了具有独立元素、定义在 $\mathbb{F}_2$ 上的稀疏方阵。其主要结果涉及这类随机矩阵的核的结构，揭示了一种颇为引人注目的分岔现象，与概率组合学中通常具有的零一行为形成对照。本文采用了 [5]中发展的 WP 消息传递方案的数学形式化。此外，论文 [5] 也采用了类似于本文用于证明命题 2.5 的矩计算，但研究的是一种截然不同的矩阵模型，旨在得到有所不同的总体结果（分析核的几何结构，而非证明矩阵具有满秩）。

2.6. **预备知识**。 我们需要考察函数 $\Phi_{d,k}$ 及其极大值。令

$$\phi_{d,k}(\alpha) = 1 - \exp(-d\alpha^{k-1}). \tag{2.30}$$

稍微运用一下 微积分可知，式 (2.30) 中的函数 $\phi_{d,k}$ 与式 (1.1) 中的函数 $\Phi_{d,k}$ 密切相关，具体如下：

$$\Phi'_{d,k}(\alpha) = d(k-1)\alpha^{k-2}\left(\phi_{d,k}(\alpha) - \alpha\right), \tag{2.31}$$

$$\Phi''_{d,k}(\alpha) = d(k-1)(k-2)\alpha^{k-3}\left(\phi_{d,k}(\alpha) - \alpha\right) - d(k-1)\alpha^{k-2}\left(1 - \phi'_{d,k}(\alpha)\right). \tag{2.32}$$

因此，$\phi_{d,k}$的不动点 $\alpha \in [0,1]$ 与 $\Phi_{d,k}$的驻点重合。事实上，$\phi_{d,k}$ 的稳定不动点恰好是 $\Phi_{d,k}$的局部极大值。此外，稍加微积分计算即可得出以下结论。

事实 2.8。 设 $d > 0, k \geq 3$。函数 $\phi_{d,k}$ 在单位区间内至多有三个不同的不动点，分别记为 $\alpha_{\mathtt{u}}(d,k) \leq \alpha_{\mathtt{s}}(d,k) \leq \alpha_{\mathtt{f}}(d,k)$。存在一个临界值 $0 < d^*k < d_k$，使得

- 对于 $d < d^*k$，我们有 $\alpha_{\mathtt{u}}(d,k) \leq \alpha_{\mathtt{s}}(d,k) \leq \alpha_{\mathtt{f}}(d,k) = 0$,
- 对于 $d = d^*k$，我们有 $0 = \alpha_{\mathtt{u}}(d,k) < \alpha_{\mathtt{s}}(d,k) = \alpha_{\mathtt{f}}(d,k) < 1$,
- 对于 $d > d^*k$，我们有 $0 = \alpha_{\mathtt{u}}(d,k) < \alpha_{\mathtt{s}}(d,k) < \alpha_{\mathtt{f}}(d,k) < 1$。

对于 $d < d_k$，该函 数 $\Phi_{d,k}$ 在 0 处取得唯一最大值，而 $\alpha_{\mathtt{f}}(d,k)$ 是 $d > d_k$ 时的唯一最大化点 k.

此外，我们还需要以下线性代数中的基本事实。

事实 2.9 ([7, 引理 2.5])**.** 设 A, B, C 分别为大小为 $M \times N$、$M' \times N$ 和 $M' \times N'$ 的矩阵。此外，设 $I \subseteq [N]$ 为 B 的非零列集合，并通过将 B 中每个 $i \in I \cap \mathscr{F}(A)$ 对应的第 i 列置零，得到 B_0。除非 I 是 A 的真关系，否则我们有

$$\operatorname{nul}\begin{pmatrix} A & 0 \\ B & C \end{pmatrix} - \operatorname{nul} A + \operatorname{rk}(B_0\ C) = N'.$$

此外，我们还记录 Tanner 图$G(\boldsymbol{A}^\dagger)$ 的度分布。由于各行是独立选取的，变量节点的度渐近服从泊松分布。更准确地说，通过常规论证可知，以下结论成立。

事实 2.10. 以高概率有 $\sum_{\ell \geq 0} \exp(\ell)\left|\mathbb{P}[\text{泊松}(d) = \ell] - \sum_{i=1}^{n} \mathbb{1}\{d_{\boldsymbol{A}^\dagger}(v_i) = \ell\}\right| = o(n)$.

对于有限集合 Ω 上概率分布 p 的熵，我们使用符号

$$H(p) = -\sum_{\omega \in \Omega} p(\omega)\log p(\omega),$$

约定 $0\log 0 = 0$。最后，对于向量 $\xi \in \mathbb{F}_q^N$，我们用 $\mathrm{k}\xi\mathrm{k}_h$ 表示 ξ 的 ℓ^h-范数，并约定 $\mathrm{k}\xi\mathrm{k}_0 = |\mathrm{supp}\xi| = |\{i \in [N] : \xi_i \neq 0\}|$。

在本节中　　我们证明命题 2.3 和 2.4。首先，我们探讨一些关于短线性关系的想法　　.

3.1. **短线性关系**。 下面的引理表明，如果矩阵 A 只有少量短真关系，那么通过向 A 添加一行得到的任何矩阵 A' 也具有同样的性质。此外，A 和 A' 拥有的冻结变量大致相同。

引理 3.1。 对于任意 $\delta'>0, \ell'\geq 2$，存在 $\delta>0, \ell\geq 2, N_0>0$，使得对于任意 $N>N_0, M>0$、任意 $M\times N$ 矩阵 A，以及通过向 A 添加一行得到的任意矩阵 A'，以下结论成立。若 A 是 (δ,ℓ)-自由的，那么

(i) A' 是 (δ',ℓ')-自由的，并

且 *(ii)* $|\mathscr{F}(A')\setminus\mathscr{F}(A)|<\delta' N$。

证明。 令 $\ell=2\ell'$ 和 $\delta=\delta'^2 2^{-\ell-16}$。反设 A 是 (δ,ℓ)-自由的，但A' 不是 (δ',ℓ')-自由的。令 $\mathscr{I}$为A'中所有大小为 $|I'|=\ell'$、且不是A的真关系的真关系I'的集合。由于$\mathscr{F}(A)\subseteq\mathscr{F}(A')$，对于任意满足以下条件的 $y\in\mathbb{F}_q^{M+1}$

$$\emptyset\neq \operatorname{supp}(y^\top A')\subseteq I'\setminus\mathscr{F}(A')\subseteq I'\setminus\mathscr{F}(A)$$

我们有 $y_{M+1}\neq 0$。此外，当 N_0充分大时，集合 $\mathscr{I}'\times\mathscr{I}'$ 至少包含 $(\delta'\binom{N}{\ell'})^2/8$ 个有序对 (I',I'')，满足 $I'\cap I''=;$。给定这样一个有序对 (I',I'')，令 $y,z\in\mathbb{F}_q^{M+1}$满足 $;\neq\operatorname{supp}(y^\top A')\subseteq I'\setminus\mathscr{F}(A')$ 且 $;\neq\operatorname{supp}(z^\top A')\subseteq I''\setminus\mathscr{F}(A')$。由于 $y_{M+1},z_{M+1}\neq 0$，存在 $\zeta\in\mathbb{F}_q\setminus\{0\}$ 使得 $y_{M+1}+\zeta z_{M+1}=0$。因此，

$$\emptyset\neq\operatorname{supp}(((y_1\cdots y_M)+\zeta(z_1\cdots z_M))^\top A)\subseteq(I'\cup I'')\setminus\mathscr{F}(A)\quad\text{and}\quad((y_1\cdots y_M)+\zeta(z_1\cdots z_M))^\top A\neq 0.$$

因此，$I'\cup I''$是 A 的一个大小为 $2\ell'$ 的真关系。因此，A 至少拥有 $(\delta'\binom{N}{\ell'})^2/8$ 个这样的真关系。然而，取足够大的 N_0，可得 $(\delta'\binom{N}{\ell'})^2/8>\delta\binom{N}{\ell}$，这与 A 是 (δ,ℓ)-free 这一事实矛盾。

关于 (ii)，令 $j,j'\in\mathscr{F}(A')\setminus\mathscr{F}(A)$ 为 A' 中冻结但在 A 中未冻结的两个不同指标。则存在向量 $y、z\in\mathbb{F}_q^{M+1}$使得 $\operatorname{supp}(y^\top A')=\{j\}$，且 $\operatorname{supp}(z^\top A')=\{j'\}$。由于 $j、j'\notin\mathscr{F}(A)$，我们有 $y_{M+1}\neq 0\neq z_{M+1}$。因此，存在 $\zeta\in\mathbb{F}_q\setminus\{0\}$ 使得 $y_{M+1}+\zeta z_{M+1}=0$。此外，

$$\operatorname{supp}(((y_1\cdots y_M)+\zeta(z_1\cdots z_M))^\top A)=\{j,j'\}.$$

因此，$\{j,j'\}$ 是 A 的真关系。因此我们得出，A至少具有 $\binom{|\mathscr{F}(A')\setminus\mathscr{F}(A)|}{2}$ 个大小为二的真关系。于是，$\binom{|\mathscr{F}(A')\setminus\mathscr{F}(A)|}{2}<\delta\binom{N}{2}$，从而得到所需的界 $|\mathscr{F}(A')\setminus\mathscr{F}(A)|<\delta' N$。□

反复应用引理 3.1 可得以下结论。

推论 3.2. 存在 $1\ll\omega'=\omega'_n\ll\omega=\omega_n$，使得以下结论成立。假设 A 是 $(\omega,1/\omega)$-自由的，且 A'是通过添加至多 ω' 行从 A 得到的。那么，A'是 $(\omega',1/\omega')$-自由的，并且 $|\mathscr{F}(A')\setminus\mathscr{F}(A)|\leq n/\omega'$。

3.2. **命题 2.3 的证明.** 命题 2.3 声称，式 (2.1) 中的标准 WP 消息是更新规则 (2.2) 的近似不动点，并且式 (2.3)–(2.4) 中定义的标签与其预期语义相符。证明的出发点是，随机矩阵 $\boldsymbol{A}^\dagger$ 的分布在以下重采样操作下渐近保持不变。

事实 3.3. 令 $\boldsymbol{A}^+$ 为通过以下操作从 $\boldsymbol{A}^\dagger$ 得到的矩阵。

> 随机选择一个变量节点 $\boldsymbol{v}\in\{v_1,\dots,v_n\}$，然后对所有 $a\in\partial_{\boldsymbol{A}^\dagger}\boldsymbol{v}$，独立地从 $\{v_1,\dots,v_n\}\setminus\{\boldsymbol{v}\}$中均匀且不放回地重新抽取 a 除 $\boldsymbol{v}$以外的邻居。

那么 $\boldsymbol{A}^\dagger$ 和 $\boldsymbol{A}^+$ 同分布。

为证明不动点性质 (2.6)，我们将证明

$$\mathfrak{m}_{\boldsymbol{v}\to a}(\boldsymbol{A}^+)=\hat{\mathfrak{m}}_{\boldsymbol{v}\to a}(\boldsymbol{A}^+)\qquad\text{for all } a\in\partial_{\boldsymbol{A}^+}\boldsymbol{v}\text{ w.h.p.;}\tag{3.1}$$

那么马尔可夫不等式意味着 $\sum_{j=1}^n\sum_{a\in\partial_{\boldsymbol{A}^\dagger}v_j}\mathbb{1}\{\mathfrak{m}_{v_j\to a}(\boldsymbol{A}^\dagger)\neq\hat{\mathfrak{m}}_{v_j\to a}(\boldsymbol{A}^\dagger)\}=o(n)$ 以高概率成立。具体而言，我们将给出一个事件 $\mathscr{E}$，它满足 $\mathbb{P}[\mathscr{E}]\sim 1$，且 (3.1) 在 $\mathscr{E}$ 上确定性成立。

为定义事件 $\mathscr{E}$，取一个序列 $\Delta=\Delta(n)\gg 1$，其随 $n\to\infty$增长得足够缓慢。此外，从 $\boldsymbol{A}^+$ 中删除所有与 $\boldsymbol{v}$相邻的校验节点 $a\in\partial_{\boldsymbol{A}^+}$，得到 $\boldsymbol{A}^-$。现在，令 $\mathscr{E}$为以下三个条件同时成立的事件。

E1: 第二邻域 $\partial^2_{\boldsymbol{A}^+}\boldsymbol{v}=\{v_j:\ \exists a\in\partial_{\boldsymbol{A}^+}\boldsymbol{v}:\ v_j\in\partial_{\boldsymbol{A}^+}a\}\setminus\{\boldsymbol{v}\}$ 的大小恰为 $(k-1)|\partial_{\boldsymbol{A}^+}\boldsymbol{v}|\leq\Delta$。

E2： $\partial^2_{\boldsymbol{A}^+}\boldsymbol{v}$ 不是 $\boldsymbol{A}^-$ 的真关系。

E3： 对于所有 $a\in\partial_{\boldsymbol{A}^+}\boldsymbol{v}$，都有 $\mathscr{F}(\boldsymbol{A}^+\setminus\{a\})\cap\partial_{\boldsymbol{A}^+}a\setminus\{\boldsymbol{v}\}=\mathscr{F}(\boldsymbol{A}^-)\cap\partial_{\boldsymbol{A}^+}a\setminus\{\boldsymbol{v}\}$。

断言 3.4。我们有 $\mathbb{P}[\mathscr{E}]=1-o(1)$。

证明。条件 E1 要求 v 的度至多为 $\Delta/(\mathrm{k}-1)$，并且由与 v 的距离至多为二的顶点所诱导的 $\mathrm{G}(\mathrm{A}^\dagger)$ 子图是无环的。事实 2.10、事实 3.3 以及 $\mathrm{A}^\dagger$ 各行中非零元素位置的独立性表明，以高概率确实如此。此外，E1 和 A^+ 的构造确保 $\partial^2\mathrm{A}^+\mathrm{v}$ 只是 $\mathrm{G}(\mathrm{A}^-)$ 中一个大小至多为 Δ 的随机变量节点集合。由于 A^+ 包含与通过钉扎操作添加到 $\mathrm{A}^\dagger$ 中的相同 t 行，且这些行中的 1 位于随机位置，引理 2.1 表明，对某个 $\omega\gg1$，A^+ 以概率 $1-\mathrm{o}(1/\omega)$ 是 $(\omega,1/\omega)$-自由的。因此，只要 $1\ll\Delta\ll\omega$ 发散得足够慢，$\partial^2\mathrm{A}^+\mathrm{v}$ 以高概率不是 A^+ 的真关系。于是，E2 以高概率成立。最后，$\mathrm{A}^+\setminus\{\mathrm{a}\}$ 是通过向 A^- 添加至多 Δ 行得到的。因此，E2 和推论 3.2 表明，只要 $\Delta\to\infty$ 增长得足够慢，E3 就以高概率成立。□

以下两个断言给出了 (3.1)。

断言 3.5. 假设 $\mathscr{E}$ 发生，并令 $a\in\partial_{\boldsymbol{A}^+}\boldsymbol{v}$。若存在 $b\in\partial_{\boldsymbol{A}^+}\boldsymbol{v}\setminus\{a\}$ 使得 $\mathfrak{m}_{b\to\boldsymbol{v}}(\boldsymbol{A}^+)=\mathtt{f}$，则 $\mathfrak{m}_{\boldsymbol{v}\to a}(\boldsymbol{A}^+)=\mathtt{f}$。此外，若 $\mathfrak{m}_{\boldsymbol{v}}(\boldsymbol{A}^+)\neq\mathtt{u}$，则 $\boldsymbol{v}\in\mathscr{F}(\boldsymbol{A}^+)$。

证明。取 $\mathrm{b}\in\partial_{\boldsymbol{A}^+}\mathrm{v}\setminus\{\mathrm{a}\}$，使得 $\mathfrak{m}_{b\to\boldsymbol{v}}(\mathrm{A}^+)=\mathrm{f}$。于是，E3 保证对所有 $\mathrm{y}\in\partial_{\boldsymbol{A}^+}\mathrm{b}\setminus\{\mathrm{v}\}$，都有 $\mathrm{y}\in\mathscr{F}(\mathrm{A}^-)$。因此，对所有 $\sigma\in\ker(\mathrm{A}^+\setminus\{\mathrm{a}\})\subseteq\ker(\mathrm{A}^-\setminus\{\mathrm{a}\})$ 以及所有 $\mathrm{y}\in\partial_{\boldsymbol{A}^+}\mathrm{b}\setminus\{\mathrm{v}\}$，我们有 $\sigma_y=0$，进而 $\sigma_{\boldsymbol{v}}=0$。因此，$\mathrm{v}\in\mathscr{F}(\mathrm{A}^+\setminus\{\mathrm{a}\})$，故由 (2.1) 得 $\mathfrak{m}_{\boldsymbol{v}\to a}(\mathrm{A}^+)=\hat{}\,\mathfrak{m}_{\boldsymbol{v}\to a}(\mathrm{A}^+)=\mathrm{f}$。类似的论证可得第二个断言。□

断言 3.6. 假设 $\mathscr{E}$ 出现，且令 $a\in\partial_{\boldsymbol{A}^+}\boldsymbol{v}$。如果对于所有 $b\in\partial_{\boldsymbol{A}^+}\boldsymbol{v}\setminus\{a\}$，都有 $\mathfrak{m}_{b\to\boldsymbol{v}}(\boldsymbol{A}^+)=\mathtt{u}$，那么 $\mathfrak{m}_{\boldsymbol{v}\to a}(\boldsymbol{A}^+)=\mathtt{u}$。此外，如果 $\mathfrak{m}_{\boldsymbol{v}}(\boldsymbol{A}^+)=\mathtt{u}$，那么 $\boldsymbol{v}\notin\mathscr{F}(\boldsymbol{A}^+)$。

证明。取 Π,Π' 适当的置换矩阵（以相应地重新排列行和列），使得 B 为一个大小为 $|\partial_{\boldsymbol{A}^+}\boldsymbol{v}\setminus\{a\}|\times(n-1)$ 的矩阵，C 为一个大小为 $|\partial_{\boldsymbol{A}^+}\boldsymbol{v}\setminus\{a\}|\times1$ 的矩阵。于是我们可以写成

$$\boldsymbol{A}^+\setminus\{a\}=\Pi\cdot\begin{pmatrix}\boldsymbol{A}^-\setminus\{\boldsymbol{v}\} & 0\\ B & C\end{pmatrix}\cdot\Pi'. \tag{3.2}$$

这里，子矩阵 $(B\,C)$ 对应于校验节点 $b\in\partial_{\boldsymbol{A}^+}\boldsymbol{v}\setminus\{a\}$，最后一列 $\binom{0}{C}$ 表示 $\boldsymbol{v}$。通过将 B 中对应于变量节点 $v_i\neq\boldsymbol{v}$ 的列替换为全零列，得到 B_0，其中这些列对应于 $i\in\mathscr{F}(\boldsymbol{A}^-)$。

现在假设 $\mathscr{E}$ 成立，并且对于每个 $\mathrm{b}\in\partial_{\boldsymbol{A}^+}\mathrm{v}\setminus\{\mathrm{a}\}$，都存在 $\mathrm{u}\in\partial_{\boldsymbol{A}^+}\mathrm{b}\setminus\{\mathrm{v}\}$，使得 $\mathfrak{m}_{u\to b}(\mathrm{A}^+)=\mathrm{u}$。实际上，令 $\mathrm{U}=\{\mathrm{u}\in\partial^2\mathrm{A}^+\mathrm{v}:\mathfrak{m}_{u\to b}(\mathrm{A}^+)=\mathrm{u}\}$。那么 $\mathrm{U}\cap\mathscr{F}(\mathrm{A}^-)=;$，因为对于每个 $\mathrm{b}\in\partial_{\boldsymbol{A}^+}\mathrm{v}$，都有 $\mathscr{F}(\mathrm{A}^-)\subseteq\mathscr{F}(\mathrm{A}^+\setminus\{\mathrm{b}\})$。根据 E1，对于每个表示变量 $\mathrm{u}\in\mathrm{U}$ 的列，B_0 中的 u 列恰好包含一个非零项。因此，$\mathrm{rk}(\mathrm{B}_0\,\mathrm{C})=|\partial_{\boldsymbol{A}^*}\mathrm{v}\setminus\{\mathrm{a}\}|$，即矩阵 $(\mathrm{B}_0\;\mathrm{C})$ 满行秩。由于 E2 保证 $\partial^2\mathrm{A}^+\mathrm{v}$ 不是 A^- 的真关系，事实 2.9 表明

$$\operatorname{nul}\begin{pmatrix}\boldsymbol{A}^-\setminus\{\boldsymbol{v}\} & 0\\ B & C\end{pmatrix}=\operatorname{nul}(\boldsymbol{A}^+\setminus\{a,\boldsymbol{v}\})-|\partial_{\boldsymbol{A}^*}\boldsymbol{v}\setminus\{a\}|-1. \tag{3.3}$$

类似地，我们可以计算再添加一行后所得矩阵的秩；该行仅在最后一列有一个 1 项，从而明确地钉扎 $\boldsymbol{v}$:

$$\operatorname{nul}\begin{pmatrix}\boldsymbol{A}^-\setminus\{\boldsymbol{v}\} & 0\\ B & C\\ 0 & 1\end{pmatrix}=\operatorname{nul}(\boldsymbol{A}^+\setminus\{a,\boldsymbol{v}\})-|\partial_{\boldsymbol{A}^*}\boldsymbol{v}\setminus\{a\}|-2<\operatorname{nul}\begin{pmatrix}\boldsymbol{A}^-\setminus\{\boldsymbol{v}\} & 0\\ B & C\end{pmatrix}. \tag{3.4}$$

结合 (3.3)–(3.4)，我们得出结论：表示 $\boldsymbol{v}$ 的最后一个坐标 n 在 $\begin{pmatrix}\boldsymbol{A}^-\setminus\{\boldsymbol{v}\} & 0 & B\,C\end{pmatrix}$ 中未冻结；否则，(3.4) 左右两边的零度就会相等。因此，由 (3.2) 可知，$\boldsymbol{v}$ 在 $\boldsymbol{A}^+\setminus\{a\}$. 中未冻结。于是，根据 (2.1)，$\mathfrak{m}_{\boldsymbol{v}\to a}(\boldsymbol{A}^+)=\mathtt{u}$。类似的论证可得第二个断言。□

我们接下来考察校验到变量消息。

断言 3.7. 假设 $\mathscr{E}$ 出现，且令 $a\in\partial_{\boldsymbol{A}^+}\boldsymbol{v}$。如果对所有 $w\in\partial_{\boldsymbol{A}^+}\boldsymbol{v}\setminus\{a\}$，$\mathfrak{m}_{w\to a}(\boldsymbol{A}^+)=\mathtt{f}$，那么 $\mathfrak{m}_{a\to\boldsymbol{v}}(\boldsymbol{A}^+)=\mathtt{f}$。

证明。 若 $\mathtt{m}_{w\to a}(\boldsymbol{A}^+)=\mathtt{f}$，则根据标准消息的定义 (2.1)，$w\in\mathscr{F}(\boldsymbol{A}^+\setminus\{a\})$。因此，**E3** 保证对所有 $w\in\partial_{\boldsymbol{A}^+}\boldsymbol{v}\setminus\{a\}$，都有 $w\in\mathscr{F}(\boldsymbol{A}^-)$。此外，由于 $\mathscr{F}(\boldsymbol{A}^-)\subseteq\mathscr{F}(\boldsymbol{A}^-\setminus(\partial_{\boldsymbol{A}^+}\boldsymbol{v}\setminus\{a\}))$，我们由 (2.1) 得到$\mathtt{m}_{a\to\boldsymbol{v}}(\boldsymbol{A}^+)=\mathtt{f}$。□

断言 3.8。 假设 $\mathscr{E}$出现，且令 $a\in\partial_{\boldsymbol{A}^+}\boldsymbol{v}$。若存在 $w\in\partial_{\boldsymbol{A}^+}a\setminus\{\boldsymbol{v}\}$ 使得 $\mathtt{m}_{w\to a}(\boldsymbol{A}^+)=\mathtt{u}$，则$\mathtt{m}_{a\to\boldsymbol{v}}(\boldsymbol{A}^+)=\mathtt{u}$。

证明。 令 $w\in\partial_{\boldsymbol{A}^+}a\setminus\{\boldsymbol{v}\}$ 满足 $\mathtt{m}_{w\to a}(\boldsymbol{A}^+)=\mathtt{u}$。那么，$\mathtt{m}_{w\to a}(\boldsymbol{A}^+)$ 的定义 (2.1) 保证 $w\notin\mathscr{F}(\boldsymbol{A}^+\setminus\{a\})$。由于 $\mathscr{F}(\boldsymbol{A}^-)\subseteq\mathscr{F}(\boldsymbol{A}^+\setminus\{a\})$，我们得出 $w\notin\mathscr{F}(\boldsymbol{A}^-)$。此外，对于适当的置换矩阵$\Pi,\Pi'$，我们得到 $D\in\mathbb{F}_q^{n-1}$以及 $\chi\in\mathbb{F}_q\setminus\{0\}$，使得

$$\boldsymbol{A}^+\setminus(\partial_{\boldsymbol{A}^+}\boldsymbol{v}\setminus\{a\})=\Pi\cdot\begin{pmatrix}\boldsymbol{A}^- & 0\\ D & \chi\end{pmatrix}\cdot\Pi';\tag{3.5}$$

因此，置换矩阵 Π,Π' 的选取使得它们将 $\boldsymbol{v}$ 列交换到最后一列，并将a 行交换到最后一行。因此，最后一行 (D,χ) 表示 a。现在，通过将对应于 $\mathscr{F}(\boldsymbol{A}^+)\setminus\{\boldsymbol{v}\}$ 中变量节点的所有元素替换为 0，从 D 得到 D_0。然后，根据 **E2**，事实 2.9 表明

$$\operatorname{nul}\begin{pmatrix}\boldsymbol{A}^- & 0\\ D & \chi\end{pmatrix}=\operatorname{nul}(\boldsymbol{A}^-)\qquad\text{and}\qquad\operatorname{nul}\begin{pmatrix}\boldsymbol{A}^- & 0\\ D & \chi\\ 0 & 1\end{pmatrix}=\operatorname{nul}\begin{pmatrix}\boldsymbol{A}^- & 0\\ D & \chi\end{pmatrix}-1.$$

因此，如同断言 3.6 的证明中一样，我们得到 $\boldsymbol{v}\notin\mathscr{F}(\boldsymbol{A}^+\setminus(\partial_{\boldsymbol{A}^+}\boldsymbol{v}\setminus\{a\}))$。因此，根据 (2.1)，$\mathtt{m}_{a\to\boldsymbol{v}}(\boldsymbol{A}^+)=\mathtt{u}$. □

命题 *2.3* 的证明。 断言 3.4–3.8 直接推出

$$\sum_{i=1}^{m}\sum_{j=1}^{n}\mathbb{1}\left\{\mathtt{m}_{v_j\to a_i}(\boldsymbol{A}^+)\neq\hat{\mathtt{m}}_{v_j\to a_i}(\boldsymbol{A}^+)\right\}=o(n)\qquad\text{and}\qquad\sum_{i=1}^{m}\sum_{j=1}^{n}\mathbb{1}\left\{\mathtt{m}_{a_i\to v_j}(\boldsymbol{A}^+)\neq\hat{\mathtt{m}}_{a_i\to v_j}(\boldsymbol{A}^+)\right\}=o(n),$$

由此得到 (2.6)。类似地，(2.7) 可由断言 3.4–3.6 得出。

最后，鉴于 (2.7)，要证明 (2.8)，只需考虑指标 j 满足 $\mathrm{j}\notin\mathscr{F}(\mathrm{A}^\dagger)$ 的变量 $\mathrm{v\,j}$。因此，设 $\mathrm{j},\mathrm{j}'\in[\mathrm{n}]\setminus\mathscr{F}(\mathrm{A}^\dagger)$ 是两个不同的指标，且 $\{\mathrm{i},\mathrm{j}\}$ 不是 $\mathrm{A}^\dagger$ 的真关系；推论 2.2 表明，至多有 $\mathrm{o}(\mathrm{n}^2)$ 个有序对 j,j' 不满足这一性质。于是，投影 $\sigma\in\mathrm{A}$ 的核$^\dagger\mapsto(\sigma_j,\sigma_{j'})\in\mathbb{F}_q^2$ 是满同态。因此，对任意 $\mathrm{s},\mathrm{t}\in\mathbb{F}_q^2$，有 $\left|\{\sigma\in\mathrm{A}\text{ 的核}^\dagger\colon\sigma_i=\mathrm{s},\sigma_j=\mathrm{t}\}\right|=\mathrm{q}^{-2}|\mathrm{A}\text{ 的核}^\dagger|$。因此，若随机抽取 $\boldsymbol{\sigma}^\dagger\in\mathrm{A}$ 的核†，则对于 $(1-\boldsymbol{\alpha}+\mathrm{o}(1))^2\mathrm{n}^2$ 个有序对 $\mathrm{j},\mathrm{j}'\notin\mathscr{F}(\mathrm{A}^\dagger)$，随机变量 $\boldsymbol{\sigma}^\dagger\mathrm{j},\boldsymbol{\sigma}^\dagger\mathrm{j}'$ 相互独立且服从均匀分布。于是，切比雪夫不等式表明，给定 $\mathscr{E}$对所有 $\mathrm{s}\in\mathbb{F}_q$，我们有

$$|\{j\in[n]\setminus\mathscr{F}(\boldsymbol{A}^\dagger)\colon\boldsymbol{\sigma}_j^\dagger=s\}|=(1-\boldsymbol{\alpha}+o(1))|)n/q\qquad\text{w.h.p.},$$

由此得到 (2.8)。 □

3.3. **命题 2.4 的证明**。 证明所采用的论证与命题 2.3 的证明大体相似。主要区别在于，我们将考虑一对均匀随机选取的变量节点 $(\boldsymbol{v},\boldsymbol{v}')$，而不是单个变量节点。首先，我们估计 $|\Delta_{z,\ell}(\mathtt{m}_{\cdot\to\cdot}(\boldsymbol{A}^\dagger))\times\Delta_{z',\ell'}(\mathtt{m}_{\cdot\to\cdot}(\boldsymbol{A}^\dagger))|$ 关于 z、$z'\in\{\mathtt{u},\mathtt{s},\mathtt{f}\}$、$\ell\in\mathscr{D}(z)$ 和 $\ell'\in\mathscr{D}(z')$ 的大小。与第 3.2 节类似，通过删除所有与 $\boldsymbol{v}\cup\partial_{\boldsymbol{A}^\dagger}\boldsymbol{v}'$ 相邻的校验节点 $a\in\partial_{\boldsymbol{A}^\dagger}$，从 $\boldsymbol{A}^\dagger$ 得到 $\boldsymbol{A}^-$。

事实 3.9。 令 $\boldsymbol{A}^+$ 为通过以下操作从 $\boldsymbol{A}^\dagger$ 得到的矩阵。

> 对所有 $a\in\partial_{\boldsymbol{A}^\dagger}\boldsymbol{v}\cup\partial_{\boldsymbol{A}^\dagger}\boldsymbol{v}'$，独立地将 a 除 $\boldsymbol{v},\boldsymbol{v}'$ 以外的邻居从 $\{v_1,\dots,v_n\}\setminus\{\boldsymbol{v}\}$ 中均匀无放回地重新抽取。

那么$\boldsymbol{A}^\dagger$ 和$\boldsymbol{A}^+$ 的全变差距离为 $o(1)$。

证明。 已知$\boldsymbol{v}$、$\boldsymbol{v}'$在$G(\boldsymbol{A}^\dagger)$和$G(\boldsymbol{A}^+)$中的距离均至少为四，因此$\boldsymbol{A}^\dagger$、$\boldsymbol{A}^+$的 Tanner 图同分布。此外，$\boldsymbol{v}$、$\boldsymbol{v}'$的距离小于四的概率以$n^{-1+o(1)}$为上界。□

计划是推　　导出以下联合概率公式，然后再利用切比雪夫不等式　　y.

引理 3.10。 以高概率，我们有 $\mathbb{P}\left[\boldsymbol{v}\in\Delta_{z,\ell}(\mathtt{m}_{\cdot\to\cdot}(\boldsymbol{A}^+)),\ \boldsymbol{v}'\in\Delta_{z',\ell'}(\mathtt{m}_{\cdot\to\cdot}(\boldsymbol{A}^+))\ |\boldsymbol{A}^\dagger\right]=\bar{\Delta}_{z,\ell}(\boldsymbol{\alpha})\,\bar{\Delta}_{z',\ell'}(\boldsymbol{\alpha})+o(1)$。

为证明引理 3.10，令 $\mathscr{E}'$ 表示以下陈述成立这一事件；令 $\Delta\gg1$ 发散得足够慢。

E0′: 我们有 $|\partial_{\boldsymbol{A}^+}\boldsymbol{v}|=\ell_{\mathtt{uu}}+\ell_{\mathtt{fu}}+\ell_{\mathtt{uf}}+\ell_{\mathtt{ff}}$和 $|\partial_{\boldsymbol{A}^+}\boldsymbol{v}'|=\ell'_{\mathtt{uu}}+\ell'_{\mathtt{fu}}+\ell'_{\mathtt{uf}}+\ell'_{\mathtt{ff}}$。

E1′： 第二邻域 $\partial^2 A^+ v, \partial^2 A^+ v'$ 满足

$$v, v' \notin \partial^2_{A^+} v \cup \partial^2_{A^+} v', \qquad |\partial^2_{A^+} v| = (k-1)|\partial_{A^+} v| \le \Delta, \qquad |\partial^2_{A^+} v'| = (k-1)|\partial_{A^+} v'| \le \Delta.$$

E2′： </style}我们有 $(A^\dagger) \setminus \mathscr{F}(A^-)| = o(n)$ 和 $|\mathscr{F}(A^+) \setminus \mathscr{F}(A^-)| = o(n)$。

E3′： </style}对于所有 $a \in \partial_{A^+} v \cup \partial_{A^+} v'$，我们有 $\mathscr{F}(A^+ \setminus \{a\}) \cap \partial_{A^+} a \setminus \{v, v'\} = \mathscr{F}(A^-) \cap \partial_{A^+} a \setminus \{v, v'\}$。

E4′： </style}对于所有 $v \in \{v, v'\}$ 以及 $a \in \partial_{A^+} v$，我们有 $\mathfrak{m}_{v \to a}(A^+) = \hat{}\mathfrak{m}_{v \to a}(A^+)$，$\mathfrak{m}_{a \to v}(A^+) = \hat{}\mathfrak{m}_{a \to v}(A^+)$.

因此，**E0′**保证v、v'的度与 ℓ、ℓ' 中各项之和相匹配。此外，**E1′**确保v、v'之间的距离至少为四，且它们的第二邻域无环。进一步地，**E2′**保证A^-、$A^\dagger$、A^+中的冻结变量数量大致相同。特别地，**E3′**要求v、v'的第二邻域中的冻结变量在A^+和A^-中一致。最后，**E4**假定接触v、v'的消息在 WP 更新 (2.2) 下保持不变。

断言 3.11. 我们有 $\mathbb{P}\left[\mathscr{E}' \mid \mathbf{E0}'\right] = 1 - o(1)$ 并且

$$\mathbb{P}\left[\mathbf{E0}'\right] = \mathbb{P}\left[\mathrm{Po}(d) = \ell_{\mathtt{uu}} + \ell_{\mathtt{fu}} + \ell_{\mathtt{uf}} + \ell_{\mathtt{ff}}\right] \mathbb{P}\left[\mathrm{Po}(d) = \ell'_{\mathtt{uu}} + \ell'_{\mathtt{fu}} + \ell'_{\mathtt{uf}} + \ell'_{\mathtt{ff}}\right] + o(1). \tag{3.6}$$

证明。 估计式 (3.6) 是事实 2.10 的直接推论。关于给定 **E0′** 时 $\mathscr{E}'$ 的概率，按照断言 3.4 证明中的相同论证，可由事实 2.10、推论 2.2 和推论 3.2 得出 **E1′–E3′**。此外，由命题 2.3 和事实 3.9 的式 (2.7) 可得 **E4′**。□

引理 *3.10* 的证明。 设 $X = |\partial_{A^+} v|$、$X' = |\partial_{A^+} v'|$ 分别为v、v' 的度。此外，设

$$X_{\mathtt{f}} = \sum_{a \in \partial_{A^+} v} \mathbb{1}\{\partial_{A^+} a \setminus \{v\} \subseteq \mathscr{F}(A^-)\}, \quad X_{\mathtt{u}} = X - X_{\mathtt{f}}, \quad X'_{\mathtt{f}} = \sum_{a \in \partial_{A^+} v'} \mathbb{1}\{\partial_{A^+} a \setminus \{v'\} \subseteq \mathscr{F}(A^-)\}, \quad X'_{\mathtt{u}} = X' - X'_{\mathtt{f}}.$$

另外，设 $\mathscr{X} = \{X_{\mathtt{f}} = \ell_{\mathtt{ff}} + \ell_{\mathtt{fu}}、X_{\mathtt{u}} = \ell_{\mathtt{uf}} + \ell_{\mathtt{uu}}\}$ 和 $\mathscr{X}' = \{X'_{\mathtt{f}} = \ell'_{\mathtt{ff}} + \ell'_{\mathtt{fu}}、X'_{\mathtt{u}} = \ell'_{\mathtt{uf}} + \ell'_{\mathtt{uu}}\}$。我们将论证命题 2.3 和断言 3.11 蕴含

$$\mathbb{P}\left[v \in \Delta_{z,\ell}(\mathfrak{m}_{\cdot \to \cdot}(A^+)), v' \in \Delta_{z',\ell'}(\mathfrak{m}_{\cdot \to \cdot}(A^+)) \mid \mathscr{E}'\right] = \mathbb{P}\left[\mathscr{X} \cap \mathscr{X}' \mid \mathscr{E}'\right] + o(1). \tag{3.7}$$

事实上，WP 不动点性质 E4′确保，变量 v, v′发出的 WP 消息由传入消息决定。此外，**E3′** 保证，对于每个 $a \in \partial_{A^+}$ v，我们都有 $\mathfrak{m}_{a \to v}(A^+) = \mathtt{f}$ 当且仅当 $\partial_{A^+} a \setminus \{v\} \subseteq \mathscr{F}(A^-)$，对 v′也同样如此。因此，(2.2)、(2.3) 和 (2.4) 表明，在 $\mathscr{E}'$ 上，随机变量 $X_{\mathtt{f}}, X_{\mathtt{u}}, X'_{\mathtt{f}}, X'_{\mathtt{u}}$ 捕捉了传入消息$\mathfrak{m}_{\cdot \to v}(A^+), \mathfrak{m}_{\cdot \to v'}(A^+)$所提供的关键信息，由此得到 (3.7)。

进一步，我们声称，若$A^\dagger$ 满足**E0′**，则

$$\mathbb{P}\left[\mathscr{X} \cap \mathscr{X}' \mid A^\dagger\right] = \alpha^{(k-1)(\ell_{\mathtt{fu}} + \ell_{\mathtt{ff}} + \ell'_{\mathtt{fu}} + \ell'_{\mathtt{ff}})} (1 - \alpha^{k-1})^{\ell_{\mathtt{uu}} + \ell_{\mathtt{uf}} + \ell'_{\mathtt{uu}} + \ell'_{\mathtt{uf}}} + o(1); \tag{3.8}$$

因为根据构造，v、v'的新二阶邻居是均匀选取的。因此，由于**E2′**，任一特定二阶邻居属于 $\mathscr{F}(A^-)$的概率等于 $\alpha + o(1)$；又由于**E1′**，这些事件渐近独立。最后，我们结合 (3.6)、(3.7) 和 (3.8) 完成证明。□

为了估计集合 $\Gamma_{z,\ell}(\mathfrak{m}_{\cdot \to \cdot}(A^\dagger))$ 的大小，我们令 a, a' 为一对随机选取的不同校验节点。令 $A^\#$ 为通过独立地重新抽样 a, a' 的邻居而从 $A^\dagger$ 得到的矩阵。那么，$A^\#$ 和 $A^\dagger$ 同分布。类比引理 3.10，我们证明如下结论。

引理 3.12. 设 $z, z' \in \{\mathtt{u}, \mathtt{f}, \mathtt{s}\}$，并设 $\ell \in \mathscr{G}(z), \ell' \in \mathscr{G}(z')$。以高概率有

$$\mathbb{P}\left[a \in \Gamma_{z,\ell}(\mathfrak{m}_{\cdot \to \cdot}(A^\#)), a' \in \Gamma_{z',\ell'}(\mathfrak{m}_{\cdot \to \cdot}(A^\#)) \mid A^\dagger\right] = \bar{\Gamma}_{z,\ell}(\alpha) \bar{\Gamma}_{z',\ell'}(\alpha) + o(1).$$

证明。 考虑以下事件 $\mathscr{A}$：

A1：邻域 $\partial_{A^\#} \mathtt{a}, \partial_{A^\#} \mathtt{a}'$ 不相交。A2：有 $|\mathscr{F}(\mathtt{A}^\#) \setminus \mathscr{F}(\mathtt{A}^\dagger \setminus \{\mathtt{a}, \mathtt{a}'\})| = \mathtt{o(n)}$，且 $|\mathscr{F}(\mathtt{A}^\dagger) \setminus \mathscr{F}(\mathtt{A}^\dagger \setminus \{\mathtt{a}, \mathtt{a}'\})| = \mathtt{o(n)}$。A3：有 $\mathscr{F}(\mathtt{A}^\# \setminus \{\mathtt{a}\}) \cap \partial_{A^\#} \mathtt{a} = \mathscr{F}(\mathtt{A}^\dagger \setminus \{\mathtt{a}, \mathtt{a}'\}) \cap \partial_{A^\#} \mathtt{a}$，且 $\mathscr{F}(\mathtt{A}^\# \setminus \{\mathtt{a}'\}) \cap \partial_{A^\#} \mathtt{a}' = \mathscr{F}(\mathtt{A}^\dagger \setminus \{\mathtt{a}, \mathtt{a}'\}) \cap \partial_{A^\#} \mathtt{a}'$。A4：对所有 $\mathtt{v} \in \partial_{A^\#} a$我们有 $\mathfrak{m}_{a \to v}(A^\#) = \hat{}\mathfrak{m}_{a \to v}(A^\#)$，并且对所有 $v \in \partial_{A^\#} a'$，我们都有 $\mathfrak{m}_{a' \to v}(A^\#) = \hat{}\mathfrak{m}_{a' \to v}(A^\#)$.

那么，推论 2.2、命题 2.3 和推论 3.2 表明

$$\mathbb{P}[\mathscr{A}] = 1 - o(1). \tag{3.9}$$

进一步，令

$$\boldsymbol{Y}_{\mathtt{f}} = |\partial_{\boldsymbol{A}^{\#}} \boldsymbol{a} \cap \mathscr{F}(\boldsymbol{A}^{\dagger} \setminus \{\boldsymbol{a}, \boldsymbol{a}'\})|, \qquad \boldsymbol{Y}_{\mathtt{u}} = k - \boldsymbol{Y}_{\mathtt{f}}, \qquad \boldsymbol{Y}'_{\mathtt{f}} = |\partial_{\boldsymbol{A}^{\#}} \boldsymbol{a}' \cap \mathscr{F}(\boldsymbol{A}^{\dagger} \setminus \{\boldsymbol{a}, \boldsymbol{a}'\})|, \qquad \boldsymbol{Y}'_{\mathtt{u}} = k - \boldsymbol{Y}'_{\mathtt{f}}.$$

另设 $\mathscr{Y} = \{\boldsymbol{Y}_{\mathtt{f}} = \ell_{\mathtt{ff}} + \ell_{\mathtt{fu}}\}$ 和 $\mathscr{Y}' = \{\boldsymbol{Y}'_{\mathtt{f}} = \ell'_{\mathtt{ff}} + \ell'_{\mathtt{fu}}\}$。我们断言

$$\mathbb{P}\left[\boldsymbol{a} \in \Gamma_{z,\ell}(\mathfrak{m}_{\cdot\to\cdot}(\boldsymbol{A}^{\#})), \boldsymbol{v}' \in \Gamma_{z',\ell'}(\mathfrak{m}_{\cdot\to\cdot}(\boldsymbol{A}^{\#})) \mid \mathscr{A}\right] = \mathbb{P}\left[\mathscr{Y} \cap \mathscr{Y}' \mid \mathscr{A}\right] + o(1); \tag{3.10}$$

A4 表明，$\boldsymbol{a},\boldsymbol{a}'$ 发给其邻居的消息由传入消息通过 (2.2) 决定。此外，**A3** 保证，对于 $v \in \partial_{\boldsymbol{A}^{\#}} \boldsymbol{a}$，有 $\mathfrak{m}_{v\to\boldsymbol{a}}(\boldsymbol{A}^{\#}) = \mathtt{f}$ 当且仅当 $v \in \mathscr{F}(\boldsymbol{A}^{\dagger} \setminus \{\boldsymbol{a}, \boldsymbol{a}'\})$，对于 $v' \in \partial_{\boldsymbol{A}^{\#}} \boldsymbol{a}'$，结论也类似。

最后，由于 $\boldsymbol{A}^{\#}$ 是通过重新抽样 $\boldsymbol{a},\boldsymbol{a}'$ 的邻域得到的，**A1–A2** 表明

$$\mathbb{P}\left[\mathscr{Y} \cap \mathscr{Y}' \mid \boldsymbol{A}^{\dagger}\right] = \boldsymbol{\alpha}^{\ell_{\mathtt{fu}} + \ell_{\mathtt{ff}} + \ell'_{\mathtt{fu}} + \ell'_{\mathtt{ff}}} (1-\boldsymbol{\alpha})^{\ell_{\mathtt{uu}} + \ell_{\mathtt{uf}} + \ell'_{\mathtt{uu}} + \ell'_{\mathtt{uf}}} + o(1). \tag{3.11}$$

因此，由 (3.9)–(3.11) 可得所述断言。 □

命题 *2.4* 的证明。 该命题由事实 2.10、引理 3.10 和 3.12 以及切比雪夫不等式得出。 □

4. 矩计算

本节证明命题 2.5 和推论 2.6，并完成定理 1.2 的证明。我们的主要工具是矩计算。具体而言，我们将计算 $\alpha \in [0,1]$ 的 α-扩展数量的均值 $\boldsymbol{X}_{\alpha}$。关键在于，定义 (2.22)–(2.23) 不仅规定了由 (2.16)–(2.21) 给出的正确「淬火」统计量，还规定了 WP 不动点性质 (2.5) 的一个近似版本，因此接下来的计算结果既紧确又相对简洁。这一点体现在最终重新得到 (1.1) 中的函数 $\Phi_{d,k}$。

4.1. **计数 WP 不动点**。我们首先计算 α-WP 不动点的期望数量，为此采用随机二部 Tanner 图的配对模型。为此，我们以由变量节点的度 $d_{\boldsymbol{A}^{\dagger}}(v_j)$ 和 $\boldsymbol{t}$ 生成的 σ-代数 $\mathfrak{D}$ 为条件。给定 $\mathfrak{D}$，令

$$\mathfrak{V} = \bigcup_{j=1}^{n} \{v_j\} \times [d_{\boldsymbol{A}^{\dagger}}(v_j)] \qquad \text{and} \qquad \mathfrak{F} = \{b_1 \cup \cdots \cup b_{\boldsymbol{t}}\} \cup \bigcup_{i=1}^{m} \{a_i\} \times [k]$$

分别为变量克隆和校验克隆集合；此处 $b_1,\dots,b_{\boldsymbol{t}}$ 表示第 2.1 节中的钉扎操作所诱导的校验节点。*pairing* 是一个双射 $\pi : \mathfrak{V} \to \mathfrak{F}$。令 $\mathfrak{P}$ 为所有配对组成的集合。和往常一样，我们通过随机抽取一个 $G(\boldsymbol{\pi})$- 均匀配对，并将克隆收缩为单个顶点，来构造一个 Tanner 图。与随机图 $G(\boldsymbol{A}^{\dagger})$ 不同，该图可能含有重边。然而，众所周知，一旦我们以事件 $\mathfrak{S}$ 为条件，即 $G(\boldsymbol{\pi})$ 是简单图，$G(\boldsymbol{\pi})$ 的分布就与 $G(\boldsymbol{A}^{\dagger})$ 的分布一致。此外，沿着 [19,Chapter 9] 中的思路进行常规论证，可得以下结论。

事实 4.1. 对于任意 $d > 0, k \geq 3$，以高概率有 $\mathbb{P}[\mathfrak{S} \mid \mathfrak{D}] = \Omega(1)$。

为了计算 $G(\boldsymbol{\pi})$ 的 α-WP 不动点的期望数量，我们计算配对 $\pi \in \mathfrak{P}$ 的总数，以及克隆上适当的、取值于 $\{\mathtt{u},\mathtt{f}\}$ 的标注。具体而言，一个 α-*cover* $(\pi,\mathfrak{p})$ 由一个配对 π 和一个映射 $\mathfrak{p} : \mathfrak{V} \cup \mathfrak{F} \to \{\mathtt{u},\mathtt{f}\}^2, (x,h) \mapsto \mathfrak{p}(x,h) = (\mathfrak{p}_1(x,h), \mathfrak{p}_2(x,h))$ 组成，并满足以下条件。

COV1: 对于所有 $(x,h) \in \mathfrak{V} \cup \mathfrak{F}$，都有 $(\mathfrak{m}_1(\pi(x,h)), \mathfrak{m}_2(\pi(x,h))) = (\mathfrak{m}_2(x,h), \mathfrak{m}_1(x,h))$。

COV2: 对于除 $o(n)$ 个以外的所有有序对 (v_j,l)，满足 $j \in [n]$ 且 $l \in [d_{\boldsymbol{A}^{\dagger}}(v_i)]$ 的情形，都有

$$\mathfrak{p}_2(v_j, l) = \begin{cases} \mathtt{f} & \text{if } \mathfrak{p}_1(v_j, h) = \mathtt{f} \text{ for some } h \in [d_{\boldsymbol{A}^{\dagger}}(v_j)] \setminus \{l\}, \\ \mathtt{u} & \text{otherwise.} \end{cases}$$

COV3: 除 $o(n)$ 个有序对 (a_i,l) 外，对于满足 $i \in [m]$ 且 $l \in [d_{\boldsymbol{A}^{\dagger}}(a_i)]$ 的所有有序对，我们都有

$$\mathfrak{p}_2(a_i, l) = \begin{cases} \mathtt{f} & \text{if } \mathfrak{p}_1(a_i, h) = \mathtt{f} \text{ for all } h \in [k] \setminus \{l\}, \\ \mathtt{u} & \text{otherwise.} \end{cases}$$

COV4： 对于任意 $z \in \{\mathtt{f},\mathtt{s},\mathtt{u}\}$，$\ell = (\ell_{\mathtt{uu}}, \ell_{\mathtt{uf}}, \ell_{\mathtt{fu}}, \ell_{\mathtt{ff}}) \in \mathscr{L}$，若 $i \in [m]$ 且 $j \in [n]$，令

$$\mathfrak{p}(v_j) = \begin{cases} \mathtt{f} & \text{if } \mathfrak{p}_1(v_j, l) = \mathtt{f} \text{ for at least two } l \in [d_{\boldsymbol{A}^\dagger}(v_j)], \\ \mathtt{s} & \text{if } \mathfrak{p}_1(v_j, l) = \mathtt{f} \text{ for precisely one } l \in [d_{\boldsymbol{A}^\dagger}(v_j)], \\ \mathtt{u} & \text{otherwise,} \end{cases} \tag{4.1}$$

$$\mathfrak{p}(a_i) = \begin{cases} \mathtt{f} & \text{if } \mathfrak{p}_1(a_i, l) = \mathtt{f} \text{ for all } l \in [d_{\boldsymbol{A}^\dagger}(a_i)], \\ \mathtt{s} & \text{if } \mathfrak{p}_1(a_i, l) = \mathtt{f} \text{ for all but precisely one } l \in [d_{\boldsymbol{A}^\dagger}(a_i)], \\ \mathtt{u} & \text{otherwise,} \end{cases} \tag{4.2}$$

$$\boldsymbol{\Delta}(z, \ell) = \sum_{i=1}^{n} \mathbb{1}\{\mathfrak{p}(v_j) = z\} \prod_{x,y \in \{\mathtt{u},\mathtt{f}\}} \mathbb{1}\big\{\big|\{l \in [d_{\boldsymbol{A}^\dagger}(v_j)] : \mathfrak{p}_1(v_j, l) = x,\, \mathfrak{p}_2(v_j, l) = y\}\big| = \ell_{xy}\big\}, \tag{4.3}$$

$$\boldsymbol{\Gamma}(z, \ell) = \sum_{i=1}^{m} \mathbb{1}\{\mathfrak{p}(a_i) = z\} \prod_{x,y \in \{\mathtt{u},\mathtt{f}\}} \mathbb{1}\big\{\big|\{l \in [d_{\boldsymbol{A}^\dagger}(a_i)] : \mathfrak{p}_1(a_i, l) = x,\, \mathfrak{p}_2(a_i, l) = y\}\big| = \ell_{xy}\big\}. \tag{4.4}$$

Then

$$\boldsymbol{\Delta}(z, \ell) = n\bar{\Delta}_{z,\ell}(\alpha) + o(n), \qquad \boldsymbol{\Gamma}(z, \ell) = m\bar{\Gamma}_{z,\ell}(\alpha) + o(n). \tag{4.5}$$

条件 **COV1** 保证与配对克隆相关联的标签保持一致。此外，**COV2–COV3**在 $(\pi, \mathfrak{p})$ 上施加不动点条件 (2.5)。类似地，标签 (4.1)–(4.2) 模仿定义 (2.3)–(2.4)。最后，(4.3)–(4.5) 确保标签/消息的统计量符合正确的"淬火"值 (2.16)–(2.21)（见命题 2.4）。下面的引理确定了 $\mathfrak{C}(\alpha)$ 中所有 α-覆盖的数量。

引理 4.2. 以高概率有 $\mathfrak{C}(\alpha) = \exp(o(n))(km)!k!^m \prod_{i=1}^{n} d_{\boldsymbol{A}^\dagger}(v_i)!$。

为证明引理 4.2，我们先给出以下直接的计数公式。

断言 4.3. 当 y, y' 遍历 $\{\mathtt{u},\mathtt{f}\}$，$z$ 遍历 $\{\mathtt{u},\mathtt{s},\mathtt{f}\}$ 且 ℓ 遍历 $\mathscr{L}$ 时，以高概率有

$$\begin{aligned} \frac{|\mathfrak{C}(\alpha)|}{(km)!} = \exp(-nH(\mathrm{Po}(d)) + o(n)) &\binom{n}{n(\bar{\Delta}_{z,\ell}(\alpha))_{z,\ell}} \binom{m}{m(\bar{\Gamma}_{z,\ell}(\alpha))_{z,\ell}} \\ &\cdot \binom{km}{\big(n\sum_{z,\ell} \ell_{yy'} \bar{\Delta}_{z,\ell}(\alpha)\big)_{y,y'}}^{-1} \prod_{z,\ell} \binom{\ell_{\mathtt{uu}} + \ell_{\mathtt{uf}} + \ell_{\mathtt{fu}} + \ell_{\mathtt{ff}}}{\ell_{\mathtt{uu}}, \ell_{\mathtt{uf}}, \ell_{\mathtt{fu}}, \ell_{\mathtt{ff}}}^{n\bar{\Delta}_{z,\ell}(\alpha) + m\bar{\Gamma}_{z,\ell}(\alpha)}. \end{aligned} \tag{4.6}$$

证明。 前两个多项式系数计算了按照 (4.5) 规定的频次为变量节点/校验节点分配标签的方式数。不过，第一个多项式系数隐含地计算了变量节点度的分配方式，而我们正是以此为条件；这是因为 $\ell_{\mathtt{uu}} + \ell_{\mathtt{fu}} + \ell_{\mathtt{uf}} + \ell_{\mathtt{ff}}$ 等于相应变量的度。为纠正这一重复计数，我们除以该多项式系数

$$\binom{n}{(|\{i \in [n] : d_{\boldsymbol{A}^\dagger}(v_i) = h\}|)_{h \geq 0}}. \tag{4.7}$$

但是，根据事实 2.10，变量节点度渐近服从泊松分布，因此 (4.7) 等于 $\exp(nH(\mathrm{Po}(d)) + o(n))$，以高概率成立。(4.6) 第二行中的第一个多项式系数计算了满足 **COV1** 的克隆匹配方式数。最后一个因子计算了为各个变量节点/校验节点的克隆分配标签的方式数。最后，$\exp(o(n))$ 误差项吸收了 (4.3)–(4.4) 中的近似误差。□

断言 4.4. 令

$$\mathfrak{l}_1 = \mathbb{E}[\log(\mathrm{Po}(d)!)], \qquad \mathfrak{l}_2 = -\sum_{z,\ell} \bar{\Delta}_{z,\ell}(\alpha) \log(\ell_{\mathtt{uu}}!\ell_{\mathtt{uf}}!\ell_{\mathtt{fu}}!\ell_{\mathtt{ff}}!), \qquad \mathfrak{l}_3 = -\frac{d}{k}\sum_{z,\ell} \bar{\Gamma}_{z,\ell}(\alpha) \log(\ell_{\mathtt{uu}}!\ell_{\mathtt{uf}}!\ell_{\mathtt{fu}}!\ell_{\mathtt{ff}}!),$$

$$\mathfrak{h}_1 = H(\bar{\delta}(\alpha, z))_z + H(\mathrm{Po}(d(1-\alpha^{k-1}))) + \bar{\delta}(\alpha, f) H(\mathrm{Po}_{\geq 2}(d\alpha^{k-1})),$$

$$\mathfrak{h}_2 = \frac{d}{k}\left[H(\bar{\gamma}(\alpha, z))_z + \bar{\gamma}(\alpha, \mathtt{u}) H(\mathrm{Bin}_{\geq 2}(k, 1-\alpha))\right], \quad \mathfrak{h}_3 = d\left[H(\mathrm{Be}(\alpha^{k-1})) - H(\mathrm{Be}(\alpha))\right], \quad \mathfrak{h}_4 = -H(\mathrm{Po}(d))$$

以高概率我们有 $\frac{1}{n}\log|\mathfrak{C}(\alpha)| - \log((k!)^m (km)! \prod_{i=1}^{n} d_{\boldsymbol{A}^\dagger}(v_i)!)$
$= \mathfrak{l}_1 + \mathfrak{l}_2 + \mathfrak{l}_3 + \mathfrak{h}_1 + \mathfrak{h}_2 + \mathfrak{h}_3 + \mathfrak{h}_4 + o(1).$

证明。结合 (2.14)–(2.21)，由斯特林公式可得

$$\frac{1}{n}\log\binom{n}{n(\bar{\Delta}_{z,\ell}(\alpha))_{z,\ell}} = H(\bar{\delta}(\alpha,z))_z + H(\mathrm{Po}(d(1-\alpha^{k-1}))) + \bar{\delta}(\alpha,f)H(\mathrm{Po}_{\geq 2}(d\alpha^{k-1})) + o(1), \tag{4.8}$$

$$\frac{1}{n}\log\binom{m}{m(\bar{\Gamma}_{z,\ell}(\alpha))_{z,\ell}} = \frac{d}{k}\left(H(\bar{\gamma}(\alpha,z))_z + \bar{\gamma}(\alpha,\mathtt{u})H(\mathrm{Bin}_{\geq 2}(k,1-\alpha))\right) + o(1). \tag{4.9}$$

同理，

$$\frac{1}{n}\log\left[\frac{1}{(km)!}\prod_{y,y'}\left(n\sum_{z,\ell}\ell_{y,y'}\bar{\Delta}_{z,\ell}(\alpha)\right)!\right] = -d\left[H(\mathrm{Be}(\alpha)) - H(\mathrm{Be}(\alpha^{k-1}))\right] + o(1). \tag{4.10}$$

此外，

$$\sum_{z,\ell}\bar{\Delta}_{z,\ell}(\alpha)\log\frac{(\ell_{\mathtt{uu}}+\ell_{\mathtt{uf}}+\ell_{\mathtt{fu}}+\ell_{\mathtt{ff}})!}{\ell_{\mathtt{uu}}!\ell_{\mathtt{uf}}!\ell_{\mathtt{fu}}!\ell_{\mathtt{ff}}!} = \mathfrak{l}_1+\mathfrak{l}_2+o(1). \tag{4.11}$$

最后，由于对所有满足 Γ_z 的 ℓ，都有 $\ell_{\mathtt{uu}}+\ell_{\mathtt{uf}}+\ell_{\mathtt{fu}}+\ell_{\mathtt{ff}} = k\ell(\alpha) > 0$，因此我们有

$$-\frac{1}{n}\log((k!)^m) + \frac{m}{n}\sum_{z,\ell}\bar{\Gamma}_{z,\ell}(\alpha)\log\frac{(\ell_{\mathtt{uu}}+\ell_{\mathtt{uf}}+\ell_{\mathtt{fu}}+\ell_{\mathtt{ff}})!}{\ell_{\mathtt{uu}}!\ell_{\mathtt{uf}}!\ell_{\mathtt{fu}}!\ell_{\mathtt{ff}}!} = \mathfrak{l}_3 + o(1). \tag{4.12}$$

结合 (4.8)–(4.12) 与断言 4.3，即完成证明。 □

引理 *4.2* 的证明。令 $\lambda = \alpha^{k-1}d$ 和 $\mu = d-\lambda$。根据事实 2.10，度的经验分布 $(d_{\boldsymbol{A}^\dagger}(v_i))_{i\in[n]}$ 近似服从 $\mathrm{Po}(d)$，结合 (2.14)–(2.21)，以高概率有

$$\mathfrak{l}_1 = \frac{1}{n}\sum_{i=1}^{n}\log(d_{\boldsymbol{A}^\dagger}(v_i)!) + o(1), \quad \mathfrak{l}_2 = -\mathbb{E}\left[\log\left(\mathrm{Po}(\mu)!\right)\right] - \bar{\delta}(\alpha,\mathtt{f})\mathbb{E}\left[\log(\mathrm{Po}_{\geq 2}(\lambda)!)\right] + o(1), \tag{4.13}$$

$$\mathfrak{l}_3 = \frac{d}{k}\bar{\gamma}(\alpha,\mathtt{s})\log(k) + \frac{d}{k}\bar{\gamma}(\alpha,\mathtt{u})\mathbb{E}\left[\log\binom{k}{\mathrm{Bin}_{\geq 2}(k,1-\alpha)}\right] + o(1). \tag{4.14}$$

此外，经过简单的变换可得

$$\mathfrak{h}_1 = d(1-H(\mathrm{Be}(\alpha^{k-1})) - \log d) + \mathbb{E}\left[\log(\mathrm{Po}(\mu)!)\right] + \bar{\delta}(\alpha,\mathtt{f})\mathbb{E}\left[\log(\mathrm{Po}_{\geq 2}(\lambda)!)\right], \tag{4.15}$$

$$\mathfrak{h}_2 = dH(\mathrm{Be}(\alpha)) - \frac{d}{k}\bar{\gamma}(\alpha,\mathtt{s})\log(k) - \frac{d}{k}\bar{\gamma}(\alpha,\mathtt{u})\mathbb{E}\left[\log\binom{k}{\mathrm{Bin}_{\geq 2}(k,1-\alpha)}\right], \tag{4.16}$$

$$\mathfrak{h}_4 = -d(1-\log d) - \mathbb{E}\left[\log(\mathrm{Po}(d)!)\right]. \tag{4.17}$$

该断言由 (4.13)–(4.17) 和断言 4.4 得出。 □

4.2. **命题 2.5 的证明**。引理 4.2 对 α-WP 不动点的数量进行了估计。为了证明命题 2.5，我们现在需要统计这样一些“平衡”赋值的数量：将值赋给 WP 不动点的未冻结变量，并使所有校验节点都满足。因此，设 $(\pi,\mathfrak{p})$ 为一个 α-覆盖。若 $\sigma\in\mathbb{F}_q^n$ 与 $(,)$ 相容，则称其为

$$\sigma_j = 0 \text{ for all } j\in[n] \text{ with } \mathfrak{p}(v_j)\neq\mathtt{u}, \text{ and} \tag{4.18}$$

$$\sum_{\ell\geq 0}\sum_{s\in\mathbb{F}_q\setminus\{0\}}(\ell+1)\left|\sum_{j=1}^{n}\mathbb{1}\{d_{\boldsymbol{A}^\dagger}(v_j)=\ell,\mathfrak{p}(v_j)=\mathtt{u}\}\left(\mathbb{1}\{\sigma_j=s\}-q^{-1}\right)\right| = o(n). \tag{4.19}$$

因此，我们要求变量 v_j 在 $\mathfrak{p}(v_j)=\mathtt{u}$ 时，其取值在 $\mathbb{F}_q$ 上近似均匀分布，即使细分到各个变量度也是如此。此外，配对 $\pi\in\mathfrak{P}$ 通过如下方式诱导出一个矩阵 $A(\pi)$：

$$A_{ij}(\pi) = \mathfrak{A}_{ij}\cdot\mathbb{1}\{\exists l\in[d_{\boldsymbol{A}^\dagger}(v_j),\, h\in[k]:\pi(v_j,l)=(a_i,h)\} \qquad (i\in[m],\, j\in[n]).$$

最后，我们称 σ $\in\mathbb{F}_q^n$ 基本满足 $(\pi,\mathfrak{p})$，如果 $\mathrm{k}A(\pi)\sigma\mathrm{k}_0 = o(n)$。回想一下，$\boldsymbol{\pi}\in\mathfrak{P}$ 表示一个随机配对 .

引理 4.5. 令 $\mathfrak{p}:\mathfrak{V}\cup\mathfrak{F}\to\{\mathtt{u},\mathtt{f}\}$，并令 $\sigma\in\mathbb{F}_q^n$。令 $\mathfrak{C}$ 表示事件：$(\boldsymbol{\pi},\mathfrak{p})$ 是一个 α-覆盖，且 σ 与之相容；令 $\mathfrak{E}$ 表示事件：σ 本质满足。那么，以高概率有 $\mathbb{P}[\mathfrak{E}\mid\mathfrak{C},\mathfrak{D}]\leq q^{-m\bar{\gamma}(\alpha,\mathtt{u})+O(n)}$。

证明。给定 $\mathfrak{C},\mathfrak{D}$，令 $\mathfrak{I}$ 为所有满足以下条件的有序对 $(\mathrm{i},\mathrm{h}) \in [\mathrm{m}] \times [\mathrm{k}]$ 的集合：对于某个变量节点 $\mathrm{v\,j}$，$\boldsymbol{\pi}(\mathrm{i},\mathrm{h}) \in \{\mathrm{v\,j}\} \times \mathbb{N}$，且 $\mathfrak{p}(\mathrm{v}j) = \mathrm{u}$。因此，$\mathfrak{I}$ 包含被未冻结变量击中的校验克隆。此外，令 $\mathscr{I}$ 包含所有满足 $\mathrm{i} \in [\mathrm{m}]$ 且 $\{\mathrm{i}\} \times [\mathrm{k}] \cap \mathfrak{I} \neq ;$ 的 i。给定 $\mathfrak{C},\mathfrak{D},\mathfrak{I}$ 后，剩下的随机性在于哪些未冻结变量克隆与 $\mathfrak{I}$ 匹配。我们的目标是估计在这种随机匹配下，所有校验节点 a_i，$\mathrm{i} \in \mathscr{I}$ 是否最终满足的概率。令 $\boldsymbol{\xi} = (\boldsymbol{\xi}_{ih})_{(i,h)\in\mathfrak{I}}$ 为一个向量，其中包含 σ 下与 $\mathfrak{I}$ 中的克隆匹配的变量的取值。用符号表示，$\boldsymbol{\xi}_{ih} = \sum_{\mathrm{j}\in[\mathrm{n}]} \sigma_j \mathbb{1}\{\boldsymbol{\pi}(\mathrm{a}_i,\mathrm{h}) \in \{\mathrm{v\,j}\} \times \mathbb{N}\}$。

为了研究 $\boldsymbol{\xi}$，我们引入一个辅助随机向量 $\boldsymbol{\chi} = (\boldsymbol{\chi}_{ih})_{(i,h)\in\mathfrak{I}}$，其各分量相互独立且服从均匀分布 $\boldsymbol{\chi}_{ih} \in \mathbb{F}_q$。考虑以下事件

$$\mathfrak{R} = \left\{ \forall s \in \mathbb{F}_q \setminus \{0\} : \sum_{(i,h)\in\mathfrak{I}} \mathbb{1}\{\boldsymbol{\chi}_{ih} = s\} = \sum_{j=1}^{n} \mathbb{1}\{\sigma_j = s\} d_{\boldsymbol{A}^\dagger}(v_j) \right\}, \qquad \mathfrak{X} = \left\{ \sum_{i\in\mathscr{I}} \mathbb{1}\left\{ \sum_{h:(i,h)\in\mathfrak{I}} \boldsymbol{\chi}_{ih} \neq 0 \right\} = o(n) \right\}.$$

给定事件 $\mathfrak{R}$，向量 $\boldsymbol{\xi}$ 和 $\boldsymbol{\chi}$ 同分布。因此，

$$\mathbb{P}[\mathfrak{E} \mid \mathfrak{C},\mathfrak{D}] = \mathbb{P}[\mathfrak{X} \mid \mathfrak{C},\mathfrak{D},\mathfrak{I},\mathfrak{R}]. \tag{4.20}$$

无条件概率 $\mathbb{P}[\mathfrak{X} \mid \mathfrak{C},\mathfrak{D},\mathfrak{I}]$ 和 $\mathbb{P}[\mathfrak{R} \mid \mathfrak{C},\mathfrak{D},\mathfrak{I}]$ 很容易计算。事实上，由于 $\boldsymbol{\chi}_{ih}$ 均匀且相互独立，对于任意 $i \in \mathscr{I}$，事件 $\sum_{h:(i,h)\in\mathfrak{I}} \boldsymbol{\chi}_{ih} = 0$ 以 $1/q$ 的概率发生。因此，

$$\mathbb{P}[\mathfrak{S} \mid \mathfrak{C},\mathfrak{D},\mathfrak{I}] = q^{-|\mathscr{I}|+o(n)}. \tag{4.21}$$

此外，条件 **COV1–COV4** 以及系数 Γ_z、$\ell(\alpha)$ 的定义 (2.19)–(2.21) 保证，给定 $\mathfrak{C}$、$\mathfrak{D}$ 时，$|\mathfrak{I}| = m(\bar{\gamma}(\alpha,\mathrm{u}) + o(1))$ 以高概率成立。因此，(4.21) 变为

$$\mathbb{P}[\mathfrak{S} \mid \mathfrak{C},\mathfrak{D},\mathfrak{I}] = q^{-m\bar{\gamma}(\alpha,\mathrm{u})+o(n)}. \tag{4.22}$$

此外，(4.19) 保证 $\mathbb{P}[\mathfrak{R} \mid \mathfrak{C},\mathfrak{D},\mathfrak{I}] = \exp(o(n))$。结合 (4.20) 和 (4.22)，利用贝叶斯法则可得

$$\mathbb{P}[\mathfrak{E} \mid \mathfrak{C},\mathfrak{D}] = \mathbb{E}[\mathbb{P}[\mathfrak{S} \mid \mathfrak{C},\mathfrak{D},\mathfrak{I},\mathfrak{R}] \mid \mathfrak{C},\mathfrak{D}] \le \mathbb{E}\left[\frac{\mathbb{P}[\mathfrak{S} \mid \mathfrak{C},\mathfrak{D},\mathfrak{I}]}{\mathbb{P}[\mathfrak{R} \mid \mathfrak{C},\mathfrak{D},\mathfrak{I}]} \mid \mathfrak{C},\mathfrak{D} \right] \le q^{-m\bar{\gamma}(\alpha,\mathrm{u})+o(n)},$$

如所需。 □

命题 2.5 的证明。首先，我们将矩阵 $\mathrm{A}^\dagger$ 的 α-WP 不动点数量与 α-覆盖数量联系起来。给定 $\mathfrak{D},\mathfrak{S}$，随机矩阵 $\mathrm{A}(\boldsymbol{\pi})$ 与 $\mathrm{A}^\dagger$ 具有相同的分布。因此，假设 $\mathfrak{m}$ 是矩阵 $\mathrm{A}(\boldsymbol{\pi})$ 的一个 α-WP 不动点。那么 $\mathfrak{m}$ 通过令 $\mathfrak{p}_{\boldsymbol{\pi}}(\mathrm{a}_i,\mathrm{h}) = (\mathfrak{m}_{v_j\to\mathrm{a}_i},\mathfrak{m}_{a_i\to\mathrm{v}j})$ 诱导出一个映射 $\mathfrak{p}_{\boldsymbol{\pi}}: \mathfrak{V}\cup\mathfrak{F} \to \{\mathrm{f},\mathrm{u}\}^2$，其中 $\mathrm{j} \in [\mathrm{n}]$ 是唯一满足 $\boldsymbol{\pi}(\mathrm{a}_i,\mathrm{h}) \in \{\mathrm{v\,j}\} \times \mathbb{N}$ 的指标。类似地，如果 $\boldsymbol{\pi}(\mathrm{v\,j},\mathrm{h}) \in \{\mathrm{a}_i\} \times [\mathrm{k}]$，则 $\mathfrak{p}_{\boldsymbol{\pi}}(\mathrm{v\,j},\mathrm{h}) = (\mathfrak{m}_{a_i\to\mathrm{v}j},\mathfrak{m}_{v_j\to\mathrm{a}_i})$。定义 (2.9)–(2.10) 和 (2.22)–(2.23) 确保 $(\boldsymbol{\pi},\mathfrak{p}_{\boldsymbol{\pi}})$ 满足 COV1–COV4。因此，$(\boldsymbol{\pi},\mathfrak{p}_{\boldsymbol{\pi}})$ 是一个 α-覆盖。

继续之前，我们需要处理一个重复计数问题。具体来说，给定 $\mathfrak{D}$，对于任意矩阵 $\boldsymbol{A}^\dagger$，有 $\Xi = (k!)^m \prod_{j=1}^n d_{\boldsymbol{A}^\dagger}(vj)!$ 个配对 π 可生成 $\boldsymbol{A}^\dagger$，也就是说，满足 $A(\pi) = \boldsymbol{A}^\dagger$。与此同时，配对 π 的总数为 $(km)!$，且给定 $\mathfrak{S}$ 时，$\boldsymbol{A}^\dagger$ 与 $A(\boldsymbol{\pi})$ 同分布。实际上，引理 4.2 对 α-覆盖总数的计数意味着，$\boldsymbol{A}^\dagger$ 的 α-WP 不动点数量 W_α 满足

$$\mathbb{E}[W_\alpha \mid \mathfrak{D}] = \exp(o(n)) \qquad \text{w.h.p.} \tag{4.23}$$

现在考虑 $\mathfrak{m}$ 的一个扩展 σ。那么，σ 与 $(\boldsymbol{\pi},\mathfrak{p}_{\boldsymbol{\pi}})$ 几乎相容，只有 (4.18) 对 $o(n)$ 个指标 $j \in [n]$ 可能不成立。为解决这一问题，令 $\tau_j = \mathbb{1}\{\mathfrak{p}(vj) = \mathrm{u}\}\sigma_j$。这样，$\tau$ 便与 $(\boldsymbol{\pi},\mathfrak{p})$ 相容，而 (2.24) 推出

$$\sum_{j=1}^{n} \mathbb{1}\{\sigma_j \neq \tau_j\} = o(n). \tag{4.24}$$

此外，由于 $\mathrm{e}\ \sigma \in \ker \boldsymbol{A}^\dagger$，事实 2.10 和 (4.24) 得出 $\mathrm{k}A(\boldsymbol{\pi})\tau\mathrm{k}_0 = o(n)$。因此，$\tau$ 本质满足 $(\boldsymbol{\pi},\mathfrak{p}_{\boldsymbol{\pi}})$.

由于 (4.24) 表明，能够产生特定有序对 $(\mathfrak{p}_{\boldsymbol{\pi}},\tau)$ 的原像 $(\mathfrak{m},\sigma)$ 的数量至多为 $\exp(\mathrm{o(n)})$，因此，为了界定 X_α，只需界定给定 $\mathfrak{D}$ 时有序对 $(\mathfrak{p}_{\boldsymbol{\pi}},\tau)$ 的期望数量。估计式 (4.23) 表明，由 α-WP 不动点诱导的 α-覆盖的期望数量至多为 $\exp(\mathrm{o(n)})$。此外，给定 $\mathfrak{p}_{\boldsymbol{\pi}}$，满足条件 (4.19) 的赋值 τ 的数量至多为 $\mathrm{q}^{\bar{\delta}(\alpha,\mathrm{u})\mathrm{n}+\mathrm{o(n)}}$。此外，引理 4.5 表明，这样的 τ 以概率 $\mathrm{q}^{\bar{\gamma}(\alpha,\mathrm{u})\mathrm{m}+\mathrm{o(n)}}$ 本质满足。结合这些估计，并回顾 Φ、$\delta(\alpha,\mathrm{u})$ 和 $\bar{\gamma}(\alpha,\mathrm{u})$ 的定义 (1.1)、(2.14) 和 (2.15)，我们得到

$$\mathbb{E}[\boldsymbol{X}_\alpha \mid \mathfrak{D}] \le q^{\bar{\delta}(\alpha,\mathrm{u})n+\bar{\gamma}(\alpha,\mathrm{u})m+o(n)} = q^{\Phi_{d,k}(\alpha)n+o(n)} \qquad \text{w.h.p.},$$

从而完成证明。 □

4.3. **推论 2.6 的证明**。事实 2.8 表明，对于$d < d_k$，函数 $\Phi_{d,k}(\alpha)$ 在 $\alpha = 0$ 处取得唯一的全局最大值。此外，观察 (1.1) 可知 $\Phi_{d,k}(0) = 1 - d/k$。因此，对于任意$d < d_k$，存在 $\zeta > 0$，使得对于任意固定的 $\xi > 0$，都有$n\max_{\alpha\in[\xi,1]}\Phi(\alpha) < n - m - 3\zeta n$。因此，命题 2.3 和命题 2.5 结合马尔可夫不等式表明

$$\mathbb{P}\left[\operatorname{nul} \boldsymbol{A}^{\dagger} \geq n - m - 2\zeta n \mid \boldsymbol{\alpha} \in [\xi, 1]\right] = \mathbb{P}\left[\max_{\alpha\in[\xi,1]} \boldsymbol{X}_{\alpha} \geq q^{n-m-\zeta n}\right] + o(1) = o(1). \tag{4.25}$$

但是，由于$\boldsymbol{A}^{\dagger}$ 有$m + o(n)$行，因此 $\operatorname{nul} \boldsymbol{A}^{\dagger} \geq n - m + o(n)$。因此，(4.25)表明 $\boldsymbol{\alpha} < \xi$ 以高概率成立。令$\xi \to 0$ 随$n \to \infty$充分缓慢地变化，我们由此得出 $\boldsymbol{\alpha} = o(1)$ 以高概率成立。因此，该断言由命题 2.3 得出。

4.4. **引理 2.7 的证明**。回忆一下，对于 $\sigma \in \mathbb{F}_q^n$，我们令 $\rho(\sigma) = (\rho_s(\sigma))_{s\in\mathbb{F}_q}$，其中 $\rho_s(\sigma) = \frac{1}{n}\sum_{j=1}^{n} \mathbb{1}\{\sigma_j = s\}$。令 $\mathscr{R} = \{\rho(\sigma) : \sigma \in \mathbb{F}_q^n\}$ 为所有可能的 $\rho(\sigma)$-向量构成的集合。此外，对于 $\chi = (\chi_1, \dots, \chi_n) \in \mathbb{F}_q^n$，令 $\chi^{\perp} = \{\sigma \in \mathbb{F}_q^n : \sum_{j=1}^{n} \sigma_j\chi_j = 0\}$。以下断言给出了一个随机向量属于 $\chi^{\perp}$ 的近似概率；该随机向量的各个分量独立地从一个与均匀分布$q^{-1}\mathbb{1}$ 接近的分布$r \in \mathscr{R}$ 中抽取。

断言 4.6。设 $\chi \in \mathbb{F}_q^n$是一个满足 $|\operatorname{supp}\chi| = k \geq 3$ 的向量。那么，对于满足 $\|r - q^{-1}\mathbb{1}\| < \varepsilon$ 的 r，我们有一致地

$$\varphi_{\chi}(r) = \sum_{\sigma\in\chi^{\perp}} \prod_{s\in\mathbb{F}_q} r_s^{n\rho_s(\sigma)} = \frac{1}{q} + O(\varepsilon^3) \qquad as\, \varepsilon \to 0.$$

证明。令 $\mathscr{X}(\chi) = \{\sigma \in \mathbb{F}^{\operatorname{supp}\chi}{}_q : \sum_{j\in\operatorname{supp}\chi} \sigma_j\chi_j = 0\}$，并且对于 $\sigma \in \mathscr{X}(\chi)$ 和 $s \in \mathbb{F}_q$，令 $R_s(\sigma) = |\{j \in \operatorname{supp}\chi : \sigma_j = s\}|$。那么 $\varphi_{\chi}(r) = f_{\chi}(r)$，其中

$$f_{\chi}(r) = \sum_{\sigma\in\mathscr{X}(\chi)} \prod_{s\in\mathbb{F}_q} r_s^{R_s(\sigma)}.$$

我们将把 $f_{\chi}(r)$ 展开到二阶。显然，$f_{\chi}(q^{-1}\mathbb{1}) = q^{-1}$，因为 $\mathscr{X}(\chi) \subseteq \mathbb{F}^{\operatorname{supp}\chi}{}_q$是一个余维为一的线性子空间，因此 $|\mathscr{X}(\chi)| = \mathbb{F}_q^{k-1}$。此外，$f_{\chi}(r)$ 的偏导数为

$$\frac{\partial f_{\chi}}{\partial r_t} = \sum_{\sigma\in\mathscr{X}(\chi)} R_t(\sigma) r_t^{R_t(\sigma)-1} \prod_{s\in\mathbb{F}_q\setminus\{t\}} r_s^{R_s(\sigma)} \qquad (t \in \mathbb{F}_q), \tag{4.26}$$

$$\frac{\partial^2 f_{\chi}}{\partial r_t \partial r_u} = \sum_{\sigma\in\mathscr{X}(\chi)} R_t(\sigma) R_u(\sigma) r_t^{R_t(\sigma)-1} r_u^{R_u(\sigma)-1} \prod_{s\in\mathbb{F}_q\setminus\{t,u\}} r_s^{R_s(\sigma)} \qquad (t, u \in \mathbb{F}_q,\, t \neq u), \tag{4.27}$$

$$\frac{\partial^2 f_{\chi}}{\partial r_t^2} = \sum_{\sigma\in\mathscr{X}(\chi)} R_t(\sigma)(R_t(\sigma) - 1) r_t^{R_t(\sigma)-2} \prod_{s\in\mathbb{F}_q\setminus\{t\}} r_s^{R_s(\sigma)} \qquad (t \in \mathbb{F}_q)。 \tag{4.28}$$

为了在$r = q^{-1}\mathbb{1}$处计算 (4.26)，我们注意到，对于每个$t \in \mathbb{F}_q$和满足$k = |\operatorname{supp}\chi| \geq 3$的$j \in \operatorname{supp}\chi$，仿射子空间 $\{\sigma \in \mathscr{X}(\chi) : \sigma_j = t\}$ 的维数为$k - 2$。因此，

$$\left.\frac{\partial f_{\chi}}{\partial r_t}\right|_{r=q^{-1}\mathbb{1}} = q^{1-k} \sum_{j\in\operatorname{supp}\chi} \sum_{\sigma\in\mathscr{X}(\chi)} \mathbb{1}\{\sigma_j = t\} = \frac{k}{q}. \tag{4.29}$$

类似地，由于当t、$u \in \mathbb{F}_q$以及j、$j' \in \operatorname{supp}\chi$满足$j \neq j'$时，仿射子空间 $\{\sigma \in \mathscr{X}(\chi) : \sigma_j = t, \sigma_{j'} = u\}$ 的维数为$k - 3$，在$r = q^{-1}\mathbb{1}$ 处计算 (4.27)–(4.28) 可简化为

$$\left.\frac{\partial^2 f_{\chi}}{\partial r_t \partial r_u}\right|_{r=q^{-1}\mathbb{1}} = \left.\frac{\partial^2 f_{\chi}}{\partial^2 r_t}\right|_{r=q^{-1}\mathbb{1}} = \frac{k(k-1)}{q}. \tag{4.30}$$

此外，所有三阶偏导数均保持有界，即

$$\frac{\partial^3 f_{\chi}}{\partial r_s \partial r_t \partial r_u} = O(1) \qquad \text{for all } s, t, u \in \mathbb{F}_q. \tag{4.31}$$

最后，由于对每个 $r \in \mathscr{R}$，都有$\sum_{s\in\mathbb{F}_q} r_s = 1$，且雅可比矩阵 $Df_{\chi}(q^{-1}\mathbb{1})$ 和海森矩阵 $D^2_{\chi}(q^{-1}\mathbb{1})$ 中非零特征值对应的特征子空间都由 1 张成，因此由 (4.29)–(4.31) 和泰勒公式可得该断言。□

引理 *2.7* 的证明。 给定$\boldsymbol{t}$的值后，随机矩阵 $\boldsymbol{A}^{\dagger}$ 由 m 行支撑大小为 k 的行以及 $\boldsymbol{t}$ 个单变量行组成。这些行在随机意义下相互独立。因此，断言 4.6 表明，对于任意$r \in \mathscr{R}$ 以及任何满足 $\rho(\sigma) = r$的 $\sigma \in \mathbb{F}_q^n$，我们有

$$\mathbb{P}\left[\sigma \in \ker \boldsymbol{A}^{\dagger} \mid \boldsymbol{t}\right] = q^{-m-\boldsymbol{t}} \exp(O(n\|r - q^{-1}\mathbb{1}\|_1^3)). \tag{4.32}$$

此外，我们回顾一下，熵函数$H(r)$的展开式为

$$H(r) = \log q - \frac{q}{2}\sum_{s\in\mathbb{F}_q}(r_s - q^{-1})^2 + O(\|r - q^{-1}\mathbb{1}\|_1^3). \tag{4.33}$$

组　　合并 (4.32)–(4.33) 并应用拉普拉斯方法，我们便可在 $\varepsilon > 0$ 足够小时得到：

$$\begin{aligned}&\mathbb{E}\left|\ker \boldsymbol{A}^{\dagger} \cap \{\sigma \in \mathbb{F}_q^n : \|\rho(\sigma) - q^{-1}\mathbb{1}\|_1 < \varepsilon\} \mid \boldsymbol{t}\right| \\ &\quad = (1+o(1))q^{n-m-\boldsymbol{t}} \sum_{r\in\mathscr{R}:\|r-q^{-1}\mathbb{1}\|_1<\varepsilon} \frac{\exp(-q\|r-q^{-1}\mathbb{1}\|_2^2/2 + O(\|r-q^{-1}\mathbb{1}\|_1^3))}{\sqrt{(2\pi n)^{q-1}\prod_{s\in\mathbb{F}_q} r_s}} \sim q^{n-m-\boldsymbol{t}},\end{aligned}$$

如所述。 □

5. 定理 1.2 (II) 的证明

定理 1.2 第二部分的证明基于数学物理中的插值法 [25]。此前已有研究应用插值法来估计更一般模型 [7]，中随机矩阵的秩；事实上， [7] 中得到的秩上界蕴含定理 1.2(ii)。尽管如此，为求完整，我们在此给出一个简化版的插值论证，专门针对特定的随机矩阵模型$\boldsymbol{A}^{\dagger}$。

基本思路是构造一个由 $\theta \in [0,1]$ 参数化的矩阵族 $\boldsymbol{A}^{\dagger}(\theta)$。首个矩阵 $\boldsymbol{A}^{\dagger}(0)$（本质上）与随机矩阵 $\boldsymbol{A}^{\dagger}$ 重合，而在另一端 $\boldsymbol{A}^{\dagger}(1)$，我们有一个零度容易显式计算的矩阵。接着，我们将对 $\mathbb{E}[\mathrm{nul}\boldsymbol{A}^{\dagger}(\theta)]$ 求导，以比较 $\mathbb{E}[\mathrm{nul}\,\boldsymbol{A}^{\dagger}(0)]$ 和 $\mathbb{E}[\mathrm{nul}\boldsymbol{A}^{\dagger}(1)]$。由此，我们得到 $\boldsymbol{A}^{\dagger}(0)$ 的零度下界，进而得到 $\boldsymbol{A}^{\dagger}$ 的零度下界。由于 $\mathrm{nul}(\boldsymbol{A}^{\dagger}) + \mathrm{rk}(\boldsymbol{A}^{\dagger}) = n$，这个零度下界便转化为 $\boldsymbol{A}^{\dagger}$ 的秩的所需上界。

插值矩阵族 $\mathrm{A}^{\dagger}(\theta)$ 的构造如下。设 $\mathrm{m}_{\theta},\mathrm{m}'_{\theta}$ 为两个相互独立的泊松变量，其均值分别为 $(1-\theta)\mathrm{dn/k}$ 和 $\mathrm{d}\theta\alpha_{\mathrm{f}}^{k-1}\mathrm{n}$；这里 $\alpha_{\mathrm{f}} = \alpha_{\mathrm{f}}(\mathrm{d},\mathrm{k}) > 0$ 是 $\phi_{d,k}$ 的最大不动点（见事实 2.8）。$\mathrm{m}_{\theta},\mathrm{m}'_{\theta}$ 也都与均匀随机变量 $\mathrm{t} \in [\mathrm{T}]$ 相互独立。随机矩阵 $\mathrm{A}^{\dagger}(\theta)$ 的大小为 $(\mathrm{m}_{\theta} + \mathrm{m}'_{\theta} + \mathrm{t}) \times \mathrm{n}$。与 A 的定义 (1.2) 一样，$\mathrm{A}^{\dagger}(\theta)$ 的前 m_{θ} 行的元素为

$$\boldsymbol{A}^{\dagger}_{ij}(\theta) = \mathfrak{A}_{ij}\mathbb{1}\{j \in \boldsymbol{e}_i\} \qquad\qquad (i \in [\boldsymbol{m}_{\theta}], j \in [n]),$$

其中，$(\boldsymbol{e}_i)_{i\ge1}$ 是由k 个n] 元素均匀随机子集构成的族；这些集合彼此独立，且与$\boldsymbol{m}_t$、$\boldsymbol{m}'_t$和$\boldsymbol{t}$独立。此外，对于$\boldsymbol{m}_t < i \le 1 + \boldsymbol{m}'_t + \boldsymbol{t}$，$\boldsymbol{A}^{\dagger}$的第$i$行在均匀随机列$j \in [n]$, 中包含一个 1，其余元素均为零。这些 1 元素的位置彼此独立抽取，且与其他所有因素独立。

引理 5.1。 我们有 $\mathbb{E}[\mathrm{nul}\,\boldsymbol{A}^{\dagger}(0)] = \mathbb{E}[\mathrm{nul}\,\boldsymbol{A}] + o(n)$ 且 $\mathbb{E}[\mathrm{nul}\,\boldsymbol{A}^{\dagger}(1)] = n\exp(-d\alpha_{\mathrm{f}}^{k-1}) + o(n)$。

证明。 根据构造，$\boldsymbol{A}^{\dagger}(0)$的前$\boldsymbol{m}_0 \wedge m$ 行与$\boldsymbol{A}$同分布。此外，以高概率有$\boldsymbol{m}_0 = m + o(n)$。由于添加或删除一行至多会使零度改变 1，因此第一个断言得证。

关于第二个断言，注意到 $\boldsymbol{A}^{\dagger}(1)$ 的各行均为全零行，只有一个元素为 1，而该元素的位置独立且均匀随机。因此，$\boldsymbol{A}^{\dagger}(1)$ 的零度就是全零列的数量。此外，由于 $\mathbb{E}[\boldsymbol{m}'_1] = d\alpha_{\mathrm{f}}^{k-1}n$，每列非零元素的期望数量为 $d\alpha_{\mathrm{f}}^{k-1} + o(1)$。由于 $\boldsymbol{m}'_{\theta}$ 是一个泊松变量，我们预计有 $n\exp(-d\alpha_{\mathrm{f}}^{k-1} + o(1))$ 个全零列。□

插值法的主要步骤是计算导数 $\frac{\partial}{\partial\theta}\mathbb{E}[\mathrm{nul}\,\boldsymbol{A}(\theta)]$。

引理 5.2. 我们有 $\frac{1}{n}\frac{\partial}{\partial\theta}\mathbb{E}[\mathrm{nul}\,\boldsymbol{A}(\theta)] \le -d\alpha_{\mathrm{f}}^{k-1} + d\,k\,(k-1)\alpha_{\mathrm{f}}^{k} + d\,k + o(1)$.

证明。 由于 $\boldsymbol{m}_\theta, \boldsymbol{m}'_\theta$ 是泊松变量，我们计算得

$$\frac{1}{n}\frac{\partial}{\partial\theta}\mathbb{P}\left[\boldsymbol{m}_\theta = m\right] = \frac{d}{k}\left[\mathbb{P}\left[\boldsymbol{m}_\theta = m\right] - \mathbb{P}\left[\boldsymbol{m}_\theta = m-1\right]\right], \quad \frac{1}{n}\frac{\partial}{\partial\theta}\mathbb{P}\left[\boldsymbol{m}'_\theta = m\right] = d\alpha_{\mathtt{f}}^{k-1}\left[\mathbb{P}\left[\boldsymbol{m}'_\theta = m-1\right] - \mathbb{P}\left[\boldsymbol{m}'_\theta = m\right]\right].$$

因此，

$$\begin{aligned}\frac{1}{n}\frac{\partial}{\partial\theta}\mathbb{E}[\operatorname{nul}\boldsymbol{A}(\theta)] &= \frac{1}{n}\sum_{m,m'\geq 0}\mathbb{E}\left[\operatorname{nul}\boldsymbol{A}^\dagger(\theta)\mid \boldsymbol{m}_\theta = m, \boldsymbol{m}'_\theta = m'\right]\frac{\partial}{\partial\theta}\mathbb{P}\left[\boldsymbol{m}_\theta = m\right]\mathbb{P}\left[\boldsymbol{m}'_\theta = m'\right] \\ &= d\alpha_{\mathtt{f}}^{k-1}\sum_{m'\geq 0}\left[\mathbb{E}\left[\operatorname{nul}\boldsymbol{A}^\dagger(\theta)\mid \boldsymbol{m}'_\theta = m'+1\right] - \mathbb{E}\left[\operatorname{nul}\boldsymbol{A}^\dagger(\theta)\mid \boldsymbol{m}'_\theta = m'\right]\right]\mathbb{P}\left[\boldsymbol{m}'_\theta = m'\right] \\ &\quad - \frac{d}{k}\sum_{m\geq 0}\left[\mathbb{E}\left[\operatorname{nul}\boldsymbol{A}^\dagger(\theta)\mid \boldsymbol{m}_\theta = m+1\right] - \mathbb{E}\left[\operatorname{nul}\boldsymbol{A}^\dagger(\theta)\mid \boldsymbol{m}_\theta = m\right]\right]\mathbb{P}\left[\boldsymbol{m}_\theta = m\right]. \end{aligned} \tag{5.1}$$

于是，通过再添加一行，从 $\boldsymbol{A}^\dagger(\theta)$ 得到 $\boldsymbol{A}^\dagger_+(\theta)$，该行恰有一个非零元素，且其位置是从所有位置中均匀随机选取的，并且与其他所有因素独立。令 $\boldsymbol{a}^+$ 表示这一新行。同理，通过添加行 $\boldsymbol{a}^-$，从 $\boldsymbol{A}^\dagger(\theta)$ 得到 $\boldsymbol{A}^\dagger_-(\theta)$，其元素为

$$\boldsymbol{a}^-_j = \mathfrak{A}_{\boldsymbol{m}_\theta+1\, j}\mathbb{1}\{j \in \boldsymbol{e}_{m_\theta+1}\}.$$

于是，由 (5.1) 可得

$$\frac{1}{dkn}\frac{\partial}{\partial\theta}\mathbb{E}[\operatorname{nul}\boldsymbol{A}(\theta)] = k\alpha_{\mathtt{f}}^{k-1}\mathbb{E}\left[\operatorname{nul}(\boldsymbol{A}^\dagger_+(\theta)) - \operatorname{nul}(\boldsymbol{A}^\dagger(\theta))\right] - \mathbb{E}\left[\operatorname{nul}(\boldsymbol{A}^\dagger_-(\theta)) - \operatorname{nul}(\boldsymbol{A}^\dagger(\theta))\right]. \tag{5.2}$$

令 $\boldsymbol{\alpha}_\theta = |\mathscr{F}(\boldsymbol{A}^\dagger(\theta))|/n$。我们声称

$$\mathbb{E}\left[\operatorname{nul}(\boldsymbol{A}^\dagger_+(\theta)) - \operatorname{nul}(\boldsymbol{A}^\dagger(\theta))\right] = -\mathbb{E}\left[1-\boldsymbol{\alpha}_\theta\right]. \tag{5.3}$$

事实上，令 $\boldsymbol{j}^+ \in [n]$ 表示 $\boldsymbol{a}^+$ 中非零元素的位置。那么，将 <style id='a'>a$^+$ 添加到 $\boldsymbol{A}^\dagger(\theta)$ 后，零度降低当且仅当 $j^+ \notin \mathscr{F}(\boldsymbol{A}^\dagger(\theta))$。由于 $\boldsymbol{j}^+$ 是均匀随机选取的，且与 $\boldsymbol{A}^\dagger(\theta)$ 独立，因此得到 (5.3)。

此外，我们声称

$$\mathbb{E}\left[\operatorname{nul}(\boldsymbol{A}^\dagger_-(\theta)) - \operatorname{nul}(\boldsymbol{A}^\dagger(\theta))\right] = -\mathbb{E}\left[1-\boldsymbol{\alpha}_\theta^k\right] + o(1). \tag{5.4}$$

为此，令 $\mathscr{E}_\theta$ 表示 $\mathrm{A}^\dagger(\theta)$ 是 (o(1),k)-自由的事件。由于 $\mathrm{A}^\dagger(\theta)$ 的构造包含了 t 个随机一元方程，如同钉扎引理（引理 2.1）中那样，我们有 $\mathbb{P}[\mathscr{E}_\theta] = 1-\mathrm{o}(1)$。此外，由于 a^- 与 $\mathrm{A}^\dagger(\theta)$ 相互独立，在事件 $\mathscr{E}_\theta$ 下，a^- 的非零元素所处的位置 $1 \leq \mathrm{j}^-_1 < \cdots < \mathrm{j}^-\mathrm{k} \leq \mathrm{n}$ 构成 $\mathrm{A}^\dagger(\theta)$ 的真关系的概率为 o(1)。因此，假设 $\mathrm{j}^-_1, \ldots, \mathrm{j}^-\mathrm{k}$ 不构成真关系。于是，除非 $\mathrm{j}^-_1, \ldots, \mathrm{j}^-\mathrm{k} \in \mathscr{F}(\mathrm{A}^\dagger(\theta))$，否则添加行 a^- 后零度会下降。由于 $\mathbb{P}\left[\mathrm{j}^-_1, \ldots, \mathrm{j}^-\mathrm{k} \in \mathscr{F}(\mathrm{A}^\dagger(\theta)) \mid \mathrm{A}^\dagger(\theta)\right] = \boldsymbol{\alpha}_\theta^k + \mathrm{o}(1)$，我们得到 (5.4)。

结合 (5.2)–(5.4)，得到

$$\frac{1}{dkn}\frac{\partial}{\partial\theta}\mathbb{E}[\operatorname{nul}\boldsymbol{A}(\theta)] = \mathbb{E}\left[1-\boldsymbol{\alpha}_\theta^k - k\alpha_{\mathtt{f}}^{k-1}(1-\boldsymbol{\alpha}_\theta)\right] + o(1). \tag{5.5}$$

为完成证明，我们注意到

$$1-\boldsymbol{\alpha}_\theta^k - k\alpha_{\mathtt{f}}^{k-1}(1-\boldsymbol{\alpha}_\theta) + \left(k\alpha_{\mathtt{f}}^{k-1} - (k-1)\alpha_{\mathtt{f}}^k - 1\right) = -\boldsymbol{\alpha}_\theta^k + k\boldsymbol{\alpha}_\theta\alpha_{\mathtt{f}}^{k-1} - (k-1)\alpha_{\mathtt{f}}^k \leq 0, \tag{5.6}$$

因为 $X^k - kXY^{k-1} + (k-1)Y^k \geq 0$ 对所有 X、$Y \in [0,1]$ 以及所有 $k \geq 2$ 均成立。结论由 (5.5) 和 (5.6) 得出。 □

定理 *1.2(ii)* 的证明。 设 $d > d_k$。在 $\theta \in [0,1]$ 上积分，根据事实 2.8 和引理 5.1，我们得到

$$\frac{1}{n}\mathbb{E}[\operatorname{nul}\boldsymbol{A}^\dagger] \geq \Phi_{d,k}(\alpha_{\mathtt{f}}) + o(1) > 1 - d/k. \tag{5.7}$$

此外，阿祖马–霍夫丁不等式表明，$\operatorname{nul}\boldsymbol{A}^\dagger$ 高度集中，因为增加或删除一行最多只会使零度改变 1。因此，由于 $\boldsymbol{A}^\dagger$ 是通过向 $\boldsymbol{A}$ 添加 $o(n)$ 行得到的，我们得出：以高概率，$n^{-1}\operatorname{nul}\boldsymbol{A} \geq \Phi_{d,k}(\alpha_{\mathtt{f}}) + o(1)$。因此，由 (5.7) 可知，以高概率，$\operatorname{rk}\boldsymbol{A} < m - \Omega(n)$。□

参考文献

[1] D. Achlioptas, M. Molloy：随机线性方程解空间的几何结构。《随机结构与算法》46 (2015) 197–231。[2] D. Achlioptas, A. Naor, Y. Peres：困难优化问题中相变位置的严格确定。《自然》435 759–764。[3] M. Aizenman, R. Sims, S. Starr：SK自旋玻璃模型的扩展变分原理。《物理评论B辑》68 (2003) 214403。[4] P. Ayre, A. Coja-Oghlan, P. Gao, N. Müller：随机线性方程的可满足性阈值。《Combinatorica》40 (2020) 179–235。[5] A. Coja-Oghlan, O. Cooley, M. Kang, J. Lee, J. Ravelomanana：稀疏奇偶校验矩阵。第 33 届 SODA 论文集 (2022) 822–833。[6] A. Coja-Oghlan, P. Gao, M. Hahn-Klimroth, J. Lee, N. Müller, M. Rolvien：稀疏随机矩阵的满秩条件。arXiv 2112.14090 (2021)。[7] A. Coja-Oghlan, A. Ergür, P. Gao, S. Hetterich, M. Rolvien：稀疏随机矩阵的秩。第 31 届 SODA 论文集 (2020) 579–591。[8] O. Cooley, J. Lee, J. Ravelomanana：警告传播：稳定性与次临界性。arXiv:2111.15577 (2021)。[9] C. Cooper：具有给定度序列的随机超图的核。《随机结构与算法》25 (2004) 353–375。[10] C. Cooper, A. Frieze, W. Pegden：关于随机二元矩阵的秩。《电子组合学杂志》26 (2019) P4.12。[11] N. Creignou, H. Daude, O. Dubois：随机 k-XOR 公式可满足性阈值的近似。arXiv:cs/0106001 (2001)。[12] M. Dietzfelbinger, A. Goerdt, M. Mitzenmacher, A. Montanari, R. Pagh, M. Rink：通过 XORSAT 得到布谷鸟哈希的紧阈值。第 37 届 ICALP 论文集 (2010) 213–225。[13] J. Ding, A. Sly, N. Sun：大 k 情形下可满足性猜想的证明。《数学年刊》196 (2022) 1–388。[14] O. Dubois, J. Mandler：3-XORSAT 阈值。第 43 届 FOCS 论文集 (2002) 769–778。[15] D. Fernholz, V. Ramachandran：稀疏随机图中的核与连通性。UTCS技术报告 TR04-13 (2004)。[16] A. Goerdt, L. Falke：k-XORSAT 以外的可满足性阈值。第 7 届俄罗斯国际计算机科学研讨会论文集 (2012) 148–159。[17] M. Ibrahimi, Y. Kanoria, M. Kraning, A. Montanari：随机XORSAT公式的解集。《应用概率年刊》25 (2015) 2743–2808。[18] S. Janson, M. Luczak：k核问题的一个简单解法。《随机结构与算法》30 (2007) 50–62。[19] S. Janson, T. Luczak, A. Rucinski：随机图。威利出版社 (2000)。[20] J.H. Kim：随机图的泊松克隆模型。国际数学家大会论文集 (2006) 873–897。[21] M. Mézard, A. Montanari：信息、物理与计算。牛津大学出版社 (2009)。[22] M. Mézard, F. Ricci-Tersenghi, R. Zecchina：稀释p自旋模型和 XORSAT 问题的两种解。《统计物理学杂志》111 (2003) 505–533。[23] M. Molloy：随机超图和布尔公式中的核。《随机结构与算法》27 (2005) 124–135。[24] A. Montanari：从随机稀疏观测中估计随机变量。《欧洲电信汇刊》19(4) (2008) 385–403。[25] D. Panchenko, M. Talagrand：稀释平均场自旋玻璃模型的界。《概率论及相关领域》130 (2004) 319–336。[26] B. Pittel, G. Sorkin：k-XORSAT 的可满足性阈值。《组合数学、概率与计算》25 (2016) 236–268。[27] B. Pittel, J. Spencer, N. Wormald：随机图中巨型k核的突然出现。《组合理论杂志》B辑67 (1996) 111–151。[28] P. Raghavendra, N. 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 SODA 论文集 (2012) 373–387。[29] O. Riordan：k核与分枝过程。《组合数学、概率与计算》17 (2008) 111–136。AMIN COJA-OGHLAN, amin.coja-oghlan@tu-dortmund.de, 多特蒙德工业大学，计算机科学学院，OTTO-HAHN-ST 12号，DORTMUND 44227，德国。MIHYUN KANG, kang@math.tu-graz.at, 格拉茨工业大学，离散数学研究所，STEYRERGASSE 30号，8010 GRAZ，奥地利。LENA KRIEG, lena.krieg@tu-dortmund.de, 多特蒙德工业大学，计算机科学学院，OTTO-HAHN-ST 12号，DORTMUND 44227，德国。MAURICE ROLVIEN, maurice.rolvien@tu-dortmund.de, 多特蒙德工业大学，计算机科学学院，OTTO-HAHN-ST 12号，DORTMUND 44227，德国。